Секция «Искусственный интеллект в контрольно-надзорной деятельности»

Искусственный интеллект в контрольно-надзорной деятельности

Научный руководитель – Назаренко Сергей Владимирович

Вэнь Х.[1]*, Го Ц.*[2]

1 - Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного администрирования (факультет), Москва, Россия, *E-mail: wenhao123@rambler.ru*; 2 - Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного администрирования (факультет), Москва, Россия, *E-mail: 877892022@qq.com*

Современные информационные технологии все больше проникают в различные сферы жизнедеятельности. Практически во всех развитых государствах основные сферы производства, промышленности, оказания услуг не обходятся без использования современных информационных технологий. Современное государственное управление также все активнее использует различные информационные ресурсы в своей деятельности.

Действительно, многое из того, что приведено в Национальной стратегии в качестве перспективных направлений использования искусственного интеллекта, *вполне может быть реализовано при осуществлении контрольно-надзорной деятельности.*

1. Применение искусственного интеллекта имеет огромный потенциал при планировании, прогнозировании и принятии управленческих решений при осуществлении контрольно-надзорной деятельности. *Планирование* контрольно-надзорных мероприятий может происходить с помощью искусственного интеллекта, который позволит более точно и объективно определить потенциально опасные объекты, которые должны в первоочередном порядке подлежать проверке контрольно-надзорными органами. *Прогнозирование* посредством применения искусственного интеллекта потенциально опасных ситуаций на объектах, подлежащих контролю и надзору, может быть использовано при осуществлении профилактической контрольнонадзорной деятельности. Действительно, компьютерное моделирование и прогнозирование аварий, инцидентов и отказов оборудования и последующее направление подконтрольному (поднадзорному) объекту предписаний о превентивном техническом обслуживании оборудования позволит избежать не столько нарушений норм и правил, сколько возможных последствий – аварий и инцидентов, повлекших причинение вреда жизни и здоровью людей, причинение ущерба окружающей среде, имуществу третьих лиц и т.д.

Например, М.С. Арабян и К.М. Гильманова указывают, что «благодаря искусственному интеллекту машины могут самостоятельно реагировать на сигналы из окружающего мира, то есть сигналы, которые программисты напрямую не контролируют и, следовательно, не могут предвосхитить. Искусственный интеллект успешно применяется в прогнозировании, контроле за качеством услуг, выработке рекомендаций и распознавании (лиц, эмоций, голоса и т.п.). Так, в Сингапуре и Южной Корее осуществляется оценка потенциала по использованию искусственного интеллекта для чтения (расшифровки) и анализа рентгеновских изображений контейнеров. Целью такой работы является выявление аномалий (нестандартных ситуаций) и формирование уведомлений таможенным органам, предупреждающих о необходимости задействовать человека для проведения досмотра подозрительных предметов»[1].

2. Применение искусственного интеллекта при рутинных (повторяющихся) операциях в сфере контрольно-надзорной деятельности может быть использовано при оценке соблюдения лицензионных требований и условий, ранее выданных разрешений, проверке

декларирования и страхования объектов и т.п. Кроме того, искусственный интеллект может быть использован для сравнения правовых и технических норм и правил на предмет их отмены, изменения и возможных противоречий.

3. Применение искусственного интеллекта при непосредственном проведении мероприятий по контролю позволит проводить более качественно и эффективно проверку подконтрольного (поднадзорного) объекта[5]. Искусственный интеллект позволит проводить одновременно сразу несколько контрольно-надзорных мероприятий в отношении разных объектов.

Например, при проведении видеосъемки компьютерная программа, основанная на искусственном интеллекте, может распознавать различные технические устройства и детали, объекты, помещения, сооружения, приспособления, и т.д. Сопоставив указанные объекты с нормами и правилами (обязательные правила), выполнение которых подлежит проверке, можно выдать аналитический отчет о соблюдении либо несоблюдении этих обязательных требований. После чего выявленные нарушения могут быть предметом личной проверки уже должностного лица контрольно-надзорного органа, а в случае согласия собственника проверяемого объекта такая проверка может и не проводиться.

4. Применение искусственного интеллекта позволит обеспечить безопасность при проведении контрольно-надзорных мероприятий. Так, сотрудникам контрольно-надзорных органов при проведении проверочных мероприятий приходится лично проверять объекты, представляющие опасность для жизни и здоровья (шахты, подъемные сооружения, химические и радиационные объекты и т.п.). В ряде случаев такая проверка представляет опасность как для проверяющих, так и для проверяемых лиц.

