Models and algorithms for optimizing security management of critical social infrastructure facilities

L V Rossikhina and D E Orlova

1Management Academy of the Russian Interior Ministry, 8, Z. and A. Kosmodemyanskikh Street, Moscow, RU
2ET Department, Voronezh Institute Federal Penitentiary Service of Russia, 1a Irkutskay Street, Voronezh, RU

Email: rossihina_lv@mail.ru

Abstract. Algorithms for managing complex security of objects of critical application are proposed. They differ from their analogues in that classical optimization models are supplemented with coordination models that allow taking into account multi-criteria, hierarchy and interconnectedness of components of managed objects.

1. Introduction
One of the main directions of development of the national economy of the Russian Federation is connected with toughening of requirements to safety of objects of critical application. Typical examples of such objects are nuclear power complexes, chemically safe production facilities, institutions of the Ministry of Defense, Internal Affairs and Penal Enforcement System, sectoral, territorial and national communication and logistics systems. At the same time, an adequate level of their security should be ensured not only by "force" means, but mainly by improving the effectiveness of management in all aspects of likely threats [1-4].

As analysis shows, this problem has not yet been properly solved. As before, security management of these objects is carried out mainly by separate components (technical, environmental, technological, information, etc.), without taking into account their interrelationships, and, practically, without the use of mathematical means of intellectual support for the decisions made. At the same time, security management systems of objects of critical application increasingly acquire the features of integrated geographically distributed human-machine complexes with a constantly expanding set of functional subsystems, in particular, such as: access control, fire alarm and fire extinguishing, life support and information security. These subsystems, being probable objects of destructive influence from different kinds of offenders, turn out to be connected through technical, electronic, infrastructural, territorial and other resources. Conflicts of interest arise in relation to which traditional methods of finding optimal solutions lose their constructiveness.

It should be noted that the general theoretical issues of management of multilevel hierarchical systems with multidimensional component links have been highlighted in studies of both foreign (M.
Mesarovich, D. Mako, I. Takahara) and native scientists: V. N. Burkov, D. A. Novikov, D. S. Kontorov, V. I. Novoseltsev. At the same time, specific issues of optimization of complex security management for objects of critical application brought up to the level of their algorithmization remain unsolved.

The aim of the article is to develop optimization algorithms for complex security management processes for objects of critical application with the above properties. The research is based on the provisions of the theory of management of organizational systems [5,6], supplemented by elements of the theory of conflict [7-9] and methods of optimal management [10-12].

2. Formulation of complex management task object security of critical applications

Structural and functional scheme of complex safety management of objects of critical application, presented in figure 1, is an initial acceptance.

![Figure 1. Structural and functional scheme of complex safety management for objects of critical application: P1-P4 – local safety processes.](image)

As it can be seen from this scheme, safety in objects of critical application is a complex category including: regime and security security, fire safety, information safety, life safety (including safety of engineering structures, health and life of people). At the same time, the specifics of management is that the persons making managerial decisions on the above mentioned local security aspects are endowed with a certain autonomy. Not only exclusion, but any infringement of this autonomy reduces the security level of the object, because it is accompanied by removal of responsibility from subordinates in the performance of their functional duties. At the same time, independence in decision making leads to conflicts between "manager-subordinate" and "subordinate-subordinate", which also negatively affects the object's security.

To describe the quality of functioning of functional subsystems, we will introduce a system of local indicators presented in Table 1.

