Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский университет «Высшая школа экономики»

На правах рукописи

Воробьев Иван Александрович

Исследования по разработке методов противодействия мошенничеству в финансовых организациях с применением машинного обучения

РЕЗЮМЕ ДИССЕРТАЦИ

на соискание ученой степени кандидата технических наук

Научный руководитель:
кандидат технических наук, доцент
Лось Алексей Борисович

Москва — 2024

Глоссарий

Фрод-мониторинг – это автоматизированная система анализа транзакций, направленная на предотвращение мошеннической деятельности и защиту средств и личных данных пользователей.

Эффективность метода обнаружения мошенничества – набор специальных характеристик, позволяющих оценить способность метода предотвращать мошеннические действия. В рамках исследования данный термин может применяться к конкретному алгоритму или системе фрод-мониторинга.

Машинное обучение – методы, основанные на выявлении эмпирических закономерностей в данных. Для разработки таких методов используются средства математической статистики, численных методов, математического анализа, методов оптимизации, теории вероятностей и теории графов.

Признак – это характеристика или атрибут, который описывает объект или данные. Признаки используются для представления информации о объектах и служат основой для обучения моделей машинного обучения.

Классификация данных — это процесс присвоения объектам различных категорий или классов на основе определённых признаков.

Обогащение данных – это процесс добавления дополнительной информации или атрибутов к существующим данным. Этот процесс может включать в себя использование внешних источников данных, анализ и преобразование данных.

Банковская операция – это финансовая транзакция, которая происходит между банком и его клиентами. Она включает в себя различные виды действий, такие как переводы денежных средств, открытие и закрытие счетов, выдачу кредитов, погашение долгов и прочее.

Страховая претензия – это запрос или требование, предъявляемое страхователем к страховой компании в случае наступления страхового случая. В рамках страховой претензии страхователь обращается к страховой компании с целью получить возмещение убытков, покрытие расходов или выплату страхового возмещения в соответствии с условиями договора страхования.

1. Введение

1.1. Постановка проблемы и актуальность исследования

В диссертационном исследовании рассматривается задача повышения устойчивости финансовых организаций к атакам мошенников, которые направлены как на активы клиентов, так и на активы самих организаций. Такие атаки называют финансовым мошенничеством или просто мошенничеством. В большинстве случаев они проводятся злоумышленниками с целью получения денежных средств клиентов или организаций незаконным путем. Как подчеркивается в [1], финансовое мошенничество является существенной проблемой, так как наносит ущерб, как экономике организаций, так и экономике государства, поэтому минимизация последствий от деятельности мошенников является одной из приоритетных задач основных участников финансового сектора – банков и страховых компаний.

Развитие технологий хранения и обработки данных позволило финансовым организациям вести учет транзакций, данных клиентов и другую информацию во внутренних базах данных. Стало возможным не только накапливать эту информацию, но и использовать технологии больших данных и искусственного интеллекта (ИИ) для автоматического принятия решений в различных процессах, включая обнаружение фактов мошенничества [2]. При этом ретроспективный анализ событий на основе данных стал широко применяться в области информационной безопасности [3]. Большинство финансовых институтов стали применять автоматизированные системы для анализа транзакций, так называемые, системы фрод-мониторинга. Их основное назначение – выявление противоправных действий против клиентов или самих организаций.

В исследовании [4] в разделе 6 финансовое мошенничество классифицируется на несколько типов в зависимости от отрасли: банковское, страховое, телекоммуникационное и т.д. При этом каждая отрасль имеет подтипы в зависимости от способа совершения мошенничества. В предлагаемом исследовании рассматривается возможность применения методов машинного обучения для повышения эффективности борьбы с мошенничеством в двух подтипах – банковском с использованием карт в электронной коммерции и в автостраховании.

Основным **объектом исследования** являются методы машинного обучения, адаптация и встраивание которых в процессы противодействия мошенничеству, позволят финансовым организациями быть более устойчивыми к рискам, связанным с мошенническими действиями.

Стратегии злоумышленников в исследуемых подтипах различны, но проблемы применения методов машинного обучения сходны – это несбалансированность классов мошеннических транзакций против

легитимных, рассмотренная, например, в исследовании [5] и низкая интерпретируемость результатов моделирования при использовании данных методов [6].

При этом дополнительную сложность обнаружения мошенничества вносит и само поведение мошенников. С течением времени, в попытках обойти систему безопасности банка или страховой компании, поведение злоумышленников меняется, и реакция экспертов финансовых организаций не всегда успевает за этими изменениями. С другой стороны, эксперты безопасности могут иметь собственные предубеждения в части определения признаков мошенничества. Например, эксперты могут оценить один и тот же случай мошенничества по-разному. Поэтому легитимные инциденты, на деле могут оказаться мошенническими, так как вследствие незнания новой схемы эксперт допускает ошибку. По этим причинам в данных о фактах мошенничества, к которым применяются методы машинного обучения, может возникнуть так называемый «дрейф концепции» (concept drift) [7], что приводит к неустойчивости моделей машинного обучения во времени.

Наличие данных проблем и существенные потери от угроз, связанных с деятельностью злоумышленников, подчеркивает **актуальность** задачи повышения эффективности алгоритмов, создаваемых для предотвращения мошенничества.

1.2. Цель и задачи диссертационной работы

Основной **целью** предлагаемого исследования является разработка метода, позволяющего более эффективно выявлять случаи мошенничества в финансовых организациях, за счет использования машинного обучения и транзакционных данных.

Для достижения цели были сформулированы следующие **задачи**:

1. Разработка метода подготовки данных о фактах мошенничества, позволяющего сократить негативное влияние на качества алгоритмов машинного обучения таких факторов, как изменение сценариев схем мошенничества и субъективная экспертная оценка.
2. Разработка новых атрибутов транзакций, оказывающих положительное влияние на эффективность выявления мошенничества.
3. Разработка алгоритма, позволяющего повысить точность системы фрод-мониторинга за счет автоматической генерации правил принятия решения.
4. Проведение экспериментов на реальных данных, позволяющих оценить эффективность выявления мошенничества, достигнутую за счет предложенных методов.

1.3. Степень разработанности темы исследования

В период 1980 – 1990 гг. научные работы, посвящённые выявлению мошенничества, ограничивались применением простых статистических и эконометрических методов [8–10]. Сегодня все чаще при решении таких-то задач применяется искусственный интеллект, в частности методы машинного обучения. Методы обнаружения мошенничества является объектом интереса, как коммерческих компаний, так и научного сообщества. Если за 2015 г. по теме было опубликовано 16 тыс. научных работ, то в 2021 г. – в 1,5 раза больше.

Алгоритмы выявления фактов мошенничества можно разделить на экспертные и статистические. В первом случае мошенничество выявляется на основе правил, созданных экспертами с учётом анализа типичного поведения мошенников в ручном режиме. Во втором случае для классификации операций на мошеннические и легитимные используются статистические методы, включая модели машинного обучения

Статистические алгоритмы, согласно [11], делятся на задачи классификации, задачи кластеризации и анализ графов. Первые помогают разделять транзакции на мошеннические и легитимные даже в том случае, если мошенники маскируют свою деятельность под легитимную деятельность. Преимущество вторых алгоритмов, которые, однако, хуже распознают замаскированные случаи, заключается в возможности обнаружения новых событий, указывающих на факты мошенничества, которые ещё не встречались в исторических данных. Анализ графов позволяет учесть взаимосвязи между объектами в выборке. Три вида статистических алгоритмов фокусируются на различных аспектах мошенничества и являются взаимодополняющими.

Задача выявления мошенничества с точки зрения машинного обучения – это задача классификации с двумя непересекающимися классами [12]. В диссертационном исследовании основной фокус направлен на повышении качества классификации, путем решения проблемы несбалансированности классов и изменчивости поведения мошенников, а также создании нового признакового описания операций (для банковского фрод-мониторинга) и претензий (для страхового фрод-мониторинга) из существующих данных.

Эффективность классификации зависит от качества данных и признаков [13,14]. В работе [13], где сравниваются результаты классификации ряда методов на различных наборах данных, все методы теряют в эффективности на данных с большим количеством нечисловых признаков. С помощью создания нового признакового описания в исследовании [14] авторы добились большего роста эффективности, чем с помощью перехода от простых и интерпретируемых статистических моделей к более сложным.

Часть исследователей придерживается мнения о более высокой эффективности статистических алгоритмов. Например, в исследовании [15] проводится сравнение эффективности процедур выявления мошенничества, основанных на экспертных правилах, и эффективности нейронной сети, разработанной авторами. Результаты показывают, что нейронная сеть превосходит экспертные правила: она обнаруживает мошенничество на порядок больше и с более высокой точностью.

Несмотря на это, указанные методы могут использоваться как взаимодополняющие. Так, в работе [16] комбинирование нейронной сети, нацеленной на выявление аномалий, и экспертного подхода даёт результаты лучше, чем эти два подхода по-отдельности.

В страховой отрасли выявление мошенничества является сложной задачей, как с использованием экспертных подходов, так и с помощью статистических методов, включая машинное обучение. Это подчеркивается во многих работах, включая исследование [17]. Дополнительную проблему создает ограниченный доступ к данным о мошенничестве. Как отмечается в [18], доступен только один полноценный набор данных для исследования мошенничества методами машинного обучения. Такая ситуация затрудняет прогресс в области выявления мошенничества и приводит к низким показателям классификации.

