Risks and threats to economic security in the digital economy

Irina Kirishchieva[1], *Mikhail* Skorev[1], *Oksana* Mishchenko[2], and *Tatiana* Grafova[1,2,*]

[1]Department of Economics, Accounting and Analysis, Rostov State Transport University, Rostov-on-Don 344038, Russia
[2]Rostov Branch of Russian Customs Academy, Rostov-on-Don, 344002, Russia

Abstract. The economic security of the company is the state of protection of the vital interests of the enterprise from the impact of internal and external destabilizing factors and threats, the emerging management and collective enterprise through the effective use of its resources, as well as the implementation of measures of economic, legal, organizational, technical, technological and social nature. -psychic directed and stable functioning of the enterprise both in the current and in the long term. Digitalization is bringing changes to the country's economy. The volume of services, the use of labor, investment in physical and human capital, technologies and their diffusion, the use of trade services, including financial, legal, managerial, informational and consulting, and is reflected in production efficiency, labor productivity and competitiveness, culture, lifestyle and system of values. The presented risks and threats to the security of an enterprise in a digital economy emphasize the need to improve the electronic security system. At the same time, the features of the process of ensuring electronic safety in the context of digital development lie in the development and use of tools for identifying and assessing risks, indicators and indicators of the level of economic security, providing subsystems, including information, technological, personnel, investment, regulatory and legal components.

1 Introduction

Modern conditions, characterized by the political influence of Western countries, sanctions and bans, an unstable economic situation in the world, the emergence of an increasing number of threats and destabilizing factors, have led to the high importance of developing and strengthening the national economy and ensuring economic security [1]. One of the most important conditions for strengthening the country's economy is the development and modernization of the industrial and technological base and priority sectors of the national economy, the development of the innovation system and increasing the country's investment attractiveness, improving the business climate and creating a favorable business environment for the national economy [2].

The essence of economic security lies in the ability of the economy to create the necessary conditions for life and personal development, socio-economic and military-political stability

* Corresponding author: grafova_to@donrta.ru

of society and preserve the integrity of the state, successfully resist the influence of internal and external threats and negative factors and be the material basis of national security [3] .

This allows us to say that "economic security" is a complex concept covering the state of many spheres of economic activity and public life of the state and is determined by the state of stability of the economic system.

The enterprise, as a cell of the economic system, has a direct impact on its sustainable and dynamic development. In this regard, the economic security of an economic entity becomes the most important and integral component of the economic security of the state and national security in general [2, 3].

The concept of economic security of an enterprise (EBS) is usually associated with its state, characterized by the ability to withstand destabilizing factors and conditions of the external and internal environment, to exclude threats of their adverse impact, the presence of potential that ensures stable and effective functioning in the current period and in the long term [4]

In the existing difficult conditions, caused by the influence on the activities of enterprises of many destabilizing factors of both external and internal environment, the so-called integrated approach, as a combination of the main above-mentioned approaches, will be effective, which will increase the efficiency and comprehensiveness of EBP [5]. should be a continuous process integrated into all production processes of the enterprise, therefore it should be organically integrated into the enterprise management system as a subsystem that ensures the effective operation of all its links, contributes to the achievement of the planned strategic goals, giving stability and reliability to the management system by neutralizing threats. At the same time, resources are the main functional elements of ensuring electronic power supply (Fig. 1).

