The concept of structural-parametric synthesis and optimization of information systems in conditions of destructive impacts

S S Kochedykov and S Yu Kobzistyy

Federal state educational institution of the higher education "Voronezh institute of the Federal Penitentiary Service", 1a, Irkutskaya, Voronezh, 396072, Russia

E-mail: infosec36@mail.ru

Abstract. Currently, information systems have become an integral part of critical information infrastructure. In particular in the energy sector, developed and successfully operated information system in the management of technological, industrial and security measures. Systems in this class are subject to destructive impact and above all by cybercriminals seeking to infiltrate their database, block, or disable electronic equipment control and management. The main feature behind the concept of structural-parametric synthesis and optimization of information systems is that the systems of this class are objects for a formal description, which there is no unambiguous analytical dependencies. In addition, there are significant limitations on the choice of the optimization parameters that cannot be precisely determined at the stage of examination of the object of the synthesis, since they depend on the design solutions. Therefore, structural-parametric synthesis of the information systems cannot be reduced to the solution of the optimization math problems. Requires a special approach, which is able to resolve the difficulties due to the operational management of the course of the synthesis.

1. Introduction

Implementation of information systems intended for the safe and reliable operation, as part of the critical information infrastructure [1] it is impossible to implement a one-act, is an evolutionary process of complex gradual increase of their capacity due to consistent optimization of the structure, the gradual improvement of software and hardware environment, constantly upgrading mathematical, linguistic and information support, and improving the means and methods of protection from various kinds of destructive impacts, including cyber attacks [2-5]. When implementing this concept, the Central of the variety of problems associated with the creation and development of information systems of critical information infrastructure as a complex system, the problem of structurally-parametric synthesis of high quality which largely depends on the efficiency of the critical information infrastructure.

Study of some aspects of the problem of structural and parametric synthesis, and optimization applied to information systems of various functional purposes are devoted to the work [6,7]. However, it should be noted that the development of information systems in this class still carried out without involving a system of ideology-based borrowing or simply compiling ready-made software and hardware products. For the considered class of systems has not received proper development of the Central issues of intellectual support of management decision-making, including development of models and algorithms for structure optimization, analysis of system integrity and functional stability of the software in terms
of destructive impacts, as well as methods and means of representation of knowledge about external and internal environment. Without solving these issues of structural and parametric synthesis is only a partial methodological support, limited evaluation of individual indicators of the type of security, reliability, timeliness, accuracy, etc. In the result the expenditure of energy, time and money on the development of information systems is continuously growing, and their quality does not correspond to time requirements. We will analyse the specifics of the construction and operation of information systems as objects of structural and parametric synthesis and optimization in part: the functional composition, design principles and system properties. The results of the analysis provide a starting base for subsequent development of substantive provisions of methodology of structural and parametric synthesis and optimization of this class of systems. In the interests of system-parametric synthesis of the information systems proposed to proceed from the fact that this class of systems should be considered as a composite object (figure 1) paired with technical, informational, intellectual, and linguistic software components for a comprehensive informational and intellectual support of the operational activities of officials of state authorities and institutions at all levels throughout the Russian Federation related to the activity of the critical information infrastructure.

Thus when carrying out systematic and parametric synthesis of such a facility should take into account the features of self-organization, low predictability, openness, large scale, complexity, and multilevel.

Determined that the underlying structure of information systems should make the following basic principles: systemacity, complexity, hierarchy, modular open architecture, standardization and harmonization, availability, phasing of development, creation and implementation, coordination of technical decisions, operational supervision of the progress of a project while minimizing risks.

Comprehensive implementation of these principles will allow you to create information systems that meet: the information security doctrine of the Russian Federation, national security strategy of the Russian Federation and the strategy of information society development of the Russian Federation on 2017-2030, etc. [8-12].
It is stated that information systems is subject to cyber attacks, by which cybercriminals will try to get into the database of the penitentiary system, block or destroy electronic objects of control and protection, to disrupt service of escort, to destabilize the work of the computer system of territorial bodies criminally-Executive system.

In these circumstances, in the course of structural-parametric synthesis of information systems come to the fore complex issues of information security by:

1) early detection, identification and monitoring of destructive impacts on information systems;

2) operational control of operational functionality of information systems in conditions of destructive impacts;

3) optimization of the structure, traffic and procedure of the regulations on the information systems in terms of destructive impacts;

4) assess the impact of cyber attacks on the operation of information systems and management protection measures.

The main feature behind the concept of structural-parametric synthesis and optimization of information systems is that the systems of this class are objects (technical systems, network structure, software components, databases and knowledge, information security, etc.) for a formal description, which there is no unambiguous analytical dependencies. In addition, there are significant limitations on the choice of the optimization parameters that cannot be precisely determined at the stage of examination of the object of the synthesis, since they depend on the design solutions. Therefore, structural-parametric synthesis of the information systems cannot be reduced to the solution of the optimization math problems (even if arbitrarily complex). Requires a special approach, which is able to resolve the difficulties due to the operational management of the course of the synthesis.

