Programming Innovations for Strengthening Economic Security and Digital Service Infrastructure

Sergey Shaytura[1*], *Natalya* Shaytura[2], *Saidmagomed* Alikhadzhiev[3]

[1]Russian University of Transport, Moscow, Russia
[2]Moscow State University of Technology and Management named after K.G. Razumovsky, Moscow, Russia
[3]Kadyrov Chechen State University, Grozny, Russia

Abstract. The work is devoted to the analysis of the risks of threats to the economic security of the service infrastructure. Algorithms for solving these problems affect the totality of interaction between economic, technical, organizational, and managerial relations in the service infrastructure. The article shows that the economic activities of service infrastructure enterprises cover a significant area of public relations related to the development, production, and provision of various types of services for individuals and legal entities. The paper highlights one of the key features of the service infrastructure in the economy — its diversified structure. The article examines a number of potential causes of possible threats to economic security in relation to the area under consideration. The article shows that the purpose of ensuring the economic security of the service infrastructure is to minimize the impact of external and internal threats with institutional, economic, technological, and social causes. To assess the impact of possible risks to the economic security of the service infrastructure, the authors propose to use a system-technical model built using a service-digital approach, which provides an optimal algorithm for searching for potential economic security problems. The application of the proposed methodology allows to determine in practice the most significant risks for a particular enterprise of the service infrastructure, which in certain conditions can turn into threats. The model allows to find solutions to reduce the level of danger from identified risks and threats.

1 Introduction

The economic activity of service infrastructure enterprises has a special specificity, which consists in the multiple nature of the types of activities of economic interaction subjects and

* Corresponding author: swshaytura@gmail.com

in the intertwining of their interests.

The key feature of the service infrastructure is its diversified structure, represented by a wide range of industries necessary to ensure the main purpose of the service — customer satisfaction in the provision of various services.

It is particularly worth noting the fact that during the coronavirus pandemic, it was the service and service infrastructure that declared themselves as one of the key components of the state's economy.

The service infrastructure involves both commercial and non-profit enterprises, state and municipal structures, individuals, and their communities. Service infrastructure enterprises are represented in all organizational and legal forms, which shows its versatility and demand from consumers [1]. The service infrastructure is involved in almost all areas of human daily life, which is why in modern market conditions of economy digitalization, service infrastructure enterprises are assigned one of the leading roles in the development of not only the economy of a particular region, but also the economy of the state as a whole.

One of the signs of the service infrastructure digitalization is the widespread use of electronic platforms (1C-Bitrix; Yandex platform; Avito platform; SalesapCRM; Intalev and others) and services for searching and posting information on the offer of works and services by both enterprises and individual performers. The most popular of them are Avito for business; Yandex.Services; Yula and others.

Security when using electronic platforms for searching and posting information on the offer of works and services in the service infrastructure should be ensured during their development and maintained at all times of use. But this is not always realized in reality, because consumers of these resources cannot be completely sure of the security of information that is entered into the database of such systems during registration and when performing any actions using such electronic platforms, resources or services [2].

Ensuring the economic security of the service infrastructure should include not only solving economic problems, but also ensuring the fulfillment of additional security conditions related to the peculiarities of society and the interaction processes in it.

Based on the above statement, the authors identify the following issues for analysis:

- Issues of service infrastructure management in general. They are associated with an inefficiently structured structure of interaction within the service infrastructure, with a low level of quality of the management system for industry subsystems, and the lack of qualified personnel – cognitive specialists capable of providing innovative development of the service infrastructure [3].
- Issues of service infrastructure development. This includes information technologies, which in recent years have been presented in the form of various electronic platforms for searching and posting information on the offer of works and services. Such platforms introduce various financial mechanisms for mutual settlements between the parent company and the platform's partners, performers and customers, attempts are being made to implement various concepts and programs. A feature of such services for searching and posting information on the offer of works and services is the solution of tasks for the information of customers and performers, but without ensuring subsequent quality control of the service provided, which opens up potential opportunities for fraudulent actions on the part of both the contractor and the customer. Payment for services and the declared quality of services are not guaranteed, which is a problem of ensuring the economic security of society and the processes of interaction in it [4].
- Issues related to the tariff policy, the dynamics of price changes in the service infrastructure. To the greatest extent, the problem of solving these issues is a consequence not only of inflationary processes, subjectivity in determining tariff policy on the part of the management of service infrastructure enterprises, abuse of a monopoly position in the market in a region or field of activity, but also the lack of a clearly defined regulatory framework –

a tariff grid, on the basis of which price lists for services can be formed, considering the demand, urgency, regional alignment, and categories of service consumers. According to the authors, the problem of pricing to determine a transparent, understandable and balanced price for the services of service infrastructure enterprises is one of the most urgent in the light of considering the risks of threats to the economic security of the service infrastructure.

