Business Process Model for Monitoring the Automatic Payments in the "Client-Bank" System

OLHA V. KUZMENKO[i], *SERHII V. MYNENKO*[ii], *SERHII V. LYEONOV*[iii], *ALEKSY S. KWILINSKI*[iv]

The innovative development of banking presupposes modernization in the approaches to anti-money laundering. The article considers the issue of financial monitoring of banking operations without bank employees' participation through the "Client-Bank" system. Two models for monitoring the automatic payments in the "Client-Bank" system are identified. The list of functions performed by the "Client-Bank" system in terms of types of clients: individuals and legal entities (including individuals-entrepreneurs) was determined. The first model describes general indicators of transactions that have the risk of money laundering. The second model focuses on the specific features of the "Client-Bank" system functionality for legal entities or individual entrepreneurs. Several criteria for the riskiness of the operation in terms of money laundering are considered. The developed business process model takes into account the verification of the participant's affiliation to countries that do not implement or improperly implement the recommendations of intergovernmental organizations, the participant's affiliation to politically significant or related persons and the withdrawal of capital abroad, including offshore areas . In addition, checks of financial condition of counterparties, regularity of receipts of payments and cash withdrawals, circulation of foreign currency, loan repayment, receipt of a significant amount of cash, ip-address of the client and description of the transaction are included. A feature of the business model for legal entities is the verification of NACE compliance, analysis of the number of contractors, analysis of the timeliness of tax payments. Directions for further development of this study identify the possibility of intellectualizing the financial monitoring system and improving the regulatory framework in the system "Client-Bank" to enhance the system of anti-money laundering in banking institutions.

Keywords: anti-money laundering, "Client-bank" systems, risks of the bank, bank, financial monitoring.

УДК 336.71:004.738.5 *JEL Codes:* G21,G24

Introduction. In recent years, the financial services market has been characterized by the development of FinTech innovations. Annually, new information technologies are introduced into the banking system. They are designed to meet the needs of as many customers as possible. However, the expansion of financial services, which begin to be online, the bank employees' work is simplified and there is a higher risk to use these tools for money laundering. Therefore, there is a problem to improve the internal system of financial monitoring, considering the peculiarities of the latest financial technologies [1].

[i] *Olha V. Kuzmenko,* Dr.Sc. (Economics), Professor, Head of the Department of Economic Cybernetics, Sumy State University;

[ii] Serhii *V. Mynenko*, PhD student (Economics), Department of Economic Cybernetics, Sumy State University;

[iii] Serhii *V. Lyeonov*, Dr.Sc. (Economics), Professor, Professor of the Department of Economic Cybernetics, Sumy State University;

[iv] Aleksy *S. Kwilinski*, Dr.Sc. (Economics), Professor of the Department of Marketing, Sumy State University.

https://doi.org/10.21272/mer.2021.91.02

Problem statement. The following domestic and foreign scientists considered this issue: Kuzmenko O. V., Yarovenko G. M., Boyko A. O. [1, 21], Stechishin T. B. [20], Dmitrov S. O., Medvid T. [1], Serbina O. G., Zaguzova O. M. [18], Tropina T. [22], Singh K., Best P. [19].

Due to lack of time, the employees from financial monitoring department cannot analyze every transaction in the system in detail. Given the significant number of transactions carried out by customers through the system "Client-Bank", it is necessary to verify their eligibility automatically. The basis of the relevant software solution is to form the business process to monitor the automatic payments.

The purpose of the article is to form a business process for automatic monitoring of payments through the system "Client-Bank".

Results of the research. The main form of banking customer service in the development of FinTech is "Client-Bank". It provides customers with the ability to obtain financial information and control bank accounts remotely. From a technical point of view, "Client-Bank" is a system or platform that combines financial tools to control the account and access to banking services [14].

For an individual client, the "Client-Bank" usually has the following functions:

1) Creating an application for a credit limit / cash loan / credit card;

2) Opening and closing of the current accounts (both in national and foreign currencies), deposit / savings accounts;

3) Ordering cards, changing the level of packages;

4) Repayment of credit debt;

5) Creation of payment orders;

6) Execution of payments in the national currency (utility, from account to account, from card to card, etc.)

7) Receiving money transfers;

8) Formation of information on the movement of funds on the account;

9) Using of account statements of different levels;

10) Carrying out transactions for the purchase and sale of foreign currency;

11) Carrying out operations on the domestic government bonds;

12) Communication with technical support via chat;

13) Formation of cost statistics by areas.

If one considers the functionality of the bank's client for a legal entity and a person-entrepreneur, it will be similar to individuals, but it is necessary to consider these economic entities' peculiarities. The functions of the "Client-Bank" may have a limited or specific nature. It is necessary to add the following functions to the above:

1) Running the salary project;

2) Execution of payments in national and foreign currency;

3) Transfer of supporting documents (invoices, acts of work performed) to the bank;

4) Working with acquiring

Given the differences in the construction of such system as "Client-Bank" for individuals and for legal entities (including persons-entrepreneurs), it is necessary to separate the business process model for monitoring the automatic payments to be made through the system "Client-Bank", depending on the type of economic agents.

