МОДЕЛЬ ВЫЯВЛЕНИЯ АНОМАЛЬНЫХ БАНКОВСКИХ ТРАНЗАКЦИЙ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

Данная статья посвящена разработке надежной модели выявления аномальных банковских транзакций, которые могут участвовать в схемах отмыывания денег и нелегального оборота товаров и услуг. В статье была предложена модель выявления аномальных банковских транзакций на основе машинного обучения. Для обучения и оценки модели используется набор данных CreditCardFraud, состоящий из 284807 транзакций кредитных карт: 492 имеют класс «незаконные», 284315 имеют класс «законные». В предлагаемой модели выявления аномальных банковских транзакций были использованы различные алгоритмы машинного обучения с подбором гиперпараметров. Для оценки предложенной модели использовалась метрика доля верных ответов, точность, полнота, F1 метрика и индекс сбалансированной точности. С помощью алгоритма ресэмплинга в условиях несбалансированности классов удалось повысить надежность классификации аномальных банковских транзакций по сравнению с лучшим известным результатом на наборе данных CreditCardFraud.

Ключевые слова: банковские транзакции, классификация, выявления аномальных транзакций, машинное обучение.

Feldman E. V., Ruchay A. N., Cherbadzhi D. Y.

MODEL FOR DETECTING ABNORMAL BANKING TRANSACTIONS BASED ON MACHINE LEARNING

This article is devoted to the development of a reliable model for detecting abnormal banking transactions that may be involved in money laundering and illegal trafficking of goods and services. The article proposed a model for detecting abnormal banking transactions based on machine learning. For training and evaluation of the model, the CreditCardFraud dataset is used, consisting of 284807 Bitcoin transactions: 492 of "illegal" and 284315 of "legal". The pro-

posed model for detecting abnormal bitcoin transactions is based on various machine learning algorithms with the selection of hyperparameters. To evaluate the proposed model, we used the metric of accuracy, precision, recall, F1 score, and index of balanced accuracy. Using the resampling algorithm in conditions of class imbalance, it was possible to increase the reliability of the classification of abnormal banking transactions in comparison with the best-known result on the CreditCardFraud dataset.

Keywords: transactions, classification, detection of abnormal transactions, machine learning.

1. Введение

Исходя из отчетов компании Nilson, занимающейся анализом банковских транзакций, общий объем денежных средств, потерянных в результате мошенничества еще в 2016 году, достиг отметки в 22,8 миллиардов долларов, а уже в 2019 году было зафиксировано значение 28,7 миллиардов долларов. Это только подтверждает необходимость того, чтобы банки научились распознавать мошенничество заранее, еще до того, как оно произошло.

Все международные платежные системы (VISA, MasterCard, PayPal и другие) имеют свои системы антифроды, предназначенные для оценки транзакций на предмет их подозрительности с точки зрения мошенничества. Как правило, антифрод состоит из списков, фильтров и правил, по которым проверяются все транзакции. В России тоже используются антифроды для поимки лиц, занимающихся мошенническими действиями в сфере информационных технологий. Но особенно остро стоит вопрос выявления нелегального оборота товаров и услуг. Такой инструмент был бы полезен для выявления незаконных транзакций по обороту товаров и услуг [1].

Данная статья посвящена разработке модели выявления аномальных банковских транзакций на основе машинного обучения. Мы используем набор данных CreditCardFraud [2], состоящий из более чем 200 тысяч банковских транзакций с помощью банковских карт.

В данной статье в предлагаемой модели выявления аномальных транзакций биткоинов были использованы следующие алгоритмы машинного обучения: линейная регрессия, квадратичная регрессия, логистическая регрессия, k-ближайших соседей, деревья решений, случайный лес, наивный байесовский классификатор, метод опорных векторов, классификатор на основе многослойных Персептронов, линейный дискриминантный анализ, квадратичный дискриминантный анализ, адаптивный бустинг. Кроме того, в ра-

боте были использованы методы оптимизации гиперпараметров для алгоритмов машинного обучения, что позволило бы повысить надежность классификации.

Было сделано одно важное наблюдение, что набор данных CreditCardFraud является несбалансированным (492 <<незаконные>> и 284315 <<законные>>). Поэтому были выполнены эксперименты по повышению надежности классификации аномальных транзакций биткоинов с помощью алгоритмов ресэмплинга в условиях несбалансированности классов. Благодаря чему удалось повысить надежность классификации аномальных транзакций биткоинов по сравнению с лучшим известным результатом на наборе данных CreditCardFraud [2].

