European Proceedings of
Multidisciplinary Sciences
EpMS

www.europeanproceedings.com

e-ISSN: 2421-826X

DOI: 10.15405/epms.2024.09.54

MTMSD 2022
I International Conference «Modern Trends in Governance and Sustainable Development of Socio-economic Systems: from Regional Development to Global Economic Growth»

THREATS AND RISKS OF DIGITAL TRANSFORMATION

Aza Aindievna Bisultanova (a)*
*Corresponding author

(a) Kadyrov Chechen State University, Grozny, Russia, nauka-fef@mail.ru

Abstract

The research investigates the threats and risks associated with the process of digital transformation across various sectors. The primary objective is to identify, analyze, and categorize potential threats and risks that organizations may encounter during their digital transformation initiatives. The study employs a comprehensive approach, combining literature reviews, case studies, and expert interviews to gather and analyze data. The research methodology involves an extensive review of existing literature on digital transformation threats and risks. Case studies from diverse industries are examined to extract real-world scenarios and challenges faced by organizations undergoing digital transformation. Additionally, expert interviews with professionals in the field contribute valuable insights into nuanced aspects of digital risks. The triangulation of these methods enhances the robustness of the findings. One notable outcome of the research is the identification and classification of various threats and risks that organizations must navigate in the digital transformation landscape. These encompass cybersecurity vulnerabilities, data privacy concerns, organizational resistance, technology integration challenges, and unforeseen cultural shifts. The research provides a structured framework for understanding these risks, enabling organizations to proactively address and mitigate potential issues.

Keywords: Digitalization of the economy, information security, threats and risks of information security

https://doi.org/10.15405/epms.2024.09.54
Corresponding Author: Aza Aindievna Bisultanova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

1. Introduction

The modern world order is impossible without an appropriate level of "digitization". Digitalization is an objective necessity in modern, rapidly developing economic conditions. However, modern theoretical studies of the essence of the digital economy have not come to a consensus on what this concept still includes. Moreover, the concepts include both goods and services created with the help of digital technologies; and digital access to goods and services. Considering the process of digitalization, you invariably encounter such concepts as "digitization" and "digitalization". It is also worth noting that these concepts are not identical. "Digitization" is a more limited concept than "digitalization". Digitization involves the modification of information into digital form whereas the process of digitalization has a broader interpretation. The digitalization process involves the use of digital technologies for faster and better performance of tasks. The process of digitalization itself is of global importance for humanity. Despite its absolute necessity, it is also impossible not to recognize the potential threats that it carries with it. Accordingly, humanity also faces the task of not only the speedy introduction of modern achievements of science and technology, but also the neutralization of threats caused by excessively rapid rates of digitalization (Kirishchieva et al., 2021). Since the coming years will be critically important for Russia in terms of maintaining national interests and increasing competitiveness in the world market. It is necessary to take all necessary measures in the legal and economic spaces of the country in order for the Russian Federation to occupy a worthy niche in the digital field. It should also be borne in mind that digital inequality will increase, lead to a deepening of technological inequality, there will also be ethical problems associated with the transformation of the person himself under the influence of digital technologies.

2. Problem Statement

In the contemporary global landscape, economic development at both the macroeconomic and microeconomic levels faces significant challenges arising from destabilizing factors, geopolitical tensions, and escalating military conflicts. These challenges compromise the economic well-being of nations and corporations alike. In particular, the advent of digital transformation introduces a myriad of threats and risks that demand urgent attention. It is imperative for both governments and corporations to bolster their economic and information security measures to effectively counteract these challenges. Hence, there arises a critical need to systematically identify, categorize, and address the risks and threats confronted by enterprises in the digital economy, with a specific focus on enhancing their electronic security systems.

3. Research Questions

i. What are the risks and threats faced by enterprises in the digital economy concerning their security?
ii. How can the electronic security system be enhanced to effectively counteract the identified risks and threats?

https://doi.org/10.15405/epms.2024.09.54
Corresponding Author: Aza Aindievna Bisultanova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

iii. What measures should be implemented to elevate the level of digital literacy and information culture across all segments of the population?

These research questions serve as the focal points for investigating the multifaceted challenges related to digital transformation, electronic security, and the broader goal of fostering digital literacy and information culture. The study aims to provide valuable insights for policymakers and stakeholders to formulate strategies that strengthen economic and information security while navigating the complexities of the digital era.