Для улучшения классификации используют различные подходы. Например, в [19] применяется оценка, которая может изменяться в зависимости от срока действия претензии и использует обработку естественного языка. В [20] авторы воспользовались тем, что мошенники могут искажать анкетные данные и, при выявлении такой аномалии, страховая компания может достичь дополнительного эффекта в уменьшении уровня мошенничества. Кроме того, исследователи стремятся уменьшить количество признаков, используемых для классификации и повысить интерпретируемость результатов [21]. В работе [22] авторы улучшают показатели выявления мошенничества в автостраховании, применяя генетические алгоритмы. В [23] исследована проблема дисбаланса классов при выявлении мошенничества в автомобильном страховании.

Сравнительная таблица результатов исследования, полученная в разные годы для задачи выявления мошенничества в страховании, представлена в [24].

В настоящей научной работе предлагается продолжить исследования, направленные на улучшение качества классификации в задаче выявления мошенничества в банковской и страховой сфере. При этом рассматривается комплекс методов, применяемых в процессе принятия решения по операциям или претензиям на предмет мошенничества.

1.4. Научная новизна исследования

1. Впервые предлагается метод повышения эффективности в задачах выявления мошенничества за счет корректировки целевого класса с помощью нейронной сети, что позволяет сбалансировать данные для использования методов машинного обучения и устранить проблемы дрейфа концепции.
2. Предлагается новый способ комбинирования традиционного экспертного подхода и машинного обучения, который повышает эффективность системы фрод-мониторинга. Метод заключается в использовании составных частей правил, созданных экспертами, для генерации новых, более эффективных правил с помощью машинного обучения.
3. Предложены методы создания новых признаков операций и претензий, улучшающих качество выявления мошенничества.

2. Основные результаты

2.1. Основные результаты, выносимые на защиту

1. Разработан метод, решающий проблему несбалансированности классов при использовании методов машинного обучения и одновременно устраняющий дрейф концепции в данных, возникающий вследствие изменения мошеннических схем или некорректной разметки данных. Данный подход, позволяет улучшить разделяющую способность классификатора путем улучшения качества данных для обучения. Детальное описание метода и полученные результаты опубликованы в [25].
2. Предложен подход, повышающий эффективность системы фрод-мониторинга за счет создания новых атрибутов операций и претензий. Для банковской сферы – операции обогащаются за счет интеграции истории операций покупок клиентов в обучающие данные для оценки переводов между клиентами. Претензии обогащаются признаками, полученными из графа связей между участниками страховых событий. Описание подходов для создания новых признаков опубликованы в [26].
3. Разработан метод, основанный на подходах машинного обучения, позволяющий финансовым организациям сократить ложные срабатывания системы фрод-мониторинга за счет внедрения автоматически созданных алгоритмов принятия решения при оценке операций. Метод опубликован в работе [27].
4. Разработаны методики проведения экспериментов, позволяющие оценить эффективность предложенных методов. Проведена серия экспериментов, результаты которых демонстрируют повышение качества выявления мошенничества в финансовой сфере при использовании разработанных подходов.

2.2. Личный вклад автора

В ходе диссертационного исследования автором был разработан подход, который позволяет повысить эффективность применения методов машинного обучения путем корректировки экспертной разметки данных.

Кроме того, предложен процесс генерации алгоритмов для принятия решения, представляющий собой совместное применение экспертного и статистического подходов и позволяющий повысить точность классификации мошенничества без ущерба для интерпретируемости. В рамках исследования также был предложен алгоритм построения графа претензий в страховании и способ извлечения новых данных из него для повышения эффективности применения методов машинного обучения. В исследовании было показано, что обогащение данных о банковских переводах сведениями из истории покупок клиента позволяет улучшить качество классификации при использовании методов машинного обучения.

Проведена серия экспериментов, результаты которых показали, что предложенные подходы имеют потенциал для повышения эффективности применения методов машинного обучения и могут быть полезным инструментом в сфере борьбы с мошенничеством, где требуется точная классификация данных.

3. Публикации и апробация работы

3.1. Публикации повышенного уровня

1. Воробьев И. А., Кривицкая А. Reducing False Positives in Bank Anti-fraud Systems Based on Rule Induction in Distributed Tree-based Models // Computers and Security. 2022. Vol. 120, http://doi.org/10.1016/j.cose.2022.102786 (**Scopus, Q1**)
2. Воробьев И. А., Fraud risk assessment in car insurance using claims graph features in machine learning // Expert Systems with Applications. 2024. Vol. 251, http://doi.org/10.1016/j.eswa.2024.124109 (**Scopus, Q1**)

3.2. Публикации стандартного уровня

1. Воробьев И. А. Методы машинного обучения в задаче оценки риска мошенничества в автостраховании // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2024 (**Scopus**)
2. Феста Ю. Ю., Воробьев И. А. A Hybrid Machine Learning Framework for E-commerce Fraud Detection // Model Assisted Statistics and Applications. 2022. Vol. 17. No. 1. P. 41-49, http://doi.org/10.3233/MAS-220006, (**Scopus**)

3.3. Доклады на конференциях и семинарах

1. Межвузовской научно-технической конференции студентов, аспирантов и молодых специалистов имени Е.В. Арменского (Москва). Доклад: Исследование применения методов машинного обучения в задаче выявления мошеннических действий в отношении клиентов банка при подтверждении операции, МИЭМ НИУ ВШЭ, 2023
2. XII Конгресс молодых ученых ИТМО (Санкт-Петербург). Доклад: Интерпретируемость моделей машинного обучения и проблема дисбаланса классов в задачах снижения рисков кредитно-финансовых организаций, 2023
3. XII Международная научно-практическая конференция «Математическое и компьютерное моделирование в экономике, страховании и управлении рисками» (Саратов). Доклад: Методы машинного обучения в задаче оценки риска мошенничества в автостраховании, 2023
4. Международная конференция International Conference on Data Analytics and Computational Techniques, ICDACT-21. Доклад: A Hybrid Machine Learning Framework for E-commerce Fraud Detection, 2021
5. Международный конгресс "Современные проблемы компьютерных и информационных наук", VI Международная научная конференция Конвергентные когнитивно-информационные технологии (Москва). Доклад: The application of artificial intelligence for improving the efficiency of transactional fraudmonitoring, 2021

6. XI Международный форум «Борьба с мошенничеством с сфере высоких технологий. Antifraud Russia – 2020» (Москва). Доклад: Антифрод в эквайринге Сбера, 2020

4. Содержание работы

Результаты диссертационного исследования представлены в следующих разделах:

1. Использование методов машинного обучения в задачах выявления мошенничества и подходы к оценке их эффективности.
2. Архитектуры систем фрод-мониторинга и потенциальные зоны их улучшения.
3. Подготовка данных для обучения классификаторов мошеннических операций и претензий.
4. Генерация новых алгоритмов для повышения качества системы фрод-мониторинга.
5. Методика проведения экспериментов и исследований.

4.1. Использование методов машинного обучения в задачах выявления мошенничества и подходы к оценке их эффективности

Под мошенничеством понимается ситуация кражи денежных средств клиента или финансовой организации профессиональными мошенниками.

Мошенничество, согласно [11], обладает следующими специфическими чертами:

1) в сравнении с частотой легитимных операций, мошенничества случается редко;
2) мошенничество тщательно продумано и спланировано;
3) мошенники пытаются замаскировать свою деятельность, выдав её за легитимную;
4) поведение мошенников меняется во времени;
5) мошенники часто работают организованными группировками.

Оценка операции или претензии (далее транзакции) на мошенничество методами машинного обучения осуществляется с помощью исторических данных. Каждая транзакции обладает своим признаковым описанием и, если она обрабатывалась экспертом или у клиента запрашивалось подтверждение о легитимности, имеет ответ на вопрос о наличии в ней признаков мошенничества. Тогда задачу выявления мошенничества можно свести к задаче обучения по прецедентам [12]. В частности, будем рассматривать задачу классификации с двумя непересекающимися классами. При этом найденная решающая функция (далее модель или классификатор) будет использоваться для оценки конкретной транзакции на факт мошенничества с помощью ее признакового описания (далее признаки).

Обозначим множество оцениваемых транзакций X, множество ответов на вопрос «является ли транзакция мошеннической?» – Y. Пары «транзакция-ответ» (x_i, y_i) будем называть прецедентами. Пусть на конечном подмножестве транзакций $\{x_1, \dots, x_l\} \subset X$ известны значения некоторой функции $y^* : X \to Y$, тогда $y_i = y^*(x_i)$. Функцию y^* будем

называть целевой функцией, совокупность пар $X^l = (x_i, y_i)_{i=1}^l$ – обучающей выборкой.

Задача обучения по прецедентам заключается в том, чтобы по выборке X^l восстановить зависимость y^*, т.е. построить решающую функцию $a: X \to Y$, которая приближала бы целевую функцию $y^*(x)$, не только на транзакциях X^l, но и на всем множестве X.

Решающую функцию a, также будем называть алгоритмом, в некоторых случаях классификатором, когда ее роль в оценки транзакции будет заключаться в классификации транзакции на категории мошенническая или легитимная. Для практического применения построенный алгоритм a должен обеспечивать эффективную компьютерную реализацию, так как предполагается, что финансовые организации будут использовать его для анализа своих транзакционных данных, хранящихся на их серверах.

