УДК 004.05, 006.015.8, 519.718, 519.876.2
doi: 10.21685/2307-4205-2023-4-16

# APPLICATION OF THE IGNATYEV ADAPTATIVE MAXIMUM PRINCIPLE IN MANAGEMENT OF CRITICAL INFRASTRUCTURES RESILIENCE

**A.V. Masloboev**

Putilov Institute for Informatics and Mathematical Modeling of the Federal Research Centre "Kola Science Centre of the Russian Academy of Sciences", Apatity, Russia;
Nanomaterials Research Centre of the Federal Research Centre "Kola Science Centre of the Russian Academy of Sciences", Apatity, Russia
masloboev@iimm.ru

**Abstract.** *Background*. The research work is aimed at adapting and applying state-of-the-art cybernetic methods for analyzing complex dynamic systems in order to improve the management efficiency of regional critical infrastructures resilience and safety, and enhancing the analytical capabilities of decision support systems used in this area. The urgency of this problem is due to the lack of a unified methodological framework and best practices for maintaining the stable resilient operating of critical infrastructures of various levels and types under conditions of uncertainty and risk. *Materials and methods*. The fundamentals of current research are the theory of holonomic and invariant automatic systems and the method of linguo-combinatorial modeling of organizational and technical systems, proposed by Professor Mikhail B. Ignatyev back in 1963. This theoretical basis provides the modern concept advancement of complex systems resilience in terms of formalizing and structuring the methodology and objectives of managing this immanent attribute (capacity) of self-preservation of these systems. *Results and conclusions*. The issues of applicability of linguo-combinatorial models for situational management of critical infrastructures and the dynamics of their adaptative characteristics are examined. A novel linguo-combinatorial model for managing the critical infrastructure resilience, formalized in the form of an equivalent system of differential equations with arbitrary coefficients, is proposed. The model can be used by critical infrastructures operators to study the system behavior and develop control actions aimed at maintaining the system performance characteristics in the range of its adaptative capabilities under various operating conditions and critical-case scenarios of adverse events via launching stabilization and coordination mechanisms that implement combined control by deviation and external disturbance.

**Keywords**: critical infrastructure, resilience, safety, management, system, adaptative capacity, linguo-combinatorial model

**Financing**: the work was carried out within the framework of the State Research Program of the Putilov Institute for Informatics and Mathematical Modeling KSC RAS (project No. FMEZ-2022-0023).

**Acknowledgments**: The author is deeply obliged to Professor Mikhail B. Ignatyev for the idea of applying the methodology of linguo-combinatorial modeling to the management problems of regional security and resilience of critical infrastructures, expressed at the end of 2018.

**For citation**: Masloboev A.V. Application of the Ignatyev adaptative maximum principle in management of critical infrastructures resilience. *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and quality of complex systems.* 2023;(4):165–178. (In Russ.). doi: 10.21685/2307-4205-2023-4-16

# ПРИМЕНЕНИЕ ПРИНЦИПА АДАПТАЦИОННОГО МАКСИМУМА ИГНАТЬЕВА В УПРАВЛЕНИИ ЖИЗНЕСПОСОБНОСТЬЮ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

**А. В. Маслобоев**

Институт информатики и математического моделирования имени В. А. Путилова Федерального исследовательского центра «Кольский научный центр Российской академии наук», Апатиты, Россия;
Центр наноматериаловедения Федерального исследовательского центра «Кольский научный центр Российской академии наук», Апатиты, Россия
masloboev@iimm.ru

**Аннотация.** *Актуальность и цели.* Работа направлена на адаптацию и применение современных кибернетических методов анализа сложных динамических систем с целью повышения эффективности управления жизнеспособностью и безопасностью региональных критических инфраструктур и расширения аналитических возможностей систем поддержки принятия решений в этой сфере. Актуальность этой задачи обусловлена отсутствием единой методологической базы и наилучших практик поддержания устойчивого функционирования критических инфраструктур различного уровня и типа в условиях неопределенности и риска. *Материалы и методы.* Фундаментальной основой настоящего исследования является теория голономных и инвариантных автоматических систем, а также метод лингво-комбинаторного моделирования организационных и технических систем, предложенный профессором М. Б. Игнатьевым еще в 1963 г. Этот теоретический базис обеспечивает развитие современной концепции жизнеспособности сложных систем в части формализации и структурирования методологии и задач управления данным имманентным свойством самосохранения этих систем. *Результаты и выводы.* Исследованы вопросы применимости лингво-комбинаторных моделей для ситуационного управления критическими инфраструктурами и динамикой их адаптационных характеристик. Предложена новая лингво-комбинаторная модель управления жизнеспособностью критической инфраструктуры, формализованная в форме эквивалентной системы дифференциальных уравнений с произвольными коэффициентами. Модель может быть использована операторами критических инфраструктур для анализа поведения системы и выработки управляющих воздействий, направленных на удержание рабочих характеристик системы в зоне ее адаптационных возможностей при различных условиях функционирования и сценариях развития критических ситуаций посредством запуска механизмов стабилизации и координации, реализующих комбинированное управление по отклонению и по внешнему возмущению.

**Ключевые слова**: критическая инфраструктура, жизнеспособность, безопасность, управление, система, адаптационная возможность, лингво-комбинаторная модель

**Финансирование**: работа выполнена в рамках государственных заданий ИИММ КНЦ РАН (НИР № FMEZ-2022-0023).

**Благодарность**: автор глубоко признателен профессору М. Б. Игнатьеву за идею применения метода лингво-комбинаторного моделирования к задачам управления региональной безопасностью и жизнеспособностью критических инфраструктур, сформулированную в конце 2018 г.

**Для цитирования**: Маслобоев А. В. Применение принципа адаптационного максимума Игнатьева в управлении жизнеспособностью критических инфраструктур // Надежность и качество сложных систем. 2023. № 4. С. 165–178. doi: 10.21685/2307-4205-2023-4-16

## Introduction

Critical infrastructures have become a phenomenon of the modern age. The government and authorities of the Russian Federation are preparing different measures to improve the security level of its critical infrastructures. A number of public documents establishing the strategic development goals of the state and ways to achieve these goals indicate the necessity of increasing the level of safety and protectability of critical facilities and infrastructures as one of the principal objectives. A major role in solving this problem is given to modern information technologies and modeling aids, the use of artificial intelligence methods and Big Data processing technologies that in aggregate allow the engineering of smart information and analytical systems intended for the decision-making support in the field of security management of critical infrastructures. Critical infrastructures, including energy, transport, social, etc. sectors and facilities are playing a central role in the state-of-the-art risk management when facing both man-made and natural hazards, and the threats in civil and military-political areas.

