Principles and Algorithms for Creating Automated Intelligent Control Systems of Electronic Banking

Yaroslav Petrivskyi[1], Volodymyr Derkach[2], Oleksandr Kravchuk[2] and Volodymyr Petrivskyi[3]

[1] *Rivne State Humanitarian University, St. Bandery str. 12, Rivne, 33000, Ukraine*
[2] *Information and analytical enterprise «Analityk 1», Rivne, 33000, Ukraine*
[3] *Taras Shevchenko National University of Kyiv, Bohdan Hawrylyshyn str. 24, Kyiv, 01001, Ukraine*

Abstract

In the article the main conceptual principles of creating intelligent information systems for monitoring and controlling the financial sector of the circulation of funds, which meets the requirements of the regulatory framework of the world community regarding the prevention and counteraction of the legalization of income obtained through criminal means are examined. The author's package of a flexible software model, Integrated Software Package for Preventing Abuses in Financial Practices, is proposed, which successfully integrates with various banking products (operational day of the bank), solves the issue of multi-faceted testing and detection of abuses in banking practice.

Keywords [1]

Information systems, anti-money laundering, financial monitoring, automation, algorithm.

1. Introduction

Shadow money circulation harms society by creating ample opportunities for criminal activities such as drug and arms trafficking, human trafficking, and terrorist attacks. The issue of the importance of combating the illegal circulation of funds is obvious for all countries. The Financial Action Task Force (FATF), which was established in 1989 to combat money laundering and terrorist financing, is an independent intergovernmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction. It is an intergovernmental agency made up of 35 member jurisdictions and two regional organizations. Ukraine is a member of the Committee of Experts of the Council of Europe as part of the FATF on the evaluation of measures to combat money laundering and terrorist financing – MONEYVAL [1,2].

Recently, the European Union (EU) adopted some important regulations (officially known as General Data Protection Regulations-GDPR) regarding the collection, storage, and use of personal information, which became law throughout the EU in May 2018 and replaced the EU Data Protection Directive 1995. In terms of scope, the new provision applies equally to industries, EU organizations, and organizations of other countries that trade with the EU. Data-driven regulations focus on some specific issues, including ownership of data, explainability and trustworthiness, and transparency of algorithms that are trained or built on such data. A detailed analysis of these rules can be found in [3,4,5]. As countries around the world implement FATF standards, they should become more effective in detecting, investigating, prosecuting, and preventing financial crimes. Criminals and terrorists are constantly looking for new ways to collect and move funds while avoiding detection. FATF's research into existing or emerging money, trends, and methods of money laundering and terrorist financing will help countries better understand the risks involved. Once these risks are properly understood, countries will be able to implement effective anti-money laundering and countering the financing of terrorism measures and reduce these risks.

Information Technology and Implementation (IT&I-2022), November 30 - December 02, 2022, Kyiv, Ukraine
EMAIL: prorectorsgu@ukr.net (A. 1); vd.docfm@gmail.com (A. 2); ok.analityk1@gmail.com (A. 3); vovapetrivskyi@gmail.com (A. 4)
ORCID: 0000-0001-9749-8244 (A. 1); 0000-0001-9298-8244 (A. 4)


FATF's high-risk public identification process and other monitored jurisdictions ensure that every country in the FATF Global Network upholds its commitment to implement FATF's international standards because there is no safe environment for criminals and terrorists to hide their activities. If one country has a weaker financial system than another, then it is a threat to all. This process is a powerful tool for preventing criminals and terrorists from abusing the financial system. On the one hand, public vigilance and control reveal information about specific risks arising from each of the jurisdictions, on the other hand, potential business partners, financial institutions, and regulators introduce necessary precautionary measures, which makes criminal devices impossible and prevents illegal financial flows in the global financial system.

