Вычислительные технологии, 2022, том 27, № 6, с. 115–123. © ФИЦ ИВТ, 2022 ISSN 1560-7534
Computational Technologies, 2022, vol. 27, no. 6, pp. 115–123. © FRC ICT, 2022 eISSN 2313-691X



DOI:10.25743/ICT.2022.27.6.010

# Information system of territorial risk assessment

V. V. Moskvichev[1,2], V. V. Nicheporchuk[3], U. S. Postnikova[1,2], O. V. Taseiko[1,4,*]
[1]Federal Research Center for Information and Computational Technologies, 660049, Krasnoyarsk, Russia
[2]Siberian Federal University, 660041, Krasnoyarsk, Russia
[3]Institute of Computational Modelling SB RAS, 660049, Krasnoyarsk, Russia
[4]Reshetnev Siberian State University of Science and Technology, 660037, Krasnoyarsk, Russia
[*]Corresponding author: Taseiko Olga V., e-mail: taseiko@gmail.com
*Received September 27, 2022, accepted October 05, 2022.*

The paper presents the process of creating an intelligent system designed to assess and manage risks. The risk can be anthropogenic, natural, or social in nature, and relate to different territorial groups. The complexity of structuring and collecting information on the state territorial security as well as various risk assessment methods, necessitates the development of a modular multitask system. The information management system support model formalizes the problem area to justify the joint use of innovation technologies. Based on the model, system architecture has been developed. This architecture defines the composition, functionality, interaction interfaces, and organization of information resources, that were used to support management. The operation results of the system prototype is presented.

*Keywords:* information system, territorial security, risk assessment.

*Citation*: Moskvichev V.V., Nicheporchuk V.V., Postnikova U.S., Taseiko O.V. Information system of territorial risk assessment. Computational Technologies. 2022; 27(6):115–123. DOI:10.25743/ICT.2022.27.6.010.

## Introduction

Maintaining the territorial safety is a challenging task, especially when the economy is under pressure. However, existing technologies readily provide an opportunity to implement low-cost measures allowing to manage social, natural, and technogenic risks. It is important to study various territorial characteristics, treating them as complex systems, in order to find and justify these measures. One of the most theoretically well-supported concepts is the idea of the territory as a complex socio-natural-technogenic system (S-N-T system) where multiple risk groups are formed and implemented [1]. The construction of an intelligent risk assessment system should be based on formalizing a sufficient number of socio-economic and natural-climatic indicators, integrated assessment algorithms, data processing and visualization, and the coordination of systemic and external services.

Various methods are used to classify risks, one of them is a sociological survey with the aim of establishing acceptable risks levels [2], analysis systems (NETworked) and management systems (NET-HARMS) developed on them are able to identify and predict systemic and emerging hazards.

To control territories in the EU countries, the concept of “smart city” or “smart territory” based on the criteria for sustainable and effective development is actively being developed. This concept covers various spheres of life: energy, transport infrastructure, resource consumption, environmental impact, etc. It requires a detailed analysis and diagnosis of the territory and key indicators to create such a system [3]. The concept of a “smart city” has a strong theoretical foundation; however, in reality it works only in isolation, and does not consider any risks thereby losing the most of its value.

The results obtained by the researches [4–6] prove the necessity of data integration, taken from incidents and formalized industrial safety indicators. Public safety requirements have became more strict recently, especially in consideration of global events and trends related to climate change, digitalization of private data, as well as constant growth and development of technical systems and industry. However, periodically occurring disasters show the failure of efforts to prevent them, alongside with the necessity to consolidate large monitoring data and utilization of intelligent technologies to search for a new knowledge [6–8].

This work proposes the “end-to-end” technology creation for designing and building an intellectual system responsible for assessing territorial risks. The architecture basis is a system model of information support for territorial risk management. The presented architecture allows creating multi-tasking problem-oriented systems, which pilot projects are implemented for the Siberian region.

