БЕЗОПАСНОСТЬ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

SAFETY IN EMERGENCY SITUATIONS

УДК 004.051, 006.015.7, 519.718, 519.876.2
doi: 10.21685/2307-4205-2025-3-12

A TERNARY CONCEPTUAL FRAMEWORK OF CRITICAL INFRASTRUCTURE RESILIENCE MANAGEMENT CYCLE

A.V. Masloboev

Putilov Institute for Informatics and Mathematical Modeling of the Federal Research Center "Kola Science Center of the Russian Academy of Sciences", Apatity, Russia
a.masloboev@ksc.ru

Abstract. *Background*. The study considers hot-button issues of analysis and modeling of the critical infrastructure resilience cycle in order to engineering automated tools for management information support of the resilient functioning of these complex multicomponent systems under triggering events of various nature and scale. *Materials and methods*. The joint use of the process approach, the formal apparatus of ternary relations and the technology of conceptual modeling provide a methodological basis for an integrated solution to the problems of analyzing the critical infrastructures resilience cycle and synthesizing effective organizational and technical systems for situational management of their resilient functioning. *Results and conclusions*. A triadic hierarchical model of a typical U-shaped critical infrastructure resilience cycle, based on a conceptual definition of entities and ternary relations between them in the form of a set of triads and modeling the process of maintaining the system resilience at different stages of situational management, is proposed. The developed model provides the possibility of a pictorial systemic knowledge representation about the stages of critical infrastructure resilience management process by constructing chains of interrelated triads, the analysis of which allows to identify new capacities and patterns of the system functioning when critical situations occur, as well as to determine adequate measures and assets of ensuring resilience to improve the effectiveness of situational management. The results obtained can find application in the field of design automation of the ontological and simulation models of critical infrastructure resilience intended for subsequent use in the development of intelligent information technologies for managing critical entities and infrastructure systems.

Keywords: system analysis, conceptual modeling, management, triadic model, life-cycle, resilience, critical infrastructure

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-2025-0054).

For citation: Masloboev A.V. A ternary conceptual framework of critical infrastructure resilience management cycle. *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and quality of complex systems.* 2025;(3):119–134. (In Russ.). doi: 10.21685/2307-4205-2025-3-12

ТРИАДНАЯ КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ЖИЗНЕННОГО ЦИКЛА УПРАВЛЕНИЯ 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
a.masloboev@ksc.ru

Аннотация. *Актуальность и цели*. Рассматриваются актуальные вопросы анализа и моделирования жизненного цикла жизнеспособности критических инфраструктур с целью разработки автоматизированных средств информационной поддержки управления устойчивым функционированием этих сложных многокомпонентных систем в условиях возникновения инициирующих событий различной природы и масштаба. *Материалы и методы*. Совместное применение процессного подхода, формального аппарата тернарных отношений и технологии концептуального моделирования обеспечивает методологическую основу системного решения задач анализа жизненного цикла жизнеспособности критических инфраструктур и синтеза эффективных организационно-технических систем ситуационного управления их устойчивым функционированием. *Результаты и выводы*. Предложена триадная иерархическая модель типового U-образного жизненного цикла жизнеспособности критических инфраструктур, основанная на концептуальном описании объектов и тернарных отношений между ними в виде совокупности триад и моделирующая процесс обеспечения жизнеспособности системы на различных этапах ситуационного управления. Разработанная модель обеспечивает возможность наглядного системного представления знаний об этапах процесса управления жизнеспособностью критических инфраструктур за счет построения цепочек взаимосвязанных триад, анализ которых позволяет выявить новые свойства и закономерности функционирования системы в условиях критических ситуаций, а также определить адекватные меры и средства обеспечения жизнеспособности для повышения эффективности ситуационного управления. Полученные результаты могут найти применение в сфере автоматизации синтеза онтологических и имитационных моделей жизнеспособности критических инфраструктур, предназначенных для последующего использования при разработке интеллектуальных информационных технологий управления критически важными объектами и системами.

Ключевые слова: системный анализ, концептуальное моделирование, управление, триадная модель, жизненный цикл, жизнеспособность, критическая инфраструктура

Финансирование: работа выполнена в рамках государственного задания ИИММ КНЦ РАН (НИР № FMEZ-2025-0054).

Для цитирования: Маслобоев А. В. Триадная концептуальная модель жизненного цикла управления жизнеспособностью критических инфраструктур // Надежность и качество сложных систем. 2025. № 3. С. 119–134. doi: 10.21685/2307-4205-2025-3-12

Introduction

Critical infrastructure is the interconnected networks of energy grids, transportation systems, water treatment facilities, and communication networks forms the foundational backbone of modern society, national security, and economic prosperity. These systems are increasingly exposed to a complex and escalating spectrum of threats, ranging from acute shocks like natural disasters, cyber-attacks, and geopolitical incidents to chronic stresses such as climate change, aging assets, and operational obsolescence. The inherent interdependency of these infrastructures means that the failure of a single node can trigger cascading effects, amplifying disruptions far beyond their point of origin and threatening societal stability.

Crisis management and safety paradigms, which are often predicated on probabilistic risk assessment and static protective measures, are proving insufficient to address this new reality. These approaches tend to be reactive, focused primarily on hardening assets against a limited set of anticipated threats, and often lack the adaptive capacity to evolve in the face of novel, unforeseen, or exponentially growing challenges. The core problem, therefore, transcends mere protection; it is the problem of ensuring systemic resilience is the ability to anticipate, prepare for, adapt to, withstand, and rapidly recover from disruptions in a dynamic and uncertain threat environment.

This gap between conventional practices and contemporary needs requires a fundamental shift in management philosophy. The central problem this research work addresses is the absence of a unified, dynamic, and cyclic framework for resilience management support that explicitly integrates the three main indispensable temporal dimensions of system resilience: (1) proactive anticipation of disruptive events; (2) operational absorption of impacts during these events, and (3) transformative adaptation following events to foster learning and improvement of the system situational control.

Consequently, the development of a triadic conceptual model of the critical infrastructure resilience cycle is presented as an urgent endeavor. This type of models is designed to formalize and orchestrate the continuous recurrent interplay between anticipation, absorption, and adaptation, transforming resilience and its situational management per se from a static goal into a dynamic, self-improving process.

Traditional risk management for critical infrastructures is often focused on response and recovery after a disruptive event and managed within a single sector like energy or transport. Meanwhile, the triadic conceptual models force a shift to a proactive, holistic mindset. By formally integrating anticipation, it mandates preparedness and planning before a disruption occurs. Its cyclical nature ensures that lessons from the absorption and adaptation phases continuously feed back to improve future anticipation, breaking down organizational silos. It is worth noting that disruptions are not single events, but processes with distinct phases: before, during, and after. Traditional models often focus on one phase (e.g., response) at the expense of others.

The triadic models allow fully overlapping the whole resilience cycle (anticipation-absorption-adaptation) and provide a structured conceptual framework to allocate resources, develop capabilities, and assign responsibilities for each phase explicitly. This ensures that preparedness is not neglected in favor of response, and that post-event learning is not lost, but is formally captured to drive further system evolution.

A system that only withstands shocks, but does not learn from them is doomed to repeat its failures. Static resilience is insufficient against evolving threats. The adaptation phase is the model's key innovation. It institutionalizes learning and systemic evolution. By formally analyzing system performance after a disruption, organizations can move from simply "bouncing back" to "bouncing forward", notably, becoming smarter, more robust, and more adaptable than before. This creates a learning loop that is essential for long-term survival. Modern critical infrastructures are systems of systems. A failure in the power grid can crash telecom networks, which can disable financial systems and hinder emergency response. A holistic triadic conceptual model requires cross-sector analysis. When designing for anticipation phase, analysts must map dependencies. During absorption phase, coordinated action across sectors is essential. Adaptation phase involves updating protocols and infrastructure across interconnected systems. This systemic view is the only way to prevent and manage cascading failures.

