Software and hardware complex for ensuring natural and technological safety in the digital ecosystem of the Smart City

A V Ginsburg1, S A Kachanov2, S N Nekhoroshev2 and A P Popov3

1 Moscow State University of Civil Engineering, 26, Yaroslavskoye Highway, Moscow, 129337, Russia
2 Federal State Budget Establishment All-Russian R&D Institute for Civil Defense and Emergencies, 7, Davydkovskaya street, Moscow, 121352, Russia
3 Joint Stock Company “Navigation and Information Systems”, 10-1, March 8 street, Moscow, 127083, Russia

E-mail: ginav@mgsu.ru

Abstract. The article considers the issues of building the software and hardware complex for ensuring natural and technological safety within the framework of the implementation of the Smart City digitalization project for the city economy. The purpose of the article is to show the role and place of the complex in the general ecosystem of the city governance. It is concluded that it is necessary to use a regional digital platform for life safety in the Smart City ecosystem that provides information and software pairing of interacting federal, regional, municipal and object information systems, consolidates their information resources, prompt and effective analytical processing of the consolidated information and provides it to interested users on a one-stop basis.

1. Introduction
The sustainability of the socio-economic development in any country is determined by the state of its national security, that is, the state’s ability to effectively counter the emerging challenges and threats.

One of the 17 strategic goals of the UN in the field of sustainable development is the goal of “Sustainable cities and towns.”

In 2012, within the framework of the thematic block “Sustainable Urban Development”, the UN Economic Commission for Europe formed a new direction “smart sustainable city”, which came to the description “… an innovative city that uses information and communication technologies as well as other means to improve the living standards, efficiency activities and services in the cities, as well as competitiveness, while ensuring the satisfaction of the needs of the present and future generations in economic, social, cultural and environmental aspects…” [1].

Thus, ensuring the required level of public life safety (including natural and technological safety) is considered as a necessary condition for building a “smart city”.

Analysts at Navigant Research believe that the integration of smart city services is inevitable and necessary as well as their central coordination [2].

According to them, the city administrations need to use a platform strategy based on the principles of openness, standardization and consistency with other technologies (interoperability).
However, in the scientific and technical literature there is still no clear understanding of the role and place of the Russian information systems and technologies for ensuring natural and technological safety in the processes of digital transformation of the urban economy in the Russian Federation.

2. Materials and methods

In the framework of the preparation of this article, the analysis of regulatory legal support on the issues of ensuring life safety in force in the Russian Federation, the current state of domestic information systems and technologies in these areas of activity, as well as the prospects for their further improvement and development was performed.

In the “Strategy for the scientific and technological development of the Russian Federation”, approved by the Decree of the President of the Russian Federation dated December 1, 2016 No. 642, of the seven major challenges identified in it, six are directly related to life safety, and the priority area of scientific and technological development is called “... countering technogenic, biogenic, sociocultural threats, terrorism and ideological extremism...”.

As the analysis of the existing regulatory legal acts [3–7] shows, ensuring security in the Russian Federation (including in urban districts and urban settlements) is, first of all, the full powers of the state authorities. At the same time, one of the National Security Strategy directions approved by the Decree of the President of the Russian Federation at the end of 2015, was also called “... improving the effectiveness of the implementation of the local authorities’ full powers in the field of ensuring the safety of the population”.

At the same time, the key direction of increasing the efficiency of state and municipal management is its informatization. In this regard, the list of the main tasks of the Government Commission on Digital Development, approved by the Decree of the Government of the Russian Federation of September 7, 2018 No. 1065, includes “... ensuring the safety of life through the active implementation of information technologies...”.

In the Forecast of scientific and technological development of the Russian Federation for the period up to 2030 (hereinafter referred to as the Long-Term Forecast), approved by the Government of the Russian Federation of January 20, 2014 №. DM-P8-5, in relation to the critical technology for the prevention and elimination of emergency situations (hereinafter - ES) lists the following promising markets and product groups:

- the systems for the early detection and prediction of natural and man-made emergencies: the systems for the early detection of conditions conducive to the formation of natural and man-made emergencies; the methods for predicting natural and man-made disasters and their consequences based on observational data and modern ideas about the processes of their preparation and development;
- the cadasters of territories and water areas with the highest level of natural and technological risk;
- the geographic information systems: specialized packages for processing the Earth remote sensing data; web services (geoportals) working on-line;
- the databases on the state of the environment: a geo-information database of online data on forest fires, floods, leaks of hazardous substances, etc., which allows real-time assessment of the number, scale and speed of the spread of disasters; natural and man-made disaster databases;
- the emergency risk management techniques: methods for assessing and reducing the risk of losses for people, territories and infrastructure from industrial disasters and natural disasters and developing measures to reduce damage from them;
- the emergency forecasting services;
- the services on information and analytical support for environmental protection and environmental safety, etc.

