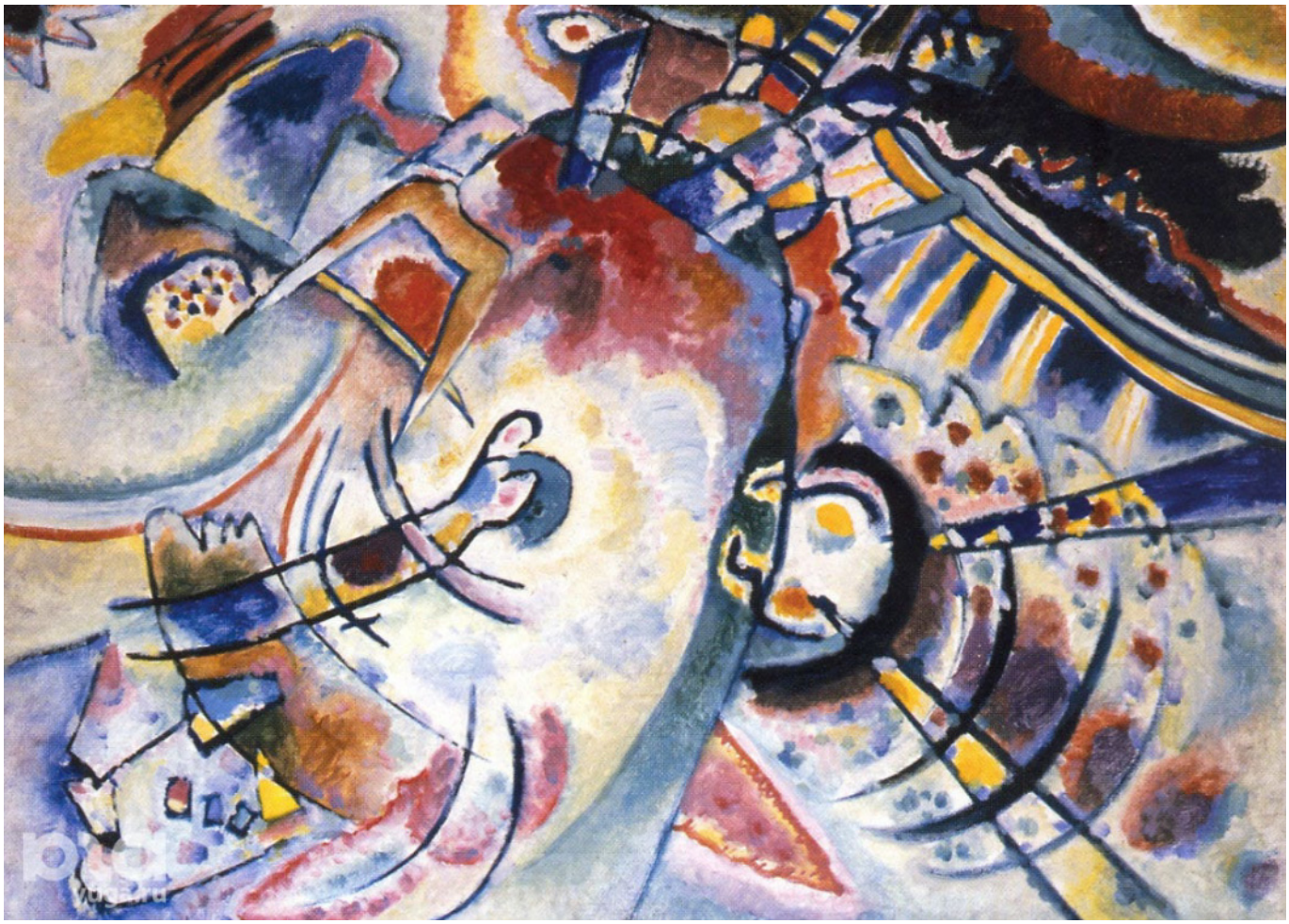
ISSN 2712-7834



W.W. Kandinsky (1866–1944)

SOCIAL NOVELTIES AND SOCIAL SCIENCES

№ 1 (6) / 2022

RUSSIAN ACADEMY OF SCIENCES

MINISTRY OF SCIENCE AND HIGHTER EDUCATION OF THE RUSSIAN FEDERATION

Federal State Budgetary Institution of Science
Institute of Scientific Information for Social Sciences
of the Russian Academy of Sciences
(INION RAN)

SOCIAL NOVELTIES AND SOCIAL SCIENCES

Scholarly journal

№ 1 (6) / 2022

Published since 2020
Issued 4 times a year

English translation by
PhD (Philol. Sci.) Nikulichev M.Y.

Moscow 2022

Founder:
Federal State Budgetary Institution of Science Institute
of Scientific Information for Social Sciences of the
Russian Academy of Sciences

Editorials

ISSN 2712-7834

DOI: 10.31249/snsneng/2022.01.00

Contents

Introducing the issue

The "Social Innovations and Social Sciences" Journal devoted this issue to the transformation of society that is caused by the explosive spread of digital technologies. For the past three years the Russian-language version of the Journal has repeatedly addressed the discussion around various humanitarian aspects of digitalization: the opportunities and risks for an individual, society and the state; influence on the formation of human capital; potential and techniques that help digitize and modernize the economy, improve the social sphere and public administration.

For our out-of-Russia readers this time we decided to select the most interesting works published in 2020–2022 and combine them in one issue. The editorial board believes that the collected materials reflect diverse views of Russian specialists on the global changes in the modern world and in Russia, in particular, under the influence of digitalization.

The issue opens with the section "**Space of Discourse**", which presents two different points of view on the global cyberspace. Thus, *D. Efremenko* analyzes the growing relationship between the geopolitical competition of the great powers and the development of digital technologies. The author shows how cyberspace is gradually turning into "cyberbalkans", where a real proxy war is unfolding. At the same time, he believes that technological leaders, the United States and China, acquire dominant positions in cyberspace and will eventually form a new bipolar world. This means that throughout the 2020s, all the states of the world will have to make their own geopolitical choice as to which of the two ecosystems to join.

In turn, *V. Korovkin* draws attention to the architectural cross-border nature of cyberspace. He also notes the conceptual differences in approaches to the legal status of cyberspace proposed by the United States, on the one hand, and Russia and China, on the other. However, the author sees the future not in the formation of two poles of power, but in the regionalization of cyberspace with the creation of alliances based on the mutual trust of the participants and similar views on the principles of cyber regulation.

The "**Point of View**" section includes articles on trends and opportunities brought by the digital transformation of economy. And it is no coincidence that they largely relate to financial and banking activities, as well as cybersecurity issues. The financial sector is the leader in introducing new digital technologies in Russia, and the security of digital technologies and applications has become one of the most pressing problems for the whole world.

For instance, the article by *I. Lebedeva* analyzes the changes in the banking sector caused by digitalization: the transformation of the market structure, business processes, products and services provided. The author examines the reasons behind digital transformation of financial institutions; describes new

technologies and trends in the banking sector; shows the extent of their penetration into the financial business in Russia. The paper also discusses the opportunities and threats of using modern financial technologies for both credit institutions and their clients.

G. Semeko provides forecast for the development of the financial sector in the context of its accelerated digitalization. The author analyzes the prerequisites for the digitalization of money, as well as the main provisions of the digital currency formulated by the Central Bank of the Russian Federation, discusses functions of the digital currency as an efficient tool for payment transactions, ensuring liquidity and financial stability.

A. Petrov reflects on the prospects and risks of automatic collecting and analyzing personal data from various sources (including the Internet and social networks). From this standpoint he analyses digital profiling of individuals and legal entities in Russia. As the author emphasizes, the ways of using the collected data largely depend on those who make decisions and those who operate the system. However, an individual remains the main carrier of personalized information.

The development and implementation of digital technologies lead to the emergence of systemic technological, organizational and economic innovations, and, perhaps even to a greater extent, of innovations in the social sphere. The issues related to social life are discussed in the section "**Man in the Digital World**".

The section opens with an article by *M. Polozhikhina*. The author shows the contradictory impact of digitalization on the institutions that determine the reproduction and use of human capital. Particular attention is paid to the transformation of family and interpersonal relations, the sphere of culture and the labor market. The author examines the interdependence between the development of digital technologies and social transformations, including the improvement of the quality of human capital and the emergence of new interpersonal models of relationships.

V. Medennikov writes about the educational system as one of the main institutions for the formation of human capital. The creation of a unified information space for scientific and educational institutions based on the use of digital technologies allows, according to the author, to significantly improve the learning process. The author also proposes a methodology for assessing the human capital created at colleges with the help of available scientific and educational resources, as well as a model for assessing the impact of human capital on the social and economic situation of the regions.

The article by *V. Petushkova* describes the experience in digitizing the archive of an outstanding Soviet political statesman, A.N. Kosygin, – and the subsequent use of the digital archive for organizing exhibitions. The author demonstrates the possibilities of digital technologies in terms of preserving and popularizing the historical heritage.

Dear reader! We hope that the materials of the Russian authors brought to your attention will contribute to a constructive discussion about social and economic development in the context of digitaliza-

tion. Modern reality is a complex tangle of old and new problems. The global nature of the unfolding events suggests, moreover, requires a broad discussion and cooperation of social scientists from different countries and with different points of view – in the name of achieving peace and social progress.

THE SPACE OF DISCOURSE

THE WESTPHALIAN WORLD ORDER IN THE DIGITAL SPACE: ON THE EMERGING PHENOMENON OF CYBERGEOPOLITICS

Dmitry Efremenko

DrS. (Pol. Sci), Deputy director of the Institute of Scientific Information for Social Sciences, Russian Academy of Sciences, leading research fellow, Moscow, Russia. E-mail: efdv2015@mail.ru

Abstract. *The article examines the strengthening link between the geopolitical competition of the great powers and the development of digital technologies. During the 2010s, the contradictions between the leading countries in the Internet space noticeably intensified, which turned the Internet into a kind of "gray zone". At present, geopolitical rivalry covers a wide range of trends in creating and using digital technologies. In this context, the term "cybergeopolitics" is well justified. Over the course of the 2020s, China and the United States are likely to create two competing and increasingly incompatible global digital ecosystems. The choice between these digital ecosystems will simultaneously become a geopolitical choice for all actors in the field of international relations in the current decade.*

Key words: *digital technologies; digital society; digital sovereignty; geopolitics; USA; China; Russia.*

For citation*:* Efremenko D. The Westphalian world order in the digital space: on the emerging phenomenon of cybergeopolitics / English transl. by Nikulichev M.Y. // Social Novelties and Social Sciences. – 2022. – N 1. – P. 7–17.

URL: https://sns-journal.ru/en/archive/ DOI: 10.31249/snsneng/2022.01.01

Introduction

Geopolitics as a struggle of powerful nations for influence in any large part of the world or on a planetary scale has traditionally been defined as a strategy designed to utilize new possibilities associated with the control of space. In this power struggle, technologies most often played an instrumental role, allowing for further expansion and effective administration of the controlled space. The development of information and communication technologies, today called digital technologies, changes these processes qualitatively. A new type of space – cyberspace – can act both as an infinite expansion and as a kind of antipode of geographic space. Control in cyberspace or in the digital sphere is becoming synonymous to establishing control over physical territories and to political and economic expansion the world over. In this context, there are sufficient grounds to start talking about cybergeopolitics.

Global Cyber-Balkans

The Internet and the most important informational technologies, almost from the very beginning of their explosive growth, became the tools for strengthening the political, economic and cultural influence of the United States and the collective West. Being centers for the development and commercialization of relevant technologies, these nations had an impressive head start over other state actors, who were forced to accept the imposed "rules of the game". In a slightly different modality than the Washington Consensus institutions, the Internet governance structure – the non-profit organization ICANN (Internet Corporation for Assigned Names and Numbers) – also quite effectively protected the interests and political and ideological standards of the American establishment. The situation did not noticeably change even after ICANN's contract with the US Department of Commerce and the National Information and Communications Administration (NTIA) expired on October 1, 2016, i.e. when its formal accountability to the American government ceased, and ICANN was transformed into an international structure with an oversight by the Governmental Advisory Committee. Institutionally, ICANN adopted multilateralism and multistakeholder model which was necessary but "too little and too late" by the time. The USA and Western countries have effectively blocked repeated efforts by Russia, China and some other countries to develop non-discriminatory cybersecurity rules for non-Western countries within the global web. From the non-Western powers' viewpoint, cybersecurity precludes the use of network technologies for political purposes, influencing public opinion and destabilizing regimes. But the USA and Western allies viewed proposals from China, Russia and their partners to develop a binding code of conduct that would guarantee international information security as attempts to undermine their "natural" privileges on the World

Wide Web, the most important pillar in the post-bipolar world order. After years of failed international negotiations non-Western nations started putting forward national regulatory initiatives, of which China's Great Firewall project has had the greatest scope and prominence. Despite criticism from the West and international human rights organizations, such projects or individual measures of national governments were defensive in geopolitical terms. At the same time, they formed a new geopolitical network reality adequately described by the term "cyber-balkanization" coined at the end of the last century [Van Alstyne, Brinjolfsson, 1997].

The tendency towards "cyber-balkanization" during the 2010s was significantly reinforced due to new circumstances. Back in 2014, Russia's reaction to events in Ukraine prompted a number of US and EU politicians to raise the question of disconnecting Russia from the SWIFT (electronic system of international financial transactions and payments) and even restricting access to the Internet, which would be similar to the use of weapons of mass destruction in the digital and financial spheres. Disconnection from SWIFT and mutual blocking of some Internet resources and services started in 2022, becoming part of the growing proxy war between Russia and the West. However, even at the stage of discussing these extreme actions, the global Web experienced a kind of resurgence of the Westphalian world order. From then on, the principle "*cuius regio eius religio*" could be reformulated as "whose server, their network" [Yefremenko, 2014]. Moreover, as Russian officials stated, the attempts to create a root domain name server (DNS)[1] on the national territory or on the territory of the BRICS countries would lead to fragmentation of the Internet at the level of hardware infrastructure. Less radical measures, mainly from the sphere of legislative and tax regulation, were aimed at forcing such large transnational corporations as Google, Twitter, Facebook (Meta)[2] and others to locate their centers in Russia, due to which the bulk of Internet traffic would remain in the zone of sovereign control of the Russian government. Characteristically, Stratfor (Strategic Forecasting Inc.), a think tank with close ties to the American intelligence community, viewed Russia's desire for an autonomous sovereign Internet as a kind of casus belli, since in this case Russia would have a hypothetical opportunity to deliver devastating blows to the global Internet without catastrophic consequences for itself, or the ability to hide traces of cyber-attacks originating from its digital space [Russia Plants ..., 2019]. The law on the national Internet traffic routing system (the "sovereign Internet" law) adopted on May 1, 2019 has led to intensive work to tighten government control over communication in the digital space. Although the expected level of state control in case the Law is fully implemented will not reach the level of China's Great Firewall project, it is nevertheless a clear step towards establishing a Westphalian order in the Internet governance.

[1] Of the 13 currently operating DNS root servers, 10 are located in the United States, one each in the Netherlands, Sweden and Japan.

[2] Since March 21, 2022, it has been recognized as an extremist organization in Russia.

At the same time, the willingness of the United States to violate the digital sovereignty of nation states, for example, by deploying a satellite constellation that provides unlimited access to the Internet for any user, in the same confrontationary logic, can be considered by Washington's geopolitical rivals as a manifestation of aggression. The US National Cyber Strategy, adopted in 2018 by the Trump administration, declares its intention to provide an "open, interoperable, reliable and secure Internet" on a global scale, and also announces a significant expansion of offensive operations in cyberspace against US rivals [National Cyber Strategy…, 2018].

It is also significant that China, Russia, Iran, and many other non-Western countries and their Internet communities have become powerful players on the World Wide Web. In the absence of universal information security rules, this means that the Internet turned into a "gray zone" where various actors can use a wide range of available tools to achieve their goals, political or otherwise, without fear of being drawn into a large-scale conflict. In essence, "gray areas" are areas of confrontational interaction that lie in the spectrum between routine diplomacy and classical military operations [By Other Means …, 2019]. These include hybrid operations in cyberspace, propaganda campaigns, the spread of "fake" news, political and economic coercion, "wars by proxy", and other types of paramilitary provocations. Since these areas are either not covered or not sufficiently covered by international legislation, political actors, operating in the "gray zones" directly or – in most cases – through a chain of intermediaries, can achieve the desired outcomes with a relatively low level of risk. The result achieved under a favorable scenario can significantly exceed the scale of the resources utilized. At the same time, the long-term risks and side effects leading to an increased confrontation between the great powers may substantially outweigh the initial political effect. These consequences of the geopolitical confrontation in the Web were fully revealed after the start of the Russian Special Military Operation in Ukraine on February 24, 2022.

Setting up an alternative technological platform as a geopolitical challenge

The geopolitical benefits through the use of network communication tools imply action in conditions of increased uncertainty, turbulence and various synergistic effects. Uncertainty involves not only future outcomes, but also the evaluation of actions already taken.

Systemic geopolitical advantages in the context of the fast developing, primarily digital, technologies can be achieved only through strategic planning and concentrating resources for the expected technological breakthrough. The most significant example is the strategic decision of the Chinese leadership to create its own technological platform, independent of the Western standards, infrastructure and supply chains. By the "technological platform" we mean the ecosystem for the development of various technologies, which takes place on the basis of rules, standards and political decisions made by one of the largest state actors.

Adopted in 2015, the ten-year plan "Made in China 2025" (MIC 2025) is aimed at comprehensively modernizing Chinese economy to secure China's position as a global powerhouse in high-tech industries. This market-oriented plan simultaneously involves the massive support of the Chinese state for national technologically innovative corporations. The government makes significant efforts to reduce China's reliance on foreign technology imports and invest heavily in its own innovations – from direct subsidies and preferential regimes to industrial espionage and coercion of foreign companies wishing to do business in China to transfer technology.

Lately, the MIC 2025 plan has been heavily modified to account for the US efforts to block it. The "Internet Plus" strategy, inspired by the Germany's "Industry 4.0" concept, was approved simultaneously with MIC 2025 plan and is being successfully implemented. The "Internet Plus" strategy is a five-year plan to integrate cloud computing, Big Data and IoT (the Internet of Things) with a variety of industries from manufacturing to commerce, healthcare services, agriculture and many others.

According to I. Bremmer, China's plans to achieve real independence in the development of digital technologies and ensure the sustainable functioning of its own standards, infrastructure and supply chains – "this is the single most consequential geopolitical decision taken in the last three decades. It's also the greatest threat to globalization" [Bremmer, 2019]. The creation of an independent Chinese technological platform will lead to a fundamental split that has actually already begun in the IT sphere.

China has already made significant progress in achieving digital sovereignty: its own instant messengers, search engines, root servers for routing, digital certification center have been created and are actively functioning; however, China remains highly dependent on American operating systems. In this regard, Russia lags noticeably behind China, despite the officially formulated task of creating an infrastructure that is duplicated and not controlled by external actors.

It is expected that during the 2020s, China and the USA will create two competing and increasingly less compatible global ecosystems for IoT, Big Data processing technologies, 5G network, additive technologies, robotics, etc. The choice between these digital ecosystems will simultaneously become a geopolitical choice for all actors in the field of international relations in the current decade. Moreover, geopolitics, as well as domestic political reasons, will in many cases outweigh considerations of economic and technological expediency. This is more than likely in the case of Russia. In 2020, President Vladimir Putin again emphasized the urgent need to create domestic technologies and standards "in the areas that determine the future" [Poslanie Prezidenta RF …, 2020]. It is obvious, however, that Russia, unlike the USSR, has limited opportunities to develop its own technological platform. The economic and structural transformations of the 1990s hit this potential hard, and the 2013 reform of the Russian Academy of Sciences drastically reduced incentives for closing the scientific gap. Western sanctions and the lack of prospects for lifting them in the foreseeable future mean that Moscow already today has no real alternative to integrating into China-centric value chains [Diesen, 2018]. Apparently, where the possibility of Russia's

technological independence is hopelessly undermined, the transition to the Chinese technological platform will be uncontested. Following Moscow, other EEU (Eurasian Economic Union) countries will make a similar transition. Iran, Pakistan, North Korea, a number of countries in the Arab East and Sub-Saharan Africa, in Latin America, Cuba, Venezuela and Nicaragua have extremely limited options, provided that the ruling regimes there remain in power for a long time. A considerable number of countries will become objects of competition between the US and China, and today a significant part of these countries are active participants in the Belt and Road Initiative (BRI).

It is logical to assume that in the future the "One Belt, One Road" initiative itself will acquire a pronounced technological dimension. Strictly speaking, the basis for this has already been created in the form of one of the BRI subprograms – "Digital Silk Road", which provides for multi-billion dollar investments in the development of telecommunications networks, satellite navigation, optical cables, electronic commerce, mobile payment systems, "big data" projects, artificial intelligence and quantum computing. Some Western experts believe that this subprogram promotes digital technologies to achieve a greater connectivity between the BRI member countries, extends China's geopolitical influence, the transcontinental spread of state capitalism and the illiberal political order [Cheney, 2019]. In particular, this applies to the adoption of Chinese video surveillance technologies and digital identification systems in some Asian, African and Latin American countries, which become integrated into the Sino-centric technological infrastructure and at the same time adopt China's socio-political practices. In addition, in the multilateral BRI format, Beijing is more effectively pursuing the principles of digital sovereignty, the concept that is actively supported by Russia.

In an attempt to compete with Beijing, Washington is putting forward initiatives to counterbalance the BRI, for example, in the Indo-Pacific region. Digital connectivity was announced as an important goal for the US Indo-Pacific strategy, but the scale and scope of the promised US investment is still an order of magnitude below the Chinese [Wroughton, Brunnstrom, 2018]. The United States is trying to compensate the insufficient investment activity by putting pressure on allies, persuading them to refuse, for security reasons, to cooperate with Huawei and other Chinese companies in the development of 5G communication networks. In particular, the United States fears that the widespread use of the Internet of Things and the implementation of "smart city" projects on 5G networks will allow Chinese servers to accumulate huge amounts of information about users of these technologies around the world day by day. The same applies to customers of Chinese digital e-commerce platforms and users of Alipay, Baidu Wallet and WeChat Pay mobile applications [Hemmings, Cha, 2020]. However, since the revelations of Edward Snowden [Snowden, 2019], it has been known that the National Security Agency (NSA) and other US intelligence agencies collect similar content, even without 5G capabilities.

Temptations and dangers of digital dominance

Sustained leadership in the development of artificial intelligence (AI), 5G and a number of other digital technologies is not just accompanied by the economic and socio-political benefits – it can be seen in many aspects as a "winner takes all" model. A breakthrough in these areas will lead to rapid and radical restructuring of value chains, dramatic changes in labor and capital markets, enhanced management efficiency. And while the political leadership of a country, a likely leader in the development of the relevant technology, attempts to minimize the negative consequences of technological innovations for its own population and economy, the same degree of delicacy could hardly be expected in relation to the socio-economic landscape of other countries. On the contrary, in case of the negative scenario, the temptation to inflict unacceptable damage on opponents without resorting to military force will be intense. Naturally, on the surface consumers around the world will be offered unprecedented benefits but taking advantage of the offer would only be possible through merging into a new global dominance system. In the military sphere, rapid progress in the development of Autonomous Weapons Systems could upset global and/or regional power balance. In this context, the words of Russian President Vladimir Putin that the monopolist in the field of artificial intelligence "will become the ruler of the world" [Putin: monopolist ..., 2019] sound like a realistic assessment of the consequences of that technological race for leadership.

Moreover, the competition for leadership in developing the key digital technologies will not be limited to intergovernmental relations. There will be fierce competition between the largest corporate players (so far, a confrontation between the American and Chinese "big five", respectively: Meta, Alphabet, Apple, Microsoft, Amazon, vs Alibaba, Baidu, Huawei, Tencent, ZTE), and between the industrial production models based on old and new technologies [Scott, Heumann, Lorenz, 2018].

The tendency towards monopolizing artificial intelligence and critical digital technologies is very dangerous. There are sufficient reasons for those who aspire to cyber superiority, as well as for other actors, not to overheat the situation, but to ensure an acceptable level of risk management. To de-escalate the tension, it is necessary to develop internationally acceptable basic norms, rules and restrictions on the development and use of artificial intelligence and digital technologies. The international actors must commit to a wide exchange of information, to joint analysis and forecasting of possible consequences, to corrective actions in case of such negative consequences as destabilization of markets or an uncontrolled increase in unemployment. The technological leaders can offer other nations and their corporations to join the new digitally reformatted value chains, i.e. share with them the "sweet fruits" of the digital revolution and the economic growth it generates. Moreover, the developing countries that follow one or another digital leader can by-pass entire stages of industrial development and "fit" into the new landscape of the digital economy. At the very least, this kind of opportunity may appeal to countries that choose to participate in multilateral initiatives like the "Digital Silk Road". All this may justify the intentions of actors aspiring

to a dominant position in the digital age. Therefore, the current situation can be described as a race to achieve a decisive advantage in the development of digital technologies and an attempt to gain the trust of their own citizens and the world community.

The Impact of the Corona Crisis

The early twenties of the XXI century will be remembered by the successive "arrival" of two "black swans": the COVID-19 coronavirus pandemic and the armed conflict between Russia, the republics of Donbass, Ukraine, and indirectly – the Western countries that support the latter.

The idea that the COVID-19 pandemic will lead to major social and political changes around the world, or at least dramatically accelerate the transformations outlined above, has become a new conventional wisdom in the spring of 2020. At least this is true with regard to the radicalization of processes that prompted reformatting of the digital society. First of all, the long-term quarantine for hundreds of millions of people in Eurasia and America has become an ideal stress test for digitalization programs and projects already implemented at various levels [Markov, 2020]. Not only advantages related to the scale and speed of the digital transition were revealed, but also disadvantages caused by poor planning and execution of relevant programs.

Digital surveillance and face recognition technologies have played a major role in curbing the virus infection, and China was the first to achieve a turning point in fighting COVID-19 with the help of these digital applications, including massive testing of cloud, super- and cognitive computing, smart fusion of sensor networks, quadcopters, smartphones and personal gadgets, digital biological and sanitary twins, etc. These digital applications worked effectively in combination with China's social credit system, which is not only a mechanism for unprecedented state control over private life, but also an attractive arrangement with the authorities which allows many loyal Chinese citizens to achieve higher social status and material well-being by following the rules [Liang, Das, Kostyuk, 2018]. The rapid reaction to the worsening epidemic situation in China, and then in a number of European countries and the United States, made it possible to take the necessary precautions in time in other countries and regions. Finally, the broad exchange of information and experience in combating coronavirus in real time between doctors from different countries was of great importance.

On the other hand, the 2020 pandemic, as the epidemics in the past, was characterized by widely circulating panic, superstition and rumors. But in the 21st century this process has become almost instantaneous, being mediated by electronic network services. For example, from December 2019 to March 2020, the number of hits on 76 US websites that spread misinformation about COVID-19 was 142 times higher than the number of hits on the World Health Organization and the American Center for Disease Control and Prevention, which are the most authoritative sources of information on developing pandemics [Perlow, 2020]. It is no coincidence that in the midst of the COVID-19 pandemic, the neologism "in-

fodemic" gained popularity [Makdonnell, 2020]. Digital technologies turned out to be the subject of conspiracy theorists, for whom the pandemic has become an opportunity of a lifetime. Sometimes individual or collective psychosis manifested itself in the form of digital Luddism. For example, in the UK, more than twenty 5G towers were set on fire after the "information" surfaced on the web about the link between the spread of the virus and the latest digital communications infrastructure [Coughlin, 2020]. The arson of 5G cell towers highlighted a paradoxical combination of panicky superstitions, network activity of various kinds of outcasts and conscious propaganda efforts of quite respectable actors in the Western political and media space. It can be assumed that in this case two factors were misinterpreted: the fear of the virus that has spread from China to all other countries and the fact that 5G networks were installed around the world by the Chinese company Huawei, whose system, according to some experts [Hemmings, Cha, 2020], would give Beijing access to sensitive information about individual and corporate customers around the world.

In general, the pandemic demonstrated how important is the ability of social management systems that started introducing digital technologies to adapt quickly. Nations with the most adaptive and flexible systems of social management will gain an important advantage not only in exerting control over individuals and groups, but, in the terminology of J. Agamben, in the production and regulation of "bare life" [Agamben, 1998]. It is easy to assume that digital technologies and artificial intelligence will become the main tools for the implementation of biopower and its projection on the global politics.

It is essential that the benefits of using digital technologies are not limited to the sphere of observation and control but cover a wider range of relationships between sovereign political power and the life of an individual. Ultimately, it is vital that the major global players break out of the "discipline and punish" vicious circle and propose a more positive agenda for the digital future, while relying on their own scientific and technological potential, as well as, to the extent possible, on the potential of allies and partners.

Conclusion

The pandemic as a social stress and the economic crisis associated with it accelerated the release of the information and digital space from the control of the Western elites. The controlling functions will gradually pass over to other sovereign nations. In this regard, innovations in Russian legislation in recent years and constitutional changes in 2020 only reinforce the trend towards the sovereignty of the digital space. Digital sovereignty, combined with the ability of the state to ensure sovereign control of the banking system, financial and commodity flows, to actively modify value chains, to form partnerships with other state actors to create new mechanisms for global governance, are becoming the most important prerequisite for survival in the international political and economic environment amid the growing level of conflicts.

In the case of Russia, it is not so difficult to prioritize the main strategies for moving towards a digital future:

1. To implement the principle of digital sovereignty while relying on domestic scientific and technological potential;

2. Where this is not possible or economically not feasible, to diversify relations with external suppliers, avoiding critical dependence on any;

3. If diversification is also impossible, switch to the Chinese technological platform (no other options are feasible in the foreseeable future without unacceptable geopolitical concessions).

Russia will obviously continue to be interested in the development by the world community of binding norms and rules (including restrictions and prohibitions) for regulating the Internet, developing artificial intelligence and digital reality technologies. The level of responsibility of the scientific community will sharply increase, which should provide expert support at the proper level for making the necessary political decisions.

References

1. Makdonnell L. Virus dezinformacii. Chemu mozhno verit' v socsetjah? // Mezhdunarodnyj diskussionnyj klub "Valdaj". – 2020. – 08.04. – URL: https://ru.valdaiclub.com/a/highlights/virus-dezinformatsii/?utm_source=newsletter&utm_campaign=165&utm_medium=email (date of access 10.04.2022).
2. Markov A. Informacionnaja bezopasnost' v uslovijah pandemii COVID-19 // Rossijskij sovet po mezhdunarodnym delam. – 2020. – 09.04. – URL: https://russiancouncil.ru/analytics-and-comments/analytics/informatsionnaya-bezopasnost-v-uslovi yakh-pandemii-covid-19/ (date of access 24.04.2022).
3. Poslanie Prezidenta RF Federal'nomu Sobraniju 2020 // Oficial'nyj sajt Prezidenta RF. – 2020. – 15.01. – URL: http://kremlin.ru/events/president/news/62582 (date of access 28.01.2022).
4. Putin: monopolist v sfere iskusstvennogo intellekta mozhet stat' vlastelinom mira // TASS. – 2019. – 30.05. – URL: https://tass.ru/ekonomika/6489864 (date of access 23.02.2022).
5. Agamben G. Homo Sacer: Sovereign Power and Bare Life. Redwood City, CA: Stanford University Press, 1998. – 228 p.
6. Bremmer I. The End of the American Order: Ian Bremmer speech at 2019 GZERO Summit // Eurasia Group, 2019. – 18.11. – URL: https://www.eurasiagroup.net/live-post/end-of-american-order-ian-bremmer-2019-gzero-summit-speech (date of access 23.04.2022).
7. By Other Means. Part I: Campaigning in the Gray Zone. A Report on the CSIS International Security Program / Hicks K.H., Friend A.H., Federici J., Shah H., Donahoe M., Conklin M., Akca A., Matlaga M., Sheppard L. – New York: Rowman & Littlefield, 2019. – 56 p. – URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_Gray Zone_interior_v4_FULL_WEB_0.pdf (date of access 22.04.2022).
8. Cheney C. China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism // Council on Foreign Relations. – 2019. – 26.09. – URL: https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political (date of access 22.04.2022).
9. Coughlin C. Our Enemies Will Seek to Exploit Britain's Vulnerability During This Moment of Crisis // The Telegraph. – 2020. – 08.04. – URL: https://www.telegraph.co.uk/news/2020/04/08/enemies-will-seek-exploit-britains-vulnerability-moment-crisis/ (date of access 09.04.2022).
10. Diesen G. China' s Geoeconomics and the "New Cold War"// Russia in Global Affairs. – 2018. – 26.12. – URL: https://eng.globalaffairs.ru/articles/chinas-geoeconomics-and-the-new-cold-war/ (date of access 18.04.2022).
11. Hemmings J., Cha P. The Hidden Dangers of China's Digital Silk Road // The National Interest. – 2020. – 11.03. – URL: https://nationalinterest.org/feature/hidden-dangers-chinas-digital-silk-road-131887 (date of access 22.04.2022).
12. Liang F., Das V., Kostyuk N. Constructing a Data-driven Society: China's Social Credit System as a State Surveillance Infrastructure // Policy & Internet. – 2018. – Vol. 10, N 4. – P. 415–453.
13. National Cyber Strategy of the United States of America // The White House. – 2018. – September. – URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (date of access 26.04.2022).
14. Perlow J. Coronavirus Misinformation Spreading Fast: Fake News on COVID-19 Shared Far More Than CDC // WHO Reports. ZDNet. – 2020. – 03.03. – URL: https://www.zdnet.com/article/coronavirus-misinformation-is-increasing-newsguard-finds/ (date of access 04.04.2022).

15. Russia Plants Its Flag in the Digital Realm // Stratfor. – 2019. – 19.03. – URL: https://worldview.stratfor.com/article/russia-plants-its-flag-digital-realm-cybersecurity-internet (date of access 18.04.2022).
16. Scott B., Heumann S., Lorenz Ph. Artificial Intelligence and Foreign Policy // Stiftung Neue Verantwortung. – 2018. – January. – URL: https://www.stiftung-nv.de/sites/default/files/ai_foreign_policy.pdf (date of access 23.04.2022).
17. Snowden E. Permanent Record. New York: Metropolitan Books, 2019. – 352 p.
18. Van Alstyne M., Brinjolfsson E. Electronic Communities: Global Village or Cyberbalkans? MIT Sloan School, 1997. – URL: http://web.mit.edu/marshall/www/papers/CyberBalkans.pdf (date of access 17.04.2022).
19. Wroughton L., Brunnstrom D. Wary of China's Rise, Pompeo Announces U.S. Initiatives in Emerging Asia // Reuters. – 2018. – 30.07. – URL: https://www.reuters.com/article/us-usa-trade/wary-of-chinas-rise-pompeo-announces-us-initiatives-in-emerging-asia-idUSKBN1KK0V5 (date of access 20.04.2022).
20. Yefremenko D. Crossing Red Lines // Russia in Global Affairs. – 2014. – N 3. – URL: https://eng.globalaffairs.ru/articles/crossing-red-lines/ (date of access 23.04.2022).

The manuscript was received on 18.05.2022.

INTERNATIONAL REGULATION IN CYBER SPACE: IS EFFECTIVE MUTUAL UNDERSTANDING POSSIBLE?

