FINANCIAL SECURITY

NO. 35 SEPTEMBER 2022

M. SHADAEV:

"Russia is successfully creating conditions for the large-scale digital transformation of the economy sectors, including the financial monitoring"

CONTENTS

Cover Topic - Digital AML/CFT transformation

Digital Transformation in the Process of AML/ CFT Personnel Training

News Block

EDITORIAL BOARD

Chairman of Editorial Board

Yury Chikhanchin

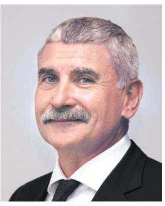
Deputy Chairman of Editorial Board

Vladimir Ovchinnikov

Members of Editorial Board

Yury Korotkiy

Galina Bobrysheva



Vladimir Glotov

Margarita Andronova

Ivan Kornev

Oleg Krylov

Sergey Teterukov

Alexey Petrenko

German Neglyad

DEAR READERS!

We present a new issue of the “Financial Security” journal, dedicated to the topic of digital transformation of the anti–money laundering and counter financing of terrorism (AML/CFT) system.

Crime transforms and acquires new forms using the opportunities of the global Internet and the development of the digital economy technologies. On the other hand, the new technologies increase the speed and quality of the work in the fight against financial crimes. Therefore, we strive to introduce the innovative technologies into the activity of the Russian AML/CFT system and to ensure the update and the effectiveness of the appropriate standards’ compliance.

Studying the models of the criminal activity and relying on the advanced methods of the identification, disclosure and investigation of the violations related to the legalization (laundering) of criminal proceeds, we see the need to combine the efforts of the government authorities and representatives of the private sector to improve the effectiveness of the AML/CFT system through the digital transformation.

Current issue of our magazine is dedicated to this topic.

Director of Rosfinmonitoring,
Chairman of the editorial board
Yuri Chikhanchin

COVER TOPIC — DIGITAL AML/CFT TRANSFORMATION

MAKSUT SHADAEV THE MINISTER OF THE DIGITAL DEVELOPMENT, COMMUNICATIONS AND MASS MEDIA

Maksut Shadaev

Dear colleagues!

Announced in 2017 by the President of the Russian Federation Vladimir Putin, the ‘Digital Economy’ program is actively changing all spheres of the Russian people life. During the Program implementation, we pay special attention to the regulation of the digital environment, information infrastructure and security, the digital technologies’ development, formation of the human resources for the digital economy and the digital government administration.

We have launched the all-Russia cyber hygiene program to attract attention of the Russian nationals to the cybersecurity issues and to form their skills of the safe behavior in the Internet. The program includes monitoring of the level of the citizens’ literacy and improving the civil servants’ skills on the information security, teaching children and teenagers’ the behavior in the Internet.

The Ministry of the Digital Development, Communications and Mass Media actively counteracts the telephone scammers: both with the help of the legislative initiatives and with the help of the technical projects for the systemic solution of this problem.

To overcome the shortage of the IT personnel, we pay special attention to the training of the school graduates and students. By the year 2030, 1.2 million pupils will be able to learn the programming languages in free-of-charge two-year courses. The students of any specialties will have the opportunity to get additional IT-sphere qualifications. The "digital sub-departments" will be formed in more than 100 universities, where more than 900 thousand trainees will be able to study.

The availability of the Internet also increases: last year we have created the communication infrastructure in more than 38 thousand settlements in 85 country regions. Thus, accordingly the level of the digital literacy of the population is increasing.

Russia is successfully creating conditions for the large-scale digital transformation of the economy sectors, including the financial monitoring. The digitalization of the popular services makes daily life of the citizens more comfortable and safe, simplifies their interaction with the government and ensures that any application will be answered. I am sure that we will continue to develop in this direction actively.

THE FINANCIAL INTELLIGENCE TRANSFORMATION IS THE FOUNDATION OF THE ROSFINMONITORING UIS[1] DEVELOPMENT

The AML/CFT system[2] effectiveness is determined by its ability to timely identify new money laundering and terrorist financing risks, objectively and qualitatively assess them and implement the mitigation measures. In modern conditions, under the financial instruments and technologies development blast, when the information space is constantly being transformed, and cash flows are intensively changing in form and volume, the information system containing data and knowledge is the most powerful weapon of the financial intelligence officers in countering ML/TF threats[3]

Mikhail Fedorov,
Head of the Rosfinmonitoring Department of the Information Technologies Development

Mikhail Fedorov

When considering the Rosfinmonitoring UIS, it is necessary to take into account the fact that the Federal Financial Monitoring Service does not provide mass and socially oriented services to the Russian population.

The Rosfinmonitoring UIS began to be designed and developed since the establishment of the Service in 2001. The goal was to create an effective tool based on the modern technical solutions, that meets the regulatory framework and the FATF requirements and provides comprehensive information support to Rosfinmonitoring activities and the national AML/CFT system.

The UIS evolution took place in several stages.

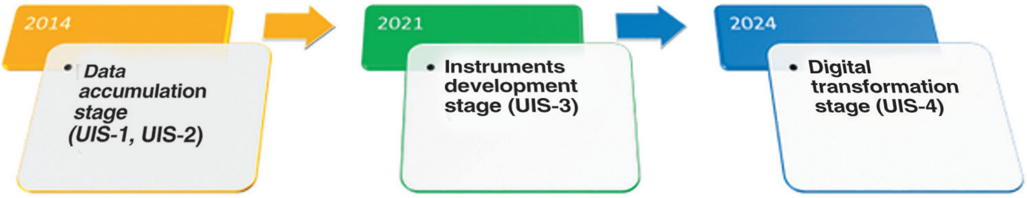
The initial period of the UIS formation (from 2001 till 2014) can be described as the **data accumulation stage** (UIS-1 and UIS-2). The work was carried out in several directions. The regulatory and methodological framework was intensively

[1] Unified information system.

[2] Countering the legalization (laundering) of proceeds from crime and the financing of terrorism.

[3] Legalization (laundering) of proceeds from crime and financing of terrorism.

Evolution of the Rosfinmonitoring UIS


2014
Data accumulation stage (UIS-1, UIS-2)
2021
Instruments development stage (UIS-3)
2024
Digital transformation stage (UIS-4)

developed. With the foreign partners help, the basic computing and communication infrastructure was created. Concurrently, the basic data storage and analytical subsystems have been developed. In 2008, the Service received first electronic messages on the financial transactions and deals through the BANKOM channel. On average, we received about 40 thousand messages per day. 3 thousand requests for additional information in paper form were sent to banks. 28 thousand requests were received from the law enforcement agencies. In a routine mode, two dozen formalized information resources were received from the various sources, mainly the Federal executive authorities.

The first stage main achievement was the correct choice of the design solutions related, in particular, to the subsystem of the external interaction and the centralized data storage, which later allowed us to move to the system further development and the consistent increase of its capabilities on a cost-effective basis.

Between 2014 and 2015, the Service was assigned new ambitious tasks within the functions of the National Assessment Center of the National Security Threats and Risks, related to ML/TF , such as monitoring of the budget funds expenditure in the implementation of the state defense order, monitoring of the strategically important organizations financial transactions, as well as countering the ITO “the ISIL” increased activity. In addition, an important factor in those years was the need to prepare the national AML/CFT system for the FATF mutual evaluation in 2019.

The information system operating at that time needed conceptually new solutions that would allow it to integrate significant amounts of incoming information on the other qualitative level and create special software for the effective work of the AML/CFT system analysts. The government supported the decision to start a new stage of the UIS life cycle, which could be briefly described as the **stage of instruments development** (UIS-3).

At this second stage, lasted from 2014 till 2021, the regulatory and methodological bases was enhanced, new technological platforms were rolled out, a risk-based approach, which formed the basis of the NRAC, was introduced. A system of interaction with the reporting entities through the Personal Accounts was created. The Data Assessment Center (DAC) and IT infrastructure have been developed.

A data storage has been designed in the form of the information objects reference registers.

The subsystem for their automatic classification has been implemented.

Interaction with the reporting entities via the portal technologies allowed to eliminate almost entirely the use of the paper documents.

Analytical tools based on the domestic iRule platform have been thoroughly advanced.

The unstructured data processing mechanism has been developed and implemented.

In addition, the approach in the analyst's work has changed. The fundamental difference from the previous UIS versions is the ability to automatically detect, identify and classify information objects from any resources received by the Service. The analyst uses marked-up data and applies tools of macrostatistical, visual and predictive analytics.

Accordingly, the system's ability to process the incoming information has increased significantly. Today we receive and process 15 times more reports per day (600 thousand), including a new type of information — the suspicious activity reports. The flow of the law enforcement agencies requests has increased appreciably (45 thousand in 2020 and 2021, 32 thousand in 8 months of 2022).

In total, the system is able to receive and process about 60 formalized information resources in a regulatory mode.

At the same time, the FATF mutual evaluation process in 2019, as well as the UIS exploitation for five years, highlighted several problematic issues.

The continuous change in the financial operational environment dictates the need for prompt response. Increased level of digitalization and the Internet accessibility, development of new channels and ways of conducting financial transactions, innovative technologies (cryptocurrencies, blockchain, artificial intelligence) require continuous and advanced updating of the AML/CFT environment. In these context, the used tools and resources often are not in line with the digital economy level.

The role of the international risks, including the sanctions, has significantly increased. The AML/CFT sphere has been and remains the most important tool of global and local risks regulation and control of the international and national trends and changes. Against this background, there is an urgent need to create a unified information space with our partners in the BRICS, CIS and EAG.

The successful information interaction of the AML/CFT system participants requires the creation of an effective and secure communication environment.

Thus, in order to solve the strategic task of improving the efficiency of the Rosfinmonitoring information and the AML/CFT systems, the third stage of the UIS life cycle – **the stage of digital transformation**, started in 2020 (planned until 2024). All participants of the AML/CFT system with various development centers should be included in this stage.

First of all, in the same year, the Concept of the UIS development was drafted and approved. Further, in 2021, the design of the updated UIS was finalized.

The basic element of the transformation is the creation of an Intelligent Digital Technology Platform (IDTP). The basis for the IDTP will be the tested and updated Specialized Information Technology Platform (SITP) and the analytical platform iRule.

The change in the functional units' activities paradigm, providing a transition from work with data to operation with knowledge, ensures the intellectual component of the IDTP. For these purposes, it is planned to create and constantly update a knowledge base based on the subject domain ontology, taking into account the objects role models and the contextual zones.

Our practices and capacities related to the predictive analytics and mechanisms to work with the unstructured data will be further developed. At the same time, the analytical tools advancement focuses on a gradual transition from the analysis of transactions to the analysis of financial schemes and flows.

A separate area from which we expect a significant increase in the efficiency of our work is the implementation on the machine learning and artificial intelligence technologies. They will allow us to obtain and apply new knowledge to identify the ML/TF risks, develop the mitigation measures and evaluate their effectiveness. The main task in this direction is the automatic classification and clustering of the financial monitoring objects. At present, space-time analysis mechanisms are being implemented to identify new facts and knowledge necessary to reveal the illegal financial schemes.

In particular, the scheme data bank is being implemented. It will ensure the collective use of the analysis findings in the form of the financial transaction schemes. Moreover, it will allow to record the results of the daily preliminary transaction reports analysis and financial investigations. Last but not least, the use of this tool will create the necessary conditions for the introduction of the machine learning technologies for the purpose of analyzing operations and their participants by forming a layer of reliably marked-up data, and in addition will increase the level of information security when using the FAST visual analysis component.

The updated UIS should change the approach to the analyst's work. His main task will not be to perform routine data processing operations, but to extract new knowledge from the data and bring this knowledge to the decision makers.

The digital component of IDTP implies the rejection of the analog services and transition to the paperless technologies. The Personal Accounts functionality development based on the portal technologies, as well as the use of new versions of the Interagency Electronic Interaction System and the Interagency Electronic Document Circulation system will significantly increase the efficiency and quality of the AML/CFT system participants' cooperation. At the same time, vertical and horizontal interaction based on a service-oriented model will be provided.

An opportunity to develop the applicable data storage and analytical software components and services based on the platform will ensure the *technological component* of the IDTP.

Taking into account the sanctions policy pursued by some foreign states, one of the main tasks of the digital transformation is the *import substitution.* The task of denying imported products related to the state bodies security and steady functioning, has been set at the very high level. At the same time, a systematic introduction of domestic production of server and switching equipment and means of virtualizing resources has already begun. As practice shows, import substitution is a very time-consuming process, involving the identification of many problems and errors in the course of work. At the moment, there is no universal tool that allows you to quickly and efficiently transfer a database from Oracle management system or MS SQL Server DBMS to PostgreSQL. This fully applies to both equipment and information security tools.

In addition, as part of the transformation, it is necessary to form a methodological and technological base for the transition from the model of the functional subsystems of the UIS to a unified environment of the collective work using a project and process approach.

One of the main principles implemented in the UIS should be the *customer-focus* of functions, aimed at both external and internal users. Based on this, the Service began reviewing and describing the internal processes focused on the employees' needs. Guided by the client-focus principle, it is necessary to form a system of preparation and coordination of the regulatory legal acts.

In the conditions of a significant increase in data and information resources, as well as the computational methods development, the Service has the opportunity to implement an *'evidence-based policy'* that provides for administrative decision-making based on the results of scientific research and experiments

The most important element of the updated AML/CFT system should be the *International Risk Assessment Center (IRAC).* Starting from 2023, the functionality implemented in the IRAC will allow to achieve a qualitatively new level of cooperation between the FIUs based on the use of the various types of communications and effective information exchange. It will provide the FIUs senior staff with up-to-date analytical data reflecting the state and trends of the interstate relations, cross-border financial flows and related risks.

In conclusion, it should be noted that the main difficulty in implementing the transformation will not be the choice of new promising technologies, but the high need for a team of new specialists possessing digital culture, who can appear only in a digital society with the development of a knowledge management system in this environment. Competent teams should be result-oriented. Team members must maintain a high rate of updating of knowledge and competencies, as well as possess a professional level involving the functional use of methods and tools for managing processes, projects, software products and the regular solution of complex professional tasks in a digital environment.

Along with this, it is necessary to cultivate the digital culture in the Service - a system of digital values, attitudes, norms and rules of conduct that our employees follow while focusing on data, not opinions and interpretations.

OVERVIEW OF THE REQUIREMENTS OF THE FATF GUIDANCE DOCUMENTS RELATED TO THE DIGITAL TRANSFORMATION OF THE AML/CFT SPHERE[1]

Digitalization in its essence is a radical change in approaches to the processing and storage of information. The transformation of text, numerical, graphic, audio and video information into "digital" form has become an impulse for the further development of production processes and social life. The multiple acceleration of data analysis procedures, the large-scale growth of the capacity potential of digital information storages, as well as the high speed of searching and extracting the necessary information have become indisputable advantages of digitalization

Sergei Teterukov,
EAG Executive Secretary

Soat Rasulov,
EAG Secretariat Administrator

Sergei Teterukov

Soat Rasulov

Complex analytical processes, including those that take place in the field of countering money laundering and terrorist financing (AML/CFT), require more and more time and resources due to the dynamic change of schemes, methods and means used by criminals to conceal their financial transactions from the law enforcement agencies.

As a global standard-setting body, the FATF strives to ensure the relevance and effectiveness of international AML/CFT standards in the context of accelerating digitalization. In particular, the FATF collects information on all innovative technologies of the financial sector and tries to ensure "smart" regulation of its activities both to achieve AML/CFT goals and to expand the availability of financial services. Thus, in the public statement made in Buenos Aires on November 3, 2017, it was stated:

"The FATF strongly supports responsible financial innovation that is in line with the AML/CFT requirements found in the FATF Standards, and will continue to

[1] Countering the legalization (laundering) of proceeds from crime and the financing of terrorism.

explore the opportunities that new financial and regulatory technologies may present for improving the effective implementation of AML/CFT measures".

In this regard, one of the most important activities of the FATF is the preparation and issuance of various guidance documents offering experience and best practices on the implementation of digital transformation of AML/CFT processes.

In June and October 2021, the FATF published papers related to three different areas:

1. Opportunities and challenges of new technologies in assisting the private sector and supervisory authorities in more effective application of AML/CFT measures;

2. The role of data aggregation, joint analytics and data protection, analysis of technologies that facilitate advanced AML/CFT analytics within regulated organizations or joint analytics between financial institutions while respecting national and international legal framework of confidentiality and data protection;

3. The role of big data and advanced analytics in transforming the capabilities of operational agencies in detecting and investigating cases of money laundering (ML) and terrorist financing (TF), as well as in understanding the risks of ML/TF.

In general, the FATF defines digital transformation as using digital technologies and digitized data to change business models, transform the way of interaction between customers and companies, and provide new opportunities for revenue generation and capacity building.

As the main directions of digital transformation, the FATF identifies the introduction of artificial intelligence, natural language processing, soft computing techniques, distributed ledger technology, digital solutions for customer due diligence, application programming interface (see notes).

Digital transformation, according to the FATF, is the way to the more effective implementation of standards and achievement of the set goals, including the introduction of a risk-based approach and the expansion of the availability of financial services.

The increased use of new technologies by supervisory authorities can contribute to the improvement of the effectiveness of the AML/CFT system by expanding its scope, better identification and understanding the risks associated with separate institutions in various sectors, monitoring compliance with legislation and taking real-time response measures, effective feedback, as well as storing, processing and sharing large volume sets of supervisory data.

The main advantages for the private sector are the following: more effective understanding and management of ML/TF risks; prompt and accurate analysis of large volume data sets; more efficient methods of customer onboarding (digital identification); cost reduction and resource allocation; and improvement of the quality of suspicious transaction reports.

Nevertheless, the difficulties that hinder the rapid and effective transition to digital procedures are highlighted separately. In particular, the first thing that countries will have to face when digitizing AML/CFT is regulatory problems. The lack of explicit support from the competent authorities leads to a decrease in interest and confidence in new technologies, despite their significant potential.

Due to the lack of necessary technical knowledge or resources, most competent authorities are in no hurry to adjust their regulatory policy. In addition, digitalization requires significant efforts to standardize and harmonize data to ensure its interpretability, which also creates certain difficulties for national AML/CFT systems.

The most serious difficulties faced by competent authorities are the costs of replacing outdated systems, the need to ensure the quality of AML/CFT data received from supervised entities, as well as the need for qualified experts or specialists with enough expertise.

At the same time, it should be remembered that digital technologies provide not only advantages, but also generate new risks. If high-quality solutions can increase the reliability of customer identification and help in the fight against fraud and cybercrime, then solutions that are implemented without consideration of the existing risks will entail undesirable consequences. They can also be intentionally used for illegal purposes.

In conclusion, it is noteworthy that technological innovations have great potential to improve the efficiency of the AML/CFT system. However, they can also lead to the deprivation or restriction of access to financial services for certain segments of society. In its guidance documents, the FATF points out the possibility of additional problems arising as the result of irresponsible or unjustified use of new technologies by the subjects without proper assessment and understanding of the existing risks.

