Секция «Технологии искусственного интеллекта в современной политике»

Искусственный интеллект и биометрическая политика: риски и угрозы

Научный руководитель – Грачев Михаил Николаевич

Котова Полина Сергеевна
Выпускник (бакалавр)
Российский государственный гуманитарный университет, Историко-архивный институт, Москва, Россия
E-mail: polinaiskotova@yandex.ru

Современная политическая сфера развивается в тесном тандеме с новыми технологиями. Вряд ли кого-то можно удивить голосовыми помощниками и чат-ботами на правительственных сайтах, сайтах государственных органов и ведомств. Эти помощники призваны упростить гражданам процесс поиска необходимой информации, ответить на их вопросы, разобраться с их проблемами и найти верное решение или обратиться к нужному специалисту. Данный пример – один из наиболее распространенный способов применения искусственного интеллекта (далее – ИИ) в политике и государственном управлении. Эти технологии находятся сейчас на пике своего развития и внедряются повсеместно во все сферы жизни общества с довольно очевидными целями: упростить сбор, хранение и анализ той или иной информации, потому что с таким количеством и объемом информации не справится ни человек, ни группа людей, ни организация. Но все ли так однозначно? При таком раскладе выходит, что возможности ИИ безграничны – а если выразиться точнее, то возможности людей, в чьих руках оказывается доступ к ИИ и его контроль, безграничны.

Еще одним мировым трендом является внедрение биометрических технологий. Биометрия – это наука об идентификации или верификации личности по физиологическим или поведенческим характеристикам, которые включают в себя: отпечатки пальцев, геометрия руки, голос человека, его подпись и многие другие. [1, с.19] Считается, что такой способ верификации и идентификации намного более безопасен и точен, так как анализируются сразу несколько уникальных параметров, присущих одной личности. Биометрические системы уже применяются в бизнес-сфере, при регистрации на государственных порталах, при оплате в магазинах и проезде на транспорте, при управлении систем «умных домов» и т.д. Тут опять же не обошлось без ИИ, так как он позволяет обрабатывать необходимые запросы в считаные доли секунд.

Однако существуют неочевидные проблемы, касающиеся и использования ИИ, и использования биометрии, а особенно – использования их в симбиозе. Технологии синтеза изображений, видео и голоса, основанные на генеративном ИИ (также известные как deepfake) уже давно заставляют людей сомневаться в том, что реально происходило, а что лишь вымысел. На таких изображениях или роликах чаще всего известные политики говорят или делают компрометирующие вещи, после чего в той или иной стране или даже во всем мире возникают недовольства, после чего те самые политики вынуждены разбираться с последствиями. Чаще всего такое публиковалось ради развлекательных целей людьми, которые разбираются в информатике и программировании, для обычных людей, и достаточно быстро люди могли осознать, что фото или видео являются подделками, но все поменялось с развитием нейронных сетей таких как ChatGPT. Midjourney, DALL-E и т.д. Эти нейросети упростили процесс создания дипфейков настолько сильно, что научиться их сделать сможет каждый. Таким образом, в корыстных целях могут быть украдены личности не только знаменитостей, но и простых людей, в случае которых вряд ли целые команды будут разбираться с последствиями для них.

В Российской Федерации существуют определенная законодательная база и правовое регулирование в области сбора, хранения и обработки биометрических данных, но сами биометрические данные не защищены ничем. Они не являются нематериальным благом и интеллектуальной собственностью личности, их наличие и принадлежность к определенному человеку никак не обозначается. [2] Сейчас, например, необходим небольшой отрывок записи голоса человека, чтобы нейросеть могла его обработать и воссоздать, а в дальнейшем использовать в своих целях. Такая же ситуация может коснуться и других биометрических данных, и уже известно множество примеров, когда голоса и изображения знаменитых людей использовались в злонамеренных целях. Как писал американский криптограф, писатель и специалист по компьютерной безопасности Брюс Шнайер: «Поскольку биометрия используется всё шире, а генеративный искусственный интеллект совершенствуется, риск его использования для кражи биометрических данных явно растёт». [3] Биометрические данные являются надежным и безопасным способом идентификации и верификации личности только в том случае, если они прочно защищены без возможности компрометирования. Ведь при потере или краже пароля к тому или иному ресурсу его можно поменять, но изменить свою внешность, свою физиологию или поведение невозможно.

Существующая сегодня тенденция сбора персональных данных, их классификация и упорядочивание с последующим использованием может быть полезна в одних сферах, но разрушительна в других, а отсутствие четкого законодательства, которое бы контролировало и запрещало использование биометрии в неправомерных целях в повседневной жизни лишь усугубляет ситуацию. Искусственный интеллект может как упростить, так и усложнить многие процессы – особенно, когда дело касается людей и общества вообще, где все нововведения должны быть очень продуманы и деликатны.

Источники и литература

1) Болл Р. М., Коннен Дж. Х., Панканти Ш., Ратха Н. К., Сеньор Э. У. Руководство по биометрии. М.: Техносфера, 2007. – 368с.

2) Мильшин, Ю. Н. К вопросу об использовании биометрических данных искусственным интеллектом / Ю. Н. Мильшин, А. М. Ахтямов // Вестник Саратовской государственной юридической академии. – 2024. – № 4(159). – С. 219-223.

3) Цит. по: Искусственный интеллект поставил биометрию под угрозу | Октагон.Медиа [Электронный ресурс.] – Режим доступа: https://octagon.media/mir/iskusstvennyj_intellekt_postavil_biometriyu_pod_ugrozu.html (дата обращения: 08.03.2025)