Vladimir Korovkin

Head of Digital Transformation Laboratory, Professor of Business Practice at the Moscow School of Management at SKOLKOVO (Moscow, Russia)[1] E-mail: Vladimir_korovkin@skolkovo.ru

Abstract. *The key challenge for effective legal regulation of cyberspace is its cross-border architecture. This article aims to analyze contradictions between the main countries participating in the discussions on the international regulation of cyberspace. As the probability of reaching a broad international consensus in the field of cyberlaw is low in the foreseeable future, the regionalization of cyberspace, the creation of alliances based on mutual trust between participants and coordinated views on the principles of cyber-regulation are predicted.*

Keywords: *digitalization; cyberspace; cyber regulation; international cyber security.*

For citation: Korovkin V. International regulation in cyber space: is effective mutual understanding possible? / English transl. by Nikulichev M.Y. // Social Novelties and Social Sciences. – Moscow : INION RAN, 2022. – N 1. – P. 18–32.

URL: https://sns-journal.ru/en/archive/ DOI: 10.31249/snsneng/2022.01.02

Introduction

The concept of "cyberspace" appeared in science fiction in the early 1980s [Benedikt, 1991 a, p. 1], but within a few years it was introduced into scientific circulation to describe the growing phenomenon of global information exchange using computer-based devices. In 1990, the first international scientific conference on cyberspace was held (at the University of Texas, Austin), a year later an urbanist, architect and philosopher Michael Benedict edited and published a collection of papers from the conference. In his keynote article in this collection, M. Benedict defined this phenomenon in the following way:

"Cyberspace is a globally networked, computer-sustained, computer-accessed, and computer-generated, multi-dimensional, artificial, or 'virtual' reality… Cyberspace is a globally connected multi-dimensional artificial or "virtual" reality supported by computers, accessible through computers and created by computers… Cyberspace has a geography, a physics, a nature, and a *rule of human law*" (emphasis mine. – V. K.) [Benedikt, 1991b, p. 122–123].

It is noteworthy that the question of legislation in cyberspace arose at the dawn of the awareness of a new phenomenon. Thirty years later, this issue remains largely unresolved despite numerous national and international efforts. The key challenge for effective legal regulation of cyberspace is its fundamentally global and cross-border nature. Consider the paradox: on the one hand, information networks that form the basis of cyberspace appear to be a kind of global public good (similar to the World Ocean or the atmosphere). On the other hand, they function and develop due to the efforts of predominantly private actors, who are concentrated in a very small number of jurisdictions [Korovkin, 2019, p. 152]. This paradox makes national regulation of cyberspace relatively ineffective. In addition, the attitudes of several individual sovereigns to cyberlaw define de facto international legal practice.

This situation has caused and continues to cause concern for countries. Russia and China have been the most explicit in their views, and over the past two decades they have been promoting the idea of creating an international regulation of cyberspace in the form of a binding convention. This idea did not find support in the USA and the countries of the European Union. The situation has largely reached a stalemate [Kerttunen, Tikk, 2018], especially after the general geopolitical situation aggravated in the mid-2010s. In 2017, an intergovernmental group of experts under the auspices of the UN failed to issue a consensus report at the end of the meeting, and representatives of Russia and the United States exchanged harsh statements, effectively denying each other the status of bona fide actors. The immediate cause for

the clash was the discussion around a principled approach to cyber warfare[1]. However, disagreements between countries run much deeper.

Typical remarks from mutual official statements show the depth of mutual distrust. According to the Russian special envoy, reaching a consensus is hampered by: "...certain countries that seek to impose their rules of the game in the information space on the whole world… Based on their technological achievements, they are trying to enforce the "rule of the gun" in the information space" [Response of the Special …, 2017]. In turn, the US Special Representative stated: "I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles [to cyber warfare] believe their States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions". [Department of State, 2017].

In many respects working on the international legislation is a more complex process than national lawmaking. International law can only be established by consensus of all parties involved; countries have the option not to accede, with the decision to accede (ratification by authorized national authorities, usually parliaments) almost always being the result of a complex internal political process. The actors within the international space perceive themselves as being in a difficult competitive situation with unequal starting positions and for this reason: 1) they are looking for ways to strengthen their standpoint and 2) they assume that other participants in the process act in a similar way. This leads to a discrepancy in the declared and actually pursued goals. Each actor may also embark on a strategy of formally acceding with no intention of fulfilling the obligations assumed. Such a strategy can give individual national actors an international competitive advantage (the "tragedy of the commons" proposed by the British economist William Forster Lloyd in 1833 [Lloyd, 1980]). The ability of the international community to rule out such strategies is limited; as a result, the overall process is characterized by a high degree of mutual distrust. The balance is maintained due to the awareness that the potential significant international destabilization may have more dangerous consequences for individual actors than following the agreed rules. However, in general, modern international law is not as comprehensive as national legislation. It is always possible to leave one or another area unregulated, which is preferable to joining legislation that violates the national interests.

The successfully adopted and enforceable international treaties[2] resulted in (1) harmonization of national legislation in areas with long established practices (for example, commercial law); (2) establishing

[1] Russia insists that cyberspace should be demilitarized, and cyber warfare excluded with the help of international law; the position of the United States is that in one form or another aggressive actions in cyberspace are an accomplished fact and the task of international law should be to create rules governing military operations in cyberspace in accordance with established military and humanitarian law. The corresponding statements were made by the special envoy of the Russian Foreign Ministry Andrey Krutskikh [Response of the Special …, 2017] and the representative of the US State Department Michel Markoff [Explanation of Position …, 2017].

[2] See the list of key UN-sponsored treaties: [International Law and Justice // United Nations. – B/d. – URL: https://www.un.org/en/global-issues/international-law-and-justice (date of access 18.07.2022)].

norms against actions with potentially catastrophic humanitarian consequences (laws on the conduct of warfare, nuclear test ban treaties, ban on chemical and biological weapons[1]), or (3) having relatively little importance to national interests (conventions on outer space and Antarctica[2]). The international Law of the Sea definitely stands apart. It was created in an unusual situation, when countries with a relatively small overall influence in the international space turned out to be, due to geography, the owners of the most important resource – the sea straits, which gave them a fairly strong negotiating position.

Cyberspace is inherently different from all of those cases. It was established relatively recently and is in the process of constant flux, which excludes recourse to established customs and practices. The humanitarian consequences of abuses in cyberspace – while significant – do not seem comparable to nuclear, chemical or biological conflict. At the same time, cyberspace has become one of the key drivers of social, economic and political development in almost all countries of the world, and its importance is constantly growing. The architecture of the current cyberspace gives a significant advantage to a limited group of countries (if not one country). The "minor" participants in the process do not have and are not expected to have any "balancing" opportunities to strengthen their position. Major actor countries can greatly benefit from non-adherence or formal but non-enforced adherence to regulation[3]. As a result, creating an effective, enforceable, coherent regulation of cyberspace is a task of unprecedented legal, technical and, above all, political complexity.

The world legal community perceives these complexities differently and the general legal discussion mostly focuses on two topics: "Is international law really a law?[4]" and "Is international law really international?" On the first issue, a rather radical point of view was expressed in 1994 by Shirley Scott, who noted that "The dominant post-war paradigm in international relations has been realism, which dismisses international law as being virtually irrelevant to matters of 'high' politics." In her opinion, the latter is generally based on the concept of "power" [Scott, 1994]. The discussion on the second issue is covered, for example, in the book [Roberts, 2017].

Indeed, it must be taken into account that international legislation in any case does not occur "from scratch" but is embedded in one or another historical context. The Internet emerged as a global phenomenon almost at the same time as the end of the Cold War and the collapse of the "socialist camp". The Internet developed in parallel with the complex political processes of the 1990s-2000s. For that reason,

[1] The participants in the relevant conventions continued to suspect other participants of violating agreements, a number of violations of the chemical weapons convention were proven (for example, the Iran-Iraq war of 1980-1988) without serious immediate consequences for the violators.

[2] In the latter case, joining the convention does not prevent countries such as Argentina and Chile from officially considering part of Antarctica as sovereign territory.

[3] For example, China ignored the Budapest Convention on Cybercrime, which criminalized certain violations in the field of intellectual property; to resolve the situation, the United States had to sign a separate bilateral agreement in 2015.

[4] "Is international law really a law?": the conceptual fields of the English term "law" and Russian "rights" and "law" intersect in a rather complicated way.

the Cold War ideologemes continue to largely determine the views of the key global cyberspace stakeholders on the interests, motives and strategies of opponents.

Differences in approaches between the main global cyberspace stakeholder nations have repeatedly become the subject of analysis both in the domestic [Zinov'eva, 2016; Zaharov, 2018] and in foreign literature [Kerttunen, Tikk, 2018]. However, this analysis, as a rule, was limited to situational and technical study of disagreements without clarifying their underlying causes. The purpose of this article is to analyze the positions of the key countries participating in discussions on the issues of international regulation of cyberspace in the context of the current practice of private and public conflict resolution. The results of the study help to gain a deeper understanding of the opposing positions and formulate more realistic expectations regarding the possibilities for reaching a consensus in the field of international cyber regulation.

Method of analysis

First of all, this task presupposes the analysis of the key documents describing the positions of the parties in the more than 20-year-old discussion on international regulation. It is fundamentally important to place these documents into the broader context of views on public administration. Any approach to regulation must implicitly or explicitly take into account the prioritization between private and public interests in the field of international information networks and a possible action plan that creates an acceptable balance between these interests.

The official position of Russia on the issues of international cyber regulation was formulated in the draft Convention on International Information Security submitted to the UN in 2011 [Konvencija ob obespechenii …, 2011], which summed up a series of prior initiatives in the UN format. Although formally the project was submitted by a group of countries, which also includes such an important global cyberspace stakeholder as China, the document was positioned as an initiative of the Russian Federation and was perceived in this capacity by the international expert community [Kerttunen, Tikk, 2018].

The United States is the main opponent of the Russian initiative in the UN [Demidov, 2013[1]; Huzhina, 2015; Zaharov, 2018; Prakesh and Baruah, 2014]. The like-minded powers include Great Britain and the Netherlands [Kerttunen, Tikk, 2018, p. 24]. The opposition strives not to propose a comparable alternative document (since the 2001 Budapest Convention on Cybercrime[2] at the Council of Europe sup-

[1] In particular, it was correctly noted that there are significant discrepancies between the concept of "information security" contained in the document, which is very broad in nature, and many common interpretations of "cybersecurity", which is reduced to the functioning of computer network infrastructure. According to the author, "the competition of Russia and its allies (PRC and other SCO states) with Western states in terms of establishing at the global level one or another understanding of the IT role in the context of international security is acquiring the features of an ideological confrontation" [Demidov, 2013, p. 137].

[2] Despite the fact that the Convention was developed by the Council of Europe, it is open for all countries. Of the major non-European countries, the United States, Canada, Australia, Japan and Israel have ratified the convention so far.

ported by the Western countries and allies is much more restrictive[1]), but to reject the very idea of an effective global cyber convention.

The 2011 International Cyber Strategy [White House, 2011] is the official document describing key US approaches to international cyber regulation. This paper outlines the Obama administration's views on the role of cyberspace in social and economic development at the national and global level, as well as the goals and principles of US policy in relation to cyberspace. In 2018, the Donald Trump administration adopted the "National Cyberspace Strategy", which focuses more the homeland, but also refers to the international context. Additionally, the position of the United States and its supporters is clarified by the statements of officials made on the platforms of international organizations or addressed to the media.

An alternative "Western" approach to global cyberspace is represented by France's "International Strategy for Digital Space" [Ministere de l'Europe, 2018]. This country is not considered to be in the immediate circle of supporters of the United States, and its strategy expresses concern about American digital hegemony. It is also important that the French "continental" legal culture is traditionally opposed to Anglo-American customary law.

Finally, the position of one of the main stakeholders in the global cyberspace, China, is expressed in the "National Strategy for Cooperation in Cyberspace" adopted in 2017 [Xinhua …, 2017].

An additional context for the study is provided by international cyber regulation projects created by individuals and organizations mainly on the "Western" side of the digital space, as well as a number of initiatives by large international corporations designed to synchronize approaches to secure digital systems [Stadnik, 2018]. Of particular interest are two editions of the so-called "Tallinn Manual to International Law Applicable to Cyber Warfare" (in the second edition, the word "cyber warfare" was replaced by "cyber operations" [Schmitt, 2013; Schmitt, 2017]. These papers are academic studies representing the opinion of a group of eminent international jurists on the applicability of existing rules of international law to military operations in cyberspace.

Our study needs a tool for a comprehensive comparative analysis of the texts listed above. Unfortunately, the comparative legal research has no agreement on the kind of methodology to follow [Van Hoecke, 2015]. The most common so-called functional method does not reveal differences between different legal systems in understanding what is or is not a problem. In particular, the functional method, if applied to international cyber regulation projects, gives the impression of disagreement over proposed solutions where there is a much deeper conflict of ideologies and legal cultures.

A possible solution was proposed by G. Frankenberg, who studied national constitutions using the comparative analysis. His "constitutional architecture" model distinguishes four levels: rights and princi-

[1] Russia has been a consistent critic of the Budapest Convention, believing that, on the one hand, it is not sufficiently comprehensive in describing information threats, and on the other hand, it does not respect the national sovereignty of the participants [RF podderzhivaet razrabotku …, 2014].

ples, values and obligations, organizational arrangements, and, finally, rules for constitutional change and interpretation [Frankenberg, 2006]. Since international cyber regulation can be seen as an attempt to create a "constitution for global cyberspace", this model is well suited for the purposes of this analysis. The first two levels are of greatest interest: rights and principles, values and duties.

Taking into account the fact that, from a practical point of view, we are interested, first of all, in the possibilities of strengthening the position of Russia in the field of international cyber regulation, the analysis must focus on the draft convention on information security proposed by the UN in 2011 and the positions of other countries in relation to it.

Analysis results

The Frankenberg model makes it possible to identify and formalize significant differences in the legal approaches of the leading global cyberspace stakeholder countries at the levels of principles and values.

Principles. The Russian draft Convention on Information Security contains two key principles: (1) the need for a separate comprehensive regulation of global information security issues within a single document and (2) the organization of global cyberspace as a set of national cyberspaces managed by states parties [Konvencija ob obespechenii …, 2011, p. 2].

The first principle is also shared by some authors of alternative concepts of cyber regulation. For example, the draft treaty by S. Scholberg has the following introduction:

> "Cyberspace, as the fifth common domain – after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. A cyberspace treaty or a set of treaties at the United Nations level, including cybersecurity, cybercrime and other cyberthreats, should be the framework for peace, justice and security in cyberspace" [Schjolberg, Ghernaouti-Hélie, 2011, p. i].

However, the "US and supporters" group does not agree with this principle, as can be judged from the opinion expressed by British Foreign Secretary William Hague [Foreign and Commonwealth Office, 2012]. As an alternative, W. Haig proposed seven principles of cooperation between states, businesses and organizations in cyberspace: 1) The need for governments to act proportionately in cyberspace and in accordance with international law; 2) The need for everyone to have the ability to access cyberspace, including the skills, technology, confidence and opportunity to do so; 3) The need for users of cyberspace to show tolerance and respect for diversity of language, culture and ideas; 4) Ensuring that cyberspace remains open to innovation and the free flow of ideas, information and expression; 5) The need to respect individual rights of privacy and to provide proper protection to intellectual property; 6) The need for us all to work together collectively to tackle the threat from criminals acting online; 7) The promotion of a competitive environment which ensures a fair return on investment in networks, services and content [Foreign and Commonwealth Office, 2012].

Thus, there is a discrepancy between the desire to create a comprehensive, formalized legal document and the proposal to act on the basis of a rather limited set of rules, with the language closer to a political declaration than to lawmaking. Here it is easy to see the general contradiction between the "continental" legal tradition, based on legal codes, and the Anglo-American "common law", traditionally skeptical of codification.

The Russian concept was created within the legal culture, which believes that codification is "the perfect form for developing legislation", and that it creates "a solid framework on which all the legal matter of a particular branch of ... legislation rests" [Rahmanina, 2008, p. 32, 36]. The common law position can be expressed as follows: "the existence of a code is neither a necessary nor a sufficient condition for achieving these principles [of liberty, equality and justice]" [Canale, 2009].

For a while, a number of legal scholars in the United States denied in principle the need for a separate regulation for the Internet, pointing out that almost all problems related to it could be resolved within the framework of common law. The so-called "Horse Law" discussion was conducted in absentia between F. Eastbrook [Easterbrook, 1996] and L. Lessig [Lessig, 1999] in the late 1990s. The position of the former was that a separate cyber law makes no more sense than a separate "Horse Law", since all the necessary rules (ownership, sale, traffic rules, etc.) are already contained in a general law. The latter pointed out that cyberspace is a more complex phenomenon, its separate regulation is necessary and, moreover, is actually already being carried out from within cyberspace itself (see below). By 2001, Lessig's point of view became dominant, the United States actively supported the Budapest Convention on Cybercrime. However, the discussion itself, which took place on the platforms of leading legal forums and journals, shows that special codification is not a legal instinct within the Anglo-American tradition.

The US insists that the amount of special regulation carried out under the Budapest Convention is quite sufficient and does not require significant expansion. On the other hand, the authors of the Tallinn Manuals generally do a convincing job of interpreting existing international norms, including humanitarian law and the laws of war, as they apply to military operations in cyberspace.

In 2011, the USA finally formulated its legal position in relation to international cyberspace: "The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete … unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them" [White House, 2011, p. 9].

The second principle of the Russian approach to international information security (the construction of global cyberspace through national ones) is also supported by a number of foreign authors. In particular, it is shared in the S. Scholberg project, largely based on his experience of cooperation with the International Telegraph Union (ITU), which is trying to become the central international agency for managing

the global Internet (similar to the existing practice in the field of telegraph and telephone communications).

However, this principle is in conflict with the historically established architecture of the Internet, which was conceived as an open multi-stakeholder space in which sovereigns are present on an equal footing with all participants[1]. The formation of cyberspace took place within the framework of a certain ideology, the most striking expression of which was the "Declaration of Independence of Cyberspace" by an American poet and political activist John Perry Barlow:

"I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us, nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you... Cyberspace does not lie within your borders. Do not think that you can build it… You cannot. It is an act of nature, and it grows itself through our collective actions" [Barlow, 1996, p. 1].

For all the declarative nature of this manifesto, it contains important indications that the architecture (or nature) of the digital space does indeed create almost insurmountable obstacles to its regulation by governments. Cyber-anarchism has deep roots in the hacker movement that developed in the late 1970s[2]. In the book by Steven Levy "Hackers: Heroes of the Computer Revolution", it is noted that many prominent computer activists of the time transferred the ideas of the 1960s hippies into cyberspace [Levy, 1984][3].

As Lessig points out, architecture is one of the modalities of regulation (along with law, society, and market). So, the moment the Internet caught the attention of government regulators, it was already effectively regulated from within. Thus, in order to radically change the modality of cyberspace regulation, it is necessary, first of all, to restructure its architecture. According to Lessig, "… while particular versions of cyberspace do resist effective regulation, it does not follow that every version of cyberspace does so as well. Or alternatively, there are versions of cyberspace where behavior can be regulated, and the government can take steps to increase this regulability" [Lessig, 1999, p. 506].

[1] Allocation of the domain .gov for government organizations put them on a par with educational institutions -.edu – and commercial companies -. com. The formal presence of country domains does not create sufficient grounds for national sovereignty (contrary to the opinion of Uerpmann-Wittzack [Uerpmann-Wittzack, 2010, p. 1256]), since a significant number of leading Internet resources are registered in cross-country domains, the number of which has been significantly expanded since 2013.

[2] At that time the word "hacker" did not have negative connotations and was used for programmers who could solve non-standard tasks related to the organization of computer networks in an underdeveloped infrastructure. Although some of the hackers used unauthorized access to telephone networks and had a fairly loose attitude to intellectual property, their actions did not have the ultimate goal of causing damage.

[3] To some extent, the continuation of these ideas can be traced in the movement for the creation of decentralized cryptocurrencies, based on the manifesto of Satoshi Nakamoto (pseudonym).

Such ideas have actually been implemented in quite numerous projects on creating a "managed national Internet". First of all, this is the "Great Firewall" of China, as well as systems in Iran, Turkmenistan, etc., not to mention the numerous cases of temporary measures to restrict the Internet attempted by governments of different countries. The problem is that such restrictions inevitably put national users in unequal competitive conditions on the global market, which is sensitive for business and educational organizations. Well-developed and successful closed national networks, like the French Minitel, at some point lost market competition to the Internet precisely because of its functional superiority [Orlovskij, Korovkin, 2020].

The "state-centric" approach of the Russian concept seems to be a weakness even to those analysts who generally sympathize with it. For instance, O. Demidov points out that "the conceptual logic of the Convention does not allow the document to include the subjects that, in general, fill the global communications system with content and without whom information exchange is impossible" [Demidov, 2013, p. 140]. However, expanding the scope of the Convention to reflect the multi-stakeholder model of cyberspace governance is impossible from a legal point of view. This would actually endow the subjects of domestic law from different states with international legal subjectivity [Pazjuk, 2012, p. 238]. For this reason, the implementation of the Russian approach to global cyberspace requires the de facto nationalization of a number of institutions that are part and parcel of the Internet architecture.

The Russian legal approach to nationalization states: "... the institution of nationalization is necessary to ensure the progressive economic development of the country ... allows to overcome the individualism of participants in civil law relations and to promote the idea of public interest (general benefit, common good, public interest)" [Shhennikova, 2012][1]. In contrast, the modern Anglo-American legal school actually refuses to consider nationalization as an institution, considering it possible only as an extremely exceptional temporary measure (economic emergency) [Davidson, 2014]. Thus, the architectural restructuring of the global cyberspace, necessary for its harmonization as a set of national cyberspaces, seems unrealistic at present.

Values. In their simplest terms, values define the degree of importance of things, events, or actions, and thus affect the complex collective decision-making process. The value system is inherent to any culture and can be reconstructed from the analysis of extended texts by isolating the central concepts.

Such an analysis of the Russian draft Convention on International Information Security allows us to single out the following concepts that make up the value framework of the document [Konvencija ob obespechenii …, 2011]:

[1] At the same time, however, nationalization in Russia is called a dormant institution due to the lack of necessary legislation, the law on nationalization was developed over a number of years, but was never adopted. In particular, in November 2019, the State Duma by a majority of votes rejected the draft law proposed by the Communist Party of the Russian Federation [Gosduma otkazalas' …, 2019].

- state sovereignty;
- security and stability;
- traditionalism.

According to experts, the proposed project is largely a continuation of the ideas contained in Russian internal strategic documents as applied to international law. And the very value structure "sovereignty – stability – traditionalism" is a transfer to cyberspace of the "sovereign democracy" ideology formulated in 2006 by V. Surkov (then Deputy Head of the Administration of the President of the Russian Federation), which gradually turned into a dominant ideologeme, extremely rarely contested in domestic public mainstream.

Taken separately, the above values are shared by many participants in the global cyberspace. For example, the Chinese "Cyberspace Cooperation Strategy" puts sovereignty in second place after "peace" in a list of fundamental principles, and "protection of sovereignty and security" in first place among the goals. The French strategy also gives homage to sovereignty and pays significant attention to the preservation of cultural identity (primarily through the promotion of francophone content on the Internet). The importance of "security" as such is at the heart of all discussions on cyber regulation. However, none of the major countries-stakeholders of the global Internet operates with the described value structure, where the sovereignty of the state, stability and tradition form a closely related group of concepts.

The "US and supporters" approach is based on a drastically different value construct. This does not mean that the values of the Russian concept are openly challenged. They are simply given low priority relative to other value concepts. The 2011 U.S. International Cyber Strategy opens with an introduction by Barack Obama who argues that "cybersecurity is not an end unto itself; it is instead an obligation that our governments and societies must take on willingly, to ensure that innovation continues to flourish, drive markets and improve lives" [White House, 2011].

Dynamism – development and innovation – stands much higher in the values of the Western world, as reflected in the fourth principle of William Haig or in the following phrase from the American International Strategy for Cyberspace: "The United States will pursue an international cyberspace policy that empowers the innovation that drives our economy and improves lives here and abroad" [White House, 2011, p. 4].

The situation is similar with statehood as the basis for sovereignty. The involvement of the state makes sense only when and to the extent that the multistakeholder model is ineffective in achieving the public good. As long as Western governments do not observe the irreparable failures stemming from the current model of cyberspace governance, they see no reason to intervene. The absence of the state at the center of the value model almost automatically eliminates the importance of sovereignty as a concept.

The main benefit of the "Western" approach is the idea of equality of all cyberspace participants, with special respect given to the commercial and academic players who created cyberspace. This manifests both the value component stemming from the American constitutional right to "pursuit of happiness" and the historically established US messianism, which is closely associated with the values of freedom and openness. "Governments that respect the rights of their citizens have no reason to fear a free Internet"[1] [Pozner, 2011]. According to W. Haig, "There is the growing divergence of opinion and action between those countries seeking an open future for the Internet and those who are inching down the path of state control. We believe that it is not simply enough to address economic and security threats on the Internet without also taking steps to preserve the openness and freedom which is the root of its [Internet] success." [Foreign & Commonwealth Office, 2012].

The values of openness and freedom are also fundamental to the French cyber strategy.

An alternative value framework for the approach to cyber regulation put forward by the USA and like-minded supporters can be formulated as "dynamism (innovation) – equality of all participants (up to scaling down the role of the state) – openness (architectural and content-oriented)". It is easy to see that it contradicts the values of the Russian concept. However, it is wrong to consider this contradiction in a purely instrumental perspective, that is, to assume that it is only a negotiating position. Getting back to the Schwartz's definition, values are trans-situational and define the principles of life: Western representatives are genuinely incapable to operate within a different picture of the world. In turn, they, too, erroneously treat the Russian concept as a tactical goal, not realizing the deep value structure underlying it.

Typology of approaches to cyber regulation. The results obtained are consistent with the existing typologies of relations between the state and society. Thus, in the early 2000s, Spencer, Murtha and Linway applied the classification proposed by R.L. Jepperson [Jepperson, 2000]. He singled out two dimensions: the type of collective agency structure (how "statist" society is) and the type of organization of society (how "corporate" it is), which formed four possible quadrants: 1) social-corporatist state; 2) corporatist state; 3) liberal pluralist state; 4) state nation [Spencer, Murtha, Lenway, 2005, p. 326].

In this typology, the authors defined the USA as a liberal-pluralistic state. Russia (and other non-Western countries, with the exception of Japan) was not considered by them, but it clearly fits the description of the "state nation" type. These two types are not diametrically opposed. They are similar in terms of the organization of society – the absence of strong non-state institutions – "corporations" in the broad sense of the word (including various professional associations, academic communities, etc.).

[1] Of course, this vision is not shared in many other parts of the world. According to Zakharov, "the United States uses threats and bribery to impose their own understanding of democracy and neoliberal economic policy" [Zakarov, 2018, p. 133], this statement is partly true, but again it ascribes an instrumental character (maintaining technical superiority) to value-driven actions.

A slightly different typology can be proposed if we use the role of the state in economic (the state-organizer and the state-regulator of the economy) and political (the state is an ideological leader and a de-ideologized state) life as factors [Korovkin, 2018]. Within this classification, Russia is relegated to the category of "superstates" (leading role in the economy and politics), and the United States and its supporters – in the strictly opposite category of "state as a service".

In both cases, it can be seen that the divergence of positions on international cyber regulation is based on deep differences in views on the role of the state, its mandate of action and the ways in which the state and various public institutions, including business, interact.

Conclusion

G. Frankenberg singled out four types of constitution: contract, manifesto, program and law [Frankenberg, 2006]. Effective international law is possible only as a contract, since it requires the consent of all parties, which can only be obtained if they have sufficiently weighty benefits. If the zone of agreement is too narrow, the contract degenerates into a manifesto – formally supported by all participants, but having no practical consequences in coordinating their actions. For this reason, developing international legislation is an extremely complex process. Differences in the positions of the parties, of course, are often instrumental in nature: the desire to negotiate the most advantageous competitive position in global markets to the nation. However, these discrepancies may also have a deeper foundation: the difference between legal cultures (and cultures in the broad sense of the word), expressed in the incompatibility of the principles and values of lawmaking.

Such incompatibility is fully evident in the Russian and US official materials on international cyber regulation. In the future, it is advisable to supplement this study with the analysis of positions of other important stakeholder countries in the global cyberspace, such as Japan or India.

We must admit that the existing cultural differences make it unlikely to reach a broad international consensus on cyberlaw in the foreseeable future. The multistakeholder architecture of cyberspace presents a particular difficulty[1]. A likely scenario is the regionalization of cyberspace, with creating alliances based on the mutual trust of the participants and the unity of their views on the key principles of cyber regulation. Examples of such alliances are the SCO declaration, the African Union data protection convention and the EU personal data protection legislation. To some extent, global cyberspace is turning into a "patchwork quilt" of norms and regulations that hinders the actions of conscientious actors (state and non-state) but opens numerous legal gaps and loopholes to unscrupulous ones.

[1] In the history of international law, there is already an example of the failed attempt to regulate a multistakeholder environment – the long-discussed UN Convention on Transnational Companies was not eventually adopted, the issue gradually left the agenda of the organization [Hedley, 1999].

References

1. Demidov O. Obespechenie mezhdunarodnoj informacionnoj bezopasnosti i rossijskie nacional'nye interesy // Indeks bezopasnosti. – 2013. – N 1 (104), Vol. 19, – P. 129–168.
2. Gosduma otkazalas' prinimat' zakon o nacionalizacii imushhestva // IA Regnum. – 2019. – 12.10. – URL: https://regnum.ru/news/economy/2775635.html (date of access 03.04.2020)
3. Huzhina A.V. Pravovaja priroda seti Internet: voprosy regulirovanija // Vestnik JuUrGU. Serija "Pravo". – 2015. – Vol. 15, N 1. – P. 101–107.
4. Konvencija ob obespechenii mezhdunarodnoj informacionnoj bezopasnosti (koncepcija) / Ministerstvo inostrannyh del Rossijskoj Federacii. – 2011. – URL: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (date of access 03.04.2020.)
5. Korovkin V.V. Nacional'nye programmy cifrovoj jekonomiki stran Blizhnego Vostoka // Ars Administrandi (Iskusstvo upravlenija). – 2019. – Vol. 11, N 1. – P. 151–175.
6. Orlovskij V., Korovkin V. Ot nosoroga k edinorogu. Kak provesti kompaniju cherez transformaciju v cifrovuju jepohu i izbezhat' smertel'nyh lovushek. – Moskva: Bombara, 2020. – 367 p.
7. Pazjuk A.V. Ponjatie mezhdunarodnogo informacionnogo prava kak kompleksnoj otrasli sovremennogo mezhdunarodnogo prava // Aktual'ni problemi mizhnarodnih vidnosin. – 2012. – Vipusk 111 (Chastina I). – URL: https://digital.report/ponyatie-informatsionnogo-prava/ (date of access 02.04.2020).
8. Rahmanina T.N. Aktual'nye voprosy kodifikacii rossijskogo zakonodatel'stva // Zhurnal rossijskogo prava. – 2008. – N 4(136). – P. 30–39.
9. Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere // Oficial'nyj sajt MID RF. – 2017. – 29.06. – URL: https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288 (date of access 02.04.2020).
10. RF podderzhivaet razrabotku konvencii po bor'be s kiberprestupnost'ju // RIA Novosti. – 2014. – 28.10. – URL: https://ria.ru/20141028/1030552154.html (date of access 02.04.2020).
11. Shhennikova L.V. Grazhdansko-pravovaja nauka o nacionalizacii // Vestnik Permskogo universiteta. Juridicheskie nauki. – 2012. – N 4. – P. 179–186.
12. Zaharov T.V. Mezhdunarodnoe sotrudnichestvo gosudarstv v sfere informacionnoj bezopasnosti i pravovye podhody k ego regulirovaniju // Gosudarstvo i pravo v novoj informacionnoj real'nosti. – 2018. – N 1. – P. 119–134.
13. Zinov'eva E.S. Perspektivnye tendencii formirovanija mezhdunarodnogo rezhima po obespecheniju informacionnoj bezopasnosti // Vestnik MGIMO-Universiteta. – 2016. – N 4(49). – P. 235–247.
14. Barlow J.P. A Declaration of the Independence of Cyberspace 1996 // Electronic Frontier Foundation. – 1996. – URL: https://www.eff.org/cyberspace-independence (date of access 02.04.2020).
15. Benedikt M. Cyberspace: Some Proposals // Cyberspace: first steps / Michael Benedikt (ed.). – Cambridge: MIT Press,1991 b. – P. 120–138.
16. Benedikt M. Introduction // Cyberspace: first steps / Michael Benedikt (ed.). – Cambridge: MIT Press, 1991 a. – P. 1–25.
17. Canale D. The Many Faces of the Codification of Law in Modern Continental Europe // A History of the Philosophy of Law in the Civil Law World / D. Canale, P. Grossi, H. Hofmann (ed.). – Dordrech: Springer, 2009. – P. 135–183.
18. Davidson N.M. Nationalization and Necessity: Takings and a Doctrine of Economic Emergency // Brigham-Kanner Property Rights Conf. (October 27, 2014). – 2014. – (Fordham Law Legal Studies Research Paper; N 2515333). – URL: https://ssrn.com/abstract=2515333 (date of access 05.04.2020).
19. Department of State Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security / Department of State. – 2017. – URL: https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016–2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/(date of access 05.04.2020).
20. Department of State International Law in Cyberspace, Remarks Harold Hongju Koh, Legal Advisor U.S. Department of State, USCYBERCOM Inter-Agency Legal Conference, (September 18, 2012) / Department of State. – 2017. – URL: https://2009–2017.state.gov/s/l/releases/remarks/197924.htm -un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/ date of access 05.04.2020).
21. Easterbrook F. Cyberspace and the Law of the Horse / University of Chicago Legal Forum. – 1996. – 207 p.
22. Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Tele // United States Mission to the United Nations. – 2017. – 23.06. – URL: https://usun.usmission.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-tele/ (date of access 05.04.2020).
23. Foreign and Commonwealth Office An open internet is the only way to suPort security and prosperity for all: Foreign Secretary speech at the Budapest Conference on Cyberspace. – 2012. – URL: https://www.gov.uk/government/organisations/foreign-commonwealth-office -un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/ (date of access 03.04.2020).
24. Frankenberg G. Comparing constitutions: Ideas, ideals, and ideology – toward a layered narrative // International Journal of Constitutional Law. – 2006. – Vol. 4, N 3. – P. 439–459.