Better to such requirement meets the system approach, the essence of which in our case is that problems of structural-parametric synthesis of information systems and optimization of their parameters are not decided once and for iterative scheme (figure 2) "from General to specific and from specific to General" with the use of quantitative and qualitative criteria of social, functional, ergonomic, pragmatic, technical, technological, economic and operational types (table 1).

Target oriented synthesis is determined at the stage of formation of the image of the system and is formalized at the stage of development and approval of technical specifications. This allows you to build the whole process of structural-parametric synthesis as a systematic iteration of cyclic search of rational technical solutions under the given constraints.

Figure 2. The General scheme of structural-parametric synthesis of information systems on the basis of a systematic approach.
Table 1. Criteria of effectiveness of information systems.

| Quality  | Criteria                                                                 |
|----------|--------------------------------------------------------------------------|
| social   | Improving the quality and increasing the efficiency of information support officers |
| functional | Functional completeness; structural completeness; the lack of structural redundancy; the lack of management duplication; information redundancy; information sufficiency; resource provision; resource consistency; structural connectivity |
| ergonomic | Usability of user interface; comfort                                    |
| pragmatic | Improving the quality of information and intellectual support of activities of officials and bodies of criminal Executive system |
| technical | The level of technical sophistication of the information system and its components (subsystems, systems), their compliance with national and international standards |
| technological | The level of technology used in the design of the information system and its components, as well as the level of technological development of the designed system |
| economic  | Financial and material costs for the creation (improvement) of the information system and its constituent parts, operating costs, needs and actual funding and lending |
| operating | The convenience of carrying out various organizational-technical actions (settings, preventive, routine maintenance, etc.) |

The theoretical basis developed in this paper the approach to structural and parametric synthesis and optimization of information systems is based on the fact that this process is obviously recognized conflict with many uncertain factors [13-17]. Moreover, conflicts occur not only in the internal target of contradictory structural and parametric synthesis, but also in the existence of multiple contradictions between customer, user, developers, hackers and other individuals somehow related to the design, development and operation of information systems. To parry these factors have been proposed: in the case of probabilistic parametric uncertainties using the experimental probability distributions or their approximations; in case of uncertainty of the linguistic and structural properties to use the apparatus of fuzzy set theory and logico-linguistic modeling; in case of uncertainties, subjective character to use a special procedure for task decomposition of the process of structural-parametric synthesis of information systems; in case of uncertainty of the conflict-reflective properties to use the apparatus of game theory and the theory of conflict.
2. Develop modeling and algorithmic tools, providing a solution to the complex problem of optimization of the structure of information systems in the course of its structural and parametric synthesis

Consider a typical geographically distributed information systems consisting of nodes for receiving, processing and transmitting information at different levels, connected by lines [18]. It is assumed that each packet of information transferred in this system can move from node to node in four directions: up, down, right and left. The choice of the direction of travel (apart from the addressee) is defined by engineering parameters on the nodes. The route of the packet of information named for a complete list of nodes in which it falls, indicating the lines along which it passes from the sender to the recipient. We assume that the processing time of an information package on the site depends on the nature and intensity of destructive impacts, the type and priority information, and the current load on the node and the operation of information systems. In addition, we take into account the fact that there may be restrictions on the possibility of parallel processing of heterogeneous information due to, for example, the requirements of the security regime. Then the problem of optimization of structure of information systems is to build a network information flows, in which, despite the destructive impact of each package of information will reach from the source to the recipient during the not exceeding a preassigned critical value $T_k^{KR}$:

$$M^*: \forall_{k \in K} \left[ T_k \leq T_k^{KR} \right],$$

subject to constraints on throughput of nodes for receiving, processing and transmitting information, the possibility of its parallel processing taking into account the conditions prevailing as the result of destructive impacts.

Problem (1) belongs to a class of task scheduling of large dimension with discrete variables and constraints expressed mainly in conceptual form. As you know, the direct use of mathematical methods to solve such tasks efficiently, since it is necessary to introduce rather strict assumptions and assumptions entailing a loss of a substantial part of the problem. The transition to expert methods because of massive information systems just does not give a constructive outcome. You have to resort to the decomposition of the problem into its component parts and the sequential solution of subproblems. However, this path is dangerous because the mechanical separation of a complex task into its component parts deprives its integrity. This breaks down the internal relations and the model, which is expected to solve the problem becomes inadequate the real object. Thus, when optimizing the structure of information systems in conditions of destructive impacts is a contradiction, the essence of which is that it is impossible without decomposition of the solution of the problem, but the decomposition may lead (and often leads) to its wrong decision. To resolve this contradiction by presenting the proposed optimized system in a composite space:

$$\Omega = \left( L \times \Psi \times F \right),$$

where: $L$ – a topological space in which information systems are exposed to destructive influences, is represented as a system with nodes receiving, processing and transmitting information and communication between them; $\Psi$ – information space, in which the same information systems is represented as a system consisting of dynamic packets of information, given their characteristics (name, type, priority, recipient, source, etc.), and facilities engaged in the transmission, processing, storing and receiving information; $F$ – functional space in which the information systems represented by the system functions performed by software modules.

