# ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

DOI: 10.18137/RNU.V9187.24.02.P.92 УДК 004.89

Д.Д. Абдурахман

## ОБНАРУЖЕНИЕ МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ ПУТЕМ СОЧЕТАНИЯ ПОВЕДЕНЧЕСКОГО ПРОФИЛИРОВАНИЯ, КЛАСТЕРИЗАЦИИ И LSTM

**Аннотация.** Мошенничество с банковскими картами представляет существенный риск как для финансовых учреждений, так и для потребителей, что требует применения сложных методов обнаружения. В этой статье представлен инновационный подход к улучшению обнаружения мошенничества с банковскими картами за счет интеграции поведенческого профилирования, кластеризации и нейронных сетей с длинной краткосрочной памятью (LSTM). Эта методология использует совокупные преимущества этих методов для повышения точности и эффективности систем обнаружения мошенничества. Поведенческое профилирование выявляет уникальные потребительские привычки и характеристики людей, а кластеризация организует похожие аккаунты на основе этих профилей. Затем модели LSTM используются для изучения временных зависимостей и последовательных шаблонов внутри каждого кластера, что позволяет точно обнаруживать мошеннические транзакции. Эта интеграция эффективно решает проблемы классового дисбаланса и сложности схем мошенничества в данных. Предложенный подход протестирован на реальном наборе данных о транзакциях по банковским картам и продемонстрировал высокую производительность с точки зрения Accuracy, F1-score и AUC-ROC по сравнению с традиционными методами.

*Ключевые слова:* машинное обучение, несбалансированный набор данных, мошенничество с банковскими картами, профилирование, кластеризация, LSTM.

D.D. Abdourahman

## OPTIMIZING CREDIT CARD FRAUD DETECTION BY COMBINING BEHAVIORAL PROFILING, CLUSTERING, AND LSTM

**Abstract.** Credit card fraud poses a substantial risk to both financial institutions and consumers, necessitating sophisticated detection methods. This paper introduces an innovative approach to enhancing credit card fraud detection by integrating behavioral profiling, clustering, and Long Short-Term Memory (LSTM) neural networks. This methodology exploits the combined strengths of these techniques to improve the precision and efficiency of fraud detection systems. Behavioral profiling identifies the unique spending habits and characteristics of individuals, while clustering organizes similar accounts based on these profiles. LSTM models are then utilized to learn the temporal dependencies and sequential patterns within each cluster, enabling precise detection of fraudulent transactions. This integration effectively addresses the challenges of class imbalance and the complexity of fraud patterns in the data. The proposed approach is tested on a real-world credit card transaction dataset, showcasing its superior performance in terms of Accuracy, F1-score and AUC-ROC compared to conventional methods.

*Keywords:* machine learning, imbalanced dataset, credit card fraud, profiling, clustering, LSTM.

**Абдурахман Джамал Джама**
аспирант кафедры информационной безопасности. Финансовый университет при Правительстве Российской Федерации, Москва. Сфера научных интересов: информационная безопасность в финансовой отрасли. Автор двух опубликованных научных работ.
Электронный адрес: jamaljolevas14psg@gmail.com

*Введение*

Рост числа цифровых транзакций приводит к увеличению случаев мошенничества с банковскими картами, что представляет значительные угрозы для безопасности финансовых операций. Традиционные системы выявления мошенничества, основанные на установленных правилах, испытывают затруднения в адаптации к новым методам мошенничества и не способны выявить сложные закономерности, характерные для транзакций. Методы машинного обучения проявляют себя многообещающими в преодолении этих проблем, однако многие из имеющихся подходов не решают проблемы обработки дисбаланса классов, несбалансированности данных и учета временных зависимостей в последовательностях транзакций. В данной работе рассматривается новый метод оптимизации обнаружения мошенничества с применением банковских карт, который объединяет в себе поведенческое профилирование, кластерный анализ и нейронные сети с использованием долгой краткосрочной памяти (LSTM). Предлагаемый подход совмещает преимущества указанных методик для решения задач обнаружения мошенничества и увеличения общей эффективности системы.

