Okhrimenko, Igor; Stepenko, Valery; Chernova, Olga; Zatsarinnaya, Elena

Article

The impact of information sphere in the economic security of the country: Case of Russian realities

Journal of Innovation and Entrepreneurship

Provided in Cooperation with:
Springer Nature

Suggested Citation: Okhrimenko, Igor; Stepenko, Valery; Chernova, Olga; Zatsarinnaya, Elena (2023) : The impact of information sphere in the economic security of the country: Case of Russian realities, Journal of Innovation and Entrepreneurship, ISSN 2192-5372, Springer, Heidelberg, Vol. 12, Iss. 1, pp. 1-18, https://doi.org/10.1186/s13731-023-00326-8

This Version is available at:
https://hdl.handle.net/10419/290312

Okhrimenko *et al.*
Journal of Innovation and Entrepreneurship (2023) 12:67
https://doi.org/10.1186/s13731-023-00326-8

Journal of Innovation and Entrepreneurship

RESEARCH Open Access

The impact of information sphere in the economic security of the country: case of Russian realities

Igor Okhrimenko[1*], Valery Stepenko[2], Olga Chernova[2] and Elena Zatsarinnaya[3]

*Correspondence:
okhrimenko_igor@rambler.ru;
ivokhrimenko@fa.ru

[1] Department of Insurance and Social Economy, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
[2] Department of State Legal Disciplines, Pacific State University, Khabarovsk, Russian Federation
[3] Department of Financial Control, Analysis and Audit, Main Control Department of the City of Moscow, Plekhanov Russian University of Economics, Moscow, Russian Federation

Abstract

Novel information technologies have facilitated not only the development of new industries, but also brought new opportunities and challenges. The range of challenges includes threats related to the information security of not only the commercial, but also the public sector of the national economy, which can adversely affect its stability and competitiveness. In view of this, the problem of ensuring information security (IS) in the economic sphere is of particular relevance. Despite the abundance of studies on IS, the impact of the information sphere on the country's economic security has not yet been sufficiently studied. The purpose of this article was to identify and systematize threats posed to economic security by the information environment and determine a set of measures to protect the areas at risk. Within the framework of the study, two interrelated models were built. The first systematized the IS threats and challenges, whereas the second demonstrated those IS threats that are directly connected with the state's economic security. At the same time, the models developed allowed focusing on the protection of objects potentially under threat. The research quintessence was represented by the development of recommendations directed at preventing and minimizing the negative impact of information sphere threats to economic security. Hence, a diversified ecosystem of information and economic security of the state was created. The study findings and recommendations can be used by officials of government bodies and other organizations to develop regulatory documents related to the strategy of ensuring information and economic security at various levels (state, regional, corporate).

Keywords: Security strategy, Information security, Information and communications technologies, Cybercrime, Informatization

Introduction

For the modern world economy, the interconnectedness of subjects, both private business and the state, is aimed at meeting their own needs and ensuring sustainable development. This is confirmed by the common efforts to introduce innovations that can improve the production and consumption of those services, products that provide tangible or intangible benefits. However, such actions can be carried out only if the security of conducting the processes of economic transactions is ensured. At the same time, the

understanding of security for each country is unique in terms of its own national security policy (Hacker et al., 2018). Meanwhile, in recent decades, given the ongoing globalization and economic integration, the relationship between the economy and national security has become increasingly interlinked. The open and interconnected nature of most economies creates risks from potential internal and external threats. Consequently, the country's economic security has emerged as an important strategic priority for its government (Retter et al., 2020).

Geopolitical instability, cyclical exchange rate fluctuations, the recession of the global and national economies, the halt of entire sectors of the economies caused by both previous global economic crises and the COVID-19 pandemic, structural dysfunction of certain economic sectors against the backdrop of sanctions pressure as a result of the military conflict with Ukraine (where the full economic damage cannot yet be assessed due to the ongoing processes of military confrontation)—all these factors adversely impact the country's economic activity. Military action especially raise the state's economic security to a new level of concern, since military instability and armed conflicts directly affect the quality of life of the population, the satisfaction of its needs and the possibility of financial planning, at least at the level of households, and at the level of the entire state. Thus, in order to reduce the risk of disasters, increase public and social protection, the security of the country's economy is an integral structural component of the national security system (Gontar et al., 2019; Metelev et al., 2016; Nicola et al., 2020).

Information has become one of the crucial factors affecting the development of the global and regional economies. However, information technologies have brought not only new opportunities, but also challenges and threats. Therefore, within the framework of economic resilience, data security acquires particular importance (Skripina, 2016). Many states are seriously concerned about information security (IS) issues, including those of information storage and non-disclosure. This has led to the emergence of a new "economy of secrecy" concept when secrecy shapes interstate relations by tuning the ratio of "knowledge" and "ignorance". The economy of secrecy involves cooperation between states in certain areas that affect their international image and that constitute a matter of national security: the fight against terrorism, the methods of combating which are undesirable for public opinion. That is, perception and representation are linked to the economy of secrecy: precisely because states want to be able to control their image and influence the perception of other actors, they are willing to maintain a certain level of secrecy in their relations with other states (Balzacq & Puybareau, 2018).

In the context of a modern state, the information space, as one of the sources of vulnerabilities and an object of IS, performs numerous constructive and destructive functions and directly impacts the country's economic security. Among the constructive, on the one hand, we can include the mobilization of society in the face of a common threat to security, while on the other hand, this provides opportunities for the dissemination of propaganda. On the other hand, the security of the information space can also be destructive due to the insecurity of individual components, which can serve as the basis for the success of various kinds of data leaks and sabotage from outside (Barannik et al., 2019). Transition to the information society has dramatically changed the status of information resources. Today, information processes affect many economic sectors and spheres of activity, including health and safety, education,

science, culture, quality of life, and socio-political sphere (Svetlakov & Glotina, 2018). Technologization, digitalization (transition of the economy and the social sector to digital technologies of functioning and interaction), and the national intellectual capital are the basic country's competitive advantages that require proper IS (Frolova et al., 2018).

By controlling the information flows and data delivery, the government can control social and economic processes. That is why modern technologies of economic confrontation are moving to cyberspace. The state's cyber power is characterized by the country's ability to use cyberspace for its own benefit and obtain the ability to influence various domains, including the economic one, thereby endangering its own economic security (Cheskidov, 2013).