It is obvious that there is an urgent need to create new and improved existing interactive automated intelligent software complexes for detecting and countering money laundering of financial institutions based on algorithms and developments using artificial intelligence. Known anti-money laundering systems work using a combination of human experience and skills and automated information processing. These methods often include artificial intelligence technologies or data analysis methods, but there remains a strong dependence on the professionalism of the human auditor. Systems for detecting and combating money laundering of financial institutions are, as a rule, simplified and based on rules where a transaction will be marked as suspicious, requiring human verification in accordance with a set of rules defined by law. Systems based on such rules lead to an uncontrollable number of transactions marked as suspicious, requiring a large expenditure of time and resources to verify legitimacy. Institutions must find a balance between the thorough review of transactions and the timely approval of legitimate transactions. The implementation of automated intelligent anti-money laundering software packages optimizes the overall decision-making process while remaining compliant with data protection regulations (GDPR). Automated intelligent systems can minimize the number of transactions falsely flagged as suspicious, achieve clear compliance with regulatory expectations, and increase operational productivity.

2. Review of known results and formulation of the problem

Among the modern automated applications of intelligent decision-making support with the help of agents in the field of logistics and anti-money laundering are known, for example, Real-Time Exception Management Decision Model [6], multi-channel data-driven, real-time anti-money laundering systems for electronic payment cards [7], Scalable graph learning for anti-money laundering [8] and others.

As a rule, the algorithms of such software complexes are based on a sequential multi-step analysis using Simon's decision-making model. First, a description of the data is carried out, and then there is a transition to the weighted assessment of transactions [9]. In [10], the authors proposed a system for identifying transactions with a high risk of illegality. The article [11] describes an intelligent anti-money laundering system that uses human agents to train and adapt such a system. The publications contain meaningful recommendations for the use of modern automated applications of intelligent decision-making support in the prevention and fight against money laundering, but they do not provide details about how the specified technology should be developed and implemented and what is the real result of its implementation.

The characteristic stages of a money laundering scheme are its placement, layering, and integration or legalization. Proceeds of crime enter the placement phase, where they are converted into monetary instruments or otherwise deposited with a financial institution (or both). Layering refers to the transfer of funds to other financial institutions or individuals through bank transactions, wire transfers, or other methods. At the final stage of integration, the funds are used to purchase legitimate assets or to continue financing criminal enterprises. Here, illegally obtained money becomes part of the legal economy.

Industry-leading anti-money laundering solutions are generally an anti-money laundering (AML) technology workflow that connects a data source to a rules-based system. Next, analysts add their own conclusions regarding the legality of the transaction. The multi-step process first collects and processes data using anti-money laundering technology using an infrastructure of AML software solutions. In the next step, the transaction is fixed and controlled, then if the transaction is suspicious, it is thoroughly checked by a human analyst who makes a decision about its legality. In general, the multi-step process of anti-money laundering technology can be defined in four levels. At the initial, first level, collection,

management, and storage of relevant data are carried out, which includes both internal data of the financial institution and external data of regulatory bodies, government agencies, and others. It is the layer where data is collected, managed, and stored by various sub-modules and agents and supports bi-directional access with other layers, and processes both internal and external data. Internal data refers to various sources of information that are identified and processed internally by various components of the system - for example, customer profiles, customer accounts, and real-time operation mode. They are used to assess a customer's profile, measure the risk of a transaction and diagnose the behavior. Outputs of various analytical engines, insights from analysis, and the history of previous blocked transactions are also processed at this level. This data is used to support the final decisions made when evaluating transactions throughout the system. External data is data collected from a source outside the financial institution (this may include data from regulatory bodies, government bodies, international standards, legislation, sanctions and watch lists). Social media and news portals are often seen as external sources of data but are currently underutilized in anti-money laundering technology solutions. From a technological point of view, traditional systems suffer from architectural deficiencies, such as data quality and data management. Big data technology and distributed data processing have not yet gained widespread use in anti-money laundering technologies.

The data tier is typically supported by an enterprise data center that includes the technologies required for efficient processing. For example, Hadoop is used for parallel processing and data collection [12], Solr is used for search, and Mahout or Spark is used for modeling and creating analytics [13, 14]. Various databases are used to store raw data, processed data, and analysis results. For a better understanding, the aggregate is divided into components depending on their purpose. The collection component deals with internal and external data and has a distributed data collection and processing structure. Such technologies as Hadoop, Kafka, and Storm are used here. The data processing component is an important but cumbersome task. Because data comes from multiple sources, it is collected and generated using different standards. All input data must be standardized for future use. Data is often enriched with metadata generation and linking techniques, formatted and compressed using information retrieval tools (such as Solr) and NLP techniques, including tokenizers.

