БЕЗОПАСНОСТЬ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

SAFETY IN EMERGENCY SITUATIONS

УДК 004.9, 006.015.8
doi:10.21685/2307-4205-2022-1-13

A UNIFIED SYSTEM FOR ENSURING THE REGIONAL SECURITY

A.V. Masloboev

Federal Research Centre "Kola Science Centre of the Russian Academy of Sciences", Apatity, Russia
masloboev@iimm.ru

Abstract. *Background*. The paper deals with general issues of regional security ensuring via development and implementation of the integrated automated systems for situational control of regional critical infrastructures resilience. *Materials and methods*. Approaches to development of the regional security management systems based on the principles of risk theory, digital transformation of public administration on the basis of situational centers and experience gained in the field of energy security are analyzed. *Results and conclusions*. The problems of security support system engineering of the region are identified and estimated. The role of situational centers in solving of these problems at the regional level is proved and justified. A conceptual model of the system for ensuring the regional security has been designed. A formalization of the security and risk concepts within the framework of this model has been proposed. The structure and composition of the decision support system for managing the regional security based on the use of situation simulation modeling aids has been developed and studied. It has been assigned that the functioning efficiency of the regional security support systems is appreciably limited by the constant growth in the volumes of diverse information that requires operational processing and analysis for making managerial decisions, as well as the imperfection of the legal regulatory framework.

Keywords: situational control, decision support system, regional security ensuring, risk-analysis, simulation, situational center

Acknowledgments. 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. FMEZ-2022-0023).

For citation: Masloboev A.V. A unified system for ensuring the regional security. *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and quality of complex systems.* 2022;(1):115–125. (In Russ.). doi:10.21685/2307-4205-2022-1-13

КОМПЛЕКСНАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ РЕГИОНАЛЬНОЙ БЕЗОПАСНОСТИ

А. В. Маслобоев

Кольский научный центр Российской академии наук, Апатиты, Россия
masloboev@iimm.ru

Аннотация. *Актуальность и цели*. Рассматриваются общие вопросы обеспечения региональной безопасности посредством создания и внедрения комплексных автоматизированных систем ситуационного управления жизнеспособностью критических инфраструктур региона. *Материалы и методы*. Анализируются подходы к созданию систем управления региональной безопасностью, основанные на принципах теории риска, цифровой трансформации государственного управления на базе ситуационных центров, и опыте, накопленном в области обеспечения энергетической безопасности. *Результаты и выводы*. Определены проблемы построения систем обеспечения безопасности региона и обоснована роль ситуационных центров в решении этих проблем на региональном уровне. Разработана концептуальная модель системы обеспечения региональ-

ной безопасности, в рамках которой предложена формализация понятия безопасности и риска. Разработаны и исследованы структура и состав системы поддержки принятия решений по управлению региональной безопасностью, использующей в своей основе средства имитационного моделирования ситуаций. Установлено, что эффективность функционирования систем обеспечения региональной безопасности существенно ограничивается постоянным ростом объемов разноплановой информации, требующей оперативной обработки и анализа для принятия управленческих решений, а также несовершенством нормативно-правовой базы.

Ключевые слова: ситуационное управление, система поддержки принятия решений, обеспечение региональной безопасности, риск-анализ, моделирование, ситуационный центр

Финансирование. Работа выполнена в рамках государственного задания ИИММ КНЦ РАН (НИР № FMEZ-2022-0023).

Для цитирования: Маслобоев А. В. Комплексная система обеспечения региональной безопасности // Надежность и качество сложных систем. 2022. № 1. С. 115–125. doi:10.21685/2307-4205-2022-1-13

Introduction

At present, the intense human activity in the way of developing of the natural resources in the Arctic and implementation of novel exploration technologies according to state-of-the-art studies [1-5] inevitably leads to the density enhancement of the potentially dangerous objects in the biosphere. At the same time, the initiation likelihood of the various types of emergency situations and man-caused accidents is increasing, as well as the consequences of natural disasters and crises in the socio-economic sphere are aggravated. These negative phenomena and trends possess a global nature and are especially acute at the regional level destabilizing the socio-economic system of the region and hindering its risk-sustainable progressive development.

Along with strategic approaches to weakening these specified trends, it is quite necessary to operative respond to initiating emergency and crises situations. Thereto, today at the state level the appropriate international and national organizational structures for security management have been set up and continue to be established. Its responsibilities enclose on-line monitoring, prevention, warning and consequence elimination of the potential threats and risk implementation in regional critical infrastructures. Timely identification of the destabilizing impact sources allows minimizing the risks of critical situations manifestation of socio-economic, natural and man-caused nature that affect the safe operation of regional systems. In the normal mode of day-to-day activities, the profile-relevant departments ensuring the security of regional critical infrastructures conduct regular exercises at critically important assets and objects of the region, design projects and plans for anti-crisis measures, allocate resources and protection means to counteracting specific threats of regional security.

Nowadays, the considerable experience and knowledge have been accumulated in this area, but in theory and practice this experience is quite disconnected, i.e. fragmented by various fields and departments, despite the sufficient similarity of the existing management forms and well-known security ensuring methods. In the latest years, there has been observed an extension of the activity scope of security management organizational entities, as well as departmental barriers overcoming under joint interaction in regional security ensuring problem-solving due to the uniform standards and technical regulations application in the field of comprehensive security. These tendencies are typical not only for Russian Federation, but for all other world powers also. For example, the establishment of the Emergency Situations Ministry (EMERCOM) in our country in 1990 provided an opportunity to concentrate and coordinate efforts to ensure security in conditions of emerging contingency situations in a variety of regional critical infrastructures and for all critically important assets and elements forming its composition. A considerable contribution in security support and risk management problem-solving of socio-economic and technical systems was introduced by the Applied Problems Section of the Russian Academy of Sciences in cooperation both with domestic and foreign research institutions, and national security services and agencies.

