Analysis of International Experience in Building Anti-Money Laundering and Counter-Terrorist Financing Mechanisms in the Digital Economy

Vladimir Ivanovich Avdiysky[a] and Vyacheslav Mikhailovich Bezdenezhnykh[b]
Department of Economic Security and Risk Management of the Faculty of Economics and Business, Financial University under the Government of the Russian Federation, Moscow, Russia

Keywords: Financial monitoring, AML/CFT system, financial intelligence, Federal Financial Monitoring Service (Rosfinmonitoring), databases.

Abstract: The objective of this paper is to analyze foreign experience in building anti-money laundering and counter-terrorist financing mechanisms to improve Russian AML/CFT legislation and government policy aimed at enhancing the effectiveness of anti-money laundering efforts under the current conditions of digital transformation. The tasks that are expected to be accomplished in order to meet the objective: analysis of the existing foreign methodologies for the collection, analysis and pre-checking of data on financial and economic transactions involving funds or other assets of an illegal or economically inappropriate nature; substantiation of the need to transform state policy in the sphere of cooperation with foreign countries and international organizations in the field of AML/CFT; formulation of proposals for the formation of a framework for digital info-analytic and organizational and methodological state control of measures to detect and suppress the legitimization (laundering) of proceeds of crime. Theoretical foundation of the study consists of the works of domestic and foreign criminologists, legal scholars, economists, sociologists and political scientists dealing with the problems of combating money laundering, identification and elimination of causes and conditions contributing to the commission of these offences, countering corruption, theft, fraud, drug trafficking and other offences for the purpose of untaxed income.

1 INTRODUCTION

Practice shows that in today's environment, financial monitoring, being a unique and very effective tool, allows for the effective use of the financial system in the fight against crime and for tracing virtually any offence where there is a financial trail using the money movement chain – in Russia this institution has been in use relatively recently. There is no doubt that since the creation of the Federal Financial Monitoring Service, and to this day, Russia has done a lot of work to improve and develop the efforts in AML/CFT, including creating mechanisms to facilitate the use of financial information in the fight against crime. However, an objective data analysis shows that it is not all that optimistic. There is certainly much to report from the point of view of establishing these institutions, but there are also a number of problems that need to be addressed quickly. Unfortunately, as of today, in our country there are still:

- low efficiency of the entire system in terms of convictions and confiscation of the proceeds of crime;
- inefficient and highly selective monitoring of financial transactions of officials and businessmen associated with them, as well as the intermediaries;
- lack of proper efficient cooperation between the executive authorities involved in the anti-money laundering and counter-terrorist financing system.

All this has an extremely negative impact on Russia's economic and national security as a whole. In this regard, it appears that the analysis of foreign

[a] https://orcid.org/0000-0002-6685-3589
[b] https://orcid.org/0000-0001-9827-6328

Avdiysky, V. and Bezdenezhnykh, V.
Analysis of International Experience in Building Anti-Money Laundering and Counter-Terrorist Financing Mechanisms in the Digital Economy.
DOI: 10.5220/0010699200003169
In *Proceedings of the International Scientific-Practical Conference "Ensuring the Stability and Security of Socio-Economic Systems: Overcoming the Threats of the Crisis Space" (SES 2021)*, pages 303-311
ISBN: 978-989-758-546-3
Copyright © 2022 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

experience in building anti-money laundering and counter-terrorist financing mechanisms, taking into account the current challenges and threats, is relevant and will make it possible to develop specific proposals for improving this activity in Russia.

2 MATERIALS AND METHODS

Analysis of the formation of national authority liaison systems in countries that have been successfully assessed by the FATF shows that most foreign jurisdictions establish a specialized national system within which a financial monitoring service operates. However, the international AML/CFT standards developed by the UN, the FATF, the EU, the Wolfsberg Group and the Basel Committee have a decisive impact on the legal and organizational framework. They become the source of the legal framework for establishing a national system, which leads to the existence of common features of a financial monitoring system in individual states. The established international and national AML/CFT requirements respectively form the rules and guidelines specifically for companies. In these conditions, the performance of well-functioning systems is aggregated in the indicators of cooperation in sharing necessary information in the areas of contact listed above.