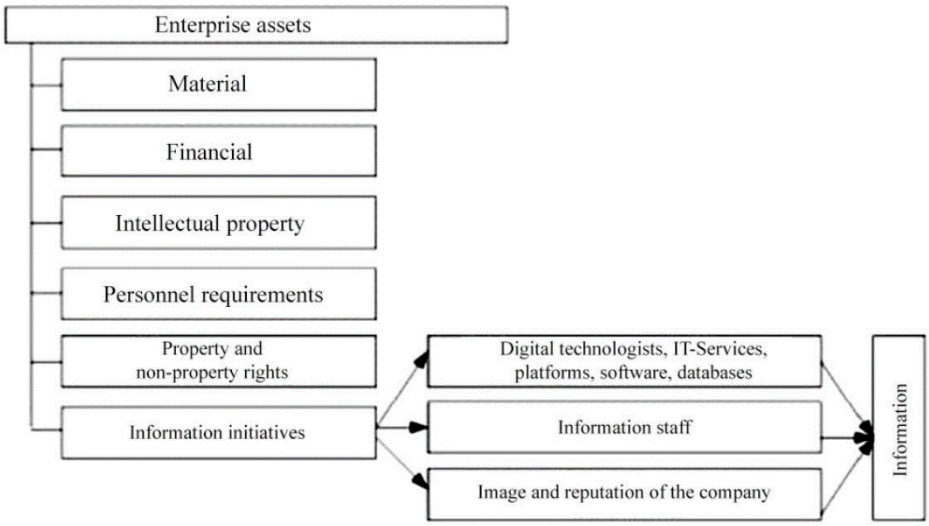

Fig. 1. The relationship of the economic security of the enterprise with efficient use of its resources

2 Basic methods

The processes occurring in the functional components of the EBP affect the economic system of the enterprise, change its parameters and indicators. Giving the economic parameters a special role is not accidental.

For example, the low speed of information flow affects the speed of production processes, hinders the adoption of effective management decisions, which, as a result, may lead to a change in the financial result of the enterprise and its indicators.

The model of an enterprise with economic parameters, which is fixed in the indicators of EBP, acts as a kind of standard of safe functioning, upon reaching which it is necessary to develop a new concept that provides sufficient flexibility, mobility, the ability to assess changes for the redistribution of internal potential and adaptation of the enterprise in response to changes in the external environment [6]. The present time is characterized by the transition of society, state and business to a new environment in which digital technologies are increasingly integrated into all spheres of the economy and society, radically changing entire industries and having a significant impact on the economic development of the country. Thus, these changes become the basis of all modern innovative management and economic systems and the driving force behind the socio-economic and innovative development of any state and society [7].

The prerequisites for the emergence of the "digital" economy "were the development of new technologies, which began with the digital (third industrial) revolution, representing the transition from mechanical and analog electronic technology to digital (late 1950s), the emergence of the global Internet (1982), radical changes caused by digital computing and communication technologies of the second half of the 20th century, as well as the concept of a new electronic economy based on the transition of humanity in its activities from processing atoms to processing electronic bits, formulated in 1995 by American information technology specialist Nicholas Negroponte in his book Being Digital [8]. Thus, the philosophy of the fourth industrial revolution as the basis of the “digital economy” can be defined as follows [9]: “a fundamentally new, qualitative transformation of all spheres of human life based on the development and application of fundamentally new digital technologies, artificial intelligence, virtual reality and digital platforms.

Since technologies are dynamically developing, the economic activity based on their use is also undergoing changes [10].

Consequently, the very subject of the digital economy is in a state of constant improvement. From this point of view, the formation of the digital economy is the result of technological development, and its theory is the fruit of the theory of the information society and the information economy [11]. Turning to the consideration of risks and threats to economic security in the digital economy directly at the enterprise level, it should be noted that the process its digital transformation is a transition from tangible assets to intangible (digital, virtual), automation of business processes through the introduction of modern information (digital) technologies and systems and the creation of new business models based on them. The entire set of information, objects of informatization, information (digital) technologies and systems, subjects using these technologies, as well as mechanisms for regulating the relevant economic relations in a given environment, represents the information sphere (digital environment) in which the enterprise operates, and the ICT and digital technologies are tools for the economic activity of an enterprise in a digital environment [12].

The introduction of ICT and the transition of an enterprise to functioning in a digital environment carries new risks and threats that are not inherent in traditional (non-digital) processes.

3 Results

Let's highlight the main groups of risks and threats to economic security that are characteristic of the digital transformation of an enterprise:

- informational risks and threats;
- risks and threats to information security (cyber security);

- the risks associated with the use of digital economy technologies;
- investment risks and threats;
- risks and threats to human resources;
- risks and threats of a "third party";
- organizational and managerial risks;
- risks and threats of a legal nature.

The first group is informational risks and threats. Among the tangible and intangible assets used by the enterprise for its functioning, in the context of digital transformation, information and information resources serve as the basic asset of "digital technologies" [13] (Fig. 2).

