https://doi.org/10.51176/JESP/issue_4_T13
МРНТИ 06.35.51
JEL:G21

The financial security management model in second-tier banks

Azhar Z. Nurmagambetova1, Sunkar Z. Nurmagambetov2, Aziya G. Mukusheva3

[1] Kazakh National University named after Al-Farabi, [2] Kazakh Economic University named after T. Ryskulov, [3] Gumilyov Eurasian National University

Abstract

With the growing socio-economic threats associated with the risk of involving second-tier banks in the legalization of illegal income, it is necessary to create an effective financial monitoring system to reduce this risk. Aim of the research is to propose and test a model of financial security management in second-tier banks in Kazakhstan, based on a combination of clustering models and recursive least squares, which allows for three-level processing of incoming information in banks in order to identify hidden data that pose a financial threat to the activities of second-tier banks. The research methodology is based on a combination of APC-III clustering algorithm models and the recursive least squares (RLS) method, with the algorithm slightly modified in accordance with the OECD recommendations. This ap proach made it possible to consider the operations of banks at three levels and, during transitions, identify suspicious transactions that require immediate examination by the bank's management. Application of the model made it possible to reveal that, on average, about a third of banks' operations can be classified as suspicious, which means they require careful study. In our case, we selected 200 cases from the original data mixed with 70 suspicious transactions to study the model. As a result of statistical processing of banking operations, 90 operational data were identified, of which 27 turned out to be suspicious, that is, about 30% of verified transactions were found suspicious. As a result of providing this information, the bank was able to identify 19 transactions aimed at money laundering.

*Keywords***:** financial monitoring, management model, financial security, banking, financial management, risk management

Екінші деңгейдегі банктердегі қаржылық қауіпсіздікті басқару моделі

Түйін

Екінші деңгейдегі банктерді заңсыз кірістерді заңдастыруға тарту тәуекелімен байланысты әлеуметтік-экономикалық қатерлердің өсуі жағдайында осы тәуекелді азайту үшін қаржы мониторингінің тиімді жүйесін құру қажет. Зерттеудің мақсаты - екінші деңгейлі банктердің қызметіне қаржылық қауіп төндіретін жасырын деректерді анықтау мақсатында банктердегі кіріс ақпараттарын үш деңгейлі өңдеуді жүзеге асыруға мүмкіндік беретін кластерлік модельдер мен рекурсивті ең кіші квадраттардың жиынтығына негізделген Қазақстандағы екінші деңгейлі банктерде қаржылық қауіпсіздікті басқару моделін ұсыну және сынақтан өткізу. Зерттеу әдістемесі APC-III кластерлік алгоритм модельдері мен ең кіші квадраттардың рекурсивті әдісінің (RLS) үйлесуіне негізделген, алгоритм OECD ұсыныстарына сәйкес сәл өзгертілген. Мұндай тәсіл банктердің операцияларын үш деңгейде қарауға және ауысу кезінде банк басшылығының дереу тексеруін талап ететін күдікті операцияларды анықтауға мүмкіндік берді. Модельді қолдану негізінде, орташа есеппен банк операцияларының үштен бірін күдікті деп есептеуге болатынын көрсетті, ал бұл өз кезегінде мұқият зерттеуді талап етеді. Біздің жағдайда модельді зерттеу үшін 70 күдікті транзакциямен араласқан бастапқы деректерден 200 жағдайды таңдадық. Банк операцияларын статистикалық өңдеу нәтижесінде 90 операциялық деректер анықталды, оның ішінде 27-і күдікті болып шықты, яғни тексерілген транзакциялардың шамамен 30% - ы күдікті деп танылды. Осы ақпаратты ұсыну нәтижесінде банк ақшаны жылыстатуға бағытталған 19 транзакцияны ан*ықтай алды.*

Түйін сөздер: қаржылық мониторинг, басқару үлгісі, қаржылық қамтамасыз ету, банк ісі, қаржылық менеджмент, тәуекел-менеджмент.

