Development of an Intelligent Module for Monitoring and Analysis of Client's Bank Transactions

Vasily Meltsov, Pavel Novokshonov,
Dmitry Repkin, Alexander Nechaev
Vyatka State University
Kirov, Russia
meltsov@vyatsu.ru, lkzcover@yandex.ru, repkin@vyatsu.ru

Nataly Zhukova
St. Petersburg Institute for Informatics and Automation
of the Russian Academy of Sciences (SPIIRAS)
St. Petersburg, Russia
nazhukova@mail.ru

***Abstract*—In the paper were analyzed the problems in the field of information security of payment systems based on plastic cards. Authorization data used for cashless payments can be compromised and used by intruders for unauthorized access to the user's bank account and conducting fraudulent transactions. To assess the main characteristics of the module being developed, an analytical review of the most well-known banking transaction risk control systems was conducted. A new method based on cluster analysis and the vectors method is proposed for identifying possible fraudulent operations using payment cards. Has been implemented an efficient algorithm for converting information from a user's payment profile to a string of numbers in an n-number system. To perform this conversion, special prepared in advance conversion maps are used. The results of completing the steps are illustrated by figures and tables. The correctness of the proposed methods and algorithms is confirmed by experiments conducted on real samples.**

I. Introduction

In recent years, operations based on non-cash payments have been actively developing around the world. The convenience of making cashless payments, the ability to provide additional services to bank account holders and more have led to the rapid development of this market.

Authorization data used for cashless payments can be compromised and used by hackers for unauthorized access to the user's bank account and for conducting fraudulent transactions [1]. Experts of the Central Bank of Russia in the field of information security suggest an increase in global losses from cyber threats to $ 2 trillion by 2019. Such type of fraudulence leads to the risks associated with financial losses and deterioration of reputation of the issuing bank. In this regard, the issuing bank in its payment system should widely apply various information security systems, introduce methods and means of detecting fraud and counteracting it [2,3,4]. Since cashless payment systems are usually tied to a virtual or physical bank card, they must contain a risk management subsystem (module) when performing transactions using payment cards. This subsystem is necessary to assess credit risk, as well as to prevent risks when using codes and passwords as analogs to a handwritten signature [5]. Unfortunately, Russian standards and regulation documents of the Central Bank put forward only general requirements for risk management, which is a serious problem to applying such subsystems on practice. Often, third-party solutions cannot be effectively integrated into an already built ecosystem and banking network architecture [6], [7]. In this regard, each payment system has a need for self-development of an effective risk control subsystem.

As mentioned above, one of the means of protection against fraudulence associated with non-cash payments is the banking transaction monitoring system or the banking transaction risk control system (RCS). The following basic requirements and tasks are imposed on the RCS [8].

1) Transaction monitoring should provide analysis of all authorization transactions in the payment system and make decisions on suspicious for fraud transactions to reduce risks.

2) The transaction monitoring system is a tool for reducing the risks associated with conducting fraudulent transactions with bank cards, and should be a part of an integrated approach to ensuring the security of the payment system.

International payment systems, such as Visa or MasterCard, also recommend further marking and analyzing the following events that occurred on the issuer's side of the means of payment:

- attacks on generated card numbers (fraud);
- negative results of card verification codes check;
- transactions on expired cards;
- transactions by wrong card numbers;
- transactions at possible points of compromise;
- credit operations and cancellation of authorization by the store;

Requirements for acquiring monitoring are quite similar, but in them the objects of monitoring are terminals and merchant's accounts. It is recommended to take into account the average transaction amount and the number of transactions on the terminal or account for the selected period.

Visa and MasterCard requirements relate primarily to monitoring in deferred (offline) mode. Other temporary monitoring options for these payment systems are currently not mandatory. Unfortunately, these measures in modern conditions of development of information and computer technologies are clearly insufficient.

It should be noted that the difficulty of making a decision on a suspicious transaction is that if a fraudulent transaction is missed, the bank may incur significant financial losses. And in case of installation of erroneous restrictions on operations by cashless payment during a legal transaction, damage to the bank's reputation, dissatisfaction on the part of the client, etc. may occur.

Given the current situation, one of the well-known Russian banks announced a competition to develop their own effective, high-speed RCS, taking into account the current state of scientific advances in information technology and cybersecurity.