Кроме того, при проведении этих мероприятий могут проводиться технические испытания, которые представляют опасность для их участников. Применение современных технических устройств: дронов, квадрокоптеров, беспилотных аппаратов, роботов – и полученные с их помощью необходимые сведения могут быть проанализированы искусственным интеллектом. Результатом таких проверок станут рекомендации по безопасной эксплуатации оборудования и производств, совершение действий, направленных на соблюдение обязательных требований.

5. Применение искусственного интеллекта позволит исключить предвзятость и «обвинительный уклон» со стороны сотрудников контрольно-надзорных органов.

6. Применение искусственного интеллекта позволит повысить эффективность обучения сотрудников контрольно-надзорных органов, а равно работников организаций, в отношении которых осуществляются мероприятия по контролю (надзору).

7. Искусственный интеллект позволяет принимать должностным лицам контрольно-надзорных органов наиболее оптимальные и эффективные управленческие решения, сокращая при этом их административное усмотрение.

Несмотря на отмеченные выше различные достоинства и положительные аспекты применения искусственного интеллекта в контрольно-надзорной деятельности, следует отметить и существующие реальные риски применения искусственного интеллекта, которые могут привести к негативным последствиям. Данные риски можно условно разделить на две большие группы: технические и социальные.

В первую группу рисков можно отнести следующие обстоятельства.

Во-первых, одним из самых вероятных рисков является вмешательство в работу компьютерной программы искусственного интеллекта. В компьютерную программу может быть запущен вирус или внесены изменения, делающие ее деятельность необъективной. Это может происходить со стороны злоумышленников, которые хотят установить препятствия для законной деятельности контрольно-надзорных органов, а равно иностранных государств, преследующих военные или политические цели.

Во-вторых, серьезным риском может являться технический сбой в работе искусственного интеллекта (то есть соответствующей компьютерной программы или компьютера). Можно в полной мере констатировать, что разработки программного обеспечения искусственного интеллекта находятся только на начальном этапе. Поэтому существует большая вероятность некорректной работы либо программного обеспечения, либо технических устройств, используемых для работы искусственного интеллекта.

Некоторыми учеными особо подчеркивается данная проблема: «как показала практика, искусственный интеллект подвержен риску не только хакерских атак, но и других сбоев, которые крайне сложно предугадать, а зачастую и невозможно предотвратить или затруднительно остановить, поскольку роботы за доли секунды могут принять неправильные решения, которые охватят своими негативными или даже опасными последствиями огромное количество людей, тогда как последствия неправильных решений живого человека редко бывают такими одномоментными и массовыми» [4, с. 46].

В-третьих, по причине технических неисправностей или наличия уязвимости системы искусственного интеллекта возможна потеря важных сведений, информации, больших данных и т.д. Кроме этого, важным аспектом также является получение, обработка и распространение персональных данных, информации ограниченного доступа, секретной информации. Отсутствие контроля со стороны человека может привести к потере важной информации либо распространению персональной информации вопреки воле человека.

В-четвертых, для работы искусственного интеллекта необходима бесперебойная работа высокоскоростного Интернета (не менее 4G или 5G). Это является большой проблемой для нашей страны, на большей части которой нет высокоскоростного Интернета. В отсутствие высокоскоростного Интернета работа искусственного интеллекта, оперирующего большими данными, не представляется возможной.

В-пятых, разработчиками искусственного интеллекта являются крупные корпорации, такие как Google, Facebok, IBM, Amazon, Apple, AlBrain, Twitter, iCarbon, Entefy, Cloudminds (Top-10), которые являются крупными зарубежными компаниями (прежде всего США). В России разработкой искусственного интеллекта занимаются две крупные российские компании – «Яндекс» и Сбербанк. Передача технологии искусственного интеллекта на государственный уровень (не учитывая военных разработок) потребует значительного времени и материальных ресурсов, которые государство может и не иметь для этих целей [2].

Ко второй группе рисков можно отнести следующее.

Во-первых, учитывая риск, связанный с ошибкой в работе системы искусственного интеллекта, остро встает вопрос о перепроверке принятых искусственным интеллектом решений. Если искусственный интеллект принял неправильное решение, то какая в этом случае существует процедура проверки? В какой степени мы можем доверять решениям, принятым искусственным интеллектом?