## 1. Digital territory safety passport

A digital portrait of the territory’s security is the ordered hierarchical indicators obtained by processing monitoring data and used to assess the S-N-T system’s risks, justifying acceptable levels of risks and planning measures for different urgency to reduce them.

The list of risk indicators that are characteristic for the territory as a complex socio-natural-technogenic system is advisable to present as a hierarchy. At the top level, the hierarchy is divided into background and emergency risks. The next level contains directly the names of indicators. Russian classifier of emergency situations, atlas of dangers and risks, and other sources have been used in its formation. Level 3 shows the attribution of the risk’s factors contribution to the hazard, vulnerability and territories protection. At the same level “risks manifestations” are located — quantitative values of indicators obtained from statistical data on events. In the absence of statistics of hazardous events, model calculations are used. At the lowest level of the hierarchy, information resources are placed as input data for calculation, analytical, simulation models. Conventionally, they are divided into the following categories:

– regular monitoring data;
– results of sampling and periodic sampling;
– reporting data collected as a part of the daily activities of territorial government bodies;
– spatial modelling results;
– the results of situational modelling consequences, causes of emergencies, hazards and the consequences of the implementation of preventive measures.

The hierarchy is built taking into account the security features of the Siberian territories. It contains several hundred elements. Figure 1 shows a fragment of the hierarchy.

Table shows examples of information resources that are used to assess territorial risks. A similar set is used in other tasks of territorial security management: for early detection of


Fig. 1. Composition of the indicator "Risk of fires"

Baseline data for risk assessment

| Risk indicator | Group | Data source |
|---|---|---|
| Instrument monitoring | | |
| Flooding | Danger | Hydrological monitoring |
| Radioactive contamination | Manifestation | |
| Earthquakes | Manifestation | Monitoring of ionizing radiation |
| Periodic tests, monitoring | | |
| Surface water quality | Manifestation | Monitoring of the Rospotrebnadzor |
| Electromagnetic emission | Manifestation | Monitoring of the Rospotrebnadzor |
| Inundations | Danger | Pre-flood surveys |
| Reporting | | |
| Morbidity | Manifestation | Medical statistics |
| Road accidents | Manifestation | Traffic police statistics |
| Accidents in life support systems | Manifestation | EMERCOM of Russia event catalog |
| Fires | Manifestation | EMERCOM of Russia event catalog |
| Spatial data | | |
| Ecological system | Danger | The risk Atlas |
| Wildfire | Vulnerability | The risk Atlas |
| Crime | Degree of protection | The risk Atlas |

emergency and hazardous emergencies, in decision-making processes for emergency response, and also to justify the new monitoring systems creation.

## 2. Model of information support management

The result of the first stage of building a system is a management support system model $M$ that formalizes the basic requirements, composition and elements interaction in the form [9]:

$$M =< G, T, L, F, C, IT, Y >,$$

where $G$ — management objectives; $T$ — control tasks; $L$ — decision levels; $F$ — system functions; $C$ — containers integrating information resources, their processing methods and characteristics for each type of risk; $IT$ — information technologies, $Y$ — formed decisions. The listed elements of the model are detailed as sets.

Management goals set $G = \{g_1, g_2, g_3\}$ include: $g_1$ — increase life expectancy by reducing the number of dead and deceased prematurely; $g_2$ — increase in the healthy life duration by reducing the number of people who need treatment, rehabilitation and social protection; $g_3$ — creation of comfortable living environment, including the environment normalization and uninterrupted resources supply. All management goals have a multiplier effect — financial investments in preventive measures are significantly less than the cost of unprevented harm [10]. Tasks set $T = \{t_1, t_2, t_3\}$ are grouped by their implementation frequency and include the following: $t_1$ — the risk of reduction measures that are performed continuously; $t_2$ — seasonal preventive measures specific cyclical emergencies, environmental, anti-epidemic and other measures; $t_3$ — single-time events that radically reduce the level of risk. Strategic decisions on the territorial security management that require collection and processing large amounts of data are made at the regional level $l_1$. Municipal $l_2$ and objective $l_3$ levels have limited functions when it comes to collecting and viewing data. Such a division is reflected in the intelligent system architecture which provides different human-machine interfaces. The set of functions $F = \{f_1, f_2, f_3, f_4\}$, where $f_1$ is the collection and consolidation of data; $f_2$ — analytical data processing and calculations; $f_3$ — dynamic visualization of results; $f_4$ — decisions making.

