СЕКЦИЯ 1. МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ, ПРЕОБРАЗОВАНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ

УДК 004

Аетбаева Р.Г., Файзуллина А.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Юнусова Д.С.
Уфимский университет науки и технологий, Уфа

ОБНАРУЖЕНИЕ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация. Данная статья рассматривает применение методов машинного обучения для выявления финансового мошенничества. Рассматриваются современные способы реализации угроз и роль искусственного интеллекта для борьбы с такими угрозами в банковской сфере.

Ключевые слова: искусственный интеллект, машинное обучение, финансовое мошенничество, мошеннические операции.

Угрозы мошенничества в банковской системе в современном мире неуклонно растут, становясь все более изощренными и сложными, тогда как традиционные методы обнаружения мошеннических операций часто оказываются неэффективными. Развитие банковских технологий, таких как онлайн-банкинг, мобильные платежи и криптовалюты, значительно упростило жизнь клиентов, но одновременно создало новые возможности для мошенников, использующих фишинговые атаки, социальную инженерию, кражу личных данных и изощренные приемы обмана банков и их клиентов. Традиционные методы выявления мошенничества, основанные на ручных проверках и простых правилах, не справляются с современными угрозами, часто приводят к ложным срабатываниям и не способны выявить сложные мошеннические схемы, требующие анализа больших объемов данных, что делает использование ИИ не просто желательным, а необходимым условием обеспечения финансовой безопасности, предоставляя банкам широкий спектр инструментов для борьбы с преступлениями на различных этапах финансовых операций.

Банки применяют ИИ для выявления мошеннических кредитных заявок. Данные, указанные в кредитной заявке, и информация из внешних источников анализируются, чтобы оценить риск мошенничества. Он также помогает банкам соблюдать требования законодательства по борьбе с незаконным оборотом денежных средств путем анализа транзакций, выявления подозрительных операций и оценки рисков. Большую роль

искусственный интеллект играет и в борьбе с кибератаками на банковские системы.

Рассмотрим конкретный пример анализа транзакций на наличие мошеннических операций, используя модель RandomForestClassifier, которая является основой большинства систем обнаружения мошенничества на основе ИИ. Алгоритмы МО обучаются на исторических данных о мошеннических и немошеннических операциях, чтобы выявлять закономерности и аномалии.

Для обучения был использован датасет, содержащий 6 362620 данных о смоделированных банковских транзакциях, на основе историй реальных операций. Датасет содержит следующие данные: тип транзакции, шаг (1 шаг равен 1 часу), код отправителя транзакции, идентификатор получателя транзакции, сумма транзакции, баланс до и после транзакции отправителя и получателя, является ли транзакция мошенничеством.

Транзакции разделены на 5 типов: вывод наличных, платеж, ввод наличных, перевод, дебет. Распределение транзакций по типам приведено на рис. 1.

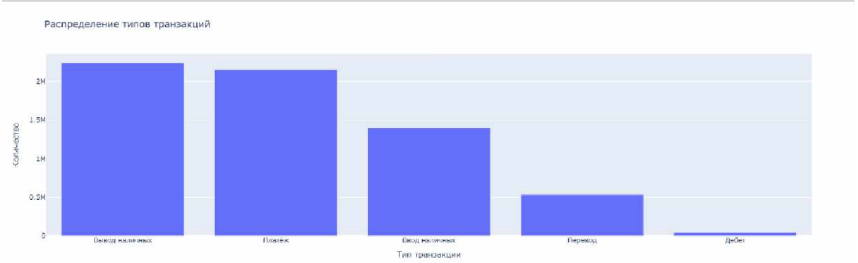

Рис. 1. Распределение типов транзакций

На основании результатов анализа корреляции между различными числовыми переменными и целевой переменной «Является_мошенничеством» составлена табл. 1.