Limited budgets require strategic investment. Without a systemic model of the resilience management cycle, spending can be misallocated, e.g., over-investing in hardening assets (anticipation phase) while under-investing in response capabilities (absorption phase) or R&D for future threats (adaptation phase). The triadic conceptual model provides a rational framework for decision-making. It allows policymakers and CI operators to identify gaps in each phase, conduct cost-benefit analyses for resilience investments across the entire cycle, and justify spending on "soft" capabilities (e.g., training, exercises, data sharing) alongside "hard" infrastructure (e.g., sea walls, backup generators).

Resilience is often discussed qualitatively. Therefore, triadic conceptual models help to manage what is difficult to measure. A formal model, especially one with mathematical formalizations, allows for the development of metrics and KPIs for each phase, i.e.: time to detect a threat, redundancy levels, preparedness scores (for the anticipation phase); minimum operating capacity, time to stabilize, performance loss (for the absorption phase); time to full recovery, percentage improvement in performance post-upgrade (for the adaptation phase). This enables objective assessment of resilience and holds organizations accountable for their performance throughout the cycle.

Resilience involves multiple stakeholders: government agencies, private critical infrastructure owners, first responders, and the public. Confusion in roles leads to chaos during a crisis. The triadic conceptual model serves as a coordination tool. It creates a common language and a shared mental model for all stakeholders. It clearly defines who is responsible for what actions in each phase, streamlining communication and collaboration before, during, and after a disruptive event.

Engineering and analyzing triadic conceptual models for management support of the critical infrastructures resilience cycle is not merely an academic exercise. It is a strategic imperative for national security, economic stability, and public safety. The importance stems from the severe limitations of traditional approaches and the unique advantages triadic models provide in addressing the complex nature of modern threats. In essence, triadic conceptual models transform resilience management from an informal, reactive practice into a formal, continuous, and proactive discipline. It is the difference between fragility (breaking under stress), robustness (resisting stress, but potentially breaking under unexpected stress), resilience (bending, but not breaking, and then recovering), and antifragility (the goal of the triadic cycle is becoming stronger and better adapted because of the stressors and disruptions encountered). For the critical infrastructures that underpin our way of life, achieving this antifragile state is not optional. It is essential. The triadic conceptual models provide the blueprint to shift from original fragility paradigm well-approved in safety sciences to the novel antifragility philosophy in resilience studies.

This ongoing research work articulates the problem space of modern critical infrastructure vulnerability, delineates the limitations of extant management models, and formally introduces the triadic conceptual model as a necessary, holistic framework for governing resilience throughout the entire life-cycle of a disruption: before, during, and after an adverse event to ensure the resilient functionality and performance of the vital services upon which society depends. Sequentially, this study is an expansion and adaptation of the earlier research results [1–3] drawn in the field of regional security and critical infrastructure resilience management information and analytical support.

Material and methods

The background of this work is based on the related research materials of domestic and foreign studies which contributed to the advancement of the modern theory and practice of ensuring reliability, stability,

security of complex systems and risk management in general [4–10], as well as to solving problems in the field of developing models, methods and technologies for situational management information support of critical entities and infrastructures [11–26].

The methodology used in this research is based on the systems analysis of various events, factors, processes, cause-and-effect relations in the field of studying the domain, subject and context of this work, evaluation of the collected information, comparative and contrastive analysis, as well as conceptual modeling of the research object (resilience management cycle and resilience in tote).

The carried out content-analysis of domestic and foreign scientific literature in the examined research domain showed that most of the studies focus on considering general methodological issues of developing the resilience concept and solving specific problems of situational management at individual phases of the system resilience cycle in various sectors of critical infrastructures. These studies propose approaches to the analysis, modeling and indicator-based assessment of the performance indices of individual elements and phases of the critical infrastructures resilience cycle based on the preventive security analytics tools, risk management, scenario and expert methods of decision support for managing the resilient functioning of given class of systems. At the same time, issues related to the automation of poorly formalized phases of the resilience cycle, including the initiation and progression of critical situations, risk anticipation and threat absorption, adaptation to the consequences of initiating events, as well as the organization of end-to-end resilience situational management and the lack of any generally accepted normative document (e.g., an official agency-level standard) regulating the development and relevant choice of tools for situational management of critical infrastructures resilience in accordance with a particular life-cycle model (scenario) of the propagation of initiating events caused by external or internal impacts on the elements and critical functions of these systems, remain insufficiently developed from a scientific point of view. Known approaches to the structural analysis and formalization of the resilience management cycle of critical infrastructures [12–26] are generally characterized by high abstractness due to the lack of formal conceptual models that take into account the specific features of ensuring the resilient functioning of critical infrastructures at various phases of situational control, as well as insufficient complementarity due to the lack of a clearly defined conjugation with the adopted classifications of potential accident facilities, critical entities and infrastructures (technical-organizational aspect).

Due to the imperfection of the regulatory and methodological base in the field of situational management of the critical infrastructures resilience, each agent of management (security agency, owner of a critical facility, operator of a situational center, etc.), responsible for ensuring the stable functioning of critical infrastructures, are forced to solve these problems at different phases of the system resilience cycle by their own efforts and means, guided by local acts, directives and their own regulations, which is not always well-founded, reasonable and effective in the conditions of the onset of complex dependent failures that generate chains of adverse, including unexpected events that initiate abnormal and emergency situations in the system. A unified representation of the resilience cycle of critical infrastructures using formal conceptual models is designed to improve the consistency and overall efficiency of the situational management of these complex systems via automated processing and analysis of expert knowledge about the static and dynamic characteristics of the safety and resilience of critical infrastructures elements and their interrelations comprised in these models in order to identify the potential for such initiating events.

The conceptual and categorical apparatus of the study comprises the following concepts and definitions [27, 28].

Vulnerability is considered as a characteristic of an element of the critical infrastructure design, implementation, or operation that renders it susceptible to disruption or destruction by a threat and includes dependencies on other types of infrastructure. In other words, it is an indicator of direct risks and an intrinsic property of something resulting in susceptibility to a risk source that can lead to the occurrence of hazardous events with negative consequences for the critical infrastructure elements making it act adversely. Threat is a potential cause of an unwanted incident in critical infrastructures, which can result in harm to a system in the large, individuals or critical entities, the environment or the society.

A disruptive event (syn.: disturbance, adverse/undesired event, etc.) is a singular instance of a phenomenon negatively affecting a system (critical infrastructure/entity) or its critical functionality which refers to the ability of a system to provide predetermined essential functions. Disruptions lead to negative consequences and decrease of performance. This implies that there is an actual (i.e., non-zero) exposure to the event and that the system is not able to fully resist or absorb its impact. Disruptive events comprise all potential causes and risk sources of a loss of functionality of the critical infrastructure system, i.e.: natural hazards, technical failures, human errors, extreme loads, and organizational issues, intentional malicious attacks, etc.

A cascading failure or effect occurs when a disruption in one infrastructure causes the failure of a component in another infrastructure or asset, which subsequently causes a disruption in another infrastructure. Cascading effects are the impacts of an initiating event. An initiating (triggering) event is the first in a sequence of natural, accidental or intentional events that may affect one or several infrastructure systems.

An incident is a chain of disruptive events affecting multiple systems or its elements either in series or spreading in parallel. Incident management is the management of appropriate measures to deal with a potential emergency situation characterized by high complexity, uncertainty and time pressure that could lead to possible large scale damages and requires a specific organization and coordination to ensure the restoration of the critical situation.

Generally, emergency means any critical situation which has or may have an adverse impact on people, the environment or property and which may result in a call for assistance and protection. Crisis is a high level emergency situation in critical infrastructure with high uncertainty that disrupts the core activities and/or credibility of critical entities and requires urgent preventive and reactive actions. Crisis management involves all processes (analysis, prevention, and preparation response plans for known and expected critical situations/scenarios) which aim at repelling the emergency and reducing the impact of crises and disasters. Crisis and resilience management are very similar to each other in recurrent nature of the system situational control and monitoring procedure.

Disaster is a serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources. Disasters are often described as a result of the combination of: the exposure to a hazard; the conditions of vulnerability that are present; and insufficient capacity or measures to reduce or cope with the potential negative consequences. Disaster impacts may include loss of life, injury, disease and other negative effects on human physical, mental and social well being, together with damage to property, destruction of assets, loss of services, social and economic disruption and environmental degradation.

For simplicity, upon further discussion the concepts critical/emergency situation, disruptive event, initiating event being used will be identified.

