Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 213 (2022) 110–118

Procedia Computer Science

www.elsevier.com/locate/procedia

2022 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: The 13th Annual Meeting of the BICA Society

Application of machine learning methods to identify suspicious actions of employees related to violation of the procedures of a credit institution

Jenny Domashova[a]*, Elena Kripak[b], Elena Pisarchik[c]

[a]*National Research Nuclear University "MEPhI", 31 Kashirskoe shosse, Moscow 115409, Russia*
[b]*Federal State Budgetary Educational Institution of Higher Education "Orenburg State University", 13 pr.Pobedy, Orenburg, 460018, Russia*
[c]*Blaze Analytics Ltd., vld. 4, p. 1, Troparevskaya str., Moscow, 119602, Russia*

Abstract

The article presents the results of the application of machine learning methods to identify suspicious actions of employees related to a violation of the procedures of a credit institution, specifically, the theft of funds from customer accounts and cards and abuse of the motivation system. The stages of data preprocessing within the considered task are analyzed. Among the considered classification algorithms, which are not sensitive to class imbalance, the method with the best value of hyperparameters was chosen. Next, the most informative features were highlighted, for which the best values of hyperparameters were selected and the optimal values of the probability thresholds of attributing an object to fraud were found. The proposed technology can be used separately or as part of an anti-fraud system for routine (for example, once a month) detection of illegitimate actions of employees of a credit institution related to the theft of funds from customer accounts and cards and abuse of the motivation system. A software tool in Python was developed that allows solving the task of detecting internal fraud based on the proposed technology.

Keywords: countering internal fraud, machine learning methods, clustering, classification, class imbalance, anti-fraud systems

* Corresponding author: Jenny Domashova.
E-mail address: janedom@mail.ru

10.1016/j.procs.2022.11.045

1. Introduction

Currently, credit organizations are one of the most important components of the financial system both at the state and global level. Fraud in this area can be detrimental not only to the organization, but also to its customers and the financial system in general. Therefore, combating fraud is a priority for both the regulator represented by the state and the credit organization.

The increase in the number of technologies and products provided by credit institutions creates vulnerabilities. Timely detection of potential and actual fraudulent activities allows to significantly reduce losses, as well as to maintain the reputation and license of the credit organization. The specificity of handling fraud implies constant organization' adaptation to changes and threats. Anti-fraud systems, capable of detecting well-known fraud patterns as well as completely new ones, are used to improve the effectiveness of combating such violations.

According to the «Tinkoff» study, the total number of cases related to fraud in 2020 increased by 60% compared to 2019, and the total amount stolen by fraudsters increased by 70%. Figure 1 shows the evolution of fraud cases in 2020 by the number and amount relative to 2019.

