Journal of AppliedMath 2023; 1(1): 68.
Original Research Article

Towards a solution to the problem of safety management of structurally complex systems

Alexander V. Bochkov

Scientific Secretary of Scientific and Technical Council, JSC NIIAS, Moscow 109029, Russia. E-mail: a.bochkov@gmail.com

ARTICLE INFO

Received: 13 March 2023
Accepted: 18 April 2023
Available online: 5 May 2023

http://dx.doi.org/10.59400/jam.v1i1.68

ABSTRACT: The non-isolation of modern, structurally complex, multipurpose systems implies not only their interaction with the external environment, but also the impact of this environment on the systems themselves. The ability to predict and assess the consequences of these impacts, which are characterised by great uncertainty about the time, place and method of implementation, as well as the choice of a particular object of influence, is a task of extreme urgency in today's globalised world. If the stability of functioning of any structurally complex system is understood as the achievement by it of the purpose of its functioning with acceptable deviations on the volumes and times of implementation of private tasks, the safety management in this system is reduced, in fact, to minimisation of unplanned losses at the occurrence of abnormal situations of various kinds and to carrying out of measures for their prevention. The success of such tactics depends largely on the effectiveness of the risk management system, on the ability of decision-makers to foresee the possibility of poorly formalised threats turning into significant risks, i.e., on having methods and tools for ranking threats and significant risk factors. Inevitably, there is the task of setting protection priorities, ranking objectives (usually of different types), problems and threats, and reallocating available (usually limited) resources. The article considers the issues involved in building an integral security model that takes into account the risks to the assets being protected.

KEYWORDS: structurally complex system; objects of protection; security threat; risk; system significance; integral assessment

1. Introduction

Ensuring the security of any object implies a certain set of measures to counter threats to that object, i.e., the concept of threat is fundamental because the security system is based on it. The resolution of the uncertainty associated with the implementation of threats is achieved by building a security system based on the so-called principle of equal protection. This principle underlies, for example, the development of requirements to ensure the security of critical transport infrastructure. The concepts considered in connection with the definition of threats allow to build the basic scheme of their interaction in the form of a model of threats to a separate object, group or class of homogeneous objects. For example, compressor stations of gas transportation systems can be recognised as homogeneous objects with respect to the spectrum of threats to critical elements of their infrastructure, since all types of these objects have the same infrastructure according to the intrasectoral classification and differ from each other only by the scale of production activities and the characteristics of individual critical elements.

Both domestic and foreign researchers have paid attention to the problems of safety and stability studies of structurally complex technical systems. The reliability of technical systems and methods of their risk assessment were developed by Kumamoto and Henley[1]. Vemuri[2] considered typical characteristics of complex technical systems widely spread in the national economy, indicators of their efficiency, reliability, quality of management. In his works a lot of attention was paid to methods of modelling the most important classes of complex systems (mass service systems, discrete and continuous production processes). Interesting are the later studies of Rainshke and Ushakov[3,4], in which they applied traditional models and approaches of reliability theory to solve problems of rational allocation of resources for protection of critical infrastructure objects. The logical and probabilistic approach to the analysis of reliability and safety of structurally complex systems was developed by Ryabinin[5], Solozhentsev[6], and Mozhaev *et al.*[7]. Glushkov *et al.*[8] introduced a new class of dynamical models based on nonlinear integro-differential equations with prehistory. They developed approaches to modelling so-called evolving systems, proved theorems on the existence and uniqueness of solutions describing their systems of equations.

In their papers, Ushakov[9–11] and Levitin[12] presented innovative approaches to the problem of protecting large numbers of critical facilities.

The work of these and many other authors has allowed us to view safety as a control problem. Since in most cases, the causes of an abnormal situation are combined; only part of the uncertainty that can be explained separately by external or separately by internal causes can be statistically eliminated. This problem can be solved by applying principles known from simulation and similarity theory.

Risk analysis is the only way to investigate those safety issues that cannot be answered by statistics, such as accidents with low probability of occurrence but high potential consequences. Of course, risk analysis is not the solution to all safety problems, but it is the only way to compare risks from different hazards, highlight the most important ones, choose the most efficient and cost-effective systems to improve safety, develop measures to reduce the consequences of accidents, etc. It is important to remember that risk analysis issues cannot be considered separately from game formulation. Today, however, the main formulas used in risk analysis have been greatly simplified and their affiliation to game theory has almost been forgotten. Risk, as a dynamic property depending on time, means and information, has been reduced to "two-dimensional estimates" of probability and damage. It is possible to say that in modern risk analysis the theories of durability and reliability are "left", but research on the theory of survivability, the theory of homeostasis, adaptive theories, including the theory of choice of decisions, the theory of perspective activity, the theory of reflexes, the theory of self-organising systems and others is curtailed.

2. General formulation of the safety management problem

The non-isolation of a complex system implies its interaction with the external environment and the impact of that environment on it. This impact can be interpreted in a very broad sense: it can be natural disasters (e.g., earthquakes leading to the destruction of dams and other structures), large-scale accidents (e.g., an explosion in a nuclear power plant leading to the disruption of electricity supply to the entire region), as well as illegal actions, where the range of impact is the widest. Such malicious external influences are characterised by great uncertainty about the time, place and method of execution, as well as the choice of a specific object for the action.

The importance of the object to the initiator of such an "active action" coincides with the importance of that object to the owner of the system. More important objects require a higher level of protection because actions against them lead to more serious losses. It follows that the assessment of the systemic importance of the objects of a complex open-ended dynamic system should be carried out using the mathematical apparatus of game theory and, more generally, the theory of conflicting systems.