The types and criteria of initiating events and emergency situations occurring in critical infrastructures are considered in detail in the research works [11, 29–32].

All types of initiating events (critical situations) have one important detail in common: the initiation process of each of them is hidden (non-obvious) in its matter and, as a rule, begins under normal conditions as a result of accumulation of contradictions, sources of threats, defects and gradual degradation of the system.

Based on the progression and propagation dynamics initiating events in critical infrastructures can be conditionally classified as follows [2, 28]:

– the slowly progressing initiating events are critical situations when there is a sufficiently large float time for adoption and implementation of preventive and reactive measures to mitigate the consequences of destructive impact of such events on the system;

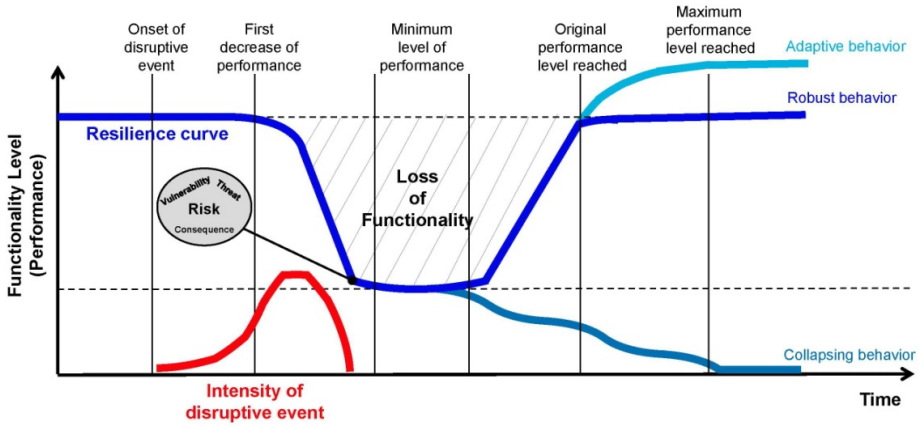
– the rapidly progressing initiating events are critical situations, the rate of intensification and spread of which is limited, that provides a float time for making and implementing the managerial decisions aimed at stabilizing the system or reducing the damage caused;

– the instantaneous initiating events when there is no float time for making operational decisions on situational management.

The sudden-onset disruptive event is a disruption whose intensity builds up instantaneously (e.g., an earthquake or a tidal flood). The slow-onset disruptive event is a disruption whose intensity increases over a longer period of time (e.g., deterioration of components or increasingly harsher conditions due to climatic changes). Meanwhile, a slow-onset disruptive event can still lead to a sudden collapse of performance (e.g., when approaching a bifurcation or tipping point). Whether the onset of a disruptive event is considered slow or fast should depend on the time-scale of the considered critical infrastructure system, i.e., if the intrinsic dynamics of the system are faster than the emergence of the event, the event should be referred to as slow-onset [28].

Each of the listed classes of initiating events may be followed by cascading effects due to the interdependence of critical infrastructure systems and their elements. Rapidly progressing and instantaneous critical situations are the most typical for most modern critical facilities, entities and infrastructures. For effective situational management of such events at all levels of decision-making (strategic, tactical and operational), appropriate methods and tools of information and analytical support are required.

Reviewing the known definitions of resilience concepts and its usage for critical infrastructure systems, it should be noted that three backbone resilience capacities (absorptive, restorative, and adaptive) are at the center of the systems-of-systems approach to analyzing and managing critical infrastructures subject to their interdependencies, and are linked with the various stages of typical critical infrastructure response cycle to disruption (before, during and after the disruptive event). In terms of the systems approach a resilience cycle corresponds a conceptual sequence of phases in the unfolding of a disruption, in which some capacities and actions are more important than others (see resilience phases in Fig. 1).



U-shaped Resilience Cycle Phases						References
Plan		Absorb		Recover	Adapt	[12]
Original steady phase		Disruptive phase		Recovery phase	New steady phase	[13]
Crisis preparedness	Detection ability	Responsiveness		Recoverability	Adaptability	[14]
Understand risks	Anticipate / Prepare	Absorb/Withstand		Respond/Recover	Adapt/Transform	[15]
	Resist	Absorb		Adapt/Restore	Improve	[16]
Preparation and Prevention		Absorption and Response		Recovery		[17]
Prepare and Prevent		Protect	Respond	Recover		[18]
Stability		Disruption effect	Reaction	Rehabilitation	Return to stability	[19]
Pre-disturbance		Disturbance	Emergency	Restoration	Post-restoration	[20]
Pre-disturbance		Disturbance progress	Post-disturbance	Restoration state	Post-restoration	[21]
Initial normal state		Damage propagation	Disrupted state	System recovery process	Recovered state	[22]
Stable original state / Reliability		Disruption / Vulnerability	Disrupted state	System recovery / Recoverability		[23]
Resilient state		Event progress	Post-event degradation state	Restorative state	Post-restoration state	[24]
Risk assessment	Prevention / Prevention	Warning	Response	Recovery	Learning	[10, 25]
Pre-event/disruption		During event/disruption		Post-event/disruption	Next event/disruption preparation	[26]
Ready mode / Problem monitoring, predictive analysis, stress-planning		Risk identification and early warning / Emergency response		Risk treatment / Restoration	Risk Mitigation / Consequence elimination and analysis	[5, 7, 11]
Normal mode of operation	Event origination and development	Event initialization and disturbance / Emergency mode of operation		Recovery	Regeneration / Post-Emergency mode of operation	[2, 7, 11]

Fig. 1. Critical infrastructure resilience cycle and its main phases across domestic and foreign studies using the performance curve (adopted and extended from [28])

Typically, it includes a anticipation/preparation/prevention phase, an absorption/response phase, a recovery phase. After the recovery phase, an adaption phase might take place, during which the system learns from the disruption and integrates the lessons learned, making it more resilient towards the next disruption. For simplicity, the resilience cycle assumes that disruptions do not overlap, and that the main effects of a disruption on the functioning of the system accumulate in a single, concise time span. It is clear, however, that the resilience capacities can only in part be mapped to the phases. For example, learning and anticipation are needed throughout the entire cycle, not only in their respective phases [28].

There is considerable variation in terminology concerning the different phases a system goes through during the unfolding of a disruption. A popular way to illustrate this resilience cycle is via an idealized performance curve, which typically starts shortly before a single disruptive event and ends after the system has recovered from the associated impacts. The curve is conceptually divided into successive phases, which are

named differently depending on the domestic and foreign studies (Fig. 1). Most authors name the phases in accordance with the resilience process that typically takes place during that time. Some refer to the resilience capacity that is thought to be most important during the corresponding time period. Others distinguish the phases based on the current state of the system or the progression of the disruption [28]. Despite all these differences in the naming, among researchers using the performance curve for illustrative purposes, there is a consensus on the general order and duration of the phases (Fig. 1), i.e., the start and end time points of the phases are largely consistent across studies. As noted in [28], the other ways to conceptualize the succession of resilience-constituting phases or processes exist, especially among frameworks which emphasize a system's ability to adapt. Notable examples in this regard are the Holling adaptive cycle [8] and the approach proposed in [33, 34] which comprises the recursive phases of sensing, anticipating, adapting, and learning.

Results and discussion

At present, various information and analytical support tools aimed at preparing guidelines for decision-makers are being developed for effective situational management of critical facilities, entities and infrastructures. Recommendations are usually elaborated through scenario analysis and forecasting possible variants of disruptive event propagation in these systems and aggregation of heterogeneous operational and historical data retrieved from various sources. These actions are performed on the basis of certain formal models that allow to study the structure and capacities of the controlled objects, as well as to describe the functions and relationships between the elements of the situational management system and the processes progressing in it. Such formal models serve as an intermediate between the mental representations of experts in problem domain and the developed management information technologies and allow to fully or partially automate the engineering process of the proper software tools for decision-making support.

