ИНСТИТУТ ЗА ИКОНОМИЧЕСКИ ИЗСЛЕДВАНИЯ НА БЪЛГАРСКАТА АКАДЕМИЯ НА НАУКИТЕ
ИКОНОМИЧЕСКИ ИЗСЛЕДВАНИЯ
ECONOMIC STUDIES

Volume 27 (5), 2018

Elena Shustova[1]
Vesselin Blagoev[2]

RISK MANAGEMENT IN THE INTERNET BANKING
The Case of Kazakhstan

The risk management in the banking sector has always been of primary concern, especially after the cases of mismanagement, which lead to big losses, and even closing down banks. For obvious reason, in the case of internet banking the risk management (RM) issues become much more complicated. This study focuses on the specifics of RM in the case of Kazakhstani banks, using as an example the policy of one of the leading banks in this area – BankCentrCredit. Kazakhstan has all the characteristics of a country which has to develop intensively the internet banking – large territory, low density of the population and as a result – very expensive coverage with bank services with the traditional methods – bank offices. We especially address the specifics of risks in case of providing digital financial services, based on artificial intelligence solutions and related robotized systems.

JEL: M15; G21; L86

1. Introduction

The risk management in the case of internet banking has some special dimensions and characteristics, compared to those in the traditional banking. First of all, it is developed on totally new technological platforms – internet and artificial intelligence, to mention a few. It goes along with transformational changes in the business and society, inspired by the technological revolution, e.g. the implementation of artificial intelligence, and chatbots as substitutes of human employees. Along with these, the provision of banking services is changing in revolutionary ways. According to Scott Vincent (2016) "there is a new central issue to focus attention on: technology and the digital world". Portilla, Vazquez, Harreis et all. (2017) argue about major trends in banking as a result of the digitalization. Although the digitalization of the banking services, and in general – the internet banking, is a mainstream trend, it is still in the emerging stage of development, in particular in

[1] *Elena Shustova, Assoc. Professor, PhD, Kazakh Humanitarian Law Innovative University, Republic of Kazakhstan, shustova_yelena@mail.ru.*

[2] *Vesselin Blagoev, Professor, PhD, Varna University of Management, Bulgaria, tel.+359-421-9595, blagoev@vum.bg.*

Kazakhstan. Obviously, all these changes – new products, new services, new agents, new barriers to entry, affect both the banks' employees, organisation, risk management, as well as the clients. In the conditions of Kazakhstan – large territory, low density and high dispersal of the population, as well as low internet penetration, the implementation of internet banking is much wanted, although probably more difficult, and riskier. It is clear that under all mentioned circumstances, the risk goes "far beyond the operational and technical risks" (Denyes & Lonie, 2016). However, the internet banking is an inevitable development, and therefore the new risk management issues have to be studied with the aim to support the process.

Internet banking defined

There are many definitions of internet banking, e.g. Mock & Zaha (2017), Khrais (2017), Portilla, Vazquez, Harreis et all. (2017), Aaron, Armstrong & Zelmer (2008). Most of them interpret it as offering financial transaction services using IT in the Internet environment. Other authors define internet banking as distance service that covers the traditional banking services (Goh, Yeo, Lim & Tan, 2016), which is about the same, expressed in different wording. Mukhtar (2015) argues that internet development in the end of 80s laid the beginning of the new era of online banking services.

International Finance Corporation (The World Bank Group) is using another term - digital financial services (Denyes & Lonie, 2016). It stresses more on the digital form, rather than on the communication environment or channels. Whatever definition used, the authors, e.g. Salihu & Metin (2017), as well as the previously mentioned authors, argue that internet banking is capable of improving the quality of services and the satisfaction of customers from the fast and secured banking services they get.

For our purposes in this paper we define internet banking as: ***providing digital financial services by the banking system using Internet-based platforms***. Based on that we define and analyse further the types of risk in the case of Kazakhstan. Of course, they cannot be substantially different from those in any other country.

2. Risk Management

The risk management in the banking sector is defined and analysed in hundreds of academic papers, e.g. Vincent (2016), Mock & Zaha (2017), Denyes & Lonie (2016), Harle et all. (2016), Aaron, Armstrong & Zelmer (2008), Pyle (1997), Portilla et all. (2017), Shustova (2018) to mention a few. Of course, they analyse the problem in the scope of the classical banking system, as this is what we had as common practice until recently. In this paper we'll analyse the risk management issue from the point of view of the internet banking/digital financial services. This imposes a critical analysis of what the classical risk management includes, but in the new technological environment. The academic literature shows different approaches in studying such not well-known problems, in which the relatively good understanding of the influence and interconnection of the factors and main actors in the system becomes insufficient because of the changes in the environment. As we discuss internet-bank risk management issues, where the problems may lie in any of those – the personnel, the system, the technological environment, and in the combination of all those, we decided to accept Grint's approach of analysis (Grint, 1997, p.162), which coincides well with Basel II. We will apply a structural approach, and action/operational approach, of course using all classical instruments of assessing the bank risks.

2.1 Structural (regulatory) approach

The structural approach presumes that the risk-management problem in the internet-banking will be analysed based on the structures/regulations in the banking sector, and in the bank itself, as they guide and stimulate the bank employees into certain risk-free behaviours. Obviously, this is based on the relevant regulations, including Basel II and Basel III, the laws on banking by countries, and even ISO31000 standards for Enterprise Risk Management, which are used to establish principles of risk management in the case of digital financial services (Denyes & Lonie, 2016). The most interesting within the structural approach, with regard to Kazakhstan, include the regulations, management of the strategic risks, and the assessment of value loss.

2.1.1 The regulatory approaches

The regulatory approaches are based on Basel II and Basel III, as well as on the country regulations. As far as they are implemented in every country in a pretty similar, if not identical, way, we shall not go into details, but will rather underline the most important. Basel II concentrates on the so-called three pillars: minimal capital requirements, supervisory review and market discipline.

In regard to the first pillar: required capital, Basel II suggests a few ways for estimating the required capital to cover credit risks (Aaron, Armstrong & Zelmer, 2008, p.42; Stanisic & Stanoevic, 2009, p.8; Zupanovic, 2013, p.86). For example, for measuring the credit risk the banks can select and apply between Foundation (internal-ratings-based) approach (IRB), advanced IRB approach and of course – the well-known standardised approach (rate weights fixed by independent internationally recognised credit assessment institutions). In the case of applying Foundation IRB and advanced IRB approaches, the banks set themselves, and use their own risk assessment models, including for the probability of default, loss-given-default (LGD), exposure at defaults and maturity for each exposure (Aaron, Armstrong & Zelmer, 2008, p.42). In case of applying foundation IRB, the probability of default (PD) must be assessed by the bank itself, while the other risk factors are provided by the supervising authority. In the case of applying Advanced IRB, for every exposure, the bank must estimate PD, LGD, and maturity. In line with Basel II Central bank of Kazakhstan, and Kazakhstani government have a clear policy for stimulating the consolidation in the banking sector (Shustova & Blagoev, 2018). For example, Central bank of Kazakhstan is controlling tightly the minimum bank capital as a risk management precaution and guarantee, and as a pressure to the banks to adopt new better risk management techniques. We presume that there is nothing specific about this pillar in regard to the risk management in the internet banking, as the regulations, if followed up strictly, should guarantee risk-free levels of liquidity, to mention the most important.

2.1.2 Management of the strategic risks

Anna Mok and Ronnie Saha (2017) of Deloitte US have published a very comprehensive paper on the strategic risk management in banking. They argue, that the strategic risks are "the most damaging risks" the organisations faced in the last decade which follows up on Harvard Business Review (2015) article, presenting the results of CEB research of the market capitalization decline in the previous decade. The analysis did show that "86 percent of the significant market capitalization decline were caused by strategic risks", while only 9 percent were caused by operational risks and 3 percent by legal and compliance risks. The analysis covers the real sector as well, but considering the share of the financial sector in the overall market capitalization, the numbers for the banks are probably pretty similar. If in the cases of Enron and WorldCom the problems were about huge accounting fraud, after the changes in legislation the main cause has changed to the decision making. A well-known example of questionable decision-making is the development of Deutsche Bank's total derivative exposure, which was USD 75 Trillion in 2013, reduced to USD 46 Trillion at the end of 2016 (Durden, 2016), and about USD 22 Trillion at the end of 2017 (Deutsche Bank, 2017). It is clear that there was, and probably is, a real risk issue that needs to be addressed. In its official Credit Overview Deutsche Bank (2018, p.8) reports USD 337 Billion as credit risk only (IFRS balance sheet derivatives trading assets as the present value of future cash flows owed to DB and as a result represent the credit risk to the Bank) which is an excellent development by March 2018. Still the question remains how could such an enormous and obviously unacceptable credit risk in 2013-2016 be formed? Most probably the huge derivative exposure was formed following strictly Basel II First pillar, but along with undertaking unacceptable strategic risk which should have been assessed by the supervisory levels (Basel II – Second pillar). But they were not.

As a result of all those cases, many banks reconsider the responsibilities of the chief risk officer and chief strategy officer, as it is clear now that they cannot perform their duties in separate independent processes. The finance institutions react differently in terms of the names of the new structures, still in one direction. Strategic risk working groups and centres of excellence are formed to coordinate the decisions of the strategic units with those in risk management.

An important change nowadays is the reduction of the influence of the mathematical modelling in the decision-making process. In our view, this is caused mainly by the market volatility of both financial and industrial markets. The low level of predictability makes the modelling less reliable instrument for making strategic decisions and assessing the risks. Thus, the formal logic would suggest, that in the foreseeable future we could expect the AI and modelling to play a less significant role in the strategic decision making, and therefore in the risk management at that level. However, the very strong orientation to digitalize, and to implement AI solutions in every process in the banking sector, may produce, and probably will lead to exactly the opposite scenario with all the risks related to such development.

2.1.3 Action/Operational Approach

Basel II suggests three methods for measuring the operational risk: Basic Indicator approach (BIA), Standardized Approach (SA), and Advanced Measurement Approach (AMA). Again, it is at banks' discretion to decide which of those approaches to use. For example, most of the banks in Canada apply Standardised approach for assessing the operational risk, while most of them apply Advanced IRB approach for the credit risk assessment (Aaron, Armstrong & Zelmer, 2008). What is most important here is to minimize the operational risks with long-lasting effects. There are many different ways to describe the ways through which the operational risk could be formed. For example, McKinsey/Institute of International Finance description of digitalization as a ground to analyse the possible risks (Portilla et al, 2017) includes as following: Data management; Process and workflow automation; Advanced analytics and decision automation; Cohesive, timely and flexible infrastructure; Smart visualization and interfaces; External ecosystem; Talent and culture.

The effect of the new technology (FinTech), including different IT platforms, on the bank risk could be illustrated enough well by the first element – Data management. According to Portilla et al (2017) it includes "overall data governance, data quality, consistency processes, and operating models to enable capturing and use of vast amounts of data—both structured (such as transactions) and unstructured (emails and text messages, social-media posts, photographs, and so on)". In the classical banking there is a human control at each one of the steps/elements, and at any instant of time. In the digital financial services most of the times the data processing and decision making are done using artificial intelligence (AI). In a large financial structure, such as a big bank, the effect of a wrong decision, or a wrong policy, will be seen at much later stage of the process because the AI system will not be set to (formally "instructed") to analyse the possible decision as good-or-wrong. Instead, the algorithm will give a GO if the set of parameters, that are defined in the AI system, is considered right or at least acceptable. Obviously, the dependence on technical and AI reliability and self-control at each one of elements of the decision-making, imposes additional requirements to the risk assessment and risk-management. The advanced statistical techniques and algorithms, as elements of the artificial intelligence (including machine learning, cognitive agents, and robots) is supposed to help managers to forecast the possible developments, assess the possible outcomes, and based on that make better decisions in terms of risk minimization. We have to understand also that these are done under the influence of the external ecosystem in which the bank operates. Knowing how volatile and unpredictable the financial and business developments might be, the idea to delegate substantial part of the decision making to AI seems to be quite frightening. To the possible problems with wrong AI-based decision making we have to add the possible fraud. For example, Michael Soppitt (2016, p. 10) argues that "the growth of the digital ecosystem will continue to work in favour of the fraudster. Social media and an exponentially growing volume of data, creates rich pools of information for criminals to utilise." According to BBC "the cost of social engineering fraud has already doubled to $1bn as a result of the digital transformation" (Soppitt, 2016, p. 11), and the number may have gone higher in 2017-2018. On the other side, the possible biases and their drivers in the digital environment are known, and it is possible to develop risk control software which makes consumer bias monitoring enough effective to help the management and supervisors, and thus mitigate or even eliminate possible risks for the bank. Different instruments are used to assess the credit risk. For example, Donovan et al. (2018) use credit default swaps (CDS) spreads for companies which are trading them and find them good to measure credit risk as indicated by future credit events (e.g., bankruptcy, credit rating downgrades, interest spreads). It has to be discussed if the classical methods, based on the intuition of the bank officers, could, and should be changed to AI (machine-learning methods), that develop a response-model based on the available statistics. The obvious answer is that in the foreseeable future the intuition-based assessment has to be used, still supported with the results from the AI tools.

2.1.4 Assessment of value loss

The main causes for value loss (Pyle, 1997, p. 3) include the following:

- *Market risk* – the change in the net asset value because of changes in the environment, e.g. interest rates, exchange rates, commodity prices, etc.
- *Credit risk* - change in the net asset value if some counterparties cannot meet their contractual obligations
- *Operational risk* – additional costs, for example, due to failure to meet regulatory requirements
- *Performance risk* and *Automated compliance* – We put these two together, as performance risk in classic banking is about losses caused by poor control of the employees, etc., as well as the "model risk", and automated compliance is about the interaction between the human factor and the AI.

Not going into many details, the market risk is measured using either stress testing, or value-at-risk (VaR) analysis. The stress testing is based on scenario that presumes that a very difficult market situation will occur again, and the bank has to prove good results. VaR analysis uses return distributions and predicted return parameters, that should not exceed certain percent at a time. The operational risk was discussed above.

As we mentioned above, the performance risk will need a special attention, as the internet-banking is based on intensive use of AI at the operational level. Presuming that in the future the AI will be given some managerial functions, this will impose problems both to the model risk, and to the human-AI interaction in the process of internet-banking. At this level we cannot discuss this issue in specifics.

2.1.5 Automated compliance

Härle et al. (2016, p. 8) argue, that "banks will likely have no choice but to eliminate human interventions as much as possible in risk's dealings with customers". Having in mind the progress in the AI even at these early stages of digitalization of the banking services, this statement sounds realistic in the long run. Such changes seem to be the main avenue of development, and the banking sector, including in Kazakhstan, already goes into that.

However, we think that such changes might impose some possible additional risks if AI-based methods would fully substitute the human involvement. The additional risks would probably stem from the limitations in the modelling, which will form/empower the AI "brain". We can model fairly well the standard banking problems and decision making, but we can hardly model the new types of problems, which the banks are facing now, and will face in the future, e.g. with the derivatives, cryptocurrencies, etc., to mention a few possible causes.

From another perspective, the risk of internet banking could be classified as following (Shustova, 2018b): Depending on the level of banking; Who causes the risk; Level of possible consequences; Depending on the time of appearance.

This classification could be used to predict possible causes of risks and plan activities to eliminate, or at least minimize them. There is one very important additional consideration – the specifics of the national banking systems. Most of them, if not all, are following the international rules and regulations, and develop using the best practices of the other countries in risk management minimization. The analysis of the specifics of such regulations and national practices in particular countries can help add knowledge and get workable ideas for more effective risk management.

3. Risk management in the case of internet banking in Kazakhstan

The development of the internet banking in Kazakhstan is characterised with some problems, which could be classified in two groups as following (Shustova, 2018a): organisational/technical, and economic problems.

The organisational and technical problems include:

- Guaranteeing the security of the e-banking services.
- Sophisticated systems of bank interfaces used by some commercial banks, which makes too complicated the communication of the clients with the bank.
- Outsourcing of some IT functions related to the security controls, which gives access of those non-bank employees to confidential information about the clients and their operations.
- Technical problems of the equipment – at the bank or at the internet provider.

The National bank of Kazakhstan (2016) has regulations according to which in 10 days from the decision to start internet banking the commercial bank has to submit to the National bank a statement that it has internal regulations and procedures for the security of the internet banking system, and specifically – that it guarantees that unauthorised access to the system is not possible. However, it should be noted, that many customers have limited knowledge/literacy of using IT services and devices, and when they face problems they are ready to accept help from authorised or even unauthorised specialists, and ordinary people. In the big banks these would be the IT specialists, while in the SMO who want to use internet banking – those might be specialists from companies to which they are outsourcing their IT services, or even other unauthorised personnel. In such cases, the main threat is that these external specialists are given the login and password, and they can copy them and use them for unauthorised access to clients' database.

Another problem arises because of massive use of external accountants who serve 3-5, or even 20 SME, when problems with the software lead to upgrading elements of, or even the whole system. In most cases, they use external specialists, which of course could lead to security problems.

The commercial banks design their own handbooks with instructions on how to use internet banking. For example, BankCenterCredit has uploaded in its website detailed instructions how to get in and use Star Banking system for individual customers (BankCenterCredit, n.d.). It includes:

- how to login in Star Banking;
- guide to work in the Star Banking system;
- log in to the mobile application Star Banking with a PIN code or thumb mark;
- registration in Star Banking system with the authorisation of National Authentication Center;
- blocking/unblocking the card in Star Banking system;
- opening a deposit account;
- working with e-invoices and emailing them;
- setting limits to the bank cards;
- transfer of money using Star Banking.

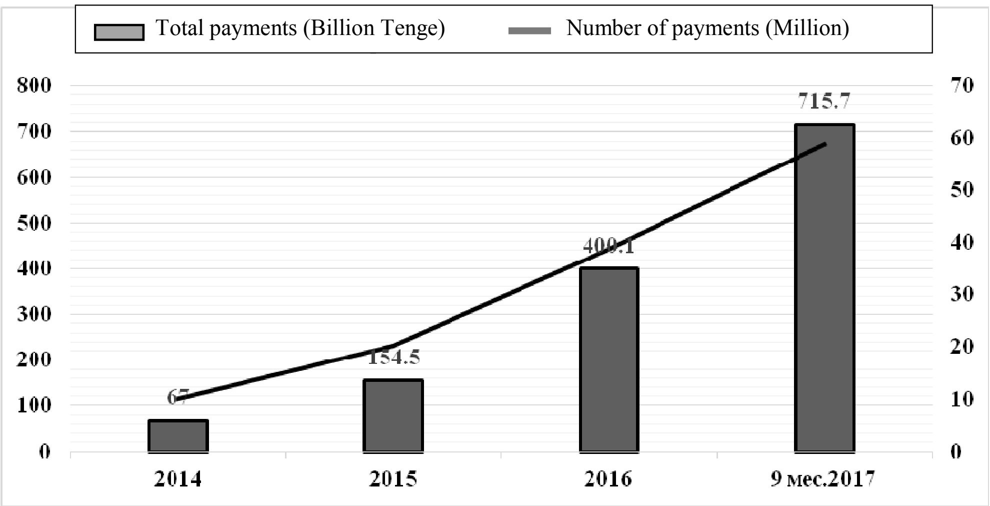
All these above make possible for every potential user of Star Banking to log in and get the desired services.

Similar instructions are available for the institutional clients. BankCenterCredit, in collaboration with InfoSoftPro has developed the so-called DirectBank technology, which makes it possible to speed up the transfer of documents between the organisations as clients, and the Internet banking system of BankCenterCredit. The important thing is, that DirectBank technology has the elements of the internet banking security to guarantee the bank services at the desired minimal level of risks.

The example of BankCenterCredit illustrates the development of the internet banking environment in the country. Practically all commercial banks, under the direct control of the National bank, have developed similar systems, which made possible a significant increase of the electronic banking services in the period 2014-2017. In this period the internet-based transfer of payments, including mobile banking, reached 38.7% of all transfers, and 36.4%

of the total amount of payments by bank cards. These results are really impressive when we consider that the number of payments with bank cards in 2017 has increased about 10 times compared to those in 2014 (Fig. 1)

Figure 1
Total amount of payments (Billion Tenge) and number of payments in the internet (Million), including mobile banking, in Kazakhstan in 2014-2017



Source: National Bank of Kazakhstan (2018).

The data of BankCenterCredit for December 2017 show that there have been 524 518 payments through internet banking system, out of total of 633 749 payments. This accounts for 83% of all payments. It is clear that the risk control system has to be really effective to guarantee the problems free banking environment, as well as fast services. The results of the other Kazakh banks are pretty similar in terms of the share of the internet banking payments, which shows a very optimistic picture for the country as a whole.

4. Conclusions

Based on the analysis of the risk management in the case of internet banking, done by different researchers, and our analysis we presume that it has some special dimensions and characteristics, compared to those in the traditional banking. We define internet banking as providing digital financial services by the banking system using internet-based platforms. From the definition it stems that the specific risk factors will be related to a very high extent to the technical issues, specific to the internet system. However, we did not limit our discussion to those factors only. Il line with Basel II we discussed the structural approach, and action/operational approach, of course, using all classical instruments of assessing the bank risks.

Further we studied the situation in the internet banking in Kazakhstan with a focus on the development and the results of one of the biggest banks in that country – BankCenterCredit. Its results in terms of amount (Billions of Tenge) of total e-payments in December 2017, as well as the number of operations, show that under the strict control of the National bank of Kazakhstan, the commercial banks, on the example of BCC, have developed a very reliable internet banking system. This applies to both internal banking systems and the inter-bank operations/transfers.

On the basis of that analysis we would suggest the following to be considered in the development of the internet banking systems in Kazakhstan and elsewhere (Shustova, 2018a):

1. Commercial banks have to guarantee the functioning of the IT system of the bank, without breakouts. They have to develop and apply technological procedures for eliminating losses and other negative consequences from fraud and unauthorised login in the system. The banks have to upgrade its software and technical support to serve their clients, including those who use internet banking, in the best possible way.
2. Special departments/teams have to be established within the bank's structure to provide electronic banking services. Authorised bank employees have to carry on regular monitoring of the risk payments and to the extent possible – analyse the risky logins, including multiple use of wrong passwords, log in from unexpected locations, etc.
3. Simplifying bank interface to make it easier for the clients, improving the work of the call-centres and departments for technical maintenance.
4. In addition – the accountants who serve individual clients and little SME have to be informed about the risks in cases of using external IT specialists to settle the internet banking, which requires sharing passwords, etc. The accountants have to login personally instead of sharing the login codes.
5. Additional information has to be provided in the website, including special instructions on how to get into the internet banking system and how to use it – both for the existing and new clients.
6. Enlarging the mobile banking coverage through additional POS-terminals with options for mobile payments. All these with the aim to increase the speed of the provided banking services to both – services, businesses and individual clients.

The main principle, which all banks have to follow, is that the provided electronic banking services should not have any negative impact on the quality of the bank operations and provided services to the clients.

In conclusion, Kazakhstan has all the characteristics of a country which has to develop intensively the internet banking – large territory, low density of the population and as a result – very expensive coverage with bank services with the traditional methods – bank offices, has developed reliable and secure infrastructure for internet banking. Our analysis shows that the level of risks in the internet banking is minimized as the internet banking systems provide the necessary level of control.

References

Aaron, M., Armstrong, J. & Zelmer, M. (2008). Financial System Review, 2008.

Bank CenterCredit AO (n.d.). System Star Banking, https://www.bcc.kz/product/starbanking_fiz/ [Retrieved on 14.08.2018].

Center-YF (2018). Internet-banking risks, http://center-yf.ru/data/economy/riski-internet-bankinga.php [Retrieved on 18.08.2018].

Denyes, L. & Lonie, S. (2016). Digital Financial Services & Risk Management Handbook, The MasterCard Foundation and IFC of World Bank Group.

Deutsche Bank. (2018). Deutsche Bank – Credit Overview, 31 March 2018, https://www.db.com/ir/en/download/Credit_Overview.pdf

Deutsche Bank. (2017). Deutsche Bank Annual Report, https://annualreport.deutsche-bank.com/2017/ar/risk-report/risk-and-capital-performance/credit-risk-exposure/main-credit-exposure-categories.html [Retrieved on 15.08.2018].

Donovan, J., Jennings, J., Koharki, K. & Lee, J. (2018). Determining credit risk using qualitative disclosure, March 2018, WHARTON SSRN-id3149945.

Durden, T. (2016). Deutsche Bank Tells Investors Not To Worry About Its €46 Trillion In Derivatives, https://www.zerohedge.com/news/2016-10-09/deutsche-bank-tells-investors-not-worry-about-its-%E2%82%AC46-trillion-derivatives.

Goh Mei Linga, Yeo Sook Ferna, Lim Kah Boona, Tan Seng Huata. (2016). Understanding Customer Satisfaction of Internet Banking: A Case Study in Malacca. Fifth International Conference On Marketing And Retailing, Science Direct, Procedia Economics and Finance 37 (2016), p. 80-85.

Härle, P., Havas, A., Kremer, A. Rona, D. & Samendari, H. (2016). The future of bank risk management. – McKinsey Working Papers on Risk.

Harvard Business Review. (2015). How To Live With Risks. July-August 2015, https://hbr.org/2015/07/how-to-live-with-risks.

Holton, G. A. (2003). Value at Risk: Theory and Practice. Academic Press. https://www.amazon.com/Value-at-Risk-Theory-Practice/dp/0123540100.

Khrais, L. T. (2017). Framework for Measuring the Convenience of Advanced Technology on User Perceptions of Internet Banking Systems. – Journal of Internet Banking and Commerce, JIBC December 2017, Vol. 22, N 3.

Mok, A. & Saha, R. (2017). Strategic risk management in banking. – Inside magazine – Edition 2017.

Mukhtar, M. (2015). Perceptions of UK Based Customers toward Internet Banking in the United Kingdom. – Journal of Internet Banking and Commerce, April 2015, Vol. 20, N 1.

National bank of Kazakhstan. (2016). Regulations for providing banking operations and electronic banking services. – Regulation of the National bank No 212 from 31.08.2016.

National bank of Kazakhstan. (2018). Oversite of the payment systems and development of the market of payment services for the first 9 months of 2017, http://www.nationalbank.kz/ [Retrieved on 06.06.2018].

Portilla, A., Vazquez, J., Harreis, H., Pancaldi, L., Rowshankish, K. & Samandari, H. (2017). The Future of Risk Management in the Digital Era. October 2017, Institute of International Finance and McKinsey and Company.

Pyle, D. H. (1997). Bank Risk Management: Theory, Conference on Risk Management & Deregulation, Jerusalem, http://haas.berkeley.edu/finance/WP/rpflist.html.

Salihu, A. & Metin, H. (2017). The Impact of Services, Assurance And Efficiency In Customer Satisfaction On Electronic Banking Services Offered By Banking Sector. – Journal of Internet Banking and Commerce, December 2017, Vol. 22, N 3.

Shustova, Y. (2018a). Analysis of the development of the electronic banking services in Kazakhstan in 2014-2017. – Journal of Siberian Financial School, N 3, p. 69-78.

Shustova, Y. (2018b). Classification of Risks in the Internet Banking. Working paper.

Shustova, Y. & Blagoev, V. (2018). M&A and Crediting: The Hybrid Growth Strategy Seems to Be The Best For The Banks In Kazakhstan. – Economic Studies, 27 (3), p. 91-108.

Soppitt, M. (2016). What does the fintech revolution mean for the risk profile of banks? Banking Risk in the Digital Age, May 2016.

Stanišić, M. & Stanojević, L. (2009). Rizici u bankarskom poslovanju i Bazel II. Beograd: Univerzitet Singidunum. p. 8.

Van Veen-Dirks RC, P. & Tillema, S. (2017). Risk Management in the Banking Sector: The influence of personality traits on the impact of Management Accountants. Chartered Institute of Management Accountants.

Vincent, S. (2016). Banking Risk in the Digital Age. – Quarterly Outlook, May 2016, Parker Fitzgerald.

Zupanovic, I. (2014). Sustainable Risk Management in the Banking Sector. – Journal of Central Banking Theory and Practice, 2014, Vol. 3, N 1, pp. 81-100.