**Supplementary Notebook (RTEP - Brazilian academic journal, ISSN 2316-1493)**

# TYPOLOGY OF RISKS AND THREATS CAUSED BY DIGITALIZATION

*Yana V. Gaivoronskaya[1]*
*Alexey Y. Mamychev[2]*
*Daria A. Petrova[3]*
*Iryna O. Rusanova[4]*

*[1]Yana V. Gaivoronskaya, Far Eastern Federal University Law School, PhD in Law, Associate Professor, Department of Theory and History of State and Law,690950, Vladivostok, Sukhanova St., 8, Russian Federation yanavl@yandex.ru. ORCID 0000-0002-7606-4444.*

*[2]Alexey Y. Mamychev ,Doctor habil. in political science, PhD in legal science, Head of the political and legal research laboratory ,Department of Theory and History of Russian and Foreign Law, Vladivostok State University of Economics and Service, Vladivostok, Russiamamychev@yandex.ru. ORCID 0000-0003-1325-7967.*

*[3]Daria A. Petrova, Far Eastern Federal University, Law School, PhD in political science, Associated Professor, Department of Theory and History of State and Law, 690950, Vladivostok, Sukhanova St., 8, Russian Federation, petrova.dan@dvfu.ru. ORCID: 0000-0003-3067-9598.*

*[4]Iryna O. Rusanova ,PhD in Law, Associate professor, Department of the Judiciary and Prosecutorial activities, Yaroslav Mudryi National Law University, Kharkiv, Ukraine,shestopals@gmail.com.*

**Abstract:** The paper shows that the intensification of digitalization processes in public relations generates a whole variety of new risks and threats. The purpose of this work is to systematize the risks and threats of the digital transformation of society for the subsequent development of advanced law-making decisions. To effectively counter digital threats and create effective legal regulation in the use of digital technologies, it is necessary to divide all digitalization threats into 3 groups: hypothetical, justifiable, and epistemological. The justifiable threats include those that appear at the present stage of technical development and urgently require legal solutions. According to the authors, it is on the study of this group of threats that scientists need to focus their attention in order to provide a practice-oriented approach to research. The authors identified three main subgroups of justifiable threats to digitalization: threats to economic security, information leaks, and cybercrime. This work was performed with financial support

from the Grant of the President of the Russian Federation No. NSh-2668-2020.6 “National-Cultural and Digital Trends in the Socio-Economic, Political and Legal Development of the Russian Federation in the 21st Century”.

**Keywords:** digitalization, digital transformation of society, end-to-end digital technologies, digitalization threats, digitalization problems, digitalization risks, economic security, information leaks, cybercrime.

## INTRODUCTION

The topic of risks and threats of digitalization is being actively studied by scientists of various fields: economists, politicians, legal scholars and many others are concerned about such a rapid spread of the digital wave. Onset of any changes in economics, politics, demography, social life, etc. is associated with certain challenges and threats, which can manifest itself in the totality of possible problems and negative results. Each of these undesirable outcomes (economic, political, demographic, social, etc.) can be represented as a risk described by such parameters as "size of possible negative outcome" and "probability of occurrence of a negative outcome".(1). However, the undesirable effects, or otherwise, the problems of digitalization need to be identified before assessing the potential risks of digital transformation of public relations and developing preventive law-making solutions. The modern manifestations of digitalization include, first of all, the so-called end-to-end digital technologies, which affect different industries and have the greatest impact on the development of the digital economy. End-to-end digital technologies are listed in the Federal project "Digital Technologies", which is part of the National Program "Digital Economy of the Russian Federation".(2). These include: Big Data, New manufacturing technologies, the Industrial Internet of Things (IIoT), artificial intelligence (AI), wireless technologies, robotics and sensor components, quantum technologies, distributed ledger systems, and also technologies of virtual (VR) and augmented (AR) realities. The purpose of our study is to systematize the risks and threats of digital transformation of society for the subsequent development of advanced law-making decisions. In this work, we will use the term "digitalization" in a generalized sense to denote all processes of digital transformation of society and its individual institutions through the introduction of information and end-to-end digital technologies.