The first work formulating the principles of scientific analysis of actions in conflict situations, a book by Morgenstern and von Neumann[13], was published in 1944. It unleashed a flood of mathematical research on games and solutions, which contributed significantly to the development of rules of optimal behaviour for a wide class of conflict situations, i.e., the development of optimal management strategies. Game theory, as it has developed to the present day, is inevitably normative in nature: the player applying it learns what he must do, what strategy he must choose, in order to secure a favourable outcome. But like many abstract mathematical models, the game-theoretic model of conflict is limited[14]. It cannot reveal the nature of conflict, the hidden sources of human activity in a conflict situation.

It is possible to put oneself in the position of one of the parties and to seek actions aimed at achieving a certain goal. In doing so, we must take into account the opposition of the opponent, whose goal is the opposite of ours. If, in this situation, we choose one of the possible strategies of behaviour, it is necessary to have a justification that this strategy is the best. We encounter this type of scheme when solving problems in operations research[15]. Since we rarely have all the necessary information about the "opponent" (about his goals, resources and strategies), we have to make decisions under conditions characterised by this or that degree of uncertainty, i.e., by the degree of ignorance of the party making the decision (i.e., the decision-maker (DM)) about these conditions. According to the information available about the "enemy" in the study of operations, the choice of strategy is usually based on the principle of a guaranteed result: whatever decision the "enemy" makes, the "defending" party must be guaranteed some gain. The conflict situation, although included in the model of an operation planned by one of the parties, is not the subject of independent research. In the specific tasks of operations research, the activity of the conflicting parties is not considered as a special type of human activity, and the conflict as such serves only as a background against which the actions of the parties are projected.

In mathematical game theory, the problem is much the same. Whether it is a real opponent or nature, the object of study is the choice of strategy, the choice of behaviour. The principle of a guaranteed outcome in game theory is concretised in the criteria for choosing a solution. The difference may be that "game theorists" work with game models from the position of objective research (both sides act in the model as equal partners), while researchers of operations necessarily take the position of one of the sides.

3. Model of the impact of on objects

We can assume that the importance of the object to the system and to the intruder is in most cases the same, which means that the required level of object protection must be determined by considering the nature of possible attacks. Three sources, or combinations thereof, can be considered as such attacks.

Firstly, the most common "local crime" and related offences that affect the economic activity of facilities is usually theft. It also includes hooliganism (vandalism) and protest actions. The level of such crime is likely to correlate with the level of general crime in the region where the facility is located. The latent (hidden) part of this type of crime can be measured quite adequately by indicators such as the unemployment rate, the proportion of migrants and the educational level of the population.

Second, there is the migration of domestic criminal and terrorist activity. Zones of active terrorist activity tend to grow: along with the migration of able-bodied people from "hot spots", criminal groups "squeezed out" by law enforcement also migrate. The most telling indicator of this profile is the distance of the facility from areas of increased terrorist activity.

Third, these are specially trained terrorist and subversive groups, sent in whole or in part in the form of instructors from abroad. The actions they carry out are characterized by well-thought-out, preparedness and non-randomness (the planned nature of the activity and the weighted measurement of the feasibility of one or another action to inflict damage).

To solve the problem, the following approach is proposed by Bochkov[16,17]. Violators are classified according to their level of preparedness j $(j = 0,1, \dots, J)$. Zero level $(j = 0)$ corresponds to the lowest level of preparedness. A maximum level $(j = J)$ corresponds to a super-prepared subversive group. Let us assume that an attack by an attacker of j-th level will require Z_j units of resources. It is natural to assume that the higher level j is, the more resources are needed Z_j (a more serious attack requires from intruders fundamentally more resources for its preparation: time, qualified personnel, studying functioning of objects and their security systems, etc.). It is also natural to suppose that the total resources of criminal world are limited (fighters, equipment, weapons), and hence the model of integral profile of intruders will be a tuple of number (intensity) of attacks of appropriate level of preparedness $\vec{N} = \{N_0, N_1, \dots, N_J\}$ taking into account the above-mentioned limitations:

$$\begin{cases} N_j \le N_{j,\max} \ (j = 0,1, \dots, J), \\ \displaystyle\sum_{j=0}^{J} \left(N_j \times Z_j\right) \le Z \,, \end{cases} \tag{1}$$

where Z is the total amount of money allocated by crime to prepare and execute attacks on facilities.

The system of restrictions Equation (1) allows us in the problem under discussion to discard "extreme" variants, namely: the conditions of a terrorist or subversive "war", when the value Z is large, as well as the conditions of a mass upsurge of low-preparedness crime (large $N_{0,\max}$, i.e., in other words, the system under study is not like a supermarket in terms of consumer value, so that the population rushes to "disperse valuables" available at its facilities). Dangerous industrial facilities, due to their fire and explosion hazard, are also remote enough from populated areas that they could be affected by a surge of vandalism.

Thus, in solving the problem of determining the systemic importance of targets, the criminal underworld is seen as a source of a variety of external attacks on targets, but a source that still has limited resources. High and medium level attacks pose the greatest threat. It is reasonable to assume that the criminal underworld will use the full range of its capabilities, i.e., we should expect both major attacks, which would "economically bankrupt" the owner, forcing him to spend excessive resources on reinforcing the physical protection of his facilities, and medium-prepared attacks, since over-prepared attacks are not feasible if the owner does not have the resources to protect all his facilities. For example, the level of protection of nuclear facilities for a system consisting of thousands of facilities is, in principle, unattainable.

In addition, crime is an active player: the choice of a target for an attack and a suitable way of carrying it out is an inherent advantage. At the same time, crime has an incomplete and inaccurate understanding of the current state of protection of the targets to be attacked, as well as the amount of damage it will cause if the attack is successful. These two nuances will be taken into account in further reasoning when formulating an optimisation problem that matches the attacker model with the target model.

