Managing organizations in the context of digital transformation

Natalia Evgenievna Muromets[1*], *Sergey Gennadievich* Goryainov[2], *Irina Anatolyevna* Pryadko[1], *Ekaterina Sergeevna* Bozhenko[1], and *Yuliya Aleksandrovna* Laamarti[3]

[1]Southern Federal University, Faculty of Management, Rostov-on-Don, Russian Federation
[2]Southern Federal University, Institute of Tourism, Service and Creative Industries, Rostov-on-Don, Russian Federation
[3]Financial University under the Government of the Russian Federation, Moscow, Russia

Abstract. In the context of dynamic digital transformation, there is a need to reconsider traditional approaches to organizational management, as information insecurity poses a threat to the security of domestic organizations and leads to the loss of their competitive positions, along with the inevitable loss of previously achieved financial, operational, and investment advantages. The practical value of the obtained results lies in the development of methodological recommendations for conducting cluster analysis of organizations based on a group of indicators for assessing the level of information authentication, as well as the level of utilization of specialized software tools and information protection instruments, which will allow for evaluation and ranking of the information security of organizations. It is concluded that the most successful organizations are financial institutions and organizations in the information technology sector, as they have been able to transform into leading technological companies by revising the content of their core business processes in the context of digitalization. Many of them have formed a comprehensive ecosystem, which has enabled them to quickly adapt to changing conditions, which would not have been possible without the implementation of digital transformation processes.
Keywords: organization management, digital transformation, management processes, information security

1 Introduction

In the face of modern challenges, the widespread implementation and active development of information technologies determine the dynamics and trends of socio-economic relations and the peculiarities of organizational management. Despite the fact that the implementation of information technologies is considered a leading factor in the development not only of national economies but also in the formation of global economic systems, the high level of risk associated with their application in the IT sphere cannot be underestimated. The importance of the discussed issue of ensuring information security and reducing the level of risk in the

*Corresponding author: muromets@sfedu.ru

information sphere is confirmed by the main provisions of the Economic Security Strategy of the Russian Federation until 2030 [12].

Therefore, one of the key directions of modern management in terms of adapting domestic organizations to new socio-economic and political threats and challenges is not only to identify factors that contribute to reducing the level of information risks but also to develop scientific and methodological approaches to monitoring and practical recommendations on organizing the control of information risks in the activities of domestic organizations in various types of economic activities. This complex approach will ensure their competitive advantages and competitiveness in the production of goods or provision of services [1].

Thus, there is a need to reconsider traditional approaches to organizational management, as information insecurity threatens the security of domestic organizations and leads to the loss of their competitive positions, along with the inevitable loss of previously achieved financial, operational, and investment advantages [5]. One of the priority directions for minimizing managerial risks that pose a high threat to the information security of domestic organizations is the improvement of the management system, taking into account modern trends in the digitalization of all processes [3].

The object of the research is the processes of organizational management in the context of digital transformation.

The aim of the research is to develop a comprehensive approach to improving the management of domestic organizations in the context of digital transformation and to enhance existing management processes aimed at reducing information vulnerability.

Research objectives:

1) Identify significant factors influencing the level of information security of organizations in order to reduce risks in the information environment.

2) Develop methodological recommendations for creating a rating of information security of organizations in the context of digital transformation.

2 Materials and Methods

In order to identify indicators for assessing the level of information security of organizations in Russia, it is important to determine which specific factors influence the level of information security, thereby reducing risks in the information environment [4]. It is proposed to consider the following parameters as the main indicators of information security in the work of domestic organizations, which should be grouped into two categories and subjected to cluster analysis: indicators of information authentication and a group of indicators of the use of specialized software tools and information security instruments.

3 Results

It is important to agree with Barnagyan V.S.'s opinion that "the ongoing transformations in the field of digital technologies require a revision of business processes in order to reduce the technological cycle time, combine and execute subprocesses in parallel, and reduce costs, thereby ensuring new qualitative characteristics and consumer properties of the produced goods" [2].

The use of modern information technologies plays a key role in shaping business development strategies. With their help, organizations can improve productivity, automate business processes, reduce costs, and enhance the quality of products or services [6].

