

Секция «Управление рисками и страхование: новые вызовы и возможности»

Разработка гибридной модели для выявления мошенничества в сфере страхования с целью уменьшения финансовых рисков

Научный руководитель – Савенко Оксана Леонидовна

Пятков Егор Олегович

Студент (бакалавр)

Южный федеральный университет, Факультет экономический, Кафедра Финансы и кредит, Ростов-на-Дону, Россия

E-mail: piatkov@sfedu.ru

Одной из самых обсуждаемых тем в сфере страхования, является тема мошенничества [2]. По данным Всероссийского союза страховщиков (ВСС) за 9 месяцев 2024 года страховыми компаниями было подано заявлений о возбуждении уголовных дел по статье «страховое мошенничество» на сумму 3 млрд рублей, что на 20% выше за аналогичный период 2023 года [7]. Страховые компании разными способами пытаются уменьшить ущерб от мошеннических действий. Одним из эффективных способов, является внедрение искусственного интеллекта (ИИ) и методов машинного обучения, которые способны обработать и учесть огромное количество информации [1]. Так, например, в 2023 году страховщики смогли избежать потенциальных потерь в сфере перевозок на сумму 175 миллионов рублей, благодаря внедрению ИИ [6]. Кроме того, существует большое количество компаний в других сферах, таких как Сбер, Т-банк, МТС, Directum, ZestFinance, которые внедрили ИИ в существующие финансовые инструменты, с целью повышения их эффективности [4].

Однако, несмотря на все преимущества (увеличение точности аналитики и прогнозов, автоматизацию огромного количества рутинных задач, и как следствие - снижение операционных расходов, мониторинг операций в режиме реального времени и др.), внедрение ИИ порождает ряд существенных проблем [4]. Например, проблема «черного ящика», при которой возникает ситуация, когда нет возможности понять, почему ИИ выдал тот или иной результат, на основе которого впоследствии, было принято определенное решение [3]. Алгоритмы ИИ напрямую зависят от качества данных, на которых они обучаются, что в свою очередь вытекает в ошибки прогнозирования, ложные закономерности, завышение данных [5]. Особенно, важно решение этой проблемы, когда речь идет о мошенничестве и создаются все более изощренные схемы, которые ИИ не сможет отследить. Все это может негативно влиять на решения, принимаемые компанией в виде финансовых и нефинансовых потерь.

Именно поэтому, была разработана и протестирована гибридная модель, основанная на сочетании методов машинного обучения и анализа, проводимого при участии эксперта. Она использует гибридные методы, позволяет комбинировать автоматические алгоритмы предсказания, с возможностью передачи особых случаев эксперту, для более точного и подробного рассмотрения.

Для проведения тестов мы использовали официальные данные по страховому сектору, а также синтетически сгенерированные, чтобы проверить работоспособность модели на различных сценариях. Наш подход включает в себя три метода:

1) Ручная проверка – способ, где все подозрительные случаи рассматриваются исключительно экспертами без предварительного анализа ИИ.

2) Автоматический метод – полностью автоматизированный метод, основанный на XGBoost-классификаторе, где модель предсказывает вероятность мошенничества, и на основе данных принимает самостоятельное решение.

3) Гибридная модель – вариант, который сочетает в себе машинное обучение и ручной анализ, при котором система прогнозирует вероятность мошенничества. Решение принимается по динамическому порогу уверенности. Если вероятность мошенничества высокая, то решение принимается автоматически, если вероятность ниже порога уверенности, но при этом все еще достаточно высока, то заявка передается на ручную проверку.

По результатам проведения тестов на реальных страховых данных, которые были разбиты на обучающую (50%) и тестовую (50%) выборки, а также принималась константа о том, что ручная проверка обнаруживает 65% мошеннических случаев, были сделаны следующие выводы:

1) Автоматическая модель сократила потери на 43% (с 1.75 миллиарда рублей до 1 миллиарда рублей), при этом пропустила 20% мошеннических заявок.

2) Гибридная модель сократила потери на 63% (с 1.75 миллиарда рублей до 650 миллионов рублей), что на 27% эффективнее автоматической модели, благодаря передаче сомнительных заявок на ручную проверку.

Реализацию самой модели, а также всех тестов и данных можно найти по ссылке на Google Drive (https://drive.google.com/drive/folders/1I_P3AQB0WcIOAbIFrWb_pUFCuiHuuHV?usp=sharing)

В заключение, можно сказать, что гибридная модель показала свою эффективность в сравнении с ручным и автоматическим методами. Конечно, стоит отметить, что, применяя данную модель на других данных, можно получить иные результаты. Так как очень много будет зависеть от качества этих данных, от выбранных методов и от того, какая модель ИИ используется для анализа. Независимо от этого, данная модель имеет огромный потенциал, не только в выявлении случаев мошенничества, но и других не менее важных и значимых факторов, которые могут повлиять на финансовые результаты компаний.

Источники и литература

- 1) Маглинова Т.Г., Шупило О.М. Внедрение искусственного интеллекта в страховую отрасль // Международный журнал гуманитарных и естественных наук. 2022. №5-4. С. 142-145
- 2) Мартыненко Д.Д., Нефедова Т.И. (2022). Мошенничество в сфере страхования. Вестник ПензГУ, №4 (40).
- 3) Незнамов А.В. (ред.). Белая книга этики в сфере искусственного интеллекта. М.: Nova Creative Group, 2024.
- 4) Чебуханова Л.В. Искусственный интеллект и его влияние на трансформацию финансовых инструментов // Вестник Академии знаний. 2024. №5 (64). С. 486-491
- 5) Maple C., Szpruch L., Epiphaniou G., Staykova K., Singh S., Penwarden W., Wen Y., Wang Z., Hariharan J., Avramovic P. The AI Revolution: Opportunities and Challenges for the Finance Sector. 2023
- 6) CNews: https://www.cnews.ru/news/line/2023-12-22_iskusstvennyj_intellekt
- 7) Banki.ru: <https://www.banki.ru/news/lenta/?id=11008582>