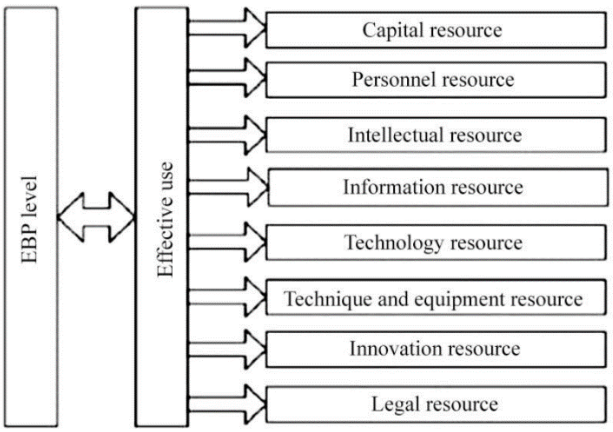

Fig. 2. Information and "digital" assets in the structure of all assets Enterprises

In this regard, in the context of digital transformation, information resources are present in the activities of any business entity - information and data in digital format, which become one of the most important management resources, along with human, financial and material resources. Their accumulation and consumption is the basis for the effective functioning and development of the enterprise's digital economy, and the integrity and reliability of information as a digital intangible asset is becoming one of the most important elements of enterprise business process management.

In this context, the risks and threats associated with information and data in digital format, the technologies used to obtain, process, store, and provide them become one of the main and significant risks of EE in the digital economy, since their component is projected onto all other risks of the main activity.

At the same time, it is important to emphasize the difference between these risks and threats from those arising as a result of a deliberate attack from an individual, organization, country or other entity considered within the framework of information security.

Information risks arise from dependence on complex information systems. They include often hidden factors such as information overload, human bias, interdependence of systems, and hidden uncertainties and incompleteness of the information itself. As digital technologies are introduced, they are also associated with failures, errors, abuse and other problems unintentionally caused by customers, suppliers, technology or employees. Information risks are less visible and therefore more insidious. In the meantime, there is no need to worry about it.

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, digitized data from

various sensors, data electronic media, information processed in corporate information systems and transmitted through data transmission channels). The main manifestation of information risk is a violation of the integrity, reliability and availability of information assets (resources). These manifestations can be associated with the reliability of the hardware components of the IS and the possibility of their failure, software failures, and non-compliance with the requirements of various standards in the operation of IS and digital services, incompetence and erroneous actions of the personnel of the enterprise (internal environment), contractors (outsourcers) and suppliers of IS and resources (external environment), the likelihood of the presence of undocumented opportunities in the system, imperfection of the organizational structure of the IS, as well as non-compliance with the requirements of standards at the stage of design, production and operation of the system.

By their nature, information risks and threats can be divided into organizational and technical, hardware and software.

Organizational risks are caused by the insufficient efficiency of the developed rules governing the activities of personnel operating and servicing the IS, as well as by the problems of the internal control system.

Technical risks - associated with the equipment and software environment of the IS or digital resource and their operation, i.e. directly related to the life cycle of the IS and, in turn, are divided into:

- hardware risks - associated with the failure of IS components, such as: servers, personal computers, network switches and routers, production equipment, machine tools, etc.
- project risks - system errors in setting goals and objectives for designing an IS, formulating requirements for the functions and characteristics of solving problems of digitalization of a process or an object, determining the conditions and parameters of the external environment in which the IS is to be used; algorithmic design errors in the direct algorithmicization of the functions of software tools and databases, in determining the structure and interaction of components of software complexes, as well as when using information from databases; programming errors in program texts and data descriptions, as well as in the source and resulting documentation for IS components;
- software risks - directly related to failures and system errors in the functioning of the software.

In addition to the listed factors of information risks, the latter can be external and internal.

External information risks do not depend on the internal environment of the enterprise and are not related to its direct activities. It is difficult for an enterprise to influence them, since they are conditioned by the political and socio-economic situation in the country.

Internal information risks are directly related to the activities of the enterprise and its personnel and depend on factors such as production and human resources, the level of technical and technological equipment and the development of information infrastructure, organization of information security.

The second group of risks is the risks and threats of information security (cyber security). The key resource of the digital economy is information and data in digital format that do not disappear when consumed, can be repeatedly used by various subjects without reference to the place, time and subject of creation (appearance). From this point of view, they become not only the main value of the enterprise, but also the object of cyber attacks, primarily aimed at finding vulnerabilities that allow access to corporate information for economic purposes, which ultimately can lead not only to the loss of competitive advantages and direct financial losses, but also to the loss of capitalization of the enterprise, a decrease in business reputation [14].