The study of the peculiarities of the impact of digital transformation processes on organizational management can be conducted through cluster analysis. To assess organizations based on the level of information security, it is expedient to group homogeneous factors into

two comprehensive sets of criteria: a group of indicators for information authentication, and a second group consisting of a range of indicators for the use of specialized software tools and information security instruments (Figure 1). Data from the cluster analysis of organizations by type of economic activity

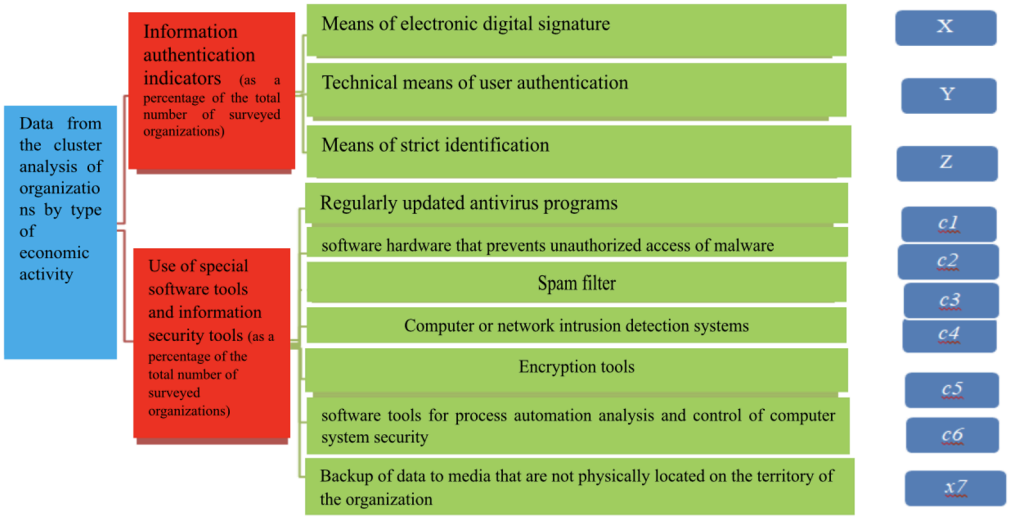

Fig. 1. A set of indicators for cluster analysis of the level of information security of organizations, taking into account the use of information security tools. *Obtained by the authors on the basis of calculations in the STATISTICA appendix for [7-9]*

Tables 1 and 2 provide initial information for conducting a cluster analysis of organizations in various sectors of the economy.

Table 1. Indicatorsof the level of authentication of information in organizations

Types of economic activity [14]	Indicators of the level of information authentication		
	means Electronic digital signature (at the end of the year; units)	Technical means Authentication users	Strong authentication tools
	X	*Y*	*Z*
Agriculture	67,5	48,2	48,2
Mining	60	47,6	47,6
Manufacturing	73,8	58,1	58,1
Energy Supply	77,2	58,1	58,1
Water supply, sewerage, waste disposal	73,6	48,6	48,6
Construction	53,6	40,3	40,3
Wholesale and retail trade	65,3	54,4	54,4
Transportation and storage	66,8	50,6	50,6
Hotels & Catering	63,2	45,8	45,8

Information & Communication	74,9	61,2	61,2
Information Technology Industry	75	65,1	65,1
Financial sector	75	58,8	58,8
Real estate transactions	59,4	42,1	42,1
Professional, scientific and technical activities	63,6	47,1	47,1
Higher education	79,2	65,8	65,8
Health and social services	82,8	64	64
Culture and sport	67,6	39,2	39,2
Public administration and social security	79,5	54,4	54,4

Compiled by the authors based on [14]

The following criteria were considered for grouping organizations based on the level of usage of specialized software tools: regularly updated antivirus programs, as well as software and hardware measures that prevent unauthorized access of malicious programs using spam filters, and the implementation of intrusion detection systems in the computer or network, among others. [Digital Economy Indicators 2022], presented in table 2.

Table 2. Indicators of the level of use of special software and information security tools in organizations of various spheres of economic activity

Views economic activity	Use of special software in organizations (as a percentage of the total number of organizations surveyed)						
	regularly updated anti-VR programs	software, hardware that prevents unauthorized access to malicious programs	Spam filter	Computer or network intrusion detection systems	Means of chif-roving	software tools for automating the processes of analysis and control of the security of computer systems	Backing up data to media that is not physically located on the territory of the organization
	C1	*C2*	*C3*	*C4*	*C5*	*C6*	*S7*
1	2	3	4	5	6	7	8
1 Agriculture	56,7	32,8	29	24,9	22,6	19,7	21,8
2 Mining	60,7	49,4	44,4	26,9	33,4	26,5	23,2
3 Manufacturing industry	72,2	57,2	51,9	37,2	39,8	30,1	28
4 Energy supply	72,4	52,5	46,7	43,6	36,7	30,3	22