2. Набор данных

Для разработки модели выявления аномальных транзакций необходимо иметь подготовленный большой набор данных для обучения модели. Поскольку дело касается банковских операций, в открытом доступе отсутствуют подходящие наборы данных. Существует единственный набор данных CreditCardFraud, который содержит транзакции, совершенные европейскими держателями кредитных карт в сентябре 2013 года. В этом наборе данных представлены транзакции, которые произошли за два дня. За это время было обнаружено 492 мошенничества из 284 807 транзакций. Набор данных сильно несбалансирован, поскольку на положительный класс (мошенничество) приходится 0,172% всех транзакций.

Набор данных CreditCardFraud содержит только числовые признаки, которые являются результатом преобразования исходных значений признаком методом главных компонент. Из-за проблем с конфиденциальностью невозможно получить исходные функции и дополнительную информацию о данных. Признаки V1, V2, ..., V28 являются основными компонентами, полученные с помощью метода главных компонент. Единственными открытыми признаками являются признаки

«Time» и «Amount». Признак «Time» содержит секунды, прошедшие между каждой транзакцией и первой транзакцией в наборе данных. Признак «Amount» отображает сумму транзакции. Признак «Class» является меткой правильного ответа, которая принимает значение 1 в случае мошенничества и 0 в противном случае.

3. Модель выявления аномальных банковских транзакций с помощью машинного обучения

Задачей машинного обучения является поиск целевой функции $f: X \rightarrow Y$, где X — набор входных данных и Y — набор выходных переменных. Процесс поиска этой целевой функции f называется обучением с учителем или построением модели. Целевая функция может быть найдена только при наличии достаточного количества помеченных данных. В выбранном наборе данных все записи являются размеченными.

Так как поиск точной целевой функции является очень сложной задачей, то зачастую на практике она аппроксимируется приближенной функцией. То есть при процессе обучения ищется определенная функция h , наилучшим образом аппроксимирующая неизвестную целевую функцию f . Для обучения модели требуется выборка из исходного набора данных, как правило, составляющая 70% от исходного объема данных. Далее настраиваются параметры модели. Для этого используется валидационный набор, объем которого обычно берется как 20% обучающих данных. Предсказательная способность модели оценивается с использованием тестового набора, которая составляет 30% от набора данных.

В модели выявления аномальных банковских транзакций есть набор данных M , который состоит из $n = 284807$ транзакций, а также метка ответа, показывающая, является ли данная транзакция незаконной или законной. С каждой транзакцией связан вектор признаков, состоящий из 30 значений. Для целевой функции f требуется определить, является ли конкретная транзакция m незаконной (в этом случае он принимается за 1) или законной (в этом случае принимается значение 0). Целевая функция f может быть найдена с помощью одного из алгоритма машинного обучения для набора из n помеченных транзакций.

Для выявления аномальных банковских транзакций, в работе были использованы

следующие алгоритма машинного обучения: линейная регрессия; квадратичная регрессия; логистическая регрессия; k -ближайших соседей; деревья решений; случайный лес; наивный байесовский классификатор; метод опорных векторов; классификатор на основе многослойных персептронов; линейный дискриминантный анализ; квадратичный дискриминантный анализ; адаптивный бустинг; градиентный бустинг.

Поскольку задача сводится к тому, что нужно определить является ли данная транзакция законной или незаконной, то в общем виде это представляется как задача бинарной классификации, где за положительный класс — это набор незаконных транзакций, а за отрицательный — незаконные.

Далее, рассмотрим общие метрики оценки, используемые в моделях машинного обучения.

Доля правильных ответов (Accuracy) — показатель того, как часто классификатор делает правильные предсказания, и равен

$$\frac{TP + TN}{TP + TN + FP + FN},$$

где TP (True Positive) — это число положительных результатов, которые были корректно предсказаны моделью и принадлежат к положительному классу; TN (True Negative) — это число отрицательных результатов, которые были корректно предсказаны моделью и принадлежат к отрицательному классу; FP (False Positive) — это число положительных результатов, которые были некорректно предсказаны моделью и принадлежат к отрицательному классу; FN (False Negative) — это число отрицательных результатов, которые были некорректно предсказаны моделью и принадлежат к положительному классу. Значения FP и FN также часто называют ошибками первого и второго рода.

Точность (Precision) — это показатель

$$\frac{TP}{TP + FP},$$

измеряющий коэффициент правильности классификатора, когда он правильно предсказывает положительную метку класса для положительного класса.