The lack of mechanisms for solving the issues raised can lead to potential threats related to social factors, since they arise as a result of a negative reaction from the client from dissatisfaction with the quality of services provided [5].

The reasons for the manifestation of such negative aspects may be the following: insufficient level of qualification of performers, their low motivation, critical level of equipment wear, which leads to long downtime during maintenance, the appearance of malfunctions after elimination during the warranty period, failure to provide services stated in the contract or the official price list of the contractor, high cost of services, unjustified increase in tariffs for services and others [6].

The above-mentioned reasons for the manifestation of negative social factors lead to exacerbations to the level of threats, which is explained by the high level of impact on the level of consumer comfort of customers and household budgets.

The above threats can negatively affect the public-state system, both individually and collectively, therefore, the search for ways to reduce the impact of potential and existing threats on the economic security of the service infrastructure is an urgent task.

Previously, these issues were not considered in a complex and in relation to the field under study, therefore, the scientific novelty of the study is a comprehensive assessment of risks and threats to the economic security of service infrastructure enterprises using a system-technical model built for specified conditions.

2 Materials and Methods

The security of the service infrastructure includes various measures aimed at reducing the impact of the consequences of various kinds of negative factors associated with insufficient qualifications of performers, aging of service infrastructure equipment, increase in the number of accidents and emergency situations during the operation of service infrastructure equipment, low management efficiency of service infrastructure enterprises.

Based on the above, it is possible to formulate the purpose of the study – to analyze the risks of threats to the economic security of the service infrastructure.

To create conditions to ensure the economic security of the economic activity of the service infrastructure, according to the authors of the study, it is necessary to focus efforts on solving the following tasks:

- monitoring and analysis of processes in the service infrastructure that occur in accordance with the implementation of objective economic laws;
- identification of relevant vectors for the formation of the most effective conditions for the implementation of interaction systems in the service infrastructure, ensuring economic security for users of digital platforms used to search and post information on the offer of works and services;
- ensuring the implementation of economic security management processes for objects and subjects of the service infrastructure.

The authors note the need to identify theoretical and methodological aspects in assessing economic security risks for service infrastructure enterprises [7]. This is advisable for optimizing management models, expressed in forms convenient for the consumer, ensuring transparency of business activities, as well as ensuring the security of the service for both the customer and the performer, which requires the formation of a logical management model, based on synthesized algorithms using something new for Russia innovative tools -

digitalization of the service sector, which will allow enterprises providing services in various sectors of the national economy to timely adapt to innovative changes arising in the Russian Federation in the digital economy [8].

The authors propose to assess the possible risks to the economic security of service infrastructure enterprises, potentially leading to problems in the field under study, in the form of a model using the service-digital approach presented in Figure 1.