4. Protection profile model

So, consider some (k-th) object. As a result of the supposed attack of intruders of this or that level of preparation to this object, through its complete (or partial) loss of serviceability, a certain damage will be caused. Let us denote it by X. Given that not every attack a priori leads to the success of the attacker, the protection profile of the k-th object can be described by interval representations by setting four matrices:

$$Q_{\min}^{[k]}(i,j), Q_{\max}^{[k]}(i,j), X_{\min}^{[k]}(i,j), X_{\max}^{[k]}(i,j) \tag{2}$$

where i ($i = 0,1,\dots,I^{[k]}$) level of protection of the k-th object (the zero level ($i = 0$) corresponds to the current state of protection).

The interpretation of the matrix elements is as follows: if the specified object k with defense level i will be attacked by an adversary with preparedness level j, then with probability from $Q_{min}^{[k]}(i,j)$ to $Q_{max}^{[k]}(i,j)$ the whole system will be damaged with probability from $X_{\min}^{[k]}(i,j)$ to $X_{\max}^{[k]}(i,j)$.

Clearly, the values of Equation (2) will increase as the level of preparedness of the "attacker" j increases and will decrease as the level of defense of the object i increases.

It is obvious that protection at any level requires certain material costs both on the part of the owner and the state. Let's denote the cost of creating and maintaining object protection k at the i-th level as $Y^{[k]}(i^{[k]})$.

Since the total resource allocated to protect all objects is limited, the inequality must be satisfied:

$$\sum_{k} Y^{[k]}(i^{[k]}) \le Y \tag{3}$$

where Y is the sum of all costs for the protection of objects under the assumption that for each object k the variant of protection system is chosen $i^{[k]}$.

If criminals did not have the advantage of target selection and attack options, that is, if criminality were indiscriminate like nature or technological failures, then the "optimal" security profile of objects could be achieved through the sequential execution of the following algorithm:

Step 1. Estimate the probabilities $\lambda^{[k]}(j)$ of each k-th object being attacked by an adversary *of j*-th level of preparedness;

Step 2. Calculate the median value of the risk of an enemy attack on the k-th object j of level of readiness for the $i^{[k]}$-th variant of realization of the defense system of the object:

$$R[k;i^{[k]}] = \sum_{j=0}^{J} \left\{ \lambda^{[k]}(j) \times \left(\frac{Q_{\min}^{[k]}(i^{[k]},j) + Q_{\max}^{[k]}(i^{[k]},j)}{2} \right) \times \left(\frac{X_{\min}^{[k]}(i^{[k]},j) + X_{\max}^{[k]}(i^{[k]},j)}{2} \right) \right\} \tag{4}$$

Step 3. Determine the amount of risk averted per unit of funds invested in protection $\theta[k,i^{[k]}]$:

$$\theta[k,i^{[k]}] = \frac{R[k,i^{[k]}]}{Y^{[k]}(i^{[k]})} \tag{5}$$

Step 4. Select for each k-th object the maximum of the values $\theta[k,i^{[k]}]$:

$$\theta[k,i^{*[k]}] = \max_{i^{[k]}} \{\theta[k,i^{[k]}]\} \tag{6}$$

i.e., at the chosen variant $i^{*[k]}$ the maximum risk reduction per unit of invested funds for the k-th object is observed.

Step 5. Make a ranked list of objects, placing them in descending order of the value of the indicator $\theta[k,i^{*[k]}]$ and then count the first $\widetilde{K}$ objects in the list such that the total cost of their protection is invested in the allocated funds

$Y$and for the $(\widetilde{K}+1)$-th object the resources are not enough.

The essence of the above procedure is simple and straightforward: it makes no sense to seek funds for additional protection for those objects that are not threatened by anything (the threat values of attacks are small $\lambda^{[k]}(j)$). It is inexpedient to additionally protect those objects whose temporary loss of functionality has almost no effect on the value of total losses (i.e., small $X_{\max}^{[k]}(i^{[k]},j)$). And finally, additional protection is unreasonable for those objects that are already so well protected that the reduction of losses can be achieved in principle, but by inadequately large means (i.e., small values $\theta[k,i^{*[k]}]$).

The key point of the algorithm described above is the compilation of a ranked list of objects by the criterion of minimizing the mathematical expectation of loss per unit of investment in their protection (in their sustainable functioning).

The Equation (4) clearly shows the need to collect and estimate data on three components: on the values of losses caused by the implementation of attacks $X_{\min}^{[k]}(i,j)$, $X_{\max}^{[k]}(i,j)$ and the indicator of "aggressiveness of criminal environment" $\lambda^{[k]}(j)$ and on the dependence of risks on types of objects k.

The values of losses X, due to the fact that the objects of a complex system are not autonomous, should reflect the system effect (or socioeconomic multi-effect), which increases significantly depending on which of the consumers of the products of the attacked object will suffer due to the reduction of its performance. Consequently, it is necessary to consider not the average, but the upper limits of damage indicators and to introduce an additional fourth component—the indicator of the importance of continuous operation of the object in connection with the cascade effect of strengthening the consequences of the object performance loss for other objects of the system and other objects of other systems interacting with it.

Finally, the model additionally requires the introduction of another component, the need for which is due to the fact that the adversary implements an active, targeted choice of attack, while having value factors and priorities unknown either to security experts or to the competent authorities of the state, which shift values $\lambda^{[k]}(j)$ from the "weighted average" (e.g., by industry). Sometimes, these "additional" values are specific: terrorists, for example, are prone to excessive bloodshed and hostage-taking, ritual murder, etc. Often, the systemic importance of protection of specific facilities temporarily increases during the stay there of the first persons of the state, ministers, especially during the commissioning of politically important production facilities not only internationally, but also regionally within the country. These circumstances should be taken into account and an additional component, the correction factor, should help. $\mu^{[k]}$, initially equal for all objects to unit, and which can be, according to LDP or experts, increased so that to increase the priority of inclusion of k-th object in the list of objects, equipped with additional protection measures for the reasons, not considered by rules, common for all objects. To some extent, the expediency of introducing the indicator $\mu^{[k]}$, becomes clearer from the following composition of the two models considered above.