В данном случае следует согласиться с учеными, отмечающими, что «юридически значимые решения, принятые искусственным интеллектом, практически невозможно опротестовать, что значительно снижает гарантии прав граждан и возможности по контролю за принятием решений государственными органами с помощью ИИ-технологий» [4, с. 47]. Исследователи приводят следующий пример такой гипотетической ситуации: «ИИ анализирует данные малообеспеченного инвалида и решает, сколько часов бесплатного ухода в неделю ему полагается от государства. Если ИИ решил отказать или назначить меньше, чем раньше, больному просто некуда обратиться: ему говорят, что решение, принятое «черным ящиком», невозможно изменить. Более того, чиновники не могут даже объяснить принятое решение – примерно, как сотрудник банка может лишь гадать, почему система не выдала потребителю кредит» [5].

Во-вторых, в целом можно констатировать, что серьезной проблемой является отсутствие доверия при оказании разнообразных услуг человеку с применением искусственного интеллекта. Так, у многих вызывает недоверие, если медицинская операция проводится не врачом, а роботом; у человека возникает недоверие к автомобилю, управляемому искусственным интеллектом; человек опасается, если его личные денежные средства переходят под управление искусственного интеллекта; и т.п.

Следовательно, вопрос о полноценном применении искусственного интеллекта в государственном управлении связан не столько с технической возможностью (технологическим прогрессом), сколько с высоким уровнем общественного доверия к этим технологиям со стороны людей.

В-третьих, существует угроза социальных конфликтов при использовании искусственного интеллекта ввиду того, что при принятии управленческого решения на основе искусственного интеллекта практически сокращается или даже обнуляется возможность административного усмотрения [6]. При таких обстоятельствах могут быть проигнорированы тяжелые жизненные ситуации, финансовое состояние, трагедии человека,социально-политические условия и др. Тем самым применение искусственного интеллекта – «бездушной машины» не позволит решить цели и задачи государственного управления, основанного в том числе на принципах целесообразности, справедливости и гуманизма.

В-четвертых, активное применение искусственного интеллекта может вызывать нигилизм, отторжение и желание противопоставить человека машине. Скоропалительная замена человеческого труда технологиями искусственного интеллекта и потеря большим числом людей своей работы приведет к активному противостоянию общества и работодателей, в том числе государства и крупных корпораций, применяющих в своей деятельности технологии искусственного интеллекта вместо использования человеческого труда. В связи с этим государство будет вынуждено сокращать сферы применения искусственного интеллекта, учитывая потребности и социальные запросы общества.

Таким образом, для дальнейшего внедрения в контрольно-надзорную деятельность технологии искусственного интеллекта необходима разработка соответствующей стратегии, в которой должны быть зафиксированы основные направления, формы и методы применения искусственного интеллекта в контрольно-надзорной деятельности, а также временные этапы его внедрения в практику и возможные риски.

Источники и литература

1) Арабян М.С., Гильманова К.М. Цифровизация как приоритетный инструмент совершенствования таможенного администрирования на примере ЕАЭС // Таможенное дело. 2019. № 4. С.17–21.

2) Мартынов А.В.. Актуальные вопросы применения искусственного интеллекта при осуществлении контрольно-надзорной деятельности органов исполнитнльной власти / Вестник Нижегородского университета им. Н. И. Лобачевского, no. 2, 2020, pp. 175-186.

3) Плаксин С.М., И.А. Абузярова, А.В. Кнутов и др. М. / Контрольно-надзорная и разрешительная деятельность в Российской Федерации. Аналитический доклад. 2018 г. : Национальный исследовательский университет «Высшая школа экономики», 2019. 148 с.

4) Тихомиров Ю.А. , С.Б. Нанба. М./ Юридическая концепция роботизации: Монография : Проспект, 2019. 240 с.

5) Шнуренко И. Искусственный интеллект на грани нервного срыва // Эксперт. 2019. № 1. URL: https://expert.ru/expert/2019/01/iskusstvennyij-intellekt-nagrani nervnogo-sryiva/

6) Шорник Е.А., Зыков Д.Д. Возможности внедрения технологии искусственного интеллекта в процессе модернизации системы публичного управления в России // Плехановский барометр. 2019. № 1 (17). С. 24–26.