CYBER SECURITY ISSUES IN DIGITAL KAZAKHSTAN

Isabaeva Symbat
Doctoral student of the Academy of Public Administration under the President of the Republic of Kazakhstan with a degree in Public Administration; chief expert of the Academy of Law Enforcement Agencies under the General Prosecutor's Office of the Republic of Kazakhstan. Address: 010000, Republic of Kazakhstan, Nur-Sultan, Abay str., 33a. E-mail:

Botagoz M. Yesseniyazova
Master student of the Academy of Public Administration under the President of the Republic of Kazakhstan; Chief Specialist of the Public Procurement Office of the Aktobe region, Kazakhstan. Address: 010000, Republic of Kazakhstan, Nur-Sultan, Abay str., 33a. E-mail: yesseniyazova@mail.ru

Abstract
Nowadays Kazakhstan is developing and implementing new digital services in order to improve the standard of living of the population. Kazakhstan is going through a period of digital transformation. Ensuring cybersecurity in cyberspace during the transformation period is one of the important issues not only for Kazakhstan, but for other countries as well. The purpose of this study is to identify the level of quality of digital services for citizens of the Republic of Kazakhstan, as well as to study the degree of awareness and public readiness for the implemented state programs and projects in the framework of the policy in the field of digitalization and cybersecurity in the country. The article will use the indicators of the Global Cybersecurity Index (GCI), the IMD World Digital Competitiveness ranking (IMD WDC) as sources to determine the level of cybersecurity and digitalization in Kazakhstan. Additionally, theoretical and empirical analysis will be carried out as a part of the research. At the same time, the research topic will examine the experience of successful countries such as Singapore, USA, Estonia and Russia. The article will apply a qualitative research method by conducting an online survey of citizens of Kazakhstan. The survey examines the issues of satisfaction, readiness and awareness on the use of digital technology and cybersecurity of the population within the framework of the adopted state program and normative documents of Kazakhstan.
Based on the results of the qualitative and quantitative analysis, practical and methodological recommendations will be proposed for further improvement of the policy of cybersecurity and digital Kazakhstan. The proposed recommendations can be useful not only for Kazakhstan, but also for other countries that are experiencing a period of digital transformation. What is more, it can be helpful for the countries of the former USSR due to post-Soviet countries have a similar history of formation and development of independence.

Points for Practitioners
Recently, the majority of developed countries have been rigorously seeking a new way of economy or as it is been mentioned in a number of academic papers digital economy[1]. The main instrument for the formation is the Internet and information technology. Digitalization is becoming one of the main factors of competitiveness, making changes in the economic and production processes of the state and organizations. Moreover, the global trend is the transition to the information society, the widespread introduction of information technologies and the implementation of state digital development programs.
In the period of globalization and digital transformation in the world is rapidly developing understanding of digital services, both in developed and developing countries. Thus, Kazakhstan citizens should be aware of the importance of the security of their personal data. However, nowadays the majority of Kazakhstanis are vulnerable to cyber attacks due to the lack of knowledge, skills and awareness in cybersecurity. The study will help to identify and reflect the main problems that occur in cyberspace. According to the study results, practical recommendations will be presented applicable to developed and developing countries that are undergoing digital transformation epoch. The main proposed recommendations of this study can be applied in the normative, organizational and managerial, as well as in the educational activities of public administration.

Keywords: cybersecurity, digitalization, international rankings, e-government, public policy.

1. Introduction

The topic of cybersecurity is relevant not only for academics and public managers, but also for business sectors. The rapidly changing world is widely using information digital technology because of their convenience. Every day the number of online services has been growing significantly. At the same time these ongoing changes increases the risk of vulnerability of recipients of the digital services. Every year the numbers of cyberattacks bring enormous financial damage to both public and business sectors. For example, in 2006, a report of Pentagon noted that six million threats were detected in order to hack its networks. Former president of the USA - Barack Obama in 2009 pointed out that cybersecurity is a threat to economic and national security, thus, he ordered to improve the quality and policy of protection of information and communication systems of America. In addition, according to some data Steve Wozniak and Steve Jobs broke the phone system in 1970. As a result, they were able to make free calls to both near and far abroad. It can also be highlighted that Kevin Mitnick has taken an important place in the history of hacking; in 1990 he managed to hack the security system of company and had access to the corporate computers. In addition, it can be noted that the Stuxnet virus was developed in 2009. The purpose of the virus was to damage the Iranian uranium

[1] "Digital economy is the economic activity that results from billions of everyday online connections among people, businesses, devices, data, and processes. The backbone of the digital economy is hyperconnectivity which means growing interconnectedness of people, organisations, and machines that results from the Internet, mobile technology and the internet of things (IoT)". Retrieved from DELOITTE, https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html

enrichment plant (Warnes, K., 2019). Thus, ensuring cybersecurity in the digital space is a critical issue at the local, national and global level.

What is more, the ongoing intersystem integration work between different states in the global world is almost washed away the boundaries that complicates the provision of cybersecurity in the online space. Due to the ongoing intergovernmental digital integration work, some countries have to come to a collaborative method to ensure cybersecurity and the development of digital services.

The experience of advanced countries in the field of digitalization and cybersecurity such as the United States of America, Singapore, Estonia and Russia show that the state plays a crucially an important role in the formation of a national information development strategy (Bhaskar C., and Ravi S., 2017). Along with the development of digital services, cybersecurity issues in the digital space are becoming relevant every year. Thus, nowadays the cybersecurity issues are one of the important problems in both private and public administration. The importance of cybersecurity issue can also be seen from the innovations that are taking place at the global level. For example, one of the important regulatory measures taken is the document adopted by the European Union in May 2018 "General Data Protection Regulation" (Greengard, S. 2018). The main message of the document is the reform in the field of personal data security of citizens of the European Union (Sousa, M. et al. 2018).

In the article the experience of Estonia and Russia is regarded as the flagship of advanced technologies. Historically, Russia has dominated in all major areas. In general, Kazakhstan's public administration policy is very similar to the Russian Federation. After the collapse of the USSR, Kazakhstan had to build its sovereign independence, as well as other states that were part of the USSR. At the same time, if we consider the index indicators of Estonia, they are surprising with their achievements not only in digitalization, but also in cybersecurity. It should be noded that Estonia was also part of the post-Soviet countries, even though they have achieved termendouse resuls among post-Soviet countries

Many scientists in their research argue that the development of digital services directly affects the level of democracy in the country. As a result, the analysis of the literature shows that the majority of scientific papers on the development of digitalization of post-Soviet countries considers E-government as the main indicator of digital society (Lagutina M., 2014), and Kazakhstan understands it in the same way. According to the research results, the main barriers to improving the digital and innovative nation is a poor level of economic performance (Bershadskaya L., Chugunov A., Dzhusupova Z., 2013), as well as the lack of democracy (Ramaswamy M., 2009).

