Nexo Revista Científica
Vol. 36, No. 05 (Especial), pp. 169-179/Noviembre 2023

ISSN-E 1995-9516
Universidad Nacional de Ingeniería

http://revistas.uni.edu.ni/index.php/Nexo
http://dx.doi.org/10.5377/nexo.vXXiXX.XXXX

Conceptual foundations and global challenges in the formation of digital sovereignty of the state

Fundamentos conceptuales y desafíos globales en la formación de la soberanía digital del Estado

Dilmurad Iakhiaev[1,*], Aleksei Grigorishchin[1], Lyudmila Voronina[2], Diana Dementeva[1], Irina Ivanova[1]

[1] Northern (Arctic) Federal University named after M.V. Lomonosov. Russia.
[2] N. Laverov Federal Research Center for Integrated Arctic Research of the Ural Branch of the Russian Academy of Sciences. Russia.
*Corresponding author: dilmurad-92@mail.ru

(recibido/received: 17-junio-2023; aceptado/accepted: 01-octubre-2023)

ABSTRACT

The study aims at determining the conceptual basis for the formation of digital sovereignty under the influence of external factors. The article uses the methods of content analysis and graphic modeling. The study shows external challenges that have the greatest impact on the formation of digital sovereignty of the state. Only international cooperation and respect for the digital sovereignty of individual countries can help ensure security during the global digital transformation.

Keywords: digital sovereignty, state, global challenges, digital security, digital infrastructure, digital transformation.

RESUMEN

El estudio pretende determinar la base conceptual de la formación de la soberanía digital bajo la influencia de factores externos. El artículo utiliza los métodos de análisis de contenido y modelización gráfica. El estudio muestra los desafíos externos que tienen mayor impacto en la formación de la soberanía digital del Estado. Solo la cooperación internacional y el respeto de la soberanía digital de cada país pueden ayudar a garantizar la seguridad durante la transformación digital global.

Palabras claves: soberanía digital, estado, retos globales, seguridad digital, infraestructura digital, transformación digital.

1. INTRODUCTION

Intensive digital globalization has a strong impact on the sovereignty of individual countries. Due to a growing number of threats in the field of digital security, it becomes relevant to study the conceptual foundations of the formation of digital sovereignty of the state.

J. Westerman and V. Dhara were among the first to use the term “digital sovereignty” (Dudin et al., 2021). The scholars introduced this concept to assess the degree of autonomy and security of a country’s digital

infrastructure from external challenges and threats. This definition is based on the ability of government institutions to respond to external hacker attacks (cyber attacks), i.e., technological threats to a greater extent.

Considering digital sovereignty, M.N. Dudin, S.V. Shkodinskii, and D.I. Usmanov (2021) define it as the resulting stage of digital reforms of the socio-economic system carried out by the state. According to their approach, digital sovereignty characterizes the stability of socio-economic systems in the face of external challenges and threats, not only technological but also economic and political.

V.A. Nikonov, A.S. Voronov, V.A. Sazhina, S.V. Volodenkov, and M.V. Rybakova (2021) understand digital sovereignty as the independence of the state in the use of digital technologies to realize national interests. This approach implies that the state is the main actor shaping the concept of digital transformation and the main regulator of the digitalization of economic sectors. The government apparatus determines both the integration of external technological solutions into domestic markets and the volume of exports of domestic innovations to foreign markets. Digital reforms of the national economy are implemented with due regard to the existing technological potential and resources. Development strategies of large businesses are adjusted considering government priorities, and new players emerge in the digital space. S.V. Volodenkov focuses on the state's ability to use digital technologies, i.e., the level of skills and competences of government entities required for the effective implementation of digitalization policies, relying on their own technological solutions. Thus, Volodenkov (2020) emphasizes no identity of digital knowledge in scientific schools, including applied ones, under rapidly changing conditions.

