Advances in Economics, Business and Management Research, volume 156
2nd International Scientific and Practical Conference on Digital Economy (ISCDE 2020)

Ensuring Information Security as a Key Factor in the Development of the Digital Economy in the Russian Federation

Khochueva F.A.*, Shugunov T.L.

Kabardino-Balkarian State University, Nalchik 360004, Russia
**Corresponding author. Email: fah11061987@mail.ru*

ABSTRACT
The article deals with the problems of ensuring information security in the conditions of the functioning of the digital economy in the Russian Federation. The study is aimed to analyze the development of the digitalization of the economy in the Russian Federation, a comprehensive assessment of the risks of digitalization of the economy, and study the problems of ensuring information security in the context of the digitalization of economic processes. The process of digitalization of the economy is a necessary condition for the development of a modern information state. The development of innovative and information technologies contributes to the formation of a digital format of the economy. 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. Information security is a strategic direction of the state policy of the Russian Federation. The development of regulatory legal acts, strategic and project documents allows to reduce the level of risk in the context of the digitalization of the economy. Moreover, the use of technical means of protecting information is among the key tools. The use of technological innovative tools makes it possible to increase the degree of information protection and thereby reduce the level of cybercrime. The materials obtained as a result of this research have theoretical and practical significance for specialists in the field of ensuring economic and information security.
Keywords: *information security, digital economy, digitalization, cybercrime, information technology, cybersecurity, cryptocurrency, competition, cyberwarfare*

1. INTRODUCTION

The digital revolution is a necessary process for the development of society at the present stage. The society is undergoing rapid and large-scale changes, which are caused by informational and innovative changes in all spheres of life. It shall be noted that such transformations create both huge opportunities and a number of difficulties.

The active use of new information technologies contributes to sustainable development, but information technologies do not act as a guarantee of achieving effective results.

In the Russian Federation, the process of digitalization of the economy was launched relatively recently and it is extremely difficult. However, the complexity and constructiveness of the digitalization of the economy in the Russian Federation shall be noted. The effective functioning of the digital model of the economy is possible only if a high level of information security is ensured. It shall be noted that the issue of ensuring information security is one of the topical areas in the context of the digitalization of economic processes.

In this situation, the most constructive will be an interdisciplinary approach, which is based on two directions:

- maximum digitalization of all economic processes;
- ensuring a high level of cybersecurity.

The term "cybersecurity" is relatively recent, which explains the existence of several definitions. In the professional environment, the term cybersecurity is actively used in this industry, but the concept is a little "vague". The current situation creates theoretical and practical difficulties. In the context of the digitalization of the economy, the key issue is precisely ensuring cybersecurity. The solution to this issue is a problem at the state level. The digital economy is becoming a key object of competition in the global space. Economic information becomes vulnerable.

2. METHODOLOGY OF THE STUDY

Within the framework of this study, theoretical methods were widely used: an analytical review of theoretical

information, analysis of information from statistics bodies, generalization, and presentation of research results in graphical form.

In 2018, the President of the Russian Federation noted that one of the most important problems of the ongoing large-scale digitalization is the problem of ensuring the security of economic activities of individuals and legal entities at the BRICS meeting (Brazil, Russia, India, China, South Africa). It is noted that information security is one of the global problems of the modern information world. The digital economy acts as an element of the integration of the modern economic space. The solution to this problem is possible by creating the safest, most open, and reliable Internet space that will meet the high requirements for ensuring information security. [1]

In the field of the digital economy, a stable and effective interaction of the BRICS member countries has been formed.

3. RESULTS OF THE STUDY

If we consider the level of development of the digital economy in the Russian Federation, it shall be noted that the country's economy is in a phase of active development.

Table 1 presents the ranking of countries in the development of the digital economy.