Полнота (Recall) — это показатель

$$\frac{TP}{TP + FN},$$

оценивающий как часто классификатор предсказывает положительную метку для данных, когда данные действительно принадлежат положительному классу.

F1 метрика (F1 Score) — гармоническое среднее точности и полноты, которая рассчитывается следующим образом:

PrecisionRecall

$$F1 = 2 \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}.$$

Метрика F1 располагается в отрезке между 0 и 1.

Геометрическое среднее (Geometric mean (Gmean)) — это показатель, равный $\sqrt{TP + TN}$, который используется для того чтобы максимизировать положительные и отрицательные результаты классификаций, предсказанные верно и сохраняя между ними баланс. Нужно помнить о том, что геометрическое среднее сводит негативное влияние перекосов распределения классов к минимуму, но оно не объясняет вклад каждого из классов в общие показатели, потому что дает одинаковый результат для разных комбинаций TP и TN.

Доминирование (Dominance) — это показатель TP – TN, используемый для оценки разницы между TP и TN.

В статье [3] была предложена метрика под названием индекс сбалансированной точности (Index of Balanced Accuracy (IBA)). IBA нужен для оценки бинарного классификатора, в котором данные являются несбалансированными. IBA может быть рассчитан как

$$IBA = (1 + \text{Dominance}) \cdot \text{Gmean}^2.$$

При замене Dominance и Gmean итоговая формула предоставляет полезную информацию для изучения того, как IBA поддерживает баланс между Dominance и Gmean, также для Dominance можно добавить взвешенный параметр α , который расположен на отрезке $0 \leq \alpha \leq 1$.

$$IBA = (1 + \alpha(TP - TN)) \cdot TP \cdot TN.$$

Однако, если $\alpha = 0$, то IBA равняется Gmean^2 .

Так как в представленном наборе данных количество незаконных транзакций равняется 492 против 284807 законных, то этот набор является несбалансированным. Класс будем называть миноритарным, когда в наборе данных доля экземпляров некоторого класса слишком мала, а другой класс — мажоритарным, когда он сильно представлен в наборе данных.

Для решения проблемы несбалансированности данных есть несколько подходов. Одним из них является применение различных стратегий ресемплинга (resampling).

Восстановление баланса классов может происходить двумя методами. В первом слу-

чае удаляют некоторое количество экземпляров мажоритарного класса (undersampling), во втором — с помощью синтетических данных увеличивают количество экземпляров миноритарного класса (oversampling).

Для решения проблемы несбалансированности данных был выбран алгоритм Tomek Links [4]. Все мажоритарные экземпляры, которые входят в связи Томека, можно удалить из набора данных. Алгоритм Tomek Links направлен на то, чтобы удалить экземпляры, которые можно рассматривать как зашумленные.

4. Результаты экспериментов

Для реализации алгоритма нахождения аномальных транзакций с помощью машинного обучения, использовался язык программирования Python 3, поскольку он больше всего приспособлен для выполнения задач такого рода, а также имеет отличную производительность при обработке данных. Стоит отметить, что в Python есть множество готовых фреймворков и библиотек, которые существенно упрощают процесс написания кода и сокращают время на разработку.

Для работы с данными была выбрана библиотека Pandas, которая использует высокоуровневые структуры данных. Выбор пал именно в пользу Pandas так как в ней есть встроенные методы для группировки, комбинирования и фильтрации данных. Pandas позволяет извлекать данные из различных источников, таких как базы данных SQL, файлы CSV, Excel, JSON для последующей обработки и изучения.

В качестве среды разработки был выбран Google Collab, поскольку в нем уже установлены основные библиотеки, требуемые в разработке. Стоит отметить простоту использования, высокую производительность и отказоустойчивость данного сервера.

Реализация включала в себя несколько этапов:

- Загрузка данных и базовое изучение
- Предобработка данных
- Визуализация
- Обучение

Для обучения данных важно грамотно изучить содержимое исходной таблицы на предмет пропущенных значений. Поэтому в первую очередь было проверено, есть ли в таблицах пропуски. Оказалось, что все значения заданы, значит, их все можно использовать в дальнейшем.

Далее, было решено проверить записи на

предмет уникальности. Оказалось, что не все данные являются таковыми и из 284807 записей уникальными были 283726. Помня небольшое количество аномальных транзакций, было решено узнать, сколько из 1081 транзакции, которые повторяются, являются мошенническими. Был получен следующий результат: не все неуникальные транзакции являются легитимными, 19 из них является аномальными.