In this regard, it is useful to consider the UK's experience in ensuring effective law enforcement cooperation, where there is a database containing information on suspicious transactions, which can be directly accessed by the police.

A similar system exists in the United States, where authorities actively and routinely use financial intelligence data and other information to identify suspects, gather evidence in investigations, and trace illicit proceeds related to ML/TF/PWMD, and predicate offences.

The greatest US strength in this area is the information processing centres and joint working teams that bring together federal, state and local partners in an inter-agency environment. Information processing centres serve as hubs for receiving, analyzing and gathering threat information, sharing such information and dissemination of important intelligence data on indicators of wrongdoing (based on financial information, national intelligence and information provided by local, state and regional authorities).

It should be emphasized that the US authorities use not only financial intelligence, but also other information from a variety of sources:

a) FinCEN database is the main financial intelligence repository in the United States, containing information on suspicious transactions, currency transaction reports, reports on international transportation of cash or monetary instruments, reports on foreign bank and financial accounts, and reports on monetary payments over USD 10,000, received during transactions, or in the course of business;
b) FEDWIRE: The Federal Reserve Bank of New York can search names, addresses and account numbers for any money transfers that are made through this system;
c) CHIPS (Clearing House Interbank Payments System): searching the CHIPS network through which bank transfers are made;
d) tax returns;
e) correspondent bank accounts;
f) operational databases that include data from prosecutors, investigative intelligence, criminal records and mutual legal assistance requests and other data;
g) information from company, vehicle and property registries as well as data from publicly available sources.

FinCEN provides direct, independent access to its data for representatives of relevant federal, state and local oversight agencies. Nine key authorities are given enhanced access, with full- and part-time staff provided, enabling the authorities to collaborate directly with FinCEN's analysts.

The situation in Austria is different, due to the limited analytical capacity and legal restrictions imposed on the Austrian Financial Intelligence Unit, performing only the most general analysis of financial information, which is also reflected in the lack of its own database that would allow conducting in-depth investigations. The FATF has therefore recommended that the jurisdiction develop its own financial information database and make it available to law enforcement agencies.

Law enforcement agencies in China, as is the case with Russia, can obtain information from the FIU upon request and do not have liaison officers at the AML Analysis and Monitoring Centre, the AML Bureau and the thirty-six provincial branches of the National Bank of China to facilitate such indirect access to information, which affects the speed with which anti-money laundering measures are implemented.

It is further noted that current financial data from financial intelligence agencies allow China to launch new investigations into predicate offences and

ML/TF/PWMD crimes, although this is often not the case due to a lack of direct access to financial information databases and the need to go through bureaucratic procedures to generate requests. Thus, the statistics reviewed by the FATF show a 100% success rate of investigations based on requested materials, while the number of proactively submitted materials has not resulted in a comparably high number of investigations and has not contributed to successful criminal investigations conducted by law enforcement agencies – a similar situation is observed in Russia.

Analysis of materials regarding Italy show that law enforcement authorities in the country receive all suspicious transaction reports, technical reports (analysis materials used only as financial intelligence information, but not as evidence and proof) and other information indicating the risk level and carry out preliminary investigations to confirm or refute the conclusions drawn by the financial intelligence unit. FATF stresses that due to the restriction on the use of technical reports and the provision of information on "clean" transactions, law enforcement agencies are forced to repeat the examination of submitted data, a situation very similar to that in Russia, where Rosfinmonitoring submits information to the Ministry of Internal Affairs with a note "not to be included in the criminal case file".

