Cyber Risk Management in Digital Environment: Case of Kazakhstani Bank

Galiya Mertai Kyzy Berdykulova

AbstractThe article is devoted to the cyber risks Kazakhstani banks are facing in the digital environment. Kazakhstani banks along with other business structures in the digital era and digital environment face the new type of risk caused by the 3rd and 4th Industrial Revolutions and named "cyber risk".Methodology of the research involves the study of key problems of Kazakhstan in cybersecurity area; types of cyber threats; indicators and results of Cyber Shield of Kazakhstan till 2020; the global position of Kazakhstan in cybersecurity as premises of risk management paradigm and its new methodology in order to find the ways of the modern management of cyber risks . The model of cyber risks management of Russian "Sberbank" is used to determine the level of risk in "Kaspi Bank".

Keywords Cyber risk; cyber threat; cyber security; cyber risk management; cyber risk assessment; Cyber Shield, Kazakhstan.

I. INTRODUCTION

The problem of cyber crime has been designated as one of global world problems. As experts note, the threats connected with information risks are as dangerous as threats of physical assets of the company. The incidents connected with data leakage, as a rule, cause chain reaction and significant reputation and financial damage. Business transformation of organizations towards creating the digital environment leads to growth of cyber threats and risks.The article is dedicated to experience and practice of commercial banks in cyber risks management in Kazakhstan; in particular in retail bank "Kaspi Bank" by usage of experience of the Russian "Sberbank". The model of cyber risk management is offered to "Kaspi Bank" on methodology of "Sberbank". The model is targeted on figure out the level of risks by procedures of objectives, assessment, and risks rating. As a result, the cyber risks for "Kaspi Bank" was determined. Besides efforst of bank it is reasonable to cover a cyber policy of Kazakhstani government "Cyber Shield" which includes precise indicators till 2022 in the field.

II. COMMERCIAL BANK OF KAZAKHSTAN IN DIGITAL ENVIRONMENT

Bank is the commercial organization which activity is functioning under the constant risks. Along with traditional financial and non-financial risks the new type of risk as a cyber risk has been occurred in digital environment. Cyber-risk is a risk connected with usage of computer equipment and program providing both in local and global Internet network; settlement and payment systems, systems of Internet trade, industrial control systems as well as a risk connected with accumulation, storage and usage of personal data.

Revised Manuscript Received on June 12, 2019.

Galiya Mertai Kyzy Berdykulova International IT University, 34a Manas street Almaty Kazakhstan

"Cyber risk" means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems [1]."Kaspi Bank" is Kazakhstani retail bank and ranks of third in terms of deposits from individuals, 6th in terms of equity capital among Kazakhstani banks on date of January 2017 [2]. The ecosystem of "Kaspi Bank" accounts for about 20% of the turnover of non-food products in the country on date of July 2017 [2]. According to business weekly rating Kapital.kz "Kaspi Bank" received "The Best Banks of Kazakhstan" award for the most thoughtful strategy during the crisis in 2014 [3], in 2016 - for the most client-oriented service [4]. Also in 2016 the bank became the winner of the IV Kazakhstan Prize "Ak Mergen" in the field of public relations in the nomination "The best project in the field of social communications and charity" [5].According to Digital Kazakhstan -2020 any economic entity has been transforming its activity and business processes. Kaspi Bank develops three unique online services on Kaspi.kz today: "Payments", "My Bank", "Shop". Kaspi.kz allows Kazakhstan citizens to pay bills for various services in one minute without commissions. "Kaspi Shop" shows high growth.Since launch of this service Kazakhstan citizens have bought more than 115 thousand goods. Only in May, 2016 more than 15 thousand purchases have been made. It is for 7 times more than in previous year. The website "Kaspi.kz"experiences the growing popularity at clients. Users of online services especially like payments without the commissions and favorable credit purchases to make quickly and in "Shop". Especially for "Shop" on the website "Kaspi.kz" the cheapest "Credit for purchases" is made [2]. Results of work of these online services are impressive. Kazakhstan citizens have made already more than 33 million payments without the commissions on the website "Kaspi.kz" and have saved more than 3 billion tenges of national currency. All services on the website "Kaspi.kz" is cheaper and more favorable, than usually. The most popular "Credit for purchases" there is in "Shop" on "Kaspi.kz" with an interest rate of 19,95% in comparison with 24, 95% for ordinary credit . "Kaspi Bank" plans to introduce new standardsof online services and new services already are implemented. There are new superconvenient services which are provided via website "Kaspi.kz" and more than 4000 "Kaspi-terminals" through the whole country. Within this year about 50 offices which don't allow providing services quickly, simply and conveniently are reformed and new standards of service have been implemented [6].Kazakhstan citizens have made already more than 33 million payments without the commissions on the website "Kaspi.kz" and have saved more than 3 billion tenges of the national currency as data of Figure 1 has shown. The

unprecedented growth of online payment increases the risks associated with new technologies. Among them technical failures in the

