Prototyping of information system for monitoring banking transactions related to money laundering

Serhiy Leonov[1], *Hanna* Yarovenko[1,*], *Anton* Boiko[1], and *Tetiana* Dotsenko[1]

[1]Department of Economic Cybernetics, Sumy State University, Sumy, Ukraine

Abstract. The article deals with the prototyping of an information system for intrabank monitoring of transactions related to money laundering. It has been proven that the automation of financial monitoring system would increase the bank's efficiency due to examining all bank transactions without exception, leveling the human factor, maximizing the speed of identifying suspicious transactions, which will provide the bank management with the possibility to reduce reputational risk and minimize losses related to paying penalties imposed by regulatory agencies. It has been established that the prototype of the information system for monitoring transactions related to money laundering through banks should consist of a model of the business process monitoring in an automated system environment, a DFD model of automated monitoring of banking transactions, a structural database model, user interface forms and the logic of validation business rules. The resulting methodological and practical developments are a universal component of the financial monitoring system of any bank since they have the opportunity to transform and adapt to new standards for reporting entities or differentiation of the business processes of a bank.

Introduction

The problem of countering the shadow economy is relevant for Ukraine since its independence. According to the Ministry of Economic Development and Trade of Ukraine, the level of the shadow sector was in the range of 32-43% of GDP in the period from 2010 to 2018 [1]. This share is confirmed by the FATF studies, which determine the value of the shadow sector in the range of 20-40% of GDP for transition economies [2]. It is fair to note that a significant part of the shadow sector in Ukraine is formed as a result of money laundering.

Given the fact that the financial system of Ukraine is bank-centered, the main participants in money laundering are banks. Thus, according to the State Financial Monitoring Service of Ukraine, the number of reports of suspicious financial transactions recorded in 2017 was 8,013,500 (by 26.8% more than in 2016), and 99% of these reports were generated by banks. At the same time, we note that more than 90% of financial transactions of records taken by the State Financial Monitoring Service belong to compulsory financial monitoring [3]. Thus, the requirements of state regulators lead to the identification of suspicious transactions, and the system of internal financial monitoring of banks is ineffective.

Thus, the formation of an autonomous, quick response and multi-functional intrabank financial monitoring system becomes relevant. The solution of this task is proposed to be implemented through the prototyping of an information system for monitoring transactions related to money laundering through banks.

Literature Review

The world scientific community pays considerable attention to the study of the peculiarities of banking transactions related to money laundering. Thus, the place of banks among other money laundering tools is highlighted in the works by P. He [4], M. Betron [5], B. Unger. [6]. These scientists determine the important role of banking transactions among all other money laundering methods and emphasize the need for active counteraction to these illegal actions, both inside the bank and at the level of state regulation. Moreover, scientists determine the continuing trend of growth in the funds that were laundered through the financial system.

Other group of scientists J. Simser [7], A. Chong, F. Lopez-De-Silanes [8], D. Sat al. [9] and F. Teichmann [10] 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.

Finance Stability Board [11], Y. Isa et al. [12], and E. Tsingou [13] studied the issue of financial monitoring in banks and the peculiarities of counteraction to the use of bank transactions for money laundering. These studies are focused on highlighting the mechanisms used in various banks worldwide to counteract the use of their transactions for money laundering, as well as the role of bank staff in this process. In parallel, the authors emphasize the need for state regulators to intensify the internal banking system of financial monitoring by developing appropriate coercive regulatory legal acts.

* Corresponding author: a.yarovenko@uabs.sumdu.edu.ua

Exploring existing research on the role of information systems in detecting fraud in the financial sector, we note that E. Karuppiah et al. [14] generalized the basic machine learning techniques for the preparation, processing and transformation of data related to money laundering.

In addition, it is necessary to pay attention to some more scientific works. Thus, V. Pramod, J. Li, P. Gao [15] 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. In turn, S. Gao, D. Xu, H. Wang, P. Green [16] proposed to use the intelligent agents technology to increase the flexibility of managerial decisions in the field of banking monitoring. 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.

Scientific paper by E. Divya, P. Umadevi [17], which deals with the Transaction Flow Analysis (TFA) system, deserves attention. The proposed information model implies the identification of banking transactions, which are not bound to any file format, and their subsequent clustering in terms of the probability of being associated with money laundering.