Introducing the vector functions \( \mathbf{q}_i = \mathbf{q}_i(\mathbf{m}_i, \mathbf{y}_i, t) \), where \( \mathbf{m}_i(i = 1, 4) \) – vectors of controls within functional subsystems, but \( \mathbf{y}_i(i = 1, 4) \) – control vectors for functional subsystems. Suppose that all vector spaces are linear, and their axes are normalized in the range of \([0,1]\). We will also assume that all security parameters are in the range \([0,1]\) and their maximum values are one.
Table 1. Local indicators used in the management of functional subsystems of security of objects of critical application.

| Mode and security indicators ($\vec{q}_1$) | $q_{11}$ - security level at special events; |
|                                          | $q_{12}$ - object security level; |
|                                          | $q_{13}$ - level of personal security of employees and special forces; |
|                                          | $q_{14}$ - timely identification and elimination of critical situations related to the actions of intruders and terrorists; |
|                                          | $q_{15}$ - privacy and security clearance control level. |
| Fire Safety Indicators ($\vec{q}_2$)     | $q_{21}$ - fire safety compliance; |
|                                          | $q_{22}$ - firefighting capacity of facilities; |
|                                          | $q_{23}$ - level of firefighting training; |
|                                          | $q_{24}$ - fire alarm status; |
|                                          | $q_{25}$ - fire safety organization and management level; |
|                                          | $q_{26}$ - fire hazard level; |
|                                          | $q_{27}$ - timely detection and elimination of fires. |
| Information Security Indicators ($\vec{q}_3$) | $q_{31}$ - reliability of information; |
|                                          | $q_{32}$ - completeness of output; |
|                                          | $q_{33}$ - timely provision of information; |
|                                          | $q_{34}$ - output reliability; |
|                                          | $q_{35}$ - data privacy preservation; |
|                                          | $q_{36}$ - level of security against unauthorized access; |
|                                          | $q_{37}$ - timely identification and elimination of critical situations related to information security. |
| Life Safety Indicators ($\vec{q}_4$)     | $q_{41}$ - environmental safety level; |
|                                          | $q_{42}$ - engineering security level; |
|                                          | $q_{43}$ - level of hygiene and medical care; |
|                                          | $q_{44}$ - dietary level; |
|                                          | $q_{45}$ - timely identification and elimination of critical situations related to life hazard. |

Then the task of complex security management of objects of critical application can be formulated as a set of interrelated optimization tasks of the following type:

$$
\Delta(t) = \left\{ \frac{1}{T} \int_0^T \left[ 1 - G_{\vec{f}}[\delta_1(t), \delta_2(t), \delta_3(t), \delta_4(t)] \right] dt \right\} \rightarrow \min_{\vec{y} \in \mathcal{Y}}
$$

where $G_{\vec{y}}$ – vector function travel time curve $\vec{r} = r_1[\delta_1(t), \delta_2(t), \delta_3(t), \delta_4(t)]; f[\delta_1(t), \delta_2(t), \delta_3(t), \delta_4(t)] = 0$ – function that reflects the relationship between variables $\delta_1(t), \delta_2(t), \delta_3(t), \delta_4(t); T$ – time interval.
Evaluation of the level of inconsistency of local safety concerns

We will interpret inconsistency as a result of conflict of interests between functional subsystems, which form the system of complex security of objects of critical application. Then, the typology presented in Table 2 may be used as the initial basis for such assessment.
Then to evaluate $\alpha_{ij}$ the following implications can be used:

$$\left[\frac{\partial G_{ii}}{\partial \alpha_{ij}} < 0 \land \left(\frac{\partial G_{ij}}{\partial \alpha_{ij}} < 0\right)\right] \rightarrow (\alpha_{ij} = -1,0) \text{– for «Negative»;} \quad (3)$$

$$\left[\frac{\partial G_{ii}}{\partial \alpha_{ij}} > 0 \land \left(\frac{\partial G_{ij}}{\partial \alpha_{ij}} > 0\right)\right] \rightarrow (\alpha_{ij} = 1,0) \text{– for «Positive»;} \quad (4)$$

$$\left[\left(\frac{\partial G_{ii}}{\partial \alpha_{ij}} < 0 \land \left(\frac{\partial G_{ij}}{\partial \alpha_{ij}} > 0\right)\right) \lor \left[\left(\frac{\partial G_{ii}}{\partial \alpha_{ij}} > 0 \land \left(\frac{\partial G_{ij}}{\partial \alpha_{ij}} < 0\right)\right)\right]\right] \rightarrow (\alpha_{ij} = -0,5) \text{– for «PositiveNegative»;} \quad (5)$$

$$\left[\left(\frac{\partial G_{ii}}{\partial \alpha_{ij}} = 0 \land \left(\frac{\partial G_{ij}}{\partial \alpha_{ij}} = 0\right)\right) \lor \left[\left(\frac{\partial G_{ii}}{\partial \alpha_{ij}} = 0 \land \left(\frac{\partial G_{ij}}{\partial \alpha_{ij}} = 0\right)\right)\right]\right] \rightarrow (\alpha_{ij} = 0) \text{– for «Neutral»}. \quad (6)$$

Using the results of calculations by formulas (3)-(6) we make 4×4 matrix $\|\alpha_{ij}\|; \alpha_{ii} = 0$, which defines the average, maximum and minimum level of mismatch of local security aspects:

$$\bar{\alpha} = \frac{1}{12} \left[\sum_{i=1}^{4} (\sum_{j=1}^{4} (\alpha_{ij}))\right]; \quad (7)$$

$$\alpha_{\min} \left(\min_{i} \left(\alpha_{ij}\right), \min_{j} \left(\alpha_{ij}\right)\right)_{\max} \quad (8)$$

$$\alpha_{\max} \left(\max_{i} \left(\alpha_{ij}\right), \max_{j} \left(\alpha_{ij}\right)\right)_{\min} \quad (9)$$

### 4. Choosing the optimal control model

In solving this problem, we will proceed from the fact that there are three types of situations in objects of critical application [13,14]: critical, regular and threatening. Accordingly, we will single out three typical models of optimal management: in critical situations; in regular situations and in threatening situations. The difference between these models is as follows. In the case of coordination management in critical situations, the site security manager takes full responsibility for ensuring the security of the institution, gives commands to the executors, and they accept these commands for strict execution. In regular coordination situations, the manager delineates the authority of the executors, while the latter manage the local security processes within the limits of the authority given to them. In coordination management in threatening situations, the manager takes over some of the functions and delegates the other part to the subordinates. The choice of the optimal management model type will be linked to the estimates $\bar{\alpha}, \alpha_{\max}$ and $\alpha_{\min}$. For this purpose, the evaluation space $[-1,0 \div +1,0]$ step by step $-1,0 \div -0,33; -0,33 \div +0,33; [+0,33 \div +1,0]$, and to select the optimal control model, we will use implication:

a) for guaranteed evaluation:
In order to take into account the impact on the security system from intruders, we will be guided by the following heuristic rule, which has been repeatedly tested in practice: the higher the security threat, the more responsible should be the decision to manage the security system. Such a rule is implication:

\[ \{\text{high threat level} \to \langle \text{guaranteed evaluation}; \rangle \langle \text{medium threat level} \to \langle \text{weighted average}; \rangle \langle \text{low threat level} \to \langle \text{optimistic assessment}. \rangle \} \]

Taking into account the above mentioned, the algorithm of choosing the model of optimal complex security management of objects of critical application looks like this:

Step 1. Using formulas (3)-(6) fill in the matrix $\|a_{ij}\|$; $a_{ii} = 0$.

Step 2. Using formulas (7)-(9) we calculate the values of $\bar{\alpha}, \alpha_{\text{max}}, \alpha_{\text{min}}$. Based on heuristic considerations, we assess the level of security threats by grading: $\langle \text{high}; \rangle \langle \text{medium}; \rangle \langle \text{low}. \rangle$

Step 3. Using implication (13) we determine the type of assessment of local security mismatch: $\langle \text{guaranteed}; \rangle \langle \text{weighted average}; \rangle \langle \text{optimistic}; \rangle$

Step 4. Using the appropriate implication (10)-(12), we choose the appropriate model for optimal management of the appropriate degree of mismatch between the local security aspects and the level of threats from the attackers.

This approach allows us to move away from detailed accounting of links between local security aspects, which made it difficult to solve the task, and move to typical algorithms of optimal control.

5. Optimal control algorithm in critical situations

In this case, the decision-making criterion is expressed by the target function (1), and the algorithm is reduced to the next iteration procedure:

Step 1: Setting up the starting vector $\vec{y}^{(0)}_i \in Y_i (i = 1,4)$.

Step 2. We decide (2), received $\vec{m}^{(0)}_i$ and $\vec{d}^{(0)}_i (i = 1,4)$; remember.

Step 3. For $\delta^{(0)}_i (i = 1,4)$, decide (1), $\vec{y}^{(0)}_i (i = 1,4)$ and $\Delta^{(0)}$; remember.

Step 4. If $\Delta^{(0)} = 0$ – problem solved, $\vec{m}^{(0)}_i$ and $\vec{y}^{(0)}_i (i = 1,4)$ are considered optimal. At $\Delta^{(0)} > 0$ task at hand.

Step 5: Choose a new random vector $\vec{y}^{(1)}_i \in Y_i (i = 1,4)$.

Step 6. We decide (2), received $\vec{m}^{(1)}_i$ and $\vec{d}^{(1)}_i (i = 1,4)$; remember.

Step 7. For $\delta^{(1)}_i (i = 1,4)$, decide (1), $\vec{y}^{(1)}_i (i = 1,4)$ and $\Delta^{(1)}$; remember.

Step 8. If $\Delta^{(1)} = 0$ – problem solved, $\vec{m}^{(1)}_i$ and $\vec{y}^{(1)}_i (i = 1,4)$ are considered optimal. At $\Delta^{(1)} > 0$ We consider the attempt unsuccessful and proceed to the step 5. Search stops after $\mu$ fails to iterate.
\[ \Delta^\mu = 0, \] and we consider the task of achieving the required security levels with available source data impossible. Amounts \[ \Delta = \min_{\mu} \Delta^\mu \] and \[ \delta_i^\mu \] (\( i = \overline{1,4} \)) and along with the values of \( q_{ij} \) highlight in the corresponding windows of the output interface shown in Figure 2 [15].

6. Optimal control algorithm in normal situations

In this case, the decision-making criterion is expressed by a set of target functions (2), and the algorithm is reduced to an iterative procedure:

Step 1. We decide (2) on the assumption that there are no coordinating departments. Received by \( \vec{m}_i^{(0)} \) and \( \delta_i^{(0)} \) (\( i = \overline{1,4} \)) remember.

Step 2. If \( \forall_{i=\overline{1,4}} (\delta_i^{(0)} = 0) \) – problem solved, \( \vec{m}_i^{(0)} \) (\( i = \overline{1,4} \)) are considered optimal. Otherwise, we continue solving the problem.

Step 3. Set the starting vector \( \vec{y}_i^{(0)} \in Y_i \) (\( i = \overline{1,4} \)).

Step 4. For \( \delta_i^{(0)} \) (\( i = \overline{1,4} \)) decide (1), \( \vec{y}_i^{(0)} \) (\( i = \overline{1,4} \)) remember.

Step 5. For \( y_i^{(0)} \) (\( i = \overline{1,4} \)) decide (2), \( \vec{m}_i^{(1)} \) and \( \delta_i^{(1)} \) (\( i = \overline{1,4} \)) remember.

Step 6. If \( \forall_{i=\overline{1,4}} (\delta_i^{(0)} = 0) \) – problem solved, \( \vec{m}_i^{(1)} \) (\( i = \overline{1,4} \)) at \( \vec{y}_i^{(0)} \) (\( i = \overline{1,4} \)) optimally. If the specified condition is not met, we proceed to the step 1. Search stops after unsuccessful iterations to get the condition fulfilled \( \forall_{i=\overline{1,4}} (\delta_i^{(\mu)} = 0) \), and the task of achieving the required security levels with available source data is considered impossible. Amounts \( \delta_i = \min_{\mu} \delta_i^{(\mu)} \) (\( i = \overline{1,4} \)) and \( \Delta \) are fixed, and together with the values of \( q_{ij} \) is displayed in the corresponding windows of the output interface similar to Figure 2.

7. Optimal control algorithm in threatening situations

In this case, the decision-making criterion is expressed both by the target function (1) and the target function (2), and the algorithm is reduced to the following iterative procedure:

Step 1. We decide (2). Received by \( \vec{m}_i^{(0)} \) and \( \delta_i^{(0)} \) (\( i = \overline{1,4} \)) remember.

Step 3. For \( \delta_i^{(0)} \) (\( i = \overline{1,4} \)) decide (1), \( \vec{y}_i^{(0)} \) (\( i = \overline{1,4} \)) and \( \Delta^{(0)} \) remember.

Step 4. If \( \Delta^{(0)} = 0 \cap \forall_{i=\overline{1,4}} (\delta_i^{(0)} = 0) \) – problem solved, \( \vec{y}_i^{(0)} \) (\( i = \overline{1,4} \)) are considered optimal. If this condition is not met, we continue solving the problem.

Step 5. Choose a new random vector \( \vec{y}_i^{(1)} \) (\( i = \overline{1,4} \)).

Step 6. We decide (2). Received by \( \vec{m}_i^{(1)} \) and \( \delta_i^{(1)} \) (\( i = \overline{1,4} \)) remember.

Step 7. For \( \delta_i^{(1)} \) (\( i = \overline{1,4} \)) decide (1), \( \vec{y}_i^{(1)} \) (\( i = \overline{1,4} \)) and \( \Delta^{(1)} \) remember.

Step 8. If \( \Delta^{(1)} = 0 \cap \forall_{i=\overline{1,4}} (\delta_i^{(1)} = 0) \) – problem solved, \( \vec{y}_i^{(1)} \) (\( i = \overline{1,4} \)) are considered optimal. Otherwise, we proceed to step 5. Search stops after unsuccessful iterations to get the condition fulfilled \( \Delta^{(\mu)} = 0 \cap \forall_{i=\overline{1,4}} (\delta_i^{(\mu)} = 0) \), and the task of achieving the required security levels with available source data is considered impossible. Amounts \( \delta_i = \min_{\mu} \delta_i^{(\mu)} \) (\( i = \overline{1,4} \)) and \( \Delta = \min_{\mu} \Delta^{(\mu)} \) are fixed, and together with the values of \( q_{ij} \) is displayed in the corresponding windows of the output interface similar to the picture 2.
8. Determining the number of iterations
Amount $\mu$, which appears in the optimal control algorithms, we will associate with the probability of missing the global extremum of target functions (1) and (2). Let it be known a priori that these target functions have $\beta$ minimums, of which $(\beta - 1)$ belongs to the region $\Delta_\rho \in Y (\rho = 1, 2, ..., \beta - 1)$, but one $\Delta_\beta \in Y$. According to the above mentioned algorithms, we will perform the simulation of the evenly distributed in the region $Y$ random point $\mu$ times.

Denote by $P$ the probability of the point hitting the area of attraction $\Delta_\rho$, but after $\alpha P (0 < \alpha < 1)$ – probability of being caught in the attraction area $\Delta_\beta$. Well, then, fair enough $(\beta - 1)P + \alpha P = 1$, and the possibility of missing a global extremum $P' = (1 - \alpha P)^\mu = \left(1 - \frac{\alpha}{\beta - 1 + \alpha}\right)^\mu$. Setting the required value $P'$, value can be estimated $\mu^*$. In our case at $P' = 0.9$ and $\beta = 2$ it turns out that $\mu = 150-200$.

9. Testing of optimal control algorithms
Testing was carried out by a computational experiment in the assumption that vector functions $\vec{q}_i = \vec{q}_i(\vec{m}_i, \vec{y}_i, t)$ and $\vec{r}_i = r_i[\delta_1(t), \delta_2(t), \delta_3(t), \delta_4(t)]$ are linear with all their variables. At the same time, it was believed that the algorithm works if for 150-200 iterative cycles ($\mu$), it allows to obtain stable results, i.e. results with no more than 15% deviation from the average. The results of the computational experiment are presented in Table 3.