The technical reports (analysis material) and STRs provided by the financial intelligence unit can only be used as financial intelligence information (i.e. they cannot be used as evidence or proof). Unlike most foreign financial intelligence units, the Italian FIU is obliged to provide to the relevant authorities (i.e. the Guardia di Finanza and the Antimafia Investigative Directorate) the STRs which it considers as unconfirmed and for which the verification has been discontinued (i.e. "closed" STRs). "Preliminary investigation", conducted by Guardia di Finanza and the Antimafia Investigative Directorate, includes verification of information provided by the FIU in databases of law enforcement bodies. "Preliminary investigation" of "closed" STRs is not carried out in all cases, however, such STRs are still provided to the Guardia di Finanza and the Antimafia Investigative Directorate in case they are required in specific circumstances.

Spanish law enforcement agencies, on the other hand, have direct access to a wide range of financial and other data, similarly to the USA [18]: the state register of land (cadastre), companies, real estate; the register of life insurance policies of the Ministry of Justice; the unified computerized directory of notaries (containing accurate legal and beneficial ownership information and to which law enforcement agencies have real-time access); the social security registry (TGSS); the database of the Bank of Spain on payment balances; the database on holders of financial assets.

Thus, a cross-section of different international practices has shown that the most effective measure of interactions is the following system:

1) FIU performs accumulation and analysis of financial information;
2) A single database is created, containing not only FIU information, but also tax, customs, banking and other information from various public and private registers.
3) Interaction between authorities is based not only on requests, but also on the provision of effective proactive investigations by the FIU, which can be the basis for preliminary investigations, but also on the provision of real-time access to the database.

So, by comparing the analysis data obtained as a result of researching the mechanism of interaction within the domestic AML/CFT system and international experience, it becomes possible to compare strengths and weaknesses, opportunities and threats to the development of the current level of interaction of federal executive bodies in detecting and combating money laundering.

Table 4 presents such a comparison in the form of a SWOT analysis, based on both the reviewed academic literature and professional materials, as well as a survey by Rosfinmonitoring experts in the field.

Table 4: SWOT-analysis of the interaction of federal executive bodies in Russian AML/CFT system

Strengths	Weaknesses
1. To date, a functioning system of inter-agency cooperation and interaction has been established, implemented through the Inter-agency Commission on Combating Money Laundering, Terrorist Financing and the Financing of Proliferation of Weapons of Mass Destruction, the Inter-agency Working Group on Combating Illicit Financial Transactions, the Inter-agency Commission on Countering Extremism, the Inter-agency Commission on Countering the Financing of Terrorism, State Anti-Drug Committee, National Anti-Terrorism Committee, as well as cooperation agreements with 27 organizations and government agencies.	1. The interaction involves constantly fine-tuned forms of real time communication. The system prioritizes the exchange of information through request-response cooperation. 2. Although the reporting entities and the responsible authorities have sufficient human resources, law enforcement agencies do not have the expert knowledge in the field of crimes related to complex ML/TF/PWMD schemes.

Table 4: SWOT-analysis of the interaction of federal executive bodies in Russian AML/CFT system (cont.).

2. Based on Federal Law No 115-FZ and Russian Government Decree No. 492, dated May 29, 2014, high qualification requirements for financial monitoring specialists have been developed, and through cooperation agreements with universities, qualified AML/CFT personnel are being trained, which has enabled the system to be filled with high-level analysts. 3. Over the years of development of the AML/CFT/PWMD mechanism in Russia, a serious methodological basis has been accumulated, based both on the FATF Recommendations and on our own experience, which is expressed in the development of relevant laws, regulations of the FFMS, Bank of Russia, Assay Chamber, Roskomnadzor, law enforcement agencies and other documents and materials.	3. There is a lack of complete methodological coherence in referring the results of financial investigations to law enforcement agencies for preliminary investigation and further legal action for fair punishment, and confiscation.
Opportunities (areas) for the development	**Threats (risks) for the current interaction**
1. Legislation should be harmonized to allow for effective forms of cooperation between Rosfinmonitoring and the law enforcement agencies, including through the development of the institution of interim measures and the creation of a unified methodology for financial and preliminary investigations. 2. Use of new (digital) methods of interaction in the implementation of cooperation between the federal executive bodies in the field of AML/CFT by providing real-time access to the federal database. 3. Creating sufficient awareness of the dangers of ML/TF/PWMD offences and social intolerance towards such offences.	1. Lowering of the priority of detecting legitimization as a politically biased trend based on the corrupt interests of government institutions. 2. Creation of a criminal misdemeanour institution making it possible to evade certain money laundering offences. 3. The impact of "double standards" in the AML/CFT/PWMD-related international interactions between FIUs.