The analytics component generates insights from the data using multiple analysis methods, namely, grouping similar transactions and customers together according to their profiles. Relationships between customers and transactions are created using data analysis tools such as Mahout. Anomalous transactions can also be identified using customer or organization profiles. This information is used at the next level to determine whether the transaction should be considered suspicious. The data storage stage is a critical component of this layer because data is collected, generated, and processed in this layer. Storage is relational (eg Oracle) or linear (eg Cassandra). Often multiple data management infrastructures are included in this layer.

The second layer, the screening, and monitoring layer check transactions and customers for illegal activity. Financial institutions have mostly automated this level into a multi-step procedure, often based on rules or risk analysis. If suspicious activity is detected, it is escalated to the notification and event level for further investigation. This process involves supplementing the data with historical transaction information and the necessary evidence to review the flagged transaction. Screening occurs before a transaction is executed and consists of a name and transaction verification. The monitoring process is carried out constantly, and the transaction and customer profiles are analyzed using analytical models. Components at this level work in a collaborative effort that includes multiple tools. They support a bidirectional connection to the data layer for data retrieval and post-operational storage operations. According to its specific tasks, the transaction verification module works before the transaction is carried out and is used to enforce sanctions. The transaction screening module maintains a connection to the data layer to receive external data for filtering. Programs that provide transaction verification services include Actimize and MANTA. Name Verification Module: This module is used to identify payments related to customer personalization or entities that have been identified by regulatory authorities as potential money launderers. Checks are carried out constantly and in real-time; this requires the module to support a data layer connection. Several organizations provide quality corporate name screening services to financial firms, including Compliance Link of Accuity, Oracle Watch-list Screening of Oracle, and LexisNexis Bridger Insight XG from LexisNexis Risk Solutions.

The transaction monitoring module identifies suspicious transaction patterns and populates a suspicious activity report. Next to its analysis engine, this module contains the results of the screening

modules and is connected to the data layer to retrieve information and store reports. The customer profile monitoring module analyzes the customer account to get an overview of the customer profile. It also supports a two-way connection to the data layer to retrieve client data and store analytical results. The component works in cooperation with other modules at the level of screening and monitoring; however, it specifically focuses on certain activities, such as high-risk country alerts, analyzing financial ties and business relationships, and understanding political preferences.

Often client profiles are compared to a database of potential or known financial offenders, Template and Risk Analysis are common techniques used in this module. Rule-based systems depend on human-defined rules and prohibitions. In turn, sufficient meticulousness in verification can cause the accumulation of a large number of transactions that will be erroneously marked as suspicious, which will lead to a significant number of manual verifications [15, 16]. On the other hand, only the formal recording of suspicious transactions leads to a small number of checks and the omission of a large number of illegal transactions [17].

Thus, most rule-driven anti-money laundering solutions cannot handle large volumes of operational and financial data, making them impractical at the scale of banks' operations. They are also unable to generalize or automatically adapt to new patterns of criminal schemes because the rules are predetermined. The results of the screening and monitoring modules are the basis for generating alerts. Transactions that are considered suspicious are flagged for further processing. The next level is the level of notifications and events, where a notification is created so that a suspicious transaction should be checked by an expert analyst. A large number of transactions to be verified and the lack of supporting data increase the time it takes to verify each transaction. To reduce both the risk and the costs of manual verification, the history of previous decisions and comparisons with similar operations and decisions are taken into account. If the transaction is marked as suspicious, the level supplements it with additional data for the evaluator. This includes decision history for similar transactions, risk scores calculated by previous levels, and transaction clearing priority. Pending transactions for which no decisions have been made are kept in the service queue. Next, the alerts created and organized in the third step are passed to the next, final operational layer.