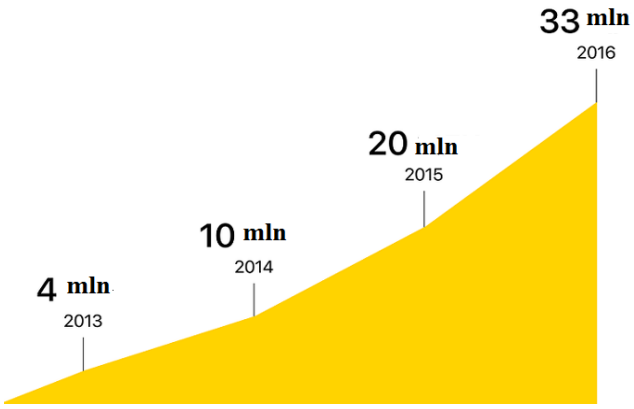

Figure 1.Dynamics of online payments on " Kaspi.kz"

software, fake mailing, fake accounts, fraud.At the end of 2018 Kazakhstani people, the clients of Kaspi bank complained that they had lost money from their accounts. In turn, as explained in the press service of Kaspi, this is due to a failure in the program, the money from the accounts did not disappear. Just a small software failure occurred. As a result, some clients' balances on Kaspi Gold accounts in Kaspi Gold are incorrectly displayed [7]. Since November 2018 in social networks, unknown people lured money from consumers using the brand Kaspi Bank. Kazakhs were offered to pass a survey, promising to pay for it up to 700 thousand tenges. The bank noted that fraudsters, as a rule, buy paid advertising from Instagram and Facebook from fake accounts.To protect customer money, the bank carried out the following actions:

- all suspicious transactions were blocked.
- each transaction was analyzed.
- all relevant information was provided to the competent authorities.
- information about these incidents was transmitted to the National Bank of Kazakhstan, MasterCard, and various cybercrime services and other services to identify individuals behind the organization of this survey [8].

III. CYBER RISK MANAGEMENT

3.1 Objectives of Cyber Risks Assessment

It is therefore "Kaspi Bank" should build cyber risk management on all stages of life cycle of bank processes to provide speed, convenience, and safety of business processes. During creation of assessment tools of cyber risks it is recommended to conduct the following objectives on the basis of the Russian Federation's "Sberbank" experience in cyber risk management. The model of cyber risk management includes five objectives, three steps of assessment, and risk level determination [9].

Table 1. Objectives of cyber risks assessment

Objective	Content
To construct model of assessment this will give an objective idea of the level of cyber risks.	The main objective of model introduction is not to spend resources for decrease insignificant risks but direct efforts for processing admissible level of risks.
To build simple and convenient process of assessment.	It is especially relevant for the experts in cyber security where processes of development and deployment are considerably accelerated, requirements to the final product can be changed every week, and there is no opportunity to allocate more than five minutes for assessment of risks.
To consider opinions of several experts from different areas.	For obtaining objective results possibility of attraction to risk assessment by experts for a different profile, including safety, business and IT have provided.
To create the universal model suitable for different activities.	Model uniformity in assessment of all identified cyber risks. At practical application such approach will allow to aggregate results of all estimates in the uniform cyber risk rating and comparison to find out a priority of risks.
To provide an opportunity to keep track of dynamics of risk level at change of internal or external factors	Levels of risks are changed simultaneously with transformation of threats, conditions of protection and business growth. For understanding dynamics of risk levels changing it is planned to estimate influence of the decisions on risk and study regularities of communication between changes of risk size and recorded actual damage.

3.2Cyber Risk Assessment

Assessment of cyber risk occurs for three steps**.**

Step 1. Formation of the system risk factors. The experts define a list of relevant threats, vulnerabilities and measures of protection for each type of cyber risk.

Step 2. Assessment of risk factors by experts. Independently of each other experts estimate each risk factor as a four-level scale (fig. 2 and 3). Criteria of criticality are developed taking into account of business scales of "Kaspi Bank".