Так как набор данных изначально являлся сильно несбалансированным с количеством мажоритарных записей равных 492, важно, что процент их уникальности порядка 96 процентов.

Исходя из вышеописанного, было принято решение исключить неуникальные записи из набора данных и работать с оставшимися 283726 строками. Как в дальнейшем показала практика, именно на этом наборе данных процент точности обучения немного выше.

Таким образом, уже на получившемся наборе данных был испробован метод решения проблемы несбалансированности данных: алгоритм Tomek Links. При помощи этого алгоритма, из полученного набора данных были удалены еще 248 записей из доминирующего класса, которые попадают под условие связи Томека. В дальнейшем использование данного алгоритма позволило повысить процент точности обучения.

Для реализации задачи классификации транзакций было принято решение попробовать различные комбинации алгоритмов машинного обучения из готовых библиотек.

Также для реализации задачи классификации данных, к исходному набору данных были применены различные методы функционального преобразования. Данные методы особенно полезно в машинном обучении, так как различные метрики могут измеряться в разных диапазонах, или значения одного метрики варьируются слишком сильно. Функциональное преобразование можно разделить на нормализацию и стандартизацию данных. Нормализация подразумевает изменение диапазонов в данных без изменения формы распределения, в то время как стандартизация изменяет форму распределения данных. Обычно достаточно нормализовать данные, тогда как стандартизацию стоит применять при использовании алгоритмов, которые основываются на измерении расстояний, например, k-ближайших соседей или метод опорных векторов.

В качестве тестовой и обучающей выборки были отобраны транзакции, помеченные как легитимные или аномальные в соотношении 30:70 соответственно. С помощью выбранных алгоритмов была обучена модель выявления аномальных банковских транзакций транзакций.

Для оценки надежности обученных моделей были рассчитаны метрики: доля верных ответов (accuracy), точность (precision), полнота (recall), F1 метрика (F1 Score) и индекс сбалансированной точности (IBA).

В ходе работы были опробованы следующие вариации обучения модели выявления аномальных банковских транзакций:

1. С удалением повторяющихся исходных данных и без (2 варианта);
2. С оптимизацией данных при помощи алгоритма Tomek Links и без (2 варианта);
3. С нормализаторами данных MinMax Scaler, MaxAbsScaler, StandardScaler, PowerTransformer, QuantileTransformer, Normalizer, FunctionTransformer, PolynomialFeatures, RobustScaler и без (10 вариантов);
4. С различными методами машинного обучения: RandomForest, AdaBoost, K-Neighbors, DecisionTree, LogisticRegression, SVC, CatBoost, XGBoost, LGBM, Trpot, AutoSklearn (11 вариантов);

Всего получается 440 различных комбинаций.

В результаты работы метода машинного обучения RandomForest было замечено, что точность построенной модели увеличилась на 0.0001, если использовать алгоритм Tomek Links. Поэтому в дальнейшем, с каждым из следующих методов применялась эта оптимизация данных. Что касается работы с удалением повторяющихся исходных данных, то их наличие никак не повлияло на точность модели.

В таблице 1 представлены результаты работы метода машинного обучения RandomForest с различными нормализаторами данных. Видно, что лучше всего себя проявили следующие функции масштабирования: StandardScaler, PowerTransformer, QuantileTransformer, Normalizer. Данные нормализаторы показали одинаковую точность, но за счет индекса IBA, лучшим методом масштабирования для данной задачи является QuantileTransformer, подтверждая теоретические тезисы о том, что данный скейлер разработан для задач классификации.

В таблице 2 представлены лучшие резуль-

Сравнение методов нормализации

Нормализатор	Accuracy	IBA
MinMaxScaler	0.9998	0.9012
MaxAbsScaler	0.9998	0.9111
StandardScaler	0.9999	0.9225
PowerTransformer	0.9999	0.9256
QuantileTransformer	0.9999	0.9306
Normalizer	0.9999	0.9199
RobustScaler	0.9998	0.9056
FunctionTransformer	0.9998	0.9168
PolynomialFeatures	0.9998	0.9044

таты для каждого метода машинного обучения. Стоит отметить, что показатели Precision, Recall и F1 Score считались отдельно для каждого из классов транзакций. Таблица 1 отображает лучшие результаты именно для аномальных незаконных банковских транзакций, так как для оценки эффективности детектирования транзакций в большей степени важно анализировать ошибки для класса неза-

конных транзакций. Из таблицы 2 видно, что лучшие показатели точности были достигнуты в методах: RandomForest, CatBoost, XGBoost, Tpot, AutoSklearn.