The security of any information (digital) resource, as you know, consists of ensuring three of its characteristics:

- confidentiality - lies in the fact that it is available only to those subjects of access (users, programs, processes) who have been granted the appropriate authority;
- integrity - assumes that it can be modified only by a subject who has the appropriate rights for this. Integrity is a guarantee of the correctness (invariability, operability) of a component at any time;
- availability - means that a subject having the appropriate authority can at any time without any problems get access to the necessary system component (resource).

Risks and threats to information security (IS), in contrast to information threats and risks, are the result of a deliberate impact on information, data in digital form, the functioning of information resources and systems in the digital space.

The mechanism of the impact of information security risks in the digital transformation of the enterprise economy is the largest classification group of information threats and risks and includes such of them as [15]:
- loss of information resource;
- loss of access to an information resource, violation of its integrity, availability as a result of deliberate influence;
- theft of information and data in digital format;
- deliberate distortion of information;
- failures and failures of hardware and software of automated control systems and information systems, as well as disruption of the functioning of software and protection means as a result of deliberate influence;
- distribution of malicious software and bookmarks;
- spyware;
- unauthorized access;
- copyright infringement.

By their nature, they can be conditionally divided into five main groups:
- software - caused by the introduction and impact of malicious software ("viruses"), software "bookmarks"; destruction and modification of data in information systems; deliberate changes in the parameters, composition and configuration of the information system and resource, leading to their non-compliance with those during testing and certification.
- technical - external influence on information and control systems and information transmission channels in order to disrupt their normal operation; failures and failures of hardware and software of the digital environment of the enterprise at all stages of their use, caused by purposeful impact;
- physical - destruction of processing facilities and information carriers; theft of media, as well as hardware or software electronic keys for access and authentication;
- informational - violation of the rules of information exchange; unauthorized access, collection, theft, use and distribution of information resources; illegal copying of data in information systems; disinformation, concealment or distortion of information, deliberate distortion and unacceptable changes in the characteristics of information flows in digital channels, coming from sources and transmitted to consumers.
- organizational - due to the ineffectiveness of the organization at the enterprise of activities to ensure cyber protection; non-observance and violation of the requirements of documents and regulations governing the field of information security; insufficient efficiency of the used methods and means of operational protection of programs and data and ensuring the security of the functioning of the IS in conditions of accidental negative influences.

Despite the variety of forms of implementation of IS threats on the electronic security system in nature and content, the main ones include:
- interception of information - copying of information or digital databases, as a result of which the attacker receives a complete duplicate of them. The current level of ICT development

provides ample opportunities and tools for intercepting data using a variety of methods and technical means;
- theft of information - the subject of the threat not only receives the relevant data, but also deprives the enterprise of it, and the object of theft can be not only closed (confidential), but also open information necessary for the functioning of the enterprise;
- damage or destruction of data and information - the subject of the threat achieves only the task of causing damage to the enterprise and disrupting its functioning;
- distortion of information and data by an employee due to intentional or unintentional actions. Often the reason for the implementation of this form of threat is the irresponsibility and incompetence of the personnel, which manifests itself in the violation of the requirements for ensuring IS in force at the enterprise, both on their own initiative and under the influence of third parties. These threats include:
- unintentional errors of users, operators, system administrators and other persons servicing and operating IS.