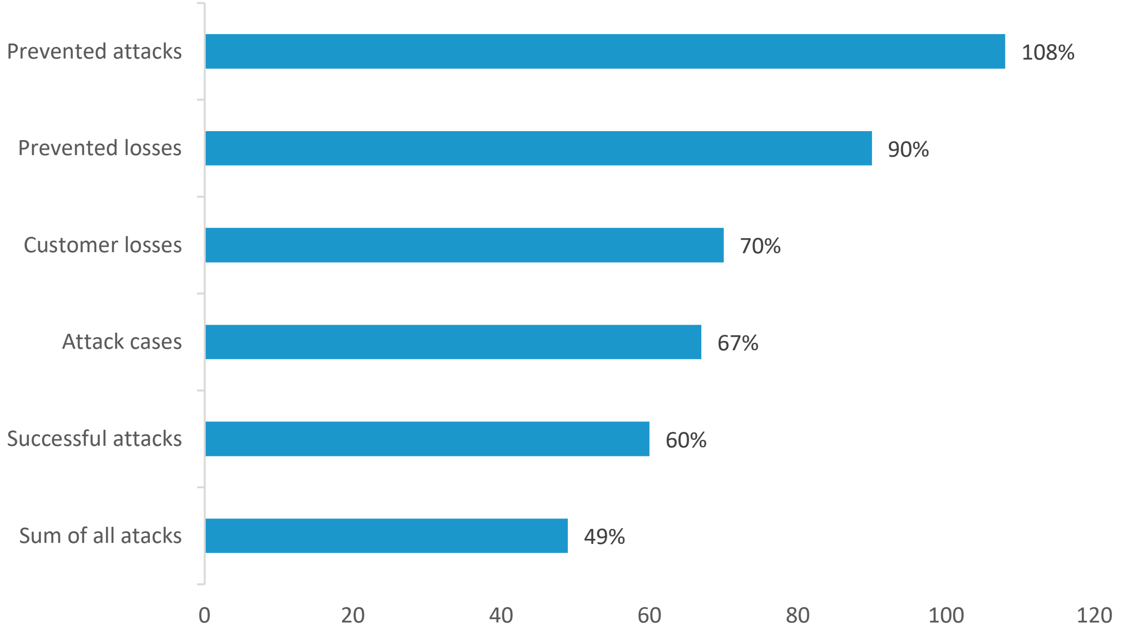

Fig. 1. Trends in the number and amount of fraud cases in 2020 compared to 2019

Despite the increase in the volume and number of successful fraud cases, an average check for successful fraud decreased by 8% from 15,061 rubles to 13,900 rubles. This means that banks process large amounts more carefully, and fraudsters tend to conduct more transactions with smaller amounts.

Figure 2 shows the evolution of financial losses by main fraud types. [1]

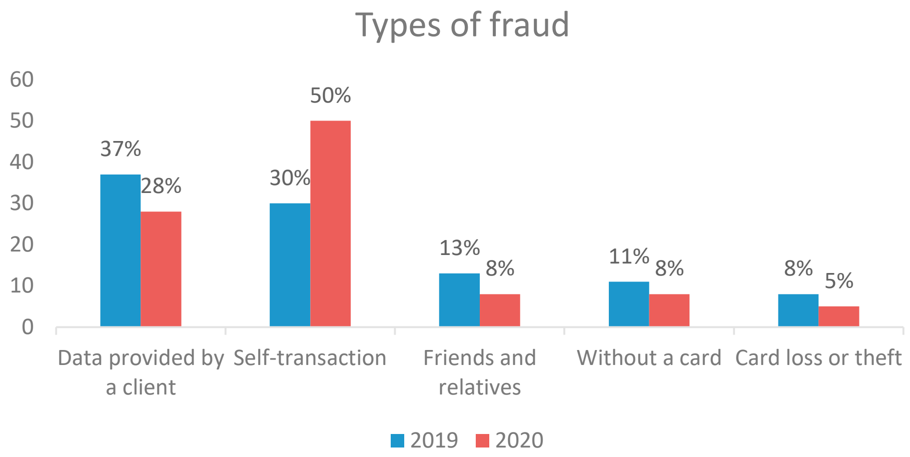

Fig. 2. Dynamics of financial losses by main types of fraud

It is possible to identify 9 main types of internal fraud in credit organizations:

- theft of funds from clients' accounts and cards;
- violation of credit procedures;
- money-laundering;
- procurement fraud;
- data theft;
- abuse of the motivation system;
- wage/salary fraud;
- accounting fraud;
- breach of procedures in the securities market.

The study revealed two types of fraud: theft of funds from clients' accounts and cards, and abuse of the motivation system.

The main objective of the study is to develop a technology to detect the actions of employees violating a credit organization procedures. To solve the task, the subtasks were formulated: to analyze the market of anti-fraud systems in credit organizations; create a feature space and a training sample; to pre-process the data; to use methods of feature selection and hyperparameter selection; to apply clustering and classification algorithms enabling development of a machine learning technology that identifies suspicious actions of employees.

The practical importance of the work includes demonstrating the effectiveness of machine learning techniques to detect the actions of employees related to the violation of credit organizations’ procedures, identifying the most informative indicators for detecting the theft of funds from customer accounts and cards and the abuse of the motivational system, as well as developing the technology to detect such actions.

2. Materials and Methods

Historically anti-fraud systems are a set of strict business rules used to identify whether an object is a fraud, or not. However, this concept is extremely nonuniversal and is highly susceptible to experts’ experience, the ones who specify the criteria.

Generation of a set of business rules can be considered as the next development stage. However, this ruleset has created some kind of risk zone. These models are more flexible but they have many disadvantages such as subjectivity (dependence on expert’s evaluation), focus on just well-known fraud schemes and cases, complicated business rules changes and updates.

Nowadays machine learning methods are used more and more often to detect fraud. They do not have the described above disadvantages. Anyway, the most effective way to create an anti-fraud system is to use a complex approach. [2, 3, 4]

Formally this task can be interpreted as a task of binary classification.

Research phases are given in Figure 3.

