Иордан Кирилл Иванович,
Магистрант направления «Бизнес-информатика»,
Кубанский Государственный Университет,
Краснодар

ПРЕИМУЩЕСТВА И ОГРАНИЧЕНИЯ МАШИННОГО ОБУЧЕНИЯ В УПРАВЛЕНИИ РИСКАМИ
ADVANTAGES AND LIMITATIONS OF MACHINE LEARNING IN RISK MANAGEMENT

Аннотация: В статье рассмотрены основные преимущества и ограничения применения методов машинного обучения в управлении рисками. Проанализированы ключевые аспекты использования алгоритмов машинного обучения, включая обработку больших объемов данных, обнаружение скрытых закономерностей и адаптацию к изменяющимся условиям. Также обсуждаются ограничения, связанные с качеством данных, интерпретацией моделей и этическими аспектами.

Ключевые слова: машинное обучение, управление рисками, прогнозирование, алгоритмы, кибербезопасность цифровизация

Машинное обучение (МО) стало неотъемлемой частью современных подходов к управлению рисками в различных отраслях, включая финансы, здравоохранение и кибербезопасность. Возможность с помощью сложных алгоритмов анализировать большие объемы данных и выявлять скрытые закономерности предоставляет новые возможности для прогнозирования и минимизации рисков.

Одним из ключевых преимуществ МО является его способность обрабатывать и анализировать большие объемы данных из различных источников. Это позволяет выявлять скрытые паттерны и аномалии, которые могут указывать на потенциальные риски. Например, в банковском секторе МО используется для обнаружения мошеннических операций путем анализа транзакционных данных и выявления нетипичного поведения клиентов [1].

Кроме того, МО способствует повышению точности прогнозов. Алгоритмы машинного обучения способны учитывать множество факторов и их взаимосвязи, что позволяет создавать более точные модели для оценки вероятности наступления тех или иных рисковых событий. В сфере кибербезопасности это выражается в способности предсказывать возможные атаки и принимать превентивные меры для их предотвращения [2].

Также, технологии машинного обучения имеют огромный потенциал в области защиты информационных систем. Они позволяют анализировать большие объемы данных и выявлять скрытые угрозы, которые могут быть незаметны для человека. Модели машинного обучения способны обучаться на основе большого количества исторических данных и выявлять аномалии с подозрительными активностями, что, в свою очередь, позволяет предотвратить наступление потенциальных атак и минимизировать ущерб для информационных систем [3].

Одним из основных преимуществ использования технологий ML в защите ИС является способность обнаруживать и идентифицировать новые и ранее неизвестные угрозы. Традиционные методы анализа данных могут быть неэффективными в случае появления новых видов атак, поскольку их работа основана на уже известных сигнатурах и шаблонах. В то время как алгоритмы машинного обучения могут обнаружить необычную или нехарактерную активность, которая может быть связана с неизвестными угрозами. Это позволяет оперативно реагировать на новые виды атак и разрабатывать соответствующие методы обнаружения и защиты.

Адаптивность МО также является значимым преимуществом. Модели машинного обучения могут обновляться и совершенствоваться по мере поступления новых данных, что позволяет им сохранять актуальность и эффективность в условиях быстро меняющейся среды. Это особенно важно в управлении рисками, где условия и угрозы постоянно эволюционируют.

Несмотря на очевидные преимущества, применение МО в управлении рисками сопряжено с рядом ограничений и вызовов. Одной из основных проблем является зависимость от качества данных. Неточные, неполные или предвзятые данные могут привести к ошибочным выводам и, как следствие, к неправильным управленческим решениям. Например, использование некорректных данных в модели оценки кредитоспособности может привести к неправильной оценке рисков и финансовым потерям [4].

Еще одним значимым ограничением является сложность интерпретации результатов, полученных с помощью МО. Многие алгоритмы, особенно глубокие нейронные сети, функционируют как "черные ящики", что затрудняет понимание того, как именно они приходят к тем или иным выводам. Это может быть проблематично в отраслях, где требуется прозрачность и обоснованность принимаемых решений, например, в финансовом секторе.

Кроме того, внедрение МО требует значительных вычислительных ресурсов и специализированных знаний. Не все организации обладают необходимой инфраструктурой и экспертным потенциалом для эффективного использования машинного обучения в своих процессах управления рисками.

Применение МО в управлении рисками также поднимает ряд этических и правовых вопросов. Например, использование персональных данных для обучения моделей может нарушать права на конфиденциальность. Кроме того, алгоритмы могут непреднамеренно усиливать существующие предвзятости, присутствующие в данных, что может привести к дискриминации определенных групп лиц. Это особенно критично в таких областях, как кредитование или найм персонала, где решения, основанные на МО, могут существенно влиять на жизнь людей.

Машинное обучение предоставляет мощные инструменты для повышения эффективности управления рисками, позволяя анализировать большие объемы данных, повышать точность прогнозов и адаптироваться к изменениям среды. Однако для успешного применения МО необходимо учитывать его ограничения, связанные с качеством данных, интерпретируемостью моделей и необходимыми ресурсами. Кроме того, важно обращать внимание на этические и правовые аспекты, чтобы обеспечить справедливость и законность принимаемых решений.

Список литературы:

1. Дядюнов Д. А. Машинное обучение для риск-менеджмента в банке: возможности и вызовы // Вестник науки. 2025. №1 (82) [Сайт] // – URL: https://cyberleninka.ru/article/n/mashinnoe-obuchenie-dlya-risk-menedzhmenta-v-banke-vozmozhnosti-i-vyzovy.

2. Ангапов В. Д., Бобров А. В., Тимонин В. А., Вишняков А. С. Использование технологий машинного обучения в защите информационных систем // Наука, техника и образование. 2023. №4 (92) [Сайт] // – URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologiy-mashinnogo-obucheniya-v-zaschite-informatsionnyh-sistem.

3. Ожиганова М.И., Куртаметов Э.С. Применение машинного обучения в защите веб-приложений // NBI-technologies. 2020. №2. С. 16-20.

4. Беликова Е.В. Machine learning в риск-менеджменте: стоимость входа // RAEX. – 2019 [Сайт] // – URL: https://raexpert.ru/press/articles/bo_belikov_jan2019/

5. Федоров, О. Л. Этические аспекты применения машинного обучения. – Новосибирск: НГУ, 2020. – 150 с.

6. Сидоров, В. П. Прогнозирование рисков с использованием методов машинного обучения. – СПб.: Политех, 2021. – 200 с.

7. Шунина Ю.С., Алексеева В.А., Клячкин В.Н. Прогнозирование кредитоспособности клиентов на основе методов машинного обучения // Финансы и кредит. – 2015. – № 27 (651). – С. 2-12.

8. Центр2М: Что такое цифровизация и какие сферы жизни она заденет [Сайт] // – URL: https://center2m.ru/digitalization-technologies?ysclid=liq1obz3em498589452

9. Мурзин А.В. Применение машинного обучения для анализа кредитных рисков // Финансы и аналитика. – 2021. – №3. – С. 32-38;

10. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации // Труды ИСП РАН. 2022. №5. С. 111-126.