УДК 004

Галяутдинов Р.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

СПОСОБЫ УПРАВЛЕНИЯ РИСКАМИ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В статье раскрыты особенности управления рисками информационной безопасности с помощью искусственного интеллекта. Особое внимание уделяется проблемам защиты информации и мерам безопасности при использовании искусственного интеллекта в работе с информационными рисками.

Ключевые слова: информация, информационная безопасности, риски, риски информационной безопасности, искусственный интеллект.

Внедрение искусственного интеллекта (ИИ) становится все более распространенным явлением в разнообразных сферах в современных реалиях. Компании непрерывно ищут инновационные способы интеграции ИИ в свои бизнес-процессы, стремясь к оптимизации и повышению производительности благодаря возможностям искусственного интеллекта.

Развитие ИИ охватывает множество областей. В каждой из этих областей существуют различные подходы, которые можно использовать как по отдельности, так и в комбинации для управления рисками. Это направлено на увеличение эффективности работы и достижение ключевых целей компаний. В настоящее время использование алгоритмов искусственного интеллекта с целью оценки вероятности наступления рисков получило широкое распространение в ряде областей:

– финансовый сектор: анализ финансовых операций для обнаружения признаков мошенничества и определения уровня риска для страховых компаний;

– здравоохранение: прогнозирование возможности наступления риска появления или усиления характера заболеваний, снижение нагрузки на систему здравоохранения;

– государственный сектор: анализ рисков государственных контрактов, предназначенный для улучшения результативности госзакупок и рационализации использования бюджетных средств;

– обеспечение информационной безопасности (ИБ): система управления рисками информационной безопасности направлена на обеспечение защиты информации организации, предотвращение финансовых потерь из-за инцидентов и поддержание прибыльности.

Традиционные подходы к управлению информационными рисками зачастую оказываются неэффективными в условиях динамичного развития информационных технологий. Возможности искусственного интеллекта по оперативной обработке больших массивов информации, выявлению взаимосвязей и прогнозированию потенциальных рисков делают его ключевым инструментом для современного бизнеса. Искусственный интеллект предлагает организациям средства для анализа рисков ИБ в режиме реального времени, автоматизации процессов принятия. Рассматривая применение ИИ при управлении рисками, потенциал особенно заметен в следующих областях: прогнозирование рисков путем анализа предыдущих периодов и выявления новых вероятных угроз ИБ, анализе рисков с помощью продвинутой аналитики, снижении рисков путем оптимизации ресурсов и превентивных мер защиты информации [1, с. 12–13].

Наиболее распространенными методами управления рисками информационной безопасностью с помощью искусственного интеллекта являются: искусственные нейронные сети, машинное обучение и глубокое обучение, обработка естественного языка.

Стоит отметить, что технологии обработки естественного языка (NLP) позволяют анализировать масштабные текстовые массивы, включая

публикации в соцсетях, статьи новостей и отзывы потребителей. Цель анализа – выявление признаков мошенничества на основе определенных ключевых слов, например, связанных с безопасностью крупного банка. В корпоративной среде для обнаружения мошеннических действий применяются программные решения, основанные на искусственном интеллекте, такие как Caseware, Feedzai и SAS [2, с. 44].

Реализация ИИ в управлении рисками и обнаружении мошенничества предоставляет организациям мощные инструменты для повышения безопасности и защиты активов. Однако, успешное внедрение требует комплексного подхода, учитывающего не только технические аспекты, но и вопросы этики, конфиденциальности и экономической целесообразности. Технологии ИИ применяются в нескольких областях управления рисками, например:

1. Выявление потенциальных рисков: ИИ применятся для изучения значительных объемов данных, чтобы находить отклонения, указывающие на вероятные риски.

2. Прогнозное моделирование: ИИ применяется построения для аналитических моделей, способных предвидеть возможность наступления тех или иных рисковых событий в перспективе.

3. Оценка рисков: ИИ помогает оценивать возможные последствия рисков и разрабатывать стратегии по их смягчению.

4. Выявление мошеннических схем: В сфере финансов ИИ идентифицирует махинации, анализируя структуру финансовых транзакций и выделяя нестандартные или вызывающие сомнения действия.

5. Автоматизация риск-комплаенса: ИИ автоматизирует процессы соответствия законодательным требованиям и профессиональным стандартам, таким образом, уменьшая риски, связанные с несоблюдением [3, с. 46].

Стоит отметить, что на рынке есть уже готовые решения для управления и анализа рисков для бизнеса с применением искусственного интеллекта:

– RiskVision от SAP: предлагает инструменты предиктивной аналитики и интеллектуального мониторинга бизнес-процессов, помогающие выявлять потенциальные угрозы;

– Oracle Risk Management Cloud: интегрированная платформа для комплексного управления корпоративными рисками с поддержкой машинного обучения;

– Qlik Risk Analytics: платформа визуализации и анализа больших объемов данных, позволяющая эффективно анализировать риски с помощью аналитического инструментария на основе AI.

В целом, внедрение ИИ в управление рисками приводит к повышению эффективности, снижению затрат и улучшению принятия решений. Однако важно помнить, что ИИ не является панацеей. Для успешного применения ИИ необходимо наличие качественных данных, опытных специалистов и четко определенных целей. Кроме того, важно учитывать

этические аспекты использования ИИ, чтобы избежать предвзятости и обеспечить прозрачность алгоритмов. Не следует забывать и о расходах на развертывание AI-решений, которые, учитывая современный дефицит и высокую цену опытных специалистов в сфере информационных технологий, могут оказаться чрезвычайно большими [4, с. 88].

Искусственный интеллект (ИИ) предоставляет компаниям множество способов для управления рисками. Он помогает быстро находить возможные проблемы, оценивать их серьезность и разрабатывать планы по смягчению последствий. Использование ИИ позволяет уменьшить непредсказуемость и сделать бизнес более устойчивым к внешним воздействиям. Чем больше компания использует современные технологии, тем лучше она сможет контролировать риски и достигать своих целей.

Список использованных источников:

1. Бессмертный И.А. Искусственный интеллект: учебное пособие / И.А. Бессмертный. СПб.: НИУ ИТМО, 2010. 132 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/43663 (дата обращения: 16.04.2025).

2. Бондаренко И.С. Информационная безопасность: учебник / И.С. Бондаренко. М.: МИСИС, 2023. 254 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/360344 (дата обращения: 13.04.2025).

3. Жданов А.А. Автономный искусственный интеллект: учебное пособие / А.А. Жданов. 5-е изд. (эл.). М.: Лаборатория знаний, 2024. 362 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/387629 (дата обращения: 16.04.2025).

4. Кацов И. Искусственный интеллект на предприятии: руководство / И. Кацов; перевод с англ. В. С. Яценкова. М.: ДМК Пресс, 2024. 710 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/456725 (дата обращения: 16.04.2025).

Galyautdinov R.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

RISK MANAGEMENT CAPABILITIES WITH ARTIFICIAL INTELLIGENCE

Abstract. The article reveals the features of information security risk management using artificial intelligence. Special attention is paid to the

problems of information protection and security measures when using artificial intelligence in dealing with information risks.

Keywords: information protection rights, information security, risks, information security risks, artificial intelligence.