25. Hedley R. Transnational Corporations and Their Regulation: Issues and Strategies // International Journal of Comparative Sociology. – 1999. – Vol. 40, N 2. – P. 215–230.
26. Jepperson R.L. Institutional Logics: On the Constitutive Dimensions of the Modern Nation-State Polities. – Florence: European University Institute, 2000. – URL: https://cadmus.eui.eu/handle/1814/1676 (date of access 05.04.2020.)
27. Kerttunen M., Tikk E. Parabasis. Cyber-diplomacy in Stalemate / Norwegian Institute of International Affairs. – 2018. – URL: https://www.nupi.no/en/Publications/CRIStin-Pub/Parabasis-Cyber-diplomacy-in-Stalemate (date of access 05.04.2020).
28. Korovkin V. A digitally transformed state // BRICS Business Magazine. – 2018. – Vol. 21, N 2. – P. 46–55.
29. Lessig L. The Law of the Horse: What Cyberlaw Might Teach // Harvard Law Review. – 1999. – N 113. – P. 501–549.
30. Levy S. Hackers: heroes of the computer revolution. – Doubleday, 1984. – 464 c.
31. Lloyd W.F. Lloyd on the Checks to Population // Population and Development Review. – 1980. – N 6(3). – P. 473–496.
32. Ministere de l'Europe et des Affairs Etrangeres Stratégie internationale de la France pour le numérique / Ministere de l'Europe et des Affairs Etrangeres de France. – 2018. – URL: https://ch.ambafrance.org/Strategie-internationale-de-la-France-pour-le-numerique (date of access 05.04.2020).
33. Pozner M. Internet Freedom and Human Rights // American Rhetoric. – 2011. – URL: https://www.americanrhetoric.com/speeches/michaelposnerinetfreedomhumanrights.htm (date of access 03.04.2020).
34. Prakesh R., Baruah D.M. The UN and Cyberspace Governance // ORF Issue Brief. – 2014. – N 68. – URL: https://www.orfonline.org/wp-content/uploads/2014/03/IssueBrief_68.pdf (date of access 05.04.2020).
35. Roberts A. Is International Law International? – Oxford: Oxford University Press, 2017. – 420 p.
36. Schjolberg S., Ghernaouti-Helie S. A Global Treaty on Cybersecurity and Cybercrime // AiTOslo. – 2011. – URL: http://pircenter.org/media/content/files/9/13480907190.pdf. (date of access 03.04.2020).
37. Schmitt M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. – Cambridge: Cambridge University Press. – 2017. – 30 p.
38. Schmitt M. Tallinn Manual on the International Law Applicable to Cyber Warfare. – Cambridge: Cambridge University Press, 2013. – 215 c.
39. Scott S.V. International Law as Ideology: Theorizing the Relationship between International Law and International Politics // European Journal of International Law. – 1994. – Vol. 5, N 3. – P. 313–325.
40. Spencer J., Murtha T., Lenway S. How Governments Matter to New Industry Creation // AMR. – 2005. – N 30. – P. 321–337. – URL: https://doi.org/10.5465/amr.2005.16387889 (date of access 05.04.2020).
41. Stadnik I. A New Cybersecurity Diplomacy: Are States Losing Ground in Normmaking? // Russian Council on International Affairs. – 2018. – URL: https://russiancouncil.ru/en/analytics-and-comments/analytics/a-new-cybersecurity-diplomacy-are-states-losing-ground-in-norm-making/ (date of access 05.04.2020).
42. Uerpmann-Wittzack R. Principles of International Internet Law // German Law Journal. – 2010. – Vol. 11, N 11. – P. 1245–1263.
43. Van Hoecke M. Methodology of Comparative Legal Research // Law and Method. – 2015. – C. 1–35.
44. White House International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / Office of President of the United States. – 2011. – URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (date of access 0504.2020).
45. Xinhua International Strategy of Cooperation on Cyberspace 2017 // Xinhuanet.com. – 2017. – URL: http://www.xinhuanet.com//english/china/2017–03/01/c_136094371_2.html (date of access 05.04.2020).

The article was first published in Russian in the journal "Социальные новации и социальные науки". – 2020. – N 1. – P. 60–76.

POINT OF VIEW

DIGITAL TECHNOLOGIES IN THE BANKING SECTOR OF RUSSIA

Irina Lebedeva

PhD (Econ. Sci.), Head of Department, Saint Petersburg Academy of the Investigative Committee of the Russian Federation (Saint Petersburg, Russia)[1] E-mail: irinaa508@mail.ru

Abstract. *In recent years significant changes have occurred in the banking sector. Traditional banking operations are becoming outdated, replaced by new, innovative, digital-based practices. Digitalization affects all spheres of banking activities: management, customer and partner relationships, security, financial accounting, strategic planning, etc. The author explains the need for such changes, describes main digital technologies and tendencies observed in the banking sector; shows the extent of digitalization in the banking sector. The article analyzes the opportunities and threats presented by new financial technologies for both credit institutions and their clients. The author shows how digitalization has affected the structure of the banking sector, the composition of participants, the needs and preferences of bank customers. The article formulates the main challenges and threats to the banking sector from digital innovations. The modern fraudulent practices are analyzed, and the degree of their influence on the banking activities is determined. The increasing role of the regulator in the financial market is substantiated.*

Keywords*: banking sector; digital transformation; digital banking services; digital technologies; digital customer profile.*

For citation: Lebedeva I. Digital technologies in the banking sector of Russia / English transl. by Nikulichev M.Y. // Social Novelties and Social Sciences. – Moscow : INION. RAN, 2022. – N 1. – P. 33–48.

URL: https://sns-journal.ru/en/archive/ DOI: 10.31249/snsneng/2022.01.03

Introduction

Sustainable economic development in the modern world is impossible without the stable functioning of the banking sector. Its ability to withstand modern challenges and threats, to ensure reliable, safe and mutually beneficial cooperation of all participants in economic relations, guarantees the financial security of the country even in the face of the economic sanctions. By accumulating and redistributing temporarily free funds, ensuring the security and continuity of the payment system, the banking sector protects the country's economic sovereignty, and common economic space, minimizes internal and external threats to the economy, and creates the foundation for implementing the country's strategic national priorities. By ensuring the safety of a significant part of personal savings, credit organizations contribute to social and political stability in the country.

Over the past decades, there have been significant changes in the world economy, which could not leave the banking system unaffected. Globalization intensifies interaction between financial market participants, expands opportunities for attracting investments, reduces costs of banking operations, stimulates innovations in the banking sector. One of the trends in the development of the banking sector is its digital transformation (the process of replacing traditional banking practices with the latest digital alternatives).

In the modern world, the role of the financial sector has increased significantly. Half a century ago the banking sector mostly functioned as a mediator of economic processes; today it influences the economy more and more, sets conditions, and sometimes even makes it possible to implement them. Some scholars talk about the tyranny of financial development [L'vova, 2017, p. 181]. Therefore, it is so important today to monitor potential threats to the banking sector, to thwart them, thus, preventing these threats from spreading to the country's economy.

The purpose of this study is to analyze the impact of digital transformation on the Russian banking sector and to assess opportunities and threats for banking market participants.

Research Methodology

When writing the article, the author employed methods of comparison, analysis and synthesis, referred to the polls of financial market participants conducted by the FinTech Association (AFT) during 2020-2022. 27 banks took part in this survey (Top-5 – 4 banks, Top-10 – 6 banks, Top-20 – 6 banks, others – 11 banks). The author also referred to the study of personal finance management services market in Russia in 2021, carried out by App Annie.

Results

The banking sector is among the leaders of digital transformation. This is due to a number of factors: the role of commercial banks in the country's economy, the requirements of the regulator, consumer expectations, and technological capabilities.

The main areas of implementing new financial technologies in the banking sector are payments and transfers, financing and capital management. Factoring, promissory notes, pledge operations, non-cash payments under letters of credit, solvency check-ups, as well as the creation and maintenance of credit histories of borrowers are beginning to move into the digital sphere.

Not all of these financial technologies have been mastered and successfully applied by credit institutions. Only industry leaders use such innovative technologies as augmented reality, the Internet of things, quantum computing.

Digital transformation has significantly changed the banking sector: the number of credit institutions is dropping, the boundaries between banking and alternative services are blurred, new players, such as fintech companies, appear in the marketplace, banks are expanding their range of services through non-banking operations.

Competition in the banking services market is shifting from the bank's pricing policy to the area of service quality, easier interaction and communication channels, comprehensive banking packages, personalization opportunities and product design.

The main effects of digitalization can be identified: increasing the value of a banking product, changing customer expectations; upgrading banking business models, offering new forms of cooperation and partnership.

Apart from advantages, innovative technologies carry new potential threats, which calls for increased responsibility of all market participants for their actions. Despite the number of fraudulent transactions is on the rise, their share is negligible, which indicates how effective are the security departments of credit institutions.

The banking system is becoming more customer-oriented, banking operations are getting more reliable, customers receive constant access to financial services that meets the requirements of the digital economy.

The developing digital banking sector sets up new goals: ensuring the high-quality financial services for a wide range of users; reducing costs and risks in the financial market, including risks associated with the use of digital technologies; promoting competition and innovation in the financial market.

Analysis

Digital transformation has already affected all spheres of human activity. Explosive development of digital technologies is due to a shift in the development paradigm, when information has become the most

important resource in socio-economic processes [Formirovanie cifrovoj jekonomiki ..., 2017]. Social and economic relations are increasingly shifting into the network space. Credit institutions cannot remain unaffected, which is due to a number of factors [Lebedeva, 2022, p. 75–76].

First, the banking sector is said to be the circulatory system of the economy, it mediates in all financial and monetary relations of economic entities, redistributes financial flows. To create conditions for high-quality, reliable, safe and mutually beneficial cooperation of all participants in economic relations credit institutions must transfer their activities to the digital sphere, introduce innovative tools and technologies, change business processes and operating principles.

Second, the Bank of Russia identified digitalization of the financial market and the country's economy as a whole as one of its strategic tasks [Proekt osnovnyh napravlenij …, 2021, p. 3]. In order for bank customers to be able to receive affordable services even in hard-to-reach places, the Central Bank offers its solutions and services, stimulating the digital transition in all credit institutions. In particular, the Bank of Russia began a gradual transition to a modern automated settlement system that operates mainly in real time [Homenko, 2022]. The major credit institutions and banks with a universal banking license must use the Faster Payment System (FPS). However, in fact, all credit organizations that provide money transfer services and related to the use of international payment cards, as well as payment cards that are issued by the payment system and receive international status, should switch to FPS in the near future [Homenko, 2022]. In 2020, the "Finuslugi" platform (Financial Services) was launched to attract deposits; in 2021, the QR code payment system began to operate and became mandatory for implementation in universal banks. It is planned to launch a platform for issuing loans and factoring, KYC platform ("Know your customer") and others [Kac, 2021].

Third, being a part of the global financial market, the Russian banking sector is forced to work within the framework of world standards and regulations, trying to match world leaders in quality and in the range of banking services. Moreover, in the digital age, the advanced technological position comes with a reward of super profits, increased market share, the opportunity to establish new standards, as well as with a chance to play a significant role in ensuring economic security at all levels.

Fourth, the banking sector opens up to new emerging market conditions and opportunities: widespread use of the Internet, rapid development of sensor technology, big data analytics, cloud computing; prevalence of personal mobile devices, cheap and affordable wireless communication [Golovenchik, 2021, p. 45].

And finally, the banking sector experiences growing consumer demand for digital services. Over the past decades, the needs of bank customers have changed significantly. Expectations for digital services have risen sharply during the COVID-19 pandemic. According to PWC, in 2020, the use of remote banking services around the world increased by 23%, and mobile banking applications – by 30%. Bank

customers have appreciated the convenience of digital services and do not want to return to the old service format [Proekt osnovnyh napravlenij …, 2021, p. 6].

Thus, credit institutions have no choice – in order to compete in the market, they need to transfer part of their operations into the digital sphere, put into practice regularly updated financial technologies (financial products based on innovative and/or digital technologies), constantly expand the list of improved digital services, adjust them to the needs of consumers.

Table 1 presents the most productive and promising digital banking.

Table 1

The most promising digital innovations for the banking sector *

Technology	Description	Benefits for banks
Artificial intelligence (AI)	a system that simulates human behavior to perform specific tasks	developing ready-made solutions both for clients and for the banks
Machine learning	a subsection of AI that does not imply solving a problem directly, but learning by solving similar problems	
Robotization	technology that automates the financial services using computer programs and robots	reduction of costs and expenses, reduction of time for each operation
Cloud technologies	provide access to data without installing special applications on the device	products available anywhere in the world due to the centralization of services in the network
Big Data	large structured or unstructured data sets	providing customers with personalized targeted offers based on the analysis of heterogeneous and rapidly changing digital information accessed via the Internet, corporate document archives, etc.
Blockchain	distribution of decentralized databases with information on all transactions carried out by all	solving many problems, including generation of smart contracts and letters of guarantee, cryptocurrency creation, authentication of documents, and document security, eCommerce maintenance
Application Programming Interface (API)	a set of customized classes, procedures, functions, structures and constants provided by an application, service or operating system for use in external software products	improving customer interaction
Social networks and mobile communication with specialized applications	special package offers for watching movies, providing mobile communications, insurance, using financial services and purchasing goods	obtaining information about customer preferences

* Source: [Makarova, Pavlika, 2022, Sovremennye tendencii …, 2020, Chernyshova, 2021; Pshenichnikov and Kovtunova, 2018].

Figure 1 shows the main trends in digital technologies in the banking sector.

For example, credit institutions almost everywhere use blockchain technologies in the following areas [Makarova, Pavlika, 2022]:

– providing bank guarantees;

– trade finance (factoring operations, non-cash payments under letters of credit);

– exchanging interbank messages at the domestic and international levels;

– bill transactions between banks (sale of bills, transfer, collection, acceptance, discounting);

– collateral transactions: accounting for tangible and intangible assets, ownership transfer (using smart contracts);

– recording borrower credit histories (generating and storing data on borrowers' credit histories allows interested users to exchange information without intermediaries).

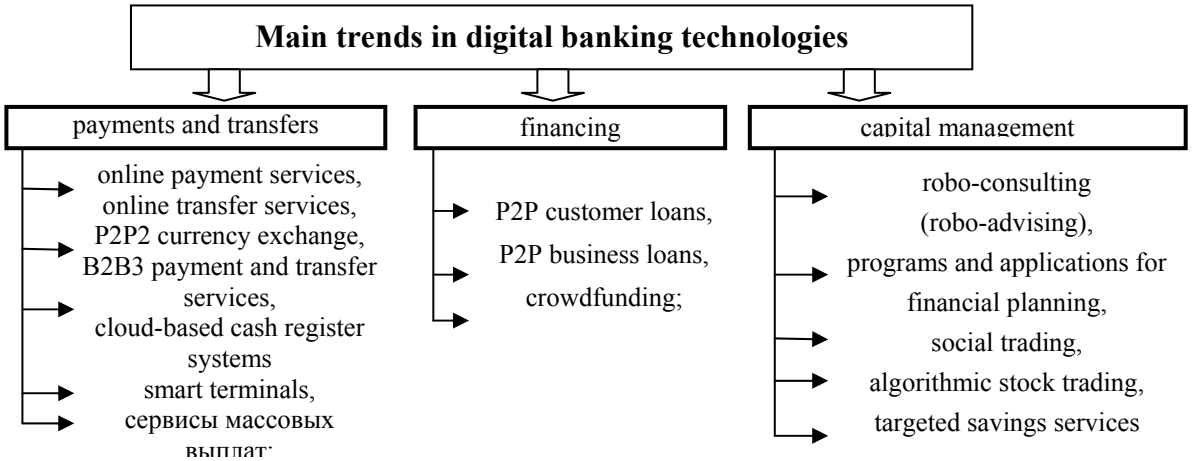


Fig. 1. The main trends in digital technologies in the banking sector

Source: [Makarova, Pavlika, 2022, Sovremennye tendencii …, 2020].

However, according to the study conducted by the FinTech Association (FTA), not all financial technologies have yet been mastered and successfully applied by Russian credit institutions (Fig. 2). For example, less than 60% of participants in the country's banking sector use cognitive technologies and biometrics in an industrial mode. And only for a very limited circle of market participants experiments with such technologies as augmented reality, the Internet of things, quantum computing [Rezul'taty issledovanija ..., 2021, p. 10].

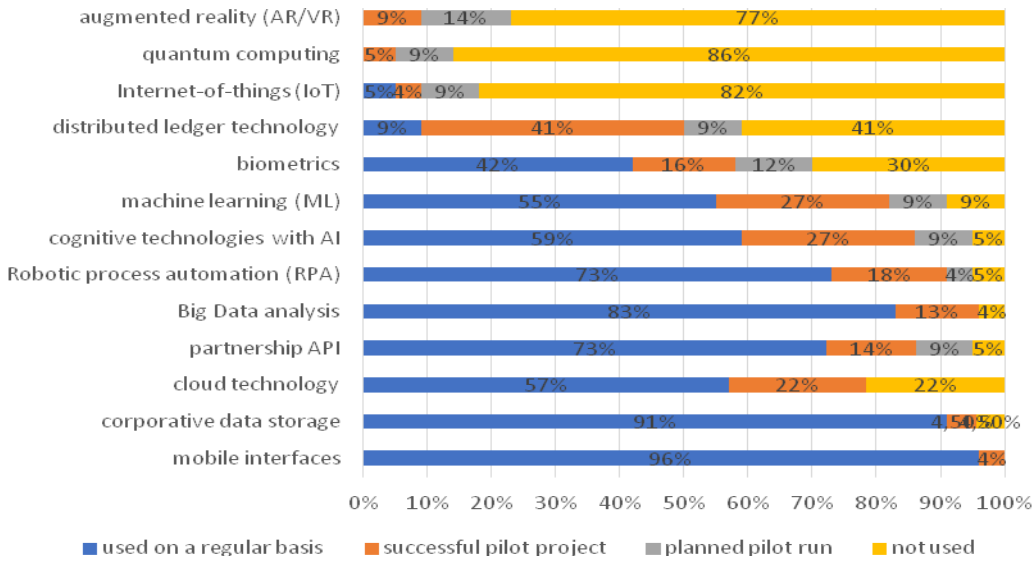


Fig. 2. The level of using technological innovations by Russian commercial banks

Source: [Rezul'taty issledovanija ..., 2021, p. 11]

As mentioned above, all credit institutions, if they plan to continue their activities in the banking market, must not only transfer their services to the digital sphere by introducing innovative tools and technologies, but also transform customer relationships, adjust business processes and work principles. However, there is no single model or way to move to a new level of operation. Depending on the maturity of the bank, its structure, the services provided, various models for the implementation of digital activities are possible (Table 2).

Table 2

Classification of digital banks based on their business models and the services they provide*

Bank type	Description	Examples
New banks	have standard banking licenses, offer the same services as traditional banks	Monzo, N26, Starling Bank and Revolut
Neobanks	do not have a banking license but cooperate with financial institutions offering licensed services. Customers can get a more user-friendly interface and free services, but only if they have an account with a licensed bank	WeBank from Tencent, Yolt, Lunarway and Moven
Beta banks	joint ventures or subsidiaries of existing banks that offer financial services under a license from a parent company. Often created to enter new markets, offering limited services to a wider range of consumers	AiBank (joint venture between China's CITIC Bank Corp and search giant Baidu); Simple (partnership between Bancorp and BBVA)
Nonbanks	are not related to traditional banking licenses. Use other methods to provide financial services. Can work independently of existing banks	Monese (operates under a license for electronic money)

* Source: [Kagan, 2020].

Digital infrastructure (presented in Figure 3) plays an important role in the development of digital financial transactions, ensuring their security and efficiency.

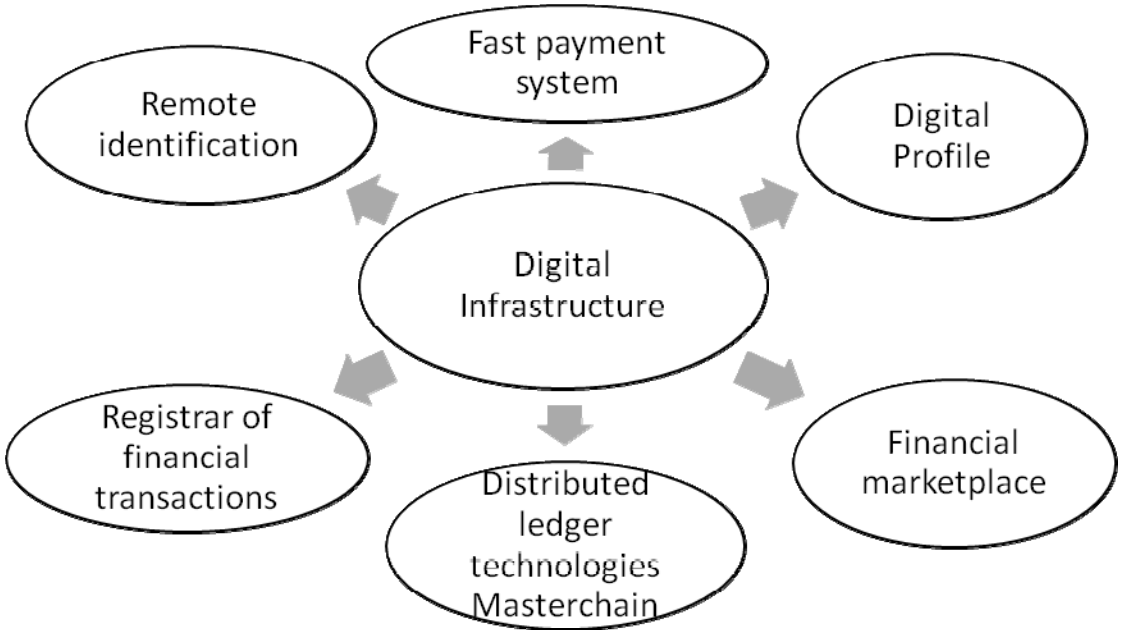


Fig. 3. Elements of the digital infrastructure on the financial market

Source: [Razvitie finansovyh tehnologij, 2022].

A study conducted by the FinTech Association (AFT) showed that not all elements of the digital infrastructure that exist in Russia meet customer needs [Rezul'taty issledovanija ..., 2021, p. 9]. "Digital Profile" and "Unified Biometric Platform" need to be improved (Fig. 4). Perhaps this attitude is due to the fact that these tools are quite new (used since May 2020 and December 2021, respectively) and need additional adjustment to the wishes and needs of users. Whereas the Masterchain platform and the fast payment system have been in operation since 2019.

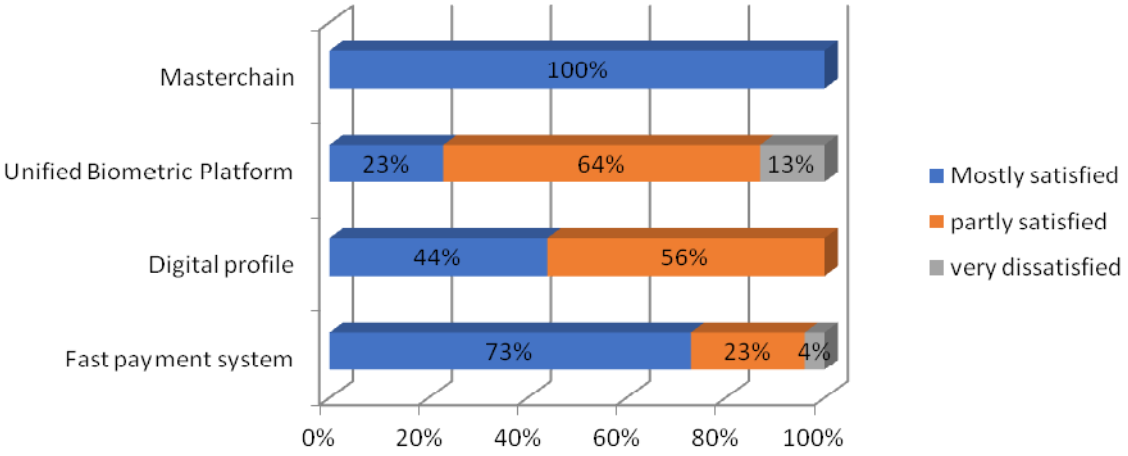


Fig. 4. The degree of satisfaction with the current state of the digital banking infrastructure

Source: [Rezul'taty issledovanija ..., 2021, p. 9]

At the same time, according to the majority of financial market participants, improvements in digital infrastructure should be initiated by their associations (Fig. 5). The role of the state is to stimulate the development of innovations with the help of the regulatory sandbox, tax breaks and by ensuring equal conditions for all market participants to digital solutions, regardless of who develops them [Rezul'taty issledovanija ..., 2021, p. 67].

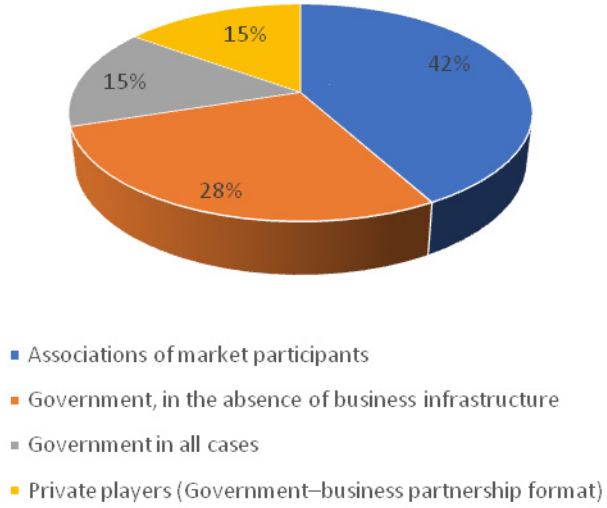


Fig. 5. Results of the survey "Who should initiate the creation and become the owner of the digital infrastructure on the financial market"

Source: [Rezul'taty issledovanija ..., 2021, p. 67].

Digitalization modifies the entire business model of a banking organization: the products and positioning of the organization change, relationships with customers are transformed. Traditional banking service is based on personal relationships and interaction. In the case of a digital service, the nature of the relationship fades into the background; in most cases, the bank does not even know about the social, cultural or emotional profile of its client [Cvetkov, Semushkina, 2009, p. 40].

It should be noted that digital competition requires significant advertising budgets (in order to convey information about products to customers) and high credit ratings, which would indicate the high information transparency within a credit institution and a low risk level [Lebedeva, 2022, p. 78].

Studies indicate that banks that embarked on a digital transformation increase their return on equity by an average of 0.9%. For banks that do not employ business process automation, this indicator decreases by an average of 1.1% [McIntyre, Skan, 2019, p. fifteen]. As digital technologies mature, this gap will widen. Thus, income redistributes in favor of corporations (mainly transnational corporations) that have achieved technological leadership both in the field of digitalization and in related areas of automation, robotics, biotechnology, etc. [Lebedeva, 2022, p. 80]

This is how global changes affected the structure of the banking sector in Russia:

First, the digital transformation of the banking business helped reduce the number of commercial banks at an accelerated pace; the process started as early as 2013 with the change in leadership of the Central Bank. Over the next 7 years, the number of banks has almost halved: 956 in 2013 and 442 in 2020 (Fig. 6).

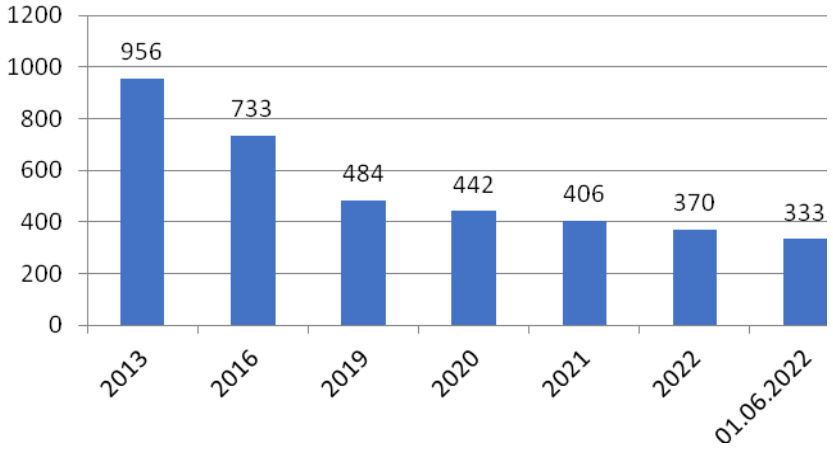


Fig. 6. Number of credit institutions at the beginning of each year (compiled by the author based on data from the Bank of Russia website)

Unexpectedly, in 2020, the number of licenses that banks gave up voluntarily exceeded the number of those withdrawn by the Central Bank: 20 banks independently refused to continue their business, while the regulator revoked the licenses of 14 banks (Table 3).

Table 3

Number of revoked and canceled licenses in 2013–2021 in Russia**

Number of licenses	2013	2014	2015	2016	2017	2018	2019	2020	2021
Revoked, total	32	86	93	103	51	60	28	16	26
Including banks	29	73	88	98	47	57	24	14	20
NPO *	3	13	5	5	4	3	4	2	6
Cancelled, total	12	9	11	14	12	17	14	22	13
Including banks	12	9	11	13	10	17	12	20	11
NPO	0	0	0	1	2	0	2	2	2

* NPO – Non-profit organization
** Source: [Kac, 2021].

Until 2018, the main reason for the withdrawal of banking licenses in Russia was non-compliance with "money laundering" legislation. In 2020 and 2021, it is tied for 3rd and 4th place with suspicious/transit e-commerce operations, including illegal online casinos and betting shops. Currently, banking licenses are revoked mainly for inadequate asset valuation and insufficient provisioning. The second place is occupied by the unsatisfactory management of customers' funds. The reasons for the voluntary surrender of licenses are the increased requirements for the level of digital banking services (both from customers and from the regulator), unfavorable economic conditions, and increased competition for high-quality borrowers [Lebedeva, 2022, p. 79]. The Russian banking market saw an increase in the number of mergers & acquisitions (M&A), many of which were carried out in order to reduce the group's costs. In 2022, seven out of 13 credit institutions were liquidated as part of a merger with other credit institutions [Tihonov, 2022].

According to experts, about 30 credit institutions, that is, 8.7% of the current participants, will be liquidated in Russia in the near future. By 2025, their number may be reduced to 200-250, and in the long term to 50-100 [Kac, 2021].

Secondly, the emergence of new players in the market has become a new trend in the development of the country's banking sector. In 2021, the head of Wildberries acquired Standard Credit bank, renamed it into Wildberries Bank, and then the OZON online retailer registered a microfinance organization. "It is beneficial for a large retailer with $1 billion assets to own a bank for online operations" [Kac, 2021]. At the same time, it is difficult and risky to own banking business today: competition is high, the regulatory activities are not always predictable, and customer demands are constantly growing. It is difficult for new high-tech banks to compete with the largest banks, both private and state-owned, but they can influence the entire banking sector [Lebedeva, 2022, p.78].

Alternative financial market actors: large technological companies, neobanks, alternative payment providers and fintech start-ups – are gradually winning back positions from traditional banks [Rezul'taty issledovanija ..., 2021, p. 5]. Fintech companies provide online services that are more accessible and convenient for the consumer. Credit institutions and investment companies are sometimes forced to follow the suit, as lagging in the service quality means the loss of borrowers and savers.

Thirdly, digital technologies expand the boundaries of the financial sector. Banks began to perform previously unusual functions. Customers can allow to make a doctor appointment, buy movie tickets or fitness center contract, choose a travel destination, etc. using modern banking applications.

In recent years, Personal Finance Management (PFM) has been actively developing – the software that powers many different personal finance and mobile banking tools. The purpose of PFM applications is to help manage personal or family budget, control expenses, analyze spending categories and manage savings. PFM services and applications may be provided by banks, or by third-party developers, whose services are usually based on a subscription model [Rynok servisov …, 2022, p. 2].

According to the research company App Annie, almost all PFM applications have a data export function (allowing to upload data for reporting, for example, expenses during business trips). The function of debt control (reminds to whom and how much the user owes, or vice versa – to whom he lent money) is offered by less than half of the services. And such functions as scanning checks, automatic accounting of banking transactions and training in financial literacy are still rare [Rynok servisov ..., 2022, p. 3]. The leaders of PFM applications and their functionality are shown in Figure 7.

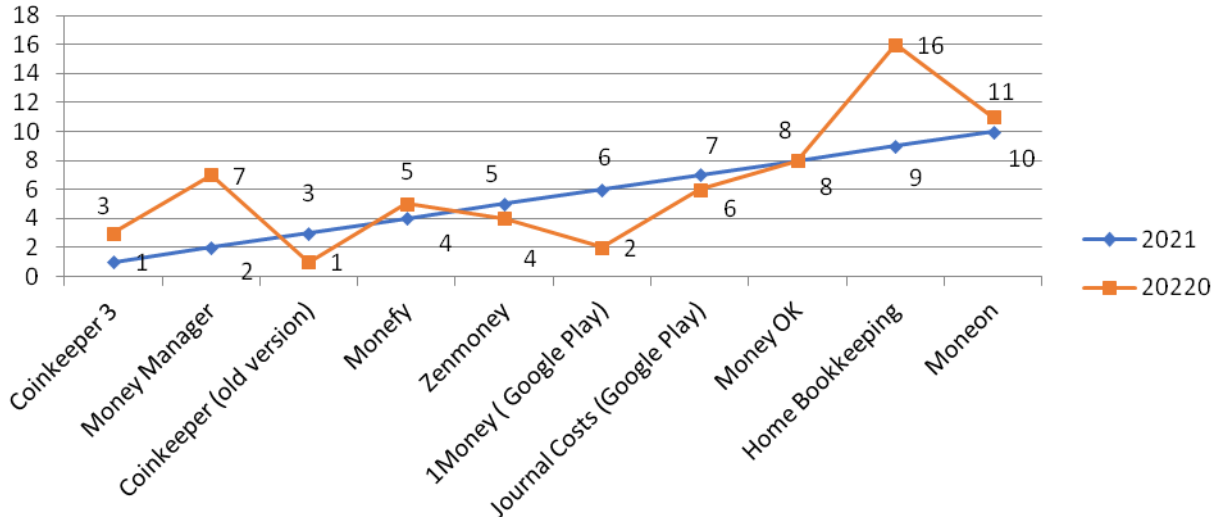


Fig. 7. Leaders in PFM applications in 2020 and 2021 (compiled by the author based on research by App Annie)

Source: [Rynok servisov …, 2022, p. 2]

The functionality of popular PFM services in Russia is given in Table. 4.

One promising feature that has not yet been offered by any of the PFM services is the initiation of payments from the PFM interface. Such an option would be convenient, for example, for transferring money from one deposit card to a card with favorable cashback conditions.

According to experts, at present, the main competition between large universal banks is concentrated in digital services and ecosystems [Kac, 2021]. For instance, large banks create special departments responsible for the development of service solutions that other players and not only financial markets can use. As a result, the boundaries between the fields of activity of various organizations are blurred.

Table 4

Popular PFM services in Russia*

PFM services / functions	Automatic accounting of banking operations	Scanning checks	Debt control	App for Apple Watch and Wear OS	Data export	Training in financial literacy
Coinkeeper 3	+					+
Money Manager, Expense Tracker					+	
Coinkeeper (old version)	+	+	+		+	
Monefy					+	
Zenmoney	+				+	
1Money (only at Google Play)					+	
Journal Costs (only in Google Play)					+	
Money OK				+	+	
Home Bookkeeping			+		+	
Moneon			+	+	+	

* Source: [Rynok servisov …, 2022, p. 3].

Challenges to banking security in the context of digitalization

Research proved that fintech technologies open up almost limitless opportunities for both credit institutions and their clients. However not all market participants are ready and/or willing to use these opportunities, preferring traditional services. And we must not forget that new technologies also carry new potential threats which all participants must be ready to cope with (Table 5).