Поскольку методы Tpot и AutoSklearn являются автоматизированными и сами подбирают лучшие гиперпараметры и методы обучения, то в таблице 2 представлены вариации этих методов, которые дали лучший резуль-

Таблица 2

Сравнение методов машинного обучения

Метод	Precision	Recall	F1 Score	Accuracy	IBA
RandomForestClassifier	0.9866	0.9366	0.9610	0.9999	0.9306
AdaBoost	0.8113	0.7273	0.7670	0.9993	0.7073
K-Neighbors	0.6881	0.6773	0.6993	0.9985	0.6885
DecisionTree	0.9129	0.9302	0.9215	0.9997	0.9236
LogisticRegression	0.7047	0.6913	0.6980	0.9990	0.6697
SVM	0.6425	0.6772	0.6328	0.9983	0.6567
CatBoost	0.9799	0.9281	0.9533	0.9998	0.9214
XGBoost	0.9820	0.9239	0.9521	0.9998	0.9168
LGBM	0.5313	0.8161	0.5634	0.9979	0.7997
Tpot	0.9888	0.9366	0.9620	0.9999	0.9306
AutoSklearn	0.9930	0.9006	0.9446	0.9998	0.8917

тат. Для Tpot это оказался метод XGBClassifier с параметрами: learning_rate=0.5, max_depth=7, min_child_weight=1, n_estimators=100, n_jobs=1, subsample=0.8, а для AutoSklearn это был метод RandomForest с параметрами: learning_rate=0.5, max_depth=10, min_child_weight=1, n_estimators=100, n_thread=1, subsample=0.7

Заметив, что параметры получаются примерно одинаковые, было принято решение не заниматься перебором гиперпараметров, а обучать модели на различных методах с этими же гиперпараметрами.

основе машинного обучения. Аномальными являются банковские транзакции, которые могут быть использованы в схеме отмывания денег или незаконного оборота товаров и услуг. Для обучения и оценки данной модели был использован набор данных, состоящий из 284807 транзакций, из которых 492 являются нелегальными, а остальные входят в класс легитимных. В предложенной модели обнаружения аномальных транзакций использовались различные алгоритмы машинного обучения. С помощью алгоритма пересчета Tomek Links в условиях несбалансиро-

Таблица 3

Сравнение результатов с другими работами

Метод	Precision	Recall	F1 Score	Accuracy	IBA
RandomForestClassifier	0.9866	0.9366	0.9610	0.9999	0.9306
CatBoost	0.9799	0.9281	0.9533	0.9998	0.9214
XGBoost	0.9820	0.9239	0.9521	0.9998	0.9168
Tpot	0.9888	0.9366	0.9620	0.9999	0.9306
AutoSklearn	0.9930	0.9006	0.9446	0.9998	0.8917
LogisticRegression[5]	0.99	0.90	0.94	0.94	-
K-Neighbors[5]	0.99	0.86	0.92	0.93	-
SVM[5]	0.99	0.88	0.93	0.93	-
LogisticRegression[6]	0.9226	0.9184	-	0.9315	-
Autoencoders[7]	0.84	0.74	0.79	0.8341	-
IsolationForest[8]	-	-	-	0.8049	-

В таблице 3 отображены лучшие результаты, достигнутые в ходе данной работы и в других статьях. С этой целью были взяты результаты из работ [5], [6], [7], [8], в которых так же строились модели выявления аномальных транзакций на этом же наборе данных. Метрики Precision, Recall, F1 Score, IBA указаны для аномальных транзакций, если же они не подсчитаны, то стоит прочерк. Видно, что полученные в ходе данного исследования результаты, являются точнее, чем ранее полученные.

5. Заключение

В данной была предложена модель выявления аномальных банковских транзакций на

важных классов и различных методов функционального преобразования удалось повысить достоверность классификации. В результате, надежность предложенной модели обнаружения аномальных транзакций на основе алгоритмов Tpot и RandomForest составляет 0,9999. Это значение на порядок выше, чем в проводимых на этом же наборе данных исследованиях [5], [6], [7], [8].

Литература

1. Фельдман Е.В. Противодействие совершению бесконтактных преступлений с использованием цифровых технологий // Вестник УрФО. Безопасность в информационной сфере. 2020. № 2 (36). С. 49-55.
2. Набор данных CreditCardFraud [Электронный ресурс] // Kaggle, Inc. URL: <https://www.kaggle.com/mlg-ulb/CreditCardFraudfraud>
3. Garcia V., Mollineda R.A., Sanchez J.S. Index of Balanced Accuracy: A Performance Measure for Skewed Class Distributions. Pattern Recognition and Image Analysis. IbPRIA 2009. Lecture Notes in Computer Science, vol 5524. Springer, Berlin, Heidelberg.
4. Tomek I. Two modifications of CNN // IEEE Trans. Syst. Man Cybern., vol. 6, 1976, 769–772.
5. In depth skewed data classif [Электронный ресурс] // Kaggle, Inc. URL: <https://www.kaggle.com/joparga3/in-depth-skewed-data-classif-93-recall-acc-now>
6. Semi Supervised Classification using AutoEncoders [Электронный ресурс] // Kaggle, Inc. URL: <https://www.kaggle.com/shivamb/semi-supervised-classification-using-autoencoders>
7. Выявление мошенничества с помощью алгоритмов случайного леса, нейронного автокодировщика и изолирующего леса [Электронный ресурс] // Habr, Inc. URL: <https://habr.com/ru/company/nix/blog/478286/>
8. 9 подходов для выявления аномалий [Электронный ресурс] // Habr, Inc. URL: <https://habr.com/ru/post/477450/>

References

1. Fel'dman E.V. Protivodejstvie soversheniyu beskontaktnyh prestuplenij s ispol'zovaniem cifrovych tekhnologij // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2020. № 2 (36). S. 49-55.
2. CreditCardFraud // Kaggle, Inc. URL: <https://www.kaggle.com/mlg-ulb/CreditCardFraudfraud>
3. Garcia V., Mollineda R.A., Sanchez J.S. Index of Balanced Accuracy: A Performance Measure for Skewed Class Distributions. Pattern Recognition and Image Analysis. IbPRIA 2009. Lecture Notes in Computer Science, vol 5524. Springer, Berlin, Heidelberg.
4. Tomek I. Two modifications of CNN // IEEE Trans. Syst. Man Cybern., vol. 6, 1976, 769–772.
5. In depth skewed data classif // Kaggle, Inc. URL: <https://www.kaggle.com/joparga3/in-depth-skewed-data-classif-93-recall-acc-now>
6. Semi Supervised Classification using AutoEncoders // Kaggle, Inc. URL: <https://www.kaggle.com/shivamb/semi-supervised-classification-using-autoencoders>
7. Vyyavlenie moshennichestva s pomoshch'yu algoritmov sluchajnogo lesa, nejronnogo avtokodirovshchika i izoliruyushchego lesa // Habr, Inc. URL: <https://habr.com/ru/company/nix/blog/478286/>
8. 9 podhodov dlya vyyavleniya anomalij // Habr, Inc. URL: <https://habr.com/ru/post/477450/>

ФЕЛЬДМАН Елена Васильевна, старший преподаватель кафедры компьютерной безопасности и прикладной алгебры; Челябинский государственный университет. 454001, Россия, Челябинск, ул. Братьев Кашириных, 129. E-mail: mila008.is@gmail.com

РУЧАЙ Алексей Николаевич, кандидат физико-математических наук, доцент, заведующий кафедрой компьютерной безопасности и прикладной алгебры. Челябинский государственный университет. 454001, Россия, Челябинск, ул. Братьев Кашириных, 129; доцент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, Россия, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: ran@csu.ru

Чербаджи Дмитрий Юрьевич, студент математического факультета, Челябинский государственный университет. 454001, Россия, Челябинск, ул. Братьев Кашириных, 129. E-mail: enorot@gmail.com

FELDMAN Elena, Senior Lecturer of the Department of Computer Security and Applied Algebra; Chelyabinsk State University. 454001, Russia, Chelyabinsk, st. Brothers Kashirins, 129. E-mail: mila008.is@gmail.com

RUCHAY Alexey, PhD in Physics and Mathematics, Associate Professor, Head of the Department of Computer Security and Applied Algebra; Chelyabinsk State University. 454001, Russia, Chelyabinsk, st. Brothers Kashirins, 129.; Associate Professor, Department of Information Security, South Ural State University (National Research University). 454080, Russia, Chelyabinsk, etc. them. IN AND. Lenin, 76. E-mail: ran@csu.ru

CHERBADZHI Dmitry, student of the Faculty of Mathematics, Chelyabinsk State University. 454001, Russia, Chelyabinsk, st. Brothers Kashirins, 129. E-mail: enorot@gmail.com