Defining digital sovereignty, A.P. Kochetkov, K.V. Maslov, V.E. Dementev, and V.V. Bukharin highlight the ability of the state to independently pursue policies in the information or digital space and control the information that is distributed in its territory (Bukharin, 2016; Dementev, 2022). Considering the growing activity of global information dissemination channels in the form of social networks, instant messengers, and video hosting sites, government agencies need to, if necessary, regulate their activities. Since these Internet technologies store personal and other data of a country's population, they can also act as platforms for waging information wars. S.Yu. Chimarov's object of research is digital data that the state can confidentially and independently use (Bertrand, 2019; Chimarov et al., 2022). Digital data created by the population and organizations in a particular country are an asset managed by the state.

However, to implement the basic principle of digital sovereignty (independence), the state needs its own digital technologies, equipment, and other solutions. Thus, the authors emphasize systemic import substitution to increase the independence of the digital economy from external supplies (Astapenko, 2022; Fadeeva, 2022; Nikonenko et al., 2021). Under the conditions of protectionist policies, countries with a low level of digital economy and technological development become dependent on progressive countries. In relation to technologically undeveloped countries, the threat of introducing artificial restrictions is, on the one hand, a mechanism to restrain the digital transformation of their economy and, on the other hand, an instrument of manipulation, which has a major impact on socio-economic and inner political processes.

It is worth mentioning the issues of ensuring the security of intellectual property as an element of information security in cyberspace (Kartskhiya, 2014).

One of the factors of the digital sovereignty of the state is the information security system, whose role is to prevent and combat cyber attacks at various levels (Emelyanov et al., 2022; Kukutai, Taylor, 2016). Until recently, cyber attacks were initiated by groups of individuals, but today these threats become more systemic. Public-private paramilitary institutions are created and developed to violate the integrity of a country's digital infrastructure.

The digital infrastructure of the state is the core of digital sovereignty. A.S. Semchenkov (2019) highlights the state's ability to maintain the security and sustainability of the national digital infrastructure as the main element of digital sovereignty. V.E. Dementev (2022) identifies the primary and secondary levels of digital infrastructure as the basis of digital sovereignty: microelectronics and 5G technologies; artificial intelligence platforms and technologies. In our opinion, these components of the digital infrastructure do not determine the entire structure of digital sovereignty.

Based on the comparative analysis of approaches to determining the digital sovereignty of the state, we formed our own approach. Digital sovereignty refers to the ability of the state to independently create, develop, and maintain the security and sustainability of the national digital infrastructure in all sectors of its economic activity.

The study aims to determine the conceptual basis for the formation of digital sovereignty under the conditions of external pressure.

2. MATERIALS AND METHODS

We compared scientific literature and analyzed data from the World Intellectual Property Organization (2021), the International Telecommunication Union (2023), and the United Nations (2020). In the process, we used the research methods of content analysis and graphic modeling.

3. RESULTS AND DISCUSSION

After a comparative analysis of scientific literature, external conditions were identified that determine the formation of digital sovereignty of a modern state with due regard to the most significant technological, economic, political, and social challenges and threats (Fig. 1).

3.1. Emerging external threats

Hacker attacks on critical infrastructure facilities and information resources have become widespread over the past decades. The negative consequences of cyber attacks are financial losses, decreased productivity, damage to reputation, liability to other actors, etc. Global damage from cybercrime in 2021 amounted to about $6 trillion. Cyber attacks have provoked the active development and implementation of mechanisms to combat cyber attacks at the state and international levels. Table 1 presents data on the ranking of countries according to the Global Cybersecurity Index, which is compiled based on a conceptual structure, including legal, technical, and organizational measures, capacity development, and cooperation. Some states are unable to prevent cyber attacks on their own and have to build cooperative ties with more developed countries or institutions. The worst-case scenario of this threat is the likelihood of control and management of government institutions and the development of cyber terrorism and cyber warfare (information warfare).