Table 5

Opportunities and Threats of New Technologies for Financial Market Players*

Market participants	Opportunities and advantages	Risks and liabilities
Credit organisations	expanding the service range within their own financial and non-financial ecosystems; compiling a psychological profile of potential customers to customize offers, predict client's solvency, increase work efficiency; earning clients' loyalty and stabilizing the client base; improving profitability by increasing operating income and reducing operating expenses; higher return on capital and business efficiency; emergence of new ways of cooperation between banks and with their partners, in particular with financial technology start-ups and partially with fintech	monopolization of the banking services market; increased competition from non-banking organizations; high risk of cyber threats that require prompt and timely monitoring, detection, assessment and development of preventive counter-measures; growing number of fraudulent transactions and their constant modification; low levels of financial literacy across the country; fewer bank employees due to job automation
Clients	remote access to financial services 24/7; lower operation cost; broader financial access (the range of potential clients is increasing due to the ability of banks to take on greater risks); personalized service packages for clients; additional services (for example, online payments, budgeting and savings plan); an integrated approach to customer service and an individual package of services; higher security of transactions due to the rapid response of banks to emerging threats	unsolicited additional services by banks; inability to get advice from a bank employee (the need to communicate with a voice assistant); higher responsibility for authorizing financial transactions; the need to improve financial and digital literacy; risk of personal data leaks, including information about the financial status and financial transactions

*Source: compiled by the author

Statistically, the main challenge of digital transformation is the security of banking operations.

According to Sift, a developer of tools for responding to cyber incidents, in 2021 the level of payment fraud attacks in the field of fintech increased by 70% (more than 34 thousand websites and applications were analyzed). Cyberattacks primarily targeted alternative payments such as digital wallets, which saw a 200% increase in payment fraud, as well as on payment service providers (+169%) and on cryptocurrency exchanges (+140%) [Bankovskij sektor …, 2022].

In the Russian Federation, according to the Bank of Russia, the volume of transactions carried out without the consent of customers increased by almost 40% (13.5 billion rubles in 2021 against 9.7 billion rubles a year earlier), and the number of transactions grew by 34% (1035.1 thousand in 2021 vs 773.27 thousand in 2020). For the most part, fraudsters target individuals: more than 99% in terms of the number of transactions and slightly less than 90% in terms of volume. In fact, the average amount transferred without the consent in 2021 for individuals was 11.8 thousand rubles, and for legal entities – 349.6 thousand rubles. The share of recovered funds is not large – 6.8% in 2021 and 11.3% in 2020 [Obzor operacij ..., 2022].

This surge in fraudulent transactions occurs against the backdrop of the actively developing new remote payment services and the growth in the volume of money transfers (+28% over the period under review, to 1,048.4 trillion rubles) using electronic means of payment (card payments and other electronic transactions). Therefore, the share of unauthorized transactions in the total volume of money transfers remains insignificant. In 2021, it amounted to 0.00130%, in 2020 – 0.00120%. These numbers do not exceed the target indicator for the share of such transactions in the total volume of transactions (0.005%), established by the Bank of Russia for payment cards. However, the situation still requires close attention from both credit institutions and the regulator [Obzor operacij ..., 2022]. Figure 8 demonstrates major the channels for fraudulent transactions.

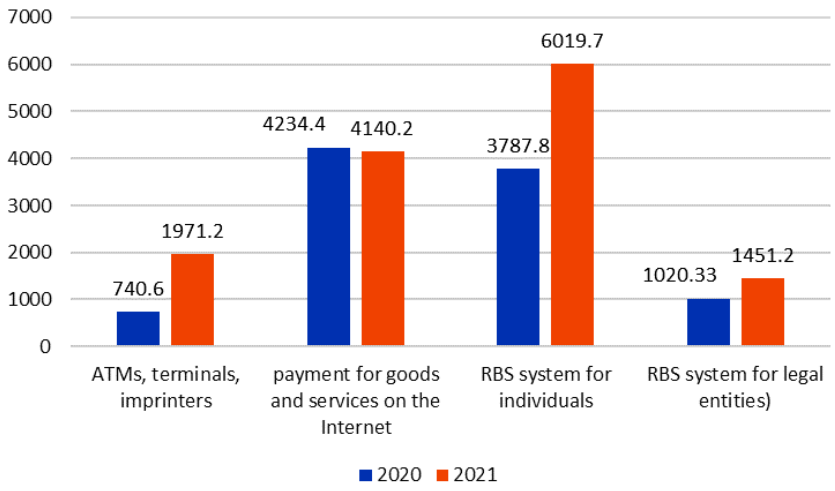


Fig. 8. Distribution of unauthorized transactions according to the methods of their execution

RBS – remote banking service.
Source: [Obzor operacij ..., 2022].

According to Sberbank, attacks are carried out mainly through social engineering methods – they account for 90% of all financial crimes. 94% of that social engineering falls on phone fraud, which has increased dramatically in 2021 compared to 2020 (Fig. 9). And if about 5 years ago in Russia fraudsters called mainly from numbers that began with 8800, in recent years they began to call more often from city numbers [Bankovskij sektor …, 2022].

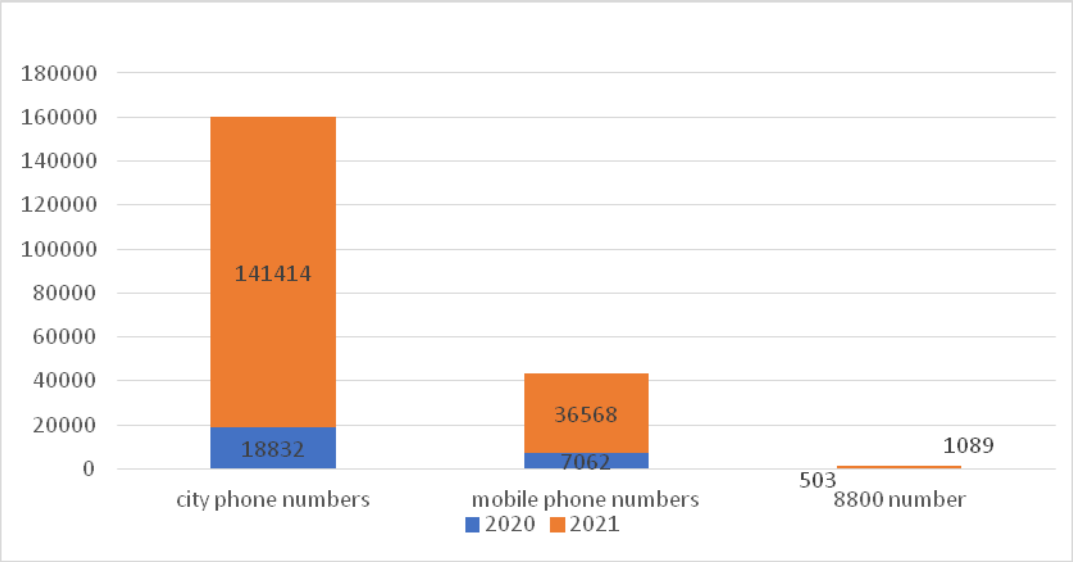


Fig. 9. Statistics of fraudulent phone calls

Source: [Obzor operacij ..., 2022].

Additionally, significant funds are lost via fraudulent websites. Most often (62% of cases) the fake websites of financial organizations are involved (Fig. 10).

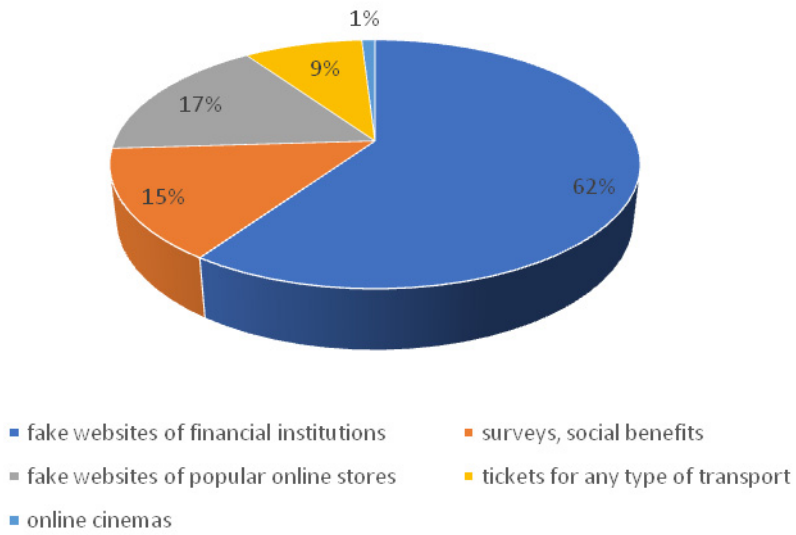


Fig. 10. Types of fraudulent sites

Source: [Obzor operacij ..., 2022].

Banking market experts listed the most relevant challenges for the development of the Russian banking sector in the context of digitalization [Rezul'taty issledovanija ..., 2021, p. 18]:

– lack of formal information exchange on financial fraud: in particular, the need for a unified database on identified fraudulent devices available to all market participants;

– lack of information security requirements for technology companies that provide financial services (fintech, telecom, e-commerce);

– fragmented regulation and lack of unified requirements, as well as a unified interpretation of information security (IS) requirements at the industry level, which leads to high cost of their implementation, threats to information security and regulatory risks.

In addition, significant problems are caused by:

– the lack of legal methods and tools that would allow financial institutions to bring fraudulent cases to court (for example, ineffective interaction with law enforcement and judicial systems), which significantly limits the market's ability to fight crime;

– insufficient level of responsibility for violations in the field of information security.

For the country's digital financial space to develop and function effectively, it is necessary to implement coordinated measures at the level of all its participants, as well as timely proportional regulation. The latter, on the one hand, should maintain the stability of the financial system and protect the rights of consumers, and on the other hand, promote the development and implementation of digital innovations [Sovremennye tendencii ..., 2020].

Conclusion

Digitalization affects all sectors of the economy, including the banking sector. In order to maintain profitable business and retain customers, banks are forced to change in accordance with the speed of changes taking place around them. The introduction of the latest digital technologies, the diversification of services and their transfer to the digital sphere is a necessary condition for banks to maintain their competitiveness.

Digital transformation of the business model is affordable only to popular credit institutions with significant resources and high ratings. The others are forced to use digital services and ecosystems of the leading participants in the banking market, thereby becoming dependent on them, or leave the market.

The digital transformation of the banking sector is fast: both the credit institutions and the services they provide are changing. Traditional banking services are becoming a thing of the past, despite the fact that some customers are not ready to give them up. Digitalization of banking services makes life more comfortable, more convenient, more dynamic. At the same time, consumers (individuals and legal entities) must increase their financial literacy and responsibility for making financial decisions in the changing market conditions.

References

1. Bankovskij sektor chashhe vseh v Rossii podvergaetsja atakam moshennikov – "Sberbank" // Finam. – 2022. – 16.04. – URL: https://www.finam.ru/publications/item/bankovskiiy-sektor-chashe-vsex-v-rossii-podvergaetsya-atakam-moshennikov-sberbank-20220416-100054 (date of access 20.06.2022).
2. Chernyshova E. Chto takoe finteh: otvety na glavnye voprosy // RBK. Trendy. – 2021. – 10.11. – URL: https://trends.rbc.ru/trends/industry/618b6f349a794772fa50adf4 (date of access 20.06.2022).
3. Cvetkov V.Ja., Semushkina S.G. Jelektronnye resursy i jelektronnye uslugi // Sovremennye problemy nauki i obrazovanija. – 2009. – N 6-1. – P. 39–40.
4. Formirovanie cifrovoj jekonomiki v Rossii: sushhnost', osobennosti, tehnicheskaja normalizacija, problemy razvitija / Babkin A.V., Burkal'ceva D.D., Kosten' D.G., Vorob'ev Ju.N. // Nauchno-tehnicheskie vedomosti SPbGPU. Jekonomicheskie nauki. – 2017. – Vol. 10, N 3. – P. 9–25.
5. Golovenchik G. Cifrovye uslugi: ponjatijnyj apparat, klassifikatory // Bankaŭski vesnik, Kastrychnik. – 2021. – N 10(699). – P. 42–55.
6. Homenko E.G. Rol' Banka Rossii v cifrovizacii bankovskoj sistemy // Predprinimatel'stvo i pravo. Informacionno-analiticheskij portal. – 2022. – 10.01. – URL: http://lexandbusiness.ru/view-article.php?id=9839 (date of access 20.06.2022).
7. Kac E. Nevygodnyj biznes: pochemu banki sdajut licenzii // Frank RG. – 2021. – 13.04. – URL: https://frankrg.com/40488 (date of access 20.06.2022).
8. Lebedeva I.A. Cifrovaja transformacija bankovskogo sektora Rossii: vozmozhnosti i riski dlja bankov i ih klientov // Social'nye novacii i social'nye nauki. – 2022. – N 1. – P. 74-85.
9. L'vova N.A. Koncepcija ustojchivogo finansovogo razvitija: priznaki stanovlenija i predposylki dominirovanija // Tehnologicheskaja perspektiva v ramkah Evrazijskogo prostranstva: novye rynki i tochki jekonomicheskogo rosta. Materialy 3-ej Mezhdunarodnoj nauchnoj konferencii /26–28 oktjabrja 2017/ Pod red. k.je.n. M.I. Barabanovoj, k.t.n. A.A. Zajcevoj, prof. V.V. Korableva, prof. O.N. Korablevoj, d.t.n. S.V. Kuleshova, prof. V.V. Trofimova, prof. L.P. Harchenko, prof. Ju.E. Shelepina, prof. E.A. Jakovlevoj, prof. P.P. Jakuceni – SPb: Izdatel'stvo "Asterion", 2017. – 413 p.
10. Makarova I.V., Pavlika A.Ju. Transformacija bankovskogo sektora v uslovijah cifrovizacii jekonomiki Rossii // Bankovskoe delo. – 2022. – 24.01. – URL: https://www.bankdelo.ru/expert-opinion/pub/6301 (date of access 20.06.2022).
11. Obzor operacij, sovershennyh bez soglasija klientov finansovyh organizacij v 2021 godu // Bank Rossii. – 2022. – 11.04. – URL: https://cbr.ru/analytics/ib/operations_survey_2021/ (date of access 20.06.2022).
12. Proekt osnovnyh napravlenij cifrovizacii finansovogo rynka na period 2022–2024 godov // Bank Rossii. – 2021. – 39 p. – URL: https://www.cbr.ru/Content/Document/File/131360/oncfr_2022-2024.pdf (date of access 20.06.2022).
13. Pshenichnikov V.V., Kovtunova E.E. Tradicionnoe bankovskoe obsluzhivanie i jelektronnyj banking: osobennosti i otlichija // Finansovyj vestnik. – 2018. – N 1(40). – P. 68–77.
14. Razvitie finansovyh tehnologij // Bank Rossii. – b/d. – URL: https://www.cbr.ru/fintech/ (date of access 20.06.2022).
15. Rezul'taty issledovanija mnenija rynka po voprosam razvitija finansovyh tehnologij na 2021–2023 gg. // Associacija FinTeh. – 2021. – 31.08. – URL: https://www.fintechru.org/analytics/rezultaty-issledovaniya-mneniya-rynka-po-voprosam-razvitiya-finansovykh-tekhnologiy-na-2021-2023-gg-/ (date of access 20.06.2022).
16. Rynok servisov dlja upravlenija lichnymi finansami v Rossii 2021 // Associacija FinTeh. – 2022. – 21.01. – URL: https://www.fintechru.org/analytics/rynok-servisov-dlya-upravleniya-lichnymi-finansami-v-rossii/ (date of access 20.06.2022).
17. Sovremennye tendencii razvitija denezhnogo i platezhnogo oborota v uslovijah cifrovoj jekonomiki // Finansovyj universitet pri Pravitel'stve Rossijskoj Federacii. Bibliotechno-informacionnyj kompleks. – 2020. – 11.11. – URL: http://library.fa.ru/exhib.asp?id=549 (date of access 20.06.2022).
18. Tihonov V. Skol'ko bankov pokinet rossijskij rynok v 2022 godu // Banki.ru. – 2022. – 02.02. – URL: https://www.banki.ru/news/daytheme/?id=10960367 (date of access 20.06.2022).
19. Kagan Ju. Financial Technology – Fintech // Investopedia. – 2020. – 27.08. – URL: https://www.investopedia.com/terms/f/fintech.asp (date of access 20.06.2022).
20. McIntyre A., Skan Ju. Caterpillars, butterflies, and unicorns. Does digital leadership in banking really matter? // Accenture. – 2019. – URL: https://www.accenture.com/_acnmedia/pdf-102/accenture-banking-does-digital-leadership-matter.pdf (date of access 20.06.2022).

The manuscript was received on 20.06.2022.

CENTRAL BANK DIGITAL CURRENCIES: PRINCIPLES, POTENTIAL AND CHALLENGES

Galina Semeko

PhD (Econ. Sci.), Leading Researcher of the Department of Economics, Institute of Scientific Information for Social Sciences, Russian Academy of Sciences (INION RAN), Moscow, Russia

E-mail: cemeko@mail.ru

Abstract. *The article discusses a new digital form of money intended for use as legal tender. The prerequisites for the digitalization of money and the concept of the Central Bank digital currency are discussed. Digital currency is considered in terms of the payment efficiency, ensuring liquidity and financial stability. It is noted that at present most countries are exploring the possibility of issuing a central bank digital currency, developing its concept or have already begun to implement pilot projects.*

Keywords: *digitalization of money; digital currencies; central bank digital currency; international practice.*

For citation: Semeko G.V. Central Bank Digital Currencies: Principles, Potential and Challenges / English transl. by Nikulichev M.Y. // Social Novelties and Social Sciences. – Moscow : INION RAN, 2022. – N 1. – P. 49–62.

URL: https://sns-journal.ru/en/archive/ DOI: 10.31249/snsneng/2022.01.04

Introduction

In recent years, the world academic community, central banks and international organizations (Bank for International Settlements, International Monetary Fund, European Central Bank, etc.) have been actively discussing the issuing of sovereign digital currencies by central banks. The increased interest in the central bank digital currency (CBDC) reflects significant changes in the economy and monetary circulation due to digitalization.

Currently, CBDC is the key innovation in the field of money circulation. According to the well-known American economist N. Roubini, the discussion and implementation of CBDC is long overdue: the "digital game with currencies" in the world market is gaining momentum, and the state cannot stand aside. Otherwise, it risks losing its leverage in managing cash and payment transactions, which is fraught with huge negative consequences for financial stability [Roubini, 2018].

Digital payments are a major battlefield between high-tech companies, payment service providers and banks that are looking to take the lead in the emerging digital platform economy. In China, Alipay and WeChat Pay already control over 90% of all mobile payments. In recent years the four largest listed payment firms – Visa, Mastercard, Amex and PayPal – have increased in value by more than the world's five technology leaders – Facebook, Amazon, Apple, Netflix and Google [Steenis van, 2019].

The rapid pace and sheer scale of innovation in digital currencies and mobile payments, says Huw van Steenis, a former senior adviser to Bank of England Governor, indicates that a monetary revolution is forthcoming. The choice for governments and central banks is whether "to stand in front of a train that is gaining steam or get on board and reap the benefits" [Steenis van, 2019].

The purpose of this article is to study one of the most significant innovations in the field of monetary circulation in the context of digital economy – a sovereign digital currency issued by a central bank and intended for use as legal tender.

Research methodology (theoretical basis)

Since the studied financial innovation is currently at the initial stage of implementation, the main attention of experts and the academic community is focused on the theoretical aspects underlying it. For this reason, the theoretical approaches and conclusions by Russian and foreign experts, by international financial organizations, in particular the Bank for International Settlements and the International Monetary Fund, and the central banks of foreign countries with on-going CBDC projects, were studied.

The study is methodologically based on the neo-institutional approach focused on the study of a formal institution – a new form of money, as well as institutional conditions for its development. The article uses a set of general scientific research methods and analytical procedures: generalization, description, systematization, comparative analysis of domestic and foreign studies and documents.

Research results

Prerequisites for the transformation of the monetary system

The most important factor contributing to the emergence of the CBDC is the fast implementation of digital financial technologies, which have affected, in particular, payment transactions. New digital technologies are able to satisfy consumer demands for fast, simple, efficient, public and secure payment services. Digital payment instruments (card payment systems, e-wallets, contactless payments, QR code payments, etc.) allow to manage money anywhere and anytime, make payments, transfers, etc. Of great importance is also the fact that digital financial technologies help reduce transaction costs.

Digitalization of payments has significantly accelerated the shift to non-cash transactions, the tendency that has been observed for a long time. The digitization of credit and debit card transactions and the development of banking applications have moved many traditional cash transactions into the digital space. Further profound changes in payment methods, limiting the use of cash, are associated with the development of Internet banking and mobile banking, SMS banking, non-bank mobile services, instant payment systems, etc.

As a result of digitalization, the stock of cash in circulation is rapidly declining, while the share of non-cash money is increasing. To date, the bulk of the money in circulation falls on non-cash money (or electronic money)[1]. Cashless payments are growing in popularity all over the world. Cash is used less and less and has almost disappeared in countries such as Sweden and China. In Sweden, cash payments have fallen by 80% over the past decade [Steenis van, 2019]. In Russia, according to the Bank of Russia, over the past five years, the share of non-cash retail payments has grown from 39 to 70% [Rubl' prevrashhaetsja v ..., 2020, p. 13]. At the same time, digital payment systems – PayPal, Venmo and others in Western countries, Alipay and WeChat in China, M-Pesa in Kenya, Paytm in India – offer attractive alternative payment services to traditional services in commercial banks. The cash servicing costs are growing rapidly as people move to non-cash payments. The falling demand for cash creates the risk of weakening the influence of the central bank on money circulation and reducing the effectiveness of its monetary policy.

[1] Cash is issued in the form of banknotes with unique numbers; non-cash money exists as records in accounts with the central bank and commercial banks. The introduction of modern account management technologies has led to the transfer of non-cash money into electronic form.

Another important consequence of digitalization was the emergence of private digital currencies – cryptocurrencies that can perform certain functions of money (means of payment, payment system, technical unit for mutual settlements, blockchain platform, capital raising tool), and also be used as an investment asset[1] [Perspektivy kriptovaljut v ..., 2020][2]. Their rapid growth causes fair concerns among regulators due to the high volatility of exchange rates, vulnerability to cyber-attacks, the lack of a legislative framework and guarantees to compensate for damages and losses, the risks of closing cryptocurrency exchanges, etc. [Agur, 2018; Yanagawa and Yamakoa, 2019].

Some risks of cryptocurrencies can be reduced by issuing so-called stablecoins, i.e. cryptocurrencies that are tied to real or financial assets – fiat currencies (recognized and guaranteed by the state) or physical commodities (gold, oil). Their rates are less liable to fluctuations compared to typical cryptocurrencies. However, according to experts, such reduction of volatility risk is often very limited, if it is found at all [Berentsen, Schär, 2019]. In addition, the release of stablecoins intended for circulation on the world market generates specific risks associated with money laundering and terrorist financing, undermining financial stability, threat to monetary sovereignty, etc.

In 2019, the most popular social network platform Facebook (about 2 million users per day) made an attempt to issue its own cryptocurrency. This was a turning point in promoting the idea of CBDC[3]. The realization that such large-scale cryptocurrency projects can lead to a loss of control over monetary policy and pose a threat to the monetary sovereignty of countries has contributed to a change in the position of many central banks regarding CBDC. A few months later, in January 2020, officials from a number of central banks (UK, Japan, Sweden, Canada, Switzerland), the European Central Bank and the Bank for International Settlements (BIS) met to discuss sovereign digital currency issues. As a result, a working group was created with the task to study the experience and potential of CBDC ("Group of Seven")[4].

Most central banks in the world are currently actively exploring CBDC despite the COVID-19 pandemic. Many central banks are moving from research to practical experimentation. The Bank of Russia is also working in this direction – a concept for issuing a retail CBDC and a prototype of digital ruble have been developed (testing of the digital ruble platform began in January 2022).

---

[1] The market capitalization of all stablecoins in 2019 was approximately $2.7 billion (i.e. 2.2% of the total market capitalization of all cryptoassets). The largest stablecoin Tether, whose rate is pegged to the dollar in a 1:1 ratio, has a market capitalization of about $2 billion [The Economics of Fintech …, 2019, p. 66]

[2] According to the website CoinMarketCap, as of December 22, 2021, there were 8457 cryptocurrencies registered in the world. Of these, 89 had a market capitalization of more than $1 trillion, 1843 cryptocurrencies had a market capitalization of more than $1 billion [Today's Cryptocurrency Prices …, 2021].

[3] Facebook had to abandon the Libra project due to disagreements with the regulators of the G7 countries, who demanded that the project be stopped to assess its consequences; Russia also opposed the project. The second attempt to issue a Diem digital currency (this time as stablecoin), which is pegged to the US dollar, was made at the end of 2021.

[4] In October 2020, the G7 finance officials released a report with a comprehensive analysis of the main principles, characteristics, design, technologies, risks of using CBDC, etc. [Central bank digital currencies: Foundational …, 2020].

The digitalization of payments and money, the reduction in the use of cash, the growing market of cryptocurrencies, which are a serious competition with the traditional currencies, justify the need to adapt the monetary system to the ongoing changes and to create a currency that can replace or supplement cash that is going out of circulation.

The main provisions of the CBDC concept

CBDC is not a well-defined term. This is partly due to the fact that the CBDC concept combines several important aspects, both technical (computer science, cryptography, etc.), and economic and financial (monetary circulation, banking, payment systems, monetary policy, etc.)[1].

Most often, regulators and experts take as a basis the definition by the BIS and the International Monetary Fund (IMF):

1) BIS: CBDC is a digital form of central bank money, i.e. a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value [Central bank digital currencies, 2018, p. 3–4];

2) IMF: CBF is a new form of money issued digitally by a central bank and intended for use as legal tender [Mancini-Grifoli, Martinez, 2018, p. 7].

In many publications, such fairly general definitions are supplemented by characteristics that describe in more detail the CBDC properties and potential. Thus, the definition of the Bank of England focuses on the availability of CBDC for both households and companies, which can create new opportunities for payments and for the central bank to maintain monetary and financial stability [Central bank digital currency opportunities …, 2020, p. 7; Broadening narrow money…, 2018, p. 4]. Bank of France experts emphasize that CBDC is part of the monetary base along with fiat currency and reserves, and can only be issued and withdrawn from circulation by the central bank [La monnaie digitale …, 2020, p. 4]. In addition, CBDC, unlike private digital currencies (cryptocurrencies), is a direct liability of the central bank and, therefore, a risk-free asset [Central bank digital currencies: Foundational …, 2020, p. 3].

The main motivation for central banks to study and develop CBDC the opportunity of using it as a means of payment. In addition, there are other arguments, and they differ for advanced economies (AEs), on the one hand, and for emerging market economies (EMEs) and developing economies (DEs), on the other [Central bank digital currencies: Foundational …, 2020, p. 5–7; Tobias, Mancini-Grifoli, 2019]:

– *Permanent access of households and companies to central bank money*. This argument is important because in jurisdictions where the use of cash is declining, there is a risk of restricting access to risk-free central bank money;

[1] The technical aspects of the design and operation of CBDC are not discussed in this article.

– *Stability of the monetary system*. CBDC can be a reserve means of payment in the event when, for whatever reason, the work of electronic payments is disrupted, i.e. the operational stability of payment systems is growing;

– *Diversification of payment options*. Since network effects (scale effects) provide additional benefits and revenues, payment systems tend to monopolize or fragment the payment services market. This creates barriers for new providers to enter the market, increases the user costs of payments and complicates the interaction between individual payment systems;

– *Promoting financial inclusion*. Digitalization creates additional barriers to access to financial services related to digital literacy, access to information technology and data privacy issues, etc. This limits the opportunities for financial inclusion of population groups not involved in financial transactions. This problem is especially acute in the EMEs and DEs, where a high "digital gap" remains between the population with different income levels. For the central banks of many countries in this group, CBDC allows for greater access to financial services for disadvantaged population groups (if they have mobile phones);

– *Improved cross-border payments*. Cross-border payments are inherently more complex than purely domestic payments. They involve a larger number of players located in different time zones and jurisdictions with different rules and regulations for conducting payment transactions. As a result, cross-border payments require more time and commission costs, and are less transparent. CBDC can facilitate transnational payments, to reduce time for their execution and the cost of transactions. In this case, it is important to ensure CBDC interoperability in countries participating in the settlements;

– *Support for the anonymity of payments (confidentiality)*. One of the main characteristics of cash is the lack of centralized accounting of transaction data, which leads to the highest level of anonymity of payments. On the contrary, the electronic payments have the lowest level of anonymity. According to experts, CBDC, which was created on the basis of tokens, similar to private digital currencies, can increase the level of anonymity of electronic payments. However, in this case, complete anonymity of payment transactions in relation to the central bank is also impossible, given that the data on transactions are recorded in the centralized data base (register) of the regulator. However, a reasonable compromise could be to restrict access to transaction data, opening it only at the request of the central bank and law enforcement agencies [Perspektivy kriptovaljut v …, 2020, p. 52];

– *Assisting budgetary transfers*. The COVID-19 pandemic has clearly shown the importance of efficient payment systems for rapid money transfers to the public and businesses in times of crisis. Such payments can be accomplished using CBDC-based payment system with registered users. This system can increase the efficiency of money transfers, but it must be tied to the digital identity system [Central bank digital currencies: Foundational …, 2020, p. 5–7].

The potential benefits and risks of a CBDC-based payment system depend on the design of the currency. Key characteristics of CBDC design are following: its accessibility (i.e. determining who and under what conditions will have access to it) and the technology for storing transaction data.

Depending on the users who have access to the sovereign digital currency, two options are being considered – retail and wholesale CBDC. If the retail CBDC (it is also called public) is available to a wide range of users, including individuals and non-financial institutions, then the wholesale CBDC is available only to a limited number of users – financial and money market participants (credit and financial institutions, payment operators, etc.). In terms of data storage technology, account-based CBDC and token-based CBCB are distinguished.

Retail CBDC, being a direct liability of the central bank to the holder, has the same advantages as cash and, unlike non-cash (electronic) money, is a completely liquid and safe payment instrument. In the event of a significant reduction in the use of cash, a retail CBDC could compensate for the lack of liquidity.

A retail CBDC, provided it is reasonably easy to access (for example, via a mobile application), can also serve as a tool to expand the circle of people engaged in financial transactions and using financial services. Consumers who, for various reasons, refrained from online payments (fear of scammers, data theft, etc.) will be able to do this safely with the help of CBDC, since their transaction data will be centralized in the regulator's register and will not be used for commercial purposes. A retail CBDC might reduce the possibility of errors, losses or theft in payment transactions.

The main economic problem for cash is the high cost of managing cash transactions. In some countries, the cost of managing money is very high due to the vast territory or the presence of remote areas, including small islands. The CBDC can reduce the costs associated with providing all regions with means of payment [Tobias, Mancini-Grifoli, 2019]. According to Fédération Bancaire Française, the cost of servicing cash in the banking sector is about 2 billion euros annually [La monnaie digitale …, 2020, p. 5–6]. According to experts, the management of the CBDC turnover will be cheaper for both the central bank and the banking sector.

Apparently, retail CBDC will be attractive to retailers some merchants if the central bank waives transaction fees. According to the calculations of Canadian experts, the retail CBDC may become the least expensive settlement method in this sector. Currently for Canadian retailers, cash has the lowest costs of all payment methods for transactions values up to $20, while accepting debit cards is the least expensive for transactions greater than $20 [Engert, Fung, 2017, p. 13].

In the current financial environment, retail CBDC will probably be less expensive payment method for consumers than cash. In particular, it will save time for visiting a cashpoint, withdrawing cash and making cash payments.

However, according to a study by the Bundesbank (Germany), the average duration of a cash payment was 22.3 seconds, which is 7 seconds longer than the duration of a card and PIN payment (on average 29.4 seconds) [Cabinakova, Knüman, Horst, 2019, S. 32]. Nonetheless, retail CBDC, given the terms of the initialization of the payment, is likely to reduce this time if it is stored on a bank card or in a mobile application. Since authentication / authorization is inherently time-consuming procedure, the token-based retail CBDC model will be more efficient in terms of speed than the account-based CBDC model. In this case, the token replaces the payment card number and allows to very quickly verify the transaction validity; while the technology provides a higher level of operation security.

In addition to being a means of payment, a medium of exchange and a measure of value, retail CBDC may also become a mean of savings equivalent to other forms of money. This is possible if the currency design provides for the accrual of interest on the CBDC account. Additionally, from a technical point of view, retail CBDC will be more convenient for savings compared to monetary counterparts (cash, bank accounts).

Depending on the structure of interaction between the central bank and customers, three models of the payment system based on retail CBDC are considered – direct, indirect and hybrid.

The direct (single-tier) model is the most radical departure from the existing system: the central bank handles payments without intermediaries and maintains records of all transactions. As a result, the central bank server participates in all payments, which requires a strong technological infrastructure. The Central Bank is fully responsible to consumers. It has all the information about account balances and can easily increase or decrease the amount of liquidity, and therefore such a payment system is very stable.

In the indirect CBDC model, the consumer has a claim on an intermediary bank, with the central bank keeping track only of wholesale accounts. This model is based on distributed ledger technology. The central bank transfers the CBDC-token to an intermediary – payment service provider, for instance, a commercial bank or non-banking financial institution (such as a fintech), which distributes the currency and maintains a ledger of transactions. The responsibility to consumers in this case lies entirely with the intermediary. For this reason, in the event a private payment service provider goes insolvent, the claims of its creditors will be transferred to the CBDC assets of consumers.

In a hybrid (two-tier) CBDC model, the central bank issues a digital currency and distributes it through intermediaries (this can be any bank or other financial institution). Digital currency is the central bank's liability to retail consumers. All CBDC transactions are performed on a digital platform managed by the Central Bank. Experts consider this model the most promising because it combines the security of a central bank's liability to consumers with the convenience of private sector payment services. In this case, if the private payment service providers are insolvent, CBDC assets of consumers will not be subject to the claims of creditors [Auer, Böhme, CBDC architectures …, 2020].

The direct model of the payment system was chosen by the central banks of the Bahamas, China, Canada, Sweden, Brazil, Great Britain, etc. The European Central Bank and Russia preferred the hybrid model.

Wholesale CBDC, the digital analogue of "money for banks", is an asset whose value is equivalent to the value of other forms of money, and therefore does not carry any liquidity or credit risk (unlike stablecoins) and can be transferred using blockchain technology [La monnaie digitale ..., 2020]. Researchers note the fact that wholesale CBDC is very close to the existing non-cash money [Saharov, 2021, p. 137]. In terms of its economic potential, wholesale CBDC "should not differ significantly from the existing central bank reserves"; the difference lies only in the technical implementation of settlements using CBDC [Kiselev, 2019, p. 10–11].

The circulation of wholesale CBDC can be based on distributed ledger technology (DLT), in particular on private and public blockchain networks. Thus, it will be a currency in the form of digital tokens, private or public.

Wholesale CBDC can be used for securities settlements, cross-border settlements and in transactions with various financial instruments, such as tokenized assets, the value of which is pegged to the rate of real assets (stocks, bonds, stock indices, commodities, cryptocurrencies, etc.).

