УДК 33 DOI: 10.14451/1.232.50

Использование искусственного интеллекта в цифровой экономике и проблемы безопасности

© 2024 **Аничкина Ольга Александровна**
Кандидат экономических наук, доцент кафедры финансов, бухгалтерского учета и экономической безопасности. Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: F-1980@yandex.ru

© 2024 **Левченко Анастасия Михайловна**
Магистрант кафедры финансов, бухгалтерского учета и экономической безопасности. Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: mar.levchenko2010@yandex.ru

© 2024 **Апачанов Антон Сергеевич**
Кандидат технических наук, доцент кафедры финансов, бухгалтерского учета и экономической безопасности. Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: aasprof@mail.ru

© 2024 **Долгов Константин Вадимович**
Магистрант кафедры финансов, бухгалтерского учета и экономической безопасности. Московский государственный университет технологий и управления им. К. Г. Разумовского (Первый казачий университет), Россия, Москва.
E-mail: mar.levchenko2010@yandex.ru

Ключевые слова: искусственный интеллект, цифровая экономика, безопасность, кибербезопасность, защита данных, конфиденциальность, регулирование, этические соображения, машинное обучение, автоматизация, управление рисками, интеграция технологий, инновации, корпоративные решения, обнаружение угроз.

В статье исследуется роль искусственного интеллекта в цифровой экономике, и рассматриваются проблемы, связанные с уязвимостями безопасности. Представлен обзор текущих тенденций внедрения искусственного интеллекта, подчеркнуты преимущества, которые он приносит предприятиям, и определены ключевые риски безопасности, связанные с его внедрением. Статья призвана повысить понимание последствий использования искусственного интеллекта в цифровой экономике и предлагает рекомендации для будущих исследований и практики.

Искусственный интеллект (далее ИИ) относится к разработке компьютерных систем, которые могут выполнять задачи, не требующие человеческого участия. Эти задачи включают обучение, рассуждение, решение проблем, восприятие и понимание языка. Целью является создание машин, которые смогут имитировать когнитивные процессы, подобные человеческим, позволяя им принимать решения, распознавать закономерности и адаптироваться к новым ситуациям без явного программирования.

Цифровая экономика включает в себя экономическую деятельность, осуществляемую с помощью цифровых технологий и сетей. Она включает в себя производство, распространение и потребление товаров и услуг при помощи цифровых платформ и электронных устройств. В цифровой экономике транзакции, общение и взаимодействие происходят преимущественно онлайн, что приводит к повышению эффективности, инновациям и глобализации рынков.

Под безопасностью понимается защита активов, ресурсов и информации от несанкционированного доступа, кражи, повреждения или разрушения. В контексте цифровых систем и сетей меры безопасности направлены на защиту разных данных, включая конфиденциальную информацию, личные данные, транзакции и интеллектуальную собственность. Методы обеспечения безопасности включают в себя принятие мер для предотвращения проблем и обеспечение надёжности.

Различные сферы в экономике изменил преимущественно искусственный эффект от этого — это продуктивность и уклон к инновациям.

Как пример, отрасль здравоохранения, где системы на базе искусственного интеллекта используются для анализа медицинских данных, диагностики заболеваний и персонализации планов лечения пациентов. Использование алгоритмов машинного обучения повышает точность диагностики, прогнозирование результатов лечения и оптимизации распределения ресурсов, что приводит к улучшению результатов лечения пациентов и снижению трат.

Сферы использования искусственного интеллекта:

- Интеллектуальный анализ данных.
- Обработка естественного языка.
- Компьютерное зрение.
- Распознование и синтез речи.
- Автоматизация процессов.

В финансовой индустрии алгоритмы используются для обнаружения мошенничества, оценки рисков и управления инвестициями. Банки и финансовые учреждения используют решения на основе искусственного интеллекта для анализа огромных объемов транзакционных данных в режиме реального времени, обнаружения подозрительных действий и предотвращения мошеннических транзакций. Алгоритмы ИИ используются для оптимизации торговых стратегий, прогнозирования рыночных тенденций и автоматизации рутинных задач.

Технологии ИИ могут быть полезны в обрабатывающей промышленности. Системы прогнозирования помогают производителям предвидеть сбои оборудования, минимизировать время простоя и оптимизировать графики технического обслуживания. Системы автоматизации на базе искусственного интеллекта повышают эффективность производства за счет оптимизации производственных процессов, улучшения качества продукции и обеспечения гибкой настройки в соответствии с требованиями клиента.

