УДК 004.9, 681.5, 338.24 DOI 10.21685/2307-4205-2020-4-13

A. V. Masloboev

TOWARDS A THEORY OF REGIONAL CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

А. В. Маслобоев

НАВСТРЕЧУ ТЕОРИИ БЕЗОПАСНОСТИ И ЖИЗНЕСПОСОБНОСТИ РЕГИОНАЛЬНЫХ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Abstract. *Background*. The work is aimed at modern theory of complex system security development in the context of an integrated methodology design for critical infrastructure security and resilience (CISR) management and CISR research systematization of regional socio-economic systems. The urgency of the study is conditioned by rising requirements for control operators and means for the purpose of CISR support at the regional level and the need to improve the regional security management system engineered on the basis of situational center network. The objective of research is to develop the theoretical and organizational-technical foundations of CISR management of the region as well as to analyze foreign experience in this field. *Materials and methods*. The research is carried out by the example of critical infrastructures of the Murmansk region, which is a part of the Russian Arctic. Three key CISR domains (dimensions) of regional socio-economic systems are considered: technological, organizational and societal resilience. The methodological base of the study includes systems approach, conceptual modeling, and convergence of control theory, reliability theory, risk analysis, safety and stability theory methods. *Results and conclusions*. An overview of the state-of-the-art research in the field of CISR management and an analysis of the existing models and methods applicability to problem-solving in this dynamic object domain are carried out. The novel holistic methodology of CISR analysis and management support is proposed. A conceptual model of CISR control system and a technique for resilience assessment of the regional critical objects and infrastructures have been developed. The application of theoretical developments will in prospect enhance the features of methods and tools used in practice to regional security support within the situational centers of the region, and to specify the information structure and forms of resilience management of the socio-economic systems as well as methods of risk assessment and analysis of the security violation of regional critical infrastructures.

Аннотация. *Актуальность и цели.* Работа направлена на развитие современной теории безопасности сложных систем в контексте разработки комплексной методологии управления безопасностью и жизнеспособностью критических инфраструктур (БЖКИ) и систематизации исследований БЖКИ региональных социально-экономических систем. Актуальность работы обусловливается возрастающими требованиями к органам и средствам обеспечения БЖКИ на региональном уровне и необходимостью совершенствования системы управления региональной безопасностью, построенной на базе сети ситуационных центров. Целью исследований является разработка теоретических и организационно-технических основ управления БЖКИ региона, а также анализ зарубежного опыта в этой сфере. *Материалы и методы*. Исследования проводятся на примере критических инфраструктур Мурманской области, региона входящего в состав Арктической зоны России. Рассмотрены три ключевые области (измерения) БЖКИ региональных социально-экономических систем: технологическая, организационная и социетальная. Методологическая база исследования включает системный подход, концептуальное моделирование, конвергенцию методов теории управления, теории надежности, анализа риска, теории безопасности и устойчивости. *Результаты и выводы*. Проведены обзор современного состояния исследований в сфере управления БЖКИ и анализ применимости существующих моделей и методов для решения задач в этой динамичной проблемной области. Предложена методология управления БЖКИ. Разработаны концептуальная модель системы управления БЖКИ и методика оценки жизнеспособности критически важных объектов и инфраструктур региона. Применение теоретических разработок в перспективе позволит расширить возможности используемых на практике методов и средств обеспечения региональной безопасности в ситуационных центрах региона, конкретизировать информационную структуру и формы управления жизнеспособностью социально-экономических систем, а также способы оценки и анализа рисков нарушения безопасности региональных критических инфраструктур.

© Masloboev A. V., 2020

Keywords: resilience, security, risk, critical infrastructure, regional socio-economic system, management, modeling, methodology.

Ключевые слова: жизнеспособность, безопасность, риск, критическая инфраструктура, региональная социально-экономическая система, управление, моделирование, методология.

Introduction

At present, it is necessary to maintain and organize an effective information support of regional critical infrastructure security and resilience (CISR) management on the basis of threat and vulnerability sources outpacing monitoring and comprehensive analysis of the regional socio-economic systems to reduce different types of uncertainty under decision-making processes in the rapidly changing conditions. A lot of various emergency situations are arising dynamically in the regional critical infrastructures both predictable and unpredictable. This leads to increased requirements for modern security support systems and technologies aimed to improve effectiveness of safety and resilience control of critical objects in the socio-economic sphere. Therefore, methodology development of the regional CISR management is urgent and perspective field of research which is facing a whole range of problems caused by crisis situations in national and world economy, escalation of international relations, conflicts and instability in social and economic sectors, uncontrolled external threats in military and political areas, anthropogenic impacts on the environment and natural challenges, etc.

Efficiency enhancement of CISR management is one of the key directions and significant strategic goals of public policy both at regional and national level in concordance with National Security Strategy of Russian Federation [1]. To purposeful goal achievement and problem-solving a network of distributed situational centers [2] was created and expanded as a relevant tool for digital transformation of governmental management in security and defense areas of socio-economic development. Physically and conceptually this network is regarded as a backbone part of the regional CISR management system.

Decision support systems are the basis of the information environment of distributed situational centers for regional security management. The central problem for this class of systems in the field of regional security and critical infrastructure resilience management is coordination of the control actions preparation and implementation at different decision-making levels in conditions of decentralized control and external environment high dynamics as well as taking into account the influence of human factor.

Effectiveness of the regional critical infrastructure resilience management processes is based on the decision-making information support quality and the results of monitoring, evaluation and comprehensive analysis of a wide range of heterogeneous security indicators that allow assessing current status of critical objects and situation in the region, as well as risks of its sustainable development destabilization. In the context of digital economy it becomes more obvious that these integral indicators used in the decision-making procedures and management information systems provide possibilities to critical infrastructure resilience level measurement and assessment, prediction and implementation of the adequate crisis-proof measures directed to various negative consequences prevention on the basis of modern information technologies and computer modeling.

The most acute CISR problems are revealed at the regional level that leads to higher-level socio-economic system destabilization (national, global, etc.). Therefore, an improvement of the existing organizational management system of regional CISR is considered as a significant and urgent problem having a strategic importance for state policy of each region and country in general. However, it is up-to-date still far from being effectively addressed. At present, this problem is especially relevant for the Arctic regions of Russia.

In our study we go towards the theory of CISR and give an overview of its state-of-the-art background and foundations. Moreover, we discuss conception of critical infrastructure resilience from the position of system approach based on security foundations analysis and propose a complex methodology to regional security and critical infrastructure resilience management and information support. Particularly, our research is carried out by the example of critical infrastructure resilience of the Arctic region, which is influenced by a multitude of heterogeneous internal and external threats and hazards.

Research motivation and Problem statement

The specificity of regional CISR, as a subject of inquiry, is determined by the following features:

– the heterogeneity of emergency situations arising in various critical infrastructures of regional socio-economic system;

– the absence of information completeness characterizing the system (situation) status, its external environment and interaction at the target time;

– the impossibility of full taking into account all the factors (threats) and clearly defining an action plan for all probable scenarios of situation dynamically changes;

– the various nature, latent character, slow rising and delayed result adjournment of the threat and danger impact on system functioning that provides a slack for operational and strategic managerial decision-making, in contrast to the safety management of critical objects under extreme emergency cases;.

– the existence of poorly formalized and difficult-to-automate initial stages of the crisis situation evolution life cycle in the critical infrastructures of regional socio-economic system associated with the emergence of potential threats and hazards;

– the presence of variety aspects influencing on managerial decision-making in the field of critical infrastructure resilience control and regional security support (political, economic, social, organizational, technical, regulatory and legal, etc.);

– the multi-aspectivity, interconnectivity and high uncertainty of processes taking place in the critical infrastructures of regional socio-economic system.

