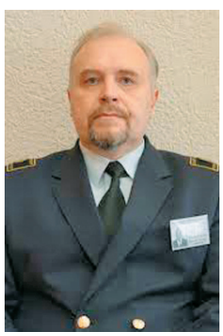
Надежность № 2 2016
Dependability no.2 2016

Original article
УДК 681.3.06+519(076.1)
DOI: 10.21683/1729-2640-2016-16-2-3-15

Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy

Gennady N. Cherkesov, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia, e-mail: gennady.cherkesov@gmail.com
Alexey O. Nedosekin, National Mineral Resources University "Gorny", St. Petersburg, Russia, e-mail: apostolfoma@gmail.com

Gennady N. Cherkesov



Alexey O. Nedosekin

Abstract. Aim. *The paper describes main concepts and definitions, survivability indices, methods used to estimate survivability in different external and internal conditions of application of technical systems, including the studies in the field of structural survivability obtained 30 years ago within the frames of the Soviet school of sciences. An attempt is made to overcome different technical understanding of survivability, which has been developed in the number of industries up to date – in ship industry, aviation, communication networks, energy, in defense industry. The question of succession between the properties of technical survivability and global system resilience is considered. Technical survivability is understood in two basic notions: a) as the system property to withstand negative external impacts (NI); b) as the system property to recover its operability after a failure or accident caused by external reasons. This paper considers the relation between the structural survivability when the system operability logic is binary, and is described by a logical function of operability, and the functional survivability when the operation of the system is described by the criterion of functional efficiency. Then the system failure is a decline in its efficiency below a preset value.* ***Methods.*** *The technical system is considered as a controlled cybernetic system, which has specialized aids to ensure survivability (SAs). Logical and probabilistic methods and results of combinatorial theory of random placements are used in the analysis. It is supposed that: a) negative impacts (NI) are occasional and single-shot (one impact affects one element); b) each element of the system has binary logic (operability – failure) and zero resistance, i.e. it is for sure affected by one impact. Henceforth this assumption is generalized for the r-time NI and L-resistant elements. The paper also describes different variants of non-point models when the system part or the system as a whole are exposed to a group affection of the specialized type. The article also considers the variants of combination of reliability and survivability when failures due to internal and external reasons are analyzed simultaneously.* ***Results.*** *Different variants of affection and functions of survivability of technical systems are reproduced. It has been educed that these distributions are based on simple and generalized Morgan numbers, as well as Stirling numbers of the second kind that can be reestablished on the basis of simplest recurrence relations. If the assumptions of a mathematical model are generalized in case of n the r-time NI and L-resistant elements, the generalized Morgan numbers used in the estimation of affection law are defined based on the theory of random placements, in the course of n-time differentiation of a generator polynomial. In this case it is not possible to set the recurrent relation between the generalized Morgan numbers. It is shown that under uniform assumptions in relation to a survivability model (equally resistant system elements, equally probable NI) in the core of relations for the function of survivability of the system, regardless of the affection law, there is a vector of structure redundancy F (u), where u is a number of affected elements, and F (u) is a number of operable states of the technical system with u failures.* ***Conclusions:*** *point survivability models are a perfect tool to perform an express-analysis of structural complex systems and to obtain approximate estimates of survivability functions. Simplest assumptions of structural survivability can be generalized for the case when the logic of system operability is not binary, but is specified by the level of the system efficiency. In this case we should speak about functional survivability. PNP computational difficulty of the task of survivability estimation does not allow solving this task by means of a simple enumerating of states of the technical system and variants of NI. It is necessary to find the ways to avoid the complete search, as well by the conversion of the system operability function and its decomposition. survivability property should be designed and implemented into a technical system with consideration of how this property is ensured in biological and social systems.*

Keywords: *survivability, vitality, resilience, risk, negative impact, survivability margin, law of vulnerability, function of survivability.*

For citation: *Cherkesov G.N., Nedosekin A.O. Description of approach to estimating survivability of complex structures under repeated impacts of high accuracy // Dependability, 2016, no.2, pp. 3-15. (in Russian) DOI: 10.21683/1729-2640-2016-16-2-3-15*

1. Introduction

A term "survivability" in relation to technical systems and in particular to a ship was for the first time introduced for consideration by the Russian admiral and scientist Stepan Osipovich Makarov. The beginning of development of the ship survivability theory should be his article "Armor-plated boat "Mermaid" published in 1870 in "Sea collected book" (No.No. 3, 5, 6), that described a number of measures taken for a ship floodability [1]. In 1875 in the article "Floodability of water crafts" ("Sea collected book", No.6, 1875) he formulated the notion of "floodability" as the "ability to remain on the float having underwater hull breaches". In 1876 S.O. Makarov published the articles "Antiflooding means" ("Sea collected book" No. 1, 1876) and "About maintenance of water-tight bulkheads and pumping appliances" ("Sea collected book" No. 7, 1876). In 1894 he published the work "Review of elements of vessel fighting forces" where he clarified the notion of floodability as the "ability of a ship to remain on the float and not to lose its fighting qualities due to underwater hull breaches".

In 1897 S.O. Makarov published his articles "Maritime essays" ("Sea collected book", No.No. 1, 2, 3, 4, 7) where he finally formulated the "survivability" as the "ability of a ship to keep a fight having damages in different fighting structures" with a proviso that a deficiency of resistance to external destructive effects is compensated by attribution of a ship with the property of survivability [14].

The academician A.N. Krylov gave the shortest and a rather pointed definition of a general sense of "survivability" and defined it as "fatigue resistance to damages". All definitions have a positive feature – that survivability is considered as a property of a ship as a whole, which is achieved by structural organization and goal-directed behavior of its functional sets of technical facilities.

Today the notion of survivability is widely used in several sectors of engineering including transport systems (aviation, railway, automobile transport), ship industry, energy, construction, in computing systems and communication networks, in industries of defense [9, 13, 14]. A renewed system and scientific interest to technical survivability in the 1980s in the USSR was determined by a large scope of works on secret subjects related to national defense capability. In times of "perestroika" all these works were scaled down, and now we observe a certain renaissance due to a marked aggravation of international atmosphere. It turns out to be important not only to raise the works on technical survivability to a former level, but also to take a fresh look at "survivability" as a complex property of a system, come to realization that the system in terms of survivability takes from the creatures that are traditionally considered living beings. An attempt of such comparison is undertaken in paper [15] where survivability is generally called vitality, and vitality projection on social, economic and technical systems is called civilization availability, mobilization resilience and survivability, respectively.

Survivability issues are considered in foreign literature as well. Approximately up to the year 1997 the surveys used the category "survivability" more often. But then the focus of attention shifted towards an area of more common properties than survivability, and a question was more about resilience. In 1997 a presidential commission delivered a report on the protection of the most mission-critical infrastructure systems [16]. And then the USA showed special demand in resilience due to a huge damage caused by 9/11 and Katrina hurricane. It became clear that resilience must be invested significantly. As an alternative – which is not to invest in resilience – usually comes at a higher cost. Therefore investments in resilience turns out to be a business of enormous earning capacity (hundreds of annual interest).