Атрибуты транзакций x, получаемые из процессов финансовых организаций (например, сумма операции, возраст клиента, сумма страховой выплаты и пр.), с точки зрения обучения по прецедентам являются признаком и формально являются отображением $f: X \to D_f$, где D_f – множество допустимых значения признака.

Различают несколько типов признаков, в зависимости от природы данных.

- $D_f = \{0, 1\}$ – бинарный признак;
- $D_f = \mathbb{R}$ – количественный признак;
- D_f – конечное множество, номинальный или категориальный признак.

В случае, если в данных все признаки одинаковые, то $D_{f_1} = \cdots = D_{f_n}$ и такие данные называются однородными, иначе разнородными. На практике данные транзакций, хранящиеся в финансовых организациях разнородные и содержат все типы признаков. В данном исследовании все категориальные признаки будут преобразоваться в бинарные, общеизвестными алгоритмами машинного обучения.

Пусть имеется набор признаков $f_1, \dots, f_n$. Вектор $(f_1(x), \dots, f_n(x))$, называют признаковым пространством транзакции $x \in X$. Совокупность признаковых описаний всех объектов выборки X^l, записанную в виде таблицы размера $l \times n$ называют матрицей объектов–признаков:

$$F = \| f_j(x_i) \|_{l \times n} = \begin{pmatrix} f_1(x_1) & \dots & f_n(x_1) \\ \dots & \dots & \dots \\ f_1(x_l) & \dots & f_n(x_l) \end{pmatrix} \quad (1)$$

Пример описания транзакций для задачи выявления мошенничества представлен в Таблице 1.

Таблица 1

Признаки операций

Date and time of transaction	Card operation type	Type of service	Shop MCC	Transaction amount	Fraud
01.02.2024 13:03	Purchase via pos	Car service	5533	26720,00	0
01.02.2024 13:10	Purchase via pos	Car service	5533	1500,00	0
02.02.2024 14:12	Purchase via pos	Gas station	5541	2202,78	0
08.02.2024 10:00	Purchase via pos	Pet Shop	5995	7399,00	0
10.02.2024 23:00	Purchase via ecom	P2P	4900	4500,00	1

В данном исследовании множество допустимых ответов $Y = \{0, 1\}$, что является задачей классификации на двух непересекающихся классов. В общем случае, если $Y = \{1, \dots, M\}$, множество транзакций X может разбиваться на M непересекающихся классов $K_y = \{x \in X: y^*(x) = y\}$. Алгоритм $a(x)$ дает ответ на вопрос «какому классу принадлежит x?», а в задаче выявления мошенничества будет получен ответ на вопрос является транзакция мошеннической или нет.

Согласно [12], моделью алгоритмов называется параметрическое семейство отображений $A = \{g(x, \theta) \mid \theta \in \Theta\}$, где $g: X \times \Theta \to Y$ некоторая фиксированная функция, множество допустимых значений параметра θ, называемое пространством параметров.

Диссертационное исследование направлено на поиск оптимальных параметров модели для классификации транзакций, а также на встраивание полученных моделей на различных этапах процесса обнаружения мошенничества в финансовой организации. В настоящее время существует множество различных подходов и техник для поиска алгоритма и оптимальных параметров (гиперпараметров), которые в итоге позволяют получить необходимый алгоритм $a(x)$ для использования в процессе принятия решений в различных задачах. Совокупность данных подходов также называется методами машинного обучения (далее ML). В данном исследование для внедрения в процесс выявления мошенничества выбраны следующие известные методы ML.

Decision Tree[1] (DT) наиболее интерпретируемый и простой инструмент, используемый в машинном обучении. Результат моделирования можно представить в виде древовидной структуры, из которой легко выделить простое правило для принятия решения.

В качестве базового алгоритма для классификации выбран Random Forest [2] (RF), показывающий наилучшие результаты в исследованиях,

[1] https://scikit-learn.org/stable/modules/generated/sklearn.tree.DecisionTreeClassifier.html
[2] https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html

посвященных выявлению мошенничества [28]. Метод заключается в использовании ансамбля алгоритмов Decision Tree, каждое из которых может и не давать высокого качества классификации, но за счет их большого количества можно достигнуть лучшего результата. Выбор в его пользу в данном исследовании обусловлен низкой чувствительностью к размеру признакового пространства, а также высоким качеством классификации при обучении на разнородных данных с категориальными и количественными признаками.

Для построения алгоритма на данных с небольшим количеством признаков выбран многослойный перцептрон [3] (MLP). Этот метод также показывает высокие результаты в исследованиях в сфере противодействия мошенничеству. При его использовании, за счет включения скрытых слоев, появляется возможность аппроксимировать нелинейную функцию для классификации.

Поиск лучшей модели из пространства параметров θ осуществляется с помощью инструмента GridSearchCV [4], который оптимизирует гиперпараметры путем перекрестного поиска по сетке параметров.

Для оценки результатов эксперимента были выбраны традиционные метрики, которые обычно используются в задачах выявления мошенничества. В данном исследовании рассматривается классификация на два непересекающихся класса $Y = \{0, 1\}$. Пусть $y_i \in \mathbb{R}$ будет ответ обученной модели для i-ой транзакции. Далее, для принятия решения по транзакции является ли она мошеннической или легитимной будем использовать порог th, который преобразует значения y_i в непересекающиеся классы $y_i^p = [y_i > th]$[5].

С точки зрения статистики, при классификации принимается решение о нулевой гипотезе H_0 о том, что транзакция относится к классу 1 и альтернативной H_1, что транзакция относится к классу 0. Решения, которые принимаются, могут содержать два вида ошибок: ложноположительную (или ошибка первого рода), когда легитимная транзакция классифицируется как мошенническая, и ложноотрицательную (или ошибка второго рода), когда мошенническая транзакция классифицируется как легитимная. Изменение порога позволяет регулировать компромисс между этими двумя типами ошибок, так как с ростом вероятности ошибки первого рода обычно уменьшается вероятность ошибки второго рода, и наоборот.

Порог th выбирается в зависимости от решаемой задачи и при его фиксации можно построить Таблицу 2 (confusion matrix или матрица ошибок):

---

[3] https://scikit-learn.org/stable/modules/generated/sklearn.neural_network.MLPClassifier.html
[4] https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.GridSearchCV.html
[5] Квадратные скобки переводят логическое значение в число по правилу [ложь] = 0, [истина] = 1.

Таблица 2

Матрица ошибок

		Верная гипотеза	
		H_0	H_1
Результат принятия решения	H_0	TP, H_0 верно принята	FP, H_0 неверно принята (ошибка второго рода)
	H_1	FN, H_0 неверно отвергнута (ошибка первого рода)	TN, H_0 верно отвергнута

В традиционных терминах машинного обучения данные реализации гипотез можно сформулировать следующим способом:

- TP (True positive) – мошенническая транзакция идентифицирована корректно,
- FP (False positive) – легитимная транзакция идентифицирована как мошенническая,
- TN (True negative) – легитимная транзакция идентифицирована корректно,
- FN (False negative) – мошенническая транзакция идентифицирована как легитимная.

Также для оценки качества классификации будем использовать следующие характеристики:

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

$$Precision = \frac{TP}{TP+FP} \quad (3)$$

$$Specificity = \frac{TN}{TN+FP} \quad (4)$$

Recall (полнота) позволит оценить долю мошенничества, выявленную классификатором по отношению ко всем мошенническим транзакциям; Precision (точность) – вероятность того, что подозреваемая классификатором транзакция действительно мошенническая. Specificity (специфичность) – доля легитимных операций, правильно выявленных классификатором.

Также в исследовании будет использоваться специальная характеристика ROC-кривая [29], которая показывает, что происходит с

числом ошибок обоих типов, если изменяется th. По оси X откладывается доля ошибочных положительных классификаций (false positive rate, FPR), вычисленные для каждого порогового значения:

$$FPR = \frac{\sum_i [y_i^p = 1]}{\sum_i [y_i = 1]} \quad (5)$$

По оси Y откладывается доля правильных положительных классификаций (true positive rate, TPR), также вычисленные для каждого порогового значения:

$$TPR = \frac{\sum_i [y_i^p = 1]}{\sum_i [y_i = 0]} \quad (6)$$

Пример построения ROC-кривой[6] для двух разных методов машинного обучения представлен на Рис. 1.