Having such trends, it is necessary to correctly assess the risks of their application. This is especially true for countries with a large sales market and resource-based economies. In the context of this study, Russia is of interest as a country that, due to its current political and economic activities, is trying to painlessly establish the process of transition to a new type of management, solving the issue of increasing its competitiveness in the world market. At the same time, in view of the continuing technological backwardness in the regions, Russia needs to intensify its digital security policy in order to ensure the smooth operation of agriculture, industry, and the service sector (Petrenko, 2018b). This is especially true against the background of such threats as the negligence of the management of industrial spies, information sabotage (hacker attacks) associated with the dissemination of possible fake information, manipulation of personal data, sanctions restrictions, etc. Given these factors, in order to guide the further progressive development of the information society in Russia, the foundations were laid for the formation of a digital economy, marking the beginning of the intensive use of modern digital technologies by government organizations, businesses and citizens (Popov & Semyachkov, 2018). The question remains in the implementation of the adopted strategies. That is why the importance of the study is explained by the search for optimal options for responding to problems affecting the economy and its competitiveness, followed by the development of a system for evaluating actions to level the threats to economic security from the information environment and determining a set of protective measures, while simultaneously developing relevant ways to monitor new risks and threats to the national economy, especially those industries that are strategic. This assessment of the threat of challenges to information security is the subject of this study. The purpose of the study is to identify and systematize threats to economic security from the information environment and to determine a set of measures to protect risk zones. In view of this, the article aims to identify and systematize threats information environment poses to economic security and determine a set of measures to protect the areas at risk using the state of affairs in Russia as an example. This goal can be achieved after the solution of the following tasks:

1. Identify the challenges and threats to the IS of the country;
2. Highlight the information sphere threats that can directly affect the economic security of the country;
3. Determine a set of measures to protect economic security.

Literature review

Speaking of a strategy for ensuring economic security, it should be based on a structural–functional approach and provide for the setting of strategic and tactical goals, as well as criteria—quantitative indicators that determine the degree of achievement of goals. However, the successful application of this approach cannot be implemented without a clear understanding of the theoretical basis of economic security and its derivative components, including informational, which intersects with the topic of this study. The same cybersecurity allows you to maintain the proper level of economic calculations, which is essential to maintain the stability of the entire economic system, and any failure to inform about the current situation can lead to unpredictable consequences (Senol & Karacuha, 2020). Nevertheless, to date, no single and generally accepted meaning of the economic security of the state exists. Murdoch et al. (2001) believe that economic security must meet two main conditions: (1) the preservation of the country's economic independence and the ability to make decisions concerning the economy pursuing its own benefit, and (2) maintaining already achieved living standard and the potential for its further improvement. Peppers (2017) argues that the basis of the country's economic security holds the entrepreneurial security and free-market system (heterogeneous and dynamic complex adaptive economic system, where activities are spontaneous, adaptive, decentralized, leaderless, and self-organizing).

Economic security is also referred to as the security of economic relations that greatly influences the development of the country's economic potential and ensures its increasing economic growth, which also contributes to the enhancement of the country's independence and defense capability in the economic sphere (Amirov et al., 2018). In the meantime, some scholars define economic security as a protection of the vital interests of a person, society and the country in the economic sphere from internal and external threats to ensure sustainable economic development of the state and society (Metelev et al., 2016). From the point of view of the state, such a paternalistic concept in the form of a policy of protectionism in economic life is typical for Asian countries or countries with a resource-based economy, such as Russia and China. The essence of the economic security of the two countries began to form and implement only in the latest period of their history in the context of a sharp transformation of socio-economic relations. At the same time, in Western countries, the concept of economic security is still used mainly in relation to ensuring the protection of individuals and companies from adverse conditions and factors associated with the presence of certain financial problems. In the legislation of many Western countries, including the United States, the concept of "economic security" is practically not used. When it comes to ensuring the protection of national interests in the economic sphere, these issues are considered together with issues of national security (Snegovaya, 2017).

Jankovska et al. (2018) propose one of the most detailed definitions of economic security, describing it as a process of ensuring sustainable and safe economic system development where the economy is able to solve the following tasks:

- Ensure national economic and energy independence and sovereignty;
- Effectively meet the material needs of a person, society and the country;
- Maintain the required level of social and political stability of society;

- Create conditions for the harmonious development of economic contacts;
- Protect domestic and foreign markets;
- Protect all forms of ownership;
- Ensure the stability of the national economy under conditions of unforeseen worsening of international economic relations;
- Ensure the national economy's resilience to natural and human-made disasters or various types of armed conflicts;
- Eliminate criminal organizations' impact on the economy.

The Strategy of Economic Security of the Russian Federation until the year 2030, published in May 2017, describes economic security as the preservation of national sovereignty by the defense against external and internal threats. At the same time, the provision of IS it defines as the implementation by state authorities, local governments and the Central Bank of the Russian Federation in cooperation with civil society institutions of a complex of political, organizational, socio-economic, informational, legal and other measures to counter economic security threats and challenges and protect the interests of Russia in the economic sphere.

The information sphere also acts as a specific carrier of safety concerns to the country's economic security. In modern conditions, informational impacts on economic processes are becoming more and more aggressive. Hence, cosmic economic losses may occur, for example, when negative information through the impact on stock markets causes a decrease in enterprises' capitalization, which in this case may be bought at a reduced price. An enterprise's competitiveness can also be harmed by means of adverse information dissemination with the aim of creating a negative image of one's competitor (Kosovets, 2011). At the global level, information attacks tend to develop into organized cybercrimes, and even cyberwars. Pursuant to the research conducted, the number of cybercrimes in the economic sector is increasing every year, both in the Russian Federation and around the world. Cybercrime is one of the global problems of the modern information community (Khochueva & Shugunov, 2020).

An additional point that merits mention is the spread of hoaxes, fakes and hate speech through information technology, primarily through websites and social networks. Hoaxes and fakes are often politicized and modified in favor of both economic and political interests. As a means of furthering specific political interests, their active spread may potentially threaten national security and stability (Gunawan & Ratmono, 2020).

In recent years, organizations large and small are exposed to more frequent and severe threats in the digital environment, which affects their economic security. From an economic point of view, such threats can affect the reputation of organizations, the financial component, damaging their competitiveness, undermining their innovation efforts and market position. Such threats can compromise the availability, integrity, or confidentiality of the information systems on which economic activity is based (Scott, 2004). Moreover, one of the challenges for the country's information and economic security is the leakage of not only classified state information, but also corporate, primarily represented by unique technical data required for the development, production, supply, and use of products or services. Such a leakage negatively affects companies, related industries, and the whole country (Na et al., 2019). According to the National Industrial Security

Center, South Korea faces over 100 cases of data leakage incidents every year, 86% of which occur in small and medium-sized enterprises. In particular, from 2013 to 2018, 637 such incidents were registered by the local authorities (National Industrial Security Center, 2018).