Модель управления финансовой безопасностью в банках второго уровня

Аннотация

В условиях нарастания социально-экономических угроз, связанных с риском вовлечения банков второго уровня в легализацию незаконных доходов, необходимо создание эффективной системы финансового мониторинга для снижения этого риска. Цель исследования – предложить и протестировать модель управления финансовой безопасностью в банках второго уровня в Казахстане, основанную на комбинации моделей кластеризации и рекурсивных наименьших квадратов, которая позволяет осуществлять трехуровневую обработку входящей информации в банках с целью выявлять скрытые данные, представляющие финансовую угрозу для деятельности банков второго уровня. Методология исследования основана на сочетании моделей алгоритма кластеризации APC-III и рекурсивного метода наименьших квадратов (RLS), при этом алгоритм немного модифицирован в соответствии с рекомендациями OECD. Такой подход позволил рассматривать операции банков на трех уровнях и во время переходов выявлять подозрительные операции, требующие немедленной проверки руководством банка. Применение модели позволило выявить, что в среднем около трети операций банков можно отнести к категории подозрительных, а значит, они требуют тщательного изучения. В нашем случае мы выбрали 200 случаев из исходных данных, смешанных с 70 подозрительными транзакциями, для изучения модели. В результате статистической обработки банковских операций было выявлено 90 операционных данных, из которых 27 оказались подозрительными, то есть около 30%

проверенных транзакций были признаны подозрительными. В результате предоставления этой информации банку удалось выявить 19 транзакций, направленных на отмывание денег.

Ключевые слова: финансовый мониторинг, модель управления, финансовое обеспечение, банковское дело, финансовый менеджмент, риск-менеджмент.

Introduction

At the present time one of the most urgent problems of increasing confidence in the banking sector and improving the investment climate in Kazakhstan is to create a real system of combating money laundering and financing of terrorism. In the recent past the involvement of banks in the legalization of criminal proceeds has not attracted significant public attention. In recent years, after a series of scandals in which major banks are at the center of public attention, the process of involving financial institutions in the legalization of illegally gained income, studies not only at the international level but also in Kazakhstan. Since Kazakhstan takes 50th place among competitive economies in the world, it has a dynamic economy, as well as a special geopolitical position in the world and is located in the proximity to areas with the high intensity drug trafficking, terrorist activity and the questions of combating the legalization (laundering) of illegally gained incomes (CLI), and overlapping sources of terrorist financing is highly relevant. The risk of involvement of second- tier banks as the main entities participating in the laundering of illegal incomes and terrorism financing especially dangerous for the banking system, leading to the loss of business reputation of credit institutions and, accordingly, prevents the activity expansion of Kazakh banks in the global financial markets [1].

With the growing of social and economic threats associated with the risk of involvement of banks in legalization of illegal incomes, necessitates the creation of an effective system of financial monitoring in order to reduce this risk.

The experience of advanced countries in the system of financial monitoring important attention were given to the risk of legalization of illegal incomes during their placements with banks. At this stage of legalization of criminal incomes is most vulnerable, both for the public and for the domestic banking financial monitoring. The purpose of financial monitoring in the banking system is a warning of processes of legalization of criminal incomes and terrorist financing directly at each bank. Therefore, reducing the risk of involvement of banks in the process of legalization of illegal incomes is of particular importance. The effectiveness of financial monitoring of legalization of criminal incomes depends on how the monitoring ensures the transparency of the bank's activities and to what extent minimize the risk of legalization of criminal incomes, where special attention is given to risk of loss of business reputation.

In this regard it might be concluded that without proper effective mechanism for combating money laundering and terrorist financing through the involvement of second-tier banks the economy cannot develop sustainably [2]. During the global financial crisis and the transition of Kazakhstan to the post-industrial society, an important condition for the effective progressive development of the economy of the republic is carrying out of state policy aimed primarily on the development of an established control system and to minimize risks for prevention of legalization (laundering) illegally gained incomes and financing terrorism.

The authors set the goal of this publication to propose and test a model of financial security management in second-tier banks in Kazakhstan, based on a combination of clustering models and recursive least squares, which allows three-level processing of incoming information in banks.

Literature Review

In modern conditions of globalization of financial markets, one of the most pressing problems of increasing confidence in the banking sector and improving the investment climate in the Republic of Kazakhstan is the creation of an operating model for managing the financial security of commercial banks. The risk of attracting banks as the main objects involved in the system of money laundering is especially dangerous for the banking system, which leads to the loss of business reputation of credit institutions and, accordingly, hinders the expansion of the activities of Kazakhstani banks.