Meanwhile, the concept “critical infrastructure” itself is collective. It covers various scopes of human activity, which are interconnected and declare the issues of preserving the vital functions of the state, the society and the individuals. In line with European Council Directive 2008 [1], the most common definition of critical infrastructure is the follows: critical infrastructure means an asset, system or part thereof, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions.

Adverse disruptive events such as current geopolitical situation in the world have shown that risk management and security ensuring are not enough to protect socio-economic, organizational and technical systems and their critical infrastructures against multiple threats. An important factor of risk management for the purpose of critical infrastructure protection is continually strengthening its resilience [2]. Therefore, recently, critical infrastructures operators, safety analysts and risk managers have moved their attention from engineering a robust critical infrastructure by risk management to establish a resilient critical infrastructure using resilience management [3, 4]. Robust systems experience sudden failure in case of disruption and lose their core value, while resilient systems absorb the adverse impacts, adapt to and recover their desired performance level after a disruption [5].

The concept of resilience has spread from ecological systems into other domains [6]. Broadly speaking, the resilience of critical infrastructure is understood as a system's ability that reduces its vulnerability, minimizes the consequences of active threats, accelerates response and rapid recovery, and facilitates adaptation to the given or potentially disruptive events [7]. In regard to [8], the resilience of critical infrastructure is defined as the ability of a system exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, for the preservation and restoration of essential services. To date, the resilience concept has been adopted and introduced in various subject fields that have led to the definition of specific domains (types) of resilience: public (community resilience, societal resilience, human resilience), economic (socio-economic resilience), engineering (technological resilience, infrastructure resilience), environmental (ecological resilience), etc. Within the bounds of the each resilience domain and type, particular characteristics of the system, processes and phenomena that are most significant in the context of solving a specific research problem are studied. In most cases, the connection between the type of system resilience being studied and other related resilience domains is omitted from examination. Allowing that critical infrastructure is a complex dynamic system, an isolated consideration of particular resilience domains, on the one hand, may overlook synergistic effects and the emergence of new emergent attributes that improve the overall system resilience, and on the other hand, the risk of a chain reaction of violations or cascade effects, leading to a reduction of system resilience level. Thus, in recent years, the popularity of critical infrastructure resilience has exploded in both academic and policy discourses.

A review of domestic scientific literature showed that systematic research of the agenda of critical infrastructures resilience in Russia has not previously been carried out. At once, domestic studies with varying level of detail touch upon certain types of system resilience in such related fields of research as reliability theory, risk analysis, global safety, crisis management and others. A distinctive feature of domestic resilience studies in comparison with foreign ones is the focus on the processes and systems being analyzed. Foreign research projects are addressed to the individual and civil society when solving the control problems of critical infrastructure resilience, while Russian research programs substantially adhere to the state interests and strategies in these issues.

The study of the state-of-the-art management problems of critical infrastructures resilience reveals that methodological approaches to formalizing, modeling and estimating the resilience of critical infrastructures have not been sufficiently developed. At the same time, the practical absence of a unified mathematical apparatus for integrating existing solutions in the field of information technology for managing the critical infrastructures resilience in the context of the transition to a digital economy makes it difficult to design and apply effective methods and facilities for decision-making support in this area. This determines the relevance of developing new methodologies and tools for managing the critical infrastructures resilience on the basis of integration, adaptation and advancement of known models and techniques for ensuring the security of complex systems. Due to the wide range of both the various methods and techniques for analyzing critical infrastructures resilience covering specific resilience domains, and the widespread various models used to estimate the overall system resilience, however, there is still a lack of exact and comprehensive simulation methodology to quantify, measure and control the resilience of critical infrastructures combining these resilience domains into one framework. The other urgent problem on-path efficient resilience analysis is a lack of complete and valid operating historical data and on-line information on the state dynamics of the critical infrastructure performance characteristics.

Thus, the current study pursues an attempt to develop and apply a methodology to manage and analyze the resilience of critical infrastructures on the basis of conjugation of the cybernetic methods, linguo-combinatorial modeling and theory of holonomic automatic system. By adopting this methodology, system resilience backbone capabilities and the influencing situational factors can be modeled effectively. The proposed linguo-combinatorial model formulated on the basis of this methodology for resilience management of critical infrastructures allows explaining numerous facts and patterns in the behavior of these systems, as well as predicting and adjusting the trajectory of their development based on the control principle of system convergence to adaptative maximum.

## Materials and methods

The linguo-combinatorial modeling methodology designed for examining the ill-formalized complex systems was proposed by Professor Mikhail B. Ignatyev in his fundamental study [9] in 1963. Generally, this research was devoted to foundations of the holonomic automatic systems and their applications. As from here on, the developed methodology has been successfully adopted and introduced in various applications, e.g., the control problems of pilotless vehicles, the coordination of cyber-physical and robotic systems, smart cities, the synthesis of physicochemical reactions and atomic-molecular systems, the simulation of organism to reduce medical errors, cybernetic geology, meteorology and economics, regional security, the modeling of climate change and the atmosphere, the engineering of high-performance computing systems, Internet of Things and virtual worlds, the in-depth analysis of biological, technical and organizational systems, etc. The initial premise of the linguo-combinatorial modeling methodology is to solve management and coordination problems of complex dynamic systems by retaining these systems in the range of their adaptive capabilities, so-called adaptative optimum (maximum) [10, 11]. The used research methodology that we follow in our study is just the same and is based on general control theory (cybernetics), system analysis (systems approach), model theory (simulation), safety science (risk management) and system stability theory (resilience concept).

To provide the efficient resilience management of real critical infrastructures, first-priority objective is system resilience modeling and analysis that should be undertaken. It is quite difficult to evaluate and compare the known modeling methodologies of system resilience considering that the methodologies are designed for a specific context and are not aiming to achieve the same goal. Nevertheless, all existing methodologies have their own validity, highs and lows, and the linguo-combinatorial modeling is well-fit for leveling possessed shortcomings in so far as it is possible. Though, the present resilience studies are not so detailed regarding the use of linguo-combinatorial modeling in resilience management problem-solving.

When managing the resilience of complex systems, such as most critical infrastructures, the decision makers and operators mainly use conventional methods and special-purpose tools based on formulations and models of the last century and their state-of-the-art modifications. Meanwhile, the models and tools themselves must include the capability of information control. This is the main point and scope of the information support of making managerial decisions in the field of safety and resilience ensuring.