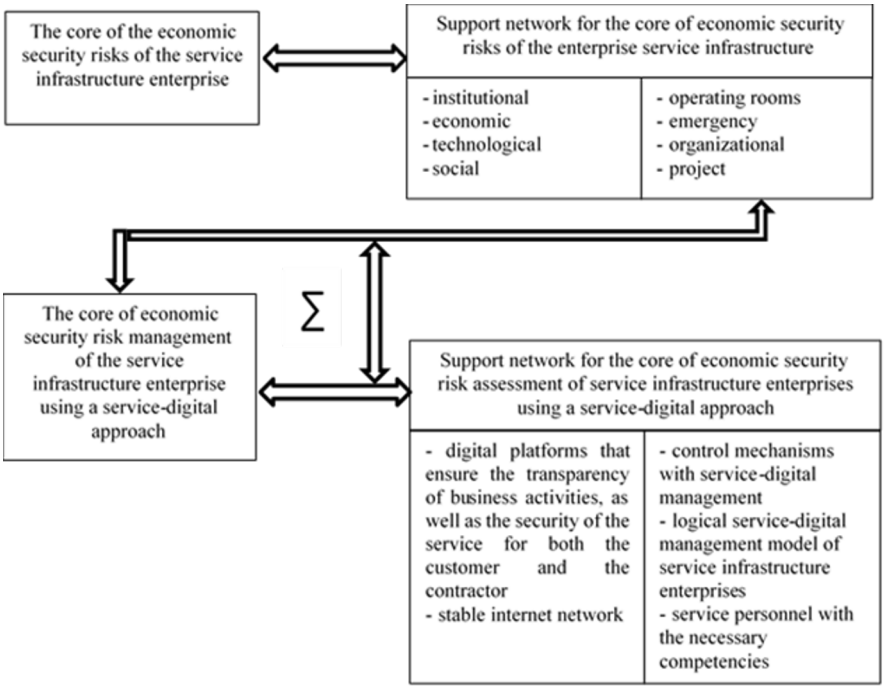

Fig. 1. The management model for the formation of a network for determining possible risks to the economic security of service infrastructure enterprises. "Compiled by the authors".

Figure 1 shows the structural relationship between the formation of a support network for the core of the economic security risk assessment of service infrastructure enterprises, built using a service-digital approach.

This model illustrates that the existing network of support for the core of economic security risks of service infrastructure enterprises does not consider the specifics of the existing conditions of the digital economy, the innovative nature of the processes taking place in the current conditions. It is shown that in modern conditions, risk management of the economic security of a service infrastructure enterprise needs to use a special approach, since it is necessary to consider the impact of digitalization on the processes taking place in the industry under study [9].

3 Results

Using the proposed research methodology, an assessment of the risks of threats to the economic security of the service infrastructure was carried out. The external and internal risks of threats were highlighted.

The possible external risks of threats are listed below:

- risks related to the security of the business environment (unfair competition, fraud, use of electronic services without user verification);

- environmental risks (natural disasters, man-made accidents, traffic);
- risks of the political environment (political instability, expropriation, introduction of external restrictions on the supply of equipment and spare parts).

Internal risks of threats should be understood as organizational problems, for example, internal fraud, boycotts, employee negligence, etc.

Let's list the most typical risks of internal threats [10]:

- operational (financial);
- organizational (loss of key employees);
- project (customer's risk, investment risk).

Under certain conditions, the bulk of the risks may fall into the category of security threats [11].

We will identify the relevant threats using the proposed methodology and carry out their decomposition:

- institutional;
- economic;
- technological;
- social.

Institutional threats arise in the following cases:

- result of the service does not meet client's expectations;
- lack of trust between the customer and the contractor in the service infrastructure;
- lack of services for ordering services in the service infrastructure, convenient for both the customer and the contractor;
- There are no relevant regulatory and legal mechanisms to ensure the effective operation of the service infrastructure in the digital economy.

The emergence of economic threats is associated with the following factors:

- security of payments in the service infrastructure is not guaranteed;
- lack of effective control mechanisms for cash and non-cash payments in the service infrastructure;
- lack of up-to-date objective data on the volume of services rendered;
- lack of clear and transparent principles for the formation of tariffs for services in the service infrastructure in the digital economy;
- taxes are not received in full from the service infrastructure.

Technological threats arise for the following reasons:

- the qualification of the performers does not provide the necessary service quality;
- performers register and offer services on various electronic platforms (agency services, aggregators) in the Internet without providing documentary evidence of the necessary professional competencies;
- absence of a single electronic database for the registration of performers for the service infrastructure in accordance with professional qualifications;
- lack of objective information about the functioning of the service infrastructure.

Social threats:

- lack of qualification requirements for the service infrastructure contractor;
- lack of feedback in the customer - contractor system;
- the presence of service provider agents in the service infrastructure does not guarantee the provision of services of proper quality;
- the absence of a regulatory framework regulating the activities of agents (aggregators, intermediaries) of the service infrastructure in the digital economy.

The listed threats are closely related to the analysis questions posed in this study.

The solution of issues related to the management of the service infrastructure in general, the development of the service infrastructure, as well as issues of tariffs and price dynamics in the service infrastructure are closely related to the need to eliminate all of the above threats,

which is fully consistent with the proposed methodology for managing the risks of economic security of the service infrastructure enterprise.

To solve the tasks set, in accordance with the proposed methodology, the authors propose:

- to use digital platforms for the service infrastructure that ensure transparency of business activities, as well as the security of the service for both the customer and the contractor;
- to ensure a stable Internet network;
- to implement mechanisms for monitoring the activities of the service infrastructure with digital service management;
- to implement a logical digital service management model for service infrastructure enterprises;
- to provide training for service personnel with the necessary competencies.