Low efficiency reasons of the regional CISR management in the Arctic region of Russia basically are:

– the absence of unified organizational management system of critical infrastructure resilience in the region, including information infrastructure of regional security control;

– the interaction coordination complexity and, in some cases, impossibility of the organizationally heterogeneous and geographically distributed security control actors at different decision-making levels;

– the decentralized nature of regional socio-economic system security management and critical infrastructure resilience control in the region;

– the diversity and isolated application of methods and tools for automation of regional security and resilience support processes at various management levels;

– the fragmentary nature of interdepartmental information interaction organizational and technical regulations under emergency situations and the absence of a unified regional security passport and critical infrastructure resilience legal standards.

The main key disadvantages of the regional CISR management system in the Arctic region are, firstly, the lack of an integrated information infrastructure for regional security control. Secondly, the non-coordination of decentralized decision-making at different security management levels. And, thirdly, the rigid centralized security and resilience management scheme implementation in the regional critical infrastructures under conditions of distribution and organizational heterogeneity of the control actors participating in the regional security support processes. Centralized security control is ineffective in real conditions and does not provide the desired effects.

Regional specificities that are individual for each region add to the issues. Such specific features of the Arctic region requiring regional security and critical infrastructure resilience management system enhancement and development are geographical location, relatively sparse population, low stability of ecological system due to enhanced climate change effects and slower natural renewal processes, underdevelopment of infrastructure, relative remoteness and distances federal and population centers, skilled personnel shortage, demographic problems, specificity of economic development and territory exploration, multiple objects redundancy of military-industrial complex. The great mixture of all these factors determines the regional critical infrastructure vulnerability in terms of emergence of the various types of natural, anthropogenic and socio-economic crisis situations. The consequences neutralization of such type of situations requires operational and effective managerial decision-making in exceedingly limited time. This necessitates a shift to the network-centric control model [3] of regional CISR management.

The solution of this problem is for the most part hampered by the needs of large volumes of semantically and organizationally heterogeneous information integration, processing and analysis for activities information support of critical infrastructure resilience management entities, as well as interaction coordination between them at all regional security control levels. Therefore, a development of the comprehensive methodology for critical infrastructure resilience management information support as well as an adaptation of the state-of-the-art security theory foundations and risk-analysis models are needed to efficient problem-solving specified above.

Background and Related work

Any society is highly reliant on interconnected infrastructures providing essential services, so-called vital societal functions [4]. The Arctic region environment with its remoteness and climate conditions illustrates the importance of building capacities and capabilities, across several elements, dimensions and domains, to withstand and rapidly recovery from human-induced, technological and natural disasters, or their combinations. That means that critical infrastructure that support vital societal functions in such environment need to be particularly resilient and secured.

The rapidly change in world policy and military situation, national economy and climate conditions introduces new threats and vulnerabilities in regional socio-economic systems, power systems, transportation systems, communication systems, and other infrastructures. Local, regional and national communities and authorities, and most notably infrastructure operators, require a realistic estimate of the security and resilience level of the available infrastructures, which should meet the expectation, needs and tolerances of the end-user, being the society.

Hence, in order to assess CISR in the Arctic region, it is not appropriate to only account for the physical-cyber infrastructure itself. Information and data from several resilience domains need to be merged and integrated, processed and analyzed, and there is a need to develop suitable models and methods for regional CISR management and assessment.

According to the European Council Directive a critical infrastructure can be defined as [5]: ”an asset, system or part thereof Member State 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 in a Member State as a result of the failure to maintain those functions”. Several non-EU countries have adopted similar definitions with some variations [6], so this is the definition used in the current study.

While there thus is some shared understanding what a critical infrastructure is, the definition of resilience is a more contested one. Nevertheless, the United Nations provides a generic definition that is suitable for our purpose, defining resilience as [7]: “The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management”. In [8] we have developed formalized multiple-theoretical models of basic concepts: system resilience, critical infrastructure and resilience control system using conceptual modeling methodology. The proposed inside [8] conceptual model of regional critical infrastructure functioning takes into account threat dynamics and provides its modeling, despite the fact that almost possible threats are assigned in advance. For each type of threat a complex of protective measures is offered.

With the above definitions in mind, and considering the available data in the Arctic region of Russia, the objective of our research is to further develop and tailor existing methods and information technologies to analysis, evaluate and improve regional CISR in Russian Arctic by the example of Murmansk region. Beside the growing scientific literature on CISR, to our knowledge there exists no serious and holistic analysis of the subject and related challenges applied to the Arctic regional context. Our study will fill in that research and practical knowledge gap. Regional CISR management guidelines, based on interdisciplinary approach and state-of-the-art research, are needed to maintain risk-sustainable development of the Arctic region.

In order to do that and to narrow the scope to realistic dimensions, there has to be a clear idea on which domains of security and resilience need to be included in closer scrutiny. In the Arctic regional CISR context, we believe that three domains are especially important: technological resilience, organizational resilience and societal resilience.

The Arctic region is one of its type in the Russia, due to many of its specific characteristics compared to other regions and northern territories. Yet, in terms of science and societies at large, it is not sui generis from the point of view of social, natural, engineering or computer sciences, et. al., as is no other region. In terms of how to manage regional CISR, the best way to approach the Arctic region challenges is to look at the more generic scientific context and available knowledge first, then apply that knowledge to the Arctic region. In so doing, we may find some clues and perhaps even solutions that have already been tested elsewhere. Yet, while data acquisition and analysis on generic phenomena relating it to the area-related idiosyncrasies from the Arctic region at the same time, one can contribute to the more generic picture of the state-of-the-art with some new insights.

In our case, it is the question about the strive towards a safe and resilient, i.e. risk-sustainable, socio-economic development of the region through enhancing its CISR. The concept of resilience emerged into the scientific literature within the ecosystem theory in the 1970s [9-10]. It received a minor attention during the subsequent two or three decades. From early 2000s onwards, however, the concept was popularized in many other fields, not least in disaster management and other fields related to safety and security. A socio-economic system risk-sustainability ("resilient society") became the new catchword, an umbrella concept indeed, comparable to, and partially overlapping with, the earlier emphasis on sustainable development for a comprehensive review of security and resilience literature [11].

While the above-mentioned UNDRR definition of resilience works rather well as a baseline, the concept is much more multi-faceted, competed and in many ways rather vague. Indeed, we could call it as resilience discourse, the exact boundaries of this discourse still being rather obscure and including several sub-discourses and application areas. In scientific literature, e.g. [12], we may differentiate between several dimensions, so-called domains of resilience: community, social, societal, ecological, environmental, economic, functional, organisational, personal, psychological, cyber-physical, technological, etc. As known, various attempts were made to manage regional CISR centrally, but this did not provide the desired effect, since there are many diverse resilience domains listed above. All of these key dimensions had to be tied together. In our opinion, an application of network-centric control approach is a convenient way to address this complex problem, because it most adequately reflects to real nature of the socio-economic system resilience management and takes into account the decentralized character of regional security support processes, both in terms of functional structure and control actor composition.

Due to the penetration of the resilience concept into multiple disciplines, its theoretical basis remains rather versatile, and even contradictory. For social scientists, it is mostly about adapting to the changes in the society. This debate is characterized by those who, on the one hand, see the resilience discourse as part of a neoliberal tendency, as transferring responsibilities of the public authorities to the civil society and citizens, in the context of further privatization of welfare and other services. On the other hand, those who see this development by contrary as emancipation of the citizen, adding to their self-adaptive capacities and survival strategies. For spatial and urban planners [13], resilience is usually about "resilient design", focusing on preventive planning against disaster consequences, as well as community ownership and empowerment issues for the same goal. In the field of engineering, over the last 10–15 years, "resilience engineering" has been proposed to deal with safety and security in socio-technical systems. The intention, as stated in [14], is to "enable systems and organisation's to continue to operate in the face of unforeseen large scale demands, as well as to improve their everyday functioning". In practice, this means to find ways to measure the protective, adaptive and restoring capacities of systems, in order to enhance them [15, 16]. The main problem is how to put these different theoretical and methodological subjects and concepts together. This problem-solving consists in the framework of resilience dimensions (security domains) integration that is helpful in the way of focusing on different but related actors, such as public authorities, civil society, infrastructure owners and operators for the efficient network-centric management of regional security and resilience.