Table 1 The level of development of cybersecurity in the world

Countries	Global Cybersecurity Index		Including sub-indices		
	Ranking place	Value	Legislative aspects	Technical aspects	Organizational aspects
Great Britain	1	0.931	0.200	0.191	0.200
USA	2	0.928	0.200	0.184	0.200
France	3	0.918	0.200	0.193	0.200
Lithuania	4	0.908	0.200	0.168	0.200
Estonia	5	0.905	0.200	0.195	0.186
Singapore	6	0.898	0.200	0.186	0.192
Spain	7	0.896	0.200	0.180	0.200
Malaysia	8	0.893	0.179	0.196	0.200
Norway	9	0.892	0.179	0.196	0.177
Canada	9	0.892	0.191	0.189	0.200
Australia	10	0.890	0.195	0.174	0.200
Italy	25	0.837	….	….	……
Russia	26	0.836	0.197	0.162	0.177
China	27	0.828	…..	……	……..

The table shows that the leading positions are occupied by Great Britain, the USA, and France. Russia is among the 30 countries.

Figure 1 presents an analysis of the state of development of information and communication technologies in the Russian Federation within the framework of the world space.

Figure 1 Russia's place in international development ratings

Figure 1 shows that the indicator of the global cybersecurity index is significantly higher than the index of the development of information and communication technologies and the development of e-government. This indicates that the pace of development of cybersecurity in the country is outstripping.

An effective assessment of cybersecurity is possible only in the context of an integrated approach, the key criteria are: the level of legislative, technical, and organizational support. [2]

Formation of the regulatory and legal foundation is one of the main conditions for creating an effective system for the functioning of the digital economy with the required level of data protection.

In recent years, a regulatory and legal mechanism has been developed in the Russian Federation, which includes federal laws, decrees, programs, strategic development plans, etc. This largely explains that this sub-index is higher than the sub-indices in terms of technological and organizational aspects.

In the Russian Federation, a system for the development of a regulatory and legal framework has been developed, which is the initial stage, and in the future, a technological and organizational foundation is being developed.

The digitalization process is technically complex, which leads to the emergence of many risks of a different nature.

The risks arising in the field of the digital economy have a negative impact not only on the economic sphere, but also on the national security of the state.

Now is the era of world confrontation, especially in the economic sphere, since it is the economy that is one of the most important resource components of each state, in modern society the development of the economy is largely determined by the development of other spheres of the state. The processes of globalization are most active precisely in the economic sphere and the information space, which in turn requires the formation of effective tools for the protection of economic and other information.

It is obvious that information is an important resource with a high degree of vulnerability, and in the 21st century the concept of "cyberwarfare" is replacing military conflicts. Most experts claim that the so-called information wars are the main conflicts of the modern world. [3]

Stable and effective economic development is a necessary condition for the functioning of a strong, modern, and dynamically developing state. The new format of the economy in its digital form makes a number of high requirements for the level of protection of the relevant information. The effective functioning of the digital economy is possible only through the creation of a sustainable cybersecurity system.

The issue of ensuring information security in the context of digitalization causes difficulties, since working with a large amount of information, artificial intelligence technologies, the Internet of Things is extremely difficult and there is a high probability of losing it.

Global companies Amazon, Apple, Google, Facebook have developed and are actively using artificial intelligence technologies, digital platforms, and other technologies. Thus, it is known that the social network Facebook has launched DeepTex technology. The technology developed made it possible to trend user actions based on messages.

The difficult economic situation that has developed in the world and in the Russian Federation as well, has an impact on the ongoing digitalization of economic processes.

In the context of the digitalization of the economy, there is an increase in the number of cybercrimes in the economy. The protection of the modern digital economy will only be ensured by the creation of a flexible and effective system of cyber protection in technical, regulatory and organizational terms.

The creation of a global digital economy system faces a number of difficulties, since a number of countries cannot make the transition to a digital format, due to their slow economic, technological and information development. The digitalization process in the Russian Federation is difficult, the reason for this is the instability of economic and technological development.

The target of cybercriminals is organizations and other business entities that have strategic information resources.

The growth of cybercrimes in the Russian Federation is quite high, which also negatively affects the development of the digital economy and its protection system. In the context of the digitalization of the economy, such processes are taking place as the growth in the use of digital technologies, the complication of these technologies, which leads to an increase in the number of information security violations. [4]

Medium and large business entities are faced with very serious cyber attacks, and their number is also increasing. For most modern companies, it is the digital technologies used that become the main resource, which is the target of cybercriminals.

Economic entities actively protect their business reputation and strive to maximally preserve the trust of their customers and counterparties. In this connection, it is necessary to ensure a high level of information protection, which will help to increase the competitiveness of economic entities and the state economy as a whole.