The article is organized as follows: the next section describes the methodology with examines the current situation of Kazakhstan in the field of cybersecurity and digitalization. Then, we look at a discussion of the results of the conducted online survey. In the following, the successful experience of number of foreign countries such as the United States of America and Singapore are considered, which were determined by the GCI, as well as IMD WDC ranking. At the same time, the authors analyzes the indicators of digitalization and cybersecurity in Estonia and Russia. In this case, Russia and Estonia were chosen due to the similar post-Soviet past and starting potential. At the same time, Kazakhstan is geographically bordereds on Russia, which directly has a geopolitical and economic impact on the country. In conclusion, the authors of the article will offer possible practical suggestions and recommendations to ensure cybersecurity in the global digital space. Aditinally will be given possible solutions that can be implemented not only in Kazakhstan, but also in other countries which are undergoing a digital transformation period.

2. Methodology

The study used both qualitative and quantitative research methods. The aim of the study is determine the level of public awareness in cybersecurity and the introduction of digitalization in Kazakhstan. An online survey conducted among digital services users by using Google Docs instruments. Total number of online respondents who showed interest is 173. The survey was conducted within a month. At the same time, interviews were conducted among employees of RSE "State technical service" and KZ-CERT. The number of interviewed is 12 experts. It should also be noted that the authors implemented empirical and theoretical analysis. In addition, the issues of the importance of public confidence in the implementation of the Concept of Cybersecurity and the State program "Digital Kazakhstan" are discussed. At the same time, it is planned to consider and analyze the adopted legal documents in the framework of the introduction of cybersecurity and digitalization of Kazakhstan. In addition, the international experience of successful countries in the implementation of digitalization and cybersecurity issues are studied.

Thus, primary and secondary dates are used and analyzed in the study. The primary date is obtained from the online survey, while secondary data is obtained from the GCI and IMD WDC ranking.

Based on the results of the analysis, practical recommendations are proposed that can be useful not only for Kazakhstan, but also for other countries that are implementing and developing digital technologies, and are undergoing a period of digital transformation. It is believed that the results of the study will be of interest to the post-Soviet countries, as these countries have a common history of independence. Information received from respondents is strictly confidential and anonymous. They are used only as part of the research and for the publication of the paper.

3. Results

3.1 Current situation in Kazakhstan

Nowadays the issues of cybersecurity along with the digitalization of public services are one of the priorities of Kazakhstan's state policy. For example, in early March 2019, the President of the Republic of Kazakhstan adopted the Law "On ratification of the Agreement on cooperation of the member States of the Collective security Treaty organization in the field of information security" (Adilet database, 2019).

It should also be noted the activities of JSC "National Infocommunication Holding Zerde". The organization was established in July 2008. In 2009 the organisation created a master plan for the development of E-government and E-services for 2010-2014, as well as a package of regulations on E-government and information security infrastructure. Zerde holding organized the international conference "Digital communication 2012" and took part in the international exhibition "GITEX technology week" (UAE, Dubai, October 6-9, 2011). In 2012, the ICT development Fund was established on the initiative and with the support of the Ministry of transport and communications. Since 2012 on the basis of holding the Technical Committee on standardization No. 34 "Information technologies" on the basis of which standards and also normative documentation on standardization in ICT are developed and coordinated functions. In 2013, the Holding took an active part in the development of the state program "Information Kazakhstan – 2020". In 2014, as part of the "Global e-Government Forum", the Holding jointly with JSC "international IT University" held the first international Scientific and practical Conference "SmartGovernment: Science and Technology". October 25, 2015 president of the Republic of Kazakhstan N. Nazarbayev signed a new Law "On Informatization". In 2016, as part of the implementation of the Law "On Informatization" by the government of Kazakhstan, the holding was determined as a service integrator of "electronic government". In addition, in 2016, in order to develop human capital and improve digital literacy of the population, JSC "Holding Zerde" held an off-site event in 6 cities of the Republic of Kazakhstan to teach students of 9-11 grades and teachers of the subject "Informatics". As a result of the event, 117 teachers and 130 puple schoolchildren were trained. In November 2016, JSC "National Infocommunication Holding "Zerde" was determined by Kazakhstan's government by the National Institute of development in the field of information and communication technologies (Zerde, 2019).

At the same time, it should be pointed out that the JSC "National information technologies" (JSC "NIT") has been operating in Kazakhstan since 2000. Currently JSC "NIT" is one of the largest companies in Kazakhstan's IT market (official site of JSC "NIT", 2019). The purpose of this company is to develop a single information space in the Republic of Kazakhstan. Within its competence, JSC "NIT" performs the following tasks of the operator of information and communication "E-government" infrastructure;

- ensuring compliance with uniform requirements in the field of information and communication technologies and information security, as well as the rules for the implementation of the service model of Informatization;
- implementation of system maintenance and maintenance of Internet resources of state bodies and objects of information and communication infrastructure of "E-government" in accordance with the list approved by the authorized body;
- provision of information and communication services to public authorities on the basis of information and communication infrastructure of "E-government" in accordance with the catalog of information and communication services;
- ensuring the security of storage of state electronic information resources placed on the information and communication infrastructure of "E-government", assigned to the operator;
- ensuring the security of storage of state electronic information resources in the provision of information and communication services;
- ensuring rapid response to the identified shortcomings in the provision of information and communication services, as well as public services in electronic form and taking measures to address them;
- implementation of integration and connection of local, departmental and corporate telecommunications networks of state bodies to the information and communication infrastructure of "E-government»;
- provision of data transmission services to state bodies, their subordinate organizations, local self-government bodies, as well as other subjects of Informatization, determined by the authorized body and connected to the unified transport environment of state bodies, for the functioning of their electronic information resources and information systems;
- creation and development of information and communication platform of "E-government" and unified transport environment of state bodies;
- support and system maintenance of the national gateway of the Republic of Kazakhstan;
- information content of the E-government web portal.

It should also be noted that the decree of the President of the Republic of Kazakhstan in January 2018 formed a Commission under the President of the Republic of Kazakhstan on the implementation of digitalization in the Republic of Kazakhstan (hereinafter – the Commission) (Adilet database, 2017).The Commission is an Advisory body under the President of the Republic of Kazakhstan. The task of the Commission is to develop proposals on the introduction of digitalization and information technologies in the Republic of Kazakhstan. To accomplish this task, the Commission:

• makes recommendations on the implementation of digitalization and digital technologies in the Republic of Kazakhstan;
• conducts monitoring on the effective implementation of the State program "Digital Kazakhstan" and undertaken by governmental agencies and other organizations of measures for implementation of the adopted decisions on the introduction of digitization in the Republic of Kazakhstan.