### Table 3. Test results of optimal algorithmsoffices.

| Algorithm diversity         | Minimum iterations to ensure convergence | Deviation from the average at tenfold repetition of cycles |
|-----------------------------|----------------------------------------|----------------------------------------------------------|
| in critical situations      | 100-110                                | 9-12%                                                   |
| in normal situations        | 80-90                                  | 8-10%                                                   |
| in threatening situations   | 120-130                                | 10-12%                                                  |

From the analysis of the above data we can see that the described algorithms work in the above sense. Moreover, the following pattern has been revealed: the simpler the algorithm, the fewer iterations it takes to produce stable results. Thus, for example, for the simplest algorithm of optimal control in standard situations, stable results are obtained in about 80-90 cycles, and for the most complex algorithm of coordination in threatening situations - in 120-130 cycles.

10. Conclusion
The proposed algorithms for optimal management of complex security of objects of critical application differ from existing analogues in that, along with the classical optimization models, they use typical coordination models in critical, threatening and routine situations. They allow to solve a task in conditions when the persons making managerial decisions on local security aspects are endowed with certain independence and at the same time their decisions are interdependent. For effective application of the proposed algorithms, two conditions must be met. First, the initial model of complex security should reflect the hierarchical structure of management with interconnected local security subsystems, and the local subsystems themselves should be represented by a set of private indicators, such as Table 1. Second, linear spaces and transformation operators should be used in their implementation, otherwise their convergence is not guaranteed.

References

[1] Puchkov V A and Dagirov S S 2014 Fire safety. Textbooketc. Edited by V.A. Puchkova  
Academy of State Fire Service of the Ministry of Emergency Situations of Russia (Moscow)  
877
[2] Dubrovolsky V B, Lavdansky P A and Yengovatov I A 2010 Construction of Nuclear Power Plants Textbook (Moscow: Published by the Association of Construction Universities) 368

[3] Mikhailov L A and Solomin V P 2006 Life Safety: Textbook for HEIs. St. Petersburg: Peter 302

[4] Rodichev Yu A 2017 Normative base and standards in the field of information security St. Petersburg: Publishing House "Peter" 256

[5] Novikov DA Management theory of organizational systems 2007 2nd ed Moscow Fizmatlit 584

[6] Models and mechanisms of control in self-organizing systems 2008 Ed. by Burkov V N (Voronezh: A Scientific Book) 300

[7] Novoseltsev V I System theory of conflict 2011 M Major 346

[8] Druzhinin V V, Kontorov D S and Kontorov M D 1989 Introduction to the theory of conflict Moscow: Radio and Communication 288

[9] Models of conflict and risk management. Edited by Novikova D A 2008 (Voronezh: Scientific Book) 495

[10] Mesarovich M, Mako D and Takahara I 1973 Theory of Hierarchical and Multi-Level Systems Moscow 344

[11] Theoretical Foundations of System Analysis. Edited by Novoseltsev V I 2013 M: Major 536

[12] Orlova D E Optimal coordination in a competitive environment Barkalov S A Novoseltsev V I and Orlova D E Theory of active systems: a collection of materials. Interd. scientific conf. 2014 Moscow: IPU RAS. 15-16

[13] Orlova D E 2017 Modeling of control systems for complex safety organization Novoseltsev V I Orlova D E and Lavlinskiy V V Vestnik of Voronezh Institute Federal Penitentiary Service of Russia. No 4 96-104

[14] Orlova D E, Novoseltsev V I and Dubrovin A S 2018 Mathematical model and coordination algorithms for providing complex security of an organization In: Journal of Physics: Conference Series Current Problems. Ser. "International Conference "Applied Mathematics, Computational Science and Mechanics: Current Problems" 012042

[15] Orlova D E 2018 Algorithm of safety assurance processes optimization in the organizational-technical systems (in Russian) Orlova DEFederal service for intellectual property. Certificate № 2037663485; registered in the Computer Program Register on September 23