In accordance with the Long-Term Forecast, the most significant scientific results that can be achieved before 2030 include the creation of monitoring, assessment and forecasting systems for the environment, natural and man-made emergencies, and research and development will be actively
carried out in the medium term in the field of software and geographic information systems, early detection and forecasting of emergencies.

As noted in the Strategy for the information technology industry development in the Russian Federation for 2014-2020 and for the long term until 2025, approved by the Government order of the Russian Federation of November 1, 2013 No. 2036-r (hereinafter referred to as the Strategy), the main points of growth for the software development segment “cloud” technologies, technologies for processing large amounts of data and applications for mobile devices will become in the coming years.

Regarding the fundamental and exploratory research in the field of information technology, the Strategy proposes to focus on several major breakthrough areas for the global industry, in which in the future 10-15 years Russia’s global technological competitiveness can be ensured with high probability. These included “big data processing” and “security in the information society” [8].

In terms of the applied research and development that determine the direction of technological development in the field of information technology, the Strategy indicates those areas with the development of which it is possible to increase the competitiveness of the Russian information technology industry in a relatively short term, in particular:

- new search and recognition systems, including the solutions for search and recognition in audio and video materials, the use of semantics (meaning) when searching and extracting information;
- analysis of large data arrays and the extraction of knowledge, including the new methods and algorithms for collecting, storing and intellectual analysis of large volumes of data (including computational linguistics), new methods and software for the distributed processing of big data;
- information security technologies, including the new applications and infrastructure solutions to increase the security in computer networks (including the prevention of cyber threats and data protection in cloud and distributed computing environments);
- “cloud” computing, including the new technological elements of the network data transmission infrastructure, new integrated sensors and sensor networks, as well as the new elements of infrastructure and software for implementing various models for providing the “cloud” services;
- development of communication and navigation technologies, including the new ways to improve the efficiency of the existing communications (including wireless and optical), as well as new types of geographic information and navigation systems, etc.

For the government bodies and state organizations, the most popular mass consumption services are supposed to be placed in the national “cloud” environment, taking care of taking sufficient security measures while maintaining ergonomics of use.

This trend will be supported by a qualitative and quantitative increase in threats and consumer awareness of information security issues, strengthening the requirements of the legislation of the Russian Federation and industry standards.

It is also noted that the development of data centers in Russia will help to create the conditions for the circulation of information within the country, reducing the possibility of its unauthorized use.

At the same time, one of the basic principles of the information technology industry development for 2014 - 2020 and a perspective until 2025 in the Strategy is called “… orientation on public-private partnership in solving problems of developing the information technology industry”, and one of the main tasks is “… the development information processing and storage centers”.

On August 1, 2018, the first meeting of the Council for the Development of the Digital Economy under the Council of the Federation was held in the Kaliningrad Region, at which the prevailing “patchwork” nature of the informatization processes of public administration and local self-government, the fragmentation of the created federal, regional and municipal information systems were noted.

This can be fully applied to life safety systems.

Over the past two decades, in the territories of the constituent entities of the Russian Federation, a significant number of poorly integrated automated systems (hereinafter - AS) have been created and developed to provide protection against crisis and emergency situations (hereinafter – C&ES).
The Concept of Regional Informatization, approved by the Government order of the Russian Federation dated December 29, 2014 No. 2769-r, says that “... it is advisable to ensure the introduction of the information systems “112” and “ERA-GLONASS”, the all-Russian integrated information system and warning of the population in the places of mass people presence, the integrated video surveillance systems, access the control systems for hazardous facilities, the use of technical safety equipment, including in the field of environmental protection iCal, seismic and other types of control, life support systems, automation of monitoring and crisis prevention, and other information systems in the areas of health and safety...”.

3. Results and discussion

The systems operating in the areas of life safety, in addition to pairing with each other, must also interact with the automated systems in other areas of state and municipal government, since it is in them that the basic information about the objects of protection (transport, energy, utilities, social, etc.) is formed [9-12].

The current situation is usually characterized:

- software and information-linguistic incompatibility of the AS used;
- lack of uniform algorithms and information exchange tools;
- limited informational, computational and intellectual capabilities for processing heterogeneous information;
- repeated duplication of data on the same objects and events (due to non-compliance with the principles of single entry of information in various databases and systems);
- lack of a single high-performance telecommunication system combining various speakers;
- the presence of heterogeneous information exchange protocols and communication channels;
- lack of unified information protection tools.