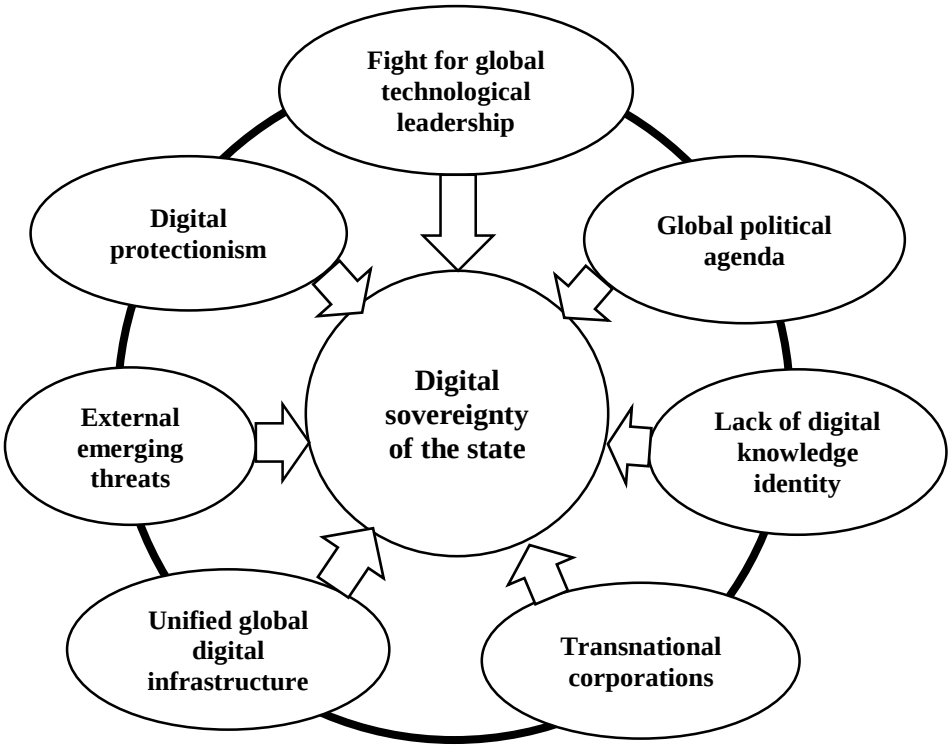

Figure 1. Scheme of external challenges that have the greatest impact on the formation of digital sovereignty of the state.

Another aspect of emerging threats is the misuse of intellectual property, including in cyberspace, which leads to a violation of the integrity of the state's digital infrastructure. Since 2010, many countries have prevented these threats by developing and implementing relevant regulations.

Table 1. Ranking of countries in the global cybersecurity index (based on the UN International Telecommunication Union data) (International Telecommunication Union, 2023).

Country	2018	2020
UK	1	2
USA	2	1
France	3	9
Norway	9	17
Japan	14	7
Germany	22	13
Russia	26	5

Some countries began to form an institutional environment. For example, Russia adopted Federal Law No. 187-FZ "On Amendments to Certain Legislative Acts of the Russian Federation on the Protection of Intellectual Rights in Information and Telecommunication Networks" in 2013. The document provides rights holders of a particular intellectual property with the opportunity to protect it by limiting access to the resources on the Internet.

In 2011-2012, the USA initiated two bills (Stop Online Piracy Act and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act) aimed at protecting copyrights and combating the theft of intellectual property. However, these bills were not supported due to severe penalties for offenses and the expansion of powers of the law enforcement system.

Along with the protection of copyright and patent rights in cyberspace, there is a need to protect trade secrets and production secrets (know-how). The European Parliament introduced the Directives on the Protection of Trade Secrets and Know-How in the EU in 2013 to harmonize legislation across all member countries. In Germany, know-how is protected by the rules on unfair competition. In the USA and UK, these are the rules of common law. In Russia, this area is regulated by Federal Law No. 98-FZ "On Trade Secrets" and Chapter 75 of the Civil Code (The European Parliament and the Council of the European Union, 2016; Kartskhiya, 2014).