In order to improve the efficiency of government bodies and the availability of public services, Kazakhstan successfully introduced E–government in 2008, a single mechanism of interaction between the state and citizens, as well as state bodies with each other, ensuring their consistency with the help of information technologies. During its existence, the electronic government of the Republic of Kazakhstan has overcome four stages of formation and development has repeatedly held high positions in international rankings and nominations (WSIS Project Prizes 2013, First World Govtechineers Race-2017, WSIS Prizes-2017, etc.). The degree of development of Kazakhstan's E-government system is estimated as "developing" (emerging leaders) and is

considered one of the most successful. According to the International Institute for Management Development's World Digital Competitiveness ranking (IMD WDR) Kazakhstan consistently over the last 2 years (2017-2018) the country occupies 38th position.

Figure 1 Comparative analysis of indicators between the World Digital Competitiveness ranking and the Global Cybersecurity Index. The diagram is developed by the author. *Source from IMD WDC ranking, 2017, pp. 28-29, and GCI, 2017, pp. 59-65) for 2017.*

However, it should be noted that the indicator of Kazakhstan in cybersecurity 2017 leaves much to be desired in comparison with digitalization. According to the GCI-2017 Kazakhstan was 83rd. A comperative diagram illustrates the indicators of the WDC IMD ranking (2017, pp. 28-29) and the GCI (2017, pp. 59-65) for 2017, it can be seen in Figure 1. If we consider the indicator of Kazakhstan in cybersecurity for 2017 among the countries of the former USSR, Kazakhstan is ahead only of Tajikistan, Uzbekistan, Kyrgyzstan, Armenia, and Turkmenistan. Given the economic and social opportunities and investment attractiveness of Kazakhstan, this indicator is one of the worst results for the country, and was a signal for taking the necessary actions to improve the level of cybersecurity. The government needs to pay attention not only to digitalization but also to cybersecurity, as the introduction of digital technologies simultaneously requires the protection of digital data. For example, Estonia emphasizes the security of information systems. Recommended measures are civil in nature and are based on legal regulation, training and cooperation. As a result, in June 2017, the Kazakhstan's government approved the Concept of cybersecurity "cyber Shield of Kazakhstan» (the Concept of cybersecurity, 2017). The cybersecurity framework was developed in accordance with the message of the President of the Republic of Kazakhstan "the third modernization of Kazakhstan: global competitiveness" with the approaches of the Strategy "Kazakhstan-2050" on the entry of Kazakhstan into number of 30 most developed countries of the world. In general, the concept of Cybersecurity is based on the assessment of the current situation in the field of Informatization of state bodies, digitalization of public services, prospects for the development of the "digital" economy and technological modernization of production processes in industry, expansion of the provision of ICT services. The cybersecurity Concept defines the main directions of implementation of the state policy in the field of protection of electronic information resources, information systems and telecommunications networks, ensuring the safe use of ICT. In order to develop the cybersecurity Concept, the international experience studied Protection of national information and communication infrastructure of the leading states, use of ICT and countries are seeking to expand their scope to achieve the goals of socio-economic development was taken into consederation to implement the Kazakhstan's cybercecurity Concept. As part of the implementation of the cybersecurity Concept at the end of 2017, the action Plan for its implementation until 2022 – "cyber shield of Kazakhstan", covering organizational, legal, technical and educational activities was approved (cyber shield of Kazakhstan plan-2022, 2017).

Additionally, in order to improve the level of cybersecurity in Kazakhstan, a number of changes in public administration have been carried out. In accordance with the decree of the President of the Republic of Kazakhstan, the Committee on information security of the Ministry of defense and aerospace industry of the Republic of Kazakhstan was formed (Adilet database, 2016).

What is more, in accordance with the decree of the Government of the Republic of Kazakhstan in 2017, the Republican state enterprise on the right of economic management "State technical service" was transferred to the national security Committee of the Republic of Kazakhstan. The main purpose of the organisation is to carry out certain activities in information security, and also contributes to the organization of the formation, development and security of information space and communication infrastructure of the Republic of Kazakhstan (State technical service's official site, 2019). KZ – CERT was also established which is a computer incident response service. KZ-CERT is a single center for users of national information systems, providing collection and analysis of information on computer incidents, advisory and technical support to users in the prevention of computer security threats. The main task of KZ-CERT is to reduce the level of cyber security threats to users of the Kazakh segment of the Internet (official website of KZ-CERT, 2019).The work carried out by the Government has a positive trend in the number of information security incidents in Kazakhstan (see Figure 2. The number of information security incidents in Kazakhstan for 3 quarters of 2018).

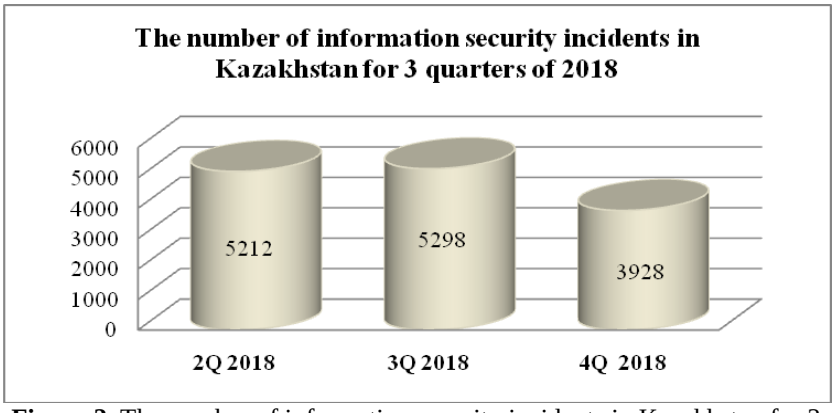

Figure 2. The number of information security incidents in Kazakhstan for 3 quarters of 2018. The diagram is developed by the author. *Source from http://kz-cert.kz/ru/infographics*

According to the data of the Committee on legal statistics and special records of the General Prosecutor's office of the Republic of Kazakhstan, 106 criminal cases were registered for 10 months of 2016 on cybercrime. The Ministry of information and communication of the Republic of Kazakhstan highlighted

that 16 576 cyber incidents were registered in 9 months of 2016: 688 of them were detected in relation to state institutions (computer incident response Service, 2016).

However, it should be noted that in the history of Kazakhstan's independence has repeatedly decided to dissolve the Government and early resignation of the President of the Republic of Kazakhstan. For example, in February 2019, the decree of the President of the country decided to dismiss the Government of the Republic of Kazakhstan (Adilet database, 2019). Later on March 20 of the same year, the President announced his early termination of powers (official site of white house, 2019). There is believed that the ongoing political and managerial changes in the country adversely affect the country's development, as a frequent change in the country reduces the interest of foreign investors. Foreign investors understand that systematic changes in the country leeds instability of the country's political activity. Thus, these changes have a direct impact on the security of the country. Unstable political processes of the nation reduce the attractiveness of not only investors, but also tourists, which directly affects the economy as a whole. Moreover, the approval of the new government will take a long time. These developments have directly affected the activities of the sectoral Executive body in the development and application of ICT in the country.