Along with the significant benefits, information technology brings complex problems related to e-government and IS management (Huang & Farn, 2016). Thus, managing the effective security of personal citizens' data located in computer networks has become a strategic business and public policy issue for the state's economy and IS (Hemphill & Longstreet, 2016; Peleshchyshyn et al., 2018).

Due to rapid technological development and growing dependence on information and communications technology (ICT), most infrastructure facilities critical for the national and economic security of the state (energy, transport, communications, financial services, etc.) are now operated, managed and/or controlled via interconnected computer networks and information flows. In view of this, they have become critical information infrastructures (CIIs), the protection of which is among the country's priority tasks (Newlove-Eriksson et al., 2018). Today, the matter of IS improvement comes to the fore due to the enhanced number of cyberattacks on information systems of financial structures, government agencies, and industrial manufacturing complexes (Fedotova et al., 2019). According to the data provided by the Russian National Coordination Center for Computer Incidents, in 2018, more than 4.3 billion cyberattacks to the critical information infrastructure (CII) of the Russian Federation were revealed (mainly on banks and government bodies) (Bareiko & Kozhukhina 2019).

In general, IS means ensure the confidentiality, integrity, and availability of data, as well as accountability and confidence that all processes are carried out according to the approved protocols (White et al., 2019). Its central aim is timely detection and further prevention of IS threats and incidents (Boranbayev et al., 2018). IS is ensured through the implementation of a complex set of policies, procedures and organizational structures that have dynamically evolved over the last decade owing to the rapid globalization and IT-based business processes expansion, which include both institutional development (creation of structural units responsible for information security, clusters of data protection and digital infrastructure) and the adoption and updating of doctrines regarding the legal regulation of information protection, including technical guidelines for data protection and structuring models (Cristea, 2020). Improper risk analysis may potentially result in the failure of IS systems (Alavi et al., 2016).

State-of-the-art literature uses many different terms to describe information security. These are "Information Systems Security", "IT Security", "Cyber Security", and "Cyber Resilience" (Diesch et al., 2018). The terms "cybersecurity" and "information security" are often used as if they are synonyms (Luiijf et al., 2013). Recently, the words "digitalization", a derivative of "digital security" with "informatization", can also be called synonymous, they are in any way associated with a set of measures aimed at digitalizing the activities of an organization, enterprise, etc. (Mansurov, 2021). Although von Solms and van Niekerk (2013) argue that IS is about protecting information as an asset, in physical or non-physical form, while cybersecurity is concerned with protecting both information and non-information assets through the ICT infrastructure. Information assets are, in fact, an integral part of such an infrastructure, so both terms should be considered

identical (Azmi et al., 2016). As a result of the analysis of 28 authoritative sources presenting the notion of "information (or cyber) security", Schatz et al. (2017) have derived a generalized definition of this concept. Researchers describe IS as the approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyberspace. They also state that this concept includes guidelines, policies and collections of safeguards, technologies, tools, and training to provide the best protection of the cyber environment and its users.

The problem of ensuring the economic and information security of the Russian Federation, including in terms of information and other technologies, is of particular concern due to the globalization of the world economy and the country's integration into the international economic system (Metelev et al., 2016). Today, Russia is experiencing growing risks of rapid informatization, vividly manifested in harming various spheres of society and the state actions classified as criminal due to their danger. In the context of the formation of a global post-industrial society, among many other problems of socio-economic development of Russia, a prominent place is occupied by the organization of the sustainable functioning and safety of information systems and information communication networks (Bareiko, 2019).

The Doctrine of Information Security of the Russian Federation approved by the Decree of the President of the Russian Federation on December 5, 2016, defines IS as the state of protection of the individual, society and the State against internal and external information threats, allowing to ensure the constitutional human and civil rights and freedoms, the decent quality and standard of living for citizens, the sovereignty, the territorial integrity and sustainable socio-economic development of the Russian Federation, as well as defense and security of the State (The President of the Russian Federation, 2016). The IS of Russia at various levels (federal, regional, corporate) is represented as a subject for investigation in many studies. As a result, a considerable number of scholars have already reviewed the organizational, legal, and technical aspects of this concept. Frolova et al. (2018) describe an IS system as a set of corporate rules, work standards, and security procedures based on an audit of a company's information system and an analysis of existing security risks that follow the requirements of regulatory documents of the Russian Federation and the IS standards provisions. After a comprehensive investigation of Russia's economic and information security, the authors conclude that the most important area of development of the national economy is the protection of vital human interests, the key element of which is IS.

Cheskidov (2013) has reviewed information warfare as a means of economic confrontation in cyberspace and defined it as a set of measures to achieve information superiority by influencing the information, information processes, information systems, and computer networks of the enemy while protecting the same aspects of one's own country. Fedotova et al. (2019) have examined the transformation of existing IS systems of large enterprises in the context of the ongoing digitalization of the national economy of the Russian Federation and distinguished several security problems of online systems associated with its implementation.

Many works are devoted to the technical aspects of ensuring the IS of the state, region, or even the enterprise. Arutyunov (2017) has systematized and compiled a list of all

current Russian IS standards and distinguished clusters of standards that allow evaluating the maturity of used technologies in various IS areas. In the meantime, Tsaregorodtsev et al. (2018) have developed a methodology for assessing information risks while using cloud technologies and substantiated the need to use private clouds with a high degree of protection. Concentrating on the problem of creating a cybersecurity system for critical state information resources, Petrenko (2018a) has synthesized early warning and opponent deterrence scenarios in the cyberspace of the Russian Federation on extremely large volumes of structured and unstructured information from a variety of sources (Internet/Intranet and IIoT/IoT). In turn, Yankovskaya et al. (2016) propose to build a hybrid intelligent system of express-diagnostics of IS system intruders based on a synergy of several sciences and scientific areas: test pattern recognition, discrete mathematics, threshold and fuzzy logic, artificial intelligence, and others.

A study by Begishev et al. (2019) is devoted to legal problems connected with the development of new government approaches to ensuring the security of CII in the context of the existence of threats to their IS, including computer attacks. The authors note that the security of CIIs directly depends on the accuracy of decision-making in countering computer attacks as well as on the speed and effectiveness of the actions taken. Moreover, they remark that the norms of the criminal legislation on liability for unlawful influence on the CII of the Russian Federation should be modified and tightened.

Examining the legal issues of ensuring international IS, Khaliullin (2018) indicates that the IS of the Russian Federation is its integral part. He argues that the effectiveness of such legislation is determined by methods and characteristics of the criminal space, as well as the average number of cybercrime offenses. At the same time, no common position is shared by countries in fighting cybercrime, which is predetermined, among other things, by the different levels of information technology penetration.