The difference between these spaces is not only essential representation of optimized systems, but primarily in the languages used to describe its various aspects. To describe a system in a topological space we shall use the language of graph theory as the most adequate to describe topological aspects of optimized systems in the information – logical language of predicate calculus of first order, functional
language of differential calculus and the elements of the theory of fuzzy sets. As a result, the problem (1) can be represented as a composition of three tasks such as topology, and functional information, the joint solution gives the solution to the General problem. Thus, the correctness of the decomposition of the problem (1) is provided for valid combinations of spaces $L$, $\Psi$ and $F$.

*Optimization of the structure of information systems at the topological level* is reduced to minimize the points of intersection of the graph describing the topology of the network: the smaller the intersection is, the smaller the number of network components is drawn into the process of transmission, processing and reception of information, and the less time the system spends in the exercise of their functions. To solve this problem, we developed an original algorithm to coplanar conversion of the graph to the form with minimal number of crossings of its edges that is different from the standard procedures that eliminated the most time-consuming operations of multiplying and inverse matrices.

*Optimization of the structure of information systems in the information space* is reduced to the search of such switching routes on the network, which, despite the destructive impact, delivery time information to the recipients does not exceed some critical value. The influence of destructive influences taken into account by the introduction of the engineering parameters at the network nodes, determining: direction of the transfer packet information from one network node to another; the processing time of the packet of information in the network nodes; security nodes information systems from destructive influences; prohibitions on simultaneous processing of information packets in the network nodes for reasons of protection against leaks.

*Optimization of the structure of information systems in the functional space* is decomposed into three partial tasks: optimization from the point of view of elimination (lock) destructive impacts; optimization from the point of view of preventative measures on its facilities; optimization in the conditions of deficit of resources. To solve these problems using discrete situational network in conjunction with the logic of predicates of first order and elements of the theory of fuzzy sets.

The algorithms proposed to be embedded in information systems as a support tool for activities of operational calculus in solving their problems of optimization of system structure in terms of destructive influences, both internal and external.

3. Development of a method and algorithm for analyzing the integrity of system software of information systems

Under the system integrity software refers to its ability to maintain its structure in the presence of the destructive effects of both external and internal nature [19-21]. The need to analyse the integrity of software. On the information systems due to at least two circumstances. First, the specificity of the systems of this class lies in the fact that their software components are developed by different teams of artists using various techniques and have different views on the use of software environments. In the end (and this is confirmed by the practice) when integrating software products into the system, despite these agreements, there are numerous internal differences that destroys the integrity of the final product.

The second reason is because almost all the elements of information systems are objects of destructive attacks by hackers, insiders, phreakers, crackers and other subjects of computer crime. The result (despite protective measures) in their software environment embedded malware, destructive software structure. These reasons force throughout the life cycle of information systems to analyze the integrity of its software and to take measures aimed at its preservation. The utilitarian importance of this task is obvious. As experience shows, the main costs of creating the software, information systems, and in the course of its operation, associated with the analysis of the integrity and elimination of internal structural contradictions are created, borrowed and illegally implemented software products. Currently, this task is viewed more as the art of system programming than a strict science based on mathematical models for analysis and optimization. As a result, it is solved by the method of trial and error with partial involvement of the assessment models for calculating individual indicators of the type of security, reliability, timeliness, accuracy etc.

We proceed from the fact that software information systems is a set of software modules: a) developed the system; b) purchased from a third party; c) introduced by cyber criminals during the
operation. We assume that each of the software modules specified by a set of actual or projected characteristics, namely: functions, control, and resource needs. Let the violation of the integrity of software information systems is connected with destructive factors of the following types:

- loss functional, informational, resource and managerial fullness due to disabling or blocking nodal software modules;
- the emergence of the information of lack or excess due to the disruption of blocking of analyzers and controllers, supplying data about the internal condition or external environment;
- the chaotic information flow as a result of the decommissioning or blocking of software modules responsible for managing traffic of packets of information;
- a violation of consistency in the use of computer and other resources required for the proper functioning of the software modules of the system, due to disabling or blocking software modules responsible for resource management;
- violation of the connectivity modules of the software information systems as a result of suppression or disruption of communication channels.

Then the condition in which, despite the existence of these destructive factors, ensures the integrity of software and information systems, will be keeping (C) the following composite criterion:

$$\forall i \in I, K_1 \Rightarrow C,$$  \hspace{1cm} (3)

where: $K_1$ – the criterion of functional completeness and the lack of functional redundancy; $K_2$ – the criterion of administrative completeness and certainty; $K_3$ – the criterion of informational conformity; $K_4$ – the criterion of manageability of information flows; $K_5$ – the criterion of resource availability; $K_7$ – the criterion of resource and consistency; $K_7$ – the criterion of structural coherence.