Containers in an intelligent system are presented as pairs $C = \{D, A\}$, where $D$ — information resources, $A$ — methods and algorithms that process and present data using information technologies $IT$ [11–13]. In its turn, $IT = \{it_1, \ldots, it_5\}$, where $it_1$ — data warehouse technologies; $it_2$ — analytical data processing technologies; $it_3$ — intelligent technologies; $it_4$ — geoinformation technologies; $it_5$ — web technologies. Information resources $D = \{d_1, \ldots, d_5\}$, where $d_1$ — system-forming elements (reference books, classifiers); $d_2$ — monitoring processes (events) data; $d_3$ — analyzed objects characteristics; $d_4$ — spatial data; $d_5$ — knowledge bases. The typical structure of $D$ elements is developed using UML notations. Based on the structure of information resources description, the intellectual system data warehouse was designed and filled with data. The intelligent system results largely depend on the volume and content of the data, which is different for different territories. The output can be represented as $Y = \{B, H, Q, K\}$, where $B$ — text recommendations and explanations; $H$ — tables; $Q$ — graphical representations; $K$ — dynamic maps visualizing the territorial risks distribution. For a better understanding, $B$ includes the extensive terminology used in risks assessment [14, 15].

Integrating these technologies in control systems allows synthesizing solutions that coordinate the actions of experts from various departments involved in the targeted risk reduction programs development. Updated information resources increase the decision effectiveness when it comes to working with time constraints, in case of incomplete and obscure initial information, and the high costs of error.

Elements from the sets of this system model can be supplemented by the new data processing technologies advent, information resources types, as well as territorial management tasks.

## 3. A conceptual description of the architecture of an intelligent system

The next step in the system implementation is architectural design, linking the system model elements, and the information processes decomposition of the system's interaction with the external environment, and the program modules functioning within the system.

The multitasking problem-oriented intelligent system architecture is based on the system management model. Figure 2 shows context diagram of the system interacting with the

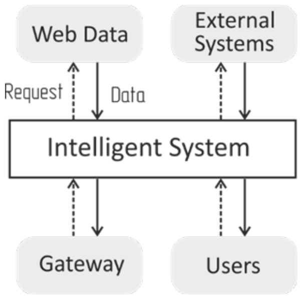


Fig. 2. Context diagram of an intelligent system

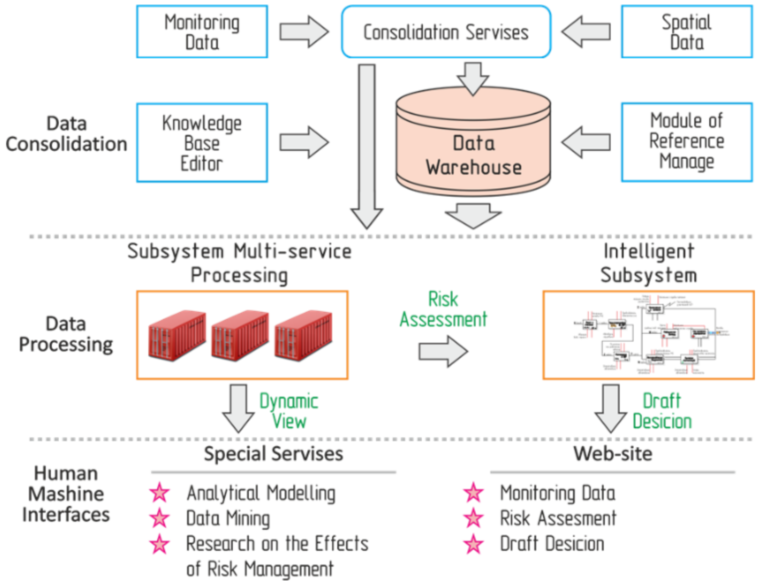


Fig. 3. The architecture of an information system

environment. This configuration allows getting results when performing various combinations of functions $F$. For example, $f_1$ data collection results and consolidation are available to other systems through a data gateway. Performing risk assessments (functions $f_2$, $f_3$) without forming solutions $f_4$ is advisable in case of information resources deficiency.