If we consider their activities since the independence of Kazakhstan, it can be noted that in 2016 №253 decree of the President of the Republic of Kazakhstan "On measures to further improve the system of public administration of the Republic of Kazakhstan" decided to form the Ministry of information and communications of the Republic of Kazakhstan with the transfer of functions and powers of the Ministry of investment and development of the Republic of Kazakhstan in the field of information and communication (Adilet database, 2016). Later in 2019 No. 848 by the decree of the President of the Republic of Kazakhstan the decision on reorganization of the Ministry of public development of the Republic of Kazakhstan by its transformation into the Ministry of information and public development of the Republic of Kazakhstan with transfer of functions and powers in the field of information from the Ministry of information and communications of the Republic of Kazakhstan was taken back. The decree also instructed to transform the Ministry of defense and aerospace industry of the Republic of Kazakhstan into the Ministry of digital development, defense and aerospace industry of the Republic of Kazakhstan with the transfer of functions and powers in the field of communication, informatization, "electronic government", development of state policy in the provision of public services from the Ministry of information and communications of the Republic of Kazakhstan (Ministry of digital development, defense and aerospace industry of the Republic of Kazakhstan, 2019).It is assumed that the ongoing frequent reorganization can be a barrier to the development and application of digital technologies, as well as the effectiveness of government programs in the field of digitalization and cybersecurity. Thus, in public administration, in order to achieve effective results and achieve long-term goals, it is necessary to form a stable structure of the government and take all necessary measures to minimize the leakage of personnel. Confirmation of this is the WDC ranking indicator, which does not change its position while remaining at the same position as in 2017 (38th place). But, it should be noted the huge breakthrough of Kazakhstan in the field of cybersecurity. According to GCI (draft) 2018 Kazakhstan raised its rating from 83rd position to 40th position, which is an incredible achievement for Kazakhstan in such a short period of time. According to the Concept of cybersecurity, Kazakhstan was given the task to increase the cybersecurity index by 2008 - 0.300, by 2019 – 0.400, by 2020 – 0.500, by 2021 – 0.550, by 2022 – 0.600, but according to GCI draft for 2018 it can be seen, that Kazakhstan has achieved a mark – 0.778. Thus, for today Kazakhstan has exceeded its expected goals. In this regard, it is necessary to update the Concept of cybersecurity by introducing new priority goals and objectives. Countries like the United States of America and Estonia, as in previous years, occupy leading positions, while the indicators of cybersecurity in Singapore decreased by 5 positions, and Russia by 16 positions. However, it should be noted that today the indicators of GCI (draft) - 2018 on the official website are not the final version yet. See Figure 3. Comparative diagram between WDC 2018 and GCI 2018 indicators.

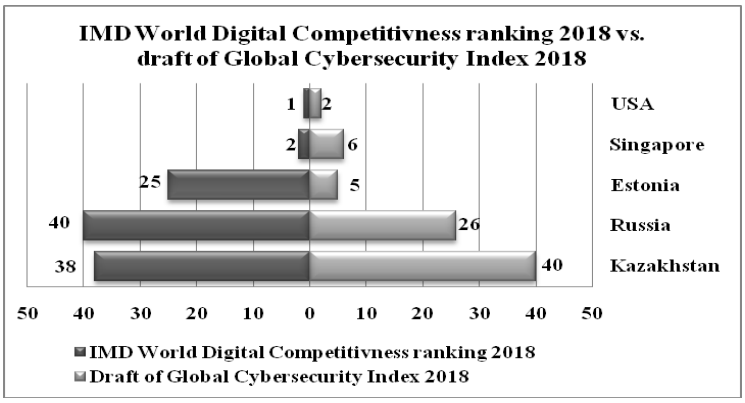

Figure 3. Comparative analysis of indicators between the World Digital Competitiveness ranking and the Global Cybersecurity Index (draft). The diagram is developed by the author. *Source from IMD WDC ranking, 2018, pp. 26-27, and GCI, 2018, pp. 51-58) for 2018.*

Certified expert on information security, president and founder of the Center for analysis and investigation of cyberattacks - Olzhas Satiev notes that more than 90% of Kazakhstan's Internet resources are vulnerable: "Previously, Kazakhstan did not face with cyberattacks due to information technologies were not so developed, thus, there was nothing to break". Also, O. Satiev stressed the lack of qualified specialists in the field of information security (N. Aslanova, 2016).

In this regard, it is necessary to conduct courses to improve literacy in the field of cybersecurity for different segments of the population, as well as training certified specialists in the field of information security. Nowadays, within the framework of the Kazakhstan's cybersecurity Concept at the expense of the national budget, it is planned to train future cybersecurity specialists under the program "Provision of personnel with higher and postgraduate education" for 2018-2020 (cybersecurity Concept, Adilet, 2018).

The goal of the third modernization is global competitiveness, it was announced the first president of the country N. Nazarbayev in January 2017. There are five main priorities of modernization, designed to ensure the growth rate of the economy above the world average and steady progress in the number of 30 advanced countries, including accelerated technological modernization of the economy (Adilet database, 2017). In December 2017, the state program "Digital Kazakhstan" (implementation period 2018-2022) was adopted, the main purpose of which is to improve the quality of life and competitiveness of the economy of Kazakhstan through the progressive development of the digital ecosystem. The development of digital technologies is considered as one of the ways of diversification of the national economy, its reorientation from the raw material to the industrial and service model and the use of new opportunities for the labor market.

Undoubtedly, the planned way of digitalization of Kazakhstan is very ambitious, and the results achieved by the state for more than 25 years of independence speak for themselves and allow us to hope for the successful implementation of the strategic objectives of “Digital Kazakhstan”. The main goal of the country is the plan of entering the number of 30 developed countries of the world, declared by the President of country by 2050.

Thus, by 2022 Kazakhstan aims to increase the level of digital literacy of 83% of the population, in the program “Digital Kazakhstan” the main part of the indicators is aimed at increasing productivity in the priority areas of the economy, creating jobs and increasing investment in start-ups. Thus, the government of Kazakhstan is carrying out a number of works aimed at improving the provision of public services using information and communication services.

3.2. Other countries experience

There are many researchers in the world who pay attention to the study of the introduction of digital technologies and methods of their protection. However, it should be noted that in Kazakhstan there are a few researchers in this field and the issues of cybersecurity for Kazakhstan is one of the important issues of public administration, and has a priority in the state policy of the country. Many scholars, such as Eileen Vilborg, Hedstrom Karin and Hanna Larsson (2017, p. 2549) believe that E-government has many advantages such as efficiency, transparency, democratization, as well as the economic feasibility of public services.

However, despite a number of advantages, the introduction of digitalization carries certain threats such as the loss of big data due to cyberattacks. For example, Weiling Ke and Kwok Ki Wei (2004, p. 95) noted that Singapore's leadership has looked forward to a digital future since the mid-1990s, but their efforts to introduce digitalization have been hampered by various challenges that other countries have also faced. However, despite all the difficulties, today Singapore is a leader in the implementation and use of digital technologies and ensure their protection according to IMD WDCR (2017, p. 2, 2018, p. 26) and GCI (2017, p. 59, 2018 p. 51) during 2017-2018. GCI is calculated annually. For the first time GCI integration was carried out in 2013-2014. In this ranking, countries such as Kazakhstan, China, Thailand, Hungary, Bulgaria, Philippines, Ukraine were at the stage of maturation, while Singapore, USA, Russia were among the leading countries in the world (GCI, 2017, p. 15).