With that said, the task of analyzing the system integrity of software information systems is formulated in the following way. You need to check the structure of the software for compliance with criterion (3) and the results of the test to adjust the system so as to ensure its integrity in the sense of (3). It is obvious that the first step towards solving this task should be the development of a mathematical model of the structure of software information systems. For this, it is proposed to use a matrix approach, where the mathematical model of the structure to be a tuple:

$$\langle \|\alpha_{ij}\|, \|\alpha'_{ij}\|, \|\beta_{jr}\|, \|\eta_{ij}\|, \|u_{jk}\|, \|S_{ir}\|, \|u'_{ir}\| \rangle$$ \hspace{1cm} (4)

In which: $\|\alpha_{ij}\|, i = 1 \div I, 0 = r - otherwise; \langle 1 \div 1 \rangle - a list of software modules in the system, \langle 1 \div F \rangle - the list of functions performed by software; $\|\alpha'_{ij}\|, i = 1 \div I, j = 1 \div J$, where $\alpha'_{ij} = 1$, if $i$-th a software module operated by $j$-th parameter, 0 – otherwise; \langle 1 \div J \rangle – the list of control parameters; $\|\beta_{jr}\|, i = 1 \div I, j = 1 \div J$, where $\beta'_{jr} = 1$, if the choice $j$-th control parameter included in the function $i$-th software modules; 0 – otherwise; $\|\eta_{ij}\|, i = 1 \div I, j = 1 \div J$, $r = 1 \div R$, where $\beta'_{ij} = 1$, if if $i$-th software modules when you select $j$-th parameter management uses $r$-th pecypce, 0 – otherwise; \langle 1 \div R \rangle – a list of resources providing functionality of the software; $\|u_{jk}\|, k = 1 \div K$, where $u'_{jk} = 1$, if $i$-th software modules for choice $j$-th required parameter $k$-th information, 0 – otherwise; \langle 1 \div K \rangle – a complete list of information necessary to ensure the functioning
of the software: \( \| u_{ik} \| \), \( \bar{k} = 1 + K \), where \( u_{ik} = 1 \), if i-th software modules when you select j-th setting management features \( k \)-th information, 0-otherwise; \( (1 + \bar{K}) \) - the full list is available in the system information; \( \| s_{ii} \| \), i or \( i'=1+1 \), where \( s_{ii} = 1 \), if between i-th and \( i' \)-th the software module has a physical connection, 0-otherwise; \( \| u_{ii}^w \| \), where \( u_{ii}^w = 1 \), if the order \( k \)-th information included in the function i-th software module, 0-otherwise; \( u_{ii}^w \), where \( u_{ii}^w = 1 \), if \( k \)-th the information comes from i-th software module \( i' \)-th, 0-otherwise.

Given the model (4) algorithm analysis the system integrity of software information system is reduced to the sequential test the following criteria:

\[
K_1 - \forall_{f \in F} \left( \sum_{i \in I} \bar{\alpha}_0 \right) = 1. \text{ If } \forall_{f \in F} \left( \sum_{i \in I} \bar{\alpha}_0 \right) = 0, \text{ the software structure of information systems blocked the work of software modules that allow for the direct fulfilment of the system functions. When } \forall_{f \in F} \left( \sum_{i \in I} \bar{\alpha}_0 \right) > 1 - \text{ in the structure of the software information systems there are situations where several software modules are beginning to perform the same function (a situation acceptable, but require special consideration because such duplication can lead to failures in the operation of the system).}
\]

\[
K_2 - \forall_{j \in J} \left( \sum_{i \in I} \alpha_j \neq 0 \rightarrow \left( \sum_{i \in I} \alpha_j' = 1 \right) \right). \text{ If } \forall_{j \in J} \left( \sum_{i \in I} \alpha_j \neq 0 \rightarrow \left( \sum_{i \in I} \alpha_j' = 0 \right) \right), \text{ then the software structure of information systems formed the unmanaged software modules operating on their own, without control from the system. When } \forall_{j \in J} \left( \sum_{i \in I} \alpha_j \neq 0 \rightarrow \left( \sum_{i \in I} \alpha_j' > 0 \right) \right) - \text{ in the structure of the software are software modules, which are objects of control by a few other software modules or operated at the same question from different places. A situation of this type is typical for software information systems, is the subject of the impact of malicious users introducing "viruses" blocking the work of the functional software modules or taking control of them).}
\]

\[
K_3 - \forall_{i \in I} \forall_{j \in J} \left( \sum_{k \in K} u_{ik} u_{jk}' \neq 0 \right). \text{ If not satisfied this criterion, the software structure is formed or information redundancy (when } u_{ik} = 1 \text{ and } u_{jk}' = 0 \text{), or is informational insufficiency (when } u_{ik} = 0 \text{ and } u_{jk}' = 1 \text{). In the first case, the situation is acceptable, but requires special consideration because the excess of information can result in a decrease in speed of software modules which, for example, streaming data processing. In the second case, the situation belongs to the class of critical, entailing a serious failure in the operation of the software.}
\]

\[
K_4 - \forall_{k \in K} \left( \sum_{i \in I} u_{ik}' = 1 \right). \text{ Violation of this criterion indicates that the software is formed of unmanaged information flows, that is, in the structure of the software circulates information that either no one owns (when } \sum_{i \in I} u_{ik}' = 0 \text{), or several software modules dispose of the same information (when } \sum_{i \in I} u_{ik}' > 1 \text{). The two situations are in principle acceptable, but require special consideration because both in fact and in another case there may be failures in the software, especially in the case of information-invasion of the intruders).}
\]