From the process approach [35] point of view, the situational management cycle of the critical infrastructure resilience under adverse events, emergency and abnormal situations can be described as an assigned sequence of performing certain control problems/functions, each of which corresponds to a specific phase of the resilience cycle. The cycle duration consists of the total time of the initiating event impact on the system and its adaptation to new operating conditions. The cycle is an iterative process (transition/recurrence of initiating events and operating scenarios over time), during which certain types of resources are consumed to restore the normal operability of the system after a failure or destructive impact of external factors, and a related set of functions and operations grouped by a certain attribute/criterion and aimed at increasing the adaptive capabilities of the system are implemented. In this case, for each cycle phase a subprocess, source materials and information, executive agents, regulations and process execution procedures, as well as its outputs are assigned. The time schedule for implementing the situational management functions of system resilience describes the time frame and sequence of the operations and program activities defined at the appropriate resilience cycle phases of the system, and is represented in the form of a network structure as a rule. Then, in general, a system resilience cycle model is understood as a structured graphical description of a network of interconnected processes and/or functions/operations that reflect the logical structure and technical-organizational aspects of system functioning, as well as the mechanisms of interaction between agents and objects of resilience situational management.

In this interpretation, the formal model of the system resilience cycle can be represented as a graph of control functions aimed at maintaining and supporting the resilient functioning of the system when an initiating event occurs:

$$RLC = G\left(CF^i, cf_0, cf_e, E, S, ES, ECF, R, ER\right),$$

where $CF^i = \left\{cf_{ij}\right\}$, $i = \overline{1,n}$, $j = \overline{1,m}$ is a set of nodes (resilience management cycle phases), each of which corresponds to the one or more resilience control functions $cf_i = \left\{ cf_{ij}\left(r_{ij}, t_{ij}\right) \right\}$, depending on the resources r_{ij} and the time t_{ij} necessary for its implementation; n is the number of cycle phases which in the most simple and general case is equal the number of control functions m implemented at the i-th phase of system resilience cycle. Then, $RLC = \bigcup_{i,j=1}^{n,m} \left\{cf_i\right\}_i$ is a process which comprises a set (composition) of control functions; cf_0 and cf_e are the input (e.g., "Monitoring" or "Understand risks" phase) and output (e.g., "Learning" or

"Evaluation" phase) nodes, respectively; E is a set of control edges, such that $\forall j,k \in CF \cup \{cf_0, cf_e\} : (j,k) \in E$, if a situation is possible when the control function j will be performed after the control function k is performed; S is a set of nodes corresponding to the agents/entities of resilience situational management, performing certain functions within the resilience cycle phases ($S \cap CF = \Omega$, where Ω is an empty set); ES is a set of subordination edges, such that $\forall j,k \in S : (j,k) \in ES$, if the agent of management k is subordinate to the agent of management j; ECF is a set of function performing edges, such that $\forall j \in S, k \in CF : (j,k) \in ECF$, if the control function k can be performed by the agent of management j; $R = \{r_q(Vol, Typ, C)\}, q = \overline{1,l}$ is a set of resources different types necessary for the support and implementation of resilience management cycle phases; Vol is the volume of the q-th resource available for the implementation of preventive measures when managing the critical situations that have arisen; Typ is the type of the q-th resource; C is the cost of a unit of the q-th resource; ER is a set of weighted edges of resource use such that $\forall j,k \in R, k \in CF : (j,k) \in ER$, if the control function k when performing uses the resource j during allotted period of time (the weights are assigned by experts).

An independent phase of the process (resilience cycle) which is represented as a composition of control functions, is illustrated in Fig. 2 and can be formally written as follows:

$$cf_i = f\left(IN^R(CF), OUT^R(CF), t\right),$$

where $IN^R(CF)$ is a set of input resources of the process implementing the i-th composition of control functions; $OUT^R(CF)$ is a set of output resources of the process implementing the i-th composition of control function; t is the time required to perform the i-th composition of control functions.

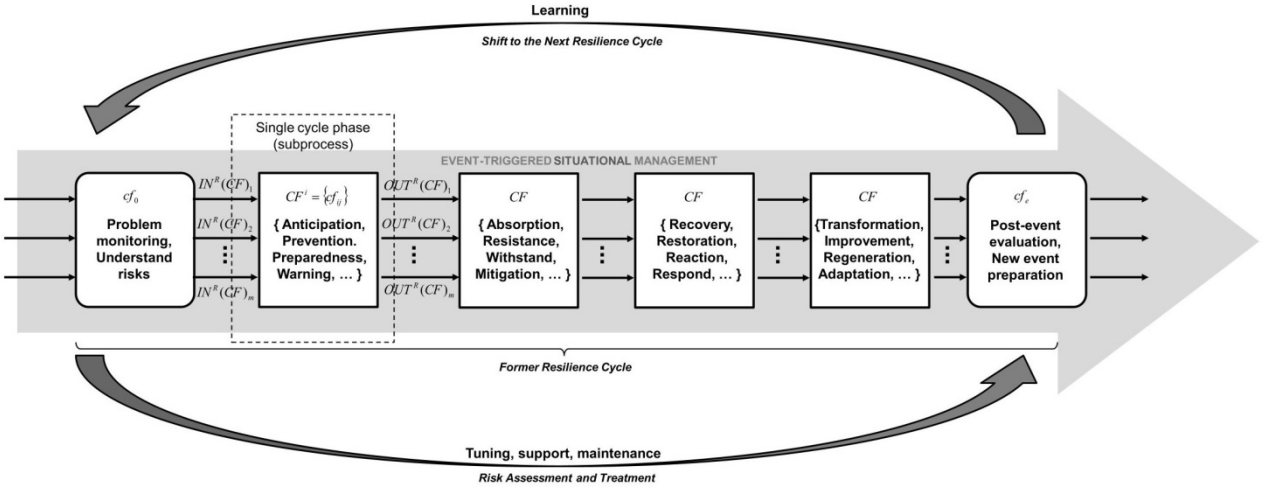


Fig. 2. A schematic illustration of the phased system resilience control cycle in the context of process approach

The system model of the critical infrastructures resilience cycle is intended for the conceptual description and subsequent analysis of the system resilient functioning phases (risk anticipation, impact absorption of the actuating threats, recovery, and adaptation) in the conditions of origination and propagation of critical situations occurring in these infrastructures, as well as for identifying the causes of initiating events. The use of the system model allows identifying and typifying the current phase of the critical situation progression, assessing the resource costs for the implementation of preventive and reactive measures at this phase depending on the selected management scenario, and provides also the possibility to predict its dynamics at a qualitative level in the specified operating conditions. The formalized representation of the resilience situational management cycle when an adverse event occurs in critical infrastructure facilities is based on the adoption and applied adaptation of the regional security conceptual model developed in the course of previous studies [1, 2] to the formal description and analysis of the process and modes of operation of this class of systems in the context of its resilience.

According to studies [6, 36], from the point of view of systems analysis, the conceptualization and definition of the concept of a system is based on ternary relations or triads as three-element sets. A triad reflects in some way the systemic law of the world structure: any triad comprises an infinite number of triads; on the other hand, it can expand infinitely, since each triad is located inside an even larger triad. Systemic triads are formed by three elements of the same level, each of which can serve as a measure of the combination of the other two. Based on the triadic approach, the methodology for managing the critical infrastructures resilience, by analogy with the methodology for ensuring the safety of complex organizational objects proposed in [6], can be considered in three ways [6]:

– as a study of the sledding process towards a goal, i.e. the generation and connection of triads that form the situational management cycle of the critical infrastructures resilience;

– as a study of the systemic logical organization of actors, entities, technologies and means necessary to achieve the objective: ensuring the resilient functioning of critical infrastructure elements, i.e. maintaining their resilience in the event of critical and emergency situations through effective situational management;

– as a study of the new knowledge producing and acquisition process based on existing approaches in the field of safety and security of complex systems, i.e. designing an integrated conceptual framework that combines methods and tools of information and analytical support used at different phases of the resilience cycle.

Therefore, to design a conceptual model of the resilience cycle of critical infrastructures, it is proposed to use a triadic approach to conceptual modeling of complex processes and systems [5, 36]. The apparatus of triadic network models provides a visual representation and formalization of knowledge about the target, structural, and dynamic operating characteristics of complex entities, possible scenarios and outcomes of the appropriate systems and processes behavior. The triadic approach is well-used to model the life-cycle of complex control objects of various natures, since it takes into account the cyclicality characteristics of the system/process functioning and development.

Next, a ternary conceptual framework of the resilience situational management cycle of the critical infrastructures shown in Fig. 3 will be designed and discussed. Each of the phases of this cycle considered above will correspond to its own triad. The triadic conceptual model of the critical infrastructures resilience cycle consists of a set of interconnected submodels, each of which is represented as a triad – a graph with three nodes. The nodes correspond to the sets of objects of the model, and the edges – the relationships of different types (e.g., functional, structural, etc.) between them. If necessary, the ends of the triads can be connected to each other, forming new triads. Such a model representation is suitable and visual for the system analysis of situational management processes and scenarios of the critical infrastructures resilience under initiating of disruptive events.

Optimization of the entire process of situational management consists in the sequential design of an effective system for ensuring the resilient functioning of critical infrastructures for all phases of the resilience cycle based on the analysis, improvement and development of each triad.

As follows from Fig. 3, the situational control cycle of the critical infrastructures resilience is ultimately represented in the form of a gradual expansion of triads nested within each other and forming an integrated holistic triad in the form of a hierarchical system. The given number of levels is not exhaustive. Triads can be expanded by supplementing with various resilience characteristics depending on the type of critical infrastructures under examination, the event-driven scenario and/or the problem situation context, the selected criteria, measures and dimensions of resilience, as well as the methods and tools of information and analytical support used at the appropriate levels of situational management.

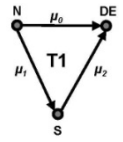
When forming triads, the following requirements must be met and fulfilled [5]:

– the components of triads must be interconnected by some relation (e.g., by activity category or by functional dependence);

– the components of triads must be adequate and relevant to each other, i.e., fit to each other by some principle and be mapped onto each other.

The first triad (*T1*) expresses the needs for elimination and mitigation of the disruptive event that has initiated or the threatening source of its occurrence in the functioning process of critical infrastructure. In this case, there is a set of needs *N* associated with the elimination and mitigation of a set of initiating events *DE*. For it, a set of strategies *S* for implementing preventive and reactive measures to mitigate the negative impact on the system elements and functions of a set of initiating events *DE*, i.e. to satisfy the needs *N*, is determined. In this case, one set can be mapped onto another:

$$\mu_0 : N \to DE,$$
$$\mu_1 : N \to S,$$
$$\mu_2 : S \to DE.$$



The inverse mapping is also possible, e.g.: $\mu_2^{-1} : DE \to S$.

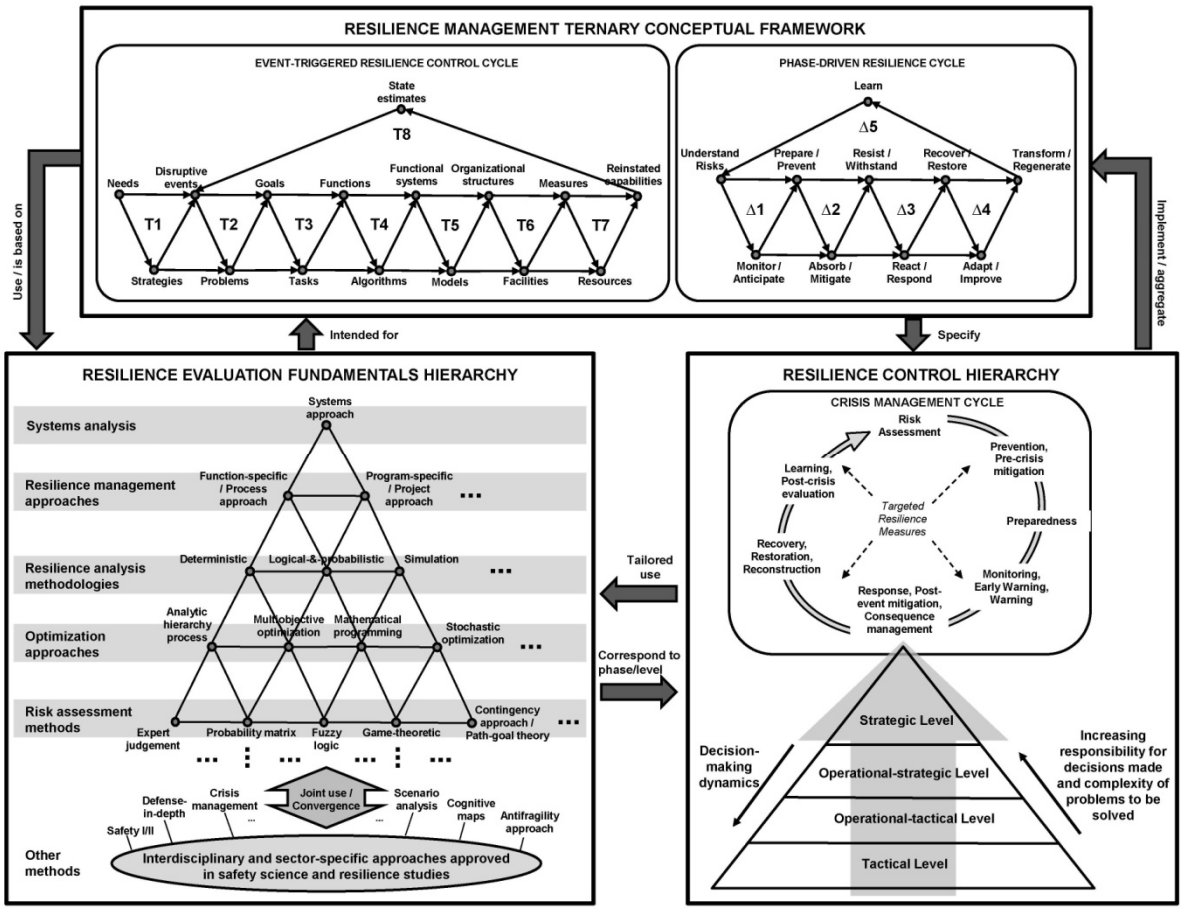
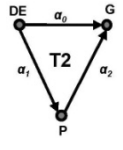


Fig. 3. Resilience cycle ternary conceptual framework for managing disruptive events in critical infrastructure systems

The second triad (*T2*) forms on the basis of the set *DE* a set of goals *G* associated with the elimination and mitigation of initiating events, and the set of problems *P* that must be solved in order to achieve the set of goals *G*. Basically, the process of generating the first two triads is poorly formalizable and is implemented on the basis of empirical data and expert knowledge, which are often enclosed in expert systems. The complexity of synthesizing the set of goals *G*, reflecting the set *DE*, lies in the fact that the global goal of the control system is hierarchical, dynamic, and the priorities of individual subgoals can change in an unforeseen way when managing the progression and propagation of initiating events, which also largely depends on the nature of the during and post event consequences at each phase of the system resilience cycle:

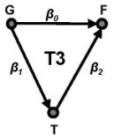
$$\alpha_0 : DE \to G,$$
$$\alpha_1 : DE \to P,$$
$$\alpha_2 : P \to G.$$



The third triad (*T3*) move up the set of goals *G* into a set of functions *F* that must be performed in order to achieve the assigned management goals for eliminating and mitigating the consequences of disruptive events. The specification of the set of goals *G* is carried out through the generation of a set of tasks *T* that reflect subgoals in qualitative and/or quantitative terms, as well as in spatio-temporal terms. The set of functions *F* that must be performed to eliminate and mitigate initiating events comprises the functions of problem monitoring, operational planning, prediction, warning, handling, decision-making, treatment, adjustment, state diagnostics and