Singapore is a country which first developed its master plan on cybersecurity back in 2005 and in 2015 created the cybersecurity Agency, and in 2016 a cybersecurity strategy was developed. That is along with the development of digital technologies, information security in cyberspace is ensured (GCI, 2017, p. 32). Theris is no secret that cyber attacks have become more frequent in recent years. According to the Global Data Protection Index survey results 72% of respondents believe that data protection is crucial for the success of the organization, the same opinion is shared by 80% of respondents in the public sector (EMC Global Data Protection Index, b.d.). Lloyd's research result showed that a cyber attack could cost the global economy more than 120 billion pounds, as much as the cost of catastrophic natural disasters such as hurricanes Katrina (the Guardian, 2017).

Additionally, other research in this area has shown that on average, the company spends $ 211 million on information technology; $ 14 million on data protection, the most spending on data protection is public sector– 10.17% of the budget (Key Findings & Results for Italy, 2014).

A significant indicator of this country's desire for digitalization is the fact that the state budget for 2018 provides funds for the creation of a unified digital society. This project has several directions (official website of Singapore, 2018):

- basic digital skills for daily activities (Infocomm Media Development Authority (IMDA), a 6-hour training program “Basic digital skills for daily activities”. The curriculum includes information retrieval, online transactions, electronic payments, and access to government digital services. The program also provides appropriate modules on cybersecurity and information literacy;
- digital clinics and experimental travel (Digital Clinics and Experimental learning journals), providing assistance in the use of smartphones by elderly people over the age of 50 years, who previously had no experience in the implementation of electronic payments;
- digital readiness and libraries promoting resources of the national Library Board (the National Library Board NLB) through the mobile application NLB, which provides access to the library and its resources and services. Also for 2018 is scheduled to launch the presentation platform for the elderly TechShare;
- future skills and libraries that encourage continuous learning of the digital economy through libraries. In the framework of programs such as workshops SkillsFuture Advice (SFA) and SkillsFuture Digital Workplace (SFW), NLB aims to train Singaporeans in new skills necessary for the development of the digital economy;
- NLB will present a series of Re-Employability to guide older people at different stages of their careers, in order to update their skills and promote their advancement. In this project it is planned to cover more than 5,000 elderly people in the course of the year.

At the same time, Singapore’s Ministry of defense plans to train national military personnel in new specializations in cyber industry. The most promising in the field of cybersecurity students will be awarded the Cyber Specialist Award, which is a short-term contract for three to four years (official site of Singapore, 2018).

It is not coincidence that Kazakhstan has chosen the strategy of E-government because as noted Gary Marchionini, Hanan Samet and Larry Brandt (2003), “Digital government is a global phenomenon, and civil servants around the world are using new methods of information technology for better service to their voters».

At the same time, the way of implementation and development of digitalization is thorny. Jing Zhanga, and Yushim Kimb (2016, p. 215) pointed out ten problematic aspects in digitalization which is the lack clear description of potential solutions to problems. According to the study, unresolved issues lead to poor implementation of state program projects in digitalization.

However, according to Sehl M.,, Luis F., Luna R., and Jing Zh (2014), in order to achieve the expected results and improve the quality of citizens life the government needs to create new services by involving citizens who will test and use new technologies. They define two main components: the widespread use of digital technologies by the government, and the citizens should interact with government by using the technologies.

The review results showed that Kazakhstan supports the global trend towards digital development and achieved good results in this industry. At the same time, like any other innovative idea introduced through the use of digital technology brings both positive and negative trends. In this regard, along with the implementation of projects in the field of digitalization, it is necessary to pay close attention to ensuring their security, as today information leakage and hacking of information systems require not only significant financial, but also highly qualified human resources in information technology and cybersecurity.

3.3. Online survey results

As part of the research in cybersecurity and digitalization an online survey was conducted among the citizens of Kazhastan during the month. The survey was conducted through the use of social networking sites as Facebook, the educational portal of the Academy of public administration under the President of the Republic of Kazakhstan – Platonus (http://platonus.apa.kz/) and what's app mobile apps, and Telegram. Overall 173 respondents were actively participated. Most of them are citizens aged 31 - 40 years (42 %). See Figure 4. An interesting fact is that the majority of respondents showing interest are women (88) and men – 85.

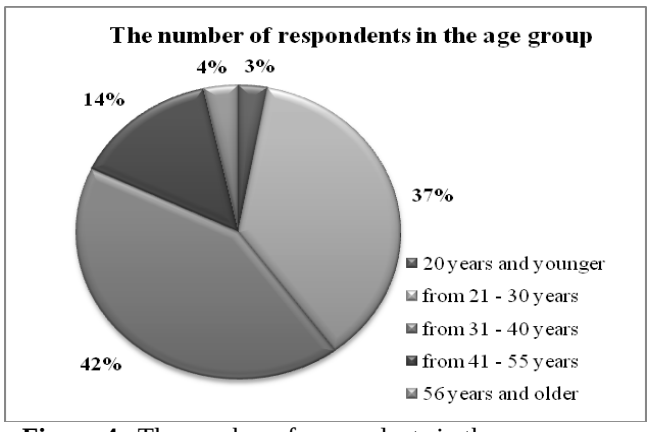

Figure 4. The number of respondents in the age group

In order to identify the activity of citizens in the use of online services the question was formulated: How often do you use online services (including public services Egov)? According to the survey results presented in Figure 5, it can be clearly seen that citizens of Kazakhstan are not so actively using online services: out of 173 respondents, only 8 people use online services every day. 78 people use it once a quarter.

It is obvious that this indicator is a signal to both the state and the private sectors to think about the motivation of citizens to use online services. After all, the state budget has been allocated quite a few funds for the introduction of digital public services. In order to identify the causes of passivity of citizens, a question was formulated to identify the quality and cost of online services. According to the survey on the question "How do You evaluate online services in the Republic of Kazakhstan, given their cost and quality?". In General, the majority of Kazakhstanis believe that online services are good (71), 64 respondents are satisfied with the quality and cost, while 22 respondents give a very good assessment, and only 16 respondents noted the low quality of services. Summing up, it can be noted that Kazakhstan online services in General have positive dynamics in terms of quality and cost.

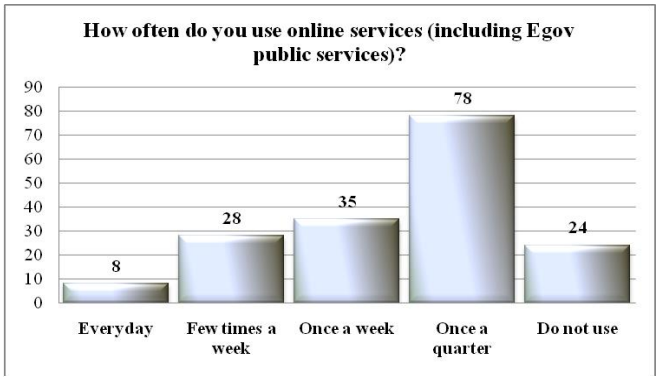

Figure 5. Q. How often do you use online services (including Egov public services)?

In order to avoid possible cyber threats, it is necessary to analyze what risks Kazakh Internet users face most often. Thus, selected a list of threats that in our opinion could be barriers to the use of online services. As a result, 92 respondents believe that there is a very high probability of loss of personal data, as well as problems with the network (68) and user problems (63), then 81 respondents believe that there are risks of cyber attacks. According to the indicators presented in Figure 6. it is necessary to pay great attention to possible cyber attacks, improve the system to ensure the security of personal data. Additionally high-speed Internet access needs to be provided.

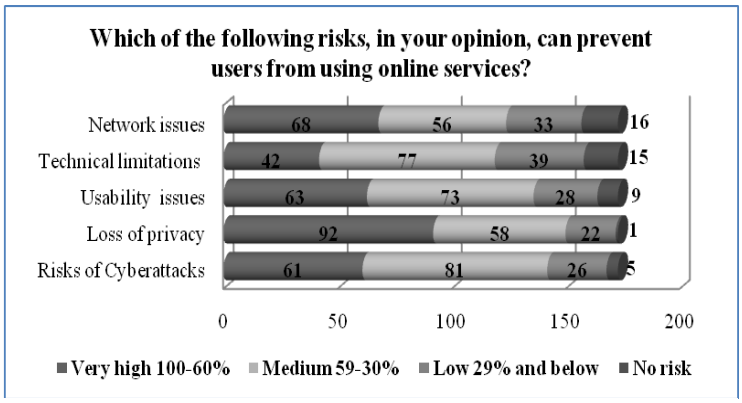

Figure 6. Q Which of the following risks, in your opinion, can prevent users from using online services?

To the question "Can you identify the main threats to the further development of digital services in the Republic of Kazakhstan?". The majority of respondents noted the lack of qualified specialists -126, the next threat to respondents is cyber attacks, i.e. the vulnerability of networks - 86. They also believe that the low level of digital literacy of the population - 66, poorly developed system of service providers – 45, and only 10 respondents noted that today there are no threats.

There is an acute problem of shortage of specialists in the field of cybersecurity, despite the fact that in this area in 2018 the number of graduates there are more than 600 specialists. Kazakhstan's government is taking into account the importance of this issue, so for the 2018-2019 academic years for training in the specialty "Information security systems" allocated 675 seats for the state order (Ministry of education and science of the Republic of Kazakhstan, 2018).

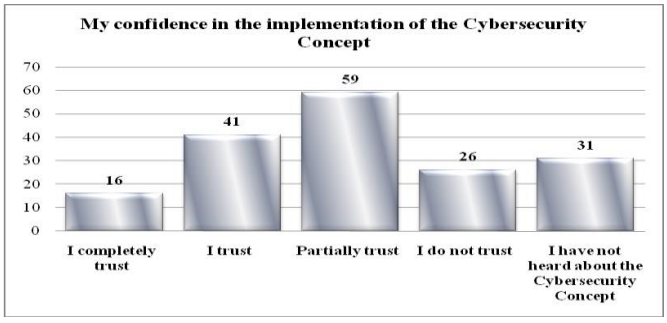

Figure 7. My confidance in the implementation of the Cybersecuriry Concept.

It should also be noted that the confidence of the population in the implementation of government policy is one of the important and priority tasks of any state. In this regard, the survey provides the opinion of respondents regarding their confidence in the implementation of the Concept of cybersecurity. The survey results illustrate that more respondents have a positive trend in the implementation of the Concept of cybersecurity in Kazakhstan (see Figure 7.). However, 31 respondents out of 173 are not aware of the existence of the Concept, and 26

respondents are pessimistic in the implementation of it. The results lead to the fact that the government needs to constantly conduct awareness-raising activities with the population in order to increase their confidence in the ongoing government projects and initiatives. Respondents believe that it is necessary to promote among the population the introduction of new technologies and their impact on the ongoing reforms in cybersecurity and digitalization. Also to increase the literacy of the population in computer and legal literacy in remote, rural areas, it is needed to organize training courses for the population on the use of public services, and make them available for large-scale use. At the same time, to analyze foreign experience and introduce proven innovations. Increase the safety of personal data of citizens and exclude the use of third parties. It is also proposed to create a Center for cybersecurity with highly qualified specialists with deep knowledge of management.

Respondents' comments

According to respondents the above measures will prevent cyber threats that may arise in the future. Moreover, it is urgently necessary to provide training of specialists in cybersecurity in Universities, academies of the national security Committee of the Republic of Kazakhstan and the Ministry of Internal Affairs of the Republic of Kazakhstan. Some respondents in the survey were not able to come up with any ideas, but they believe that cybersecurity is extremely important nationally as well as globally.

One of the respondents gave an example of a cyber incident in one of the largest oil and gas Company "North Caspian operating company", which occurred in 2016. According to the data is provided by the respondent, the company's network was hacked and within 2 months the company's employees could not use computers in the workplace, despite the fact that the company allocated quite a few funds for foreign, licensed information technology and software.

More respondents believe that it is necessary to develop human capacity in cybersecurity, as it is practiced in the United States and India, and at the same time to have large international hubs. If necessary, consider increasing the number of servers located in the territory of the Republic of Kazakhstan, gradually abandoning foreign services, which hang in turn on the security and at the same time increase the domestic market. Try to make maximum use of domestic software solutions and products, as this will increase the competitiveness of the Kazakh market and will reach the international level.

Make information as accessible as possible to the people by improving quality. Most important is that we need to increase consumer confidence.

To consider the possibility of stimulating University teachers in order to attract highly qualified specialists, and systematically send them to trainings on cybersecurity. Develop cybersecurity regulations by using blockchain technology. Expand the use of mobile gadgets using security protocols. Modern cybersecurity is a team effort. On the basis of the plan "Cybershit", the government should not shut out the world and to do it in a closed form is a utopia. It is also necessary to work with other countries and companies within the framework of cooperation.

As an example, you can and should use cloud services such as Amazon Web Service, Microsoft Azure, etc., as these companies are more competent, and also better ensure the security of their servers.

One of the respondents answered critical conducted an online survey expressing their opinions in the following way

R. *"It is necessary to punish civil servants in order to really identify poor-quality execution. For example, the Ministry of information and communication of the Republic of Kazakhstan (hereinafter-MIC RK) reports that all districts and counrtysides are connected to the Internet. But in fact, they do not have access to the Internet. What is more, with such small salaries, it is difficult for civil servants to accept innovations. High risks of corruption and failure of the program due to formal reporting and the MIC RK will never admit its mistakes. All figures and statistics are drawn by civil servants for fear of being punished.... ".*

Other respondents are also comments as following:

R. "*To improve the quality of an informed, qualitative approach to the study of the topic, because of this I can not make any proposals, because first all citizens must be educated in this matter*".

R. "*Organizing open discussion platforms with the involvement of IT experts are important. Openly discuss existing problems and issues. Also, need to allocate time to domestic TV channels, so people can be informd about current issues*".

R. "*Create a platform within egov.kz to collect proposals (feedback) from the population to finalize the program in terms of the implementation of new initiatives that are not included in the 1st edition of the state program of Digital Kazakhstan*".

R. "*Replace TIN with bar code. And it is also necessary to increase the overall confidence in the government. The government, private companies should organize training courses for citizens of Kazakhstan*".

R. "*It is necessary to study users and their values in more detail. The villages of the country shoul are connected to the Internet*".

R. "*For me, digital Kazakhstan is a departure from the paper bureaucracy in the first place. If this state program will help us to cope with this huge disadvantage, I think that it will be excellent*".

R. "*It is necessary to radically simplify the mechanism of Public Private Partnership and the service model of Informatization and facilitate the procedures for the purchase of IT services for government agencies, and provide for the transition to smart government".*

R. "*Organize cooperation with community, conduct training seminars for a few days free of charge. Invite specialists from quasi-public and private sectors*".

As part of the research work among the employees of Republican state enterprise on the right of economic management "State technical service" of the National Security Committee of the Republic of Kazakhstan and KZ-CERT conducted interviews.

During the interview, the employees of KZ-CERT and Republican state enterprise on the right of economic management "State technical service" of the National Security Committee of the Republic of Kazakhstan noted that the ongoing state reform in the field of cybersecurity, the transfer of their activities under the leadership of the National Security Committee of the Republic of Kazakhstan has significantly improved the efficiency and efficiency of their work. Employees also note that the bureaucratic barriers that were previously experienced at the Ministry of information and communications of the Republic of Kazakhstan have decreased significantly. However, they are not entirely satisfied with the amount of wages. As they mantined the number of highqualifide experts in IT and certified employees in cybersecurity are leaving the coutry due to salary. Thus, policymakers should worry about keeping own qualified emplyees and make Kazakhsatan more attractive to other nations. In this case Singapore experiences should be used. To make border open for highly qualified experts.

4. Conclusion

The article deals with the issues of cybersecurity and digitalization of Kazakhstan. In addition, the experience of successful countries such as the USA, Singapore, Estonia and Russia, which were determined according to the GCI and IMD WDC ranking, were also partially considered. Moreover, Russia and Estonia are chosen taking into account the fact that these countries like Kazakhstan were part of the former USSR. The authors also describe the current situation of Kazakhstan in the field of cybersecurity and digitalization. An online survey was conducted with the participation of 173 respondents. At the same time, interviews were conducted with 12 employees of RSE State technical service and KZ-CERT.

According to the results of the analysis, in order to minimize the negative consequences of cyber attacks, it is necessary to work to improve the literacy of the population in the use of digital, information and communication technologies. On an ongoing basis, to study the experience of other states to minimize possible risks and not to repeat the faults have been made by other countries.

Currently, Kazakhstan is developing with an emphasis on the introduction of advanced technologies, seeking to improve the efficiency of public administration. The introduction of digital technologies undoubtedly has a positive impact on the development of social and economic situation of the country and on the overall effectiveness of the government. However, the implementation of projects on the use of digital technologies requires an integrated approach with the mandatory consideration of their protection and security. It is necessary to consider the possibility of reducing the tariff for mobile services and the Internet.

At the same time, the government should take measures on a permanent basis to reduce the risks of inequality of implemented technologies, as in the context of globalization, intersystem integration works with near and far foreign countries are considered. This work should be carried out not only by the government but also by business with the involvement of civil society. Only in case of active involvement of civil society in the implemented state programs it is possible to achieve universal recognition, trust of the population and successful implementation of strategic objectives.

Despite Kazakhstan's adoption of the cybersecurity Concept and its realization plan as such a fundamental strategy of the country. Accordingly, there is no clear trajectory of the strategic plan on cybersecurity in the country, identified only the main directions without their implementation assessment. In this regard, it is considered that there is necessaty to develop and adopt Kazakhstan's cybersecurity strategy thorough study of the strategies of successful countries and adapt it by concidering Kazakh national, cultural and mental characteristics.

There is a shortage of highlyqualified, certified experts in cybersecurity in Kazakhstan. State policy should focus on attracting and training highlyqualified specialists in information security. In order to effectively implement the adopted state programs and concepts, heads of state bodies need to provide their employees with additional time for training, selfdevelopment and learning from the best practices of the world, which in the future will make it possible to avoid faults and risks faced by other nations.

Undoubtedly, Kazakhstan over the years of independence has done a lot in cybersecurity and digitalization but there is still a long way to go. Based on the results of the study, Kazakhstan despite the advance of Russia in digitalization, focused on general issues of digitalization, whereas the Russian Federation aims of the digitalization of the economy in general with achieving ambitious goals on a global masstime.

After analyzing the existing performance indicators in international rankings and their impact on socio-economic development of the country, and with the view discussed in the article the achievements of foreign countries, the authors come to the conclusion about the necessity of active measures by Kazakhstan to development of digitization and cybersecurity.

In order to obtain a large-scale effect, it is necessary to attract foreign investors to obtain additional funds for the implementation of the cybersecurity Concept and the state program "Digital Kazakhstan" by creating appropriate conditions for business development in IT industry for domestic and foreign companies. It is assumed that the above mentioned comprehensive measures will have a large-scale effect to increase the level of digitalization and cybersecurity of the country.

However, futher deep study is needed in order to minimise possable risks during the adoption and implimantation of national projects and programms in terms of cybersecurity and digitalisation. What is more, it has to be considered that IT market is growing and changing people's way of living in daily basis considerably.

References

1 Warnes, K., PhD (2019) '*Cybersecurity*', Salem Press Encyclopedia. Available at: https://ezproxy.nu.edu.kz/login?url=https://ezproxy.nu.edu.kz:2358/login.aspx?direct=true&db=ers&AN=89677538&site=eds-live&scope=site [Accessed 20 March 2019].

2 Bhaskar Chakravorti and Ravi Shankar Chaturvedi. Digital Planet 2017: *How competitiveness and trust in digital economies vary across the world*. – Available at: https://sites.tufts.edu/digitalplanet/files/2017/05/Digital_Planet_2017_FINAL.pdf, [Accessed 20 March 2019].

3 Greengard, S. (2018). Weighing the Impact of GDPR: *The EU data regulation will affect computer, Internet, and technology usage within and outside the EU; how it will play out remains to be seen.* Communications of the ACM, 61(11), 16–18. Available at: https://doi.org/10.1145/3276744, [Accessed 2 March 2019].

