Секция «Государственная служба России и Китая: новый цифровой порядок государственного администрирования»

Проблема использования искусственного интеллекта в государственном управлении Китая.

Научный руководитель – Панич Наталья Александровна

Хань Сяо
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного администрирования (факультет), Москва, Россия
E-mail: tiantian19971202@sina.cn

Прежде всего, в большинстве технологий искусственного интеллекта не учитывается защита конфиденциальности. В отсутствие институциональных норм конфиденциальность людей может быть раскрыта очень легко, что позволяет компаниям, обладающим возможностями сбора данных, использовать их в своих интересах и может использовать технологию искусственного интеллекта для наблюдения за людьми и вмешательства в их личные предпочтения. оригинальное поведение. Кроме того, если компании, владеющие этими данными, недостаточно осведомлены о безопасности и допускают утечку этих личных данных или их злонамеренное похищение хакерами, это еще больше увеличит вероятность мошенничества. Однако стоит отметить, что из-за стремления предприятий к получению прибыли, если они будут полагаться только на строгое самоуправление и повышать осведомленность о профилактических мерах, они не обязательно смогут эффективно предотвращать такие проблемы. Более разумным способом является установление всеобъемлющих правил защиты конфиденциальности на национальном уровне и пересмотр систем, которые могут существовать на предприятиях, которые получают личную информацию без разрешения и приводят к утечке конфиденциальной информации, чтобы защитить безопасность населения и страны. Исходя из этого, интеграция технологии или систем искусственного интеллекта с функциями защиты конфиденциальности в национальную систему управления поможет добиться эффективной защиты прав и интересов граждан в управлении. Предвзятые данные приводят к ошибочным суждениям. Кроме того, в процессе сбора данных могут быть ошибки, что приведет к неточным оценкам в процессе управления. Например, в задаче классификации по идентификации хаски и хаски на фотографиях ученые обнаружили, что в этом наборе данных изображения большинство хаски было снято в снегу, так что процесс распознавания фактически осуществляется путем распознавания изображений. Есть ли «ложно правильная» классификация сделано Сираюки. Кроме того, существует не только риск предвзятости при сборе данных, но даже при гендерно-ориентированном анализе естественного языка искусственный интеллект также будет отражать тенденциозные гендерные ответы. Следовательно, необходимо тщательно анализировать и решать предвзятые проблемы, связанные с данными, связанными с корпоративным управлением, при модернизации управления, а также обеспечивать справедливость управления на основе источника данных и методов обработки. Мошенничество с данными. Модель искусственного интеллекта не является полностью зависимой, и она также может предоставлять поддельные данные. В частности, с 2014 года искусственный интеллект подвергся новому витку обновлений. «Фальшивые» данные, генерируемые через сеть генеративной конфронтации, и ее варианты, предложенные Яном Гудфеллоу, могут почти доходить до фальсификации. Хотя сеть генеративной конфронтации изначально была предложена для увеличения объема данных и помощи в обучении

модели, в практических приложениях есть преступники, которые используют эту лазейку для генерации данных, которые могут быть использованы для мошенничества. Кроме того, существующие модели глубокого обучения также имеют недостатки с точки зрения стабильности и легко подвергаются атаке небольшими данными о нарушениях, что может привести к очевидным ошибочным суждениям. Таким образом, чтобы сделать искусственный интеллект и связанные с ним технологии более эффективными в области государственного управления в будущем, необходимо доработать некоторые новые устройства и алгоритмы. При полном использовании преимуществ искусственного интеллекта для улучшения возможностей управления он необходимо для реализации атак на поддельные или ложные данные Эффективная защита. Короче говоря, искусственный интеллект - это палка о двух концах. Он может повысить уровень модернизации управления на основе своих собственных характеристик, обеспечить эффективность и справедливость процесса управления, повысить эффективность управления и усилить чувство выгоды и счастья у людей. Но в то же время потенциальные риски искусственного интеллекта с точки зрения защиты конфиденциальности, предвзятости и достоверности данных могут отрицательно сказаться на социальной стабильности и безопасности людей. Следует также напомнить, что искусственный интеллект еще не полностью достиг уровня человеческого интеллекта во многих аспектах, поэтому использование гибридного улучшенного интеллекта человека и машины для модернизации управления может быть более эффективной моделью управления.