At the last level, analysts make the final decision to block, release or queue a transaction based on the data obtained at the previous stages. It is legally required that the final decision on the transaction be made by an authorized person of the financial institution. Previous levels are used to monitor all transactions and flag potentially fraudulent operations. Intelligence agents use a number of techniques to gather and visualize additional information about a suspicious transaction. This includes querying the World Wide Web (WWW) and Lexis Nexis for information about entities associated with a transaction and visualizing the relationships used by the subject link analysis.

This layer suffers from a high number of false positives, namely legitimate transactions that are falsely flagged as suspicious. This leads to significant queues in making the right decision regarding the transaction and a sufficient workload for the work of a specialist analyst.

Despite the simplicity and potential for error in deciding whether a transaction is legal, the use of rules is common because they make it easier to demonstrate compliance. There are more sophisticated implementations of rule-based systems, for example[18, 19], where categories of specific accounts and transactions are separated by building reasoning based on the ontology, then querying the ontology with new transactions, or using hard-coded rules that identify transactions from suspicious countries, people, organizations and accounts when a certain threshold is exceeded, using link analysis as a visualization tool to identify indirect links to suspicious entities.

3. Main part

Anti-money laundering systems are implemented by financial institutions, such as banks and other credit institutions, to combat money laundering by identifying money laundering risks, potential thieves, and money laundering operations. The consequences of the mistake are obvious.

In April 2020, the new Law of Ukraine "On Preventing and Countering the Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing the Proliferation of Weapons of Mass Destruction", or the Law on Financial Monitoring, which is appropriate for financial policy FATF. The law changed the threshold amounts for checking financial transactions, the number

of evaluation criteria, and the rules for identification and verification, expanded the list of subjects of financial monitoring (organizations responsible for tracking suspicious financial transactions), and significantly increased penalties for non-compliance. The adoption of the law seriously stirred up the financial market. After all, many financial organizations have not thought about the issues of financial monitoring before. And according to the new requirements, the subjects of financial monitoring within the framework of the risk-oriented approach to assessing a financial transaction must use more than 200 criteria, which poses a difficult task for financial monitoring analysts. But technologies came to the rescue, greatly simplifying the tasks of financial monitoring entities in identifying dubious transactions.

The modern Ukrainian market already offers separate "complex solutions" for the study of financial flows for the purpose of financial monitoring. But at their core, these are financial constructors that provide only general information data that is already available in banking institutions [20-25]. The disadvantages of such solutions are the lack of combined scenarios for solving individual problems; the need for constant updating of algorithms (tasks) taking into account financial market trends. To solve the above problems that arise in banking institutions in modern conditions, the authors of the article and a group of specialists from the Analyst-1 information and analytical firm developed ISPPA in FP (Integrated Software Package for Reinventing Abuses in Financial Practices - a package of integrated software for preventing abuse in financial practice. It provides automation of control over the activities of bank customers based on the analysis of banking operations performed by customers, the status of customer accounts, the risk levels of their legalization of proceeds from crime, as well as the identification of affiliated customers by their contractors, the timeliness of updating personal data and their compliance with real activities. To write the ISPPA in FP software product, an object-oriented programming language JAVA was chosen, which provides reliability, security, and functionality and is a universal environment connection of users with various sources of information, regardless of their location. And "architecture independence" allows you to run the software on any platform that has a JAVA virtual machine installed. The main repository of information for the operation of the ISPPA in FP software is the PostgreSQL object-relational database management system. This DBMS provides high stability, fault tolerance, functionality, and speed, has a wide range of tools for storing, processing, and retrieving information, and also supports full compliance with the SQL standard.

When tracking cash flows, the system used an innovative approach to analyze cash flows using mathematical models. This is a scoring of client risks - the identification of atypical (doubtful) cash flows using 20 multi-level mathematical scenario cases with their further ranking according to the degree of riskiness. In an in-depth study of the client, in order to increase the accuracy of identifying a dubious transaction, we also use an assessment of reputational risks, as well as simplified operational indicators. To date, we have automated the identification of more than 70 risks and indicators in order to obtain additional data for the final decision on the client.