3.2. Global political agenda

Currently, serious transformations are taking place in the global political world order: the bipolar world of the 20th century established after the collapse of the USSR was first replaced by a unipolar one, and now several poles of power are steadily forming, which will reshape relations based on new principles in the near future. The author and ideologist of the political science concept of a multipolar world is the Russian political thinker and philosopher A.G. Dugin (2011). The rejection of past globalization is only gaining momentum. It is considered natural and inevitable, but a serious challenge for the world community, which is expressed in increased political confrontation, struggle for spheres of influence, undermining the foundations of international relations, and the outbreak of local military conflicts.

The current geopolitical situation, on the one hand, causes exponential growth in the development of digital technologies due to the rivalry between countries and corporations. On the other hand, it leads to the digital superiority of some states and associations in the struggle for resources and, ultimately, for global political leadership. Under the conditions of uncontrollability, these processes can provoke a further increase in tension and contradiction between states. Thus, the role and importance of international institutions and organizations in establishing and consolidating the basic principles and rules of the digital development of civilization is also increasing.

Being the main international institution for maintaining peace and security, the UN creates conditions for universal digital equality and calls for using digitalization to accelerate the achievement of sustainable development goals for the planet. Population inequality can be significantly reduced with a balanced introduction of digital technologies in public administration, education, healthcare, labor organization, food production, communications, etc. (United Nations, 2020). Digital data and technology should be used to create more flexible policy strategies. Cooperation between countries in the digital space will help reduce geopolitical tensions and create global fair standards in the field of security and respect for human rights. These theses are contained in the reports of the High-level Panel on Digital Cooperation and the UN Secretary-General's Strategy on New Technologies (United Nations Secretary-General, 2018).

Thus, balanced digital development of the world and its regions can be achieved only based on the principles of international cooperation, healthy competition, and mutual respect for the digital sovereignty of countries.

3.3. Fight for global technological leadership

In the last decade, structural changes occurred in the national economies of the leading powers. The active implementation of innovative strategies in the economic model of developed and developing countries accelerated technological progress, and centers of scientific and technological development (clusters) began to form. In 2021, according to the World Intellectual Property Organization, the top 100 science and technology clusters are located in 26 countries, including six middle-income economies (China, India, Brazil, Iran, Turkey, and Russia) (Fig. 2). The largest number of clusters is located in the USA (24), China (19), Germany (9), and Japan (5). Many Western clusters conduct more intensive scientific and

technological activities compared to Asian ones. However, Chinese clusters have demonstrated the greatest growth in scientific and technological results over the past year.

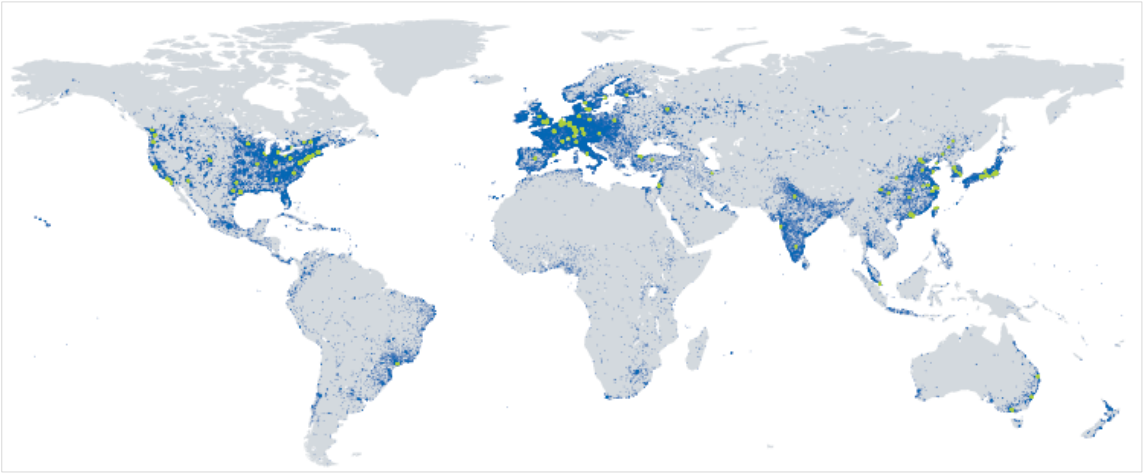

Figure 2. Map of the 100 leading science and technology clusters in the world, 2021 (Nugraha, Sastrosubroto, 2015).