*Связанные исследования*

Заметный прогресс достигнут в исследованиях мошенничества с банковскими картами, рассматривающих различные методологии, такие как контролируемое обучение, неконтролируемое обучение и глубокое обучение. В области контролируемого обучения в работе [1] изучались возможности таких моделей, как логистическая регрессия, деревья с градиентным усилением (GBT) и нейронные сети, для обнаружения мошенничества. Они включают в себя генерацию функций с помощью как экспертных знаний в предметной области, так и неконтролируемого метода – автокодировщика. Исследование показывает, что функции, основанные на экспертных знаниях в предметной области, значительно улучшили значение AUC, а нейронные сети продемонстрировали высокую производительность.

Исследование [2] подтверждает эффективность деревьев с экстремальным повышением градиента (XGBoost) при обнаружении мошенничества с банковскими картами. Их сравнительный анализ оценивает Random Forest, XGBoost и метод пользовательского ансамбля как наиболее эффективные классификаторы, подчеркивая проблемы, связанные с несбалансированными данными.

Авторы работы [3] внесли свой вклад в контролируемые методы, используя функции, разработанные на основе опыта в предметной области и сравнивая различные нейронные сети, при этом показали, что Gated Recurrent Unit превосходит другие. Это исследование подчеркивает прогностическую силу методов глубокого обучения, использующих информацию временных рядов. В сфере обучения без учителя преобладают методы кластериза-

ции, особенно K-средние. В работах [4; 5] применяется кластеризация K-средних к данным банковских карт. В [5; 6] этот подход расширен на нечисловые атрибуты, используется One-Hot-Encoding и исследуются K-прототипы, гибридный метод, объединяющий как числовые, так и категориальные атрибуты.

В исследовании [7] представлен иной подход, в котором состязательное обучение осуществляется с помощью метода подкрепления, называемого марковским процессом принятия решений. В этой парадигме агент-мошенник взаимодействует с классификатором мошенничества банка, используя классификатор логистической регрессии. Состязательная структура учитывает динамическое поведение мошенников, стремясь облегчить разработку адаптивных систем обнаружения мошенничества за счет максимизации положительных отзывов или совокупного вознаграждения. Эти разнообразные методологии в совокупности способствуют многогранному исследованию мошенничества с банковскими картами.

*Методология (профилирование и кластеризация счетов)*

**Сбор и предварительная обработка данных.** Использовался общедоступный набор данных, содержащий анонимные записи транзакций по банковским картам. Набор данных включает сумму транзакции, данные продавца, временную метку (timestamp) и двоичную метку, указывающую, является ли транзакция мошеннической. Данные о транзакциях по банковским картам предварительно обрабатываются на предмет пропущенных значений, выбросов (outliers) и асимметрии данных (data skewness) [8]. Такие методы, как преобразование журналов (log transformation) и масштабирование функций (feature scaling), применяются, чтобы гарантировать, что данные подходят для моделей глубокого обучения [9].

Ключевые этапы предварительной обработки:

• *Normalization* (нормализация). Нормализация сумм транзакций и других числовых признаков для обеспечения сопоставимости. Все непрерывные признаки были нормализованы так, чтобы иметь нулевое среднее значение и единичную дисперсию;

• *Sequence Generation* (генерация последовательностей). Организация транзакций в последовательности на основе идентификаторов держателей карт и хронологического порядка;

• *Feature Engineering* (разработка признаков). Создание дополнительных признаков, таких как временные интервалы между транзакциями и частота транзакций;

• *Encoding* (кодирование). Категориальные переменные были закодированы с использованием горячего кодирования;

• *Imputation* (вменение). Пропущенные значения были вменены с использованием ***mean*** для непрерывных признаков и ***mode*** для категориальных признаков.

Набор данных был разделен на обучающий (70 %), проверочный (15 %) и тестовый (15 %) наборы для оценки производительности предложенной модели.