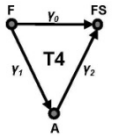
analysis of critical infrastructure facilities, as well as scenario analysis of the progression and propagation of disruptive events, effectiveness assessment of the implemented preventive and reactive measures (control over the execution of adopted managerial decisions), estimation of costs, resource needs, etc.:

$$\beta_0 : G \to F,$$
$$\beta_1 : G \to T,$$
$$\beta_2 : T \to F.$$



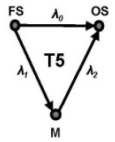
The fourth triad (*T4*) represents the need to determine an adequate set of functional systems *FS* (forces and means of ensuring the system resilience) for the implementation and launching of a set of functions *F* when a disruptive event occurs. In this case, each functional system must have a certain structure that reflects the control algorithm it implements (a set of actions, competencies, etc.). Thereby, the problem of synthesizing a set of control algorithms/programs *A* and choosing such an algorithm that will best allow the resilience situational management system to perform the appropriate function in terms of the selected efficiency criteria for each phase of the resilient system functioning cycle arises. In this case, the functions *F* can be performed both in automatic and automated modes:

$$\gamma_0 : F \to FS,$$
$$\gamma_1 : F \to A,$$
$$\gamma_2 : A \to FS.$$



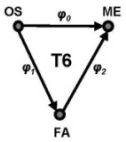
The fifth triad (*T5*) maps the set of functional systems *FS* onto the set of organizational structures for resilience situational management *OS* (compositions of elements of the set *FS*) through the set of models *M* of these compositions. Each model (specification) of the functional system configuration represents specific elements of its composition: agents/entities of resilience management (individual actors or even entire organizations), resources, means, technologies, costs, needs, restrictions, etc. The problem of choosing a configuration model for given conditions is formalized on the basis of configuration optimization according to the selected efficiency criteria:

$$\lambda_0 : FS \to OS,$$
$$\lambda_1 : FS \to M,$$
$$\lambda_2 : M \to OS.$$



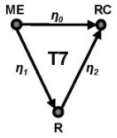
The sixth triad (*T6*) maps the set of organizational structures *OS* configurations of functional systems (a set of interconnected management agents/authorities united by a common goal/task) onto a set of preventive and reactive measures *ME* that must be implemented using a set of available facilities and assets *FA*. When solving the problem of selecting forces and means, it is necessary that it be consistent and compatible not only with the capabilities of the functional system *FS* and the competencies of the organizational structures *OS* (agents of management) using it, but also with the nature of the initiating event itself, as well as the features of the measures being implemented to counteract its further progression and destructive impact on the system:

$$\varphi_0 : OS \to ME,$$
$$\varphi_1 : OS \to FA,$$
$$\varphi_2 : FA \to ME.$$



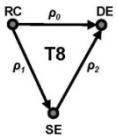
The seventh triad (*T7*) forms a set of new states of the disruptive event propagation process (reinstated capabilities of the system) *RC* based on a set of implemented preventive and reactive measures *ME*. In this case, a shift to the next event and new operating scenario (regeneration and adaptation of the system) occurs. These new states turn out as a result of targeted control actions on the initiating event progression process by using a set of available resources *R* to manage the critical situation. In this case, the set of resources *R* is selected both based on the situational management requirements by "just in time" principle taking into account spatio-temporal and other constraints in order to move the system from a critical state to a stable one, and based on the requirements for reducing the risk of a new critical event initiation. This process is a direct control of disruptive event, which consists in the targeted transition of a critical situation or a threatening source of its initiation from one (critical) state to another (stable):

$$\eta_0 : ME \to RC ,$$
$$\eta_1 : ME \to R ,$$
$$\eta_2 : R \to RC .$$



The eighth triad (*T8*) maps the set of new situations *RC* onto the set of previous disruptive events *DE* through the set of new state estimates *SE*, characterizing these situations for each phase of the resilience cycle. The set of state estimates *SE* allows judging the effectiveness of the preventive organizational and administrative measures taken to eliminate the threats of progressing new disruptive events in the system. The effectiveness estimation is carried out according to a scalar or vector criterion, characterizing the proximity of a disruptive event to a situation with the required (desired) level of system resilience:

$$\rho_0 : RC \to DE ,$$
$$\rho_1 : RC \to SE ,$$
$$\rho_2 : SE \to DE .$$



The integration of the generated triads into a unified system conceptual model is shown in the top of Fig. 3. Elements of the lower-level sets can be also connected to each other. In this case, new triads are formed, which are the objects for further systemic research and analysis.

Thus, the management processes formalization of the critical infrastructures resilience under sudden failures and adverse initiating events in the form of a triadic conceptual model provides the possibility of integrating into a holistic system the main preventive activities of management agents and entities implemented at different phases of the resilience cycle and associated with these processes. At the same time, the proposed model provides a basis for analyzing and assessing the effectiveness of the selected program of anti-crisis measures to achieve the global goal of situational management of the system resilience: minimizing the risks of critical situations and mitigating their consequences to maintain the resilient functioning of the system.

In fine, let's discuss several challenges and limitations of triadic conceptual models intended for system resilience cycle analysis and management support. First of all, when building such type of models, we meet complexity in modeling and accounting interdependencies. Critical entities and infrastructures are deeply interconnected (e.g., power grid failure disrupts water treatment and communications). Accurately modeling these complex dynamic feedback loops within and between the all resilience cycle phases is extraordinarily difficult. A change in one part (triad) of the model can have unforeseen consequences elsewhere when making decisions under situational control. In addition, efficient use of such models is heavily dependent on historical and on-line data, as well as its quality. For instance, adequate modeling of the anticipation phase requires threat intelligence and predictive data, while absorption phase requires real-time operational data, and adaptation phase requires historical performance and failure analysis data. Integrating, representing and accounting these disparate data from various sources, often in different formats, within a triadic conceptual model and ensuring their quality and timeliness is a massive technical and logistical undertaking.

The absorption phase requires rapid analysis of incoming data during a high-stress, time-critical event. Developing simulation models and automated decision-support systems on the basis of triadic conceptual frameworks that can quickly synthesize information and provide actionable recommendations to operators is extremely challenging. Meanwhile, testing the resilience cycle through simulations (e.g., digital twins) requires simulating not just the physical infrastructure, but also human operators, organizational procedures, and external threats. Creating these high-fidelity multi-domain simulations is resource-intensive, but the resources are finite both computational, and financial. At once, a core challenge is optimizing the investment in resilience maintaining facilities across the all resilience cycle phases. Quantifying the return on investment for proactive resilience measures is notoriously difficult, because their value is only realized if a disruptive event occurs. The anticipation phase relies on predicting low-probability, high-impact events ("black swans" or "gray rhinos"). The inherent uncertainty in these predictions can lead to either under-preparation or costly over-preparation for scenarios that never materialize. Thus, investments in anticipation and adaptation (e.g., upgrading critical entities/infrastructure for a future earthquake) have high upfront costs with long-term, uncertain benefits. This creates a misalignment with quarterly earnings reports or political terms, making it hard to secure sustained funding and commitment.

Safety systems oriented to critical infrastructure protection are rarely designed from scratch. Implementing a triadic conceptual model often means retrofitting it onto legacy safety systems that were designed

for managing reliability, not resilience. These legacy safety systems may lack the sensors for monitoring (hindering absorption phase) or the modularity for easy upgrades (hindering adaptation phase). Unlike reliability or risk, which has more established and well-defined metrics, resilience is a multi-dimensional property. Thereat, another problem consists in quantitatively measuring the ability of a system to adapt or its capacity to anticipate, if it is really possible. Developing meaningful, universally accepted key performance indicators for each phase of the resilience cycle and fully accounting it within a triadic conceptual model is a major hurdle.

Unlike more mature fields (e.g., environmental safety, cybersecurity, etc.), there are no universally accepted standards for formally establishing and implementing a critical infrastructure resilience management cycle. This lack of standardization perfection makes it difficult to compare practices, share lessons learned, and develop best practices across industries. Besides, defining clear accountability and responsibility for each phase of resilience management cycle within a complex, interconnected system like critical infrastructure is legally and organizationally difficult. The need to take into account the influence of a human factor within the all phases and levels of resilience management cycle adds specificity to the considered problem agenda. Human factor in decision-making is subject to biases that directly undermine the used triadic, conceptual, simulation and other classes of resilience management cycle models. Therefore, all these factors mentioned above should be implemented within the state-of-the-art conceptual models and frameworks which form the methodological basis for resilience cycle management support of complex dynamic systems such as critical infrastructures and critical entities.