When assessing reputational risks, information registers are used, and only those that are in the public domain. A deep professional understanding of the processes taking place in the banking sector allows us to develop and improve for our clients exactly those databases that are directly needed for high-quality financial monitoring. The gradual filling of our information platform with new databases is not our desire, this is a market requirement, because the market is developing, mutating, and unscrupulous clients are constantly looking for new and new ways to conduct dubious transactions. We, on the other hand, are on guard and monitor risky areas that appear on the market, which financial institutions need to control more deeply and carefully. Currently, there are two ways for ISPPA in FP to interact with automated accounting systems: integration and conditional integration. The order of interaction for each of these methods is shown schematically in fig. 1 and fig. 2 (on the example of integration with automated banking systems - ABS).

In the case of interaction between ISPPA in FP and an automated accounting system using the integration method (Fig. 1), the ISPPA in FP system is directly connected via a local network to data arrays (DBMS) formed in an automated accounting system, and in the reading, mode receives data online for further processing (1). As a result of data processing, templates of dubious transactions and schemes are formed that can be used by clients when carrying out transactions in a financial institution. A library of such templates is formed into a protective shield designed to prevent dubious operations or the use of dubious schemes for such operations. The results obtained during data processing, intermediate and final forms of ISPPA in FP work reports can be used to make appropriate management decisions. In the case of interaction between ISPPA in FP and an automated accounting system using

conditional integration, the ISPPA in FP system receives data in file mode - offline. As a result of data processing, templates of dubious transactions and schemes are formed that can be used by clients when carrying out transactions in a financial institution. A library of such templates is formed into a protective shield in the form of template files, which are loaded into the system to ensure the timely termination of dubious operations or the use of dubious schemes for such operations.