Thus, it is possibly declared the relevance for design and engineering of the security support systems of various classes [3, 6] – global, international, national, regional, local and its systemic integration at all public administration management levels. The necessity for the development and implementation of such automated situational management systems is due to the needs for big data processing and analysis, containing diverse information on the state of critically important assets and elements of regional socio-economic systems and influencing factors on the one hand, and the requirements for prompt and adequate response to this information in the process of managerial decision-making, on the other. In this case information and control systems and networks already existing in the regions can be used, primarily integrated automated systems for situation awareness and monitoring of regional security in situational centers.

This survey-study is devoted to general issues of unified system engineering for ensuring the regional security. For definiteness the regional level is discussed. Moreover, all the statements and contributions set forth below can be attributed to other levels of management and government. This work is an extended version of the research represented earlier in conference proceedings of the 26th International Symposium "Reliability and Quality" held in Penza State University at the end of May 2021.

Background

Nuclear power engineering is one of the strategic areas of national economy, which has accumulated in long-term historical period mostly significant theoretical and practical experience in the field of security ensuring and risk management of complex systems. Therefore, it is rationally and objectively to study all essential aspects of regional security problem domain and possible ways of it ensuring on the basis goal-setting in this strategic area. Point is that for nuclear power area all kinds of "threat – counteraction" models and mechanisms are well-developed and analyzed. These risk management solutions are applicable to a wide range of other potentially dangerous elements and critical infrastructures of socio-economic systems also and consequently can be disseminated to various spheres of human life safety and regional development. The research works [7-11] formally define and analyze rather general and sufficient criteria of reliability, sustainability, safety, risk and damage concepts in this way.

Currently, the integrated automated systems for environment monitoring nearby and around nuclear power facilities are being intensively developed. Examples of such successfully proven systems are the system for monitoring the radiation situation in the location area of ground-based nuclear power plants ARSMS [12], the subsystem for geo-monitoring of underground nuclear facilities [13], foreign systems SPEED I (Japan), APAS (USA), RIMNET (Great Britain), TELERAD (Belgium), EMMA (Sweden), RECASS NT (Republic of Belarus), Gamma-1 (Ukraine) and others. Nuclear power plant monitoring system is represented as a multi-level automated management system, where nuclear power facilities and assets are considered as a single technological control objects, and constitutes of security control systems and functionally related set of equipment which provides maintaining process parameters within the specified limits, protecting facilities from overload and other safeguarding operation functions. Such management systems consist of the following main components: information and analytical subsystem, decision-making support subsystem, regulatory control subsystem, technological protection subsystem, etc.

The studies [14, 15] propose a terminological and categorical apparatus and conceptual foundations of the regional security management system "nuclear power facilities – environment". Moreover, a system of standards and rules that regulates various aspects of nuclear power facilities safety in the region, e.g. [16–18], has been developed and approved. This system of norms is closely interrelated with socio-economic, industrial and ecological factors of regional development and territorial specificities. As is obvious from the above-stated a great deal of these research efforts have built the basis and certain prerequisites for organizing efficient information-management systems for control and ensuring safety of critical infrastructure components and the regional security as a whole, as well as provided the possibility to use monitoring systems of external environment of nuclear power plants and facilities as a prototype. In turn, the implementation of such an approach allowed obtaining new results in the field of synthesis and analysis of network-centric systems for situational management of security and resilience of the regional critical infrastructures and critically important facilities in the Arctic zone of Russia [3, 19].

Another relevant approach to developing an integrated system for ensuring the regional security is based on methods and technologies of public administration digital transformation [20, 21] by means of implementation and deployment of the network-centric system of distributed situational centers and regional management centers. Situational centers are a state-of-the-art and high-end instrument of information-analytical support and a new form of management based on the National economy total digitization intended for ensuring a high level of comprehensive security at the regional, federal and international levels. Currently, situational centers are designed and deployed in order to prevention of critical situations in socio-economic, public and military-political spheres of country's development, as well as for the purpose to resilience and security control problem-solving of the critical facilities and critical infrastructures in the regions. Such an approach can be also adapted for the development of security support systems used in the field of nuclear power engineering. Nevertheless, this relatively novel approach to digital situational management is not normatively enshrined anywhere or is partially reflected in the existing legal acts and standards that regulate operating modes and application of situational centers. The leading role of situational centers in generalization of all diverse information on the security state and situation in the regions should be

enshrined at the legislative level. Moreover, the research level of situational center design and implementation is developing very slowly too.

The issues of modeling critical situations in the face of the new threats and hazards emergence using the situational center tools and functionality are extremely relevant. Nowadays, it is needed to concentrate our forces, facilities and expert knowledge on the management analytical support based on computer modeling. Monitoring and accumulation of the large volumes of information for making managerial decisions is ineffective today. No tangible effect of it is observed. For predicting the state of regional economy, generating solution variations of problem situations in the regions, scenario analysis and forecasting the development of national strength, assessing the level of national security, the instrumental modeling tools, domain-specific models, software and hardware systems based on these models are needed. These instruments must be embedded and implemented in the operating framework of situational centers.