In general, the business process of determining the transaction to be financially monitored is shown in Figure 1.

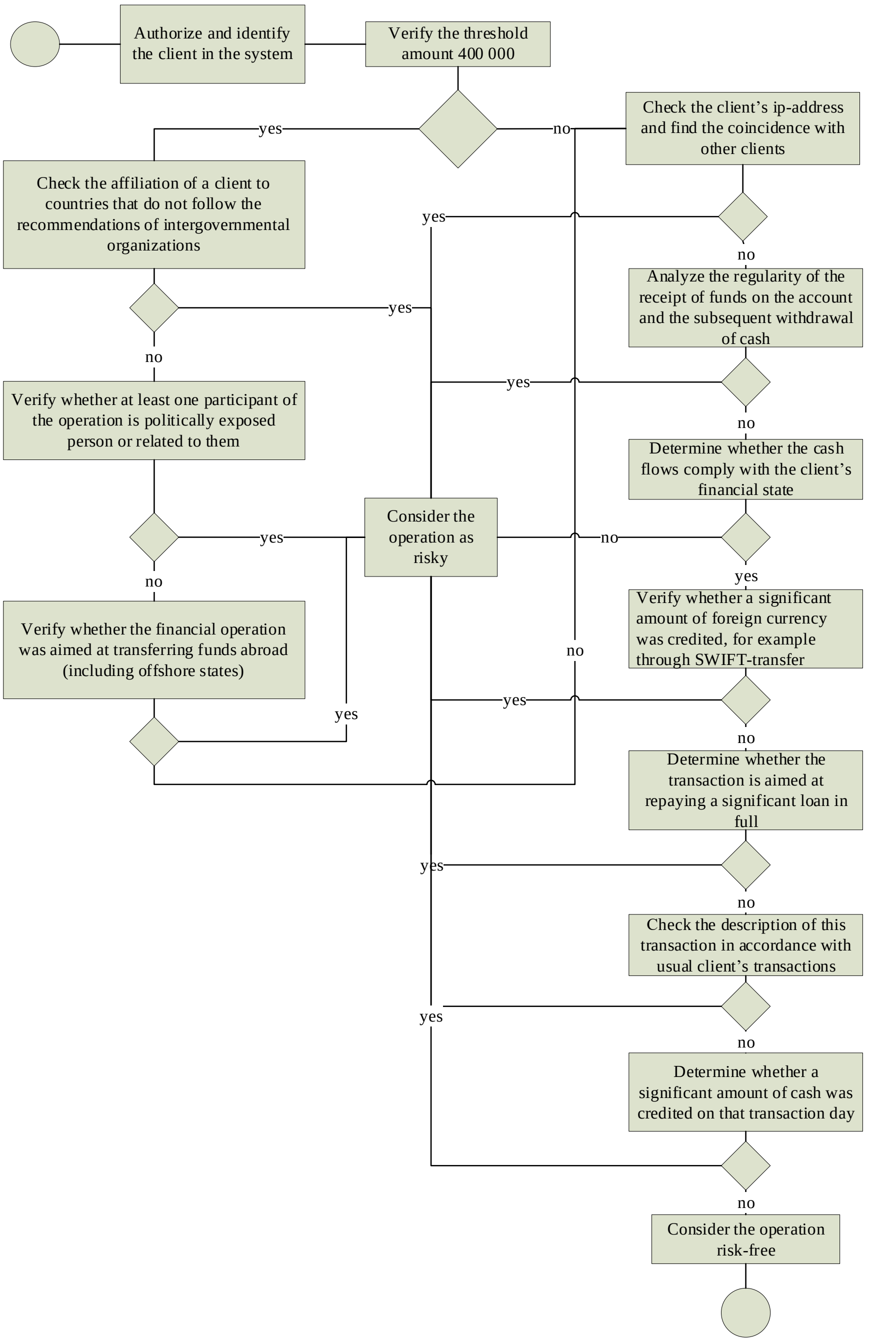
Authorize and identify the client in the system
Verify the threshold amount 400 000
yes
no
Check the client's ip-address and find the coincidence with other clients
Check the affiliation of a client to countries that do not follow the recommendations of intergovernmental organizations
yes
no
Analyze the regularity of the receipt of funds on the account and the subsequent withdrawal of cash
yes
no
Verify whether at least one participant of the operation is politically exposed person or related to them
yes
no
Determine whether the cash flows comply with the client's financial state
Consider the operation as risky
yes
no
no
yes
Verify whether the financial operation was aimed at transferring funds abroad (including offshore states)
Verify whether a significant amount of foreign currency was credited, for example through SWIFT-transfer
no
yes
yes
no
Determine whether the transaction is aimed at repaying a significant loan in full
yes
no
Check the description of this transaction in accordance with usual client's transactions
yes
no
Determine whether a significant amount of cash was credited on that transaction day
no
Consider the operation risk-free