Using the control support model elements, control tasks $T$ were decomposed as functional diagrams. This allowed describing in detail the transformation processes of information resources using $IT$. The architecture concretizes the intelligent system design describing a unit of consolidating information resources, subsystems and data processing services, and human-machine interfaces (Fig. 3).

Consolidation processes are described in accordance with the classification of information resources and information technologies introduced in the system model. The use of system-forming resources $d_1$ to enrich monitoring data during the consolidation process in the repository made it possible to implement various analytical processing technologies, such as POD (post OLAP dynamics), Data Mining, and others [16, 17]. The main information resources array used for assessing territorial risks is data from monitoring processes and events $d_2$, as well as analyzed objects $d_3$ characteristics. The basic spatial data $d_4$ is used for the formation of cartograms and overview maps is placed in the repository. Detailed cartographic territorial descriptions are available through WMS and other services described in [18]. To collect formalized management processes in $d_5$ knowledge bases, a graphical method proposed for displaying a sequence of "elementary" operations, similar to IDEFx notation.

Due to significant differences in the data structure, processing and presentation result methods, it is advisable to integrate them for each risk type by the type of container processing. The growth of intellectualization system is possible with the mass knowledge bases formation that describes the preventive measures management processes. A graphical interface is being developed to transform formalized descriptions of multi-step actions. The large training sample formation makes it possible to use neural networks and other intelligent technologies. This allows creating several alternative solutions with ranking them by priority.

Human-machine interfaces are designed taking into account different decision-making levels $L$. Different dynamic representations of the processing results (elements of the set $Y$) allow avoiding the reduction of risk assessments as a single numerical indicator. The support includes various access mechanisms for individuals who form and make managerial decisions — desktop software systems, websites, and mobile applications.

The developed architecture made it possible to determine the synthesized intelligent system functionality and substantiate the software components and rational methods choice for the integrated control problems solution.

## 4. Assessment of territorial risks in the intelligent system

The functioning of man-made systems, natural complexes and processes, the territorial formations development is accompanied by the implementation of various types and risk groups. These risks need to be purposefully identified and take the necessary measures to protect and mitigate the consequences in the event of a hazard. Table present groups of basic risks for element of the system technosphere [18–20]. The territory of an industrial region is a single complex system. The system elements have a mutual influence on each other and are characterized by different components of risks. The sociosphere is characterized by individual, social and material risks. The technosphere is defined by the risks of emergencies and accidents, the technical risk and reliability, and the economic component. The ecosphere is characterized by risks of acceptable anthropogenic impact, ecosystem vulnerability, and material damage.

Detailed consideration of the sociosphere, technosphere and ecosphere leads to the tasks related to the classification of risk assessment models. The classification of risk assessment models is shown in Fig. 4. The mathematical approaches used in the variety of regulatory and methodological documents on risk assessment have a common basis. Risk assessment models are classified according to the source of occurrence, object of impact, and purpose.

