УДК 331.452:004.89

Игнатьева Елена Александровна, аспирант, старший преподаватель,
(КузГТУ, г. Кемерово)
Elena A. Ignatieva, postgraduate student, senior lecturer
(KuzGTU, Kemerovo)
Федосов Алексей Алексееевич, студент
(КузГТУ, г. Кемерово)
Aleksey.A. Fedosov, student
(KuzSTU, Kemerovo)

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА БЕЗОПАСНОСТЬ НА РАБОЧЕМ МЕСТЕ

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON WORKPLACE SAFETY

Невозможно точно сказать, полезен или вреден искусственный интеллект для рабочего процесса. Человек создал новые технологии, чтобы упростить себе многие сферы жизни. Ни одно действие в рабочих отраслях не обходится без помощи искусственного интеллекта. Как же он влияет на безопасность процессов на рабочем месте?

Obviously, it is impossible to say for sure that artificial intelligence is useful or harmful to the work process. Man has created new technologies to simplify many areas of life. Not a single action in the working industries can do without the help of artificial intelligence. How does it affect the safety of processes in the workplace?

Ключевые слова: искусственный интеллект, безопасность, рабочее место, система СКУД (система контроля управления доступом), персональные данные, транспорт, видеонаблюдение.

Рассмотрим один из основных показателей, влияющий на работоспособность человека и способность находится в нормальном состоянии на рабочем месте. Этим показателем является здоровье. Так вот, по данным на сентябрь 2024 года, в Российской федерации, Росздравнадзором зарегистрировано 37 медицинских изделий на основе искусственного интеллекта (далее – ИИ). [1]

Благодаря использованию ИИ в анализе медицинских изображений и автоматическому распознаванию патологий, значительное развитие получили лучевая диагностика и пат морфология (исследования изменений

в клетках, тканях и органах, позволяющие, например, провести дифференциальную диагностику между злокачественными и доброкачественными опухолями). Можно сделать вывод, что минимизация повторных диагностических процедур пациента минимизирует риск облучения как самого пациента, так и медицинского работника. Это позволяет говорить о положительном влиянии ИИ на рабочем месте медицинского персонала.

Высокоинтеллектуальные машины и искусно сделанные роботы выполняют сложнейшие задачи, которые ранее могли выполняться исключительно людьми. ИИ использует технологии, основанные на обработке больших объемов данных и распознавании паттернов в этих данных. Это позволяет машинам «учиться на опыте» и впоследствии выполнять самые сложные задачи. В сфере здравоохранения ИИ опирается на прогностические алгоритмы, которыми руководствуются врачи в своей медицинской практике. [2]

Рассмотрим обратную сторону «медали». В мире очень тщательно отслеживают действия медицинских работников. Очень часто выявляют врачебные ошибки, которые анализируют и расследуют. Не редко причиной такой ошибки и оказывается ИИ. Ведь данные, которые обрабатывает машина, вносит человек. Для эффективной работы ИИ должен постоянно получать высококачественные наборы данных, что неизбежно затрагивает конфиденциальность персональных данных пациентов. На сегодняшний день в сфере защиты персональных данных существует ряд основополагающих принципов. Одним из таких принципов является принцип минимизации данных – концепция, согласно которой данные не должны собираться, использоваться или храниться дольше, чем требуется для достижения целей их обработки. Кроме того, субъект персональных данных должен быть изначально извещен о целях обработки персональных данных.

ИИ создает серьезные проблемы для минимизации данных ввиду следующего:

1) центральным фактором успеха в работе ИИ является максимизация данных, а не их минимизация;

2) зачастую в работе ИИ не всегда заранее известно, какие элементы данных будут полезны для принятия конкретного решения;

3) данные, собранные и обработанные ранее, могут быть чрезвычайно полезны для будущей работы ИИ, ввиду этого нельзя изначально указать цели обработки персональных данных [3].

Одним из решений данной проблемы может стать обезличивание персональных данных. Однако ИИ может повторно идентифицировать пациентов из обезличенных наборов данных. Как было указано ранее, ИИ функционирует только тогда, когда ему предоставляется устойчивый поток данных в значительных объемах. Обычно эти данные собираются в наборах

«больших данных» или больших агрегированных базах данных, хранящихся у облачного провайдера. Для заполнения базы данных организации часто также закупают обезличенные наборы данных, например, у страховых организаций или используют общедоступные наборы данных. Когда эти наборы данных объединяются и запускается утилита ИИ, любой пациент со значительной вероятностью может быть повторно идентифицирован. Если алгоритмы станут неотъемлемой частью медицинской помощи и врачи станут зависимы от этих систем для принятия решений, пациенты, которые не делятся своими медицинскими данными, могут не получить надлежащее лечение [4]. С этой точки зрения безопасность использования ИИ на рабочем месте (в данном случае – в медицинском учреждении) неоднозначна.

А если рассмотреть использования ИИ в виде камер видеонаблюдения, фиксации материала, обработки данных и передаче информации в различные правоохранительные органы, становится понятным, что это улучшает безопасность на рабочем месте, т.е. минимизирует мошенничество, несчастные случаи, влияние вредных и/или опасных факторов на жизнь и здоровье людей и т.д. На российском рынке продукты видео аналитики представлены решениями отечественных и мировых производителей, часто оснащающих свои камеры наблюдения различными встроенными функциями анализа видеопотока. Постепенно видео аналитика превращается в явление, с которым мы сталкиваемся практически ежедневно. Она используется в сканерах 2D-кодов и отпечатков пальцев, счетчиках посетителей в торговых точках, устройствах слежения за усталостью водителя и др. [5]

Нельзя обойти использование ИИ в транспортной сфере. Искусственный интеллект постепенно начал трансформировать наши транспортные средства посредством интегрированных инноваций различных марок автомобилей. Производители автомобилей используют искусственный интеллект практически во всех аспектах процесса производства автомобилей. Примерами искусственного интеллекта в автомобильной промышленности являются промышленные роботы, создающие транспортное средство, и автономные автомобили, управляющие дорожным движением с помощью машинного обучения и видения. Хотя многие считают, что будущее за персональными автономными транспортными средствами, существует множество способов внедрения искусственного интеллекта и машинного обучения в то, как создаются транспортные средства и как они эксплуатируются на дороге. Искусственный интеллект в автомобилях направлен на повышение безопасности транспортных средств, повышение топливной экономичности и предоставление водителям расширенных возможностей подключения. [6] По мере того, как ИИ становится все более доступным для производителей транспортных средств, многие автомобильные компании ставят во главу

угла одну центральную цель: безопасность. Безусловно, исследования в области разработки технологии «умных автомобилей» сосредоточены, в частности, на проблеме восприятия окружающей среды: инфраструктуры, других транспортных средств, пешеходов или любого другого объекта, который может рассматриваться как препятствие для автомобиля. Радары, датчики, камеры, погодные условия, дорожные работы и другие чрезвычайные события: машина должна быть способна распознавать каждый тип внешнего воздействия и оценивать его возможное влияние на траекторию движения автомобиля, чтобы вносить соответствующие коррективы в систему управления движением в режиме реального времени. Так, Tesla, производитель автомобилей, ускоряющий переход мира к устойчивой энергетике, является одним из лидеров по внедрению искусственного интеллекта в автомобилестроении с момента своего основания в 2003 году. Одним из основных нововведений компании является внутренняя камера на базе искусственного интеллекта над зеркалом заднего вида для повышения безопасности в салоне. Используя инновации в области ИИ, камера обнаруживает и отслеживает глаза водителей, чтобы распознать их сонливость и избежать дорожно-транспортных происшествий. Технология основана на технологии нейронных сетей компании, которая анализирует изображения дорог для выполнения обнаружения объектов и оценки глубины. Используя высококачественные обучающие данные, полученные из автопарка компании, насчитывающего почти 1 миллион автомобилей, в режиме реального времени, ИИ компании эффективно предупреждает водителей о возможных рисках, чтобы избежать столкновений. Безусловно, что будущее автомобильной промышленности будет связано с ИИ. Более того, учитывая многие другие тенденции в области искусственного интеллекта в автомобильной промышленности, предполагается, что беспилотные автомобили появятся на улицах к 2030 году. Согласно исследовательским отчетам, по оценкам, мировые продажи систем автономного вождения достигнут 80 миллионов единиц к 2032 году. Ожидаемые темпы роста невероятны и создают плодотворный бизнес для производителей интеллектуальных автомобилей. В отчетах исследований говорится, что доля рынка полностью автоматизированного вождения составит всего 0,01% в 2023 году. А к 2030 году его доля на автомобильном рынке достигнет 19%. [7]

Следует отметить отличную безопасность работников на местах, благодаря использованию системы СКУД, оснащенную ИИ. Эти системы используются не только в офисах, но и в жилых комплексах, по той причине, что они являются дополнительным и достаточно надежным рубежом защиты от проникновения на территорию нежелательных лиц. А в совокупности с другими системами позволяет реализовать достаточно функциональную систему защиты и обеспечения безопасности. Говоря о

системах контроля и управления доступом, уже неоднократно отмечался тот факт, что это зачастую сложная система, в состав которой входят различные устройства [8].