They are the most dangerous in terms of the amount of damage, since they are not only threats to the normal functioning of the IS (incorrectly entered data, an error in the program that caused the system crash), but also can create vulnerabilities that can be exploited by cyber attackers;
- theft and forgery - are in second place in terms of damage. As a result of such illegal actions with the use of personal computers, Russian organizations are annually inflicted with a total damage of tens of billions of rubles;
- unauthorized access to information and unauthorized change of data - unauthorized exit from the circle of persons of the enterprise to whom this information is entrusted. This also includes the risks and threats associated with its leakage or misappropriation of it and thereby obtaining the opportunity to use it in their own interests. At the same time, the source of leakage of protected information is any carrier of confidential information to which an attacker managed to gain unauthorized access.The third group of risks is the risks associated with the use of digital economy technologies (the so-called technological risks).
These include [16]:
- internet of Things (IoT). All kinds of chips and sensors built into equipment and vehicles, various technical devices, which are controlled using the Internet and applications, provide ample opportunities for optimizing resources, rationalizing transactions, and automating routine operations. But, along with a positive effect, they are accompanied by risks, since IoT technologies are a rather vulnerable segment of ICT for unauthorized attacks and cyber attacks, and the security level of most of its technologies is close to zero;
- risks of Blockchain distributed ledger technology. One of the developing areas of application of blockchain technology is blockchain platforms and smart contracts implemented through them. At the same time, the fundamental principle of the blockchain is the immutability of the transactions carried out, that is, even if the transaction was incorrect, caused by a failure, erroneous or fraudulent, but it was confirmed, it cannot be corrected in any way ", creates a number of vulnerabilities in the platform that can lead to branches (Forks) in the ecosystem of cryptocurrencies or smart contracts;
- risks of using artificial intelligence (AI) and robotization and automation technologies based on it. Along with new opportunities, the use of artificial intelligence technologies is accompanied by high risks. Thus, the use of artificial intelligence by cybercriminals creates threats of information leakage representing a commercial secret, etc.;
- risks and threats associated with the use of imported hardware components and the borrowing of new digital technologies. A potential threat is associated with the ability of the ICT manufacturer to embed targeted tabs in the manufactured components in the interests of special services. Considering that the schematic diagrams and source codes of the software

are known only to the developer, the risks associated with this vulnerability can lead to a decrease in the level of data security and a threat to the digital integrity of the IP;
- risks and threats associated with the use of cloud and distributed computing. Changes are taking place in the behavior patterns of producers and consumers; the company's dependence on the reliable functioning of ICT is increasing. Distribution of responsibility in the field of information security between enterprise users, the organization that owns the cloud platform and the Internet provider objectively entails blurring the boundaries of responsibility, reducing the level of control and management of protection means, and also increases legal uncertainty;
- risks and threats associated with the stability of the Internet.

Today, there are many examples of the need to pay attention to the risks of third parties. For example, through the use of a third-party point-of-sale system, more than 5 million Saks Fifth Avenue customers have received credit card data. Also, personal information related to credit cards has been publicized in BestBuy and Delta due to the involvement of a third party to establish online support [18].

These cases demonstrate that unjustified expectations regarding the quality and responsible work of third parties have serious consequences for the company itself. The enterprise needs to take into account the interdependence of the partners involved from other persons, for example, suppliers with whom they may be associated.

Another equally significant factor is cyber security and confidentiality. In the face of digital transformation, businesses and companies are increasingly turning to online procurement practices, cloud computing and digital data analytics, using third parties to drive processes. The danger is that business and company leaders may not always have an idea of their level of access to valuable information.

Equally important are the risks associated with the problems of integrating digital technologies between the main stakeholders, such as:
- risks of interaction with suppliers (search for suppliers of the necessary equipment (services) for the production of innovative products);
- the risks of the lack of unified IT platforms for the interaction of the enterprise with suppliers, transport companies, consumers of products or services, and regulatory organizations;
- risks of limited (or lack) digital integration with resource / service providers;
- risks of interaction with consumers (buyers) of products (services) of the enterprise.

The seventh group of risks is organizational and managerial risks. The risks included in this group are due to:
- the need to build a new organizational structure aimed at increasing the efficiency of digitalization of the enterprise;
- lack of well-established horizontal and vertical integration of the company's divisions;
- the underdevelopment of the digital infrastructure, which, on the one hand, is already a significant risk for EBS, and on the other hand, the accelerated digitalization of the enterprise in the direction of creating online platforms for cooperation can itself cause risks due to the complication of interaction models at different levels of digital development of participants.