## MATERIALS AND METHODS

The regulatory framework of the study was made up of strategic planning documents in the field of digitalization, namely: The National Program "Digital Economy of the Russian Federation" (approved by the Minutes of the meeting of the Presidium of the Government Commission on Digital Development, the Use of Information Technologies to Improve the Quality of Life, and the Conditions of Doing Business dated 28.05.2019 No. 9), National project design passport for the "National Program "Digital Economy of the Russian Federation" (approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects, minutes of 04.06.2019 N7); Resolution of the Government of the Russian Federation dated 02.03.2019 No. 234 "On the management system for the

implementation of the National program "Digital Economy of the Russian Federation".

The theoretical basis of the study was the latest research in the field of prospects for the use of artificial intelligence (Dremlyuga R.I., 2019; Mamychev A.Yu., Miroshnichenko O.I., 2019; Gaivoronskaya Ya.V., 2019; Ponkin I.V., Redkina A.I., 2019; Roizenzon G.V., 2018), works on digital transformation of the economy (Piskunov A.I., 2019; Popov E.V., Semyachkov A.A., 2018; Khalin V.G. , Chernov G.V., 2018), cybercrime (Bekher V.V., Zelenykh E.V., 2019; Martyanov N.R., 2019) and the problem of information leaks (Kasperskaya N., 2019; Saveliev A.I. , 2015; Oganesyan A., 2019; Talapina E.V., 2018). The factual material, which became the basis of the analysis, was studied on the basis of periodicals and news data of information and analytical media. The proposed study is the author's point of view and is an attempt to systematize the threats that arise in the process of digital transformation of public relations.

## METHODS

The study is based on such methods as system-structural analysis, which allows differentiation of modern digital threats; formal legal method, with the help of which the regulatory legal acts regulating relations with the use of digital technologies are analysed; methods of typology and scientific modelling allowing creation of an author's typology of digital threats.

## MAIN PART

To date, many problems of the digital transformation of society in the field of economics, politics, law and culture have been described. We believe that it is necessary to distinguish between the levels of potential risks and threats of such a transformation. It seems reasonable to divide all potential threats of digitalization into hypothetical, that is, possible in the future at a high level of technological development (the level predicted, but currently unavailable), and justifiable (urgent), that is, obvious and stated in our modern society at the existing level of technological development. Hypothetical threats are associated primarily with the potential emergence of a strong AI, which has autonomy and is comparable to human intelligence. Hypothetical threats include, in particular, a possible confrontation between AI and humanity, a conflict between AI and the noosphere, which, in turn, generate various threats to the existence of humanity.(3). In the legal plane, the hypothetical problems of digitalization include the issues of legal existence of AI,(4).the spread to AI units and autonomous robotic devices (ARD) of the legal status elements of a human, in particular, human rights.(5).

Summarizing, we can say that artificial intelligence generates threats and challenges "associated with risks and polyvarieties which are extremely difficult to calculate and creates an unprecedented amount of uncertainties."(6). In other words, one of the biggest problems with the spread of AI is the inability to clearly predict and forecast possible threats and risks associated with this technology in the future. Most of the threats predicted to date in the field of AI concern ethical issues, more precisely, possible conflicts between modern anthropocentric morality and the logic of the functioning (behaviour?), which belongs to future autonomous carriers of strong AI. The researchers state that "... the development of certain dangerous technologies without taking into account ethical issues can lead humanity to a completely catastrophic result".(7). On the other hand, severe restrictions formulated at the dawn of the

formation of a new technology can hinder the technological and, consequently, the socio-economic and political development of the community, which in itself can also be recognized as one of the threats of the digital age (artificial retardation of development associated with the impossibility of deontological, legal and cultural mediation of the ongoing changes).

