

УДК 336.71:004

V. V. BOBYL^{1*}^{1*}Department «Accounting, auditing and intellectual property», Dnipropetrovsk National University of Railway Transport named after academician V. Lazaryan, Lazaryan st., 2, Dnipropetrovsk, Ukraine, 49010

RISK MANAGMENT «CLOUD» TECHNOLOGIES IN BANK'S RISK MANAGMENT

Purpose. To investigated the risks of using «cloud» technologies in operating activities and to provide the recommendations in decreasing of those risks. **Methodology.** The methodological approach involves the consideration of bank risk management (including the operational one, which appeared from the use of «cloud» technologies) as from the standpoints of bank accepting the optimal management decisions, and from the standpoints of implementation of these solutions through the organizational structure. **Results.** The article emphasizes the risks of «cloud» technologies, the measures of reducing the operational risk to its components are investigated, and the recommendations in relation to the elimination of technological risk which appearing from the use of «cloud» computing are suggested. **Scientific novelty.** We propose the scientific approach to the management of banking risks, which in contrast to the existing one, includes the instruments of reducing the negative impact of the use of «cloud» technologies in the operating activities. **Practical implications.** The use of the stipulated recommendation in risk management «cloud» technology improves the efficiency of the risk management system of the bank.

Keywords: «cloud» technologies, operational risk, a bank, risk management system

Introduction

«Cloud» computing dates back to 1950, when the scientist Herb Grosh in his research wrote, that in the future the whole world would work on the terminals, which would be directed by about 15 large centers of processing operations [1].

Currently the category «cloud» technologies» includes a lot of different concepts: software, infrastructure, communication platform, data, individual working place etc.

The main thing is that «cloud» technologies give the opportunity to the enterprises (including banks) to refuse from the necessity to create and to support personal computing infrastructure.

As a result, «cloud» reveals the new approach to the computing where neither equipment nor software belongs to the bank. Instead of this the provider, with the help of Internet, gives to bank-customer the released product.

But the implementation of «cloud» technologies into banks may cause the defined risk (first of all operational ones).

The operational risks are not connected with bank's business line, but with organization of its financing and operating activities.

The main obstacle that complicates the operational risk management is a low probability in defining the size of these risks (furthermore the incidents' list of realization operating risks is quite wide).

The latest research analysis

The problems of classification and estimation of operational risks are studied by such native and foreign scientists as O. Bogdanov [2], Yu. Boruch [3], O. Derevska [4], V. Kovalenko [5], O. Kovalchuk [6], O. Kryklii [7], B. Sazykin [8], V. Kharlamov [9], A. Shynkarenko [10].

In justice to scientific insights of Ukrainian and foreign economists, the gained experience in appraisal practice and operational risk management, it should be emphasized that the open questions of IT-technologies influence (including «cloud») on operational risk of the bank have not been solved yet.

Purpose

The purpose of the article is the research of «cloud» technologies as the potential factor of increasing operational risk and also the providing advices according to the size reducing in this kind of risk.

Methodology

The methodological basis of the research consists of the complex approach to operational risks' management. The approach assumes the study of operational risks' management (including those, which appeared through the use of «cloud» technologies) as from the position of bank's acceptance of optimal management decisions through the organizational structure. From these peculiarities there is the method union of business economics with the method of system's analysis in bank's functioning.

Results

Bank's risk management system is the constituent part of economic stability of a bank, the task of which is identification, estimating and risk management, which are appeared through the debit and credit operations, poor organization, business and the change of factors in the environment.

Among the banking risks through the management complexity the operational risks took the particular place.

In Basel framework II operational risk is defined as «default risk in the result of faults and mistakes in internal bank process which were made on the part of employees through the information system and also on the part of external events» [11].

In such case Basel Committee indicates a particular place of operational risk in bank's risk management system, whereas in the work of western banking organizations this risk towards paper losses takes the second place, being among credit (the 1st place) and market (the 3rd place) risks. Taking into consideration this fact Basel II reasonably recommends to consider operational risk as class of its own risks, which must be supported by some of bank stock, the name of which is «economic capital under operational risk» [11].

Basel II suggests examining such categories of operational risks as: staff risk, the risk of systems and technologies, business risk, environmental bank's functioning risk.

A range of foreign pecuniary institutes uses operational risk's classification, proposed by Banker Trust [12]:

staff risk is all risks, which are connected with company's employees, as to their unauthorized

actions, incompetence, dependence on certain experts, etc.;

technological risk is the risk, caused by information system failure programmers or database, data-transmission systems and other equipment which is necessary for bank activities;

physical harm risk is the risk which occurs as the result of natural catastrophes and other factors, which can cause the damage of main equipment, systems, technologies and banking resources (such kind of risk is minimized by property insurance);

risk of relationship is the risk which appears as the result of relationships that are in business such as difficulties in bank customer relationship and lack of internal control;

external risk appears as the result of criminal acts of external organizations, individuals and also in the case of applicable regulatory change.

In methodological recommendations of National Bank of Ukraine (NBU) from the evaluation risk's system such term as «operation-process risk» is introduced. Under this risk the specialists of NBU understand «potential risk for long-term existence of banking establishment that appears through the disadvantages in corporate management, internal control system or information technologies and reduction process from the standpoint of management, universality, safety, control and continuity of work» [13].

From our point of view present day operational risk should be divided into the following subtypes [14]:

1. Technological is the probability of rejection from the planned financial indicators through inefficiency of information technologies and reduction process etc.

2. Executing risk is the probability of rejection from financial indicators in the result of inadvertent violation and neglect official duty.

3. Deception is financial losses in the result of fraud or embezzlement or property etc.

4. Corporative is the probability of rejection from planned financial indicators through the mistakes in corporate management (conflict of interests, mistakes in workflow definition, distribution of responsibilities etc).

5. Innovation is the probability of rejection from planned financial indicators through the mistakes on the stages of the development and implementation of new (improved) banking products.

6. Strategy risk is the probability of rejection from planned financial indicators through the mistakes in target formation and development strategy

of the bank and extreme reaction into changes in business environment of the bank.

The methods of operational risk decreasing for its constituents are shown in table 1.

Table 1

The methods of operational risk decreasing for its constituents

Operational risk constituents	The methods of risk decreasing	Bank's structures that controls operational risk constituents
1	2	3
Technological risk	<ul style="list-style-type: none"> – to monitor, to refresh to test the information systems, equipment, channels of communication etc.; – to hatch a plan of resumptioning IT- service; – to introduce the backup systems and the conservation of banking data; – to divide the functions among the departments which are dealing with software development and Network service etc. 	Bank management; Administration (department) of automation of bank technologies; Executing agency of risk management
Executing risk	<ul style="list-style-type: none"> – to develop and to introduce the banker's code of conduct; – to raise the service standards and to monitor the customer experience; – to introduce the employee incentive programmer; – to carry out the motion and time study of wholesale banking; – to analyze the indicators of personnel administration (staff turnover, the amount of trained personnel etc). 	Bank management; Back office; Executing agency of risk management
Deception	<ul style="list-style-type: none"> – to implement the mechanism of timely identification and to stop the deception possibilities through banking information systems. 	Administration (department) automation of bank technologies; Back office
Corporative risk	<ul style="list-style-type: none"> – to provide the same attitude to the shareholders, apart from the amount of stocks which belongs to them; – to implement the principles of independent internal control; – to introduce the procedures of defining people connecting with the bank and also the control and regulatory authorities for the operations of people connecting with the bank; – to draw up and to implement the assessment influence system of managerial decisions on financial result of the bank; – to make a clear division of functional responsibilities of bank divisions; – to depict and to describe the business processes of financial institutions; – to provide the timely and full financial information. 	Board of supervisors; Bank management; Executing agency of risk management
Innovation risk	<ul style="list-style-type: none"> – to implement the defining system of priority in development of new banking products (taking into consideration the risks); – to establish the quality standards of a new or improved banking product (operation card); – to provide all banking institutions of necessary regulatory documents ,software,promotional materials; – to conduct staff training; – to make the test-market sales of a new product to loyal customers; – to develop the effective advertising campaign with the purpose of sale promotion. 	Board of supervisors; Bank management; Executing agency of risk management

Continuation of Table 1

Operational risk constituents	The methods of risk decreasing	Bank's structures that controls operational risk constituents
1	2	3
Strategy risk	<ul style="list-style-type: none"> – to make up the plan as to the structural bank reorganization (for example, bank merger or take-over); – to monitor competing banks; – to implement the control system of quality realization of banking purposes (the performance of strategic plans and budgets); – to make up the plan as to the increasing of bargaining position (diversification of a product, geography and clients); – to make marketing research. 	Board of supervisors; Bank management; Executing agency of risk management

«Cloud» technologies increase the rate of technological risk.

Before the reviewing the instruments of decreasing the negative influence of «cloud» calculation in operational bank activities it is necessary to find out the main banking advantages, of «Cloud» technologies, they are:

1. *Profitability.* «Cloud» technologies essentially allow to decrease the capital bank outlays on the construction of tabulation centers, the purchase of head-end equipment, hardware and software decisions etc. (the main part of these expenses is gobbled up by the provider of «cloud» services). Additionally the bank saves on maintaining IT-personnel, administrating etc.

2. *Elasticity.* «Cloud» technologies provide the opportunity to change the configuration of corporative IT- infrastructure rapidly depending on the current bank expenditures (a financial institution purchases as many resources as it needs on the present moment). «Cloud» resources are enough for ordering a virtual «super-computer» or the infrastructure for a bank and there are no problems in

software updating (the last copies are always available), the compatibility of different operating systems etc. During the peak demands (for example during the preparation of year-end financial statement) there is no need for planning the introduction of supplementary information capacities as far as «cloud» services may be fit automatically and practically without limitation. The services may be given, extended, narrowed at all times without additional outlays on the engagement with a provider, as a rule in automatic mode.

3. *Mobility.* «Cloud» technologies give the opportunity in a literal sense to carry individual working place with you with mobile device and Internet access at hand, a bank employee despite

his location always has the opportunity to access his own virtual computer corporate systems, database etc.

4. *Self-service on demand.* A bank independently defines and changes the computational requirements (server time, the speed of access and information handling, stored data amount) without engagement with the representative of service provider.

5. *High availability.* «Cloud» services are available during 99,5 percent of time but some providers guarantee the access at the level of 99,9 percent

6. *Data storage.* The employees of the bank do not need to worry about information change-over, as the supporting materials are saved in «cloud» («cloud» infrastructure guarantees data storage).

Despite of the above mentioned advantages, «cloud» market in Ukraine, in contrast with U.S or EC markets, at the present time are in the process of accumulation of primary experience of using «cloud» decisions. But after the experts' predictions, already since 2015 it demonstrates the exponential increasing for «cloud» markets of developed nations. Reusable market increasing in the coming years causes the appearing of a new specific and important sector of Ukrainian economy and infrastructure [15].

We offer to investigate the main risks of «cloud» technologies:

1. Attacks on hypervisor. Hypervisor is one of key element of «cloud» technologies. The main function is the division of resources among virtual machines. Attack on hypervisor may lead to the fact that one virtual machine can get the memory access and the access to the resources of another one. Also it will be able to capture network traffic,

to select physical resources and even to displace a virtual machine out of server.

2. Attacks on operating systems. A great number of virtual machines that are used in «cloud» technologies require the availability of defined management system that can effectively control formation, transmitting and reclamation of virtual machines. Interference into management system can cause the appearance of virtual stealth-machines, which can block the work of other ones.

3. Stability of connection. The main point of «cloud» technologies requires the constant being in online mode (Internet connection). The connection through Internet must be stable and as well broadband. Partially the risk of the absence of connection may be decreased by data randomizing or the development of branching algorithm into free running connection to change only critically important data.

4. Dependence on supplier (provider) «cloud» technologies or its failure. As the bank expenses on migration from local environment into «cloud» are rather significant so in the way when the sup-

plier of «cloud» decisions stops to satisfy bank needs on any criteria (the pay hike for the use, problems on the path data communication), so to change it will be problematically. Firstly, in the It-technologies market a provider can be absent, that will be able to offer an appropriate level of «cloud» decisions, secondly cash expenses and time expenditures may be very large.

5. *DDOS- attacks*. DDOS- attacks are the attacks on computer system with a view of making computer resources not available for the users. One of widespread methods of attacks is the saturation of attacked computer or network equipment by a large quantity of external queries (so attacked equipment cannot answer the users or answers so slowly that becomes unavailable in fact).

6. *Data safety*. The most banks are afraid of eavesdropping data communication, the loss of control on data and impossibility of information destruction on the Internet.

The main risks of «cloud» technologies and the tools of their decreasing are shown in table

Table 2

The main risks' management of «cloud» technologies

Risk	Characteristics	Management
1	2	3
Attacks on hypervisor	The risk of resource division which may lead to the fact that one virtual machine gets illegal access to the storage unit and resources of another one	The standardization of algorithms' access to the management funds of host-server; the use of native firewall (programmer that protects computer systems) host virtualization
Attacks on operating system	The risk of appearance of virtual stealth machines which can block the work of another virtual machines	The use of passwords, certificates and codes
Connection stability	The risk of degradation (or absence) Internet connection	The data randomizing; the development of branching algorithm into low rate mode connection
Dependence on supplier (provider) «cloud» technologies	The risk of absence the opportunity to change the provider of «cloud» technologies through the absence on the market another providers, means or time	The detailed approach to the choice of a provider; the work with the provider, which uses the open standards
Provider's bankruptcy	The risk of tie-up in giving of «cloud» decisions through provider's bankruptcy	The detailed approach to the choice of provider; the work with a few providers; the availability of strategy in changing provider
Communication loss with a provider	The risk of tie-up in business processes through the absence of access to provider	The choice of provider, that has data centers in a few countries; the use of satellite Internet connection; availability of backup copy of critical systems in private «cloud»

Continuation of Table 2

Risk	Characteristics	Management
1	2	3
Eavesdropping through the transmission	The risk of illegal access to the information during data operation	The use of cryptography through the information transmission; the users' training of information security rules
Compliance risk	The risk of receiving the penalties and other sanctions from control device through the violation of obligations from active legislation	The consultation with a regulator and foreign auditors
The loss of control at data or infrastructure	The risk of opportunity absence to provide at the appropriate level the security through the loss of control at data and infrastructure	The conducting of an audit provider's security; making agreement with provider about data confidentiality; the service level monitoring and incidents of contravention in information security
The impossibility of data deletion	The risk of information outflow through the impossibility of data deletion in «cloud» technologies	The data encryption in «cloud»; masking out the information; specifically including the requirements on the procedure of data deletion in SLA (the contract about the level of providing services)
Management interface cracking	The risk of deception through management interface of «cloud» technologies	Two-factor authentication; data link encryption
DDOS-attacks	The risk of attack on computer system with a view of making computer resources unavailable for users	The choice dos-stable provider; the work with a few providers
The activity of another users of «cloud»	The risk of illegal access to the information and the tie-up of business process through the activity of another users of «cloud» technologies	Detailed approach to the provider's choice; the work with a few providers

Conclusions

«Cloud technologies» in the nearest future lead the operational banking activity on a transformational new level. This IT-technology may become the main factor of improvement of competitiveness in modern financial institutions.

But the use of «cloud» decisions is connected with the certain operational risks in the first place is the technological one.

On the bank level (micro level) to decrease the size of risks that appear in the process of using «cloud» technologies may be done with the help of the following management decisions: detailed approach to the provider's choice (supplier) «clouds»; the development of plan actions in changing a provider; the implementation of two-factor authentication, data encryption and data masking out; the training of bank employees to the rules of information security; the advising with a regulator and foreign auditors as to the risks of implementing of «cloud» technologies.

From the positions of National Bank of Ukraine (regulator) it is reasonable to make complex analy-

sis and summing-up, tendencies and perspectives in developing of introduction of «cloud» technologies into banks, and also the development of national standards which establishes the appropriate requirements to the quality and reliability of «cloud» technologies and services on the financial market of Ukraine.

REFERENCES

1. Grosch, H. R. J., *Bibliography on Chebyshev Polynomials and Their Use as Optimum Approximation Functions*, Proceedings of the 1949 Scientific Computation Seminar, IBM, 1951.
2. Bogdanov A., Operatsionnyy risk i ego vliyanie na ustoychivuyu rabotu finansovoy organizatsii [Operational risk and its impact on the stable operation of the financial institution]. *Bankovskie tekhnologii*, 2008, issue 7, pp80–88.
3. Boruch Yu., Konsortsium dlya sbora dannykh po operatsionnym riskam kak instrument otsen-ki i snizheniya riska [Consortium to collect data on operational risk as a tool for risk assessment and mitigation]. *Bankovskoe delo*, 2009, issue 10, 40 p.
4. Derevs'ka O., Operacijnyj ryzyk: katehoriji upravlinnja [Operational risk: category of man-

- agement]. *Visnyk UBS NBU.*, 2010, issue 3, pp. 136-140.
5. Kovalenko V., Upravlinnja operacijnymy ryzykamy v bankivskij systemi [Operational risk management in the banking system]. *Aktual'ni problemy ekonomiky*, 2010, issue 5 (107), pp.189-1976.
 6. Kovalchuk O. Osnovni pidkhody do klasyfikatsii vydiv operatsiinoho ryzyku v banku [Basic approaches to classification of operational risk in the Bank]. *Problemy i perspektyvy rozvytku bankivskoi systemy Ukrainy: zb. nauk. prats / Derzhavnyi vyshchyi navchalnyi zaklad «Ukrainska akademiia bankivskoi spravy Natsionalnogo banku Ukrainy»*. Sumy, 2010, vol. 30, pp.142-151.
 7. Kryklii O. Instrumentarii otsinky operatsiinoho ryzyku banku [Tools for assessing operational risk of the bank]. *Visnyk UABS*, 2010, issue 4, pp. 45-48.
 8. Sazykyn B., Upravlenye operatsionnym ryском v kommercheskom banke [Management of operational risk in commercial bank]. Moscow, Vershyna Publ., 2008, 291 p.
 9. Kharlamov V., Operatsionnye rysky y rysky ynformatsionnoi bezopasnosti [Operational risks and information security risks]. *Bankovskoe delo*, 2009, issue 7, pp. 41-42.
 10. Shynkarenko A. Otsinka operatsiinoho ryzyku investytsiinykh operatsii banku ta formuvannia rezervu yak metod yoho minimizatsii [Evaluation of operational risk investment bank operations and provisioning as a method to minimize]. *Finansov-kredytna systema*, 2011, issue 3, pp. 309-313.
 11. International Convergence of Capital Measurement and Capital Standards. Basel. November 2005. Access: <http://www.bis.org>. Title from the screen.
 12. Dmytrova, O. S., Honcharov, K. H., Merenkova O. V., *Modeliuvannia otsinky operatsiinoho ryzyku komertsiinoho banku* [Modeling assessment of operational risk of commercial banks]. Sumy, DVNZ «UABS NBU» Publ., 2010, 264 p.
 13. Metodichni vkazivky z inspektuvannia bankiv «Systema otsinky ryzykiv» zatverdzheno Postanovoiu Pravlinnia NBU vid 15.03.2004 r. [Guidelines for the examination of banks' risk assessment system "approved Ser-verifies the NBU Board dated 15.03.2004, issue 104]. Available at: <http://liga.com.ua>. – Nazva z ekranu.
 14. Bobyl, V. V., Osoblyvosti operatsiinoho ryzyku: klasyfikatsiia, kilkisna otsinka, upravlinnia [Features of operational risk: classification, measurement, management]. *Bankivska sprava*, 2012, issue 1 (98). Kyiv, pp. 36-50.
 15. Analitychna zapyska Natsionalnogo instytutu stratehichnykh doslidzhen pry Prezydentovi Ukrainy «Perspektyvy rozvytku rynku khmarnykh obchyslen v Ukraini: perevahy ta ryzyky» [A snapshot of the National Institute for Strategic Studies under the President of Ukraine "Prospects for the cloud computing market in Ukraine: Advantages and Risks]. Available at: <http://www.niss.gov.ua/articles/1191/>.
 16. Bobyl, V. V., Antykryzove upravlinnia bankivskymy ryzykamy monohraf [Crisis management of banking risks]. Dnipropetrovsk, «Svidler A.L.», Publ., 2012, 270 p.

В. В. БОБИЛЬ^{1*}

^{1*}Каф. «Облік, аудит та інтелектуальна власність», Дніпропетровський національний університет залізничного транспорту імені академіка В. Лазаряна, вул. Лазаряна, 2, Дніпропетровськ, Україна, 49010

УПРАВЛІННЯ РИЗИКАМИ «ХМАРНИХ» ТЕХНОЛОГІЙ У СИСТЕМІ РИЗИК-МЕНЕДЖМЕНТУ БАНКУ

Мета. Дослідити ризики застосування «хмарних» технологій в операційній діяльності банку та надати рекомендації щодо зменшення таких ризиків. **Методика.** Методологічний підхід передбачає розгляд управління банківськими ризиками (у тому числі операційними, що виникли через застосування «хмарних» технологій) як з позицій прийняття банком оптимізаційних управлінських рішень, так і з позицій реалізації цих рішень через організаційну структуру. **Результати.** У роботі виокремлено ризики «хмарних» технологій, досліджено заходи зменшення операційного ризику за його складовими, запропоновано рекомендації щодо нейтралізації технологічного ризику, який виникає через застосування «хмарних» обчислень. **Наукова новизна.** Запропоновано науковий підхід щодо управління банківськими ризиками, який, на відміну від існуючого, включає інструменти зменшення негативного впливу застосування «хмарних» технологій в операційній діяльності банку. **Практична значимість.** Використання наданих рекомендацій стосовно управління ризиками «хмарних» технологій підвищує ефективність системи ризик-менеджменту банку.

Ключові слова: «хмарні» технології, операційний ризик, банк, система ризик-менеджменту

В. В. БОБЫЛЬ^{1*}

^{1*}Каф. «Учет, аудит и интеллектуальная собственность», Днепропетровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, ул. Лазаряна, 2, Днепропетровск, Украина, 49010

УПРАВЛЕНИЕ РИСКАМИ «ОБЛАЧНЫХ» ТЕХНОЛОГИЙ В СИСТЕМЕ РИСК-МЕНЕДЖМЕНТА БАНКА

Цель. Исследовать риски применения «облачных» технологий в операционной деятельности банка и предоставить рекомендации по уменьшению этих рисков. **Методика.** Методологический подход предполагает рассмотрение управления банковскими рисками (в том числе операционными, которые возникли из-за использования «облачных» технологий) как с позиций принятия банком оптимизационных управленческих решений, так и с позиций реализации этих решений через организационную структуру. **Результаты.** В работе выделены риски «облачных» технологий, исследованы меры для уменьшения операционного риска по его составляющим, предложены рекомендации относительно нейтрализации технологического риска, возникающего из-за применения «облачных» вычислений. **Научная новизна.** Предложен научный подход к управлению банковскими рисками, который, в отличие от существующего, включает инструменты уменьшения негативного влияния применения «облачных» технологий в операционной деятельности банка. **Практическая значимость.** Использование предоставленных рекомендаций по управлению рисками «облачных» технологий повышает эффективность системы риск-менеджмента банка.

Ключевые слова: «облачные» технологии, операционный риск, банк, система риск-менеджмента