The main requirements for RCS were the following:

- availability of business analysis tools in real time;
- analysis of the behavior of cardholders to identify transactions that are not typical for the client;
- processing of false positives in automatic mode;
- supporting the investigation process to conduct all the procedures performed until the completion of the investigation and making the final decision on the incident;
- monitoring and analysis of all transactions on the account;
- automation of loading and parsing data for analysis from external systems or other bank systems;
- possibly, a set of several analytical models (the choice of a particular model is carried out depending on the characteristics of the current transaction).

The strict requirement for a speed of the system (both in automatic mode and with human participation), ease of setup and maintenance of performance by ordinary operators (and not highly qualified specialists in IT) seriously limits the use of such a powerful mathematical apparatus as artificial neural networks [9,10].

II. Risk control system analysis

For comparison and a reasonable choice of the most essential characteristics of the developed RCS, we consider the classification of such systems.

1) By the response rate the RCS are divided into the following classes:

- real time systems. Such systems operate in real time, and have the ability to directly affect the result of authorization of a transaction;
- pseudoreal time systems. Transaction analysis is performed in real time, but the system cannot affect the result of authorization. The decision can be made only after the completion of a suspicious transaction;
- delayed mode systems. Periodically, for example, at the end of the operational day special reports are generated, based on the analysis of which decisions are made;

2) By the type of decision making:

- automatic. The decision on the transaction is made automatically by the system without human intervention;
- automated. The system provides the authorized employee with information for deciding on a suspicious transaction;

3) According to the information used in the analysis:

- systems that use only the data of the transaction itself. The analysis takes into account only the parameters - the amount, the name of the trading and service enterprise (TSE), the category of the TSE, country, etc.;
- systems that involve the history of card operations for analysis;
- systems using cardholder behavior patterns. The system builds models of cardholder behavior and performs an analysis according to the existing model, based on the deviation of behavior from the model, the transaction is considered suspicious;

4) According to the used mathematical apparatus for analysis:

- systems based on simple logic checks. Logic checks include operations such as: >, <, =, ?;
- systems using known methods of mathematical statistics, for example, methods of descriptive statistics, correlation analysis, regression analysis;
- systems using methods of intellectual analysis - data mining (except neural networks). When analyzing transactions, methods of classification, forecasting, cluster analysis, search for associations, etc. can be used;
- systems based on neural networks. Analysis of operations is carried out on the basis of adaptive schemes built on neural networks, which also makes it possible to identify previously unknown schemes of fraud. These systems are expensive and require substantial resources to configure and train the neural network;

5) By the type of analyzed data:

- emission. Such systems have access to detailed information on the bank card account holder and can use it to assess the risks of a specific transaction;
- acquiring. Such systems can control only the model of user behavior within a particular trade and service enterprise and do not have access to personal data of the bank card holder;

6) By way of interaction with the processing center:

- integrated into the processing center. Systems of this type are an integral part of the payment system architecture and can access complete customer information;
- systems provided as a service. Usually presented as a separate, third-party service that monitors and controls banking operations.

The classification of the RCS in the form of a scheme is presented in the Fig. 1.

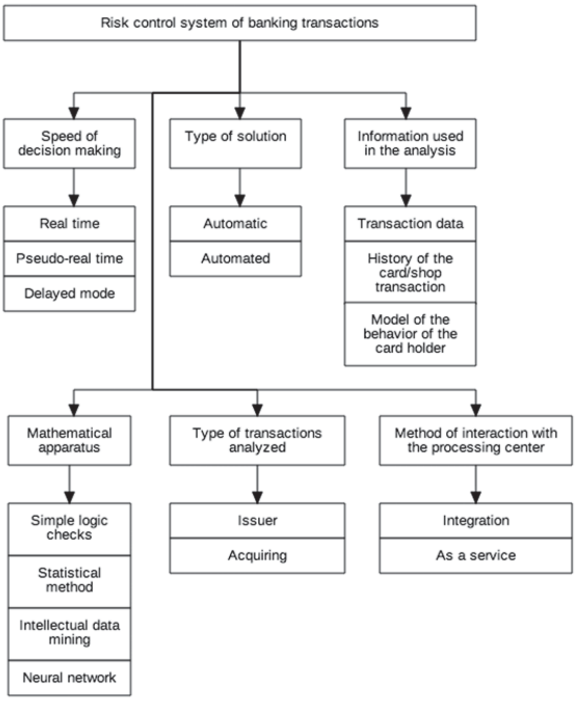


Fig. 1. Classification of banking transaction risk control systems

At the initial design stage, an analytical review of the most well-known RCSs was carried out to assess the main characteristics of the system being developed.

Visa and MasterCard [11, 12]. Visa and MasterCard, in addition to the transaction monitoring parameters mentioned above, also offer anti-fraud solutions. Visa provides CyberSource Fraud Management services for detecting and preventing e-commerce fraud, MasterCard - Expert Monitoring Solutions, providing transaction evaluation both in real time and after authorization, including using artificial intelligence methods.

Card Suite Fraud Management [13]. Developed by Tieto, the Card Suite Fraud Management system is distributed with the Tieto Card Suite platform. The decision under consideration is based on the principle of creating specialized rules and subsequent verification of card operations for compliance with these rules. The system not only fully complies with all the security requirements of Visa and MasterCard, but also allows you to stay ahead of fraudsters, preventing fraud attempts at the earliest stage - at the time of initial authorization, even before the participation of risk analyst.

SAS Fraud Framework [14]. The system was developed by SAS Institute Inc in 2009 and it is an integrated conter-fraud system. The SAS Fraud Framework provides a hybrid approach to identifying fraud - it ensures maximum accuracy in determining potential fraudsters and reducing the False Positive indicator to the lowest possible values. This reduces unproductive load on the security unit.

The system contains of four main ways to detect potentially dangerous transactions: special rules for detecting fraudulent transactions; analysis of deviations from the usual pattern of client behavior; predictive client behavior patterns; social network analysis. The social network creation and analysis tool (SAS Social Network Analysis) allows to build client interaction networks and analyze them. Such interconnection structures help to identify organized fraud groups.

Falcon Fraud Manager 6 [15]. The system was developed by FICO. A feature of this system is the usage of models based on artificial neural networks. The system allows both issuer and acquirer monitoring. Decision making is possible either with the participation of the operator, or in automatic mode. The system is used by 17 of the 20 largest card issuers in the world.

Proactive Risk Manager [16]. The system was developed by ACI Worldwide. The basis also formed by algorithms and models based on artificial neural networks. Decision making is possible in both real and pseudo-real time. A special feature is the implementation of the analytics module based on the transaction history. Along with the system from FICO, analysts have repeatedly recognized it as the best-in-class.

ReD PRISM [17] systems from Retail Decisions, Fractals (Alaric) [18], SmartGuard (BPC Technologies) [19] and some others were also reviewed.

It should be noted that all such RCSs are closed products of companies, which significantly complicates the analysis of the used methods and functioning algorithms [20].

On the basis of the information found in the open press and on the Internet, the main characteristics of the RCS were highlighted:

- as the initial data, system should receive a transaction for analysis, and as the output it is necessary to provide an estimated degree of risk of the transaction being analyzed;
- the system should be easily integrated into the existing payment system architecture;
- the system should be lightweight and not require a dedicated server;
- all data necessary for analysis should not be transferred to the external environment;
- the system should have an open source code for possible modification to the requirements of the payment system available in the bank;
- the developed system should work around the clock and have fault tolerance of at least 99,9%.

In addition, one of the main factors for choosing a risk management system for banking transactions is the speed of the system and its cost. Based on the requirements presented, it can be concluded that none of the available systems fully meets the basic requirements of the customer.

III. Transaction Monitoring Module design

Since the development of a complete, efficient, fast-acting, but at the same time, with powerful functionality, the RCS of banking transactions is extremely labor-consuming and time-consuming, it was decided to firstly develop the main module of this system - the monitoring and evaluation module of client banking transactions. When developing this module, in accordance with the terms of reference, it is necessary to implement the following steps.

1) Develop a user payment profile format.

2) Develop algorithms for encoding and decoding a payment profile.

3) Develop and implement a risk analysis module of a transaction entering the system, taking into account the features of the selected programming environment.

Was defined the following generalized structure of the module for monitoring and evaluating banking transactions. (Fig. 2).

The issuing server sends transaction data to the developed module for analysis. According to a certain algorithm, the next block selects from all the information received only those data that are necessary for risk assessment. Then, using the identification number of the owner of electronic money (or the identifier of the bank account holder), the module receives a coded user profile from the database. After decrypting the received profile, the data is analyzed for the degree of risk of the operation. The resulting estimate is sent to the issue server to continue processing the operation in accordance with the decision of the developed RCS. After analyzing the transaction, the module supplements the user profile with the necessary data to improve the quality of analysis of client actions in subsequent operations.

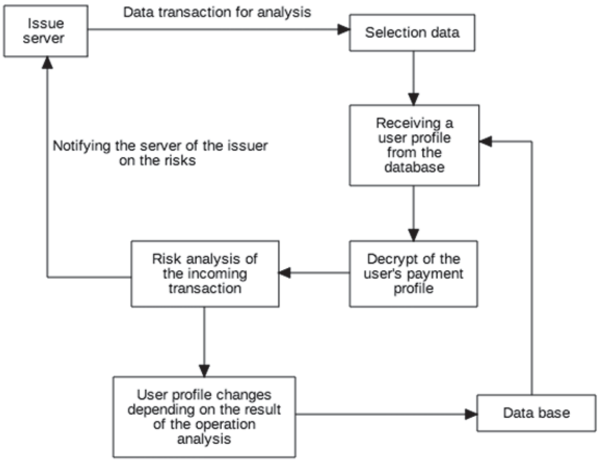

Issue server
Data transaction for analysis
Selection data
Receiving a user profile from the database
Notifying the server of the issuer on the risks
Risk analysis of the incoming transaction
Decrypt of the user's payment profile
User profile changes depending on the result of the operation analysis
Data base

Fig. 2. General structure of the monitoring module

The proposed module makes a decision about the degree of risk of an incoming transaction based mainly on data that is obtained from the user profile. Thus, as more detailed and more accurate this profile can describe the behavior of the account holder, the more effective and accurate will be decisions that the system will make [21]. Therefore, special attention was paid to determining the format and structure of user input data and the transactions performed by it. Let us point out a few basic parameters that are used by the developed module for decision making:

- ID of account holder;
- flag indicating the type of operation (onus/offus);
- flag that takes into account the user's account currency and the check currency;
- transaction amount in minimum monetary unit of user account currency;
- time of transaction completion;
- the time it took for the client to confirm the operation;
- coordinates of the terminal that initiated the transaction.

The operation type flag and the account currency flag are used to refine the decision being made. The remaining data is used to build a user profile. The complete data structure describing the user's payment profile is presented in the Table I.

Field *TimeOperation* reflects the distribution of user operations by time of day. The implementation of the user's payment profile involves dividing the day into eight segments, three hours each.

In the design specification was stated that the user's payment profile should be stored as a fairly short string. It is also determined that the payment profile is confidential information, the leakage of which could potentially lead to reputational and financial risks. To meet these requirements, the proposed module implements a special method of creating a unique user profile in the form of an encoded string. The profile is created and dynamically updated based on the customer's payment transactions.

TABLE I. USER'S PAYMENT PROFILE STRUCTURE

Field name	Data type	Field description
Amount	Integer, unsigned, 64 bit	Contains accumulator of the amount of user operations for n months
NumOfOperation	Integer, unsigned, 64 bit	Number of operations in n months
TimeOperation	Array of 8 integer, unsigned values, 64 bit	Distribution of operations by time of day.
SpeedConfirmation	Integer, unsigned, 8 bit	The time for which the user confirms the payment transaction
Coordinates	Array of 8 integer, unsigned values, 32 bit	The coordinates of the last successful payment

We should also consider the algorithm for converting information from any field of the user's payment profile into a string of numbers in the n-number number system. To perform this transformation, previously prepared transformation maps are used. The essence of the algorithm is reduced to converting a decimal number from a profile field (profile operation) to an n-ary number, where n corresponds to the number of key-value pairs in transformation maps. An example of a transformation map for a 62-level system is presented in Fig. 3.

In the process, the module also performs the inverse transformation. For this purpose exists a map of the inverse transformation from the n-ary system to the decimal.

```
var coderConverter = map[uint8]string{

10: "A", 11: "B", 12: "C", 13: "D", 14: "E", 15: "F", 16: "G",
17: "H", 18: "I", 19: "J", 20: "K", 21: "L", 22: "M", 23: "N",
24: "O", 25: "P",   26: "Q", 27: "R", 28: "S", 29: "T", 30: "U",
31: "V", 32: "W", 33: "X",   34: "Y", 35: "Z", 36: "a", 37: "b",
38: "c", 39: "d", 40: "e", 41: "f",   42: "g", 43: "h", 44: "i",
45: "j", 46: "k", 47: "l", 48: "m", 49: "n",   50: "o", 51: "p",
52: "q", 53: "r", 54: "s", 55: "t", 56: "u", 57: "v", 58: "w",
59: "x", 60: "y", 61: "z",
}
```

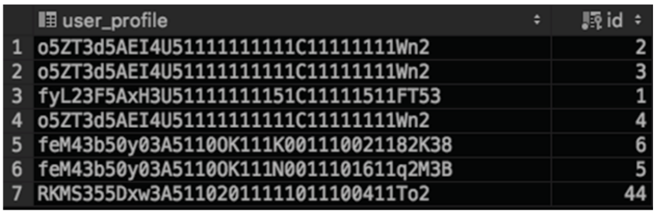
Fig. 3. A number transformation map for a 62-level system

Fig. 4 shows an example of the data included in the payment profile of a bank card holder and the corresponding encoded string.

```
The data structure of the user payment profile:

{Amount:23215 NumOfOperations: 26
TimeOperations:[1 1 2 12 1 7 1 1]
SpeedConfirmation:30 Coordinates:{X:58628725 Y:49590121}}

Encoded as a string, the user payment profile, built on the basis
of the specified data:

35Ms1O12101011151C1h181A54EIAd53ZT5o
```

Fig. 4. Example of encoded string

The user's payment profile encoded in this way is entered into the user_profile field of the table containing the list of users of the payment system and the list of their accounts and cards. (Fig. 5).



	user_profile	id
1	o5ZT3d5AEI4U51111111111C11111111Wn2	2
2	o5ZT3d5AEI4U51111111111C11111111Wn2	3
3	fyL23F5AxH3U51111111151C11111511FT53	1
4	o5ZT3d5AEI4U51111111111C11111111Wn2	4
5	feM43b50y03A51100K111K001110021182K38	6
6	feM43b50y03A51100K111N0011101611q2M3B	5
7	RKMS355Dxw3A51102011111011100411To2	44

Fig. 5. Example of the user's payment profile stored in the database

To determine the specific value of the risk of a transaction which entered the system, a vector model for assessing the similarity of data is used. The analyzed data, in this case, is considered as an unordered set of terms. Terms are the words that make up the analyzed text, as well as any other elements of the text.

There are several known methods for determining the weight of a term in a document, i.e. "Importance" of a word to identify a given text. We will use one of the simplest options - counting the number of terms used in a document, or the so-called term frequency. The more often a word appears in a document, the more weight it will have. If a term is not found in a document, then its weight in this document equals zero.

All terms that are found in documents of the processed collection must be ordered. If now for some document to write out the weights of all terms in order (including those that are not present in this document), we get a vector, which will be the representation of this document in vector space. The dimension of this vector, like the dimension of space, is equal to the number of different terms in the entire collection. It is important that the dimension of the vector is the same for all documents.

Mathematically, this can be written as follows

$$d_j = (w_{1j}, w_{2j}, \dots, w_{nj}), \qquad (1)$$

where d_j – vector representation of the j-th document, w_{ij} – the weight of the i-th term in the j-th document, n –total number of different terms in all collection of documents.

Having such representation for all documents, it is possible to find the distance between points of space and thereby solve the problem of similarity of documents. The closer the points are, the more similar the presented documents are. In the case of a document search on request, the request is also represented as a vector of this space. This allows to calculate the compliance of documents to formed query.

Thus, the essence of the proposed transaction risk assessment method can be reduced to converting the transaction input data and data from the user payment profile into the multidimensional vector space. After that, the distance between the analyzed vectors is calculated. That is, the developed module estimates how the incoming transaction corresponds to the "traditional" behavior of the bank card holder.

The distance, or degree of similarity between multidimensional vectors, is estimated by the formula for finding the cosine distance between vectors.

$$\cos(\theta) = \frac{\sum_{i=1}^{n} A_i \times B_i}{\|A\| \times \|B\|} \qquad (2)$$

where A and B – vector of equal dimension.

Scalar product of compared vectors is divided by the product of their Euclidean norms.

$$\|x_2\| = \sqrt{\sum_{i=1}^{n} x_i^2} \qquad (3)$$

To assess the risk of a transaction, the developed module builds two vectors according to the following rules. The first vector is the reference vector of the operation, which can be considered non-fraudulent. The second vector is the vector of the transaction to be verified.

The system uses six special rules to evaluate the transaction performed on this card.

1) Onus/offus operation. This rule evaluates the direction of the client's cash flow. If money is sent to a bank that differs

than the bank in which the customer's account is registered, the risk of this operation is considered higher;

2) Operation currency check. The risk of a transaction is considered higher if the currency of the client's account differs from the currency of the check or the destination account currency;

3) The amount of the operation. The operation is considered more risky if the amount of the operation is higher than the average amount of the client's check;

4) Operation time. In a percentage value, the probability of the customer performing the transaction at this time is calculated. These calculations are based on the distribution of user operations by the time of day. The lower the likelihood of a transaction at the current time, the higher the risk of a transaction;

5) The transaction confirmation time. The more the transaction confirmation time differs from the average, the higher the risk of a transaction;

6) Evaluation of the coordinates of the current operation. If the coordinates of the operation differ by more than a predetermined delta from the coordinates of the last successful operation, then this transaction is considered more suspicious. The operation is all the more suspicious the larger the delta between the coordinates of these operations.

It should be noted that the modular architecture of the RCS itself and the developed module makes it easy to expand and add rules for assessing the risks of a transaction.

After completing the construction of a vector according to the specified rules, the vector is modified by "multiplying" by the predetermined weights of its parameters. An example of a vector constructed to assess the risk of a transaction after these transformations is presented below.:

{Vector:[1 0.2434534 1.3 0.1956521739130435 0.00456 0.5 1]}

IV. Experiment results

The designed module for evaluating the user's banking transactions was implemented in the Golang programming language. Golang (or Go) is a multi-threaded programming language developed by Google [22]. Currently, the language works and runs on operating systems FreeBSD, OpenBSD, MacOS, Windows, BSD, Android, Solaris, and some others. Golang has a very concise and simple syntax, automatically manages memory, collects garbage and has a testing mechanism built into the standard library. The standard library is well documented and worked out, which allows access to a third-party library only in exceptional cases. Programs written on it are very easy to test and deploy on a production server.

Since the presented research is carried out in cooperation with one of the payment systems, the development team has a direct opportunity to test the prototype of the module and implement it into the existing system of bank transactions risk control. The presented risk control module of bank transactions went through a preliminary testing stage on the real integration circuit of one of the payment systems. Verification showed the correct functioning of the module and the performance of all the proposed methods and algorithms.

The analyzed subsystem of one of the banks refers to real-time systems with automatic (in special cases-with automated) type of decision-making, based on a specialized model of cardholder behavior. As analogues of the proposed module, two implementations of risk assessment subsystems of bank transactions available in the company were considered: the currently used software module based on fuzzy logic (simple rules of logical verification) and the module based on an artificial neural network (ANNB-module) [23]. The average transaction values of a regular customer of the VISA payment system were reviewed to assess the efficiency of the elaborated module. The initial profile of the customer:

- the average amount of operations – 500 rubles;
- the client performs all its operations in the afternoon (from 12:00 to 21:00);
- all operations were carried out within the Kirov region.

It must be noted that the payment profile in the real system will be formed and dynamically updated during the customer uses the payment system.

To determine the set of well-defined conditions (in the first module) and to form a neural network training sample the following operations were selected:

- operations with a small excess of the check average amount (up to 30%): the amount of the transaction is 600 rubles, the time of the transaction is 12:00, the place of the transaction is Kirov;
- operations with three times excess of the check average amount: the amount of the transaction is 1500 rubles, the time of the transaction is 12:00, the place of the transaction is Kirov;
- operations with a significant excess of the check average amount: the amount of the transaction is 8000 rubles, the time of the transaction is 12:00, the place of the transaction is Kirov;
- operations with a considerable excess of the check average amount: the amount of the transaction is 25000 rubles, the time of the transaction is 12:00, the place of the transaction is Kirov. According to the experimental conditions, this operation was considered as a fraudulent;
- the amount of the transaction is 3000 rubles, the time of the transaction is 00:00, the place of the transaction is Kirov;
- the amount of the transaction is 600 rubles, the time of the transaction is 14:00, the place of the transaction is Khabarovsk. According to the experimental conditions, this operation was considered as a fraudulent.

The result's comparison of various modules of banking transactions risk assessment work is presented in TABLE II.

If the operation was suspended in the proposed module, it is required the additional verification - either by the bank operator (now) or by a special module of the RCS (further development). Based on the results of the conducted estimated experiments, it can be concluded that:

1) Cheap and easy to implement and maintain systems with clear logic give a very large number of false triggering, which negatively affects the bank's reputation and user's interest.

2) The modules based on neural networks can achieve a sufficiently high quality of work, but they are expensive and the maintenance is difficult. Adding new operational risk assessment parameters also can be difficult. In addition, there should be a very large amount of analyzed data already evaluated by experts or by other banking systems for effective training and work.

TABLE II. RESULTS OF THE BANKING TRANSACTION RISK ASSESSMENT MODULES WORK

Estimated parameter	**Clear logic module**	**Elaborated module**	**ANNB-module**
A small excess of the check average amount	Operation was approved	Operation was approved	Operation was approved
Three times excess of the check average amount	Operation was rejected	Operation was suspended	Operation was approved
Significant excess of the check average amount	Operation was rejected	Operation was suspended	Operation was rejected
Considerable excess of the check average amount (fraudulent)	Operation was rejected	Operation was rejected	Operation was rejected
Atypical time for the customer's transaction	Operation was rejected	Operation was approved	Operation was approved
Atypical place for the customer's transaction (fraudulent)	Operation was rejected	Operation was rejected	Operation was rejected
The difficulty of adding a new parameter	Easy	Easy	Difficult, requires new learning
The complexity of setting up the system	Easy	Medium	Very difficult
Module support cost	Cheap	Medium	Expensive

The elaborated module allows to estimate the degree of banking transactions risk with the same accuracy as the modules used the mathematical apparatus of neural networks. At the same time, it is simpler and cheaper to maintain, it has significant advantages if it is necessary to add new transaction estimate parameters and to prepare the system before it start working. The latter properties are very important for risk management systems of banking operations, taking into account the increasing growth rate of fraudulent transactions using plastic cards.

V. CONCLUSION

Despite the fact that the largest vendors in the world offer monitoring services as a service (Fraud Management, FIS Card Fraud Management, TSYS Fraud Management), currently the most popular are RCSs installed on the bank's servers.

As a result of the development carried out as part of this study, the main component of the RCS, a module for monitoring and assessing the risks of customer banking transactions, was implemented. The module is easy to implement, operate and modify.

The module is designed to implement the following functions of the RCS.

1) Based on the user's payment operations, build his payment profile. It is possible to store this profile in the database, in a short (less than 100 characters) string.

2) Providing the possibility of changing the encryption of stored data in case of suspected compromise.

3) Receiving the evaluation of risk degree at the output of the risk control system.

4) Ensuring the possibility of adaptation and modification of the RCS, in order to increase its efficiency in the process of operation.

It should be noted that at present in Russia, and in Europe as a whole, there is no generally accepted quantitative methodology for assessing the risks associated with fraudlence in non-cash transactions.

From the point of view of the chosen programming environment, at the moment, Golang is one of the most promising languages for implementing various server solutions. And the support of such a large corporation as Google gives reason to hope that this language will be used in the development of high-performance information systems in a long term.

In further studies on this project, it is planned to conduct experiments to assess the effectiveness of applying various modern approaches to the development of automated information systems for financial calculations in order to increase the intelligence of decision making. It also assumes a serious development of the functionality of both individual modules and the system as a whole. If a suspicious transaction is detected, the payment system should take the following measures to limit the negative consequences:

- denial of authorization of this suspicious transaction, if technically possible;
- blocking a card or account making it impossible to perform subsequent transactions on it;
- setting money value limits on subsequent operations of purchases in TSEs for the selected period, cash withdrawals at ATMs and cash points for the selected period, or on the total amount of transactions for the selected period;
- setting limits on subsequent operations on the region of use of the card or the category of merchants;

- informing the cardholder about a suspicious transaction, via SMS notifications or Push notifications;
- restriction of transactions in a specific terminal or service.
- activation of additional methods of verification of the transaction.

Implementation of these response measures depends on technical capabilities of the partner bank's payment system and the adopted risk management policy associated with banking fraud [24],[25],[26].

REFERENCES

[1]. Risk Management. 2016 Annual Report, *PT Bank Central Asia Tbk*. 2017.

[2]. C. Atheeq, "Secure intelligence algorithm for data transmission in integrated internet Manet", *International Journal of Computer Science and Applications,*. vol 14(2), 2017, pp. 142–163.

[3]. M. Bayyoud, and N.A. Sayyad, "The Impact of Internal Control and Risk Management on Banks in Palestine", *International Journal of Economics, Finance and Management Sciences*, vol. 3(3), 2015, pp. 156-161.

[4]. Best Practices for Managing Bank Transaction Risk, *CaseWare Analytics*. Toronto, 2015.

[5]. Y. Yun, *Temporal Data Mining via Unsupervised Ensemble Learning,* Elsevier, 2016.

[6]. J.A. Adeyiga, J.O. Ezike, and A. Omotosho, "Neural Network Based Model for Detecting Irregularities in e-Banking Transactions", *African Journal of Computing & ICT*, vol. 4(3), 2011, pp. 7-14.

[7]. A. Gupta, D. Kumar, and A. Barve, "Hidden Markov Model based Credit Card Fraud Detection System with Time Stamp and IP Address", *International Journal of Computer Applications*, vol. 166(5), 2017, pp. 33–37.

[8]. N. Carneiro, G. Figueira, and M. Costa, "A data mining based system for credit-card fraud detection in e-tail", *Decision Support Systems*, vol. 95, 2017, pp. 91–101.

[9]. S. Krishna, "Financial Applications of Neural Networks. Available, Web: https://blog.aspiresys.com/banking-and-finance/financial-applications -neural-networks.

[10]. M. Tkáč, and R. Verner, "Artificial neural networks in business", *Applied Soft Computing*, vol. 3, 2016, pp. 788-804.

[11]. SyberSource. A Visa Solution. Web: https://www.cybersource.com /products/fraud_ management.

[12]. MasterCard Academy. Web: https://www.eiseverywhere.com/ ehome/index.php?eventid=221749&.

[13]. Tieto Card Suite. Fraud & Dispute Management. Web: https://docplayer.ru/ 29275759.html.

[14]. SAS Fraud Framework. WEb: https://www.sas.com/software/fraud-framework.html.

[15]. FICO. Falcon Fraud Manager. Web: https://www.fico.com/en/latest-thinking/product-sheet/ falcon-fraud-manager

[16]. ACI. Proactive Risk Manager. Available at: https://www.aciworldwide.com/products/proactive-risk-manager (accesed at 20 December 2018).

[17]. Retail Decisions. Web: https://nabvelocity.com/developers/api-docs /retail-decisions-red-fraud-prevention.

[18]. Fractals – Digital Payment Fraud Prevention. Web: https://www. ncr.com/ financial-services/enterprise-fraud-prevention/fractals.

[19]. BPC. Risk & Fraud Management. WEb: https://www.bpcbt.com/ smartvista- solutions/risk-fraud-management.

[20]. A. Abraham, P. Dutta, J.K. Mandal, A. Bhattacharya, and S. Dutta, (Eds.), "Emerging Technologies in Data Mining and Information Security", *Proceedings of IEMIS-2018*, Springer, Singapore, 2018.

[21]. M.L. Dolzhenkova, V.Yu. Meltsov, and D.A. Strabykin, "Method of Consequences Inference From New Facts In Case Of An Incomplete Knowledge Base", *Indian Journal Of Science And Technology*, vol. 9, issue 39, October 2016, P.100413.

[22]. The Go Programming Language. Web: https://golang.org.

[23]. Zh. Zhang, X. Zhou, and X. Zhang, "A Model Based on Convolutional Neural Network for Online Transaction Fraud Detection", *Security and Communication Networks*, vol. 1, 2018, Article ID 5680264.

[24]. A. Correa, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature engineering strategies for credit card fraud detection", *Expert Systems with Applications*, vol. 51, 2016, pp. 134–142.

[25]. S. Wen, and B. Katt, "An Ontology-Based Context Model for Managing Security Knowledge in Software Development," *in 23th Conference of Open Innovations Association (FRUCT)*, November 2018, pp. 416–424.

[26]. M.F. Zeager, A. Sridhar, N. Fogal, S. Adams, D.E. Brown, and P.A. Beling, "Adversarial learning in credit card fraud detection", *in Proceedings of the 2017 Systems and Information Engineering Design Symposium, (SIEDS '17),* IEEE Press. USA, 2017, pp. 112–116.