5 Water supply, sewerage, waste disposal	55,3	31,3	27,1	43,1	22,1	18,7	18,6
6 Construction	50,5	34,5	33,1	28,7	25,6	20,1	19,9
7 Wholesale and retail trade	72,5	60,2	59,9	25,9	49,1	41,4	37
8 Transportation and storage	66,1	50,6	43,5	48	34,4	26,5	22,9
9 Hotels & Catering	59,2	39,8	40,9	39,7	30,1	27,8	26,8
10 Information and communication	70,8	54,1	51,7	30,8	44,8	39,4	31,7
11 Information Technology Industry	73,6	64,9	59,4	48,1	54,1	47,8	36,1
12 Financial sector	76,5	69,5	64,9	58,5	56,9	54,2	46
13 Real estate transactions	46,2	29,1	27	67,1	21,1	17,1	16,8
14 Professional, NTD	55,6	37,1	35,2	25,7	26	22,2	21
15. Higher education	79,3	69,5	62,5	31,7	47,4	36,6	23,3
16 Health and social servicesand	74,7	55,8	41,1	60	34,6	26,7	25,1
17 Culture and sports	50,5	25,2	23,7	53,3	15,4	14	14,3
18 Public administration and social security	66,4	39,5	31,3	22,9	24,4	21,9	18,2

Compiled by the authors based on [14]

Table 3 shows the descriptive characteristics and elements of cluster analysis of organizations.

Table 3. Descriptive statistics of cluster analysis of organizations

Variables of the use of special software tools in organizations	Number of observations	Average meaning	Minimum values	Maximum values	Standard deviations
C1	18	64,40000	46,20000	79,30000	10,21930
C2	18	47,38889	25,20000	69,50000	14,12128
C3	18	42,96111	23,70000	64,90000	13,20932
C4	18	40,65882	22,90000	67,10000	13,58957
C5	18	34,69111	15,40000	56,90000	12,17027
C6	18	28,94444	14,00000	54,20000	11,02213
S7	18	25,15000	14,30000	46,00000	8,06468

Obtained on the basis of calculations carried out on [14]

Based on the graphical information on the scatter diagram of the elements of the analysis of clustering of organizations according to the criterion of using information security tools, four clusters were obtained, which are presented in Table 4.

Table 4. Results of clustering of organizations by the level of information security and the use of information security tools in 2021

Cluster name	Number of economic activities of the Russian Federation included in the cluster	List of economic activities included in the cluster[9]
1	7	Agriculture Mining, Energy supply, Transportation and storage, Hotels and catering, Professional, scientific and technical activities, Health care and social services, Public administration and social security
2	4	Manufacturing Wholesale and retail trade Information & Communication Higher education
3	4	Water supply, sewerage, waste disposal Construction Real estate transactions Culture and sport
4	2	Information Technology Industry Financial sector

Obtained by the authors on the basis of calculations carried out in the STATISTICA application for [14]

Thus, based on the conducted cluster analysis of organizations by types of economic activities, both in terms of information authentication level and the level of usage of specialized software tools and information security measures, it is possible to draw conclusions about the distribution of organizations by types of economic activities in 2021 into four clusters.

The second cluster takes the second place in the ranking of information security. It includes economic sectors such as manufacturing industry, wholesale and retail trade, information and communication, and higher education. Although organizations in this cluster achieve high authentication indicators, their utilization of specialized software tools, such as software and hardware measures preventing unauthorized access of malicious programs, implementation of spam filters, intrusion detection systems, encryption tools, and automation of analysis processes and security control of computer systems, is significantly lower.

Further down the information security level, the activities of organizations belonging to the largest first cluster are characterized. This cluster represents almost 40% of the total number of economic activities in Russia as of the end of 2021.

The third cluster consists of organizations in sectors such as water supply, wastewater treatment, waste management, construction, real estate operations, culture, and sports. These sectors exhibit the lowest levels of information authentication as well as the usage of specialized software tools and information security measures.

It should be noted that the fourth cluster, which is the smallest in terms of the number of

organizations included, consists of only two sectors, namely the information technology industry and the financial sector.

4 Discussion

It should be noted that organizations represented in the fourth cluster have a high level of information security in the context of dynamic digital adaptation. Another important aspect of information security in the financial sector is ensuring data confidentiality through various methods such as data encryption during transmission and storage, the use of virtual private networks (VPNs) for secure information exchange, and the implementation of physical security measures, such as access control to server rooms or restricting access rights to confidential data only to authorized personnel [13].

Another crucial aspect is the training and awareness of employees regarding information security. Organizations in this cluster can conduct regular training programs aimed at educating staff about safe handling of information, recognizing and preventing social engineering, and staying informed about current information security threats [11]. All these measures contribute collectively to the establishment of resilient information security and protection of confidential data in organizations belonging to the fourth cluster.

The most dynamic transformation of core business processes takes place in organizations in the banking sector, as reflected in their key corporate governance documents, such as the bank's code of conduct, charter, and relevant internal documents. This analysis is based on the content of corporate documents of PJSC Sberbank, which are available on the bank's website [10].

PJSC Sberbank actively promotes the social and environmental agenda within the bank to create an efficient system and become a leader in ESG (Environmental, Social, and Governance) on the Russian and international markets. Sberbank includes several strategic business units:

- Retail business: Includes services for individual clients such as current and savings accounts, loans, debit and credit cards, mortgages, insurance, pension services, and other banking services for individuals.
- Corporate business: Includes services for corporate clients such as lending, transaction support, project financing, leasing, payment services, and other banking services for enterprises and organizations.
- Investment business: Includes asset management services, investment funds, brokerage services, securities trading, and other investment products and services.
- Digital services and innovations: Sberbank actively develops digital platforms, technologies, and innovative products to enhance the customer experience and provide new digital services.

It is important to highlight the current set of tasks that Sberbank aims to achieve in order to meet its goals, which dynamically change based on societal demands and the external environment. These tasks include revenue growth and cost reduction, risk minimization, and assistance in promoting digitalization. The tasks of PJSC Sberbank for the period from 2009 to 2016 focused on achieving maximum customer orientation, which involved transforming business processes, improving service quality, implementing innovative approaches, and adopting Agile methodology. Special technologies were employed to accomplish these tasks, such as the establishment of customer operations support centers and the implementation of various online services [10].

A new set of tasks for PJSC Sberbank was defined for the period from 2017 to 2020, focusing on the implementation of a large-scale digital transformation. The main mechanism for achieving these goals during this stage was the introduction of various financial and non-financial services for customers, providing round-the-clock accessibility. This allowed the bank to assume a leading position in the implementation of the national project "Digital

Economy of Russia" [14].

It should be noted that the structure of PJSC Sberbank and the presence of its strategic business units may change depending on market developments, changes in the bank's strategy, and other factors, which may lead to a revision of the existing vision, mission, goals, strategies, and tasks of PJSC Sberbank, as presented in Fig. 2.

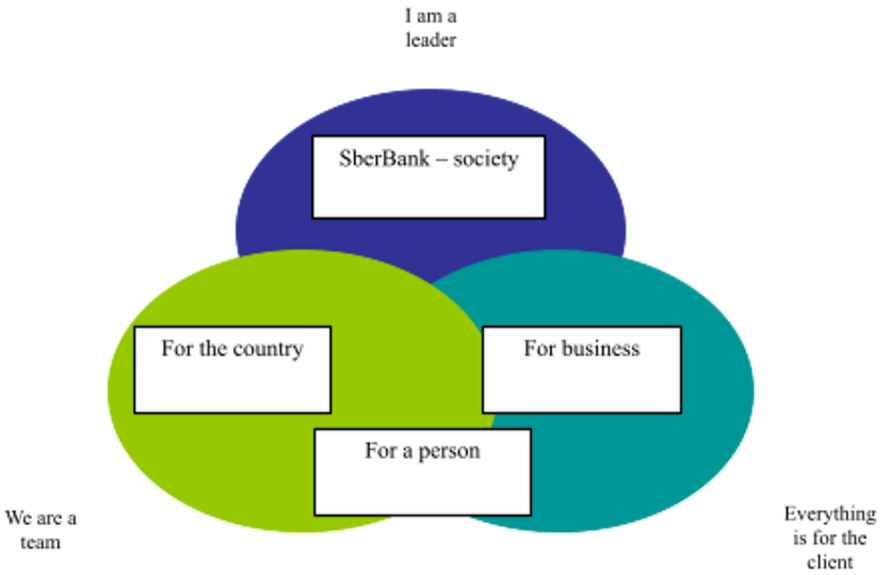

Fig. 2 A systematic approach to understanding the values and strategy of PJSC Sberbank of Russia. Obtained by the authors on the basis of a study on *[10]*.

5 Conclusion

The practical significance of the obtained results lies in the development of methodological recommendations for conducting cluster analysis of organizations, both in terms of the group of indicators assessing the level of information authentication and the level of utilization of specialized software tools and information security instruments. This will allow for assessment and the construction of a rating of organizational information security.