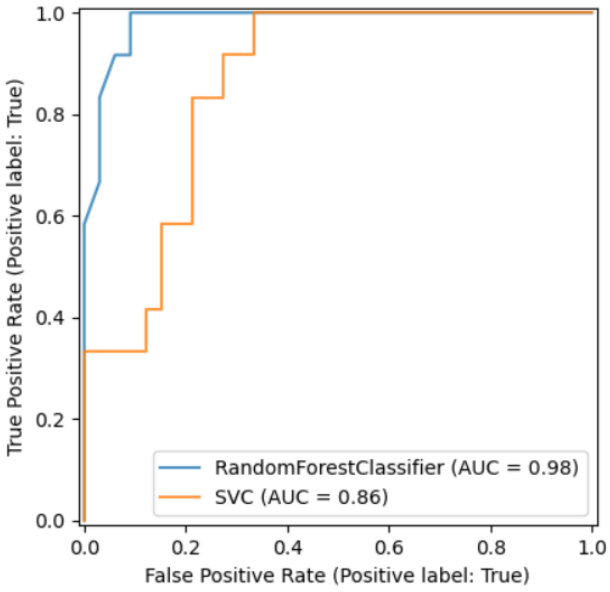


Рис. 1. Пример сравнения ROC-кривых для двух разных методов

Чем выше проходит ROC-кривая, тем выше качество классификации. Идеальная ROC-кривая проходит через левый верхний угол – точку (0, 1). Наихудший алгоритм соответствует диагональной прямой, соединяющей точки (0, 0) и (1, 1). В роли общей характеристики качества классификации, выступает площадь под ROC-кривой (area under curve, AUC).

При работе с сильно несбалансированными данными, как в случае с обнаружением мошенничества, AUC (и кривые ROC) могут быть слишком оптимистичными. Поэтому предлагается использовать еще одну характеристику для оценки классификаторов – кривую точности и полноты (PR-кривая). Пример[7] построения представлен на Рис. 2.

[6] https://scikit-learn.org/stable/auto_examples/miscellaneous/plot_roc_curve_visualization_api.html
[7] https://scikit-learn.org/stable/auto_examples/miscellaneous/plot_display_object_visualization.html

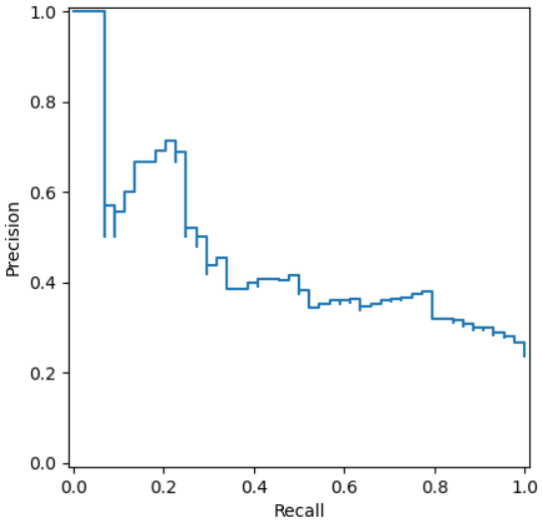


Рис. 2. Пример построения PR-кривой

Площадь под данной кривой (AUPRC) также будет использована в качестве количественной характеристики для оценки модели. Как следует из названия, кривая точности-полноты отображает точность (ось Y) в зависимости от полноты (ось X) для каждого возможного порога. AUPRC также представляет собой значение от 0 до 1.

В следующем разделе будет представлен краткий обзор систем фрод-мониторинга в финансовых организациях и их основные компоненты, в которых предполагается использование методов машинного обучения.

4.2. Архитектура систем фрод-мониторинга и потенциальные зоны их улучшения

В диссертационном исследовании рассматривается два процесса, где финансовые организации применяют инструменты для обнаружения мошенничества, основанные на данных. Эти процессы включают проведение банковских операций клиентами и рассмотрение страховых претензий.

На Рис. 3 схематично представлен путь банковского платежа через систему фрод-мониторинга.

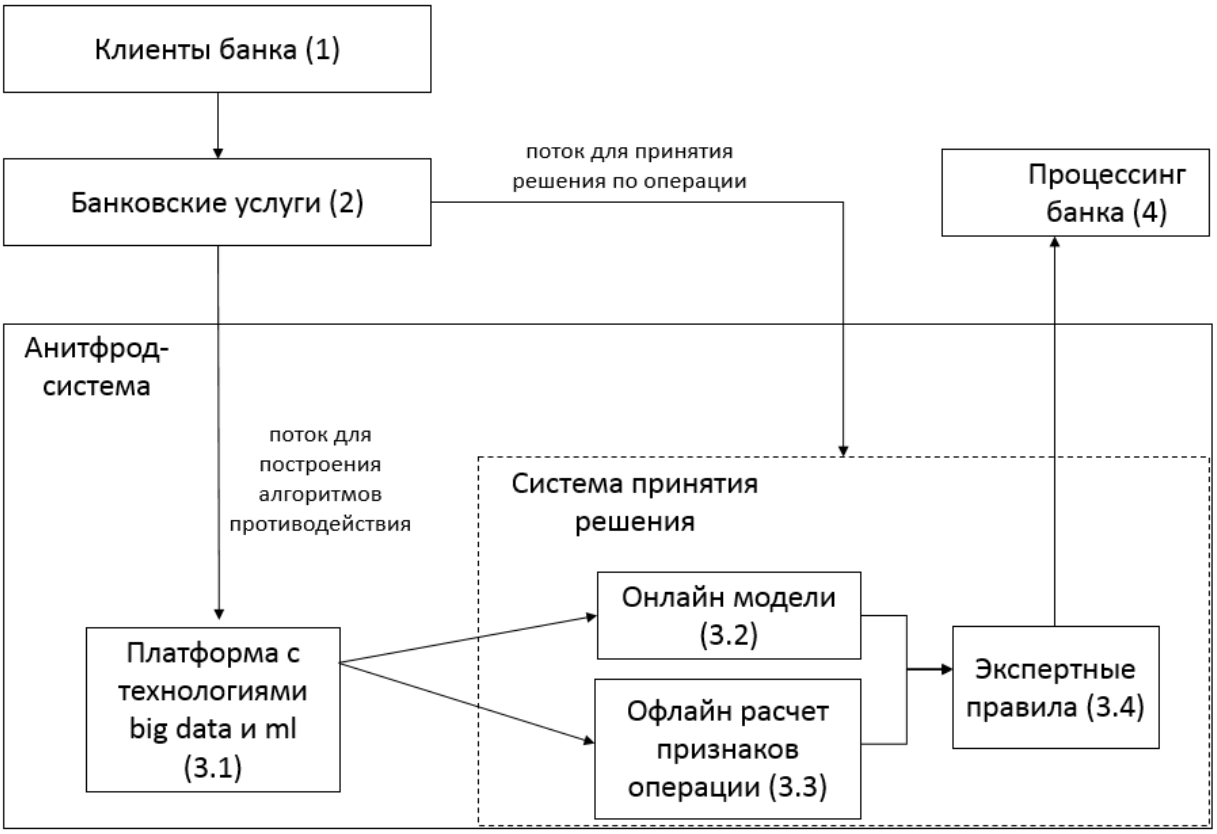


Рис. 3. Пример этапов работы системы фрод-мониторинга банка

(1) Клиенты банка, которые используют банковские услуги – делают покупки на сайтах в интернете, в розничных магазинах, привязывают карты для оплаты с помощью смартфонов и т.п.

(2) Банковские сервисы для оплаты товаров и услуг, в том числе через Интернет, совершения переводов, а также снятия наличных.

(3) Антифрод-система банка (фрод-мониторинг).

(3.1) Аналитическая платформа, на которой проводится разработка алгоритмов выявления мошенничества. В крупных банках с большим транзакционным поток для этих целей обычно используется стек технологий BIG DATA.

(3.2) Технологические блок для исполнения моделей машинного обучения в режиме реального времени (model-based подход).

(3.3) Обогащение транзакций дополнительными признаками, созданными на аналитической платформе.

(3.4) Технологические блок для вынесения окончательного решения по операции, основанный на экспертных правилах (rule-based подход).

(4) Процессинг банка, в котором происходит непосредственное исполнение операции после вынесения вердикта фрод-мониторингом.

Во втором случае рассматривается процесс страховой компании, в котором снижается риск мошенничества со стороны страхователей. Первой преградой для мошенников является проверка клиента перед заключением

договора страхования. Помимо актуарных расчетов страховщик может обратиться к внутренним черным или белым спискам, внешним источникам данных о клиенте, применить собственные модели оценки риска мошенничества со стороны страхователя. Такие процедуры напрямую влияют на страховщика – удлиняют процесс продажи полиса, ухудшая клиентский опыт; а ложные отказы снижают уровень сбора страховой премии. Эти факты заставляют страховые компании упрощать и автоматизировать проверки на данном этапе. В этом случае, компании фокусируются на точности выявления мошенничества, но не уделяют достаточного внимания полноте, что дает возможность профессиональным мошенникам успешно проникать в страховой портфель.

Далее страховщик анализирует заявленные претензии и, при выявлении признаков страхового мошенничества, отказывает в выплате. На данном этапе применяются как экспертные методы оценки со стороны службы безопасности страховщика, так и техники с использованием методов машинного обучения. Положительный эффект дает совмещение работы эксперта и систем, позволяющих оценивать претензии с помощью анализа данных и социальных сетей [30]. В текущем процессе страховая компания ориентируется на полноту выявления мошенничества, чтобы остановить уже проявившего себя профессионального мошенника и снизить его влияние на показатель убыточности портфеля.

Схематично рассматриваемые процессы можно представить следующим образом (Рис 4).