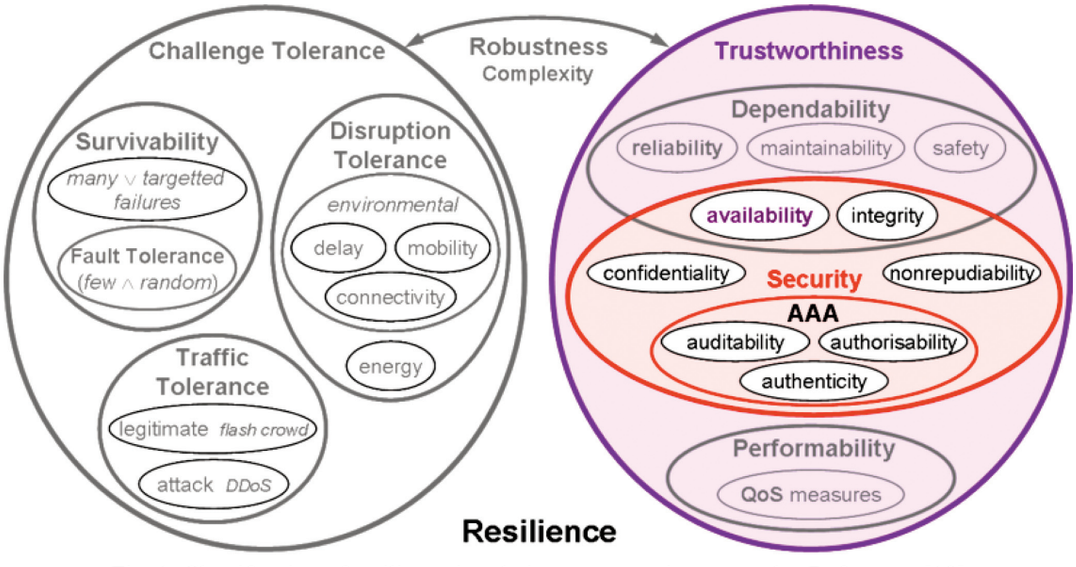


Fig. 1. Classification of resilience in relation to computing networks. Reference: [18]

That is why, for example, in [17] we read: "*Resilience attracts attention as a denominator to move beyond survivability and even to succeed in aggressive conditions … Resilience is an emergent property related to the ability of an organization to proceed with its mission despite damages, through awareness, dexterity provided by resources, flexible infrastructures and restorability.... Therefore resilience is a combination of technical structural features such as reliability and dependability and organizational features such as awareness, training and decentralized decision making"*.

And [18] provides the following sector classification of resilience (Figure 1).

We can see from the given classification that resilience is considered as a global property that takes up the properties of dependability (in all senses), survivability, safety, operational perfection. Such view has not been conceived by the Russian sector science yet, and it is unlikely to be conceived without a critical analysis and natural antagonism. We are not going to get involved in this polemic, but we would like to attract a reader's attention to the following paradox. Many companies and certain experts study technical survivability ad consider it if their projects. However, in practice there is no consistent system of notions, survivability indices, conditions of functioning, with availability of which survivability and survivability requirements should emerge, i.e. exactly that makes a core of the respective theory. There is also no unity in understanding of the most efficient means of survivability assurance for different classes of systems and definite scenarios of external impacts on the structure and algorithms of functioning. To make the picture of survivability developments complete we should mention about a total absence of national standards reflecting the issues of terminology, survivability indices, classification, methods and recommendations on the order of system design by survivability criteria.

We also should keep in mind that the issues of technical survivability shall not be considered locally, but in the context of a more common demand in a mobilization resilience of a state and a country in general [15, 19, 21, 22]. In limited investment opportunities of a state, defense budgets shall be sequestered, and projects shall be loaded only with the specific properties that shall be economically efficient in a broad sense. In terms of technical survivability (as well as of reliability) – a right to live will go only to those design implementations that proved an optimal proportion between the strength of property and the expenses spent on its realization, and besides, an optimum has been found for return of capital employed. I.e. with time it is necessary to learn not only to estimate survivability, but also to introduce economic and financial measures to this estimate. Thirty years ago there was no need to think about it (defense money was not watched); but now we live in another epoch.

This article represents topical questions of system design by the criteria of technical survivability that may be considered as possible directions for the development of survivability theory as a general technical discipline. Basic study in this sphere was made 30 years ago, and it is not reproduced here. However, there is a number of new circumstances that may influence a new revealing of survivability, the character of development of the respective branch of science, and we shall speak about it in this work as well.

2. Main concepts and definitions

There are several industrial definitions and a common technical definition of survivability. GOST 19176–80 [1] defines survivability of the system of ship facilities control as a constituent part of complex property of the control system functioning which emerges in case of part damages of equipment and communication lines. Survivability **involves** maintaining of operability of a ship which was not affected by emergency environmental impacts, as well as fail-safety of set of technical facilities under violations of control system. The work [3, p.194] defines survivability of a ship as the ability to withstand wind strength and wave force, fires, enemy's weapons, and if damages occurred to keep and recover sea capabilities and combat qualities either totally or partially. Survivability of a ship is provided by structural design and equipment efficiency, as well as by allocation of tight junctions, hatches, handholes, doors, glass parts, signaling systems, automatic protective devices. Let us note that this definition indicates the **conditions** when survivability emerges (spontaneous forces of wind and wave, fires, weapons), **stages** of the process development and the **degree of severity** of negative impacts (to withstand damages, if a damage occur to keep sea capabilities and combat qualities, and in case of their loss to recover them either totally or partially). And the methods to provide survivability are listed (limitation of adverse consequences, structural design efficiency, tight junctions, signaling and control: signaling systems, protective devices). Such a large structure of definition could be repeated for other sectors of engineering

In electric power industry [4] survivability is understood as the property of an object to withstand perturbing actions, avoiding their successive development with mass supply interruptions. Here we should pay our attention to the requirement to the system that it must withstand deactivation of its components due to technologically related failures caused by violations of external conditions of functioning. The paper [6] gives such example of violation of external conditions under a system failure. When removing of one of two 220 kV power lines out of service for repair the unit of a condensing plant was disconnected due to a boiler damage. The other power line was overloaded and caused a blow out of a wire in a faulty contact joint. After this line was also disconnected under relay protection, asynchronous operation was phased out which disconnected 110 kV power lines. Then frequency

reduction caused the activation of frequency relief devices machinery of thermal power station, etc. As the result it interrupted a normal supply mode of the whole district for 15 hours. A "domino" effect in the system is caused by successive violation of functioning that leads to a supply disconnection.

In computing systems [2] survivability is connected with loss free conditions of any task (function) under a loss of certain resource caused by negative external impacts.