Based on the SWOT analysis, it can be concluded that, in addition to the above proposals, in present-day conditions the most effective methods and tools to improve the effectiveness of the existing AML/CFT/PWMD interaction system are those based on modern digital solutions that allow for the fastest exchange of necessary information, which must be processed and analyzed in accordance with a common methodology, in order to avoid repetition of actions by different authorities (e.g. the situation with the stamp "not to be included in the criminal case file" on the results of financial investigations). These measures are particularly necessary at a time of digital transformation, when a potential offender has the ability to commit malicious acts in an extremely short period.

3 RESULTS AND DISCUSSION

When researching the market for digital financial and security solutions, it should be noted that the development of modern financial technology is far ahead of AML/CFT regulation. What is also clear is that the second decade of the twenty-first century has seen an explosion of digital technologies that have literally entered the lives of everyone on the planet. The first descriptions of the ongoing process were published in the '90s by Don Tapscott in his book «The Digital Economy: Promise and Peril in the Age of Networked Intelligence", and a little later by Nicholas Negroponte in "Being Digital", where the digital economy is described as "bits instead of atoms". To date, an in-depth scientific view of the phenomenon of the "Great Digital Revolution", linked to the concepts of "Industry 4.0" and "Society 5.0" as it is also known as the fourth industrial revolution, which certainly brings many challenges and threats to modern humanity, has already been formed.

The digital economy is already going far beyond the Internet or process automation to include hyperconnectivity, the Internet of things, big data, advanced analytics, wireless networks, mobile devices and social media, and so on. In this regard, the global phenomenon of digitalization is leading to fundamental changes in business models, in the way the government works and in the way the social relations are organized.

Thus, domestic academics already estimate that "the information and communications technology complex is growing at a rate of around 30% a year", a clear example being the United States, where the level of digitalization is now estimated at a third of the country's GDP, amounting to around USD 6 trillion. – such trends set the appropriate trends in global economic development, making the 6th technological stage the growth driver. Thus, the overall focus on digitalization lays down a powerful vector for the development of both the economy of individual sectors and the country as a whole. Digitalization and economic growth are closely linked concepts in the current environment.

The digitalization in the long term entail the automation of the implementation of some activities in various fields: financial, industrial, political, socio-cultural and others. The capital assets of enterprises, renewed due to robotic automation, will be able to

carry out their functions without or with minimal human intervention.

For example, a research by KPMG, shown in Table 5, shows that the private sector is already fully engaged in the digitalization trend, actively developing this area, which, if it achieves the necessary investment levels, will become one of the main drivers of economic growth: its contribution to GDP growth will exceed 50% by 2030, driven by improvements in the efficiency and competitiveness of other economic sectors. Overall, Russia's gross product will increase by 34% between 2017 and 2030, precisely because of the information industry and the digitalization of sectors of the economy.