The justifiable threats of digitalization, fully realized and relevant today, include the insecurity of personal data in cyberspace and the related inability of modern legal means to regulate and protect public relations; the intellectualization of military robotics and related consequences, in particular, the threat of people losing control over military computer systems; labour market changes and technological unemployment; the spread of cybercrime and the inability of law enforcement agencies to ensure the safety of individuals on the Internet; lack of legal regulation of the Internet and mechanisms of effective state and legal control in the Internet environment, etc. We would like to set apart the "epistemological" problems of digitalization: threats to classical scientific theories and models that underlie the current political, legal, economic and other social institutions. For example, in the subject area of jurisprudence, digitalization poses threats to the classical theories of state sovereignty(8), legal existence, persons, legal relations that become unrealizable in cyberspace and / or with the participation of fundamentally new quasi-actors (AI units, robotic agents, etc.)(9). The theory of human rights requires modification (at least in terms of expanding the list of rights officially enshrined and guaranteed by the state in a digital society), which will entail changes in the ideology based on this theory.

The concept of information forms a separate interdisciplinary area that has a lot of applied aspects. Legal regulation of information as a universal object of law is extremely complex and becomes outdated even before the appearance of the draft law (this partly explains the completely unsatisfactory state of the concept of information in the modern legal field from the point of view of modern achievements of technical progress). This situation, by the way, in itself becomes one of the threats of digitalization: the permanent lag of information technology legislation from the real level of technology and the absence of advanced law-making decisions. Changes in the categorical apparatus of science, methodology and subject area of research under the influence of digitalization affect, of course, not only jurisprudence, but practically all types and areas of scientific knowledge. Currently, the main emphasis should be placed on the prevention of "justifiable" threats of digitalization (in the terminology of our conventional classification). Without diminishing the importance of other scientific research, we would like to emphasize the urgent applied nature of research in the field of justifiable threats to the digital transformation of society. The risk level of this group of threats is high and is critical for some unresolved issues. At the same time, the level of risk of hypothetical digitalization problems is currently low (or medium), which makes it possible to postpone their resolution at the level of law-making decisions. Studies of a group of pressing digitalization threats should provide concepts and models for the legal regulation of existing public relations, closing the regulatory vacuum and creating opportunities for further development and technical progress, and scientific research of digitalization. With a certain degree of conventionality, the following subgroups of "justifiable" threats from digitalization can be distinguished:

## Threats to economic security

Economists identify the following groups of economic security problems for a digital society: systemic, structural, sectoral problems, problems of the activities of individual enterprises, problems of individual citizens. Problematization in this case is carried out according to the criterion of a subject / institution, in relation to which interests a threat is formed in connection with the spread of digital technologies. The systemic problems of economic security include problems related to the economy as a whole or its significant parts (dependence on digital technologies of other states, lack of their own elementary base, and the problem of "digital inequality"). Structural problems caused by digitalization are associated with changes in individual social institutions or backbone processes in society (for example, significant changes in the labour market and an increase in unemployment). Industry problems include the lack of digital solutions for certain industries (for example, the lack of their own payment system). The problems of economic security in the activities of individual enterprises affect specific business participants (theft of corporate data, industrial espionage, hacker attacks, insufficient provision of digital technologies, competent personnel, etc.). The problems of digital security of individual citizens include theft and manipulation of personal data(10).

An interesting generalizing classification was proposed in the study by A.I. Piskunov on the digitalization of industry. The classification of global challenges and threats to the digital transformation of society identified on the basis of studying the materials of the economic forums Davos-2016 and Davos-2017 is based on the definition of the spheres where potential threats are spread. The challenges and threats of digitalization are divided into 5 groups: Group I is threats that can provoke social and economic instability (technological unemployment and all its manifestations); Group II is threats of a gap in the levels of technological development between countries, as well as between different economic groups depending on the access and efficiency of use of intellectual resources; Group III is the likelihood of man-made disasters, the inability of a person to lead in making management decisions in comparison with intelligent systems; Group IV is environmental risks and threats (intensification of production can lead to significant climate change); Group V is threats of reducing the level of national security of a country (risks of increasing terrorism, the complexity of ensuring the confidentiality of information, the threat of creating new models of cyber weapons)(11).

## Cybercrime

Now the world is experiencing a turning point being the transition from an "industrial society" to an "information society". The development of information technology poses a number of new tasks that require effective and high-quality resolution. Global cybercrime becomes the source of threats and dangers in these conditions.(12) In the WEF's Global Risks Report (2018), global threats such as cybercrime and data theft are ranked third and fourth in importance(13).

The Internet knows more about every person than they themselves, their friends and family: in the era of information technology development, this is no longer a joke. "Automatic research of information requests of users on the Internet, information from personal gadgets, transactions with bank cards, e-mails and instant messengers form a block of information about persons that they themselves may not know," the

researchers point out, explaining the essence of the threat of identity theft and using the personal information of others for lucrative purposes(14).

According to law enforcement agencies, only in 2019 the number of IT crimes registered in Russia increased by 70% (294 thousand); they already account for 15% of all crimes registered in the country. According to the head of the Ministry of Internal Affairs, their detection rate has grown by 1.5 times(15). Experts call cybercrime with the use of ransomware viruses as one of the main threats to information security today. The danger is associated with the fact that such "high technologies" penetrate not only personal computers, but also classified data of strategic facilities, airports, oil pipelines, spaceports, defence enterprises, military bases, and nuclear power plants, which threatens man-made disasters and huge damage(16).

In addition, the risks associated with damage and loss of information due to viral infections of communication channels and databases are becoming more and more severe(17). In the era of the industrial Internet of things, more and more data will appear on the network, which means that industrial production will become more and more vulnerable: attackers can remotely make changes to the codes on the basis of which machines communicate with each other, making decisions without human intervention. Negative consequences in such cases can be catastrophic: from data theft, loss of intellectual property, damage to the company's reputation and commercial losses, to stoppages of production, and man-made or environmental disasters.(18).

**Digital information leaks**

Getting personal data into the hands of fraudsters and third parties is possible both through cyberattacks and through information leakage due to weak protection of a data warehouse. According to statistics from the President of InfoWatch company, 7.28 billion records were leaked in the world in 2018 and already 8.74 billion for the first half of 2019(19). This is due, first of all, to the too rapid introduction of digital technologies. The most notorious cases of leaks in Russia are the sale in 2019 of personal data of customers, including credit history and data of documents, Alfa-Bank and Sberbank. Foreign examples include an error in the interaction code between the Apple online store and the T-Mobile server, which led to a leak of financial information.(20).

Information leakage is an uncontrolled spread of information outside the organization, premises, building, any territory, as well as a certain circle of people who have access to this information.(21) When speaking about information leakage, they, first of all, analyse the channels of its leakage. An information leakage channel is a set of a source (information carrier), information receiver (violator), as well as the physical environment through which information is disseminated from a source to a receiver. Based on the methods of implementing threats to information security, the channels of information leakage can be classified as follows: Technical channels of information leakage; Unauthorized access to information; Channels of information leakage without the use of technical means.

Information leakage through a technical channel is an uncontrolled spread of information from a protected information carrier through a physical medium to a technical means that intercepts information. Unauthorized access to information is an access to information carried out with violation of the established rights and (or) rules of access to information using standard means of the information system or means similar to them in their functional purpose and technical characteristics(22). According

to Article 14 of the Federal Law "On State Protection", one of the duties of state security bodies is to implement, in cooperation with the bodies of the federal security service, measures to counter information leakage through technical channels(23).

If information constituting state, official and commercial secrets has always been the goal of interested parties, then attacks on user data records have become especially relevant after entering the practice of Big Data. With the emergence of a new practice, new players have also emerged; they are information brokers or data brokers, i.e. companies specializing in the collection and sale of personal data.(24). Data brokers are especially popular in the United States, where there is no dedicated law on personal data protection. Companies compile dossiers on persons from various sources, reflecting in it the level of income, food preferences, frequently used sites, circle of acquaintances on social networks, etc., and then transmit this information to interested organizations. One illustrative example is the activities of a Singapore bank, which services monitored banking transactions, inferred client tastes and sent him or her individual proposal. For example, a client paid at lunchtime with a bank card next to a street with an Italian restaurant. The bank and the restaurant have entered into a partnership agreement. Knowing that the client prefers Italian food, the bank sends an SMS notification with a special offer in this institution.(25)

In Russia, the activities of information brokers are limited by the Law on the Protection of Personal Data,(26). which requires the written consent of the owner to process information about him/her. However, when filling out the consent to processing information when receiving a discount card, and when subscribing to the store's new items, a client may find an item in the consent form that allows the transfer of data to third parties. This line will allow brokers to use client data in the future. Citizens' dissatisfaction with the state's policy regarding the use of personal data has already caused a trial. On October 7, 2019 in Moscow, a citizen Popova challenged the actions of the Moscow Government on the use of face recognition technology in the video surveillance system of the Russian capital. The citizen demanded that the actions of the Moscow Government be declared illegal. The court dismissed the claim, but made a reservation that the system compares the image from the video camera with the photo that the police have. The case was sent to the appellate instance.

## CONCLUSION

Summing up, we can say that the main problem of digitalization today is ensuring the safety of an individual, business, society, and the state in the digital era. The problem of security in the context of the development of information technologies has many manifestations that act as threats either to individual social institutions or to the rights and interests of individuals protected by law. The list of justifiable threats we have proposed is conditional and requires further development and detailing. However, such attempts to systematize digital threats are necessary, from our point of view, since they allow not scattering scientific efforts, and also creating a matrix of digital threats suitable for point legal regulation in the long term.

**REFERENCES**

1. Khalin V.G., Chernov G.V. Digitalization and Its Impact on the Russian Economy and Society: Advantages, Challenges, Threats and Risks // Management Consulting. 2018. No. 10.P. 53.

2. National project design passport for the "National Program "Digital Economy of the Russian Federation" approved by the Minutes of the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects dated 04.06.2019 N 7 // Access from the reference legal system KonsultantPlus; National program "Digital economy of the Russian Federation" (includes 6 federal projects) approved by the Minutes of the Meeting of the Presidium of the Government Commission on Digital Development, the Use of Information Technologies to Improve the Quality of Life and Conditions for Doing Business No. 9 dated May 28, 2019 // Official website of the Ministry of Digital Development, communications and mass communications of the Russian Federation. URL: https://digital.gov.ru/ru/activity/directions/858/; On the management system for the implementation of the national program "Digital Economy of the Russian Federation": Resolution of the Government of the Russian Federation dated 03/02/2019 No. 234 // Official Internet portal of legal information. URL: http://publication.pravo.gov.ru/Document/View/0001201903070015.

3. For example: Sterledev R.K., Sterledeva T.D. Artificial intelligence in the aspect of the noosphere: is it almost fantastic? // Bulletin of PNRPU. Culture. History. Philosophy. Right. 2017.No. 2. P. 64, etc.

4. For example: Mamychev A.Yu., Miroshnichenko O.I. Modeling the Future of Law: Problems and Contradictions of Legal Policy in the Field of Regulatory Regulation of Artificial Intelligence Systems and Robotic Technologies. // Legal policy and legal life. 2019. No. 2. P. 125-133.

5. Read more: Dremlyuga R.I., Dremlyuga O.A. Artificial intelligence as a subject of law: arguments for and against // Legal policy and legal life. 2019. No. 2.P. 120-125; Gaivoronskaya Ya.V., Miroshnichenko O.I. Legal problems of digitalization: theoretical and legal aspect // Legal Concept = Pravovaya paradigma. 2019. Vol. 18.No. 4.P. 27-34.

I. V. Ponkin, A. I. Redkina Artificial intelligence from the point of view of law / Bulletin of RUDN. Series: Legal Sciences. 2018. Vol. 22.No. 1.P. 105.

6. Roizenzon G.V. Problems of formalizing the concept of ethics in artificial intelligence // Sixteenth National Conference on Artificial Intelligence with International Participation KII-2018. Conference proceedings: in 2 volumes. - M .: Publishing house: Federal State Enterprise "Information Telegraph Agency of Russia (ITAR-TASS)", branch "Russian Book Chamber", 2018. - P. 248. URL: https://elibrary.ru/item.asp?id= 35568660 (date of treatment 09/25/2019).

7. Read more: Shestopal S.S., Mamychev A.Yu. Sovereignty in the global digital dimension: current trends. // Baltic Humanitarian Journal. 2020. No. 1 (30). P. 398-403.

8. Read more: E.V. Talapina. Law and digitalization: new challenges and prospects // Journal of Russian Law. 2018. No. 2. P. 5-17.

9. Details: Popov E.V., Semyachkov A.A. Problems of economic security of digital society in the context of globalization // Economy of the region 2018.Vol. 14. Issue 4. P. 1088-1101.

10. Details: A.I. Piskunov Challenges, threats and expectations of digitalization for industrial enterprises. // Production organizer. 2019. Vol. 27. No. 2. P. 12.

11. Martyanov N.R. Criminal law fight against cybercrimes at the present stage. // Public service and personnel. 2020.No. 1 P. 175-177.

12. The Global Risks Report 2018 13th Edition. Retrieved from: http://www3.weforum.org/docs/WEF_GRR18_Report. pdf (date of access: 26.03.2020).

13. Bekher V.V., Zelenykh E.V. Digital technologies: threats and risks of implementation // Eurasian Scientific Association. 2019. No. 1-3 (47). P. 146. Access mode: https://www.elibrary.ru/item.asp?id=36993290 (date of access:15.03.2020).

14. A cybercrime investigation department has been created in the Investigative Committee of the Russian Federation. Access mode: https://tass.ru/proisshestviya/7889859 (date of access: 03/15/2020).

15. Bekher V.V., Zelenykh E.V. Digital technologies: threats and risks of implementation // Eurasian Scientific Association. 2019. No. 1-3 (47). P. 146. Access mode: https://www.elibrary.ru/item.asp?id=36993290 (date of access: 03/15/2020).

16. Suleymanov M.D. Digitalization: Are They Threats or Disruptive Economic Transformation? // Science and Education Foundation: official site. Access mode: http: //fond-nauki.rf/menu/novosti-fonda/558-tsifrovizatsiya-ugroza-ili-proryvnaya-transformatsiya-ekonomiki.html (date of access: 03/15/2020).

17. A.I. Piskunov Challenges, threats and expectations of digitalization for industrial enterprises. // Production organizer. 2019.Vol. 27. No. 2. P. 11.

18. Kaspersky N. Confidential information leaks: why there are more and more of them and how to deal with them. [Electronic source] // Tass.ru. 11/21/2019URL: https://tass.ru/opinions/7164059.

19. Oganesyan A. Disease of the digital world: how to protect yourself from personal data leaks [Electronic resource] // Forbes. 23.05.2019. URL: https://yandex.ru/turbo?text=https%3A%2F%2Fwww.forbes.ru%2Ftehnologii%2F376499-bolezn-cifrovogo-mira-kak-zashchititsya-ot-utechek-personalnyh-dannyh.

20. P 50.1.056-2005 Technical protection of information. Basic terms and definitions from 01.06.2006 [Electronic source]. Access mode: http://docs.cntd.ru/document/1200044768. (Date of access: 02.04.2020).

21. Standard P50.1.056-2005 Technical information security. Basic terms and definitions; dated 01.06.2006 [Electronic source]. Access mode: http://docs.cntd.ru/document/1200044768. (Date of access: 02.04.2020).

22. Federal Law dated 27.05.1996 N 57-FZ (as amended on 27.12.2019) "On state protection" [Electronic source] // KonsultantPlus. Access mode: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=341973&fld=134&dst=1000000001,0&rnd=0.6522750962871502#018310521226940502 (access date 04/06/2020).

23. Urmantseva A. Transition to personal: in 2019, twice as much personal data has flowed [Electronic source] // Izvestia iz. Access mode: https://iz.ru/958561/anna-urmantceva/perekhod-na-lichnoe-v-2019-godu-uteklo-vdvoe-bolshe-personalnykh-dannykh (date of access: 04.02.2020).

24. Savelyev A.I. Problems of the application of legislation on personal data in the era of "Big Data" // Law. Journal of the Higher School of Economics. 2015. No. 1. P. 43–66.

25. Federal Law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On Personal Data" [Electronic source]. // ConsultantPlus. Access mode: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=286959&fld=134&dst=1000000001,0&rnd=0.514433496105853#09751787726001224.

26. The Global Risks Report 2018 13th Edition. Retrieved from: http://www3.weforum.org/docs/WEF_GRR18_Report. pdf (date of access: 26.03.2020).

27. Bekher V.V., Zelenykh E.V. Digital technologies: threats and risks of implementation // Eurasian Scientific Association. 2019. No. 1-3 (47). P. 146. Access mode: https://www.elibrary.ru/item.asp?id=36993290 (date of access: 03/15/2020).

28. Bekher V.V., Zelenykh E.V. Digital technologies: threats and risks of implementation // Eurasian Scientific Association. 2019. No. 1-3 (47). P. 146. Access mode: https://www.elibrary.ru/item.asp?id=36993290 (date of access: 03/15/2020).

29. A department for investigation of cybercrimes has been created in the UK // Information portal TASS.ru. Access mode: https://tass.ru/proisshestviya/7889859 (date of access: 03/15/2020).

30. Gaivoronskaya Ya.V., Miroshnichenko O.I. Legal problems of digitalization: theoretical and legal aspect // Legal Concept = Pravovaya paradigma. 2019. Vol. 18. No. 4. P. 27-34.

31. Dremlyuga R.I., Dremlyuga O.A. Artificial intelligence as a subject of law: arguments for and against // Legal policy and legal life. 2019. No. 2. P. 120-125.

32. Kasperskaya N. Leaks of confidential information: why there are more and more of them and how to deal with them. [Electronic source] // Tass.ru. 21.11.2019 URL: https://tass.ru/opinions/7164059.

33. Mamychev A.Yu., Miroshnichenko O.I. Modeling the future of law: problems and contradictions of legal policy in the field of normative regulation of artificial intelligence systems and robotic technologies. // Legal policy and legal life. 2019. No. 2. P. 125-133.

34. Martyanov N.R. Criminal law fight against cybercrimes at the present stage. // Public service and personnel. 2020. No. 1 P. 175-177.

35. National program "Digital Economy of the Russian Federation" (includes 6 federal projects): approved by the Minutes of the meeting of the Presidium of the Government Commission on Digital Development, the Use of Information Technologies to Improve the Quality of Life, and the Conditions of Doing Business No. 9 dated 05.28.2019 // Official website of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation. URL: https://digital.gov.ru/ru/activity/directions/858/.

36. On the management system for the implementation of the national program "Digital Economy of the Russian Federation": Decree of the Government of the Russian Federation dated 02.03.2019, No. 234 // Official Internet portal of legal information. URL: http://publication.pravo.gov.ru/Document/View/0001201903070015.

37. Oganesyan A. Disease of the digital world: how to protect yourself from personal data leaks [Electronic source] // Forbes. 05/23/2019 URL: https://yandex.ru/turbo?text=https%3A%2F%2Fwww.forbes.ru%2Ftehnologii%2F376499-bolezn-cifrovogo-mira-kak-zashchititsya-ot-utechek-personalnyh-dannyh.

38. National project design passport "National Program "Digital Economy of the Russian Federation" approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects, Minutes of 04.06.2019 N 7 // Access from the reference legal system "KonsultantPlus ".

39. Piskunov A.I. Challenges, threats and expectations of digitalization for industrial enterprises. // Production organizer. 2019. Vol. 27. No. 2.P. 12.

40. Piskunov A.I. Challenges, threats and expectations of digitalization for industrial enterprises. // Production organizer. 2019. Vol. 27. No. 2.P. 11.

41. Ponkin I.V., Redkina A.I. Artificial intelligence from the point of view of law / Bulletin of RUDN. Series: Legal Sciences. 2018. Vol. 22.No. 1. P. 105.

42. Popov E.V., Semyachkov A.A. Problems of economic security of digital society in the context of globalization // Economy of the region 2018.Vol. 14. Issue 4.P. 1088-1101.

43. P50.1.056-2005 Technical protection of information. Basic terms and definitions dated 01.06.2006 [Electronic source]. Access mode: http://docs.cntd.ru/document/1200044768. (Date of access: 02.04.2020). R 50.1.056-2005 Technical information protection. Basic terms and definitions from 01.06.2006 [Electronic source]. Access mode: http://docs.cntd.ru/document/1200044768. (Date of access: 02.04.2020).

44. Roizenzon G.V. Problems of formalizing the concept of ethics in artificial intelligence // Sixteenth National Conference on Artificial Intelligence with International Participation KII-2018. Conference proceedings: in 2 volumes. - M .: Publishing house: Federal State Enterprise "Information Telegraph Agency of Russia (ITAR-TASS)", the branch "Russian Book Chamber", 2018. - P. 248. URL: https://elibrary.ru/item.asp?id=35568660 (date of access 09/25/2019).

45. Savelyev A.I. Problems of the application of legislation on personal data in the era of "Big Data" // Law. Journal of the Higher School of Economics. 2015. No. 1. P. 43–66.

46. Standard P50.1.056-2005 Technical information security. Basic terms and definitions; dated 01.06.2006 [Electronic source]. Access mode: http://docs.cntd.ru/document/1200044768. (Date of access: 02.04.2020).

47. Sterledev R.K., Sterledeva T.D. Artificial intelligence in the aspect of the noosphere: almost fantastic? // Bulletin of PNRPU. Culture. History. Philosophy. Right. 2017. No. 2.P. 64 and others.

48. Suleimanov M.D. Digitalization: Is This Threats or Disruptive Economic Transformation? // Science and Education Foundation: official site. Access mode: http:

//fond-nauki.rf/menu/novosti-fonda/558-tsifrovizatsiya-ugroza-ili-proryvnaya-transformatsiya-ekonomiki.html (date of access: 03/15/2020).

49. Talapina E.V. Law and digitalization: new challenges and prospects // Journal of Russian Law. 2018. No. 2.P. 5-17.

50. Urmantseva A. Transition to personal: in 2019, twice as much personal data has flowed [Electronic source] // Izvestia iz. Access mode: https://iz.ru/958561/anna-urmantceva/perekhod-na-lichnoe-v-2019-godu-uteklo-vdvoe-bolshe-personalnykh-dannykh (Date of access: 02/04/2020).

51. Federal Law dated 27.05.1996 N 57-FZ (as amended on 27.12.2019) "On state protection" [Electronic source] // Consultant plus. Access mode: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=341973&fld=134&dst=1000000001,0&rnd=0.6522750962871502#018310521226940502 (Access date 04/06/2020).

52. Federal Law of 27.07.2006 N 152-FZ (as amended on 31.12.2017) "On personal data" [Electronic source]. // KonsultantPlus. Access mode: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=286959&fld=134&dst=1000000001,0&rnd=0.514433496105853#09751787726001224.

53. Khalin V.G., Chernov G.V. Digitalization and Its Impact on the Russian Economy and Society: Advantages, Challenges, Threats and Risks // Management Consulting. 2018. No. 10.P. 53.

54. Shestopal S.S., Mamychev A.Yu. Sovereignty in the global digital dimension: current trends. // Baltic Humanitarian Journal. 2020. No. 1 (30). P. 398-403.