Computer modeling is one of the effective methods for risk and security analysis of complex dynamic systems of various nature and scale. This technique allows running series of computational experiments with virtual prototypes (models – digital twins) of real world objects without violating the integrity and resilience of these objects or systems, as well as without negative consequences and harm-causing for human health or the environment. In addition, computer models provide the variability of making the simulation experiments in cases, when the real experiments with complex objects are hampered by financial or other resource constraints, or are physically impracticable. Therefore, almost all the state-of-the-art support systems for ensuring the regional security are using polymodel suites and situational management tools based on simulation models. The conception of computer modeling application for the critical situation analysis and decision-making support in the field of security ensuring of the regional socio-economic systems is schematically illustrated on Figure 1.

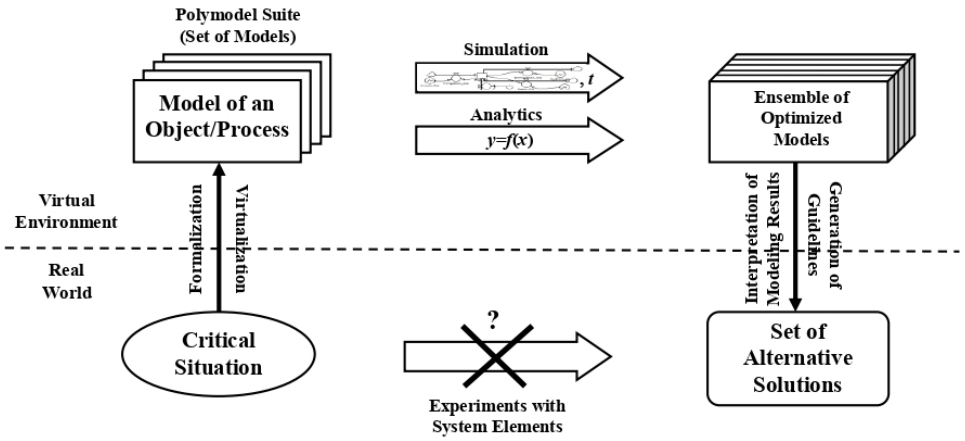

Fig. 1. The conceptual scheme of computer modeling application in regional security management

Situational centers of various levels (national, regional, municipal, sectoral, corporate) specialize in a wide range problem-solving concerned with risk assessment and analysis of the population and personnel safety, public and transport security, industrial-environmental and energy security, radiation and chemical protection, and others. The key mission of situational centers based on integration of digital platforms is to be a kind of intelligent buffer between the variety of relevant data sources and corresponding information users (decision makers) processed and systematized to provide the efficient management of regional and national security.

Any crisis or emergency situation (e.g. the up-to-date pandemic) is a powerful impetus for the search and development of new technological solutions, including the engineering of situational centers, in the field of security. It is just impossible to manage and ensure the security of a country or region in such conditions without the use of situational centers that provide digital transformation and information and analytical support for management processes.

System Conception and Framework

When engineering the security systems for ensuring critical facilities, critical infrastructures and complex socio-economic objects from effecting internal and external threats, it is important to understand the mathematical essence and fundamental control principles of management processes that predetermine adequate security control procedures (programs) generation, selection and implementation under current

situation. That promotes the developing of security theory of the complex systems. Without going into the deep details, the conceptual essence of the security theory problems is related to sudden concatenation of fatal circumstances in the socio-economic, military-political and environmental spheres that can at worst lead both to a loss of resilience, stability or safety of the critical facilities and critical infrastructures, and to further destructive impacts on quality of human life, life-support system functioning and other negative consequences. These risks are mostly expected and predictable for technical systems, even so most often accidental for socio-economic systems.

Taking into consideration the specificity and multifold nature of the control object (regional socio-economic system), as well as the security system engineering problem scope, it is quite difficult to solve fully the problem of ensuring the regional security. Traditionally in practice, there are several approaches to this problem-solving distinguished in the classical mechanisms of implementing the control actions (institutional, motivational, information control) and organization methods of the "object – regulator" type management systems (open-loop, closed-loop and combined control system models).

An open-loop security management system is applied in case, when external disturbances (threats) can be identified, accurately measured and estimated. This class of control systems provides a possibility to obtain the complete invariance of external threats. However, such security management systems are inapplicable to control unstable critical objects and processes.

On the other hand, a closed-loop security management system is operating by deviation principle of control object state variables from the set point values. In that case, the control principle of negative (balancing) feedback is implemented under security management process. At the same time, there is no need to know accurately all the effecting threats and nature of hazard sources. These security control systems are well-applicable to protect and operate with unstable critical objects and processes, since it provide stabilization of the “object – regulator” system by means of actual changing the dynamics of the system itself.

To provide the efficient operation of a multi-level system for decentralized control of regional security, the given control schemes ("by deviation" and "by disturbance") should be used simultaneously, since the combined control is intended for large-scale systems that are characterized by structural and dynamic complexity. Regional socio-economic systems are classified to this type of complex systems, where it is possible to single out a deterministic part that can be analyzed in detail, estimated and rigidly planned, and non-deterministic that is almost not suitable for such an in-depth analysis. The design and implementation of regulators (control and support systems) in the context of security system organization for ensuring the complex objects, critical facilities and infrastructures is an independent research problem required further special studying.

The integrated system for ensuring the regional security is intended for comprehensive and continuous problem monitoring and forecasting the state of potentially dangerous facilities and critical infrastructures in the region, risk management and dynamics prediction of the regional emergency and crisis situations development and finally to improve the level of regional security.