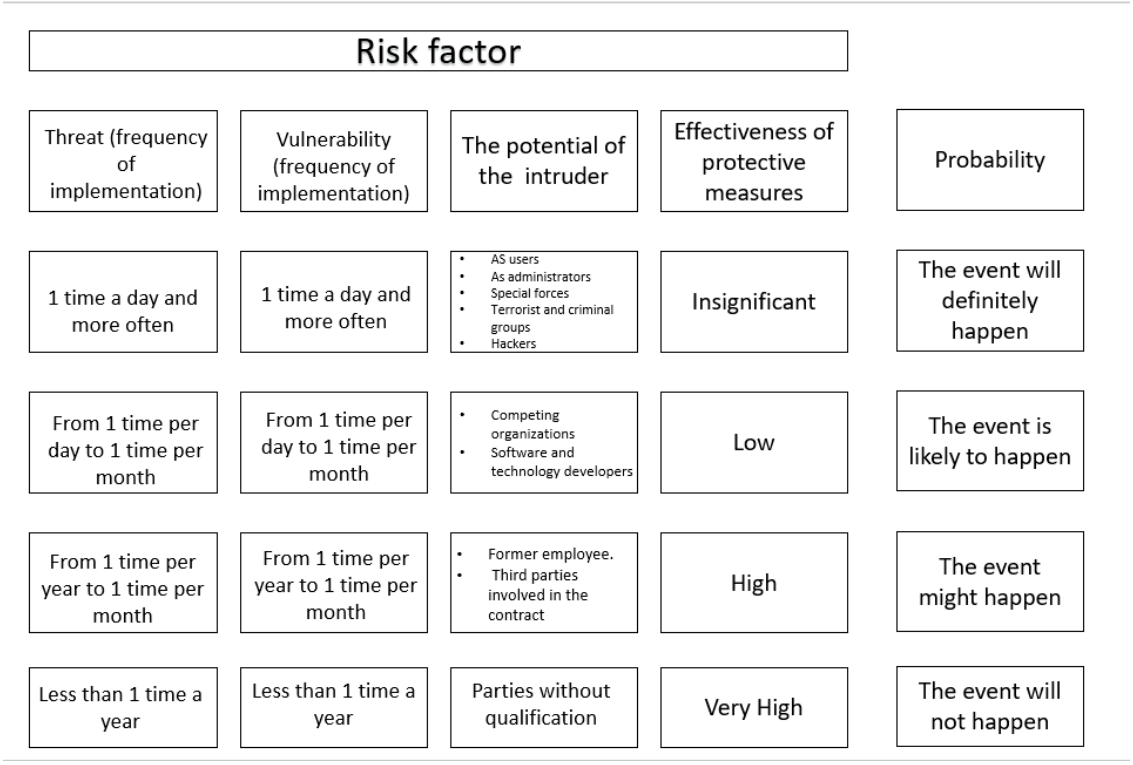

Figure 2. A four-level scale of threat risk estimation

At the same stage the weight of every risk factor is defined to reduce influence on total risk factors, noncritical for it. Example: for risk of information leakage damage assessment from violation of processes can be not considered, and the "category of information" parameter acts as decisive, and his weight has to be increased. The weight of factors is estimated on a scale from one to nine.

Step 3. Calculation of cyber risk rating. The key difference of the model from existing qualitative methods is in opportunity to unite a large amount of received opinions and scales in one value of risk rating. Whereas the classical tabular method doesn't allow to operate with a such amount of experts opinions. For calculation of total risk rating it is recommended to use the matrix method of calculations which aggregate all qualitatively estimated factors in one quantitative value for "Kaspi Bank". It allows considering the experts participating and dispersion of their opinions as well as differencing in scales that increases assessment objectivity.