Findings

When studying the features of the prototyping of the information system for intrabank financial monitoring, we note that the process of identifying transactions related to money laundering is quite arduous, periodic in nature, significantly dependent on personnel decisions, but well formalized. Therefore, we analyze the existing system of intrabank financial monitoring, which was developed using BPMN 2.0 notation [18] and Bizagi Studio [19] (Fig. 1).

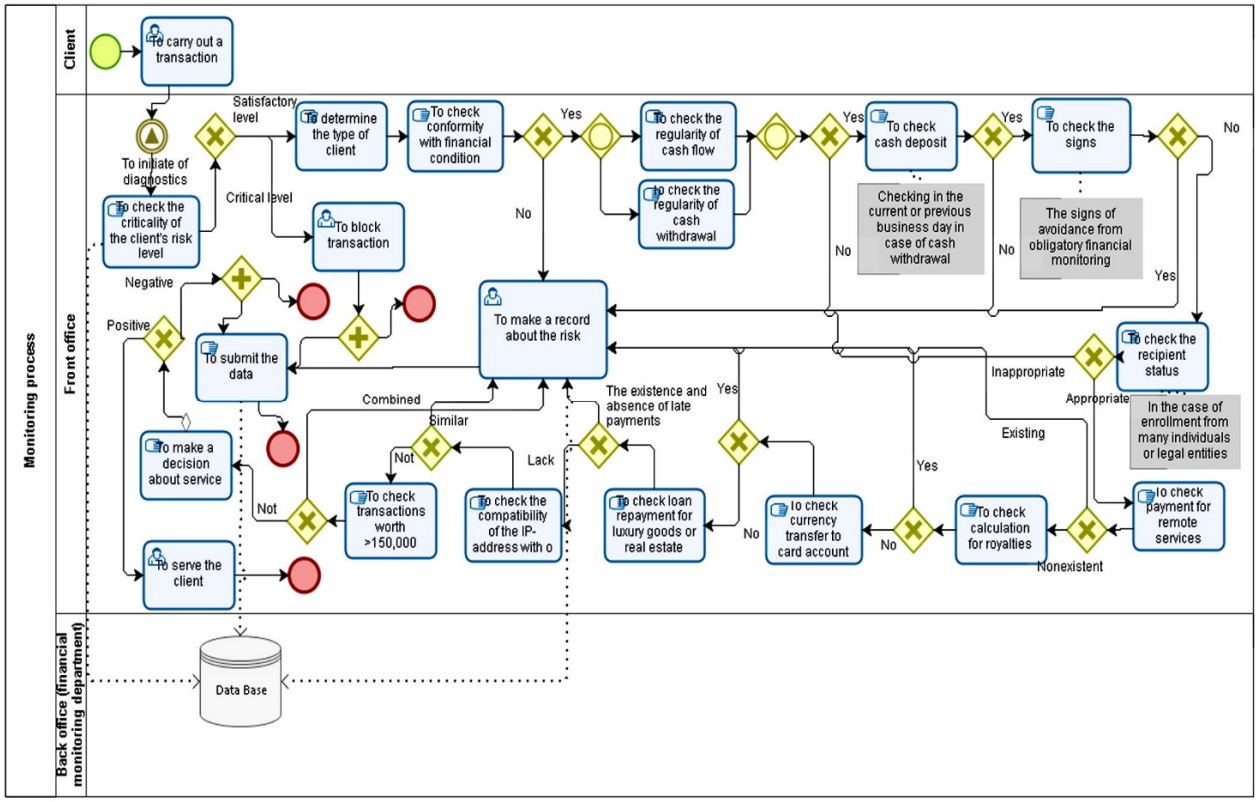

Fig. 1. Diagram of the existing intrabank monitoring business process.

Thus, the identification of the risk related to using bank services for money laundering consists in assessing the sources of income received by the entity or individual. Thus, we check:

- compliance of the funds credited to a bank account with the financial status of the client;
- regularity of receipt of funds, and further cash withdrawals;
- signs of evasion from the mandatory financial monitoring procedure on the part of a client;
- status of a beneficiary in the case of crediting funds from many individuals or legal entities;
- payment by the client for remote services;
- payment of the royalty fee, crediting foreign currency to the card account of the client;
- paying off client's loan for elite goods or real estate;
- similar IP-addresses of client transactions with other transactions;
- transactions exceeding 150,000 UAH.

After each verification, the transaction risk record is entered into the database.

Thus, there are the following shortcomings of the existing system for financial monitoring of risks related to using bank services for money laundering:

- the absence of a unified system of obligatory transactions, which, depending on the level of their

regulation by a particular regulatory legal act, are mandatory or recommended;
- all transactions are carried out manually by a bank employee, requiring the appropriate competence and a considerable amount of time;
- the introduction of a transaction into the risk operations base occurs at the discretion of the banking specialist, which renders impossible a high level of impartiality of the assessment;
- risk assessments of money laundering are not conducted by the bank employees during each transaction. Definition of suspicious transactions is carried out periodically depending on the risk level of the client, depending on the suspicion of the specialist in accordance with the client's transactions or in accordance with the requests of the back office employees.

Thus, an effective solution to the problems of low efficiency of the intrabank system for financial monitoring of risks associated with money laundering is the use of information technologies. Domestic banks do not have such systems due to the specifics of the subject area. Therefore, we propose to create a prototype of an automated system for financial monitoring of banking transactions. For this purpose, the team of authors improved the existing bank monitoring process, taking into account the possibility of its automation. Figure 2 is a diagram of the improved business process of financial monitoring, which was developed using BPMN 2.0 notation [18] and Bizagi Studio [19].

Considering the data presented in Figure 2, it can be argued that the automated system, instead of the employees of the bank front office, should deal with the main actions related to the verification of suspicious transactions. This will allow unloading the front office managers regarding verification of potential transactions related to money laundering. Their automation will assist in improving the efficiency of the bank staff during the implementation of financial monitoring. Namely, first, it will allow for constant online verification. Secondly, the situation of the employee's impact on the verification process and concealing or distorting its results will no longer be possible. This will occur because the system provides for the application of business rules logic that will assist in the automatic selection of those transactions that do not meet the specified conditions. An administrator is responsible for their settings, and other bank employees will not be able to purposefully influence the verification process. Thirdly, such a system allows verifying a larger volume of transactions concerning their involvement in money laundering and terrorism financing. Since monitoring is necessarily applied to transactions, for example, the amount of which exceeds UAH 150,000, transactions with lower amounts, which may also have criminal sources of origin, remain without attention. The use of an automated system will facilitate the verification of all transactions, regardless of their amount. Fourthly, the advantage of the proposed solution is the flexibility of setting up this system in case of changes in legislation or the provisions of the National Bank of Ukraine and bank instructions for verifying such transactions. This is possible due to changes in the parameters of business rules used to verify transactions.

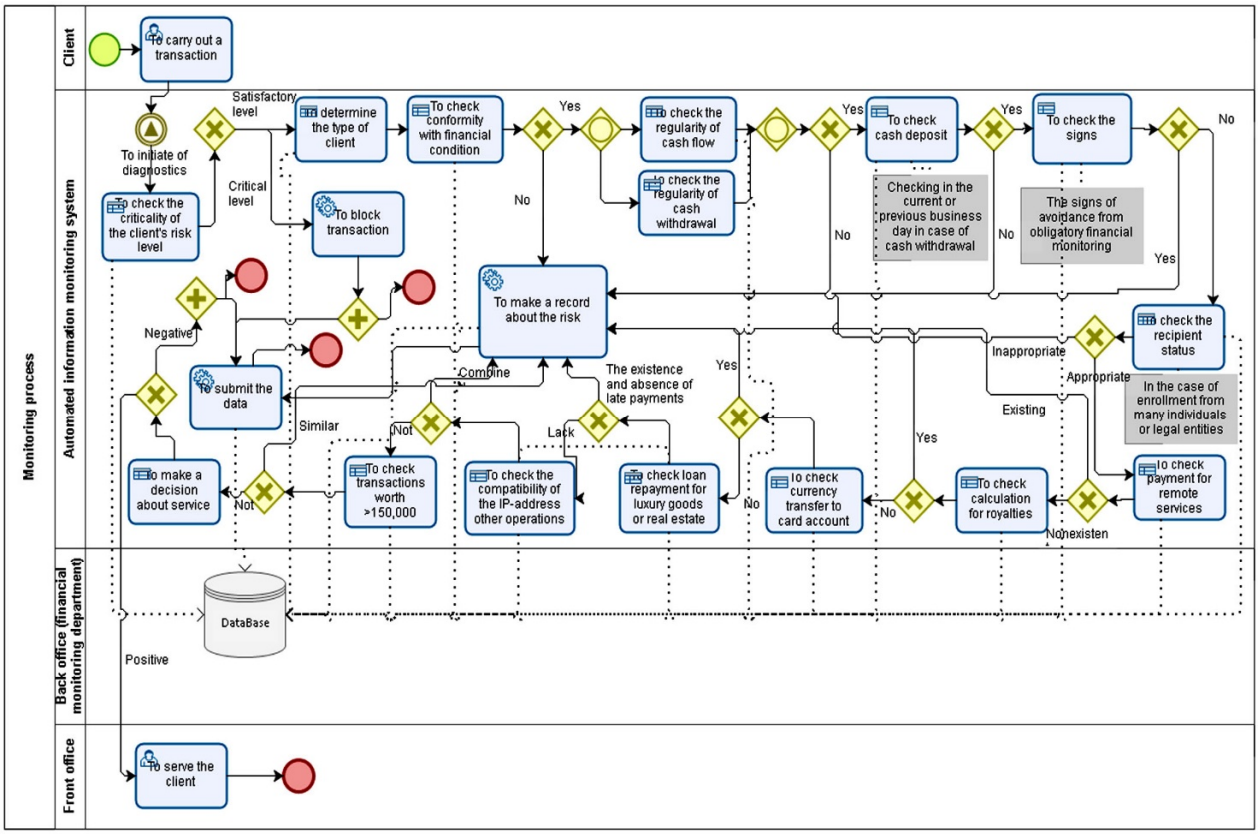

Fig. 2. The monitoring business process model in an automated system environment.

When designing an intrabank financial monitoring system, it is important to build an information model that provides insight into the interconnections between the system objects and their structure. For this purpose, based on the proposed business process (Figure 2), the authors developed an information model based on the Structured Analysis and Design Technique (SADT) in the DFD (Data Flow Diagrams) notation. The authors chose this methodology due to its capabilities of the description of data flows, taking into account their interaction in the process of manual and automated processing of information. Thus, Figure 3 shows the result of this simulation – the DFD-model of financial monitoring of banking transactions performed in the software environment All Fusion Process Modeller [20].

The proposed model includes the following main entities, such as "Bank Client" and "Front Office Manager", 14 main functions related to the verification of banking transactions concerning their use in money laundering or terrorist financing, and 8 basic structures for storing information. Input and output streams of information are defined between the presented objects.

The functions 1-13 from Figure 3 show the main areas of monitoring: the first verification the criticality of the client's risk level, the second verification the type of client, the third verification conformity with financial condition, the forth verification the regularity of cash flow and cash withdrawal, the fifth verification the signs of avoidance from obligatory financial monitoring, the sixth verification the cash deposit, etc. In these areas, there are transactions identified as if there is a risk of money laundering. The results of verifications are accumulated in the block "Make a decision" where the decision is made on whether there is a risk on a transaction or there is no risk.

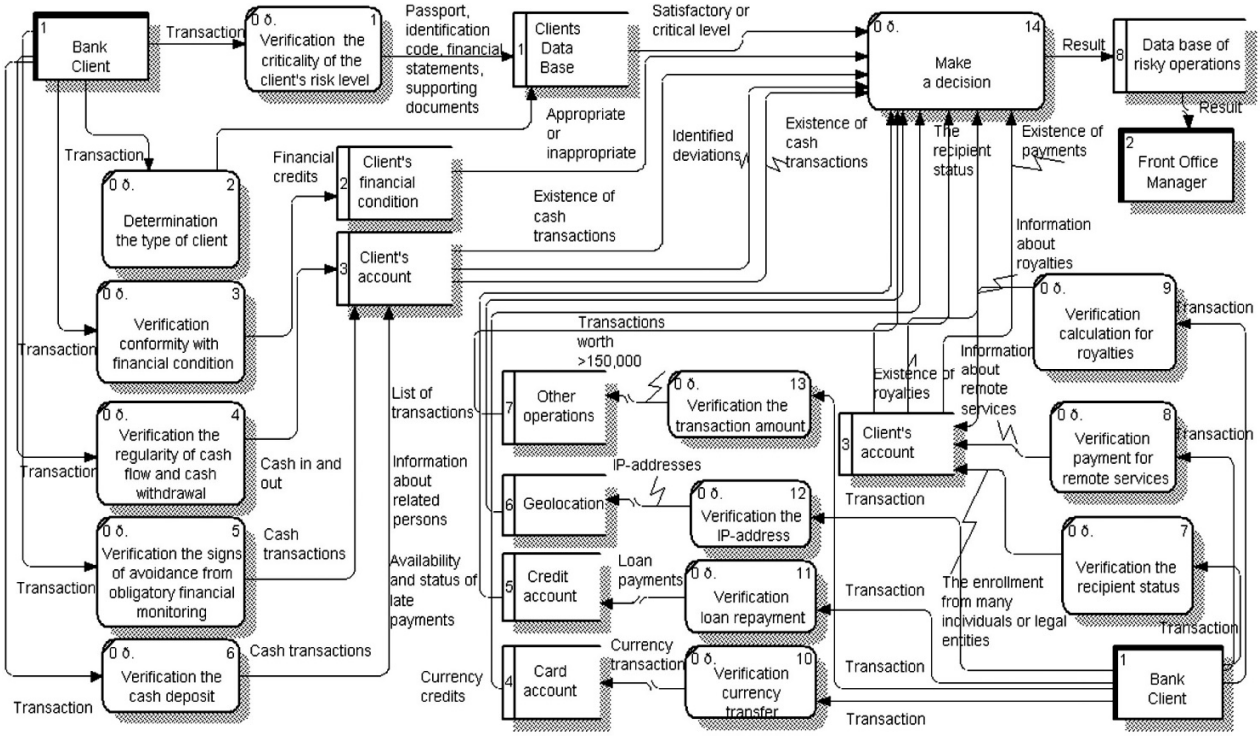

Fig. 3. DFD-model of automated monitoring of banking transactions.

Understanding information about incoming and outcoming streams is very important. Since the main subject of monitoring is a client transaction, it is verified by comparing with the criteria. As criteria, a bank can use the client's financial documentation, loan payments, information about payments for expensive purchases, transactions that do not correspond to the client's type of activity, information about payments of author's fees, the IP-address of the operation, etc. This information is usually contained in an automated banking system, where the automated financial monitoring module will be integrated.

The developed DFD-model formed the basis for the creation of a logical data scheme, which implementation allowed forming the internal information system of the system prototype. For this purpose, entities were created, relationships were established, relations types were selected, and attributes were specified. Thus, a complete data structure was created to develop a database of automated monitoring system, which was developed using Bizagi Studio [19] (Figure 4).

The proposed model (Figure 4) identifies a structured database model running SQL Server that determines how data is available, stored and used in the system. The value of the model lies in the fact that it takes into account the main specificity of monitoring transactions in the bank.

The next step in developing the system prototype is the development of interfaces and the definition of basic business rules. Thus, the user interface forms have been developed that allow seeing how the user will interact with the system. Since the proposed system carries out the entire verification process without the employee's participation, the verification results form were created (Figure 5).

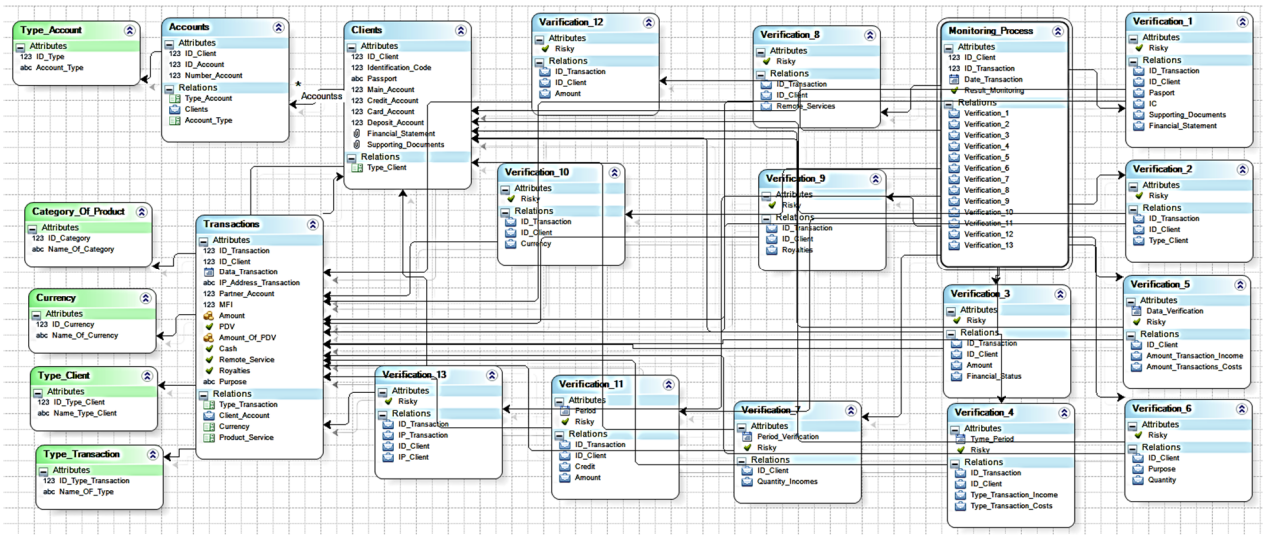

Fig. 4. Database structural model of automated monitoring system.

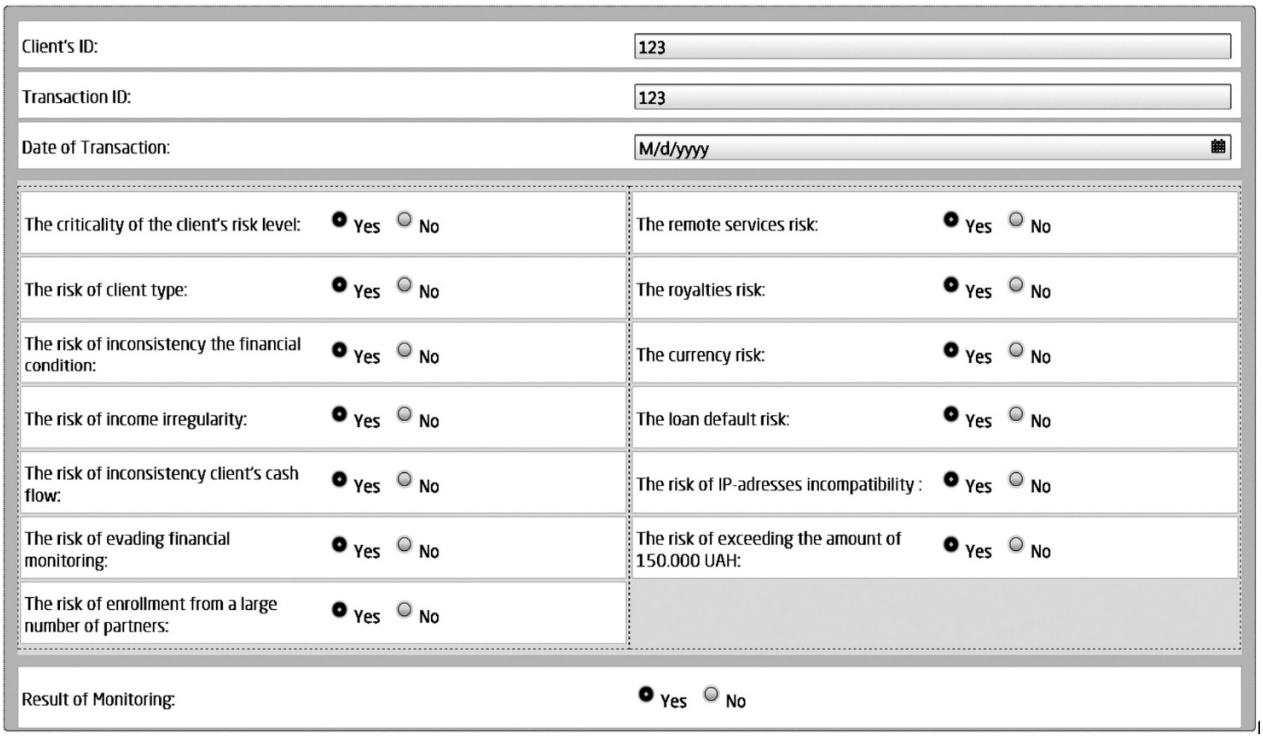

Fig. 5. User interface form with results of verification.

The developed form allows us to get information about the client, the transaction and the results of the monitoring according to thirteen rules. Only two options were proposed for each risk position. The system gives the option "YES" if there is a risk of a transaction. The system issues "NO" in the absence of risk. The information system also allows us to get a general result of monitoring. The "YES" answer will indicate the presence of risk at any level of verification and a transaction will be rejected. If there is no risk at all levels of monitoring, the system will give the answer "NO" and a transaction will be accepted.

For automatic execution of actions, the system has developed basic business verification rules. These rules are important for the further development of the automated system. The development of the rules was carried out according to the following logic, represented by the formulas 1-3.

To conduct monitoring, there are next business rules (Formulas 1-2):

$$IF\ [Condition\ of\ Verification\_1 \neq Criteria\ of\ Verification\_1]\ THEN\ [Risk = 1]\ ELSE\ [Risk = 0] \quad (1)$$

…

$$IF\ [Condition\ of\ Verification\_N \neq Criteria\ of\ Verification\_N]\ THEN\ [Risk = 1]\ ELSE\ [Risk = 0], \quad (2)$$

where *Condition of Verification_1* – a condition for verifying a transaction for a certain type of risk that corresponds to the first function of Figure 3; *Condition of Verification_N* – a condition for verifying a transaction for a certain type of risk that corresponds to one of the functions of Figure 3 (as an example, it is the condition of verification the signs of avoidance from obligatory financial monitoring); *N* – a number of verifications from 1 to 13; *Criteria of Verification_1* – the first criterion that is chosen to verify the transaction for the risk of money laundering; *Criteria of Verification_N* - the criteria 2-13 that is chosen to verify the transaction for the risk of money laundering (as an example, it is the criterion that corresponds to the information about client's cash transactions on him account); *Risk = 1* – presence of money laundering transaction risk; *Risk =0* – lack of money laundering transaction risk.

To obtain the overall monitoring result, the following business rule is set (Formula 3):

$$\begin{aligned} &IF\ [Verification\_1 = 1\ OR\ Verification\_2 = 1\ OR \\ &Verification\_3 = 1\ OR\ Verification\_4 = 1\ OR \\ &Verification\_5 = 1\ OR\ Verification\_6 = 1\ OR \\ &Verification\_7 = 1\ OR\ Verification\_8 = 1\ OR \\ &Verification\_9 = 1\ OR\ Verification\_10 = 1\ OR \\ &Verification\_11 = 1\ OR\ Verification\_12 = 1\ OR \\ &Verification\_13 = 1]\ THEN\ [\text{“}YES\text{”}\ Risk\ AND \\ &Reject\ operation]\ ELSE\ [\text{“}NO\text{”}\ Risk\ AND\ Accept \\ &Operation], \end{aligned} \tag{3}$$

where *Verification_1,2,…,13* – the result of each verification; *“YES” Risk AND Reject operation* – the decision when the risk of money laundering is present and the transaction is rejected; *“NO” Risk AND Accept Operation* – the decision when there is no risk of money laundering and the transaction is accepted.

The developed rules constitute a group “Define Expressions”, determining the behavior of the system under certain conditions. Thus, the rules take into account branching conditions that correspond to a positive verification result when the transaction is not at risk related to money laundering or negative when the transaction is entered into the database of risky operations and blocked by the system.

Conclusion

It is fair to note that despite the fact that the problem of assessing the risk related to using banks for money laundering or terrorism financing is not a priority, but its solution is extremely important both for banks and for the state as a whole. Thus, over the past five years, the rate of money laundering through banking transactions significantly exceeds the rate of economic growth in Ukraine. In turn, for banks, the risks are manifested in the strengthening of supervision on the part of the National Bank of Ukraine, increased motivation of bank staff to fraud and the future loss of financial stability.

Banks, as entities of initial financial monitoring, should analyze client's transactions to identify the features that are typical for the laundering of money obtained illegally. As part of this activity, they can only detect these operations by post factum. Practical experience of Ukrainian banks shows that financial monitoring is periodic, non-systematic, carried out manually, its results can be influenced by the “human factor”, which is a manifestation of a corrupt component. But the main task of monitoring is to prevent transactions which there is a risk of money laundering with. Therefore, the prototyping of an information system for monitoring banking transactions related to money laundering is a very topical issue.

Thus, a prototype of an automated system for financial monitoring of transactions was obtained to find their connection with money laundering. The prototype consists of a monitoring business process model in an automated system environment, a DFD automated banking monitoring model, a database structural model, user interface forms and validation business rules logic.

The application of the proposed information system allows us to verify the client's transactions on the thirteen risk rules. This approach makes it possible to assess the risk of money laundering for each transaction. If an operation does not correspond at least one rule, then it is rejected. The system concludes that there is an increased risk of this transaction. Because of the automatic process, the influence of bank employees on risk transactions is excluded. Furthermore, the front-office worker can make a decision based on information obtained from the information system.

The implementation of the proposed system will automate the monitoring process, reduce its labor intensity, increase the efficiency of verification by processing more transactions, and shift the focus from the employee to the automated system to reduce the impact on the verification results.

In the future it is planned to implement the proposed prototype into the practical activity of banks at the level of subjects of initial financial monitoring. Since this implementation involves the necessity to optimize the monitoring business process in a bank, it requires a considerable amount of time. In today's conditions of intensifying the struggle with the problem of money laundering, the interest of banks in this decision is unconditional. Under the influence of regulation of this problem by the National Bank of Ukraine, the implementation by banks an automated monitoring system will contribute to the creation of a unified information base of monitoring and information integration at the level of subjects of state monitoring.

The article was executed in the framework of state budget scientific research work No. 0118U003574 “Cyber security in the fight against bank fraud: protection of financial services consumers and growth of financial and economic security of Ukraine” and scientific research work No. 0117U002251 “Improvement of national anti money laundering system in terms of increasing financial and economic security of the state”.

References

1. Ministry of Economic Development and Trade of Ukraine. http://www.me.gov.ua/?lang=en-GB (2018). Accessed 20 Feb 2019
2. FATF-GAFI.ORG - Financial Action Task Force (FATF). http://www.fatf-gafi.org (2019). Accessed 20 Feb 2019
3. The State Financial Monitoring Service. http://www.sdfm.gov.ua/index.php?lang=en (2018). Accessed 20 Feb 2019
4. He, P.: A typological study on money laundering. Journal of Money Laundering Control. **13**(1), 15–32 (2010). doi:10.1108/13685201011010182
5. Betron, M.: The state of anti-fraud and AML measures in the banking industry. Computer Fraud ^ Security. **2012**(5), 5–7 (2012). doi:10.1016/S1361-3723(12)70039-8
6. Unger, B.: Can Money Laundering Decrease? Public Finance Review. **41**(5), 658–676 (2013). doi:10.1177/1091142113483353
7. Simser, J.: Money laundering: emerging threats and trends. Journal of Money Laundering Control. **16**(1), 41–54 (2012). doi:10.1108/13685201311286841
8. Chong, A., Lopez-De-Silanes, F.: Money laundering and its regulation. Economics & Politics. **27**(1), 78–123 (2015). doi:10.1111/ecpo.12051
9. 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. http://www.jatit.org/volumes/Vol83No2/11Vol83No2.pdf (2016). Accessed 21 Mar 2019
10. 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
11. Finance Stability Board: Global Shadow Banking Monitoring Report 2014. http://www.fsb.org/wp-content/uploads/r_141030.pdf (2014). Accessed 21 Mar 2019
12. Isa, Y.M., Sanusi, Z.M., Haniff, M.N., Barnes, P.A.: Money Laundering Risk: From the Bankers' and Regulators Perspectives. Procedia Economics and Finance. **28**, 7–13 (2015). doi:10.1016/s2212-5671(15)01075-8
13. Tsingou, E.: New governors on the block: the rise of anti-money laundering professionals. Crime, Law abd Socical Change. **69**(2), 191–205 (2018). doi:10.1007/s10611-017-9751-x
14. Karuppiah, E.K., Lam, K.S., Chen, Z., Van Khoa, L.D., Teoh, E.N., Nazir, A.: Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. Knowledge and Information Systems. **57**(2), 245–285 (2018). doi:10.1007/s10115-017-1144-z
15. 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
16. Gao, S., Xu, D., Wang, H., Green, P.: Knowledge-based anti-money laundering: A software agent bank application. Journal of Knowledge Management. **13**(2), 63–75 (2009). doi:10.1108/13673270910942709
17. Divya, E., Umadevi, P.: Money laundering detection using TFA system. In: International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012), 19-21 Dec. 2012 (2013). doi:10.1049/ic.2012.0150
18. BPMN Specification - Business Process Model and Notation. http://www.bpmn.org (2019). Accessed 20 Feb 2019
19. Bizagi Studio Process Automation & Workflow Software - Free Download. https://www.bizagi.com/en/products/bpm-suite/studio (2019). Accessed 20 Feb 2019
20. BPWin Software Download. BPM Microsystems. https://bpmmicro.com/support/software/downloads (2019). Accessed 20 Feb 2019