The importance of financial security in banks has been emphasized by many authors. So, E. V. Karanina and O. I. Blednykh define financial security as the protection of financial interests at all levels of financial relations [3]. Author Yu.G. Averyanova emphasizes that in the conditions of the existence of a commercial bank, financial security is its ability to build up and maintain its financial potential, which will be used in the future to solve the assigned tasks and strategic goals, including ensuring the independence and stable operation of the bank [4].

Chong, F. Lopez-De-Silanes [5], D. Sat et al. [6] and F. Teichmann [7] study the prospects of using different money laundering tools. Scientists concluded that despite the active use of the latest technologies (cryptocurrency) for illegal activity, banks in certain regions of the world would remain a very relevant money laundering tool.

In modern scientific literature, various approaches and models of financial security management of banks are presented. So, Melnik D.Yu. examines a model of the conceptual relationship of threats, risks and security of banks, presenting the factors that contribute to the realization of a hazard for a specific object at a certain point in time [8].

Serdyuk V.A. distinguishes two classes of methods for detecting cyberattacks, such as ensuring the financial security of banks: methods for detecting anomalies and methods for detecting abuse. In both cases, the input data for the operation of the system are behavior patterns formed on the basis of a set of input parameters - event patterns [9].

V. Pramod, J. Li, P. Gao [10] proposed a new structure for the prevention of money laundering in banks formed by mapping COBIT (Control for Information and Related Technology) processes to the COSO (Committee of Sponsoring Organization) components. Thus, the authors have developed a multi-agent framework in the form of a stand-alone system, which can be integrated into the business processes of a bank and will detect transactions related to money laundering.

Gaiduk V.I. and et al consider an approach to the model of financial security of banks through a set of indicators and their threshold values, justifying this by the fact that by analyzing trends in indicators, one can draw conclusions about the increase or decrease of threats to the financial security of commercial banks in the course of their activities and development, and also assess the reaction and adaptation of commercial banks in an unsafe environment [11].

Evseev S.P. offers a model for increasing the level of security of banking information by maximizing the number of its emergent properties with minimal resource costs [12]

Kozminykh S.I. considers the functional dependence for finding the numerical value of the vulnerability coefficient, which estimates the level of complex security of the object of the credit and financial sector, which made it possible to obtain a quantitative assessment of both the existing and the predicted level of vulnerability of the information object [13].

Given the different nature of threats to banking security, Arunabha Mukhopadhyay, Samir Chatterjee and others propose to use a cyber risk assessment and mitigation system (CRAM) to assess the likelihood of an attack using generalized linear models (GLM) [14].

Thus, despite the fact that the authors use various statistical models, they pursue one goal - the formation of an effective method for managing the financial security of banks. At the same time, from our point of view, the greatest importance in the management of the financial security of banks should be assigned to the information processing and monitoring system. It is for this purpose that we propose a combination of clustering models and recursive least squares, which allows three-level processing of incoming information in banks.

Methodology

The effectiveness of financial security depends on the extent to which monitoring ensures the transparency of the bank's activities and how the risks of money laundering are minimized, where special attention is paid to the risk of losing business reputation.

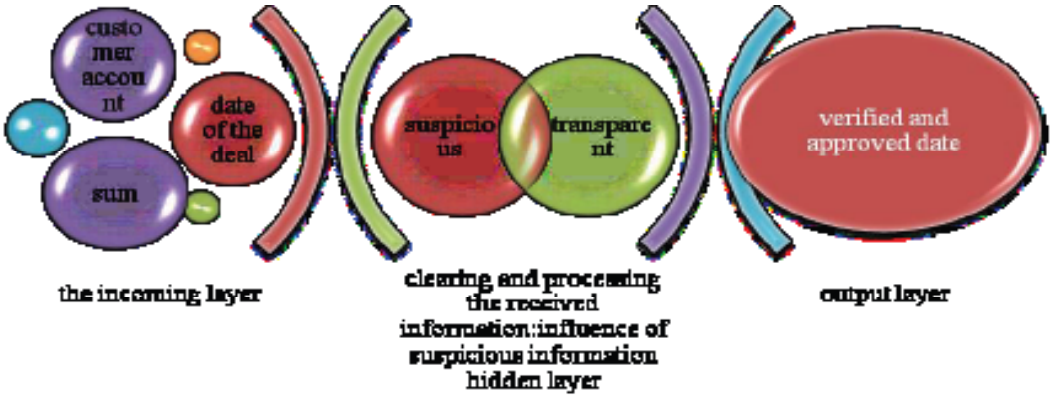
We propose an approach based on a combination of models, the parameters of which are based on the APC-III clustering algorithm and the method of least squares (RLS), while the algorithm is slightly updated in accordance with the OECD recommendations [15].