4. Purpose of the Study

i. Examine and understand the risks and threats confronted by enterprises in the digital economy.
ii. Propose strategies to enhance the electronic security system, offering effective countermeasures against identified risks and threats.
iii. Emphasize the significance of elevating digital literacy and information culture across diverse segments of the population.

By achieving these objectives, the study aims to equip policymakers and stakeholders with comprehensive insights, enabling them to make well-informed decisions. Ultimately, the goal is to contribute to the reinforcement of economic and information security while effectively addressing the challenges posed by digital transformation.

5. Research Methods

In this scientific article, the following research methods are employed:

1. System Analysis:

i. Description: Applied to study interrelations in digital transformation, identify key risk factors, and understand their impact on the system.

2. Empirical Document Analysis:

ii. Description: Academic articles, reports, and laws are analyzed to form an overview of the current state of knowledge and highlight commonly accepted terms.

3. Expert Interviews and Surveys:

iii. Description: Involves interacting with experts to gather their opinions on specific threats and risks in digital transformation.

These methods ensure a comprehensive analysis of threats and risks by combining a systems approach, literature review, and expert assessments.

Speaking in more detail about the threats and risks associated with the digitalization of all spheres and areas of human activity, it is worth emphasizing that the process of digital transformation is a transition from tangible assets to intangible (digital) assets. Therefore, the following classification of risks and threats associated with the digital transformation of the economy can be given (Figure 1):

https://doi.org/10.15405/epms.2024.09.54
Corresponding Author: Aza Aindievna Bisultanova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

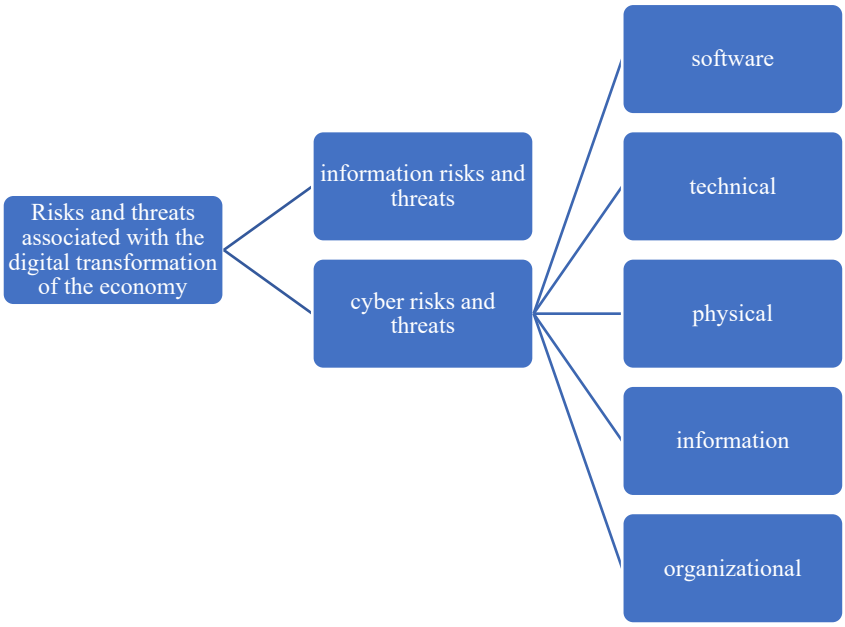

Figure 1. Risks and threats associated with the digital transformation of the economy

Information risks and threats are threat risks associated primarily with the risk associated with the use and dissemination of information. Since it is information that is one of the most important management resources, then issues related to maintaining the integrity, credibility and reliability of its storage and use are among the key issues in the activities of any organization. Information risks and threats depend on complex information systems, which in turn are influenced by factors that can be classified as hidden and open. Hidden factors affecting information systems include excessive information consumption, human factors, unintentionally caused by customers, suppliers or employees problems with the functioning of the information system (Markov, 2010).

The obvious factors affecting information systems include the level of maturity of the management apparatus, the degree of automation and informatization of the organization itself, etc. At the same time, we emphasize once again that the main source of information risks are information assets, which include any information and data in digital form (digital models of business processes, digitized services, digital content, digital services, databases, web resources, software, etc.) (Dzhemaldinova et al., 2021).

The second group of risks is the risks and threats to information cybersecurity. One of the most important characteristics of information is that it does not disappear when it is used, that this resource is not tied to the place, time and subject of creation. Consequently, these signs of information contribute to the fact that it becomes the object of cyber-attacks, in order to achieve vulnerability and gain access to confidential information, which in the future will contribute to the organization receiving direct financial losses, reducing business reputation, etc. (Kazaryan, 2022; Vasyukov et al., 2021).

Cyber risks, unlike information threats and risks are the result of deliberate impact on information, data in digital form, the functioning of information resources and systems in the digital space. Cyber risks, in turn, can also be classified depending on their nature into the following types:

i. programs;
ii. technical;
iii. physical;

https://doi.org/10.15405/epms.2024.09.54
Corresponding Author: Aza Aindievna Bisultanova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

iv. information;

v. organizational.

If we look in more detail at each of the types of cyber risks, then the first group of cyber risks, that is, software ones, is associated with the introduction of malicious programs that destroy and distort data in information systems, and this can happen both intentionally and unintentionally.

Technical cyber risks are risks associated with external influence on data transmission channels in order to exert influence entailing distortion of information.

Physical cyber risks are risks associated with the destruction and damage of information processing and storage facilities, as well as electronic keys for access and authentication.

Informational – cyber risks associated with violation of the rules of exchange and dissemination of information, risks associated with unauthorized access to digital information, illegal copying and dissemination of information, etc.

Organizational risks are risks associated with the inefficiency of the organization's activities to protect digital rights and digital information, insufficient effectiveness of methods and means of protecting information from unauthorized access and theft (Chenzeeva, 2021; Chesnokov, 2022).

At the present stage of economic development, there is no methodological basis for determining the magnitude of risks and threats of digital transformation. First of all, the reason for the lack of methodological bases for determining the quantitative magnitude of risk is the lack of a statistical base for the study. Secondly, the difficulty of determining the value of a particular information unit should be mentioned (Derevyanchenko & Kalinin, 2020). However, despite the apparent complexity of determining the risks of digitalization, it is impossible to deny the need to solve the primary task in the conditions of total digitalization - the development of methods and means of forecasting and combating the threats and risks of digitalization. Since the development of methods and tools for forecasting and combating the threats and risks of digitalization will rationalize the human, financial digital resources of the enterprise, and, consequently, will further lead to an increase in the competitiveness of enterprises, the country as a whole (Chesnokov, 2022).

6. Findings

The findings reveal a historical perspective on the recognition and prioritization of information security by governments globally. The initiation of knowledge formation on information security began with the issuance of the "Criteria for Evaluating Reliable Computer Systems" by the US Department of Defense in 1983. Similar documents were subsequently published in European countries, and in 1992, the Russian State Technical Commission addressed the issue of protection against unauthorized access.

In a contemporary context, the data from 2021 highlight a significant focus on information security, with the adoption of 287 regulatory legal acts. This emphasizes the continued commitment of governments to address evolving threats and risks in the digital era, reflecting the dynamic nature of information security efforts.

https://doi.org/10.15405/epms.2024.09.54
Corresponding Author: Aza Aindievna Bisultanova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Table 1. Number of regulatory legal acts adopted

I quarter 2021	**28**
II quarter 2021	57
III quarter 2021	91
IV quarter 2021	111
Total accepted regulatory legal acts for 2021	287

Source: (InfoWatch Expert and Analytical Center, 2022).

According to the table (Table 1), it can be concluded that during 2021, the state paid due attention to the issues of the state's rule–making activities in the field of information security and the digital economy, and the 4th quarter of 2021 turned out to be the most fruitful - almost 40 percent of all normative legal acts adopted in 2021 fell on the 4th quarter. If in the future we proceed to a more detailed analysis of regulatory legal acts in the field of information security and the digital economy to consider the structure of the adopted regulatory legal acts by topic, then we can output the data in the following table 2:

Table 2. Adopted regulatory legal acts in the field of information security and digital economy, on the following topics

Subject of the regulatory legal act	**Number of accepted acts**	**Share of total %**
Digital Economy	129	45%
Biometrics and personal data	51	18%
Information security (IS, TIP)	45	16%
Import substitution	18	6%
National security	10	3%
CII safety	9	3%
Licensing of TIP and master data management activities	9	3%
State secret	8	3%
Certification of ISS and CIPF, certification of objects informatization	6	2%
Accreditation and expertise in the field of information security and IT	2	1%
Sum total	287	100%

Source: (InfoWatch Expert and Analytical Center, 2022).