If we consider the sectors of the economy pursuant to the degree of their information vulnerability, then the most vulnerable is the banking sector. Since it was the banking cluster that was subject to the active digitalization process. Banking information is of most interest to cybercriminals. Most cyber attacks are performed in the banking sector. Each year, the percentage of cybercrimes in the banking sector is increasing, given the technological and regulatory advances in this sector.

Cybercriminals are expanding their activities as the use of information technology in the banking sector increases. That is, as the banking sector widens the range of technologies and software applied, the cybercriminals are also expanding their technological tools. But cybercrime is committed not only by external offenders but also by bank employees. It is bank employees who pose the greatest threat to the information and financial security of credit institutions. Thus, it is the banking sector that is exposed to the highest risks, in contrast to other sectors of the economic space. [6]

Consideration of the problem of ensuring cybersecurity in the context of the development of a digital format of the economy shall be considered only within the framework of a new technological and scientific paradigm. [7]

As reported at the 2019 World Economic Forum, the cyberattacks and information (database) fraud are the fourth and fifth global risks faced by legal entities. These risks are equated in importance with environmental problems.

In 2020, there is a sharp increase in the number of cyberattacks committed (Figure 2). The growth is especially noticeable in March, April, May, and June compared to the same period in 2019. This is explained by the extremely difficult economic situation, which was provoked by the epidemiological situation around the world. During this period, the actions of fraudsters intensified significantly, who used the current difficult situation to their advantage.

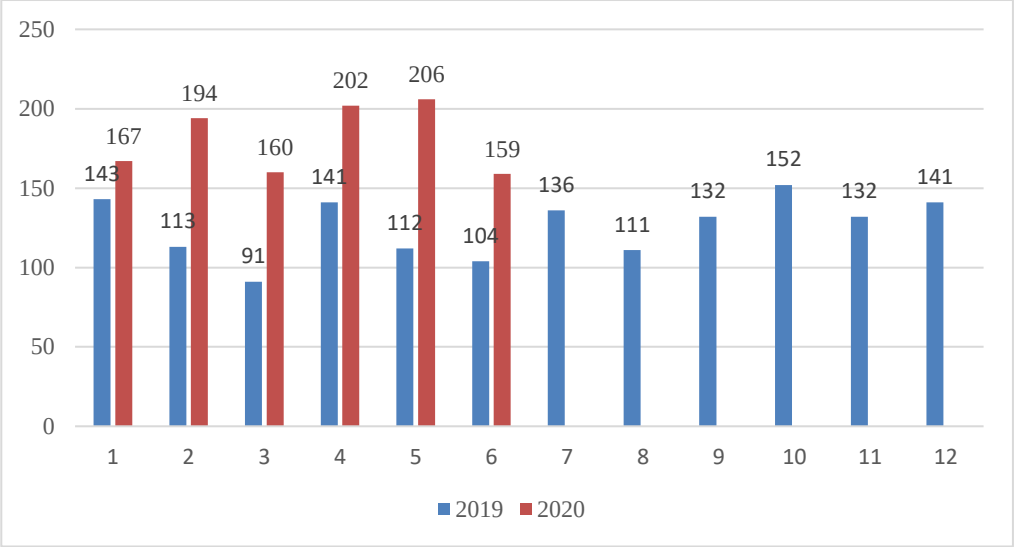

Figure 2 Number of attacks in 2019 and 2020 by month

Pursuant to the Cybersecurity Ventures' 2019 Cybercrime Report (ACR), the cyber attacks in the world occurred every 14 seconds in 2019, and their frequency could be 11 seconds by 2021. InfoWatch specialists reported that over 14 bln. confidential records were leaked to the network over the past year. The growth in the number of leaks in the world compared to 2018 increased by 10%, in Russia - by more than 40%.

If we consider the structural composition of committed cybercrimes, which is shown in Figure 3, then the largest number is committed precisely in relation to databases. Cybercriminals commit crimes for financial gain.

For the period from January 28, 2019, to January 27, 2020, the number of notifications per day increased from 247 to 278 compared to the period from May 25, 2018, to January 27, 2019. The growth was 12.6%. In 2020, experts predict the growth of these indicators.