5. Integration model

So let $\tilde{Z}$ an estimate of the total resource available to the forces interested in violating the security of some objects. If $\tilde{Z} < Z$, then the defending party underestimates the adversary's capabilities; if $\tilde{Z} > Z$, on the contrary, there is an overestimation of his forces. Further we will assume that at the moment of choosing the attack, the intruder has his own ideas about the amount of resources allocated by the owner to protect his objects, i.e., he also has some ideas about how the “zero option” known to him could have changed.

Intruders have the right to choose targets, and they are able to choose the sets of objects they will attack. Let their choice be based on their own model of expected damage, that is, they have four analogous Equation (2) matrices at their disposal for each of the objects: $\tilde{Q}_{\min}^{[k]}(i,j)$, $\tilde{Q}_{\max}^{[k]}(i,j)$, $\tilde{X}_{\min}^{[k]}(i,j)$, $\tilde{X}_{\max}^{[k]}(i,j)$ and their own idea of how many resources $\tilde{Y}$ is spent by the owner to protect all objects in the system. Similarly, if $\tilde{Y} < Y$, then the adversary underestimates the ability to protect the objects and, if $\tilde{Y} > Y$, then he overestimates them.

Obviously, the estimates $\tilde{Q}_{\min}^{[k]}(i,j)$, $\tilde{Q}_{\max}^{[k]}(i,j)$, $\tilde{X}_{\min}^{[k]}(i,j)$, $\tilde{X}_{\max}^{[k]}(i,j)$ can also be both overestimated and underestimated by intruders; nevertheless, in accordance with their right of choice, they choose such a set of objects for attack and such options of intruder preparedness for each object, at which the maximum damage is caused.

Let us denote the characteristic function by $\delta^{[k]}(i,j)$, which means that against the k-th object with the expected level of protection i ($i = 0,1,\dots,I^{[k]}$), the attack of level j ($j = 0,1,\dots,J^{[k]}$) is chosen. If for all i ($i = 0,1,\dots,I^{[k]}$), values of $\delta^{[k]}(i,j)$ are equal to zero, then the k-th object will not be subject to an attack level of *j*. If for all *j* and all *I*, values of $\delta^{[k]}(i,j)$ are equal to zero, then the k-th object under the enemy’s assumed targeting variant is completely dropped from the target list.

If for some $\tilde{\imath}$, value $\delta^{[k]}(\tilde{\imath}, j(\tilde{\imath})) = 1$, we consider that the object k with defense level 0 is chosen by the adversary as a target for an attack with the preparedness level $j(\tilde{\imath})$.

The listed properties are written down by a system of equations:

$$\begin{cases} \forall k \forall i \forall j \ \delta^{[k]}(i,j) \times \left(1 - \delta^{[k]}(i,j)\right) = 0, \\ \forall k \left(\sum_{i=0}^{I_k} \sum_{j=0}^{J} \delta^{[k]}(i,j) - 1\right) \times \left(\sum_{i=0}^{I_k} \sum_{j=0}^{J} \delta^{[k]}(i,j)\right) = 0 \end{cases} \tag{7}$$

Considering that

$$\forall j \sum_{i=0}^{I_k} \sum_{k} \delta^{[k]}(i,j) = N_j \tag{8}$$

and supplementing Equations (7) and (8) with a system of constraints in Equation (1), then we obtain an estimate of the total damage to the object:

$$\tilde{R} = \sum_{k} \sum_{i=0}^{I_k} \sum_{j=0}^{J} \left\{ \delta^{[k]}(i,j) \times \left(\frac{Q_{\min}^{[k]}\left(i^{[k]},j\right) + Q_{\max}^{[k]}\left(i^{[k]},j\right)}{2} \right) \times \left(\frac{X_{\min}^{[k]}\left(i^{[k]},j\right) + X_{\max}^{[k]}\left(i^{[k]},j\right)}{2} \right) \right\} \tag{9}$$

Let us denote $\tilde{R}$ as $\tilde{R}(Var_I, Var_J)$, underlining that $\tilde{R}$ depends on both the variant of defending objects Var_I, and on the variant of the attack Var_J.

Looking for the maximum $\tilde{R}$ for all variants of attacks satisfying the constraints, when considering all variants of equipping with additional protection as parameters:

$$\tilde{R}^*(Var_I) = \max_{Var_J} \{\tilde{R}(Var_I, Var_J)\} \tag{10}$$

Thus, it is postulated that the adversary chooses the worst option for the defending party. Consequently, the problem of defense comes down to limiting the set of choices for the adversary—we look for such a reinforcement of objects that minimizes $\tilde{R}^*(Var_I)$. That is, the security management problem is reduced to find an equilibrium value $\tilde{R}^{**}$:

$$\tilde{R}^{**} = \min_{Var_I} \{\tilde{R}^*(Var_I)\} \tag{11}$$

The proposed formulation has the typical form of game theory problems. The solution of this problem is a Nash equilibrium—saddle point (Var_{I^*}, Var_{J^*}):

$$\tilde{R}^{**} = \tilde{R}\left(Var_{I^*}, Var_{J^*}\right) \tag{12}$$

At this point, it is not advantageous for the defender to change his equipment strategy Var_{I^*}, because outside of this strategy, the opponent has opportunities for more "sensitive" strikes.

At the same time, it is not advantageous for the attacker to change his plan $Var_{J^*}(Var_{I^*})$, because any change leads to a reduction in the total damage it seeks to inflict on the individual objects of the system, and through them the entire system and the state as a whole.

The problem in this formulation theoretically has a very large dimension, has great combinatorial complexity, but is quite solvable due to the monotonicity of the criteria used and the linearity of the constraint systems.