Experts believe that the main potential benefits of wholesale CBDC include higher efficiency of existing wholesale payment systems caused by lower costs and settlement time as well better traceability and security of transactions etc. However, similar to the existing wholesale payment systems, wholesale CBDC payment systems are subject to the same risks inherent in financial transactions (credit, settlement, operational risks) [Perspektivy kriptovaljut v ..., 2020, p. 63–64].

For market participants it is also important that wholesale CBDC does not fundamentally reform the existing decentralized financial infrastructure but creates opportunities for modernization: in particular, wholesale CBDC issued on distributed ledger technology (blockchain technology) provides protection against "disorderly tokenization of the financial infrastructure" [La monnaie digitale …, 2020, p. 12].

The issue of CBDC, both retail and wholesale, has great potential in terms of ensuring the monetary sovereignty of the issuing countries in the field of payment transactions. The issuance of a sovereign currency in a digital format can protect DEs with insufficient development of the banking sector (however, possessing modern means of communication such as smartphones) from the "invasion" of foreign payment providers and cryptocurrencies that are taking over the whole world, and will allow maintaining control over the payment market [Investigating the impact …, 2019]. The problem of sovereignty in the area of payments is relevant even for the EU countries, where a significant part of the payment market is controlled by foreign providers, such as VISA and MasterCard, Google Payment, as well as international

Internet giants, such as the five American big techs GAFAM[1] or the four Chinese BATX[2] [La monnaie digitale ..., 2020].

International experience in creating sovereign digital currencies

In 2020, BIS studied attitudes to CBDC around the world and noted that a growing number of central bank governors and board members have made public speeches about CBDCs. In 2017 and 2018, many of these had a negative or dismissive stance, particularly toward retail CBDCs. Since late 2018, the number of positive mentions of retail and wholesale CBDCs in speeches has risen, and in fact there have now been more speeches with a positive than a negative stance. [Auer, Cornelli, Frost, 2020, p. 8].

At the same time, since 2016, there has been an increase in the number of studies and pilot CBDC projects. Such projects were launched by the central banks of Canada (2016), Singapore (Monetary Authority of Singapore, MAS, 2016), Hong Kong (Hong Kong Monetary Authority, HKMA, 2017), European Central Bank (Stella project, 2017), Central Bank of Sweden (Sveriges Riksbank, 2017), as well as the Eastern Caribbean Central Bank (Eastern Caribbean Central Bank, 2019) – the central bank of the eight island states of the Caribbean that are members of the Eastern Caribbean Currency Union (Eastern Caribbean Currency Union). Monetary authorities of Saudi Arabia and the United Arab Republic, Hong Kong and Thailand announced cross-border work on wholesale CBDCs (2019) [Auer, Cornelli, Frost, 2020, p. 4].

As of mid-2021, at least 56 central banks have published studies related to the issuance of retail or wholesale CBDC. Three countries (Ecuador, Ukraine and Uruguay) have completed pilot projects for retail CBDC. Eight retail CBDC pilot projects are currently underway, including in China, South Korea and Sweden. 40 central banks have published research on retail CBDC and 19 have announced research or development on wholesale CBDC (in some cases in addition to retail CBDC) [Central bank digital currencies: Motives …, 2021, p. 9].

In recent years, BIS has been regularly polling central banks about their engagement in CBDC work, their motivations and their intentions regarding CBDC issuance [Boar, Wehrli, 2021]. The survey conducted in late 2020 among 65 central banks outlined how far countries have progressed towards creating a new digital currency, their motivation and plans for the future as well as their views on legal frameworks for CBDCs and their assessment of the use of cryptocurrencies and stablecoins in their jurisdictions.

The 2020 survey is highly representative: 65 participating countries represent 72% of the world's population and 91% of global economic output, including 21 central banks in advanced economies (AEs)

[1] Google, Apple, Facebook, Amazon and Microsoft.
[2] Baidu, Alibaba, Tencent and Xiaomi.

and 44 in emerging market and developing economies (EMDEs), including Russia [Boar, Wehrli, 2021, p. 5].

The results of the survey testify to the increased interest of central banks in CBDC. Thus, the share of central banks (among those surveyed) that are actively involved in CBDC research in one form or another reached 86% in 2020 against 65% in 2017 [Boar, Wehrli, 2021, p. 6]. Studies related to retail CBDC are relatively more popular, although central banks are considering both forms of CBDC – retail and wholesale. Central banks that do not take any steps towards CBDC are mostly small jurisdictions. Jurisdictions with a high level of development of mobile communications and the Internet, and with significant innovation capacity have advanced the furthest in the CBDC work.

In the process of CBDC engagement, central banks go through several stages – from conceptual research to experimentation. In 2020, about 60% of central banks (up from 42% in 2019) were conducting experiments or proofs-of-concept, while 14% were moving forward to development and pilot arrangements [Boar, Wehrli, 2021, p. 6].

Central banks mostly focused on retail CBDC (about 40% of respondents give priority to retail and only 10% to wholesale). Moreover, over the past four years, the number of central banks focused on retail CBDC has grown, while the interest in wholesale CBDC has decreased [Boar, Wehrli, 2021, p. 6].

Although the idea of issuing CBDC is gaining popularity, according to BIS experts, most central banks are unlikely to issue any type of CBDC in the foreseeable future [Boar, Wehrli, 2021, p. 11]. There are serious reasons for such a conclusion: for example, far from all projects of issuing CBDCs ended successfully. In particular, such projects were closed in Ecuador, Venezuela, Tunisia, Denmark and a number of other countries [Today's Central Bank …, 2021].

The first fully implemented digital version of a payment system based on the retail CBDC was launched in 2020 in the Bahamas. Sand Dollar is pegged to the Bahamian dollar, BSD (and it, in turn, to the US dollar) [Sand Dollar is on schedule …, 2020]. Apart from the Bahamas, as of December 2021, according to the CBDC tracker website (https://cbdctracker.org/), the digital version of the sovereign currency was launched in 2021 by the Central Bank of Nigeria [Ree, 2021].

In 2021, 12 countries launched pilot projects to test digital currencies (including China, France, Canada, South Africa, the United Arab Emirates, Singapore, etc.). Ten countries are at the proof-of-concept stage, and 61 countries at the research stage [Today's Central Bank …, 2021].

Conclusion

It is obvious that discussions around CBDCs will continue in the coming years and will probably intensify. As is the case with any technological innovation, the creation of CBDC requires careful evaluation of pros and cons, the intended consequences, as well as analysis of the first successful and unsuccessful experience. According to N. Roubini, "... the transition to digital currencies is only a matter of time ...

central banks will introduce digital currencies slowly and gradually and learn from each other's experience" [Titova, 2021].

Although the implementation of CBDC projects in the world has just begun, it is already possible to make certain generalizations about their features, possibilities and consequences:

– interest in CBDC is global in nature, but the motives for issuing this currency are determined by national conditions;

– availability of financial services remains the key motivation for issuing CBDCs in the EMDCs; AEs are more interested in improving the efficiency and security of payments;

– it is most likely that in the near future, along with traditional currencies, various digital currencies will be in circulation, including both sovereign digital currencies based on accounts and tokens, as well as cryptocurrencies and stablecoins;

– transition to CBDC will have a positive impact on money circulation and financial stability, as it will allow to resist the expansion of the cryptocurrency market;

– creation of CBDC network will help optimize not only domestic, but also cross-border payments;

– in many cases, the turnover of the CBDC will be based on partnerships between the public and private sectors, for example, if a hybrid model of the payment system is adopted;

– companies should prepare for much greater state control and oversight of their business, because with introduction of CBDC, the regulator and government agencies will receive powerful tools to manage money circulation and payment systems;

– as consumer interest in CBDC rises, there will be an opportunity to expand agreements between the private sector and central banks. This process may involve regulatory sandboxes and innovation hubs created by central banks or other financial institutions;

– consumer concerns about data privacy may be offset by the potential benefits of CBDC. This implies raising the profile of the relationship between law, technology and finance in public policy and practice [Boar, Wehrli, 2021; Central bank digital currencies and the future…, 2021; Schueffel, 2021; Unlocking…, 2021; Titova, 2021].

In conclusion, it should be noted that introduction of CBDC, like any financial innovation, is associated with both benefits and risks. This must be taken into account when developing the concept and implementing relevant projects.

References

1. Kiselev A. Est' li budushhee u cifrovyh valjut central'nyh bankov? Analiticheskaja zapiska. – Moskva : Bank Rossii, 2019. – 23 p.
2. Perspektivy kriptovaljut v sovremennyh jekonomikah / P. Trunin, A. Levashenko, E. Sinel'nikova-Muryleva, I. Ermohin, K. Shilov, M. Girich. – Moskva : RANHiGS, 2020. – 72 p. – (Nauchnye doklady: Jekonomika, 2020 ; № 4). – URL: http://delo.ranepa.ru/shop/elektronnye-knigi/perspektivy-kriptovalyut-v-sovremennyh-ekonomikah/ (date of access 16.02.2022).

3. Rubl' prevrashhaetsja v cifru: zachem Rossii nuzhna cifrovaja valjuta // Kommersant. – 2020. – 02.12, N 221. – P. 13. – URL: https://www.kommersant.ru/doc/4566287 (date of access 16.02.2022).
4. Saharov D.M. Cifrovye valjuty central'nyh bankov: kljuchevye harakteristiki i vlijanie na finansovuju sistemu // Finansy: teorija i praktika. – Moskva, 2021. – Vol. 25, N 5. – P. 133–149.
5. Titova I. Jekonomist Nurijel' Rubini – Forbes: "Krizis mozhet sluchit'sja v blizhajshie 3–5 let" // Forbes. – 2021. – 02.10. – URL: https://www.forbes.ru/biznes/441631-ekonomist-nuriel-rubini-forbes-krizis-mozet-slucit-sa-v-blizajsie-3-5-let (date of access 16.02.2022).
6. Agur I. Central bank digital currencies: An overview of pros and cons. // SUERF: Do we need central bank digital currency? Economics, technology and institutions / E. Gnan, D. Masciandaro (ed.). – Vienna, 2018. – 149 p. – P. 116–117. – (SUERF Conference Proceedings 2018/2). – URL: https://www.suerf.org/docx/s_cf0d02ec99e61a64137b8a2c3b03e030_7025_suerf.pdf (date of access 16.02.2022).
7. Auer R., Böhme R. CBDC architectures, the financial system, and the central bank of the future // VOXeu/CEPR. – 2020. – 29.10. – URL: https://voxeu.org/article/cbdc-architectures-financial-system-and-central-bank-future (date of access 16.02.2022).
8. Auer R., Böhme R. The technology of retail central bank digital currency // BIS Quarterly Rev. – Basel, 2020. – March. – P. 1–16. – URL: https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf (date of access 16.02.2022).
9. Auer R., Cornelli G., Frost J. Rise of the central bank digital currencies: Drivers, approaches and technologies. – 2020. – 44 p. – (BIS Working Papers ; N 880). – URL: https://www.bis.org/publ/work880.pdf (date of access 16.02.2022).
10. Berentsen A., Schär F. Stablecoins: The quest for a low volatility cryptocurrency // The economics of fintech and digital currencies / édité par A. Fatás. – London : A VoxEU.org Book, CEPR Press, 2019. – P. 65–75. – URL: https://voxeu.org/content/economics-fintech-and-digital-currencies (date of access 16.02.2022).
11. Boar C., Wehrli A. Ready, steady, go? Results of the third BIS survey on central bank digital currency. – Basel : BIS, 2021. – 23 p. – (BIS Papers ; N 114). – URL: https://www.bis.org/publ/bppdf/bispap114.pdf (date of access 16.02.2022).
12. Broadening narrow money: Monetary policy with a central bank digital currency / Meaning J., Dyson B., Barker J., Clayton E. – 2018. – 36 p. – (Working paper of Bank of England ; N 724). – URL: https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2018/broadening-narrow-money-monetary-policy-with-a-central-bank-digital-currency.pdf?la=en&hash=26851CF9F5C49C9CDBA95561581EF8B4A8AFFA52 (date of access 16.02.2022).
13. Cabinakova J., Knüman F., Horst F. Kosten der Bargeldzahlung im Einzelhandel. – Frankfurt a. Main : Deutsche Bundesbank, 2019. – 61 S. – URL: https://www.bundesbank.de/resource/blob/776464/16e3a025236aa4d52f1b2c0a27e1b852/mL/kosten-der-bargeldzahlung-im-einzelhandel-data.pdf (date of access 16.02.2022).
14. Central bank digital currencies and the future of money. – London : PwC, 2021. – June. – 10 p. – URL: https://www.pwc.com/m1/en/media-centre/2021/documents/central-bank-digital-currencies-and-the-future-of-money-part1.pdf (date of access 16.02.2022).
15. Central bank digital currencies. – Basel : Bank of international settlements, CPMI, 2018. – March. – 34 p. – URL: https://www.bis.org/cpmi/publ/d174.pdf (date of access 16.02.2022).
16. Central bank digital currencies: Foundational principles and core features / Group of Central Banks, Joint Report N 1. – Basel : BIS, 2020. – October. – 26 p. – URL: https://www.bis.org/publ/othp33.pdf (date of access 16.02.2022).
17. Central bank digital currencies: Motives, economic implications and the research frontier / Auer R., Frost J., Gambacorta L., Monnet C., Rice T., Hyun Song Shin. – 2021. – November. – 30 p. – (BIS Working Papers ; N 976). – URL: https://www.bis.org/publ/work976.pdf (date of access 16.02.2022).
18. Central bank digital currency opportunities, challenges and design. – 2020. – March. – 57 p. – (Discussion paper of Bank of England). – URL: https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593 (date of access 16.02.2022).
19. Engert W., Fung B. Central bank digital currency: Motivations and implications. – 2017. – 30 p. – (Bank of Canada Staff Discussion Paper ; N° 2017–16). – URL: https://www.bankofcanada.ca/wp-content/uploads/2017/11/sdp2017-16.pdf (date of access 16.02.2022).
20. Esselink H., Hernandez L. Study on the use of cash by households in the euro area. – 2017. – 71 p. – (ECB occasional paper series ; N°201). – URL: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op201.en.pdf (date of access 16.02.2022).
21. Investigating the impact of global stablecoins. – Basel : BIS, Group of seven working group on stablecoins, CPMI, 2019. – 37 p. – URL: https://www.bis.org/cpmi/publ/d187.htm (date of access 16.02.2022).
22. La monnaie digitale de banque centrale. – Paris : Banque de France, 2020. – 08.01. – 52 p. – URL: https://publications. banque-france.fr/sites/default/files/media/2020/01/14/la_monnaie_digitale_de_banque_centrale.pdf (date of access 16.02.2022).
23. Mai H. Why would we use crypto euros? Central bank-issued digital cash – a user perspective // Deutsche Bank Research: EU Monitor Global financial markets. – Frankfurt a. Main, 2018. – S. 1–16 – URL: https://www.dbresearch.com/PROD/RPS_DE-PROD/PROD0000000000462095/Why_would_we_use_crypto_euros%3F_Central_bank-issued.PDF?undefined&realload=dlAJZnNGFk4U4fKONK1TRGVe1dgP/UDcdmqJ0~YCdxpkZUG1/RLjHIDU3opNEWp7 (date of access 16.02.2022).
24. Mancini-Grifoli T., Martinez M. S. Casting light on Central Bank. – 2018. – 39 p. – (IMF Staf Discussion Note ; N 8). – URL: file:///C:/Users/cemek/AppData/Local/Temp/SDN1808.pdf (date of access 16.02.2022).

25. Ree J. Five Observations on Nigeria's Central Bank Digital Currency // IMF Country Focus. – 2021. – 16.11. – URL: https://www.imf.org/en/News/Articles/2021/11/15/na111621-five-observations-on-nigerias-central-bank-digital-currency (date of access 16.02.2022).
26. Roubini N. Why central bank digital currencies will destroy bitcoin // The Guardian. – 2018. – 19.10. – URL: https://www.theguardian.com/business/2018/nov/19/why-central-bank-digital-currencies-will-destroy-bitcoin (date of access 16.02.2022).
27. Sand Dollar: For establishing the first government-backed digital currency // Most influential projects 2021: 50 most influential projects. Project management institute. – URL: https://www.pmi.org/most-influential-projects-2021/50-most-influential-projects-2021/sand-dollar (date of access 16.02.2022).
28. Schueffel P. Central bank digital currency (CBDC) – digital money for our central banks: What is it and why should I care as a business owner and consumer? // More than digital. – 2021. – 25.02. – URL: https://morethandigital.info/en/central-bank-digital-currency-cbdc-digital-money-for-our-central-banks/ (date of access 16.02.2022).
29. Steenis van H. The digital money revolution // Project-syndicate. – 2019. – 13.11. – URL: https://www.project-syndicate.org/commentary/digital-money-payments-revolution-by-huw-van-steenis-2019-11?a_la=english&a_d=5dcbe13a44cb701da84bc4b9&a_m=&a_a=click&a_s=&a_p=%2Farchive&a_li=digital-money-payments-revolution-by-huw-van-steenis-2019-11&a_pa=archive-results&a_ps=&a_ms=&a_r=&barrier=accesspaylog (date of access 16.02.2022).
30. The economics of fintech and digital currencies / édité par A. Fatás. – London : A VoxEU.org Book, CEPR Press, 2019. – 108 p. – URL: https://voxeu.org/content/economics-fintech-and-digital-currencies (date of access 16.02.2022).
31. The Sand Dollar is on schedule for gradual national release to the Bahamas in mid-October 2020 // Central Bank of the Bahamas. – 2020. – URL: https://www.centralbankbahamas.com/news/public-notices/the-sand-dollar-is-on-schedule-for-gradual-national-release-to-the-bahamas-in-mid-october-2020 (date of access 16.02.2022).
32. Tobias A., Mancini-Grifoli T. Central bank digital currencies: 4 questions and answers // IMFblogs. – 2019. – 12.12. – URL: https://blogs.imf.org/2019/12/12/central-bank-digital-currencies-4-questions-and-answers/ (date of access 16.02.2022).
33. Today's Central Bank Digital Currencies Status. – 2021. – December. – URL: https://cbdctracker.org/ (date of access 16.02.2022).
34. Today's Cryptocurrency Prices by Market Cap // CoinMarketCap. – 2021. – 22.12 – URL: https://coinmarketcap.com
35. Unlocking $120 Billion Value In Cross-Border Payments: How banks can leverage central bank dogotal currencies for corporates / Ekberg J., Tek Yew Chia, Ho M., Liu L. – New York : Oliver Wyman, JPMorgan. – 2021. – URL: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2021/nov/unlocking-120-billion-value-in-cross-border-payments.pdf (date of access 16.02.2022).
36. Villeroy de Galhau F. Innovation numérique: Quel rôle pour les banques centrales? / Discours au Singapore Fintech Festival. – 2021. – 8 novembre. – 6 p. – URL: https://www.banque-france.fr/sites/default/files/medias/documents/2021.11.08_sff_2021_vf_fr_cl.pdf (date of access 16.02.2022).
37. Yanagawa N., Yamaoka H. Digital innovation, data revolution and central bank digital currency. – Tokyo, 2019. – 21 p. – (Bank of Japan Working Paper Series ; N 19-E-2). – URL: http://www.boj.or.jp/en/research/wps_rev/wps_2019/data/wp19e02.pdf (date of access 16.02.2022).

The article was first published in Russian in the journal "Социальные новации и социальные науки". – 2022. – N 1. – P. 86–100.

DIGITAL CONTROL AND MONITORING SYSTEMS

Alexander Petrov

Doctor of Economic Sciences, Professor, Kutafin Moscow State Law University (Moscow, Russia)[1] Email: palar-1@bk.ru

Abstract. *The advances in digital technology have accelerated the development and implementation of new population monitoring systems. Scoring systems are already in place in the banking sector. The digital profile system for individuals and legal entities has been launched in Russia. How it will be used depends on those who make decisions and those who operate the system. However, an individual remains the main carrier of personalized information.*

Keywords*: monitoring systems; scoring; digital profile; safety of digital technologies.*

For citation*:* Petrov A. Digital control and monitoring systems / English transl. by Nikulichev M.Y. // Social Novelties and Social Sciences. – Moscow : INION RAN, 2022. – N 1. – P. 63–75.

URL: https://sns-journal.ru/en/archive/ DOI: 10.31249/snsneng/2022.01.05

Introduction

New digital technologies help to combine, process and analyze the most diverse and versatile information collected from a variety of sources. This allows governments to establish control over citizens and organizations using modern systems with standard but gradually upgraded algorithms. The degree of control depends on the level of democracy, protection of human rights and freedoms. Undoubtedly, China is the leader in establishing total control (a large-scale and comprehensive analysis of the mood and behavior of citizens with 100% coverage) using digital technologies, including artificial intelligence technologies (AI).

The launching pad for creating such control systems around the world is the "credit history" system used by banks, which allows to determine the borrower's creditworthiness and associated level of risk based on previous credit activity. However, "credit history" system covers only those individuals and legal entities that resort to bank loans. Part of the population remains out of its control. In a family with a common budget, one family member takes out a loan, while the others stay out of banks' sight.

The next step is the widespread use of bank cards, which provide the opportunity to conduct non-cash payments and track the user's solvency, which overcomes the limitations of the "credit history" system. But bank cards do not give a complete picture of a person's purchasing activity, since some transactions, for one reason or another, are paid-out in cash. The third component was the improvement in the tax system that monitors tax payments on official income. One should remember that in Russia, state pensions that are not subject to taxation (in accordance with paragraph 2 of Article 217 of the Tax Code of the Russian Federation)[1] are not taken into account by the tax system. In addition, only persons with a taxpayer identification number (TIN) pay taxes. Although today the TIN in Russia can be obtained at the birth of a child.

The next step is to digitize the payment of fines and penalties for violation of established norms and passportization of the population. In China, paper passports are already being replaced by lifetime electronic identity cards. Since March 2020, an electronic passport has been introduced in Russia.

Finally, digital technologies were introduced into the processes of analyzing various and versatile data from government agencies, retail chains, and the leisure industry followed. Even at the beginning of the XXI century huge arrays of disparate data on various data carriers were not amenable to integrated

[1] With the exception of payments from voluntary insurance of the self-funded part of the pension and non-state pensions (according to the norms of paragraphs 1 and 2 of article 213.1 of the Tax Code of the Russian Federation)

accounting and processing. With the advent of data science and state-of-the-art digital technologies, the combination, processing and analysis of huge continuously updated streams of information began.

One should not forget that information is a capital and a powerful tool in competition and profit. In addition, information can be sold and bought.

Scoring system

Banks have always been searching for tools and technologies to reduce credit risk. One of the relevant tools in this direction is the client's credit history, showing liabilities, accuracy or delay in loan repayment, payment discipline for household payments. In the financial world, an assessment of an individual's credit rating based on close circle, or "affinity risk", has also been used for a long time. Today, this system is better known as the Refer-a-Friend program. However, a credit history is no longer enough to make a decision on issuing a loan; the additional data about the client is required. Such data is provided by the scoring system.

A scoring model or a customer value score is a system for assessing a potential client by parameters that a bank can track using a bank card, open Internet resources and social networks, including: 1) the client's financial behavior, savings and spending patterns, style of life; 2) payments abroad, 3) profile in social networks, 4) information from mobile operators, 5) information from tax authorities, 6) marital status, 7) education, etc.

For example, information from mobile operators and payment systems allows credit institutions to clarify client's income status and learn about trips abroad. Psychometric scoring is also widely used to identify inclinations, basic qualities and patterns (model, style) of individual behavior. With the consent of the client, banks may request legally relevant information from government agencies.

In the United States, some banks, in addition to standard information about a potential borrower, expand scoring to include the education of a future client, occupation and career, seniority and work experience. The new startup company UpStart (Google) helps banks to obtain this information. In addition, the Kabbage startup provides statements from a PayPal account and data about purchases on eBay and Amazon.

In Russia, banks are interested in whether a person is registered on job recruitment websites and is searching for a job (which may imply that he is "not solvent"). A working client may arouse suspicion if the declared income does not match the salary bracket in his resume [Leonidov, 2017].

Transactional scoring is gaining popularity in the financial industry; it allows banks to evaluate the movement of funds on client's accounts, the categories of his expenses when paying with a bank card, and the nature of settlements with companies and organizations.

To determine the credit status of a client, banks sift through large amounts of data. On the basis of the scoring assessment, the client is awarded points that help the bank decide if the client is eligible. The

assessment score is a variable, it can either decrease or increase. The scoring system allows to immediately reject a loan application on reasons of job loss, tax debt, low wages. Additionally, it can serve as a basis for granting individual benefits, for establishing a personalized loan rate that decreases as the score increases.

Prompt access to the necessary information about customers in Russia was granted by the amendment to the Federal Law "On Credit Histories", which came into force on December 31, 2019, according to which citizens can obtain a personal credit rating and the report from the credit history bureau.

Yandex, the largest technology and IT search engine company in Russia, together with the "Equifax" credit bureau and the United Credit Bureau (OKB) have launched a joint Internet Scoring Bureau program that allows to assess clients' credit risks, creditworthiness and solvency. In this program, Yandex analyzes large amounts of aggregated and depersonalized statistical user data, without sharing confidential information with third parties. Based on the results of the analysis, only one number is generated – the result of a scoring assessment, which is advisory in nature and is used exclusively for marketing purposes.

Currently, the scoring system can be used to comprehensively collect and analyze data about any citizen, entrepreneur or company. Based on the assessment score (the sum of points obtained as a result of the scoring), organizations can issue or refuse a loan, accept a job application, or offer another job to the candidate.

Based on mathematical and statistical algorithms, scoring data processing is impartial and eliminates the human factor. Bad mood, inattention or bias of a manager do not affect how the application is processed. However, huge amounts of information are not always needed for decision making. According to the Pareto Principle, 20% of information is enough to make the accurate decision. According to bank employees, sometimes even 5% of available information is enough. At the same time, the largest possible volumes of information are necessary to identify patterns of client behavior.

Five clusters of information are particularly valuable to organizations and government agencies in analyzing individuals, groups of people and the population as a whole: 1) client's online behavior when filling out a questionnaire / application – fills it in quickly or thinks over each item; 2) client's IP address, used browsers and social networks; 3) the Internet search history; 4) black lists from the open sources; 5) posts and activity (duration and regularity of entry) in social networks.

In Russia, as in other countries, scoring systems are used to identify unreliable passengers and citizens of other states who remain in the country without registration. Scoring methods are also used by governments and private companies for socio-economic purposes. Currently, credit scoring models are widely used in healthcare, dating services, customer assessment in the auto insurance system, rental housing, hiring and providing mobile services. The aggregated information is also useful for trading platforms that create their own customer scoring information systems.

One of the scoring methods is reputation scores. According to some experts, it allows for a more efficient and targeted distribution of social benefits to individuals, and can also be used to assess the activities of legal entities in order to increase efficiency and stimulate the growth of the national economy. In some countries reputation scoring is used as a source of customer information. In others, it is an integral part of the public administration system. The scoring results are used to allocate social benefits to certain population groups the from local budgets of municipalities and cities. A good example is China with its reputation scores as part of the social credit system.

The demand for scoring personality assessment is growing. However, the introduction of such reputation assessment system in Russia requires major legislative changes. At the same time, Russia already has implemented a "fiscal data operator" system (OFD), which allows the tax authorities to control sales transactions in real time (online). It currently covers wholesale and retail trade, but its effectiveness depends on product labeling capability.

Digital technologies have closed many loopholes for tax evasion for both legal entities and individuals. Meanwhile, the OFD system puts household budgets under state control. At the same time, OFD promotes online services and mobile applications for managing family budgets and expenses.

Problems with using scoring systems

With the improvement of artificial intelligence (AI) technology and neural networks, the capabilities of monitoring systems increase exponentially. The accumulated diverse and versatile information from numerous sources makes it possible to generate a complete personality profile with individual preferences, inclinations and moral and psychological qualities, to accurately determine potential capabilities, to predict and manage financial behavior and future of an individual.

The main "informants" for scoring are individuals themselves, their gadgets and other manifestations of their vital activity in the virtual and real worlds. An important source of information is the "voluntary" consent of an individual to personal data processing when contacting an online store, healthcare and educational institutions, visa centers. Experts believe that Google and Apple know more about their users than their governments, and in some areas – more than a person himself [Mozhet li vash …, 2019].

It should be borne in mind that modern digital devices are not just hardware, but, above all, an operating system that monitors the user's Internet activity and transfers the collected information to the main server. The functions of a digital "spy" can be illustrated by the example of the "Windows 10" operating system, which, through a Microsoft account: 1) tracks the user's behavior on the Internet, including location and range of interests; 2) analyzes visited websites and scans downloaded files; 3) browses web content, accesses applications; 4) identifies applications with an advertising identifier and sends the information to Microsoft; 5) keeps track of recently used files and folders; 6) remembers recently opened files and frequently used folders.

Social networks are a constantly growing and bottomless source of information. Each of such social networks as Facebook, Google+, Tumblr, Twitter, LinkedIn, Tencent Qzone, Sina Weibo, VKontakte, Odnoklassniki, Renren has more than 100 million users [Petrov, 2020]. Social networks, open to everyone and at all times, actually cover the entire population of many countries. The law enforcement agencies, tax authorities, the banking system, and commercial organizations easily get access to the information from social networks. The collected information is also used by advertisers to develop effective targeted advertising and to send users customized advertisements. Social media cooperate with intelligence agencies, providing them with user dossiers (as reported by former employee of the US National Security Agency Edward Snowden). Cookies and social plug-ins, such as the "Like" button, "Subscribe" button and others, which are available on almost every site, play a special role in tracking user behavior. This information gathering is a potential threat to privacy. Therefore, one should think twice before posting personal information on social networks.

This hidden side of social networks can be glimpsed in the report of Facebook founder Mark Zuckerberg: the system collects information about the owners of accounts and about users without accounts; track mouse movement, battery level and monitor devices near the user; analyze contact information, including the phone book, call log, SMS correspondence; monitor and archive GPS location data; collect information about the Internet browsing outside social networks; receive data about the Internet service provider and the user's mobile operator. According to the British political consulting firm Cambridge Analytica, Facebook has collected personal data from more than 50 million of its users, and dossiers on users are transferred to certain organizations under certain conditions [Litvinenko, 2020].

Since 2012, Facebook has been implementing its own customer authorization and identification system, taking into account their behavior in social networks, in order to assess the customer reliability in relation to other Web users and block the dissemination of information that is undesirable for the client. Facebook intends to transform this system into credit scoring and provide loans to the network members using rating information about the applicant's friends. Under the US law such transformation of the company's activities changes its status and requires that the company regularly reports to supervisory authorities as a financial institution.

Facebook also launched a program to provide banks with information about the profile (portrait) of network users who can become their customers. Moreover, the number of positive contacts turns into quality: the more contacts with a reliable credit history, the higher the chances of getting a loan at a reduced rate. This program represents the internal scoring of the company's social network – Facebook scoring.

Avoiding social networks and paying in cash does not guarantee protection against intrusion into personal / private life. People are increasingly using mobile phones, Internet information, online shopping, displaying growing online activity. All this makes up a database for scoring.

The scoring model, like any phenomenon, has positive and negative sides. The invasion of privacy and the transfer of collected information to commercial companies are the obvious negative aspects, to say nothing of the transfer of personal user data to special services. But the latter also has a positive effect – the fight against terrorism and extremism, the prevention of terrorist attacks. The use of scoring technologies also significantly reduces the scale of fraud in the banking and insurance sectors, and is the basis for improving the financial system.

Currently, there is a need to consolidate and unify the information received from various systems, as well as to ensure its reliability and objectivity. The scoring system operates only with the data that users reveal about themselves. To verify their validity, programs analyze the frequency, quality, activity, and loyalty of customer relationships.

Improving scoring technologies

Biometric technologies allow to evaluate the unique characteristics of an individual. By integrating scoring and biometric technologies it is possible to create the most effective (impenetrable or ultra-reliable) protection in all areas of human and business activity.

The banking and credit industry employs such biometric technologies as: 1) fingerprint authentication, 2) hand geometry, 3) matching the client's speech with "voice casts", 4) retinal scanning, 5) signature dynamics or handwritten keyword imitation, 6) face recognition by photo, 7) DNA, 8) vein pattern recognition. Biometric technologies guarantee a more advanced financial protection system compared to a PIN code and SMS from a bank.

In many countries, the provision of biometric data is the basis for a visa-free regime. For example, the United States has agreements with 27 countries on a visa-free regime with the mandatory availability of biometric data. In Russia since 2018, as part of the "Digital Economy" program, a Unified Biometric System has been in operation that recognizes a person's identity by image and voice. In addition, neural network technology or a unique system of neural brain pathways may replace fingerprinting as a personal identification system as early as 2030-2040.

However, the collection of biometric data is a very sensitive issue – and this procedure can only be carried out with the consent of the person (or on the basis of a special legislative act).

New scoring technologies have received an additional impetus with the development of Data Science.

Data Science (often datalogy) is an interdisciplinary field, a branch of computer science that studies a wide range of issues related to the analysis, processing and presentation of large amounts of various data. In fact, data science integrates various methods of statistics, processing and mining, database design, machine learning and optimization of the entire decision-making process. The practical goal of data science is to discover patterns in data and extract knowledge in a generalized form.

Machine learning algorithms learn to identify patterns in data that remain out of sight of a person, and then, on this basis, build forecasts, develop projects, plan their implementation and evaluate the effectiveness of solving specific problems. For example, 85% of Fortune 500 companies use big data as a basis for building competitive advantage. In turn, data scientists since 2010 have become one of the highest paid and promising occupations around the world. However, the system operates effectively only with the continuous flow of large amounts of information. With small parcels of periodically received data, the system falters and fails.

Digital profile of individuals and legal entities in Russia

The Russian e-government infrastructure includes the Unified Identification and Authentication System (ESIA) that consists partly of digital profiles of individuals and legal entities or a set of digital records about citizens and organizations contained in government information systems. The infrastructure of the digital profile provides the ability to access information from various systems simultaneously. At the same time, the digital profile is constantly replenished and updated non-stop (every 15 seconds), while maintaining the relevance and reliability of the data[1].

The digital profile is created to improve the quality of electronic interchange between financial institutions, businesses, government agencies and the public, to simplify and accelerate the receipt of government and commercial services online. The data collected for the digital profile of individuals and legal entities differ somewhat, which is determined by their different roles and status in society and the state.

The digital profile for every citizen includes three components: 1) key data about the citizen (57 types of legally significant data); 2) links to other government agencies, 3) a register of consents for the processing personal information provided by an individual to various departments and companies. This means that the collection of information about a person will become almost total, covering all state, non-state, public and commercial organizations. But "there is nothing to be afraid of if you follow generally accepted norms of behavior" [Kostyleva, 2019].

The citizen will control what personal information to disclose and to what agency, will at any time browse and revise the register of his consents for processing personal data. The ability to withdraw consent for processing personal data in order to block its use is an important parameter of the Russian digital profile. However certain information in some cases can be obtained from a digital profile without the consent of a person.

The Federal Tax Service, on the basis of information from registry offices, creates the Federal Population Register, which will become the source of data for a citizen's digital profile. Another source of data will be personal activity on the Internet and social networks. By accessing the Internet in order to

[1] The digital profile system was launched into commercial operation in Russia in May 2020 – edit.

read the news, find the necessary information, order goods and services, or communicate with a virtual community and to discharge stress and accumulated emotions in social networks, a person leaves digital footprint. Those digital footprints can reveal what a person would prefer to keep private. According to A. Khachuyan (CEO at Tazeros Global Systems, a firm specializing in the AI development), 40% of the digital profile is generated from data about an individual and 60% represent data about personal environment [Semenec, 2019]. But not all information collected is public. Banking and medical data can only be accessed by the owner and the operator of these data.