The recursive least-squares (RLS) is a very popular algorithm, especially for its fast convergence rate. This approach is considered for example by Honghong Duan, Jie Jia, Ruifeng Ding [16].

The most important parameter of this algorithm is the forgetting factor. It is well-known that a constant value of this parameter leads to a compromise between misadjustment and tracking. In this paper, we present a variable forgetting factor approach, aiming to better compromise between the performance criteria of the RLS algorithm. Also, we propose a practical solution to estimate the power of the system noise (in a system identification scenario), which is required within the algorithm. Experiments performed in the context of network echo cancellation support the advantages of the proposed approach.

The least squares (LS) approach has wide-spread applications in many fields, such as statistics, numerical analysis, and engineering. Its greatest progress in the 20th century was the development of the recursive least squares (RLS) algorithm, which has made the LS method one of the few most important and widely used approaches f or real-time applications in such areas as signal and data processing, communications and control systems [17]. Considerable efforts and significant achievements have been made in developing even more efficient RLS algorithms.

The model assumes the presence of three layers of information processed by banks: incoming, suspicious and outgoing (Figure 1).



Note - Compiled by the author

Figure 1-**Three layers of model information**

Let the values of the input, hidden and output layers be denoted by p, m, n, respectively. For any example, x_p [x_1, x_2, ..., x_p] in the input layer set X = (X_1, X_2, ..., X_m), the income will be Y = (Y_1, Y_2, ..., Y_n). Thus, the anti-money laundering model can be described by the following equation:

$$(x \in R_a) \rightarrow (h \in R_b) \rightarrow (y \in R_c) \quad (1)$$

$$y_i = f_i(x) = w_0 + \sum_{i=1}^{m} w_i \varphi (x - c_i) \quad (2)$$

$$x \rightarrow \varphi_i(x) \quad (3)$$

Where,

x – information submitted to the bank to be verified;

h – hidden information to be discovered;

y - processing result (output layer of the model);

$w_i = (w_1, w_2, ..., w_a)^t$ - the value of the weight of the connection between the hidden layer and the output layer.

We estimate the nonlinear reflection in the model of the transition of the processed information to the hidden layer using the Gauss function:

$$\varphi (x - c_i) = \left[wi - \frac{/x - c_i/}{\sigma_i^2} \right] \quad (4)$$

$$i \in [a; b]$$

Where,

$c_i = \left(c_i^1, c_i^2, ..., c_i^b\right) \in R_b \quad i = 1,2, ..., b$ - represents the *i*-th process in a hidden layer;

C_i - controls the rate of attenuation of the Gauss function;

b - this is the number of units (information) in the hidden layer.

Examining bank accounts, we found that if we start from analysing transactions between accounts, we will get real information about our customers. The set under study consists of many records in the database. Each record includes some attributes, forming a special vector. In addition, there is a unique class label. Corresponding to each sample in the studied data set, the specific form of the data sets of the studied sample is expressed as follows:

$$E = (I_1, I_2, ..., I_a; S) \quad (5)$$

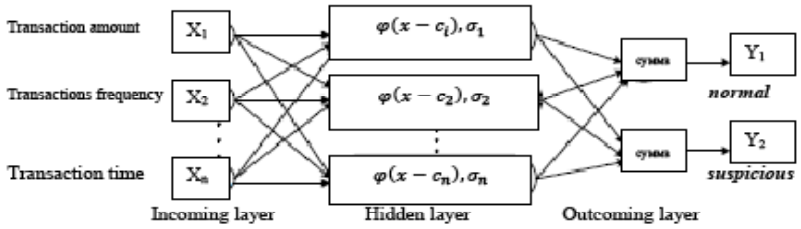
Where,

$I_1, I_2, ..., I_a$ - denote input data attributes;

S - this is the value of the class label (example).

The essence of processing and filtering data according to the model is shown in Figure 2.

The confidence interval is as follows: from 0 to 1 - normal output layer, from 1 and higher - suspicious data. It should be noted that suspicious data is not always confirmed. If they find confirmation, they go to the category of normal output layer. Available attributes include the client's name, client number, client current account number, client certificate number, transaction date, types of business associated with the client's current account, transaction zone code, transaction amount, transaction time, transaction currency, transaction types, and transaction frequency.



Note - Compiled by the author

Figure 2 - **Model Algorithm**

Results

We can consider the large and suspicious data on operations used in the fight against money-laundering provided by financial institutions. This transaction data is used as preparation for the output layer. Then we use computer data to judge whether the transaction data has undergone preliminary processing, possibly at the first stage illegal transactions have been identified. When the data of a suspicious transaction has been identified, we add this scheme to the existing examples and the computer system again begins to recognize the parameters.

A false positive level is defined as the total number of normal cases that are incorrectly classified as unusual, divided by the total number of normal cases. Take for example the assessment of the real financial transactions made in the established database of the bank "X" (table 1).

To build a consumer behaviour profile, we take three attributes processed according to statistical theory, namely, withdrawal frequency (d_1), replenishment frequency (d_2) and operating amount (d_3). As a result, we obtain the data presented in table 2.

Table 1 - **Structure of the source data sets**

Customer number	Business area	Deal date	Type of transaction	Top-up Frequency	Account Withdrawal Frequency	Transaction Amounts
187366	Industry	20150806	Deposit	7	6	109060
157801	Services	20150804	Witdhrawal	5	2	8610
199643	Individual entrepreneur	20150708	Witdhrawal	4	3	76431
164578	Non-profit organization	20150712	Deposit	8	5	112342
192209	Industry	20150604	Witdhrawal	2	1	230567
194211	Trading	20150509	Deposit	1	0	120411
Note - Compiled by the author on the basis of the source of the bank (Reporting data of AO Bank "X" for 2018 - 2019)						

Table 2 - **Attributes of parameters (characteristics) for the processed data**

Set (example)	d_1	d_2	d_3
1	2	3	4
S_1	0,04	0,21	0,65
S_2	0,18	0,15	0,71
S_3	0,21	0,18	0,77
S_4	0,09	0,07	0,82
S_5	0,11	0,05	0,76
S_6	0,15	0,1	0,58

Note - Compiled by the author

Since the resulting data falls into the normal output layer, to validate the model, we can add some suspicious event to the normal operational data to determine the efficiency of the statistical processing.

Let us define in the model the designation of normal transactions carried out in banks. Let's say this designation will look like:

$$\psi_1(k) \to \max k\, \psi_1(k) \to \max k \quad (6)$$

Where k – amount of input data considered.

With this formulation of the question, suspicious transactions will be presented as follows:

$$\psi_2(k) = \psi_1(k) + \gamma_k(k) \quad (7)$$

where,

k=1,2,…200

γ - continuous measurement of the intensity of unusual transactions.

According to the analytical result of the experiment, we found this when the parameter α, which determines the grouping radius of the APC-III algorithm is lower than 1.04, the accuracy of the model is higher.

We selected 200 cases from the initial data mixed with 70 suspicious operations to study the model. As a result of statistical processing of banking operations, 90 operational data were included, of which 27 were suspicious. Using this model in the identification of suspicious transactions in banks, we offer parameters based on the APC-III clustering algorithm and least squares (RLS) method. So the model has three layers of data processed by banks: incoming, suspicious and outcoming. So the matrix is based on five measured points of inherent compliance risks: low, limited, moderate, significant, high. Consumer risk inherent compliance is the risk associated with banking products and services offered that could result in significant harm as a result of non-compliance with laws and regulations to protect consumer rights. Therefore, it is very important for the bank to effectively identify, measure, monitor and control its compliance risks in order to limit any potential negative consequences of non-compliance [18].

Banks that are engaged in more risky operations exhibit a higher risk tolerance and are expected to have a compliance management program commensurate with their risk profile. [19]. A higher risk tolerance may be reflected in product offerings that pose a greater threat of compliance. In general, a bank with a high reputation should assume the inherent compliance risk in its operations; stronger banks must effectively manage these risks. Many factors influence the level of systemic (inherent) risk compliance. Effective identification and assessment of this risk is an important part of the risk-focused research process [20].

Institutional profile involves discussion of information about the bank and its personnel, which need to determine the impact of institutional, legal, and environmental factors on the level of compliance risk. Considering these factors, it is possible to form a conclusion about the level of inherent compliance risk for each banking operation. The matrix identifies specific risk components for each of the three broad sources of risk (institutional, regulatory, and environmental). While a full assessment of risk compliance should be documented only for each operation, the matrix allows analysis of the potential level of risk associated with each source of risk, as well as each of the auxiliary risk components that are shown in the matrix. In this case, it is advisable to assign ratings first to individual auxiliary risk components and then develop total ratings.

