ПРАВОВОЕ РЕГУЛИРОВАНИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Бекетова В.А.

Научный руководитель: Инюшкин А.А.

Россия, г. Самара,
Самарский национальный исследовательский университет
имени академика С.П. Королева

***Аннотация**. В современном мире одно из ведущих направлений развития занимает искусственный интеллект и, в частности, нейронные сети. В данной работе был проведен анализ существующих правовых аспектов в Российской Федерации, в частности, в медицинской сфере, а также приведены возможные направления дальнейшего развития права относительно систем искусственного интеллекта. Кроме того, был затронут вопрос безопасности нейронных сетей.*

***Ключевые слова:** искусственный интеллект, национальная техническая инициатива, правовое регулирование, нейронные сети, машинное обучение.*

Введение

Для обеспечения технического развития в том числе данной сферы в соответствии с поручением Президента России В.В. Путина по реализации послания Федеральному Собранию от 4 декабря 2014 г. началась разработка Национальной Технической Инициативы (НТИ). Основной целью НТИ является развитие ключевых рынков за период 10-20 лет и переход к новому технологическому укладу в стране. Одним из таких рынков является «Хелснет», который отвечает за развитие в области медицины. Одной из первостепенных задач является преодоление технологического барьера. В формулировке, взятой с официального сайта, [1] в качестве одного из технологических барьеров указано следующее:

«Разработаны системы поддержки принятия решений (СППР) с использованием алгоритмов обработки больших объемов данных (технологий больших данных) для локального использования в МО при оказании медицинских услуг в дистанционной форме при заболеваниях и высоком риске их развития по назначению врача/по обращению пациента по заболеванию. Алгоритмы выявления признаков заболеваний с чувствительностью и специфичностью не ниже лучших мировых практик».

За последние годы наблюдается колоссальный рост в использовании искусственного интеллекта (ИИ) для решения данной задачи. В частности, разработан ряд технологических решений, использующих нейронные сети для работы с медицинскими изображениями, в частности, компьютерная томография, рентгенография, МРТ, УЗИ. Часть существующих разработок на данную тематику уже активно применяется на практике. К плюсам используемых на данный

момент систем относят сокращение времени на выполнение рутинных задач, а также уменьшение вероятности совершения врачебной ошибки. Это происходит потому, что система концентрирует внимание специалиста на обнаруженных аномалиях. Происходит некоторое голосование между специалистом и системой, в которой специалисту возможно необходимо оспорить поставленный диагноз, что стимулирует к повышению уровня внимания и обеспечивает постановку более точного диагноза в сложных случаях.

Международное правовое регулирование

На текущий момент для мирового сообщества общей является проблема практически отсутствия нормативно правового регулирования в области искусственного интеллекта. Лишь часть государств начала вводить некоторые документы, направленные на решение неоднозначных вопросов с эксплуатацией современных систем и заполнять пробелы в законодательстве. На данный момент существует два основных подхода правового регулирования для систем ИИ. Первый подход наивысшим приоритетом обозначает существующие правовые нормы и правовую систему. В связи с этим при возникновении неоднозначных или неопределенных вопросов, которые связаны с ответственностью сторон или же безопасностью лиц, системы, персональных данных, возникающих из-за использования систем искусственного интеллекта, необходимо обособлять и выделять данные вопросы по мере их возникновения и только в том случае, когда текущая правовая система не способна их урегулировать. Второй подход основывается на идее вторичности права и в первую очередь направлен на поддержание технологических изменений. Этот подход основывается на широком разнообразии систем искусственного интеллекта и направленности их использования. Поэтому преждевременное введение регулирующих документов может иметь последствием невозможность развития некоторых частных систем и последующей потребности в изменении законодательства, что в свою очередь приведет к неизбежной потере времени, за которое могло бы осуществиться внедрение принципиально новой технологии. А также упущение возможности становления государства в качестве основоположника некоторой системы в мире.

В 2019 году на конференции ЮНЕСКО «Принципы искусственного интеллекта: в направлении гуманистического подхода» было достигнуто соглашение в отношении необходимости обеспечения управления человеком системами ИИ. На 2021 год запланированы два межправительственных совещания для окончательной доработки этических норм ИИ на основе фундаментальных прав человека.

Правовое регулирование в России

Основы регулирования искусственного интеллекта в России заложены Указом Президента Российской Федерации от 10 октября 2019 года № 490 «О развитии искусственного интеллекта в Российской Федерации», [3] утвердившим «Национальную стратегию развития искусственного интеллекта на период до 2030 года». В соответствии с текстом данного документа выделим из основных принципов развития и использования технологий искусственного интеллекта наиболее значимые для ИИ в данной области:

1) безопасность является важнейшим аспектом при разработке системы ИИ. Является недопустимым использование системы, которая создана с целью нанесения преднамеренного вреда её пользователям, т.е. несущей потенциальную угрозу здоровью человека. Также необходимо минимизировать вероятность негативных последствий внедрения данной технологии;

2) результаты работы ИИ должны быть понятны и объяснимы, те же условия распространяются на процесс достижения им результатов, – данный аспект является вторым по значимости фактором при обработке медицинских данных. Наиболее понятным примером является предварительная постановка диагноза системой искусственного интеллекта. Обоснование и понятный алгоритм определения является неотъемлемой частью при введении в эксплуатацию и непосредственном использовании данной системы;

3) технологический суверенитет является важным для всех отраслей, в которых используются системы искусственного интеллекта. Но данный аспект оказывает значительное влияние на возможную безопасность данной системы. И если частью системы является зарубежное программное обеспечение и замена не представляется возможной объективно, необходимо проведение комплекса мероприятий по анализу используемого программного обеспечения, так как в данной сфере речь идет о безопасности жизни и здоровья граждан.

Также данный документ обозначил основные задачи, которые предстоит выполнить для развития ИИ и выделил перечень обязательных действий со стороны органов государственной власти для реализации этих задач.

На текущий момент системы искусственного интеллекта объективно не выполняют требования прозрачности и понятности алгоритма и работают по принципу черного ящика. Оператор системы принимает только результат работы системы, обоснования причины принятия такого решения система не выдаёт. В связи с необоснованностью решения могут быть также проигнорированы даже обнаруженные системой аномалии.

Если говорить об интеллектуальных правах на системы ИИ, то, как и на любую другую программу, право на интеллектуальную собственность регламентируется главой 4 Гражданского кодекса Российской Федерации от 18 декабря 2006 года (ред. 31 июля 2020 года) [4]. Но что касается ответственности за «решения», принятые искусственным интеллектом, на текущий момент данный вопрос является открытым. В большинстве случаев медицинские учреждения используют стороннее ПО, а не разрабатывают его самостоятельно, и ответственность возлагается на одну из сторон, согласно составленному договору. На практике чаще встречается, что ответственность несет врач, который производит диагностирование пациента, или же медицинское учреждение, и отчасти это оптимальный выход в данной ситуации. Всё же данная стратегия не выделяет решения ИИ на данном этапе как весомую компоненту, диагностирующим врачам по-прежнему необходимо подробно ознакомиться с каждым конкретным исследованием, что, вероятно, указывает на недостаточный уровень развития технологии ИИ в медицине в настоящий момент.

Также в области медицины есть немаловажный аспект, который нельзя оставить без внимания. Это персональные данные и врачебная тайна. В идеаль-

ном случае также должна регламентироваться политика обработки персональных данных в системе и осуществляться максимальное обезличивание данных при обработке системой ИИ. Полное обезличивание данных представляется невозможным в условиях данной задачи, кроме основных данных для обработки, вероятнее всего, для более точной постановки диагноза системой ИИ будут передаваться также данные о поле пациента, возрасте.

Самым первым законом, который направлен непосредственно на устранение неопределенности, связанной с системами ИИ, является Федеральный закон от 24 апреля 2020 года № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта». [5] Здесь описываются условия и определения для установления экспериментального правового режима для разработки и внедрения технологий искусственного интеллекта в одном из субъектов Российской Федерации – городе федерального значения Москве. Новый закон вносит изменения в Федеральный закон «О персональных данных» [6]. Согласно действующим правкам, обезличенные персональные данные допускается обрабатывать, в том числе в качестве таких данных отдельно выделяются данные о состоянии здоровья пациентов, с целью поддержания эксперимента по разработке и внедрению системы ИИ.

Отдельным образом необходимо регламентировать безопасность систем ИИ. На текущий момент существует ряд атак на нейронной сети, который заставляет систему изменять решение на основе незначительно измененных входных данных. Искажения входных данных могут быть незаметны для пользователя системы, но при обработке системой будет получен некорректный результат. В сфере медицины такие ошибки могут нести критический характер и необходимо минимизировать их вероятность. Существует два наиболее очевидных способа осуществления: обучение нейронной сети с учетом возможных атак, то уменьшение вероятности успешного проведения атаки с учетом того, что злоумышленник уже имеет доступ к системе. И второй – достижение определенного уровня защищенности системы в целом, внедрение ряда определенных средств защиты при эксплуатации в медицинских учреждениях, их тщательная настройка, наличие специалистов, поддерживающих безопасность всей системы в режиме реального времени. Также необходимо осуществление контроля соблюдения сотрудниками внутренних нормативных актов медицинского учреждения для обеспечения безопасности системы в целом. В идеале применение обоих подходов нужно сделать обязательным и осуществлять контроль за выполнением данных требований для всех систем ИИ.

Кроме того, 24 июля 2020 года был принят закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации». [7] Этот закон вступает в силу в начале 2021 года. Он допускает введение экспериментального правового режима в ряде субъектов РФ. Использование таких режимов позволит развивать технологии, не урегулированные законодательством Российской Федерации в настоящий момент. Предполагается, что, исходя из результатов внутри участвовавших субъектов, упростится определение принципиально новых видов и форм экономической деятельности, будут со-

зданы оптимальные условия для технического развития и внедрения инновационных технологий.

Стоит обратить внимание с правовой точки зрения на такой аспект систем искусственного интеллекта, как набор данных, на которых было произведено обучение. Во-первых, говорящий сам за себя факт, что разработчики данных систем в подавляющем большинстве случаев не имеют глубоких медицинских познаний для грамотной постановки диагноза или определения аномалий на изображении. Таким образом, имеется два возможных выхода из ситуации. Первый – поиск уже существующих данных с определенными метками для кадров, с размеченными аномалиями. В таком случае актуален вопрос об уровне качества этих данных даже при их успешном нахождении. Второй – работа с группой специалистов в данной области. Стоит подчеркнуть, именно группой, так как человеческий фактор оказывает высокое влияние и ошибки, поданные модели при обучении, могут иметь крайне негативные последствия в будущем. Таким образом, как минимум, стоит регламентировать предоставление используемого для обучения нейронной сети набора данных и проверку их квалифицированными работниками медицинских учреждений во избежание эксплуатации некачественного программного обеспечения в сфере здравоохранения.

Заключение

Из вышеописанного следует, что актуальные правовые документы направлены на поддержание развития в сфере технологий. Введение новых правовых режимов только облегчает сбор данных для обучения нейронных сетей, упрощает разработку и интеграцию данных систем в ключевые сферы. Искусственный интеллект является одной из основных частей, предназначенных для технического развития текущей экономической, промышленной и медицинской деятельности. В связи с этим необходимо последовательно развивать правовую базу для качественного регулирования возникающих вопросов, учитывать возможные риски и специфики использования данной технологии в различных сферах.

Библиографический список

1. Официальный сайт НТИ [Электронный ресурс]. URL: https://nti2035.ru/ (дата обращения: 25.11.2020).

2. РОБОПРАВО. Исследовательский центр проблем регулирования робототехники и искусственного интеллекта [Электронный ресурс]. URL: http://robopravo.ru/modielnaia_konvientsiia (дата обращения: 20.04.2020).

3. Указ Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [Электронный ресурс]. URL: http://publication.pravo. gov.ru/Document/ View/0001201910110003 (дата обращения: 25.11.2020).

4. Гражданский кодекс Российской Федерации часть 4 от 18 декабря 2006 года (ред. 31 июля 2020 года) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_64629/ (дата обращения: 25.11.2020).

5. Федеральный закон от 24.04.2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202004240030 (дата обращения: 25.11.2020).

6. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 25.11.2020).

7. Федеральный закон от 31.07.2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [Электронный ресурс]. URL: http://public ation. pravo.gov.ru/Document/View/0001202007310024 (дата обращения: 25.11.2020).

LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE SYSTEMS

Beketova V.A.

Scientific adviser: Inyushkin A.A.

Samara National Research University, Samara, Russia

Abstract. *In the modern world, one of the leading areas of development is artificial intelligence, and, in particular, neural networks. In this paper, an analysis of the existing legal aspects in the Russian Federation, in particular in the medical field, was carried out, and possible directions for the further development of law in relation to artificial intelligence systems were given. In addition, the issue of the safety of neural networks was raised.*

Keywords: *artificial intelligence, national technical initiative, legal regulation, neural networks, machine learning.*