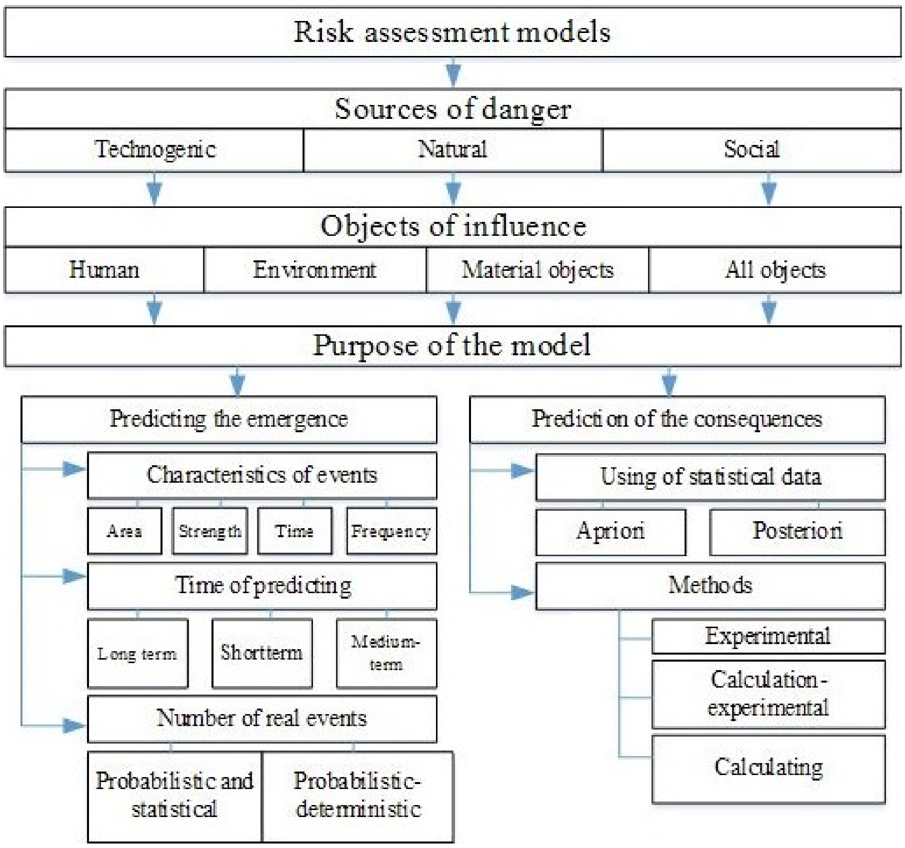


Fig. 4. Classifying of risk models

To assess territorial risks, it is proposed to collect and analyze monitoring data and statistics on emergencies and dangerous events, including industrial safety violations, public health, and environmental monitoring data. The specifies of the proposed approach difference is in using formalized characteristics of the danger sources, objects' vulnerability, and the state of protection systems [21].

The territorial risks assessment takes place in three main stages:
– definition and formation of a source data array;
– risks calculations and analytical modelling;
– analysis results dynamic presentation, including risks mapping.

During the first stage, there possible dangers are determined for the territories, initial data, general target information and models for the analytical risks study are formed. When performing the second stage, it is necessary to divide the risks into two fundamental groups, characterized by the exposure duration (instant and long-term effect). At the third stage, recommendations are developed for risk management at the municipal level.

The risk calculation is carried out in order to determine the necessity and effectiveness of preventive measures, as well as measures to manage the municipality's developmental risks by executive authorities.

## Conclusion

The architecture's basic functions are implemented in the integrated management support systems “ESLA-PRO” and the Risk Analysis System SAR ES. Operational experience has shown the necessity to improve intersystem information exchange using distributed ledger technologies, cloud data storage, consolidating information from industry systems. Also updated regional atlases of emergency situations covering natural and anthropogenic natures have been created, some of them are published on the INM SB RAS [22] geographic informational portal.

The proposed creation method of an intelligent system for assessing and managing social, natural and anthropogenic systems' risks allows building up a comprehensive information platform for solving a wide range of territorial management tasks. The method is based on the management information support model and the intelligent system architecture that substantiate the original integration of information resources and technologies. The combination of an intelligent system with integrated monitoring services will systematically reduce the human and social life risks, as well as the ecological systems' state to acceptable levels that are currently achieved in only a small number of countries [22].

**Acknowledgments.** This research project No. 18-47-240006 “Methods and information technologies for risk assessment of the development of socio-natural-technogenic systems in an industrial region” was funded by the Russian Foundation for Basic Research, Government of Krasnoyarsk Territory, Krasnoyarsk Regional Fund of Science.