Our analytical survey of the domestic scientific literature and experience showed that systemic basic research on the regional CISR problems in Russia have not been previously carried out. This also applies to the Arctic region and socio-economic and environmental safety management of its critical objects. Domestic publications for the most part touch upon the issue of individual dimensions of the critical infrastructure security and socio-economic system resilience with varying level of problem domain detailing based on system approach principles, control theory, reliability theory, risk analysis and safety methodologies. Thus, [17–19] analyze and discuss a wide range of problems and issues of the theory and practice of critical infrastructure security violation risk management as well as certain resilience aspects of socio-economic system critical objects in conditions of the uncertainty and incompleteness of source information for decision-making. Appropriate models and methods are proposed for various relevant applications in the field of comprehensive security of critical infrastructures. The recommendations for safeguarding of the critical infrastructure objects from the natural and anthropogenic emergency situations, as well as for taking into account the impact of human factor within the risk assessment and analysis of critical infrastructure functioning by the example of system research and development of the regional security and social resilience management support, are given. The distinctive feature of domestic studies as compared with foreign research is the point of view on resilience and security of the socio-economic systems and processes studied.

Thus, foreign researchers are focused on the personal and civil society point of view in analysis of the critical infrastructure security problems, while Russian scientists often abide by state and national interests in these issues.

A wide variety of methods is observed in the theoretical base of basic research on the CISR control problems. Generally, the methodology for CISR research and analysis has overlaps in methods used within the other scientific disciplines: reliability theory, risk management, security control, sustainable development, crisis management, viability theory, stability theory, system safety, acceptable risk conception, etc. These fields of research have made an essential effect on the fundamental formation and development of the theory of critical infrastructure resilience. Thus, the position of critical infrastructure resilience theory among the specified scientific concepts can be represented as a symbiosis result of the corresponding field of knowledge. On the basis of mentioned scientific paradigms and control theory foundations we have designed a generic conceptual model of the regional CISR management system, including control object, regulator, external environment, input and output resources, data flows, system state evaluator, etc. This conceptual model is schematically shown on Figure 1. Figure 1 also illustrates the main steps of security and resilience control algorithm and accounting of various factor impacts occurred in management process.

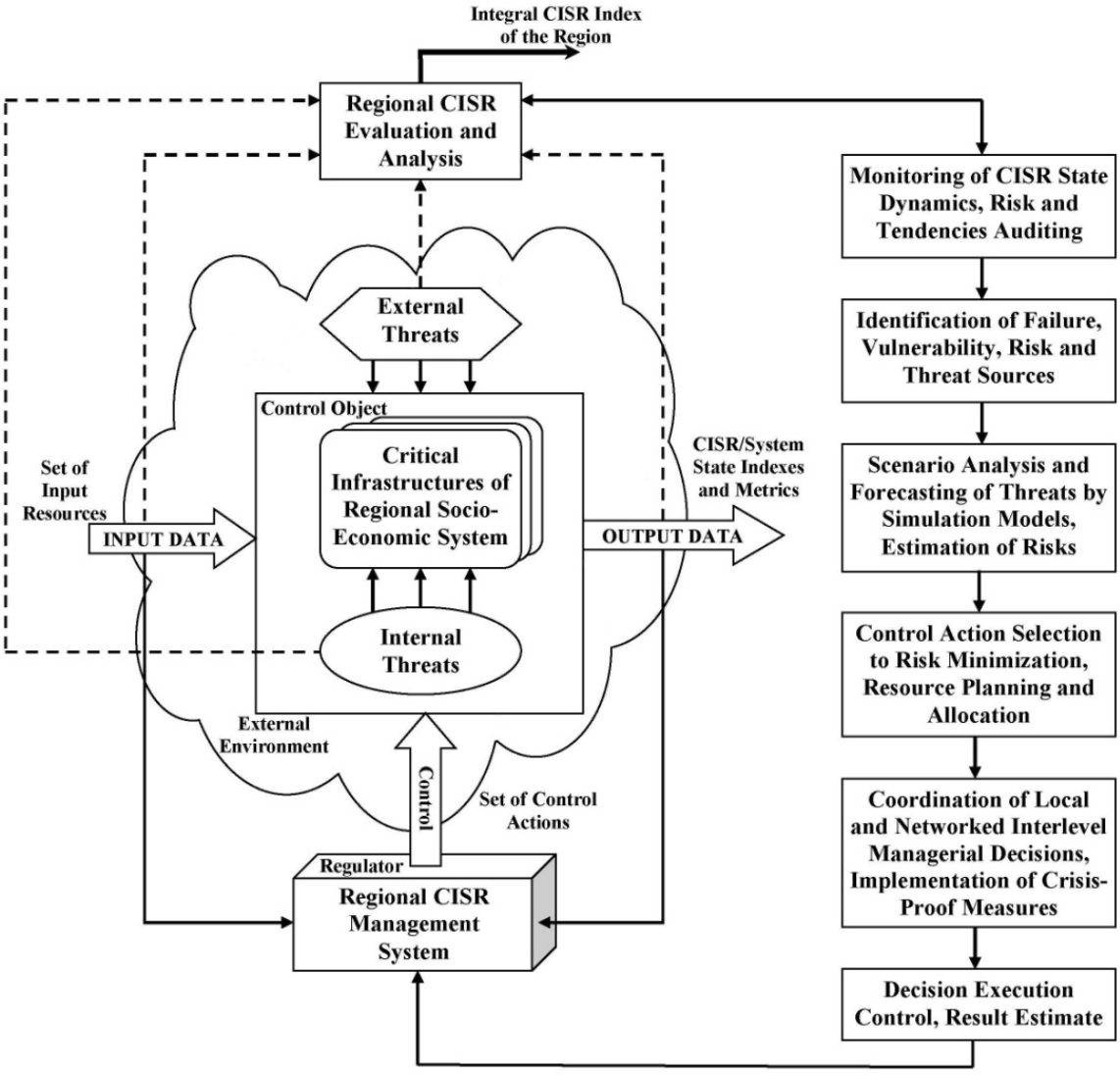

Fig. 1. Conceptual model of regional CISR control system

In the general case, a choice of particular method for critical infrastructure resilience and security analysis and control depends on the measuring of system resilience domain on which the each individual researcher focuses his or her attention (e.g. community resilience, societal resilience, human resilience, economic resilience, environmental resilience, technological resilience, organizational resilience, cyber re-

silience, etc.). Within the bounds of the given measurements of critical infrastructure resilience separate systems, processes and phenomena are studied that are most significant for specific problem-solving under research. At the same time, in most cases coherence and associations of the studied type of system resilience with other components of critical infrastructures are omitted from the consideration and analysis.

CISR conceptual domains

While the definitions differ and overlap, technological, organizational and societal domains are most notably connected to our research subject and objectives. To keep these domains analytically separate is justifiable as they are crucial in defining which actor is responsible for a certain type of resilience action. Technological and organizational resilience domains are the most important ones from the perspective of regional critical infrastructure operators. The societal domain cannot however be ignored as critical infrastructure operators are obliged by government regulation, and in the event of a major disturbance, they are in direct relation with emergency services and the clients. Finally, the critical infrastructure is supposed to secure vital societal functions, first and foremost, to the regional socio-economic risk-sustainable development and society at large. Therefore, technological, organizational and societal resilience domains are tightly interconnected and provide joint risks and challenges for critical infrastructures of regional socio-economic system declared above and taking into consideration under our discourse.

Let us take a closer look at these three interrelated resilience domains that cover most of the issues related to CISR of the Arctic region, as well as their overlapping area of risks and challenges.

Societal resilience refers not only to public policy and services related to infrastructure or related vital societal functions, but also to the ability of social groups and the society at large to cope with external stresses and disturbances as a result of contingencies. It is thus related to the needs and tolerances of the community, which is dependent on the service provided by critical infrastructure. Having this information the regional critical infrastructure operators could set their minimum required service levels required from them. Closing the gap between public expectations and the actual service level provided, can be solved through effective communication, illustrating the bi-directional link between a resilience assessment in technological and organizational domains, on the one hand, and societal resilience, on the other hand.

There exist many efforts to define societal resilience (or social, sometimes community, although defined in a various ways), and there can be found a lot of good practices of resilient communities. In any case, the focus in societal resilience is on the problems of local communities when it faces crises, emergencies or disasters, where critical infrastructure, or its service disruption, may or may not play a crucial role. Yet, even if the source of a disaster is the disruption of critical infrastructure service, the question is not usually on absorptive but adaptive capacities toward these critical infrastructure disturbances. Often societal resilience research is connected to bio-socio-economic issues and social capital.

There is no one, agreed-upon metrics to evaluate societal security and resilience. Moreover, many of the societal resilience approaches are very generic ones, and thus difficult to handle. While quite a few efforts to develop societal resilience indicators and indices exist e.g. [20], they often only list socio-economic or institutional-political indicators at a very general level. They typically present a set of indicators for measuring baseline levels of community resilience. These can include a number of elements of society that are supposed to measure security and resilience, such as: educational equity, age structure, transportation access, communication capacity, language competency, special needs, health coverage, place attachment, political engagement, social capital in terms of religion, social capital in terms of civic involvement and advocacy, innovation, cohesiveness and trust, societal relationships, contentment with life, conflicts, communication between stakeholder groups, power and political structures, engagement of young people, responses to and opportunities for influencing change, learning and knowledge, knowledge utility and transfer (learning from experience), participation in decision-making, engagement of community resources, stakeholder agency, etc.

At best, in terms of concreteness, the scientific literature on societal security and resilience suggests indicators that reflect the emergency management and self-assistance capacities of the community. Occasionally, one can find efforts to consider the linkage between infrastructures and social systems [21], arguing that there is a need to link physical systems and human communities in order to measure and enhance societal security and resilience. From the perspective of regional CISR and related disturbances, it has how-

ever been emphasized at least three essential criteria or guidelines that should be taken into account: know the public stakeholders and their expectations; meet expectations; share disaster-related information [22].

Organizational resilience refers to the sectors, organizations and institutions that manage the regional critical infrastructures, including processes of organizational capacity and capability, planning, training, leadership, communication, etc. Organizational analysis is most often done qualitatively, but can in some cases be transformed to quantitative or semi-quantitative scales.

In the field of organizational resilience, there is a growing body of scientific literature that literally aims at developing indicators to measure an organizations resilience, e.g. [23], as well as a number of national and international standards ISO 28002:2011, ISO 28004:2014, etc. In fact, the first resilience standards are related to organizational resilience. Thus, the ISO 28002 standard for resilience in the supply chain was approved in 2011, based on the U.S. ANSI/ASIS.SPC.1:2009 organizational resilience standard.

The focus of this literature is primarily on organizations that own and manage regional critical infrastructure facilities. The purpose is to measure the ability of an organization to withstand disturbance of regional critical infrastructure facilities and maintain or quickly regain function. In practice, this takes place mostly in self-auditing manner, motivated by self-interested profit-seeking in terms of business continuity, although also public good considerations might be taken into account, at least for the sake of possible reputation costs.

To be safe and resilient, organizations must take into account such factors as strong and flexible leadership, an awareness and understanding of their operating environment, their ability to adapt in response to rapid change, etc. Yet, while at the first sight, this is a rather straightforward process, and as such suitable for standardization, it becomes more complicated due to the fact that social and cultural differences must be considered. Also such indices as innovativeness, creativity and improvisation skills of the organization leadership are often put forward, which however are rather difficult to measure, except post factum.

Technological resilience (sometimes technical or engineering) refers mainly to the physical properties of the regional critical infrastructures, focusing on their ability to resist damage and their loss of function during an over-stress situation. Technological security and resilience looks the issue at stake from an engineering point of view. While technological resilience includes elements of organizational resilience, and these two domains in a way require each other in many cases, the main difference is that resilience is achieved by technological rather than organizational solutions.

The main actors in the context of this domain of regional security and resilience are critical infrastructure operators, that is, those very facilities that produce the critical services. The role of authorities might be to regulate or control that the technical standards are followed. Furthermore, in most cases, the in-house technological or engineering capacities and capabilities of a service producer are not enough, but one has to rely on manufacturers or vendors for resilience-related technological solutions.

There is no officially approved definition of technological resilience in the context of regional critical infrastructure security in terms of international standard. However, a certain level of consensus has been emerging in the related scientific literature. From the standard definition of security, including resilience, one can already derive the main elements of technological resilience. If a resilient infrastructure is a component, system or facility that is able to withstand damage or disruption, but if affected, can be readily and cost-effectively restored, then there are three key technological concepts in resilience that should be demanded from a resilient critical infrastructure: resistance, absorption-adaptation (minimizing the consequences of disruption) and restoration capacity. Resistance could also be described with the term robustness [24], which is the ability of a system to resist or withstand an extreme event of a given level and still maintain some degree of system function.

Every engineering solution is naturally one of its own kinds. Yet, already this rather minimalist definition provides us a rather straightforward understanding about what are the general attributes or elements could be measured in respect to resilient infrastructure – especially from a technological perspective.

In modern literature on technological security and resilience, one can find more or less detailed typologies and indicators [25–27]. In fact, [28] provided already early on a typology of the resilience aspects of an earthquake that could be applied to critical resilience as well. This typology included four levels: robustness, redundancy, resourcefulness and rapidity of recovery. This typology, in turn, has been repeated with some variations in most definitions of resilience. For instance, the politically influential definition [29]

includes four factors: robustness, which is the ability to keep a critical infrastructure operating or stay standing in the face of disaster; resourcefulness, which means a skilful management of a disaster once it unfolds; rapid recovery, which refers to the capacity to get things back to normal as quickly as possible after a disaster; and, finally, learning, that is, the ability to absorb new lessons that can be drawn from a catastrophe [26].

Often when one approaches technological resilience it is illustrated by the so-called resilience triangle [30], which expresses performance loss in function to time of recovery. Increased resilience means that the triangle space will be reduced, and, hopefully moved to the right to enhance time for preparedness measures. By definition, this triangle presupposes the phase before any disruption, that of a downward curve and the upward curve, and last, post-disruption phase when the service level has been restored. In some fields, such as urban planning, the idea of ”rebuild it better” is applied, thus the starting performance level becoming higher as it was before the incident. Thus, local communities may use a disaster as an opportunity to regenerate an area. In pure technological fashion, which however captures the essence of security and resilience in many ways, Figure 2 illustrates this “resilience triangle” function as reproduced in [31].

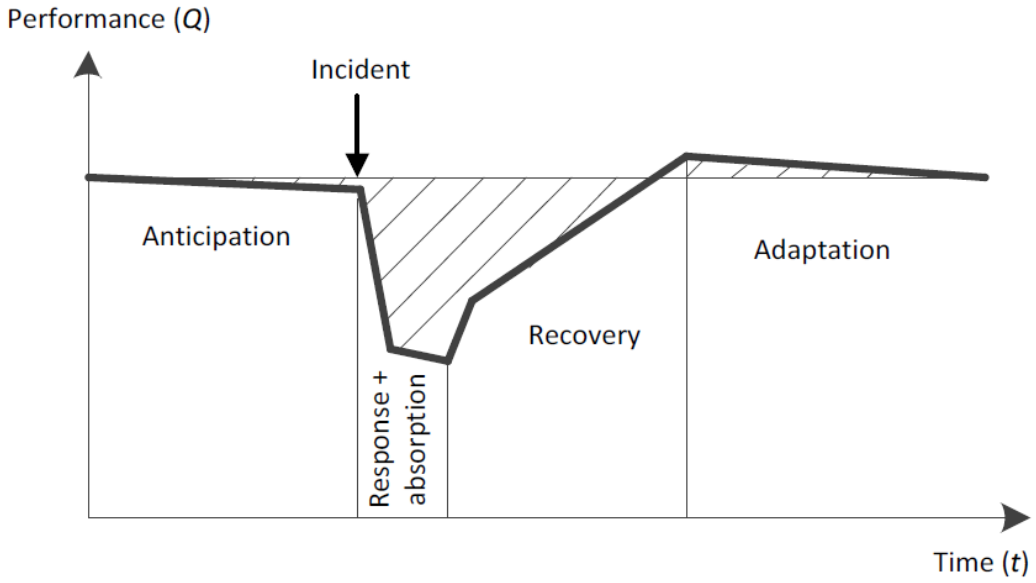

Fig. 2. Resilience triangle function: performance loss and recovery [31]

Regional CISR management technique

The question arises how we can evaluate regional CISR, and through that, enhance it. How to make the Arctic region more secured and resilient, especially those elements that are related to vital societal functions and socio-economic sphere of development, in order to “meet the basic needs of the population and society” and those “services and supplies” that have to be maintained in order to meet needs [4].

To address this problem a systematization and development of the CISR network-centric management system in the Arctic region is basically needed by preparing and implementing fundamental and practical guidelines (namely, holistic methodology), which, on the one hand, draw on the generic CISR foundations but, on the other hand, are tailorable to the specific regional conditions, taking into account the emergence of dynamic changes and challenges that Arctic specificity and external environment are bringing.

To assess and improve regional CISR, a step-by-step guidelines, inspired by ISO 31000 risk management standard (ISO 31000:2018, ISO 31000:2009) and applied to CISR in more generic contexts according to IEC/FDIS 31010:2019 standard, can be used and adopted to the Arctic regional environment. By mapping CISR against the widely approved and applied risk management standard, and using the same terminology and structure, has its advantage in that many organizations and institutions already are familiar with it. The approach thus enhances the current risk management, prevention and preparedness practices by adding the CISR component to it, and in so doing, enhances and systematizes especially the during-and-after contingency management and overall resilience of the community, its vital functions, and societal and infrastructure elements that these functions are dependent on. The main phases and elements of this kind of approach are illustrated in Figure. 3.

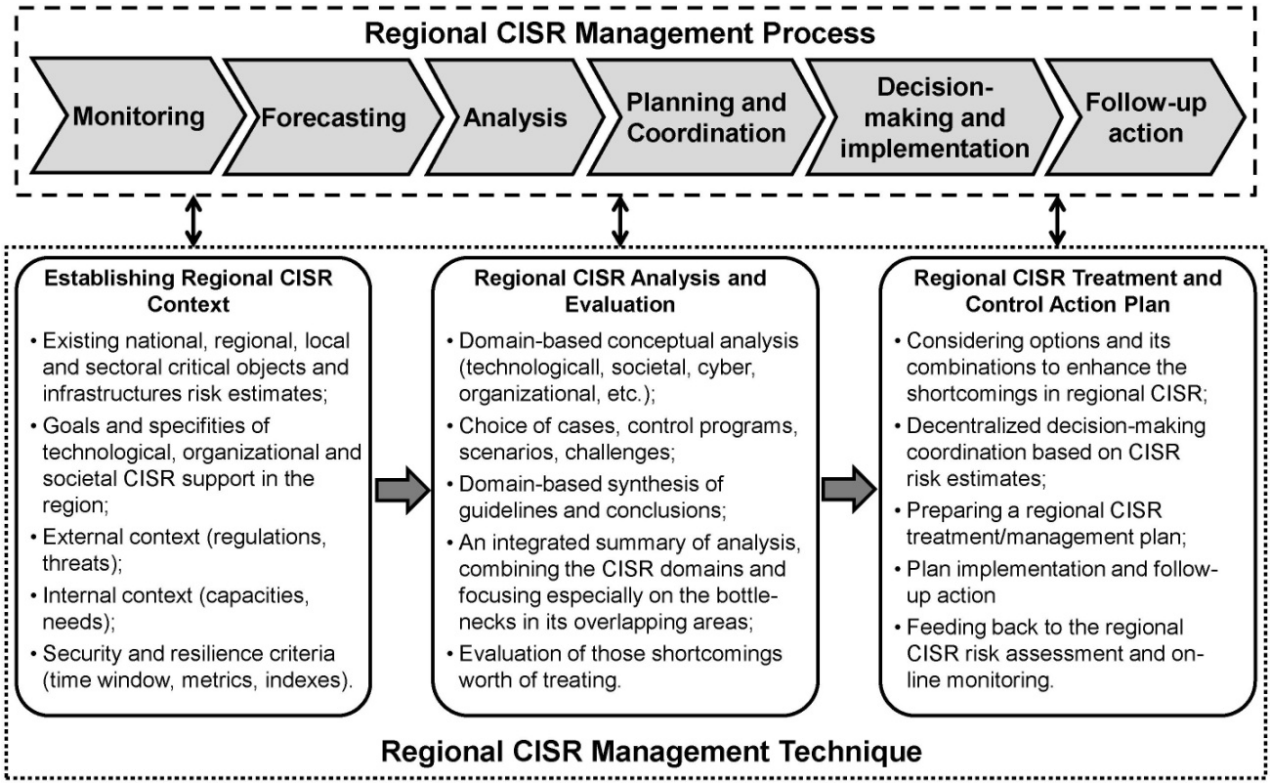

Fig. 3. Steps and components of regional CISR management technique

In the above illustration of the regional CISR management and assessment process, the following definitions are used:

– regional CISR management is the name of all of the coordinated activities to defined the below processes;

– regional CISR context refers to establishing the basic parameters for CISR assessment, taking into account the regional specificity and especially creating a shared understanding about the risks that might play out at the all levels of management;

– regional CISR analysis is the process to comprehend and to determine the level of regional security and resilience;

– regional CISR evaluation is the process of comparing the results of the regional security analysis with criteria or objectives to determine whether the level or resilience is acceptable and to identify areas for improvement;

– regional CISR treatment is the process of developing plans for enhancing regional security and resilience, focusing on the absorptive, adaptive or restorative capacity of socio-economic systems.

Novel holistic methodology of CISR management support

Regional CISR management is multifunctional in its structure and generally includes such control functions as targeting, strategic planning, operational management as well as control, accounting, monitoring and coordination functions. Therefore, information and analytical support of CISR management is a complex and multidimensional problem.

To address this issue we propose a methodology and model suite that provide workflow automation and interaction consistency of the critical infrastructure resilience management actors and entities at all decision-making levels (strategic, operational and tactical) at the expense of appropriate information support and coordination of the regional security network-centric control based on application of autonomous software agents and simulation tools. Our methodology is designed on the basis of methods integration for conceptual, system-dynamic and multi-agent modeling of multi-level distributed systems [32].The methodology and its principal components are schematically represented in Figure 4.

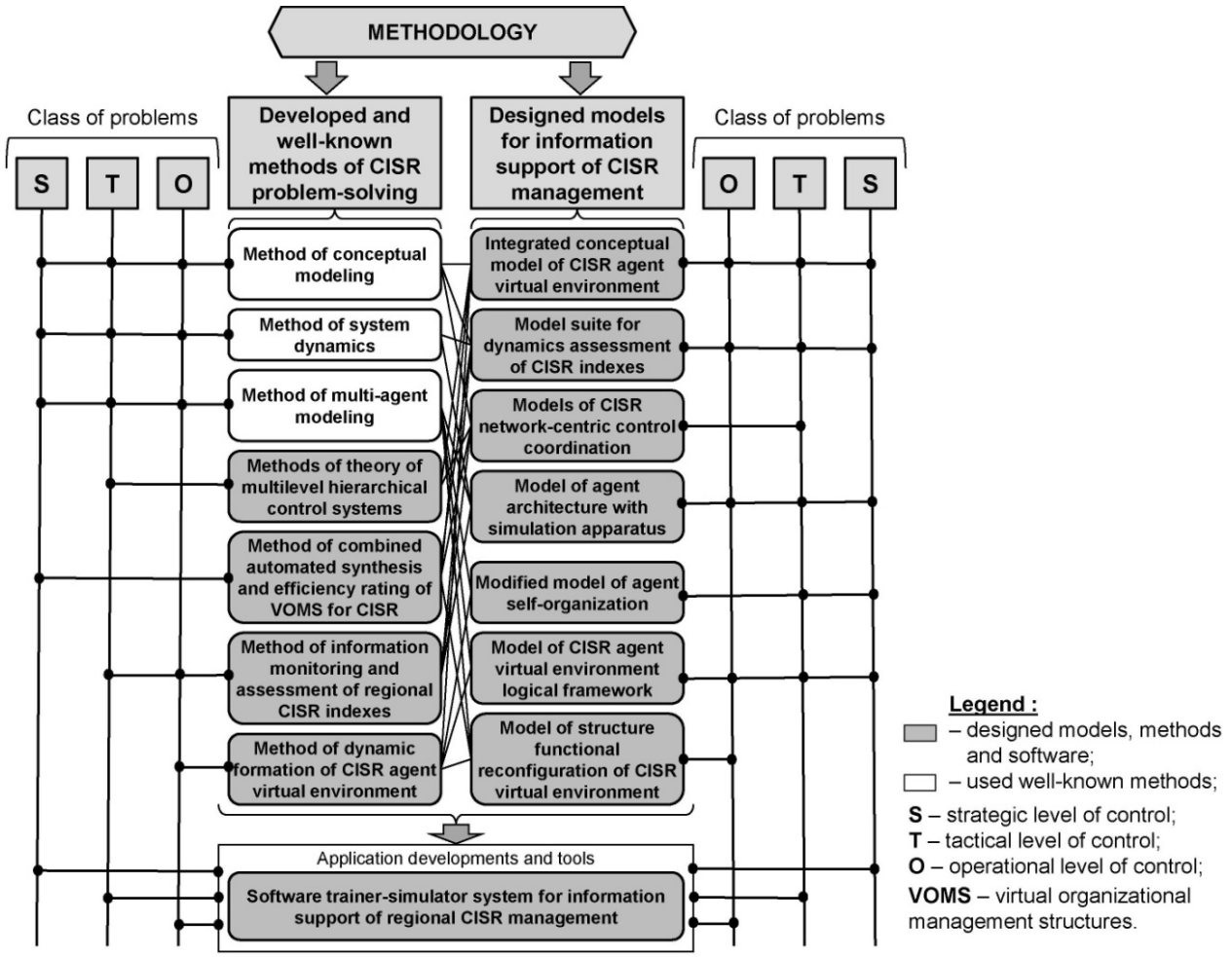

Fig. 4. Holistic methodology of CISR analysis and management support

The methodology tool framework includes following developed models and methods [32]:

1) Modeling tools:

– An integrated conceptual model of the multi-agent information environment for regional CISR which is a formal framework for automation and simulation of regional CISR management processes. Formalized models of the regional security problem domain and the executive environment for information and analytical support of critical infrastructure resilience control are combined within the model. For practical applications the model is implemented as an unified OWL-ontology used in decision support system of regional situational centers.

– An agent-based multi-level recurrent hierarchical model for risk-sustainable development management of regional socio-economic systems. The model is designed to network-centric control coordination of regional CISR. The model specificity consists in the use of functional-target technology and mathematical apparatus of hierarchical multi-level system theory for the purpose of coordination procedures implementation of local network-centric managerial decisions. The model combines coordination techniques by unleashing interactions and agent coalition formation at various control levels.

– A set of simulation models for risk and failure prediction of the regional CISR based on the original metrics derived by a number of groups convolution of the generally accepted reliability indices. The model suite provides both derivation of the integral estimate of regional CISR, and assessment of its individual components.

– A functional organization model of the intelligent agents having hybrid architecture with built-in simulation apparatus. The simulation apparatus corresponds to a complete or simplified model of the agent functioning environment recurrently evoked during the modeling process and provides a local forecast of results of the agent potential activity. System-dynamic models are used as a framework of agent simulation apparatus engineering and implementation.

2) Methodical tools:

– A method for automated synthesis of the multi-agent model specifications of organizational structures for regional CISR management under emergency situations of various types. The method is based on a joint analysis of the semantic description of solving control problems, information resources and agent services. The method provides dynamic formation of agent coalitions and associated virtual resources that are appropriate to the security management problems being solved.

– A method for a comprehensive assessment of the integral security and resilience indices of regional socio-economic system critical infrastructures based on matrix formation and analysis of the CISR metrics (indices) and providing an indicated assessment of regional security and critical infrastructure resilience under various regional development scenarios on the basis of expert-simulation modeling.

– A method and tools for multi-agent virtualization of regional CISR management process providing purposeful behavior adaptive modeling of each security control actor as an autonomous pro-active agent with its own interests and goals at all decision-making levels. The method is based on multi-agent and ontological modeling toolkit enhancement by means of implementation the agent simulation apparatus and semantic-driven integration of heterogeneous information resources and services.

– An agent-based technology for information monitoring of regional CISR threats and failures using autonomous software agents and special sensors for data acquisition and processing.

– A multi-agent technology for dynamic synthesis and configuration of the virtual environment of regional CISR based on the agent self-organization models and algorithms.

3) Software Tools:

– A peer-to-peer agent platform for distributed modeling of regional CISR management and software agent functioning support of the heterogeneous security control actors. The platform is designed on the basis of a service-oriented architecture.

– A software multi-agent system for information support of regional CISR management, which provides formation of virtual organizational structures for safety management in the region.

– A software trainer-simulator complex for modeling, forecasting and scenario analysis of the critical infrastructure functioning and development of regional socio-economic systems, which allows assessing and studying the dynamics of regional security and resilience indices.

– A multi-subject-domain web-oriented information system Ru-Arctic, which implements a unified access point to information environment (i.e. shared resources and services) of the regional CISR.

– Professional social network BarentsNet, which provides an automated search and selection of CISR control actors and their joint virtual cooperation within the distributed information environment of the region.

– A trainer-simulator tooling suite «Virtual Cognitive Center» intended for distributed expert-simulation modeling of emergency situations development in the regional critical infrastructures and network-centric control coordination of regional socio-economic system security and resilience. Technologically, this virtual management-simulator is implemented as a hybrid cloud service, e.g. SaaS (Software-as-a-Service) or IaaS (Infrastructure-as-a-Service).

The methodology provides wide and flexible possibilities to bundled software and modeling tools engineering for multi-agent network-centric information environment implementation of the regional CISR management. This software and model suite can be used to a range of practical control problem-solving in the field of CISR information support of the Arctic region as well as in other critical applications of regional socio-economic system risk-management (economic, ecological, personnel, social, political, military, cyber, etc.).

Conclusion

Prevention and control of the regional CISR is a novel and prospective problem domain for researchers and developers in the field of risk analysis of complex systems. Our study shows that today it is a dynamic problem domain, which is characterized by the complication of existing and the emergence of new control problems of regional and higher-level socio-economic systems. These problems are essentially related to the need of accident prevention and security ensuring in the all spheres of public relations that condition on toughening of existing and forming of fundamentally new safety requirements and standards for managing means and technologies of socio-economic system resilience. In our opinion the effectively solving of these problems first of all requires applying and development of network-centric framework to in-

formation support system engineering for management of regional CISR, methods for decentralized control coordination in multi-level distributed safety systems, managerial decision-making processes virtualization technologies based on multi-agent approach, methodology for dynamic model conceptual synthesis of complex systems, implementation mechanisms of intelligent cyber-physical systems, etc. The integration of specified toolkit within the unified instrumental base will provide through-driven design of the sufficient holistic methodological approach to engineering and implementation of information and analytical support tools appropriated to regional CISR management problem-solving.

The proposed background and developed methodology to control, prevention and analysis of regional CISR based on combination and partnering of conceptual, system-dynamic and multi-agent models and methods for decision-making information support provide:

– identification, evaluation and diagnostic situational analysis of the internal and external threats and vulnerability sources of the regional CISR;

– comprehensive risk assessment of regional CISR and prediction of its consequences;

– continuous monitoring and prevention of CISR indicators representing regional critical infrastructure functioning status to the timely threat-driven counteracting and consequence eliminating of its negative impacts on socio-economic development of the region;

– situational awareness analysis and assessment under conditions of uncertainty to selection and coordination of joint control actions under appearing emergency situations;

– synthesis of security management scenarios and formation of guidelines for decision-makers to efficiency enhancement of regional critical infrastructure resilience control and implementation;

– flexible adjustment and automated configuration of knowledge-based decision support systems for CISR management in the framework of regional situational center network.

Further research and developments in the problem domain discussed upon will provide wide opportunities to solve a whole range of specific fundamental and applied problems related to CISR on-line control, prevention, strategic planning and information support both at regional, national and higher levels.

***Acknowledgements**. The work was carried out within the framework of the State Research Program of the Institute for Informatics and Mathematical Modeling of the Kola Science Centre of RAS (project No. 0226-2019-0035). Author thanks Dr. Christer Pursiainen and his colleagues from The Arctic University of Norway (UiT) for research collaboration with Kola Science Center RAS.*

Работа выполнена в рамках государственного задания ИИММ КНЦ РАН (НИР № 0226-2019-0035). Автор выражает благодарность проф. К. Х. Пурсиаинену и его коллегам из Арктического университета Норвегии за сотрудничество с Кольским научным центром РАН.

Библиографический список

1. О Стратегии национальной безопасности Российской Федерации : указ Президента РФ № 683 от 31.12.2015. – URL: http://kremlin.ru/acts/bank/40391
2. *Ильин, Н. И.* Особенности современного этапа создания системы распределенных ситуационных центров в интересах государственного управления Российской Федерации / Н. И. Ильин, Р. М. Юсупов // Информатизация и связь. – 2019. – №. 3. – С. 7–13.
3. *Маслобоев, А. В.* Модель и технология поддержки принятия решений в условиях сетецентрического управления региональной безопасностью / А. В. Маслобоев // Надежность и качество сложных систем. – 2019. – № 2 (26). – С. 43–59.
4. *Pursiainen, C.* Critical infrastructure resilience: A Nordic model in the making? / C. Pursiainen // International Journal of Disaster Risk Reduction. – 2018. – Vol. 27. – P. 632–641.
5. Council 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. – URL: https://eur-lex.europa.eu/eli/dir/2008/114/oj
6. CIPedia© – A service of CIPRNet: Critical Infrastructure Protection (CIP) and Critical Infrastructure Resilience (CIR) related issues. – URL: https://websites.fraunhofer.de/CIPedia/index.php/CIPedia%C2%A9_Main_Page
7. Terminology on disaster risk reduction. – URL: https://www.unisdr.org/we/inform/terminology
8. *Маслобоев, А. В.* Концептуальная модель жизнеспособности критических инфраструктур в контексте современной теории безопасности сложных систем / А. В. Маслобоев, В. В. Быстров // Экономика. Информатика. – 2020. – Т. 47, № 3. – С. 555–572.
9. *Holling, C. S.* Resilience and stability of ecological systems / C. S. Holling // Annual Review of Ecology and Systematics, – 1973. – № 4 (1). – P. 1–23.

10. *Pimm, S. L.* The complexity and stability of ecosystems / S. L. Pimm // Nature. – 1984. – № 307 (5949). – P. 321–326.
11. *Hosseini, S.* A Review of Definitions and Measures of System Resilience / S. Hosseini, K. Barker, J. E. Ramirez-Marequez // Reliability Engineering and System Safety. – 2016. – Vol. 145. – P. 47–61.
12. *Francis, R.* A metric and frameworks for resilience analysis of engineered and infrastructure systems / R. Francis, B. Bekera // Reliability Engineering and System Safety. – 2014. – Vol. 121. – P. 90–103.
13. Resilience-Oriented Urban Planning. Theoretical and Empirical Insights / ed. by Y. Yamagata, A. Sharifi. – Springer Intl. Publ. – 2018. – Vol. 65. – 228 p.
14. *Righi, A. W.* A systematic literature review of resilience engineering: Research areas and a research agenda proposal / A. W. Righi, T. A. Saurin, P. Wachs // Reliability Engineering and System Safety. – 2015. – Vol. 141. – P. 142–152.
15. Evaluation of resilience assessment methodologies / B. Rød, et al. // Safety and Reliability, Theory and Applications / ed. by M. Cepin, R. Briš. – Boca Raton : CRC Press, 2017. – P. 1039–1051.
16. Critical Infrastructure Resilience Index / C. Pursiainen, et. al. // Risk, Reliability and Safety: Innovating Theory and Practice / ed. by L. Walls, M. Revie and T. Bedford. – Boca Raton : CRC Press, 2017. – P. 2183–2189.
17. *Цыгичко, В. Н.* Безопасность критических инфраструктур / В. Н. Цыгичко, Д. С. Черешкин, Г. Л. Смолян. – Москва : Красанд, 2018. – 200 с.
18. *Офицеров, А.* Концептуальные основы обеспечения комплексной безопасности критически важных объектов / А. Офицеров, О. Басов, С. Бачурин // Экономика. Информатика. – 2020. – Т. 47, № 1. – С. 154–163.
19. *Шульц, В. Л.* Сценарный анализ в управлении геополитическим информационным противоборством / В. Л. Шульц, В. В. Кульба, А. Б. Шелков, И. В. Чернов. – Москва : Наука, 2015. – 542 с.
20. *Aldrich, P. A.* Social Capital and Community Resilience / P. A. Aldrich, M. A. Meyer // American Behavioural Scientist. – 2015. – Vol. 59, iss. 2. – P. 254–269.
21. *Shishaev, M.* Analysis of Online Social Networking When Studying the Identities of Local Communities / M. Shishaev, A. Fedorov, I. Datyev // Digitalization and Human Security. A Multi-Disciplinary Approach to Cybersecurity in the European High North / ed. by M. Salminen, G. Zojer, K. Hossain. – Palgrave Macmillan Publ., 2020. – P. 267–295.
22. Social resilience criteria for critical infrastructures during crises / L. Petersen, et al. // IMPROVER D4.1. – 2016. – URL: https://pauljreillydot.files.wordpress.com/2014/04/improver-d4-1-social-resilience-criteria-for-critical-infrastructures-during-crises_draft.pdf
23. *Labaka, L.* Resilience framework for Critical Infrastructures: An Empirical Study in a Nuclear Plant / L. Labaka, J. Hernantes, J. M. Sarriegi // Reliability Engineering and System Safety. – 2015. – Vol. 141. – P. 92–105.
24. *Поляк, Б. Т.* Робастная устойчивость и управление / Б. Т. Поляк, П. С. Щербаков. – Москва : Наука, 2002. – 303 с.
25. Complex approach to assessing resilience of critical infrastructure elements / D. Rehaka, et al. // International Journal of Critical Infrastructure Protection. – 2019. – Vol. 25. – P. 125–138.
26. *Pursiainen, C.* Towards Testing Critical Infrastructure Resilience / C. Pursiainen, P. Gattinesi // Publications Office of the European Union, JRC Scientific and Policy Reports. – 2014. – URL: https://core.ac.uk/download/pdf/38627770.pdf.
27. Novel methodologies for analyzing critical infrastructure resilience / K. Storesund, et al. // Safety and Reliability – Safe Societies in a Changing World / ed. by S. Haugen, et al. – 2018. – P. 1221–1229.
28. A framework to quantitatively assess and enhance the seismic resilience of communities / M. Bruneau, et al. // Earthquake Spectre. – 2003. – Vol. 19, № 4. – P. 733–752.
29. *Flynn, S. E.* America the Resilient: Defying Terrorism and Mitigating Natural Disasters / S. E. Flynn // Foreign Affairs. – 2008. – Vol. 83, № 2. – P. 2–8.
30. *Zorn, C. R.* Post-disaster infrastructure restoration: A comparison of events for future planning / C. R. Zorn, A. Y. Shamseldin // International Journal of Disaster Risk Reduction. – 2015. – Vol. 13. – P. 158–166.
31. Technological resilience concepts applied to critical infrastructure / D. Honfi, et al. // IMPROVER D3.2. – 2017. – URL: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b12eb01d&appId=PPGMS
32. *Маслобоев, А. В.* Информационное измерение региональной безопасности в Арктике / А. В. Маслобоев, В. А. Путилов. – Апатиты : КНЦ РАН, 2016. – 222 с.

References

1. *O Strategii natsional'noy bezopasnosti Rossiyskoy Federatsii: ukaz Prezidenta RF № 683 ot 31.12.2015* [On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation No. 683 of 31.12.2015]. Available at: http://kremlin.ru/acts/bank/40391 [In Russian]
2. Il'in N. I., Yusupov R. M. *Informatizatsiya i svyaz'* [Informatization and communication]. 2019, no. 3, pp. 7–13. [In Russian]

3. Masloboev A. V. *Nadezhnost' i kachestvo slozhnykh system* [Reliability and quality of complex systems]. 2019, no. 2 (26), pp. 43–59. [In Russian]
4. Pursiainen C. *International Journal of Disaster Risk Reduction*. 2018, vol. 27, pp. 632–641.
5. *Council 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* [ ]. Available at: https://eur-lex.europa.eu/eli/dir/2008/114/oj
6. *CIPedia© – A service of CIPRNet: Critical Infrastructure Protection (CIP) and Critical Infrastructure Resilience (CIR) related issues*. Available at: https://websites.fraunhofer.de/CIPedia/index.php/CIPedia%C2%A9_Main_Page
7. *Terminology on disaster risk reduction*. Available at: https://www.unisdr.org/we/inform/terminology
8. Masloboev A. V., Bystrov V. V. *Ekonomika. Informatika* [Economy. Computer science]. 2020, vol. 47, no. 3, pp. 555–572. [In Russian]
9. Holling C. S. *Annual Review of Ecology and Systematics*. 1973, no. 4 (1), pp. 1–23.
10. Pimm S. L. *Nature*. 1984, no. 307 (5949), pp. 321–326.
11. Hosseini S. A, Barker K., Ramirez-Marequez J. E. *Reliability Engineering and System Safety*. 2016, vol. 145, pp. 47–61.
12. Francis R., Bekera B. *Reliability Engineering and System Safety*. 2014, vol. 121, pp. 90–103.
13. *Resilience-Oriented Urban Planning. Theoretical and Empirical Insights*. Ed. by Y. Yamagata, A. Sharifi. Springer Intl. Publ., 2018, vol. 65, 228 p.
14. Righi A. W., Saurin T. A., Wachs P. *Reliability Engineering and System Safety*. 2015, vol. 141, pp. 142–152.
15. Rød B. et al. *Safety and Reliability, Theory and Applications*. Boca Raton: CRC Press, 2017, pp. 1039–1051.
16. Pursiainen C. et. al. *Risk, Reliability and Safety: Innovating Theory and Practice*. Boca Raton: CRC Press, 2017, pp. 2183–2189.
17. Tsygichko V. N., Chereshkin D. S., Smolyan G. L. *Bezopasnost' kriticheskikh infrastruktur* [Critical infrastructure safety and security]. Moscow: Krasand, 2018, 200 p. [In Russian]
18. Ofitserov A., Basov O., Bachurin S. *Ekonomika. Informatika* [Economy. Computer science]. 2020, vol. 47, no. 1, pp. 154–163. [In Russian]
19. Shul'ts V. L., Kul'ba V. V., Shelkov A. B., Chernov I. V. *Stsenarnyy analiz v upravlenii geopoliticheskim informatsionnym protivoborstvom* [ ]. Moscow: Nauka, 2015, 542 p. [In Russian]
20. Aldrich P. A., Meyer M. A. *American Behavioural Scientist*. 2015, vol. 59, iss. 2, pp. 254–269.
21. Shishaev M., Fedorov A., Datyev I. *Digitalization and Human Security. A Multi-Disciplinary Approach to Cybersecurity in the European High North*. Palgrave Macmillan Publ., 2020, pp. 267–295.
22. Petersen L. et al. *IMPROVER D4.1.* 2016. Available at: https://pauljreillydot.files.wordpress.com/2014/04/improver-d4-1-social-resilience-criteria-for-critical-infrastructures-during-crises_draft.pdf
23. Labaka L., Hernantes J., Sarriegi J. M. *Reliability Engineering and System Safety*. 2015, vol. 141, pp. 92–105.
24. Polyak B. T., Shcherbakov P. S. *Robastnaya ustoychivost' i upravlenie* [Robust stability and control]. Moscow: Nauka, 2002, 303 p. [In Russian]
25. Rehaka D. et al. *International Journal of Critical Infrastructure Protection*. 2019, vol. 25, pp. 125–138.
26. Pursiainen C., Gattinesi P. *Publications Office of the European Union, JRC Scientific and Policy Reports*. 2014. Available at: https://core.ac.uk/download/pdf/38627770.pdf.
27. Storesund K. et al. *Safety and Reliability – Safe Societies in a Changing World*. 2018, pp. 1221–1229.
28. Bruneau M. et al. *Earthquake Spectre*. 2003, vol. 19, no. 4, pp. 733–752.
29. Flynn S. E. *Foreign Affairs*. 2008, vol. 83, no. 2, pp. 2–8.
30. Zorn C. R., Shamseldin A. Y. *International Journal of Disaster Risk Reduction*. 2015, vol. 13, pp. 158–166.
31. Honfi D. et al. *IMPROVER D3.2.* 2017. Available at: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b12eb01d&appId= PPGMS
32. Masloboev A. V., Putilov V. A. *Informatsionnoe izmerenie regional'noy bezopasnosti v Arktike* [Information dimension of regional security in the Arctic]. Apatity: KNTs RAN, 2016, 222 p. [In Russian]

Маслобоев Андрей Владимирович
доктор технических наук, доцент,
ведущий научный сотрудник,
Институт информатики и математического
моделирования технологических процессов
Кольского научного центра РАН
(Россия, Мурманская область, г. Апатиты,
ул. Ферсмана, 14)
E-mail: masloboev@iimm.ru

Masloboev Andrey Vladimirovich
doctor of technical sciences, associate professor,
leading researcher,
Institute of Informatics and mathematical
modelling of technological processes
of the Kola Science Centre RAS
(14 Fersmana street, Apatite,
Murmansk region, Russia)

Образец цитирования:

Masloboev, A. V. Towards a theory of regional critical infrastructure security and resilience / A. V. Masloboev // Надежность и качество сложных систем. – 2020. – № 4 (32). – С. 115–130. – DOI 10.21685/2307-4205-2020-4-13.