Магазины используют искусственный интеллект, чтобы улучшить обслуживание покупателей, персонализировать рекламу и управлять запасами товаров. Это необходимо для анализа данных о клиентах, прогнозирования покупательского поведения и рекомендации персонализированных продуктовых предложений, что приводит к повышению удовлетворенности клиентов и повышению прибыли. Персонализированную поддержку клиентам обеспечивают онлайн-помощники. Это помогает сделать процесс покупки чего-либо более удобным.

Исследования показывают, что ИИ способствует развитию разных отраслей и положительно влияет на качество принимаемых решений. Искусственный интеллект постоянно развивается и его влияние растёт. В будущем, вероятно, ИИ будет ещё глубже интегрирован в общество.

Сейчас нейросети помогают компаниям экономить ресурсы и повышать эффективность работы. Быстрота и точность является преимуществом искусственного интеллекта.

Ключевые свойства достоинств ИИ:

- Понимание языка.
- Обучение.
- Способность мыслить.
- Действовать.

Через выявление предпочтений и поведения покупателей, компания более эффективно адаптирует свои продукты и услуги для удовлетворения потребностей клиентов. Это даёт рост продаж и повышает лояльность клиентов.

Рабочие могут работать эффективнее, используя инструменты и системы, лучше общаться с потенциальными клиентами и быстрее получать доступ к нужной информации, оптимизировать планирование встреч, управление документами. Искусственный интеллект помогает компаниям оставаться на шаг впереди и адаптироваться к переменам проще.

Применение ИИ в цифровой экономике влечёт за собой риски. Они связаны с проблемами при анализе большого количества данных и с незаконным распространением личной информации. Для бизнеса это означает потерю денег и репутации. Данные как крупных, так и мелких компаний являются конфиденциальными. Если эти данные станут доступны общественности — это сильно ударит по финансам и репутации бренда. Последствия могут проявиться как в виде увольнения сотрудников, так и в снижении лояльности сотрудников.

Умышленная кража данных, активность мошенничества, манипуляция и шпионаж — это всё имеет долгосрочные последствия. Затрагивая любую сферу и любого человека, это может сказаться на дальнейшей жизни всего живого и материального.

Конфиденциальность информации — что-то высшее в наше время, сейчас каждый находится в любой доступной социальной сети, имеет доступ ко многим ресурсам, на которых оставляет свои данные, будь то паспорт, имя или номер личного счёта. Нарушение приватности подрывает не только безопасность одного человека, ведь человек может хранить многое на своём устройстве, а эта цепочка уже подрывает структуру общества.

Необходимо учитывать и продумывать шаги для их устранения. Нам необходимо убедиться, что ИИ используется этично, ответственно и с соблюдением надлежащих мер безопасности для защиты конфиденциальности людей, обеспечения справедливости и снижения потенциального вреда.

Последствия нарушений безопасности могут быть далеко идущими и долгосрочными, затрагивая не только бизнес, но и структуру самого общества. Вот почему так важно учитывать безопасности в сети и принимать меры предосторожности для предотвращения и сокращения рисков нарушений безопасности.

Использование пароля или тайного шифра — выход для желающих максимально защититься от окружающего мира и обезопасить свои личные данные. Пользуясь паролем, человек может максимально оградить себя от потенциальных вредителей, ведь только от него теперь зависит спокойствие и надежность данных.

Разновидность паролей включает цифровые, буквенные, смешанные, отпечатки пальцев, сетчатки глаза, распознавание голоса. Используя надежные пароли, а иногда мешая их между собой, люди закрывают от других самое ценное.

Польза ИИ проявляется также в его умении учитывать происходящие вокруг негативные события. Обнаруживая угрозу раньше, чем мы её сами заметим, ИИ посылает нам информацию

в виде смс, звонка, оповещения и помогает нам вовремя среагировать и не потерять спрятанные данные. Человек уязвим, именно поэтому так важно искать как можно более надежные практики для осуществления надзора за нашей деятельностью, которые могут быть большой угрозой.

Сохранять бдительность человека помогают именно возможности ИИ, так как они быстрее реагируют на подозрительную активность в сети.

Коммерция в интернете не для кого уже не новость, а это значит, что это хлеб для мошенников. Чем легче становится совершать покупку, тем бдительнее нужно быть при оформлении и уже доставленной проверке товара.

Гиг-экономика — речь идет о людях, которые занимаются внештатной работой и выступлениями в Интернете, будь то вождение в Uber, доставка еды для DoorDash или работа в качестве внештатного писателя. ИИ меняет наше стандартное представление об уровне комфорта и заработка, указывая людям на большую гибкость и возможности зарабатывать на жизнь более удобным путём.

Покупка, продажа, сдача, обмен, обсуждение условий — всё это стало максимально легким. Теперь позволить себе что-то приобрести может каждый, у кого есть гаджет или это может вам помочь сделать тот, у кого он есть, а это значительно сокращает время, деньги, ведь даёт возможность решить всё в удобный для вас момент.

Сохранение личных данных, а иногда и их сокрытие, стало в наш век основной задачей у программистов и тех, кто имеет отношение к разработкам ИИ. Именно через возможности ИИ и качественно построенный процесс сейчас каждый, кто имеет бизнес, может регулировать просмотры в сети, частоту ответов или просто работу персонала, чтобы получить представление о поведении потребителей, персонализировать продукты и услуги и принимать более разумные решения относительно бизнеса.

Новое будущее строим именно мы — активные пользователи сети. Ведь сети для нас — сейчас это дом, работа, наше детище. Технологии улучшаются, а общество адаптируется к его изменениям, мы можем ожидать еще больше событий в мире цифровой коммерции.

Обнаружение угроз — представляет собой алгоритм искусственного интеллекта для анализа закономерностей и поведения данных и выявления любых признаков подозрительной активности. Контролируя сетевой трафик, поведение пользователей и системные журналы, системы искусственного интеллекта могут обнаруживать аномалии, которые могут указывать на происходящую атаку на ваши данные.

Автоматическая реакция на угрозы — это уникальная система. Блокировка нежелательного трафика, изоляция зараженных устройств или исправление уязвимостей, системы искусственного интеллекта могут быстро принять меры по сдерживанию и смягчению последствий кибератак до того, как они нанесут серьезные последствия.

Активное использование не одного, а нескольких процессов и платформ, улучшают общее состояние безопасности и защиты уже наступивших или от ещё развивающихся угроз, что представляет единую стратегию защиты.

Применяя именно разные подходы, вы сможете добиться быстрого реагирования на угрозы, уменьшая негативные инциденты в вашей жизни или жизни ваших клиентов, что снижает риск утечки данных и защищает конфиденциальную информацию.

Ход цифровой экономики меняет именно приспосабливаемость человечества к искусственному интеллекту. От повышения эффективности и производительности до стимулирования инноваций и роста это помогает менять способы ведения бизнеса.

ИИ обладает колоссальным успехом и интересом среди населения по всему миру и крайне

важно действовать осторожно и принимать любые благоприятные меры для решения проблем безопасности. Любая система, даже самая идеальная, имеет в себе недочёты, ведь из-за большого объема анализа данных, есть высокий риск потери данных, так как нельзя контролировать всё и сразу. Но для того чтобы не бояться использовать возможности искусственного интеллекта, внедряя надежные меры и сохраняя бдительность, мы можем обеспечить долгое и спокойное будущее.

Всем важно учитывать внимание кибербезопасности и инвестировать в передовые технологии безопасности, чтобы защитить свои данные и системы от киберугроз. Это означает внедрение инструментов шифрования, аутентификации и обнаружения угроз, а также проведение комплексного обучения сотрудников.

Необходимо более тесно сотрудничать и чаще обмениваться информацией между заинтересованными сторонами для эффективной борьбы с киберугрозами. Это включает в себя обмен информацией об угрозах, передовым опытом и извлеченными уроками для повышения коллективной защиты.

Именно тем, кто имеет власть над большим количеством людей, а именно политическим деятелям или просто тем, кто имеет отношение к управлению жизнью людьми, нужно обеспечить соблюдение стандартов безопасности. Обеспечить грамотное использование ИИ и защищать права людей на неприкосновенность частной жизни — это главная задача в современное время, ведь с каждым годом становится всё больше тех, кто хочет нажиться на ком-то другом. Через законы о защите данных, защите частного права и собственности, мы поможем в создании систем для полной безопасности.

Добавляя к вышесказанному, также помогут опережать угрозы мониторинг, оценка и адаптация, а также пресечение, выявление и помощь тем, кто попадает в ситуацию с утечкой данных или в руки к мошенникам. Дружное и сплочённое внедрение и контроль над деятельностью ИИ помогут снизить риски и обеспечить устойчивость к недочётам.

В заключение в статье подчеркивается значительное влияние искусственного интеллекта на цифровую экономику, подчеркивая его потенциал для стимулирования инноваций и повышения эффективности. Также подчеркивается важность устранения рисков безопасности, связанных с внедрением ИИ.

Снижать вред необходимо через комплекс мер, внимательному отношению к проблеме, неравнодушию, которое только способствует устранению возникающих проблем. Осторожные, но тщательные и только активные, а не пассивные подходы необходимы для улучшения всего потенциала искусственного интеллекта в формировании стабильной, честной и качественной экономики любой страны мира.

На протяжении всей статьи мы искали и анализировали связь ИИ и безопасности. Предлагая ценную информацию о рисках, плюсах и минусах, преимуществах и рекомендациях в различных секторах экономики.

Только через баланс между разными подходами экономика, население и сами процессы могут подвинуться к решению проблем безопасности. Важность сотрудничества пересекается с бдительностью, анализом того, что происходит вокруг и того, что вам предлагают защитить цифровые активы и укрепить доверия к новым технологиям. Ведь большое значение для чего-то нового имеет именно улучшение уже старого. Рассмотрение проблем доказывает то, что необходим не прекращаемый контроль и поиск разных улучшений, будь то честность в людях или внедрение всё больших возможностей, которые предлагает нам окружающий нас мир. Статья содержит в себе только полезную и необходимую информацию как для обычных людей, так и для нынешних и будущих исследователей, практиков и политиков, стремящихся разобраться в проблемах и стремящихся прийти к конечному улучшению ситуации, преследуя при этом только безопасность и желание будущего и нынешнего процветания общества.

Библиографический список

1. *Архипов В. В.*, *Наумов В. Б.* Теоретико-правовые вопросы охраны прав человека при использовании биометрических данных системами искусственного интеллекта: европейский опыт // Вестник Удмуртского университета. Серия Экономика и право. — 2022.
2. *Бегишев И. Р.* Робототехника и право. — Проспект, 2022. — 120 с.
3. *Бутл Р.* Искусственный интеллект и экономика: Работа, богатство и благополучие в эпоху мыслящих машин. — Альпина Паблишер, 2023. — 424 с.
4. *Душкин Р. В.* Искусственный интеллект. — ДМК Пресс, 2019. — 280 с.
5. *Карамова О. В.*, *Терская Г. А.*, *Соловых Н. Н.* Человеческий капитал в модели устойчивого экономического роста России. — Прометей, 2023. — 514 с.
6. *Козлова Н. Ш.*, *Довгаль В. А.* Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. — 2023.
7. *Козырева А. А.*, *Надтока Р. В.*, *Хряков А. В.* Правовые подходы к минимизации рисков, связанных с применением технологий искусственного интеллекта // Социально-политические науки. — 2021.
8. *Мануйленко В. В.*, *Вититникова Я. Ю.*, *Конарева Ю. И.* Влияние банковских инноваций на развитие теневых экономических отношений в регионе. — Финансы и статистика ЭБС, 2022. — 283 с.
9. *Минин А. Я.* Актуальные проблемы цифрового права: учебное пособие для магистрантов и бакалавриата. — Московский педагогический государственный университет, 2021. — 132 с.
10. *Никитин Г. М.*, *Никитина Е. А.* Социальные и философские проблемы информационного общества. — Лань, 2024. — 76 с.
11. Проблемы трансформации системы законодательства в условиях развития цифровых технологий. — Проспект, 2021. — 176 с.
12. Реализация конституционных социальных прав и свобод с использованием искусственного интеллекта. — Проспект, 2022. — 208 с.
13. *Сердюков Ю. М.* Философия виртуальной реальности и искусственного интеллекта. — Дальневосточный государственный университет путей сообщения, 2020. — 169 с.
14. *Старостина Т. Г.*, *Романенко Е. В.* Искусственный интеллект в банковской сфере // Вестник Ульяновского государственного технического университета. — 2022.
15. *Федорченко С. Н.* Значение искусственного интеллекта для политического режима россии: проблемы легитимности, информационной безопасности и «мягкой силы» // Вестник Московского государственного областного университета. Серия: История и политические науки. — 2020.
16. *Харитонова Ю. С.*, *Савина В. С.*, *Паньини Ф.* Гражданско-правовая ответственность при разработке и применении систем искусственного интеллекта и робототехники: основные подходы // Вестник Пермского университета. Юридические науки. — 2022.
17. Цифровая экономика: концептуальные основы правового регулирования бизнеса в России. — Проспект, 2021. — 490 с.
18. Цифровое право : учебник. — Проспект, 2020. — 637 с.
19. Человек и системы искусственного интеллекта / В. А. Лекторский [и др.]. — Юридический цент, 2022. — 328 с.
20. *Чесалин А. Н.* Основы искусственного интеллекта с приложениями в информационной безопасности. — МИРЭА — Российский технологический университет, 2020. — 75 с.