Inherent compliance risk can be assessed based on a five-point rating system:

1. Low
2. Limited
3. Moderate
4. Significant
5. High

The low probability of a significant negative impact (1) indicates that compliance risk is unlikely to have a significant negative impact on the Bank or its clients before any mitigation of risk management processes is considered. The expected sanctions, losses or damage to reputation due to compliance risk will have a minor negative impact on the Bank. Limited probability of significant adverse impact (2) indicates that compliance risk, before considering any mitigating effects of risk management processes, may have a minor negative impact on the Bank or its customers. The expected penalties, losses or reputational damage associated with this risk are moderate and may be absorbed by the Bank in the normal course of business.

A moderate probability of significant negative impact (3) indicates that the expected sanctions, loss or damage to reputation due to compliance risk may have a negative impact on the bank.

The probability of significant negative impact (4) indicates that the expected sanctions, loss or damage to reputation due to compliance risk can seriously affect the bank. High (5) indicates a high probability that the expected sanctions, losses, or damage to reputation due to compliance risk will require significant changes in the management of the established practice and operations of the bank.

The matrix above includes standard elements of a risk management system:

1. Board and management oversight.
2. Policies, procedures and limits.
3. Risk monitoring and IIAs.
4. Internal control.

The matrix also includes a number of components that banks should consider when drawing conclusions about risk management, as appropriate. For each of the risk management elements, the matrix defines the number of related components that provide a more detailed analysis of risk management practices. The extent to which these components are present and should be documented as part of the analysis will vary depending on the complexity of each individual Bank. The following five-point system used to

evaluate compliance risk management. Ratings Risk Management :

Strong(1)
Fair (2)
Medium (3)
Ultimate (4)
Poor (5)

Strong (1) - compliance risk management exists when management determines effectively and controls all the main compliance risks arising from the activities of the bank. Management is fully prepared to address the risks arising from new products and changing market conditions. The Board of Directors and senior management are forward-looking and active participants in risk management. Management ensures that appropriate policies are in place and that there are limits that are reviewed and approved by the board. Risk management practices and bank infrastructure are flexible and respond to changing industry practices and current regulatory guidance. The staff has sufficient experience, knowledge and depth to manage risks. Internal control and audit procedures are quite comprehensive and correspond to the size and activities of the bank. The management effectively and accurately monitors the state of the bank, in accordance with compliance standards and in accordance with internal and supervisory policies and practices of the bank [21].

Satisfactory (2) - compliance risk management exists when the bank's risk management is largely effective, but not enough to a small extent. The management demonstrates responsiveness and ability to successfully cope with existing and predictable risks that may arise in the implementation of the bank's business plan. While a bank may have some minor risk management flaws, these problems have been recognized and are being addressed. In general, risks are controlled in a way that does not require more than normal observation. The bank's risk management strategy and infrastructure are satisfactory and generally adjusted accordingly in response to changes in industry practices and the existing regulatory framework. The experience of the staff is advisable to manage the risks taken by the institution. Internal controls may appear with minor flaws, but they may be fixed in the ordinary course of business. Supervisors may have recommendations for improvement, but should not have a significant impact on the bank's compliance position.

Medium (3) - compliance risk management exists when practice is lacking in some important areas and therefore causes significant attention.

Ultimate (4) - compliance risk management exists when practice is not able to identify, measure, control and manage significant exposure to risk in many significant respects. In general, this situation reflects a lack of adequate management and control by the board of directors and senior management. One or more of the four elements of risk management is inadequate and requires immediate and coordinated corrective action by the board of directors and senior management. The Bank may have serious weaknesses identified, such as a lack of independence or conflicting lines of authority, which require a significant improvement in internal control or better compliance with control standards or requirements. The lack of compliance risk management guarantees a high degree of attention oversight, because if not properly resolved, they can lead to serious sanctions, losses or damage to the bank's reputation.

Unsatisfactory (5) - compliance risk management exists as a critical lack of effective risk management methods in relation to identification, measurement, monitoring, control or serious exposure to risk. One or more of the four elements of risk management is considered completely inadequate, and the board and management have not demonstrated the ability to address these weaknesses. Internal controls are critically weak and therefore can seriously jeopardize the viability of the bank. There is a direct interest in the reliability of accounting and capacity regulation for sanctions and losses if corrective measures are not taken immediately. Deficiencies in the compliance risk management and internal control procedures require immediate and observant attention. According to the analysis of compliance control in Bank X, it was revealed that according to the compliance matrix the risk is rated as moderate and has an average rating. This means that one or more of the four elements of sound risk management (such as active supervision of directors and senior management; adequate policies, procedures and limits; adequate risk monitoring and IIAs; integrated internal control systems) are considered less acceptable, which prevented the bank from fully as one or more significant risks are resolved for their operations. The management of certain risks needs to be improved to ensure that management and the board of directors are able to identify, measure, monitor and control all significant risks for the organization. In addition, the risk management structure may need to be improved in areas of significant business activity (product or service), or the experience of employees cannot be commensurate with the scale and complexity of activities. In addition, management's decision to change existing compliance control practices may need to be improved. The internal control system may be absent in some important aspects, the weaknesses of compliance risk management can adversely affect the general situation of the bank and, as a result, if the management does not take the necessary measures, the bank cannot avoid sanctions, losses or damage to the reputation.

Conclusion

In our proposed model, the parameters are based on the APC-III clustering algorithm and

the least squares method with some updates in accordance with the OECD recommendations. The model assumes the presence of three layers of information processed by banks: incoming, suspicious and outgoing. The analysis made it possible to reveal that, on average, about 25-40% of banks' operations can be classified as suspicious, and therefore requiring a thorough study.

In our case, we selected 200 cases from the original data mixed with 70 suspicious transactions to study the model. As a result of statistical processing of banking operations, 90 operational data were identified, of which 27 turned out to be suspicious.

The inherent risk of compliance, according to the matrix, can be assessed on the basis of a five-point rating system: low, limited, moderate, significant, high. In our case, it turned out that almost 30% of the reviewed transactions were classified as suspicious. As a result of submitting this information, the bank was able to identify 19 transactions aimed at money laundering.

This approach requires banks to work together with the country's government to counter money laundering and ensure the financial security of banks.

Overall, this model shows promising results in identifying suspicious transactions in banks. At the same time, the authors consider the possibility of further studying the possibilities of using the presented model and its improvement for the purpose of increasing the efficiency of monitoring the financial security of banks and promoting anti-money laundering through banking operations.

References

1. Alpysbayev K.S. O natsional'noy sisteme protivodeystviya legalizatsii dokhodov, poluchennykh prestupnym putem (na materialakh Kazakhstana) // Izvestiya SPbGEU. 2017. - №4 (106). – S.11-115.

2. Chernikova L.I., Zayernyuk V.M. Rol' bankovskogo sektora v bor'be s otmyvaniyem deneg: otechestvennyy i zarubezhnyy opyt // Natsional'nyye interesy: prioritety i bezopasnost'. 2012. №18. – S.46-54.

3. Karanina E. V., Blednykh O. I. Financial security as a component of the concept of economic security of the state / / The Genesis of Genius. 2016. no. 6. Pp. 94-99

4. Averyanova Yu. g. Theoretical aspects of financial security of a commercial Bank // Economic Sciences, 2011, no. 4, Pp. 220-225.

5. Chong, A., Lopez-De-Silanes, F.: Money laundering and its regulation. Economics & Politics. 27(1), 78–123 (2015). doi:10.1111/ecpo.12051

6. Sat, D.M., Krylov, G.O., Bezverbnyi, K.E., Kasatkin, A.B., Kornev, I.A.: Investigation of money laundering methods through cryptocurrency. Journal of Theoretical and Applied Information Technology. 83(2), 244–254.

7. Teichmann, F.M.J.: Twelve methods of money laundering. Journal of Money Laundering Control. 20(2), 130–137 (2017). doi:10.1108/jmlc-05-2016-0018

8. Melnik D.Yu. (2018). Basic elements and main components of a bank economic safety. The Eurasian Scientific Journal, [online] 4 (10). Available at: https://esj.today/PDF/13ECVN418.pdf (in Russian)

9. Serdyuk V.A. New in protection against hacking of corporate systems / V.A. Serdyuk. - M .: Technosphere, 2007. - 360 p.

10. Pramod, V., Li, J., Gao, P.: A framework for preventing money laundering in banks. Information Management & Computer Security. 20(3), 170–183 (2012). doi:10.1108/09685221211247280

11. Gayduk Vladimir Ivanovich, Vorokov Anzor Ladinovich, Gayduk Natal'ya Viktorovna Finansovaya bezopasnost' kommercheskikh bankov: kriterii i indikatory // Nauchnyy zhurnal KubGAU - Scientific Journal of KubSAU. 2015. №114. URL: https://cyberleninka.ru/article/n/finansovaya-bezopasnost-kommercheskih-bankov-kriterii-i-indikatory (дата обращения: 28.09.2020).

12. Evseev S.P. A Synergistic approach to assessing the security of banking systems // Information processing systems, 2016, issue 4 (141). - S.90-103.

13. Kozminykh S.I. Mathematical modeling of ensuring complex security of objects of informatization of the credit and financial sphere // Issues of cybersecurity, 2018. -№1 (25) -. - S.54-63.

14. Mukhopadhyay, A., Chatterjee, S., Bagchi, KK et al. Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. Inf Syst Front 21, 997-1018 (2019). https://doi.org/10.1007/s10796-017-9808-5

15. Official website of the OECD [Electronic resource]//http://www.oecd-ilibrary.org/

16. Honghong Duan, Jie Jia, Ruifeng Ding Two-stage recursive least squares parameter estimation algorithm for output error models// Mathematical and Computer Modelling Volume 55, Issues 3–4, February 2012, Pages 1151-1159.

17. Benesty J., Paleologu C., Gänsler T., Ciochină S. (2011) Recursive Least-Squares Algorithms. In: A Perspective on Stereophonic Acoustic Echo Cancellation. Springer Topics in Signal Processing, vol 4. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22574-1_6

18. Rafal Drezewskia, Jan Sepielaka, Wojciech Filipkowskib, System supporting money laundering detection // Digital Investigation, 2012. – Vol.9(1). – pp. 8-21.//http://dx.doi.ofg/10.1016/j.diin.2012.04.003

19. Shaten P. L. Prevention of money laundering and terrorist financing: a practical guide for banking professionals-Moscow: Alpina publishers, 2011. – 316p.//https://openknowledge.worldbank.org bitstream/handle/10986/2638/488950PUB00RUS00Box0361504B0PUBLIC0.pdf?sequence=7&isAllowed=y

20. Bonnie Buchanana, Money laundering-a global obstacle [Electronic source] // Research in International Business and Finance, 2004. – Vol. 18(1). – pp. 115-127. - //http://dx.doi.org/l0.1016/j.ribaf.2004.02.001.

21. Shijia Gao, Dongming Xu, Coneeptual modeling and development of an intelligent agent-assisted decision support system for anti-money laundering // Expert Systems with Applications, 2009. – Vol. 36 (2). – pp. 1493-1504 // http// dx.doi.org/10.1016/j.eswa.2007.11.059.

Information about the authors

Azhar Z. Nurmagambetova – corresponding author, Kazakh National University named after Al-Farabi, Almaty, Kazakhstan, e-mail:azhar.nurmagambetova@kaznu.kz

Sunkar Z. Nurmagambetov – Kazakh Economic University named after T. Ryskulov, Almaty, Kazakhstan

Aziya G. Mukusheva – Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan, e-mail:mukushevaaziya@gmail.com, ORCID iD: https://orcid.org/0000-0003-1952-5301

Авторлар туралы мәліметтер

Нурмагамбетова А.З. - хат-хабаршы авторы, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, e-mail:azhar.nurmagambetova@kaznu.kz

Нурмагамбетов С.З. - Т. Рысқұлов атындағы Қазақ экономикалық университеті, Алматы, Қазақстан

Мукушева А.Г. - Гумилев атындағы Еуразия ұлттық университеті, Нұр-Султан, e-mail: mukushevaaziya@gmail.com, ORCID iD: https://orcid.org/0000-0003-1952-5301

Дата поступления рукописи: 13.05.2020.
Прошла рецензирование: 25.09.2020.
Принято решение о публикации: 10.10.2020.

Received: 13.05.2020
Reviewed: 25.09.2020
Accepted: 10.10.2020.

Қарастыруға қабылданды: 13.05.2020.
Рецензиялауды өтті: 25.09.2020
Жариялауға қабылданды: 10.10.2020.