The main problems in solving this problem are of an information-technological rather than a mathematical nature:

- For each k-th object, it is necessary to have estimates of the consequences of possible enemy attacks of different levels of preparedness j, which is not yet achievable in practice;
- For the whole system, it requires consideration of the risks to which objects are exposed, in a set of possible, including poorly formalized threats: the more effective optimization of protection is the more accurate the assessment of the potential capabilities of the enemy (and they are heterogeneous in both the technological and the regional aspect).

Within the framework of the considered statement, which takes into account the complex impact of a potential adversary, radically changes the understanding of assessing the effectiveness of defense systems. Thus, due to the limited resources available to intruders, it is natural to expect them to shift their targeting from well-protected objects (with low expected effectiveness of attacks) to less protected objects (with greater effectiveness, but with less one-time damage).

Obviously, it is irrational to additionally protect facilities that are not attacked. Perhaps that is why they are not attacked, because routine work is being done to reinforce the guards. Another key element of the problem under consideration is that the search for effective solutions on both opposing sides lies largely in the information plane:

- The criminal, when preparing to attack a target, ideally looks for accomplices to help him choose a target that is achievable given his level of preparation and equipment;
- The defense system would have been capable of more concentrated counteraction if it had known the intentions of crime.

That is wh,y in the description of the abovementioned procedure, it has been repeatedly emphasised that we are talking only about assessments on both sides. Because of the irreducible uncertainty of the assessments, as a solution of the problem of working out the strategy and tactics of strengthening the protection of objects against possible illegal actions, including terrorist acts and attacks of subversive groups, it is reasonable to "load" the game statement[14]. In this coarsening, we should "idealise the enemy's capabilities" and toughen the characteristics of possible losses, for example, by switching from median to maximum risk estimates.

As noted above, the adversary's development of a plan begins with the procedure for selecting targets, i.e., their ranking. Since the meaning for the "attacker" and the "defender" is usually the same, let us consider the problem of ranking in more detail.

6. Model for assessing the level of impact of negative factors and justification of the scale of measurement of threats to the stability of the functioning of facilities, taking into account their specifics

Many current rating systems are based only on the results of the evaluation of one of the indicators describing the objects (for example, the activities of economic subjects, and their criticality)[19,20].

However, in practice, both criticality and unconditional vulnerability of objects (in the problems of ranking objects by their system significance and ensuring safe functioning of these objects) are composed of a large number of assessments by private criteria. The importance of these criteria is not known in advance and the problem of multicriteria ranking[21,22] under conditions of uncertainty[23,24]. This is very important for the analysis of systems of with different purposes[25,26].

6.1 Selection function language

Let us define on some set of objects $O = \{o_1, \dots, o_D\}$ a logical function $\pi: \pi(o) \to \{0,1\}$, which indicates that the alternative o is mapped to some subset of $\pi(o)$ ($\pi(o) = 1$) or not ($\pi(o) = 0$). The function $\pi(o)$ will be called *the selection function*. The subset $\pi(o)$, in particular, can be a subset of the most systemically important critical infrastructure objects (CIPOs) or a subset of objects for which it is potentially necessary to implement additional protection measures. In general, the selection functions can be arbitrary, but in order for their use to give a correct description of the acts of selection, it is necessary to $\pi(o)$ to impose a number of constraints or the so called axioms of choice[27].

If the selection problem has a solution, it can be used to rank all objects $O = \{o_1, \dots, o_D\}$ according to their systemic importance. Here D is the total number of objects.

With this in mind, let us describe the proposed ranking algorithm.

Step 1. By applying the function $\pi(O)$, we find the most systematically important objects $\pi(O = O^{[1]+}) = O^{[1]} = \{o_{1,1}, \dots, o_{1,D_1}\}$. Next, by "removing" D_1 objects included in the $O^{[1]}$ from O, we get an opportunity to make a choice on set of remained objects $O^{[2]+} = O^{[1]+}\mathrm{O}^{[1]}$.

Step 2. D_2 objects $\pi(O^{[2]+}) = O^{[2]} = \{o_{2,1}, \dots, o_{2,D_2}\}$ followed by their deletion: $O^{[3]+} = O^{[2]+}\backslash\mathrm{O}^{[2]}$.

Then, the procedure of selection and deletion at step s is repeated $s = 3,4, \dots$:

$$\begin{cases} \pi(O^{[s]+}) = O^{[s]} = \{o_{s,1}, \dots, o_{s,D_s}\}, \\ \qquad O^{[s+1]+} = O^{[s]+}\backslash\mathrm{O}^{[s]} \end{cases} \tag{13}$$

the algorithm is complete when all objects from the set O are "disassembled" into sets $O^{[s]}$:

$$\begin{cases} O = O^{[1]} \cup O^{[2]} \cup \dots \cup O^{[s]}, \\ D = D_1 + D_2 + \dots + D_s \end{cases} \tag{14}$$

The rule for determining the system significance of any object in this constructional solution is simple: the more significant the object is, the earlier s it is chosen as an element of the set $O^{[s]}$. The objects that happen to be in the same $O^{[s]}$ are considered to be of equal importance.

But in the general case of the objects of a complex system perform different functions, different assessments of the results of their activities (or the consequences of their failure), and, therefore, it is important not only to know how much (how many times) one type of object is more significant than another, but also to be able to compare the estimates of objects of different types.

This requires the introduction of additional axioms specifying classes of selection functions among heterogeneous objects, but it should be understood that so far the general problem of selecting such axioms for collections of objects containing objects of different types has not been solved. There are several reasons for this, among the most important ones the following should be noted:

- large dimensionality of the choice problem;
- diversity of data;
- the presence of "missing values";
- Noisiness: the presence of fuzzy and random indicators;
- multicriteria.

For these reasons, it is advisable to solve the problem of ranking a large set of objects of different types in several stages. At the first stage for objects of each type, it is necessary to construct private models of system significance estimation of objects of the selected type and to carry out the ranking by them. At the second stage, it is required to "stitch" the ranked lists of objects into a unified list. At the third stage, correction of values of estimations where it is necessary to take into account special conditions of functioning of separate objects is carried out.