4 Discussion

A large number of studies have been devoted to the consideration of economic security problems and the analysis of risks and threats. "Risk is understood as a value characterizing potential damage (losses) that are associated with incorrect management decisions and are made during the study of the economic, political and social situation in which the organization operates" [12]. When determining possible levels of security threats to service infrastructure enterprises, the risk associated with strategic decision-making is considered. The occurrence of such a risk is indicated when a solution is chosen from several alternatives.

The researchers in [2] note that the risk can be both strategic and of strategic decision, while a situation of undesirable development of events arises, which is considered in conjunction with the possible damage from the onset and development of such an event.

To ensure the economic security of service infrastructure enterprises, mechanisms should be used that can minimize the impact of risks of external and internal threats from the financial, material, information and personnel spheres [1]. The article [4] identifies the risks of external and internal threats to economic security.

The proposed service-digital approach to assessing existing and potential problems of economic security of the service infrastructure in the context of the digital economy development makes it possible to optimize the search for possible ways to reduce their impact on processes in industrial and social subsystems using these models [8]. In [10], it is noted that the model presented in Figure 1 is a system engineering model. This model shows characteristic connections in solving problems of constructing algorithms for the interaction of systems with multidirectional vectors into a single control system with a convenient and understandable structure for research.

5 Conclusion

The identified distinctive signs of threats to the economic security of the service infrastructure suggest that the development and implementation of mechanisms to ensure the economic security of this area should be solved in a complex, considering not only economic, but also social aspects. In the context of the development of the digital economy, the issues of economic security of the service infrastructure affect a complex of institutional, economic, technological and social factors of the functioning and development of the socio-economic system of society, as well as its individual subjects.

The proposed model for managing the formation of a network for determining possible risks to the economic security of service infrastructure enterprises can be used in practice when solving problems to ensure the economic security of service infrastructure enterprises

at the regional, municipal level or private enterprises.

The model allows to analyze risks and threats to the economic security of the enterprise, assess possible manifestations and impacts on the business activities of the enterprise, assess the likelihood of risks in the context of the digital economy development.

As of the current year 2024, economic security in the service infrastructure has more questions than answers, therefore, unresolved problems of economic security in the service infrastructure at the moment are rather a deterrent to the innovative development of the service infrastructure than its driver, which indicates the relevance of the study.

Based on the above material, the authors conclude that research aimed at solving the problems of economic security of the service infrastructure should be conducted constantly and consider the changes taking place in the economy.

References

1. I.Ya. Bogdanov, *Economic security: essence and structure* (Institute of Socio-Political Studies of the Russian Academy of Sciences, 2018) 234.
2. L.N. Chernyshov, Economics and management of the housing and communal services enterprise **1-5** 38-41 (2016)
3. A.V. Demenev, R.N. Lopatko, V.G. Zharov, *Operation of Buildings and Structures Based on BIM Standards in the Digital Economy*, International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon, 2019) 8934034.
4. L.P. Goncharenko, F.V. Akulinina, *Economic security Textbook* (Yurayt, 2017) 478.
5. G.A. Karpova, M.D. Sushchinskaya, *Service sector in the modern economy* (Publisher SPbGEU, 2016) 114.
6. N.M. Komarov, N.V. Ivanov, V.M. Safronov, V.G. Zharov, N.V. Duntsova, K.N. Komarov, Internet journal Naukovedeniye, **1(14),** 30 (2013) http://naukovedenie.ru/
7. N.M. Komarov, V.G. Zharov, Service plus, **2,** 74-81 (2013)
8. G.V. Latyshev, K.V. Latyshev, A.I. Mokhov, V.O. Chulkov, Electrical and information complexes and systems **1(8)** 3-9 (2012)
9. Yu.A. Loktionova, Socio-economic phenomena and processes, **3(049),** 12-19 (2019)
10. A.I. Mokhov, L.A. Mokhova, N.M. Komarov, S.G. Novozhenov, Internet journal Naukovedeniye, **4(13) (**2012) http://naukovedenie.ru/
11. S.V. Shaitura, A.M. Minitaeva, V.G. Zharov, V.V. Ivanova, Bulletin of the Kursk State Agricultural Academy, **1,** 138-144 (2021)
12. V.V. Velikorossov, Bulletin of IGEU, **2,** 32-39 (2016)