\[
K_5 - \forall_{i \in I} \forall_{j \in J} \left( \sum_{k \in K} \beta_{ik} \geq 1 \right). \text{ Violation of this criterion indicates that in software there are situations when the generated software modules the control signals are not supported by appropriate computational resources or memory resources. A situation of this type is typical for the case of introduction of virus programs blocking access program module resources.}
\]
\[ K_6 \rightarrow \forall_{i \in I} \forall_{j \in I} \forall_{j \in J} \{(\sum_{r \in R} \beta_{ijr} > 1) \rightarrow (\eta_{ij} = 1)\} \]. Violation of this criterion indicates that software becomes associated with the wrong choice of resource-dependent departments. In particular, the manifestation of such situations will be artificially caused by a shortage of computing resources, when such deficiency is actually there, but it is incorrect (inconsistent) use of.

\[ K_7 \rightarrow \forall_{i \in I} \forall_{j \in I} \forall_{k \in J} \forall_{k \in K} \{((\alpha_{ijk} = 1) \lor (\eta_{ik} = 1) \lor (u_{ik} = 1)) \rightarrow (s_{i'} = 1)\} \]. Violation of this criterion indicates that the communication needs of software modules are not supported by appropriate communication channels. A situation of this type is typical for spatially distributed systems in which communication channels are susceptible to intentional interference on the part of the attackers.

In your graphic image analysis algorithm system integrity software is presented in figure 3.

Figure 3 (the beginning). The algorithm of multicriteria analysis system integrity software.
The peculiarity of the considered algorithm is that it allows in real time to solve problems identify bottlenecks in software information systems, when implemented in a programming language, can be used as a software module that provides control of integrity of software information systems in real time. The results obtained during the development of this algorithm, and have methodological value. They allow the designers at the early stages of the development of information systems with the requirements of the criteria $K_1 + K_\gamma$, and thereby ensure subsequent workability of the system.

Figure 3 (the end). The algorithm of multicriteria analysis system integrity software.
4. Development of a method and algorithm for analysis of the functional stability of the software of information systems in terms of destructive impacts on their components

Under the functional stability is the ability of a system to perform its functions in the presence of the destructive factors of different nature. Interest in the study of the functional stability of the software of information systems emerged simultaneously with the emergence of these systems. The approach to solving this problem was originally based on the identification of the concepts "reliability" and "stability" and was to transfer the known methods of classical reliability theory into a new soil. With minor modifications it remains up to the present time. However, with the development of information technologies has come to understand that the theory of reliability with regard to assessing sustainability of software information systems in terms of destructive effects has a conceptual incompleteness. First of all, in this theory, the dominant factors are random defects and errors in their design and operation, and factors of destruction of special software modules at the expense of purposeful influences in fact, the field of vision. In addition, the identification of the concepts "reliability" and "sustainability" often leads to fuzzy identification of causes of failures in the operation of the software: 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 [22]. The purpose of the research in this paper was to develop a method for solving this problem. The specific objectives of the study was to: a) the choice of criterion for evaluating the stability of software information systems in terms of destructive impacts; b) developing a method of analysis of the functional stability of the software in terms of destructive impacts according to the criteria; c) development of algorithm of an Express assessment of the risk of violation of stability of the software as the result of destructive impacts.

The choice of criterion for evaluating the functional stability of the software. We introduce in consideration continuous and differentiable functions $E_1(t), \ldots, E_N(t)$, characterizing the current functionality of each software module included in software information systems. $N$ – the total number of the software module in the software of information 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 $[0 \div k_1), [k_1 \div k_2) \cup [k_2 \div 1]$, which will be interpreted in the following way: if $E_i(t) \subseteq [0 \div k_1)$, when i-th a software module subjected to destructive effect ceases to perform its function ("unhealthy"); if $E_i(t) \subseteq [k_1 \div k_2)$, when i-th a software module subjected to destructive exposure, continues to perform its function, but not in full ("working part"); if $E_i(t) \subseteq [k_2 \div 1]$, when i-th software modules have been subjected to destructive exposure, continues to perform its function in full ("healthy"). Let: $\mu_{l_1}(t)$ – the probability that $E_i(t) \subseteq [0 \div k_1)$; $\mu_{l_2}(t)$ – the probability that $E_i(t) \subseteq [k_1 \div k_2)$; $\mu_{l_3}(t)$ – the probability that $E_i(t) \subseteq [k_2 \div 1]$, if the normalizing condition:

$$\sum_{i=1}^{N} \frac{\mu_{l_1}(t) + \mu_{l_2}(t) + \mu_{l_3}(t)) = 1}{N}$$

Then the criterion for evaluating the sustainability of software information systems in terms of destructive effects can be written in the following form:

- if $\sum_{i=1}^{N} \frac{\mu_{l_1}(t) = 1}{N}$, the software operates steadily, that is, in spite of the destructive effects, the system is able to perform its functions in full;

- if $\sum_{i=1}^{N} \frac{\mu_{l_1}(t) = 1}{N}$, 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 $\sum_{i=1}^{N} \frac{\mu_{l_2}(t) = 1}{N}$, 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.
Method of analysis of the functional stability of the software in terms of destructive impacts. We believe that the effect of the destructive influences manifested through the values of functions $E_1(t), \ldots, E_N(t)$, characterizing the functionality of the program module components of the software. Two options of such evaluation: quantitative and qualitative.

In the quantitative variant believe that the process of functioning of each software module 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:

$$\frac{dE_i(t)}{dt} = E_i(t)\rho_i(1 - E_i(t)); i = 1, N, \quad (5)$$

where $N$ – the number of software modules in the software; $\rho_i$ – the dimensionless coefficient characterizing the ability $i$-th software modules to enhance 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 on $S$ - curve with saturation $E_i(t) = \left(1 - \frac{E_i^0 - 1}{E_i^0 e^{\rho_i(t-t_0)}}\right)^{-1}; i = 1, N$, which is the solution of equation (5) in which the symbol $E_i^0(0 < E_i^0 < 1)$, designated starting functionality $i$ -th software modules at a time $t_0$.

Though as a result of destructive effects in the software was implemented "K" malicious software modules. In response to this, in the same software environment was introduced by the "M" software modules, is able to find and eliminate (block) malicious modules. Suppose also that the mutual influence of the modules (native and introduced by cyber criminals) on the functionality of each other in proportion to their current functionality, that is, the relation is valid:

$$f_i\left(E_1(t), \ldots, E_{N+K+M}(t)\right) = E_i(t)\rho_i\left(1 - \rho_i \sum_{j=1}^{N+K+M} c_{ij}E_j(t)\right) ; i = 1, N + K + M, \quad (6)$$

where $c_{ij}(-1 \leq c_{ij} \leq 1)$ and $(c_{ij} = 1, i = j)$ – coefficients whose values are a measure of the relative influence of software module at each other:

- if $c_{ij} = 0$ and $c_{ji} = 0$, between $i$-th and $j$-th software modules there 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 of information 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 program modules 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 information 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 program modules there is 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 $c_{ji}$; such a situation may occur, for example, when the software modules of information systems supporting 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 the \( i \)-th and \( j \)-th software modules 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 functioning of software modules \( M \) is happening in terms of destructive impacts, which influence can be both positive and destructive, depending on the coefficients \( c_{ij} \) and \( c_{ji} \).

On the basis of assumptions the operation of the software of information systems in terms of destructive effects can be described by a system of equations:

\[
\frac{dE_i(t)}{dt} = E_i(t)\rho_i\left(1 - \sum_{i=1}^{N+K+M} c_{ij}E_j(t)\right)\left(i = I,(N+K+M)\right),
\]

\[
E_i(t_0) = E_i^0\left(i = I,(N+K+M)\right).
\]

Given the necessary initial data and solving the system of equations (7) numerically (using, for example, Mathcad), we assess the current functionality of the software modules \( E_i(t),...,E_N(t) \) depending on the nature of destructive effects, defined by the matrix \( \{c_{ij}\} = I,(N+K+M); j = I,(N+K+M) \).

The qualitative analysis of the functional stability of the software in terms of destructive impacts probability \( \mu_{ji}(t) \) proposed to interpret as the membership functions of the current state of the software modules \( M \) to one of three gradations: "unhealthy", "healthy", "working partially", and therefore used to obtain estimates expert method Saaty. Obtained using this method results allow us to construct a function \( \mu(E_i) \), characterizing the grade of membership function values \( E_i(t) \) at the time \( t \) one of the grades: \( \langle \text{zero level} \rangle, \langle \text{low level} \rangle, \langle \text{normal level} \rangle, \langle \text{high level} \rangle \). An example membership function is shown in figure 4.

![Figure 4](image)

**Figure 4.** The view of membership functions of fuzzy assessment values \( E_i(t) \) - example.

As can be seen from this figure, the degree of belonging of security \( i \)-th software modules against 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: \( E_i(t) = 0.52 / \langle \text{zero level} \rangle +0.22 / \langle \text{low level} \rangle + 0.01 / \langle \text{normal level} \rangle + 0.05 / \langle \text{high level} \rangle \). Conclusion: the most probable, we must assume that at the moment \( t \) \( i \)-th module, from software information systems, with a high degree of probability infected by the malicious software introduced by the cyber criminals.

Algorithm for the rapid risk evaluation of stability of software information systems as a result of destructive impacts is based on the concept of stationary equilibrium equations [23], describing the dynamics of the process, treating it in the following way: the process described by (7), has the property...
of equilibria, if \( t \to \infty \) this system of equations has a solution with coordinates \( \left( E_1^*, \ldots, E_{N+K+M}^* \right) \), otherwise, i.e. when (7) does not have solutions, the process has no stationary equilibrium. The lack of stationary equilibrium in the equations describing the studied process shows that the software operation of information 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 (7) point or area stationary equilibrium eliminates this uncertainty and suggests that: a) if \( \forall i=1 \ldots N, E_i^* > 0 \), the risk of loss of stability of the software as the result of destructive effects can be described as "normal"; b) if \( \forall i=1 \ldots N, E_i^* \leq 0 \), the risk of loss of stability software as the result of destructive effects can be described as "maximum". Based on the foregoing, the formula for risk assessment (R) loss of stability software as the result of destructive effects can be written in the following form:

\[
R = \begin{cases}
\text{"normal"} & \text{if (7) there is a point of stationary equilibrium and } \forall i=1 \ldots N, E_i^* > 0 \\
\text{"undefined"} & \text{if (7) there is no point of stationary equilibrium.} \\
\text{"maximum"} & \text{if (7) there is a point of stationary equilibrium, but } \forall i=1 \ldots N, E_i^* \leq 0
\end{cases}
\]

(8)

In that case, when the risk as in (8) is estimated as "normal", it is possible to switch to a more accurate assessment. The reasoning in this case is as follows. Let the information system occurs in a linear \((N + K + M)\)-dimensional phase space with coordinates \( \left( E_1, \ldots, E_{N+K+M} \right) \) and this process has a stationary equilibrium point with coordinates \( \left( E_1^*, \ldots, E_{N+K+M}^* \right) \), and its current position at time is given by coordinates \( [E_1(t), \ldots, E_N(t)] \). Then, a rapid assessment of the current level of risk of loss of stability \( R(t) \) can be obtained using the formula:

\[
R(t) = \sqrt{\frac{\sum_{i=1}^{N} \left( E_i^* - E_i(t) \right)^2}{\sum_{i=1}^{N} E_i^2}}.
\]

(9)

Thus, rapid assessment of the risk of buckling of software information systems as a result of destructive influences is obtained by the following algorithm shown in figure 5.

1. Set the initial conditions and initial data.
2. We write the system of differential equations (7).
3. Set the stationary point of equilibrium (7) and define its coordinates \( \left( E_1^*, \ldots, E_{N+K+M}^* \right) \).

Step 4. and Step 5. Using (8), estimate the level of risk in qualitative gradations of "normal", "uncertain", "maximum". In the case that the level of risk is "uncertain" or "maximum" assessment completed.

Step 6. If \( R = \text{"normal"} \), then, solving the system (7) the numerical method defined by \( [E_1(t), \ldots, E_{N+K+M}(t)] \).

Step 7. Using the formula (9) evaluate the risk at the time \( t \).
5. Conclusions and recommendations
In section 3 a new method of multidimensional analysis of system integrity software for information systems in terms of destructive factors of external and internal nature, based on the matrix approach to representing and analyzing the structure of complex organizational-technical systems. In contrast to a narrow understanding of integrity as the coherence of the graph, imitating the structure of the analyzed system, this approach allowed to introduce a multidimensional criterion of preserving the integrity of software information systems to identify violations of the integrity of the eleven types namely: the "functional incompleteness", "functional duplication", "administrative incompleteness" "structural
redundancy”, “redundancy management”, “information redundancy”, “information failure”, “unmanaged information flows”, “lack of resource”, “inconsistent resource”, “disorders of connectivity”.

The peculiarity of the method lies in the fact that it allows in real time to carry out diagnostics software, information systems, and being implemented in the programming language can be used as a software module that provides control to the system integrity of software and information systems in real-time. The results obtained during the development of this method, another important methodological significance. They allow the designers at the early stages of the development of information systems with the requirements of the criteria $K_1 \leq K_7$, and thereby ensure subsequent workability of the system. Moreover, the more complex structurally designed information systems, the more efficient becomes the use of this method.

Proposed in section 4 method of analysis of the functional stability of the software of information systems in conditions of destructive impacts has the feature that it is designed 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 information systems as a result of destructive impacts. The idea of this algorithm is that the notion of system resilience is associated with the concept of stationary equilibrium equations describing the function of the software of information 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, from outlined in this article, it follows that, using mathematical tools can adequately simulate the operation of software of information systems in conditions of destructive impacts, and to formulate and solve the problem of stabilization of the process in real time.

6. Conclusion
Thus, the presented models and algorithms of structural and parametric synthesis and optimization of information systems in conditions of destructive impacts are a complex of organizational-technical dynamic system, operating in the parametric environment, the methods and algorithm of system integrity and methods and algorithms for the functional stability of the software information systems are a type of the two control loops built – in software information systems, as a system of management and control of quality and safe functioning of the software module responsible for providing the required level of security in terms of impact on software external and internal threats, how control system impacts with antagonist purposes functioning.

If implemented in a programming language, model and algorithms can be used as a test for modeling of information processing in information systems and the subsequent assessment of efficiency of functioning of subsystems of the control and detection of destructive impacts, providing diagnostics of the integrity and efficiency of the software and control the functional stability of the software of information systems in conflict with hackers, insiders, the phreakers, the crackers and other subjects of computer crime [24].

The proposed concept can be used to develop new strategies for performance management software of information systems in conditions of a complex influence of malicious software for computer intelligence.

References
[1] Federal law of 26.07.2017 N 187-FZ About the security of critical information infrastructure of the Russian Federation Collected legislation of the Russian Federation 31.07.2017 N 31 (Part I) article 4736
[2] Kochedykov S S, Grechishnikov E V, Dushkin A V and Orlova D E 2018 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.

[3] Grechishnikov E V, Dobryshin M M, Kochedykov S S and Novoselcev V I 2019 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 DOI: 10.1088/1742-6596/1203/1/012064.

[4] Kochedykov S S, Dushkin A V, Noev A N and Gubin I A 2018 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 IOP Conf. Series: Journal of Physics: Conf. Series 1015 (2018) 032101 DOI: 10.1088/1742-6596/1015/3/032101.

[5] Kochedykov S S, Dushkin A V, Novoseltsev V I, Stolnik V V and Minin Yu V 2018 Mathematical model of cyber threats for the software of the automated control system Industrial ACS and controllers 2 43-55

[6] Tsvirkun A D 1975 Structure of complex systems (Moscow: Sov. Radio)

[7] Tsvirkun A D 1982 Basis for synthesis of structures of difficult systems (Moscow: Science)

[8] Decree of the President of the Russian Federation from 05.12.2016 № 646 On approval of the Doctrine of information security of the Russian Federation Sz the Russian Federation 12.12.2016 N 50 article 7074

[9] Decree of the President of the Russian Federation from 31.12.2015 № 683 On the strategy of national security of the Russian Federation Sz the Russian Federation 04.01.2016 N 1 (part II) article 212

[10] Decree of the President of the Russian Federation from 09.05.2017 No. 203 On the Strategy of information society development in Russian Federation to 2017-2030 Sz the Russian Federation 15.05.2017 N 20 St. 2901

[11] Common Criteria for Information Technology Security Evaluation. National Institute of Standards and Technology & National Security Agency (USA), Communication Security Establishment (Canada), Communications-Electronics Security Group (United Kingdom), Bundesamt fur Sichereit in der Informationstechnik (Germany), Service Central de la Securite des Systemes d'Information (France), National Communications Security Agency (Netherlands) Version 2.1 1999 URL http://www.commoncriteriaportal.org/files/ccfiles/ccpart1v21.pdf

[12] RD. Requirements to ensure information protection in automated control systems of production and technological processes at critically important objects, potentially hazardous objects and objects of increased danger to life and health of people and the environment (app. the order of FSTEC of Russia 14.03.2014 g No. 31 (ed. by 09.08.2018))

[13] Balan V P, Dushkin A V, Novoseltsev V I and Sumin V. I. 2015 Conflict Management (Moscow: Hot line)

[14] Makarenko S I 2015 Dynamic model of a communication system in terms of functional-multi-level information conflict monitoring, and suppression System control, communication and security 3 122-185

[15] Dushkin A V, Kochedykov S S, Novoseltsev V I, Pavlov V A, Zolnikov V K and Grechushkin A Y 2017 Analysis of conflict interaction of the Executive devices of automated control systems Industrial ACS and controllers 10 8-16.

[16] Kochedykov S S, Pavlov V A and Nistratov R S 2018 Resource Management of hardware components in an information conflict Vestnik of Voronezh Institute FSN of Russia 1 61-70

[17] Kochedykov S S, Dushkin A V, Novoseltsev V I and Sokolovskyi S P 2017 Modeling of the system conflict interactions in the information system critical applications Vestnik of Voronezh Institute FSN of Russia 4 74-84.
[18] Dushkin A V, Kochedykov S S, Novoseltsev V I and Sumin V I 2016 Optimization of information flow in systems of critical appointment in terms of the impact of external forces Vestnik of Voronezh Institute FSIN of Russia 4 67-72

[19] Kochedykov S S, Kravchenko A S, Novoseltsev V I and Sumin V I 2017 The typology of the mutual influence of software components of information systems in conditions of external and internal threats Vestnik of Voronezh Institute FSIN of Russia 2 77-84

[20] Perminov V G, Rodin S V and Kochedykov S S 2015 Computational experiment to test the properties of the criterion of dynamic efficiency control of integrity of software environment reference ADIS Vestnik of Voronezh Institute of MIA of Russia 1 263-270

[21] Dubrovin A S, Dushkin A V, Kochedykov S S and Novoseltsev V I 2017 Simulation of highly reliable information processing in automated information system special purpose in the conditions of influence of internal threats to information security Vestnik of Voronezh Institute FSIN of Russia 2 48-54

[22] Kochedykov S S, Novoseltsev V I, Dushkin A V, Solovyov A S and Nurutdinov G N 2017 The solution of the problem of sustainability of the software of automated control systems in conditions of limited resource Industrial ACS and controllers 8 39-47

[23] Kochedykov S S, Dushkin A V and Markin P V 2019 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) DOI: 10.1109/EIConRus.2019.8657323

[24] Kochedykov S S, Novoseltsev V I, Sumin V I, Dushkin A V and Eliseev A I 2017 Mathematical model of the process of processing and protecting information in information and communication systems management of mission critical facilities taking into account the mutual influence of software components in terms of the impact of information security threats Industrial IKS and controllers 9 33-46.