A drawback of the modern resilience concept is that an event is considered reliable if it is reproducible. In complex organizational systems, especially, socio-economic ones, it is almost impossible to ensure repeatability of similar critical events. The manner and nature of each critical situation are very individual. It is only arguable that there are utterly few repeating phenomena in operation of socio-economic systems. To manage the resilience of such class of systems, not only reproducible information is significant and needed, but also non-reproducible data.

Any subject field is based on models of real processes designed on the basis of expert knowledge. Moreover, in each field these models have different completeness of formalization, but they all use natural language for conceptualization. Natural language is considered as a universal simulation machine (modeling system). Modeling theory should help to deal with still unsolved problems. One of such a problem is the resilience management of socio-economic systems and, in particular, critical infrastructures. These systems belong to the class of ill-formalized systems. Therefore, in order to develop new and adapt known models and methods of information support and turn them into an end-to-end technology for resilience management of critical infrastructures, it is necessary to perform the large-scale efforts to describe and formalize these systems in the form of strict and further applicable formulations. Thereto, the following actions are required:

– to formulate expert knowledge on the observable subject field or entity in natural language;
– to describe situations and problems within the given subject field in natural language;
– to design a mathematical model of a system or control object;
– to assign a problem statement in the relational language using relationships and correlations;
– to translate mathematical formulations into one of known useable programming languages;
– to implement the program code on a computer in the language of a specific machine;
– to obtain the results of the problem solved in the result language: textual, tabular, graphical, animated, etc.

The principal problem of conceptual modeling ill-formalized systems is how to shift from a description in natural language to a description in the relational language using basic relationships and correlations. To solve this problem effectively, the linguo-combinatorial modeling methodology [10] based on the use of keywords and basic concepts that are specific to the subject field under consideration can be well-applied. The typical linguo-combinatorial model consists of three groups of variables: characteristics of basic concepts, changes in these key characteristics, and structured uncertainty in equivalent equations, which can be used for system control and adaptation.

When studying complex dynamic systems, a central issue is the choice of system description language for defining elements and relationships of these systems. As a system description language in linguo-combinatorial modeling methodology, the natural language as a universal sign system that allows considering a wide class of systems, including ill-formalized ones, is used. The main feature of natural language is the designation of words and the implication of meanings. This difficulty is overcome by formally introducing the concept of the meaning of words as factors of these words in the original phrase and by transition to a linguistic equation, which makes it possible to construct a calculus of meanings. Such an approach can be applied to the analysis of the entire corpus of natural language texts. Meaning mining is a time-consuming problem both for modelers and for high-end computers. Relying on domain-specific keywords, this approach can also be used to synthesis new models for that knowledge domain. In this case, linguo-combinatorial modeling expects identifying keywords in a specific subject field combined into phrases on the basis of which equivalent systems of equations with arbitrary coefficients are constructed. In a particular case, it can be differential equations and a well-known mathematical apparatus can be used to test it. In practice, the linguo-combinatorial modeling methodology is an effective heuristic device to analysis of ill-formalized systems and design of their conceptual models before running the simulation [11]. Such a heuristic device applies to conceptual models with a large number of words and phrases and the constructed set of models needs to be examined for adequacy and completeness.

Linguo-combinatorial models provide the possibility of constructing a calculus of meanings that can be easily and well-implemented on computers. The definition of meaning includes two significant characteristics: contextuality (meanings are calculated based on the abstract or applied context) and intentionality (arbitrary coefficients allow assigning such and such certain aspirations). As a result, the analysis problem of complex systems solved using linguo-combinatorial modeling methodology is reduced to the study of equivalent equations with arbitrary coefficients. In [9] it was proven that the number of these arbitrary coefficients is equal to the number of combinations of $n$ by $m+1$, where $n$ is the number of system variables (the number of different words in the original phrases); $m$ is the number of restrictions imposed on the variables describing the system (the number of different phrases). The following crucial conclusions can be drawn from the analysis of this formulation. Firstly, for all multidimensional systems with more than six variables, there is an optimum in the number of arbitrary coefficients in the structure of equivalent equations. Arbitrary coefficients are used to control the system, preserve and adapt it under external disturbances. This optimum is called the phenomenon of adaptative maximum [9]. The principle of resilient managing of the complex dynamic systems is that the systems must be controlled in such a way as to retain it in the range of adaptative maximum under changing environment. Secondly, to maintain the system performance, mobility and flexibility in the range of adaptative maximum, it is necessary to impose and remove restrictions, to increase the number of variables, degrees of freedom and coordinates of system basis, as well as to integrate or compose systems into the higher-level complexes.

For instance, let's consider two critical infrastructure systems, which are a part of regional critical infrastructure as such:

$$CIS_1 = C_{n_1}^{m_1+1},\ CIS_2 = C_{n_2}^{m_2+1},\ CIS_1 \subseteq RCI,\ CCIS_2 \subseteq RCI, \tag{1}$$

where $n_1$ and $n_2$ are the number of variables in the systems, respectively; $m_1$ and $m_2$ are the number of restricting manifolds imposed on the system variables, respectively; $s_1$ and $s_2$ are the number of arbitrary coefficients in the structures of equivalent equations, respectively.

Then, by superposition of common restricting manifolds $m_{\text{int}}$, a unified covering system, so-called integrated complex or joint ensemble, as a result is constructed. This unified complex can be expressed by the following formulation:

$$CIS_{\text{int}} = C_{n_1+n_2}^{m_1+m_2+m_{col}+1}. \tag{2}$$

Meanwhile, depending on specific parameters, two cases are possible in terms of increase in system adaptative capabilities:

1. When integration and unification into an ensemble is advisable and leads to an increase in the adaptative capabilities of the entire system and the original systems: $CIS_{\text{int}} > CIS_1 \cup CIS_2$. This leads to an increase in the system learnability and self-adjustment.

2. When the adaptation capabilities are less than the sum of the adaptation capabilities of the original systems (integration and unification into an ensemble is inexpedient or impracticable): $CIS_{\text{int}} < CIS_1 \cup CIS_2$.

In a first approximation, considering the combination of transport critical infrastructure and public health care critical infrastructure systems into an unified ensemble, the enhancement in joint adaptative capabilities of the social critical infrastructure system may be conditionally achieved. As a result, thereby, the resilience of entire critical infrastructure system can be improved. Following further the logic in a given example, this applies to all critical infrastructures (energy, cyber, safety, industrial, etc.) up to the regional critical infrastructure system as a whole.

