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

Digital Economy Challenges and Opportunities: HR Specialists for Information Security of the Financial Sector

Artamonova Y.S.[1], Beloborodko A.M.[2,*] Fridman M.F.[3]

[1]*Technical University of Communications and Informatics, Moscow, Russia*
[2]*Moscow Economic Institute, Moscow, Russia*
[3]*Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Moscow, Russia*
[*]*Corresponding author. Email: alex_belob@mail.ru*

ABSTRACT
This article is devoted to a topical and important issue. Information security is one of the most pressing problems of the modern digital economy. To a large extent, this concerns the financial sector, which carries out electronic transactions and is actively looking for more efficient analogues of metal coins, paper banknotes, plastic cards, etc. Thus, the intensive introduction of information technologies entails cybersecurity problems. The emergence and consolidation of the cryptocurrency on the world market causes a tangible need to reinstitutionalize the existing economic relations. The main reason for these problems, most likely, should be called an acute shortage of specialists in the field of modern information technologies and who understand the essence of the ongoing changes associated with the digitalization of the economy.
Keywords: *digital economy, information security, financial sector, human resources*

1. INTRODUCTION

Currently, the digitalization of the economy has become an objective reality. With the advent of the information society, the system of social relations is undergoing very significant changes [1]. The development of information technologies in the context of NBIC convergence and the deployment of the sixth technological paradigm will inevitably lead to automation and robotization of not only a wide range of labor functions, the entire way of life, everyday life depends now on the intensive acceleration of the movement of information [2]. Today, the digital economy in "The Strategy for the Development of the Information Society of the Russian Federation for 2017-2030" means "economic activity in which digital data is a key factor in production, the processing of large amounts of data and the use of the analysis results of which, in comparison with traditional forms of management, significantly to increase the efficiency of various types of production, technologies, equipment, storage, sale, delivery of goods and services" [3]. Since 1995, russian and foreign researchers have been studying the political economic phenomenon of the digital economy, including N. Negroponte (author of the term), E.N. Veduta, L.P. Goncharenko, S.Yu. Glazyev, A.I. Gretchenko , V.V.Ivanov, M.Yol, G.Kaidzyun, M.V.Kudina, V.I.Maevsky, G.G. Malinetsky, D. Tapscott, A. Espinosa and others [4].

With the development of automation, computerization, robotization, artificial intelligence, economic activity based on digital technologies is exposed to threats, the minimization of which did not require much attention from almost all existing social institutions before. Information security (the practice of protecting information by mitigating information risks, sometimes shortened to infosec) is becoming a key problem today. This is especially true for the financial sector, which uses various forms of electronic transactions (ATMs, terminals, online services, etc.).

The financial sector of the economy traditionally includes organizations that provide financial services to legal entities and individuals and combine the tax, budget and monetary systems. Information security is aimed at implementing a full range of measures to ensure comprehensive protection of confidentiality, integrity and availability of information, preventing unauthorized access to data, which entails the use, distribution, falsification, alteration or destruction of information. Information security problems were studied in the works of Yu.F. Abramov, G.A. Atamanov, V.G. Afanasiev, N.P. Vashchekin, S.V. Markov, I.S. Melyukhin, N.N. Moiseev, Yu.M. Plotinsky, A.I. Rakitov, A.A. Rodionov, A.V. Sokolov, B.A. Suslakov, A.D. Ursul, V.F. Khalipov, O.M. Tsydenova, F. I.Sharkov, V.P. Shemyakin, Yu.V. Yakovets and others [4].

2. RESEARCH METHODOLOGY

Analysis of the current regulatory framework, public statements by officials, expert assessments, public opinion polls and federal projects and programs revealed a great

need for personnel who would be able to provide the modern financial sector of the Russian economy with the necessary level of information security.

Currently, according to the Ministry of Digital Development, Communications and Mass Media of the Russian Federation [6], in Russia in the context of the implementation of the Decree of the President of the Russian Federation dated May 7, 2018 No. 204 "On national goals and strategic objectives of the development of the Russian Federation for the period up to 2024 " in the context of the need to ensure the accelerated introduction of digital technologies in the economy and social sphere, the Government of the Russian Federation has developed and is implementing the national program "Digital Economy of the Russian Federation", approved by the Protocol of the meeting of the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects No. 7 dated June 4, 2019, and aimed at increasing internal costs for the development of the digital economy at the expense of all sources; creation of a stable and secure information and telecommunications infrastructure for high-speed transmission, processing and storage of large amounts of data, accessible to all organizations and households; preferential use of domestic software by state agencies and local governments. Obviously, the goals specified in the passport of the national program do not fully reflect the personnel policy that ensures information security of the financial sector of the Russian economy.