4 Sousa, M. et al.(2018) 'openEHR Based Systems and the General Data Protection Regulation (GDPR)', Studies In Health Technology And Informatics, 247, pp. 91–95. Available at: https://ezproxy.nu.edu.kz/login?url=https://ezproxy.nu.edu.kz:2358/login.aspx?direct=true&db=mdc&AN=29677929&site=eds-live&scope=site [Accessed 2 March 2019].

5 Lagutina M. Eurasian Economic Union Foundation: Issues of Global Regionalization // Eurasia Border Review. – 2014. – №5(1). – P. 102

6 Bershadskaya L., Chugunov A., Dzhusupova Z. *Understanding E-Government Development Barriers in CIS Countries and Exploring Mechanisms for Regional Cooperation* // Technology-Enabled Innovation for Democracy, Government and Governance. Springer Edition. – 2013. – P. 87–101.

7 Ramaswamy M. *E-government implementation in transition countries* // Handbook of Research on ICT-enabled Transformational Government: A Global Perspective. – 2009. – P. 441–451.

8 The legal information system of normative legal acts of the Republic of Kazakhstan, Adilet database, the Law of the Republic of Kazakhstan from March 5, 2019 No. 234-VI ZRK *"On ratification of the Agreement on cooperation of the States members of the Organization of the collective security Treaty in the field of information security"*, Available at: http://adilet.zan.kz/rus/docs/Z1900000234, [Accessed 2 March 2019].

9 Official website Joint Stock Company "Zerde", 2019 Available at: https://zerde.gov.kz/holding/history/, [Accessed 20 March 2019].

10 History of national information technologies Joint-Stock company», Available at: https://www.nitec.kz/index.php/pages/test, [Accessed 10 March 2019].

11 The legal information system of normative legal acts of the Republic of Kazakhstan, Adilet database *About formation the Commission at the President of the Republic of Kazakhstan concerning introduction of digitalization in the Republic of Kazakhstan*, the decree of the President of the Republic of Kazakhstan of January 10, 2018 № 621, Available at: http://adilet.zan.kz/rus/docs/U1800000621/info, [Accessed 10 March 2019].

12 The legal information system of normative legal acts of the Republic of Kazakhstan, Adilet database *About the approval of the Concept of cybersecurity ("cyber Shield of Kazakhstan")* the Resolution of the Government of the Republic of Kazakhstan of June 30, 2017 № 407, Available at: http://adilet.zan.kz/rus/docs/P1700000407, [Accessed 20 March 2019].

13 The legal information system of normative legal acts of the Republic of Kazakhstan, Adilet database *About the approval of the Plan of actions for implementation of the Concept of cybersecurity* ("cyber Shield of Kazakhstan") till 2022, the Order of the Government of the Republic of Kazakhstan of October 28, 2017 № 676, Available at: http://adilet.zan.kz/rus/docs/P1700000676, [Accessed 20 March 2019].

14 Some issues of the Ministry of defense and aerospace industry of the Republic of Kazakhstan, Resolution of the Government of the Republic of Kazakhstan dated November 15, 2016 № 704. Available at: http://adilet.zan.kz/rus/docs/P1600000704, [Accessed 23 March 2019].

15 Official website of RSE "State technical service" of the national security Committee of the Republic of Kazakhstan, General information, Available at: http://sts.kz/ru/organization , [Accessed 20 March 2019].

16 Official website of KZ-CERT Kazakhstan, *About team* KZ-CERT, Available at: http://kz-cert.kz/en/about, [Accessed 23 March 2019].

17 The legal information system of normative legal acts of the Republic of Kazakhstan, Adilet database, the Law of the Republic of Kazakhstan, About the Government of the Republic of Kazakhstan,the Decree of the President of the Republic of Kazakhstan of February 21, 2019 № 845, Available at: http://adilet.zan.kz/rus/docs/U1900000845, [Accessed 23 March 2019].

18 Official site of the President of the Republic of Kazakhstan, Decree of the President of the Republic of Kazakhstan of March 19, 2019. "On the execution of powers of the President of the Republic of Kazakhstan" 2019, Available at: http://www.akorda.kz/ru/legal_acts/decrees/ob-ispolnenii-polnomochii-prezidenta-respubliki-kazahstan, [Accessed 13 March 2019].

19 The legal information system of normative legal acts of the Republic of Kazakhstan, Adilet database *About measures for further improvement of system of public administration of the Republic of Kazakhstan*, Decree of the President of the Republic of Kazakhstan, may 6, 2016 № 253, Available at: http://adilet.zan.kz/rus/docs/U1600000253, [Accessed 22 March 2019].

20 Ministry of digital development, defense and aerospace industry of the Republic of Kazakhstan (Decree of the President of the Republic of Kazakhstan dated February 25, 2019 № 848 Available at: http://adilet.zan.kz/rus/docs/U1900000848) [Accessed 21 March 2019].

21 The legal information system of normative legal acts of the Republic of Kazakhstan, Adilet database, the Law of the Republic of Kazakhstan, "*The third modernization of Kazakhstan: global competitiveness"* – Available at: http://adilet.zan.kz/rus/docs/K1700002017 [Accessed 13 March 2019].

22 IMD World Digital Competitiveness Ranking, 2017, Available at: https://www.imd.org/globalassets/wcc/docs/release-2017/world_digital_competitiveness_yearbook_2017.pdf [Accessed 13 March 2019]..

23 Global Cybersecurity Index 2017, Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [Accessed 10 March 2019].

24 Official site of Singapore. *Building an inclusive digital society.* 6 March 2018. Available at: https://www.gov.sg/microsites/budget2018/press-room/news/content/building-an-inclusive-digital-society [Accessed 20 March 2019].

25 Gary Marchionini, Hanan Samet and Larry Brandt, *Digital government, Guest Editors*, COMMUNICATIONS OF THE ACM January 2003/Vol. 46, No. 1, стр. 25-27

26 Jing Zhanga, and Yushim Kimb, *Digital government and wicked problems: Solution or problem?*, Information Polity 21 (2016) 215–221 215 DOI 10.3233/IP-160395 IOS Press, Special Issue Editorial, pp. 215-221 Available at: https://content.iospress.com/download/information-polity/ip395?id=information-polity%2Fip395 [Accessed 24 March 2019].

27 Sehl Melloulia, Luis F. Luna-Reyesb and Jing Zhang, *Smart government, citizen participation and open data, Information Polity* 19 (2014) 1–4 1 DOI 10.3233/IP-140334 IOS Press, pp. 1-4, Available at: https://pdfs.semanticscholar.org/e2c5/8b04ebcb0c8e5a4d9f2627bb2d9e103b1183.pdf [Accessed 20 March 2019].

28 Official letter from the Ministry of education and science of the Republic of Kazakhstan №ФЛ-И-956/14-5-05 August 10, 2018. pages 1-3