The heterogeneity and independence of all these systems impede interagency and inter-level interaction, reduce the efficiency of the joint coordinated use of such AS in the process of managing the measures to prevent and eliminate the negative consequences of C&ES (anti-crisis management) and, ultimately, increase the time and reduce the effectiveness of response to crisis and emergency situations [13-15].

As a result, the prevailing “digital feudalism” does not lead to a decrease in the level of possible negative socio-economic and political consequences of the C&ES expected by the state authorities and local authorities from the informatization of the crisis management processes [16-17].

The Concept of Regional Informatization recommends “... to implement an automated information exchange between state authorities of the constituent entities of the Russian Federation, territorial bodies of federal executive authorities, local authorities and administrations of facilities for the organization of comprehensive monitoring and management of the level of threats to public security, coordination of actions to prevent crisis and emergency situations and their consequences”.

To solve this problem, a regional information and communication infrastructure should be used. This infrastructure in accordance with the above-mentioned concept, is created in the constituent entities of the Russian Federation on the basis of the following basic principles:

- the formation of an integrated computing and network environment shared by public authorities and local authorities;
- construction of regional information systems for service in architecture, standardization and ensuring compatibility of information and communication systems used in the region.

One of the tasks of the state policy of the Russian Federation in the field of protecting the population and territories from emergency situations until 2030, the basis of which was approved by Decree of the President of the Russian Federation dated January 11, 2018 No. 12, is “... Implementation of integrated systems for ensuring the safety of life of the population ...”.

In the federal project “Formation of a Comfortable Urban Environment” of the National Project “Housing and Urban Environment”, the task to implement the measures stipulated by the passport of
the departmental project on digitalization of urban economy “Smart City” (approved by order of the Russian Ministry of Construction No. 695 / pr on October 31, 2018) was set.

At the same time, the Methodological Recommendations on the urban economy digitalization, approved by the Order of the Ministry of Construction of Russia dated April 24, 2019 No. 235 / pr, define the creation of integrated systems for ensuring public safety as one of the directions for spending the allocated subsidies from the federal budget (point “d”).

An integrated system for ensuring the life safety of the population of a constituent entity of the Russian Federation (hereinafter – ISELSP) should be a geographically distributed integrated automated information management system created by the state authorities of a constituent entity of the Russian Federation in cooperation with the interested federal executive bodies, local authorities and organizations, including the regional information and communication infrastructure of ISELSP and, in conjunction with the automated systems of regional executive bodies, relevant territorial bodies of the federal executive bodies, local governments and organizations that are used to solve crisis management tasks in the subject of the Russian Federation using this infrastructure in the areas of protecting the population and territories from the emergency situations, to provide public safety, law, order and habitat safety [18].

ISELSP should ensure the initiated digital transformation of the existing life safety systems in the Russian Federation, the formation of a single digital ecosystem for life safety as an integral part of the overall ecosystem of the digital economy of the Russian Federation [19-21].

The digital transformation of the life safety systems provides for a comprehensive, end-to-end and “seamless” digitalization of crisis management processes, including:

- development and implementation of vertically integrated federal, regional and municipal multiservice digital life support platforms for interdepartmental and inter-level interfacing of interacting federal, regional, municipal and object-based automated systems, consolidation of their information resources, analytical processing of consolidated information, formation and provision of integrated information and communication one-stop services;
- creation (development) of the specialized information and communication infrastructure in order to ensure the functioning of the above-mentioned digital platforms, prompt the effective collection, storage, processing and provision of information;
- gradual decrease in the total number of automated systems in the areas of life safety based on the implementation of their functions in a comprehensive integrated system.

The need to create a specialized digital ecosystem for life safety is due to the significantly more stringent requirements for the responsiveness, stability and information security of the crisis management systems in comparison with the similar requirements for the information systems in other areas of state and municipal government.

The possibility of digital transformation of the life safety systems is determined by the following global trends in the information technology development:

- cost-effective storage and processing of information in a “cloud” environment;
- the emergence of low-cost sensors and effective technologies for remote access to them (“Internet of things”);
- successful developments in the field of information and analytical technologies, such as “artificial intelligence”, “big data”, etc.

The main functional segments of the ISELSP will be:

- the segment of natural and technological safety, designed to comprehensively address the challenges of preventing and eliminating emergencies of a natural and technogenic nature, ensuring fire safety and the safety of people at water bodies;
- the law enforcement segment, designed to comprehensively address the challenges of protecting against criminal and other unlawful attacks (including from terrorist acts, social and interethnic conflicts);
the habitat security segment, designed to comprehensively address the challenges of reducing public health risks from the natural environment and the techno-sphere objects.

Taking the fact that the vast majority of management bodies - participants in the creation and development of ISELSP are included in the unified state system for the prevention and liquidation of emergency situations (USSPLES), which has a developed regulatory framework to ensure the required intersystem, interagency and inter-level interaction, into account, the USSPLES management system can be considered as an organizational and managerial basis for the ISELSP construction and development.

At the same time, a regional software and hardware complex (SHC) for providing natural and technological safety (PNTS) can be proposed as an information and technological base for building and developing a segment of natural-technological safety and ISELSP in general.

SHC PNTS within the framework of ISELSP is designed to organize the effective inter-agency and inter-level interaction of federal, regional, municipal and object-based automated systems in the areas of protecting the public in emergencies, fire safety and the safety of people at water bodies, consolidating their information resources, operational analytical processing of consolidated information and providing comprehensive information and communication services on a “one-stop shop” basis. To ensure end-to-end and “seamless” integrated digitalization of crisis management processes, the following functional subsystems should be implemented as a part of the SHC PNTS:

- integrated monitoring, intended for the collection and primary processing of monitoring data from stationary and moving objects;
- receiving and processing messages intended for the analysis of appeals from the population, as well as from the integrated monitoring subsystem;
- decision support intended for informational and analytical support of processes for forecasting and assessing the situation, decision support and planning for their implementation;
- ensuring coordination and interaction, designed to form a single information space between interacting governing bodies, prepare and coordinate joint action plans and ensure control over their implementation;
- comprehensive information and warning designed to bring to the public information about the occurrence or threats of crisis situations and incidents, as well as ways to protect against possible dangers.

In order to provide technological support for the development and solution of the functional tasks complexes in the SHC PNTS, the available capabilities of the corresponding external digital platforms of “end-to-end” information technologies (such as “big data”, neuro-technologies and “artificial intelligence”, distributed registry systems, “Internet of things” should be used”, virtual and augmented reality technologies, etc.), on the basis of which, the necessary supporting (technological) subsystems of the SHC PNTS will be formed, including:

- a subsystem for storing and processing the data, intended for the provision of information and computing resources necessary to ensure the functioning of all the SHC PNTS subsystems;
- telecommunication subsystem providing data exchange between the regional and municipal links of the SHC PNTS, as well as their software and technical interaction with external information systems;
- an integration subsystem that provides the necessary information and software interface between the internal components of the PTK OPTB with each other and their information and software interface with external systems;
- the content management subsystem, which includes the Internet / Intranet portal and electronic document management system;
- the analytical subsystem providing the necessary tools for data analysis (including big data), predictive analytics and visualization of the results of their analytical processing;
- the geo-information subsystem providing effective work with spatial data;
the operation support subsystem designed to monitor the state of the SHC PNTS and organize its maintenance;

- the information protection subsystem created to ensure the SHC PNTS information security.

SHC PNTS should be fully harmonized with the Automated Information and Control System (AICS) of the ISELSP, put into continuous operation in 2019, and provide interdepartmental and inter-level automated interaction of the functional and territorial subsystems of the ISELSP, the formation of a single information space of the ISELSP.

To ensure the necessary sustainability of functioning, the general ecosystem of the city’s digital economy (the ecosystem of the “smart city”) should include not only the digital ecosystem of the urban resource management, but also the closely related digital ecosystem for ensuring life safety.

In this regard, it is urgent for large cities to develop a municipal digital platform for ensuring life safety, interfaced with interacting city resource management platforms, as well as with a higher regional digital platform for ensuring life safety.

At the same time, the regional digital platform should provide not only efficient and high-quality interconnection of the created municipal platforms with the state systems, but also the provision of basic integrated security services in small cities and rural areas, in which the creation of municipal platforms for ensuring life safety is not planned at all.

Pairing the platforms of the “smart city” with regional and federal automated systems for ensuring life safety will allow not only to obtain the initial data they need at higher levels, but also to use the information and computing resources of these state systems to solve urban problems, to eliminate duplication of their functions at the local level, significantly reduce total costs from the consolidated budget.

4. Summary

1. In the framework of building a common ecosystem of the “smart city” digital economy, it is necessary to form a specialized digital ecosystem for ensuring life safety, interfaced with digital platforms for managing the urban resources and including a segment of natural and technological safety.

2. The need to create a specialized digital ecosystem for life safety is due to significantly more stringent requirements for the responsiveness, sustainability and information security of the crisis management systems in comparison with similar requirements for information systems in other areas of state and municipal government.

3. Within the framework of the “smart city” in the ecosystem for life safety, it is necessary to effectively use the services of the regional digital platform, which provides information and software interconnection of interacting federal, regional, municipal and object information systems, consolidates their information resources, prompt and efficient analytical processing of consolidated information and its provision interested users on a one-stop basis.

References

[1] Indicators of smart sustainable cities developed by UNECE-ITU // Economic Commission for Europe. ECE/HBP/2015/4.
[2] Navigant Research Leaderboard Report: Smart City Suppliers 2014 (Navigant Research).
[3] Federal Law of October 6, 2003 № 131 - On General Principles of the Organization of Local Self-Government in the Russian Federation».
[4] Federal Law of October 6, 1999 № 184 - «On the general principles of the organization of legislative (representative) and executive bodies of state power of the constituent entities of the Russian Federation».
[5] Federal Law of December 28, 2010 № 390- «On Security».
[6] Federal Law of December 21, 1994 № 68 - «On the protection of the population and territories from natural and man-made emergencies».
[7] Federal Law of December 21, 1994 № 69 - «About fire safety».
[8] Chirikov A G, Kachanov S A, Popov A P 2018 Methodology for creating an integrated life support system for a subject of the Russian Federation Civil Security Technologies. Scientific and technical journal 13 (4) (50) 4-12.

[9] Ginzburg A, Kachanov S 2016 Methodology for building automated systems for monitoring engineering (load-bearing) structures, and natural hazards to ensure comprehensive safety of buildings and constructions Research India Publications, International Journal of Applied Engineering Research 11 (3) 1660.

[10] Ginzburg A, Kachanov S 2015 Technology for Enhancing Safety of Buildings and Constructions International Journal of Applied Engineering Research 10 (20) 40869-40872. ISSN 0973-4562. Research India Publications.

[11] Ginzburg A, Ryzhkova A 2015 Information system of risks analysis and management for construction projects with energy-efficient technologies in use International Journal of Applied Engineering Research 10(21) 41828-41830. ISSN 0973-4562. Research India Publications.

[12] Ginzburg A, Kachanov S, Nigmetov G 2016 Risk monitoring for the city in geological hazards conditions 5th International Scientific Conference on Integration, Partnership and Innovation in Construction Science and Education, IPICSE 2016; Moscow State University of Civil Engineering: MATEC Web of Conferences 86 04066.

[13] Volkov A 2012 Intelligence of buildings: formula Promyshlennoe I grazhdanskoie stroitelstvo [Industrial and Civil Engineering] 3 54.

[14] Ginzburg A, Kuzina O, Ryzhkova A 2018 Unified resources marking system as a way to develop artificial intelligence in construction IOP Conf. Series: Materials Science and Engineering 365 062021. doi:10.1088/1757-899X/365/2/062021.

[15] Volkov A 2014 General information models of intelligent building control systems: basic concepts, determination and the reasoning Applied Mechanics and Materials 838-841 2973.

[16] Ginzburg A V 2018 LE IM: Living Environment Information Modelling International Scientific Conference Environmental Science for Construction Industry, ESCI 2018; Ho Chi Minh City; Viet Nam: MATEC Web of Conferences 193 05030.

[17] Volkov A, Chulkov V, Kazaryan R, Gazaryan R 2014 Cycle reorganization as model of dynamics change and development norm in every living and artificial beings Applied Mechanics and Materials 584-586 2685.

[18] Ginzburg A 2016 Sustainable Building Life Cycle Design 15th International Conference on Topical Problems of Architecture, Civil Engineering, Energy Efficiency and Ecology, TPACEE-2016; Tyumen State University of Architecture and Civil Engineering: MATEC Web of Conferences 73 02018.

[19] Garyaeva V, Garyaev N 2014 Integrated assessment of the technical condition of the housing projects on the basis of computer technology Computing in Civil and Building Engineering Proceedings International Conference 1336.

[20] Kozhevnikov M M, Ginzburg A V, Kozhevnikova S T 2020 Creation of the information system based on the integrated evaluation of a construction object at various life cycle stages International Scientific Conference on Modelling and Methods of Structural Analysis 2019, MMSA 2019; Moscow, Russian Federation; 13-15 November 2019. Journal of Physics: Conference Series 1425(1) 012117.

[21] Ginzburg A V, Shilov L A, Shilova L A 2020 The methodology of storing the information model of building structures at various stages of the life cycle International Scientific Conference on Modelling and Methods of Structural Analysis 2019, MMSA 2019; Moscow, Russian Federation; 13-15 November 2019. Journal of Physics: Conference Series 1425(1) 012156.