The conclusion has been made that the most successful organizations are financial institutions and organizations in the field of information technology. Due to the revision of their core business processes in the context of digitization, they have been able to transform into leading technological companies, many of which have formed a comprehensive ecosystem. Thanks to this, they were able to quickly adapt to the changing conditions, which would have been impossible without the implementation of digital transformation processes. Therefore, it is necessary to implement a comprehensive approach to improving the management of domestic organizations in the context of digital transformation and reevaluate existing approaches to the implementation of processes related to increased information vulnerability.

References

1 A. M. Astakhov, The Art of Information Risk Management. Moscow: DMK-Press, **312** p. (2019).

2 V. S. Barnagyan, Changes in Management during the Transition to Digitization. Economic Problems of Russia and the Region. Scientific Notes. Issue No. **27**. Publisher: Rostov State Economic University "RINKH" (Rostov-on-Don), Rostov-on-Don, pp. **118-125**. (2022).

3 N. V. Grineva, Theoretical Aspects of Information Risks. Accessed on: April 04, 2023. [Online]. Available: https://cyberleninka.ru/article/n/teoreticheskie-aspekty-informatsionnyh-riskov. (2019).

4 T. V. Gurunyan, Institutional Barriers of Digital Transformation for SMEs. Innovations and Investments. Accessed on: April 15, 2023. [Online]. Available: https://cyberleninka.ru/article/n/institutsionalnye-bariery-tsifrovoy-transformatsii-subektov-msp. (2023).

5 Dynamics of Cyber Threats in Russia for March-April 2019. Accessed on: April 08, 2023. [Online]. Available: https://cybermap.kaspersky.com/ru. (2019).

6 G. V. Egorova, O. Yu. Fedoseeva, Enterprise Information Risk Management. Bulletin of VUIT. Accessed on: March 04, 2023. [Online]. Available: https://cyberleninka.ru/article/n/upravlenie-informatsionnymi-riskami-predpriyatiya-1. (2021).

7 Indicators of the Digital Economy: 2022: Statistical Compilation. G. I. Abdrakhmanova, S. A. Vasilkovsky, K. O. Vishnevsky, L. M. Gokhberg, et al.; National Research University "Higher School of Economics". Moscow: NRU HSE, **332** p. Accessed on: March 10, 2023. [Online]. Available: https://issek.hse.ru/mirror/pubs/share/780810055.pdf. (2023).

8 I. A. Kiseleva, S. O. Iskajyan, Information Risks: Assessment and Analysis Methods. ITportal. No. **2 (14)**. Accessed on: May 15, 2023. [Online]. Available: https://cyberleninka.ru/article/n/informatsionnye-riski-metody-otsenki-i-analiza. (2021).

9 V. V. Kuzmin, Information Risks in the Post-Industrial Society. Manuscript. 2018. No. **9 (95)**. Accessed on: May 14, 2023. [Online]. Available: https://cyberleninka.ru/article/n/informatsionnye-riski-v-postindustrialnom-obschestve. (2018).

10 Official Website of Sberbank of Russia. Electronic resource. Accessed on: May 14, 2023. [Online]. Available: https://2017.report-sberbank.ru/pdf/ar/ru/performance-overview_best-customer-experience_retail-clients_loans.pdf.

11 Pestova, R. G. Information Risk Management. Innovative Science. No. **6-1**. Accessed on: March 17, 2023. [Online]. Available: https://cyberleninka.ru/article/n/upravlenie-informatsionnymi-riskami. (2018).

12 Strategy of Economic Security of the Russian Federation until 2030. Decree of the President of the Russian Federation dated May 13, 2017, No. **208**. Accessed on: March 10, 2023. [Online]. Available: https://www.garant.ru/products/ipo/prime/doc/71572608/16

13 O. P. Shamkina, Information Security Risks in Credit Organizations. Financial Markets and Banks. No. **3**. Accessed on: March 19, 2023. [Online]. Available: https://cyberleninka.ru/article/n/riski-informatsionnoy-bezopasnosti-v-kreditnyh-organizatsiyah. (2018).

14 Digital Economy of the Russian Federation. National Program. June 4, 2019. Ministry of Digital Development, Communications, and Mass Media of the Russian Federation. Accessed on: April 13, 2023. [Online]. Available:

https://digital.gov.ru/ru/activity/directions/858/?utm_referrer=https%3a%2f%2fwww.google.com%2f. (2019).