К их числу относятся:

1. Контроллер – это центральное устройство, отвечающее за функционирование всей системы и входящей в её состав устройств. Непосредственно в нем хранятся все идентификаторы, на основании которых контроллером будет принято решение о допуске владельца идентификатора на охраняемую территорию. В том случае, если СКУД обладает довольно обширным масштабом, допускается использование в ее составе сразу нескольких контроллеров, которые объединяются между собой посредством сети передачи данных.

2. Исполнительные устройства в составе СКУД – это оборудование, управляемое контроллером. Устройства данного типа делят на две категории – устройства, монтируемые на дверях, и устройства, монтируемые на проходах. Данные устройства являются механизмами, которые более всего подвержены износу в рамках работы СКУД, по причине чего требуют выполнения не только настройки их работы, но и периодического технического обслуживания. К данным устройствам относятся: замки, защелки, ворота, турникеты, шлюзовые кабины, барьеры.

3. Идентификаторы – это устройства, в которых записывают специальный код доступа. Визуально представляют собой брелок, карту памяти или иной небольшой предмет, который выдается сотруднику, для которого был назначен записанный в идентификатор код доступа. Существует еще вариант, когда в роли идентификатора выступает специальный цифровой код, набираемые на цифровой панели доступа, либо в качестве идентификатора могут выступать определенные биометрические данные – отпечаток пальца, изображение сетчатки глаза и т.д.

4. Считыватели – устройства, выполняющие работу по считыванию кода из идентификатора и передаче его на контроллер. В зависимости от используемых в системе идентификаторов могут быть использованы и различные считыватели – начиная от простых считывателей магнитных карт и заканчивая сканерами сетчатки глаза или отпечатка пальца.

5. Вспомогательное оборудование – это технические средства, которые применяют для обеспечения корректного взаимодействия между перечисленными выше элементами СКУД. Наиболее ярким примером данного оборудования являются конверторы сигналов, блоки питания, датчики и т.д. Их использование обусловлено необходимостью обеспечения надежной и удобной работы СКУД.

6. Программное обеспечение – это необязательный компонент СКУД, однако оно существенно расширяет функционал СКУД в плане контроля работы оборудования системы, выполнения анализа со стояния устройств и оповещения ответственных сотрудников о различных происшествиях [9].

Несмотря на неточности в системе ИИ или несовершенстве пользования данными, которые имеются на сегодняшний день, развитие этой отрасли продвигается оперативно. Ошибки в ходе использования ИИ анализируются и устраняются. Таким образом, изучив информацию об интеграции ИИ с рабочими процессами в жизни людей, можно сделать вывод, что ИИ в целом оказывает положительное влияние.

Список литературы

1. Сведения о медицинских изделиях в РФ. Росздравнадзор http://www.roszdravnadzor.ru/services/misearch

2. Kamensky S. Artifificial Intelligence and Technology in Health Care: Overview and Possible Legal Implications // DePaul journal of health care law. – Chicago, 2020. – Vol. 21, N 3. – P. 1–18

3. Tschider C.A. The healthcare privacy-artificial intelligence impasse // Santa Clara high technology law journal. – Santa Clara, 2020. – Vol. 36, N 4. – P. 439–443

4. The ethical, legal and social implications of using artificial intelligence systems in breast cancer care / M.S. Carter, W. Rogers, K.T. Win, H. Frazer, B. Richards, N. Houssami // The breast. – Elsevier, 2020. – Vol. 49. – P. 25–32.

5. Орлов С. Журнал сетевых решений. Искусственный интеллект в видео аналитике, 2019 Искусственный интеллект в видеоаналитике - IKSMEDIA.RU

6. Капустин А.В., Березовский Ю.А. Вопросы использования искусственного интеллекта при эксплуатации высокоавтоматизированных транспортных средств. // Текст научной статьи по специальности «Право». 2021. С. 21-24

7. Яндекс: Статистика эксплуатации транспортных средств с использованием искусственного интеллекта [Электронный ресурс]. — Режим доступа: https://yandex.ru/company/technologies/yaprobki/3 (Дата обращения 25.05.2023)

8. Щеглов, А.Ю. Защита информации: основы теории: учебник для вузов / А.Ю. Щеглов, К.А. Щеглов. – М.: Изд-во Юрайт, 2021. – 309 с.

9. Казарин, О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О.В. Казарин, А.С. Забабурин. – М.: Изд-во Юрайт, 2021. – 312 с.