An attempt to give a common technical definition to survivability was taken in the work [9]. Here survivability is defined as the property of a system to keep and recover the ability to perform basic functions in a prescribed scope during a specified operating hours to failure under a change of the system structure and (or) algorithms and terms of its functioning due to external negative impacts (NI) that were not specified by the rules of normal operation. Basic functions and specified operating hours can be determined not only for one, but also for several NI different in severity. This definition admits the **consideration of various NI consequences**, affecting the task execution, including:

• loss of operability of the elements and their links due to their physical destruction or integrity damage;

• change (deterioration) of their technical characteristics (speed, productivity, capacity, etc.);

• distortion of algorithms of functioning;

• reduction of structure redundancy, level of production stock;

• deterioration of failure-free operation of the elements, system controllability;

• change of external terms of functioning (sharp reduction of increase of loading, loading redistribution, change of dynamic characteristics of loading).

More severe consequences of NI are also probable: inherent loss of operability, accident with possible partial or total system breakdown.

3. Evolution of the system states after negative impacts

NI are followed by primary consequences that are expressed in the deterioration of performance of the elements or functional connections, distortion of algorithms of functioning of functioning [9].

The system that has the property of survivability develops it in the property of gradual **degradation** that occurs due to introduction of passive and active survivability aids (SAs). Information about primary consequences goes to SAs that include operability control facilities, tools of emergency protection, means of reconfiguration and control. SAs influence the development of primary consequences. Depending on the intensity of processes, certain external conditions, SAs efficiency, the system finally passes to one of possible resilient states. This process is stochastic by its nature.

We know from the example described in section 2 that after certain intermediate states the system passed to a resilient state under which the units of a condensing plant ware disconnected and machinery of thermal power station were cut off. After transition to a new state the estimation of primary consequences is performed as the result of which the system state is referred to one of three classes: operable, inoperable (or non-emergency), emergency. Based on the results of this classification the estimation for survivability by the system state is carried out. Under an operable state the system turns to the task execution immediately. If the state is inoperable the system may turn to the task execution after certain recovery procedures. The transition of the system to a new resilient state does not complete the struggle for survivability, as under further functioning secondary consequences of NI may occur before the task execution.

Secondary consequences are farther but not less dangerous than the primary ones. They are related to uncontrolled or ill controllable thermal, electric and other proc-

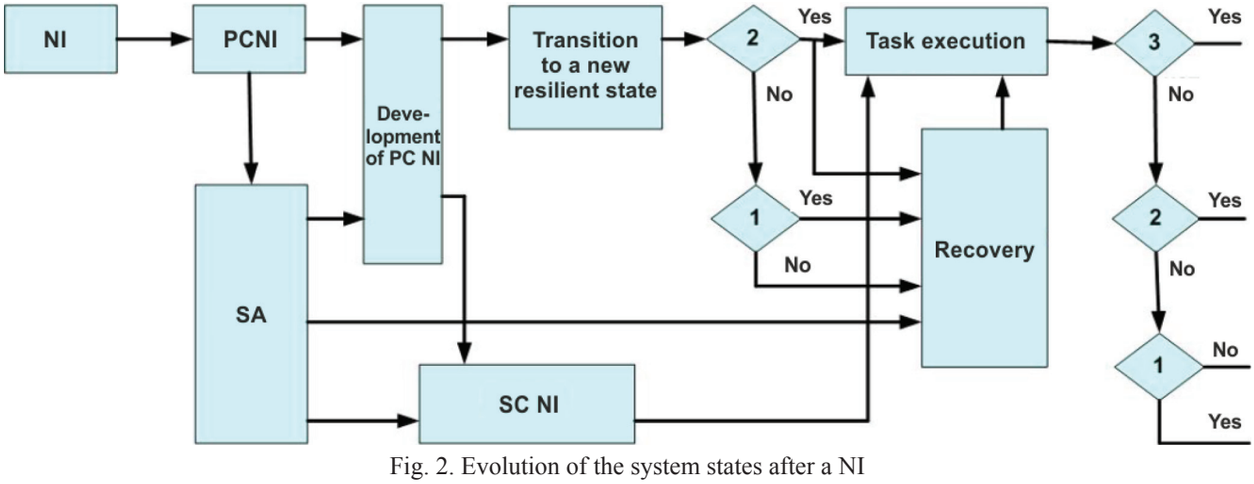


Fig. 2. Evolution of the system states after a NI
(PC – primary consequences, SC – secondary consequences, SAs– survivability aids,
1 – accident; 2 – operable; 3 – task execution)

esses (fire spread, cooling of space in heat supply system, etc.). The rate of development of secondary consequences and the end result depend significantly on SAs operation at struggle for survivability. After a certain period of time, the estimation of the task execution results is performed with four possible outcomes. Therefore, at struggle for survivability we can allocate three stages. The first stage includes the efforts for accident prevention, the second stage struggles for the system operability, and the third stage includes the struggle for a successful execution of a task despite primary and secondary consequences of NI. Accordingly, there are two tasks for estimation and assurance of survivability.

Trajectories of evolution of the system states with the consequences different in intensity and severity fit in the general scheme (Figure 2), but only in the cases when an impact is single. The scheme becomes much more complicated when the impacts are multiple and the processes of consequences of different NI overlap. In addition to that, in all possible schemes a "racing effect" plays a great role: the processes of consequences development and the processes of struggling for survivability proceed through time. That is why the severity of NI consequences, system state and, finally, its destiny are mainly determined by SAs capabilities, their operational efficiency and effectiveness. A certain productivity margin of SAs creates favorable conditions for a timely decision that makes it possible to limit secondary NI consequences and keep the system operability at least with a bit worse technical characteristics. That is why it is important to underline the following: struggle for survivability often takes place under severe time constraints. And therefore, the survivability models should be dynamic. A racing effect could not be taken into account, we could use static models in two extreme cases when the speeds of the competing processes are essentially different.

In the first case a SA has time to complete its algorithms and perform the required disconnection, activation and change-over switching before the technologically interconnected failures occur. **In the second case** a SA does not have time to step in high-speed processes of the development of primary NI consequences, and the transition to e new resilient state is implemented without SAs. Only later survivability aids will influence the secondary NI consequences and recovering processes. In both cases a role of stochastic factors decreases, because a final state of the system can be definitely traced by the system and NI characteristics.

4. Factors and scenarios that are considered in survivability models

All factors that specify the system survivability can be divided into three groups by a functional feature: 1) factors of negative impacts; 2) **factors** that specify the system and its elements in terms of survivability; 3) factors that specify **external aids** of survivability.

The first group includes the scope of NI (a point, a closed figure on a plane, in space), number of **affecting** factors and their characteristics, NI duration (**impulse** and with **finite duration**), degree of NI, strategy of multiple NI, internal and external sources of NI that require the creation of survivability aids.

The second group is formed by:

1) factors that specify the system and its elements in terms of survivability (resistance of the elements, topology of the system and its elements, resilience to the development of NI consequences of a certain type, speed of processes caused by NI; fail-safety of the elements);

2) factors that specify **internal SAs (**due notice of a NI danger; emergency protection; redundancy; factors of localization and elimination of secondary NI consequences; factors of recovery of technical characteristics of survivability: fire resistance, strength, etc.).

The third group includes the factors that specify **external survivability aids** and perform the functions of rescue services and mobile centralized redundancy used for recovering.

Based on the combination of assumptions about current factors the scenarios of impacts on the system, as well as the scenarios of struggling for survivability occur. For example, we may take a scenario of multiple negative impulse impact with one affecting factor of high intensity (affection is guaranteed) and a high accuracy with availability of the structure of a certain class with no SAs. Alternative scenarios may consider zero resistance of the elements; non-ordinary flows of NI affecting several element at once; development of the impact with time, making it possible to take a countermeasure and analyze a racing effect; availability of the reserved time sufficient for probable recovery of operability with external SAs and further execution of the prescribed works, etc.

Scenarios are getting much more complicated if multiserial NI are considered not only with a strategy of the system protection form NI, but also with a strategy of influence on the number and degree of impacts in the mode of antagonistic, management game and efficient counter efforts against a game partner.

A concept of survivability model is more restricted and specific than the concept of survivability struggle scenario. And each scenario could be generally correlated with a variety of models. A survivability model is not only used for a quantitative estimation, it also has a calculation base and further comparison with the requirements as one of major targets of development at the designing and at the operation of mission-critical systems. For comparison and analysis the survivability indices are required.

5. Survivability indices

Proposals for survivability indices in technical literature first occurred in the 1970-1980s [2-7]**,** in work [9] in more

detail. For the ranking purposes they should be classified by two features. **According to the first feature** indices are divided into two groups: indices used to estimate survivability by the system state and by the results of task execution. Indices of the first group estimate the system property to keep operability after NI. Indices of the second group estimate the ability not only to withstand NI, but also to execute the prescribed task successful in future despite NI. **According to the second feature** indices are divided into additive and mini-max indices. They differ in the way of leading of a vector index to a scalar one. Additive indices also include probabilistic indices based on the formula of total probability.

5.1. Indices of survivability by the system state

Let us use A_n to indicate the event of n-tuple occurrence of NI, and F to indicate a logic function of the system operability that takes a value 1 if the system is operable, and 0 if its is inoperable. Then a conditional law of vulnerability

$$Q(n) = P\{F = 0 \mid A_n\} \tag{1}$$

is a probability of loss of operability in case of a n-tuple NI.

Survival rate of the system under n-tuple NI

$$R(n) = P\{F = 1 \mid A_n\}. \tag{2}$$

Margin of survivability (d-survivability)

$$d = C - 1 \tag{3}$$

is a critical number of defects C decreased by one. Defect is a unit of measurement of damage of the system caused by a negative impact. It could be one element removed from the system as the result of NI, certain nominal capacity in energy system, lost for consumers as the result of NI, etc. A word "critical" is used to call a minimum number of defects occurrence of which leads to the loss of operability.

Maximum margin of survivability (m- survivability)

$$m = \max_{(i)}(m_i) \tag{4}$$

is a maximum number of defects that could be suffered by the system without loss of operability.

Average number of negative impacts that cause loss of operability

$$\overline{\omega} = \sum_{n=0}^{\infty} R(n) \tag{5}$$

is an expected value of the number of NI that is set by distribution (1).

Average margin of survivability

$$\overline{d} = \overline{\omega} - 1. \tag{6}$$

This is not a negative value because $\overline{\omega} \geq 1$. It follows from (5), as $R(0) = 1$. Indices (1), (2), (5) and (6) are probabilistic, (3) and (4) are deterministic.

Deterministic indices also include index K^A_S which is a minimum number of affected elements with total damage for the system not less than A, offered in [6]. Let a certain system consist of n_S objects, S is a number of the system variant. Single negative impact on the i-th element causes the damage C^S_i. The elements are ranged in order of damage decrease $C^s_1 > C^s_2 > \ldots > C^s n_s$. Let us set a threshold acceptable value of damage A and assume that in case of multiple negative impact different elements are affected, and first of all the elements with the most damage. And damage for the system as a whole is obtained by addition of damages of separate elements. Then K^A_S is defined by formula

$$K^A_S = \min_{(C_S > A)} K_S, C_S = \sum_{i=0}^{K_S} C^S_i. \tag{7}$$

Here K_S is the number of faulty elements or elements lost as the result of NI in S structure.

Besides we can amplify a model perception of survivability by introducing the following additional characteristics to a NI model and its consequences:

r – **frequency** of NI is a number of simultaneously affected elements or subsystems by one NI. In this case by the result of one NI we can observe r defects in the system. Such approach is used for dispersed systems in which a single NI causes multiple consequences (for example, act of nature or a military strike);

L – **resistance** of the element to an affecting impact. It is an integer number of NI endured by an element without loss of operability. In a more general case a deterministic L-criterion of resistance should be substituted by the function of resistance that may have a stochastic or a fuzzy set nature. We speak about resistance when the survivability of the system element is provided by external SAs, for example, be means of defense measures (air defense, underground fortifications, etc.). For the models that are considered here $L = 0$.

5.2. Indices of survivability based on the results of task execution

Let now the system with a basic structure S_0 execute a certain task during a period of time t. As the result of NI a new structure S_i may occur in the system, one of the variety of operable structures $S^{O}=\{S_i,\ i=1,\ldots,N_p\}$ or inoperable structures $S^{IO} = \{S_i,\ i = N_p+1,\ldots, N\}$. After a n-tuple NI the system with a new structure should start the execution of a prescribed task and complete it within the time period t. The estimation of survivability based

on the results of task execution is carried out using the following indices.

Conditional function of survivability

$$G_i(t) = G(t \mid S_i) = P(t \mid S_i) / P(t \mid S_0) \qquad (8)$$

is a relation of probabilities of task execution by the system for two cases: for a basic structure S_0 and for a new one S_i. And it may be possible that for a new structure S_i the task will be formulated differently than for S_0 structure. However, in this case $G_i(t) < 1$ have to be fulfilled. If recovery is available inoperable structures ($i > N_\text{P}$) also could be considered, because for them $P(t/S_i) > 0$ also may hold true. If recovery is unavailable $P(t/S_i) = 0$ with $i > N_\text{P}$.

The function of the system survival in case of a n-tuple impact (an event A_n):

$$G(t,n) = G(t \mid A_n) = \sum_{k=1}^{N} P_n(k) G_k(t) \qquad (9)$$

is the survivability function averaged by all possible structures; $P_n(k)$ is a probability of occurrence of structure S_k after a n-tuple NI.

Absolute function of survivability

$$G(t) = \sum_{n=1}^{\infty} P(A_n) G(t \mid A_n) = \sum_{k=1}^{N} P(S_k) G_k(t) \qquad (10)$$

is the function of survival averaged by all possible events A_n. Probability $P(S_k)$ is defined by formula

$$P(S_k) = \sum_{n=1}^{\infty} P(A_n) P_n(k). \qquad (11)$$

Indices (9) and (10) refer to the additive class and they ensure a turning of the vector index $\{G_k(t),\ k = 1, \ldots, N\}$ into a scalar one. If there is no consistent information about probabilities $P_n(k)$ and $P(S_k)$ they can be substituted with weight coefficients α_k and β_k, that are assigned expertly. If it is also difficult, then it is necessary to proceed with mini-max indices.

Sequence $G(t,n)$ is a decreasing function n and it changes from 1 with $n = 0$ to 0 with $n \to \infty$. That is why an average number of NI that causes non-execution of a task is defined by formula

$$\overline{\omega}(t) = \sum_{n=1}^{\infty} n(G_i(t,n-1) - G(t,n)) = \sum_{n=0}^{\infty} G(t,n). \qquad (12)$$

with $t = 0$ or $\lambda_i = 0$ (elements are absolutely reliable) formulas (9) and (12) change into (2) and (5) respectively. Indeed, with $t = 0$ function $G_k(0) = 1$ for $k \le N_\text{P}$ and $G_k(0) = 1$ for $k > N_\text{P}$. Based on (9) we have the function of survival with a zero duration of a task:

$$G(0 \mid A_n) = \sum_{k=1}^{N_\partial} P_n(k) = R(n), \qquad (13)$$

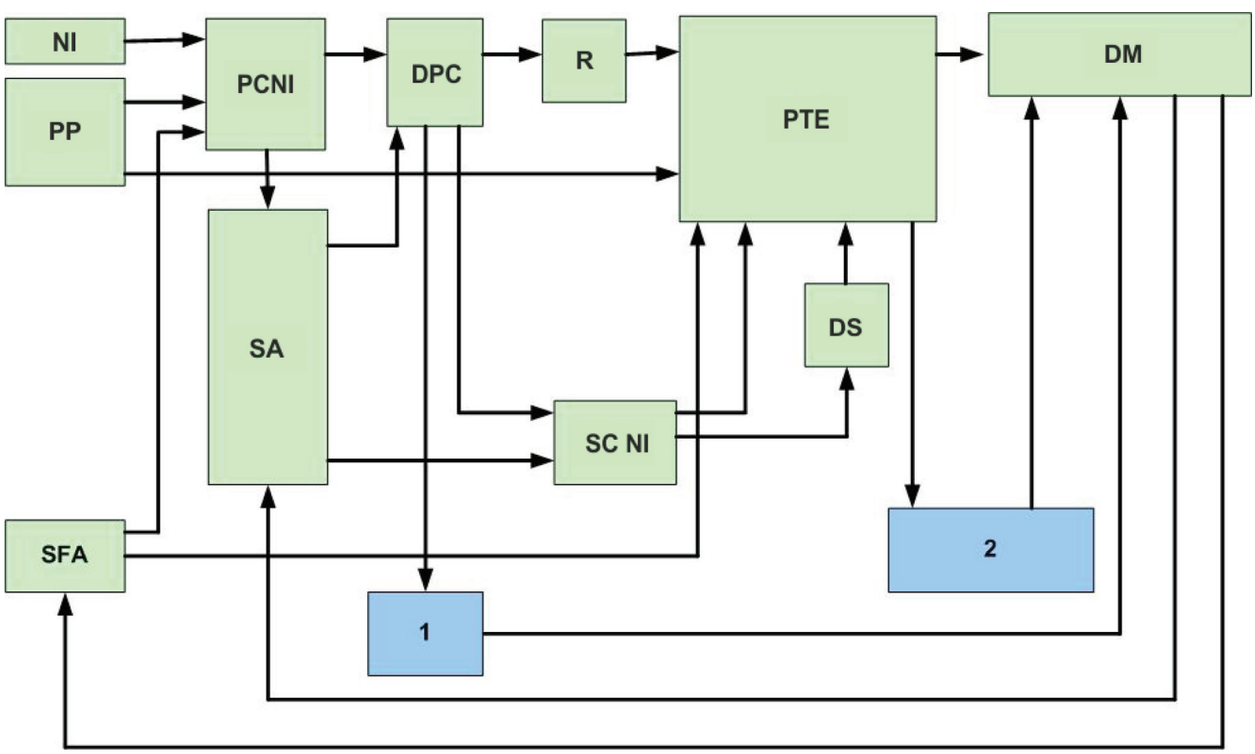


Fig. 3. Structure scheme of the survivability model
(1 – estimation of survivability by the system state, 2 – estimation of survivability by the results of task execution);
PP – physical processes, DPC – development of primary consequences, R – reliability, PTE – process of task execution, DM – decision making, SC NI – secondary consequences of NI, DS – development of secondary consequences, SFA – structure, function, algorithm)

and based on (10) we obtain an absolute function of survivability with a zero duration of a task

$$G(0) = R = \sum_{n=1}^{\infty} P(A_n)R(n).$$

Indices (8) – (13) could be generalized also for the case of branching and multipoint structures. For this purpose probability of task execution in (8) should be substituted with a certain quality factor $E(S)$. So for a system with branching structure, a functioning within a time interval t can be expressed by a composed function

$$E(t, S) = \varphi\,(P(t/S)), \qquad (14)$$

where $P(t/S) = \{P_m(t/S), m=0, \ldots, M\}$ is the distribution of the number of inoperable branches at the moment of time t provided that initially the system had S structure. Then a conditional function of survivability is defined by formula

$$G_i(t) = G(t/S_i) = E(t, S_i) / E(t, S_0). \qquad (15)$$

With $M = 1$ we shall get $E(t/S) = P(t/S)$, and formula (15) changes into (8). Other indices can be found by formulas (9) – (12).

6. Survivability models

Model of survivability of a complex system is actually a set of a large number of particular models of different application that use both deterministic and probabilistic methods to describe processes (Figure 3).

NI model. By the scope of application we can distinguish point models and spatial models. In point models NI is assumed to affect one or several elements. In the latter case the scope of NI is a group of points in which the system elements are located. That is why the number of elements in the system is always more than the number of points in the scope of NI. For each element or a group of elements a probability of occurrence in the scope of NI is set. If the scope is single-point the following distribution is set $\{\alpha_i, i = 1, \ldots, N\}$, where N is the number of the system elements, α_i is a probability that the i-th element occurs in the scope of NI. One of possible distributions is a n equal distribution $\alpha_i = 1/N$. For a multipoint scope the following distribution is set $\{\beta_i = P(X = i), i = 1, \ldots, N\}$ where β_i is a probability that i elements occur in the scope. In models we can use, for example, truncated binominal distribution

$$\beta_i = C_N^i p^i (1-p)^{N-i} / (1-p^N), i = 1...N \qquad (16)$$

or a truncated Poisson distribution

$$\beta_i = \frac{a^i}{i!} / \sum_{k=1}^{N} \frac{a^k}{k!}, i = 1...N; a = -\ln(Np).$$

In spatial models it is necessary to set two-dimensional distribution of orthogonal coordinates of the NI epicenter $p_2(x_0, y_0)$ and distribution of the radius of the circle $p_0(r_0)$, where NI is observed.