Figure 1. Business process model for determining a risky financial transaction in an automated financial monitoring system carried out through the "Client-Bank"
[Compiled by the authors based on [26, 27, 25, 24, 23, 11]

While considering Figure 1 in more detail, there is the client's authorization and identification in the system before entering it. Using personal login and password, or an electronic key, the client gets access to the functionality of the "Client-Bank" system. The next step is to check the threshold amount of the transaction carried out by the client through the system, defined at 400.000 UAH by the Law of Ukraine "On Prevention and Counteraction to Money Legalization (Laundering), Terrorist Financing and Proliferation of Mass Destruction Weapons" [16]. If the transaction amount exceeds UAH 400.000, the client's inspections specified by the Law are launched. The affiliation of a client or counterparty to countries that do not follow the recommendations of intergovernmental organizations to prevent money laundering is checked [28, 4, 2]. Such transactions may include receiving or sending a SWIFT payment equivalent to UAH 400.000 to Iran or the Democratic People's Republic of Korea (DPRK) (as of 2020, these countries are in the High-Risk Jurisdictions subject to a Call for Action from the FATF) [8]. In addition, banks may consider the transactions risky which are carried out in countries of Jurisdictions under Increased Monitoring FATF. These countries actively cooperate with the FATF to eliminate shortcomings in national systems to prevent money laundering. As of 2020, this list included Albania, The Bahamas, Barbados, Botswana, Cambodia, Ghana, Iceland, Jamaica, Mauritius, Mongolia, Myanmar, Nicaragua, Pakistan, Panama, Syria, Uganda, Yemen, Zimbabwe [9].

The next step is to verify that the participants in the transaction are politically significant or related persons. It is carried out in its database and from an open database, for example, the Center for Counteraction to Corruption "Register of National Public Figures of Ukraine" [17]. The next criterion is the transfer or receipt of funds from countries that belong to offshore areas. The Cabinet of Ministers of Ukraine determines the full list of offshore zones [15].

If any of the above criteria meets the transaction over 400.000, it is risky, and there is a notification to the regulatory authorities.

If the amount is less than the threshold or none of these conditions is met, the following checks, defined in the Typological Studies of the SCFM, are launched [26, 27, 25, 24, 23].

The client's IP address is checked in this way. It will be a risky transaction if other clients often make transactions from this IP address or if the client's counterparty also uses this IP address. It is almost impossible, and therefore, illegal activity occurs.

The next important criterion is frequent cash inflows with their subsequent transfer to another account or cash withdrawal. Such transactions risk being part of the money-laundering scheme, including concealing the ultimate beneficial owner of funds [11, 1].

The next identifier is the crediting of funds in foreign currency. After that, the purpose of transactions is checked for unusual descriptions for this client. For example, if a customer usually receives a credit in the form of salary and spends money on food and household goods, suddenly begins to receive and transfer significant funds for gifts, services, which are difficult to verify [10, 3].

The scheme considered in Figure 1 covers customers of individuals. However, customers of legal entities (individuals – entrepreneurs) have their unique functions in the system "Customer-Bank", which will be considered in Figure 2.

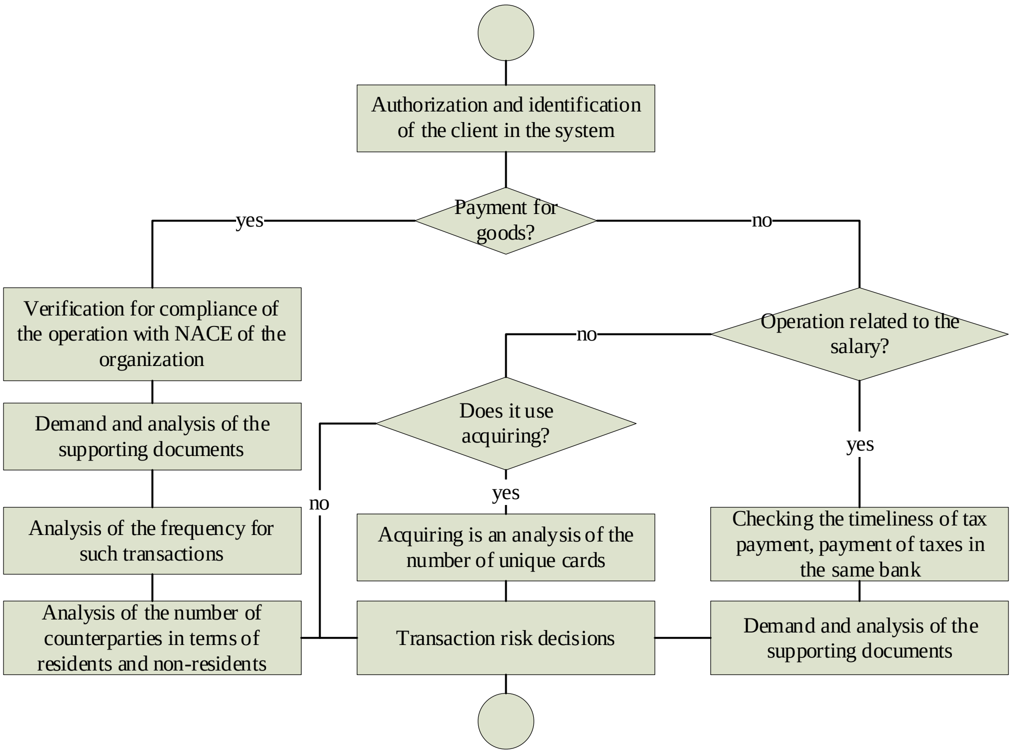
Authorization and identification of the client in the system
Payment for goods?
yes
no
Verification for compliance of the operation with NACE of the organization
Demand and analysis of the supporting documents
Analysis of the frequency for such transactions
Analysis of the number of counterparties in terms of residents and non-residents
Operation related to the salary?
no
yes
Does it use acquiring?
no
yes
Acquiring is an analysis of the number of unique cards
Checking the timeliness of tax payment, payment of taxes in the same bank
Transaction risk decisions
Demand and analysis of the supporting documents