Table 5: The use of digital technology in the Russian economy

Technology	Overall	Retail	Telecom	Financial institutions	Metallurgy	IT	Oil and gas	Transport
Big Data	68%	55%	100%	84%	67%	100%	50%	14%
Chat-bots	51%	50%	75%	60%	33%	40%	50%	29%
Robot automation	50%	40%	100%	56%	83%	20%	50%	14%
OCR	36%	20%	25%	56%	67%	1%	50%	14%
AI	28%	5%	75%	40%	17%	80%	25%	1%
IoT	24%	15%	100%	12%	50%	20%	25%	29%
VR/AR	21%	20%	25%	16%	33%	40%	25%	14%
Blockchain	19%	20%	25%	32%	1%	20%	1%	1%

Source: compiled by a team of contributors.

In the financial sector, however, there are particularly striking trends indicating the enormous potential for digital financial services (or fintech – "a complex system combining the new technology and financial services sector, start-ups and related infrastructure"), which will be based, as the Bank of Russia states in its study, on the mobile technology, Big Data, robots, AI, biometrics, etc. Firstly, it is defined that by 2021, 35-50% of bank customers will use mobile banking; secondly, 82 percentage points of financial institutions are going to increase interaction with fintech companies within 3-5 years; thirdly, 56% of financial sector representatives position digital transformation as the basis of their business strategy; fourthly, investment in fintech companies in the US in 2016 - 2013 has doubled to a record USD 24.7 bln.

Also under the Digital Economy national project, BIG DATA technologies are included in the list of priority technologies, along with artificial intelligence and neurotechnology. In November 2017, experts developed a draft "Convention on Robotics and Artificial Intelligence" (adopted by the State Duma Committee on Economic Policy, Industry, Innovation and Entrepreneurship in the first half of 2018), which combined all the currently existing principles for regulating the industry into one system.

Thus, the digitalization process in Russia today is an undeniable reality that must also be used to create the most effective AML/CFT/PWMD system, including the establishment of digital inter-agency cooperation.

Touching on the oversight practices already today, the digital transformation offers great opportunities to realize this goal.

For example, RegTech, which includes compliance, identity management and control, risk management, regulatory reporting and transaction monitoring, is already a technology that helps financial services firms comply with regulatory requirements and financial compliance rules. It allows businesses to build a constructive dialogue with regulators, which is necessary against the background of radical digital transformation.

SupTech, on the other hand, includes real-time analysis of credit institution data on various transactions in order to detect fraud, analyze the affiliations of persons of interest, including borrowers, predict cash demand and, based on payment data, draw conclusions regarding the stability of credit institutions. Practice shows that this digital technology can also be used extensively for financial intelligence, fiscal and operational information on the illegal activities of a business entity.

Thus, the technology makes it possible to automate administrative procedures, improve the reporting quality and enhance the decision-making system. Therefore, it becomes possible to carry out automated remote verification of certain economic entities in a continuous manner by creating customized algorithms.

Of course, the availability of technical and technological capabilities to implement RegTech and SupTech provides conditions for, but does not

guarantee the improvement in the quality of control and supervisory and regulatory activities, since these are only tools or a "superstructure" of the overall public administration system, so the crucial role will be played by qualitative changes in the legal framework, in the organization and methodological support of business processes and their adaptation to new conditions.

Indeed, advanced big data analysis has the potential to detect potentially criminal transactions not only in the traditional financial system, but also in its virtual superstructure by forming special criteria or risk indicators and training neural networks in this way, although the overall impact of digitalization on money laundering is clearly mixed: not only are the mechanisms of financial institutions and, therefore, money laundering schemes becoming more complex, but new ways of carrying out control and oversight functions are also emerging, although unfortunately, Russian regulators are now lagging behind the "miscreants" in terms of realizing the potential of modern technology for their own purposes, which means that the volume of legalized assets is only increasing.

It is also important to note that the application of digital technologies is only possible when the traditional anti-money laundering system works effectively and is ready for the implementation of an "add-on" designed to simplify the technical work of financial monitoring specialists by providing the ability to process large volumes of information at lower cost in an automated mode, and it is vital to consider information security risks, which is now possible with the introduction of special DLP software, and the increasing complexity of the management system due to the use of new solutions.