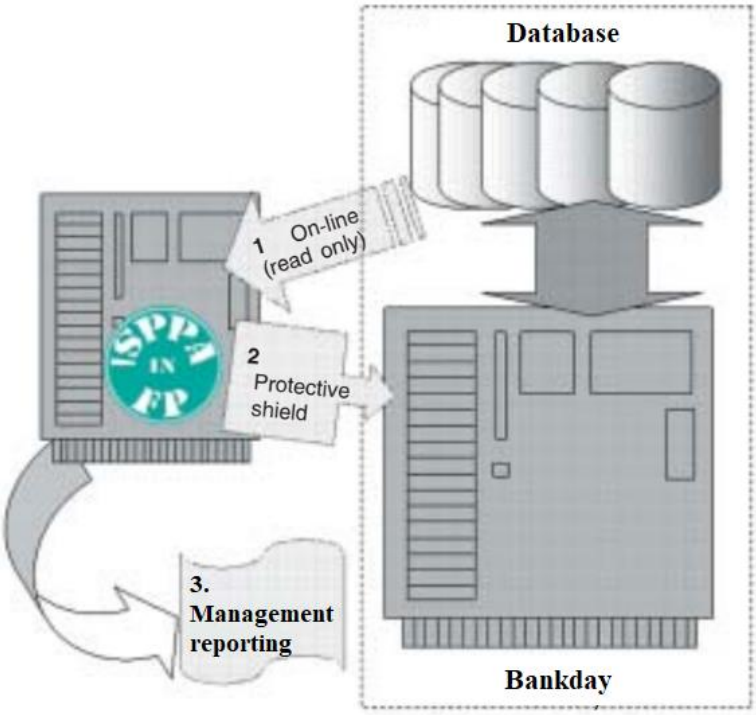

Figure 1: First method of integration

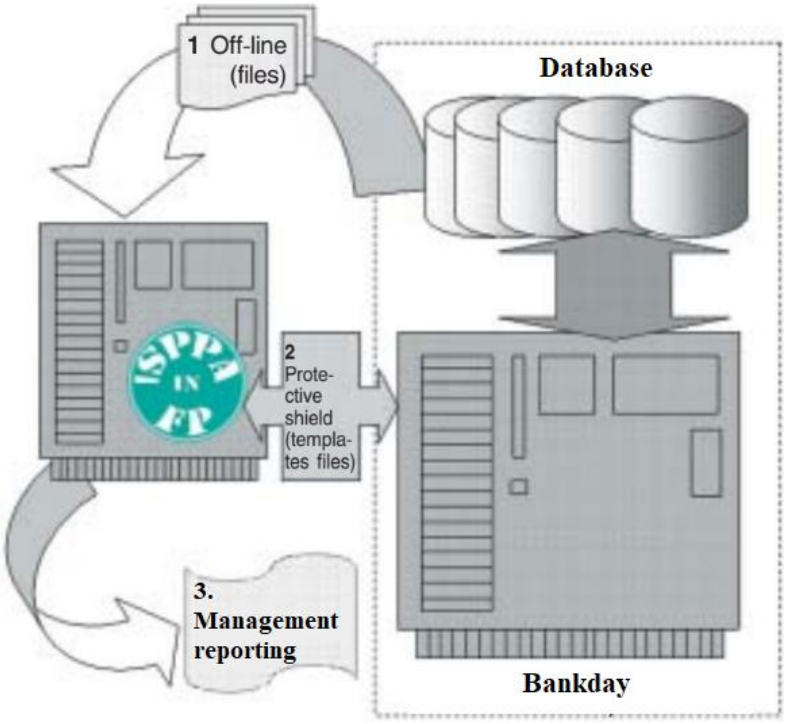

Figure 2: Second method of integration

The results obtained during data processing, intermediate and final forms of ISPPA in FP work reports can be used to make appropriate management decisions. The integrated software package has

proven itself and has been successfully tested in a number of leading Ukrainian banks, such as Ukreximbank, Alfa-Bank, TASCOMBANK, PUMB, Raiffeisen Bank, OTP Bank, Kredobank, Piraeus Bank, and other banks. Our solutions are used by more than 25 insurance companies, including Universalnaya, Oranta, Etalon, Providna, Persha, UPSK. TAS Group and Eximleasing are also our clients. Financial companies "SS LOUN", "CASH TO GO", "FREEDOM FINANCE Ukraine", and Money4You cooperate with us. And there are many other clients that are equally important to us.

4. Conclusion

The main objective of the ISPPA in FP software product was to create a flexible model that makes it possible to quickly integrate with a variety of banking products (the bank's operating day), as well as to create a technological map for diverse testing of the integration using functional analysis, analysis of limit values, broken down into equivalence classes and taking into account multilevel mathematically integrated components to test the structural and functional criteria of software. Conducting multi-vector statistical and dynamic testing of the software package confirms the correctness of the mathematical model of the software product and ensures successful certification and verification. The cross-platform nature of the ISPPA in FP software package allows you to easily and quickly integrate with the environment of a financial institution. The implementation of the ISPPA in FP software package makes it possible to use: typical information search scenarios with the possibility of using "alerts"; new unified algorithms that are already successfully operating in banking institutions and developed by practicing financial analysts; the latest developments in the field of processing large data arrays and systematization of technological processes that allow you to quickly and efficiently operate information.

5. References

[1] FATF Annual Report 2020-2021 This report summarizes the work of the Fi-nancial Action Task Force (FATF) from 1 July 2020 to 30 June 2021. URL: www.fatf-gafi.org/

[2] FATF Recommendations. Financial Action Task Force (FATF): website. URL: https://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)

[3] B. Geedman, S. Flaxman, European union regulations on algorithmic decision-making and a right to explanation, 2016.

[4] D. Kamarinou, C. Millard, J. Singh, Machine learning with personal data: Profiling, decisions and the EU General Data Protection Regulation, URL: http://www.mland the law.org/papers/kamarinou.pdf.

[5] C. Kuner, D. J. B. Svantesson, F. H. Cate, O. Lynskey, C. Millard, Machine learning with personal data: is data protection law smart enough to meet the challenge, International Data Privacy Law, Volume 9, 2017.

[6] S. Gao, D. Xu, Real-Time Exception Management Decision Model (RTEMDM): Applica-tions in Intelligent Agent-Assisted Decision Support in Logistics and Anti-Money Laundering Domains. Proceedings of the 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA,2010.

[7] J.S. Kolhankar, S.S. Fatnani, Y. Yao, K. Matsumoto, Multi-channel data driven, real-time anti-money laundering system for elec-tronic payment cards. U.S. Patent No. US 8,751,399 B2, URL: https ://patent images storage googleapis .com/20/52/22/4f12c 57929 b368/US8751399.pdf.