**Профилирование** (Behavioral Profiling) предполагает анализ исторических данных транзакций для установления нормальных моделей поведения для каждого пользователя банковской карты. Создавая эти профили, системы могут оценить, что представляет собой нормальную активность для отдельных учетных записей. Любое существенное отклонение от этого установленного поведения может вызвать предупреждение о потенциальном мошенничестве [10]. Поведенческий анализ включает разработку подробных профилей пользователей на основе их транзакционных привычек.

Ключевые аспекты поведенческого анализа:

• структура расходов (Spending Patterns) – анализ обычных сумм покупок, частоты транзакций и типов магазинов, посещаемых пользователем;

• временные действия (Temporal Activities) – изучение времени и дней транзакций для выявления необычных действий, выходящих за рамки обычного поведения пользователя;

• географическое местоположение (Geographical Locations) – мониторинг общих мест транзакций для обнаружения аномалий, таких как неожиданные международные покупки;

• использование устройств (Device Usage) – отслеживание типичных устройств и каналов, используемых для транзакций, для выявления любых подозрительных изменений в моделях использования.

Установление базового уровня нормального поведения для каждого пользователя позволяет более точно выявлять отклонения, указывающие на потенциальное мошенничество. Профилирование предполагает создание модели нормального поведения для каждой учетной записи на основе исторических данных.

Математически этот процесс можно представить следующим образом:

*Вектор транзакции (T)*. Для каждой транзакции создается вектор ***T***, который включает в себя такие признаки, как сумма транзакции, время, местоположение и др.:

$$T_i = [x1, x2, ..., xn],$$

где $T_i$ – вектор транзакции для *i*-й транзакции; *x*1, *x*2, ..., *xn* – значения признака (feature).

*Средний вектор профиля (Profile Mean Vector) (μ)*. Вычисление среднего вектора для всех транзакций счета (account), чтобы представить типичное поведение:

$$\mu = \frac{1}{N}\sum_{i=1}^{N} T_i,$$

где ***N*** – общее количество транзакций.

*Mahalanobis Distance* (*D*). Использование *Mahalanobis Distance* для измерения того, насколько новая транзакция отклоняется от профиля:

$$D(T) = \sqrt{(T-\mu)^T \Sigma^{-1} (T-\mu)}$$

Если ***D(T)*** превышает определенный порог, транзакция помечается как потенциально мошенническая.

**Кластеризация** (Clustering) – это метод машинного обучения без присмотра, используемый для категоризации аккаунтов со схожими моделями поведения. Общие алгоритмы для этой цели включают кластеризацию k-средних и иерархическую кластеризацию (hierarchical clustering) [4]. Эти методы делят базу пользователей на кластеры на основе сходства транзакций. Например, частые путешественники могут образовывать один кластер, а ежедневные небольшие транзакции – другой.

Процесс кластеризации включает группировку похожих аккаунтов для выявления выбросов (outliers), которые могут указывать на мошенническую деятельность [5]. Обычно это достигается с помощью таких алгоритмов, как k-means или DBSCAN.

Упрощенный математический подход:

*Матрица признаков (features) транзакции (X)* – это матрица ***X***, где каждая строка представляет вектор транзакции:

$$X = \begin{bmatrix} T_1 \\ T_2 \\ \vdots \\ T_N \end{bmatrix}$$

*Кластеризация k-means* – применяется для разделения транзакций на ***k*** кластеров:

$$\min \sum_{i=1}^{k} \sum_{T \in C_i} \|T - \mu_i\|^2,$$

где $C_i$ – *i*-й кластер; $\mu_i$ является центроидом (centroid) кластера $C_i$.

*Cluster Centroids (μi)* – вычисление центроида для каждого кластера:

$$\mu_i = \frac{1}{|C_i|} \sum_{T \in C_i} T$$

где $|C_i|$ – количество транзакций в кластере $C_i$.