But it shall be noted that the official statistics does not correspond to the real situation. Thus, the head of the department of the center for complaints on Internet crimes of the US Federal Bureau of Investigation informed that only 10-12% of the total number of crimes were registered. Affected citizens, legal entities that are subjected to extortion on the Internet, rarely seek professional help, arguing this with a number of assumptions: the risk of publishing the stolen information; lack of assistance from the organs in sufficient volume.

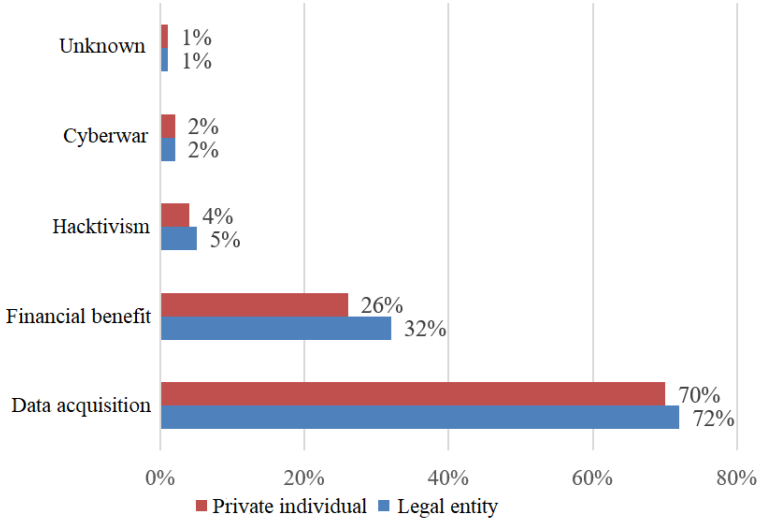

Figure 3 Structural composition of cybercrime committed

It is obvious that the format of the digital economy leads to an increase in the number of cybercrimes.

Pursuant to a study by the University of Sydney in Australia, most anonymous transactions and illegal activities on the network occur using the cryptocurrency - bitcoin. The total turnover of the cryptocurrency is USD 76 bln.

One of the most important factors in the development of the national economy is an effective system for the functioning of the digital economy, which will include an integrated information security system. The introduction of the digital form of the economy has a huge impact on the sustainable development and competitiveness of organizations and the state as a whole. One of the priority areas for ensuring the national security of the Russian Federation is the introduction of innovative technologies.

In terms of the competitiveness of countries in the context of the transition to the digital age, the influence of the digital economy on the national and information security of the state is especially noticeable. The digital economy is the main engine for the introduction of innovations and the development of the entrepreneurial sector of the economy. [8]

In order to develop the digital economy in the Russian Federation, the "Digital Economy" national project for the period 2019-2024 was developed and systematically implemented. The main directions of this national project are as follows:

– Creation of a stable and secure information and telecommunication system;
– Comprehensive and safe processing of large amounts of information;
– Ensuring the availability of the information and telecommunication system;
– Formation of a network providing high-speed data transmission.

RUR 403 bln. has been allocated for the implementation of the "Digital Economy" program in 2019-2021. However, the events of 2020, associated with a difficult epidemiological situation and unplanned government spending, led to a revision of the costs of the national project [9]

In mid-September 2020, the government decided to cut costs for the implementation of a number of national programs, including the "Digital Economy". This follows from the explanatory note to the draft budget for the next three year period. The financial support of the "Digital Economy" is planned to be reduced by RUR 92.2 bln.

4. DISCUSSION

Ensuring information security in modern conditions is difficult. Information security professionals define the protection of the integrity and confidentiality of strategically important information and ensuring accountability as the main vectors of their work.

Building an effective security system presupposes the creation of an extensive information infrastructure that will provide timely and secure access to information that personnel needs. Today, threats to the information environment appear in new forms and forms, therefore, it is extremely important to be aware of changes in the information infrastructure.

Ensuring information security of the digital economy of the state is possible only using innovative protection tools. [10]

Today, innovative tools for protecting personal data include, first of all, biometric technologies, which are based on a mechanism for recognizing the unique biological characteristics inherent in each individual person. Depending on the composition of individual characteristics of a person, two types of biometric data are distinguished: statistical, which are inherent in a person from birth (for instance, DNA, fingerprint, retina), and dynamic, which a person acquires and is able to change them with age (for instance, speech dynamics, handwritten signature or pace of typing on the keyboard, etc.). The global biometric technology market is increasing its growth rate every year. Pursuant to the forecast of the international consulting company "J'son & Partners Consulting", the market volume by 2022 will reach more than 40 billion US dollars (Fig. 4). [11]

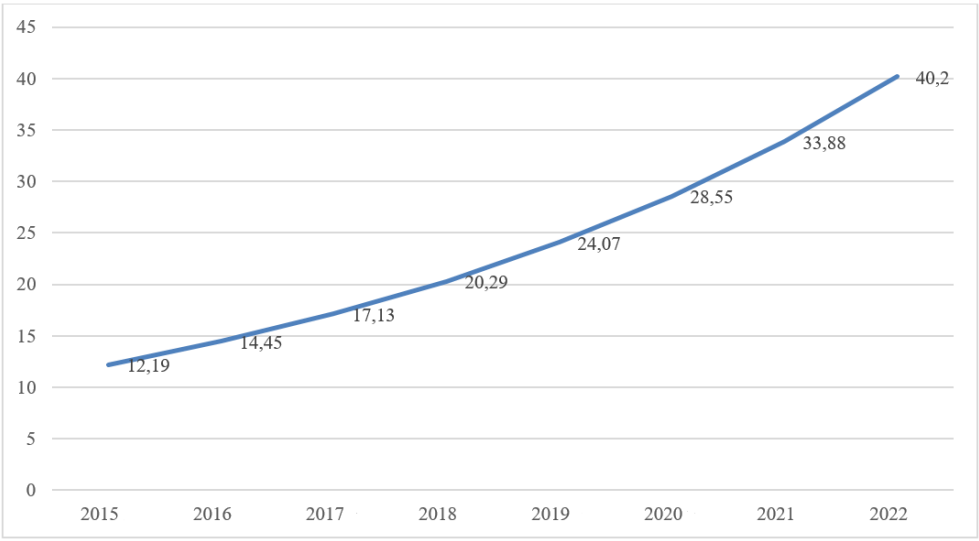

Figure 4 Volume of the 2015-2022 world market of biometric technologies, USD bln USA

5. CONCLUSIONS

The main segments of the world market for biometric technologies are the state segment, which includes electronic documents (citizens' passports, driving licenses, etc.) and national security systems, as well as tourism (migration), financial, corporate segments, biometric technologies in the field of healthcare and retail. The main development trend of the world market for biometric technologies is the active development of the commercial segment. [11]

The main driver of growth in the use of biometrics in the financial market is the active development of mobile technologies, and, accordingly, the popularization of mobile banking, which has occupied a leading position in the electronic banking market for several years. Today, all modern mobile phones have a fingerprint scanner, which once again confirms the leading position in the market for this biometric technology. Moreover, smartphones are able to record a voice, take pictures, and high-quality cameras even allow a person to be identified by the iris of the eye.

Naturally, in the current environment, an integrated approach is required, which includes regulatory protection and a modern technological system to ensure cybersecurity.

The basic technological tool for ensuring cyber protection is cryptography. Domestic cryptography products are being actively developed, but they are not recognized in the global information security market. It is necessary to enhance this area, which will enhance the quality of these software products. [12]

Thus, the digitalization of the economy entails a number of risks. The problem of ensuring cybersecurity in the context of the digitalization of the economy is not only a local problem, it is global in nature. Cybersecurity specialists exchange experience in the framework of ongoing international events on information security, which significantly increases the level of cybersecurity development.

REFERENCES

[1] A.Z. Zhukov, T.L. Shugunov, Ch. Kh. Ingushev, F.A. Khochueva, Topical issues of ensuring cybersecurity in the context of digitalization of the economy of the Russian Federation, Problems of economics and legal practice, 4 (2020) 310-313

[2] D.V. Udalov, Threats and Challenges of the Digital Economy, Economic Security and Quality, 1 (2018) 12-18

[3] E. E. Frolova, Information Security of Russia in the Digital Economy: The Economic and Legal Aspects, J. of Advanced Research in Law and Economics, 9 (1) (2018) 89-95.

[4] B.A. Tarchokov, Analysis of Criminal Acts Committed in the Banking Sector Using Internet Technologies, Gaps in Russian Legislation, 5 (2017) 211-212

[5] F.A. Khochueva, T.L. Shugunov, A.Z. Zhukov, Ch.Kh. Ingushev, Information security through the prism of the digital economy, Modern high technologies, 11 (2018) 65-71.

[6] A.Z. Zhukov, Ways to improve methods of countering cyber terrorism in the Russian Federation, Gaps in Russian legislation, 13 (4) (2020) 67-70.

[7] T.R. Peltier, Information Security Fundamentals (2nd ed.), CRC Press: 438, 2013.

[8] T.L. Shugunov, T.Yu. Khashirova, A.S. Ksenofontov, M.A. Georgieva, S.M. Arvanova, Topical Issues of Information Security in Modern Economic Conditions, Int. J. of Engineering & Technology, 7 (4.38) (2018) 1227-1230

[9] Program for the development of the digital economy in the Russian Federation until 2035. http://spkurdyumov.ru/uploads/2017/05/strategy.pdf

[10] T.L. Shugunov, A.Z. Zhukov, F.A. Khochueva, Problems of ensuring the cyber resilience of the banking system of the Russian Federation: legal and methodological aspects, Gaps in Russian legislation, 6 (2019) 250-253.

[11] C.S. Teoh, A.K. Mahmood, National Cyber Security Strategies for Digital Economy, ICRIIS-2017, Langkawi, 2017, pp. 1-6.

[12] I. Miles, Services in the New Industrial Economy. Futures, 25 (6) (1993) 653-672.

[13] M.D. Cavelty, V. Mauer, Power and Security in the Information Age: Investigating the Role of the State in Cyberspace, Routledge: 182, 2016.

[14] M.A. Averyanov, S.N. Evtushenko, E.Yu. Kochetkova, Digital Society: New Challenges, Economic Strategies, 7 (141) (2016) 90-91.

[15] G.N. Andreeva, S.V. Badalyants, T.G. Bogatyrev, V.A. Borodai, O. V. Dudkina, A.E. Zubarev, L.N. Kazmina, L.A. Minasyan L.V. Mironov, S.A. Strizhov, M.L. Sher, Development of the digital economy in Russia as a key factor in economic growth and improving the quality of life of the population: monograph, Nizhny Novgorod: Publishing House "Professional Science", 2018, 131 p.

[16] A.Z. Zhukov, T.L. Shugunov, Current trends in the legal regulation of information security abroad, Gaps in Russian legislation, 3 (2019) 224-226.

[17] A.V. Keshelava, V.G. Budanov, V.Yu. Rumyantsev et al., Introduction to the Digital Economy, 2017, 28 p.

[18] IN Kuznetsov, Business Security Publishing and Trading Corporation "Dashkov and K" 2016, 416 p.

[19] On the approval of the program “Digital Economy of the Russian Federation: Order of the Government of the Russian Federation of July 28, 2017 N 1632-r. http://www.consultant.ru/document/cons_doc_LAW_221756/

[20] Economics. Information security. https://data-economy.ru/security

[21] A. Aja, D. Bustillo, Jr. W. Darity, D. Hamilton, Jobs Instead of Austerity: A Bold Policy Proposal for Economic Justice. Social Research: An International Quartlery, 80 (3) (2013) 781–794.

[22] K. J. D. Boutin, China’s Industrial Development and Regional Economic Security, Alfred Deakin Research Institute, 2014. www.deakin.edu.au/research-services/forms /v/7808/wps-44w.pdf

[23] D. Roshidi, G. Osman, J.Q. Alaa, Analytical Review on Graphical Formats Used in ImageSteganographic Compression Indonesian J. of Electrical Engineering and Computer Sci. 5 (3) (2017) 401-408. DOI: 10.11591/ijeecs.v5.i3.pp401-408

[24] Securing Information in The New Digital Economy, McKinsey & World Economic Forum, 2014.

[25] Collection of Legislation of the Russian Federation 2017, No. 42.http: //www.szrf.ru/szrf/oglavlenie.phtml?nb=100&issid=10002017042000