Global technological leadership has become an aspect of economic policy that has influenced the import and export priorities of both states and state unions. The struggle of countries for technological superiority is a way to develop their technological independence. The model of globalization based on cooperation in the field of science and technology has been replaced by a model of creating technological autonomies.

The digital sovereignty of underdeveloped states suffers from high-tech threats, i.e., it becomes an object and a means of influence of world technological leaders, which can lead to the digital colonization of undeveloped countries.

Thus, the introduction of high technologies in many areas, including nationally significant ones, guarantees the competitiveness of national economies (Yan, 2021). According to the Global Innovation Index, the level of innovative development of some states in the period 2019-2022, which was also associated with current challenges (for example, the COVID-19 pandemic), is presented in Table 2. Index values characterize both activity in the field of innovation and the innovative potential of the state.

A race is unfolding among the leading countries to develop technologies in the field of AI (Acharya, Arnold, 2019). In 2017, China introduced a plan for the development of AI by 2030, with a total funding of $150 billion.

Table 2. Ranking of countries in the Global Innovation Index (based on the database of the World Intellectual Property Organization (2023)).

Country	2019	2020	2021	2022
Switzerland	1	1	1	1
UK	5	4	4	4
USA	3	3	3	2
France	16	12	11	12
Norway	19	19	20	22
Japan	15	15	13	13
Germany	9	9	10	8
China	14	14	12	11
Russia	46	47	45	47

3.4. Unified global digital infrastructure

Existing elements of digital infrastructure in the form of fiber-optic communication lines and mobile towers (3G, 4G, 5G) provide access to the global Internet only for part of the world's population. Creating and maintaining infrastructure in remote and rural areas (especially Arctic territories) is a difficult task that requires serious financial investments.

In the last decade, an alternative method has emerged, i.e., high-quality and high-speed satellite Internet from low-Earth orbit, which will allow developers of space technologies and satellites to cover the whole world. However, not all states have the capabilities and resources necessary for the development of their space industry. The leaders in the number of spacecraft and their launches remain the USA, Russia, China, Japan, India, France, and the UK (Kamolov, Mirakova, 2019).

Other countries are also trying to enter the new space race, but the lack of infrastructure to launch satellites, their own scientific and technological developments in the space industry, and other resources limit their capabilities.

Not only states and state corporations are interested in developing services to provide high-speed broadband satellite Internet access. The SpaceX project Starlink to form the global satellite system is actively developing.

Thus, the accessibility of a unified global digital infrastructure also affects the digital maturity of countries.

3.5. Digital protectionism

Many states have to implement a policy of digital protectionism due to the digitalization of the global economy, the blurring of national boundaries of digital markets, cross-border modes of communications and data transfer, and the vulnerability and weak risk protection of digital infrastructure.

Artificial restrictions on the import of digital technologies, goods, data, and services have both positive and negative consequences for the digital sovereignty of the state. On the one hand, an active import substitution policy can contribute to the development of the state's own digital technologies. On the other hand, the lack of competition from imported goods can lead to a decrease in the quality of domestic goods and an incentive to innovate, weakening digital sovereignty.