The structure of the national project includes six federal projects, including "Normative regulation of the digital environment"; "Information infrastructures"; “Human Resources for the Digital Economy”; "Information Security"; "Digital Technologies" and "Digital Public Administration". It should be noted that two out of six projects indicate the relevance and importance of the problem we are considering, and also emphasize the fact that the country's government is showing attention to solving these issues.

The federal project "Information Security" is aimed at "ensuring information security based on domestic developments in the transfer, processing and storage of data, which guarantees the protection of the interests of individuals, business and the state." As part of the implementation of this area of work in the current year (06/30/2020) “a specialized resource has been created for interaction with authorized organizations in terms of the prompt transfer of data on the signs and presence of illegal actions in the field of information technology (computer fraud, imposed services of telecom operators, phishing schemes) in order to combat computer crime, especially in the financial sector, as well as other cases of criminal and illegal use of information technology." This result clearly illustrates the real attitude to the problem of information security of the financial sector of the Russian economy, indicating the absence of preventive measures to counter illegal actions in this area.

The federal project "Human Resources for the Digital Economy" is aimed at "ensuring the training of highly qualified personnel for the digital economy." As the analysis of the passport of the national project shows, the question of staffing the information security of the financial sector of the Russian economy remains open. 32 Positions are declared in the draft, delicately bypassing this issue, which, in our opinion, is of the utmost importance. X International Sociological Grushin Conference “Living in Russia. Live in peace. Sociology of Everyday Life”, which took place from May 20 to November 14, 2020 [7], in the report by O. P. Novozhenina and O.V.Grebnyak "Features of the implementation of the" digital economy "project in a pandemic reality" also did not leave this problem unattended, having studied it in the context of the epidemic, which led to an unprecedented self-isolation of the population. The authors found that with a sufficiently high development of the level of information technology in Russia, due to the efforts of the business community, the attitude of the population to the above-considered national program remains rather negative. At the same time, it should be noted that in 2018 there was a very important document "GOST R 57580.1-2017. Security of financial (banking) transactions. Protection of information of financial institutions. Basic composition of organizational and technical measures” was approved and adopted. Knowledge and management of this document, in our opinion, is necessary for almost any employee in the financial sector.

However, it must be stated that professional standards, which are a kind of expression of employers' demand for labor, were developed and adopted a little earlier, so the question of the competence of financial employees in the field of information and digital security was not adequately reflected and clarified there. So, for example, in the professional standards of a specialist in payment systems (registered with the Ministry of Justice of Russia on April 23, 2015 N 37025); specialist in payment services (registered with the Ministry of Justice of Russia on November 24, 2016 N 44419); specialist in remote banking (registered with the Ministry of Justice of Russia on May 11, 2017 N 46685), etc. no significant aspects of ensuring information security in the labor and official functions of these employees are not reflected [8]. Meanwhile, the business community is extremely concerned about these issues. So, in particular, the Council of the Chamber of Commerce and Industry of the Russian Federation (RF CCI) on financial, industrial and investment policy [9] this year (06/02/2020) held a webinar for representatives of the business community and chambers of commerce on the topic "Information security for financial organizations", such webinars are often held by leading universities of the country (the Russian Presidential Academy of National Economy and Public Administration (RANEPA) under the President of the Russian Federation, Financial University under the Government of the Russian Federation, Plekhanov Russian University of Economics etc.). The issue of ensuring information security is very acute not only within the country, but also at the international level. So on September 25, 2020, the President of the Russian Federation V.V. Putin made a statement on the

development of a comprehensive program of measures to restore Russian-American cooperation in the field of international information security [3].

3. RESEARCH RESULTS

In our opinion, the key problem of ensuring the information security of the financial sector, which inhibits a full, fast and painless transition to the digital economy [10], is the discrepancy between the demand of financial organizations for personnel and the existing labor market offers [11].