The basic sources of information for the digital profile of organizations and individual entrepreneurs are PSRN (Primary State Registration Number)[1] and TIN. The digital profile of organizations quantitatively and qualitatively speeds up and improves the interaction between the center with the subjects of the Federation, between government agencies, as well as between the population and the business community, between entrepreneurs or between entrepreneurs and consumers. The digital information exchange system minimizes paper turnover and will reduce the cost of services, making them more accessible to the consumer. The principle of operation remains almost the same, but a number of stages are removed, and digital logistics simplifies interaction. Theoretically, this should reduce costs and increase the competitive advantages of Russian business, as well as increase the efficiency of tax collection.

Initially, it was planned to spend 3.1 billion rubles for creating digital profile system by "Rostelecom". The corporation agreed to assume the functions of the project executor / operator. Under this option, Rostelecom would receive the following competitive advantages: 1) free access to a database of customers of other economic entities and 2) information about its competitors. The rejection of Rostelecom's proposal made it possible to reduce the cost of the Project by 13 times [Korolev, 2019].

Granting the operator status for the digital profile system to the Ministry of Telecom and Mass Communications helped significantly reduce Project cost. According to the new plan, the federal budget allocated 235 million rubles to set up the digital profile system, including: 1) 184 million rubles for the modernization of existing mechanisms in the ESIA software architecture, 2) 51 million rubles for the creation of digital profiles and the corresponding infrastructure, for the development of algorithms and documentation for filling in profiles and verifying data, as well as for creating a subsystem for informing applicants [Korolev, 2019]. Financing of the digital profile infrastructure is carried out from the federal budget; for security reasons commercial organizations were not allowed to finance the Project.

To allow "Rostelecom" to develop the system was equal to transferring the national database about the entire population and economic entities to the corporation for monopoly control, which could destroy the competitive environment. At the same time, due to the limited state financial resources, the ministry is forced to reduce the cost of the Project many times over. Reduced budget caused concern about the qual-

[1] Primary State Registration Number assigned during registration to all organizations – edit.

ity of work, but this is the price for equal access to the digital profile information system. Although saving at the expense of quality is a false path, and the miser pays twice. In addition, one should not lag behind world trends while the time for innovation runs fast.

After all, it is not enough to create a digital profile. The system must be fully budgeted, funds must be allocated for maintenance and operation. Or it could become self-financed and turn into a source of income for the state budget. Currently, it is planned to allow free access to the digital profile for individuals. For commercial structures should pay for the access, and the tariff can be "tied" to the income received.

The digital profile is primarily focused on the financial market, on reducing the cost of banking products. Since the autumn of 2019, banks in Russia have begun to evaluate the debt burden of borrowers and, taking into account the client profile, determine his/her creditworthiness. Such measures were taken by the Central Bank to prevent the "growth of a bubble" in the consumer lending market. The Central Bank of Russia also selected 16 banks to test the digital profile [Cifrovoj profil' rossijanina …, B/d].

At the same time, some AI experts question the effectiveness of the Russian digital profile system. Perhaps, in this case, desires outstrip possibilities. Problems arise in connection with the quality of data digitization, as well as the depth and breadth of digitization. For example, "smart" meters installed in private apartments cannot automatically transmit information about consumed resources to the database for the lack of the necessary infrastructure. It took China 15 years to concentrate the entire array of data from the border service, educational institutions, healthcare institutions and other agencies in electronic databases, which became the basis for creating a digital profile and / or a social credit system [Semenec, 2019].

However, it should be remembered that any innovation, especially innovative, is not easy to implement. At the initial stage of operation, vulnerabilities and bottlenecks are always identified. It takes time and, most importantly, practice of using the product (program) to eliminate these weaknesses. It is necessary to start using the system in order to ensure its improvement.

The introduction of a digital profile increases the efficiency and effectiveness of public services and makes life easier for citizens. The digital profile allows to automatically enter data from the electronic database into the questionnaire, which takes 10-20 times less time than when filling out a paper questionnaire. Digital system excludes the human factor (errors and falsification), the risks of providing fake documents, while the number of rejections due to incorrect paperwork are reduced. The digital profile accelerates the process of finding the right solution and increases the volume of services provided. It is not required to fill out the questionnaire every time when applying for a public service.

But the accumulated information can be used to harm citizens. Therefore, experts warn, it is necessary to think through all the nuances and consequences of creating a digital profile, to take into account historical experience and modern realities, including corruption factor [Aitov, 2019].

Algorithmic processing of big data shows not only what happened, but also all alternatives and possible developments. However, errors may occur. Mistakes and distortions of information can cause irreparable damage to both the individual and the organization.

Security and data protection

The digital profile must be reliably protected from hackers, cyber-hacking and invasion into personal life. For this reason, the genetic certification of the population should remain voluntary.

The most difficult question is who, on what basis, for what reasons, for what purpose gets access to a comprehensive digital database about every citizen of the country, about every owner, about every entrepreneur and company. This is an issue of moral and ethical integrity that can both strengthen and destroy the balance of trust, which serves as the basis of an unwritten social contract between government and citizens, government and entrepreneurship.

The concentration and centralization of all information about the population and organizations in one agency poses a serious threat to democratic development. Moreover, it creates opportunities for manipulating some social groups and, in the event of a leak, data can be used against people and organizations, causing significant damage to their interests. Information from a single database can be obtained by a competitor, a fraudster, a criminal. The demand for digital data can give rise to a digital shadow market, and dealers in stolen data will soon appear.

The Federal Security Service (FSS) of Russia and other law enforcement agencies oppose such future for the digital profile system. In their opinion, the centralization of data on one platform increases the risk of leakage of confidential information about state employees, and may also lead to the disclosure of personal information about persons under state protection and their families [Cifrovoj profil' rossijskogo ..., 2019].

The problem of data leakage is not an empty threat. Security measures can be hacked from the outside as a result of hacker attacks or compromised from the inside. Suffice it to recall the appearance on the black market of the Sberbank customer database. In addition to these threats, there are economic intelligence and industrial espionage, which can cause irreparable damage to the national and economic security of the state and business. One should take into account the steady growth in the number of hacker attacks perpetrated by different groups and states. In 2019, the number of hacker attacks on infrastructure and government facilities in Russia increased by 200% [Fedunenko, 2019].

The security of digital systems depends primarily on software. In this regard, it is desirable to use domestic software and Russian-made storage devices.

In general, the digital profile problem should be solved based on the interests of an individual. Experts believe that digitization ushers in a new ethics, which is based on two interrelated postulates: 1) a person must have access to his data in a digital profile; 2) a person must understand the principles of

algorithm operation [Semenec, 2019]. An individual must also maintain the right to: 1) control the personal data collection process, correct this data and erase it if necessary; 2) know the collector / operator of personal data; 3) protect reputation in the event of a system error and/or cyber security breach. The regulatory legal framework in the field of personal data protection can help curb and regulate digital data collection and algorithmization.

Conclusion

In Russia, there are (at the time of writing this article – *editor's note*) more than 40 poorly integrated state information systems (GIS). Along with the federal portal of public services, there are local portals. Data on individuals and legal entities are collected by various government agencies with different goals and objectives. Banks, Internet companies and social networks, mobile operators and advertising platforms, taxi aggregators and the tourism industry are also regularly collecting personal user data. Each state agency and private organization uses proprietary model for collecting, storing, processing and analyzing the collected information. In this regard, the task at hand is to integrate these flows of information in one center.

The country still employs a mixed model for the provision of public services with the gradual displacement of paper forms by electronic ones. The public services portal contains a significant amount of data from various state agencies (financial institutions, law enforcement agencies, Rosstat, etc.) and successfully copes with a large amount of information. But some services can only be obtained on the websites of individual state departments. Moreover, there are frequent failures due to "hanging" systems. Therefore, the need to create a single personal account for each citizen is obvious.

The logic of developing a digital profile / electronic passport demands to unify the digital systems of all government agencies and provide access to digital platforms of commercial organizations, including banks, mobile operators, the leisure industry, as well as social networks. The task to combine all data bases into a single system is complicated for the lack of a single standard.

As a result, absolutely all information about an individual can be collected, which makes it possible to form, among other things, moral and psychological portrait of every citizen. It is doubtful that a social credit system similar to the one in China would be created in Russia, but this option cannot be ruled out, given the history of the country. However, the integration of all electronic resources on one platform greatly increases the efficiency of the digital profile system.

Access to the electronic database of public services and the digital profile system remains a point of a heated dispute. Such access must be regulated. If access remains free, state information resources can be used to the detriment of a person or an entrepreneur. The digital profile system must ensure the confidentiality and integrity of legally relevant information. Any accidental or deliberate distortion of data harms

the owner or the one who makes the request. Therefore, the information base of the digital profile must be reliably protected by domestic software and hardware resources.

References

1. Aitov T. Cifrovoj profil' grazhdanina: voprosov bol'she, chem otvetov // Finversia. – 2019. – 28.05. – URL: https://www.finversia.ru/publication/ocenka/tsifrovoi-profil-grazhdanina-voprosov-bolshe-chem-otvetov-58249 (date of access 12.03.2020).
2. Cifrovoj profil' rossijanina: otvety na glavnye voprosy // NTV. – B/d. – URL: https://www.ntv.ru/cards/2941/ (date of access 12.03.2020).
3. Cifrovoj profil' rossijskogo grazhdanina mozhet stat' udobnoj mishen'ju dlja hakerov // Kommersant. – 2019. – 13.11. – URL: http://www.iksmedia.ru/news/5623672-Czifrovoj-profil-rossijskogo-grazhd.html (date of access 12.03.2020).
4. Fedunenko E. Hakery nacelilis' na infrastrukturu. Kolichestvo kiberatak vyroslo v tri raza // Kommersant. – 2019. – 06.08. – URL: https://www.kommersant.ru/doc/4053350 (date of access 12.03.2020).
5. Korolev I. Cifrovoj profil' grazhdan podeshevel v 13 raz, kogda ego otobrali u "Rostelekoma" // CNews. – 2019. – 06.08. – URL : https://www.cnews.ru/news/top/2019-08-06_tsifrovoj_profil_grazhdan_podeshevel_v_13_razkogda (date of access 12.03.2020).
6. Kostyleva T. Cifrovoj profil' grazhdanina – chto izvestno na segodnjashnij den'. // D-Russia.ru. – 2019. – 27.03. – URL: http://d-russia.ru/tsifrovoj-profil-grazhdanina-chto-izvestno-na-segodnyashnij-den.html (date of access 12.03.2020).
7. Leonidov S. Skoring vo vremena "Bol'shogo brata": kak banki budut vydavat' kredity k 2020 godu // Forbes Contributor. – 2017. – 12.05. – URL: https://www.forbes.ru/tehnologii/342269-skoring-vo-vremena-bolshogo-brata-kak-banki-budut-vydavat-kredity-k-2020-godu (date of access 12.03.2020).
8. Litvinenko Ju. Facebook raskryl dannye o "slezhke" za pol'zovateljami // Vedomosti. – 2020. – 28.01. – URL: https://www.vedomosti.ru/technology/articles/2020/01/28/821653-facebook-slezhke (date of access 12.03.2020).
9. Mozhet li vash cifrovoj profil' srabotat' protiv vas? // Executive.ru. – 2019. – 14.06. – URL: https://www.e-xecutive.ru/finance/novosti-ekonomiki/1990700-mozhet-li-vash-tsifrovoi-profil-srabotat-protiv-vas (date of access 12.03.2020).
10. Petrov A.A. Informacionno-cifrovoj sled: kommercheskie i social'nye aspekty v cifrovuju jepohu // Торговая политика. – 202. – № 2. – С. 62–86.
11. Semenec A. Cifrovoj sled privedet k ljubomu // Rosbalt. – 2019. – 22.05. – URL: https://www.rosbalt.ru/moscow/2019/05/22/1782565.html (date of access 12.03.2020).

The article was first published in Russian in the Journal "Социальные новации и социальные науки". – 2020. – No. 1. – P. 128–142.

MAN IN THE DIGITAL WORLD

DIGITALIZATION AND HUMAN CAPITAL: MUTUAL INFLUENCE AND DEVELOPMENT

Maria Polozhikhina

PhD (Geogr. Sci.), Leading Researcher of the Department of Economics, Institute of Scientific Information for Social Sciences, Russian Academy of Sciences (Moscow, Russia)

E-mail: Polozhikhina2@mail.ru

Abstract. *The contradictory impact of digitalization on the institutions that determine the reproduction and use of human capital is analyzed. Particular attention is paid to changes within family and interpersonal relationships, culture and the labor market. The article explores how the quality of human capital affects the spread of new technologies, conversely, how the social environment transforms under the influence of digitalization.*

Keywords: *digitalization; human capital; interpersonal relationships; cultural environment; labor market; Russia.*

For citation: Polozhikhina M.A. Digitalization and human capital: mutual influence and development / English transl. by Nikulichev M.Y. // Social Novelties and Social Sciences. – Moscow : INION. RAN, 2022. – N 1. – P.76–88.

URL: https://sns-journal.ru/en/archive/ DOI: 10.31249/snsneng/2022.01.06

Introduction

The COVID-19 coronavirus pandemic has dramatically accelerated digitalization in all aspects of human life. The wider use of new (digital) technologies is causing global, diverse, ambiguous and long-term consequences changes in society. In this regard, it becomes increasingly important to study the impact of digitalization on social processes in order to reduce their negative and enhance positive effects.

The concept of human capital serves as the methodological basis of this study. It appeared in the 1950s (M. Friedman, 1956; J. Mincer, 1958) and received broad public recognition due to the works of G. Becker (1964), T. Schulz (1972) and a number of other scientists [Grigor'ev, 2020, p. 83–84]. The dissemination of these views was also facilitated by the support at the international level by such organizations as the UN, the OECD, the World Bank.

The appeal of the concept of human capital lies in its compliance with the ideas of a post-industrial society, comfortable modern life and creative human labor. This approach helped reformulate the role of the human factor in the economy, the characteristics of labor force and labor resources, and promote a new attitude to the so-called non-productive industries (primarily, education and healthcare) and the corresponding investments.

Currently, the widely spread ideas about human capital are accompanied by a variety of interpretations, definitions and classifications, while the very provisions of this concept are laced with inconsistencies [Kudelina, Adova, 2020, p. 71-72]. The doctrine of human capital and its composition continues to develop due to progress in sociology, economic theory and other scientific disciplines. The set of resources included in its structure is expanding: "they now include all the intangible resources, owned by an individual, that can generate income" [Grigor'ev, 2020, p. 86]. Modern studies of human capital are becoming interdisciplinary, and interest in studying human capital is on the rise [Kudelina, Adova, 2020, p. 75].

This paper discusses the transformations caused by digitalization of some institutions, within which the formation and use of human capital takes place. Based on domestic research materials, the study attempts to identify significant and long-term trends in the area.

Theoretical approaches

Digitalization, as a term describing a new phenomenon, appeared in the second half of the 1990s, but has come into active circulation since the 2010s. And as is the case with many other concepts, it is characterized by a variety of approaches, definitions and views.

In a narrow (technological) sense, digitalization can be represented as a transition to a digital communication, i.e. data recording and transmission using digital devices. In this interpretation, digitalization

is just the next stage of the automation, affecting not only the physical abilities of a person, but also some of his intellectual functions. On this basis, new technical solutions appear and spread, including unmanned technologies and robotics, complex platforms ("smart" systems and devices), Internet of things (IoT), 3D printing, etc. The resulting changes are in many respects similar to the transformations caused by the electrification at the beginning of the 20th century.

In a broad sense, the process of digitalization means a transition to a system of economic, social and cultural relations based on the use of new information and communication technologies (ICT) [Mitin, 2017]. At the same time, there are two parallel (albeit interconnected) directions in the digital transformation of society. The first direction is social: the formation of a new social environment with the help of new ways of communication and constructions of the virtual world – the so-called Internet of people (IoP). This process includes the digitization of scientific and cultural heritage (the creation of electronic libraries, museums and publications); online public events (on-line broadcasts, web conferences, etc.); the spread of social networks, and finally, the formation of an electronic state. In this context, we can talk about the artificial process of creating the noosphere, the concept introduced by V.I. Vernadsky. The new (digital) social environment inevitably leads to psychophysical changes in an individual and to a serious transformation of the whole society. The second direction of transformation involves mainly the economic and financial spheres, as well as management. It consists in the formation of the so-called digital economy – the emergence of new activities, products, services (creation of new value) and new business models while traditional industries are modernized by digital technologies [Polozhikhina, 2018, p. 11–12].

Obviously, different interpretations of digitalization appear mainly due to methodological differences in the different scientific disciplines. Convergence of approaches is achievable on the basis of general scientific methods. For example, the systemic approach and some provisions of information theory make it possible to create a simplified digitalization model in terms of the impact of new (digital) technologies on socio-economic objects (Fig. 1).

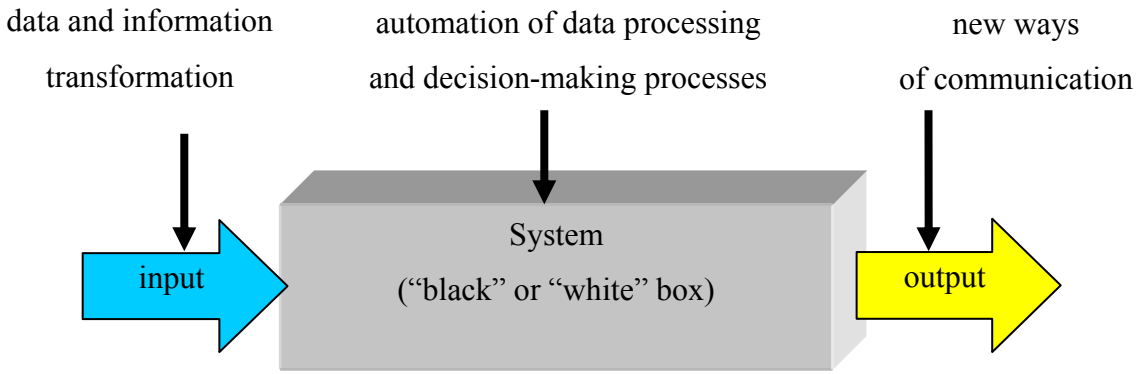


Fig. 1. The impact of digitalization on functioning of an open system. Compiled by the author

Any socio-economic object (personality, community, organization) can be represented as an open information system – a "black" (if internal processes are unknown to an external observer) or "white"

(when internal processes are understandable to an external observer) box that shares information with other systems and the environment. Such system functions in stages: input of external (incoming) information or data; processing this information (data); transfer of newly created (outgoing) information (data) to other systems or to the external environment.

Currently, the share of external information (data) entering the socio-economic systems (objects) in a transformed (digital) form is constantly growing (Internet, online publications, etc.). The scale of digital data processing in these systems is also growing fast (artificial intelligence, virtual and augmented reality, machine learning, etc.). Finally, the methods of communication and data transfer are increasingly based on digital technologies (mobile devices, social networks, etc.). Thus, the use of new (digital) technologies has a systemic impact on the functioning of socio-economic objects (open information systems) and society itself.

But the reverse influence of an individual on the rate and direction of digitalization is also obvious. People need to be able to use various gadgets or programs, navigate the information flows, analyze and interpret data. Therefore, knowledge and skills, i.e. the quality of human capital is of particular importance for the development of digitalization.

At the same time, IT and any other complex technologies cause new challenges. The 2019 World Bank report identified the following risks of digitalization: cyber security; the possibility of mass unemployment; the growth of the "digital divide" (a gap in digital education, in terms of access to digital services and products and, as a result, a gap in the level of well-being) between citizens and industries of any one country, as well as between countries [Doklad o mirovom ..., 2019, p. 18]. Numerous works devoted to the topic of digitalization of society and the development of the digital economy have significantly expanded this list. Whatever the case, one cannot ignore the radical differences between the world "before and after the Internet", as well as how well new ITs "fit" into modern reality.

"Digital technologies have gone beyond information processes, penetrated into material technologies and interact with the "analog technologies" of the organic world... science is faced with the need to understand and interpret the analog-digital dualism" inherent in modern society [Kefeli, Kolbanev, 2018, p. 218]. And it is hard to disagree with this statement.

It must be borne in mind that the digitalization is still under development, and society is still at the initial stage of transformation and the formation of new social relations. "We still know very little about ourselves", about the functioning and features of the human psyche, consciousness and subconsciousness [Kolin, Ursul, 2015, p. 268]. In addition, human capital is reproduced, accumulated and used within certain social institutions: the family, education and healthcare systems, social support institutions, culture, and the labor market. The impact of digitalization on them and, accordingly, on how human capital develops, is very contradictory.

Family and interpersonal relationships

The creation of human capital, of course, begins in the family. Family and interpersonal relationships in general play a major role in its reproduction.

In the economic science, the family (household) is considered mainly as a form of material support – income, consumption, property ownership, etc. The family is considered as a wholesome unit, while intra-family relations, including economic ones, are usually neglected. This approach has significant drawbacks. First, not all incomes and activities of households can be accurately estimated (primarily, the so-called informal production – the production of products for one's own needs). Secondly, not all types of such activities are taken into account, which distorts reality and makes managerial decisions inaccurate. Here is a theoretical and methodological paradox: household work performed by family members (primarily women) is not perceived as an economic activity. But the same work performed by hired workers is already considered as such. This can be seen as a form of discrimination against women when the social significance of the intra-family division of labor is underestimated. It should be recognized that without the performance of certain functions at the family level (cooking, cleaning, etc.), human life is generally impossible – and who performs them, external or internal persons in relation to the household, is not a matter of principle. There is a human labor involved anyway. The fallacy of traditional views is especially obvious in the light of the human capital concept: after all, its reproduction requires actions within the family, and not only external activities.

Family and interpersonal relationships receive much more attention in sociology, psychology, and pedagogical sciences. However, a number of related important topics are still a taboo in Russia. As a result, discussions are not comprehensive, many issues remain undeveloped, and management decisions are not always accurate. The state either does not interfere in family and interpersonal relations (even when necessary), or, on the contrary, interferes too strongly (and unreasonably). Consider for example the controversial practice of juvenile justice in Russia.

Meanwhile, Russia faces many problems in the sphere of family and interpersonal relations. Experts note that dysfunctional families have much in common: difficult financial situation, parental abuse due to alcohol or drug addiction, avoidance of parental duties, domestic violence, social orphanhood, etc. [Issledovanie prichin social'nogo …, 2019, p. 49].

The state institute of social support is called upon to help families and individuals overcome life's hardships. Charitable public organizations and volunteers can also play a significant role. Although, according to experts, certain stereotypes have developed in Russia both in relation to dysfunctional families (irresponsible, have themselves to blame, etc.), and in the work of specialists from social support organizations (disregard for individual peculiarities, lack of interaction with other departments and etc.) [Issle-

dovanie prichin social'nogo …, 2019, p. 51]. All this reduces the effectiveness of support measures, hinders the preservation and accumulation of human capital in the country.

The attitude of society (and individuals) to adverse life circumstances and common practices for overcoming crises play an important role in preventing them. It is no secret that in Russia the most common reaction to a stressful situation is drinking or even alcohol abuse [Issledovanie prichin social'nogo …, 2019, p. 47]. In recent years, drug use has been added to this list. In spite of this, most citizens are not ready to personally seek help from specialists – psychologists.

The Internet and digital technologies help to use other, more constructive ways to cope with stress. Undoubtedly, facilitating the process of communication, new opportunities for social interaction and expansion of contacts helps to resolve crises on a personal level. The Internet resources help to discuss a "sore" issue with various specialists (personally or anonymously), learn about someone else's experience in solving a problem, find the necessary information and even raise funds (for example, for expensive treatment), etc. No doubt, in the virtual space people feel more relaxed emotionally, free in choosing words and behavior. Here it is easier to get acquainted and communicate, revealing your true self [Kodaneva, 2020, p. 150].

Interpersonal communication is currently "digitized" to the greatest extent, although this situation has developed spontaneously. A variety of blogs (bloggers), master classes, online consultations, reviews and recommendations, membership or event communities, etc.: today, these are ubiquitous forms of communication with millions of subscribers. Currently, an unusual phenomenon from the point of view of the historical process can be observed: the younger generation (children and adolescents), who are better at using digital gadgets, helps older people (parents, grandparents) in mastering them.

Meanwhile, digitalization of the state social support system remains insufficient and is associated mainly with the automated process of collecting and processing data. The slow introduction of new technologies into the work of social institutions is partly due to the type of people in need of such assistance – the underprivileged and with poor digital skills.

The advantages of digital communications have become especially clear during the coronavirus pandemic. During self-isolation and a restriction of transport links between countries, digital technologies have become the main means of communication between different generations or between geographically dispersed relatives and acquaintances, as well as a way to maintain business contacts and communication between the population and government agencies. In addition, they were used to trace the sick and their contacts, control compliance with the isolation regime, etc.

However, digitalization of interpersonal relations leads to both positive and negative consequences. "In social networks and blogs, one can say and do things that are difficult to do in the physical world, including bullying and insults" [Kodaneva, 2020, p. 150]. In the virtual environment, various types of destructive behavior are spreading: trolling, cyber-bullying, identity theft, fraud, etc. To prevent and limit of

cyber-crime people must acquire better psychological stability (especially children and adolescents), need to learn and follow the rules of safe online behavior, reject cyber violence on moral grounds and admit a certain degree of content censorship and regulation over the Internet resources.

In addition to psychological risks, digitalization may threaten physical health: excessive computer time might be harmful for both children and adults. It is no coincidence that the new concept and rules of "digital detox" appeared – a temporary conscious refusal to use digital devices in order to immerse (return) into the real environment.

On the bright side, the pandemic has proven that fears about young people "drowning" in virtual environment are groundless. Direct personal communication remains a social necessity. Moreover, person-to-person communication remains important for young people, despite their advanced skills in using gadgets.

However, digital technologies currently stand in the center of various socio-humanitarian dilemmas (for example, tracking people; preventing various types of destructive online behavior; disseminating fake information; censoring the Internet, etc.) [Levashov, Sar'jan, 2020; Kodaneva, 2020]. The coronavirus pandemic has demonstrated that it is impossible to completely transfer everyday life to the digital space and that people need to adapt to virtual reality. Coexistence and harmonization of online and offline spheres are emerging as major regulatory issues at the national and international level.

Cultural environment

According to one of the most common definitions, the cultural environment is a set of cultural preferences, localized within the boundaries of a certain space, which is usually expressed (materialized) in the norms of people's social behavior. Cultural environment is a territory for different cultural interactions, a special space for social rituals, social memix (phenomenon of imitating cultural heroes), a hierarchical value system of social concepts. Structurally, cultural environment consists of symbolic activity, normative social behavior, language and customs [Flier, 2013]. According to another approach, cultural environment comprises artifacts, institutions and organizations (types of activity), including libraries, theaters, museums, film industry, etc.

Experts emphasize that "digitalization affects not only the economy, the sphere of production and consumption of new items ... It becomes the basis of culture and, before our eyes, is changing both this culture and the society that surrounds us. And that means changes in all of us." Nonetheless, "digital" "… has not become part of the vocabulary or even the cultural world picture for most of Russians. In this sense, digital society and its inherent digital culture is still at the early stage of development in Russia. This, of course, does not mean that the digital infrastructure as a complex of technologies and related useful products... is not present in the country" [Kuznecova, 2020, p. 8, 116]. But is that really so?

Today it is difficult to imagine people (for example, in Russia) unaffected by digitalization. There are two parallel processes running: digitalization of traditional cultural institutions and the emergence of a specific digital culture that is directly related to operations in the digital environment.

New digital technologies are introduced into by traditional cultural institutions both at the initiative of these cultural institutions, volunteers, businesses and non-profit organizations, and as a result of support from the state.

For example, in Russia, the National Project "Culture" (initiated in 2018) includes the Federal Project "Digital Culture" which calls to create virtual concert halls and excursions (guides) to the popular exhibitions; online broadcasts of concerts and shows; book digitization. As of 2019, the budget of the federal project is 6,8 billion rubles – about 6% of the budget of the "Culture" national project [Nacional'nye proekty: Celevye ..., 2019, p. 28]. And although this is hardly sufficient, the trend is a positive sign.

Digital trends change the role of libraries and archives – they are turning into platforms for communication and intellectual growth. At present, there are more than 37 thousand public libraries in Russia and about 4.5 thousand other institutions providing library services. The Russian library network makes up about 10% of the global number of public libraries and is the largest in the world. "Model libraries" are among the most popular innovations of the "Culture" national project. Comfortable space, new computers and office equipment, digital laboratories, interactive workplaces, high-speed Internet, world bestsellers – all this can now be available in any part of the country [Fedjakina, 2020].

The content on the Kultura.RF portal (a humanitarian educational channel dedicated to the Russian culture; in operation since 2016) is constantly upgraded. The portal publishes various materials about events and people in the history of literature, architecture, music, cinema, theater, folk traditions and natural monuments; arranges live broadcasts of cultural events; creates multimedia projects and virtual tours of the country's museums, as well as tourist routes; offers a collection of Russian films, performances, lectures and classical literature, etc., free of charge. In 2022, 1908 films, 722 books, 1004 performances, 1382 concerts and 1930 lectures were available here ["Kul'tura.RF" …, 2022].

Online resources of books and periodicals are expanding due to opening specialized electronic libraries (for example, the National Electronic Library – eLibrary (https://www.elibrary.ru), CyberLeninka (https://cyberleninka.ru), etc.) and digital publications, as well as the digitization of traditional collections. More and more printed products are transferred to electronic format. In addition, ordinary people play an important role in replenishing Internet resources by spontaneously, of their own free will, uploading their own or diverse digitized products to the Web – from excursions to beautiful nature spots, museums and cities to the results of scientific research. At times, questions arise of how to reconcile open access and copyright. It should be noted that the actions of some enthusiasts are sometimes organized and directed

via crowdsourcing. However, in Russia the potential of such forms of cooperation remains underdeveloped.

During the pandemic, digital resources were in great demand. At the time when visiting theaters, museums or concerts was limited, digital resources provided access to online cultural events [Gen', Rybnikova, 2020]. Libraries in Russia actively developed virtual platforms: lectures and seminars moved to Zoom, the Kultura.RF platform was in great demand. Virtual tours, bedtime stories and reading fairy tales for children over the phone, online lectures and master classes – this is an incomplete list of what Russian libraries offered during the period of self-isolation [Fedjakina, 2020]. The number of people who eagerly accessed such electronic resources as NEB and others grew significantly.

The pandemic has definitely stimulated the digital trend in the field of culture. The government recognized the need for faster digitization of books and documents, for more remote services for readers and for training librarians in new digital skills. Additional funds were allocated for annual acquisition and preservation of book collections [Fedjakina, 2020].

The need for digitalization of traditional cultural institutions is quite understandable. However, ideas about the formation of digital culture are very dissimilar.

The term "digital culture" is borrowed from the works of Ch. Gere (2002) [El'kina, 2018, p. 195]. In a narrow sense, according to the experts from the consulting company KMDA, this is a set of principles and competencies that characterize the predominant use of information and communication digital technologies for interacting with society and solving problems in professional sphere. Digital culture includes: competence and application of modern digital technologies (technological adaptability); the priority of using digital technologies to solve problems (digital thinking); widespread use of digital channels for interaction (communication); decision making based on the analysis of digital data; adherence to ethical principles of behavior in the digital environment; compliance with the principles of information security [Ryzhkov, 2019]. This approach does not cause any protest among specialists.

In a broad sense, digital culture is extended to modern culture as a whole or used as a marker of the post-industrial era. Thus, within the framework of the transhumanism movement, digital culture is defined as a totality formed by NBICS (Nano-Bio-Info-Cogno-Social) technologies, and is seen as the transformation of culture and the technosphere into an artificial world. "This raises serious objections, ideological and conceptual… From the humanitarian point of view, digital culture is defined as a set of modern practices that arise at the intersection of artistic culture, computer technology and semiotic systems of the information society in connection with a change in ideological and moral attitudes…. Taken together, they represent a variety of digital culture phenomena that have replaced the culture of industrial civilization" [El'kina, 2018, p. 195, 197, 201].

The discussion about what is actually happening – the formation of digital culture or the transformation of culture in the modern (digital) age – continues. It should be noted that firstly, the traditional

culture does not disappear anywhere and remains in demand (as the pandemic has proven). Secondly, people throughout history transform the surrounding world, which became artificial in many respects long before the advent of digital technologies.

Finally, culture continues to evolve. On the one hand, it adapts to new communication technologies. For example, language is changing: ICT terms and slang are increasingly used in literary and colloquial speech. Innovations in written messages are caused by technical parameters of the gadgets used. But similar processes were observed during the electrification at the beginning of the 20th century. On the other hand, new forms, cultural practices, and artifacts are constantly emerging. The very history of culture – from the advent of printing to radio, film and television – serves a convincing proof.

The influence of digital technologies on the cultural environment is not something exceptional from a historical point of view. How painless this transformation will be depending largely on the regulatory measures, primarily introduced by the state. However, the transformation of the cultural environment is inevitable – as well as the corresponding changes in human capital.

Changes in the labor market

Digitalization, automation and robotization of production, the strengthening role of information technology, the modification of business processes, the integration of IT infrastructure into business, etc. significantly changes the nature of modern workplace. Naturally, the skills and competencies of employees and the demand in the labor market are being transformed. For example, studies have shown that the ICT introduction at workplaces changes standard work operations and, thus, reduces the demand for semi-skilled workers. At the same time, the demand for high and low-skilled workers is growing [Doklad o mirovom …, 2019; Korovnikova, 2018].

The nearly complete disappearance of street pickpockets replaced by cyber-scammers illustrates a strong demand for certain professional skills in our digital age. But, of course, this is not the most important innovation caused by digitalization.

So far, predictions have not been justified that new technologies will replace (force into retirement) some popular traditional professions and create a class of jobless people who will become a source of social tension [Korovnikova, 2018]. Unemployment, which has risen in recent years, is caused by completely different factors. At the same time, the demand for digitally skilled labor grows all over the world, including Russia.

On the one hand, this situation serves as an incentive for the influx of personnel into the IT sector. On the other hand, it hinders the digital transformation of many enterprises at the moment. The budgetary organizations in the non-productive sphere (education, healthcare, science), as well as small and medium-sized businesses are among the most negatively affected. Accordingly, in this case, government intervention is required to adjust the labor market conditions.

It is also necessary to expand the scale of IT personnel training. Luckily, Russia possesses solid basis for ICT training of specialists – the sufficient number of colleges and the mathematical culture are available [Opaleva, 2020, p. 22]. Another driver for personnel retraining is the changing requirement for competence and labor skills in the digital age.

Digital environment objectively modernizes workplace. The number of freelancers is growing, self-employment and remote (work-from-home) formats are becoming more popular. And, most importantly, labor productivity grows, working conditions in manufacturing sphere qualitatively improve.

During the pandemic, remote work has become especially widespread. Many activities continued only in the from-home mode. But it turned out, that this format was not to everybody's liking. Therefore, a return to familiar practices often facilitates and simplifies production activities. However, in some cases, the benefits of remote work are obvious.