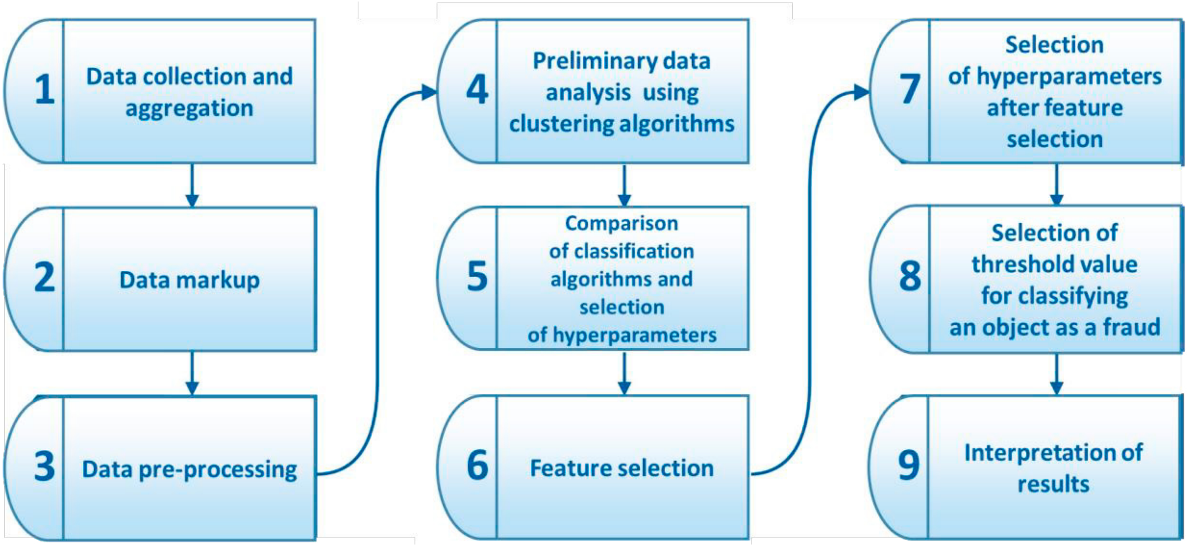
1 Data collection and aggregation
2 Data markup
3 Data pre-processing
4 Preliminary data analysis using clustering algorithms
5 Comparison of classification algorithms and selection of hyperparameters
6 Feature selection
7 Selection of hyperparameters after feature selection
8 Selection of threshold value for classifying an object as a fraud
9 Interpretation of results

Fig. 3. Stages of the study

The described sequence of stages ensures the technique efficiency.

Common methods for carrying out the stages presented in Figure 3 were analyzed prior to the research. [5]

Features can be divided into four types:

- neutral (employee' work experience in months, change of name);
- associated with profession (average number of client views per month, average number of changes in client's full name, etc.);
- associated with possible fraud (a total number of clients viewed in periods 00:00-09:30 or 19:30-00:00 per month, an average number of changes in client's actual phone number to make the number incorrect made by an employee per month, an average number of transactions conducted from a customer to an employee, etc.);
- associated with gambling (an average number of debit transactions in rubles over the last year connected with gambling, etc.).

The peculiarity of the task is that collected raw data for learning is daily statistics on employees without fraud markup. Since fraud information contained only the date of fraud detection and data on the worker, employee statistics were aggregated by averaging the feature per month or showing its maximum value per month. Concerning the foregoing information on incidents, data labelling was carried out in the following way:

1) the difference between the month of fraud detection and the month for which statistics on the employee were collected was presented in a special column;
2) the information from this column was used as an input to select "employee-month" objects with the difference greater than or equal to 0 among the objects containing employees who committed fraud;
3) the objects "employee-month" with zero sum of the values for all features were deleted (i.e., we delete months when the employee definitely was not active).

This algorithm is presented in Figure 4.

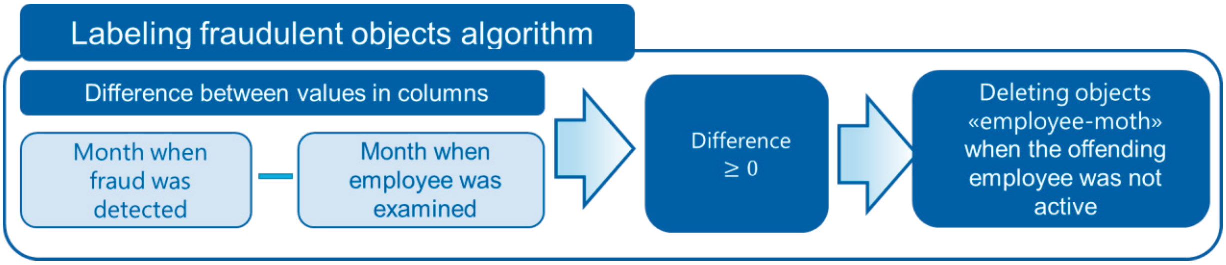
Labeling fraudulent objects algorithm
Difference between values in columns
Month when fraud was detected
Month when employee was examined
Difference ≥ 0
Deleting objects «employee-moth» when the offending employee was not active

Fig. 4. Algorithm of labeling fraudulent objects

Therefore, 49 objects were labelled as fraud.

After marking preliminary data processing was carried out, which included:

1) reduction of the sample by deleting objects with zero sum for all features, except neutral ones;
2) removal of some correlated and duplicated features;
3) removal of features with low variation.

Thus, after preliminary data processing, 40 features, about 71,000 objects, among which 49 are fraudulent were left.

Before solving the binary classification task, the data was standardized and the positions of objects in the feature space were visualized through their transformation by means of the principal component analysis.

In the next step, clustering was performed using the KMeans and DBSCAN (Density-based spatial clustering of applications with noise) methods. The results of the Kmeans and DBSCAN algorithms are presented in Table 1 and Table 2, respectively.

Table 1. The result of the algorithm KMeans

KMeans	Count of fraud	Count in cluster	Ratio
0	1.0	1828	0.000547
1	0.0	320	0.000000
2	13.0	35453	0.000367
3	12.0	5159	0.002326
4	23.0	28452	0.000808

Table 2. The result of the algorithm DBSCAN (sorted by decrease in the number of frauds in the cluster)

DBSCAN	Count of fraud	Count in cluster	Ratio
0	27.0	56077	0.000481
-1	22.0	13733	0.001602
128	0.0	6	0.000000
127	0.0	4	0.000000
94	0.0	11	0.000000
...	…	…	…
37	0.0	12	0.000000
36	0.0	8	0.000000
35	0.0	12	0.000000
34	0.0	21	0.000000
129	0.0	5	0.000000

Therefore, according to the results of using clustering algorithms, it could not be assumed that there is a separate cluster of fraudulent objects.

The following algorithms were used to solve the task: Logistic Regression, Random Forest, XGBoost, Easy Ensemble, Balanced Bagging, Multi-layer Perceptron, RUSBoost, Balanced Random Forest.

3. Results

Specificity of the task involves working with unbalanced samples, consequently, algorithms which are immune to such samples were used for conducting classification. [6, 7] Logistic regression, sensitive to class imbalance, was also used as an example.

ROC AUC was chosen as the most objective metric for evaluating the quality of the model. Validation was carried out using cross-validation for 5 blocks estimating the mean value of ROC AUC. Hyperparameters were chosen during building models using hyperopt library. Figure 5 shows plots of ROC curves for classifiers.

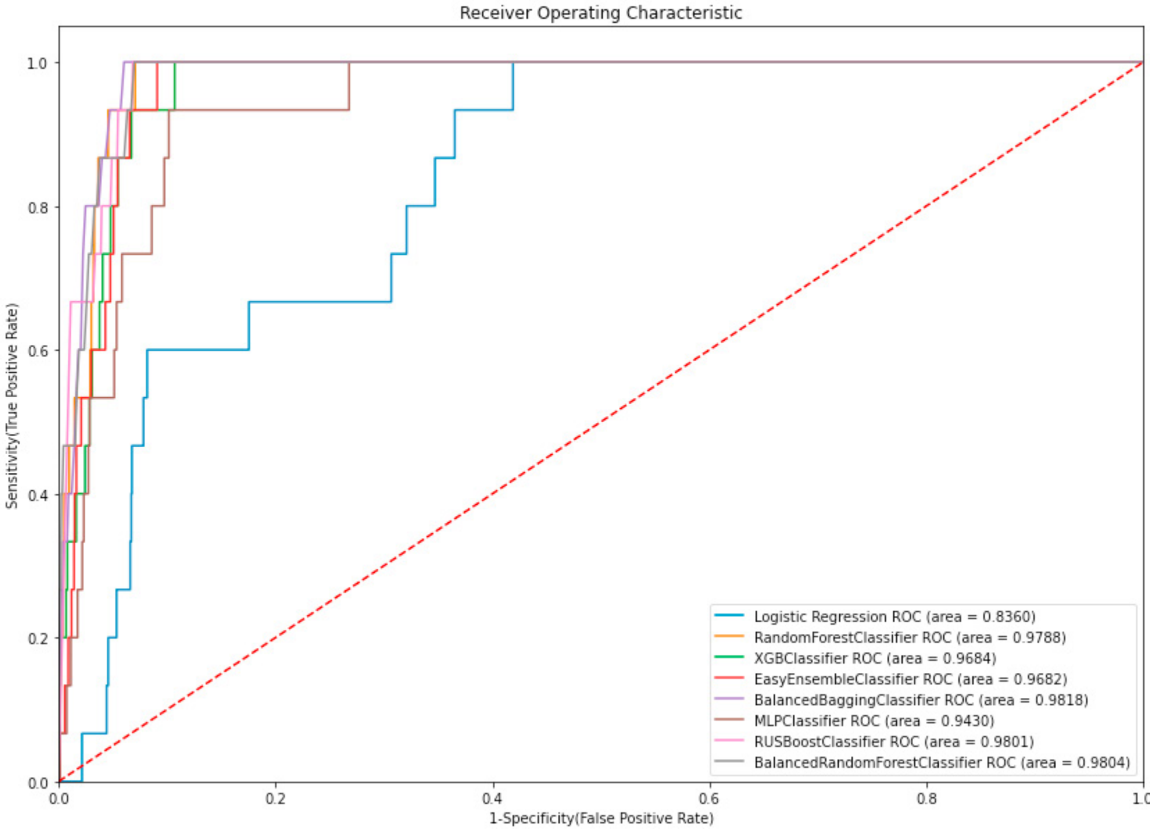

Fig. 5. ROC-curve plots for algorithms Logistic Regression, Random Forest, XGBoost, Easy Ensemble, Balanced Bagging, Multi-layer Perceptron, RUSBoost, Balanced Random Forest

Table 3 presents estimates of the results of the algorithms.

It can be clearly seen from Table 3 and Figure 5 that the best algorithm is Balanced Bagging with the simple tree-classifier, and it has the ROC AUC test-sample value 0.981837 and validation value 0.958191. This algorithm was used in further research.

Table 3. Comparison of classification algorithms

Method	ROC AUC on a test-sample	ROC AUC during validation
Logistic Regression	0.836024	0.828219
Random Forest	0.978797	0.937242
XGBoost	0.968379	0.950256
Easy Ensemble	0.968248	0.971134
Balanced Bagging	0.981837	0.958191
Multi-layer Perceptron	0.943029	0.913182
RUSBoost	0.980086	0.963263
Balanced Random Forest	0.980368	0.960720

At the next stage, features were selected by discarding the least informative without losing the quality of the model. After conducting this stage, 14 signs remained, and ROC AUC increased to 0.983692.

Further work was to refit hyperparameters after feature selection. Table 4 presents the best-fitted values of the hyperparameters of the model.

Table 4. Best selected values of hyperparameters

Hyperparameter name	Description of hyperparameter	Value of hyperparameter
n_estimators	number of trees in the ensemble	100
max_depth	maximum depth of the tree	6
max_samples	part of the sample to be extracted to train each tree	0.8
max_features	part of all features to be extracted to train each tree	0.5
bootstrap	are objects selected with return?	True
bootstrap features	are features selected with return?	True

The final stage in the implementation of the technology was the selection of the threshold value for classifying an object as a fraud. The optimal value was found using the Youden index and is equal to 0.72. As a result, we got the matrix of errors shown in Table 5.

Table 5. Matrix of errors

	Predicted True	Predicted False
Actually True	15	0
Actually False	960	20389

4. Discussion

In this work, we propose a technology to identify suspicious actions of employees related to the violation of the procedures of a credit institution.

Table 6 presents the features ranged by their information value in descending order.

Unfortunately, interpreting the results of algorithms based on bagging is an extremely difficult task. The criteria by which the classifier relates the object to fraud were not received.

Thus, this technology can be used for monthly detection of employee actions related to violation of banking procedures, namely, theft of customer funds from customer accounts and cards and misuse of the motivation system. Each month, the features presented in Table 6 are used as inputs to the model. For this, aggregation of these features for each employee on monthly basis will be necessary.

Table 6. The best matched values of hyperparameters

№	Name	Description
1	months_of_work	Months of work
2	sum_susp_time_cl_count_day	The total number of clients viewed in the intervals: 00:00-9:30 or 19:30-00:00 per month
3	avg_views_day	Average number of customer views per month
4	avg_dormant_mob_ch	The average number of changes to the mobile number of a sleeping client without his signature by an employee per month
5	avg_views_day_ratio	The average ratio of the number of views of an employee versus the average number of views of his colleagues per month
6	avg_new_card_mob_ch	The average number of cards issued after changing the client's full name or date of birth by an employee per month
7	sum_big_balance_cl_day	The total number of clients with a total balance of more than 1 million rubles viewed per month
8	avg_sum_week_cl	Average amount of transactions from customers to an employee per month

The built model can be considered as part of an anti-fraud system, which is used as an additional tool for tracking employees’ fraudulent actions.

5. Conclusion

During the research, a technology based on the use of machine learning methods was proposed to identify employee actions related to violations of the procedures of a credit institution, namely, to identify theft of funds from customer accounts and cards and abuse of the motivation system.

In this work, methods of counteracting fraud in credit organizations were analyzed, as well as the current situation in this field were researched.

As part of the research, an initial feature space was formed, consisting of 58 features and about 130,000 "employee-month" objects, 49 of which were marked as fraudulent. As a result of data pre-processing, about 71,000 objects and 40 features were selected.

At the next stage, a preliminary data analysis was carried out using clustering algorithms, during which it turned out that fraudulent objects cannot be allocated to a separate cluster.

The results of the classification algorithms with the best set of hyperparameters are presented. Balanced Bagging turned out to be the best algorithm.

For the best algorithm, the selection of features was carried out using their information value. As a result, 14 most informative features remained. For this algorithm, the best values of hyperparameters were selected for the chosen features, and then the optimal value of the probability of attributing an object to fraud was determined using the Youden's index.

The practical significance of the work lies in the development of technology based on the complex application of machine learning methods for identifying employees actions related to violation of the procedures of a credit institution, specifically the theft of funds from customer accounts and cards and abuse of the employee motivation system. The proposed technology can be used for regular (monthly) detection of these actions, both independently and as one of the modules of an anti-fraud system.

Acknowledgement

This work was supported by the National Research Nuclear University "MEPhI".

References

[1] Official website of Tinkoff Bank. Tinkoff Research: Fraud in the Russian Banking Sector in 2020 [Electronic resource]. URL: https://www.tinkoff.ru/about/news/19022021-tinkoff-fraud-research-2020/ (Accessed 01.04.2022);

[2] Pinchuk, Aleksandr. Machine learning against fraud in the banking sector. [Electronic resource]. URL: https://www.it-

world.ru/cionews/manage_secure/118786.html (Accessed 01.04.2022);

[3] Amineva, Julia. Review of anti-bank fraud (anti-fraud) systems. [Electronic resource]. URL: https://www.anti-malware.ru/analytics/Market_Analysis/anti-fraud-Bank-systems#part512 (Accessed 01.04.2022);

[4] Domashova, J. Identification of non-typical international transactions on bank cards of individuals using machine learning methods. In Domashova, J., Kripak, E. (eds.). Procedia Computer Science, 2020, 190, pp. 178-183. https://www.sciencedirect.com/journal/procedia-computer-science/vol/190/suppl/C

[5] Vorontsov, K.V. Lectures on methods of evaluation and selection of models // Professional information and analytical resource MachineLearning.ru [Electronic resource]. URL: http://www.machinelearning.ru/wiki/images/2/2d/voron-ml-modeling.pdf (Accessed 01.04.2022);

[6] Hido, Shohei, Kashima, Hisashi. Roughly Balanced Bagging for Imbalanced Data. [Электронный ресурс]. – URL: https://sci2s.ugr.es/keel/pdf/specific/congreso/hido_roughly_2008.pdf (Accessed 01.04.2022);

[7] Seiffert, Chris, Khoshgoftaar ,Taghi, Van Hulse, Jason, Napolitano, Amri. RUSBoost: A Hybrid Approach to Alleviating Class Imbalance. [Электронный ресурс]. – URL: https://www.researchgate.net/publication/224608502_RUSBoost_A_Hybrid_Approach_to_Alleviating_Class_Imbalance (Accessed 01.04.2022).