It is important to note that in the Atlas of new professions 3.0, developed by Skolkovo and the Agency for Strategic Initiatives, the profession "Cybersecurity analyst in the financial sector" [12] is highlighted, which will specialize in the analysis and search for optimal solutions to minimize risks associated with automation of management of personal finances, machine-to-machine transactions and cloud solutions, and will also have the skills to identify vulnerabilities in smart contracts [13]. From our point of view, this innovation is fully justified. The need for such a specialist is long overdue [14]. Moreover, we believe that the arrival of this specialist should be treated very carefully, paying special attention not only to the knowledge of the rapidly developing financial sector, to the knowledge of the latest information technologies, but also to the professionally significant personal qualities of such employees [15]. It is extremely important that this specialist has a wide scale of strategic thinking, high moral ideals of social justice, an active position in terms of social construction.

Probably, along with the profession of a cybersecurity analyst in the financial sector, developers, manufacturers and administrators of information security systems, as well as promoters of digital financial literacy for the population will be needed. Most likely, it will be necessary to make appropriate changes to the current legislation, to the operating procedure of government organizations, industrial enterprises, financial and non-profit organizations. Therefore, lawyers and government civil officials specializing in these issues will be in demand.

Obviously, appropriate educational programs for higher and secondary vocational education should be developed. The existing federal state educational standards are focused exclusively on the training of technical specialists, which indicates a systemic gap between the needs of the labor market and the capabilities of the education system.

Apparently, the problem of information security of the financial sector needs to be solved in a comprehensive and constructive manner [17, 18, 19].

Political management of the financial sector information security personnel system seems to us to be a very important, if not a priority, area in the activities of the ruling elite. Under the circumstances of the promised declared transparency of management, society needs a timely and complete understanding of the ongoing processes. This is especially true in the context of the digitalization of public relations: the development of social networks, electronic voting, the transition to the calculation and accrual of pensions, compensations and other payments to a bank card. Globalization and the development of the international labor market leads to an increase in the migration of the working-age active population, which is interested in modernizing the electronic document management system and payment systems. In the context of information and economic confrontation, which entails the so-called hybrid war, it is very important to formulate and legislate international agreements with strategic partners to strengthen cooperation in the field of information security of the financial sector. The economic context of modernization of the personnel system for information security of the financial sector means changes in the theoretical and methodological basis for improving the modern financial system, which leads to a gradual depreciation of money, the formation of a behavioral economy based on knowledge, achievements, abilities, intelligence and worldview. The desire for possession is replaced by the need to use. The world is changing, the role and speed of information movement is increasing significantly, the intensification of the introduction of high technologies into everyday life and production is fundamentally transforming the environment of society and, accordingly, the economic consciousness of business entities. The Internet, or rather virtual reality, for a modern person largely replaces the state, the market, and the family.

Now the completeness or degree of satisfaction of needs depends not on physical prey in the course of hunting, fishing or gathering, not on agricultural crops, not on salary or wages earned in the process of dangerous service or exhausting hard work, but on the degree of capitalization of one's own intellectual potential, which is developing in the face of fierce competition. The social aspect of the development of a personnel system for the information security of the financial sector is, first of all, associated with the lack of readiness of the population to change the political and economic paradigm, to continuous self-improvement, to organize self-employment in the field of mental labor, to voluntarily reduce consumption volumes. Modern society is in dire need of reinstitutionalization, it is now on the verge of forming new stable groups (communities), defined on completely different grounds than estates, classes and traditional social institutions. The legal component of a radical change in the staff for the information security of the financial sector consists in updating the current legislation, in the emergence of more effective instruments for state regulation of electronic interaction of business entities, in raising the legal consciousness of citizens. The digitalization of the financial sector will inevitably lead to an increase in the skills of thieves and fraudsters, who will require a thorough knowledge and skills in the field of information technology.

This circumstance suggests that under the new economic conditions, the "profession" of a criminal can seduce a wide group of people who have never before gravitated towards criminal activity. The brawny, arrogant, unprincipled and aggressive punks will be replaced by

smart, intelligent, competent specialists, often driven not so much by the thirst for easy and unpunished profit, as by the motives of noble robbers who independently seek social justice such as Robin Hood or the orderlies of society. An environmental factor that determines the direction and order of social and professional transformation of the staff for the information security of the financial sector can in many ways be the emergence of a new environment - a virtual space, which is distinguished by its characteristics and approaches to the formation of social relations, to solving global problems of our time, to changing social roles, character traits and structure of the worldview of a modern person.
Technologically, the development of human resources for the information security of the financial sector will be associated with the emergence of a new organization of society, the structure of which will be determined by the architect of the information environment, content creators, developers and administrators of mass media, managers of high-tech equipment and science-intensive technologies.