Remote work also comes with challenges. For instance, new and unpredicted labor safety issues had to be addressed. In particular, remote work requires a higher degree of self-control and self-organization from workers. Without office-hours framework, labor activity can turn into work "from dawn to dusk" or, conversely, into an uncontrolled relaxation. Therefore, an employee and an employer must have an agreed schedule of interaction, outside of which no new can be set tasks or work done, i.e. offering an employee free or leisure time.

There is no doubt that the experience gained during the period of self-isolation will prompt the use of flexible employment formats (partially remote work, work with flexible hours, etc.). Moreover, various states are now taking steps to legislate new types of labor relations. For example, in December 2020, Federal Law (N 407-FZ of December 8, 2020) amended the Labor Code of the Russian Federation in terms of regulating remote work and temporary transfer of an employee to remote work format at the initiative of the employer in exceptional cases. Since 2020, electronic workbooks have been introduced in Russia, which, as expected, may simplify many formal procedures (registration for work, pensions, social benefits, etc.).

It is evident that the labor market "drives" the process of digitalization forward and, at the same time, depends on it. As experts emphasize, a "cheap worker" is not suitable for a new technological (or, as it is also called, the fourth industrial) revolution – specialists are required who can create new products and work in a digital environment [Opaleva, 2020, p. 24]. On the other hand, a new kind of social inequality is emerging – digital divide.

In general, the digital divide is understood as limited opportunities for different social groups and different countries due to unequal access to ICT and applications. Studies have shown that less educated people, people with physical health problems, low literacy levels, the elderly or living in rural areas are limited in using digital technologies. Accordingly, these social groups receive fewer benefits from the digitalization process and are in need of support from the state [Polozhikhina, 2017, p. 120, 123].

Conclusion

The process of digitalization has a strong and diverse impact on the formation and use of human capital. However, the introduction of new technologies and the directions of their application are largely determined by the human factor. Thus, there is an equally significant inverse relationship between digital transformations and the quality of human capital.

Digital technologies penetrate various institutions within which human capital is reproduced, developed and used with different speed and efficiency. Digitalization often does not resolve but exacerbates the existing problems and adds new challenges. At the same time, one cannot fail to emphasize that digital technologies were extremely usefulness and highly relevant in the extreme conditions of the pandemic.

The greatest positive effect from the introduction of digital technologies can be achieved with official support on the legal, financial, and other levels. The emerging technological opportunities cannot be implemented without resolving institutional, theoretical and methodological issues. Government regulation plays a decisive role in harmonizing online and offline spheres.

Modern digital technologies usher in not only a new stage of industrial or economic progress. They can be considered as a step-up mechanism for the new stage in the development of humanity. Previously, transformation of society under the influence of scientific and technological achievements proceeded spontaneously (as, for example, at the beginning of the 20th century in the course of electrification). At present, countries can at least partly direct and control these processes, to consciously use the new emerging opportunities. It should not be forgotten that, as in the case of any other new technology, digitalization also creates new problems. Based on the accumulated social and humanitarian knowledge and experience, we can avoid repeating past mistakes and overcome new risks.

References

1. “Kul’tura.RF” – gumanitarnyj prosvetitel’skij proekt, posvjashhennyj kul’ture Rossii // Kul’tura.RF. O proekte. – B/g. – URL: https://www.culture.ru/about (date of access 17.06.2022).
2. Doklad o mirovom razvitii 2019: Izmenenie haraktera truda / Vsemirnyj bank. – Vashington, 2019. – 138 p.
3. El’kina E.E. Cifrovaja kul’tura: ponjatie, modeli i praktiki // Informacionnoe obshhestvo: obrazovanie, nauka, kul’tura i tehnologii budushhego. – 2018. – N 2. – P. 195-203.
4. Federal’nyj proekt “Cifrovaja kul’tura” // Ministerstvo kul’tury RF. Nacional’nyj proekt. – 2019. – URL: https://culture.gov.ru/about/national-project/digital-culture/ (date of access 24.01.2021).
5. Fedjakina L. Nadezhnost’, udobstvo i jempatija sotrudnikov: Minkul’tury – o nastojashhem i budushhem bibliotek // Ministerstvo kul’tury RF. Nacional’nyj proekt. – 2020. – 27.05. – URL: https://culture.gov.ru/about/national-project/publications/nadezhnost_udobstvo_i_empatiya_sotrudnikov_minkultury_o_nastoyashchem_i_budushchem_bibliotek/ (date of access 24.12.2020).
6. Flier A.Ja. Kul’turnaja sreda i ee social’nye cherty // Informacionnyj gumanitarnyj portal “Znanie. Ponimanie. Umenie”. – 2013. – N 2. – URL: http://www.zpu-journal.ru/e-zpu/2013/2/Flier_Cultural-Milieu/ (date of access 25.01.2021).
7. Gen’ Ju., Rybnikova I. Artefakt v karmane // RBK. Federal’nyj vypusk. Kul’tura. – 2020. – N 203 (8257). – URL: https://rg.ru/2020/09/09/reg-skfo/kak-meniaiutsia-muzei-v-ramkah-programmy-cifrovaia-kultura.html (date of access 24.01.2021).
8. Grigor’ev K.N. Transformacija ponjatija “chelovecheskij kapital” // Sociologija. – 2020. – N 3. – P. 83–89.
9. Issledovanie prichin social’nogo sirotstva – zhiznennyh situacij, kotorye privodjat k popadaniju detej v detskie uchrezhdenija / Analiticheskij centr pri Pravitel’stve RF. – Moskva, 2019. – 54 p.

10. Kefeli I.F., Kolbanev M.O. Asfacefotronika – nauka global'noj bezopasnosti v jepohu antropocena // Perspektivnye napravlenija razvitija otechestvennyh informacionnyh tehnologij. Materialy IV Mezhdunarodnoj konferencii, Sevastopol', 18–22 sentjabrja 2018 g.; nauch. ruk. B.V. Sokolov. – Sevastopol', 2018. – P. 216–219.
11. Kodaneva S.I. Kiberbulling: prichiny javlenija i metody preduprezhdenija // Social'nye novacii i social'nye nauki. – 2020. – N 1. – P. 149–159.
12. Kolin K.K., Ursul A.D. Informacija i kul'tura. Vvedenie v informacionnuju kul'turologiju. – Moskva: Izd-vo "Strategicheskie prioritety", 2015. – 288 p.
13. Korovnikova N.A. Rynok truda i cifrovaja jekonomika: Tendencii i perspektivy // Jekonomicheskie i social'nye problemy Rossii: Sb. nauch. tr. / RAN. INION. Centr social'nyh nauch. – inform. issled. Otdel jekonomiki; Red. kol.: Makasheva N.A., gl. red., i dr. – M., 2018. – № 1: Cifrovaja jekonomika: Sovremennoe sostojanie i perspektivy razvitija / Sost. vyp. Polozhikhina M.A. – P. 96–110.
14. Kudelina O.V., Adova I.B. Razvitie teorii chelovecheskogo kapitala v XXI v.: Novye trendy i rossijskij kontent // Vestnik Tomskogo gos. un-ta. Jekonomika. – 2020. – N 51. – P. 60–87.
15. Kuznecova T. F. Cifrovoe obshhestvo, cifrovaja kul'tura i gumanitarizacija vysshego obrazovanija: tezaurusnyj podhod. – Moskva: Izd-vo Mosk. gumanit. un-ta. – 2020. – 192 p.
16. Levashov V.K., Sar'jan V.K. Cifrovizacija i bezopasnost': problemy i reshenija // Social'nye novacii i social'nye nauki. – 2020. – N 1. – P. 37–46.
17. Mitin V. Sem' opredelenij cifrovoj jekonomiki // CRN IT-biznes. Novosti. – 2017. – URL: https://www.crn.ru/news/detail.php?ID=116780 (date of access 12.03.2020.).
18. Nacional'nye proekty: Celevye pokazateli i osnovnye rezul'taty. – Moskva, 2019. – 110 p.
19. Opaleva O.I. O nekotoryh aspektah podderzhanija chelovecheskogo kapitala v sovremennoj Rossii // Vestnik Moskov. gos. oblastnogo un-ta. Serija Jekonomika. – 2020. – N 1. – P. 19–26.
20. Polozhikhina M.A. Informacionno-cifrovoe neravenstvo kak novyj vid social'no-jekonomicheskoj differenciacii obshhestva // Jekonomicheskie i social'nye problemy Rossii: Sb. nauch. tr. / RAN. INION. Centr social'nyh nauch. – inform. issled. Otdel jekonomiki; Red. kol.: Makasheva N.A., gl. red. i dr. – Moskva: INION, 2017. – N 2: Neravenstvo v sovremennom mire: Jekonomicheskij i social'nye aspekty / Red.-sost. vyp. Prjazhnikova O.N. – P. 119–142.
21. Polozhikhina M.A. Sistema obrazovanija v Rossii s tochki zrenija formirovanija chelovecheskogo kapitala // Jekonomicheskie i social'nye problemy Rossii: Sb. nauch. tr. / RAN. INION. Centr social'nyh nauch. – inform. issled. Otdel jekonomiki; Red. kol.: Polozhikhina M.A., gl. red. i dr. – Moskva, 2018. – N 2: Obrazovanie v sovremennom mire: Social'nye i jekonomicheskie aspekty / sost. vyp. Semeko G.V. – P. 8–36.
22. Ryzhkov V. Chto takoe cifrovaja kul'tura? // KMDA. – 2019. – 15.04. – URL: https://komanda-a.pro/blog/digital_culture (date of access 29.01.2021).

The article was first published in Russian in the journal "Социальные новации и социальные науки". – 2021. – N 1. – P. 8–34.

HUMAN CAPITAL ASSESSMENT MODEL ON THE BASIS OF A UNIFIED DIGITAL PLATFORM OF SCIENTIFIC AND EDUCATIONAL RESOURCES

Viktor Medennikov

Doctor of Technical Sciences, Leading Researcher, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (Moscow, Russia)[1] E-mail: dommed@mail.ru

Abstract. *The article substantiates the need to reassess the role of human capital in the digital age. The author justifies the necessity to create an information space for scientific and educational institutions at the time when adequate education is the main source of human capital formation in any country. A method for assessing the level of human capital based on information scientific and educational resources is proposed. The corresponding calculations on the example of agricultural educational institutions are provided. The mathematical model for assessing the impact of human capital on the socio-economic situation in various regions of the country is also presented.*

Keywords: *human capital; digital economy; assessment of human capital; mathematical model; regional ratings.*

For citation: Medennikov V. Human capital assessment model on the basis of unified digital platform of scientific and educational resources / English transl. by Nikulichev M.Y. // Social Novelties and Social Sciences. – Moscow : INION. RAN, 2022. – N 1. – P. 89–100.

URL: https://sns-journal.ru/en/archive/ DOI: 10.31249/snsneng/2022.01.07

Introduction

The events associated with the coronavirus epidemic have triggered general demand for digital technologies in the economy and public life. Entrepreneurs are forced to accelerate digitalization of internal business processes, customer interaction, remote management, etc. The online insurance and banking services market is growing noticeably. The transition from offline to online mode had a deep impact on education, entertainment and retail, due to the need to transfer schoolchildren and students to a distance learning format, and company employees to a remote work mode.

At the same time, problems of staffing and user competencies of the population (human capital) became apparent. More than ever the digital economy requires highly qualified specialists and personnel retraining, from workers to senior managers, as well as modern management methods that match new information and communication technologies (hereinafter referred to as ICT).

In this context, there is a growing demand for research in the field of human capital (hereinafter, HC) and for redefining the role of digital technologies in the economy and society. At present, the increase in human capital, in addition to the factor of economic growth, is recognized as the target setting for individual development. HC is seen as an essential factor in the development of society.

Awareness of this factor predictably set the task of HC assessment using mathematical methods. Such an assessment, if it is based on an integrated approach, on a sufficient and reliable amount of information, makes it possible to choose the most effective ways for the development and use of human capital.

Problems in assessing human capital

Initially, HC was understood only as a set of investments in an individual that increased his ability to work – education and professional skills. Later, this concept began to expand due to an increase in the number of factors taken into account that affect wages, education, and work skills [Dobrynin, 1993]. For example, Francis Fukuyama introduces the concept of "trust" and proves that trust is the basis of HC. "The capitalization of the state lies not in GDP," he writes, "but in the level of trust, which creates value to a much greater extent than productive assets. Even American capitalism and in general any successful enterprise is born out of trust" [Fukujama, 2004].

Investment in people today includes not only expenses on education, healthcare, science, and labor mobility, but on finding economically valuable information as well. This is justified by the fact that information is one of the most important resources used by an individual in everyday activities. The information is understood as economic, social, scientific, technical and other information or indicators neces-

sary for making decisions. Therefore, the information must be objective, complete, reliable and up to date. And, of course, it should be understandable, as well as accessible to all strata of society. It is this information that becomes the decisive factor in human development and economic growth.

The importance of investments in the information sphere was substantiated by Jac Fitz-Enz in the form of the basic principles for measuring human capital [Nesterov, Ashirova, 2003].

1. People plus information – the path to the informational economy.

2. Management requires meaningful data; management without reliable data is impossible. The one with the best information wins.

3. Information about costs, time, quantity and quality in relation to HC serves as the basis for effective action.

Various methods for HC assessment, especially Russian methods, consist basically of verbal descriptions covering such a large number of factors that it is extremely difficult to establish their influence on human capital. This is primarily due to intercorrelation, i.e. functional relationship of variables, often leading to unreliable and fuzzy estimates [Uravnenie regressii …, 2015]. Unfortunately, the mathematical methods in HC analytics are based on too many assumptions about the homogeneity and constancy over time of both individual behavior and the functional dependencies of various factors, which does not correspond to reality and hinders practical application. In addition, there are few studies in this area in Russia, and foreign experience does not adequately describe domestic conditions. In this regard, there is a need to search for new approaches to the assessment of human capital.

Today, the major problem in Russia is the insufficient amount of structured data. This fact is confirmed by the developers of artificial intelligence technologies, who unexpectedly encountered this problem [Galust'jan, 2019]. After all, as mentioned above, the formation of a structured information space containing objective, complete, reliable and relevant data is one of the important areas of investment in HC.

Based on these conditions, a model was developed for the formation of the country's Unified Information Internet Space for Digital Interaction (hereinafter referred to as UIISDI), which integrated the unified digital platform (hereinafter referred to as the DP) for management of the economy and the unified information Internet space for scientific and educational resources (hereinafter referred to as UIISSER) [Medennikov, Muratova, Sal'nikov, 2014]. The DP is the unified cloud database for primary, technological and statistical data in various branches of the economy based on the unified system for collecting, storing and processing information, as well as on unified classifiers, directories, standards and other registers of all material, intellectual and human resources [Medennikov, Sal'nikov, Muratova, 2017].

UIISSER integrates in the unified cloud database the information scientific and educational resources (hereinafter referred to as ISER). The latter perform the following functions: supporting scientific

research, raising the educational level (including retraining) of people, and transferring scientific and educational knowledge to the economy. The ISER effectiveness is achieved due to unlimited access not only by traditional users (e.g., researchers, students and teachers), but also by future applicants and employers, representatives of government agencies, business, management and other interested parties. UIISSER can serve as a basis for assessing and improving the quality of the human capital generated in colleges, for determining its impact on the social and economic situation in the country.

ISER-based methodology for human capital assessment

Despite the different understanding of factors influencing the growth of human capital, most specialists agree that it is formed within the framework of the education system. Everyone agrees that HC includes, first of all, knowledge, skills and practical experience acquired by a person in the process of study, professional retraining, advanced training and self-education. Therefore, human capital is directly related to the quality of education in any country.

Taking into account the above considerations, a methodology for assessing the created human capital in the system of formal college education. To identify essential factors that affect the HC quality, it is advisable to rely on the Decree of the Ministry of Education and Science of the Russian Federation dated July 14, 2013 N 462 "Procedure for conducting self-examination by an educational institution", which defines the procedure for assessing college activities, which can be interpreted as an assessment of potential HC. Accordingly, the evaluation criteria should include the most important performance indicators of educational institutions that affect the quality of human capital by achieving the following goals:

– training of highly qualified specialists and scientists;

– conducting scientific research culminating in obtaining practical results, for instance, in the form of patents for inventions.

The results of these activities are affected, in addition to the use of UIISSER, by many other factors: for example, the level of applicants' readiness and motivation to study; the amount of funding for educational institutions; the state of science itself, the financial and moral work environment (the prestige); professional literacy of scientific technical management in ministries; demand for training specialists in a certain area from the society and the country's economy. However, not all of these diverse indicators can be expressed numerically, especially in terms of functional mathematical dependencies.

In this regard, the effectiveness of ISER of educational institutions presented on the Internet is taken as a general criterion for assessing the created HC. The integral criterion includes both data from the self-examination report, taking into account the basic requirements of the Ministry of Education and Science [Prikaz Ministerstva obrazovanija …, 2017] to the websites of educational institutions, as well as the demand for ISER from the society and the country's economy, the degree of influence on the quality of teaching and training of highly qualified specialists and scientists in colleges. Evaluation of sites using

sitemetric methods provides an opportunity to take into account the image and reputation of educational institutions.

The analysis of websites of industrial and educational institutions made it possible to identify a trend in services on the Internet in the form of various electronic trading platforms (hereinafter – ETP) and labor exchanges (hereinafter – ELE). Based on the modern understanding of human capital, it is obvious that such services affect its growth and should be included in the evaluation criteria. In addition, the choice of distance learning (hereinafter – DL) and retraining as a particular criterion of the methodology, as well as the possibility of obtaining qualified advice on professional issues, is justified. The basic principles of HC assessment dictate the need to account for the use of application software packages (hereinafter referred to as ASP), databases (hereinafter referred to as DB) and their quality in the methodology [Medennikov, Sal'nikov, Muratova, 2017].

Information resources (hereinafter, IR), included in the requirements of the Ministry of Education and Science and having the greatest impact on the educational results in colleges, are considered secondary educational information resources (hereinafter, SEIR). Indicators from the UIISSER list, with information about the ISER types (scientific research, publications, consulting activities in the form of the number of consultants in a particular field of knowledge, legal information, DO, ASP and DB), are primary scientific and educational information resources (hereinafter – PSEIR).

The ontological classification of ISER is associated with modern trends and capabilities of digital technologies, when hosting providers offer services for storing and processing site content in structured databases with powerful management systems (hereinafter, DBMS). The database content can be stored both in the form of an electronic catalog and as a full-format representation and is recognized as a form of IR storage. Storing site content in a non-DBMS (the predominant form today) is considered unordered representation. Storing site content in DBMS is called an ordered presentation (with the ability to navigate, for example, based on the CSCSTI catalogue (Code of State Categories Scientific and Technical Information): by organizations, industries and regions, by authors and their qualifications, by keywords, etc.). This can be considered as IR integration levels.

The ontological standardization of the IR representation in UIISSER allows to develop an independent comprehensive assessment methodology both for human capital formation at the macro level and for the entire activity of educational institutions. If colleges start introducing standardized sites, the use of techniques becomes automated and low-cost. Standardization of IR representation with measurable and comparable indicators (stored, for example, in a unified cloud DBMS) allows to evaluate not only college activities, but also the performance of research institutes using the same methodology. When indicators of regional development are added, this methodology allows to assess the readiness of educational institutions to influence the digital transformation of the economy in regional territories.

Based on the description presented, the general criterion for evaluating the human capital created by an educational institution is the sum of weighted groups of auxiliary evaluation criteria with the sum of weights equal to 1. The auxiliary evaluation criteria are: by PSEIR representation formats, by IR efficiency using sitometric methods, by ETP IR efficiency, by ELE IR efficiency, by SEIR status, by IR representation for DL, by the number of consultants on sites (with displaying main consultations topics).

The methodology was verified conducting test assessment of the human capital created by agricultural colleges based on the analysis of the relevant sites. A questionnaire was specially developed that included all indicators of auxiliary human capital assessment criteria. The questionnaire contains 214 college performance indicators of which 122 refer to college-level performance, 40 – to faculty level, 46 – to department level, and six indicators assess the structure and quality of the college site. The weight coefficients of the criteria were obtained by using a large set of different means: by expert evaluation; analysis of verbal opinions of specialists in the field of assessing the quality of education; methods for calculating ratings of educational institutions; by opinion polls among teachers; by using mathematical statistics methods suitable for these purposes [Medennikov, Sal'nikov, Muratova, 2017; Sirotkin, 2013; Ajvazjan, 2001]. To formalize the description, the following expressions are introduced:

i – PSEIR integration level code, $i \in I$;

l – PSEIR storage form code, $l \in L$;

n – PSEIR type code, $n \in N$;

m – number of the educational institution, $m \in M$;

h – code of the SEIR representation type, $h \in H$;

t – the moment of calculation time (calculations can be carried out at any moment when UIISSER is implemented);

P_j^{tm} – an auxiliary criterion for human capital assessment in terms of the efficiency of using the IR at the m-th college according to the j-th indicator at the moment t, $j \in J$;

P^{tm} – general criterion for evaluating the HC in terms of the efficiency of using IR at the m-th college at the moment t;

α_i^1 – the weight coefficient of the PSEIR integration level;

α_l^2 – the weight coefficient of the l-form of PSEIR storage;

α_n^3 – the weight coefficient of the n-th type of PSEIR representation;

β_j – the weight coefficient of the auxiliary criterion for human capital assessment in terms of the PSEIR efficiency the according to the j-th indicator;

$v_i^{tm}{}_{\ln 0}$ – the volumetric PSEIR characteristics at the i-th integration level, the l-th storage form, the n-th type of representation at the level of the m-th college at the moment t;

$vf_i^{tm}{}_{\ln f}$ – the volumetric PSEIR characteristics at the *i*-th integration level, the *l*-th storage form, the *n*-th type of representation at the level of the *f*-th faculty of the *m*-th college at the moment *t*;

$vk_i^{tm}{}_{\ln k}$ – the volumetric PSEIR characteristics at the *i*-th integration level, the *l*-th storage form, the *n*-th type of representation at the level of the *k*-th department of the *m*-th university at the moment *t*;

$\lambda_i^{tm}{}_{\ln}$ – the level of PSEIR evaluation at the *i*-th integration level, the *l*-th storage form, the *n*-th type of representation of the *m*-th college at the moment *t*, where:

$$\lambda_i^{tm}{}_{\ln} = (v_i^{tm}{}_{\ln 0} + \Sigma_f \, vf_i^{tm}{}_{\ln f} + \Sigma_k \, vk_i^{tm}{}_{\ln k}) \,/\, \max_m \, (v_i^{tm}{}_{\ln 0} + \Sigma_f \, vf_i^{tm}{}_{\ln f} + \Sigma_k \, vk_i^{tm}{}_{\ln k}) \quad (1);$$

d_{rm}^{t2} – the volumetric characteristics of the *r*-th indicator of the auxiliary criterion for HC assessment by sitometry methods at the *m*-th college at the moment *t2* ;

q_{rm}^{t2} – the volumetric characteristics of the *r*-th indicator of the auxiliary criterion for HC assessment by sitometry methods at the *m*-th college at the moment *t2*, where:

$$q_{rm}^{t2} = d_{rm}^{t2} \,/\, \max_m d_{rm}^{t2} \quad (2);$$

ω_r^2 – the weight coefficient of the *r*-th indicator of the auxiliary criterion for HC assessment by sitometry methods;

d_{sm}^{t3} – the volumetric characteristics of the *s*-th indicator of the auxiliary criterion for HC assessment in terms of the state of the ETP at the *m*-th college at the time *t3*;

ω_s^3 – the weight coefficient of the *s*-th indicator of the auxiliary criterion for HC assessment in terms of the ETP status, s ϵ S;

d_{gm}^{t4} – the volumetric characteristics of the *g*-th indicator of the auxiliary criterion for HC assessment in terms of the ELE status at the *m*-th college at the time *t4*;

ω_g^4 – the weight coefficient of the *g*-th indicator of the auxiliary criterion for HC assessment in terms of the ELE status, g ϵ G;

d_{hm}^{t5} – the volumetric characteristics of the *h*-th indicator of the auxiliary criterion for HC assessment in terms of the SEIR effectiveness at the *m*-th college at the time *t5*;

q_{hm}^{t5} – the volumetric characteristics of the *h*-th indicator of the auxiliary criterion for HC assessment in terms of the SEIR effectiveness at the *m*-th college at the time *t5*, where:

$$q_{hm}^{t5} = d_{hm}^{t5} \,/\, \max_m d_{hm}^{t5} \quad (3);$$

ω_{hm}^5 – the weight coefficient of the *h*-th indicator of the auxiliary criterion for HC assessment in terms of the SEIR effectiveness at the *m*-th college, h ϵ H.

The mathematical formula looks like:

$$P^{tm} = \sum_j \beta_j \cdot P_j^{tm} \quad (4), \text{ where}$$

$$P_1^{tm} = \sum_{i,l,n} \lambda_{i\ln}^{tm} \alpha_i^1 \alpha_l^2 \alpha_n^3 \quad (5),$$

$$P_2^{tm} = \sum_k \omega_k^2 q_{km}^{t2} \quad (6),$$

$$P_3^{tm} = \sum_s \omega_s^3 d_{gm}^{t3} \quad (7),$$

$$P_4^{tm} = \sum_g \omega_g^4 d_{gm}^{t4} \quad (8) \text{ and}$$

$$P_5^{tm} = \sum_h \omega_h^5 q_{hm}^{t5} \quad (9)$$

The presented model was used to assess the level of college-generated human capital (Table 1).

Table 1

Assessment of the human capital generated at agricultural colleges, in terms of SEIR representation

№	Description	Value, %
1.	Percentage of PhD teachers among the whole teaching personnel e share of the number of faculty members with a PhD degree in the total number of faculty members of the university	4,27
2.	Percentage of teachers with Doctorate degree among the whole teaching personnel	4,44
3.	The total area of teaching classrooms per to one student, sq m	4,59
4.	Computers per student, pcs	4,70
5.	College income from all types of activities per one faculty member	4,57
6.	College income from commercial activities per one faculty member	4,67
7.	Income of one average faculty member from all types of activities to the average salary in the region	3,98
8.	Number of students funded by the federal budget	4,43
9.	Number of students funded by the regional budget	8,39
10.	Number of students funded by private individuals or by business	4,50
11.	The number of full-time undergraduates admitted to the first-year classes without entrance exams as a result of victories at all-Russian and international school competitions	4,59
12.	The average score of full-time first-year students enrolled on the basis of the Unified State Examination	4,95
13.	Percentage of first-year students from rural areas	4,27
14.	Citations in the Web of Science database per one hundred faculty members	4,69
15.	Citations in the Scopus database per one hundred faculty members	4,64
16.	Citations in the Russian Science Index database per one hundred faculty members	4,55
17.	Number of articles indexed in the Web of Science database per 100 faculty members	4,60
18.	Number of articles indexed in the Scopus database per 100 faculty members	4,59
19.	The number of publications listed in the RSCI per 100 faculty members	4,49
20.	The share of students settled in dormitories to the number of students in need of accommodation	4,58
21.	The share of state-funded full-time graduates who got employed in the agricultural sector, in government-run institutions, or were drafted into the Armed Forces	4,55

The weight coefficients of assessment criteria for college-generated HC by types of SEIR representation were determined by four methods of mathematical statistics: correlation analysis, Kendall's concordance coefficient, probabilistic assessment model, calculation of the competence matrix. The calculation results of all four statistical methods were highly consistent [Medennikov, Sal'nikov, Muratova, 2017]. This means that any of the considered methods, as well as their combination, may be used in practice, depending on the availability of information (for example, average performance results and ratings).

Estimates of the college-generated HC in terms of the IR effectiveness are given in: [Medennikov, Sal'nikov, Muratova, 2017].

General estimates of the ISER effectiveness in Russian agricultural colleges, as well as their ratings according to this indicator, are presented in Table. 2.

Table 2

Evaluation of the ISER effectiveness (%) and ratings of agrarian colleges in Russia

College	Score	Rating	College	Score	Rating
Kuban State Agrarian University	39,09	1	Buryat State Agricultural Academy	22,48	28
Orlovsky State Agrarian University	38,31	2	Altai State Agrarian University	22,19	29
Russian State Agrarian University	32,49	3	Ivanovo State Agricultural Academy	21,29	30
Krasnoyarsk State Agrarian University	30,79	4	Kursk State Agricultural Academy	21,21	31
Novosibirsk State Agrarian University	30,55	5	Kurgan State Agricultural Academy	21,11	32
Kemerovo State Agrarian University	30,26	6	State University for Land Management	20,79	33
Bryansk State Agrarian University	29,37	7	Izhevsk State Agricultural Academy	20,66	34
Belgorod State Agrarian University	29,23	8	Primorskaya State Agricultural Academy	20,28	35
Kazan State Agrarian University	28,31	9	Samara State Agricultural Academy	19,69	36
Saratov State Agrarian University	27,51	10	Orenburg State Agrarian University	19,59	37
Moscow State Academy of Veterinary Medicine and Biotechnology	26,39	11	Yaroslavl State Agricultural Academy	19,49	38
Penza State Agricultural Academy	26,28	12	Voronezh State Agrarian University	19,12	39
Volgograd State Agrarian University	26,21	13	Ryazan State Agrarian University	19,11	40
Bashkir State Agrarian University	25,57	14	Far-East State Agrarian University	18,89	41
St-Petersburg State Agrarian University	25,22	15	Irkutsk State Agrarian University	18,79	42
Vyatka State Agrarian University	24,59	16	Kazan State Academy of Veterinary Medicine	18,69	43
Omsk State Agrarian University	24,49	17	St. Petersburg State University of Veterinary Medicine	18,49	44
Vologda State Dairy Academy	24,42	18	South Ural State Agrarian University	18,38	45
Don State Agrarian University	24,31	19	Kabardino-Balkarian State Agrarian University	17,55	46
Michurinsky State Agrarian University	24,19	20	Yaroslavl State Agricultural Academy	17,19	47
Stavropol State Agrarian University	24,12	21	Kostroma State Agricultural Academy	16,67	48
Ural State Agrarian University	23,79	22	State Agrarian University of the Northern Trans-Urals	16,59	49
Velikoluga State Dairy Academy	23,69	23	Gorsk State Agrarian University	15,89	50
Nizhny Novgorod State Dairy Academy	23,49	24	Russian State Agrarian Correspondence University	15,52	51
Chuvash State Dairy Academy	23,31	25	Smolensk State Dairy Academy	15,41	52
Ulianovsk State Dairy Academy	23,21	26	Dagestan State Agrarian University	12,43	53
Perm State Dairy Academy	22,79	27	Tver State Dairy Academy	5,78	54

The low information density of websites demonstrates that the influence of the ISER quality on the college-generated HC is underestimated (Tab. 3).

Studies have shown that, in general, information density of websites is still very far from optimal. On average, they contain a little more than half (55.4%) of all the necessary information. The R&D indicators reflect only 18.3% of research activities. This confirms the assumption that the Ministry of Education and Science and Rosobrnadzor underestimate scientific activity of colleges which is reflected in the requirements to websites.

Table 3

The quality and quantity of ISER on the websites of agricultural colleges

№	Types of ISER	Percentage of sites with this ISER, %	Unsorted list	E-catalog	Unsorted full-length representation	Sorted full-length electronic representation
1.	R&D	85	3684	391	337	248
2.	Publications	89	18649	408	344	0
3.	Data bases	11	530	45	0	0
4.	ASP	2	828	2	25	0
5.	DL	12	1195	0	0	3
6.	Consultants	25	216	43	9	0
7.	Regulatory and legal information	55	65	0	328	19

It can also be concluded that colleges still consider their sites as showcases and do not make efforts to use rationally. The visiting audience consists primarily of applicants and students, but not businessmen, managers, scientists and the public. The ISER data is not informative (quality) and is presented rather unprofessionally. Gradually websites are improving: electronic catalogs and unsorted full-format presentations have become common; however, the sorted full-format DBMS-based presentations, as well as ASP and DB, cannot be found on web-sites. The absence of a DBMS results in a visible discrepancy between ISER types at the college-, faculty- and department levels.

Model for assessing the human capital impact on the socio-economic situation in the regions

In the method described above, the obtained values can be interpreted as an estimate of the human capital generated by the educational institution of the *m*-th region in the *t*-th period.

To assess the HC impact on the social and economic situation in the regions, it is necessary to consider assessment criteria. This requires to account for regional ratings R_k^{tm}, reflecting their socio-economic status, where k is the rating number, $k \in K$. To simplify the model, we will assume that there is only one college in each region, or, if there are several, P^{tm} will reflect some average estimates for these colleges. By normalizing P^{tm} ranks, we will derive the college ratings according to the HC assessment – P^{0tm}.

Some generalized regional rating of the social and economic situation in the regions must be introduced:

$$R^{tm} = (\sum_{k=1}^{K} \eta_k R_k^{tm}) / K \quad (10),$$

where η_k are positive numbers reflecting the weights of all terms and $\sum_{k=1}^{K} \eta_k = 1$ (11). The weights are selected depending on the industry potential of the regions and the degree of statistical dependence of P^{0tm} and R_k^{tm}.

At the same time, the set K can be divided into three groups, the first two of which, K_1 and K_2, are the components of social well-being, and the third, K_3, reflects the economic situation.

The first group of criteria includes: Gini coefficient (level of income distribution); poverty level; unemployment rate; mortality rate, etc. When normalized, they are ranked in ascending order, i.e. the best rates of the social well-being component have lower values. For example, a region with a lower Gini coefficient is more socially prosperous, since the income discrepancy in the population is lower, etc. The second group of criteria includes: employment level; fertility rate; share of the population with higher education; life expectancy, etc. When normalized, they are ranked in the descending order, i.e. the best rates of the social well-being component have higher values. For example, a region with a higher employment level is more socially prosperous, and so on. The third group represents the regional ratings of the economic situation: socio-economic development; subsidies to regions; production efficiency, etc.

The assessment of HC impact on the social and economic situation and development in the region will depend on the P^{0tm} and R^{tm} ratio. When $P^{0tm} < R^{tm}$ the HC in the region is underdeveloped. The reasons may be different: lack of funding for the education system, insufficiently qualified teaching personnel in colleges, the curriculum that does not meet the requirements of the region, etc. The $P^{0tm} > R^{tm}$ ratio means that regional HC is underused. Again, the reasons can be different: low innovation level in the region, the regional requirement for specialists below the potential of colleges, migration of college graduates from the region, etc. The $P^{0tm} = R^{tm}$ ratio reflects a balance between the potential of colleges and the local demand for specialists. If necessary, this rating can be converted into digital form.

By introducing the value $\Delta^{tm} = P^{tm} - P^{t-t_1,m}$, where t-t_1 is the time lag, it is possible to estimate the degree of change for better or worse in the quality of regional human capital.

By summing up the corresponding regional estimates with some weights, it may be possible to assess HC impact on the social and economic situation and development of society at the federal level. For this purpose, appropriate methods can be used to find statistical dependencies of college rankings, reflecting the assessment of the HC quality, and the most important regional rankings, reflecting the social and economic situation in the regions.

