

ТЕМА НАУЧНОЙ СТАТЬИ

Аннотация: Статья посвящена использованию искусственного интеллекта (ИИ) и машинного обучения (МО) для борьбы с финансовыми преступлениями, такими как отмывание денег, мошенничество и финансирование терроризма. ИИ и МО позволяют эффективно анализировать огромные объемы данных для выявления подозрительных транзакций, автоматизировать процедуры проверки клиентов и обнаруживать новые типологии финансовых преступлений. Однако внедрение этих технологий сопряжено с рядом технических, этических и управленческих проблем, требующих междисциплинарного подхода. Успешное применение ИИ и МО в борьбе с финансовыми преступлениями открывает значительные возможности для повышения эффективности и безопасности финансовой системы в будущем.

Ключевые слова: Машинное обучение (МО), Финансовые преступления, Отмывание денег, Мошенничество, Финансирование терроризма, Мониторинг транзакций, Процедуры должной проверки клиентов (KYC)

Title: The Use of Artificial Intelligence and Machine Learning for Detecting and Combating Financial Crimes

Author: Vladimir Rozhkov

Abstract: The article explores the application of artificial intelligence (AI) and machine learning (ML) in combating financial crimes such as money laundering, fraud, and terrorist financing. AI and ML enable efficient analysis of vast amounts of data to identify suspicious transactions, automate customer due diligence procedures, and detect new typologies of financial crimes. However, the implementation of these technologies is associated with a range of technical, ethical, and managerial challenges that require an interdisciplinary

approach. The successful application of AI and ML in the fight against financial crimes opens up significant opportunities for enhancing the efficiency and security of the financial system in the future.

Keywords: Machine Learning (ML), Financial Crimes, Money Laundering, Fraud, Terrorist Financing, Transaction Monitoring, Know Your Customer (KYC) Procedures

Использование искусственного интеллекта и машинного обучения для выявления и борьбы с финансовыми преступлениями

В последние годы финансовая отрасль сталкивается с растущим числом финансовых преступлений, включая отмывание денег, мошенничество и финансирование терроризма. Традиционные методы обнаружения и предотвращения этих преступлений оказались недостаточными перед лицом меняющейся тактики преступников и огромного объема финансовых операций. Однако появление искусственного интеллекта (ИИ) и машинного обучения (МО) позволило создать мощный набор инструментов, помогающих финансовым учреждениям и регулирующим органам более эффективно выявлять эти преступления и противодействовать им.

Одним из основных примеров использования ИИ и МО в борьбе с финансовыми преступлениями является мониторинг транзакций. Обучая алгоритмы ИИ на огромном количестве исторических данных о транзакциях, финансовые учреждения могут выявлять закономерности и аномалии, которые могут указывать на подозрительную активность. Эти алгоритмы могут анализировать широкий спектр переменных, таких как сумма, частота, местоположение и поведение клиента, чтобы в режиме реального времени выявлять потенциальные случаи отмывания денег или мошенничества. Это позволяет оперативно вмешаться и провести расследование, снижая риск финансовых потерь и репутационного ущерба.

Еще одно ключевое применение ИИ и МО - это процедуры должной проверки клиентов (Know-your-customer, KYC). Финансовые учреждения обязаны проверять личность своих клиентов и оценивать риск их вовлечения в незаконную деятельность. Однако ручные процессы KYC могут отнимать много времени, быть дорогостоящими и подверженными человеческим ошибкам. Используя ИИ и МО, финансовые учреждения

могут автоматизировать процесс анализа данных о клиентах из различных источников, таких как государственные базы данных, социальные сети и публичные записи, для выявления потенциальных «красных флажков» и лиц с высоким риском. Это не только упрощает процесс регистрации, но и помогает предотвратить использование финансовой системы преступниками.

ИИ и МО также могут сыграть решающую роль в обнаружении и предотвращении киберпреступлений, таких как фишинговые аферы, кража личных данных и захват счетов. Анализируя модели поведения пользователей, информацию об устройствах и сетевой трафик, алгоритмы ML могут выявлять подозрительную активность и потенциальные нарушения безопасности в режиме реального времени. Это позволяет финансовым учреждениям незамедлительно принимать меры по защите счетов своих клиентов и предотвращению мошеннических операций.

Кроме того, ИИ и МО могут помочь финансовым учреждениям и регулирующим органам выявлять новые тенденции и типологии финансовых преступлений. Постоянно анализируя огромные объемы данных из разных источников, эти технологии могут выявлять новые закономерности и методы, используемые преступниками для отмывания денег или совершения мошенничества. Эти данные могут быть использованы для обновления моделей обнаружения, усиления мер по предотвращению и принятия политических решений.

Однако использование ИИ и МО в борьбе с финансовыми преступлениями не обходится без проблем. Одной из главных проблем является возможность предвзятости алгоритмов, что может привести к ложным срабатываниям или несправедливому отношению к определенным группам клиентов. Чтобы снизить этот риск, финансовые учреждения должны убедиться, что их модели ИИ и МО обучаются на разнообразных и репрезентативных наборах данных и подвергаются регулярному аудиту и оценке на предмет справедливости и точности.

Интеграция ИИ и МО в борьбу с финансовыми преступлениями не только доказала свою эффективность, но и открыла новые возможности для сотрудничества и инноваций в финансовой отрасли. Одним из таких направлений является разработка совместных интеллектуальных платформ, позволяющих финансовым учреждениям объединять свои данные и сведения о финансовых преступлениях. Используя возможности коллективного разума и алгоритмов МО, эти платформы могут выявлять закономерности и связи, которые могут быть незаметны для отдельных

учреждений, что повышает общую эффективность усилий по выявлению и предотвращению преступлений.

