Ежегодно 15 марта отмечается Всемирный день прав потребителей, девиз 2024 года – «Справедливый и ответственный искусственный интеллект для потребителей».

Искусственный интеллект стал неотъемлемой частью цифрового мира, проникнув в большинство сфер жизни людей, оказав огромное влияние на развитие ключевых областей экономики – банкинга, ретейла, медицины и промышленности.

Несмотря на множество преимуществ искусственного интеллекта, вызывает обеспокоенность последствия его применения для безопасности потребителей.

В настоящее время правовой статус искусственного интеллекта законодательно не определен и нет ясности, кто несет ответственность за создание и распространение недостоверной или неточной информации, попадающей в открытые источники при использовании искусственного интеллекта.

Уже началась работа по повышению прозрачности в сфере искусственного интеллекта. Чтобы гарантировать, что люди станут получателями этой новой технологии, необходимо обеспечить эффективную защиту потребителей на трех ключевых этапах:

1. Создание

Потребители серьезно обеспокоены тем, как создается искусственный интеллект и как интегрируются данные. Многим генеративным моделям искусственного интеллекта необходимы большие наборы данных для обучения. Нам необходимо задаться вопросом, как создаются и поддерживаются модели искусственного интеллекта – и было ли это сделано справедливо по отношению к потребителям с самого начала.

Например, собираются ли данные, используемые для обучения модели искусственного интеллекта, законно и с согласия людей? Этичен ли человеческий труд, который маркирует и классифицирует эти данные? И ответственно ли управляются задействованные экологические ресурсы? Разработчики должны быть прозрачными в отношении того, что потребовалось для создания инструмента, которым будут пользоваться потребители, точно так же, как маркировка продуктов помогает людям понять, что входит в состав их продуктов питания, текстиля или лекарств.

2. Распространение

После того как модель искусственного интеллекта создана, ее необходимо развернуть с учетом интересов потребителя.

Разработка с открытым исходным кодом или с закрытым исходным кодом

стала ключевым спором. В случае открытых моделей исходный код приложения открыт для общего использования, тогда как закрытая модель остается частной.

Существуют аргументы в пользу любого подхода, и приятно видеть, что обществу становятся доступны новые инструменты. Но чтобы должным образом защитить потребителей, нам необходимо знать, как повлияет на общество появление модели искусственного интеллекта.

Рассмотрели или раскрыли ли разработчики и пользователи этих продуктов риски, которые они могут представлять? Позволяют ли они внешним сторонам – например, исследователям или правоохранительным органам – независимо проверять эти утверждения? А в случае открытых моделей существуют ли правила относительно того, кто может использовать этот код и что им разрешено с ним делать?

Мы знаем, например, что открытые генеративные модели искусственного интеллекта уже использовались для создания различных образов без согласия. Это потенциально может открыть новую эру дезинформации, а также усилить мошенничество со стороны злоумышленников. Это также может затруднить обнаружение киберобмана: люди могут идентифицировать написанный искусственным интеллектом контент только в половине случаев , как показывают исследования.

Разработчики систем искусственного интеллекта должны признать и сообщить все, что им известно о потенциальном вреде.

3. Ответственность

Нам также необходимо выяснить, существуют ли надежные процедуры для решения возникающих проблем и установлен ли правильный уровень подотчетности и обращения за помощью в промышленности, правительстве и гражданском обществе. Это включает в себя право потребителей на возмещение ущерба, раскрытие запросов правительства на доступ и нарушение прав интеллектуальной собственности.

Другими словами, если система искусственного интеллекта создает проблему для человека, кто виноват – и кто должен ее исправить? Необходимо провести четкие границы подотчетности.

Много было написано о том, что искусственный интеллект и другие технологии могут несправедливо дискриминировать или закреплять предубеждения, но меньше о том, кто должен нести за это ответственность или должны ли быть какие-либо средства правовой защиты для тех, кто пострадал. Должны быть серьезные дебаты о способах обжалования решений, принятых алгоритмами искусственного интеллекта, например, в

кредитовании, здравоохранении, страховании или найме.

Мы все осознаем, какую силу имеет ИИ, чтобы изменить нашу жизнь полезным и эффективным способом. Но темпы перемен и отсутствие регулирования требуют активной политики по защите потребителей.

В целях обеспечения ускоренного развития искусственного интеллекта в Российской Федерации, проведения научных исследований в области искусственного интеллекта, повышения доступности информации и вычислительных ресурсов для пользователей, совершенствования системы подготовки кадров в этой области разработана Национальная стратегия развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента Российской Федерации от 10.10.2019 № 490.

Настоящей Стратегией определяются цели и основные задачи развития искусственного интеллекта в Российской Федерации, а также меры, направленные на его использование в целях обеспечения национальных интересов и реализации стратегических национальных приоритетов, в том числе в области научно-технологического развития.

Мы все хотим использовать возможности технологий, и если мы будем делать это ответственно, генеративный искусственный интеллект может иметь широкие преимущества с минимальными недостатками. Без обсуждения и смягчения этих рисков результат может быть совсем другим.