Despite the abundance of studies devoted to IS, the impact of the information sphere on the country's economic security, in particular, on that of the Russian Federation, has not yet been sufficiently studied. Unlike Russian researchers, Western colleagues began to focus more on the technical part of the problem in order to develop a policy in the field of using information to ensure economic security. These are the problem of data leakage, the management of online systems with big data processing (Albeshri & Thayananthan, 2018) and the practice of combining operational backbones or digital service platforms by interested stakeholders (Sebastian et al., 2020). These approaches affect broader corporate governance and compliance issues. Western experts are more focused on how firms or governments might have to think about their IT security investments at the public–private partnership level (Chatterjee & Sokol, 2019). At the same time, many researchers from Russia are limited only to forecasts regarding the consequences of the introduction of the digital economy for the population, organizations, and authorities. Considering the novelty of the digital economy and security policy during digital transformation, few studies are devoted to the analysis of the results of the past years in the field of monitoring the risks associated with the manipulation of information and its role in changing economic indicators. It should not be forgotten that potential digital transformation is a more complex type of technology-based transformation of business or public sector than, for example, some kind of reorganization, which requires rethinking the strategic roles of new digital technologies and the opportunities for successful

implementation of digital innovation policy without damaging the already existing infrastructure and the operation of either business or state bodies (Ismail et al., 2017).

Methodology and methods

Since the present study intends to identify and systematize threats posed to economic security by the information environment as well as define a set of measures to protect the areas at risk, the research was carried out according to the following three phases:

1. Identification of threats to the information and economic macro-conjuncture;
2. Recognition of IS vulnerabilities;
3. Development of a set of measures to minimize the macroeconomic consequences of the IS systems' shortcomings.

To achieve better clarity and comprehensiveness of the material given, the first and second phases were presented in the form of mind maps.

The research materials, which became the basis for the developed models, were:

- National Security Strategy of the Russian Federation, approved by the Decree of the President of the Russian Federation of July 2, 2021 (The President of the Russian Federation, 2021);
- Strategy of Economic Security of the Russian Federation for the period until 2030 approved by the Decree of the President of the Russian Federation of May 13, 2017 (The President of the Russian Federation, 2017);
- Doctrine of Information Security of the Russian Federation approved by Decree of the President of the Russian Federation of December 5, 2016 (The President of the Russian Federation, 2016).

Considering the fact that an actual cybersecurity system is closed in nature, the research methodology is focused on the use of data from open sources. The research is based on the method of content analysis, since the materials of strategic documents are in the public domain. Analyzing the data obtained, the authors structure the IS threats by means of a qualitative assessment, distribute them into internal and external based on the classifications presented in strategic documents adopted by Russian officials' decrees, and then form the modeling of IS challenges and threats. As a result, the first model was based on the above-presented materials and accompanied by the systematization of IS threats and the identification of objects that can be affected by them (government bodies, businesses, etc.). The combination of theoretical and empirical methods made it possible to discover threats, which, with the help of modeling, were subsequently identified into internal and external ones.

The second model was based on the analysis of the belonging of objects of IS threats to the economic sphere through the selection of those IS threats that are directly related to the state's economic security. For descriptive reasons and based on existing relevant literature, threats were also conditionally divided into external and internal ones.

The final phase of the study presupposed the development of a practical plan to minimize negative consequences and prevent the influence of IS threats on the economy.

The proposed activities are applicable at different levels and spheres of public life, which considerably enhances their practical significance. According to its systematic approach, this study does not delve into technical issues, but involves a review of documented corporate policies, concepts, as well as an overview of existing detailed public and corporate practices. Future results will be related solely to law enforcement practice and taking into account the constantly changing realities that the state faces.

Results

The assessment and modeling of the challenges and threats faced by the Russian IS can be assessed on the basis of objective factors highlighted by the state, which controls the constantly changing situation. On the part of the state, this is expressed in the development of norms and strategic provisions that characterize the situation with national security and its information component. Thus, the National Security Strategy of the Russian Federation, approved by Decree of the President of the Russian Federation dated July 2, 2021 No. 400 (President of the Russian Federation, 2021). This document forms the basis of state policy in the field of protecting national interests and focuses on taking measures that ensure the well-being of the country's citizens. In particular, among the identified problems affecting security, including economic security, such theses stand out as in Article 16: resources, the practice of using tools of unfair competition, protectionist measures and sanctions, including in the financial and trade spheres, is becoming more common. Article 17 also points to the growth of geopolitical instability and conflict, the strengthening of interstate contradictions is accompanied by an increase in the threat of the use of military force, which, in turn, is carried out through outer space and information space, which are actively developed as new areas of military operations. Articles 42 and 44 directly record the fact of an increase in the number of crimes committed using information and communication technologies, as well as the activity of intelligence or other special services and organizations of foreign states (President of the Russian Federation, 2021). These theses emphasize the relevance of the problem of ensuring Russia's national security in the affected areas and systematize potential threats that come from outside.

In turn, the Economic Security Strategy of the Russian Federation for the period up to 2030, approved by the Decree of the President of the Russian Federation of May 13, 2017, also systematizes the challenges and threats to economic security, separately identified in Chapter II. As the conflict potential increases in the areas of Russia's economic interests, the exposure of the Russian financial system to global risks, as well as the vulnerability of the information infrastructure of the financial and banking system, is separately recorded (President of the Russian Federation, 2017).

As for the Information Security Doctrine of the Russian Federation, approved by the Decree of the President of the Russian Federation of December 5, 2016 (President of the Russian Federation, 2016), here he focuses on the system of official views on ensuring the national security of Russia, as well as taking measures to avoid potential threats. The Doctrine lists the main information threats facing the country and society, such as: threats of information and technical impact on the information infrastructure for military purposes; conducting technical intelligence to the detriment of Russia's interests, destabilization of the internal political and social situation, obstacles to journalistic

activity, scaling of cybercrime, high level of dependence of the domestic industry on foreign information technologies (electronic component base, software, computers, communications), including those associated with the low level of efficiency of Russian scientific research aimed at creating promising information technologies due to the fact that local Russian developments are poorly implemented, the personnel potential in this area is low (President of the Russian Federation, 2016).

After analyzing the main provisions taken from the above documents, it should be noted that the challenges and threats that Russia's IS faces can be conveniently classified as internal and external. External challenges are of extraterritorial origin, while internal ones are caused by domestic factors (Fig. 1).

Figure 1 displays the IS challenges and threats as well as the subjects that can be influenced by them (they are related to the state's economic security: enterprises, economic policy, financial and stock markets). Internal IS threats include: distortion of reports, including regional ones, the use of incorrect methodology when calculating macroeconomic indicators. Due to distorted regional and institutional reporting, or in case of methodological errors, macroeconomic indicators may be distorted as well, which can affect those government bodies' decisions that form economic, domestic, and foreign policies; low research and development (R&D) efficiency. Due to the chronic underfunding of the state's scientific and technical field and constant brain drain, the quality and efficiency of domestic scientific developments often lag significantly behind foreign ones, which leads to enterprises' dependence on foreign technologies and equipment; poor domestic developments' application. Since the prevailing share of industries does not support the idea of "science–production", many domestic developments fail to be implemented in the production process or utilized when morally and technically obsolete. This fact also affects the dependence of national companies on foreign technologies and equipment; insufficient staffing in the IS sector. The country's insufficient scientific and technological development leads to the situation when education fails to keep pace with modern science and technology development, primarily in ICT. Given this, IS specialists in both the public and private sectors are not always ready to respond to current challenges and threats, especially external ones: user data leakage due to the illegal actions of third parties. Weak security of computer networks can lead to data leakage of both government and business service users; insufficient public awareness of personal IS matters may result

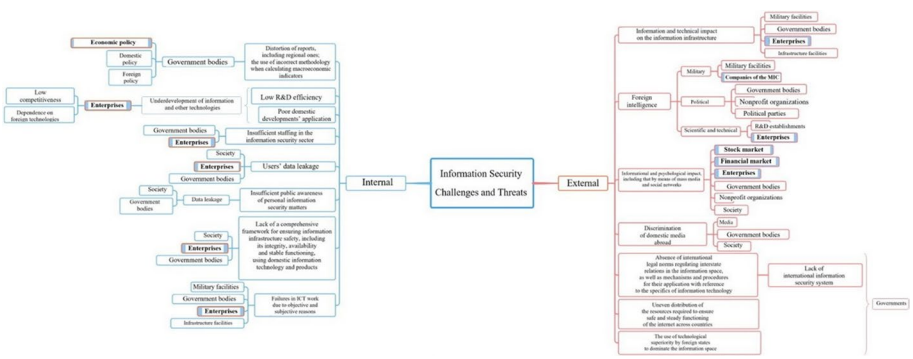

Fig. 1 Information security threats and challenges. Source: developed by the authors

in the fact that private, state and corporate data are released to the public; lack of a comprehensive framework for ensuring information infrastructure safety, including its integrity, availability, and stable functioning, using domestic information technology and products; failures in ICT work due to objective and subjective reasons (insufficient personnel qualification, low quality and deterioration of equipment, etc.).

External IS threats also include next options. Firstly, is that information and technical impact on the information infrastructure (as well as on the CII), which affects the functioning of government bodies, enterprises, and military/infrastructure facilities. Secondly, it is a collection of military, political, economic, scientific, and technical information by foreign intelligence services. Thirdly, it is an informational and psychological impact on public opinion, financial, stock and other markets in the country and abroad (including by means of mass media and social networks) with a view to destabilizing the internal political, social, and economic situation in the country. Next option is a discrimination of domestic media abroad, which leads to the impossibility of delivering important information to a foreign audience. Another important factor is the absence of international legal norms regulating interstate relations in the information space, as well as mechanisms and procedures for their application with reference to the specifics of information technology. As final options, it also includes an uneven distribution of the resources required to ensure safe and steady functioning of the internet across countries and the use of technological superiority by foreign states to dominate the information space.

Based on the analysis of objects of IS threats belonging to the economic sphere (economic policy, enterprises, financial sector, etc.), challenges and threats to the state's economic security were outlined (Fig. 2).

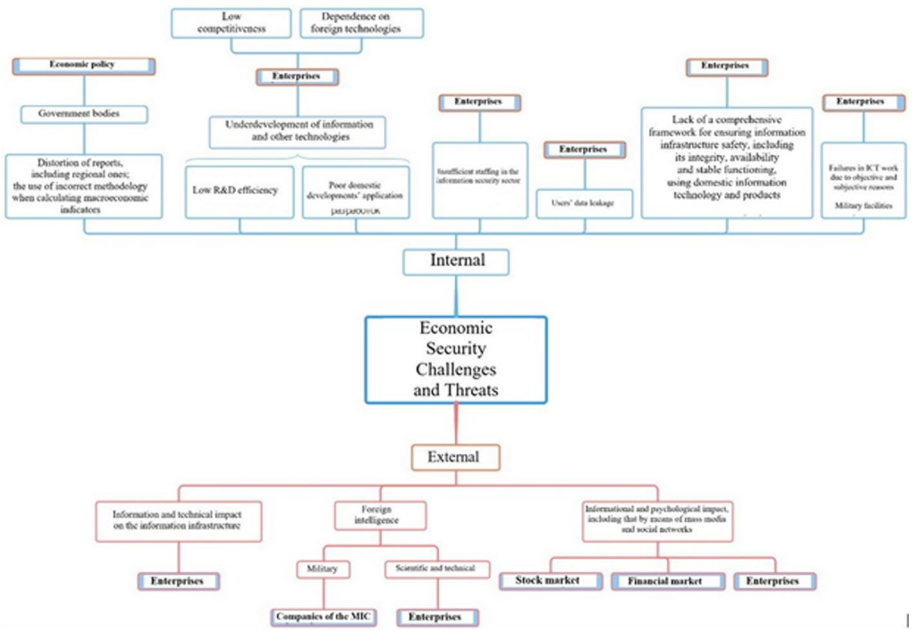

Fig. 2 Economic security challenges and threats posed by information sphere. Source: developed by the authors

As shown in Fig. 2, external threats to the country's economic security from the information sphere include information and technical impact on the information infrastructure, activities of foreign intelligence services, informational and psychological impact on public opinion, financial, stock and other markets (including by means of mass media and social networks). On the contrary, internal challenges include distortion of regional and institutional reports and the use of incorrect methodology when calculating macroeconomic indicators, low R&D efficiency, poor domestic developments' application, insufficient staffing in the IS sector, user data leakage due to the illegal actions of third parties, lack of a comprehensive framework for ensuring information infrastructure safety, and failures in ICT work due to objective and subjective reasons.

The proposed model provides an understanding of potential gaps in the state's economic security, thereby giving rise to the development of a system of multi-level measures aimed at eliminating or at least minimizing each of the potential threats (Retter et al., 2020). Taking into account the data in Figs. 1 and 2, this set of measures should include: strengthening of technical data protection (including that related to employees and users of government and corporate services) and CII for military, government and civil purposes both at the national level and at the level of particular enterprises; increasing the security of storage and access to classified military, political, economic, scientific, and technical information with the help of technical, organizational, and counterintelligence measures; implementation of effective strategies to counteract the influence of propaganda and external information on public opinion and markets; introduction of a unified methodology for calculation and a system of centralized collection and verification of macroeconomic indicators at all levels (federal, regional, departmental); increasing the funding of science and R&D, including through their targeted funding by enterprises-customers of novel developments, with a priority focus on high-tech branches of science and an emphasis on the research results' practical applicability; creation of "science-production" chains by building virtual science and technology parks, in which the enterprise and research institutes are not necessarily located close to each other but rather linked by a joint research or production area; improving the quality of education in the field of IS, both basic and specialized, including by revising curricula and tightening certification requirements; raising awareness of citizens about the risks of non-compliance with personal IS measures and about the need for more careful storage of personal, state, or corporate data by means of mass media, social networks, and similar communication channels; improvement of personnel qualifications and requirements for the conditions of their admission to information and communication systems that ensure the performance of government bodies as well as military and critical information infrastructure facilities.

On the basis of the measures proposed, future actions should be distributed among responsible bodies and officials at federal, departmental, regional, and corporate levels with a clear strategy implementation plan. If the preceding is performed successfully, the country's IS will improve. What is more of paramount importance is the definition of a clear set of indicators that would allow tracking the effectiveness of measures taken to address IS challenges posed to the country's economic security (Bareiko & Kozhukhina, 2019; Diesch et al., 2018; Kosovets, 2011).

Discussion

Under the current context of globalization and the development of global information and telecommunication systems, the problem of ensuring the country's economic sovereignty acquires new content and meaning. The economic security system is, in fact, the guarantor of the overall country's sovereignty and independence since the national security and defense are closely connected with the economic situation (Kosovets, 2011).

Due to the rapid ICT development, the information has become one of the most important objects to protect while ensuring the country's economic security. Its substantial significance stems from the fact that it permeates all spheres of our life (Skripina, 2016). However, the global interest in this matter has arisen drastically only in recent years. There are technical, behavioral, managerial, philosophical and organizational aspects that address the protection of assets and mitigate threats. Ignoring these factors can significantly harm the interests of the economy and the state (Diesch et al., 2018).

The digital era we live in facilitates the restructuring of information systems and forces the government to adopt new strategies that meet IS requirements. In addition to the obvious advantages, IT usage also brings challenges [e.g., internet fraud, information insecurity issues (at all levels, including government), processing large data volumes]. Cybercrime, including organized and state-sponsored, has become a global problem, a complex transnational threat operating on an industrial scale (Cristea, 2020). Under the influence of the information economy, technologies related to economic and competitive activity have moved from the traditional space to the virtual one. In this day and age, businesses widely use information warfare to create market advantages and weaken their opponents. As a threat to economic security in the information sphere, information warfare itself is characterized by the polarization of the scale of the source and the object of influence, latent nature, irreversibility of consequences, long-distance influence, and the impossibility of complete elimination (Cheskidov, 2013).

One of the forms of information warfare is the creation and proliferation of hoaxes and hate speech. It is a deliberate practice intended to promote certain motives and interests performed by actors seeking to spread deceit and hate in the digital ecosystem for the sake of their political or economic interests. The mongering of hate in cyberspace by virtue of modern media platforms effectively turns freedom of speech into freedom to hate, which is used to attack those opposed. The proliferation of hoaxes and hate speech in cyberspace threaten national security and stability. Therefore, not only the government and intelligence agencies, but also businesses and civil society should pay serious attention to the risks posed by such hoaxes (Gunawan & Ratmono, 2020).

The development of ICT and its implementation in all spheres of government control and the national economy raises the issue of vulnerability of CII to a new level. Without a doubt, that major disruption of CII would have dire consequences for society, economy and government. In addition, given cross-sectoral interconnectedness through joint ICT systems, breakdown of safety and security of one or more CIIs may cause a "domino effect" affecting other critical national infrastructures and thus creating the possibility of cascading disasters. Moreover, even though CIIs are mostly developed and built at the national level, they are closely interconnected with other countries' infrastructures. This implies that a breakdown in one place may negatively impact the neighboring countries and regions (Newlove-Eriksson et al., 2018).

The widespread application of ICT broaches the subject of how best to define a cybersecurity strategy that would effectively work for the benefit of the government, economy, and civil society. An effective cybersecurity strategy must balance the accepted norms of a country with the opportunities presented by the internet. From one side, the internet is deemed a disruptive technology that puts into question many generally accepted norms of public policy, business, and civil society. However, from the other side, the government is to level this danger with the openness of the internet and free information flow. While a strict security policy ensures stability, it may also reduce the potential information technology benefits (Azmi et al., 2016; Glushkova et al., 2019). Using the example of scandals involving the use of personal data of individuals and legal entities on the part of social networks, the inconsistency of authorities is costly for potential victims of all kinds of personal data leaks. The issue of institutionalization and good governance should again become a matter of improving judicial practice regarding information security that affects the general welfare (Park, 2019).

Therefore, it should be emphasized that the state`s policy in relation to the information agenda regulation should be flexible. However, when pursuing such a policy, it should be understood that ensuring the cybersecurity of economic activity is a complex task and requires many resources in providing a crisis response strategy. And the importance of learning to counter such threats should be paramount, whether it be private or public (Schilling, 2017). With a stable consensus of interests of the state, business and civil society, the learning process should also be made its continuity in order to maintain all the necessary conditions for the stable provision of information security.

Conclusions

The present research was conducted in three phases. The first phase focused on collecting, summarizing, and systematizing IS threats as well as on defining objects that can be affected by them (government bodies, businesses, etc.). Based on this data, a model of IS has been presented, where all of them were distributed into two types—internal and external ones. In the second phase, the revealed IS threats and challenges directly connected with the country's economic security were identified and derived into a separate model (they were also categorized according to "internal/external" indicator). In the final phase of the study, based on the model of IS threats to the country's economic sphere, general recommendations were developed to overcome or at least minimize each of the model's threats.

The developed model of economic security challenges and threats posed by the information sphere provides one with the opportunity to thoroughly examine potential gaps in the state's economic security. Based on the analysis of these vulnerabilities, practical recommendations in the form of necessary measures to prevent and minimize the negative impact of threats to economic security from the information sphere were developed. The study findings and recommendations can be used by officials of government bodies and other organizations to develop regulatory documents related to the strategy of ensuring information and economic security at various levels. Besides, other researchers in the field may apply the model offered as a basis for identifying quantitative and qualitative indicators determining the security level for each of the threats distinguished as well as for assessing the effectiveness of measures proposed.

This research was limited to the theoretical analysis of IS threats and challenges posed to economic security and the general nature of the proposed measures. Future work in this field will be focused on the identification and analysis of indicators that allow defining the economic security level, evaluating the effectiveness of measures proposed in this paper, and a more in-depth examination of IS measures, in particular, from the perspective of the implementation level (federal, departmental, regional, corporate) and plan. In case of successful application of such developments, interested entities in the form of countries and regions will have the opportunity to form a sustainable infrastructure capable of ensuring the integrity of information security for the benefit of the development of the national economy, while adequately responding to new challenges.

Acknowledgements
Not applicable.

Author contributions
Conceptualization, IO and VS; methodology, OC and EZ; software, OC; validation, VS, IO, EZ; formal analysis, IO; investigation, VS; resources, EZ; data curation, OC; writing—original draft preparation, EZ; writing—review and editing, IO; visualization, VS and OC; supervision, EZ; project administration, IO; funding acquisition, EZ.

Funding
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of data and materials
Data will be available on request.

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 9 August 2021 Accepted: 2 September 2023
Published online: 05 October 2023

References

Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Information & Computer Security, 24*(2), 205–227. https://doi.org/10.1108/ICS-01-2016-0006

Albeshri, A., & Thayananthan, V. (2018). Analytical techniques for decision making on information security for big data breaches. *International Journal of Information Technology & Decision Making, 17*(2), 527–545. https://doi.org/10.1142/S0219622017500432

Amirov, A., Kozhukhova, M., Koshebaeva, G., Biryukov, V., & Zhiyenbayev, M. (2018). Economic and Energy Security of the Republic of Kazakhstan. *International Journal of Energy Economics and Policy, 8*(6), 16–21. https://doi.org/10.32479/ijeep.6935

Arutyunov, V. V. (2017). Clustering of information-security standards of the Russian Federation. *Scientific and Technical Information Processing, 44*(2), 125–133. https://doi.org/10.32479/ijeep.6935

Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind cyber security strategy development: a literature review of national cyber security strategy. In *Australasian Conference on Information Systems* (pp. 1–12). University of Wollongong.

Balzacq, T., & Puybareau, B. (2018). The economy of secrecy: Security, information control, and EU-US relations. *West European Politics, 41*(4), 890–913. https://doi.org/10.1080/01402382.2018.1431490

Barannik, V., Belikova, T., & Gurzhii, P. (2019, December). The model of threats to information and psychological security, taking into account the hidden information destructive impact on the subconscious of adolescents. In 2019 *IEEE International Conference on Advanced Trends in Information Theory (ATIT)* (pp. 267–270). IEEE.

Bareiko, S. N. (2019). Development of small and medium-sized businesses in Russia as one of the key factors of economic and social stability. *National Security, 1*, 49–55.

Bareiko, S. N., & Kozukhina, K. A. (2019). Economic and information security of Russia in the digital economy. *Krasnoyarsk Science, 8*(5), 7–18. https://doi.org/10.12731/2070-7568-2019-5-7-18

Begishev, I. R., Khisamova, Z. I., & Mazitova, G. I. (2019). Criminal legal ensuring of security of critical information infrastructure of the Russian Federation. *Revista Gênero & Direito, 8*(6), 283–292.

Boranbayev, A., Boranbayev, S., Nurusheva, A., & Yersakhanov, K. (2018). The modern state and the further development prospects of information security in the Republic of Kazakhstan. In S. Latifi (Ed.), *Information Technology-New Generations* (pp. 33–38). Springer. https://doi.org/10.1007/978-3-319-77028-4_6

Chatterjee, C., & Sokol, D. D. (2019). *Data security, data breaches, and compliance*. Cambridge University Press.

Cheskidov, M. A. (2013). Information warfare as a threat to the economic security of the state. *New University. Series: Economics and Law, 4*(26), 1–7.
Cristea, L. M. (2020). Current security threats in the national and international context. *Journal of Accounting and Management Information Systems, 19*(2), 351–378.
Diesch, R., Pfaff, M., & Krcmar, H. (2018). Prerequisite to measure information security. *Information Management and Computer Security, 99*(7), 7. https://doi.org/10.5220/0006545602070215
Fedotova, G. V., Kovalenko, O. A., Malyutina, T. D., Glushchenko, A. V., & Sukhinin, A. V. (2019). Transformation of information security systems of enterprises in the context of digitization of the national economy. In E. Popkova (Ed.), *Ubiquitous computing and the Internet of Things: Prerequisites for the Development of ICT* (pp. 811–822). Springer. https://doi.org/10.1007/978-3-030-13397-9_84
Frolova, E. E., Polyakova, T. A., Dudin, M. N., Rusakova, E. P., & Kucherenko, P. A. (2018). Information security of Russia in the digital economy: the economic and legal aspects. *Journal of Advanced Research in Law and Economics, 9*(1), 89–95.
Glushkova, S., Belotserkovich, D., Morgunova, N., & Yuzhakova, Y. (2019). The role of smartphones and the internet in developing countries. *Revista ESPACIOS, 40*(27), 1–10.
Gontar, A. A., Lomakin, N. I., Gorbacheva, A. S., Chekrygina, T. A., & Tokareva, E. V. (2019). Methods of data intellectual analysis in assessment of economic security level. In E. Popkova (Ed.), *Ubiquitous computing and the Internet of Things: Prerequisites for the Development of ICT* (pp. 455–464). Springer. https://doi.org/10.1007/978-3-030-13397-9_53
Gunawan, B., & Ratmono, B. M. (2020). Social media, cyberhoaxes and national security: Threats and protection in Indonesian Cyberspace. *IJ Network Security, 22*(1), 93–101. https://doi.org/10.6633/IJNS.20200122(1).09
Hacker, J. S., Stiglitz, J. E., Fitoussi, J. P., & Durand, M. (2018). Economic security. In *For good measure: Advancing research on well-being metrics beyond GDP* (pp. 203–240). OECD Publishing.
Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the US retail economy: Restoring confidence in information technology security standards. *Technology in Society, 44*, 30–38. https://doi.org/10.1016/j.techsoc.2015.11.007
Huang, C. C., & Farn, K. J. (2016). A study on E-Taiwan promotion information security governance programs with e-government implementation of information security management standardization. *IJ Network Security, 18*(3), 565–578.
Ismail, M. H., Khater, M., & Zaki, M. (2017). Digital business transformation and strategy: What do we know so far. *Cambridge Service Alliance, 10*, 1–35. https://doi.org/10.13140/RG.2.2.36492.62086
Jankovska, L., Tylchyk, V., & Khomyshyn, I. (2018). National economic security: an economic and legal framework for ensuring in the conditions of the European integration. *Baltic Journal of Economic Studies, 4*(1), 350–357. https://doi.org/10.30525/2256-0742/2018-4-1-350-357
Khaliullin, A. I. (2018). Aspects of information security of the Russian Federation. *Russian Journal of Legal Studies, 5*(1), 59–65. https://doi.org/10.17816/RJLS18349
Khochueva, F. A., & Shugunov, T. L. (2020). Ensuring information security as a key factor in the development of the digital economy in the Russian Federation. In *2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)* (pp. 250–256). Atlantis Press. https://doi.org/10.2991/aebmr.k.201205.042
Kosovets, A. A. (2011). Information security in the system of ensuring the economic and national security of Russia. *Economic Security Bulletin, 2*, 7–13.
Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures, 9*(1), 3–31. https://doi.org/10.1504/IJCIS.2013.051608
Mansurov, G. (2021). International legal mechanisms for ensuring digital security. *SHS Web of Conferences., 93*, 02031. https://doi.org/10.1051/shsconf/20219302031
Metelev, S. E., Murat, M. M., & Lizunov, V. (2016). *Economic security policy of the Russian Federation*. Libertas.
Murdoch, C., Knorr, K., & Trager, F. (2001). *Economic factors as objects of security: Economics security & vulnerability*. Lawrence Publishing Company.
Na, O., Park, L. W., Yu, H., Kim, Y., & Chang, H. (2019). The rating model of corporate information for economic security activities. *Security Journal, 32*(4), 435–456. https://doi.org/10.1057/s41284-019-00171-z
National Industrial Security Center. (2018). Press release. National Intelligence Service. Retrieved January 25, 2021, from https://eng.nis.go.kr
Newlove-Eriksson, L., Giacomello, G., & Eriksson, J. (2018). The invisible hand? Critical information infrastructures, commercialisation and national security. *The International Spectator, 53*(2), 124–140. https://doi.org/10.1080/03932729.2018.1458445
Nicola, M., Alsafi, Z., Sohrabi, C., Kerwan, A., Al-Jabir, A., Iosifidis, C., Agha, M., & Agha, R. (2020). The socio-economic implications of the coronavirus pandemic (COVID-19): A review. *International Journal of Surgery (london, England), 78*, 185–193.
Park, S. (2019). Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics, 58*, 132–145. https://doi.org/10.1016/j.irle.2019.03.007
Peleshchyshyn, A., Vus, V., Albota, S., & Markovets, O. (2018). A formal approach to modeling the characteristics of users of social networks regarding information security issues. In Z. Hu, S. Petoukhov, & M. He (Eds.), *International Conference of Artificial Intelligence, Medical Engineering, Education* (pp. 485–494). Springer. https://doi.org/10.1007/978-3-030-12082-5_44
Peppers, S. F. (2017). Entrepreneurial security: A free-market model for national economic security. *Economics and Statistics, 1*, 28–36.
Petrenko, S. (2018a). *Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation.* Springer.
Petrenko, S. (2018b). *Cyber security innovation for the digital economy*. River Publishers.
Popov, E. V., & Semyachkov, K. A. (2018). Problems of economic security for digital society in the context of globalization. *Ekonomika Regiona, 4*, 1088–1101. https://doi.org/10.17059/2018-4-3
Retter, L., Frinking, E. J., Hoorens, S., Lynch, A., Nederveen, F., & Phillips, W. D. (2020). *Relationships between the economy and national security: Analysis and considerations for economic security policy in the Netherlands*. RAND Corporation.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law, 12*(2), 53–74. https://doi.org/10.15394/jdfsl.2017.1476
Schilling, K. R. (2017). *Cybercrime – when employees become a risk factor.* HornetSecurity. Retrieved April 20, 2022, from https://www.hornetsecurity.com/en/security-information/cybercrime/
Scott, J. (2004). Measuring dimensions of perceived e-business risks. *Information Systems and e-Business Management, 2*(1), 31–55. https://doi.org/10.1007/s10257-003-0026-y
Sebastian, I. M., Ross, J. W., Beath, C., Mocker, M., Moloney, K. G., & Fonstad, N. O. (2020). How big old companies navigate digital transformation. *Strategic information management* (pp. 133–150). Routledge.
Senol, M., & Karacuha, E. (2020). Creating and implementing an effective and deterrent national cyber security strategy. *Journal of Engineering, 2020*, 5267564. https://doi.org/10.1155/2020/5267564
Skripina, A. A. (2016). Influence of the information factor on the economic security of the market. *Bulletin of Belgorod State Technological University named after V. G. Shukhov, 9*, 1–6.
Snegovaya, I. (2017). Theoretical and legal underpinnings of economic security of the Russian Federation as a component of the state national security. *Problems of Economics and Legal Practice, 3*, 173–182.
Svetlakov, A., & Glotina, I. (2018). Impact of information space on economic security in the region. *Economy of Region, 1*(2), 474–484.
The President of the Russian Federation. (2016). *Decree of the President of the Russian Federation of December 5, 2016 No. 646 "On Approval of the Doctrine of Information Security of the Russian Federation"*. Retrieved January 25 2023 from http://kremlin.ru/acts/bank/41460/page/1
The President of the Russian Federation. (2017). *Decree of the President of the Russian Federation of May 13, 2017 No. 208 "On the Strategy of economic security of the Russian Federation for the period until 2030".* Retrieved January 25, 2021, from https://www.garant.ru/products/ipo/prime/doc/71572608
The President of the Russian Federation. (2021). *Decree of the President of the Russian Federation of July 2, 2021 No. 400 "The Strategy of National Security of the Russian Federation".* Retrieved January 25, 2023, from http://www.kremlin.ru/acts/bank/47046
Tsaregorodtsev, A. V., Kravets, O. J., Choporov, O. N., & Zelenina, A. N. (2018). Information Security Risk Estimation for Cloud Infrastructure. *International Journal on Information Technologies & Security, 10*(4), 67–76.
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
White, G. L., Hewitt, B., & Kruck, S. E. (2019). Incorporating global information security and assurance in IS education. *Journal of Information Systems Education, 24*(1), 11–16.
Yankovskaya, A. E., Shelupanov, A. A., & Mironova, V. G. (2016). Construction of hybrid intelligent system of express-diagnostics of information security attackers based on the synergy of several sciences and scientific directions. *Pattern Recognition and Image Analysis, 26*(3), 524–532. https://doi.org/10.1134/S1054661816030238

Publisher's Note