тание технических, организационных и человеческих факторов способно обеспечить реальную устойчивость промышленных систем к киберугрозам.

Литература

1. ГОСТ Р 56939-2016. Защита информации. Обеспечение безопасности промышленных систем управления.
2. ISO/IEC 27001:2022. Information Security Management Systems – Requirements.
3. Грачев, П. А. Кибербезопасность промышленных систем. – СПб. : Питер, 2020.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРИКЛАДНЫХ ПРИЛОЖЕНИЯХ

П. С. Мырадов

Государственный энергетический институт Туркменистана, г. Мары

Современные технологии искусственного интеллекта (ИИ) активно интегрируются в различные сферы человеческой деятельности, такие как медицина, финансы и образование. Машинное обучение и обработка естественного языка становятся основой прикладных решений, способных анализировать большие объемы данных, прогнозировать события и автоматизировать сложные процессы. В медицине ИИ помогает в диагностике заболеваний и персонализированном лечении, в финансовой сфере – в управлении рисками и выявлении мошенничества, а в образовании – в создании адаптивных систем обучения. Использование ИИ способствует повышению эффективности, точности и доступности услуг. Однако его внедрение требует соблюдения этических принципов и защиты персональных данных.

Ключевые слова: искусственный интеллект, машинное обучение, обработка естественного языка, автоматизация.

USING ARTIFICIAL INTELLIGENCE IN APPLICATIONS

P. S. Myradov

The State Energy Institute of Turkmenistan, Mary, Turkmenistan

Modern artificial intelligence (AI) technologies are increasingly integrated into various areas of human activity such as medicine, finance, and education. Machine learning and natural language processing form the basis of applied solutions capable of analyzing large data sets, predicting outcomes, and automating complex processes. In medicine, AI aids in disease diagnosis and personalized treatment; in finance – in risk management and fraud detection; in education – in creating adaptive learning systems. The use of AI improves efficiency, accuracy, and accessibility of services. However, its implementation requires adherence to ethical principles and data protection.

Keywords: artificial intelligence, machine learning, natural language processing, automation.

Развитие искусственного интеллекта (ИИ) стало одним из ключевых направлений цифровой трансформации общества. Сегодня ИИ перестал быть абстрактным понятием из научной фантастики и превратился в мощный инструмент, внедряемый в практические решения, направленные на повышение эффективности и точности в разных сферах деятельности человека. В основе большинства прикладных приложений лежат алгоритмы машинного обучения и методы обработки естественного языка, которые позволяют системам не просто выполнять запрограммированные действия, но и обучаться на данных, выявлять закономерности и принимать решения [1, с. 25].

В медицинской практике искусственный интеллект используется для анализа изображений, прогнозирования заболеваний и выбора оптимальных схем лечения.

Например, системы компьютерного зрения, основанные на нейронных сетях, способны с высокой точностью распознавать опухоли на рентгеновских снимках и МРТ, превосходя по эффективности традиционные методы диагностики [1, с. 47]. Это не только ускоряет процесс постановки диагноза, но и снижает риск человеческих ошибок.

В финансовом секторе ИИ применяется для анализа поведения клиентов, выявления мошеннических операций и управления инвестиционными портфелями. Алгоритмы машинного обучения анализируют миллионы транзакций, определяя подозрительные паттерны и предотвращая финансовые преступления [2, с. 112]. Кроме того, технологии ИИ используются для прогнозирования рыночных тенденций, что помогает компаниям принимать стратегические решения на основе данных, а не интуиции.

В сфере образования ИИ способствует формированию персонализированных образовательных траекторий. Интеллектуальные обучающие системы анализируют успеваемость студентов и подбирают учебные материалы в зависимости от их уровня подготовки и стиля обучения [3, с. 64]. Такие подходы позволяют повысить мотивацию учащихся и эффективность образовательного процесса. Более того, чат-боты на основе обработки естественного языка предоставляют студентам круглосуточную поддержку и помогают решать учебные вопросы в интерактивной форме.

Интеграция искусственного интеллекта в прикладные приложения открывает новые горизонты для развития человеческого общества. В медицине ИИ спасает жизни, в финансах – обеспечивает безопасность и устойчивость, а в образовании – делает процесс обучения более гибким и доступным. Однако для успешного внедрения необходимо уделять внимание этическим вопросам, конфиденциальности данных и прозрачности алгоритмов. В будущем роль ИИ будет только возрастать, и от того, насколько ответственно человечество подойдет к его использованию, зависит эффективность и безопасность цифрового прогресса [2, с. 118].

Литература

1. Кудрявцев, А. И. Искусственный интеллект и машинное обучение: современные тенденции и приложения / А. И. Кудрявцев. – М. : Наука, 2021. – 256 с.
2. Новиков, Д. А. Технологии искусственного интеллекта в экономике и управлении / Д. А. Новиков. – СПб. : Питер, 2022. – 304 с.
3. Смирнова, Е. В. Цифровизация образования: роль искусственного интеллекта / Е. В. Смирнова // Образовательные технологии и общество. – 2023. – № 2. – С. 60–70.

МЕТОДЫ ЗАЩИТЫ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

А. М. Хамраев

Государственный энергетический институт Туркменистана, г. Мары

Рассмотрены ключевые методы защиты данных, применяемые в телекоммуникационных системах. Особое внимание уделено криптографическим технологиям, аутентификации, контролю доступа и новым направлениям – гомоморфному шифрованию и дифференциальной приватности. Цель исследования – определить наиболее эффективные подходы к обеспечению безопасности данных в условиях возрастающих угроз и усложняющихся сетевых архитектур. Методика основана на анализе современных публикаций и практического опыта специалистов отрасли. Результаты показывают, что комплексное сочетание классических и инновационных методов защиты позволяет повысить устойчивость сетей к несанкционированному доступу и утечкам информации.

Ключевые слова: телекоммуникации, защита данных, шифрование, аутентификация, приватность.