Regulating the flows and volumes of digital data transmission on the World Wide Web creates a trend of data deglobalization at the national level (Nugraha, Sastrosubroto, 2015). In this regard, individual states (groups or unions) try to ensure the security of their national digital space (Markova, Meleshkina, 2021). Problems with information security have formed a global trend of digital culture/digital hygiene. The population, business organizations, and government agencies strive for the safe use of digital technologies. The latter leaves a digital footprint, jeopardizing the security of personal data. Many countries have established mandatory requirements for global digital companies (for example, Google) to localize the databases of their citizens in their territory.

The need to localize and protect citizens' personal data has gradually developed into digital protectionism in the trade sector. With the launch of large global marketplaces, it became possible to buy goods from anywhere in the world. However, it also became more difficult for national economies to support domestic producers and control the movement of goods and their quality in terms of compliance with internal standards. In response to these challenges, countries decided to establish various trade and financial barriers to the import of digital goods and services. To increase the share of local companies in the national e-commerce market, Australia adopted a value-added tax from the sender for each foreign goods parcel in

2017. Foreign marketplaces are required to register legal entities in the country and pay taxes to the budget (Australian Taxation Office, 2020).

In a global market economy, it is necessary to find a balance between the sovereign interests of the state in matters of digitalization of the national economy and ensuring its digital security. Domestic digital technologies should be improved through imported innovations and not completely replaced by foreign ones. National digital technologies should be exposed to world markets while being reasonably regulated and considering the interests of the producing country.

3.6. Lack of digital knowledge identity

In the era of intensive digitalization, digital competences become a new pole of power. The system of higher education and science performs the functions of reproduction, dissemination, and protection of scientific ideas. It formulates requirements and qualitative criteria for assessing the digital competences of university graduates and researchers. In many countries, unique research clusters are built that use their own methodologies for creating and developing academic and scientific knowledge. This results in fragmented and sometimes closed-door solutions to the same fundamental and applied problems.

Although leading universities are integrated into the Bologna Process and the scale of international academic exchange programs is increasing, the development of scientific schools, including in the field of information technology and information security, is still fragmented. Heterogeneous knowledge in the field of information security is a key problem in the digital integration of economic systems.

3.7. Transnational corporations

The expanded geography of transnational corporations has a positive impact on the socio-economic systems of the countries where they operate. Positive changes are connected with the transfer of knowledge and the introduction of new technologies and management methods. Transnational corporations act as a source of foreign direct investments in regions and industries.

Many transnational corporations are moving to digital business design. The share of digital corporations that provide services through their own platforms (Google, Amazon, Apple, Microsoft, eBay, Airbnb) is increasing and entering new countries through not only geographic diversification but also digital expansion (the collection, storage, and processing of data). The number of users is gradually growing and the coverage of user data is expanding. This data becomes a new resource in the digital and high-tech market. Possessing a unique array of data, including personal data, corporations can influence social, economic, and political processes in the territories where they operate. Thus, the main threat is the transition of certain state functions to the influence area of transnational corporations.

Other negative trends may arise during investment expansion and vertical integration through a merger of local small- and medium-sized businesses that either compete with corporations in attempts to develop and implement innovative technologies or provide other services to the same consumers (Dhulipala et al., 2023).

These threats affect the digital sovereignty of states that need to take active measures. One of the main approaches to reducing risks is international cooperation to develop uniform regulatory standards in the functioning of the largest transnational technology companies.

4. CONCLUSION

The matrix of external conditions we developed will allow both leading powers and developing countries to build a system of response measures in the field of digital transformation policy with due regard to current

threats and challenges. The systematic approach reflected in digital reforms of the socio-economic development of states will reduce risks in the adoption of digital solutions by various industries. A scientifically based and well-balanced approach to studying the positive potential and specifics of external factors in the formation of digital sovereignty can turn these global challenges into global opportunities.

5. ACKNOWLEDGMENTS

The research was conducted with the financial support of the project FSRU-2023-0017 as part of the state assignment for fundamental scientific research on the topic "Challenges and prospects for the development of digital sovereignty of the Russian Federation", 2023.