Figure 2. Business process model for defining a risky financial transaction in an automated financial system, carried out through the "Client-Bank" of a legal entity (individual entrepreneur)
[compiled by the authors based on [26, 27, 25, 24, 23, 11]

Figure 2 shows that the system of monitoring transactions carried out through the "Client-Bank" for a legal entity (individual entrepreneur) checks whether the transaction is a payment for goods or services immediately after authorization and identification [7].

If "yes", the coincidence of this operation is checked by the NACE of the organization. If necessary, the system may require supporting documents. The frequency of such transactions is also checked: if this transaction occurs infrequently, it can be risky. The counterparties are also analyzed. If there is a frequent change of non-resident counterparties, or for example a newly created organization has many non-resident counterparties [6].

If the transaction involves a salary, it is important to check whether taxes have been paid. Unpaid or late taxes can point the fictitious activities of the organization. Such an organization can be part of a conversion center.

Then, when using acquiring, it is important to check the frequency to use cards and the number of unique cards. If the calculations are made using the same cards, and their number is small – most likely the organization is part of the conversion center [13].

Conclusions and prospects for further research. The use of innovative technologies leads to new challenges in money laundering control. The introduction of the "Client-Bank" system in customer service helps banks to retain customers, provide services online, automate the work of some processes and, as a result, free up working time. The considered business process model for monitoring the automatic payments carried out by economic agents through the Client-Bank system will reveal operations on money laundering at an early stage.

Prospects for further research consist of the possibilities to intellectualize algorithms for analyzing transaction assignments to identify the attackers' semantic advantages. Besides, it is objective to improve the business process model at the regulatory level. Currently, the systems of "Client-Bank" in each banking institution are configured according to internal recommendations. Therefore, this model can work in each bank in its way. Due to this, the unification of regulatory documentation for the "Client-Bank" systems becomes relevant.

Acknowledgements. The article was prepared based on the results of a study funded by the National Research Fund of Ukraine "Optimization and automation of financial monitoring processes to increase information security in Ukraine ". (registration number: 0120U104810).

