JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 915-923
https://publishoa.com
ISSN: 1309-3452

Methods and Tools for Building Network Security Management Centers in Information and Communication Networks

Malika BahadirovnaMirzaeva
Associate Professor of Hardware and Software Management Systems in Telecommunications, PhD. Tashkent University of Information Technologies named after Muhammad al-Khwarizmi,

Aziz Odiljono'g'liMuhamedaminov
Engineer Basic organization for standardization SUE "UNICON.UZ"
E-mail: azizusmonov1992@gmail.com

Aziza Murat qiziQayumova
Belarusian State University of Informatics and Radioelectronics at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi 3rd year student

Received 2022 April 02**; Revised** 2022 May 20**; Accepted** 2022 June 18**.**

Annotation: The purpose of the study is to increase the efficiency of functioning and interaction of information and control systems of regional situational centers. The objects of research are the architecture and implementation technologies of network-centric information and control systems of the situational centers of the region, focused on solving the problems of managing regional security, as well as the interoperability property of these systems. The problems and means of ensuring the interoperability of distributed information systems of situational centers at the technological, semantic and organizational levels of interaction are considered.Technological solutions are proposed to ensure the interoperability of components of network-centric systems for managing regional security, based on a service-oriented approach and the joint use of multi-agent technologies and semantic models of knowledge representation. This ensures the integration of system components into a single virtual network-centric environment and the unification of the presentation of shared information resources and services, which helps to improve the efficiency of regional security management based on a system of distributed situational centers.

Keywords: network-centric system, regional security, architecture, management, information interaction, interoperability, situation center.

INTRODUCTION

A strategic task of national importance is the intensification of large-scale automation and informatization processes in various sectors of the economy and the life of the country's population through the introduction and integrated use of new information and analytical systems and big data processing technologies. In modern conditions, the

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 915-923
https://publishoa.com
ISSN: 1309-3452

pace of these processes determines the level of development of the country's digital economy. At present, an important role in the implementation of state programs for the transition to a digital economy and in solving the problems of ensuring national security is given to the system of distributed situational centers operating in the mode of daily activities according to a single interaction regulation. This system is built according to the network-centric principle from situational centers (SCs) of different types in their structure and departmental affiliation at various levels - federal, regional, municipal, industry and corporate. The integration of distributed SCs into a single system and the organization of their interaction on the basis of common organizational and technical regulations are aimed at improving the public administration system and the structure for ensuring integrated security through problem-oriented information and analytical support for managerial decision-making in the conditions of emerging new crisis situations in the socio-economic and military-political spheres of the country's development.

Most of the SCs created in the regions of the country are unique, both in terms of information technology architecture and software and hardware implementation of analytical support for situational management of critically important objects of the regional economy. At the same time, today there is a need for the design of new and modernization of existing SCs, as well as their subsequent integration and adaptation within the framework of the already created network of SCs. This is a serious problem that still remains insufficiently developed from a scientific and methodological point of view, which in practice leads to a decrease in the effectiveness of managing socio-economic systems using existing and newly created SCs.

At the stage of integration of information and functional components of various SCs within the framework of a distributed information environment, many problems arise related to ensuring their interoperability (compatibility) at the conceptual, model, software, hardware and organizational levels of detail. This generates an increase in time and resource costs for “docking” SCs and adapting their tools to a dynamically changing external environment, as well as for correcting system technical and methodological errors identified during the operation of SC components, and harmonizing information interaction formats.

MATERIALS AND METHODS

Interoperability in the generally accepted sense refers to the ability to integrate two or more information systems or their components into a single information environment (system). According to the approved standard [1], this should ensure the exchange of information between all elements of the integrated environment and the possibility of using information obtained as a result of integration and exchange. To ensure the property of interoperability of heterogeneous systems, modern standards of information and communication technologies are applied in practice. Interoperability is one of the properties of open systems [2].

An analysis of domestic and foreign studies on the problems of

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 915-923
https://publishoa.com
ISSN: 1309-3452
integrating distributed information and control systems for solving problems in various fields, both in the civil and military spheres, shows that interoperability is a key backbone principle for building network-centric control systems for complex objects of various nature and scale. – from technical to socio-economic. This principle serves as the basis for the modern concept of horizontal and vertical information technology interface of existing and newly created network-centric control systems designed to implement promising government projects and programs in the digital economy, industry, energy, space, healthcare, transport, and national security and other strategic areas.

A network-centric system is an association of all subjects, objects and controls into a single information space (virtual network-centric control environment), which provides full functional compatibility of all elements, coordination of decentralized decision-making and free exchange of information at all levels of the control hierarchy, regardless of functions performed by the elements. The virtual environment is focused not only on the integration of human and technical resources for management tasks, but also on automation tools for obtaining, processing and analyzing information for decision-making in the management process, which ensures an increase in the efficiency of joint activities of management subjects and coordinated information interaction between them. Interaction means not only the exchange of information in the system to maintain situational awareness, but also the development of a common strategy and coordination of joint actions in the interests of solving a certain target task.

RESULTS AND DISCUSSION

The basic functions and structure of a typical network-centric control environment are outlined in the Net-Centric Environment Joint Functional Concept [3]. Network-centric control systems, according to [4], are characterized by a weak hierarchy in the decision-making loop, the ability to generate goals within themselves, as well as openness and self-organization. At the same time, the advantage of the network-centric control method compared to the hierarchical one is that with this approach to control, the total error of making the wrong decision under conditions of uncertainty is reduced, which leads to stability and the ability of the system to adapt to a dynamically changing external environment, and also provides rational distribution of resources in the process of decentralized system management.

In this paper, we consider a system of network-centric management of regional security, built on the basis of the regional SC network. Regional SCs are a comprehensive situational management tool that provides problematic monitoring, risk forecasting and strategic planning of sustainable socio-economic development of the region to support effective management decisions both in stable conditions and in critical situations.

Network-centric management of regional security consists in the implementation of a network structure of organizational management with dedicated control centers, the interaction between which is carried out on the basis of the integration of their components

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 915-923
https://publishoa.com
ISSN: 1309-3452

(monitoring tools, control subjects, executive resources, etc.) into a single regional information space [5] . Regional SCs as centers of group decision-making (situational control points), being nodes of a network-centric regional security management system, are implemented physically at a certain point in space, as well as virtually, when individual SC components are localized at other network nodes. At the same time, in the process of solving a specific control problem, decision centers are able to move between the nodes of the virtual environment. The decision to migrate the center is made on the basis of coordinating signals and assessing the degree of situational awareness [6] of all participants in the security management process.

Under the situational awareness of the subject of management in the SC is understood information about the problem situation, focusing on which, if he has the necessary resources, the subject gets the opportunity to adjust his behavior and activity strategy, coordinate the actions of other participants in the management process and thereby influence the functioning of the management object. The network is large, there are many decision centers and everyone is required to provide information that is exactly relevant to the situation. In this regard, the interoperability of the means of information support of the SC largely determines the level of situational awareness at the stages of development, implementation and control of the execution of management decisions in critical situations.

Regional SCs are characterized by the following problems: limited functionality and isolation of the means used for monitoring and analytical processing of the growing volume of diverse information about the influence of various factors on the state of regional systems for managing the risks of critical infrastructures, as well as the need to coordinate the interaction of spatially distributed SCs and ensure properties of flexible scalability and interoperability of SC information systems. The solution of these problems is largely hampered by the confusion of the spheres of interest of various departments and organizations involved in the processes of managing regional development through the SC system. As a rule, the data presentation format and the information exchange regulations are determined by the local goals and functionality of individual control subjects, and the amount of information necessary for decision-making is determined based on the requirements for the completeness of knowledge about a critical situation, about the state of operation of the control object. and about the parameters of the external environment. These aspects make it difficult to share resources for assessing the situation and increase the time for collective development and coordination of management decisions in a critical situation.

The heterogeneity and territorial distribution of the subjects of regional security management determines the technological and semantic heterogeneity of the network-centric environment of regional security. The information support of the regional security management SC is characterized by a high degree of not only technological (use of various formats for storing, presenting and exchanging data, different DBMS and database structures,

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 915-923
https://publishoa.com
ISSN: 1309-3452

etc.), but also the semantic heterogeneity of information resources (the use of specialized domains of their own thesauri and regulations, synonymy in the naming of information objects, the use of different rating scales, etc.). At the same time, specialists/experts from different subject areas are involved in the work in the Regional Security Management Center, using different terminology and different mental models of the same concepts and processes. The source of technological heterogeneity of information resources is the organizational heterogeneity of security management entities, which, as a rule, already have and use their own, different in architecture and technology, information infrastructures by the time joint activities begin. These features hinder the development of a modern SC system and the creation of a single virtual environment for network-centric management of regional security.

Another circumstance that complicates integration processes in the construction of a virtual network-centric environment of the regional security management SC is the existence of a class of so-called “legacy systems” – unrelated heterogeneous information security management systems. These include various kinds of departmental and corporate information systems, information and analytical systems of the SC, individual web services and Internet resources, etc. These systems operate with a large amount of diverse information about various aspects of regional security, objects, processes and security events, incidents. When integrating "legacy systems" into a network-centric environment, the technological heterogeneity of resources is expressed in various formats for storing data, various technologies for creating resources and, as a result, various ways of organizing user work with them. Semantic heterogeneity consists in the use within the resources of various semantic models that determine the meaning of the content contained in them. As a result, outwardly (syntactically) the same concepts can have different semantic meanings and, conversely, one concept can be denoted formally by different syntactic constructions, which makes it difficult to unify the methods of operating information contained in these resources. Organizational heterogeneity implies different affiliation and goal setting when using information resources, which gives rise to specific problems of regulating access to information. All this requires ensuring the interoperability of SC components, resources and services integrated within the network-centric virtual environment of regional security to improve the efficiency of decision support systems in this area.

Taking into account the fact that the situational awareness of decision makers in a network-centric control system is formed on the basis of the perception of elements in the environment, understanding the situation and forecasting the future state of the control object, as well as mutual information exchange, at each level of the interoperability model it is necessary provide:

1) the use of common protocols, interfaces and formats for storing, representing and exchanging data, unified technical regulations for the joint use of software and hardware for obtaining, processing and analyzing information within the framework of interaction, standards for ensuring information security

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 915-923
https://publishoa.com
ISSN: 1309-3452
- at the level of technological interoperability;

2) the ability of interacting information systems of the SC to unambiguously understand and correctly interpret the semantic and content aspects of the information about the situation obtained in the process of collecting and communicating, to verify it and combine it with other information already available in the course of joint processing, taking into account the influence of the human factor (psychological and cultural characteristics of users when working with different types of human-machine interfaces) within the framework of information exchange - at the level of semantic interoperability;

3) harmonization of the parameters of local target functions of all participants in the information exchange (subjects of management) with the common global goal of interaction between regional SCs, depending on the mode of operation of the SCs and the situation in the region, the use of unified administrative regulations (contracts, agreements and other regulatory and legal documents) that define the rules and responsibilities of subjects and objects of information interaction - at the level of organizational interoperability.

Thus, based on the foregoing, we can conclude that in order to achieve the interoperability of information systems of the SC at all levels of network-centric management of regional security, the use of only agreed sets of information and communication technology standards seems to be a necessary but insufficient condition. To obtain a tangible complex effect, interoperability should be provided at higher levels - semantic and administrative, associated with the perception, comprehension and use of information in the organizational decision-making circuits. The development of formal procedures and means of ensuring semantic and organizational interoperability in the process of coordinating information interaction in network-centric control systems is a difficult task. This problem has not yet been completely solved, despite its acute relevance for various applications.

To date, there are many methods and technologies for providing various aspects of interoperability of distributed systems. However, these tools are used in isolation from each other and are not linked into a coherent methodological system. The whole set of known approaches to solving interoperability problems at the technological, conceptual and organizational levels can be divided into the following categories [7]:

1) a bottom-up approach ("bottom-up" approach), which is focused primarily on solving the problems of technological interoperability of information systems by using common standards and technologies for transmitting, storing, presenting and processing information at all levels of integration of these systems;

2) a top-down approach ("top-down" approach), which focuses on decomposing the solution to interoperability problems in terms of the architecture of the system as a whole, and then in terms of individual subsystems and processes down to atomic elements;

3) a system-wide approach based on the analysis of internal communications between components within an integrated system and focused on solving interoperability problems by forming a

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 915-923
https://publishoa.com
ISSN: 1309-3452
single environment for information interaction between them;

4) an interactive approach that takes into account the nature of the interfacing and interaction of various systems with each other and the external environment and is focused on achieving the interoperability of those systems and their components that already have different technological implementation and use excellent standards for transmitting, storing, presenting and processing information.

5) a process approach focused on solving problems of interoperability, taking into account the identification, analysis and optimization of a complete group of technological, organizational and organizational and technical factors that trigger various processes throughout the life cycle of systems that affect the functioning of systems as a whole and change their interoperability properties.

The choice of one or another approach depends on the functional fragmentation of information systems, the principles of their construction and the technical implementation of individual components, and other factors.

CONCLUSION

The growing complexity of managing socio-economic systems under conditions of high uncertainty and multiple risks, on the one hand, as well as the need to automate and intellectualize the means of managing these systems in the context of the transition to a digital economy, on the other hand, increase the requirements for a modern network-centric system. SCs focused on information and analytical support for making strategic and operational management decisions at all levels of state and regional government. At the same time, the problem is exacerbated by the need to promptly adapt various means of information and analytical support and ensure the possibility of their joint use within the existing SC system. The final solution to this problem has not yet been obtained, and therefore the problem of ensuring the interoperability of information systems of regional SCs for the needs of public administration and security is a promising scientific and technical task. This is due today to modern trends in the field of integration of problem-oriented dual-purpose information systems, as well as to the development and application of network-centric control systems for various relevant applications in the socio-economic sphere.

Despite the fact that the integration of "inherited" information systems of the SC into a single virtual network-centric environment is associated with certain difficulties, the paper suggests possible ways to solve the problem of ensuring the technological, semantic and organizational interoperability of the components of these systems. Improving these solutions may be the subject of future research and development. At the same time, in order to overcome the limiting factors of interoperability of a technical nature in order to widely use the entire functionality of the network-centric SC system, it is advisable to adhere to common approaches based on domestic and foreign methods and open ICT standards that regulate ensuring the interoperability of components of network-centric information and control systems. taking into account the formation of interoperability profiles at the level of

protocols, interfaces and processes in these systems.

Further research is aimed at improving the multi-level regional security management system in terms of developing new technologies for dynamic configuration of the network-centric environment for regional security management at the conceptual, virtual and organizational levels based on modern standards of interoperability and system integration.

REFERENCES

1. Information Technology. Industrial automation systems and their integration. Interoperability. Basic provisions. - Moscow: Standartinform, 2014. - 12 p.
2. Technology of open systems / ed. A. Ya. Oleinikova. - Moscow: Janus-K, 2004. - 288 p.
3. Net-Centric Environment Joint Functional Concept. - Washington : Department of Defense Washington DC, 2005. - 76 p.
4. Masloboev, A. V. Information dimension of regional security in the Arctic / A. V. Masloboev, V. A. Putilov. - Apatity: KSC RAS, 2016. - 222 p.
5. Masloboev, A. V. Model and technology of decision support in the conditions of network-centric management of regional security / A. V. Masloboev // Reliability and quality of complex systems. - 2019. - No. 2 (26). – P. 43–59.
6. Endsley, M. R. Final Reflections: Situation Awareness Models and Measures / M. R. Endsley // Journal of Cognitive Engineering and Decision Making. - 2015. - Vol. 9, No. 1. – P. 101–111.
7. Systems, Capabilities, Operations, Programs, and Enterprises (SCOPE) Model for Interoperability Assessment. Version 1.0. - NCOIC, 2008. - 154 p.
8. Wooldridge, M. An Introduction to MultiAgent Systems. Second Edition / M. Wooldridge. - John Wiley & Sons, 2009. - 484 p.
9. Oleinik, A. G. Development of the ontology of the integrated knowledge space / A. G. Oleinik, P. A. Lomov // Design ontology. - 2016. - V. 6, No. 4 (22). - S. 465-474.
10. Kuzmin, I. A. Distributed information processing in scientific research / I. A. Kuzmin, V. A. Putilov, V. V. Filchakov. - Leningrad: Nauka, 1991. - 304 p.
11. Lomov, P. A. Ontology integration using thesaurus for semantic search / P. A. Lomov, M. G. Shishaev // Information technologies and computing systems. - 2009. - No. 3. - P. 49-59.
12. Sukhoroslov, O. V. Integration of computing applications and distributed resources based on a cloud software platform / O. V. Sukhoroslov // Program systems: theory and applications. - 2014. - T. 5, No. 4 (22). - S. 171-182.
13. Makarenko, S. I., Oleinikov, A. Ya., and Chernitskaya, T. E. Models of information systems interoperability, Sist. - 2019. - No. 4. - P. 215–245.
14. Frangulova, E. V. Classification of approaches to integration and interoperability of information systems / E. V. Frangulova // Bulletin of the Astrakhan State Technical University. Ser.: Management, computer technology and informatics. - 2010. - No. 2. - P. 176–180.
15. Kupriyanov, A. A. Network-centric military actions and issues of interoperability of automated systems / A. A. Kupriyanov // Automation of control processes. - 2011. - No. 3. - P. 82–97.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 915-923
https://publishoa.com
ISSN: 1309-3452
16. Zatsarinny, A. A., Kozlov S. V., Shabanov A. P. Interoperability of consolidated organizational systems // Management Problems. - 2017. - No. 6. - P. 43–49.
17. Akatkin, Yu. M. Digital transformation of public administration: data-centricity and semantic interoperability / Yu. M. Akatkin, E. D. Yasinovskaya. - Moscow: LENAND, 2019. - 724 p.