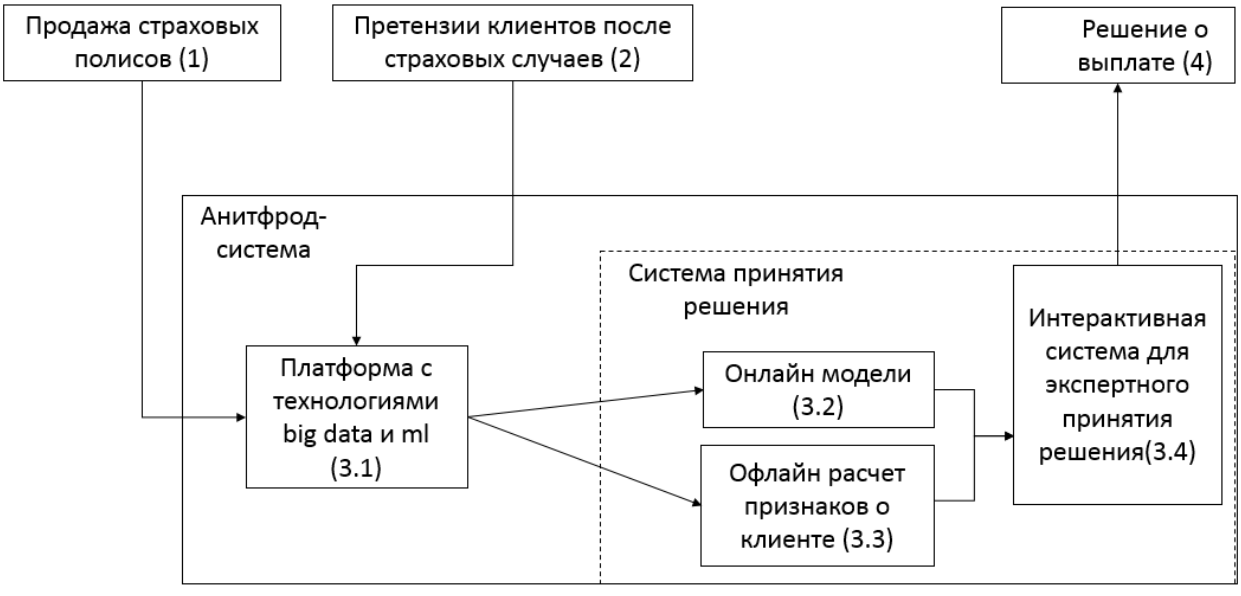


Рис. 4. Пример этапов работы системы фрод-мониторинга страховой компании

В настоящем исследовании выбраны следующие составляющие систем фрод-мониторинга, в которых будут интегрированы методы машинного обучения для повышения эффективности обнаружения мошенничества:

1. подготовка данных для построения алгоритмов принятия решения по транзакции;
2. настройка алгоритмов в системе принятия решения.

На этапе подготовки данных применяется корректировка классовой разметки с помощью многослойного перцептрона, а также расширение пространства признаков путем использования данных, отличных от тех, которые содержатся в оцениваемой транзакции, а также данных, извлеченных из графа.

Этап экспертной настройки алгоритмов будет автоматизирован с помощью методов машинного обучения, что позволит повысить точность обнаружения мошенничества.

4.3. Подготовка данных для обучения классификаторов мошеннических операций и претензий

Для улучшения качества классификации мошеннических транзакций предлагается следующий процесс подготовки данных:

1. набор данных разбивается на четыре части из разных временных периодов;
2. более ранняя часть (D_{init}) используется для обучения модели M_L, с помощью которой будет корректироваться экспертная оценка;
3. следующая по времени (D_{train}) используется для обучения модели M_S на переразмеченном наборе данных, а также для обучения базовой модели M_B, с которой будет сравниваться результат эксперимента;
4. следующая ($D_{control\_1}$), предназначена для поиска точек отсечения (TH_{fraud}, $TH_{legitimate}$) модели M_L, в зависимости от значений которых будет приниматься решение о корректировке разметки в D_{train};
5. наконец, на выборке $D_{control\_2}$ будет проводиться валидация результатов – измерение характеристик качества классификации.

Разбиение данных и классификаторы для оценки транзакций можно схематично представить на Рис 5.

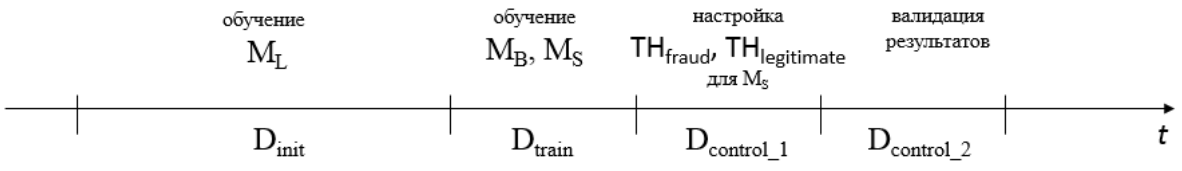


Рис. 5. Разбиение данных при корректировке разметки

В Таблице 3 приведены используемые параметры и ссылки на описание классификаторов, применяемые предложенном подходе.

Таблица 3

Используемые классификаторы в процессе обучения

Классификатор	Название	Ссылка на описание
M_L	Multilayer perceptron	https://scikit-learn.org/stable/modules/neural_networks_supervised.html (дата обращения: 12.02.2024)
M_B	RandomForest Classifier	https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html (дата обращения: 12.02.2024)
M_S	RandomForest Classifier	https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html (дата обращения: 12.02.2024)

Выбор RandomForest и многослойного перцептрона в качестве классификаторов обусловлен исследованием [28], в котором показано сравнение основных методов машинного обучения в задачах выявления мошенничества в автостраховании.

Этапы корректировки разметки схематично можно представить на Рис. 6.

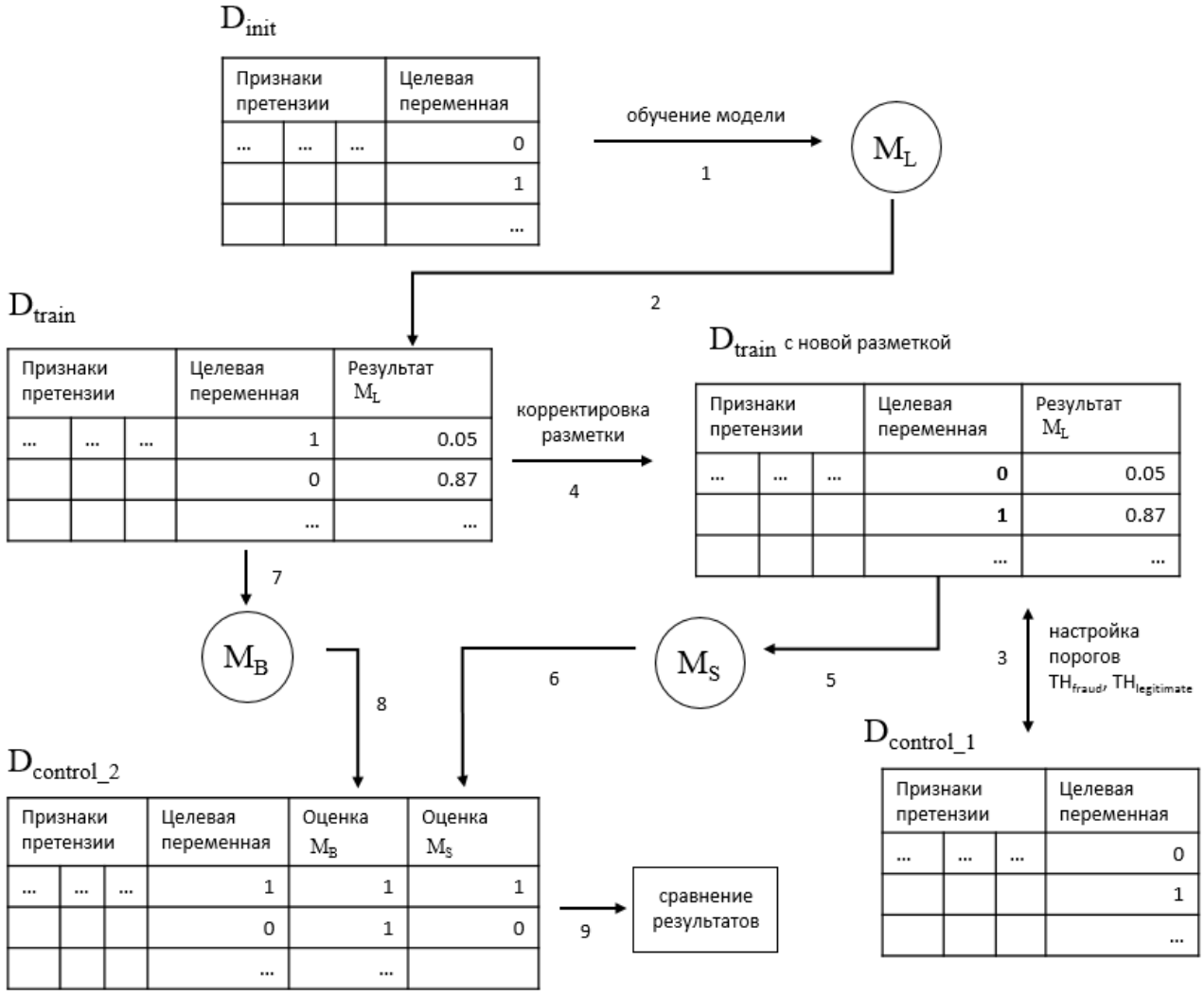


Рис. 6. Предлагаемая последовательность этапов корректировки разметки

Для расширения признакового пространства предлагается включать в него информацию из источников, не связанных с оценкой текущей транзакции. Например, в банковской отрасли при оценке переводов между клиентами можно интегрировать историю операций покупок клиентов. В таком случае улучшение характеристик достигается за счет того, что мошенники не могут обеспечить легитимную историю счетов, которые они используют в схеме мошенничества.