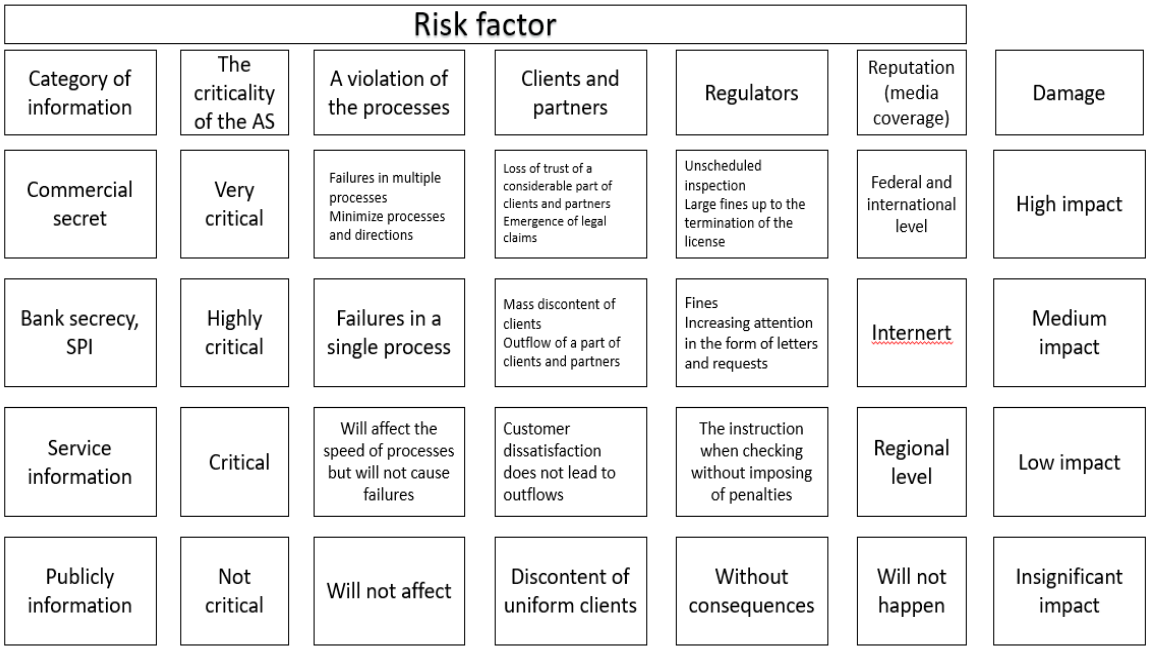

Figure 3. A four-level scale of information risk estimation

3.3.Cyber Shield of Kazakhstan:Concept and Practice

At the World Economic Forum in Davos the problem of cyber crime has been designated as one of global world problems.As experts note, the threats connected with information risks are as dangerous as threats to physical assets of the company. The incidents connected with data leakage, as a rule, cause chain reaction and cause significant reputation and financial damage.Business transformation of organizations toward creating the digital environment causes a growth of cyber threats and risks. According to Allianz research cyber threats have increased from 1% in 2011 to 28% in 2016 [10].

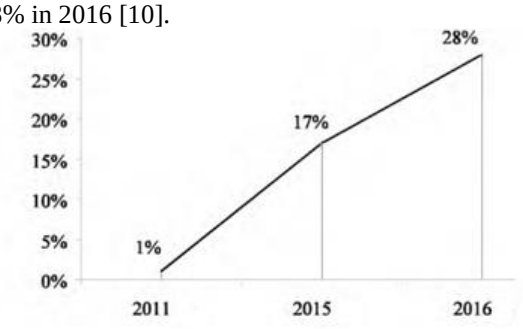

Figure 6. Cyber threats in the world, 2011-2016

Quite often the companies realize the risk connected with illegal access to data, but have no sufficient resources for effective response to actions of criminals. In this case the system of insurance of cyber-risks becomes a powerful barrier on the way of cyber crime.Cyber crime is not a just fashionable word; it is reality of the market. The industry of world cyber crime develops with great strides and in the field of the financial organizations crime is even quicker. Now the main risk of the financial sphere is cyber risk [11].Recently Kazakhstani banks have undergone large-scale cyber attack. The Committee of National Security has risen in their defense, thereby having given gravity of a situation in the opinion of ordinary Kazakhstani citizens but at the same time without having explained what has occurred and what it as a result has turned back for banks which names, by the way, were also not called. Now a hacker bank attack is the international problem, and Kazakhstan is in trend. For the last 10 years yesterday's students who for the sake of an entertainment developed earlier viruses and malicious applications have turned into commercial activity in recent years. Initially they specialized only in stealing from ordinary citizens, then cybercriminals have switched to the companies which are served in bank — there are more sums, the latest trend now is the target attacks on corresponding accounts of banks. Appetites as well as technical capabilities of hackers all the time have been growing.According to research conducted by Kaspersky Lab and B2B International in 2014, DDoS attacks to Internet resources of the company can lead to substantial damages – on average from 52 to 444 thousand dollars depending on size of the enterprise. Such contingencies for many the organizations are serious encumbrance. Attacks of hackers also can do harm to reputation of the enterprise because of a long absence of access to its online resources and pour out in additional even more serious financial losses[12].