Traditionally, the system operates in two main modes: the normal duty (in case of stable operation of the critical facilities and in the absence of emergency situations) and the malfunction (in case of origination of the designed and beyond designed accidents, external or internal threat implementation, manifestation and development of critical situations or initiation of the hazardous phenomena). Some of critical elements and processes must be monitored continuously, and others periodically.

The system for ensuring the regional security is functioning interactively with:

- particular (local) security support systems of critical facilities in the region (lower level);
- the national (federal) security management system (higher level);
- the administration of the region and municipalities (the same level of management).

The generic model of a system for ensuring the regional security consists of control object (regional socio-economic system), regulator (security management system), external environment, control and data flows, system state monitor, input and output resources, etc. This generic model is schematically shown on Figure 2. Figure 2 illustrates the main steps of security ensuring procedure and accounting of various factor impacts occurred in management process.

In accordance with research [22, 23] the main functions of the system are:

1) data acquisition and preprocessing;
2) data logging and registration, maintenance of databases and knowledge bases;
3) external data accessing, exchange and transfer;
4) data mapping and visual representation in a geospatial form;

5) analysis and assessment of the situational awareness and situation dynamics;
6) on-line and long-term forecasting based on simulation models of situation development;
7) guidelines generation for decision-makers and operators to managing the situation;
8) execution control of made decisions and implementation analysis of anti-crisis measures;
9) business process documenting and preparation of accounting summary data.

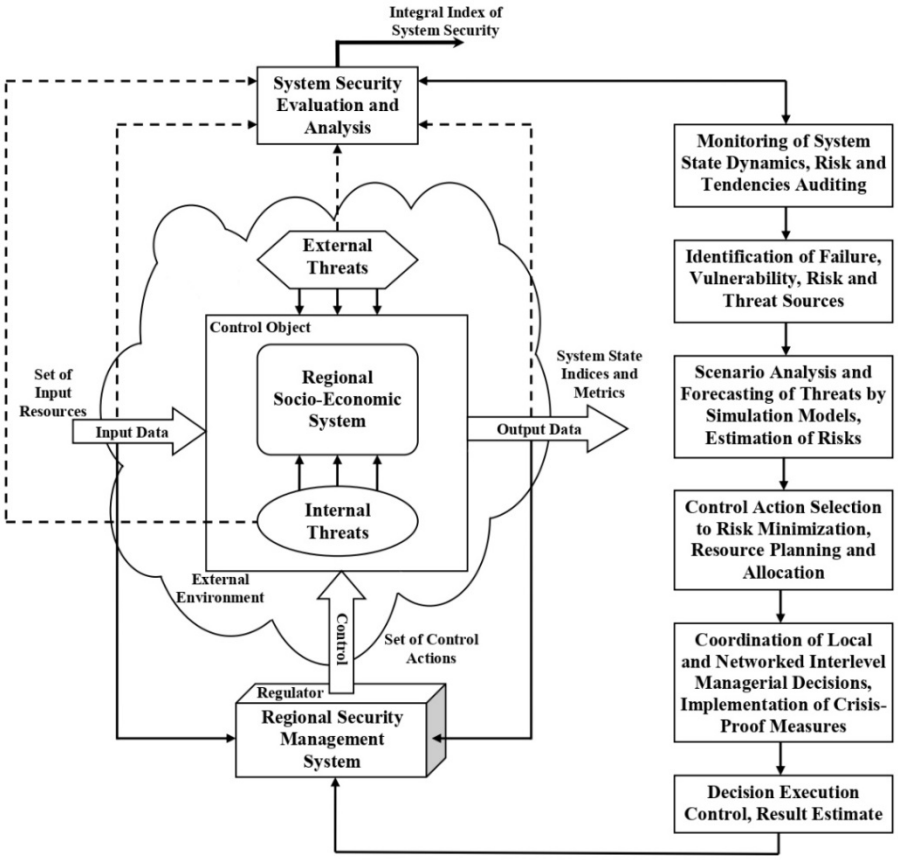

Fig. 2. The generic model of a system for ensuring the regional security

Listed above functions are implemented within the framework of a unified organizational and technical system and must be provided at the low-level activity (hardware), high-level activity (software) and organizational (user/management) level. The notation of particular (local) subsystems reflects the regional specificity in terms of the presence of potentially dangerous and critical facilities (nuclear power plants, oil and gas pipelines, life support systems, etc.). Figure 3 illustrates the architecture and functional components of the decision support system for managing the regional security based on computer modeling, scenario analysis and project management.

Key legend to Figure 3 includes: 1 – vector of control actions; 2 – selection of efficiency criteria and determination of relationships between them; 3 – accounting the criteria in the models under simulation process; 4 – adequacy analysis of the decisions according to the selected criteria; 5 – parameterization of models and input of initial data; 6 – report generation on a series of simulation experiments made; 7 – running models in the forecasting mode; 8 – running models in test mode; 9 – results of the test model executions; 10 – adequacy and performance evaluation of the model solutions; 11 – initial data; 12 – simulation results; 13 – interpretation of simulation results; 14 – a set of guidelines for decision makers to managing the system (process) critical elements and facilities.

When designing automated security systems for ensuring the resilience of critical facilities and regional critical infrastructures, it is necessary to take into account the delimitation of activity areas, jurisdiction (competences) and goal-setting (interests) of the regional security services and consequently the delimitation of on-line and analytical information between various separated departments responsible for ensuring the security of certain critical elements of regional systems. Thereupon, it is worth to draw attention to such a complicating factor as the interconnection of directions and the coordination of joint actions under security ensuring and management of the regional critical infrastructures and facilities. In turn, this

means the urgent needs to provide at once situational awareness and information negotiation and matching on various activity areas of the profile-relevant departments, as well as the possibility of data integration when assessing risks in the process of managerial decision making and implementing to regional security support.

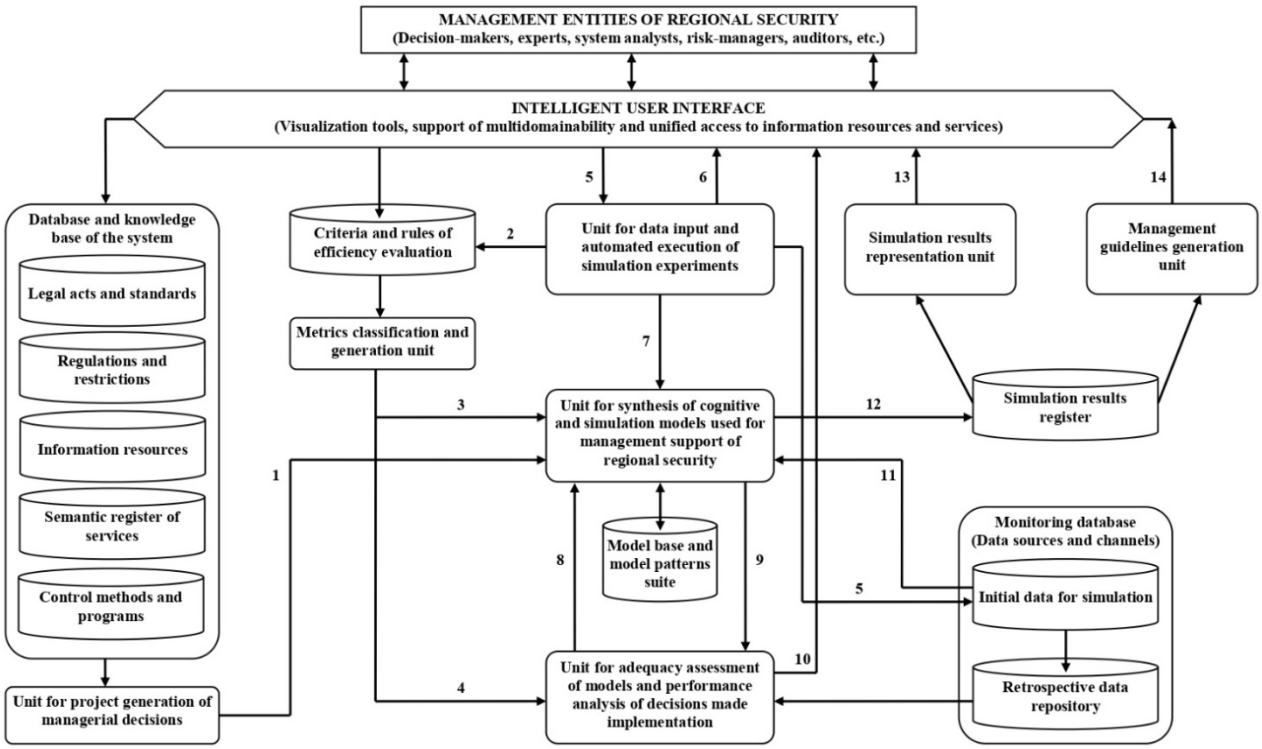

Fig. 3. The structure of a decision support system for managing the regional security

Problem Statement and Formalization

The principal difficulty lies in the need to unify information on various aspects of security and resilience of regional development and vital functions. This heterogeneous information should be represented in certain unified form that allows data deep analysis and drawing conclusions on the risk level and the state of critical facilities, as well as on the situation in the region as a whole. Then, general proposals for such unification will be considered.

All security control objects in the region are subdivided into three groups:

1) critically important facilities;
2) critical situations;
3) critical infrastructures.

Critical facilities are such complex elements of regional system as nuclear power plants, oil pipelines, industries, life support systems, etc. These critical objects are prone to emergencies and undesired events that give rise to various threat sources initiation of regional security. Critical situations are complex developing processes, e.g. man-caused accidents, natural phenomena, social tension, economic crises, etc. Critical situations constitute and are accompanied by potential threats and risk of regional security. Critical facilities are mostly static objects of control, whereas critical situations are purely dynamic objects of risk management. At the same time, critical situations are not necessarily associated with specific critically important facilities, i.e. there may exist or occur design and beyond design critical situations. Thus, the nomenclature of critically important facilities and critical situations should be assigned and determined.

Critical infrastructures are in the wide sense defined as physical or virtual systems and assets that are so vitally to a country and region that partial or total violation and disruption of it resilient functioning would adversely affect the national security, economic development, defense, health or social well-being of population.

As an assessment of the safety level of critical facilities, it is possible to assume such a quantitative characteristic as the class of potential risk (hazard). Therein and below risk and hazard concepts are sub-

stantially synonymous. Hazard is considered as a threat in action or implementation of threat, where threat is a set of influencing factors and conditions which produce hazards. Three classes of potential risks are established: I, II, III. The first class is assigned to critical facilities and complex objects, where critical situations emerged lead to the most severe consequences, while the third class deals with critical situations of the least severe consequences. The second class occupies an intermediate place. Therefore, a nomenclature of consequences should be formed and established. Similarly, for critical situations the 1st, 2nd and 3rd hazard classes can be determined. Based on these indices it is possible to estimate overall indices of potential hazard classes and risk classes of critical situations for the region as a whole.

More detailed information on the hazard structure can be obtained by introducing the hazard fields into consideration. It is possible to distinguish the potential and actual hazard fields which are associated with critical facilities, critical situations and critical infrastructures respectively. The structure of the deterministic field is defined and formalized by the spatiotemporal hazard function:

$$R = R(X, Y, Z, t),$$

where R is a risk level at the point with coordinates X, Y, Z at time t.

The most general characteristic of a stochastic field is the risk distribution function:

$$F(r) = P\{R < r\}.$$

Discrete (e.g. the risk level can possess three values corresponding to the potential hazard classes) and continuous probability distributions can be considered. In any case, the probability of an event $\{r_1 < R < r_2\}$ can be formally defined using the Lebesgue-Stieltjes integral [24]:

$$P\{r_1 < R < r_2\} = \int_{r_1}^{r_2} dF(r).$$

For the average value of risk level the following expression is valid:

$$\overline{R} = \int_{-\infty}^{+\infty} r dF(r).$$

In practice, it is convenient to represent hazard fields in the form of "spots" or isolines plotted on the interactive map respectively equal the risk level, e.g. in the form of circles (in the simplest way) or in the other animated forms, and to control and analysis the dynamics of risk development. Thereto, the state-of-the-art geoinformation technologies (GIS) are widely used [25].

The concept of risk has a probabilistic interpretation and is defined as a probabilistic measure of some unfavorable events that generate a critical situation at the control object with expected losses (damages). Therefore, the concept of risk can be formally defined as the average (expected) value of the loss function of an object (system) in a critical situation:

$$R = \sum_{j=1}^{K} L_j \Pr_j(E_j),$$

where R is the risk value; E_j, $j = \overline{1, K}$, is the set of all elementary combinations of adverse events compiled on the basis of conditions, when the state variables of control object exceed the bounds of acceptable values (the limits of the normal operation mode of the object); $\Pr_j(E_j)$ – initiation probability of unfavorable events combination E_j, $0 \le \Pr_j(E_j) \le 1$; L_j – losses (damage) as a result of implementation of the adverse events combination.

Other formalization methods of the risk and security concepts in an analytical form are based on the formal apparatus of mathematical statistics, stability theory and sensitivity analysis.

One of the principal issues and problems in quantitative calculations and simulation of risk level is to determine the potential sources of negative influence, i.e. objects of hazard, and to answer the question: "the risk for whom or for what?". In this case, different interdisciplinary approaches based on foundations of the risk management and analysis, situational control theory, reliability and security theory and other

fields of knowledge can be well applied. It is worth mentioning the well-known sanitary-hygienic and environmental principles in the nuclear power outlined in [26-27] as a good example. Depending on the answer to the question posed, specific security systems or subsystems can be chosen and implemented. Such are the rather general foundations of the risk concept formalization in the context of support and ensuring the regional security.

Conclusion

As a result of the carried out study, the key approaches to system development for ensuring and support the regional security based on distributed situational centers deployment have been outlined. It is worth mention the complex character of this poorly-formalized multifaceted problem. To successful problem-solving joint efforts of theorists and practitioners in the field of risk analysis and security are required. In addition, the support at the public administration level and appropriate rule-making activities are required. In general, it is significant to state that from a methodological point of view the concept and foundations of security is gradually obtaining the same fundamental and universal character as for example the concepts and theory of information or entropy.

A conceptual model of the system for ensuring the regional security has been designed and a formalization of the security and risk concepts within the framework of this model has been proposed. The structure and composition of the decision support system for managing the regional security based on the use of situation simulation modeling aids has been developed and studied.

The contributions of this general research work have found application for risk management problem-solving of the security violation of regional critical infrastructures of Murmansk region in the context of mainstream implementation of the public policy of Russian Federation in the Arctic for the period up to 2035 on the basis of developing decision support systems for situational control and monitoring used in the regional management centers.

References

1. Huebert R. Understanding Arctic security: A defence of traditional security analysis. *Breaking Through: Understanding Sovereignty and Security in the Circumpolar Arctic*. Toronto: University of Toronto Press, 2021:80–96.
2. Sergunin A. Arctic security perspectives from Russia. *Routledge Handbook of Arctic Security*. London: Routledge, 2020:129–139.
3. 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. (In Russ.)
4. Shul'ts V.L., Kul'ba V.V., Shelkov A.B., Chernov I.V. *Stsenarnyy analiza v upravlenii geopoliticheskim informatsionnym protivoborstvom = Scenario analysis in the management of geopolitical information confrontation*. Moscow: Nauka, 2015:542. (In Russ.)
5. Gjørv G.H., Bazely D.R., Goloviznina M., Tanentzap A.J. *Environmental and human security in the Arctic*. Abindgon; New York: Routledge, 2013:312.
6. Tsygichko V.N., Chereshkin D.S., Smolyan G.L. *Bezopasnost' kriticheskikh infrastruktur = Safety of critical infrastructures*. Moscow: URSS, 2019:200. (In Russ.)
7. Dover R., Dylan H., Goodman M. *The Palgrave handbook of security, risk and intelligence.* Palgrave Macmillan UK, 2017:501.
8. Burkov V.N., Novikov D.A., Shchepkin A.V. Control Mechanisms for Ecological-Economic Systems. *Studies in Systems, Decision and Control*. 2015;10:166.
9. Severtsev N.A., Betskov A.V. *Modelirovanie bezopasnosti funktsionirovaniya dinamicheskikh system = Modeling the safety of functioning of dynamic systems*. Moscow: TEIS, 2015:327. (In Russ.)
10. Yurkov N.K. Security of complex technical systems. *Vestnik Penzenskogo gosudarstvennogo universiteta = Bulletin of the Penza State University*. 2013;(1):128–134. (In Russ.)
11. Ryabinin I.A. *Nadezhnost' i bezopasnost' slozhnykh system = Reliability and safety of complex systems*. Saint Petersburg: Politekhnika, 2000:248. (In Russ.)
12. Korotkov A.S., Turlova A.V., Kosov A.D., Orekhov A.A. Automated system for monitoring the radiation situation in the NPP location area as a safety tool. *Atomnaya energiya = Atomic energy*. 2018;125(1):38–43. (In Russ.)
13. Mel'nikov N.N. [et al.]. *Nauchnye osnovy sozdaniya podzemnykh kompleksov dlya razmeshcheniya atomnykh stantsiy maloy moshchnosti v usloviyakh Arktiki = Scientific foundations for the creation of underground complexes for the placement of low-power nuclear power plants in the Arctic*. Apatity: FITs KNTs RAN, 2020:304. (In Russ.)
14. Bezlepkin V.V., Semashko S.E., Frolov A.S. The NPP-2006 project: radiation impact on the environment. *Bezopasnost' okruzhayushchey sredy = Environmental safety*. 2009;(3):135–137. (In Russ.)

15. Yastrebenetskiy M.A. *Bezopasnost' atomnykh stantsiy. Sistemy upravleniya i zashchity yadernykh reaktorov = Safety of nuclear power plants. Control and protection systems of nuclear reactors*. Kiev: Osnova-Print, 2011:763.
16. *Normy radiatsionnoy bezopasnosti (NRB-99/2009). Sanitarno-epidemiologicheskie pravila i normativy = Radiation safety standards (NRB-99/2009). Sanitary and epidemiological rules and norms*. Moscow: Federal'nyy tsentr gigieny i epidemiologii Rospotrebnadzora, 2009:100. (In Russ.)
17. *Federal'nye normy i pravila v oblasti ispol'zovaniya atomnoy energii «Obshchie polozheniya obespecheniya bezopasnosti atomnykh stantsiy» (NP-001-15) = Federal norms and rules in the field of atomic energy use "General provisions for ensuring the safety of nuclear power plants" (NP-001-15).* Moscow: FBU NTTs YaRB, 2016:57. (In Russ.)
18. Mel'nikov N.N., Amosov P.V., Klimin S.G., Novozhilova N.V. *Ekologicheskie aspekty bezopasnosti podzemnoy atomnoy stantsii maloy moshchnosti v usloviyakh Arktiki = Environmental aspects of safety of a low-power underground nuclear power plant in the Arctic*. Yaroslavl: Printkhaus-Yaroslavl', 2018:170. (In Russ.)
19. Masloboev A.V. The concept of the Center for Advanced Research and security of the Arctic. *Arktika: ekologiya i ekonomika = Arctic: ecology and economics*. 2019;(2):129–143. (In Russ.)
20. Zatsarinnyy A.A., Suchkov A.P. *Informatsionnoe vzaimodeystvie v raspredelennykh sistemakh situatsionnogo upravleniya = Information interaction in distributed situational control systems*. Moscow: FITs IU RAN, 2021:256. (In Russ.)
21. Masloboev A.V. Regional management center framework for G2C-feedback and public safety support. *Reliability and quality of complex systems*. 2021;(4).
22. Ryzhenko A.A., Khabibulin R.Sh., Topol'skiy N.G., Bedilo M.V. *Adaptivnaya sistema podderzhki deyatel'nosti tsentrov upravleniya v krizisnykh situatsiyakh = Adaptive support system for the activity of control centers in crisis situations*. Moscow: Akademiya GPS MChS Rossii, 2014:151. (In Russ.)
23. Masloboev A.V. Conceptual foundations for the development of an intelligent information and control system for ensuring regional security of the Murmansk region. *Arktika: ekologiya i ekonomika = Arctic: ecology and economics*. 2017;(4):87–101. (In Russ.)
24. Tolstov G.P. *Mera i integral = Measure and integral*. Moscow: Nauka, 1976:392. (In Russ.)
25. Yakovlev S.Yu., Shemyakin A.S. Methods and software tools for information support of techno-sphere security of polar regions (on the example of the Murmansk region). *Istoriya nauki i tekhniki = History of Science and technology*. 2019;(4):46–54. (In Russ.)
26. *SP AS 03 Sanitarnye pravila proektirovaniya i ekspluatatsii atomnykh stantsiy = SP AS 03 Sanitary rules for the design and operation of nuclear power plants*. Moscow: FBU NTTs YaRB, 2003:36. (In Russ.)
27. Egorov Yu.A. Assessment of environmental safety and consequences of NPP operation in Russia. *Regional'naya ekologiya = Regional ecology*. 2006;(1–2):53–68. (In Russ.)

Список литературы

1. Huebert R. Understanding Arctic security: A defence of traditional security analysis // Breaking Through: Understanding Sovereignty and Security in the Circumpolar Arctic. Toronto : University of Toronto Press, 2021. P. 80–96.
2. Sergunin A. Arctic security perspectives from Russia // Routledge Handbook of Arctic Security. London : Routledge, 2020. P. 129–139.
3. Маслобоев А. В., Путилов В. А. Информационное измерение региональной безопасности в Арктике. Апатиты : КНЦ РАН, 2016. 222 с.
4. Шульц В. Л., Кульба В. В., Шелков А. Б., Чернов И. В. Сценарный анализа в управлении геополитическим информационным противоборством. М. : Наука, 2015. 542 с.
5. Gjørv G. H., Bazely D. R., Goloviznina M., Tanentzap A. J. Environmental and human security in the Arctic. Abindgon ; New York : Routledge, 2013. 312 p.
6. Цыгичко В. Н., Черешкин Д. С., Смолян Г. Л. Безопасность критических инфраструктур. М. : УРСС, 2019. 200 с.
7. Dover R., Dylan H., Goodman M. The Palgrave handbook of security, risk and intelligence. Palgrave Macmillan UK, 2017. 501 p.
8. Burkov V. N., Novikov D. A., Shchepkin A. V. Control Mechanisms for Ecological-Economic Systems // Studies in Systems, Decision and Control. 2015. Vol. 10. 166 p.
9. Северцев Н. А., Бецков А. В. Моделирование безопасности функционирования динамических систем. М. : ТЭИС, 2015. 327 с.
10. Юрков Н. К. Безопасность сложных технических систем // Вестник Пензенского государственного университета. 2013. № 1. С. 128–134.
11. Рябинин И. А. Надежность и безопасность сложных систем. СПб. : Политехника, 2000. 248 с.
12. Коротков А. С., Турлова А. В., Косов А. Д., Орехов А. А. Автоматизированная система контроля радиационной обстановки в районе размещения АЭС как инструмент обеспечения безопасности // Атомная энергия. 2018. Т. 125, № 1. С. 38–43.

13. Мельников Н. Н. [и др.]. Научные основы создания подземных комплексов для размещения атомных станций малой мощности в условиях Арктики. Апатиты : ФИЦ КНЦ РАН, 2020. 304 с.
14. Безлепкин В. В., Семашко С. Е., Фролов А. С. Проект «АЭС-2006»: радиационное воздействие на окружающую среду // Безопасность окружающей среды. 2009. № 3. С. 135–137.
15. Ястребенецкий М. А. Безопасность атомных станций. Системы управления и защиты ядерных реакторов. Киев : Основа-Принт, 2011. 763 с.
16. Нормы радиационной безопасности (НРБ-99/2009). Санитарно-эпидемиологические правила и нормативы. М. : Федеральный центр гигиены и эпидемиологии Роспотребнадзора, 2009. 100 с.
17. Федеральные нормы и правила в области использования атомной энергии «Общие положения обеспечения безопасности атомных станций» (НП-001-15). М. : ФБУ НТЦ ЯРБ, 2016. 57 с.
18. Мельников Н. Н., Амосов П. В., Климин С. Г., Новожилова Н. В. Экологические аспекты безопасности подземной атомной станции малой мощности в условиях Арктики. Ярославль : Принтхаус-Ярославль, 2018. 170 с.
19. Маслобоев А. В. Концепция Центра перспективных исследований и обеспечения безопасности Арктики // Арктика: экология и экономика. 2019. № 2. С. 129–143.
20. Зацаринный А. А., Сучков А. П. Информационное взаимодействие в распределенных системах ситуационного управления. М. : ФИЦ ИУ РАН, 2021. 256 с.
21. Masloboev A. V. Regional management center framework for G2C-feedback and public safety support // Reliability and quality of complex systems. 2021. № 4.
22. Рыженко А. А., Хабибулин Р. Ш., Топольский Н. Г., Бедило М. В. Адаптивная система поддержки деятельности центров управления в кризисных ситуациях. М. : Академия ГПС МЧС России, 2014. 151 с.
23. Маслобоев А. В. Концептуальные основы разработки интеллектуальной информационно-управляющей системы обеспечения региональной безопасности Мурманской области // Арктика: экология и экономика. 2017. № 4. С. 87–101.
24. Толстов Г. П. Мера и интеграл. М. : Наука, 1976. 392 с.
25. Яковлев С. Ю., Шемякин А. С. Методы и программные средства информационного обеспечения техносферной безопасности полярных регионов (на примере Мурманской области) // История науки и техники. 2019. № 4. С. 46–54.
26. СП АС 03 Санитарные правила проектирования и эксплуатации атомных станций. М.: ФБУ НТЦ ЯРБ, 2003. 36 с.
27. Егоров Ю. А. Оценка экологической безопасности и последствий эксплуатации АЭС в России // Региональная экология. 2006. № 1–2. С. 53–68.

Информация об авторах / Information about the authors

Андрей Владимирович Маслобоев
доктор технических наук, доцент,
ведущий научный сотрудник,
Институт информатики и математического
моделирования технологических процессов
Кольского научного центра Российской академии наук
(Россия, Апатиты, ул. Ферсмана, 24А)
E-mail: masloboev@iimm.ru

Andrey V. Masloboev
Doctor of technical sciences, associate professor,
leading researcher,
Institute of Informatics and Mathematical Modelling
of Technological Processes of Kola Science Centre
of the Russian Academy of Sciences
(24A Fersmana street, Apatity, Russia)

Авторы заявляют об отсутствии конфликта интересов /
The authors declare no conflicts of interests.

Поступила в редакцию/Received 20.06.2021
Поступила после рецензирования/Revised 10.09.2021
Принята к публикации/Accepted 25.10.2021