Advances in Economics, Business and Management Research, volume 114
First International Volga Region Conference on Economics, Humanities and Sports (FICEHS 19)

Information Security Issues in the Age of Digital Economics

Dzobelova V.B.
Costa Levanovich Khetagurov State University
Vladikavkaz, Russia
dzobelova@mail.ru

Ilaeva Z.M.
Chechen State University
Grozny, Russia
dzobelova@mail.ru

Melenchuk A.S.
Maikop State Technological University
Maikop, Russia
aleksandr.melenchuk@russianpost.ru

***Abstract*—Ensuring information security in the modern conditions of establishing digital economy is one of the primary objectives both at the state level and at the level of individual organizations. This article is devoted to the issues of information security in the context of digital economy. The purpose of the article is to analyze the existing issues in the field of information security and to consider measures for the solution of this problem, including those ones based on the study of foreign experience in this field. The main trends in the Russian information security market, formed under the influence of Russian legislation and changes in the spectrum of internal and external threats, are highlighted**.

Keywords—digital economy; strategy; information society; economic security; information security.

I. INTRODUCTION

The process of formation of the global information society is developing at a steadily increasing pace. Today we are witnessing the widespread introduction of fundamentally new tools for managing economic systems both at the level of separate countries and on a global scale. There even appeared a new term "digital economy", implying the use of modern information and communication technologies (ICT) in securing of the economic system functioning. On the other hand, digital economy, basing on the concept of artificial intelligence, also means the implementation of decision-making support systems, grounded upon a wide range of digital predictive models.

When introducing the digital economy, the problem of information security becomes very critical, since our country has a poorly developed legislative framework on this issue, and software, including the Russian one, is insufficiently developed. Leakage of any information can cost any enterprise dearly, for this reason it is necessary to strengthen information security. The positive effect of implementing the processes of economy digitalization is possible only in a secure information environment. Otherwise, the consequences of such "digitalization" can be merely disastrous.

II. RESEARCH METHODOLOGY

The transition to digital technologies has fundamentally changed the attitude to information, to data storage devices, what has significantly modified the relation to economic security, shifting priorities from the physical protection of the personality and property to ensuring sustainable progressive development. The digital economy is extensively replacing the old pattern in many areas of activity. This increases the efficiency of all industries, because the use of modern information technologies actively contributes to this. Private life and workplaces are transformed, new professions and tools of interaction appear. In the era of large-scale transformations, the problem of information security in organizations is becoming increasingly urgent.

Information security as one of the most important components of general security determines economic and general security at all levels [1].

Nowadays, active development of information technologies in the field of information transmission and processing has made information the most valuable resource. Today, information has a unique value; one can even say that it is one of the most critical resources.

Information security of the country in the 21st century has become the most important component of the modern digital economy of any state. Its development and strengthening is possible only in the context of using the most relevant IT-technologies and complex measures concerning the education of the population in terms of main threats that lie in wait for the uninformed participants of the cyberspace [3].

In 2017, the Government Committee on the use of information technology approved the action plan for the line of "Information security" of the program "Digital economy of the Russian Federation over a period of 2018-2024" in order to improve the quality of life and business environment. The plan contains measures that allow to prevent cybercrimes at the modern technological level. This concerns not only the security in the information space, but also legal protection in the age of digital economy. One of the main objectives of this plan is first of all to improve the skillfulness of users when surfing Internet and network information resources.

Information security in the program "Digital economy" is allocated in a separate – fifth section, which is nowadays actively discussed in expert groups [2].

Information security is the practice of preventing unauthorized access, use, disclosure, misrepresentation, alteration, research, recording or destruction of information. It covers many industries, one way or another related to information technology.

Development and implementation of the Program activities are based on the following principles of information security: availability, integrity and confidentiality of information and its reduction processes should be ensured through the use of Russian technologies; preferential use of domestic software and equipment; use of Russian standards for cryptographic protection of information.

All this testifies to a special importance of solving the problems of information security in the era of digital economy.

The digital economy will not be able to exist without information security, which means that information security is not a matter of domain anti-hacker specialists, but the concern of all stakeholders: architects, designers, developers, testers and users themselves. Information security needs to be strengthened at the legislative level, as well as through the training of young professionals in this area, because in the age of internet technologies and hacker attacks, information can be expensive.

As the technological process develops, information becomes the most valuable resource. In this regard, the problem of information security as a guarantee of social and economic stability of society during the transition to the digital economy is actualized.

III. RESULTS

In today's context, the work of any large company is based on information. Computers have almost replaced the human brain. That is why computers are becoming a tasty morsel for competing organizations and attackers who earn living by information theft. Recently, the number of targeted hacker attacks has increased significantly, as well as the use of spyware has become more frequent. Espionage moves to the industrial level, and the modern world is seized by a wave of cybercrime. Creating and improving Trojans, virus programs, systems of simplified penetration hackers seek to improve the quality of their products. The number of hacks in the future is likely to decrease, but it won't be possible to track them.

Now information is used as an auxiliary link for making important strategic decisions, in the future much depends on how reliable it will be and how relevant it will be. Disclosure or loss of confidential commercial information may cause significant losses to the company, including financial damage as well as a negative impact on the company's reputation. The loss of one or more links of information resources can permanently stop the activity of the whole enterprise. Therefore, it becomes obvious that the issues of information security will always be the key problems of doing business.

The traditional model of information security, which has long been based on confidentiality, integrity and accessibility, is gradually transforming into a model focused on accessibility and cyber resistance. The ability of companies to resist information threats and recover quickly in case of their implementation comes to the fore. There is a shift in emphasis towards risk-based security and protection against various threats.

According to McAfee experts, the global damage from cybercrimes in 2017 alone is estimated at about $ 600 billion, which is 0,8% of world GDP. Compared to 2014, the amount of damage increased by about 35%. The main factors contributing to the growth were hacker attacks, the expansion of the market for cybercriminal services and the spread of crypto currencies. So, in 2017, hackers stole 172 billion dollars from 978 million consumers in 20 countries, having proved in practice that online users are overconfident in matters of cyber security [2].

The targets of most attacks are financial sector companies. According to experts of Russian Sberbank, the global damage from cyber attacks in 2018 amounted to $ 1 trillion, and in 2022 this amount is expected to grow up to $ 8 trillion [5]. Herewith, more than 80% of hacker attacks are based on social engineering methods. Still, only 20% of incidents become public, as companies try not to disclose this information. Among all the most famous cyber threats in the world, we can mention viruses-cryptographers such as WannaCry [5].

In the event of an information security incident, the amount of damage depends largely on the readiness of the company to respond to it in a timely and adequate manner and on the correctness of the employees' actions. However, a study conducted by workers of Positive Technologies showed that in practice companies rarely use specialized security tools. For example, web application firewalls (WAF) are used by only 23% of all the surveyed industrial companies, only 17% apply security information and event management systems (SIEM) and only 13% of industrial companies regularly conduct penetration tests. 33% of companies have never carried out inventory and control over the appearance of unsafe resources within the perimeter of the enterprise network. 40% of companies have never analyzed the security of corporate wireless networks; 23% of surveyed companies do not control the installation of software updates, and regular training of employees in terms of information security basics is carried out by only 23% of companies [2].

Companies' awareness of the cyber threats danger contributes to more effective security strategy planning. Therefore, at the level of companies, the role of information security as part of the overall corporate business strategy is currently being re-thought and the costs of protecting information resources are increasing.

Another tendency that can be traced in the information security market is involvement of the top management of enterprises in information security issues. This is caused by the law "About security of critical information infrastructure of the Russian Federation", which introduced criminal liability for non-compliance with information security requirements, if it entailed serious consequences [4].

Channels through which corporate information is transmitted are constantly appearing and becoming more difficult to control. However, the most unpredictable source of threats to information security is human. Therefore, the focus of developers' interest shifts to the personality. As a result, there is a trend in the information security market to create technologies that prevent incidents by analyzing the user's behavior, identifying abnormalities in his actions. Such technologies are already used by Sberbank of Russia.

Development of the digital economy of Russia is accompanied by strengthening of the information technologies role. There is a growing need to protect information resources and critical information infrastructure. In recent years, much has been done in the Russian Federation to develop the domestic information security market; the leading consumers of its services are organizations that process large amounts of personal data and

financial information. Trends in the information security market, formed over the last years under the influence of Russian legislation and a variety of information threats, indicate the increasing role of information security in the digital economy.

In the conditions of digital economy development, the issues of information protection should be considered not only at the level of separate organizations, but also at the country level.

Initially, it is necessary to form a group of experts at the state level, which will develop an information security policy through cross-industry cooperation. The result of such work should be an information security strategy with clear targets, objectives and action plan for its effective implementation; the developed strategy should take into account various specific aspects of economic sectors. The state strategy should also include regulations on the risks assessment in the field of information security in order to optimally respond to their occurrence in various areas. Moreover, a separate element of the strategy should be a critical information infrastructure, on which the national security of the state depends.

The next step is to improve the legal and regulatory support for information security, as well as to develop new legal rules for certain cases of fraud that are not covered by existing laws. This stage of information security should become a continuous process of updating the regulatory framework, as every day there appear new threats to the data safety, which previously the society has not faced, or they have not demonstrated themselves on such a large scale.

Further, on the basis of the adopted strategy and the updated regulatory framework in the field of information security, it is necessary to develop and approve industry standards for information security. It is also important to establish reliable data collection on cases of data security violations: at present, the population and organizations cannot always confidently say that they came up with information leakage, so it is necessary to create conditions for effective cooperation between the state and other business units. Moreover, education policy is also related to information security: in the modern conditions of digital technology development, the amount of information collected and analyzed is constantly increasing, which creates new threats that require special professional skills to combat. Therefore, the development of country's human resources is an important element of maintaining information security at all levels of the economy.

IV. CONCLUSION

Thus, the digital transformation, carried out in many sectors of the economy, has led to the change in the scale of activity of economic entities and appearance of new risks and threats, which the world has not faced before. The formation of the digital economy largely depends on ensuring information security: the emergence of threats to the safety of digital data becomes one of the main areas of security protection, both at the state level and at the level of individual organizations and citizens. Currently, attacks on data storage systems are becoming more complex and frequent, that is why information security issues should be a top target for maintenance of the economy resilience.

References

[1] Buryak V.V. Digital economy: breakthrough technologies in education. Innovative science. 2018, 7-8, pp. 55-59.

[2] Vagurina I.V. Problems of introduction of digital technologies in education. In the collected book: Transprofessional as a predictor of socio-professional mobility of the youth. Materials of all-Russian scientific-practical conference (with international participation). 2019, pp. 340-342.

[3] Kotova L.R. Influence of digital technologies on education. In the collected book: View of the XXI century generation on the future of digital economy. Collection of articles by teachers of the IX International scientific and practical conference "Modern economy: concepts and models of innovative development". 2018, pp. 183-186.

[4] Filatova O.N., Krupa V.V., Bystrova N.V. Professional education in the strategy of digital technologies development. Problems of modern pedagogical education. 2018, 61-2, pp. 200-202.

[5] Dzobelova V.B. New Ways of Qualified Staff Training by the Example of the Republic of North Ossetia-Alania. Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region, PTES. 2018, pp. 23-28.

[6] Dzobelova V.B., Olisaeva A.V. Staffing Needs in the Regional Economy under the Modern Conditions of Labor Market. Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region, PTES. 2018, pp. 185-188.

[7] Dzobelova V.B., Olisaeva A.V. Analysis of innovative development of the NCFD regions in Russia. IDIMT 2018: Strategic Modeling in Management, Economy and Society – 26th Interdisciplinary Information Management Talks. 2018, pp. 473-479.

[8] Olisaeva A.V., Dzobelova V.D., Yablochnikov S.L., Cherkasova O., Davletbayeva N. Formation and development of the digital economy in modern conditions - development within the framework of industry 4.0. In the collection: IDIMT-2019. Innovation and Transformation in a Digital World Ttrauner Druck GmbH & Co KG, Linz. 2019, pp. 83-88.

[9] Rysin Y.S., Terekhov A.N., Yablochnikov S.L., Ievlev O.P., Dzobelova V.B. On the Issue of Speaker's Identification in Communication Networks and Terminal Equipment of Onboard System 2019. Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG. 2019.

[10] Yablochnikov S.L., Yablochnikova I.O., Vidov S.V., Kuptsov M.I., Olisaeva A.V. The Aspects of Modeling Information Processes Realized in Complex Telecommunication Systems. In the collection: Wave Electronics and its Application in Information and Telecommunication Systems, WECONF. 2018, pp. 8604360.

[11] Digital Economy: Innovation, Growth and Social Prosperity OECD Ministerial Meeting. Canchn, Mexico 21-23 June 20l6. URL: http://www.oecd.org/sti/ieconomy/sti-cancun- 2016-flyer.pdf Retrieved: Dec, 2016.

[12] Sukhomlin V.A. Open system of education as a tool of formation of digital skills of the person. Strategic Ppriorities. 2017, 1, pp. 70-81.

[13] Kupriyanovskiy V.P., Sukhomlin V.A., Dobrynin A.P., Raikov A.N., Shkurov F.V., Drozhzhninov V.I., Fedorova N.O., Namiot D.E. Skills in the digital economy and challenges of the education system // International Journal of Open Information Technologies. 2017, 5, pp. 19-25.

[14] Bondarenko, V.M. World outlook approach to the formation, development and implementation of the "digital economy". Modern IT and IT-education, 2017. URL: https://inecon.org/docs/2017/Bondarenko_IT_2017.pdf.

[15] Dobrynin, A.P. Digital economy - various ways to effective application of technologies (BIM, PLM, CAD, IOT, Smart City, Big Data and others). International journal of open information technologies. 2016, vol. 4, 1, pp. 4-11.

[16] Alexsandr S. Kuznetsov. Russian Professor's meeting. Russian Journal of Physical Education and Sport. 2019, 14(1), pp. 17-22. DOI: 10.14526/2070-4798-2019-14-1-18-24

[17] Preobrazhenskiy A.P., Choporov O.N. Analysis of features of quality assessment of educational processes at preparation of experts. Science of Krasnoyarsk region. 2016, 3-3(26), pp. 186-191.