Key problems of Kazakhstan in cyber security [13]:

1. In the Republic of Kazakhstan from 2010 for 2016 density of Internet users has increased from 36,1% to 75%, and the number of users of the mobile Internet from 3 million 694 thousand has practically trebled and has reached 10 million 567 thousand. Such exponential increase in number of Internet users increases criticality and does by more notable consequences in case of refusals or harmful impact on technical means.
2. Insufficient awareness in methods of information security and low supply in information security systems of the enterprises of small and medium business including occupied in the sphere of rendering information and communication services which often can't even estimate a condition of the belonging information and communication infrastructure result in a large number of not analyzed events and incidents of information security complicating both prevention of technological vulnerabilities, and fight against the criminals using ICT as means for commission it is broken.
3. The domestic sector of IT industry doesn't make an essential practical contribution to the program of diversification of national economy (less than 5 percent of products from used in public sector have the Kazakhstan origin), and the culture of cyber security, including production culture in the sphere of development and use of products, not always is defining.
4. The measures connected with automation of the state functions and rendering public services in an electronic form and also the continuing digitalization of access to information on activity of public authorities bear in themselves certain risks. The low-quality services and applications provided to citizens and the private organizations within "the electronic government" including machine-readable open data, can lead to violation of the rights and legitimate interests of citizens.
5. The transnational and cross-border character of many products of ICT and the international coherence of networks of public telecommunications are used by crime for commission of illegal acts concerning users and operators of ICT services and owners of the Internet resources placed in a national segment and also the information systems interacting with the Internet.
6. The militarization of the sphere of ICT, difficulty forced by the certain countries in proof of participation of the states in use of ICT in defiance of the principles of international law, caused substantially by spontaneously developed character of the existing international control system of the Internet, the remaining digital divide between the countries interferes with formation in the world community of reliable international legal instruments of prevention of military use of achievements in the sphere of informatization and telecommunications.
7. The existing Kazakhstan model of school, specialized secondary, higher and postgraduate education in the field of ICT, including specialization in the sphere of information security, demands the constant and careful analysis from all interested persons (including the Ministry of Education and Science of the Republic of Kazakhstan, higher educational institutions and potential employers) regarding compliance to modern requirements of society and to tendencies of ensuring safe development of information

technologies in a type of dynamic development of this area.Thus, Kazakhstan in the sphere of cyber security experiences such serious threats as:

- low legal literacy of the population, workers of the sphere of ICT and heads of the organizations for information security;
- violation of informatization by the state and non-state actors and users of services in the sphere of ICT of the established requirements, technical standards and regulations of collecting, processing, storage and information transfer in an electronic form;
- the inadvertent human errors and technological failures making negative impact on information systems, the software and other elements of information and communication infrastructure;
- actions of the international criminal groups, communities and individuals for implementation of plunders in the financial and bank sphere, harmful influence for violation of operation of automated process control systems of the industry, power, communication and in the sphere of information and communication services;
- the activity of political, economic, terrorist structures, intelligence and special services of the foreign states directed against the interests of the Republic of Kazakhstan by rendering prospecting and blasting impact on information and communication infrastructure.

Concept of the cyber security "Cyber Shield Kazakhstan" was issued in 2017. Purpose of the Concept is achievement and maintenance of security level of electronic information resources, information systems, information and communication infrastructure from external and internal threats providing sustainable development of the Republic of Kazakhstan under the conditions of global competitiveness [13].

Table 2. The expected results of Cyber Shield of Kazakhstan in 2017-2022

Indicator	2018	2019	2020	2021	2022
The global index of cyber security	0,300	0,400	0,500	0,550	0,600
Increase in awareness on threats of information security, %		5	10	15	20
The number of the trained experts in the sphere of information security	300	500	600	700	800
Increase in a share of the domestic software products in the sphere of ICT used in the state and quasi-public sectors, %	10	20	30	40	50
Share of use of domestic certificates of safety at encoded data transmission by Internet resources with the domain. KZ and. • AZ, %	20	40	60	80	100
Share of use of domestic certificates of safety at encoded data transmission by Internet resources with the domain. KZ and. • AZ, %	20	40	60	80	100

At the same time Kazakhstan has taken the 83rd place in rating by determination of cyber security level. In total in the Global index of cyber security 193 countries were considered.The updated Global index of cyber security has made 2017 the International Telecommunication Union. The rating represents poll based on five key indicators: legislative base, specifications, organizational issues, improvement of quality and cooperation. Based on them, the International Telecommunication Union makes the list on the level of commitment of the states to questions of ensuring cyber security. The republic has got 0.352 points and has improved the positions in comparison with the previous rating for 2014 (0.177 points).Among the states of the Eurasian Economic Union (EEU) of a position were distributed as follow:

- Russia – the 10th (0.788 points);
- Belarus – the 39th (0.592);
- Kazakhstan – the 83rd (0.352);
- Kyrgyzstan – the 97th (0.27);
- Armenia – the 111th (0.196) place.

In TOP-5 Singapore, the USA, Malaysia, Oman and Estonia have entered. The Central African Republic, Yemen and the Republic of Equatorial Guinea close rating [14].

IV. CONCLUSION

1. As the results of the study the following factors have been revealed:

- the problem of cybercrime is one of the global world problems.
- the threats connected with information risks are as dangerous as threats of physical assets of the company.
- data leakage cause chain reaction for reputation and financial damage to the economic activity.
- business transformation of organizations in the digital environment leads to the growth of cyber threats and risks.

2. Kazakhstan citizens have made already more than 33 million payments

without the commissions on the website “Kaspi.kz” and have saved more than 3 billion tenges of national currency. The unprecedented growth of online payment in Kazakhstan increases the risks associated with new technologies. Among them technical failures in the software, fake mailing, fake accounts, fraud.

3. Management of cyber risks is based on a methodology which identifies objectives and steps of cyber risks assessment according to the Russian Federation’s “Sberbank” practice.
4. Calculation of cyber risk rating is based on the formation of the system risk factors and assessment of risk factors by experts.
5. Key problems of Kazakhstan in cybersecurity derive from exponential increase in number of Internet and mobile users, Insufficient awareness in methods of information security and low supply in information security systems of the enterprises, the low-quality services and applications provided to citizens and the private organizations within "the electronic government", and violation of the rights and legitimate interests of citizens.
6. The transnational and cross-border character of many products of ICT and the international coherence of networks of public telecommunications.
7. Concept of the cybersecurity "Cyber Shield Kazakhstan" was issued in 2017 with the purpose of the Concept is achievement and maintenance of security level of electronic information resources, information systems, information and communication infrastructure from external and internal threats providing sustainable development of the Republic of Kazakhstan under the conditions of global competitiveness

V. ACKNOWLEDGMENTS

My thanks to my family for allowing me to study problems, experience and practice of cyber risks in our country and abroad, propose of cyber risk management development for commercial bank.

REFERENCES

1. *Cyber risk and risk management*. (2018).Institute of Risk Management. https://www.theirm.org
2. *Svedenia o finansovyh pokazatelyah*.(2017). Finansovye pokazateli bankov vtorogo urovnya po sostoyaniyu na 01.01.2017. http://stat.gov.kz/faces/homePage
3. Luchshie banki Kazahstana (2014).. Kapital 24.12.2014. https://kapital.kz/
4. Luchshie banki Kazahstana (2016).. Kapital 24.12.2016. https://kapital.kz/
5. Pobediteli premii “Ak Mergen” (2015) Dixinews. 26.02.2016. http://dixinews.kz/articles/zhizn/2
6. *Klienty Kaspi Bank vybirayut online servisy*. (2016). https://forbes.kz/finances/finance/klientyi_kaspi_bank_vyibirayut_onlayn-servisyi/
7. V Kaspi.kz obyasnili propazhu millionov/ Tengri News. (.2018). https://tengrinews.kz/money/v-Kaspikz-obyyasnili-propaju-deneg-so-schetov-klientov-359670/
8. Kaspi Bank o moshenichestve v Internete/ Inform Buro (2019).
9. N.Simachevskaya. *Kak sberech milliony: model otsenki kiberriskov*. (2017). https://bosfera.ru/bo/kak-sberech-million-model-ocenki-kiberriskov
10. *Allianz Risk Barometer* (2016). Reports. http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2016/
11. Katerina Klemenkova. *Kiberataki na kazahstanskie banki.(*2017). https://ru.sputniknews.kz/economy/2017
12. Kremer. *Kiber riski –eto serezno. (2016).*https://www.aig.ru/content/dam/aig/emea/russia/documents/brochures/sst-aig-or-5-brochure.pdf
13. Ob utverzhdenii Kontseptsii kiberbezopasnisti (“Kibershit Kazakhstan”). Postanovlenie Pravitelstva Respubliki Kazakhstan ot 30 iyunya 2017 goda № 407. https://zakon.uchet.kz/rus/docs/P1700000407
14. Global Cybersecurity Index (GCI) .(2017). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf