Курто Я. А.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ФАКТОР РИСКА В ОТНОШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Курто Яна Андреевна, магистрант Полоцкого государственного университета имени Евфросинии Полоцкой, г. Новополоцк, Беларусь, 20pr3.kurto.y@pdu.by

Научный руководитель: канд. юрид. наук Соловьев П. В.

Современное цифровое пространство развивается под воздействием технологий искусственного интеллекта (далее – ИИ). Несмотря на то, что применение ИИ демонстрирует эффективность в различных областях, оно также связано с большими рисками. Рассмотрим влияние ИИ на сферу защиты персональных данных.

Актуальность рассматриваемого вопроса подтверждается Концепцией правовой политики Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 28.06.2023 г. № 196. Концепция устанавливает, что необходимо урегулировать вопрос применения искусственного интеллекта в сферах законодательства.

М. С. Абламейко определяет ИИ как мультимодальную интеллектуальную компьютерную систему принятия решений, которая на основе входных данных, используя самообучающие технологии, получает результаты, сопоставимые с результатами интеллектуальной деятельности человека, функционируя в определяемом правовом поле. Данное понятие позволяет проанализировать как преимущества, так и негативные стороны применения технологий ИИ в отношении персональных данных.

Обработка персональных данных системами ИИ состоит из двух этапов: этапа обучения, в течение которого ИИ учится выявлять закономерности и выполнять требуемые задачи, и этапа использования, при котором ИИ непосредственно применяет полученные данные для достижения целей ИИ. Входные данные, на основе которых ИИ проходит самообучение, могут состоять в том числе и из персональных данных.

Обработка персональных данных ИИ имеет ряд преимуществ.

Во-первых, скорость и эффективность систем ИИ позволяют обработать массивы информации быстрее и результативнее, чем человек.

Во-вторых, ИИ может быть использован для защиты персональных данных. При применении технологии возможно предотвращение утечек информации, предупреждение возможных угроз и выявление несанкционированного доступа к данным с помощью машинного обучения. Однако наличие преимуществ использования ИИ не исключает соответствующих рисков.

На этапе обучения ИИ может преднамеренно либо непреднамеренно запомнить полученные данные в своей системе. Чем больше информации получают системы ИИ на этапе обучения, тем эффективнее они выполняют свои задачи. К сожалению, данные, используемые для совершенствования

технологии, в большинстве случаев собираются в отсутствие свободного, однозначного и информированного согласия со стороны субъекта персональных данных.

Информация, получаемая от пользователей, обычно хранится в базах данных ИИ. Персональные данные, хранящиеся в этих системах, могут включать конфиденциальную информацию, такую как паспортные данные, место проживания, номера телефонов и т. д.

Алгоритмы ИИ анализируют огромные массивы данных клиентов, такие как их пользовательская активность в Интернете, покупки и др. ИИ также используется банками, страховыми компаниями и иными учреждениями для анализа информации о пользователях, например, их семейного или финансового положения, места проживания и т. д.

Некоторые системы ИИ обучены идентифицировать человека с помощью биометрических данных, что ставит под угрозу конфиденциальность персональных данных человека и неприкосновенность частной жизни. К примеру, такими системами являются технологии распознавания лиц Facebook, Apple Siri, Amazon Alexa и т. д. Полученные данные могут использоваться для создания дипфейков, а именно сгенерированного фото-, аудио- или видеоконтента на основе реальных данных. Дипфейки могут создаваться с целью шантажа либо достижения иных целей, т. е. причинения ущерба человеку.

В случае нарушения требований к защите персональных данных при применении ИИ разработчики систем должны быть привлечены к ответственности. Так, в январе 2022 г. Национальная комиссия по информатике и свободам (CNIL) Франции наложила штраф на компанию Google и социальную сеть Facebook за нарушения при сборе информации о пользователях. В октябре 2022 г. компания Clearview AI была подвержена наказанию в виде штрафа тем же органом по причине незаконного сбора, обработки, хранения и использования биометрических данных граждан Франции.

Республика Беларусь не обладает должным уровнем защиты персональных данных при использовании ИИ. На современном этапе предлагается использование общих требований, установленных Законом Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных».

Развитие технологий ИИ способствует повышению результативности различных отраслей. Делается вывод о том, что быстрое развитие технологии ИИ создает значительные риски в отношении персональных данных и конфиденциальности. Разработчики должны уделять большое внимание информационной защите систем ИИ.