Based on this, the FATF suggests that jurisdictions focus their efforts on the creation of the favorable conditions for the innovations in order to improve the effectiveness of AML/CFT. Thus, when applying new AML/CFT technologies, countries are recommended to pay attention to confidentiality and data protection, expanding access to financial services, implementing informed supervision and cooperation.

For these purposes, the competent authorities should develop policies and approaches for the introduction of flexible, technology-neutral, result and risk-oriented innovations.

Notes to the article[2]:

Artificial intelligence is a machine system that can, for a certain set of goals defined by a person, make predictions, give recommendations or take decisions that affect the real or virtual environment (and work with different levels of autonomy). Currently, the most well-known and developed form of artificial intelligence is machine learning.

Natural language processing is a type of artificial intelligence technology that allows computers to understand, interpret and manipulate natural language.

Soft computing techniques are methods of the problems' solution using the technique of fuzzy systems (fuzzy sets, fuzzy logic, fuzzy regulators), artificial neural networks, genetic algorithms and evolutionary modeling[3]. Fuzzy logic is a logical method that takes inaccurate or approximate data and processes it applying multiple values in such a way as to obtain a useful (but inaccurate) result.

Distributed ledger technology (also known as blockchain) is a type of technological protocol that provides simultaneous access, validation and update of a permanent registry (digital record) distributed between several computers (usually located in different organizations or locations).

The application programming interface (API) is a set of definitions and protocols for the development and integration of application software. Application programming interfaces allow digital products or services to easily interact with other products and services.

[2] Annex A: Glossary, FATF Report "Opportunities and Challenges of New Technologies for AML/CFT" (https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf)

[3] Soft computing – Wikipedia (wikipedia.org).

NEW TOOLS AND TECHNOLOGIES OF THE BANK OF RUSSIA'S CONTROL AND SUPERVISORY ACTIVITIES IN THE AML/CFT SPHERE

Ilya Yasinsky,

Director of the Department of Financial Monitoring and Currency Control, Bank of Russia

Ilya Yasinsky

Since July 1, 2022, the Bank of Russia has launched a full-scale operation of the KYC platform ("Know Your Customer"). On a daily basis, all Russian operating credit institutions receive via the telecommunication channels the registers of clients – legal entities and individual entrepreneurs. They are distributed by the level of risk of conducting suspicious transactions[1]. The banks have the right to use these registers for the assessment of their own clients risk level, as well as for the anti-money laundering measures development.

This format of information exchange between the regulator and the supervised organizations meets the principles of the " proactive" or "advisory" supervision aimed at assisting in the preventive identification of the ML/TF risks[2] at the early stages of the organization and conduct of the illegal activity.

The KYC platform marks the next stage in the "proactive" supervision forms evolution in the AML/CFT[3] sphere.

We see the new quality of the created information service, first of all, in the immediate receipt by the credit institutions in an operational (daily) mode of summary information on high-risk clients of all such organizations.

[1] Suspicious transactions – operations with monetary funds and other assets, supposedly performed for ML/TF purposes (article 3 of the Federal Law No.115 FZ adopted on 07.08.2001.

[2] Legalization (laundering) of proceeds from crime and financing of terrorism.

[3] Countering the legalization (laundering) of proceeds from crime and the financing of terrorism.

Efficiency of the regulator's assessments delivery to banks is of key importance to minimize the period and volume of the suspicious transactions carried out by their clients, and the timeliness of measures taken to stop them.

The differences between the level of information and analytical support of the banks AML/CFT units, complication of the schemes and layering of suspicious transactions across various financial organizations objectively make it difficult for a single credit institution to identify such transactions, especially in case of the recent customers or those who, for various reasons, do not actively use their account.

The Bank of Russia, having unique information resources and a long-term practice of detecting suspicious transactions, can mitigate the above vulnerabilities of the national AML/CFT system by centrally sharing the results of the operational activities analysis, financial condition and risks of participation in suspicious transactions of certain legal entities and individual entrepreneurs with the supervised organizations.

In our opinion, provision of information on other banks clients with risk indicators and links to the particular bank clients by the KYC platform creates new opportunities for an in-depth assessment. These clients may be, for example, the beneficial owners of his/her client, beneficiaries and counterparties to his/her transactions, affiliated persons who may not be the bank clients themselves, but should be considered as sources of risk associated with the client.

Finally, the analytical product of the KYC platform has a great potential for application by credit organizations not only in the anti-money laundering sphere, but also in other areas of banking activities using the results of partner assessment and business intelligence, including:

- assessment of the borrower, the guarantor, the warrantor, the pledger when considering loan applications;
- assessment of a potential investor in case of changes in the a credit institution shareholding structure;
- assessment of the credit institution's own risks when investing in new types of business, projects, purchase of companies, etc.;
- search for and evaluation of candidates for a job in a credit institution.

A set of criteria is used in the KYC platform to identify the suspicious transactions. Such criteria correspond to all algorithms and data sources used by the Bank of Russia, as well as all relevant typologies of suspicious transactions and the ML/TF risks. The risk level assessment criteria cover all aspects of business and relationship between its subjects, possible negative and "whitewashing" factors, which allows us to give a very high accuracy of the client's risk assessment.

The risk level criteria are divided into the following fields:

1) evaluation of a legal person (individual entrepreneur), types, nature and financial results of its activities;

2) assessment of transactions on accounts of a legal person (individual entrepreneur) in credit institutions;

3) evaluation of founders (participants), managers of a legal entity, as well as a natural person registered as an individual entrepreneur;

4) assessment of the legal person (individual entrepreneur) affiliation with other legal persons (individual entrepreneurs) carrying out suspicious transactions;

5) results of the national risk assessment and sectoral risk assessment conducted in accordance with the Federal Law No. 115-FZ;

6) information received from the state authorities.

Each of the criteria is used in the KYC platform as a set of the code mini-algorithms, which we call “the risk scenarios”.

In 2021-2022, during the piloting of the KYC platform before its full–scale implementation, the participating credit institutions highly appreciated the reliability and usefulness of the estimates generated by the Bank of Russia on the basis of the above criteria.

The KYC platform introduction in its current form became possible largely due to the *new effective IT solutions* implemented by the development team of the Bank of Russia with the participation of the specialized organizations.

Firstly, the assessment of the above risk scenarios (criteria) requires the analysis (search and processing) of information from more than two dozen databases of different origins, structures and formats. If earlier the processing of these resources was largely carried out in a decentralized manner, followed by a "manual" consolidation of the results, now the formation and consolidation of the risk criteria that "matched" the client through the entire set of resources (databases) occur automatically.

Secondly, various groups of criteria "triggered" based on the rules incorporated in the algorithm activate one or more typologies of suspicious transactions that are most similar to the client activity.

The measure of this "similarity" is calculated automatically using a *scoring* procedure based on a mathematical *model of linear regression*, widely used in application artificial intelligence systems and providing for calculating the sum of the values of the "triggered" criteria multiplied by their weight coefficients, followed by the derived sum comparison with a set threshold.

In terms of content, the manual work replacement by the program at the most time-consuming stages of checking the risk criteria and forming a summary assessment of the similarity of the client's activity with a particular typology of the suspicious transactions based on the set of criteria that "matched" made it possible to completely eliminate the risk of the "human factor" at both stages. It ensures *reproducibility, verifiability, objectivity and impartiality of the assessment* (taking into account both "negative" and "positive" (rehabilitating) factors), a correct uploading of individual factors into an integral assessment according to the unified rules fixed in the scoring algorithm.

In the technological aspect, the digitalization of the above-mentioned "manual" sections of the analytical process made it possible to form and transfer a consolidated register of legal persons and individual entrepreneurs with the high-risk indicators to credit institutions on a daily basis.

This technical solution, as the calculations showed, at the same time turned out to be more preferable compared to the alternative solution – the provision by the Bank of Russia of information on the risk group of certain customers or their groups upon the credit institutions *individual requests.* Taking into account the high requirements for the response time to such requests, the probabilistic nature of their receipt and, as a result, the increased load on the computing and telecommunications facilities of the KYC platform, such an alternative option would be significantly more costly.

A *machine learning model* has been developed for each typology of the suspicious transactions, which uses the *linear regression with regularization* as its base algorithm. The training samples were created for each model. The samples include only clients with a risk level confirmed by an analyst, criteria peculiar to this typology are used as variables.

Based on the training sample variables values analysis results, the software algorithm itself selects the model parameters (weight ratios, trigger threshold) that ensure the accurate recognition of the customer data as high-risk.

It is important to note that for the "red" risk level clients (prior to their inclusion in the register), the final confirmation of the KYC platform conclusion about the level of risk and similarity with a particular typology is made by a specialist-analyst.

Also, an essential aspect of the functioning of the KYC platform is the constant feedback from the credit institutions authorized to inform the Bank of Russia about the disagreement with the received risk assessment of their customers with the submission of the necessary justification in accordance with clause 9 of Article 7.7 of the Federal Law No. 115 FZ of 07.08.2001.

We carefully consider such requests and in some cases agree with the credit institutions and make adjustments to the parameters of the risk assessment models.

In conclusion, I express the hope that the possibilities of the KYC platform discussed in the article will be used to the maximum extent by all credit organizations of Russia, which will raise the effectiveness of the domestic anti-money laundering system to a qualitatively new level.

ARTIFICIAL INTELLIGENCE IS A RELIABLE PARTNER FOR COMPLIANCE ANALYSTS

Alexander Tarelkin,
“Sberbank of Russia” PJSC data researcher

Team of “Sberbank of Russia” PJSC data researchers

Alexander Tarelkin

How do we manage to monitor the customers transactions in Sberbank, the bank that provides services for over 100 million individual customers and about 3 million organizations?

Customers make over 1 billion transactions every day, use remote services and come to 14 thousand branches available all over the country. The client makes thousands of transactions per month, all of which are characterized by a large number of attributes. The history of the user operations together with other meaningful internal and external sources of information generate the big data, large volumes of data suitable for analysis. It has a high potential for analytics and makes it possible to use modern numerical methods in compliance work. Artificial intelligence (AI) and machine learning demonstrate rapid development and are already leading to fundamental changes. They help to improve the accuracy and efficiency of the dubious schemes identification, compliance risks, allow you to analyze a large number of sources, hypotheses and discover new insights.

The basic concept of the machine learning is quite simple – the model can be represented in the form of a certain function. When we set the function input parameters, we expect an answer to the question posed at the output. For example, we will submit a client's transactions for a month at the input, and at the output we want to get the probability of the client's involvement in dubious activities. First of all, we should teach the function to deal with such a task, to "show" it a lot of historical positive and negative examples of the decision-making. This is the machine learning, which is based on the mathematical formulation of the optimization problem and the numerical methods. This type of the machine learning is called the "supervised teaching", which means that there is a markup of examples for the model (in this case, the history of checks conducted by the bank with their recorded result).

AI model solutions are based on a comprehensive analysis of the client/affiliated persons/ transactions/ counterparties. The complexity of the model directly results in its expressive power. However, simple algorithms also have a number of advantages: interpretation of solutions, development and predictions speed, low cost of maintenance. Due to these features, they are also relevant in the dubious transactions identification. Interpretable models with easily explained solutions are called ‘white box’. Examples of such models are linear regression algorithms or decision trees. Complex models such as ‘black box’ allow you to get more accurate solutions. Statistical methods for assessing the contribution of features to the model solutions make it possible to raise the interpretability of the results to the required level. Examples of black box models are the ensemble models, gradient boosting, neural networks et al.

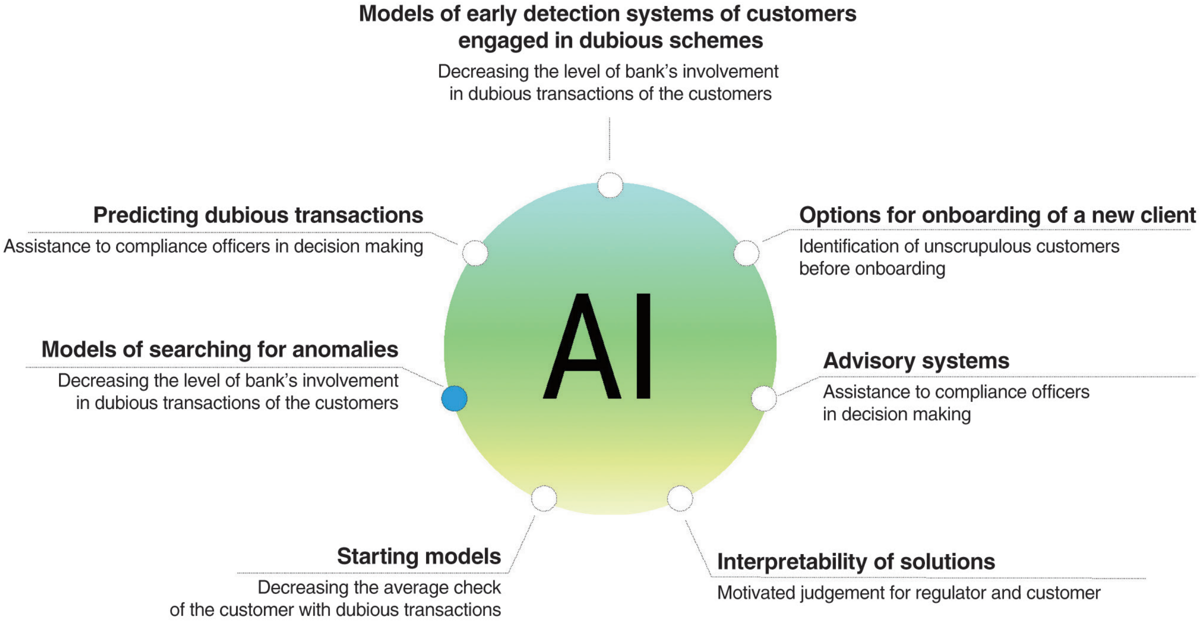
Due to the flexibility and variety of available solutions, AI has taken a solid place in all key compliance control nodes. Figure 1 shows the concept of using AI in a bank to manage the compliance risk.

The bank has implemented a scoring system, an automated method of multifactor analysis of the client's activity. The superposition of the cluster of models at various stages of customer service allows to timely assess the compliance risks and prevent the high-risk actions. For example, to assess the client's "tendency" to commit dubious transactions when accepting him/her for service; to prevent transactions that have indications of doubtfulness; to analyze the transactions that have already been performed; to assess the feasibility of restricting access to the bank's services.

Gradient boosting models, trained with utilizing historical markup, are used to make a decision about onboarding a new client and scoring his/her activity. "Speedy" white box models are used to evaluate transactions in real time.

The bank also uses models with no markup for teaching – the history of decisions made by a person. Models are trained by themselves, identifying various patterns from the data. An example is the anomaly search model: a neural network of the transformer architecture type analyzes current patterns in client activity and compares them "with itself in the past",

Fig. 1


Models of early detection systems of customers engaged in dubious schemes
Decreasing the level of bank’s involvement in dubious transactions of the customers
Predicting dubious transactions
Assistance to compliance officers in decision making
Options for onboarding of a new client
Identification of unscrupulous customers before onboarding
AI
Models of searching for anomalies
Decreasing the level of bank’s involvement in dubious transactions of the customers
Advisory systems
Assistance to compliance officers in decision making
Starting models
Decreasing the average check of the customer with dubious transactions
Interpretability of solutions
Motivated judgement for regulator and customer

as well as in the context of the current state of all clients in the industry. Such model tries to build the transactional embedding of the client in the best way. Embedding is the transformation of the complex structured data, for example, words, texts, sequential events and their attributes into a machine-readable set of numbers – a numeric vector. The model is trained by the contrastive method: the sequence of customer transactions is cut into subsequences, then pairs of these subsequences are formed, and the model learns to predict whether the elements of the pair belong to the same customer or to different ones. Thus, the markup appears from the data itself, and this type of training is called "unsupervised teaching". In addition to the anomaly detection process, the resulting embeddings are used as additional features in the "supervised teaching" tasks mentioned above. With the help of a simpler and lightweight "isolation forest" model (Fig. 2), anomalies are searched for throughout the flow of customers in previously unexplored areas. The algorithm is a method that explicitly isolates anomalies using binary trees, demonstrating the ability to quickly detect anomalies, without the need to profile all ordinary instances.

Anomaly detection models are an integral part of the concept of ongoing training (Fig. 3). The identified anomalies are sent to the compliance analyst for marking (review), thereby ensuring an uninterrupted flow of fresh examples for teaching with a teacher beyond the known scenarios. In conditions of constant changes and transformations of fraudulent schemes, this allows the trained models not to lose relevance.

Fig. 2

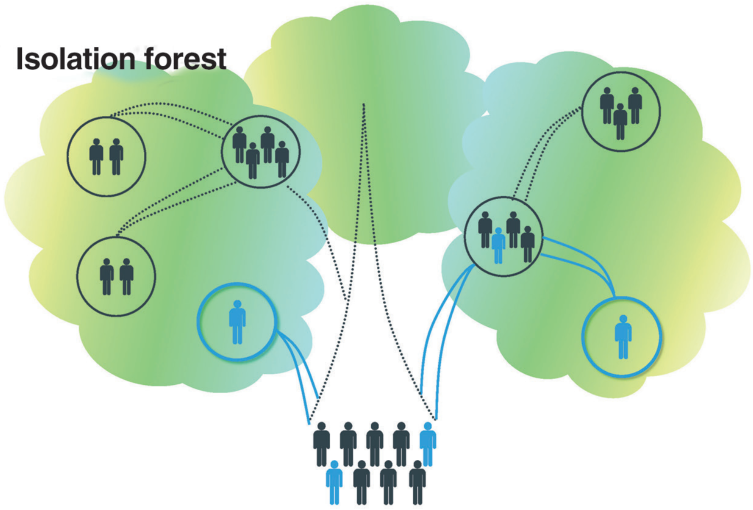
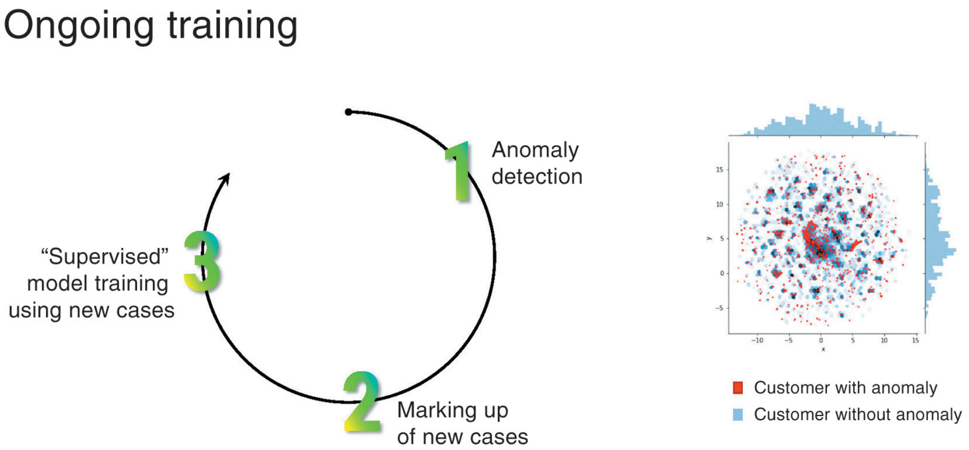


Fig. 3


Ongoing training
1 Anomaly detection
2 Marking up of new cases
3 "Supervised" model training using new cases
15
10
5
0
−5
y
−10
−5
0
5
10
15
x
🟥 Customer with anomaly
🟦 Customer without anomaly

Models that work with text data deserves a special mention. For example, the introduction of AI to help with the existing documents analysis. The neural network for the named entities recognition (the NER model) initially assess the text content for completeness and meaningfulness.

The development and implementation of automated solutions based on AI is impossible without an extensive technological infrastructure, as well as the coordinated work of qualified specialists in the field of Data Science. There are three main areas: Data Engineers (DE), Data Scientists (DS) and Data Analytics (DA). DE brings new data sources into industrial use, monitors their consistency and relevance. DS develops and trains new models; DA integrates models into business processes, conducts AB tests to quantify the impact directly on business metrics. The bank not only attracts such specialists from outside, but also trains them on its digital platforms.

The numerical methods used in the work allow us to solve several tasks simultaneously: to minimize the risk of the bank's involvement in dubious customer transactions, to reduce costs by automating routine actions, not to bother bona fide customers with additional questions. Of course, it is difficult to overestimate the importance of compliance work when evaluating complex schemes, developing typologies, because AI does not replace a person, but helps to make better decisions. It is important to constantly analyze models, scenarios, approaches for organizing work to comply with the requirements of the regulator and the functioning of the economy in modern conditions.

OWN IT SYSTEM FROM SCRATCH – READY FOR THE GROWING LOAD ON COMPLIANCE

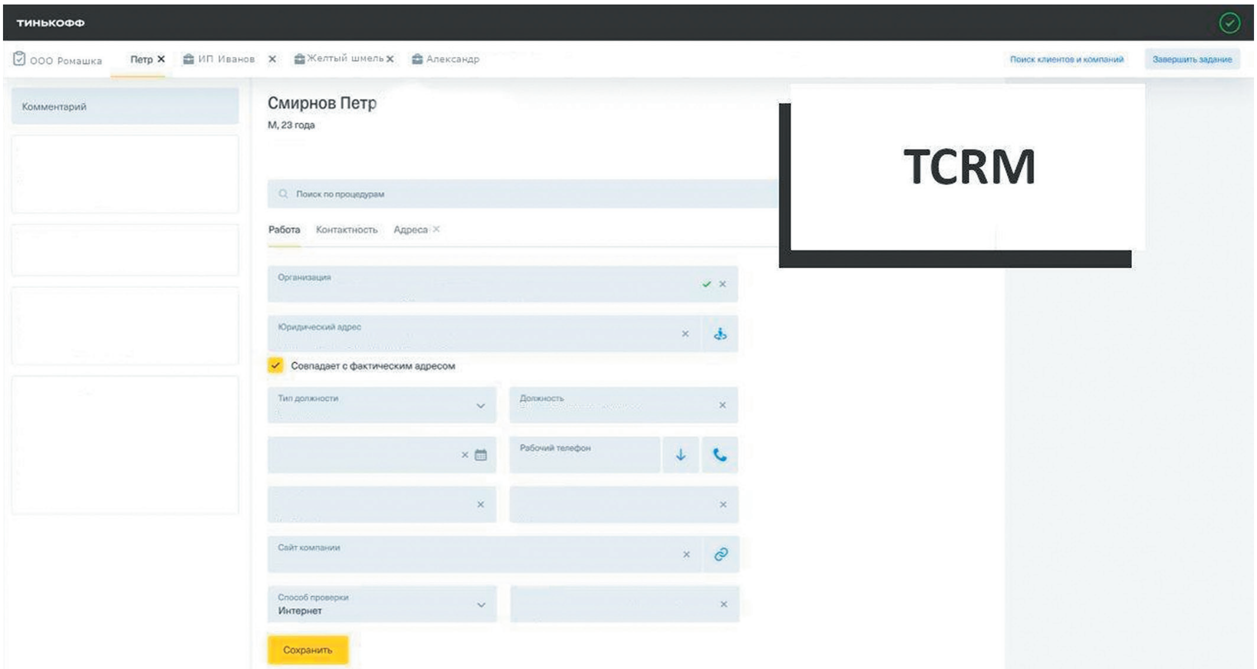
Galina Kuznetsova,
Director of Tinkoff Bank Compliance Department

Galina Kuznetsova

The economy and banking activities are developing rapidly. People are becoming more and more financially literate. Unfortunately, at the same time, new schemes are increasingly emerging, presenting challenges to banks' compliance. Regulation becomes more complicated. There are more and more new recommendations that banks should take into account in their daily work.

According to new recommendations, our bank compliance screening processes of natural persons and businesses are constantly refined and improved. However, it is not enough to have comprehensive instructions and trained staff. Employees must have reliable, fast working tools - internal software and services, to work effectively under conditions of the rapid information growth.

Previously, our specialists used a third-party IT system. Different bank divisions used it, so the information that compliance staff worked with was general and insufficiently detailed. Employees noted the inconvenience of screening – extra clicks; the need to “flag” the result of each screening step; they often had to swith to the instructions, and so on. Largely because of this, the load on the employee increased, specialists did not meet the deadlines, and the list of tasks for processing grew longer. From the perspective of our company's growth, we could face serious difficulties, and we understood that we needed a different solution.



Смирнов Петр
М, 23 года

Организация
Юридический адрес
☑ Совпадает с фактическим адресом
Тип должности
Должность
Рабочий телефон
Сайт компании
Способ проверки
Интернет

Interface example

Tinkoff has a strong system of internal IT development, many programs have been developed at Tinkoff taking into account the bank's business models and tasks. Therefore, we decided to develop our own product for compliance employees.

At the start of the project in 2019, together with the rank-and-file employees, we identified the critical shortcomings of the work that we wanted to eliminate:

- Long load time (a lot of data was transferred to the frontend, the client's tab was overloaded),
- Lack of a well-structured client data to meet the compliance tasks,
- Inability to optimally integrate the task management tools for group and department managers. Additional programs were used,
- Time-consuming onboarding process of new employees.

We specified the new software tasks and started development. Already at the end of 2020, we conducted the first tests in our own more efficient compliance interface with embedded prompts instead of complicated instructions, tools for convenient data collection, analysis and search for new development ways.

New interface allowed to simultaneously check dubious transactions of several related clients. Instead of “flags”, some of the actions are now performed automatically, smart hints for each check step became available. There is no need to use several software programs at once, open instructions and clients tabs separately. Also, using our TCRM, it was finally possible to implement monitoring of indicators.

> On average, the employee's work time on the verification task decreased by 15%. In some cases (online payment processing) even by 30%.

The employees work has become not only faster, but also more convenient. All this has had a positive effect, including on customers, because verification tasks are processed faster. At the moment, we have not fully switched to TCRM yet, but we plan to do it in the near future.

> Now 95% of all verification tasks for natural persons are performed in TCRM, more than 50% of natural persons and SME were transferred to TCRM.

The results have improved significantly. This, among other things, allowed us to achieve new heights. We have recently reached the mark of 25 million customers. With the growing number of clients and their recent higher activity in the relevant application, countering criminals became more complicated. It means that the need for more advanced methods and tools for compliance verification is increasing. Additionally, in recent years, we have introduced the 'premium' service. In 2021, we started working with the private clients who have a special service status, which requires more fine-tuning of the bank processes. Thanks to the timely switching from the outdated software to our own product, we were ready for new demands and the customers number increase.

The switching effectiveness, even in conditions of a multiple increase in the number of customers, the emergence of new categories of customers (premium service), can be seen, *inter alia* from the ratio of the number of AML employees to the rising number of compliance verification tasks. Since September 2020, the compliance burden, expressed in man-hours, has increased 4 times, while the staff has grown only 2.5 times over the same period. Thus, the process optimization allowed us to focus on each employee efficiency and comfort, reduce the backlog. All this helped to avoid hiring new specialists following each new increase in workload.

We do not stop our optimization work, there are many plans ahead, including the increased automation of processes. Now it is impossible to switch to full automatic verification by 100%, or even in some noticeable proportion of cases, without compromising quality, since the schemes are constantly evolving and becoming more complicated. However, we have already taken an important step – we have designed our own software and outlined tasks for further development.

ELECTRONIC MONEY SERVICE REGULATION, PROBLEMATIC ISSUES AND INTERNAL CONTROL

Dmitry Gronin,
Head of the Internal Control Service, Non-Profit Organization "YUMANI" LLC

Elizaveta Demidova,
Head of Financial Monitoring Department, Non-Profit Organization "YUMANI" LLC

Dmitry Gronin

Elizaveta Demidova

The dynamic development of popular electronic wallet platforms in the Russian payment market has led to a detailed regulation of the specifics of their activities with the entry into force of Federal Law No. 161-FZ of 27.06.2011 "On the National Payment System", which introduced definitions of electronic monetary funds (EMF) and electronic means of payment (EMP). The defining features of the EMP, according to the law, were the preliminary provision of money by the client to the operator and the submission of payment orders exclusively using the EMP, which, in turn, requires the use of information and communication technologies and technical devices[1]. The Law limits the quantity of electronic money operators and includes mainly credit institutions, and accordingly, electronic money circulates within the Russian banking system and follows general approaches to its regulation.

[1] Article 3 of the Federal Law No. 161-FZ of 27.06.2011 "On the National Payment System"

EMF account		Wallet	
√	No statuses	x	Statuses available (anonymous, simplified identification-SI, full identification-FI, Corporate electronic means of payment - CEMP)
√	No limits	x	Limits available
x	Physical presence obligatory	√	Physical presence non-obligatory
x	Obligation to open*	√	No obligation to open
x	No one-sided closing*	√	One-sided closing permitted
√	Foreclosure in all cases	x	Foreclosure only for FI and CEMP

*Only for cases specially defined by law.

Fig. 1. Differences in the regimes of EMF and bank accounts

ELECTRONIC WALLET AND BANK ACCOUNT

With the obvious similarity of EMF accounts with a bank account, there are also fundamental differences shown in Figure 1. With respect to EMF accounts, credit institutions are endowed with greater discretion in the possibility to open/refuse to open them or unilaterally terminate contractual relations with customers. These conditions may be regulated by banking rules. In particular, this allows the operator to incorporate in the contract the condition for EMF account closure in case of suspicion of money laundering without the procedure of two formal refusals to conduct an operation, as well as to close accounts proactively in case of account inactivity even if there is a balance. In the latter case, in our opinion, there is no contradiction with the prohibition of expenditure transactions before the annual update of the dossier[2] (which is relevant for long-term inactive "sleeping" accounts), since the balance is written off after the termination of contractual relations with the client.

An important advantage of EMF is the right to open an electronic wallet without the personal presence of a client, which makes it possible to use the tools of notarized documents copies and postal communication during the identification, indefinitely expanding the geography of presence without the need to open representative offices of the operator. For individual wallet statuses, there is also the possibility of remote and almost instant identification using communication tools and the Internet, which increases the availability of financial services, convenience for customers, especially in conditions of quarantine restrictions.

The described simplifications in the procedures for onboarding and the risks arising from this are compensated by the legislator via introduced gradation of EMF accounts according to the levels of identification carried out, as well as by setting limits and restrictions (presented in the table in Figure 2).

	Non-personalized		Personalized	CEMP
	Anonymous	SI	FI	FI
Balance, occasional payment, RUB	15 000	60 000	600 000	
EMF transfers RUB/month	40 000	200 000	Not limited	
Cashing-out RUB/day	x	5 000	Not limited	x
Cashing-out RUB/month	x	40 000	Not limited	x
Cash depositing	x *	√	√	x
Transfers to natural persons' accounts	x	√	√	x
Transfers to legal persons' accounts	√	√	√	x
Crediting from natural persons' accounts	x	√	√	x
Crediting from legal persons' accounts	√ **	√	√	x

*except for transport and educational cards
**may be limited by regulator

Fig.2 Statuses, limits and restrictions for EMF use

[2] Clause 3, para.1.6 of the Regulation of Bank of Russia No.499-P dated 15.10.2015 "On identification by credit organizations of customers, customer representatives, beneficiaries and beneficial owners for purposes of countering money laundering and terrorist financing".

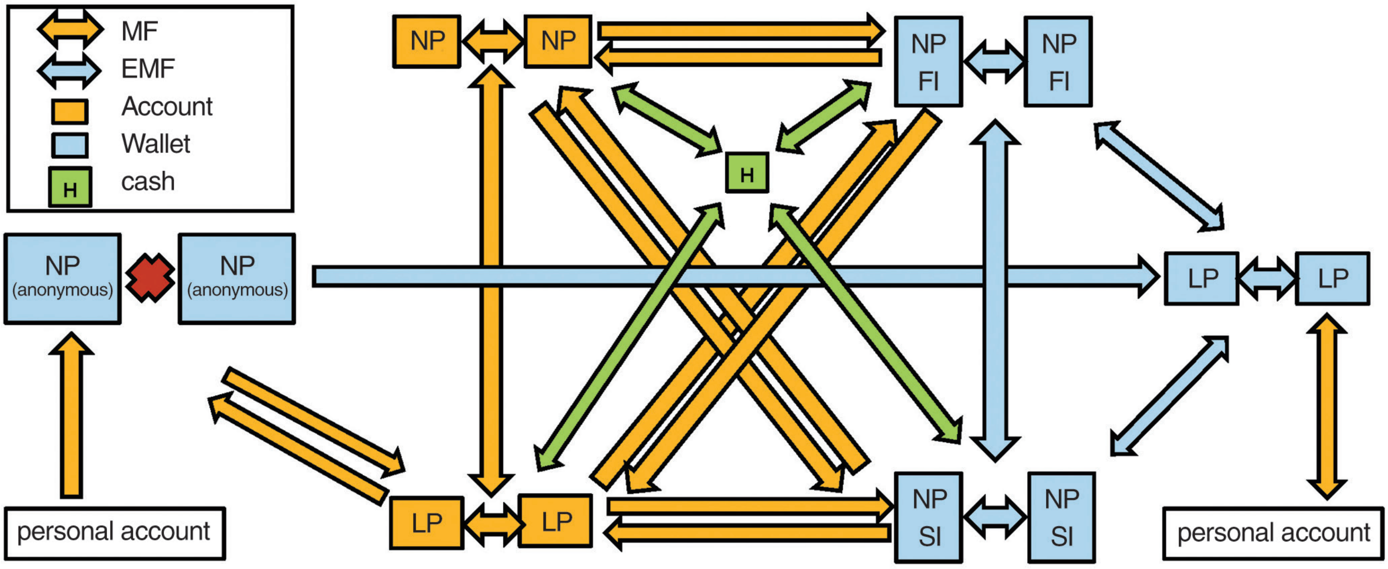


Fig.3 Permissible directions of MF and EMF transactions

The Law provides for the following categories of EMP: corporate means of payment (CEMP) for business entities, personalized and non-personalized EMP for individuals. The latter are also divided into two groups, depending on whether a simplified identification of the owner has been carried out. Pursuant to the table, the maximum balance and, accordingly, the amount of a one-time payment is limited for all EMP categories. There are restrictions on the turnover of EMF, as well as the possibility for depositing and withdrawing cash. The most restricted in the rights are the EMP, the owners of which were not exposed to the procedure of identification or simplified identification (anonymous). Owners of EMP of this category have the opportunity to pay only to legal persons and entrepreneurs and replenish their balance exclusively from their accounts or accounts of other legal persons and entrepreneurs, but the latter option may be restricted by the regulator. CEMP have the ability to transfer electronic money to most types of EMP, however, transactions in non-electronic money can only be carried out with their own bank account. The permissible directions of monetary funds transfers - MF (yellow), EMF (purple) and cash (green) are shown in Figure 3 in the form of a diagram.

IDENTIFICATION AND CHANNELS OF ATTRACTION

The absence of regulatory requirements for the personal presence of customers when issuing an electronic payment means allows the operator to use a wide infrastructure to attract and identify customers. Along with the traditional personal presence in the office for identification purposes, bank payment agents, telecom operators, partner banks and traveling courier employees can be involved. In addition, the clients of the EMF operator have the right to choose any other convenient way to deliver their personal information, contacting notaries to make the apostilled documents' copies and sending them by mail, courier or otherwise. The disadvantage of regulation in this case, in our opinion, is the inability to attract a non-resident organization as a bank payment agent (BPA). Despite the absence of a direct prohibition in the law, the established reporting on the engaged BPA[3] requires specifying the details of a resident of the Russian Federation. This restriction reduces the distribution of wallets abroad, imposes significant notary costs on interested non-resident clients and, in our opinion, has no explicit regulatory purpose.

[3] Reporting form 0409602 “Information on persons charged with performing identification”, Regulation of the Bank of Russia No.4927-Y dated 08.10.2018 “On the list, forms and procedures of submitting reporting forms of credit organizations to the Central Bank of the Russian Federation”.

In this regard, the possibility to hire the remote employees to perform the identification abroad becomes a justified, but more costly measure.

To identify a foreign citizen in the Russian Federation, apart from the identifying documents details, EMF operators request for the document on the legitimate subject's stay in Russia: visa, residence permit, temporary residence permit, patent and, for visa-free regimes, a migration card within validity period and other documents. Unfortunately, the law does not allow identification on the basis of derivative documents indirectly indicating the legality of stay, for example, notification of arrival, which de facto imposes increased requirements for legal literacy on non-residents. An employee of the wallet service cannot always help them, because in the conditions of openness of the list of possible documents on the right of stay, it is difficult to guess which document the client has and which one he/she needs to find and provide. In our opinion, in conditions when a client, having received and using a wallet, can enter and leave the country an unlimited number of times, or even get an EMP remotely from abroad, control over the availability of a document on the right to stay in the Russian Federation loses its meaning originally elaborated by the legislator.

The possibility of simplified identification (SI) also facilitates access to the electronic money service and reduces bureaucratic procedures. Its remote implementation becomes possible by checking client data in the information systems of government agencies available to EMF operators in Interagency electronic cooperation system (IECS) and Unified system of identification and authentication (USIA) transport environments (on the public services platform). In order to successfully pass the SI, the client provides, in particular, information including the surname, first name and patronymic, the number of the identity document and one of the additional documents on choice, the mutual consistency of which must be subsequently confirmed by the IECS. Alternatively, the operator receives the necessary details from the USIA after the client authorization in this system. Thus, when introducing the simplified remote identification, the legislator proceeds from the assumption that only the client can know the exact details of two documents at the same time or the login and password of the account on the public services website.