Based on the type of distribution of NI intensity we can distinguish NI with an infinite intensity, with a constant intensity I on the whole scope, and with an intensity decreasing from the epicenter by a certain law $I(r,\varphi)$, in particular, in accordance with Rayleigh rating:

$$I(r, \varphi) = I_0 \exp(-r^2 / ar_0^2), \qquad (17)$$

where I_0 is a maximum intensity in the epicenter, r_0 is a radius of a circle of the NI scope, a is a constant parameter, r and φ are polar coordinates of a point with the origin in the epicenter.

By duration we can distinguish impulse NI (zero duration), with a constant τ and random duration T, set by dis-

Table 2

Factors	NI model						
	1	2	3	4	5	6	7
Scope	point	point	group of points	group of points	area	area	area
Intensity	∞	∞	∞	∞	∞	I_0	I_0
Duration	0	0	0	0	0	τ	τ
Strategy	1	2	1	2	1	1	2

Table 3

Factors	System model				
	1	2	3	4	5
Type of element	Point	Point	Point	Point	Area
Resistance	0	0	0	0	0
System topology	arbitr.	arbitr.	set	set	set

tribution $F_\tau(t)=P(T < t)$. Under a constant duration a range of disturbance I_0 can be set as a time function, for example, using formulas:

$$I_0(t) = I_0^0(1-t/\tau);\ I_0(t) = I_0^0 \exp(-t^2/b\tau^2). \quad (18)$$

where $b = 0{,}3 \div 0{,}5$ is a parameter. Similar dependences are also set under a random duration, only in this case τ in (18) is substituted with a random T.

In case of multiple NI the simplest strategies of the choice of characteristics of a recurrent NI are the strategy of independent NI (strategy 1) and the strategy with an exclusion of affected elements from the scope of a recurrent NI (strategy 2). By the distinguished characteristics different models could be created. Some of them are given Table 2.

System model. *SFA*-model [10] gives a description of technical, functional and algorithmic structure of the system including the models of functioning and characteristics of the elements, system topology, traffic of information, material and energy flows, functional and structure hierarchy, purpose tree.

Let us take a closer look at four characteristics of the model: dimensions of the elements, their reliability, resistance and system topology. In terms of dimensions elements may be point, linear, flat with a boundary of arbitrary shape, solid with a boundary of simply connected surface. In terms of reliability level of the elements, the models can have absolutely reliable elements and the elements of limited reliability. The first case is an idealization used to estimate the survivability by the system state. In terms of resistance we can distinguish the elements with zero resistance and the elements with non-zero resistance. The first case is an idealization which is used in order to consider all elements occurring in the scope of NI to be inoperable. In the second case a probability of disturbance of operability depends on the NI intensity and on the size of the part of area (or scope) of the element that occurred in the scope of NI.

ПIBy the system topology let us distinguish the models with arbitrary and specified topology. A model of the first type can be used with point elements and point NI. The second type model is used with spatial NI and flat or solid elements.

Combinations of three characteristics lead to the models of the system that are listed in Table 3.

A model of physical processes (PP). This model is used for analysis of transient processes in the system after a NI. It describes a trajectory of the process of functioning occurred as the result of its own movement.

A model of primary consequences (PC) is obtained as the result of interrelation of a PP model with a model of NI. Disturbances related to NI are imposed into a PP model, with consideration of deterministic transient processes occurred as the result of own movements and forced movements caused by disturbances, but without any controlling actions of SAs.

A SA model reflects the characteristics of control means, emergency protection, reconfiguration and control. Decision algorithms of struggle for survivability which are the part of this model, form certain controlling actions aimed at the change of a structure and parameters of the system, as well as at the use of internal reserve created for the operation in extreme situations. Characteristics of external SAs should also be considered in this model.

A model of development of primary consequences (DPC) is obtained as the result of combination of a PP model and a SA model. It makes it possible to find a trajectory of the controlled transient process taking into account SA actions. A final objective of the analysis of a DPC model is a determination of a new resilient state of the system. Since certain SA characteristics are probabilistic, the results of DPC analysis can also be represented in a probabilistic form.

A dependability model (D) contains the information about reliability and maintainability of the elements, the system of maintenance, a system response to certain failures of the element, as well as about the influence of different affecting factors of NI on the reliability of the elements. This model is used to estimate the survivability by the results of task execution.

A model of secondary consequences (SC) reflects those late consequences of NI that may occur in the system as the result of reduction of scope of functions and deterioration of technical characteristics. Secondary consequences include a longer time of function performance, a faster ageing and deterioration of the elements, an additional expansion of errors in information systems, an increased consumption of energy and materials for performance of the same functions, and other consequences leading to the reduction of available reserves in the system and to a further degradation of technical characteristics.

A recovery model (R) contains the description of emergency resources, rules and methods of their use in extreme situations in order to recover technical and functional algorithmic structure of the system part which executes the prescribed task. It could be interpreted as a model of the system development after a NI.

A model of the processes of task execution (PTE) is obtained as the result of combination of five models (*SFA*, PP, D, R, SC). The analysis of this model helps to estimate the survivability by the results of task execution.

When developing a system, it would be very useful to provide a developer with a model of decision making (DM) about how to improve survivability, if the estimates show its unsatisfactory level. A model helps to formulate recommendations for developers related to a change of the system structure and parameters, as well as to an additional development of SAs.

7. Calculation and analysis of survivability

When describing the elements we assume that each element may be in one of three states: e_0 – the element

is operable and put into operation; e_1 – the element is operable but is taken out of operation due to different reasons; e_2 the element is inoperable. State transitions are determined by four groups of factors: natural failures of the elements, recovery of operability, switches by actuation of emergency protection and reconfiguration, external disturbances. Connections between ht elements are determined and stationary in time, so the element state could be determined at any time by the state of operability of this element and of the states of other elements. Features of the system operability are permanent in time and help to define the system state by the set of states of its elements.

To calculate the survivability indices we can take one of the following approaches: approach 1 based on a logical and probabilistic method or approach 2 based on the results of theory of random placements including **Morgan and Stirling** numbers.

7.1. Methods of calculation based on logical and probabilistic method

Let as consider the basic stages of the **analysis of the system survivability based on a logical and probabilistic model.**

Stage I. Description of states of elements. For each element two logic variable are set: x_i is an indicator of operability of the i-th element ($x_i = 1$, if it is operable and $x_i = 0$ if it is not), y_i is an indicator of the state of an operable element ($y_i = 1$, if the element is in operation, $y_i = 0$ if it is not). To counter disturbances which affect the elements indicators are set z_{ij} ($z_{ij} = 1$, if a disturbance of the j-th kind affects the i-th element, $z_{ij} = 0$ if it does not) and z_i is a logical sum by all kinds of disturbances. Then the indicators of three states of an element are set:

$$u_{i0} = 1[e_0] = x_i\overline{y_i}\overline{z_i};\ u_{i1} = 1[e_1] = x_i\overline{y_i}\overline{z_i};$$

$$u_{i2} = 1[e_2] = \overline{x_i} \vee x_i z_i. \qquad (19)$$

Stage 2. Construction of logical dependences. Based on the preliminary analysis of dynamic models of physical processes, with consideration of operations of the means of emergency protection, reconfiguration and control, logic equations are constructed in relation to unknown states of operable elements:

$$y_i = f_{yi}(x_k, y_j, z_k, k = 1,\ldots,N; j \in M_i),\ i = 1,\ldots,N, \quad (20)$$

where N is a number of elements in the system, M_i is a variety of elements, neighboring to the i-th element. A set of equations like (20) makes a closed system of logic equations represented in a vector form:

$$Y = f_Y(X,Y,Z) \qquad (21)$$

An advantage of this equation is that when describing s state of an operable element we use only its immediate surround, and it is not necessary to check the whole system. Later these particular and rather simple dependences are used to find an explicit dependence of the state of an operable element on the operability of the rest elements and characteristics of NI.