## Results and discussion

Using linguo-combinatorial modeling methodology let's give a formal representation of the critical infrastructure resilience conceptualization by transition from system resilience description in natural language to mathematical formulations, i.e., combined equations. Let the following keywords, describing the critical infrastructure resilience, in a abstract phrase:

$$\begin{aligned} &\text{System Resilience} = \text{Preventive Capacity} + \text{Absorptive Capacity} + \\ &+\text{Restorative Capacity} + \text{Adaptive Capacity}. \end{aligned} \tag{3}$$

This phrase denotes keywords and implies only their meanings. In the existing structure of natural language, meanings are not indicated. Formally, the concept of meaning can be introduced in the following form:

$$\begin{aligned} &\text{System Resilience} = \text{Preventive Capacity} * \text{Measure}_1 + \text{Absorptive Capacity} * \text{Measure}_2 + \\ &+\text{Restorative Capacity} * \text{Measure}_3 + \text{Adaptive Capacity} * \text{Measure}_4. \end{aligned} \tag{4}$$

Let's denote the keywords characterizing system resilience as $C_i$ (C – Capabilities), and the meanings as $M_i$ (M – Measures). Then, formulation (4) can be represented as follows:

$$\sum_{i=1}^{4} C_i M_i = 0 . \tag{5}$$

Formulations (4) and (5) are the prime models of phrase (3). If the system resilience is formalized in the form of rough equilibrium mathematical equation: $F(r_1, r_2, r_3, r_4, t) = 0$, which can be conditionally used for balancing resilience capacities, the form (5) is obtained by differentiating this equation. Then, $C_i$ will be partial derivatives, and $M_i$ will be time derivatives of the variables.

This model is an algebraic ring and equation (5) can be resolved with respect to $C_i$, or with respect to $M_i$, by introducing a third group of variables so-called arbitrary coefficients $U_S$:

$$\begin{cases} C_1 = U_1 M_2 + U_2 M_3 + U_3 M_4, \\ C_2 = -U_1 M_1 + U_4 M_3 + U_5 M_4, \\ C_3 = -U_2 M_1 - U_4 M_2 + U_6 M_4, \\ C_4 = -U_3 M_1 - U_5 M_2 - U_6 M_3 \end{cases} \tag{6}$$

or in a different way:

$$\begin{cases} M_1 = U_1 C_2 + U_2 C_3 + U_3 C_4, \\ M_2 = -U_1 C_1 + U_4 C_3 + U_5 C_4, \\ M_3 = -U_2 C_1 - U_4 C_2 + U_6 C_4, \\ M_4 = -U_3 C_1 - U_5 C_2 - U_6 C_3 \end{cases} \tag{7}$$

where $U_1, U_2, U_3, U_4$ are the arbitrary coefficients that can be used to solve various problems on the manifold (5). For example, if it is necessary to achieve a maximum in system adaptive capacity (variable $r_4 \rightarrow \max$), then the arbitrary coefficients can be assigned as follows: $U_3 = -bC_1$, $U_4 = -bC_2$, $U_5 = -bC_3$, $U_6 = -bC_4$, and, thereof, the following formulation can be written:

$$\begin{cases} \dfrac{dr_1}{dt} = U_1C_2 - U_2C_3 - bC_1C_4, \\ \dfrac{dr_2}{dt} = -U_1C_1 - bC_2C_3 - bC_3C_4 = -U_1C_1 - b\left(C_2C_3 + C_3C_4\right), \\ \dfrac{dr_3}{dt} = -U_2C_1 + bC_2C_2 - bC_4C_4 = -U_2C_1 + b\left(C_2^2 + C_4^2\right), \\ \dfrac{dr_4}{dt} = bC_1C_1 + bC_2C_3 + bC_3C_4 = b\left(C_1^2 + C_2C_3 + C_3C_4\right). \end{cases} \quad (8)$$

If $b > 0$, then the variable $r_4$ steadily tends to a maximum, and the arbitrary coefficients $U_1$ and $U_2$ remain for manipulation of system motion path.

In the general case, with $n$ variables and $m$ manifolds (restrictions), the number of arbitrary coefficients $S$ will be equal to the number of combinations of $n$ by $m+1$:

$$S = C_n^{m+1},\ n > m\ . \quad (9)$$

The number of arbitrary coefficients $S$ is a measure of system uncertainty and adaptability. It can be also used for system control under interaction with external environment and adaptation to the dynamics in these interactions. The quantification rule of the number of arbitrary coefficients is schematically shown in Table 1.

Table 1

The matrix for number determination of the arbitrary coefficients (introduced from [12])

| $n$ | $m$ | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 1 | | | | | | | |
| 3 | 3 | 1 | | | | | | |
| 4 | 6 | 4 | 1 | | | | | |
| 5 | 10 | 10 | 5 | 1 | | | | |
| 6 | 15 | 20 | 15 | 6 | 1 | | | |
| 7 | 21 | 35 | 35 | 21 | 7 | 1 | | |
| 8 | 28 | 56 | 70 | 56 | 28 | 8 | 1 | |
| 9 | 36 | 84 | 126 | 126 | 84 | 36 | 9 | 1 |

Structural stability and the stability of system inherent relationships that ensures its integrity and identity, that is, the preservation of system basic attributes and features under influencing of various external and internal factors, is maintained by the adaptative capabilities of the elements of these systems [11]. In the proposed linguo-combinatorial model of critical infrastructures resilience, the adaptative capabilities of critical infrastructure systems are directly determined by the number of arbitrary coefficients in the structure of equivalent equations, and the optimum structural stability is achieved in the range of adaptative maximum, which is disclosed in various classes of systems with the dimension of more than six variables [10]. The more of arbitrary coefficients is, the higher the adaptative capabilities of the system are. On the other hand, the number of arbitrary coefficients depends on the number of imposed couplings. When imposing additional couplings, the number of arbitrary coefficients can either decrease or increase. In the case $n > 6$, when imposing additional restricting manifolds, the number of arbitrary coefficients will firstly grow, reach a maximum, and then go down. Therefore, the superposition of restricting manifolds can be considered as a way of adapting the system to environmental dynamics. In the limit, the number of arbitrary coefficients can be reduced to zero. In this case, it will be a critical infrastructure system with a rigid structure, which, with the slightest change in the external environment, will not be able to operate correctly. The system inability to effectively reduce mismatches in such-and-such way may be identified with system degradation when the resilience level is narrowed down. On-stream of resilience managing, system degradation results from the contradiction between the chosen modes of adaptation through self-learning or bootstrapping. Thus, the manipulations with arbitrary coefficients represent tuning or self-adjustment of the system performance to maintain the required level of resilience.

The Figure 1 schematically illustrates communication model of system interactions with the external environment. This combined control model by deviation and external disturbance shows how the system variables $X_1(t), \ldots, X_k(t)$ interact with environmental variables $P_1(t), \ldots, P_k(t)$, and mismatch error signals are transmitted to the system control unit. Therein, $\Delta_1(t), \ldots, \Delta_k(t)$ are the deviations of variables $P_1(t), \ldots, P_k(t)$ and $\Delta(t)$ is a deviation of the state variables $Y_1(t), \ldots, Y_n(t)$ that determine the trajectory of dynamic system in the resilience domain at the development cycle $[0, T]$ from the given values $Y_0(t)$. $\xi(t)$ are the random nature parametric disturbances of the external environment.

In this case, the system uses two adaptation mechanisms:

1) tuning or self-adjustment by manipulating arbitrary coefficients in the structure of system equivalent equations (control actions $U_A(t)$ in Figure 1);

2) training or self-learning, which involves the imposing of new restrictions on the system variables (control actions $U_B(t)$ in Figure 1).

In addition to these adaptation mechanisms, others are possible and programmable, such as reproduction, effective forgetting, restricting communications with the external environment, etc.

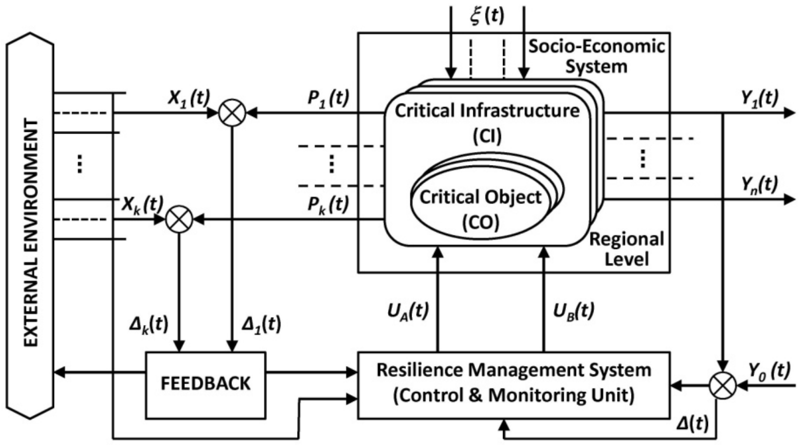


Fig. 1. The critical infrastructure resilience model based on combined control of system and external environment interactions

With regard to regional critical infrastructure systems that closely interact with a changing environment, the management goal of this type of systems is to keep them in the range of adaptative maximum: if it is necessary to maintain the resilience of the critical infrastructure, and vice versa, to remove them from the range of adaptative maximum: if the destabilization or resilience reduction of these systems is needed.

In the continuous learning and self-adjustment mode, the number of arbitrary coefficients changes in compliance with formulation (9), and this leads to the appearance of cycles in system development, which is illustrated in Figure 2, where the system development cycle starts at point 1, passes through a maximum in the number of arbitrary coefficients and ends at point 2, when transformation should occur, resetting previously imposed restrictions. Then, a new cycle begins at point 3, the system goes through maximum adaptive capabilities again, reaches the point 4, when transformation occurs again, and the system starts a new cycle at point 5, etc.

Solid line in Figure 2 shows evolutionary processes (system adaptation). The dotted line shows creative processes. The control algorithm of creative processes consists in selecting elements from a set and combining them into formulations like (4) or (5), resolving which a generating integrated system is obtained.

At point 2, several outcomes are possible: either the system will continue to evolve, or the system will move through a creative process to a new state, or will be destroyed. This model allows explaining the presence of cycles and crises in the development of complex dynamic systems. The emergence of crises (points 2, 4, 6, etc.) is the immanent attribute of these systems. It is only possible to influence the depth of crisis situations by launching the creative processes as early as possible.

The discussed model of complex dynamic systems self-organization implements the pattern of an adaptative maximum existence in the life cycle of these systems under flow of variables. The system resilience life cycle corresponds a set of crisis management phases (in [13, 14], there are: risk assessment, prevention, preparedness, warning, response, recovery, mitigation, learning) through which the system reaches maturity and becomes capable of operating effectively in recent conditions and challenges, and moving to a new performance quality.

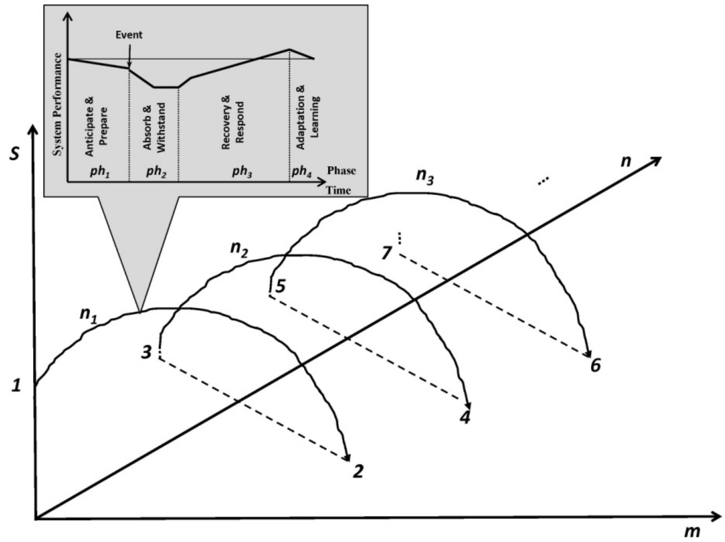


Fig. 2. Transformation of critical infrastructure system $n_1 < n_2 < ... < n_k$ (adopted from [11]). System resilience management life cycle phases: $ph_1 < ph_2 < ... < ph_4$. Trajectory of dynamic system: 1–2–3–4–5–6–7–…

Next, a linguo-combinatorial model of the regional critical infrastructure resilience based on the reference principals and regulations that have already been established in this research field [15, 16], will be considered.

If it is considered as keywords "Anticipatability", "Absorbability", "Responsiveness", "Recoverability", "Adaptability", "Resistibility", "Learnability", then in compliance with the methodology proposed above, the formulation for modeling critical infrastructure resilience in the form of conventional equation will be expressed as follows:

$$\sum_{i=1}^{7} C_i M_i = 0\,, \tag{10}$$

and the equivalent equations will be of the following form:

$$CIR:\begin{cases} M_1 = U_1C_2 + U_2C_3 + U_3C_4 + U_4C_5 + U_5C_6 + U_6C_7, \\ M_2 = U_1C_1 + U_7C_3 + U_8C_4 + U_9C_5 + U_{10}C_6 + U_{11}C_7, \\ M_3 = -U_2C_1 - U_7C_2 + U_{12}C_4 + U_{13}C_5 + U_{14}C_6 + U_{15}C_7, \\ M_4 = -U_3C_1 - U_8C_2 - U_{12}C_3 + U_{16}C_5 + U_{17}C_6 + U_{18}C_7 \;\; \to opt, \\ M_5 = -U_4C_1 - U_9C_2 - U_{13}C_3 - U_{16}C_4 + U_{19}C_6 + U_{20}C_7, \\ M_6 = -U_5C_1 - U_{10}C_2 - U_{14}C_3 - U_{17}C_4 - U_{19}C_5 + U_{21}C_7, \\ M_7 = -U_6C_1 - U_{11}C_2 - U_{15}C_3 - U_{18}C_4 - U_{20}C_5 - U_{21}C_6 \end{cases} \tag{11}$$

where $C_1$ is the anticipation ability of critical infrastructure, which includes such system attributes as preparedness degree, reliability, detection capability, planned maintenance, prognostic and health management, joint activity cooperation plan (agreements), protectability, operability, error and disturb sensitivity, etc.; $M_1$ is a variation in preventive capacity; $C_2$ is the absorbability of critical infrastructure, which includes such system characteristics as robustness, fragility, stress rate testing, damage level, limits of disruption, deviation and negative disturbance, internal redundancy, etc.; $M_2$ is the dynamics of absorptive capacity; $C_3$ is the responsiveness of critical infrastructure, which considers such system attributes as resource deployment, degree of concordance, facilitation ability, decoupling rate, communication plan, facilities and assets loss, vulnerability, independency, situational awareness, etc.; $M_3$ is a change in reactive capacity; $C_4$ is the recoverability of critical infrastructure, which considers such system performances as restoration index, maintainability (technological repairability), supportability, external redundancy, unplanned maintenance, recovery time, spare parts availability, resource storage capacity, modularity, segregability, decomposability, etc.; $M_4$ is the dynamics of restorative capacity; $C_5$ is the adaptability of critical infrastructure, which includes such system characteristics as self-organization ability, technological upgradability, technological transformability, integrability, interoperability, composability, reconfiguration ability, diversification coefficient, etc.; $M_5$ is a variation in adaptive capacity; $C_6$ is the resistibility of critical infrastructure, which considers such system performances as resistance/resistivity index, downtime ratio, safety margin, functionality, feasibility, autonomy, insurance, restart ability, etc.; $M_6$ is a change in resistive capacity; $C_7$ is the learnability of critical infrastructure system, which characterizes such system attributes as tuning and self-adjustment, creativity and improvisation, service level and costs, personnel availability, diagnozability, long-term/short-term reconstruction, etc.; $M_7$ is the dynamics of cognitive capacity; $U_1, U_2, ..., U_{21}$ are the arbitrary coefficients that can be used to solve various control problems on the manifold (10).

Using and resolving the formulation (11), the overall critical infrastructure resilience can be estimated and expressed in the following way:

$$CIR = CIS + \lambda \cdot (1 - CIS), \qquad (12)$$

$$\lambda = \prod_{i=1}^{7} M_i . \qquad (13)$$

where $CIR$ is the overall index of critical infrastructure resilience; $CIS$ is the overall index of the critical infrastructure safety evaluated using the methodology and mathematical formulations proposed in [17-19]; $\lambda$ is the efficiency of system self-preservation and self-recovery; $M_i$ are the target measures of system resilience capacities (critical infrastructure capabilities) described above.

The number of units in the linguo-combinatorial model of a critical infrastructure may vary. In terms of simulation accuracy, the more units are assigned and involved, the better. However, at the same time, the model visibility and pictorial presentation, and consequently, its perception by decision makers become worsen. For instance, if the unit “Recoverability” is decomposed into three units “Maintainability”, “Supportability” and “Redundancy”, either the model unit “Adaptability” is segregated in units “Transformability”, “Upgradability” and “Integrability”, then the total number of system variables will increase to nine. Hence, a formulation modeling the critical infrastructure resilience will contain nine variables:

$$\sum_{i=1}^{9} C_i M_i = 0 . \qquad (14)$$

In Figure 3 a framework of decision-making support technology in the field of resilience management of the critical infrastructures using a unified linguo-combinatorial model of regional critical infrastructure is shown.

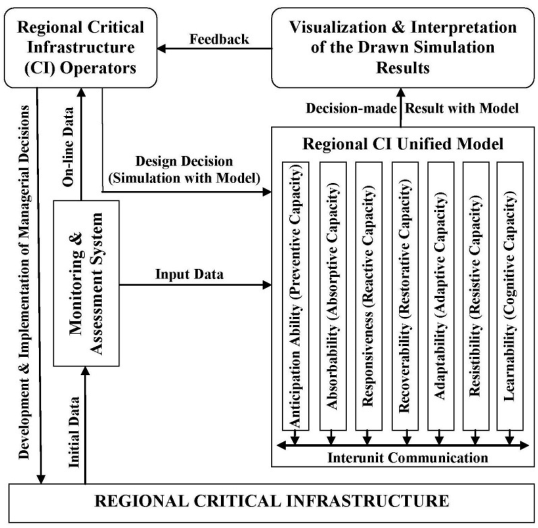


Fig. 3. Decision-making support technology in the field of resilience management of regional critical infrastructures (introduced and adopted from [12])

When modeling the resilience of critical infrastructures, it is important to consider the entire hierarchy of backbone capacities that make it up. Thereto, the decomposition principle based on the application of the seven-modular model proposed in [10, 11] can be used. In this case, the structure of units for each of the backbone capacity will be of the same type, and only the context and scope of individual units will vary. The uniformity of submodels allows for flexible synthesis and analysis of such complex dynamic systems as the critical infrastructures.

Operating situational centers in the regions possess practically all the historical data and on-line information necessary to implement and launch a linguo-combinatorial model of situational management of the critical infrastructures resilience using own or outsourced information-analytical and decision support systems. Missing control data for critical infrastructure resilience assessment and analysis can be obtained by expert judgements, public opinion polls and official statistics, if the materials are available and open-access.

The onrush of information technologies makes it possible to raise the question of mandatory preliminary modeling of the consequences of managerial decisions made in the field of ensuring the resilience of regional critical infrastructures. In perspective, this will allow identifying and avoiding many unjustified or erroneous decisions in resilience management, as well as provide the effective preventive analysis and control of the critical infrastructure facilities stability on a regional scale under adverse events and acting multiple threats. While developing by researchers and engineers all over the world system resilience models, critical infrastructure resilience modeling and estimation framework must be compatible and commensurable with the current guidelines for risk analysis and international standards for safety and security.

## Conclusion

The government's and the public's perception of critical infrastructure resilience may vary in terms of the choice of regulatory mechanisms. Within a specific group of people, the perception of the level of resilience can be relatively similar. Studying the issue, personal experience and up-to-date information allow to continually improving the level of resilience. The society is able to protect itself against the risks, which it has already experienced relatively well. However, the protection against threats that have not yet occurred is essential. The advancement of science and research identifies new and new threats that were not considered in the past. The current trend of this era should be a culture of resilience in all levels ranging from personal, corporate, regional and national security to global safety. The resilience community within the globalized society will adopt new roles and activities. Thus, in the last years the focus has shifted from engineering robust critical infrastructure systems by risk management methodologies to design resilient critical infrastructure systems using resilience conceptual frameworks.

The reference point for the high-quality and effective resilience management is the ability to model, analyze and estimate it for the purpose of identifying and reducing system vulnerabilities, as well as improving the critical infrastructures based on SWOT-simulation results. The crucial step of resilience management is resilience modeling and analysis. However, there are many obstacles in front of the resilience managers and analysts to control and estimate the system resilience. Ones of these obstacles are availability of adequate models and the accessibility of precise information for resilience modeling and assessment. In addition, resilience management practice requires, on one hand, qualified safety experts and security operators and, on the other hand, skilled resilience analysts and risk managers for the purpose of critical infrastructures sustainable development and protection. Hence, the modeling and conceptualization of critical infrastructures resilience is important when attempting to evaluate and explain different resilience management strategies. A variety of resilience control models is needed to design and implementation, since it is vital for placing national security strategies in their wider socio-economic and military-political contexts, as well as for in-depth identifying the multifaceted external and inherent threats that generate emergency situations and initiate adverse events.

Linguo-combinatorial models are a new type of models of the ill-formalized systems such as most critical infrastructures, and use the mathematical apparatus of post-non-classical science. At the level of non-classical science, observers and experts occupied a central place in managing safety and stability, and at the level of post-non-classical science, the main role is already assigned to resilience managers, operators and analysts. This mathematical apparatus propagation for designing linguo-combinatorial models of this type of systems of various scale and nature, and its wide applications provided the foundation for identifying a new emergent attribute of complex systems, namely, the phenomenon of adaptative maximum. The presence of adaptative maximum phenomenon in the operating life cycle of organizational and technical systems allows explaining the manner of critical situations that periodically occur in these systems. Hence, the resilience management strategy of the critical infrastructures implies that system resilience must be controlled in such a way as to keep it in the range of adaptative maximum under dynamically changing environment. The intensity of critical situations and crises is determined by the deviation from the range of adaptative maximum. This intensity can be significantly reduced by carrying out continuous problem monitoring of the system status and resilience characteristics, and taking appropriate anti-crisis measures. The use and availability of arbitrary coefficients, as well as the ability to extend the model provide the flexibility of model adjustment and customization for critical infrastructure resilience adequate estimation and efficient simulation.

The applicability of the linguo-combinatorial modeling of critical infrastructures resilience and the approach to situational management of the dynamics of their adaptative characteristics, have been examined. A linguo-combinatorial model for managing the critical infrastructures resilience, formalized in the form of an equivalent system of differential equations with arbitrary coefficients, has been developed. Manipulation of arbitrary coefficients provides the correction of system motion path within the bounds of resilient state space and retaining system operating characteristics in the admitted region for the purpose of performing optimal adaptative functions and balancing resilience capacities of the system. The advancement of system resilience theory, i.e., conceptual framework and formal representation, and the expanding of linguo-combinatorial modeling application domain to the class of critical infrastructure systems, has been proposed.

When managing and analyzing the resilience of critical infrastructures assisted by linguo-combinatorial modeling methodology, for each specific application case, it is necessary to verify the model, check its fitness for real system behavior and examine the convergence of control algorithm implemented in the model. Moreover, it is necessary to evaluate the mismatch errors of connecting inputs when synthesizing the resilience management structure, determine the optimal configuration of model parameters to problem-solving of system feedback stabilization in the range of adaptative capabilities and coordination of the modeled system features interaction at resilience management life cycle phases taken into consideration. Studying the matter of these issues is the subject of our further research.

## References


1. Council of the European Union Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*. 2008;L345:75–82.
2. Labaka L., Hernantes J., Sarriegi J.M. Resilience framework for Critical Infrastructures: An Empirical Study in a Nuclear Plant. *Reliability Engineering and System Safety*. 2015;141:92–105.
3. Mottahedi A., Sereshki F., Ataei M. et al. The Resilience of Critical Infrastructure Systems: A Systematic Literature Review. *Energies*. 2021;14(6):1571–1603.
4. Sathurshan M., Saja A., Thamboo J. et al. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks. *Infrastructures*. 2022;7(5):67–93.
5. Mottahedi A., Sereshki F., Ataei M. et al. Resilience analysis: A formulation to model risk factors on complex system resilience. *International Journal of System Assurance Engineering and Management*. 2021;(12):871–883.
6. Holling C.S. Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*. 1973;(4):1–23.
7. *Critical Infrastructure Resilience: National Infrastructure Advisory Council Final Report and Recommendations*. September 8, 2009. U.S. Department of Homeland Security. Washington, D.C., 2009:54.
8. Petersen L., Lange D., Theocharidou M. Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators. *Reliability Engineering and System Safety*. 2020;199(106872).
9. Ignat'ev M.B. *Golonomnye avtomaticheskie sistemy = Holonomic automatic systems*. Moscow-Leningrad: AN SSSR, 1963:204. (In Russ.)
10. Ignatyev M. Linguo-combinatorial simulation of complex systems. *Journal of Mathematics and System Science*. 2012;2(1):58–66.
11. Ignat'ev M.B. *Prosto kibernetika = Just cybernetics*. Saint Petersburg: Strata, 2016:248. (In Russ.)
12. Masloboev A.V., Putilov V.A., Ignat'ev M.B. Linguistic-combinatorial model of regional security management. *Trudy Kol'skogo nauchnogo tsentra. Informatsionnye tekhnologii = Proceedings of the Kola Scientific Center. Information technology*. 2018;(9):9–20. (In Russ.)
13. Pursiainen C. *The Crisis Management Cycle*. UK, London: Routledge, 2017:194.
14. Rehak D., Senovsky P., Hromada M., Lovecek T. Complex approach to assessing resilience of critical infrastructure elements. *International Journal of critical infrastructure protection*. 2019;(25):125–138.
15. Masloboev A.V., Bystrov V.V. Conceptual model of critical infrastructure viability in the context of modern security theory of complex systems. *Ekonomika. Informatika = Economy. Computer science*. 2020;47(3):555–572. (In Russ.)