REFERENCES

Acharya, A., Arnold, Z. (2019). Chinese public AI R&D spending: Provisional findings. Center for Security and Emerging Technology (CSET) Issue Brief. Retrieved from https://cset.georgetown.edu/research/chinese-public-ai-rd-spending-provisional-findings/ (date of access: October 20, 2023).

Astapenko, P.N. (2022). Tsifrovoi suverenitet kak uslovie realizatsii gosudarstvennogo suvereniteta v internet-epokhu [Digital sovereignty as a condition for the implementation of state sovereignty in the Internet era]. Zakon i pravo, 9, 27-33.

Australian Taxation Office. (2020). Goods and services tax (GST) when you sell to Australia. Retrieved from https://www.ato.gov.au/General/Other-languages/In-detail/Information-in-other-languages/Goods-and-services-tax-(GST)-when-you-sell-to-Australia/

Bertrand, A. (2019). How does digital government become better government? Retrieved from https://www.ey.com/en_za/government-public-sector/how-does-digital-government-become-better-government (date of access: October 20, 2023).

Bukharin, V.V. (2016). Komponenty tsifrovogo suvereniteta Rossiiskoi Federatsii kak tekhnicheskaya osnova informatsionnoi bezopasnosti [Components of the digital sovereignty of the Russian Federation as a technical basis for information security]. Vestnik MGIMO Universiteta, 6(51), 76-91. https://doi.org/10.24833/2071-8160-2016-6-51-76-91

Chimarov, S.Yu., Chimarov, N.S., Byalt, V.S. (2022). Pravovoe soderzhanie tsifrovogo suvereniteta Rossii v kontekste natsionalnoi paradigmy konstitutsionalizma [Legal content of Russia's digital sovereignty within the national paradigm of constitutionalism]. Vestnik Sankt-Peterburgskoi yuridicheskoi akademii, 4(57), 31-34.

Dementev, V.E. (2022). Perspektivy Rossii pri tsifrovom dominirovanii Kitaya i SShA [Prospects for Russia under the digital dominance of China and the United States]. Problemy prognozirovaniya, 4(193), 6-17. https://doi.org/10.47711/0868-6351-193-6-17

Dhulipala, R., Mehrotra, N., Kanitkar, A. (2023). The vision of a digital public infrastructure for agriculture. T20 Policy Brief. Retrieved from https://t20ind.org/wp-content/uploads/2023/06/T20_PolicyBrief_TF2_252_DPI4A-N.pdf

Dudin, M.N., Shkodinskii, S.V., Usmanov, D.I. (2021). Tsifrovoi suverenitet Rossii: Barery i novye traektorii razvitiya [Digital sovereignty of Russia: Barriers and new development directions]. Problemy rynochnoi ekonomiki, 2, 30-49. https://doi.org/10.33051/2500-2325-2021-2-30-49

Dugin, A.G. (2011). Geopoliticheskoe budushchee Rossii: Mnogopolyarnost i osnovnye strategicheskie perspektivy v XXI v [Geopolitical future of Russia: Multipolarity and main strategic prospects in the 21st century]. Vestnik Moskovskogo universiteta. Seriya 18. Sotsiologiyaipolitologiya, 2, 68-97.

Emelyanov, A.A., Korshunov, I.L., Mikadze, S.Yu. (2022). K voprosu o tsifrovom suverenitete Rossii [On the issue of digital sovereignty of Russia]. Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta, 6(138), 84-90.

The European Parliament and the Council of the European Union. (2016). Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Retrieved from https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0402 (date of access: October 7, 2023).

Fadeeva, I.A. (2022). Tsifrovaya ekonomika i tsifrovoi suverenitet: Vyzovy i ugrozy [Digital economy and digital sovereignty: Challenges and threats]. Konkurentosposobnost v globalnom mire: Ekonomika, nauka, tekhnologii, 10, 75-78.

International Telecommunication Union. (2023). Global cybersecurity index. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (date of access: October 7, 2023).

Kamolov, S.G., Mirakova, D.A. (2019). Kommertsializatsiya kosmicheskoi deyatelnosti: Klyuchevye trendy sovremennosti [Commercialization of space activities: Key trends of our time]. Intellekt. Innovatsii. Investitsii, 7, 52-63. https://doi.org/10.25198/2077-7175-2019-7-52

Kartskhiya, A.A. (2014). Kiberbezopasnost i intellektualnaya sobstvennost [Cybersecurity and intellectual property]. Voprosy kiberbezopasnosti, 3(4), 42-49.

Kukutai, T., Taylor, J. (Eds.). (2016). Pathways to first nations' data and information sovereignty. In Indigenous data sovereignty: Toward an agenda (pp. 139-156). Canberra: Australian National University Press.

Markova, O.A., Meleshkina, A.I. (2021). Tsifrovoi protektsionizm: Mif ili realnost [Digital protectionism: Myth or reality]. Nauchnye issledovaniya ekonomicheskogo fakulteta. Elektronnyizhurnal, 13(2), 26-40. https://doi.org/10.38050/2078-3809-2021-13-2-26-40

Nikonenko, N.D., Klimashenko, V.V. (2021). Obespechenie tsifrovogo sovereniteta Rossiiskoi Federatsii kak bazis tsifrovoi transformatsii [Ensuring the digital sovereignty of the Russian Federation as the basis for digital transformation]. Aktualnye nauchnye issledovaniya v sovremennom mire, 11-12(79), 23-25.

Nikonov, A.V., Voronov, A.S., Sazhina, V.A., Volodenkov, S.V., Rybakova, M.V. (2021). Tsifrovoy suverenitet sovremennogo gosudarstva: Soderzhanie i strukturnye komponenty (po materialam ekspertnogo issledovaniya) [Sovereignty of a modern state: Content and structural components (based on expert research)]. Vestnik Tomskogo gosudarstvennogo universiteta, 60, 206-216. https://doi.org/10.17223/1998863X/60/18

Nugraha, Y.K., Sastrosubroto, A.S. (2015). Towards data sovereignty in cyberspace. In 3rd International Conference on Information and Communication Technology (ICoICT), May 27-29, 2015, Nusa Dua, Bali, Indonesia (pp. 465-471). IEEE. https://doi.org/10.1109/ICoICT.2015.7231469

Semchenkov, A.S. (2019). Tsifrovoi suverenitet i politicheskaya stabilnost Rossii [Digital sovereignty and political stability of Russia]. In A.V. Sokolov, A.A. Vlasova (Eds.), Vozmozhnosti i ugrozy tsifrovogo obshchestva: Sbornik nauchnykh statei (pp. 134-140). Yaroslavl: Tsifrovaya tipografiya.

United Nations. (2020). The impact of digital technologies. Retrieved from https://www.un.org/ru/un75/impact-digital-technologies (date of access: October 20, 2023).

United Nations Secretary-General. (2018). Secretary-General's Strategy on new technologies. Retrieved from https://www.un.org/en/newtechnologies/ (date of access: October 20, 2023).

Volodenkov, S.V. (2020). Fenomen tsifrovogo suvereniteta sovremennogo gosudarstva v usloviyakh globalnykh tekhnologicheskikh transformatsii: Soderzhanie i osobennosti [The phenomenon of digital sovereignty of a modern state in the context of global technological transformations: Content and features]. Zhurnal politicheskikh issledovanii, 4, 3-11. https://doi.org/10.12737/2587-6295-2020-3-11

World Intellectual Property Organization. (2021). Global innovation index. Retrieved from https://tind.wipo.int/record/44369 (date of access: October 20, 2023).

World Intellectual Property Organization. (2023). Global innovation index. Retrieved from https://www.wipo.int/global_innovation_index/ru/ (date of access: October 7, 2023).

Yan, X. (2021). China-US competition in digital era. Global Times. Retrieved from https://www.globaltimes.cn/content/1177615.shtml (date of access: October 20, 2023).