References

1. Belen Suarez Lopez, David Issó García, Antonio Vargas Alcaide (2019). Blockchain Technology Facing Socioeconomic Challenges. Promise versus Probability. *SocioEconomic Challenges, 3*(4), 13-24. Retrieved from http://doi.org/10.21272/sec.3(4).13-24.2019
2. Buriak, An. & Artemenko, Al. (2018). Reputation risk in banking: application for Ukraine. *Financial Markets, Institutions and Risks, 2*(2), 100-110. Retrieved from https://doi.org/10.21272/fmir.2(2).100-110.2018
3. Demkiv, Yu. M. (2018). The ISO 9001 International Standards in a System of the Banking Services Quality Management. *Business Ethics and Leadership, 2*(3), 94-102. Retrieved from https://doi.org/10.21272/bel.2(3).94-102.2018
4. Djalilov, Kh., Ngoc Lam, T. (2019). Ownership, Risk and Efficiency in the Banking Sector of the ASEAN Countries. *Financial Markets, Institutions and Risks, 3*(2), 5-16. Retrieved from http://doi.org/10.21272/fmir.3(2).5-16.2019
5. Dmytrov, S., Medvid, T. (2017). An approach to the use of indices-based analysis subject to money laundering and terrorist financing national risk assessment. *SocioEconomic Challenges, 1*(1), 35-47. Retrieved from http://doi.org/10.21272/sec.2017.1-04
6. Dmytrov, S., Merenkova, O., & Levchenko, L. (2009). Modeliuvannia otsinky ryzykiv vykorystannia posluh bankiv z metoiu lehalizatsii kryminalnykh dokhodiv abo finansuvannia teroryzmu [Modeling of risk assessment of the use of bank services on the issues of money laundering or terrorist financing]. *Visnyk Natsionalnoho banku Ukrainy – Bulletin of the National Bank of Ukraine*. 1. 54-59 [in Ukrainian]
7. Dudchenko, V. Yu. (2020). Interaction of Central Bank Independence and Transparency: Bibliometric Analysis. *Business Ethics and Leadership, 4*(2), 109-115. Retrieved from https://doi.org/10.21272/bel.4(2).109-115.2020
8. High-Risk Jurisdictions subject to a Call for Action – 21 February 2020. *FATF.* Retrieved from https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html
9. Jurisdictions under Increased Monitoring – 21 February 2020. *FATF*. Retrieved from https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html
10. Karaoulanis, A. (2018). Big Data, What Is It, Its Limits and Implications in Contemporary Life. *Business Ethics and Leadership, 2*(4), 108-114. Retrieved from http://doi.org/10.21272/bel.2(4).108-114.2018
11. Kerivni nastanovy shchodo rozkryttia informatsii pro kintsevykh benefitsiarnykh vlasnykiv [Guidelines for Disclosure of Information on Final Beneficiary Owners]. Retrieved from https://fiu.gov.ua/assets/userfiles/340/201209_1707_170x240_KerivniNastanovy.pdf [in Ukrainian].
12. Kuzmenko, O. V., Yarovenko, H. M., Boyko, A. O. & Mynenko, S. V. (2019). Rozrobka biznes-modelei protsesiv finansovoho monitorynhu ekonomichnykh ahentiv [Development of business models of financial monitoring processes of economic agents]. *Efektyvna ekonomika – Efficient*

economy, 12. Retrieved from https://doi.org/10.32702/2307-2105-2019.12.4 [in Ukrainian]

13. Mynenko, S. V., Kuzmenko, O. V., Yarovenko, H. M., Levchenko, V. P. (2019) Avtomatyzatsiia protsesu finansovoho monitorynhu lehalizatsii koshtiv, otrymanykh nezakonnym shliakhom [Automation of the process of financial monitoring of legalization of illegally acquired money]. *Naukovi zapysky Natsionalnoho universytetu "Ostrozka akademiia". Seriia "Ekonomika": naukovyi zhurnal – Scientific notes of the National University "Ostroh Academy". Series "Economics": a scientific journal*, *15(43)*. 162-171. Retrieved from https://eprints.oa.edu.ua/id/eprint/8069 [in Ukrainian].
14. Oliinyk, A. V. & Shatska, V. M. (2006). *Informatsiini systemy i tekhnolohii u finansovykh ustanovakh: navch. posibn. [Information systems and technologies in financial institutions: a textbook]*. Lviv: "Novyi svit – 2000" [in Ukrainian].
15. Pro vidnesennia derzhav do pereliku ofshornykh zon [On the inclusion of states in the list of offshore zones] (2011). *Verkhovna Rada Ukrainy – Verkhovna Rada of Ukraine*, 143. Retrieved from https://zakon.rada.gov.ua/laws/show/143-2011-%D1%80#Text [in Ukrainian].
16. Pro zapobihannia ta protydiiu lehalizatsii (vidmyvanniu) dokhodiv, oderzhanykh zlochynnym shliakhom, finansuvanniu teroryzmu ta finansuvanniu rozpovsiudzhennia zbroi masovoho znyshchennia [On prevention and counteraction to legalization (laundering) of proceeds from crime. financing of terrorism and financing of proliferation of weapons of mass destruction] (2020). *Verkhovna Rada Ukrainy – Verkhovna Rada of Ukraine*, *25* Retrieved from https://zakon.rada.gov.ua/laws/show/361-20#Text [in Ukrainian].
17. Reiestr natsionalnykh publichnykh diiachiv Ukrainy [Register of national public figures of Ukraine]. *PEP*. Retrieved from https://pep.org.ua/uk/data/ [in Ukrainian].
18. Serbyna, O. H. & Zahuzova, O. M. (2014). Internet-bankinh: ukrainska praktyka ta svitovyi dosvid [Internet banking: Ukrainian practice and world experience]. *Molodyi vchenyi – Young scientist, 4*. 122-125. Retrieved from http://molodyvcheny.in.ua/files/journal/2014/4/34.pdf [in Ukrainian].
19. Singh, K. & Best, P. (2019). Anti-Money Laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems, 34*. Retrieved from https://doi.org/10.1016/j.accinf.2019.06.001
20. Stechyshyn, T. B. (2014). Problemy formuvannia systemy finansovoho monitorynhu v bankivskii sferi Ukrainy [Problems of formation of the system of financial monitoring in the banking sphere of Ukraine]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu – Scientific Bulletin of Kherson State University*, *8*. 183-187. Retrieved from http://dspace.wunu.edu.ua/jspui/handle/316497/3604 [in Ukrainian].
21. Subeh, M. A., Boiko, A. (2017). Modeling efficiency of the State Financial Monitoring Service in the context of counteraction to money laundering and terrorism financing. *SocioEconomic Challenges, 1*(2), 39-51. Retrieved from http://doi.org/10.21272/sec.1(2).39-51.2017
22. Tropina, T. (2014). Fighting money laundering in the age of online banking, virtual currencies and internet gambling. *ERA Forum, 15*. 69-84. Retrieved from https://doi.org/10.1007/s12027-014-0335-2
23. Typolohichne doslidzhennia "Aktualni metody i sposoby lehalizatsii (vidmyvannia) dokhodiv, oderzhanykh zlochynnym shliakhom, ta finansuvannia teroryzmu" (2012) [Typological study "Actual methods and ways of legalization (laundering) of proceeds from crime and terrorist financing"]. *Derzhavna sluzhba finansovoho monytorynhu – State Financial Monitoring Service*. Retrieved from https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu/tipologichne-doslidzhennya-aktualni-metodi-i-sposobi-legalizacziji-vidmivannya-doxodiv-oderzhanix-zlochinnim-shlyaxom-ta-finansuvannya-terorizmu.html [in Ukrainian].
24. Typolohichne doslidzhennia "Kiberzlochynnist ta vidmyvannia koshtiv» (2013) [Typological study «Cybercrime and money laundering"]. *Derzhavna sluzhba finansovoho monytorynhu – State Financial Monitoring Service.* Retrieved from https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu/tipologichne-doslidzhennya-kiberzlochinnist-ta-vidmivannya-koshtiv.html [in Ukrainian].
25. Typolohichne doslidzhennia "Ryzyky vykorystannia subiektiv z neprozoroiu strukturoiu vlasnosti u

skhemakh vidmyvannia kryminalnykh dokhodiv" (2018) [Typological study "Risks of using entities with non-transparent ownership structure in money laundering schemes"]. *Derzhavna sluzhba finansovoho monytorynhu – State Financial Monitoring Service.* Retrieved from https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu/tipologichne-doslidzhennya-riziki-vikoristannya-sub-jektiv-z-neprozoroyu-strukturoyu-vlasnosti-u-sxemax-vidmivannya-kriminalnix-doxodiv.html [in Ukrainian].

26. Typolohichne doslidzhennia "Vidmyvannia dokhodiv vid podatkovykh zlochyniv» (2020). [Typological study «Money laundering from tax crimes"]. *Derzhavna sluzhba finansovoho monytorynhu – State Financial Monitoring Service.* Retrieved from https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu/tipologichne-doslidzhennya-vidmivannya-doxodiv-vid-podatkovix-zlochiniv-2020-rik.html [in Ukrainian].
27. Typolohichne doslidzhennia "Vidmyvannia dokhodiv vid pryvlasnennia koshtiv i maina derzhavnykh pidpryiemstv ta inshykh subiektiv, yaki finansuiutsia za rakhunok derzhavnoho ta mistsevykh biudzhetiv" (2019) [Typological study "Money laundering from the misappropriation of funds and property of state enterprises and other entities financed by the state and local budgets"]. *Derzhavna sluzhba finansovoho monytorynhu – State Financial Monitoring Service.* Retrieved from https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu/tipologichne-doslidzhennya-vidmivannya-doxodiv-vid-privlasnennya-koshtiv-i-majna-derzhavnix-pidprijemstv-ta-inshix-sub-jektiv-yaki-finansuyutsya-za-raxunok-derzhavnogo-ta-misczevix-byudzhetiv.html [in Ukrainian].
28. Yarovenko, H., Kuzmenko, O., Stumpo, M. (2020). Strategy for Determining Country Ranking by Level of Cybersecurity. *Financial Markets, Institutions and Risks, 4*(3), 124-137. Retrieved from https://doi.org/10.21272/fmir.4(3).124-137.2020

Manuscript received 24 December 2020

Mechanism of Economic Regulation, 2021, No 1, 17–27
ISSN 1726-8699 (print)

Модель бізнес-процесу автоматизованого моніторингу платежів у системі «Клієнт-Банк»

***Ольга Віталіївна Кузьменко* [*],**
***Сергій Володимирович Миненко* [**],**
***Сергій В'ячеславович Лєонов* [***],**
***Алексій Станиславович Квілінський* [****]**

[*] *доктор економічних наук, професор, професор кафедри економічної кібернетики*
Сумського державного університету,
вул. Р.-Корсакова, 2, м. Суми, 40007, Україна,
тел.: 380-542-665023, e-mail: o.kuzmenko@uabs.sumdu.edu.ua

[**] *аспірант кафедри економічної кібернетики Сумського державного університету,*
вул. Р.-Корсакова, 2, м. Суми, 40007, Україна,
тел.: 380-542-665023, e-mail: s.minenko@uabs.sumdu.edu.ua