The system operability id determined by operability of its elements and by dependences (21). For many systems the main state is the state of relatively small group of output elements. However, due to the availability of indirect connections reflected in (21), the system operability is determined by the state of all other elements as well. For a single-functional system a logic function of operability (LFO) is written as

$$F = f(X, Y, Z) \qquad (22)$$

In a multi-functional system the dependence (22) is constructed for each function separately. If simultaneous performance of all functions is required, then

$$F = \underset{(i)}{\&} f_i(x, y, z). \qquad (23)$$

where f_i is a logic function – the indicator of performance of the i –th function of the system. This method of description of the system state does not required a combinatorial enumerating of all states of the elements, and functions f_i are formally found from the systems of logic equations.

Stage 3. Solution of logic equations. Equation system (21) is linear and it can be transformed into:

$$y_i = a_i \vee a_{i1}y_1 \vee a_{i2}y_2 \vee \ldots \vee a_{iN}y_N;\ a_{ii} = 0, \qquad (24)$$

where a_i and a_{ij} are the coefficients expressed through x_i and z_i. There are different ways to solve logic equations, including a method of determinants, substitution method, matrix method, etc. The method of determinants, as well as its application in relation to dependability is described in paper [11]. Solution (24) in form of $Y = g_Y(X,Z)$ should be put into (22) or (23) and obtain an explicit expression

$$F = f(X, g_Y(X,Z), Z) = g(X,Z). \qquad (25)$$

Solution of the system of logic equations should be carried out repeatedly: one time for a basic structure S_0, when all $z_{ij} = 0$, and several times more, depending on the number of different types of disturbances. Searching through all variants under a single and multiple impacts, it is possible to obtain a complete set of operable structures in the system. Function (25) allows for analysis of d- and m-survivability by means of enumerating of the vector of states of the elements.

Stage 4. Probabilistic description of the elements and external disturbances. Each element is represented in a

probabilistic model by probability $p_i = P(x_i = 1)$ that at this moment or at any arbitrary moment the element of operable. When disturbance $z_{ij} = 1$ occurs, the resistance of the i-th element in relation to the j-th disturbance can be taken into account using probabilities α_{ij} that an element will keep its operability in case of disturbance. Besides, the probabilities are set that an element will occur in the scope of the j-th factor of NI.

Stage 5. LFO conversion to a form of transition to substitution. According to [8] we can distinguish the forms of transition to a total and partial substitution. Forms of transition to a total substitution are a full disjunctive normal form, a noniterated form in a "joint-denial" basis, a disjunction of orthogonal noniterated forms. After the reduction to one of these forms, a one step substitution of logic variables and logic operations with probabilities and arithmetic operations is made. If such conversions are difficult to realize due to their complexity, one can use a form of transition to a partial substitution. Current varieties of these forms and conversion rules are listed in [8].

Stage 6. Writing a mixed form. Substitution of noniterated variables in the conversed LFO is a partial substitution as the result of which certain logic variables and operations are substituted with probabilities and arithmetic operations, and the rest variables and operations transit into the indices of arithmetic expressions. The obtained form is called a mixed form because it contains logic variables and probabilities and two groups of operations: logic and arithmetic. Methods and algorithms of transition to a mixed form are described in [11].

Stage 7. Determination of survivability indices. Multistep substitution of logic variables in mixed forms constructed for a basic structure S_0 and other operable structures S_i is used to find probabilities $P(t/S_0)$ and $P(t/S_i)$, and then formula (8) is used to find a conditional function of survivability $G_i(t)$. Formulas (9) – (12) are used to find a function of survival, absolute survivability function, average number of NI.

For the systems of branching structure after stage 6 it is necessary to perform three more stages (stages 8, 9 and 10) and only then get back to stage 7.

Stage 8. Constructing a generator polynomial of the distribution of probabilities of states of the i-th branch [11]:

$$\Phi_i(z, X) = 1 + (z-1)Q(X), \tag{26}$$

where $Q(X) = P\{F(X) = 0\}$ is a mixed form, X is a vector of non-substituted logic variables.

Stage 9. Constructing a generator polynomial for the system. If the structure is isotropic a polynomial (26) is raised to a power equal to a branching coefficient at a bottom layer of a branching structure. Then logic variables of the next layer are substituted, and again raising to a power, substitution, etc. As the result of a multi-step procedure we obtain a polynomial whose coefficients express probabilities that certain amount of branches is inoperable. If the structure is not isotropic, a raising into a power is substituted by multiplying of polynomials.

Stage 10. Determination of survivability indices. Stage 9 includes distributions $P(t/S_0)$ and $P(t/S_i)$, then scalar indices $\varphi(P(t/S_0))$ and $\varphi(P(t/S_i))$ are calculated, formulas (9) – (15) are used to find $G_i(t)$, $G(t,n)$, $G(t)$ and other survivability indices.

7.2. Estimation of survivability by the system state based on the theory of random placements

Let a two-pole system contain k subsystems and N point elements with arbitrary connections and have the LFO

$$F = f(X),\ X = \{x_1, x_2, \ldots, x_N\}$$

The system is a subject to the flow of n point independent NI with equally probable affection of each element at the occurrence of NI. We consider the elements resistance to be 0, and the intensity of NI is insufficient to ensure a transition of the element that occurred in the scope of NI, to an inoperable state. Let us estimate the survivability by indices (2) – (6).

Survival rate of the system with a n-tuple NI can be represented as follows

$$R(n) = \sum_{X \in X_1} P(X \mid A_n) = P\{F = 1 \mid A_n\}, \tag{27}$$

where X_1 is a subset of vectors X, corresponding to operable states of the system. Probability $P(X / A_n)$ is found by formula:

$$P(X \mid A_n) = \sum_{\vec{n} \in M_n} P(\vec{n}) P(X \mid \vec{n}), \tag{28}$$

where $\bar{n} = (n_1, n_2, \ldots, n_k)$ is a vector of the number of NI affecting k subsystems, M_n is a set of vectors that fulfill condition $n_1 + n_2 + \ldots + n_k = n$. Probability

$$P(\bar{n}) = \frac{n!}{n_1!\, n_2! \ldots n_k!} \gamma_1^{n_1} \gamma_2^{n_2} \ldots \gamma_k^{n_k}, \tag{29}$$

where γ_i is a probability that the i-th subsystem is within the scope of NI. In particular, it can be that $k = N$. At an equally probable affection of the elements formulas (27) – (29) could be clarified.

By representing LFO as an orthogonal disjunctive normal form

$$F = \bigvee_{i=1}^{m} Q_i, \tag{30}$$

we shall write (27) as follows

$$R(n) = \sum_{i=1}^{m} P(Q_i = 1 \mid A_n). \tag{31}$$

For implicants with $l_i = 0$, 1 or 2 denials, formulas in (31) can be written in explicit form:

$$P(Q_1 = 1 \mid A_n) = (1 - s_1 / N)^n, l_1 = 0, n \geq 1, \quad (32)$$

$$P(Q_i = 1 \mid A_n) = \sum_{j=1}^{n} C_n^j (1 - s_i / N)^{n-j} / N^j, l_i = 1, n \geq 1,$$

$$P(Q_i = 1 \mid A_n) = \sum_{k=2}^{n} \sum_{j=1}^{k-1} C_k^j (1 - s_i / N)^{n-k} / N^n, l_i = 2, n \geq 2,$$

where s_i is a number of letter in implicant Q_i . These formulas refer to a particular case of (29) with k = 2 and different values of n_1 and n_2 .

7.3. Estimation of survivability by the system state based on a combinatorial method

A basic structure S_0 is used to define all possible operable structures S_i, i = 1, …, N_p. then:

$$R(n) = \sum_{j=1}^{N_p} r_j(n) / N^n = r_n / N^n, \quad (33)$$

where $r_j(n)$ is a number of cases when S_j structure occurs at a n-tuple NI. This number is defined by formula

$$r_j(n) = \sum_{(k)} L_{nk} B_{kj}, \quad (34)$$

where L_{nk} is a number of conversions from n elements of k kinds, B_{kj} is a number of different vectors X with k zeros that lead to S_j structure. Since parameters d and m from formulas (3) and (4) are usually very large, it is not difficult to find B_{kj} by simple enumeration of vectors. A maximum number of vectors under test is mN , but in practice it is much smaller.

Numbers L_{nk} are so called **Morgan** numbers. They are related to **Stirling numbers of the second kind** by formula

$$L_{nk} = k!\, S_{nk}, \quad (35)$$

where S_{nk} could be found using a recurrence relation

$$S_{nk} = S_{n-1,k-1} + k\, S_{n-1,k};\ S_{nk} = 0 \text{ with } n < k;\ S_{nn} = 1. \quad (36)$$

But numbers L_{nk} could be calculated by formula:

$$L_{nk} = \sum_{i=1}^{k} C_k^i i^n (-1)^{k+i}. \quad (37)$$

We obtained the result of this paragraph already in 1987. In the course of research work we also obtained calculation formulas for the case of r-tuple NI and the systems with L-resistant elements **[20]**.

References

1. GOST 19176-80. Control systems of ship's equipment. Terms and definitions.

2. Dictionary of cybernetics. Edited by V.M. Glushkov. – Kyiv: Chief editorial board of the Ukr. Sov. Encyclopedia, 1979.

3. Great Soviet Encyclopedia, Vol. 9. – M.: Soviet Encyclopedia, 1972. – 570 p.

4. dependability of energy systems: Terminology. Collection of recommended terms. – Issue 95. – M.: Science, 1980. – 42 p.

5. Gorshkov V.V. Logical and probabilistic method of calculation of survivability of complex systems. – AS UkrSSR, Cibernetics, 1982, Mo.1. – P.104-107.

6. Rudenko Y.N., Ushakov I.A. Dependability of energy systems. – M.: Science, 1986.- 252 p.

7. Volik B.G., Ryabinin I.A. Efficiency, dependability and survivability of control systems // Automation and remote control. -1984.- No. 12.

8. Ryabinin I.A., Cherkesov G.N. Logical and probabilistic methods of study of dependability of structural complex systems. – M.: Radio i Svyaz, 1981. – 238 p.

9. Cherkesov G.N. Methods and models of estimation of survivability of complex systems. – M.: Znanie, 1987. – 55 p. – On web-site also: http://www.gcherkesov.com/articles/article02.pdf .

10. Cherkesov G.N. Dependability of hardware and software complexes. – SPb: Piter, 2005. – 480 p.

11. Rudenko Y.N., Ushakov I.A., Cherkesov G.N. Dependability of energy systems and their equipment. Reference guide in 4 volumes edited by Y.N. Rudenko. Vol. 1. Reference guide for general models of analysis and synthesis of energy systems. – M.: Gosatomizdat, 1994. – 474 p..

12. Bodner V.A. Systems aircraft control. – M.: Mashinostroenie, 1973. – 240 p.

13. Ryabinin I.A. Three pillars of navy: dependability, survivability, safety. – Novocherkassk: Temp, 2006. – 116 p.

14. Simakov I.P., Merzlyakov V.A. Choice of functional and algorithmic structure of ship control systems by the criteria of fail-safety and dependability – Ship industry. Series "Automation and remote control", issue. 5, 1987, p. 52 – 60.

15. Nedosekin A.O. About a demonstration of the "vitality" property in technical, economic and social systems. – On site also: http://an.ifel.ru/docs/Vitality_110416.pdf .

16. Marsh T. (ed.). Critical Foundations: Protecting America's Infrastructures. Technical report, President's Commission on Critical Infrastructure Protection, October 1997.

17. Muller G., Koslowski T. and Accorsi R. Resilience – a New Research Field in Business Information Systems? – On site: http://www2.informatik.uni-freiburg.de/~accorsi/papers/bis13.pdf .

18. ResiliNets Initiative (University of Kansas and Lancaster University, USA). – On site: https://wiki.ittc.ku.edu/resilinets/Main_Page.

19. Nedosekin A.O., Reishakhrit E.I. Mobilization economy in the Russian way. – SPb: SPbSTU, 2013. – On web-site also: http://an.ifel.ru/docs/Mob_AN_ER.pdf .

20. Nedosekin A.O. Application of random placement theory on relation to the analysis of survivability of technical systems // Cibernetics of AS USSR. 1991. No.6.

21. Nedosekin A.O., Cherkesov G.N. Estimation of survivability of energy systems under strike conditions // dependability and quality control, 1992, No. 11. – P. 51 – 62.

22. Nedosekin A.O., Abdoulaeva Z.I. Mobilized economy fuzzy model // Proceedings of International Conference on Soft Computing and Measurements, SCM 2015, 7190479, pp. 267-268.

About the authors

Gennady N. Cherkesov – Dr. Sci., professor, professor of Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia,

e-mail: gennady.cherkesov@gmail.com

Alexey O. Nedosekin – Dr. Sci., Ph.D., academician of the International Academy of Ecology, Man and Nature Protection Sciences, professor of National Mineral Resources University “Gorny”, St. Petersburg, Russia,

e-mail: apostolfoma@gmail.com