[8] M. Webber, J. Chen, T. Suzumura, A. Pareja, T. Ma, H. Kanezashi, T. Kaler, C.E. Leiserson, T.B. Schardl, Scalable graph learning for anti-money laundering: a first look, 2018.

[9] Z. Gao, M. Ye, A framework for data mining-based anti-money laundering research. Journal of Money Laundering Control, Volume 10, 2007, pp. 170-179.

[10] S. Gao, D. Xu, H. Wang, Y. Wang, Intelligent Anti-money Laundering System. Proceedings of the IEEE International Conference on Service Operations and Logistics and Informatics, Shanghai, Peoples Republic of China, 21–23 June 2006, 2006, pp. 851–856.

[11] S. Gao, D. Xu, Conceptual modeling and development of an intel-ligent agent-assisted decision support system for anti-money laundering. Ex-pert Systems with Applications. Vol. 36, Issue 2,

2009, pp 1493-1504. URL:
https://www.sciencedirect.com/science/article/pii/S0957417407005891/
[12] T. White, Hadoop: The Definitive Guide (1st ed.). Newton: O'Reilly Media Inc, 2009.
[13] S. Owen, R. Anil, T. Dunning, E. Friedman, Mahout in Action. Greenwich: Manning Publications Co, 2011.
[14] M. Zaharia, M. Chowdhury, M.J. Franklin, S. Shenker, I. Stoicam Spark: cluster computing with working sets, Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing (HotCloud'10), Boston, Massachusetts, USA, June 2010, 2010, pp. 1–7.
[15] D.P. Lucia, M. Donato, The risk-based approach in the new European anti-money laundering legislation: a law and economics view. Review of Law & Economics, 5(2), 2009, pp. 31–52.
[16] T. H. E. Helmy, M. Z. Abd-El Megied, T. S. Sobh, K. M. S. Badran, Design of a detecting money laundering and terrorist financing. International Journal of Computer Networks and Applications, Volume 1, Issue 1, 2014, pp. 15–25.
[17] S. Gao, D. Xu, H. Wang, Y. Wang, Intelligent Anti-money Laun-dering System. Proceedings of the IEEE International Conference on Service Operations and Logistics and Informatics, Shanghai, Peoples Republic of China, 21–23 June 2006, 2006, pp. 851–856.
[18] Q. Rajput, N. S. Khan, A. Larik, S. Haider, Ontology based expert-system for suspicious transactions detection". Computer and Information Science, Volume 7, 2014, p.103.
[19] T. H. Moustafa, M. Z. A. El-Megeid, T. S. Sobh, K. M. Shafea, Anti money laundering using a two-phase system. Journal of Money Laundering Control, Volume 18, Issue 3, 2015, pp. 304–329.
[20] T.G. Ivanova, Zabezpechennya bezpeky informacii u galuzi bankivsjoidiialnosti yak element rozvytku cyfrovoi ekonomiky v Ukraini, 2018, URL: http://nbuv.gov.ua/UJRN/molv_2018_7(1) 62.
[21] M. I. Zubok, Bezpeka bankivskoi diyalnosti, 2002, URL: http://www.megabank.ua/articles/rules/information_security_policy.pdf.
[22] Cybersecurity policy PAT PIB, URL: http://www.pinbank.ua/wpcontent/uploads/2017/02/Polityka_IB_2016_2.0_2_KT-1.pdf.
[23] Pro organizaciu zahodiv zabezpechennya informaciinoi bezpeky v bankivskyi systmi Ukrainy, 2017, URL: https://bank.gov.ua/document/download?docId=56426049.
[24] Typologichne doslidzennia: Ryzyky vykorystannia gotivky, URL: http://www.sdfm.gov.ua/content/file/Site_docs/2018/20180103/2017%20Nalichka.
[25] Typologichne doslidzennia: Ryzyky teroryzmu I separatyzmu, URL: http://www.sdfm.gov.ua/content/file/Site_docs/2018/20180103/typ_terror.pdf.