4. THE DISCUSSION OF THE RESULTS

The results of the study are a model of human resources for the information security of the financial sector, created on the basis of an analysis of a wide range of regulatory documents, scientific papers, expert assessments and generalization of extensive practical experience. They were repeatedly presented to the academic community, as well as to representatives of financial organizations, recruitment agencies and information security specialists during regularly held scientific and practical conferences, trainings, seminars and courses of additional professional education (including MBA). The expert community has more than once approved the issues discussed in this article and supported the proposed approach.

5. CONCLUSION

At present, it should be stated that the digital economy is firmly rooted in the life of every person, which significantly changes the conditions of his life, his living environment. The development of digital technologies dramatically accelerates decision-making processes, the movement of information, the pace of social interaction. The financial sector is among the first to experience the influence of information technologies, which provide it with high competitiveness, on the one hand, and leading to a qualitative change in consumer behavior, on the other. Electronic payments, digital document flow, virtual communication change a person, shifting his strategic guidelines and target behavioral attitudes. To a large extent, this circumstance brings the problem of information security to the first rank in importance. However, the creation of such a system - an information security system - requires an appropriate staff with not only the appropriate level of qualifications, but also special professionally significant personal qualities, which indicates the urgent need to reform the training system.

REFERENCES

[1] T. Dufva, M. Dufva, Grasping the future of the digital society, Futures, 107 (2019) 17-28. DOI: https://doi.org/10.1016/j.futures.2018.11.001

[2] J. van Dijck, Governing digital societies: Private platforms, public values, Computer Law & Security Review, 36 (2020) 105377. DOI: https://doi.org/10.1016/j.clsr.2019.105377

[3] http://kremlin.ru/

[4] VAK - minobrnauki. https://vak.minobrnauki.gov.ru/

[5] Y. Chen Improving market performance in the digital economy, China Economic Review, 62 (2020) 101482. DOI: 10.1016/j.chieco.2020.101482

[6] Ministry of Digital Development, Communications and Mass Media of the Russian Federation. https://digital.gov.ru/

[7] VTsIOM News. https://wciom.ru/

[8] Professional standards. Ministry of Labor of Russia. https://profstandart.rosmintrud.ru/

[9] Chamber of Commerce and Industry of the Russian Federation. https://tpprf.ru/

[10] E. Kristoffersen, F. Blomsma, P. Mikalef, J. Li The smart circular economy: A digital-enabled circular strategies framework for manufacturing companies, Journal of Business Research, 120 (2020) 241-261. DOI: https://doi.org/10.1016/j.jbusres.2020.07.044

[11] M. Alshaikh Developing cybersecurity culture to influence employee behavior: A practice perspective, Computers & Security, 98 (2020) 102003. DOI: https://doi.org/10.1016/j.cose.2020.102003

[12] Moscow School of Management SKOLKOVO. https://www.skolkovo.ru/

[13] K. Macnish, J. van der Ham Ethics in cybersecurity research and practice, Technology in Society, 63 (2020) 101382. DOI: https://doi.org/10.1016/j.techsoc.2020.101382

[14] S. AlGhamdi, W. Khin Than, E. Vlahu-Gjorgievska Information security governance challenges and critical success factors: Systematic

review, Computers & Security, 99 (2020) 102030. DOI: https://doi.org/10.1016/j.cose.2020.102030

[15] Financial information systems and cyber security: A public policy perspective, Journal of Accounting and Public Policy, 25 (2) (2006) 119-120. DOI: https://doi.org/10.1016/j.jaccpubpol.2006.01.004

[16] A. R. Otero, An information security control assessment methodology for organizations' financial information, Int. J. of Accounting Information Systems, 18 (2015), pp. 26-45. DOI: https://doi.org/10.1016/j.accinf.2015.06.001

[17] H.-Y. Chong, A. Diamantopoulos, Integrating advanced technologies to uphold security of payment: Data flow diagram, Automation in Construction, 114 (2020) 103158. DOI: 10.1016/j.autcon.2020.103158

[18] M. Ficco, F. Palmieri Leaf, An open-source cybersecurity training platform for realistic edge-IoT scenarios, J. of Systems Architecture, 97 (2019) 107-129. DOI: https://doi.org/10.1016/j.sysarc.2019.04.004

[19] Ya.S. Artamonova, Methodology for identifying threats in the field of information security, Social and humanitarian knowledge, 1 (2012) 111-126.