Для выявления аномального поведения клиентов в страховой компании предлагается составить ненаправленный граф, вершинами которого являются претензии на возмещение страхового случая, а ребрами – объекты аварий (водители, страхователи и т. д.), а также сам инцидент. Граф строится за некоторый период, например, календарный год.

В качестве новых признаков по претензии можно рассмотреть свойства вершины построенного графа. В Таблице 4 представлены признаки, рассмотренные в рамках диссертационного исследования.

Таблица 4

Атрибуты претензий, построенные на основе графа претензий

Объект графа	Описание признака
Вершина	• Степень вершины • Минимальная степень смежных вершин • Количество смежных вершин • Средняя степень смежных вершин
Компонента связанности	• Количество вершин в связанной компоненте вершины
Клика	• Размер максимальной клики, в которой состоит вершина • Количество клик, в которых состоит вершина
Цикл	• Длина цикла, в которой состоит вершина • Средняя степень вершин цикла, в которой состоит вершина

4.4. Генерация новых алгоритмов для повышения качества системы фрод-мониторинга

Экспертную настройку правил в системе принятия решения предлагается автоматизировать с использованием методов машинного обучения. Подход состоит из трех этапов:

- подготовка и предварительная обработка данных;
- применение методов машинного обучения;
- извлечение и оценка правил.

Этап подготовки данных осуществляется включает в себя:

1. загрузка исторических данных из системы фрод-мониторинга;
2. эмуляция работы фрод-мониторинга;
3. отбор признаков, фильтрация зашумленных данных и разработка дополнительных признаков.

На следующем этапе к подготовленным данным применяются методы Decision Tree или Random Forest.

На последнем этапе происходит выбор правил для их интеграции в систему фрод-мониторинга. Для этого правила извлекаются из обученных алгоритмов, построенных методами Decision Tree или Random Forest. Затем правила сравниваются между собой на основе характеристик качества классификации. Лучшие правила внедряются в систему фрод-мониторинга финансовой организации, чтобы они работали согласно экспертным правилам.

4.5. Методика проведения экспериментов и результаты

В ходе исследования были разработаны методики для проведения четырех различных экспериментов, позволяющие оценить применимость предложенных подходов.

4.5.1. Корректировка классовой разметки транзакций

Для проведения эксперимента выбраны два набора данных автстрахования. Один из них – широко известный и используемый в различных исследованиях «carclaims.txt». В нем содержатся страховые случаи, зарегистрированные в США за период с 1994 по 1996 год [31].

Также для демонстрации применимости подхода на различных страховых данных рассмотрен файл «insurance_claims.csv» [8] , в котором содержатся претензии за период с января по февраль 2015 года.

Для целей диссертационного исследования выбраны признаки, приведенные в Таблице 5.

Таблица 5

Описание признаков претензий для оценки мошеннической составляющей

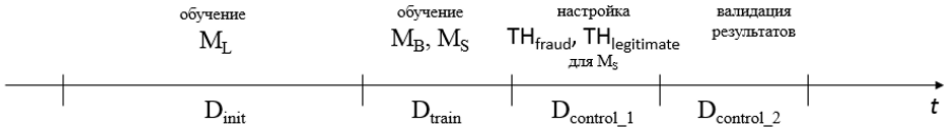
Набор данных	Название признака	Описание
«carclaims.txt»	Age	Возраст страхователя
	DriverRating	Рейтинг водителя, участвовавшего в ДТП
	Gender	Пол страхователя
	BasePolicy	Тип полиса
	Fault	Виновная сторона
	NumberOfSuppliments	Количество дополнительный опций в полисе
	PastNumberOfClaims	Количество страховых случаев по текущему
	VehiclePrice	Стоимость автомобиля, участвовавшего в ДТП
	AgeOfPolicyHolder	Возраст страхователя
«insurance_claims.csv»	age	Возраст страхователя
	months_as_customer	Количество месяцев в качестве страхователя
	policy_annual_premium	Страховая премия
	insured_sex	Пол страхователя
	total_claim_amount	Сумма претензии
	incident_severity	Серьезность страхового случая

Такой малочисленный состав признаков выбран с целью сохранения применимости предложенного подхода для оценки мошеннической составляющей в различных портфелях претензий страховых компаний. Данный набор признаков можно получить из анкетных данных страхователей и претензий при урегулировании страхового случая.

Набор данных «carclaims.txt» состоит из 15 420 записей, из которых 14 497 являются легитимными претензиями, а 923 (6 %) с признаками

[8] https://www.kaggle.com/datasets/buntyshah/auto-insurance-claims-data

страхового мошенничества. Размер «insurance_claims.csv» составляет 1 000 записей, из которых 247 – мошеннические (24,7 %). Претензии можно выстроить в хронологическом порядке по тому, как они поступали в страховую компанию, потому качество модели предлагается проверять на более поздних данных. Разбиение данных схематично представлено на Рис 7.



		D_{init}	D_{train}	$D_{control\_1}$	$D_{control\_2}$
«carclaims.txt»	количество претензий:	6420	3000	3000	3000
	дисбаланс классов:	6,6%	5,7%	5,8%	5,2%
«insurance_claims.csv»	количество претензий:	255	241	253	251
	дисбаланс классов:	26.6%	25.3%	28.4%	18.3%

Рис. 7. Разбиение данных для проведения эксперимента

В Таблице 6 приведены используемые параметры, примененные в процессе обучения классификаторов.

Таблица 6

Настройка параметров классификаторов

Классификатор	Название	Параметры
M_L	Multilayer perceptron	«carclaims.txt»: hidden_layer_sizes=(10), solver='lbfgs' «insurance_claims.csv»: hidden_layer_sizes=(2), solver='lbfgs' , activation = 'relu'
M_B	RandomForestClassifier	«carclaims.txt»: class_weight = {0: 1, 1: 1}, criterion = ‘entropy', n_estimators = 5 «insurance_claims.csv»: class_weight = {0: 1, 1: 1}, criterion = ‘entropy', n_estimators = 2, 'max_depth': 3

M_S	RandomForestClassifier	«carclaims.txt»: class_weight = {0: 1, 1: 3}, criterion = ‘entropy', n_estimators = 5 «insurance_claims.csv»: class_weight = {0: 1, 1: 1}, criterion = ‘entropy', n_estimators = 2, 'max_depth': 3

Экспериментально с помощью измерения качества классификации на $D_{control\_1}$ подобраны значения TH_{fraud}, $TH_{legitimate}$:

a) для набора данных «carclaims.txt»: $TH_{fraud} = 0,75$; $TH_{legitimate} = 0,1$;

b) для «insurance_claims.csv»: $TH_{fraud} = 0,8$; $TH_{legitimate} = 0,05$.

После этого претензии в D_{train} были переразмечены следующим образом:

- если результат оценки (вероятность отнесение к мошенничеству) претензии с помощью M_L больше TH_{fraud}, то она переразмечается как мошенническая;
- если результат оценки менее $TH_{legitimate}$, то претензия переразмечается как легитимная;
- в остальных случаях разметка претензии не подвергается изменению.

Данная корректировка классов улучшила баланс в D_{train} до 36,3 % в наборе данных «carclaims.txt» и до 35,8 % в «insurance_claims.csv». Далее проведено обучение M_B на данных D_{train} до корректировки классов и M_S на данных D_{train} после корректировки.

Полученные модели M_B и M_S применены в выборке $D_{control\_2}$, которая никаким образом не участвовала в обучении классификаторов или настройке параметров и является более поздней по времени, с точки зрения появления претензии у страховщика. Также в данной выборке разметка не подвергалась корректировке. На Рис. 8 представлены ROC кривые для этих моделей.