It is necessary to note a problem that can have a negative impact on the level of EBP - the misconception of managers regarding the principles and goals of digital transformation. As noted earlier, enterprise digital transformation is the process of transforming business models under the influence of SCT. However, digital transformation doesn't really come down to just numbers. Digital technologies can bring about massive change, but they are still just a tool, because any enterprise or company can use digital technologies, but they do not always create a competitive advantage. In other words, digital transformation is not so much about new technologies as about how they will change the business processes of an enterprise. ”The eighth group is risks and threats of a legal nature. This group includes:

- lagging behind the normative legal regulation of economic relations from the speed of "digitalization";
- legal uncertainty of responsibility of subjects of legal relations in the digital economy;
- regulatory issues, ensuring the legal significance of digital economy technologies;
- uncertainty of the legal status of labor relations in the digital environment;
- lack of legal regulation of the activities of commercial organizations for the collection, transfer, storage, processing of digital data of the subject;
- lack of a legal mechanism for control and supervision of compliance with the established requirements.

4 Conclusion

The introduction of digital technologies in the business processes of an enterprise and its transition to functioning in a digital environment carries new risks and threats that are not inherent in traditional (non-digital) processes and are due to new technologies and features of the digital economy.

Identifying possible risks and threats is one of the most important tasks in ensuring the economic security of an enterprise in the digital economy. The efficiency of the developed and applied measures to minimize risks and neutralize threats to the economic security of an enterprise depends on the quality and timeliness of the implementation of this task. The approach to the analysis of risks and threats of an enterprise in the digital economy should be comprehensive and cover all the main business processes of an enterprise in the internal and external environment.

References

1. Chichkanov V.P., Belyaevskaya-Plotnik L.A., Andreeva P.A. Modeling the assessment of the impact of industry factors on the level of socio-economic development and economic security of territories // Economy of the region. **1**, 1-13, (2020).
2. Decree of the President of the Russian Federation of December 31, 2015 No. 683 "On the National Security Strategy of the Russian Federation" [Electronic resource]: Access from the reference legal system "Consultant Plus".
3. Decree of the President of the Russian Federation of 13.05.2017 No. 208 "On the Strategy of Economic Security of the Russian Federation for the Period up to 2030" [Electronic resource]: Access from the reference legal system "Consultant Plus".
4. Sergeev A.A. Economic security of the enterprise / A.A. Sergeev. - M .: Yurayt Publishing House, (2020).
5. Sannikova I.N., German O.I. Methodological aspects of assessing the economic safety of industrial enterprises // Economics Profession Business. **4**, 7-13, (2016).
6. Keshelava A.V. Introduction to the "digital" economy /: VNII Geosystem. (2017).
7. Moshella D. Guide to the digital future: Industries, organizations and professions / Alpina Publisher. (2020)
8. Stolbov M.I., Brendeleva E.A. Fundamentals of the digital economy: study guide / Publishing House "Scientific Library". (2018).
9. Decree of the President of the Russian Federation of 05.12.2016 No. 646 "On Approval of the Doctrine of Information Security of the Russian Federation" [Electronic resource]: Access from the reference legal system "Consultant Plus".
10. Litvintseva G.P., Karelin I.N. Effects of digital transformation of the economy and the quality of life of the population in Russia // Terra Economicus. **18(3)**. 53-71, (2020).

11. Zatsarinny A.A., Korolev V.I. Technological aspects of ensuring information security of the financial market in the context of digital transformation of the Russian economy // Systems and means of information. **29**, 12-24, (2019).
12. The assets of the organization as key risk factors. - URL: http: //analysis-riska.rf
13. Bulatenko M.A., Goronok D.L. Key problems of ensuring the economic security of an enterprise in modern conditions // Bulletin of the Altai Academy of Economics and Law. **2**, 71-75, (2019)
14. Derbin E.A., Klimov S.M. Organizational basis for ensuring the information security of an enterprise / Financial University. (2013).
15. Kuznetsova M.A. Industry 4.0 Risks and Their Impact on Industrial Organizations - Economy: Problems, Solutions and Prospects. - URL: https: // cyberleninka / article / n / riski-industrii-4-0-i-ih-vliyanie-na-promyshlennye-organizatsii.
16. Afanasenko I.D., Borisov V.V. Digital logistics / Peter. (2019).
17. Development of the Digital Economy in Russia. Program until 2035. URL: http://spkurdyumov.ru/uploads/2017/05/strategy.pdf. (date of access: 10.03.2021).
18. Third Party Risks: Is Control Possible? - URL: https://bizeducate.com/06/2019/riski-tretih-storon-vozmozhen-li-kontrol/