[***] *доктор економічних наук, професор, професор кафедри економічної кібернетики*
Сумського державного університету,
вул. Р.-Корсакова, 2, м. Суми, 40007, Україна,
тел.: 380-542-665023, e-mail: s.lieonov@uabs.sumdu.edu.ua

[****] *доктор економічних наук, професор кафедри маркетингу*
Сумського державного університету,
вул. Р.-Корсакова, 2, м. Суми, 40007, Україна,
тел.: 380-542-687935, e-mail: a.kwilinski@london-asb.co.uk

Інноваційний розвиток банківської діяльності зумовлює модернізацію у підходах до протидії легалізації доходів, отриманих незаконним шляхом. В статті розглядається питання фінансового моніторингу банківських операцій, які відбуваються без участі працівника банку через систему «Клієнт-банк». Було визначено перелік функцій, які виконує система «Клієнт-банк» в розрізі типів клієнтів: фізичних та юридичних осіб (в тому числі фізичних-осіб підприємців). Було виділено дві моделі бізнес-процесу автоматизованого моніторингу платежів, здійснених у системі «Клієнт-банк». Перша побудована модель описує загальні індикатори транзакцій, які мають ризик легалізації доходів, отриманих незаконним шляхом. Друга – фокусується на специфічних особливостях функціоналу системи «Клієнт-банк» для юридичних осіб чи для фізичних осіб-підприємців. Було розглянуто ряд критеріїв ризиковості операції з точки зору легалізації кримінальних доходів. Розроблена модель бізнес-процесу враховує перевірку на приналежність учасника операції до країн, які не виконують чи неналежним чином виконують рекомендації міжурядових організацій, приналежність учасника до політично значущих чи пов'язаних з ними осіб та на виведення капіталу за кордон, в тому числі до офшорних зон. Окрім цього, включені перевірки фінансового стану контрагентів, регулярності надходження платежів та зняття готівки, обігу іноземної валюти, погашення кредиту, надходження значної суми готівки, IP-адреси клієнта та опису транзакції. Особливістю бізнес-моделі для юридичних осіб визначено перевірку відповідності КВЕД, аналіз кількості контрагентів, аналіз своєчасності сплати податків. Напрямками подальшого розвитку даного дослідження визначено можливість інтелектуалізації системи фінансового моніторингу та удосконалення нормативно-правової бази у сфері діяльності систем типу «Клієнт-банк» з метою покращення системи протидії легалізації кримінальних доходів у банківських установах.

Ключові слова: протидія легалізації кримінальних доходів, системи «Клієнт-банк», ризики банку, банк, фінансовий моніторинг.

JEL Codes: G21,G24 Figure: *2*; References: *28*

Language of the article: English

Література

1. *Belen* Suarez Lopez, David Issó García, Antonio Vargas Alcaide. Blockchain Technology Facing Socioeconomic Challenges. Promise versus Probability. SocioEconomic Challenges. 2019. 3(4). 13−24. http://doi.org/10.21272/sec.3(4).13-24.2019.
2. *Buriak, An.*, Artemenko, Al. Reputation risk in banking: application for Ukraine. Financial Markets, Institutions and Risks, 2018. 2(2), 100−110. DOI: 10.21272/fmir.2(2).100-110.2018
3. *Demkiv, Yu. M.* The ISO 9001 International Standards in a System of the Banking Services Quality Management. Business Ethics and Leadership, 2018. 2(3), 94−102. DOI: 10.21272/bel.2(3).94-102.2018
4. *Djalilov, Kh.*, Ngoc Lam, T. Ownership, Risk and Efficiency in the Banking Sector of the ASEAN Countries. Financial Markets, Institutions and Risks, 2019. 3(2), 5−16. http://doi.org/10.21272/fmir.3(2).5-16.2019.
5. *Dmytrov, S.*, Medvid, T. An approach to the use of indices-based analysis subject to money laundering and terrorist financing national risk assessment SocioEconomic Challenges, 2017. 1(1), 35−47. http://doi.org/10.21272/sec.2017.1-04.
6. *Дмитров, С.*, Меренкова, О., Левченко, Л. Моделювання оцінки ризиків використання послуг банків з метою легалізації кримінальних доходів або фінансування тероризму. Вісник Національного банку України. 2009. № 1. С. 54‒59.
7. *Dudchenko, V. Yu.* Interaction of Central Bank Independence and Transparency: Bibliometric Analysis. Business Ethics and Leadership, 2020. 4(2), 109−115. https://doi.org/10.21272/bel.4(2).109-115.2020
8. *High-Risk* Jurisdictions subject to a Call for Action – 21 February 2020. URL: https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html