## References

[1] **Dallat C., Salmon P., Goode N.** Identifying risks and emergent risks across sociotechnical systems: the NETworked hazard analysis and risk management system (NET-HARMS). Theoretical Issues in Ergonomics Science. 2018; 19(4):456–482. DOI:10.1080/1463922X.2017.1381197. Available at: `https://www.tandfonline.com/doi/abs/10.1080/1463922X.2017.1381197?journalCode=ttie20`.

[2] **Neirotti P., Marco A., Cagliano A.C., Scorrano F.** Current trends in Smart City initiatives: some stylised facts. Cities. 2014; (38):25–36. DOI:10.1016/j.cities.2013.12.010. Available at: `https://www.sciencedirect.com/science/article/abs/pii/S0264275113001935`.

[3] **Scheer D.** Risk governance and emerging technologies: learning from case study Integration. Journal of Risk Research. 2013; (3–4):355–368. DOI:10.1080/13669877.2012.729519. Available at: `https://www.tandfonline.com/doi/abs/10.1080/13669877.2012.729519`.

[4] **Knijff P., Allford L., Schmelzer P.** Process safety leading indicators — a perspective from Europe. Process Safety Management — Improving Performance. 2013; 32(4):332–336. DOI:10.1002/prs.11641. Available at: `https://aiche.onlinelibrary.wiley.com/doi/10.1002/prs.11641`.

[5] **Leveson N.** A systems approach to risk management through leading safety indicators. Reliability Engineering and System Safety. 2015; (136):17–34. DOI:10.1016/j.ress.2014.10.008. Available at: `http://sunnyday.mit.edu/leadingindicators-published.pdf`.

[6] **Oien K., Utne I.B., Tinmannsvik R.K., Massaiu S.** Building safety indicators: part 2 — application, practices and results. Safety Science. 2011; 49(2):162–171. Available at: `https://trid.trb.org/view/1083888`.

[7] **Goodfellow I., Bengio Y., Courville A.** Deep learning. London: MIT Press; 2016: 653.

[8] **Kossiakoff A., Sweet W.N., Seymor S.J., Biemer S.M.** System engineering principles and practice. New Jersey: Wiley; 2011: 624.

[9] **Malinetskii G.G., Podlazov A.V., Kuznetsov I.V.** On a national scientific monitoring system. Herald of the Russian Academy of Sciences. 2005; 75(4):323–336. Available at: `https://www.elibrary.ru/item.asp?id=9133358`.

[10] **Negus C., Henry W.** Docker containers. Build and deploy with Kubernetes, Flannel, Cockpit, and Atomic. London: Pearson Education; 2015: 319.

[11] **Mouat A.** Using Docker: developing and deploying software with containers. Sebastopol: O'Reilly Media; 2015: 328.

[12] **Nozhenkova L.F.** Information management systems in the territorial and corporate management. Journal of Computational Technologies. 2013; 18(1):52–59. Available at: `https://www.elibrary.ru/item.asp?id=22575114`.

[13] ISO 22300:2021 Security and resilience — vocabulary. Available at: `https://www.iso.org/ru/standard/77008.html`.

[14] PreventionWeb. The knowlege platform for disaster risk reduction. Available at: `www.preventionweb.net/Terminology`.

[15] **Zaki M.J., Wagner M.J.** Data mining and machine learning fundamental concepts and algorithms. Cambridge: Cambridge University Press; 2020: 760.

[16] **Penkova T.G., Korobko A.V., Nicheporchuk V.V., Nozhenkova L.F.** On-line control of the state of technosphere and environment objects in Krasnoyarsk region based on monitoring data. International Journal of Knowledge-Based and Intelligent Engineering Systems. 2016; 20(2):65–74. DOI:10.3233/KES-160330. Available at: `https://www.elibrary.ru/item.asp?id=27075197`.

[17] **Bychkov I.V., Vladimirov D.Ya., Oparin V.N., Potapov V.P., Shokin Yu.I.** Mining information science and Big Data concept for integrated safety monitoring in subsoil management. Journal of Mining Science. 2016; 52(6):1195–1209. DOI:10.1134/S1062739116061747. Available at: `https://www.elibrary.ru/item.asp?id=31142560`.

[18] **Ivanova U.S., Taseiko O.V., Chernykh D.A.** Probabilistic methods for risk assessment of anthropogenic accidents and emergency. Procedia Structural Integrity. 2019: 136–142. DOI:10.1016/j.prostr.2019.12.129. Available at: `https://www.elibrary.ru/item.asp?id=43253864`.

[19] **Ivanova U.S., Moskvichev V.V., Taseiko O.V.** Classifying of Krasnoyarsk territory using a risk-based approach. Issues of Risk Analysis. 2019; 16(4):48–63. DOI:10.32686/1812-5220-2019-16-4-48-63. Available at: `https://www.elibrary.ru/item.asp?id=39239488`.

[20] **Penkova T., Nicheporchuk V. Metus A.** Comprehensive operational control of the natural and anthropogenic territory safety based on analytical indicators. Lecture Notes in Computer Science. 2017; (10313):263–270. DOI:10.1007/978-3-319-60837-2_22. Available at: `https://www.elibrary.ru/item.asp?id=31044573`.

[21] Geoportal of ICM SB RAS. Available at: `https://gis.krasn.ru/blog`.

[22] DRMKC-INFORM. Country risk profile. Available at: `https://drmkc.jrc.ec.europa.eu/inform-index/INFORM-Risk/Country-Risk-Profile`.

Вычислительные технологии, 2022, том 27, № 6, с. 115–123. © ФИЦ ИВТ, 2022 ISSN 1560-7534
Computational Technologies, 2022, vol. 27, no. 6, pp. 115–123. © FRC ICT, 2022 eISSN 2313-691X

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

DOI:10.25743/ICT.2022.27.6.010

**Информационная система оценки территориального риска**

В. В. Москвичев[1,2], В. В. Ничепорчук[3], У. С. Постникова[1,2], О. В. Тасейко[1,4,*]

[1]Федеральный исследовательский центр информационных и вычислительных технологий, 660049, Красноярск, Россия

[2]Сибирский федеральный университет, 660041, Красноярск, Россия

[3]Институт вычислительного моделирования СО РАН, 660049, Красноярск, Россия

[4]Сибирский государственный университет науки и технологий им. акад. М.Ф. Решетнева, 660037, Красноярск, Россия

[*]Контактный автор: Тасейко Ольга В., e-mail: `taseiko@gmail.com`

*Поступила 27 сентября 2022 г., принята в печать 05 октября 2022 г.*

**Аннотация**

В работе представлен процесс создания интеллектуальной системы, предназначенной для оценки и управления рисками. Риск может иметь антропогенный, природный или социальный характер и относиться к различным территориальным группам. Сложность структурирования и сбора информации о государственной территориальной безопасности, а также различные методы оценки рисков обусловливают необходимость разработки модульной многозадачной системы. Модель поддержки системы управления информацией формализует проблемную область для обоснования совместного использования инновационных технологий. На основе модели разработана архитектура системы. Эта архитектура определяет состав, функциональные возможности, интерфейсы взаимодействия, а также организацию информационных ресурсов, которые использовались для поддержки управления. Здесь представлен результат работы прототипа информационной системы.

*Ключевые слова*: информационная система, территориальная безопасность, оценка рисков.

*Цитирование*: Москвичев В.В., Ничепорчук В.В., Постникова У.С., Тасейко О.В. Информационная система оценки территориального риска. Вычислительные технологии. 2022; 27(6):115–123. DOI:10.25743/ICT.2022.27.6.010. (на английском)

**Благодарности.** Проект № 18-47-240006 “Методы и информационные технологии оценки риска развития социоприродно-техногенных систем в промышленном регионе” выполнен при финансовой поддержке РФФИ, Правительства Красноярского края, Красноярского краевого фонда науки.