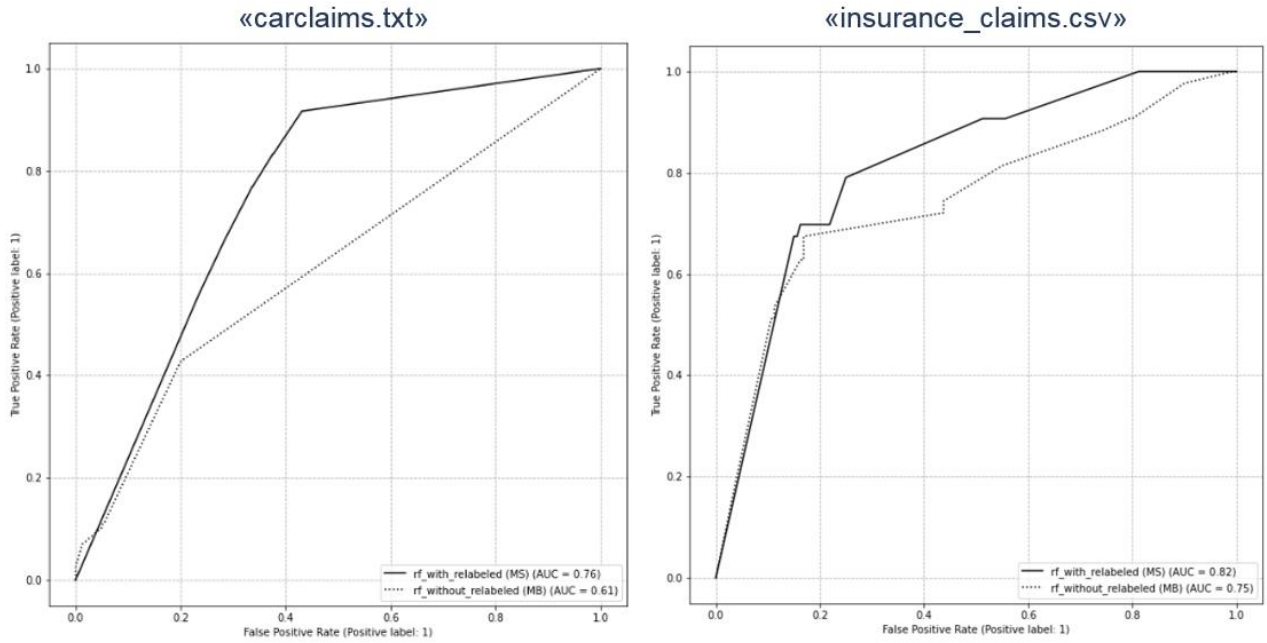


Рис. 8. Сравнение ROC кривых для моделей M_B и M_S

Значения площадей под данными кривыми (AUC) показывает значительно лучшее качество классификации для предложенного подхода в сравнении с традиционным обучением без корректировки разметки. В Таблице 7 также приведено значения Recall при фиксированной точности для сравнения моделей.

Таблица 7

Сравнение метрик качества выявления мошенничества

Набор данных	Метрика	Предложенный подход, M_S	Традиционный подход, M_B
«carclaims.txt»	ROC AUC	**0,76**	0,61
	Precision	0,1	0,1
	Recall	**0,92**	0,43
«insurance_claims.csv»	ROC AUC	**0,82**	0,75
	Precision	0,55	0,55
	Recall	**0,7**	0,51

4.5.2. Использование в пространстве признаков данных иной природы

В качестве набора данных для изучения выбраны операции переводов крупного банка за недельный период, которые система фрод-мониторинга зафиксировала как подозрительные и запустила один из сценариев обработки, например, предупреждение клиента о возможном мошенничестве

или вовсе отклонение операции. Также в выборку добавлены кейсы, по которым не было срабатываний системы фрод-мониторинга, но в течение рассматриваемого периода клиент оставил жалобу, что данная операция является мошенничеством. Пропущенное и выявленное при срабатывании операции мошенничество объединены и далее будут рассматриваться как целевой класс при построении классификатора. Ложные срабатывания относятся ко второму классу. Мошенничество разметим 1, ложные срабатывания 0. Таким образом будет сформирована таблица (hits_fm) следующего вида:

Таблица 7

Пример данных (hits_fm), построенных на основе срабатываний системы фрод-мониторинга

Клиент инициирующий перевод	Клиент получатель перевод	Разметка: 0 – операция легитимная 1 – фрод	Дата операции
cl_1	cl_2	0	20.02.2021
cl_3	cl_4	1	20.02.2021
…	…	…	…
cl_m	cl_k	0	27.02.2021

Далее будем полагать, что если в таблице hits_fm проставлен класс 1, то профиль получателя платежа можно отнести мошенническому (дропу). В случае 0 получатель легитимный. По каждому получателю банк имеет возможность построить таблицу, основанную на истории карточных операций (Таблица 8). С целью ограниченности эксперимента используется история операций, произошедших в двухнедельный период до первого перевода на клиента из таблицы hits_fm. Например, в столбце «Сумма операции в группе MCC_1» по клиенту cl_2 находится значение суммы всех платежей клиента, которые он совершил за две недели до операции из Таблица 7. В данном случае за период с 05.02.2021 по 19.02.2021 в категории MCC_1 осуществлены траты на сумму 40000 руб.

Таблица 8

Набор данных (clients_profile), построенный на основе истории карточных операций клиента

Клиент банка	**Сумма операции в группе MCC_1**	**Сумма операции в группе MCC_2**	**…**	**Сумма операции в группе MCC_N**
cl_2	40000	0	…	11112
cl_4	0	30000	…	0
…	…	…	…	…

Таблица clients_profile позволяет расширить признаковое пространство для применения метода машинного обучения при выявлении мошенничества в банковских переводах.

В результате использования новых данных удалось значительно повысить значение характеристики Precision с 0,07 до 0,69.

4.5.3. Использование в пространстве признаков данных извлеченных из графа

В данном эксперименте также рассматриваются два набора данных «carclaims.txt» и «insurance_claims.csv».

Рассматриваемые наборы данных не имеют явных атрибутов, которые позволяли бы построить граф претензий, например, номер договора. Поэтому для построения связей между двумя претензиями установлены следующие допущения.

a. Претензии связаны между собой участником страхового события, если у них совпадают атрибуты: Make, Sex, MaritalStatus, Age, VehicleCategory, VehiclePrice, AgeOfVehicle, DriverRating, AgentType, NumberOfCars, BasePolicy для «carclaims.txt»; POSTAL_CODE для «insurance_claims.csv».

b. Претензии связаны между собой страховым событием, если у них совпадают атрибуты: Year, Month, WeekOfMonth, DayOfWeek, AccidentArea, PoliceReportFiled, WitnessPresen для «carclaims.txt»; INCIDENT_CITY, INCIDENT_HOUR_OF_THE_DAY, INCIDENT_SEVERITY для «insurance_claims.csv».

Построенный таким образом граф можно визуализировать следующим образом (Рис. 9)

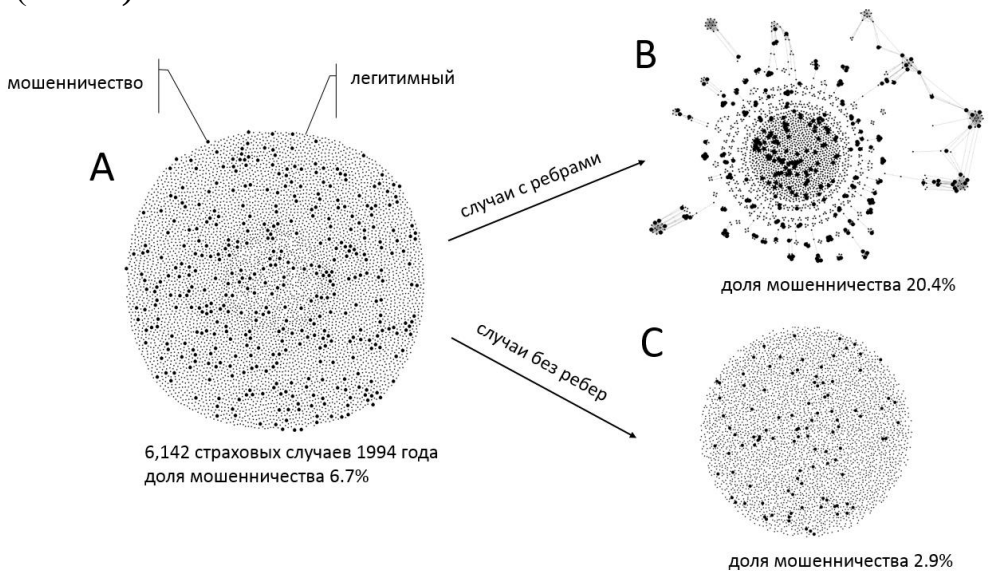


Рис. 9. Пример визуализации графа, построенного на связях между страховыми событиями и страхователями

Можно отметить, что сам факт наличия связи между претензиями повышает вероятность мошенничества в претензии.

Для каждой претензии извлекается набор признаков из Таблицы 4, а затем применяется метод машинного обучения RandomForest как к исходному набору данных, так и к расширенному.

На Рис. 10 продемонстрировано сравнение характеристик эффективности при использовании новых данных, извлечённых из графа, и без них. Эксперимент показал значительный рост эффективности обнаружения мошенничества для двух независимых наборах данных.

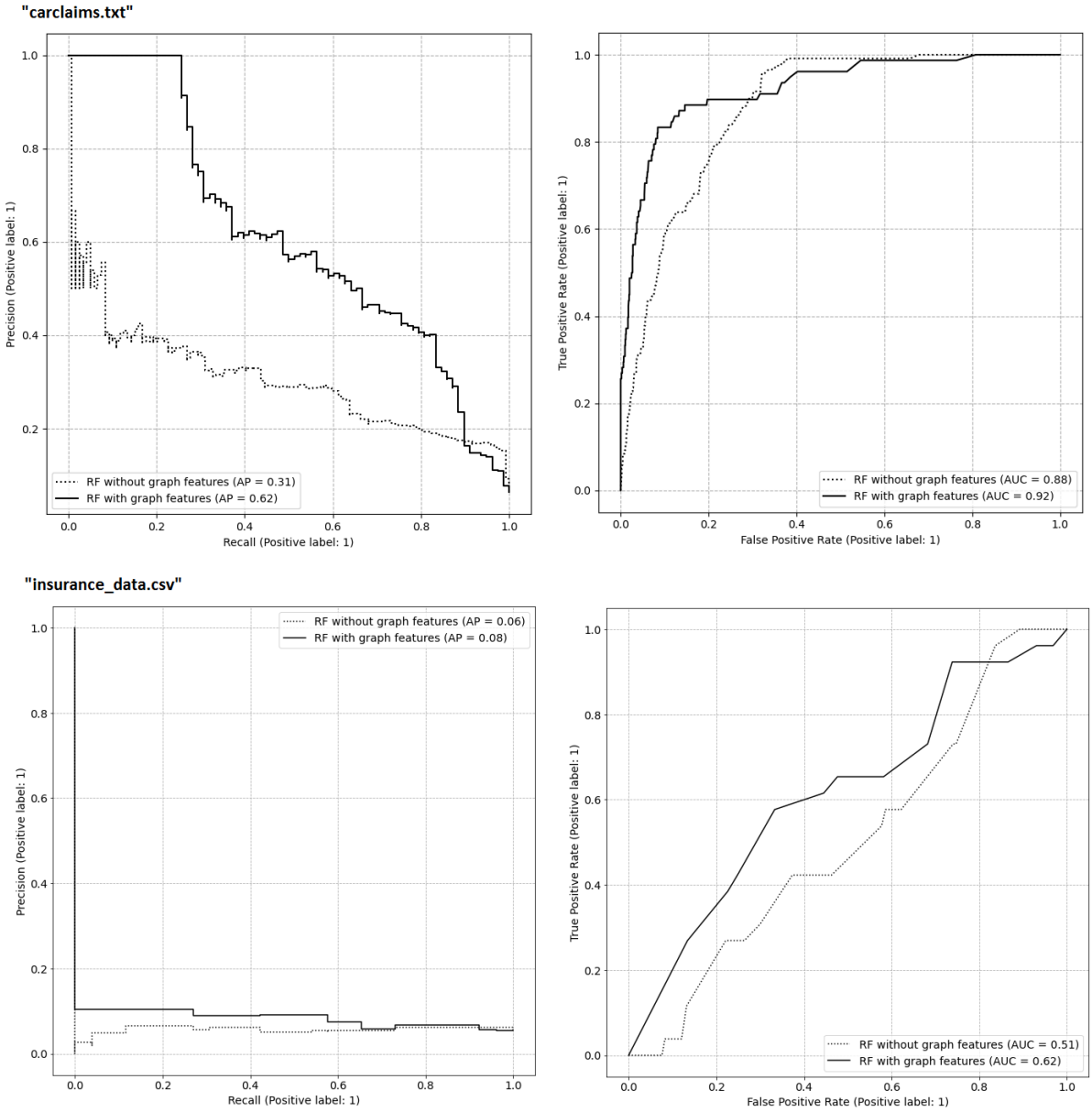


Рис. 10. Сравнение кривых ROC и Precision-Recall для моделей, обученных с использованием признаков графа претензий и без них.

4.5.4. Настройка алгоритмов в системе принятия решения

Разработанные с использованием предложенного в Разделе 4.4 подхода правила для принятия решений были успешно внедрены в реальную банковскую систему фрод-мониторинга. Результаты показали, что средняя точность правил составила 50%, а средняя полнота обнаружения мошенничества достигла 0,6%.

5. Заключение

Важно отметить, что разработанные методы имеют потенциал для улучшения эффективности применения методов машинного обучения в области борьбы с мошенничеством. Эти результаты могут быть полезными для различных финансовых организаций, которые сталкиваются с проблемой классификации при использовании методов машинного обучении в системе фрод-мониторинга.

Основные результаты работы.

1. Разработан метод улучшения качества разметки данных для применения машинного обучения в задаче обнаружения мошенничества.
2. Разработаны методы расширения признакового пространства, позволяющие повысить эффективность обнаружение мошенничества.
3. Предложен метод настройки системы принятия решения во фрод-мониторинге, использующий элементы машинного обучения.
4. Проведены экспериментальные исследования, подтверждающие эффективность предложенных подходов.

Список литературы

1. Al-Hashedi K.G., Magalingam P. Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019 // Computer Science Review. 2021. Vol. 40. P. 100402.
2. Bao Y., Hilary G., Ke B. Artificial Intelligence and Fraud Detection. 2022. P. 223–247.
3. Bezzateev S.V. et al. Risk assessment methodology for information systems, based on the user behavior and IT-security incidents analysis // Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2021. Vol. 21, № 4. P. 553–561.
4. Abdallah A., Maarof M.A., Zainal A. Fraud detection system: A survey // Journal of Network and Computer Applications. 2016. Vol. 68. P. 90–113.
5. Gupta P. et al. Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques // Procedia Computer Science. 2023. Vol. 218. P. 2575–2584.
6. Pant P., Srivastava P. Cost-Sensitive Model Evaluation Approach for Financial Fraud Detection System // 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2021. P. 1606–1611.
7. Jin C., Feng Y., Li F. Concept drift detection based on decision distribution in inconsistent information system // Knowledge-Based Systems. 2023. Vol. 279. P. 110934.

8. Anderson O.D. A Note on “Trial by Computer”—A Case Study of the Use of Simple Statistical Techniques in the Detection of a Fraud // Journal of the Operational Research Society. 1986. Vol. 37, № 4. P. 423–427.
9. Mercer L.C.J. Fraud detection via regression analysis // Computers & Security. 1990. Vol. 9, № 4. P. 331–338.
10. Wolf D., Greenberg D. The Dynamics of Welfare Fraud: An Econometric Duration Model in Discrete Time // Journal of Human Resources. 1986. Vol. 21, № 4. P. 437–455.
11. Baesens B., Vlasselaer V.V., Verbeke W. Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques. Hoboken, NJ, USA: John Wiley & Sons, Inc, 2015.
12. Воронцов К. В. Математические методы обучения по прецедентам (теория обучения машин) // Сайт «Машинное обучение», курс лекций. 2011.
13. Kumari P., Mishra S.P. Analysis of Credit Card Fraud Detection Using Fusion Classifiers. 2019. P. 111–122.
14. Baesens B., Höppner S., Verdonck T. Data engineering for fraud detection // Decision Support Systems. 2021. Vol. 150. P. 113492.
15. Ghosh, Reilly. Credit card fraud detection with a neural-network // 1994 Proceedings of the Twenty-Seventh Hawaii International Conference on System Sciences. 1994. Vol. 3. P. 621–630.

16. Baader G., Krcmar H. Reducing false positives in fraud detection: Combining the red flag approach with process mining // International Journal of Accounting Information Systems. 2018. Vol. 31. P. 1–16.
17. Nian K. et al. Auto insurance fraud detection using unsupervised spectral ranking for anomaly // The Journal of Finance and Data Science. 2016. Vol. 2, № 1. P. 58–75.
18. Subudhi S., Panigrahi S. Use of optimized Fuzzy C-Means clustering and supervised classifiers for automobile insurance fraud detection // Journal of King Saud University - Computer and Information Sciences. 2020. Vol. 32, № 5. P. 568–575.
19. Yankol-Schalck M. The value of cross-data set analysis for automobile insurance fraud detection // Research in International Business and Finance. 2022. Vol. 63. P. 101769.
20. Vandervorst F., Verbeke W., Verdonck T. Data misrepresentation detection for insurance underwriting fraud prevention // Decision Support Systems. 2022. Vol. 159. P. 113798.
21. Aslam F. et al. Insurance fraud detection: Evidence from artificial intelligence and machine learning // Research in International Business and Finance. 2022. Vol. 62. P. 101744.
22. Yan C. et al. Improved adaptive genetic algorithm for the vehicle Insurance Fraud Identification Model based on a BP Neural Network // Theoretical Computer Science. 2020. Vol. 817. P. 12–23.

23. Salmi M., Atif D. Using a Data Mining Approach to Detect Automobile Insurance Fraud. 2022. P. 55–66.
24. Soufiane E. et al. Automobile Insurance Claims Auditing: A Comprehensive Survey on Handling Awry Datasets. 2022. P. 135–144.
25. Vorobyev I. ML methods for assessing the risk of fraud in auto insurance // Izvestiya of Saratov University. Mathematics. Mechanics. Informatics.
26. Festa Y.Y., Vorobyev I.A. A hybrid machine learning framework for e-commerce fraud detection // Model Assisted Statistics and Applications. 2022. Vol. 17, № 1. P. 41–49.
27. Vorobyev I., Krivitskaya A. Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models // Computers & Security. 2022. Vol. 120. P. 102786.
28. Itri B. et al. Performance comparative study of machine learning algorithms for automobile insurance fraud detection // 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS). IEEE, 2019. P. 1–4.
29. Fawcett T. An introduction to ROC analysis // Pattern Recognition Letters. 2006. Vol. 27, № 8. P. 861–874.
30. Šubelj L., Furlan Š., Bajec M. An expert system for detecting automobile insurance fraud using social network analysis // Expert Systems with Applications. 2011. Vol. 38, № 1. P. 1039–1052.
31. Phua C., Alahakoon D., Lee V. Minority report in fraud detection // ACM SIGKDD Explorations Newsletter. 2004. Vol. 6, № 1. P. 50–59.