9. *Jurisdictions* under Increased Monitoring – 21 February 2020. URL: https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html
10. *Karaoulanis, A.* Big Data, What Is It, Its Limits and Implications in Contemporary Life. Business Ethics and Leadership, 2018. 2(4), 108−114. http://doi.org/10.21272/bel.2(4).108-114.2018
11. *Керівні* настанови щодо розкриття інформації про кінцевих бенефіціарних власників. URL: https://fiu.gov.ua/assets/userfiles/340/201209_1707_170x240_KerivniNastanovy.pdf
12. *Кузьменко О. В.*, Яровенко Г. М., Бойко А. О., Миненко С. В. Розробка бізнес-моделей процесів фінансового моніторингу економічних агентів. Ефективна економіка, 2019. № 12(2019). DOI: https://doi.org/10.32702/2307-2105-2019.12.4
13. *Миненко С.В.*, Кузьменко О. В., Яровенко Г. М., Левченко В. П. Автоматизація процесу фінансового моніторингу легалізації коштів, отриманих незаконним шляхом (Automation of the process of financial monitoring of legalization of illegally acquired money). Наукові записки Національного університету «Острозька академія». Серія «Економіка» : науковий журнал 2019. (15(43)). с. 162−171. https://eprints.oa.edu.ua/id/eprint/8069
14. *Олійник, А. В.*, Шацька, В. М. Інформаційні системи і технології у фінансових установах: навч. посібн. Львів: «Новий світ – 2000». 2006. 436 с.
15. *Про віднесення* держав до переліку офшорних зон. № 143-р (2011). URL: https://zakon.rada.gov.ua/laws/show/143-2011-%D1%80#Text
16. *Про запобігання* та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. №25 (2020). URL: https://zakon.rada.gov.ua/laws/show/361-20#Text
17. *Реєстр* національних публічних діячів України. URL: https://pep.org.ua/uk/data/
18. *Сербина О. Г.*, Загузова О. М. Інтернет-банкінг: українська практика та світовий досвід. Молодий вчений, 2014. №4. С. 122-125. URL: http://molodyvcheny.in.ua/files/journal/2014/4/34.pdf
19. *Singh, K.*, Best, P. Anti-Money Laundering: Using data visualization to identify suspicious activity. International Journal of Accounting Information Systems, 2019. №34. DOI: https://doi.org/10.1016/j.accinf.2019.06.001.
20. *Стечишин, Т. Б.* Проблеми формування системи фінансового моніторингу в банківській сфері України. Науковий вісник Херсонського державного університету, 2014. № 8. С.183−187. URL: http://dspace.wunu.edu.ua/jspui/handle/316497/3604
21. *Subeh, M. A.*, Boiko, A. Modeling efficiency of the State Financial Monitoring Service in the context of counteraction to money laundering and terrorism financing. SocioEconomic Challenges, 2017. 1(2), 39−51. http://doi.org/10.21272/sec.1(2).39-51.2017.
22. *Tropina, T.* Fighting money laundering in the age of online banking, virtual currencies and internet gambling. ERA Forum 15. 2014. P. 69–84. DOI: https://doi.org/10.1007/s12027-014-0335-2
23. *Типологічне* дослідження «Відмивання доходів від податкових злочинів» (2020 рік). URL: https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu/tipologichne-doslidzhennya-vidmivannya-doxodiv-vid-podatkovix-zlochiniv-2020-rik.html
24. *Типологічне* дослідження «Відмивання доходів від привласнення коштів і майна державних підприємств та інших суб'єктів, які фінансуються за рахунок державного та місцевих бюджетів» (2019 рік). URL: https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu/tipologichne-doslidzhennya-vidmivannya-doxodiv-vid-privlasnennya-koshtiv-i-majna-derzhavnix-pidprijemstv-ta-inshix-sub-jektiv-yaki-finansuyutsya-za-raxunok-derzhavnogo-ta-misczevix-byudzhetiv.html
25. *Типологічне* дослідження «Ризики використання суб'єктів з непрозорою структурою власності у схемах відмивання кримінальних доходів» (2018 рік). URL: https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu/tipologichne-doslidzhennya-riziki-vikoristannya-sub-jektiv-z-neprozoroyu-strukturoyu-vlasnosti-u-sxemax-vidmivannya-kriminalnix-doxodiv.html

26. *Типологічне* дослідження «Кіберзлочинність та відмивання коштів» (2013 рік). URL: https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu/tipologichne-doslidzhennya-kiberzlochinnist-ta-vidmivannya-koshtiv.html
27. *Типологічне* дослідження «Актуальні методи і способи легалізації (відмивання) доходів, одержаних злочинним шляхом, та фінансування тероризму» (2012 рік). URL: https://fiu.gov.ua/pages/dijalnist/tipologi/tipologi-derzhfinmonitoringu/tipologichne-doslidzhennya-aktualni-metodi-i-sposobi-legalizacziji-vidmivannya-doxodiv-oderzhanix-zlochinnim-shlyaxom-ta-finansuvannya-terorizmu.html
28. *Yarovenko, H.*, Kuzmenko, O., Stumpo, M. Strategy for Determining Country Ranking by Level of Cybersecurity. Financial Markets, Institutions and Risks, 2020. 4(3), 124−137. https://doi.org/10.21272/fmir.4(3).124-137.2020