A significant disadvantage of the procedures under consideration is the fact that, in the absence of legislative restrictions, there are virtually no tools in the available information systems to verify the non–residents' documents details, which leaves them with the only way to pass the SI - by visiting the office, or by other means similar to full identification (FI). With an equal set of difficulties, the opportunities provided by the SI status are significantly limited, that is why this method is not in demand by non-residents at all. Moreover, the actual exclusion of non-residents from the legal procedures for passing the SI pushes them into the illegal sphere, increases the demand for illegal trade in personal data and the services of so-called "drops", i.e. fake account holders. Even without criminal intent, a non-resident often resorts to such a forgery solely because of its simplicity and accessibility on the one hand, and the inaccessibility of legal procedures on the other. Needless to say, monitoring and analysis of transactions on such EMPs become completely uninformative.

The solution to the issue could be to allow the use of foreign systems – analogues of IECS and USIA. Companies that provide legal access to checks in such systems have been successfully operating on international markets for a long time. It would also be useful to provide credit institutions with access to other national information systems, for example, the creation of a service for verifying the details of non-resident passports accumulated by migration services. This would increase the quality and accessibility of services for foreign citizens residing in the Russian Federation, which in first place is relevant for residents of neighboring countries.

TRANSACTIONS MONITORING

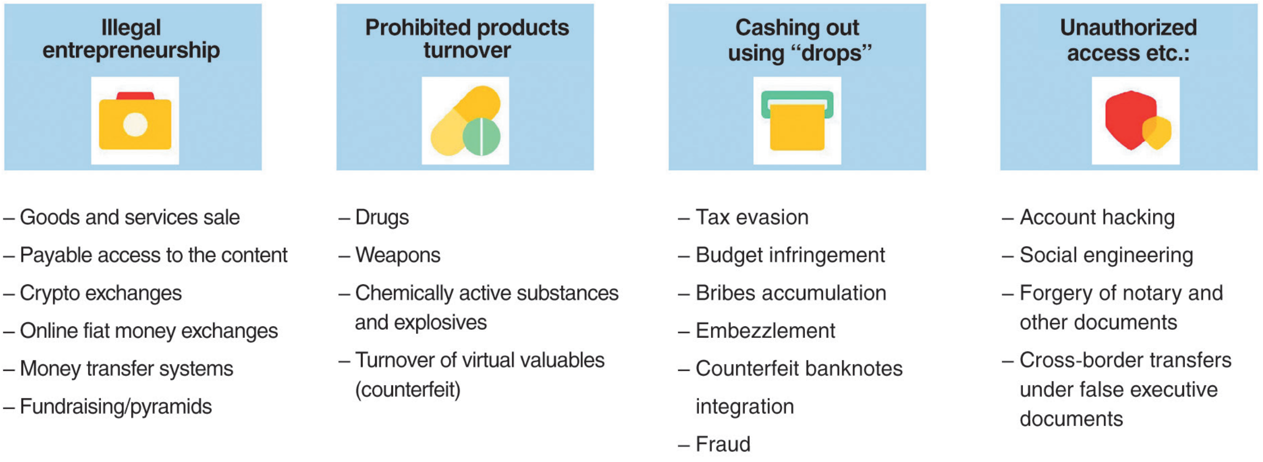
According to the Rosfinmonitoring public report on the national assessment of the risks of legalization (laundering) of criminal proceeds[4], e-wallet services are classified as a high-risk group. These risks, as well as the sector specifics related to the remote nature of services, simplicity and high speed of payments, require the electronic money services to regularly take into account the illegal financial transactions typologies characteristic of the sector, develop and update the necessary compliance procedures.

Monitoring of e-wallet and bank account transactions is based on similar principles. EMF operator assigns an important role to analytics and investigations by the compliance departments employees, who use the arsenal of regular reports on high-risk client transactions (cash withdrawals, transit transfers and other schemes), accumulate external information: about suspicions in banks' client departments, incoming requests from the government agencies. More complex automated systems (the so–called analytical engine) are also in demand - a set of algorithms that describe reliable and unreliable customer profiles and payment behavior. Such continuous-action algorithms are developed and maintained by a team of analysts, including machine learning specialists. Among the sources of information for such rules are all available characteristics of the client and their interrelations, the results of checking the client and his/her counterparties against blacklists, linguistic analysis of the client's website and text fields of comments on the payment for the presence of dangerous keywords, various metrics provided by news agencies and other external services. It should be noted that a significant contribution to the assessment of clients and counterparties was made by "Know your customer" system (KYC) developed by the Bank of Russia. In the framework of KYC, banks are daily informed about the result of the Central Bank's risk assessment of the entire customer base. In many cases, such an assessment is proactive in relation to other indicators identified in the client's activities.

ILLEGAL ACTIVITIES MAIN TYPOLOGIES

The main illegal activities typologies identified in the wallet service are also characteristic of the financial market as a whole (shown in Figure 4).

The group of schemes of illegal entrepreneurship includes offers of legal products, which are carried out, however, with the entrepreneur's avoidance of state and tax registration, violation of licensing and other permissive regimes. In the practice of identifying and suppressing illegal schemes, there are also attempts to organize an online crypto exchange using the wallets. Schemes of illegal entrepreneurship with the organization of



Illegal entrepreneurship

- Goods and services sale
- Payable access to the content
- Crypto exchanges
- Online fiat money exchanges
- Money transfer systems
- Fundraising/pyramids

Prohibited products turnover

- Drugs
- Weapons
- Chemically active substances and explosives
- Turnover of virtual valuables (counterfeit)

Cashing out using "drops"

- Tax evasion
- Budget infringement
- Bribes accumulation
- Embezzlement
- Counterfeit banknotes integration
- Fraud

Unauthorized access etc.:

- Account hacking
- Social engineering
- Forgery of notary and other documents
- Cross-border transfers under false executive documents

Fig.4 Possible EMF service typologies of illegal activities

[4] National ML risk assessment 2017-2018: Rosfinmonitoring public report - https://www.fedsfm.ru/content/files/documents/2018/оценка%20рисков%20од_5.pdf.

the prohibited products turnover are allocated to a separate group, which includes a newly identified trend: organization of "exchanges" of virtual valuables – game items from popular online games. Such private platforms operate without the knowledge and permission of the copyright holders. Schemes involving front persons - "drops" represent the final phase of obtaining already accumulated criminal income, when an unscrupulous person faces the task of cashing out or transit of funds. Other schemes are connected with hacking or other means of obtaining unauthorized access to wallets, forgeries of executive and other documents. Each of these schemes is characterized by its own combination of features, so prompt identification and, in some cases, analysis by an expert is required.

In conclusion, it should be noted that electronic money operators follow the general banking regulation in the Russian Federation. Despite the above-mentioned regulatory shortcomings, the used modern organizational and software methods make it possible to effectively carry out identification and simplified identification of customers, promptly identify, classify and disrupt a wide range of illegal schemes, conduct preventive work that inhibits their penetration into the electronic money system. The modern machine algorithms for detecting dubious activities, prompt and automated application of sanctions measures (closure, blacklisting, service denial) allow ensuring, in general, a low percentage of a credit institution involvement in the illegal turnover.

APPLICATION OF NEURAL NETWORKS AND THE PRINCIPAL COMPONENT ANALYSIS FOR IDENTIFICATION OF CREDIT INSTITUTIONS POTENTIALLY INVOLVED IN THE ML[1] PROCESS

The article discusses the use of artificial neural networks and the principal component method of factor analysis for the identification of credit institutions potentially involved in laundering of criminal proceeds

Viktor Ivanov,
Doctor of Physical and Mathematical Sciences, the National Research Nuclear University "MEPhI" Professor,
Chief Researcher of the Joint Institute for Nuclear Research

Elena Akishina,
Candidate of Physical and Mathematical Sciences, leading programmer in theJoint Institute for Nuclear Research

Anastasia Prikazchikova,
Consultant of the Information Resources Unit of the Rosfinmonitoring Information Technology Development Department

Victor Ivanov

Elena Akishina

Anastasia Prikazchikova

Modern technologies of analysis of credit organizations financial condition are based on the assessment of the banks statements. However, the number of financial parameters that banks show in their reports is quite large, which significantly increases the complexity of the analysis. To solve the problem of the banking organizations financial monitoring it is necessary to develop the methodology of information analysis that allows to work with numerous indicators of credit institutions activity.

One of the goals of the financial intelligence units is to improve the effectiveness of identification of credit institutions, potentially-involved in the legalization of criminal proceeds.

[1] Legalization (laundering) of proceeds from crime.

The processing of information on the banking organizations activities begins with the representation of the analysis objects by vectors of indicators x(1), x(2), ..., x(p), for which the ratio "more-less" is not defined. This uncertainty is fundamental and requires the research and development of adequate estimates of vector nature objects in order to overcome it.[2]

The neural networks theory and principal component method of factor analysis were used as mathematical tools to conduct scientific research.

The artificial neural networks are one of the main directions of the modern AI theory. The possibility of learning is one of the main advantages of neural networks over traditional statistical algorithms.[3] Technically, training is about finding the coefficients of connections between neurons.

In the learning process, the neural network is able to identify complex dependencies between input and output data, as well as perform generalization[4].

For the analysis of credit institutions, the ‘Statistic’ application software package version 6.0 was used. Data from the credit institutions bank statements No. 101 was analyzed. Based on it, a training sample was created with the target indicator "Revocation of the license". In total, 23 most informative indicators were selected to build the model.

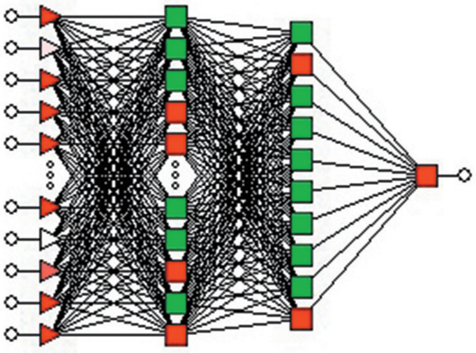


Fig. 1. Neural network architecture

A multilayer perceptron was used as a model of a neural network. Neural network architecture (see Fig. 1) was selected according to the highest productivity value and the lowest error value of the neural network training. The highest value of the neural network performance from the constructed models was 74%.

Next, Figure 2 shows the distribution of credit institutions according to the neural network output . The red line in the figure differentiates reliable and high-risk credit organizations from the point of view of involvement in illegal activities (reliable banks are located to the left of the red line).

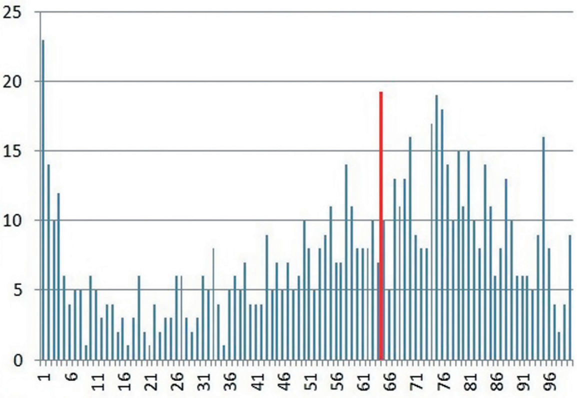


Fig. 2. Neural network output distribution (for all banks): aggregation window = 0.01, initial indicators

On the next stage the feature space of Russian credit organizations activities results were analyzed based on the principal component method of factor analysis.

The principal component method is based on all possible linear transformations of the initial features, which allow us to move to a fundamentally new feature space, so-called principal components.

So, the initial data sample included 814 banking organizations. The principal components were measured using 23 input variables in the ‘Statistic’ application. As a result of the method, 23 principal components were generated, the total cumulative variance of which was 98%. Figure 3 shows the "scree plot", which clearly demonstrates the contribution of each main component to the overall variance.

[2] Prikazchikova A.S., Ivanov V.V. Application of artificial neural networks for forecasting deviant activity of credit organizations as subjects of financial monitoring // Threats and risks of financial security in the context of digital transformation [Proceedings of the VII International Scientific and Practical Conference of the International Network Institute in the field of AML/CFT]. — M., 2021. — pp. 517-525.

[3] Simon Haykin. Neural networks: A comprehensive foundation. 2nd edition. Prentice Hall, Inc, 1999.

[4] Artificial neural networks and applications: studies. manual / F.M. Gafarov, A.F. Galimyanov. — Kazan: Kazan Publishing House. un-ta, 2018. — 121 p.

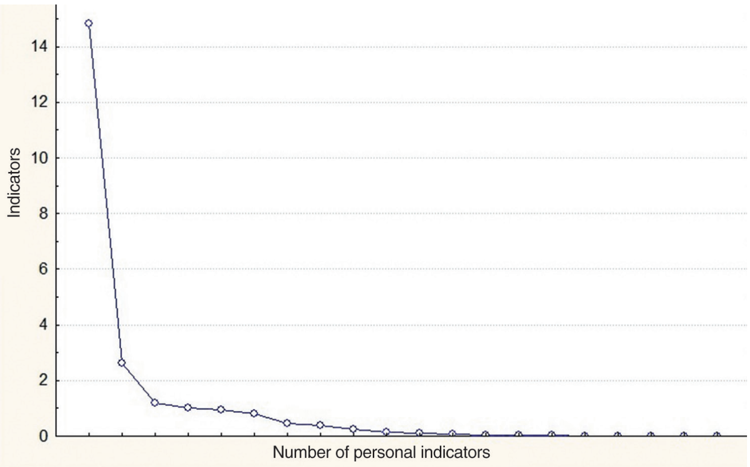
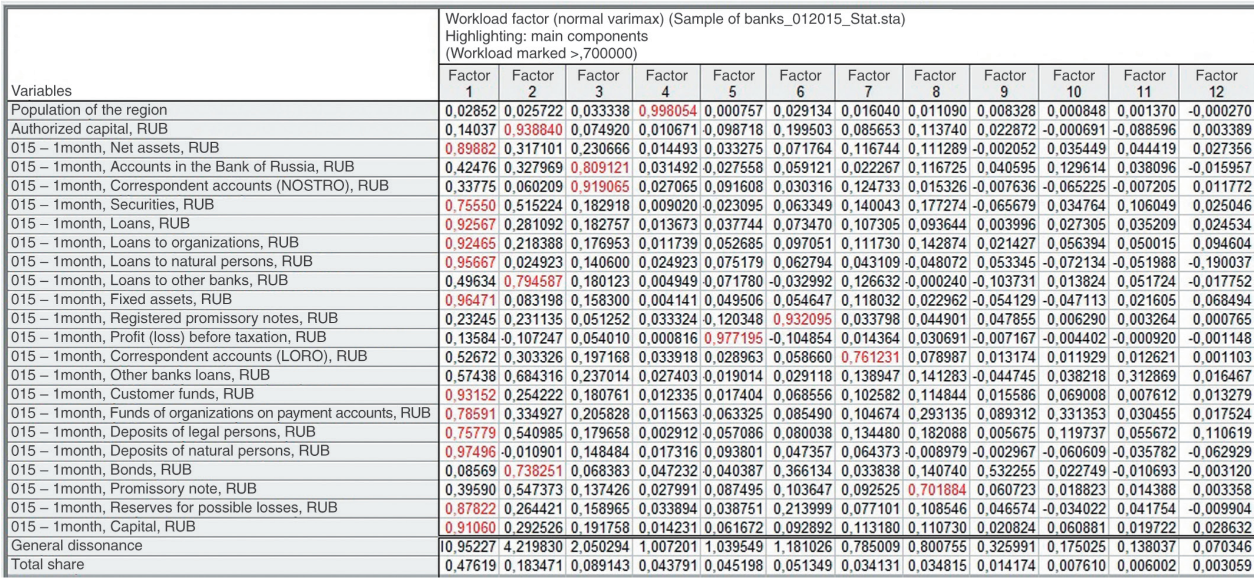


Fig. 3. Graph of personal indicators



Workload factor (normal varimax) (Sample of banks_012015_Stat.sta)
Highlighting: main components
(Workload marked >,700000)

Variables	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7	Factor 8	Factor 9	Factor 10	Factor 11	Factor 12
Population of the region	0,02852	0,025722	0,033338	0,998054	0,000757	0,029134	0,016040	0,011090	0,008328	0,000848	0,001370	-0,000270
Authorized capital, RUB	0,14037	0,938840	0,074920	0,010671	-0,098718	0,199503	0,085653	0,113740	0,022872	-0,000691	-0,088596	0,003389
015 – 1month, Net assets, RUB	0,89882	0,317101	0,230666	0,014493	0,033275	0,071764	0,116744	0,111289	-0,002052	0,035449	0,044419	0,027356
015 – 1month, Accounts in the Bank of Russia, RUB	0,42476	0,327969	0,809121	0,031492	-0,027558	0,059121	0,022267	0,116725	0,040595	0,129614	0,038096	-0,015957
015 – 1month, Correspondent accounts (NOSTRO), RUB	0,33775	0,060209	0,919065	0,027065	0,091608	0,030316	0,124733	0,015326	-0,007636	-0,065225	-0,007205	0,011772
015 – 1month, Securities, RUB	0,75550	0,515224	0,182918	0,009020	-0,023095	0,063349	0,140043	0,177274	-0,065679	0,034764	0,106049	0,025046
015 – 1month, Loans, RUB	0,92567	0,281092	0,182757	0,013673	0,037744	0,073470	0,107305	0,093644	0,003996	0,027305	0,035209	0,024534
015 – 1month, Loans to organizations, RUB	0,92465	0,218388	0,176953	0,011739	0,052685	0,097051	0,111730	0,142874	0,021427	0,056394	0,050015	0,094604
015 – 1month, Loans to natural persons, RUB	0,95667	0,024923	0,140600	0,024923	0,075179	0,062794	0,043109	-0,048072	0,053345	-0,072134	-0,051988	-0,190037
015 – 1month, Loans to other banks, RUB	0,49634	0,794587	0,180123	0,004949	-0,071780	-0,032992	0,126632	-0,000240	-0,103731	0,013824	0,051724	-0,017752
015 – 1month, Fixed assets, RUB	0,96471	0,083198	0,158300	0,004141	0,049506	0,054647	0,118032	0,022962	-0,054129	-0,047113	0,021605	0,068494
015 – 1month, Registered promissory notes, RUB	0,23245	0,231135	0,051252	0,033324	-0,120348	0,932095	0,033798	0,044901	0,047855	0,006290	0,003264	0,000765
015 – 1month, Profit (loss) before taxation, RUB	0,13584	-0,107247	0,054010	0,000816	0,977195	-0,104854	0,014364	0,030691	-0,007167	-0,004402	-0,000920	-0,001148
015 – 1month, Correspondent accounts (LORO), RUB	0,52672	0,303326	0,197168	0,033918	0,028963	0,058660	0,761231	0,078987	0,013174	0,011929	0,012621	0,001103
015 – 1month, Other banks loans, RUB	0,57438	0,684316	0,237014	0,027403	-0,019014	0,029118	0,138947	0,141283	-0,044745	0,038218	0,312869	0,016467
015 – 1month, Customer funds, RUB	0,93152	0,254222	0,180761	0,012335	0,017404	0,068556	0,102582	0,114844	0,015586	0,069008	0,007612	0,013279
015 – 1month, Funds of organizations on payment accounts, RUB	0,78591	0,334927	0,205828	0,011563	-0,063325	0,085490	0,104674	0,293135	0,089312	0,331353	0,030455	0,017524
015 – 1month, Deposits of legal persons, RUB	0,75779	0,540985	0,179658	0,002912	-0,057086	0,080038	0,134480	0,182088	0,005675	0,119737	0,055672	0,110619
015 – 1month, Deposits of natural persons, RUB	0,97496	-0,010901	0,148484	0,017316	0,093801	0,047357	0,064373	-0,008979	-0,002967	-0,060609	-0,035782	-0,062929
015 – 1month, Bonds, RUB	0,08569	0,738251	0,068383	0,047232	-0,040387	0,366134	0,033838	0,140740	0,532255	0,022749	-0,010693	-0,003120
015 – 1month, Promissory note, RUB	0,39590	0,547373	0,137426	0,027991	0,087495	0,103647	0,092525	0,701884	0,060723	0,018823	0,014388	0,003358
015 – 1month, Reserves for possible losses, RUB	0,87822	0,264421	0,158965	0,033894	0,038751	0,213999	0,077101	0,108546	0,046574	-0,034022	0,041754	-0,009904
015 – 1month, Capital, RUB	0,91060	0,292526	0,191758	0,014231	0,061672	0,092892	0,113180	0,110730	0,020824	0,060881	0,019722	0,028632
General dissonance	10,95227	4,219830	2,050294	1,007201	1,039549	1,181026	0,785009	0,800755	0,325991	0,175025	0,138037	0,070346
Total share	0,47619	0,183471	0,089143	0,043791	0,045198	0,051349	0,034131	0,034815	0,014174	0,007610	0,006002	0,003059

Fig. 4. A table with the correlation of the initial indicators and the principal components

Figure 3 shows a graph of the "rocky scree", which clearly demonstrates the contribution of each principal component to the overall variance.

It can be seen from Fig. 3 that the largest contribution is made by the first main component, and starting from the 12th component, the contribution increase is minimal. Figure 4 shows the results of the correlation analysis of the initial indicators and the generated principal components. Using the values of the correlation coefficients between the principal components and the initial predictors, the Rosfinmonitoring analyst has the opportunity to analyze each new factor (the principal component).

We interpret the first three principal components. The first factor has a strong relationship (a high value of the correlation coefficient) with the following initial indicators: net assets, securities, loans, loans to organizations, loans to individuals, fixed assets, customer funds, funds of organizations on current accounts, deposits of legal persons, deposits of natural persons, reserves for possible losses, capital. In this connection, this factor characterizes the financial viability of the bank, its solvency and active work with clients - both natural and legal persons.

The second factor has a high correlation coefficient with the authorized capital, loans to other banks, bonds. Thus, the second principal component characterizes the financial ability of the bank to lend funds, as well as guarantee the interests of its creditors.

The third factor has a high correlation coefficient with accounts in the Bank of Russia and correspondent accounts (NOSTRO). The third principal component characterizes the state of the bank's correspondent accounts opened with the Central Bank of Russia or with other banks for mutual settlements.

At the final stage of the study, a new neural network was built, the input of which was supplied with the values of 23 principal components. The network architecture was chosen according to a model based on the initial indicators of banking activity. The highest value of the productivity of the new neural network from the constructed models was 72%.

The authors also analyzed the values of the productivity of neural networks built on different numbers of principal components. Thus, during the development of a neural network on 12 principal components generated during factor analysis, the value of network performance was 69.4%.

Figure 5 shows the distribution of credit institutions according to the output of a neural network built on the first 12 principal components. The red line in the figure differentiates reliable and high-risk credit organizations from the point of view of involvement in illegal activities (reliable banks are located to the left to the line).

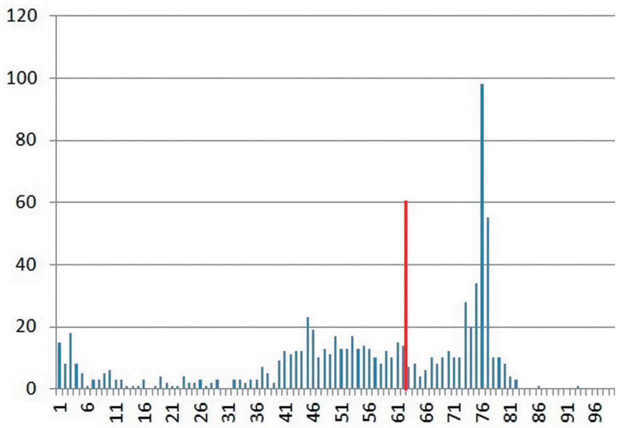


Fig. 5. Neural network output distribution (for all banks): aggregation window = 0.01, 12 principal components

Based on the results obtained during the study, we can conclude the following:

- application of artificial neural networks to the task of identifying credit institutions potentially involved the activity of money laundering is appropriate and justified from a practical point of view. The neural network performance for data characterizing banking activity was 72%;
- application of the principal component method for the analysis of data contained in in the bank reporting form No. 101, allowed to reduce the initial feature space from 23 indicators to 12 principal components, the contribution of which the total variance was more than 98%;
- the value of the performance of the neural network, to the input of which was submitted 12 principal components (69%), commensurate with the performance value of a neural network built on the initial performance indicators of credit institutions (72%).

THE DEVELOPMENT OF AML/CFT SYSTEMS[1] IN THE CONTEXT OF BLOCKCHAIN FUNCTIONING

Christina Kochetkova,

The First Category Specialist, the supervision and legal division of the Rosfinmonitoring North-West Federal District Interregional Department

Christina Kochetkova

In the context of technological development, there is an increase in the creation and use of the digital platforms. The concept of such platforms is implemented by the digital transformation, which covers a wide range of products and services that form the economic sector, as well as key business processes: from communication with counterparties to keeping and processing of the data stock, from decision-making procedures to servicing channels for products and services. Advanced technologies and the creation of the new forms of economic cooperation between subjects today transform the usual methods of control within the functioning of financial systems around the world. A characteristic feature is the use of intelligent infrastructure as a combination of the modern tools and interfaces that provide the processing of various kinds of data and the use of a set of tools for protecting and processing information using advanced analytics technologies for decision-making. Algorithms based on machine learning, distributed registry technologies and other forms of engagement under the increasing influence become the basis for creating an effective and advanced system of the data analysis processes automation and the continuous interaction with information flows, allowing qualitative improvement of the cooperation within the framework of the AML/CFT system.

The use of new technologies is primarily aimed at creating the possibility of a proper assessment of ML/TF risks in dynamics. Full or partial automation of the process makes it possible to neutralize the human factor in the analysis and the risks assessment when necessary, as well as to take into consideration a large amount of transactions details. According to the

[1] Countering the legalization (laundering) of proceeds from crime and the financing of terrorism.

data of the FATF Digital Transformation questionnaire, the greatest potential in the development of AML/CFT systems in terms of efficiency improvement is possible with the integration of artificial intelligence (hereinafter – AI) and its components, as well as the use of application programming interfaces (API) and customer due diligence tools (hereinafter – CDD). However, in the context of increasing threats posed by the development of the shadow sector of the economy associated with the illegal circulation of digital financial assets (hereinafter referred to as the DFA) and illegal activities, the organization of the operation of financial intelligence units (hereinafter referred to as FIU) in the context of functioning of the blockchain becomes especially relevant. To date, virtually all operations with the DFA take place on foreign blockchain platforms, and therefore the control over performed operations is carried out by FIUs of foreign countries. At the same time, the legislative framework for regulating the cryptocurrency market and other DFAs abroad is in quite different.

This fact highlights the need to build up the effective communication and the information exchange between the FIUs. It is of high importance for the countering of money laundering and terrorist financing (hereinafter referred to as CML/TF) activity international regulations, the database of digital asset owners expansion, sharing the experience and best practices in identifying, suppressing, documenting, investigating and prosecuting for commission of crimes using cryptocurrencies.

The trend of increasing the degree of use of blockchain technologies has a global scale and has an impact on the development of the economy and social environment of many countries. Russia is the eighteenth of the twenty-three countries having been studied for the best conditions for the blockchain projects development. It indicates the need for blockchain innovations, getting out of the initial stage and increasing the influence. There is a need to create a legitimate and infrastructural environment for the governing of the blockchain technologies. Currently within the development of the DFA regulation it has become possible to create a new tool for transactions monitoring - “Transparent Blockchain". Its functionality aims at the centralized control and deanonymization of the beneficiaries of performing the ML/TF operations. The internal structure of the service allows you to subdivide operations into clusters conducting a more effective analysis of the of virtual assets (VA) flows to identify and suppress the illegal activities. At the same time, it is worth noting that the service is aimed at analyzing transactions in the Bitcoin currency, but currently the use of the alternative blockchains (Ethereum, Cosmos, Ripple and others) is also relevant. The above-mentioned platforms are participants in the “open” blockchain, since they are not only used by most digital assets, but also allow to access the data of any transaction. Thus, there is a need to introduce functionality into the service that allows to cover a wider range of operations with the DFA by integrating it with other currencies.

Blockchain should not be considered as a static unit, as it is constantly improved and strives to occupy key positions. Since blockchain is changing the traditional ways of counterparty interaction, a company that has implemented blockchain in its processes has the opportunity, and in some cases, the need to create a new type of business model for itself. Within the framework of the AML/CFT system, the integration of advanced elements of intellectual infrastructure into systems and services will change the situation in the DFA market and create a sustainable competitive advantage for Rosfinmonitoring in this area.

Thus, the factors determining the development of AML/CFT systems within the DFA control of the blockchain platforms transactions as well as the identification of risks require the communication with the FIU, expanding the functionality of the existing tools that overview transactions in order to reduce economic crime and enhance the monitoring of the dubious operations.

The digitalization of the AML/CFT systems and the complication of the internal structures within the existing problems of the DFA control markets turnover will effect positively on the further implementation of the powers of Rosfinmonitoring under the Federal Law No. 115-FZ dated 07.08.2001 "On combating legalization (laundering) of proceeds from crime and financing of terrorism."

DIGITAL TRANSFORMATION IN THE PROCESS OF AML/ CFT PERSONNEL TRAINING

GRAPHUS EDUCATIONAL GAMING PLATFORM: TASKS, ADVANTAGES, PROSPECTS

Oleg Ivanov,
Deputy Development Director of the Lebedev Physical Institute

Rodion Gusev,
Engineer of the Laboratory of Mathematical Modeling of Complex Systems of the Lebedev Physical Institute

Aleksander Kovalenko,
Researcher at the Laboratory of Mathematical Modeling of Complex Systems of the Lebedev Physical Institute

Oleg Ivanov

Rodion Gusev

Aleksander Kovalenko

In the modern world of digital technologies, various tools for storing and processing data are constantly being created. These tools are quite complex to master and use. Young experts have to take long to study them and only simplify. In the field of financial intelligence the situation is similar due to the specifics of the investigation process: it's necessary to combine the fragmented information from the completely different sources. The modern software interfaces become more complex in terms of their practical application. The need for analysts of the specific competence is growing constantly. The Federal Financial Monitoring Service This has declared this problem. To solve it, the International Training and Methodology Center for Financial Monitoring in 2020 started the training system for financial investigations conduct. The ITMCFM goal was met by the Lebedev Physical Institute of the Russian Academy of Sciences.

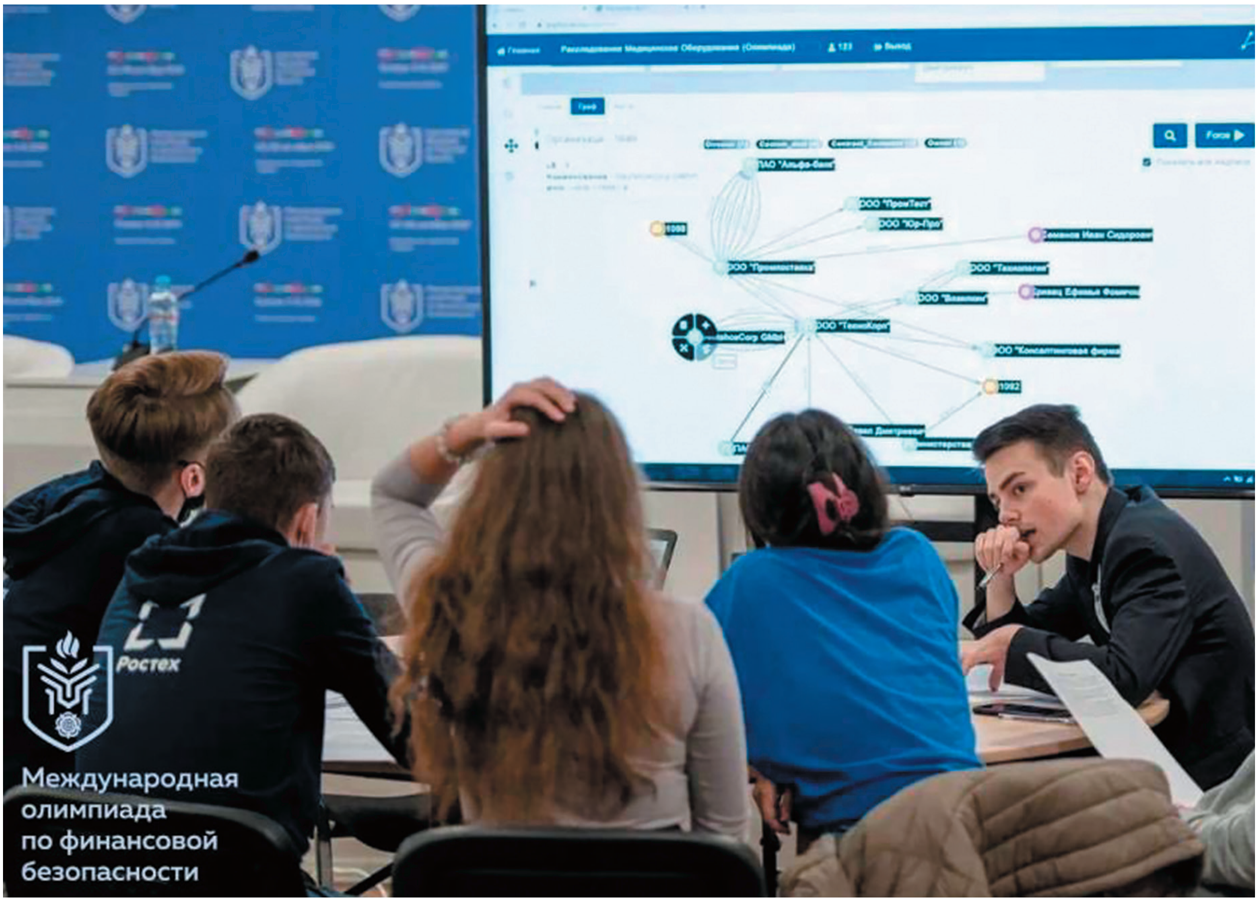
The newly created system, named "Graphus" was developed in the first half of 2021. It is based on a modern interface approach and NO-CODE methodology, thanks to which the simplest tasks of an analyst can be completed in 1-2 clicks, and even a senior pupil is able to master the system. For students and experienced specialists, respectively, it became possible to solve problems of various degrees of complexity: from initial training to proficiency testing during the application for the job. At the first International Financial Security Olympiad held in October 2021 in Sirius, the finalists were able to learn how to use the interface in less than 20 minutes, after which they successfully passed the test conducting real financial investigations.

The presentation of information in the form of a table is familiar to an experienced analyst, but using this form it is not possible to fully display all the interactions of objects with each other, unlike an image in the form of a graph. Graph — mathematical abstraction for a system with the interconnected objects.

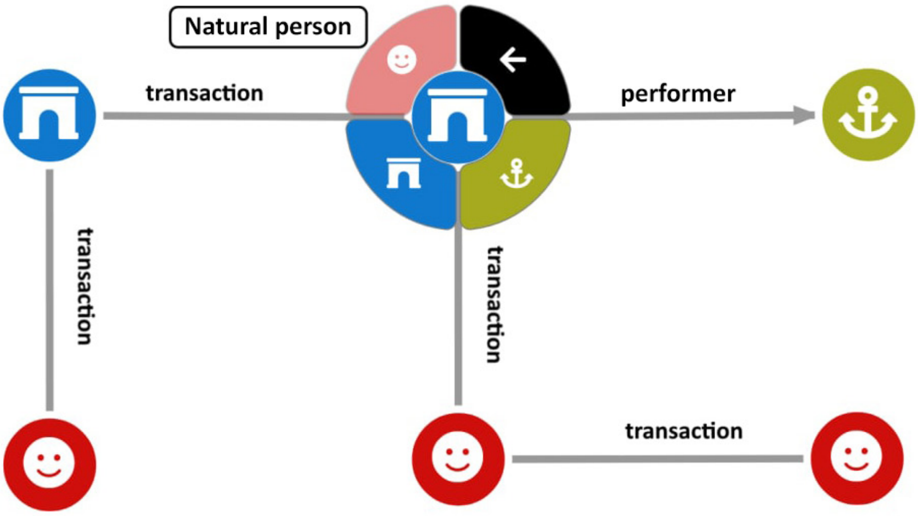
The simplest example of a graph is any social network. People get to know each other through friends, friends of their friends. Everyone has encountered something similar by clicking on a link to someone else's page. Thus, he walked along the social graph. This abstraction is also suitable for describing transactions between bank users' accounts. That is, people's connections with each other by phone calls, family ties or air travel.

In any work with data, it is necessary to filter it in order to find the required information. Today there are several ways to achieve this. The most widespread of them are: for databases — SQL queries; for tables — filters; in the Internet — the browser search bar. These methods are suitable for graph description of information, but they become difficult for the user. For this reason, scientists from around the world are constantly experimenting with visual query tools. With their help, the user actually recreates visually that object or a row of connected objects that he/she needs to find.

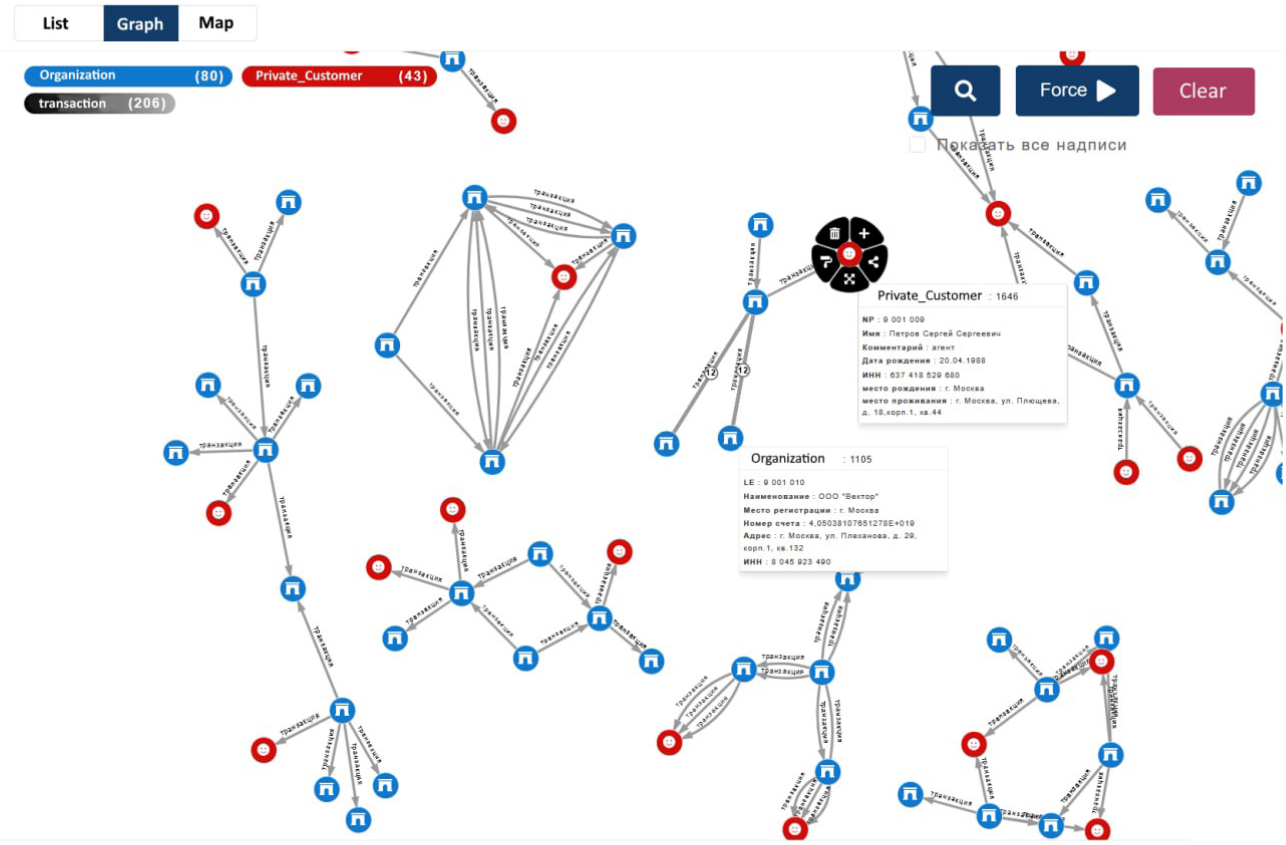
Graphus has developed the ability to construct the filter for data in a simple and clear way, thanks to which the user of the system spends a minimum amount of time on training and immediately starts solving the task — identification and analysis of a financial crime.



The Sirius Olympiad



Visual query



Private_Customer : 1646

NP : 9 001 009
Имя : Петров Сергей Сергеевич
Комментарий : агент
Дата рождения : 20.04.1988
ИНН : 637 418 529 680
место рождения : г. Москва
место проживания : г. Москва, ул. Плющева, д. 18,корп.1, кв.44

Organization : 1105

LE : 9 001 010
Наименование : ООО "Вектор"
Место регистрации : г. Москва
Номер счета : 4,05038107651278E+019
Адрес : г. Москва, ул. Плеханова, д. 29, корп.1, кв.132
ИНН : 8 045 923 490

Query result

Joint work with Rosfinmonitoring and ITMCFM analysts allowed us to create an almost complete imitation of a financial investigation with all its stages. Real crimes have been digitized, sanitized and transferred to the system. The investigation is presented in the form of a game in which, with the help of full-text search and visual query tools, it is necessary to solve a crime and answer specially formulated questions. All user actions are recorded in real time and displayed on the scoreboard, where all the statistics of their investigation are displayed. The jury can evaluate not only the answers to the questions directly, but also the quality of analytical work - the path that the user has traveled. If you somehow get the ready answer, but do not go through the entire chain of vertices of the graph, which are necessary for correct reasoning, it is impossible to get the maximum score. For administrators the system provides the possibility of creating new tasks. The peculiarity of the platform is that the system does not require installation on a computer. Graphus works as a website and is accessible to any user with Internet access.

Systems with similar functionality are used by financial intelligence officers in different countries, but they are quite difficult to master, which distinguishes the Graphus platform favorably and allows even children to study on it. It is worth noting that abstract thinking is actively developing during such training, since graphs clearly describe various complex structures due to intuitive visualization. In the future, it is planned to actively use the system in the process of training new personnel, as well as to continue to use the platform as part of the International Financial Security Olympiad at Sirius.

THE INTERNATIONAL SCIENTIFIC AND EDUCATIONAL DIGITAL PLATFORM "SODRUZHESTVO" IS A NEW FORMAT OF COOPERATION IN THE SPHERE OF FINANCIAL SECURITY AND AML/CFT

Alexey Bakharev,

Chief Specialist of the Department for Coordination of Scientific and Educational Projects, ITMCFM

Alexey Bakharev

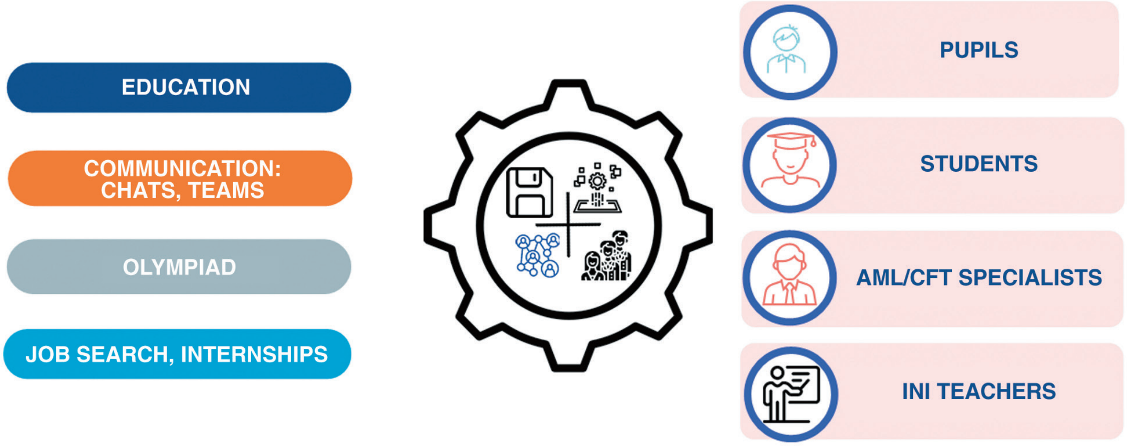
The economic problems of the beginning of the 21st century became a catalyst for revising the countries' position on ensuring the financial system transparency, giving a new impetus to the efforts of states to counter the use of global and national financial systems for illegal purposes, as well as to ensure the financial security of their citizens and enterprises. The shadow economy distorts the market distribution of capital flows between countries and poses a potential threat to the stability of national economies.

All this poses new challenges for the Russian Federation and its partner countries in the sphere of financial security, the implementation of which depends on the personnel's training and qualification level, as well as on the population's knowledge level, in general.

In modern realities, education is increasingly immersed in the digital space. In the digital space, it is necessary to create safe conditions for young people to obtain the required knowledge, opportunities for communication, including with the expert community in the areas of financial security, and to enable pupils and students to become full members of this community, regardless of their residence and future specialty.

“SODRUZHESTVO” PLATFORM:

- **The main financial security information resource**
- **The largest professional social network in the CIS**
- **Basis for the development of professional personnel reserve**



By Assignment of the President of the Russian Federation (Pr-103 dated 26.01.2021), the International Financial Security Olympiad (hereinafter referred to as the “Olympiad”) has been held for the second consecutive year. About 40 thousand pupils and students from Armenia, Belarus, Brazil, India, Kazakhstan, China, Kyrgyzstan, Russia, Tajikistan, Turkmenistan, Uzbekistan, South Africa attended the event. By Order of the Government of the Russian Federation (No. 2604-r dated September 18, 2021), the Olympiad received the status of an annual event. Also, every year the Olympiad is preceded by a thematic lesson on financial security (hereinafter – the “Lesson”), in which more than two million high school pupils from the CIS countries took part this year. Financial intelligence units of the BRICS countries showed the great interest to the Lesson.

The Olympiad creates conditions for the organization of international youth movement in the field of financial security, which unites pupils and students with professors and teachers of the International Network AML/CFT Institute (hereinafter – the “INI”) and financial intelligence experts of Russia's partner countries in the international anti-money laundering system. According to preliminary estimates, the number of the united community in the CIS countries alone may amount to several million participants.

The basis for the development of such youth movement, including its geographic scope expansion, will be the International Scientific and Educational Digital Platform "Sodruzhestvo" (hereinafter referred to as "Sodruzhestvo" platform). Its mission will be the attraction of the younger generation’s attention to knowledge, new forms of thinking, modern formats of activity and key aspects of financial security from the individual to the state and commonwealth of countries. “Sodruzhestvo” platform will provide a technological base (digital environment) for the development and support of the youth Olympiad movement of pupils and students on financial security in the Russian Federation and its partner countries in the international anti-money laundering system. It will allow them to maintain communication, acquire new knowledge, exchange experience and, among other things, accompany each participant of the Olympiad.

In the context of the digital transformation of modern society, “Sodruzhestvo” creates the following opportunities:

- to develop unified digital environment that ensures joint implementation of research and educational projects using analytical tools within geographically distributed interdisciplinary groups involving pupils, students, teachers, young scientists and all interested users;
- to accumulate information and form knowledge bases in the sphere of financial security, as well as the results of educational and research activities in integration of internal platform services with external information systems and Internet resources;

- to provide access to digital platform resources through the platform portal and users' personal accounts;
- to promote the initiatives of the Russian Federation and its partner countries in the international anti-money laundering system for the development of the youth international Olympiad movement on financial security on the international EAEU, CIS, EAG, BRICS, FATF platforms, etc., including by increasing the number of participating countries;
- to ensure the materials preparation for the Olympiad organization in the mass media in Russia and the participating countries, to promote the financial security information distribution and the population’s financial literacy improvement;
- to facilitate the career guidance for pupils and students – participants, prize-winners and winners of the Olympiad and their support;
- to develop socio-humanitarian tools of cooperation between partner countries on the international anti-money laundering platform for education and science in the area of information and financial security with an emphasis on the joint holding of the Olympiad.

It is planned to organize interaction between users of the “Sodruzhestvo” platform, including by providing information in a game form, which, from our point of view, will increase the interest of young people in expanding their knowledge and skills with the use of its services: chats, lecture halls, discussion platforms, supranational research laboratories, scientific, educational and project centers on financial security.

The rating system of the “Sodruzhestvo” platform will allow to organize cooperation between students, teachers and experts, taking into account the level of available knowledge and demands on obtaining the necessary competencies. As for employers, scoring will allow them to choose the best junior expert with the required level of professional training.

Human potential is the most important criteria for the society welfare. Support of the younger generation and assistance in building a professional trajectory is a general state, supranational task. Correct value system and behavioral models of modern youth are a significant contribution to the political stability, economic and financial security of the country, enterprises, households and individuals in the commonwealth of countries of the international anti-money laundering system.

The “Sodruzhestvo” platform will become a unified digital space for the formation of an extensive base of knowledge and competencies, enable expansion of new formats of interaction between young people and the expert community, including within the framework of the International Financial Security Olympiad, strengthen cooperation and promotion of integration of the EAG, CIS and BRICS countries, as well as will make the significant contribution to the educational process and personnel training for national anti-money laundering systems.

“SODRUZHESTVO” DIGITAL PLATFORM OF FINANCIAL SECURITY

With the support of PJSC "Promsvyazbank", the international digital platform "Sodruzhestvo" is being created in Russia. It will become the technological basis for the International Financial Security Olympiad. Rosfinmonitoring is the project initiator

“Promsvyazbank” (PSB) is one of the technological leaders in the Russian financial market: over the past few years, the bank has implemented a number of its own large–scale projects in the field of digitalization. Today, PSB is ready to share its experience with partners, and one of such joint IT projects is the digital platform "Sodruzhestvo".

FROM IDEA TO IMPLEMENTATION

Following the results of the International Financial Security Olympiad held in October 2021, the head of Rosfinmonitoring, **Yuri Chikhanchin**, had suggested that the President of the Russian Federation **Vladimir Putin** should support creation of the international digital platform "Sodruzhestvo", which would unite young people and the expert community, provide a communication space and access to a knowledge base on the topic of financial security, and also serve as an electronic platform for the Olympiad participants. The President and the Government of the Russian Federation supported the initiative, appointing PSB as an industrial partner of the project.

> *"The reliable information systems development guarantees us transparency and sustainability. The focus is on the personal financial security in the context of globalization and digitalization. It is necessary to teach the younger generation the basics of financial literacy," Dmitry Chernyshenko, Deputy Prime Minister of the Russian Federation, explained the project goals at the conference "Threats and Risks of Financial Security in the Context of Digital Transformation".*

In a short time, the PSB developed the digital platform draft concept and technical specifications, prepared a package of documents necessary for its launch, conducted focus groups with students of the Russian universities, as well as the comparative analysis of educational platforms operating in the country and abroad. The concept has been examined in the specialized agencies – the Ministry of Science and Higher Education, the Ministry of Education, Rosfinmonitoring and the Ministry for Digital Technology, Communication and Mass Media of the Russian Federation.

THE PLATFORM MAIN FEATURES

The digital platform is designed for 8-11th grade pupils, university students and AML/CFT specialists. The annual potential audience of “Sodruzhestvo” in Russia and the EAG member states will amount to approximately 3 million people. As the digital platform develops, it will expand the functionality called-for by the users at leading domestic and foreign educational platforms: UCHI.ru, Moscow Electronic School (MES), Linkedin, Discord. However, the international cooperation in the field of financial security will be the main thematic focus of the platform.

According to the concept presented by PSB, the “Sodruzhestvo” digital platform will consist of five main blocks: education; communication in the format of chats; personal account; communication in the format of a web laboratory; job search, internships.

The "Education" block will provide a user with the access to the relevant courses, all the necessary information on the topics of the International Financial Security Olympiad, and to the registration. The AML/CFT specialists will be able to improve their qualifications and confirm it with the help of certification. The "Communication: chats" block will give users the opportunity to communicate in person and in group chats dedicated to a certain topic. The information support of the Olympiad will be implemented in this block. Within the "Personal Account" users will be able to get information about completed and current Olympiad courses and about the certificates received. A user rating and a loyalty points system will be introduced into the digital platform. Within the "Communication: Web Labs" block, users will have the opportunity to carry out projects in geographically distributed teams, including the preparation of bachelor's and master's graduation projects, as well as conducting joint research in the AML/CFT sphere. In the "Job search, internships" block, profile areas job vacancies will be placed. The user will be able to study the requirements of vacancies and assess his/her training level. Employers will get acquainted with candidates' CVs, including courses completed on the Digital Platform, user rating, competence map.

LONG-TERM COOPERATION

At the XXV St. Petersburg International Economic Forum, which took place this year, PSB and Rosfinmonitoring consolidated cooperation with an official document – an agreement on intentions. The signatories were the head of Rosfinmonitoring **Yuri Chikhanchin**, Chairman of PSB **Petr Fradkov**, Minister of Science and Higher Education of the Russian Federation **Valery Falkov**, Director General of the Autonomous Non-Profit Organization "International Training and Methodology Center for Financial Monitoring" **Margarita Andronova**.

The document stipulates that the parties become the organizers of the International Financial Security Olympiad final stage in the federal territory "Sirius" in October 2022, and PSB is the developer of the international digital platform "Sodruzhestvo". In addition, the partners shall create for the platform the educational programs on financial security and compliance control.

> *"The modern digital platform "Sodruzhestvo" will provide a convenient tool for testing and enrich the knowledge of the Olympiad participants through plentiful educational programs prepared jointly with PSB, which has an extensive expertise in the field of banking," commented Petr Fradkov.*

Yuri Chikhanchin pointed that the successfully held International Financial Security Olympiad in 2021 demonstrated a high level of pupils' and students' involvement in financial security issues, their desire to test and increase their strengths and knowledge in a competitive environment.

"In this regard, the creation of the international digital platform "Sodruzhestvo", which will become the foundation of a large educational movement, is an important stage in the modern teaching methods development. We hope for the earliest possible implementation of the project," said **Yuri Chikhanchin.**

According to the developers, the digital platform will also strengthen cooperation and promote the Eurasian countries integration.

PROMSVYAZBANK ACADEMY – PLACE WHERE THE BEST EDUCATIONAL SOLUTIONS ARE ACCUMULATED

Press service of PJSC "Promsvyazbank"

ABOUT PROMSVYAZBANK (PSB) ACADEMY

The PSB Academy is the corporate university of PJSC “Promsvyazbank”.The purpose of the PSB Academy activity is to provide services of the additional professional education and to increase the knowledge level and competencies of the specialists from the military-industrial complex, the militaries and their families, as well as of the external trainees.

PSB ACADEMY EDUCATIONAL PLATFORM

The Academy activity relies on the modern trends in the professional areas and provides perspective educational technologies and solutions.

By the end of 2022, it is planned to launch the Digital Educational Platform - a unified informational and learning space based on the modern technological solutions expanding the usual course marketplace model. The Platform provides not only the organization and support to the training process, but also gives tools to assess the competencies, to form the individual learning trajectories, to create the author's educational content by the experts – the PSB Academy partners.

The content of the Platform will be based on the courses and programs developed by the PSB Academy, the joint programs with the leading universities, industrial and technological partners, and author's courses of the well-known experts.

Photo: Press Service of the Agency for the Strategic Initiatives (ASI)

The registered companies will post information on the Platform on the vacancies, internships and online events to give the PSB Academy trainees the opportunity to apply their knowledge in practice.

The digital Platform will provide remote log to the educational materials, courses and will allow the classes to be held in the most comfortable and accessible format for the trainees.

> *«The creation of the PSB Academy educational ecosystem implies, on the one hand, the significant expansion of the opportunities for the citizens to acquire knowledge, improve their professional competencies, skills and find their application in the dynamically developing world. On the other hand, the opportunity to train highly qualified and motivated specialists and leaders able to find the best solutions. Accordingly, our task is to implement such a mechanism that will create the best conditions for the successful career track», - says Alexey Nechaev, the Rector of the PSB Academy.*

THE SOCIAL MISSION OF THE PSB ACADEMY

As the corporate university of the basic bank for the Russian military-industrial complex, the Academy sets the integrated task of the professional retraining. It is planned to ensure the maximum adaptation of the former military personnel to build their civil professional career and the subsequent full employment of the citizens after the completed the PSB Academy special programs.

During the International Military-Technical Forum "Army-2022", the PSB Academy presented the draft model "Ecosystem of the social adaptation, training and career development of the citizens resigning from the Ministry of Defense of the Russian Federation", also planned to be implemented on the basis of the Academy's digital platform.

In addition, the Academy's project "Small Business Course" was announced at the Forum. The project provides free-of-charge education for the military staff and their wives. The course was developed jointly with the National Research University Higher School of Economics with the support of Promsvyazbank and the Russian Ministry of Defense.

In the near future, it is planned to start the course "Information Security" for the reserve officers who want to develop themselves in the IT field.

Alexey Nechaev positively assessed the participation of the PSB Academy at the «Army-2022» Forum:

«The PSB Academy concluded several important agreements with the country's leading universities and educational platforms, such as MGIMO, the Federal State Autonomous Higher Education Institution, Pirogov Russian National Research Medical University of the Ministry of Health of the Russian Federation, Autonomous Non-Profit Organization of Additional Professional Education Multidisciplinary Qualification Center "Goal" (the group of the affiliate audit and consultancy network "Rukon"), University 20.35. We plan to share the experience, work on the development of the joint educational programs and to contribute to the development of the country's human resources potential».

INTERNATIONAL NETWORK AML/CFT INSTITUTE: ELECTRONIC SERVICES AS AN ELEMENT OF PERSONNEL TRAINING FOR THE PRIVATE SECTOR OF THE RUSSIAN ANTI-MONEY LAUNDERING SYSTEM

Igor Barinov,

Head of the Information Technology Department, International Training and Methodology Center for Financial Monitoring (ITMCFM)

Igor Barinov

For a modern employer who recruits recent graduates, the phrase "forget everything you were taught" becomes less relevant. "Show what you can do" — that is what he expects from the new generation now.

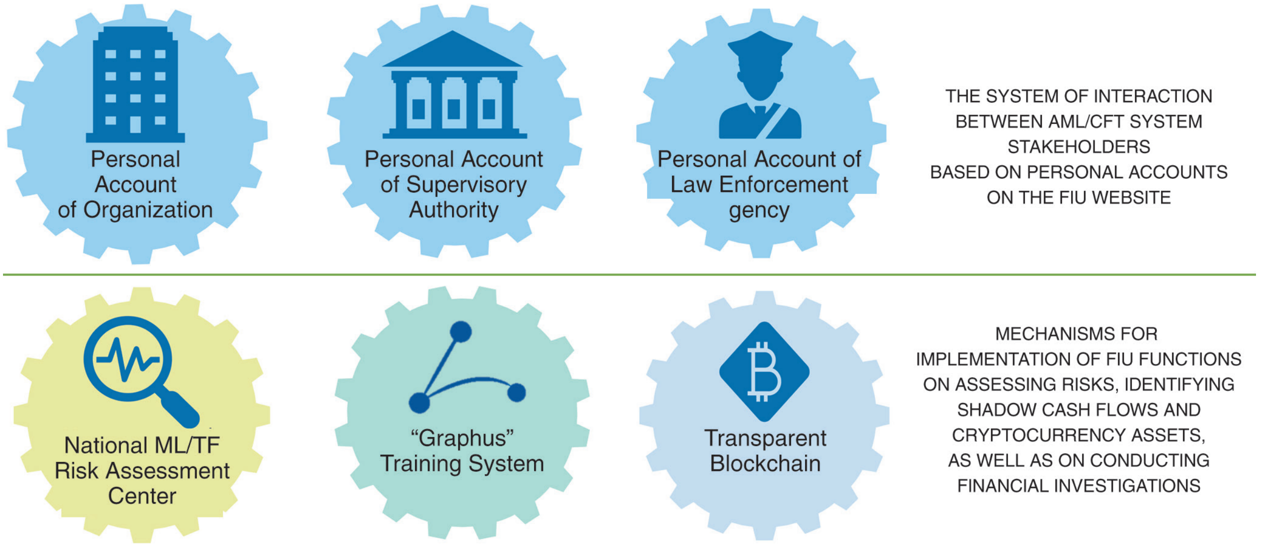
One of the measures taken by the ITMCFM as a reaction to the new paradigm is the priority of the practice-oriented approach introduction into the educational activities of the International Network AML/CFT Institute's (INI) universities, reinforcing theoretical knowledge in the AML/CFT sphere.

The operation of the anti-money laundering system can be represented as an AML/CFT process, which consists of several stages.

For each of these stages, its own mechanism has been created using IT tools aimed at ensuring the effectiveness of the entire process.

It is worth noting that the FATF experts have estimated the Russian AML/CFT system and its mechanisms as one of the most effective in the world.

Basic AML/CFT Electronic Services at the ITMCFM Digital Polygon


Personal Account of Organization
Personal Account of Supervisory Authority
Personal Account of Law Enforcement gency
National ML/TF Risk Assessment Center
“Graphus” Training System
Transparent Blockchain

THE SYSTEM OF INTERACTION BETWEEN AML/CFT SYSTEM STAKEHOLDERS BASED ON PERSONAL ACCOUNTS ON THE FIU WEBSITE

MECHANISMS FOR IMPLEMENTATION OF FIU FUNCTIONS ON ASSESSING RISKS, IDENTIFYING SHADOW CASH FLOWS AND CRYPTOCURRENCY ASSETS, AS WELL AS ON CONDUCTING FINANCIAL INVESTIGATIONS

It is obvious that efficiency largely depends on the quality and quantity of the allocated resources, primarily, on staff capacity. It was the logical decision to implement a large-scale project on integration into INI universities’ educational process of practical AML/CFT training based on existing mechanisms and software products.

As a result, in the spring of 2021, the list of IT solutions approved for educational purposes was formed. In the summer of the same year, the ITMCFM expanded a digital platform on the cloud infrastructure. Six basic electronic educational services, almost completely covering the entire AML/CFT process, were launched.

Three of them develop a system of interaction between AML/CFT system stakeholders based on Personal accounts on the website of financial intelligence units (FIUs):

- Personal account of organization
- Personal account of supervisory authority
- Personal account of law enforcement agency

This well-established system proved itself well in Rosfinmonitoring.

The second block is the mechanisms for implementation of FIU functions on assessing risks, identifying shadow cash flows and cryptocurrency assets, as well as on conducting financial investigations.

It also consists of three services simulating Rosfinmonitoring’s original solutions:

National ML/TF Risk Assessment Center

- "Transparent Blockchain"
- “Graphus” training tystem for conducting financial investigations

The introduction of electronic services into educational process began with the tournament using “Graphus” training system in the final stage of the International Financial Security Olympiad.

This new educational project was launched in early October 2021.

The AML/CFT system as one of the main components of financial security was comprehensively presented in the Olympiad program.

The Olympiad positioning as a competitive platform for financial security skills, primarily in AML/CFT, may become one of the directions of this activity’s development.

AML/CFT electronic services will act both as interactive simulators and as an infrastructure for conducting the competitions. In fact, it will be an AMLskills tournament.

The electronic services introduction into the educational environment continued this year with the launch of a pilot project by testing one service in several INI's universities and, in this regard, the parallel studying of two tasks:

- technical support of electronic services exploitation;
- training programs creation.

Programs are needed both to improve the qualifications of teachers and for students. Since the service is only a digital instrument for professional skills development, it is necessary to prepare an educational content for each service — a set of training and methodological materials: cases, assignments, tests that upgrade these skills in each specific area of study.

However, if it is necessary to go through the full cycle of AML/CFT process, the educational effect can be achieved by integrating electronic services with each other at the data level. It means that for each service, the case is created so that the uploaded information correlates with cases in other services.

Last year, the first stage of formation of a unified electronic service database was implemented.

As a result, AML/CFT electronic services will be combined into an educational ecosystem.

If we imagine the strategic prospects for the development of an ecosystem, then, including new services, modules and elements of artificial intelligence in it, we will get a kind of virtual model - an imitation of AML/CFT working system. Similar to the digital twins of cities or enterprises being created now, the next relevant solution may become the creation of a digital twin of the national AML/CFT system. It will be possible to consider its use as a "Hypper Sandbox" for testing regulatory and financial technologies, determining the effectiveness of measures taken and even the effectiveness of the system itself.

INTERDISCIPLINARY LABORATORY OF FINANCIAL INTELLIGENCE AND COMPUTER FORENSICS IS OPEN AT THE ROSTOV STATE UNIVERSITY OF ECONOMICS (RINH)

Elena Makarenko,

Rector of the Federal State Budgetary Higher Education Institution «Rostov State University of Economics (RINH)», Doctor of Economic Sciences, Professor

Yulia Yevlakhova,

Acting Head of the Department of Financial Monitoring and Financial Markets, Federal State Budgetary Higher Education Institution «Rostov State University of Economics (RINH)», Doctor of Economics, Associate Professor

Elena Makarenko

Yulia Yevlakhova

Modern society is a society of mass communications and big data, where the transformation of social reality takes place under the influence of technologies and the risks of manipulating the behavior of the population are actualized.

The progressive digital transformation of economy is related to scientific and technical progress and increased level of financial inclusion of population. The functionality of digital technologies creates a new platform for financial activities: support in taking credit and investment decisions, the availability of financial products and services and their personification through the processing and analysis of big data, new types of investment assets that have arisen on the basis of a distributed ledger system, etc. The progress in the big data processing technologies made it possible to research and analyse the new types of data (texts, videos, photographs, audio).

At the same time, the intensification of financial activity in the virtual aria, the change in the format of human interaction with financial organizations, the emergence of fintech companies, the digitalization

E. Makarenko with Consul of the Republic of Uzbekistan

of the financial sector has a wide range of consequences: from the problem of digital trust, that is, not readiness of the population, processes and technologies for the digital era, to the emergence of new types of financial fraud, actualization of digital threats to financial stability.

In the modern world, traditional methods of ensuring security, conducting investigations and data analysis should be effectively combined with digital technologies, and the digital environment itself should be subject to risk-based control that does not hinder its development. This request for interdisciplinarity explains the relevance of intersection of financial intelligence and computer forensics.

On June 1, 2022, the Interdisciplinary Laboratory of Financial Intelligence and Computer Forensics was opened at the Rostov State University of Economics (RINH). This is a high-tech scientific and educational laboratory, which is designed to respond to the modern challenges of the digital world, integrate cases from the real economic practice into the educational process and solve the tasks set by the current geopolitical situation, which changes the directions of scientific and educational cooperation, security requirements and IT infrastructure.

The activities of the Interdisciplinary Laboratory of Financial Intelligence and Computer Forensics are aimed at solving the following main tasks.

Firstly, it is expert, informational, analytical, organizational support to the projects of strategic partners of the Rostov State University of Economics (RINH) and joint cases and events.

Secondly, the involvement of students, postgraduates, and novice researchers in the laboratory work, their adaptation and integration into the international and national scientific network.

Thirdly, it is the enrichment of educational process through the implementation of the results of scientific research, the solution of the practice-oriented tasks, the use of digital design and modelling technologies, the preparation of new training courses.

The Interdisciplinary Laboratory of Financial Intelligence and Computer Forensics created all the conditions for the training of specialists capable of rapid adaptation in the modern conditions and competent in the latest digital technologies. The participation in the laboratory activities allows students not only to develop their skills in working with digital tools, improve their competencies at the intersection of finance and information technology and successfully solve professional tasks, but also to join the scientific and professional community at the national and international levels.

In the summer of 2022, RINH students and teachers tested the "Graphus" training system at the Interdisciplinary Laboratory and gave their suggestions for improving its work.

The functions of the Interdisciplinary Laboratory of Financial Intelligence and Computer Forensics are as following:

- to implement the fundamental and applied research projects, including by the request of the public authorities and local self-government bodies of the Russian Federation, enterprises and organizations of all forms of ownership, international organizations;
- to fulfill the expert projects, including within the relevant public, non-governmental and international working groups and commissions;
- to prepare and hold the relevant RINH's scientific conferences, seminars and discussions, as well as jointly with the public authorities and other interested structures; the support and expansion of the relevant scientific relations, including international ones;
- to public the scientific research results on the Internet and mass media;
- to organize training sessions for RINH students & postgraduates and master classes;
- to establish stable relations with professional participants to improve the employment opportunities for RINH graduates, etc.

The activities of the Interdisciplinary Laboratory of Financial Intelligence and Computer Forensics should achieve a number of effects. First of all, it is a synergetic effect generated from combination of the traditional financial research methods with the digital technologies and computer forensics.

In the future, such an interdisciplinary synergy, such a network interaction within the university will allow to achieve the external system effects, particularly the development of cooperation within the International Network AML/CFT Institute. Currently, Rosfinmonitoring and INI is working actively to create "Sodruzhestvo" scientific and educational digital platform with a network of virtual laboratories. We believe that the «digital twin» of our laboratory could also join "Sodruzhestvo" network.

Another important system effect we see is the development of expert activities at the national and regional levels, together with the strategic partners of RINH and in our common interests.

Thus, the Interdisciplinary Laboratory of Financial Intelligence and Computer Forensics is another innovative platform for solving scientific and educational tasks, as well as for the Rostov State University of Economics interaction with its key partners in the region and entire Russia.

NEWS BLOCK

THE PRESIDENT OF THE RUSSIAN FEDERATION VLADIMIR PUTIN AND THE DIRECTOR OF ROSFINMONITORING DISCUSSED HOW THE ANTI-MONEY LAUNDERING SYSTEM IS DEVELOPING IN NEW CONDITIONS

On June 27, 2022, the President of the Russian Federation Vladimir Putin met the Director of the Federal Financial Monitoring Service in the Kremlin. The meeting was dedicated to the fight against money laundering and terrorism financing

As part of the dialogue, the Director of Rosfinmonitoring told about the process of the development building an anti-money laundering system in new conditions. The most important areas of the work at the moment are:

- protection of the Russian Federation interests on the international fora, including at the FATF (International organization for combating money laundering, terrorism financing);
- improvement of the legal base;
- development of the cooperation with the financial institutions;
- control on the targeted use of the public funds;
- prevention of the crimes in the economic sphere.

THE DIRECTOR OF ROSFINMONITORING YU. CHIKHANCHIN DELIVERED A SPEECH AT THE MEETING OF THE FEDERATION COUNCIL OF THE FEDERAL ASSEMBLY WITHIN THE FRAMEWORK OF THE "GOVERNMENT HOUR"

At the meeting of the Federation Council of the Federal Assembly as part of the "Government Hour" the Director of Rosfinmonitoring Yu. Chikhanchin noted that it is necessary to intensify the international cooperation. To date, some unfriendly countries are attempting to exclude the Russian Federation from the Financial Action Task Force (FATF), as well as to include us in the sanctions lists. This may lead to the financial settlements' block not only with the unfriendly countries, but also with the entire international community: "There are ongoing attempts in the Egmont Group to restrict us in the exchange of the information with other financial intelligence units, which will make it difficult to conduct investigations, primarily related to the assets' search and recovery. Ultimately, only criminals will benefit from it."

Yu. Chikhanchin also informed that in concert with the national agencies we are able to uphold on international profile fora the goals set by the national anti-money laundering system related to the fight against terrorism, organized crime and the criminal use of the new technologies. "Thus, within the Egmont Group, we continue active professional cooperation with about 70 countries, including with the several unfriendly ones, participate in more than 100 international financial investigations, more than 50 of which were launched after February this year."

The separate part of the speech was devoted to national projects' monitoring, particularly the socially oriented ones like "Healthcare", "Demography", "Housing and Urban Environment", etc.

The Head of Rosfinmonitoring stated: "The Service notes the overcoming of the negative exposure of the uncertainty in the state defense procurement and the increase by 16% in the quantity of contracts concluded in 2022 in comparison with 2021, their amounts increase by more than 40%".

Currently, the targeted measures are being taken to enhance the anti-corruption work during the effected control, expert and analytical arrangements based on the emerging economic conditions.

Yu. Chikhanchin noted the reorientation of the Russian financial flows to the Southeast, Central Asia, Middle East and some other regions. This entails collaboration with new financial organizations and clients. "We are increasing cooperation with the colleagues, primarily from the Eurasian Group to maintain the level of control."

To ensure the financial security, except the operational and long-term response arrangements, the preventive measures are required to reduce the possibility of the organizations, financial institutions and citizens' involvement in the illegal transactions.

Rosfinmonitoring expects to increase the financial security literacy to minimize the fraudulent activity in the financial market.

From the previous year, based on the assignment of the President of the Russian Federation V. Putin, the annual International Financial Security Olympiad takes place. The goal is to increase the informational, financial and legal literacy of the younger generation and to search for the talented youth. Yu. Chikhanchin informed that two Olympiad stages were already completed, namely the lesson on the financial security for 2.2 million pupils and the qualifying round to the tournament final stage that determined 500 talented school graduates and students from more than 39 thousand applicants.

The Head of the financial intelligence unit expressed his gratitude to the senators for their support and attention to the initiatives of the Russian anti-money laundering system.

Yu. Chikhanchin answered the questions of the senators who were interested in such topics as the cooperation with the BRICS countries, the risks of the cryptocurrencies misuse, the promotion of the financial literacy of the population, combating corruption in the public procurement, etc.

INTERNATIONAL FINANCIAL SECURITY OLYMPIAD: THE RESULTS OF THE PAST STAGES

The most important element of the AML/CFT system is a sound and balanced workforce policy. Its main objectives are not only to provide government agencies, private and public sector structures with trained personnel in this field who are capable of implementing professional abilities in the context of current challenges and threats, but also to create conditions for the most effective use of their intellectual potential. The successful development of the financial security training system should start from high school. This comprehensive approach to personnel training allows us to form an integral model of a worldview at the earliest educational stages based on financial literacy and security. .

The year 2021 was marked by the first International Financial Security Olympiad, which became an important tool in achieving this goal. More than 31 thousand pupils and students from Russia, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan participated in the Olympiad. 122 students and pupils from Russia and EAG countries became the winners and prize winners.

In 2022, the geography of the Olympiad participants expanded significantly: students from Armenia, Brazil, India, China and South Africa joined the Olympic movement.

STAGES OF THE OLYMPIAD, PARTICIPANTS AND NOMINATIONS

The International Financial Security Olympiad is held by the Ministry of Science and Higher Education of the Russian Federation, the Ministry of Education of the Russian Federation, Rosfinmonitoring, as well as by higher education institutions – members of the International Network AML/CFT Institute (hereinafter – INI).

The Olympiad is aimed at improving the general informational, financial and legal literacy of young people, creating conditions for an individual professional growth trajectory, involving them in the AML/CFT work, increasing their interest and creative activity in the field of financial security, as well as at stimulating educational, cognitive and research activities, popularizing scientific knowledge in the financial security.

The competition is held in two stages: the 1st qualifying (at university level) stage and the 2nd final stage. In case of successful qualification, the participant reaches the final stage. Participation in the final stage is possible only in the nomination selected in the 1st stage.

The Olympiad tasks for pupils were formed on the basis of educational programs in mathematics, computer science, social studies and economics. Nominations for students were prepared on the basis of higher education programs in the following areas: law, economics, international relations, information security.

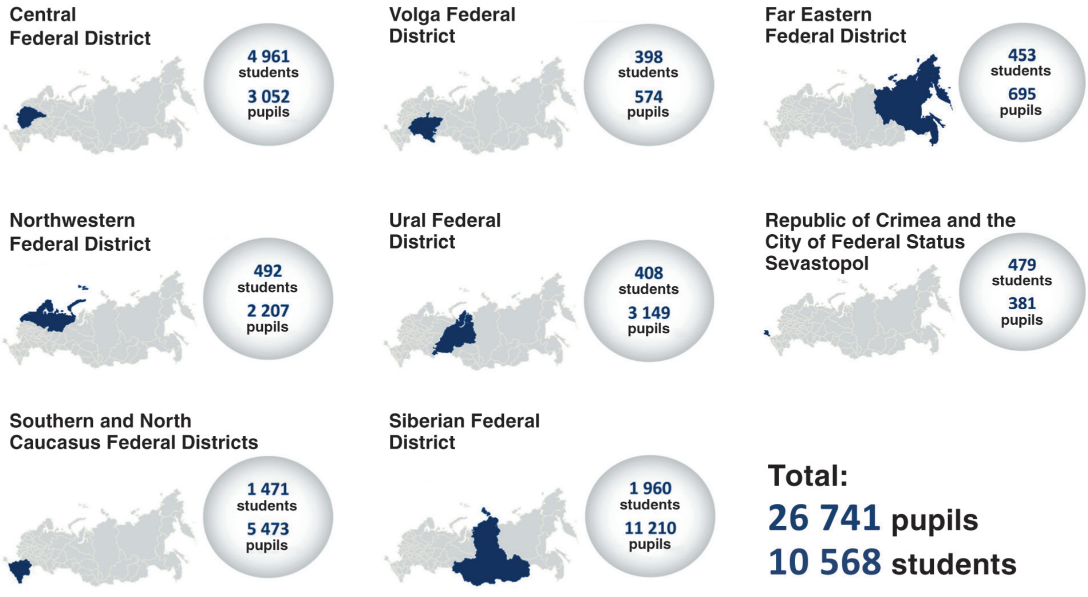
THE QUALIFYING STAGE OF THE 2022 INTERNATIONAL FINANCIAL SECURITY OLYMPIAD

Preparations for the 2nd International Financial Security Olympiad began in the first half of 2022. At the meeting of the Organizing Committee within the framework of the INI's conference on March 15-16, 2022, the main directions of preparation of the "Financial Security" thematic lesson, as well as timelines, procedures of carrying out Olympiad stages and the countries - participants were determined.

The 1st stage of the Olympiad was planned in an online format. The International Network AML/CFT Institute's member universities approved by the Olympiad Organizing Committee as venues for conducting qualifying stage became active co-organizers of the Olympiad. The INI's universities in concert with the Rosfinmonitoring Interregional Departments informed the potential participants about the stages of the Olympiad, timelines and nominations in which they could register. The participants' registration for the qualifying stage in accordance with the specialized training areas was available on the official websites of these universities.

This year, the Russian pupils of 8-10th grades, as well as bachelor's degree students (1-3 course), specialty degree students (1-4 course) and master's degree students (1 course) studying in the higher education institutions of Russia, BRICS and CIS countries were able to improve their level of knowledge and competencies and gain the important experience of participation in the international event.

The Russian and foreign students chose any of the presented universities for registration and completion of the first stage. The pupils had to register in accordance with the universities' distribution by the federal districts and subjects of the Russian Federation. The relevant information about the universities was available on the official websites of the International Financial Security Olympiad and the Federal Financial Monitoring Service. All the participants, both students and pupils, could choose only one of the suggested universities to pass the qualifying round.



Picture 1. Distribution of Russian students and pupils by federal districts

In total, more than 26 thousand pupils and 10 thousand students from the Russian Federation registered for the preliminary events. The largest number of registered students was with the INI member universities in the Central Federal District (4961 participants), the Siberian Federal District (1960 participants) and the Southern and North Caucasus Federal Districts (1471 participants).

This year more than 2 thousand foreign students from Armenia, Belarus, Brazil, India, Kazakhstan, China, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan and South Africa took part in the qualifying stage. They were able to register for the preliminary events by choosing one of the Russian universities - members of the International Network AML/CFT Institute. Such a large number of participants confirmed the continuing interest of young people in financial security issue, as it becomes more relevant in the current economic situation. Invitation of students from the CIS (Picture 2) and BRICS (Picture 3) countries is of great importance for strengthening integration with friendly countries.

Picture 2. EAG and CIS countries that took part in the qualifying stage of the Olympiad

Picture 3. BRICS countries that took part in the qualifying stage of the Olympiad

The jury from the involved universities assessed the Olympiad projects of the participants.

THEMATIC LESSON ON FINANCIAL SECURITY

For the second straight year the Russian educational institutions held the "Financial Security" thematic lesson for 8-10th grade pupils within the framework of the Olympiad. The methodological recommendations for the Lesson were developed by the Peoples' Friendship University of Russia (RUDN) to form students' basic knowledge about various types of financial fraud and the main rules of financial literacy.

This year, a thematic lesson on financial security was held for more than 2,2 million Russian pupils. The schools from the Kyrgyz Republic, the Republic of Kazakhstan, the Republic of Armenia and the Republic of Uzbekistan also joined this lesson. The training materials were sent in the format of a video lesson (Picture 4) for the pupils from the Republic of Belarus.

Picture 4. Participants of the "Financial Security" thematic lesson, 2022

PREPARATION FOR THE OLYMPIAD FINAL STAGE

On July 1, 2022, a meeting of the Organizing Committee of the International Financial Security Olympiad took place. The Committee discussed the final stage of the event scheduled for October 10 to 14 at the “Sirius” Educational Center.

Participants who have reached the 2nd stage of the Olympiad will be offered tasks formed based on the requirements of the relevant educational and professional standards. Such integrated approach will allow the best assessment of knowledge, skills and abilities of the participants, taking into account the recommendations of the Russian Council of School Olympiads.

In October 2022 at the “Sirius” Educational Center the finalists will receive not only Olympiad tasks, but also will have a rich program, including seminars, master classes, workshops, meetings and communication with international experts in the field of financial security and employers, a cyber tournament on conducting financial investigation, panel discussions and round tables, sports and entertainment events. The winners and prize winners of the Olympiad will be determined by the Olympiad jury appointed by the Organizing Committee, based on the results of the Olympiad tasks and the participants’ scores.

THE INTERNATIONAL EURASIAN GROUP FORUM ON AML/CFT[1] IN THE CAPITAL OF THE REPUBLIC OF KAZAKHSTAN

In the period from July 19 to 20, 2022, the 2nd Eurasian Group Forum on AML/CFT for the representatives of the law enforcement agencies and financial intelligence units of the EAG member states was held in Nur-Sultan[2] (Republic of Kazakhstan)

The Forum was organized by the EAG Secretariat, the Financial Monitoring Agency of the Republic of Kazakhstan, the International Training and Methodology Center for Financial Monitoring (ITMCFM, Russia).

The Forum agenda was devoted to effective identification, investigation and judicial consideration of the criminal cases on laundering (legalization) of criminal proceeds (ML).

EAG Chairman - Director of Rosfinmonitoring Yuri Chikhanchin, Chairman of the Financial Monitoring Agency of the Republic of Kazakhstan Zhanat Elimanov and EAG Executive Secretary Sergey Teterukov addressed the Forum participants with welcoming speeches.

More than 100 AML/CFT professionals took part in the Forum, 25 speakers delivered reports and presentations, including representatives of the FATF Secretariat John Carlson and Dmitry Putyatin, international expert Igoris Krzechkovskis, Brigadier General of the Italian Financial Guard Maurizio Muscara, representative of the Swedish Prosecution Authority Jan Tibbling, representatives of FIUs, law enforcement agencies and judicial authorities of the EAG member states and observers.

EAG
THE EURASIAN GROUP ON COMBATING MONEY LAUNDERING AND FINANCING OF TERRORISM
QAZAQSTAN RESPUBLIKASYNYŃ QARJYLYQ MONITORING AGENTTIGI
МУМЦФМ
Форум Евразийской группы по ПОД/ФТ | Eurasian Group Forum on AML/CFT
Обеспечение эффективного выявления, расследования и судебного рассмотрения уголовных дел в сфере отмывания преступных доходов
Ensuring effective detection, investigation, prosecution and conviction for money laundering offences

[1] Countering the legalization (laundering) of proceeds from crime and the financing of terrorism.

[2] Since 19.09.2022, Astana is the capital of the Republic of Kazakhstan.

Еуразиялық топтың АЖ/ТҚК жөніндегі форумы
Форум Евразийской группы по ПОД/ФТ
Eurasian Group Forum on AML/CFT
EAG

The Forum showed that the study of aspects of identification, investigation and judicial consideration of ML crimes, both practical and theoretical, is still relevant for the EAG member states.

The participants shared their experience and exchanged views on regulation of the procedure for conducting financial investigations, national and international cooperation, the specifics of identification, investigation and judicial consideration of ML crimes from various types of predicate crimes.

On July 21, 2022, the heads of delegations of the EAG member states also held a meeting in a narrow format. They discussed the results of the regional ML/TF risk assessment and possible measures to minimize the risks. The other issues were related to exchange of experience on strengthening the knowledge and qualifications of AML/CFT stakeholders based on the training and methodology centers, as well as the need to develop a unified AML/CFT feedback form for the EAG member states.

Following the results of the meeting, the heads of delegations of the EAG member states noted the holding of the Eurasian Group Forum on AML/CFT and its results as a significant contribution to further strengthening of national AML/CFT/CPF systems and increasing the professional capacity of national experts. The speakers also highlighted the usefulness and further need for targeted activities for AML/CFT/CPF stakeholders within the framework of the EAG typological projects.

The high level of organization and hosting of the Forum was also noted by its participants.

The EAG Secretariat expresses its gratitude to all the Forum members and speakers for their active participation and informative discussion, as well as to the Financial Monitoring Agency of the Republic of Kazakhstan and the ITMCFM for the valuable assistance.

The next Forum is planned in 2023.

THE INTERNATIONAL "RISK ASSESSMENT OF THE NON-PROFIT ORGANIZATIONS SECTOR" WORKSHOP IN THE CITY OF MINSK (THE REPUBLIC OF BELARUS)

The International Training and Methodology Center for Financial Monitoring (ITMCFM) training was arranged within a three-day international workshop "Risk Assessment of the Non-Profit Organizations Sector" held from August 9 to 11, 2022

The event was aimed at the FIU-CIS member states competent authorities experience and best practices exchange on countering the misuse of non-profit organizations (hereinafter referred to as "NPOs") for the purpose of terrorism financing (hereinafter referred to as "TF").

The Rosfinmonitoring Head of the Legal Department O. Tisen and the Head of the Department for Countering the Financing of Terrorism I. Kornev attended the event as well as the representatives of the financial intelligence authorities of the FIU-CIS member states and non-profit organizations.

The thematic lectures of the Rosfinmonitoring experts were devoted to the regional risks of the NPOs misuse for the TF purposes, to the reduce of the NPOs vulnerability (to being misused for TF purposes) and to the interaction between Rosfinmonitoring and the private sector (NPOs) within the sectoral risk assessment, as well as to the risks assessment of the TF in the NPO sector itself.

The speakers provided the analysis of the best regional practices in mitigation of the risks of the NPOs misuse for terrorism financing.

Within the three round tables of the international workshop, the participants directly exchanged their views with the experts and the foreign delegations representatives drawing on the experience of the colleagues to improve the effectiveness of the national anti-money laundering system.

VISIT OF THE CAMBODIAN EMBASSY REPRESENTATIVES

August 23, 2022 Ambassador Extraordinary and Plenipotentiary of the Kingdom of Cambodia to the Russian Federation Seyla Eat, as well as Minister-Counsellor Sophannara Keo visited the Federal Financial Monitoring Service to discuss important issues of cooperation

The meeting was attended by the Ambassador Extraordinary and Plenipotentiary of the Kingdom of Cambodia to the Russian Federation **Seyla Eat**, Minister-Counsellor of the Kingdom of Cambodia to the Russian Federation **Sophannara Keo**, Head of the International Relations Department **A. Petrenko**, Deputy Head of the International Relations Department **O. Zakharchenko**, employees of the Division for Coordination and Interaction in the Field of International Challenges and Threats of the International Relations Department **A. Samarin** and **A. Semkina**.

During the bilateral meeting, an exchange of views took place on the state and prospects of cooperation between Russia and Cambodia.

Rosfinmonitoring provided advisory assistance, and also noted the progress of the Kingdom of Cambodia in the implementation of the FATF action plan to exit the "gray" list. The FATF's "gray" list includes jurisdictions that have strategic shortcomings in the sphere of countering money laundering and terrorist financing.

THE INTERNATIONAL EXHIBITION "EDUCATION AND CAREER IN THE AREA OF AML/CFT[1]" HOSTED BY THE REPUBLIC OF TAJIKISTAN

On September 15-16, 2022, the international educational exhibition "Education and Career in the Area of AML/CFT" was held. The event was organized by the International Training and Methodology Center for Financial Monitoring (ITMCFM) jointly with the International Network AML/CFT Institute (INI) and the Department of Financial Monitoring under the National Bank of the Republic of Tajikistan

The aim of the exhibition held in Tajik National University was to increase the interest of the young generation in AML/CFT education, popularize the professional financial intelligence, as well as to enhance the high schools cooperation and the development of their joint research and educational projects.

The Russian, Tajikistan and other international experts delivered to the participants the lectures, master classes and video tutorials on the financial security. The "Graphus" game training simulator caused great interest to the students and pupils. Guided by the ITMCFM representatives, they were able to live "One day of a financial intelligence officer" and solve themselves an AML/CFT criminal case.

The exhibition space organized by the INI worked throughout the day: here pupils and their parents had a chance to get acquainted with the presentations and videos of the leading Russian and Tajikistan's high schools, talk with their representatives about the training programs and admission terms.

During the exhibition, the multilateral work sessions for the representatives of the ministries and agencies of the Republic of Tajikistan, INI and the ITMCFM participating universities were held in the Roundtable format.

The final event of the series for all the INI participating universities will take place within the last stage of the International Financial Security Olympiad in October 2022 at the "Sirius" federal territory.

[1] Countering the legalization (laundering) of the proceeds from crime and terrorism financing

HIGH PROFESSIONALISM AND SELF-DEDICATION. 20 YEARS OF ROSFINMONITORING INTERREGIONAL DEPARTMENTS AML/FT EXPERIENCE

Thanks to the acquired skills, competent management and its unique approach, the Federal Financial Monitoring Service is a real success in the international AML/CFT/CPF standards[1] implementation and may be followed as a high example of virtue

Rosfinmonitoring Interregional Departments financial investigators work not only on the requests of the Russian law enforcement agencies under the previously initiated criminal cases of economic nature, but on a proactive basis as well. We have numerous examples of how the financial intelligence activity let to the social tensions decrease in the regions.

The staff competence and high qualification are of great importance for money laundering and terrorist financing combat. From year to year, the Rosfinmonitoring Interregional Departments employees increase their potential and make a significant input into the financial crimes detection and investigation. The specialists' professionalism contributes to the high level of the interagency cooperation that enables to focus on the money laundering and terrorist financing prevention.

> *For two decades, you have already been safeguarding your federal districts national security, fighting the shadow economy, and preventing the financing of terrorism. Your efforts on combating the laundering of criminal proceeds is of highly estimated social irreplaceability, importance and of great significance. You are devoted to a weighty and a meaningful service being ready to complete the assigned tasks efficiently and responsibly daily. At the forefront of protecting the public finances you fearlessly fight crime and iniquity, provide the nation with the reliability and the welfare confidence. We are convinced of your further worthwhile contribution to the development of the Russian economy.*

Rosfinmonitoring Headquarter Office

[1] Counteracting the legalization (laundering) of the proceeds from crime, financing of terrorism and the WMD proliferation

Interregional Department of Rosfinmonitoring in the Northwestern Federal District

ROSFINMONITORING NORTH WEST FEDERAL DISTRICT INTERREGIONAL DEPARTMENT

The incorporation date: July 1, 2002

Sergey Katkov – Acting Head 01.07.2002 – 04.09.2002

Alexander Fedyuchek – Head 05.09.2002 – 26.06.2003

Boris Grigoryev – Head 31.10.2003 – 20.12.2015

Igor Loskutov – Head 25.05.2016 – 31.08.2020

Evgeniy Gileta – Head 01.09.2020 – 31.07.2022

German Shatskiy – Head 05.09.2022 – until now

The specifics of the Northwestern Federal District is the timber industry (Arkhangelsk, Pskov, Leningrad, Vologda regions, Karelia), biological resources (Baltic, North Sea), border proximity, etc. The financial investigations reflect the regional economic distinctive features. Due to our Interregional Department assistance, the complex criminal schemes can to be unraveled.

ROSFINMONITORING FAR EAST FEDERAL DISTRICT INTERREGIONAL DEPARTMENT

The incorporation date: August 2, 2002

Sergey Kravtsov – Head 02.08.2002 – 13.09.2013

Viktor Chevelev– Head 09.09.2014 – until now

The region has an impressive mineral resources potential guiding the development of the most important industries, namely, electro energetics, fossil fuel and mining sectors, non-ferrous metallurgy. One of the main tasks of the Far East Federal District Interregional Department of Rosfinmonitoring is to work in concert with the Far East Region law enforcement agencies to prevent the economic situation destabilization combating the legalization of the criminal proceeds, as well as to establish the favorable environment for the development of the regional economics.

Interregional Department of Rosfinmonitoring in the Far Eastern Federal District

ROSFINMONITORING SIBERIAN FEDERAL DISTRICT INTERREGIONAL DEPARTMENT

Date of establishment: August 20, 2002

Alexander Timoshenko – Head 20.08.2002 – 25.05.2017
Andrey Dolbnya – Head 26.05.2017 – 13.09.2019
Nikolay Buymov – Head 16.12.2019 – until now

The Siberian Federal District is the largest in Russia occupying the 3rd part of the country's territory and the richest in the main natural resources. The Rosfinmonitoring Siberian Federal District Interregional Department with the effective risk-based approach follows the regional financial intelligence timely modes of analysis.

Interregional Department of Rosfinmonitoring in the Siberian Federal District

Interregional Department of Rosfinmonitoring in the Ural Federal District

ROSFINMONITORING URAL FEDERAL DISTRICT INTERREGIONAL DEPARTMENT

Date of establishment: September 4, 2002

Alexey Kardapoltsev – Head 04.09.2002 – until now

The work of the financial intelligence department in the Urals is of a distinctive importance and responsibility. The base of the Russian metallurgy, heavy and the defense industries is concentrated here. The electric power generation, chemical, oil, gas and timber sectors, as well as the agro–industrial complex support the regional economy. To ensure the reliable control of the budget public funds flows the Rosfinmonitoring Ural Federal District Interregional Department has developed a special algorithm of actions, which is currently under implementation.

Rosfinmonitoring and ITMCFM in Telegram and VKontakte

Publisher

Autonomous Non-Profit Organization ITMCFM
Staromonetny Lane 31, bld.1,
Moscow, Russia, 119017. E-mail: info@mumcfm.ru.

Opinions and viewpoints expressed by authors do not necessarily reflect opinions and viewpoints of the “Financial Security” journal editorial board

Autonomous Non-Profit
Organization ITMCFM

2022