To date, a number of standardized approaches to describing choice have been developed. The simplest option is to assume that for all alternatives $x \in X$ can be given a function $Q(x)$ which is called a criterion (a quality criterion, a target function, a preference function, a utility function, etc.) and has the property that if an alternative x_2 is preferable to alternative x_1, then $Q(x_2) > Q(x_1)$. Choice as maximization of a criterion is reduced to the search for such a value $x^* \in X$, which achieves the maximum of function $Q(x)$ on the set of alternatives X: $x^* =$ argmax $Q(x)$.

Often, however, constructing a utility function $Q(x)$ is either very difficult or practically impossible, since the options being compared are similar to the choices for a person when he is offered either only "to drink" or only "to breathe". At the same time, the ideas of construction of utility functions for choice can be useful at the initial stages of selection of variants when LDP on a limited amount of data tries to interpolate some nonlinear scale of utility.

6.2 On solving multi-criteria problems

The practice of decision-making in scientific, design, management and entrepreneurial activities shows that in the vast majority of cases there are several, and in some situations a very large number of criteria according to which it is necessary to optimise the parameters of technical systems or evaluate management decisions. Multicriteria methods are used in problems where it is necessary to choose compromise solutions, for example between price and quality, expected profit and possible risk.

So, let the evaluation of an alternative x several criteria be used $q_i(x)$ $(i = 1, \dots, p)$. If for x, there is an alternative x^*, which is not worse than x by all criteria $q_i(x^*) \geq q_i(x)$ $(i = 1, \dots, p)$, and there is at least one criterion $q_j(x)$ $(j \in \{1, \dots, p\})$ such that a strict preference on this criterion is satisfied $q_j(x^*) > q_j(x)$, then we will say that x^* dominates over x, and the alternative x with respect to x^* is dominant. The relation between the elements of the set of alternatives introduced in this way defines a partial order relation on this set.

The variant $x \in X$ will be called Pareto-optimal if there is no single option $x^* \in X$ dominating x. The allocation of the set of Pareto-optimal solutions is the first step in the search for optimal alternatives. By construction, the elements of this set are incomparable with each other, and none of the Pareto-optimal solutions cannot be improved by any criterion without worsening the values of other criteria.

The Pareto-optimal set of solutions is constructed by discarding the dominant options. Initially, the Pareto-optimal set contains alternatives with maximum values of partial criteria. **Figure 1** illustrates the process of construction of such set in two-dimensional parameter space.

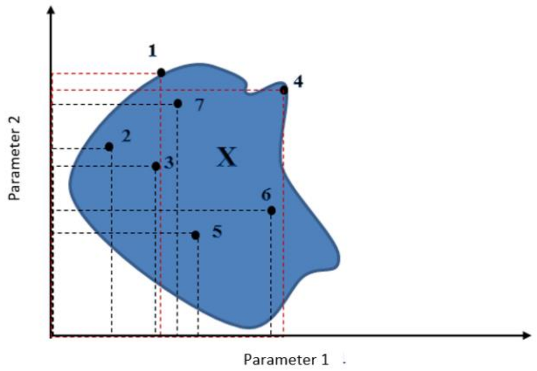

Figure 1. The process of building a Pareto-optimal set on many possible solutions.

For the solution variant, a rectangle is constructed, the corner points of which are the origin of coordinates and the point corresponding to the solution variant. **Figure 1** shows that point 1 dominates over points 2 and 3 (points 2 and 3 are inside the rectangle for point 1), and point 4 additionally dominates over points 5, 6, and 7. Thus, point 1 and point 4 form a Pareto-optimal set. The process is repeated for all points of the set X.

So, let the evaluation of an object o several criteria be used $q_i(\vec{x}(o))$ $(i = 1, \dots, r)$. If for an object o, there is an alternative o^*, which is not worse than o according to all criteria $q_i(\vec{x}(o^*)) \geq q_i(\vec{x}(o))$ $(i = 1, \dots, r)$, and there is at least one criterion $q_j(\vec{x})$ $(j \in \{1, \dots, r\})$ such that a strict preference on this criterion is satisfied $q_j(\vec{x}(o^*)) > q_j(\vec{x}(o))$, then we will say that o^* dominates over o. Accordingly, the alternative o with respect to o^* is dominant. As already mentioned, the relation between the elements of the set of alternatives introduced in this way defines a partial order relation on this set.

The variant $o \in O$ will be called Pareto-optimal if there is no single option $o^* \in O$ dominating o.

When the dimensionality is large r, it is likely that the set of Pareto-optimal solutions may consist not only of a large number of elements, but also have a complex multi-connected structure. Due to the fact that a limited number of objects and a limited number of coordinates in which these objects admit a "visual" image are available to the LPR, there is a natural task of further selection of variants.

Note that when all criteria are a priori equivalent and it is impossible to replace some criteria by others, further selection (selection optimization) is impossible. In this case, the procedure of search for solutions of a multicriteria problem is completed by a list of Pareto-optimal solutions.

In other cases, the simplest variant of choosing the best variant is realized when the criteria are fundamentally unequal, namely, when the best variant is chosen from the previously selected candidates to the best ones. For this purpose, the so-called lexicographic ordering of the set is often used O: first in O, the best elements (variants of solutions) with the maximal value according to the criterion q_1 and all other elements O are discarded. If the remaining subset contains more than one element, then the best elements by criterion are chosen among these elements q_2. Further, if necessary, it is necessary to optimize and discard options, using the criteria q_i $(i = 3, \dots, r)$ and so on, until there is only one element in the set O, it will be the desired solution.

In addition to lexicographic ordering, which gets its name from the arrangement of words in the dictionary and which almost immediately establishes a strict order on the set of objects under study, there are a number of constructive methods for solving problems of multicriteria choice due to the fact that a certain interchangeability of some criteria with others is allowed.

Consider, for example, the linear substitution method.

As in the method of lexicographic ordering, let the criteria q_i $(i = 1, \dots, r)$ be ordered in descending order of importance. Let us introduce replacement coefficients for the i-th criterion by the next $(i$+1)-th criterion in importance $k_{i+1,i}$ $\left(\forall i\ k_{i+1,i} > 1\ (i = 1, \dots, r-1)\right)$. Thus we take into account that "loss" of a unit of criterion

q_i can be "compensated" in principle by increasing of criterion q_{i+1}, but only if compensation is done "with percents" (**Figure 2**).

So the option o_2 turns out to be preferable than o_1, because the loss of $q_1(o_1) - q_1(o_2)$ units by the first criterion is "more than compensated" by the gain by the second criterion $q_2(o_2) - q_2(o_1)$.

If concessions of any size are admissible, the method is reduced to a non-strict ordering of Pareto-optimal solutions with the help of the generalized criterion $q_0(x)$ as a weighted linear convolution of private criteria:

$$q_0(x) = 1 \times q_1(x) + (k_{2,1})^{-1} \times q_2(x) + (k_{3,2} \cdot k_{2,1})^{-1} \times q_3(x) + \cdots + (k_{p,p-1} \cdot \ldots \cdot k_{2,1})^{-1} \times q_r(x) \quad (15)$$

If the size of the concessions is limited, then locally the optimal option is quickly found, because the options that require large size concessions are not considered. The method with limited concessions is reasonable to use in cases where the set of possible options O can be replenished.

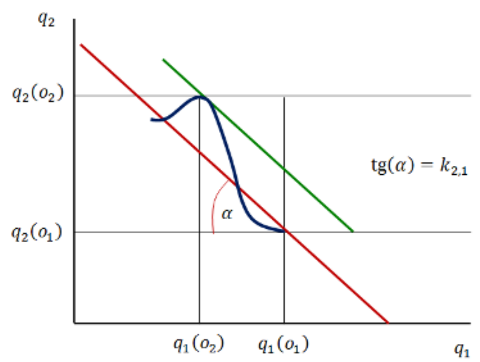

Figure 2. Illustration of the linear substitution method.

It should be noted that optimization using additive linear criterion $q_0(x)$ leads to solutions on the boundaries of the admissible domain O which relates the problem of finding the optimal choice of an option to linear programming problems.

When the values of particular criteria q_i $(i = 2, \ldots, r)$ are considered as coefficients that strengthen (weaken) the system significance estimated through the previously constructed criteria, the equation for the general criterion of "hyperbolic" substitution will take the following form:

$$\log(q_0(x)) = 1 \times \log(q_1(x)) + (\tilde{k}_{2,1})^{-1} \times \log(q_2(x)) + (\tilde{k}_{3,2} \cdot \tilde{k}_{2,1})^{-1} \times \log(q_3(x)) + \cdots + (\tilde{k}_{p,p-1} \cdot \ldots \cdot \tilde{k}_{2,1})^{-1} \times \log(q_r(x)) \quad (16)$$

In Equation (16), the coefficients with tilde are the coefficients of linear substitution of criteria presented in logarithmic scales.

Potentiating Equation (15), we obtain another form of the generalized criterion:

$$q_0(x) = (q_1(x)) \times (q_2(x))^{(\tilde{k}_{2,1})^{-1}} \times (q_3(x))^{(\tilde{k}_{3,2} \cdot \tilde{k}_{2,1})^{-1}} \times \ldots \times (q_r(x))^{(\tilde{k}_{p,p-1} \cdot \ldots \cdot \tilde{k}_{2,1})^{-1}} \quad (17)$$

If private criteria are properly scaled during construction, the coefficients marked with "tilde" will become equal to one, and the index of system significance $q_0(x)$ will be the product of basic index $q_1(x)$ by the product of criteria-dimensionless "correction" coefficients. Their number $(r - 1)$ is determined by how many will be needed to remove contradictions in the examples of the training sample, i.e., according to the scheme similar to the one presented in the previous section.

Note that, as a rule, $q_0(q_1, \ldots, q_p)$ is assumed to be a monotonically increasing bounded unit positive function of its arguments. Hence, every projection of a convolution function $q_0(q_1, \ldots, q_p)$ when some of its arguments take fixed values, there will also be a monotonic function of the remaining arguments. This allows us to construct the convolution q_0 or supercriterion as a monotone superposition of monotone superpositions, etc.

As such, monotonic convolution functions are used additive (Equatation (18)) or multiplicative (Equatition (19)) functions.

$$q_0(q_1, \ldots, q_p) = \sum_{i=1}^{3} \frac{\alpha_i}{S_i} \times q_i \tag{18}$$

$$q_0(q_1, \ldots, q_p) = 1 - \prod_{i=1}^{p} \left(1 - \frac{\beta_i}{S_i} \times q_i\right) \tag{19}$$

Coefficients α_i и β_i in Equation (18) and (19) reflect the weight coefficients of the criteria q_i. The coefficients s_i are chosen so as to make dimensionless the numbers q_i and, if needed, to provide their normalization $0 \leq \left(\frac{\beta_i}{s_i} \times q_i\right) \leq 1$. In practice, the parameters α_i and β_i are determined by training on a finite set of examples.

A practical application of the risk synthesis concept described with a notional calculation example is given in other author's work[28].

7. Concluions

At present, it is more important than ever to develop theoretical foundations and to construct models and technological tools of information-analytical work in the field of decision support that are adequate to the existing challenges, with the aim of ensuring the complex security of structurally complex systems. Inevitably, there is a need to identify priorities, rank objectives, problems and threats, and reallocate available (usually limited) resources.

It is shown that the task of ranking critical objects by system importance leads to the problem of multicriteria ranking under uncertainty, which is of great importance for the analysis of structurally complex systems with different purposes. Since in the general case, the objects of a complex system perform different functions and the results of their activity (or the consequences of their failure) are estimated differently, it is important not only to know how much (how often) one object of the same type is more important than another, but also to be able to compare the estimates of objects of different types. For this purpose, additional axioms are introduced that concretise the classes of functions of a choice among heterogeneous objects. A solution to the problem, of the Pareto analysis type, is proposed, which makes it possible to select the parts (objects) of the system under study that require priority attention from the point of view of their safety.

The presented algorithm provides decision support in the so-called problem of group selection of critical infrastructure objects of a structurally complex system that require increased attention in terms of their protection against the existing range of threats, taking into account the resources required for this. Such problems arise in the analysis and aggregation of heterogeneous information about the preferences of compared objects into a single "group" preference.

The algorithm is based on game theory with a set of assumptions about the resources of intruders attacking the system (negative action factors) and its "defenders". The algorithm allows to reasonably align scales of system importance of objects of different types, i.e., to embed objects described by different resource and basic criteria in a single scale of comparison.

The obtained results can be applied in critical industries—complex process control systems, transport, aerospace and military spheres, banking and financial structures, as well as in central and sectoral management bodies for methodological and technical support of relevant decision-making.

Conflict of interest

The author declares no conflict of interest.

References

1. Henley EJ, Kumamoto X. Reliability of technical systems and risk assessment (Russian). Mashinostroenie; 1984.
2. Vemuri V. Modeling of complex systems. Academic Press; 1978.
3. Rainshke K, Ushakov IA. Evaluation of the reliability of systems using graphs (Russian). Radio and Communications; 1988. p. 208.
4. Ushakov IA. Counter-terrorism: Protection resources allocation. In: Reliability: Theory & applications. Wiley; 2006.
5. Ryabinin IA. Reliability and safety of structurally complex systems (Russian). St. Petersburg University Publisher; 2007.
6. Solozhentsev ED. Scenario logic and probabilistic management of risk in business and engineering. New York: Springer; 2004.
7. Mozhaev AS, Gladkova IA, Musaev AA. Method of logic-deterministic modeling of network systems (Russian). Izvestiya St. Petersburg State Technological Institute (Technical University) 2012; 14: 89–96.
8. Glushkov VM, Ivanov VV, Yanenko VM. Modeling of developing systems (Russian). Nauka; 1983. p. 351.
9. Ushakov I. Counter-terrorism: Protection resources allocation. Part I. Minimax criterion. Reliability: Theory and Applications 2006; 1(2).
10. Ushakov I. Counter-terrorism: Protection resources allocation. Part II. Branching system. Reliability: Theory and Applications 2006; 1(3).
11. Ushakov I. Counter-terrorism: Protection resources allocation. Part III. Fictional “case study”. Reliability: Theory and Applications 2007; 2(1).
12. Levitin G. Optimal defense strategy against intentional attacks. *IEEE Transactions on Reliability* 2007; 56(1): 148–157. doi: 10.1109/TR.2006.884599.
13. Mongerstern O, von Neumann J. Game theory and economic behavior (Russian). Nauka; 1970. p. 708.
14. Lefebvre VA, Smolyan GL. In: Tsygichko VN (editor). Algebra of conflict (Russian). 6th ed. LENAND; 2018. p. 72.
15. Smolyan GL. Operations research—An instrument of effective management (Russian). Znanie; 1967.
16. Bochkov AV. Hazard and risk assessment and mitigation for objects of critical infrastructure. In: Ram M, Davim JP (editors). Diagnostic techniques in industrial engineering. Management and industrial engineering. Springer Cham; 2017. p. 57–135.
17. Bochkov AV. Approaches to the construction of adaptive situation control systems of structurally complex systems under uncertainty. In: Proceedings of the International Conference ISAHP-2011; 15–18 June 2011; Sorrento, Naples, Italy.
18. Bochkov AV, Zhigirev NN, Lesnykh VV. Dynamic multi-criteria decision making method for sustainability risk analysis of structurally complex techno-economic systems. Reliability: Theory & Applications 2012; 1(25): 36–42.
19. Karminsky AM. Peresetsky AA, Petrov AE. Ratings in economics: Methodology and practice (Russian). Finance and Statistics; 2005.
20. Baranov S, Skufyina T. Analysis of inter-regional differentiation and the construction of rankings of the subjects of the Russian Federation (Russian). Voprosy Ekonomiki 2005; 8: 54–75. doi: 10.32609/0042-8736-2005-8-54-75.
21. Larichev OI. A property of decision-making methods in multi-criteria individual choice problems. Automation and Remote Control 2002; 63(2): 304–315. doi: 10.1023/A:1014207910716.
22. Keeney RL, Raiffa H. Decisions with multiple objectives: Preferences and value tradeoffs. Cambridge University Press; 1993. p. 569.
23. Kuvshinov BM, Shaposhnik II, Shiryaev VI, Shiryaev OV. Using committees in problems of pattern recognition with inaccurate expert estimates (Russian). Izvestiya Chelyabinskogo Nauchnogo Center 2001; 2(11): 81–88.
24. Mazurov VD. The Method of Committees in Problems of Optimization and Classification (Russian). Nauka; 1990.
25. Zhukovsky VI. Cooperative games under uncertainty and their applications (Russian). Editorial URSS; 1999.
26. Kweid E. Analysis of complex systems (Russian). Soviet Radio; 1969.
27. Podinovsky VV. Decision under multiple estimates for the importance coefficients of criteria and probabilities of values of uncertain factors in the aim function. Automation and Remote Control 2004; 65: 1817–1833. doi: 10.1023/B:AURC.0000047896.61645.43.

28. Bochkov A, Lesnykh V, Zhigirev N, Lavrukhin Y. Some methodical aspects of critical infrastructure protection. Safety Science 2015; 79: 229–242. doi: 10.1016/j.ssci.2015.06.008.