Кроме того, ИИ и МО можно использовать для повышения эффективности и точности расследований финансовых преступлений. Традиционные процессы расследования часто предполагают ручной анализ больших объемов данных, что отнимает много времени и чревато человеческими ошибками. Используя инструменты ИИ и МО для анализа и приоритизации соответствующих данных, следователи могут сосредоточить свои усилия на наиболее важных делах и принимать более обоснованные решения. Например, алгоритмы обработки естественного языка (NLP) могут использоваться для анализа неструктурированных данных, таких как сообщения электронной почты и посты в социальных сетях, с целью выявления потенциальных случаев инсайдерской торговли или манипулирования рынком.

Еще одним перспективным направлением применения ИИ и МО в борьбе с финансовыми преступлениями является предиктивная аналитика. Анализируя исторические данные о финансовых преступлениях и характеристики вовлеченных в них физических и юридических лиц, алгоритмы МО могут выявлять закономерности и факторы риска, которые могут указывать на повышенную вероятность преступной деятельности в будущем. Эта информация может быть использована для упреждающей профилактики и более эффективного распределения ресурсов. Например, прогностические модели могут использоваться для выявления клиентов или операций с повышенным риском, которые могут потребовать усиленной проверки или мониторинга.

Автоматизируя повторяющихся задач, связанных с этими процессами, ИИ и МО могут помочь сократить расходы, повысить эффективность и высвободить человеческие ресурсы, чтобы сосредоточиться на более важных видах деятельности. Например, чат-боты на базе ИИ могут использоваться для обработки рутинных запросов клиентов, связанных с процедурами AML и KYC, а алгоритмы МО - для постоянного мониторинга и обновления оценок рисков с учетом меняющихся рыночных условий и поведения клиентов.

Однако для успешного применения ИИ и МО в борьбе с финансовыми преступлениями требуются не только технологические инновации. Это также требует фундаментальных изменений в подходах финансовых учреждений и регулирующих органов к управлению данными, конфиденциальности и этике. Использование ИИ и МО предполагает сбор, хранение и анализ огромных объемов конфиденциальных данных о

клиентах, что вызывает беспокойство по поводу конфиденциальности и безопасности данных. Финансовые учреждения должны обеспечить надежную систему управления данными для защиты информации о клиентах и соблюдения соответствующих норм.

Кроме того, использование ИИ и МО в процессах принятия решений, связанных с финансовыми преступлениями, также вызывает этические проблемы, связанные со справедливостью, прозрачностью и подотчетностью. Финансовые учреждения должны убедиться, что их модели ИИ и МО не только точны, но и объяснимы и проверяемы, чтобы решения можно было обосновать и оспорить в случае необходимости. Это требует совместных усилий ученых, занимающихся изучением данных, специалистов по соблюдению нормативных требований и экспертов по этике для разработки и внедрения соответствующих рамок управления и механизмов надзора.

Помимо этих проблем, использование ИИ и МО в борьбе с финансовыми преступлениями также требует значительных инвестиций в таланты и инфраструктуру. Финансовые организации должны нанимать и обучать специалистов по изучению данных и инженеров по МО для разработки и поддержки моделей ИИ и МО, а также инвестировать в необходимые вычислительные мощности и системы хранения данных для обработки больших объемов данных. Для небольших учреждений это может стать существенным барьером на пути к выходу на рынок и может потребовать совместных усилий и государственно-частного партнерства, чтобы уравнивать шансы.

Несмотря на эти проблемы, потенциальные преимущества использования ИИ и МО для выявления финансовых преступлений и борьбы с ними слишком велики, чтобы их игнорировать. Поскольку объем и сложность финансовых операций продолжают расти, а преступники становятся все более изощренными в своих тактиках, потребность в передовых технологиях для опережения становится все более острой. Внедряя ИИ и МО в рамках комплексной стратегии борьбы с финансовыми преступлениями, финансовые учреждения и регулирующие органы могут не только защитить целостность финансовой системы, но и способствовать повышению доверия клиентов и заинтересованных сторон.

В заключение следует отметить, что использование ИИ и МО в выявлении и противодействии финансовым преступлениям открывает перед финансовой индустрией широкие возможности для повышения

эффективности борьбы с преступностью и опережения возникающих угроз. Используя возможности этих технологий, финансовые учреждения могут повысить эффективность и результативность мониторинга транзакций, комплексной проверки клиентов и выявления мошенничества, а также получить ценные сведения о новых тенденциях и типологиях финансовых преступлений. Однако для успешного внедрения ИИ и МО требуется совместный междисциплинарный подход, позволяющий решить технические, этические и управленческие проблемы. Только совместная работа финансовых учреждений, регулирующих органов и поставщиков технологий позволит раскрыть весь потенциал ИИ и МО в борьбе с финансовыми преступлениями и создать более устойчивую и безопасную финансовую систему будущего.

Источники:

1. Васильева Т.В. АНАЛИЗ СОВРЕМЕННЫХ ТЕНДЕНЦИЙ НА РЫНКЕ FINTECH В РОССИИ // Фундаментальные исследования. – 2023. – № 11. – С. 15-19; [электронный ресурс] режим доступа: <https://fundamental-research.ru/ru/article/view?id=43511>
2. Брянов Г. А., Морозов С. В. Развитие финтех-стартапов в Российской Федерации //Глобальные рынки и финансовый инжиниринг. – 2019. – Т. 4. – №. 1. – С. 57-63
3. Giglio F. et al. Fintech: A literature review //European Research Studies Journal. – 2021. – Т. 24. – №. 2В. – С. 600- 627