Таблица 1

Корреляция

Сумма	0.076688
Шаг	0.031578
Старый_баланс_отправителя	0.010154
Новый_баланс_получателя	0.000535
Старый_баланс_получателя	-0.005885
Новый_баланс_отправителя	-0.008148

Анализ корреляции помогает выявить признаки, наиболее сильно связанные с мошенническими операциями. Таким образом, можем выявить, что сумма транзакции, шаг и старый баланс отправителя являются признаками, относительно которых можно определить является ли транзакция мошеннической.

Данные разделяются на обучающую и тестовую выборки. Для обучения используется модель Random Forest Classifier. Рассчитываются метрики качествамодели, такие как точность (accuracy), матрица ошибок (confusionmatrix) и отчет о классификации (classificationreport). Полученные значения приведены на рис. 2.

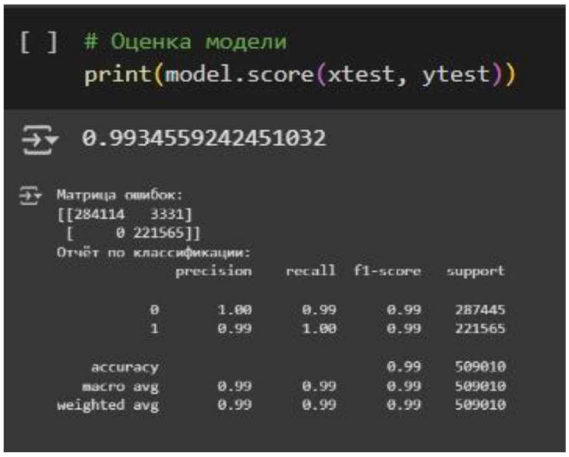

Рис. 2. Метрики качества модели

Этот пример демонстрирует, что искусственный интеллект может быть использован для обнаружения и предотвращения мошеннических транзакций. Так, с помощью модели RandomForestClassifier выявляются подозрительные операции на основе анализа различных признаков транзакции. Также такой метод помогает в анализе поведения клиентов. Анализ корреляции может показать, какие признаки поведения клиентов (например, изменение баланса, сумма транзакции) наиболее сильно связаны с мошенничеством.

Несмотря на огромный потенциал ИИ в борьбе с мошенничеством, существуют и определенные проблемы, и вызовы при его внедрении в банковский сектор:

- качество данных: в примере кода использовался готовый набор данных, реальных условиях необходимо обеспечить высокое качество данных, которые используются для обучения модели;
- интерпретируемость: важно понимать, почему модель приняла то или иное решение, RandomForest - относительно интерпретируемая модель, но более сложные модели (например, нейронные сети) могут быть «черными ящиками»;
- адаптация: мошенники постоянно разрабатывают новые методы, поэтому модель необходимо регулярно переобучать на новых данных.

Таким образом, банки, которые успешно внедрят ИИ, смогут значительно повысить свою безопасность, снизить финансовые потери и защитить своих клиентов от мошеннических действий. Дальнейшее развитие и распространение ИИ в банковском секторе несомненно приведет к появлению новых и более эффективных методов борьбы с мошенничеством, делая финансовую систему более безопасной и устойчивой.

Рассмотренный пример демонстрирует, как ИИ может быть применен для решения конкретной задачи в банковской сфере – выявлении мошеннических транзакций.

Список использованных источников:

1. Искусственный интеллект в банках. URL: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_банках (дата обращения: 15.04.2025).

2. Применение искусственного интеллекта на финансовом рынке России. URL: https://elibrary.ru/item.asp?id=54013778 (дата обращения: 16.04.2025).

Aetbaeva R.G., Fayzullina A.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa

DETECTING FRAUDULENT TRANSACTIONS USING MACHINE LEARNING METHODS

Abstract. This article discusses the application of machine learning methods for detecting financial fraud. It examines modern ways that threats are executed and the role of artificial intelligence in combating such threats in the banking sector.

Keywords: artificial intelligence, machine learning, financial fraud, fraudulent activities.