Conclusion

The application of the triadic approach to studying the issues of the situational management of critical infrastructures resilience allows a systematic approach to the problems of modeling, analysis and automation of this cyclic iterative process, namely, to generate the sequence of triads related to each other and aimed at achieving the ultimate goal – designing an efficient decision support system to maintain the resilient functioning of critical infrastructures under the impact of multiple threats and the emergence of unforeseen events. The triadic conceptual model of the resilience situational management cycle of critical infrastructures built using the apparatus of ternary relations quite fully describes the hierarchical system of objects and methods for ensuring resilience at various phases of the cycle. Thus, the application of the triadic approach made it possible not only to systematically represent knowledge about the subject of inquiry: the resilience of critical infrastructures, but also expanding and supplementing the constructed triads to identify new properties and patterns inherent in this subject under examination. The following main results were drawn in the course of the study:

1. The issues of analysis, modeling and automation of the resilience cycle of the critical infrastructure systems based on the combined use of conceptual modeling technology, a process approach and a formal apparatus of ternary relations have been studied.

2. A diversification (expansion) of the application scope of the process and triadic approaches to the problems of formalization, analysis and modeling of the resilience situational management cycle of critical infrastructures has been proposed.

3. For the problem-solving of a comprehensive analysis of the critical infrastructure resilience cycle and the synthesis of effective models of technical-organizational systems for situational management of its resilient functioning, a triadic hierarchical model of the typical U-shaped resilience cycle of critical infrastructures based on a conceptual description of objects and ternary relations between them in the form of a set of triads and modeling the process of ensuring the system resilience at different phases of situational management has been developed. The proposed model has a multi-level structure and is distinguished by the completeness of the formal description of all phases of the system resilience cycle and the related processes of situational management, which provides the possibility of automation and variability of the choice of appropriate (relevant) measures and means for the effective maintenance of the stable functioning of the system under the influence of adverse or undesired factors.

The drawn results can find perspective application in the field of engineering automation of the ontological and simulation models of critical infrastructures resilience intended for subsequent use in the development and path planning process of intelligent information technologies for the situational management support of critical facilities and systems.

References

1. Putilov V.A., Masloboyev A.V., Bystrov V.V. Modeling of regional security management processes. *Trudy Kol'skogo nauchnogo tsentra RAN = Proceedings of the Kola Scientific Center of the Russian Academy of Sciences*. 2017;8(3-8):9–27. (In Russ.)

2. Masloboyev A.V., Putilov V.A. *Informatsionnoye izmereniye regional'noy bezopasnosti v Arktike = Informational dimension of regional security in the Arctic*. Apatity: KNTS RAN, 2016:222. (In Russ.)
3. Masloboev A.V. An index-based method for integral estimation of regional critical infrastructure resilience using fuzzy calculations. Part 2. Resilience capacity models and backbone capabilities. *Reliability and quality of complex systems*. 2024;(3):130–156.
4. Severtsev N.A., Yurkov N.K. *Bezopasnost' dinamicheskikh sistem na etapakh zhiznennogo tsikla = Safety of dynamic systems at the stages of the life cycle*. Penza: Izd-vo PGU, 2023:568. (In Russ.)
5. Yamalov I.U. *Modelirovaniye protsessov upravleniya i prinyatiya resheniy v usloviyakh chrezvychaynykh situatsiy = Modeling of management processes and decision-making in emergency situations*. Moscow: BINOM. Laboratoriya znaniy, 2007:288. (In Russ.)
6. Vasil′yev V.I., Il′yasov B.G., Ivanova T.A. Methodology of ensuring security in complex organizational systems based on a triadic approach. *Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskiye nauki = Proceedings of the Southern Federal University. Technical sciences*. 2014;(2):7–16. (In Russ.)
7. Shul′ts V.L., Kul′ba V.V., Shelkov A.B., Chernov I.V. *Stsenarnyy analiz v upravlenii geopoliticheskim informatsionnym protivoborstvom = Scenario analysis in the management of the geopolitical information confrontation*. Moscow: Nauka, 2015:542. (In Russ.)
8. Holling C.S. Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*. 1973;(4):1–23.
9. De Marco A., Berardi D., Galuppi M., Lombardi M. Quantitative resilience assessment on critical infrastructures – A systematic literature review of the last decade (2014–2024). *Journal of Safety Science and Resilience*. 2025;6(3):100201.
10. Pursiainen C. *The Crisis Management Cycle*. UK, London: Routledge, 2017:194.
11. Tsygichko V.N., Chereshkin D.S., Smolyan G.L. *Bezopasnost' kriticheskikh infrastruktur = Safety of critical infrastructures*. Moscow: URSS, 2019:200. (In Russ.)
12. Klimek P., Varga J., Jovanovic A.S., Székely Z. Quantitative resilience assessment in emergency response reveals how organizations trade efficiency for redundancy. *Safety Science*. 2019;113:404–414.
13. Nan C., Sansavini G., Kröger W., Heinimann H.R. A Quantitative Method for Assessing the Resilience of Infrastructure Systems. *Proceedings of the Probabilistic Safety Assessment and Management Conference (PSAM12)*. Honolulu, HI, USA, 2014;10:359–370.
14. Rehak D., Senovsky P., Slivkova S. Resilience of critical infrastructure elements and its main factors. *Systems*. 2018;6(2):21.
15. Jovanović A. et al. Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards. *Environment Systems and Decisions*. 2020;40(2):252–286.
16. Braun M., Hachmann C., Haack J. Blackouts, restoration, and islanding: A system resilience perspective. *IEEE Power Energy Magazine*. 2020;18(4):54–63.
17. Häring I. et al. Towards a generic resilience management, quantification and development process: General definitions, requirements, methods, techniques and measures, and case studies. *NATO Science for Peace and Security Series C: Environmental Security*. Springer Netherlands, 2017:21–80.
18. Fischer K., Hiermaier S., Riedel W., Häring I. Morphology dependent assessment of resilience for urban areas. *Sustainability.* 2018;10(6):1800.
19. Taleb-Berrouane M., Khan F. Dynamic resilience modelling of process systems. *Chemical Engineering Transactions*. 2019;77:313–318.
20. Mishra D.K., Ghadi M.J., Azizivahed A. et al. A review on resilience studies in active distribution systems. *Renewable and Sustainable Energy Reviews*. 2021;135:110201.
21. Oboudi M.H., Mohammadi M., Rastegar M. Resilience-oriented intentional islanding of reconfigurable distribution power systems. *Modern Power Systems and Clean Energy*. 2019;7(4):741–752.
22. Mottahedi A., Sereshki F., Ataei M. et al. The Resilience of Critical Infrastructure Systems: A Systematic Literature Review. *Energies*. 2021;14(6):1571.
23. Hossain N.U.I., Jaradat R., Hosseini S. et al. A framework for modeling and assessing system resilience using a Bayesian network: a case study of an interdependent electrical infrastructure system. *International Journal of Critical Infrastructure Protection*. 2019;25:62–83.
24. Panteli M., Mancarella P. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. *IEEE Systems Journal*. 2015;11(3):1733–1742.
25. Rød B., Pursiainen C., Reitan N.K. et al. Evaluation of resilience assessment methodologies. *Safety and Reliability – Theory and Applications: proceedings of the 27th European Safety and Reliability Conference (ESREL, June 18–22, 2017, Portoroz, Slovenia)*. London, UK: Taylor & Francis Group, 2018:1039–1052.
26. Yang Zh. et al. Indicator-based resilience assessment for critical infrastructures – A review. *Safety Science*. 2023;160:106049.
27. Theocharidou M. et al. Final lexicon of definitions related to critical infrastructure resilience. *IMPROVER Project Report: Deliverable 1.3*. 2016:38.

28. Mentges A., Halekotte L., Schneider M. et al. A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. *Disaster Risk Reduction*. 2023;96:103893.
29. Report of criteria for evaluating resilience. *IMPROVER Project Report: Deliverable 2.2*. 2016:37.
30. Rehak D., Hromada M. Failures in a critical infrastructure system. *System of system failures*. IntechOpen, 2018:75–93.
31. *Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies*. Paris: OECD Publishing, 2019:118.
32. Urlainis A., Ornai D., Levy R. et al. Loss and damage assessment in critical infrastructures due to extreme events. *Safety Science*. 2022;147:105587.
33. Alderson D.L., Darken R.P., Eisenberg D.A. et al. Surprise is inevitable: how do we train and prepare to make our critical infrastructure more resilient? *Disaster Risk Reduction*. 2022;72:102800.
34. Park J., Seager T.P., Rao P.S.C. et al. Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis*. 2013;33(3):356–367.
35. Kalyanov G.N. *Teoriya biznes-protsessov = Theory of business processes*. Moscow: Goryachaya liniya. Telekom, 2023:296. (In Russ.)
36. Yuditskiy S.A., Vladislavlev P.N., Toch D.S. A triadic approach to modeling network-centric management systems. *Upravleniye bol'shimi sistemami = Management of large systems*. 2010;(28):24–39. (In Russ.)

Список литературы

1. Путилов В. А., Маслобоев А. В., Быстров В. В. Моделирование процессов управления региональной безопасностью // Труды Кольского научного центра РАН. 2017. Т. 8, № 3-8. С. 9–27.
2. Маслобоев А. В., Путилов В. А. Информационное измерение региональной безопасности в Арктике. Апатиты : КНЦ РАН, 2016. 222 с.
3. Masloboev A. V. An index-based method for integral estimation of regional critical infrastructure resilience using fuzzy calculations. Part 2. Resilience capacity models and backbone capabilities // Reliability and quality of complex systems. 2024. № 3. P. 130–156.
4. Северцев Н. А., Юрков Н. К. Безопасность динамических систем на этапах жизненного цикла. Пенза : Изд-во ПГУ, 2023. 568 с.
5. Ямалов И. У. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций. М. : БИНОМ. Лаборатория знаний, 2007. 288 с.
6. Васильев В. И., Ильясов Б. Г., Иванова Т. А. Методология обеспечения безопасности в сложных организационных системах на основе триадного подхода // Известия Южного федерального университета. Технические науки. 2014. № 2. С. 7–16.
7. Шульц В. Л., Кульба В. В., Шелков А. Б., Чернов И. В. Сценарный анализ в управлении геополитическим информационным противоборством. М. : Наука, 2015. 542 с.
8. Holling C. S. Resilience and stability of ecological systems // Annual Review of Ecology and Systematics. 1973. № 4. P. 1–23.
9. De Marco A., Berardi D., Galuppi M., Lombardi M. Quantitative resilience assessment on critical infrastructures – A systematic literature review of the last decade (2014–2024) // Journal of Safety Science and Resilience. 2025. Vol. 6, iss. 3. P. 100201.
10. Pursiainen C. The Crisis Management Cycle. UK, London : Routledge, 2017. 194 p.
11. Цыгичко В. Н., Черешкин Д. С., Смолян Г. Л. Безопасность критических инфраструктур. М. : УРСС, 2019. 200 с.
12. Klimek P., Varga J., Jovanovic A. S., Székely Z. Quantitative resilience assessment in emergency response reveals how organizations trade efficiency for redundancy // Safety Science. 2019. Vol. 113. P. 404–414.
13. Nan C., Sansavini G., Kröger W., Heinimann H. R. A Quantitative Method for Assessing the Resilience of Infrastructure Systems // Proceedings of the Probabilistic Safety Assessment and Management Conference (PSAM12). Honolulu, HI, USA, 2014. Vol. 10. P. 359–370.
14. Rehak D., Senovsky P., Slivkova S. Resilience of critical infrastructure elements and its main factors // Systems. 2018. Vol. 6, № 2. P. 21.
15. Jovanović A. [et al.]. Assessing resilience of healthcare infrastructure exposed to COVID-19: emerging risks, resilience indicators, interdependencies and international standards // Environment Systems and Decisions. 2020. Vol. 40, № 2. P. 252–286.
16. Braun M., Hachmann C., Haack J. Blackouts, restoration, and islanding: A system resilience perspective // IEEE Power Energy Magazine. 2020. Vol. 18, № 4. P. 54–63.
17. Häring I. [et al.]. Towards a generic resilience management, quantification and development process: General definitions, requirements, methods, techniques and measures, and case studies // NATO Science for Peace and Security Series C: Environmental Security. Springer Netherlands, 2017. P. 21–80.
18. Fischer K., Hiermaier S., Riedel W., Häring I. Morphology dependent assessment of resilience for urban areas // Sustainability. 2018. Vol. 10, № 6. P. 1800.
19. Taleb-Berrouane M., Khan F. Dynamic resilience modelling of process systems // Chemical Engineering Transactions. 2019. Vol. 77. P. 313–318.

20. Mishra D. K., Ghadi M. J., Azizivahed A. [et al.]. A review on resilience studies in active distribution systems // Renewable and Sustainable Energy Reviews. 2021. Vol. 135. P. 110201.
21. Oboudi M. H., Mohammadi M., Rastegar M. Resilience-oriented intentional islanding of reconfigurable distribution power systems // Modern Power Systems and Clean Energy. 2019. Vol. 7, iss. 4. P. 741–752.
22. 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.
23. Hossain N. U. I., Jaradat R., Hosseini S. [et al.]. A framework for modeling and assessing system resilience using a Bayesian network: a case study of an interdependent electrical infrastructure system // International Journal of Critical Infrastructure Protection. 2019. Vol. 25. P. 62–83.
24. Panteli M., Mancarella P. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events // IEEE Systems Journal. 2015. Vol. 11, № 3. P. 1733–1742.
25. Rød B., Pursiainen C., Reitan N. K. [et al.]. Evaluation of resilience assessment methodologies // Safety and Reliability – Theory and Applications : proceedings of the 27th European Safety and Reliability Conference (ESREL, June 18–22, 2017, Portoroz, Slovenia) / ed. by M. Cepin, R. Bris. London, UK : Taylor & Francis Group, 2018. P. 1039–1052.
26. Yang Zh. [et al.]. Indicator-based resilience assessment for critical infrastructures – A review // Safety Science. 2023. Vol. 160. P. 106049.
27. Theocharidou M. [et al.]. Final lexicon of definitions related to critical infrastructure resilience // IMPROVER Project Report: Deliverable 1.3. 2016. 38 p.
28. Mentges A., Halekotte L., Schneider M. [et al.]. A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures // Disaster Risk Reduction. 2023. Vol. 96. P. 103893.
29. Report of criteria for evaluating resilience // IMPROVER Project Report: Deliverable 2.2. 2016. 37 p.
30. Rehak D., Hromada M. Failures in a critical infrastructure system // System of system failures / ed. by T. Nakamura. IntechOpen, 2018. P. 75–93.
31. Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies. Paris : OECD Publishing, 2019. 118 p.
32. Urlainis A., Ornai D., Levy R. [et al.]. Loss and damage assessment in critical infrastructures due to extreme events // Safety Science. 2022. Vol. 147. P. 105587.
33. Alderson D. L., Darken R. P., Eisenberg D. A. [et al.]. Surprise is inevitable: how do we train and prepare to make our critical infrastructure more resilient? // Disaster Risk Reduction. 2022. Vol. 72. P.102800.
34. Park J., Seager T. P., Rao P. S. C. [et al.]. Integrating risk and resilience approaches to catastrophe management in engineering systems // Risk Analysis. 2013. Vol. 33, iss. 3. P. 356–367.
35. Калянов Г. Н. Теория бизнес-процессов. М. : Горячая линия. Телеком, 2023. 296 с.
36. Юдицкий С. А., Владиславлев П. Н., Точ Д. С. Триадный подход к моделированию систем сетецентрического управления // Управление большими системами. 2010. № 28. С. 24–39.

Информация об авторах / Information about the authors

Андрей Владимирович Маслобоев
доктор технических наук, доцент,
ведущий научный сотрудник,
Институт информатики и математического
моделирования имени В. А. Путилова
Федерального исследовательского центра
«Кольский научный центр
Российской академии наук»
(Россия, г. Апатиты, ул. Ферсмана, 14)
E-mail: a.masloboev@ksc.ru

Andrey V. Masloboev
Doctor of technical sciences,
associate professor,
leading researcher,
Putilov Institute for Informatics
and Mathematical Modeling
of the Federal Research Center
"Kola Science Center
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 06.06.2025
Поступила после рецензирования/Revised 30.06.2025
Принята к публикации/Accepted 07.07.2025