As can be seen from the table, half of the adopted regulatory legal acts relate to the digital economy – 45%, the next place in terms of the number of adopted acts was taken by the topic of biometrics and personal data - 18%, the third place with a share of 16% was taken by the topic of information security. All this indicates that the pandemic and the consequences of coronavirus infection have led to a sharp jump in digitalization processes. The coronavirus infection has led to the need to activate trade through digital platforms, to the development of such digital services that would allow you to continue your studies in order to preserve the health of yourself and others (Tavbulatova & Tashtamirov, 2020; Udalov, 2018). Enterprises and organizations had to transfer their employees to remote work, which also required the development and implementation of appropriate programs and

https://doi.org/10.15405/epms.2024.09.54
Corresponding Author: Aza Aindievna Bisultanova
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

technologies. In this regard, it is also worth noting the financial benefits of transferring employees to a remote work mode, since it will not require renting office space, paying utility bills, and office infrastructure costs. According to numerous studies, the "work from home" saves about 25 percent of the costs of the operation of the enterprise.

7. Conclusion

In conclusion, the study underscores the imperative for increased state control in the contemporary business and governmental landscape due to the unconventional threats and risks posed by digital transformation. Despite the positive aspects associated with digitalization, it is crucial for the state to minimize risks that may jeopardize the socio-economic environment. The gap between the speed of digitalization and the comprehension of associated processes is rapidly widening, and although digitalization may lead to increased state control, the real threats it presents are challenging to fully grasp and prevent.

Identifying potential threats to develop means of neutralization becomes a key task for both the state and the business environment. Recognizing the need for a gradual increase in information culture and digital literacy across all segments of the population, irrespective of differences, is crucial. Success in digitalizing the economy relies heavily on the digital literacy of legal entities and individuals, necessitating enhanced educational activities at all levels, including distance technologies. Attention to improving educational program content, establishment of scientific and educational centers, and global cooperation between countries for the spread of digitalization processes are essential components for addressing challenges associated with digital transformation.

In addressing digital risks, it is acknowledged that no single entity, whether at the micro or macro level, can independently cope with the challenges. Interconnectedness and interdependence across all levels highlight the necessity of global cooperation for effective solutions and minimizing global risks in the ever-evolving landscape of digital technologies.

References

Chenzeeva, D. V. (2021). Risks and threats of the digital economy, ways to solve them. *Materials of the XIII International Student Scientific Conference Student Scientific Forum*. https://scienceforum.ru/2021/article/2018023816

Chesnokov, A. D. (2022). Information security. *StudNet, 1*. https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-6

Derevyanchenko, A. A., & Kalinin, D. V. (2020). Digital Society: New opportunities and old threats. *Scientific Works of the Moscow University for the Humanities, 6*. http://doi.org/10.17805/trudy.2019.6.2

Dzhemaldinova, M. Y., Esmurzaev, Z. K., & Guzueva, E. R. (2021). Industry 4.0. Digital transformation of business. *Trends in the development of natural sciences in the modern information space and their application in agrobiotechnologies. Collection of articles of the I student scientific and practical conference* (pp. 52-56). Kadyrov Chechen State University. https://doi.org/10.36684/51-2021-1-52-56

InfoWatch Expert and Analytical Center. (2022, March 10). *Review of regulatory legal acts in the field of information security and the digital economy by the end of 2021*. www.infowatch.ru/analytics

Kazaryan, K. K. (2022). Cybersecurity risk management. *StudNet, 5*(1). https://www.elibrary.ru/item.asp?id=47890290

Kirishchieva, I., Skorev, M., Mishchenko, O., & Grafova, T. (2021). Risks and threats to economic security in the digital economy. *SHS Web of Conferences, 110*, 01028. https://doi.org/10.1051/shsconf/202111001028

Markov, A. A. (2010). The concept and characteristics of information risks, dangers and threats in modern post-industrial society. *Logos et Praxis, 1*. https://cyberleninka.ru/article/n/ponyatie-i-harakteristika-informatsionnyh-riskov-opasnostey-i-ugroz-v-sovremennom-postindustrialnom-obschestve

Tavbulatova, Z. K., & Tashtamirov, M. R. (2020). Regional trends of digitalization of the banking sector. *Business and Education in the Digital Economy. Materials of the All-Russian scientific and practical conference with international participation* (pp. 70-79). Alef. https://www.elibrary.ru/item.asp?id=44619164

Udalov, D. V. (2018). Threats and challenges of the digital economy. *IDB, 1*(30). https://cyberleninka.ru/article/n/ugrozy-i-vyzovy-tsifrovoy-ekonomiki

Vasyukov, V. F., Bisultanova, A. A., Kuchkovskaya, N. V., & Pershin, A. N. (2021). Cyber fraud: information threat of the past, present and future. *Questions of history, 11*-3, 275-281.