At the same time, as can be seen from the analysis of international practices, leading countries around the world, such as the US, have already developed specific legal and digital solutions to ensure compliance with the necessary AML/CFT/PWMD regulations. This experience should be used and Russia.

So, firstly, it would seem rational to develop a single model platform for processing financial information at the level of reporting entities in order to make high technology available to the whole sector, which would increase the efficiency of anti-money laundering system. Secondly, it is necessary to improve the existing federal database by combining it with the proposed complex for the reporting entities and providing specialized access for other competent authorities, following the example of the US, Spain and other countries.

Having formulated the general directions for the development and improvement of the existing main aggregator of financial information collection and analysis - the federal database of the FFMS - it is necessary to describe in detail the structure and functioning mechanisms of the proposed system.

While stipulating at the outset the availability of information from this database to various authorities, it should be noted that bank secrecy will be respected, as it will transform into a business secret or secrecy of the investigation. We would also like to immediately note our support for a unified household database [14], given that a federal database could be the basis for such a "unified base", following the example of the US, including not only financial information on suspicious transactions, but also the following information:

- Unified State Register of Taxpayers;
- Unified National Register of Legal Entities;
- Information from the judiciary and law enforcement agencies;
- Information on education and academic degrees, including those obtained abroad;
- Data on compulsory pension and health insurance;
- Data on registration with the Federal Service for Labour and Employment for the unemployed and on the granting of a work permit for foreigners;
- Information on the registration of private entrepreneurs and self-employed persons;
- Numbers assigned when a citizen is registered with the tax office;
- Information on military registration;
- Tax and banking information.

In order to ensure the security of this database, it is necessary, as mentioned above, to develop a unified inter-agency regulation defining not only the procedure for interaction between agencies, but also the procedure for the formation and use of the database. At the same time, a special training of Rosfinmonitoring staff on the system and instructing on the secrecy regime should be provided for, with their further secondment to other authorities, accessing the system from a special computer device equipped with an information security system to counter data leaks (DLP system), which would block any unauthorized access to the system and any illegitimate data uploads. It is also possible to configure the access system to prevent the acquisition of information containing state secrets relating to the country's political leaders and other designated individuals, the access to which could result in critical damage to Russia's national security.

Based on this analysis, three modes of access to the system are envisaged:

1) Reporting entity, which should use this software to track transactions carried out in accordance with Law No. 115-FZ, blocking them or reporting them to Rosfinmonitoring if necessary. This stage is formulated as the processing of transaction reports by means of an automated selection of the riskiest transactions, after processing of which and confirmation of such status by the officer responsible for the implementation of financial monitoring measures, an event is created, expressed in the identification of a suspicious transaction, and sent to Rosfinmonitoring.

2) Federal Financial Monitoring Service as an operator and a database administrator having access to all the operations that took place in the system, but receiving reports of recorded events related to the identification of suspicious transactions, which are further processed by AI based on UEBA system (User and Entity Behavioral Analytics), and after confirmation of abnormality the events become incidents and are transferred to the employee for further verification and financial investigation.

3) Other competent authorities which are granted access through inter-agency cooperation and which receive the full scope of analytical financial information without the right to administer the base, but with the ability to conduct their own investigations. Access granted to these authorities, through seconded FFMS analysts, may be restricted in accordance with legal requirements by the administrator of the database – Rosfinmonitoring.

Figure 3, for example, graphically illustrates the functioning of the proposed system with the designation of responsibilities, the flow of information and the rules for processing it, as well as the availability of this information to various entities subject to inter-agency cooperation.

In addition, there appears to be a need to transition from using a federal database for transaction analysis to a mechanism used in Europe and the US called the "People-Centric Approach". The approach is not based on looking for suspicious transactions, but on comparing the cash flows of an individual entity or individual. In other words, the comparison of its income and expenditure. It is clear that the combination of both techniques, using modern digital technology, will yield the greatest results in the field of anti-money laundering. This is why the developed mechanism, based on transaction analysis with the addition of in-depth and comprehensive information on a person or entity stacked from other public registers and databases, will make it possible to analyses the behaviour of a particular subject for anomalies using the UEBA system, as well as to build graphs of that subject's links with other persons for the most expeditious investigations.

Speaking of the UEBA (User and Entity Behavioral Analytics) function, we note that it is a class of systems that allows, based on data sets about subject-users, using machine learning algorithms and statistical analysis, to build their behavior models, forming user patterns (criminal behavior, conscientious behavior, etc.), identify deviations from these models, both in real time and retrospectively. So, the UEBA systems, architecturally, solve 4 main tasks:

- Applied analytics of data from various sources, both simple statistical and advanced, using machine learning techniques, in real time and/or at specific intervals;
- Rapid identification of irregularities, most of which are not detected by classical analysis tools;
- Prioritization of events based on risk level for faster response by administrators;
- A more efficient response to events by providing administrators with enhanced incident information, including all entities that were involved in the abnormal activity. Based on the above, the core of any UEBA system includes technologies for dealing with large data arrays.

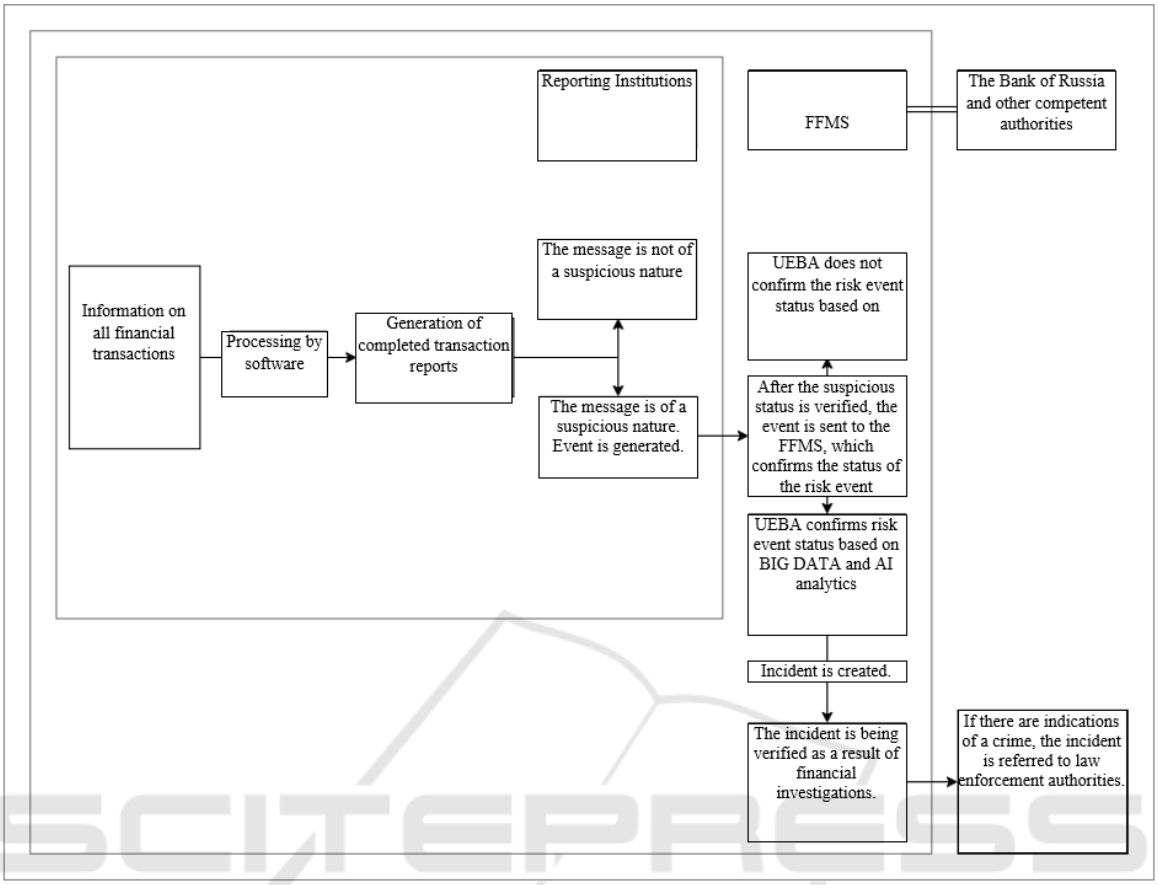

Figure 4: Operation scheme of the proposed system. Source: developed by the author.

SCITEPRESS
SCIENCE AND TECHNOLOGY PUBLICATIONS

4 CONCLUSIONS

Thus, the most comprehensive mechanism of effective interaction between federal executive bodies in detecting and combating money laundering is proposed, based on the implementation of a set of organizational and practical measures using new digital forms of communication, which are fully implemented based on Rostelecom-Solar technology, with the analytical support from relevant experts.

In summary, the proposed measures would improve the domestic AML/CFT/PWMD system in full compliance with the FATF recommendations described in the 2019 Russian Federation Mutual Evaluation Report:

1. Supplementing the information available to Rosfinmonitoring by using other data sources.
2. Enhancing law enforcement agencies' use of financial analysis and other relevant information to better identify bribery and abuse of power, consistent with the risks identified in the national money laundering risk assessment report.
3. Enabling the investigation and prosecution of offences involving sophisticated money laundering schemes to be prioritized, with intelligence and in-depth advanced analytical techniques to support effective detection.
4. With UEBA and a People-Centric Approach, including link graph tools, it will be possible to conduct the most comprehensive analysis of sources of funds and their possible links to predicate offences, including corruption offences.

REFERENCES

Presidential Decree No. 203 dated 09.05.2017 "On the Strategy of the Information Society Development in the Russian Federation for 2017-2030", www.consultant.ru/

Federal Law No. 273-FZ "On Combating Corruption" dated December 25, 2008, http://www.consultant.ru/

Federal Law No. 115-FZ "On Countering the Legalisation (Laundering) of Criminally Obtained Incomes and the Financing of Terrorism" dated August 07, 2001, http://www.consultant.ru/

Austria Mutual Evaluation Report – 2016. FATF, https://mumcfm.ru/

Spain Mutual Evaluation Report – 2014. FATF, https://mumcfm.ru/

Italy Mutual Evaluation Report – 2015. FATF, https://mumcfm.ru/

PRC Mutual Evaluation Report – 2019. FATF, https://eurasiangroup.org/

Russian Federation Mutual Evaluation Report – 2019. FATF, https://eurasiangroup.org/

US Mutual Evaluation Report – 2016. FATF, https://mumcfm.ru/

Official website of the Federal Financial Monitoring Service. Rosfinmonitoring, http://www.fedsfm.ru

Official website of the Japan Financial Intelligence Centre (JAFIC), https://www.npa.go.jp/

Eskindarov, M.A., Abramova, M.A., Maslennikov, V.V., Amosova, N.A., Varnavsky, A.V., Dubova, S.Ye., Zvonova, Ye.A., Krivoruchko, S.V., Lopatin, V.A., Pischik, V.Ya., Rudakova, O.S., Ruchkina, G.F., Slavin, B.B., Fedotova, M.A., (2018) Directions of development of financial technologies in Russia: expert opinion of the University of Finance. *In The world of the new economy*. 2. pp. 6-23.

Money Laundering Stages. Finance and Credit, https://pravo.studio/

National risk assessment of money laundering and terrorist financing 2017, https://assets.publishing.service.gov.uk/

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS