attract more investors and create a favourable investment climate. Work is underway to improve the tax system.

1. On investments [Electronic resource]: the law of the Republic of Belarus of 12.07.2013 № 53-Z // Consultant Plus: Belarus. Technology 3000 / Yurspektr LLC. - Minsk, 2020.
2. Results of investment policy. – Mode of access: http://www.economy.gov.by/ru/pezultat-ru/. – Date of access: 02.11.2020.

LEGAL BASIC PRINCIPLES REGULATION OF THE ONLINE SPACE IN THE NATIONAL CYBER SECURITY STRATEGIES IN THE EU COUNTRIES

Darya Mazurtsova
VSU named after P.M. Masherov, Vitebsk, Belarus

In the last decade, due to the growing vulnerability of society in the Internet space, many states have adopted national cybersecurity strategies, the fundamental principles of which are designed to form the basis for a more effective countering cyber threats. The purpose of this study is to analyze and compare the concepts of national cybersecurity of a number of European states.

Material and methods. The main materials of the study are the concepts of national cybersecurity of Germany, Sweden, Finland, Spain, etc. In the course of the research, formal legal and comparative legal methods were used.

Findings and their discussion. One of the first European states to adopt in 2011 a special act in the field of cyberspace security in order to maintain and promote the economic and social prosperity of the state and society is Germany. The adoption of the Cyber Security Strategy was primarily driven by the increasing intensity of IT threats both within Germany itself and from abroad. The document notes that only the creation of special standards of the international level and their responsible observance will guarantee a successful counteraction to online threats of both the entire world community and individual countries. Protection of information and communication technologies is named among the basic principles according to the Strategy; integrity, authenticity and confidentiality of data in cyberspace; international coordination and intensive exchange of information between law enforcement agencies. The document also highlighted 10 strategically important goals in the achievement of which Germany sees a significant improvement in the level of national cybersecurity: the reliability of IT systems, increased IT security in public administration, the creation of the National Cybersecurity Center and the National Cybersecurity Council, effective suppression of cybercrime, coordination of actions to ensure cybersecurity in Europe and around the world, development of mechanisms for responding to cyber-attacks, etc. [1].

At the legislative level, the Nordic countries also pay significant attention to this problem. Thus, in 2013, the Cybersecurity Strategy of Finland was adopted with the aim of ensuring proper protection of all processes occurring on the Internet, preventing Internet threats to citizens. The key tasks according to the Strategy define the need to protect the strategically important functional state structures of Finland from any cyber threats, access of citizens to the safe Internet space, which should be achieved by active interaction of subjects not only at the national, but also at international level. Effective cooperation between authorities and other participants in Internet relations, increasing comprehensive awareness of the cybersecurity situation among key actors involved in ensuring the vital functions of society and the state, empowering enterprises and organizations as leading subjects of the business community to promptly respond to cyber threats, equip law enforcement agencies with sufficient means to disclose cybercrimes, provide conditions for the effective implementation of cyber security measures in accordance with national legislation, etc. [2].

In 2016, the Swedish Government also constructively approached the urgent need for the development of legal cyber regulation in the state, in connection with which the National Cybersecurity Concept was adopted, designed not only for power structures of all levels, but also for individuals. The document emphasizes that this Concept is an integral part of the legislation in the field of ensuring comprehensive security in Sweden, which implies compliance with the fundamental principles of protecting the life and health of the population, the general functioning of society in the online space. However, it lacks a clear definition of the concept of cybersecurity, despite a detailed list of key provisions on which, in the understanding of the Swedish legislator, the most complete cybersecurity should be based, namely: ensuring confidentiality, reliability and availability of information, guaranteeing fundamental values and goals of society such as human rights, Swedish sovereignty, the right to autonomy, economic stability. As a means of implementing the declared principles, the Swedish legislator has provided for the provision of a systematic and comprehensive approach to ensuring cybersecurity; expanding the capabilities of preventing, detecting and managing cyber-attacks and other IT incidents; increasing the ability to prevent and combat cybercrime; constant increase in the level of knowledge about the phenomena occurring on the Internet; expansion of international cooperation, etc. [3].

In addition to the Spanish government structures, invited EU expert consultants also took part in the creation of the Spanish National Cyber Security Strategy 2019. The Strategy provides a brief definition of the term cybersecurity: “a common global space, technically equipped and broadly connected”, which is complemented by listing the goals and activities of the Spanish state in the field of online relations: centralized public administration of countering cyber threats; the use of high-level technological systems; ensuring

the sustainability of the online structures most important to society. The Spanish legislator has identified a number of fundamental goals, the adherence to which should provide the society with the state of the most effective cybersecurity: an integrated national segment of the Internet; protection of information processed by the public sector; safe and secure use of cyber space to protect against illegal or malicious activity; proper prosecution of cybercriminals; protection of business, social ecosystem and citizens; formation and commitment to legal online culture and strengthening of technological skills; security of international cyberspace, etc. [4].

Conclusion. Similar specialized concepts of national cybersecurity, which partially define the conceptual apparatus of legal regulation of the online sphere and consolidate the fundamental goals and principles of the functioning of the cyber society, currently exist in many European states, including Hungary, Poland, Portugal, France, Czech Republic, Estonia and other countries. They are the necessary basis for building a legal online space. In our opinion, there is a need for the adoption of such a special act in the Republic of Belarus.

1. Cyber Security Strategy for Germany 2011 [Electronic resource]. – Available at: file:///D:/DE_NCSS_2011_en.pdf. – Accessed: 27.10.2020.

2. Finland's Cybersecurity Strategy 2013 [Electronic resource]. – Available at: file:///D:/FI_NCSS_en.pdf. – Accessed: 28.10.2020

3.National Cyber Security Strategy Sweden Skr. 2016/17:213 [Electronic resource]. – Available at: https://vk.com/doc447341862_566520076?hash=9b0781b08b8dfe3e31&dl=67abfe77996c9467f3. – Accessed: 28.10.2019.

4.National Cyber Security Strategy Spain 2019 [Electronic resource]. – Available at: https://vk.com/doc447341862_566520059?hash=1bdeff1ae3cee9e273&dl=e72aa560416c5408ae. – Accessed: 29.10.2020.

THE PROBLEM OF HUMAN RIGHTS IMPLEMENTATION IN THE CONTEXT OF COVID-19 PANDEMIC

Ekaterina Minchukova
VSU named after P.M. Masherov, Vitebsk, Belarus

The article examines the features and problems of natural human rights implementation in a pandemic, identifies the main reasons for the violation of such rights in these conditions.

The purpose of the work is to analyze the implementation of human rights in the context of the COVID-19 pandemic.

Material and methods. The main materials of the work are International Covenant on Economic, Social and Cultural rights, International Covenant on Civil and Political rights, Report of the Congressional Research Service «Sanctions against Iran», etc. Formal-legal and comparative-legal research methods were used.