*Назначение кластера* – назначение каждой транзакции ближайшему кластеру на основе евклидова расстояния (Euclidean distance)

$$\text{Cluster}(T) = \arg\min_i \|T - \mu_i\|$$

**Нейронная сеть LSTM.** Вариант рекуррентной нейронной сети (RNN), известный как Long Short-Term Memory (LSTM), представляет собой мощную архитектурную структуру, способную фиксировать последовательные шаблоны и долгосрочные зависимости в данных временных рядов (time-series data), что делает ее хорошо подходящей для задач обнаружения мошенничества с банковскими картами [11]. Предлагаемый подход использует архитектуру нейронной сети LSTM для фиксации временных зависимостей и последовательных закономерностей, присущих данным транзакций по банковскими картам и поведению пользователей в каждом кластере.

Модель LSTM включает в себя ряд взаимосвязанных ячеек памяти, каждая из которых содержит *input gate*, *forget gate*, *output gate* и *cell state*. Эти ворота (gate) регулируют поток информации в ячейку и из нее, позволяя модели выборочно сохранять или удалять соответствующую информацию из входной последовательности. Этот механизм пропускания позволяет LSTM эффективно моделировать долгосрочные зависимости и смягчать проблему исчезновения градиента, обычно встречающуюся в традиционных RNN [11].

Вычисления, выполняемые ячейкой LSTM на каждом временном шаге ***t*** (time step), определяются следующим образом.

1. *Forget Gate* – определяет, какую долю предыдущего состояния ячейки *Ct*-1 сохранить:

$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] + b_f\right)$$

2. *Input Gate* – определяет новую информацию для хранения в cell state:

$$i_t = \sigma\left(W_i \cdot [h_{t-1}, x_t] + b_i\right)$$

3. *Candidate Cell State* – создает значения-кандидаты $C_t$ для добавления в *Cell State* ячейки:

$$\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$$

4. *Update Cell State* – обновляет состояния ячейки $C_t$ путем объединения *input gate* и *forget gate*:

$$C_t = f_t \cdot C_{t-1} + i_t \cdot \tilde{C}_t$$

5. *Output Gate* – определяет выход на текущем временном шаге:

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o)$$

6. *Hidden State* – вычисляет скрытое состояние *ht*, которое должно быть передано на следующий временной шаг:

$$h_t = o_t \cdot \tanh(C_t)$$

где

***xt*** – входной вектор на временном шаге *t*, представляющий данные транзакции и поведенческие характеристики;

***ht-1*** – скрытое состояние (*hidden state*) с предыдущего временного шага;

***Ct-1*** – состояние ячейки (*cell state*) с предыдущего временного шага (*time step*);

***Wf, Wi,WC, Wo*** – весовые матрицы (Weight Matrices) для вентилей (*gates*) забывания, ввода, ячейки и вывода соответственно;

***bf, bi, bc, bo*** – векторы смещения для соответствующих ворот;

***σ*** – сигмоидная функция активации (*activation function*).

Модель LSTM в предлагаемом подходе принимает в качестве входных данных предварительно обработанные данные транзакций и назначения кластеров, полученные на этапе кластеризации. Данные транзакций, а также поведенческие характеристики последовательно передаются в ячейки LSTM, что позволяет модели изучать временные зависимости и закономерности внутри каждого кластера.

Борьба с неравномерным распределением классов (*class imbalance*), преобладающим в наборах данных о мошенничестве, является критической задачей. Чтобы решить эту проблему, предлагаемый подход использует такие стратегии, как увеличение данных и взвешивание классов на этапе обучения модели. Увеличение данных (*data augmentation*) включает искусственное создание синтетических образцов, представляющих мошеннические транзакции, тем самым балансируя распределение классов, в то время взвешивание классов (*class weighting*) при расчете функции потерь дает то, что классу меньшинства (мошеннические транзакции) присваиваются более высокие веса. Механизм взвешивания гарантирует, что модель научится точно идентифицировать недостаточно представленный класс, смягчая смещение (*bias*), вызванное дисбалансом классов.

Целевой функцией, используемой для обучения модели LSTM, является взвешенная потеря перекрестной энтропии (*Weighted Cross-Entropy Loss*), которая определяется как

$$\mathcal{L}(\theta) = -\frac{1}{N}\sum_{i=1}^{N} w_i \left[y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i)\right]$$

где

***N*** – количество обучающих выборок;

***yi*** – истинная метка (0 для законного, 1 для мошеннического) ***i*-го** образца;

***ŷi*** – прогнозируемая вероятность того, что ***i***-й образец окажется поддельным;

***wi*** – вес класса, присвоенный ***i***-му образцу, с более высокими весами для класса меньшинства.

В процессе обучения модели LSTM используется алгоритм обратного распространения ошибки во времени (BPTT), который представляет собой специализированный вариант алгоритма обратного распространения ошибки, адаптированный для рекуррентных нейронных сетей. Методы оптимизации на основе градиента, такие как *Adam* или *RMSProp*, используются для обновления параметров модели на этапе обучения. Кроме того, используются методы регуляризации, в том числе *dropout* и *L2 regularization*, чтобы снизить риск переобучения, являющийся распространенной проблемой в сложных моделях нейронных сетей [12]. Стратегии регуляризации вводят контролируемые возмущения и наказывают за чрезмерную сложность, тем самым улучшая возможности обобщения модели и не позволяя ей запоминать обучающие данные.

Предлагаемая методология использует синергию моделей LSTM, поведенческого профилирования и методов кластеризации для эффективного выявления сложных закономерностей и временных зависимостей, присущих данным транзакций. Этот синергетический подход обеспечивает повышенную точность обнаружения мошенничества и общую производительность. Интегрируя эти взаимодополняющие компоненты, предлагаемая методология использует сильные стороны каждого метода, в результате чего создается надежная и комплексная структура для выявления мошеннических действий в данных транзакций.

*Результаты эксперимента*

**Конфигурация модели.** Предлагаемая модель сочетает в себе поведенческое профилирование, кластеризацию и сети с длинной краткосрочной памятью (LSTM). Ключевые гиперпараметры сети LSTM включали:

- количество слоев LSTM: 2;
- количество единиц на слой: 64;
- скорость обучения: 0,001;
- размер патча (Batch): 128;
- количество эпох (epochs): 50.

**Кластеризация.** Поведенческое профилирование было улучшено с помощью кластеризации K-means для группировки схожего поведения пользователей. Количество кластеров (K) определяли методом *elbow*, в результате чего (K = 5). Каждая последовательность транзакций была помечена соответствующим кластером, выступающая в качестве дополнительного признака (feature) для модели LSTM.

**Показатели эффективности.** Эффективность модели оценивалась с использованием стандартных метрик классификации:

- *Accuracy* – отношение правильно предсказанных экземпляров к общему количеству экземпляров;
- *Precision* – отношение правильного предсказания результатов к общему количеству предсказанных результатов;
- *Recall* – отношение правильно предсказанных положительных наблюдений ко всем наблюдениям в реальном классе;
- *F1-Score* – гармоническое среднее *Precision* и *Recall*;
- *AUC-ROC* – этот показатель измеряет способность модели различать классы.

**Полученные результаты.** Результаты эксперимента продемонстрировали эффективность комбинированного подхода при обнаружении мошеннических транзакций. Чтобы контекстуализировать эффективность предлагаемой модели, ее сравнивали с традиционными моделями и современными подходами (см. Таблицу).

*Таблица*

**Полученные результаты**

| Learning Algorithms | Accuracy | Precision | Recall | F1-score | AUC-ROC |
|---|---|---|---|---|---|
| Logistic Regression (LR) | 0,923 | 0,895 | 0,85 | 0,87 | 0,901 |
| Random Forest (RF) | 0,956 | 0,941 | 0,91 | 0,925 | 0.967 |
| Standard LSTM | 0,97 | 0,955 | 0,942 | 0,948 | 0,975 |
| Proposed Model | 0,984 | 0,972 | 0,968 | 0,97 | 0,991 |

*Источник:* составлено автором.

**Сравнительный анализ.** Чтобы оценить эффективность предложенной методологии, был проведен сравнительный анализ с традиционными методами машинного обучения, такими как логистическая регрессия и случайные леса, а также с моделями LSTM, которые не включали компоненты поведенческого профилирования и кластеризации. По всем показателям предложенный подход продемонстрировал отличную производительность, превзойдя традиционные методы и модели LSTM, в которых отсутствовали элементы поведенческого профилирования и кластеризации. Синергетическое сочетание поведенческого профилирования, кластеризации и моделей LSTM позволило предложенной методологии более эффективно различать сложные закономерности и временные зависимости, присущие данным транзакций. Такой комплексный подход способствовал повышению эффективности обнаружения мошенничества, подчеркивая преимущества интеграции этих взаимодополняющих методов.

**Исследование абляции.** Исследование абляции было проведено для оценки индивидуального влияния компонентов поведенческого профилирования и кластеризации на общую эффективность предлагаемого подхода. Результаты показали, что оба компонента сыграли решающую роль в расширении возможностей модели LSTM по обнаружению мошенничества. Когда модель LSTM обучалась без компонента поведенческого профилирования, наблюдалось заметное снижение производительности: метрика AUC-ROC снизилась до 0,968, а показатель F1 для мошеннического класса упал до 92,1 %. Аналогичным образом, когда компонент кластеризации был исключен из процесса обучения, показатель AUC-ROC составлял 0,974, а показатель F1 для мошеннического класса составлял 93,8 %. Эти результаты подчеркивают важность включения в предлагаемый подход как элементов поведенческого профилирования, так и элементов кластеризации, поскольку это способствует повышению эффективности обнаружения мошенничества.

**Вычислительная эффективность.** Также была проведена оценка вычислительных требований с учетом времени, необходимого для поведенческого профилирования, кластеризации, обучения и вывода модели LSTM. Результаты показали, что предложенный подход демонстрирует вычислительную эффективность, а время обработки считается приемлемым для систем обнаружения мошенничества в реальном времени в практических приложениях. В совокупности экспериментальные результаты подчеркивают эффективность предложенной методологии в оптимизации обнаружения мошенничества с банковскими картами за счет синергетической интеграции моделей поведенческого профилирования, кластеризации и LSTM. Этот подход продемонстрировал отличную производительность, достигнув высокого уровня точности, полноты и AUC-ROC, превосходя традиционные методы и модели LSTM, которые не включали компоненты поведенческо-

го профилирования и кластеризации. Примечательно, что такая повышенная производительность была достигнута при сохранении вычислительной эффективности, что является решающим фактором для практического развертывания в реальных сценариях.

*Заключение*

Данная исследовательская работа представила инновационный подход к оптимизации обнаружения мошенничества с банковскими картами путем синергетического сочетания моделей поведенческого профилирования, кластеризации и LSTM. Предлагаемая методология использовала сильные стороны этих методов для решения проблем, связанных с обнаружением мошенничества, включая дисбаланс классов, асимметрию данных (data skewness) и временные зависимости в последовательностях транзакций. Экспериментальные результаты продемонстрировали эффективность предложенного подхода, обеспечивающего высокий уровень *Accuracy*, F1-score и AUC-ROC при выявлении мошеннических транзакций. Интеграция поведенческого профилирования, кластеризации и моделей LSTM позволила этому подходу эффективно фиксировать сложные закономерности и временные зависимости в данных транзакций, превосходя традиционные методы машинного обучения и модели LSTM, которые не включали компоненты поведенческого профилирования и кластеризации. Ключевой вклад этой работы – включение поведенческого профилирования для обнаружения отклонений от типичного поведения пользователя, кластеризацию аккаунта на основе их поведенческих профилей и использование моделей LSTM для изучения последовательных шаблонов и временных зависимостей внутри каждого кластера. Кроме того, предложенный подход эффективно решает проблему дисбаланса классов посредством увеличения данных и методов взвешивания классов.

Несмотря на то, что предложенный подход дал многообещающие результаты, существуют возможности для дальнейшего совершенствования и будущих направлений исследований, таких как включение дополнительных источников данных, изучение ансамблевых методов, а также изучение онлайн-обучения и дополнительных обновлений моделей для адаптации к развивающимся моделям мошенничества в режиме реального времени. В целом это исследование демонстрирует потенциал сочетания передовых методов машинного обучения со знаниями в конкретной области для оптимизации обнаружения мошенничества с банковскими картами, тем самым повышая безопасность и целостность финансовых транзакций, одновременно сводя к минимуму потери и сохраняя доверие клиентов.

## Литература / References

1. Rushin G., Stancil C., Sun M., Adams S., Beling P. (2017) Horse race analysis in credit card fraud – deep learning, logistic regression, and Gradient Boosted Tree. In: *2017 Systems and Information Engineering Design Symposium (SIEDS)*. Charlottesville, VA, USA, April 28, 2017. Pp. 117–121, DOI: 10.1109/SIEDS.2017.7937700.

2. Dhankhad S., Mohammed E., Far B. (2018) Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study. In: *2018 IEEE International Conference on Information Reuse and Integration (IRI)*. Salt Lake City, UT, USA, July 06–09, 2018. Pp. 122–125. DOI: 10.1109/IRI.2018.00025

3. Roy A., Sun J., Mahoney R., Alonzi L., Adams S., Beling P. Deep learning detecting fraud in credit card transactions. In: *2018 Systems and Information Engineering Design Symposium (SIEDS)*. Charlottesville, VA, USA, April 27, 2018. Pp. 129–134, DOI: 10.1109/SIEDS.2018.8374722

4. Viji D., Kothbul S., Banu Z. (2018). An Improved Credit Card Fraud Detection Using K-Means Clustering Algorithm. *Semantic Scholar*. Corpus ID 212460596. URL: https://www.semanticscholar.org/paper/An-Improved-Credit-Card-Fraud-Detection-Using-Viji-Kothbul/18d503a91615413f6eb87e12f36e2d0873c038ac

5. Vaishali (2014) Detecting credit card fraud using a cluster approach. *International Journal of Computer Applications.* Vol. 98. No. 3. Pp. 29–32. URL: https://research.ijcaonline.org/volume98/number3/pxc3897225.pdf (accessed 17.02.2024).

6. Huang Z.X. (1997) Clustering large data sets with mixed numeric and categorical values. In: *Proceedings of the First Pacific Asian Conference on Knowledge Discovery and Data Mining*. Pp. 21–34. URL: https://typeset.io/papers/clustering-large-data-sets-with-mixed-numeric-and-hexk053uky?ysclid=lxwe077xp7375330157 (accessed 17.02.2024).

7. Mead A., Lewris T., Prasanth S., Adams S., Alonzi P., Beling P. (2018) Detecting fraud in adversarial environments: A reinforcement learning approach. In: *2018 Systems and Information Engineering Design Symposium (SIEDS)*. Charlottesville, VA, USA, April 27, 2018. Pp. 118–122, DOI: 10.1109/SIEDS.2018.8374720

8. Bhattacharyya S., Jha S., Tharakunnel K., Westland J. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*. Vol. 50. Pp. 602–613. DOI: 10.1016/j.dss.2010.08.008

9. Bahnsen A.C., Aouada D., Stojanovic A., Ottersten B. (2016). Feature Engineering Strategies for Credit Card Fraud Detection. *Expert Systems with Applications*. Vol. 51. Pp. 134–142. DOI: 10.1016/j.eswa.2015.12.030

10. Bolton R.J., Hand D.J. (2002). Unsupervised Profiling Methods for Fraud Detection. *Semantic Scholar.* Corpus ID 14365948. URL: https://www.semanticscholar.org/paper/Unsupervised-Profiling-Methods-for-Fraud-Detection-Bolton-Hand/5b640c367ae9cc4bd072006b05a3ed7c2d5f496d (accessed 17.02.2024).

11. Benchaji I., Douzi S., El Ouahidi B. (2021) Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks. *Journal of Advances in Information Technology*. Vol. 12. No. 2. Pp. 113–118. DOI: 10.12720/jait.12.2.113-118

12. Dorronsoro J.R., Ginel F., Sgnchez C., Cruz C.S. (1997) Neural fraud detection in credit card operations. In: *IEEE Transactions on Neural Networks*. Vol. 8. No. 4. Pp. 827–834. DOI: 10.1109/72.595879