Conclusion

Back in the 1960s, the outstanding Soviet scientist A.I. Kitov together with Academician V.M. Glushkov proposed a draft of the National Automated System for Collecting and Processing Information for Accounting, Planning and Management of the National Economy (NAS) [Glushkov, 1975; Peters, 2016]. NAS was intended for operational accounting and control over any object in the country. On its basis, it was possible to effectively plan and predict the development of society, including human capital. The rejection of this project led to emergence of numerous heterogeneous and functionally incompatible information systems in most organizations in the country. The continuation of that trend hin-

ders the progress of National projects in Russia (especially the "Digital Economy" project) and decreases the quality of human capital in the country.

The Unified Internet Information Space of the country's scientific and educational resources considered in the work is the implementation of the NAS project in the digital age. The proposed UIISSER digital platform, which is organically included in the Unified Internet Information Space for Digital Interaction within the country, is a powerful tool for transferring the most effective innovative solutions to the economy, for improving the HC quality and welfare of the society as a whole.

References

1. Ajvazjan S.A. Teorija verojatnostej i prikladnaja statistika. – Moskva : JuNITI-DANA, 2001. – 656 p.
2. Dobrynin A.I. Proizvoditel'nye sily cheloveka: struktura i formy projavlenija. – Sankt-Peterburg: Izd-vo UJeF, 1993. – 164 p.
3. Fukujama F. Doverie: social'nye dobrodeteli i put' k procvetaniju. – Moskva: OOO "Izdatel'stvo AST", 2004. – 730 p.
4. Galust'jan A. Pjat' problem, kotorye poka ne mozhet reshit' Iskusstvennyj intellekt // RUSBASE. – 2019. – 26.02. – URL: https://rb.ru/opinion/problemy-ii/ (date of access 01.02.2021).
5. Glushkov V.M. Makrojekonomicheskie modeli i principy postroenija OGAS. – Moskva: Statistika, 1975. – 160 p.
6. Medennikov V.I., Muratova L.G., Sal'nikov S.G. Modeli i metody formirovanija edinogo informacionnogo internet-prostranstva agrarnyh znanij. – Moskva: Izdatel'stvo GUZ, 2014. – 426 p.
7. Medennikov V.I., Sal'nikov S.G., Muratova L.G. Metodika ocenki jeffektivnosti ispol'zovanija informacionnyh nauchno-obrazovatel'nyh resursov. – Moskva: Analitik, 2017. – 250 p.
8. Nesterov L., Ashirova G. Nacional'noe bogatstvo i chelovecheskij kapital // Voprosy jekonomiki. – 2003. – N 2. – P. 103–110.
9. Peters B. How not to network a nation: the uneasy history of the soviet internet. – MIT Press, 2016. – 298 p.
10. Prikaz Ministerstva obrazovanija i nauki RF ot 14 ijunja 2013 g. N 462 "Ob utverzhdenii Porjadka provedenija samoobsledovanija obrazovatel'noj organizaciej" (s izmenenijami i dopolnenijami) /Garant. – 2017. – 14.12. – URL: https://base.garant.ru/70405358/ (date of access 01.02.2021).
11. Sirotkin G.V. Sistemnyj analiz faktorov kachestva obrazovanija v vuze // Prikaspijskij zhurnal: upravlenie i vysokie tehnologii. – 2013. – N 2 (22). – P. 109–118.
12. Uravnenie regressii. Uravnenie mnozhestvennoj regressii // SYL. – 2015. – 07.04. – URL: https://www.syl.ru/article/178055/new_uravnenie-regressii-uravnenie-mnojestvennoy-regressii (date of access 01.02.2021).

The article was first published in Russian in the Journal "Социальные новации и социальные науки". – 2021. – No. 1. – P. 107–120.

DIGITALIZATION OF PERSONAL ARCHIVES AND THEIR FURTHER APPLICATION. CASE STUDY

Vlada Petushkova

PhD in Economics, Senior Researcher, Department of Economics, Institute for Scientific Information on Social Sciences, Russian Academy of Sciences (Moscow, Russia)

E-mail: vladapetushkova@yandex.ru

Abstract. *The article discusses the process of digitalization of personal archives, specifically, of the unique archive of the Chairman of the Council of Ministers of the USSR A.N. Kosygin. The article describes the algorithm for creating a complete, systematized electronic version of the collection in stages, as well as the preparation for a historical and biographical exhibition.*

Keywords: *digitalization; personal archives; A.N. Kosygin; document digitization; documentary exhibitions; creation of an electronic database.*

For citation: Petushkova V.V. Digitalization of personal archives and their further application. Case study / English transl. by Nikulichev M.Y. // Social Novelties and Social Sciences. – Moscow : INION RAN, 2022. – N 1. – P. 101–114.

URL: https://sns-journal.ru/en/archive/ DOI: 10.31249/snsneng/2022.01.08

Introduction

The 21st century ushered a fundamental change in data representation. Since the advent of book printing in the 15th century, which marked the transition from the Middle Ages to the Modern Age, society has pursued the goal of verbalizing concepts, but with the transition to digital technologies, it is now moving towards the visualization of facts. This process has affected all spheres of human life and fully relates to archival historical and biographical work.

Meanwhile, a huge layer of visual historical heritage is still little known to the public due to difficulties in access. This particularly concerns the 20th century materials, when photography and documentary cinematography helped make a significant progress in the preservation, transmission, and presentation of visual historical materials to the mass consciousness. At present, technologies are developing so rapidly that whole classes of the 20th century recording devices, which previously were considered the pinnacle of technical achievements, are now being archived in the literal and figurative sense. The main problem is that the carriers of historical information have a limited lifetime and are gradually disappearing.

Personal archives demand particular attention because they provide a glimpse into the deep essence of events and make an invaluable contribution to filling in the "blank spots" associated with some historical facts. Unfortunately, there is no generally accepted procedure for dealing with such historical and cultural values in Russia; it still remains at the discretion of private owners, non-state foundations or trustees. Personal archives get sometimes lost for lack of demand, difficulties with storage and cataloguing for the owners, not to mention the lack of professional research processing and presentation to the public. This task dictates the need for the fastest digitalization of such historical heritage, understood as a set of measures for processing, systematization and analysis of materials using modern digital technologies.

Important theoretical approaches to digitalization of archival collections are listed in the fundamental work – a collection of articles by leading specialists in the field, compiled by E.A. Vorontsova [Rol' arhivov v informacionnom ..., 2017].

The purpose of this article is to acquaint readers with the project of streamlining a large personal archival collection, carried out on the basis of the non-state "Ekaterina" Cultural Foundation in 2010-2016 with the support from the State Archive of the Russian Federation (GARF). The project deals with the personal archival collection of the Chairman of the USSR Council of Ministers Alexei Kosygin – a man who lived a unique life, starting as a young Red Army soldier, a successful businessman-gold miner in Siberia, director of a weaving factory in Leningrad and author of the ice Road of Life project during the

years of the Leningrad blockade and becoming the Chairman of the USSR Council of Ministers. For 16 years A.N. Kosygin was the Premier of the Soviet government, and is remembered as an effective organizer of the economy and an outstanding diplomat, known for his peacekeeping initiatives [Fenomen Kosygina, 2016]. The task of working on the archive was not only to generalize and perpetuate its content with the help of digital technologies, but also to implement the historical and biographical exhibition project "The Kosygin Phenomenon", designed both for professionals and for the wide audience. The project management focused on practical, rather than theoretical, issues, but certain methods and approaches may be of use to the scientific community.

Digitalization of A.N. Kosygin's archive

Presenting the biography of a major statesman, directly related to the events that changed the course of the Russian history, required serious documentary justification and a balanced approach.

At the first stage of digitizing the Kosygin's archive it was necessary to physically design the electronic database in order to generalize the entire array of storage units. Almost any personal archive contains several main sections: documents, photographs, letters, material objects. Physical systematization allows to quickly navigate in the materials. The electronic database created later fully corresponds to the real structure described above.

Electronic databases of large archives are usually created with Microsoft Access or similar software; this is a standard practice at GARF [Rol' arhivov v informacionnom ..., 2017, p. 571]. It was decided to use Microsoft Excel to digitize the archive for the purposes of a private fund; at least data input and changes to the documents in Excel did not require the participation of trained IT specialists. It was essential to provide specialists with quick and error-free access to the originals, since among the storage units there were both reprints made from electronic copies and virtual / interactive works created on their basis and original documents. The original photographic albums and folders for documents themselves are of historical value, but in some cases, it is possible to apply inventory numbers and names to them using a manual printer.

At first glance, the digitization of manuscripts and photographic documents seems to be a technically simple process that can be performed by an employee with basic skills in the Photoshop graphics editor. As a rule, it is carried out with a specialized scanner using A4 – A2 paper format. Alternatively, a professional camera mounted on a vertical tripod can be used. Digitizing at a resolution below 300 dpi does not make sense. A resolution of 300 dpi or more allows to get high-quality typographic prints for catalogs in future. In order to obtain prints of higher quality and larger format used for exhibitions, as a rule, photographs are scanned at 600 dpi in TIFF format. Since the scanned high-resolution images take up a lot of memory, it is advisable to store them on removable hard drives [Metodicheskie rekomendacii ..., 2013].

It should be noted that when a document is scanned, a short-term intense light exposure occurs, which can accelerate the aging of documents. Multiple scanning is simply unacceptable. Photographic documents from the beginning of the 20th century are considered to be the most resistant to light. Particularly sensitive, vulnerable to such influence are color photographs, as well as black and white prints of the 1990s. Such sensitivity to scanning can be explained by the technological process and the quality of materials used in those years in photographic workshops. To minimize the "flare" effect on documents, the specialized archival scanners using reflected light are used to digitize valuable historical documents [Metodicheskie rekomendacii ..., 2013].

Archival planetary scanners are very expensive and only a few organizations can afford them [Shmajlov, 2011]. For example, they were used to scan unique documents of the USSR State Defense Committee, which was the highest body of power and authority during the Great Patriotic War. To digitize the documents in the Fund No. 644, stored in the Russian State Archive of Socio-Political History, six planetary scanners were required. With their help, more than 200 thousand pages were digitized, most of which were in poor condition. To convert these documents into electronic form, A2 format scanners and lampless projectors were used to save worn-out copies from exposure. In order to protect documents from physical damage, non-contact scanning methods have been applied. The scanned array was posted on the site "Documents of the Soviet era" along with other World War II materials [Ocifrovany dokumenty ..., 2015].

When digitizing documents, it is recommended to simultaneously create electronic thumbnail (preview) images with full size not exceeding several tens of Kb. They will be used in the future to form an electronic inventory of the archive. The inventory serves as an addition to the electronic database, is the first step in preparing for an exhibition or creating a catalog and includes the following data presented in the table format: date a document was created, author, content (description), persons, size, thumbnail image. The table may be called a "museum" inventory – such a system is applicable regardless of the type of storage units: photographs, manuscripts or objects (for example, personal items and gifts that need to be photographed and the resulting thumbnail images must be included in the museum inventory).

After systematizing the A.N. Kosygin's archive, a fairly large array of data was obtained, which could be used both statistically and graphically. Various filters provided in some software programs sort data chronologically, by titles, personal names or by other parameters that users deem necessary to enter into the table. Statistica-10 is a convenient electronic database package for managing personal archives.

Computer statistical analysis can be considered a very useful technique for making decisions regarding the creation of sections of the catalog or exhibition. The "Archive Structure" diagram for visualizing archive contents (Fig. 1).

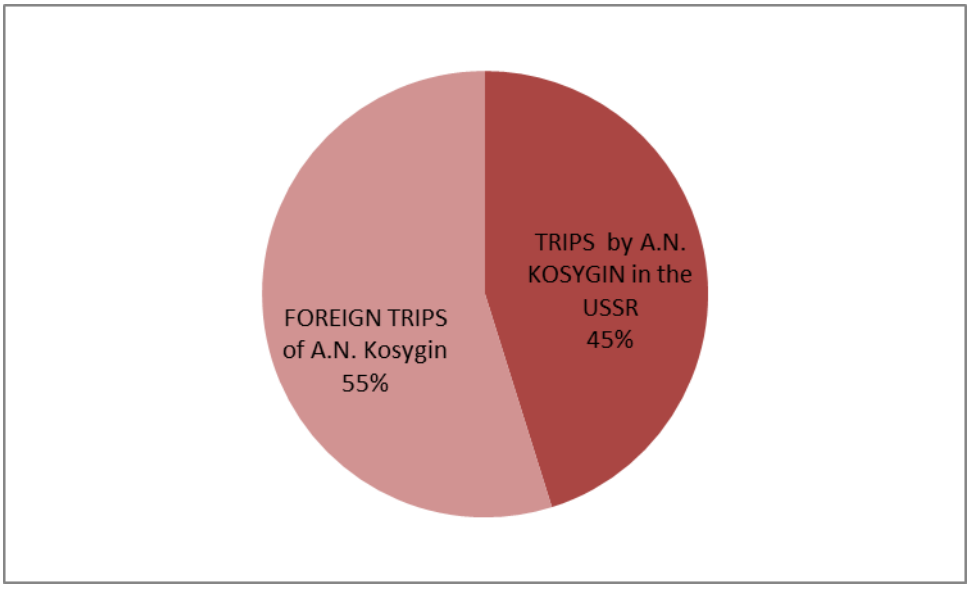


Fig 1. The structure of the section "Official photographic documents" from the personal archive of A.N. Kosygin

For example, documents in the section "Foreign trips of A.N. Kosygin" could be stored chronologically or alphabetically to correspond to the names of the countries visited. According to the results of statistical analysis, the main share of photographic documents related to foreign trips falls on one decade, the period from the early 1960s to the early 1970s (Fig. 2). Consequently, the chronological principle of constructing a section is useless, and it is reasonable to use an alphabetical catalog by the name of the host countries.

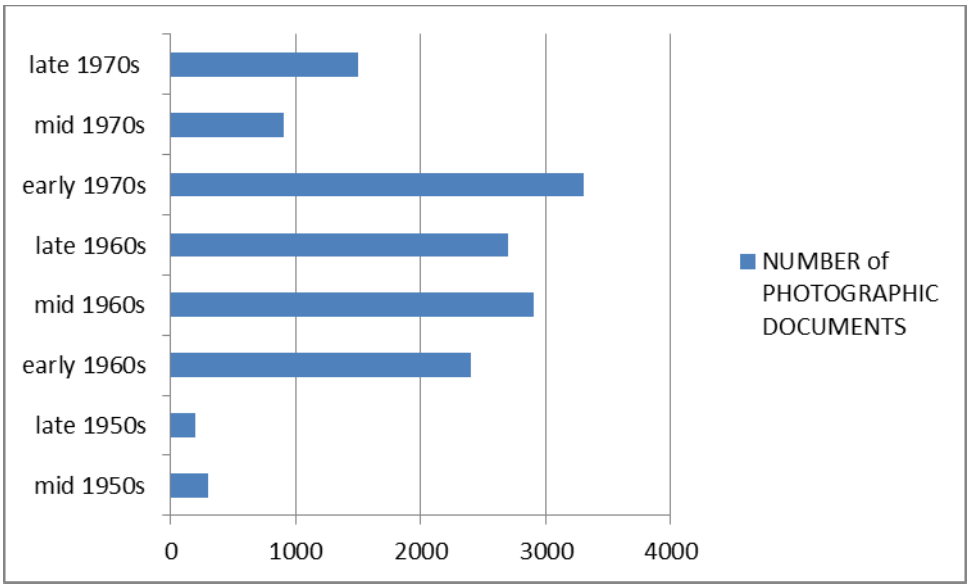


Fig. 2. The structure of the section "Foreign visits" from A.N. Kosygin's personal archive. The number of photographic documents relating to different periods

After six years of work a complete, systematized electronic copy of A.N. Kosygin's personal archive was created. Subsequently, the material archive itself was transferred to the SARF in order to ensure its safety. The "Ekaterina" Cultural Foundation retained its digital version, which makes it easy to carry out museum exhibition projects, print catalogs, create Internet content and virtual exhibitions.

The digital version of personal archives opens up wide opportunities for curators and designers of exhibitions. Quite often there is a need to mend small scratches, glue particles, folds, traces of rust (resulting from the use of paper clips) or compensate for losses on photographic documents. Some photos require color correction. Should archival photographic documents be modified before printing? This question cannot be answered unambiguously. The documentary exhibition favors photographs without editing or artistic improvements. Editing of photographic documents carried out during digitization can also interfere with further identification of materials, create unnecessary layers. The presentation style of photographic documents is largely determined by the goals and objectives of the exhibition – documentary or artistic, as well as its design. In any case, work should be carried out with a copy, keeping the original digitized documents untouched [Metodicheskie rekomendacii ..., 2013]. The subsequent exhibitions dedicated to the activities of A.N. Kosygin serve as excellent examples of how digitized archival materials can be used.

Express exhibition "A.N. Kosygin. Lines of Life"

In 2015, the Express Exhibition "A.N. Kosygin. Lines of Life" was conducted to commemorate the 50th anniversary of his economic reforms. The exhibition included video materials and archival documents, as well as unique gifts received by A.N. Kosygin during foreign visits and trips around the USSR. For instance, exhibits from his out-of-town residence in the Arkhangelskoye village were presented, most of them never shown before. The project was implemented with the participation of the Multimedia Art Museum, Moscow, the press service of the President of the Russian Federation, the All-Russian State University of Cinematography.

The project was planned as a documentary exhibition with elements of artistic design and, according to the official press release, combined "scientific themes with elements and conceptual principles of contemporary art" [Kosygin, 2015]. Documentary exhibition as a genre "unites heterogeneous elements with a single idea, concept, artistic design: originals and copies of documents, explanatory texts and descriptions of documents, artistic, architectural and spatial elements. Documentary exhibition combines scientific and artistic elements into a single documentary-object-spatial and visual-figurative system, which possesses information and sensory potential to influence the visitor and remains one of the important channels of communication between the archive and the user of archival information," writes Yu. AT. Afiani [Rol' arhivov v informacionnom ..., 2017, p. 740].

The curators attracted much attention, including the student audience, by designing a poster depicting Mona Lisa holding a magazine with a photograph of Kosygin under her arm. The A2 canvas image was placed on a stretcher at the entrance. The image is not a modern computer collage, but an archival document, an imprint from a digitized cover of the "Vecko Journalen" magazine, which published a report on the visit of A.N. Kosygin to Sweden in 1972 (Fig. 4).

Fig. 3. View of the exhibition gallery "A.N. Kosygin. Lines of Life", Financial University, Moscow, 2015

The express exhibition "A.N. Kosygin. Lines of Life" is a visual demonstration of achievements in domestic and foreign policy during the forty years of A.N. Kosygin's tenure in the highest power structures, thanks to which the scientific community is turning to his legacy today.

Fig. 4. The poster from the exhibition "A.N. Kosygin. Lines of Life". Financial University, Moscow, 2015

"The Kosygin Phenomenon" exhibition

The project "A.N. Kosygin. Lines of Life" served as a dress rehearsal for the large-scale exhibition "The Kosygin Phenomenon", which took place in November 2016 – February 2017 in Moscow. The general concept of presenting the material was suggested by the structure of his personal archive. The exhibits were divided into the following topics: Kosygin during the Great Patriotic War, Kosygin as the head of the Soviet Government, Kosygin as an international politician and diplomat. The economic and foreign policy sections were considered equally important and reflected the significance of these two areas in A.N. Kosygin's work.

Overview of the section "A.N. Kosygin during the Great Patriotic war".

Interestingly, the documents available until 2015 at the disposal of non-state funds could not provide direct documentary evidence of A.N. Kosygin's activities as a member of the State Defense Committee (GKO) and one of the authors of the "Road of Life" project. But in the last decade, many documents related to the period of the Great Patriotic war have been declassified. Researchers were allowed access to the most important, previously classified materials (the Politburo of the Central Committee, All-Union Communist Party Communist Party of the Soviet Union, etc.), and could copy documents and their publications on the pages of domestic and foreign magazines and newspapers. This phenomenon has been called the "archival" or "archaeographic revolution" [Rol' arhivov v informacionnom ..., 2017, p. 63]. In 2015, in the "Documents of the Soviet era" section on the "Archives of Russia" website, thousands of documents from the highest Soviet governing body during the Great Patriotic War were posted in the public domain. In an interview with "Rossiyskaya Gazeta", the head of the Federal Archival Agency of Russia, A.N. Artizov said that on the archive portal, anyone can look through and read 239,700 digital documents, including: signed resolutions and orders, minutes of meetings of the GKO Operations Bureau in 1943-1945, signed by L. Beria, draft resolutions edited by I. Stalin and other GKO members of the USSR [Novosjolova, 2015; Ocifrovany dokumenty ..., 2015].

At present, not only archivists, but researchers of related specialties, as well as interested citizens, have received free access to sources that previously were sealed within the walls of state archives. Creating custom sites that post abstracts, and sometimes offer previews of documents, allows to better navigate the material even without visiting the State Archives. Nevertheless, the search for thematic documents is still a rather specific and complex task that requires special training and skills in working with archival materials. Perhaps documentary exhibitions will become some kind of intermediaries between the public and archival materials prepared by specialists.

The exhibition "The Kosygin Phenomenon" displayed the originals of the most significant documents related to the work of A.N. Kosygin during the war and orders from the State Defense Committee. For example, a report by L.M. Kaganovich, A.N. Kosygin, N.A. Voznesensky and L.P. Beria to I.V. Sta-

lin on approving the draft resolution on the construction of the railway from the Voybokalo station to Leningrad dated January 10, 1942, i.e. link to the legendary "Road of Life" [Kosygin: K 112-letiju …, 2016, p. 70]. The exhibition also featured original maps and diagrams on routes for people and freight on the frozen Lake Ladoga for the period from November 24, 1941 to March 30, 1943. The exhibition materials were accompanied by a video sequence "Traffic on the ice of Lake Ladoga", prepared on the basis of digitized documentary film provided by the Russian State Documentary Film and Photo Archive (RGAKFD).

It should be noted that the "Ice Road of Life" Museum (village Kokkarevo, Leningrad Region) features an independent historical monument, an "Ice Road" diorama with an extraordinary artistic impact, created by the participants in those tragic events [Pod Peterburgom umiraet ..., 2020]. The curators of the exhibition had a plan to gradually digitize the stationary diorama and to re-create it in the exhibition space of the "Ekaterina" Cultural Foundation. However, due to the complexity of the work, this idea was never implemented.

The section "A.N. Kosygin as the head of the Soviet government".

The next part of "The Kosygin Phenomenon" exhibition focused on the post-war recovery of the USSR economy. Numerous exhibits of the Council of People's Commissars (SNK) of the Russian Federation (RSFSR) and the USSR of this period, provided by the GARF in the form of digital copies of documents, were presented on several electronic multimedia tablet kiosks. Visitors to the exhibition could independently familiarize themselves with the materials using computer navigation and a specially designed menu.

In particular, the activity of A.N. Kosygin as chairman of the commission on the 1947 monetary reform, which was carried out in order to strengthen the ruble exchange rate, abolish the rationing system and move to uniform state prices [Gvishiani, 2004, p. 74]. "The Kosygin Phenomenon" exhibition featured originals and reprints of banknotes and securities that existed before and after the 1947 currency reform.

In the late 50ies A.N. Kosygin becomes the Premier of the USSR. In 1959 he was appointed Chairman of the State Planning Committee, and in May 1960 – First Deputy Chairman of the Government. Simultaneous he became the full member of the Presidium of the Central Committee of the CPSU. A.N. Kosygin perfectly understood how the life of Soviet people differed from the Western standards and sought to establish the production of consumer goods in the USSR, including light industry and automotive products [Kosygin: K 112-letiju …, 2016, p. 113, 220]. At "The Kosygin Phenomenon" exhibition, a podium with the "Moscow Fashion House" collection was installed in the center of one of the halls, displaying samples of costumes from the late 1940s, 1950s and 1960s. Bright, light fabrics, fashionable

styles have become a symbol of a new, peaceful time. An honorable place in the exhibition was also given to the "Zhiguli" car first model.

But the most famous were the so-called "Kosygin reforms", put into effect by the resolutions of the Central Committee of the CPSU and the Council of Ministers in 1965–1969 that affected various sectors of the Russian economy. A facsimile signature of Leonid Brezhnev and A.N. Kosygin can be seen on the documents displayed in the "Head of the Soviet Government" section. Although the ideas that shaped 1965 reforms were called "libermanism" in the West, after the name of Evsei Liberman (professor at the Kharkov Institute of Engineering and Economics), it was A.N. Kosygin's article "Plan, Profit, Prize", published in the newspaper "Pravda" on September 9, 1962, that initiated the all-Union economic discussion, which confirmed the effectiveness of the proposed measures [Lisovickij, 2016, p. 433–452]. The eighth or so-called "golden five-year plan" (1966–1970), during which impressive economic indicators were achieved in the USSR, became the crowning achievement of A.N. Kosygin's government.

A.N. Kosygin, like no other among the Soviet power elite, knew and understood economic mechanisms. Consider for example a little-known fact of his biography, reflected in the exhibition at the "Ekaterina" Foundation. After graduating from the Petrograd cooperative technical school, Alexei Kosygin was sent to work with the Siberian Krai (Regional) Union, and then with the Novosibirsk Cooperative Union as an instructor-organizer [Andrianov, 2004, p. 37]. He becomes a successful and prosperous prospector, participates in a gold mining enterprise in Siberia, and only in 1930 returns to his native St. Petersburg (by that time already Leningrad) [Gvishiani, 2004, p. 34].

Based on the in-depth study of the personal archive, it can be concluded that A.N. Kosygin, having spent forty years in the highest power echelons, never aspired to occupy a dominant position in the Soviet state, being content with second or third roles. His attempt to carry out reforms in 1965 was also dictated by considerations to optimize the economy, and not by the desire to rise on the political Olympus [Andrianov, 2004].

A.N. Kosygin as an international politician and diplomat.

A.N. Kosygin's foreign policy is an interesting topic for research. It should be noted that his role in international relations, as well as his contribution to the Victory in the Great Patriotic war, apparently, were downplayed deliberately during the Brezhnev period, as they could lead to unnecessary comparisons with the head of state. During the years of perestroika the public and historiographers lost interest in the Soviet period; as a result, the legacy of the Chairman of the USSR Council of Ministers was largely forgotten. "The Kosygin Phenomenon" exhibition partially filled in the gap.

For instance, in 1966, A.N. Kosygin initiated and mediated the meeting in Tashkent between the leaders of India and Pakistan, which ended with the signing of the historical peaceful Tashkent Declaration. The exhibition featured photographs, documents and gifts presented to A.N. Kosygin in those days.

The Soviet newsreel documentary "Meeting in Tashkent", provided by the RGAKFD, featured prominently at the exhibition [Rybakova, 1966]. For many years the documentary was stored in the Krasnogorsk archive, and the faded film was not suitable for viewing. The "Ekaterina" Cultural Foundation had the film digitized, restored and presented at "The Kosygin Phenomenon" exhibition (Fig. 5).

Fig. 5. Participants of the Tashkent meeting from left to right: President of Pakistan Mohammed Ayub Khan, Prime Minister of India Lal Bahadur Shastri, Chairman of the Council of Ministers of the USSR A.N. Kosygin. Tashkent, 1966

In 1970, on the initiative of the Chairman of the Council of Ministers of the USSR A.N. Kosygin, negotiations were held with the Federal Chancellor of the West Germany Willy Brandt, who arrived in Moscow on an official visit, and the first peace treaty between the USSR and West Germany (FRG) was concluded. The Article 3, Treaty of Moscow, was essential. It clearly stated that both countries "regard today and shall in future regard the frontiers of all States in Europe as inviolable such as they are on the date of signature of the present Treaty, including the Oder-Neisse line which forms the western frontier of the People's Republic of Poland and the frontier between the Federal Republic of Germany and the German Democratic Republic." [Kosygin: K 112-letiju …, 2016, p. 284–289]. From the German side, the Treaty was signed by the Federal Chancellor of the Federal Republic of Germany W. Brandt, and from the Soviet side – by the Chairman of the USSR Council of Ministers A.N. Kosygin (Fig. 6).

Fig. 6. Federal Chancellor of the Federal Republic of Germany W. Brandt and Chairman of the Council of Ministers of the USSR A.N. Kosygin after signing the Treaty of Moscow, Moscow, August 11, 1970

In June 1967, the summit was held between US President Lyndon B. Johnson and Chairman of the USSR Council of Ministers A.N. Kosygin in Glassboro (New Jersey) in connection with the Six Day War between Israel and the Arab countries. Despite the fact that no final agreements were reached, the meeting between L.B. Johnson and A.N. Kosygin initiated dialogue between the two countries during the Cold War and paved the way for the 1968 treaty on the non-proliferation of nuclear weapons (Fig. 7).

Fig. 7. "Life" magazine cover with a photograph of the Chairman of the Council of Ministers of the USSR A.N. Kosygin, US President Lyndon B. Johnson and translator V.M. Sukhodrev, June 30, 1967

Conclusion

A.N. Kosygin is a prominent figure in the 20th century Russian history. "Aleksey Nikolaevich Kosygin for two decades headed the Soviet government – the Council of Ministers of the USSR. Many significant pages of our history are connected with his name. Large-scale evacuation of factories to the east of the country during the Great Patriotic War, the supply of besieged Leningrad and the rescue of people along the Road of Life, the post-war development of oil and gas and mining complexes, and light industry. Among his achievements is the economic reform, rightfully called after his name – "Kosygin", – said in the welcoming speech of the Chairman of the Government of the Russian Federation Dmitry Medvedev to the organizers and guests of the historical and documentary exhibition "The Kosygin Phenomenon" [Medvedev: idei Kosygina ..., 2016]. However, there are few biographical literary sources about Kosygin and only two historical monographs. Work with the personal archive of the chairman of the Council of Ministers of the USSR opens up little-known facts about his biography, about his foreign policy achievements and peacekeeping initiatives.

"The Kosygin Phenomenon" exhibition in 2016–2017 for the first time presented unique documents of the Soviet period, demonstrated the potential of using the latest digital technologies in archiving. About 30 exhibitors took part in "The Kosygin Phenomenon" exhibition, including museums, archives,

libraries, as well as private collectors. But the core of the exhibition was made up of the virtual version of A.N. Kosygin's personal archives.

Personal archives are an invaluable source of documentary historical materials that can become the foundation, among other things, for modern monographic exhibitions built around digital technologies. Researchers of personal archives face such tasks as identification, preservation and sorting of physical objects, processing and classification of digitized documents, setting up a multimedia archive, creative processing of the electronic materials for subsequent usage, including exhibitions. These tasks can be performed using various methods for digitizing documentary historical heritage.

This article shows the path taken by the personnel of "The Kosygin Phenomenon" project from creating an electronic database of the personal archive to designing a modern exhibition catalog with the help of advanced technologies. Some approaches to organizing a historical and archival exhibition project from developing the concept to arranging an exhibition space are applicable in many other similar cases and can be quite universal.

References

1. A.N. Kosygin. Linii zhizni // Finansist. Novosti, sobytija, meroprijatija Finansovogo Universiteta. – 2015. – N 161. – URL: http://old.fa.ru/projects/finansist/Documents/journals/160.pdf (date of access 04.12.2020).
2. Andrianov V.A. Kosygin / ZhZL: Ser. Biogr. – Moskva: Molodaja gvardija, 2004. – Vyp. 878. – 366 p.
3. Fenomen Kosygina // CULTOBZOR. – 2016. – 16.11. – URL: http://cultobzor.ru/2016/11/fenomen-kosygina/ (date of access 26.02.2021).
4. Gvishiani A.D. Fenomen Kosygina. Zapiski vnuka. – Moskva: Fond kul'tury "Ekaterina", 2004. – 308 p.
5. Kosygin: K 112-letiju so dnja rozhdenija. Katalog istoriko-dokumental'noj vystavki / vstup. st. A.N. Artizova, O.V. Hlevnjuka. – Moskva: Kuchkovo pole, 2016. – 352 p.
6. Lisovickij V.N. Evsej Liberman – ideolog Kosyginskoj hozjajstvennoj reformy // Istoriko-jekonomicheskie issledovanija. – 2016. – Vol.17. – N 3. – P. 433–452.
7. Medvedev: idei Kosygina vazhny dlja ponimanija slozhnosti zadach, stojavshih pered stranoj // ITAR TASS. – 2016. – 16.11. – URL: https://tass.ru/obschestvo/3788229 (date of access 04.12.2020).
8. Metodicheskie rekomendacii po jelektronnomu kopirovaniju arhivnyh dokumentov i upravleniju poluchennym informacionnym massivom // Federal'noe arhivnoe agentstvo. – 2013. – URL: http://archives.ru/documents/rekomend_el-copy-archival-documents/razdel-2.shtml#39 (date of access 04.12.2020).
9. Novosjolova E. Dokumenty jepohi v odin klik // Rossijskaja gazeta. Federal'nyj vypusk. – 2015. – N 129 (6700). – 17.06. – URL: https://rg.ru/2015/06/17/dokumenti.html (date of access 04.12.2020).
10. Ocifrovany dokumenty Gosudarstvennogo komiteta oborony SSSR / Oficial'nyj sajt korporacii "JeLAR". – 2015 – 09.04. – URL: https://elar.ru/press-center/news/otsifrovany_dokumenty_gosudarstvennogo_komiteta_oborony_sssr/ (date of access 04.12.2020).
11. Pod Peterburgom umiraet unikal'nyj muzej ledovoj Dorogi zhizni. Potomki veteranov prosjat uchastija Putina / Fontanka.Ru. – 2020. – 06.03. – URL: https://www.fontanka.ru/2020/03/06/69019093/ (date of access 04.12.2020).
12. Rol' arhivov v informacionnom obespechenii istoricheskoj nauki: sb. st. / sost. E.A. Voroncova; otv. red. V.Ju. Afiani, Ju.A. Petrov. — Moskva: Jeterna, 2017. – 1008 p.
13. Rybakova A. Vstrecha v Tashkente / Annotacija k dokumental'nomu fil'mu CSDF // Oficial'nyj sajt RGAKFD. – 1966. – URL: http://old.rgakfd.ru/catalog/films/ (date of access 04.12.2020).
14. Shmajlov D. Planetarnoe skanirovanie — ot konkretnyh zadach k vozmozhnostjam // Oficial'nyj sajt mezhotraslevogo jekspertnogo izdanija "Je. Dok". – 2011. – 02.03. – URL: https://www.edok-journal.ru/articles/kultura/planetarnoe_skanirovanie_ot_konkretnykh_zadach_k_vozmozhnostyam/ (date of access 04.12.2020).
15. Vizit Villi Brandta k A.N. Kosyginu i podpisanie dogovora mezhdu SSSR i FRG / Annotacija k dokumental'nomu fil'mu CSDF // Oficial'nyj sajt RGAKFD. – 1970. – URL: http://old.rgakfd.ru/catalog/films/ (date of access 04.12.2020).

The article was first published in Russian in the Journal "Социальные новации и социальные науки". – 2021. – N 1. – P. 155–168.

SOCIAL NOVELTIES AND SOCIAL SCIENCES

scholarly journal

№ 1 (6) / 2022

Technical editing and computer layout
V.B. Sumerova

Proofreader L.N. Kazimirova

Institute of Scientific Information for Social Sciences,
Russian Academy of Sciences (INION RAN)
Nakhimovsky pr., 51/21
Moscow, B-418, ГСП-7, 117997

Editions e-mail: sns.journal@bk.ru

Подписано на выход в свет – 27/IX – 2022 г.

Формат 60×90/8 Уч.-изд.л. 8,1