16. Masloboev A.V. Towards a theory of regional critical infrastructure security and resilience. *Reliability and quality of complex systems*. 2020;(4):115–130.
17. Severtsev N.A., Yurkov N.K. *Bezopasnost' dinamicheskikh sistem na etapakh zhiznennogo tsikla = Security of dynamic systems at the stages of life the cycle*. Penza: Izd-vo PGU, 2023:568. (In Russ.)
18. Yurkov N.K., Mikhaylov V.S. *Integral'nye otsenki v teorii nadezhnosti. Vvedenie i osnovnye rezul'taty = Integral estimates in reliability theory. Introduction and main results*. Moscow: Tekhnosfera, 2020:152. (In Russ.)
19. Tsygichko V.N., Chereshkin D.S., Smolyan G.L. *Bezopasnost' kriticheskikh infrastruktur = Safety of critical infrastructures*. Moscow: URSS, 2019:200. (In Russ.)
20. Severtsev N.A. System analysis of determining the parameters of the state and the parameters of object surveillance to ensure safety. *Nadezhnost' i kachestvo slozhnykh system = Reliability and quality of complex systems*. 2013;(1):4–10. (In Russ.)
21. Mikheev M.Yu., Prokof'ev O.V., Savochkin A.E., Semochkina I.Yu. Ensuring reliability in the life cycle of artificial intelligence systems of responsible purpose. *Nadezhnost' i kachestvo slozhnykh system = Reliability and quality of complex systems*. 2023;(3):12–20. (In Russ.)

## Список литературы

1. Council of the European Union Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection // Official Journal of the European Union. 2008. L345. P. 75–82.
2. Labaka L., Hernantes J., Sarriegi J. M. Resilience framework for Critical Infrastructures: An Empirical Study in a Nuclear Plant // Reliability Engineering and System Safety. 2015. Vol. 141. P. 92–105.
3. Mottahedi A., Sereshki F., Ataei M. [et al.]. The Resilience of Critical Infrastructure Systems: A Systematic Literature Review // Energies. 2021. Vol. 14, № 6. P. 1571–1603.
4. Sathurshan M., Saja A., Thamboo J. [et al.]. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks // Infrastructures. 2022. Vol. 7, iss. 5. P. 67–93.
5. Mottahedi A., Sereshki F., Ataei M. [et al.]. Resilience analysis: A formulation to model risk factors on complex system resilience // International Journal of System Assurance Engineering and Management. 2021. № 12. P. 871–883.
6. Holling C. S. Resilience and stability of ecological systems // Annual Review of Ecology and Systematics. 1973. № 4. P. 1–23.
7. Critical Infrastructure Resilience: National Infrastructure Advisory Council Final Report and Recommendations. September 8, 2009. U.S. Department of Homeland Security. Washington, D.C., 2009. 54 p.
8. Petersen L., Lange D., Theocharidou M. Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators // Reliability Engineering and System Safety. 2020. Vol. 199. Article no. 106872.
9. Игнатьев М. Б. Голономные автоматические системы. М.-Л. : АН СССР, 1963. 204 с.
10. Ignatyev M. Linguo-combinatorial simulation of complex systems // Journal of Mathematics and System Science. 2012. Vol. 2, № 1. P. 58–66.
11. Игнатьев М. Б. Просто кибернетика. СПб. : Страта, 2016. 248 с.
12. Маслобоев А. В., Путилов В. А., Игнатьев М. Б. Лингво-комбинаторная модель управления региональной безопасностью // Труды Кольского научного центра. Информационные технологии. 2018. Вып. 9. С. 9–20.
13. Pursiainen C. The Crisis Management Cycle. UK, London : Routledge, 2017. 194 p.
14. Rehak D., Senovsky P., Hromada M., Lovecek T. Complex approach to assessing resilience of critical infrastructure elements // International Journal of critical infrastructure protection. 2019. № 25. P. 125–138.
15. Маслобоев А. В., Быстров В. В. Концептуальная модель жизнеспособности критических инфраструктур в контексте современной теории безопасности сложных систем // Экономика. Информатика. 2020. Т. 47, № 3. С. 555–572.
16. Masloboev A. V. Towards a theory of regional critical infrastructure security and resilience // Reliability and quality of complex systems. 2020. № 4. P. 115–130.
17. Северцев Н. А., Юрков Н. К. Безопасность динамических систем на этапах жизненного цикла. Пенза : Изд-во ПГУ, 2023. 568 с.
18. Юрков Н. К., Михайлов В. С. Интегральные оценки в теории надежности. введение и основные результаты. М. : Техносфера, 2020. 152 с.
19. Цыгичко В. Н., Черешкин Д. С., Смолян Г. Л. Безопасность критических инфраструктур. М. : УРСС, 2019. 200 с.
20. Северцев Н. А. Системный анализ определения параметров состояния и параметры наблюдения объекта для обеспечения безопасности // Надежность и качество сложных систем. 2013. № 1. С. 4–10.
21. Михеев М. Ю., Прокофьев О. В., Савочкин А. Е., Семочкина И. Ю. Обеспечение надежности в жизненном цикле систем искусственного интеллекта ответственного назначения // Надежность и качество сложных систем. 2023. № 3. С. 12–20.

## Информация об авторах / Information about the authors

**Андрей Владимирович Маслобоев**
доктор технических наук, доцент,
ведущий научный сотрудник лаборатории
информационных технологий управления
промышленно-природными системами,
Институт информатики и математического
моделирования имени В. А. Путилова
Федерального исследовательского центра
«Кольский научный центр Российской академии наук»;
главный научный сотрудник лаборатории
природоподобных технологий
и техносферной безопасности Арктики,
Центр наноматериаловедения
Федерального исследовательского центра
«Кольский научный центр Российской академии наук»
(Россия, г. Апатиты, ул. Ферсмана, 14)
E-mail: masloboev@iimm.ru

**Andrey V. Masloboev**
Doctor of technical sciences, associate professor,
leading researcher of the laboratory of information technologies for industrial-natural system management,
Putilov Institute for Informatics
and Mathematical Modeling
of the Federal Research Centre "Kola Science Centre
of the Russian Academy of Sciences";
chief researcher of the laboratory of nature-inspired
technologies and environmental safety of the Arctic,
Nanomaterials Research Centre
of the Federal Research Centre "Kola Science Centre
of the Russian Academy of Sciences"
(14 Fersmana street, Apatity, Russia)

**Автор заявляет об отсутствии конфликта интересов / The author declares no conflicts of interests.**

**Поступила в редакцию/Received** 08.09.2023
**Поступила после рецензирования/Revised** 15.09.2023
**Принята к публикации/Accepted** 08.10.2023