Примут ли закон об ИИ в России?

Тема регулирования искусственного интеллекта (ИИ) в России вновь оказалась в центре внимания. В СМИ появились новости, что власти, эксперты и бизнес-сообщество активно обсуждают необходимость создания правовых рамок, которые позволили бы стране не отстать в технологической гонке, но при этом защитили права граждан от потенциальных рисков, связанных с использованием ИИ.

Стоит сказать, что в России не первый месяц ведётся активная разработка законопроекта о государственном регулировании искусственного интеллекта. Как сообщила председатель правления Ассоциации разработчиков программных продуктов (АРПП) «Отечественный софт» Наталья Касперская, существует несколько вариантов текста будущего закона, которые «достаточно сильно друг от друга отличаются». Так, Касперская, участвующая в работе одной из экспертных групп, выступает за запрет цифровых рейтингов граждан и за право человека отказаться от цифровизации. Она подчёркивает, что системы анализа данных, эффективные внутри компаний, не должны масштабироваться на уровень всей страны, так как это создаёт угрозу тотального наблюдения за людьми. В свою очередь, представители бизнеса и технологического сектора предупреждают об опасности излишнего регулирования. Например, директор по аналитике АНО «Цифровая экономика» Карен Казарян отмечает, что позиция правительства достаточно ясна: регулирование ИИ вредно для технологического лидерства России. По его словам, если закон и будет принят, он должен стимулировать развитие технологий, снимать барьеры для их использования и развивать оборот данных для ИИ. В целом же экспертное сообщество убеждено, что жёсткие запреты на использование тех же персональных данных при разработке ИИ — прямой путь к технологическому отставанию России. Вместо ограничений необходимы стимулирующие меры: развитие технологий повышения конфиденциальности, использование синтетических данных и создание безопасной инфраструктуры.

Да и, как отмечает заведующий лабораторией доверенного искусственного интеллекта РТУ МИРЭА Юрий Силаев, закон должен быть адаптивным и учитывать специфику разных отраслей, используя рискориентированный подход.

Вообще, несмотря на споры о регулировании, российский рынок технологий ИИ на сегодняшний день демонстрирует активный рост. По оценкам аналитической компании Smart Ranking в 2025 году он может вырасти на 25–30%, достигнув 1,9 трлн рублей. При этом 95% выручки генерируют пять крупнейших компаний: «Яндекс», «Сбер», «Т-Технологии», VK и «Лаборатория Касперского».

Что касается примеров в использовании ИИ в различных отраслях, то они следующие: Финансовый сектор: Банки активно внедряют ИИ для кредитного скоринга, выявления мошенничества и персонализации продуктов. Так, «Сбер» сообщил, что финансовый эффект от внедрения технологий ИИ в компании в 2024 году составил более 450 млрд рублей. Образование: Девять из десяти студентов ведущих вузов используют нейросети для обучения. ИИ позволяет за ночь написать курсовую работу, которую не распознаёт ни один антиплагиат. Медицина: ИИ анализирует результаты исследований организма человека, но диагноз всегда ставит врач. Это позволяет ускорить процесс обработки данных, но сохраняет за человеком право принятия решений. Сельское хозяйство: Предприятия, такие как «Иркутская клубника», используют ИИ для выращивания клубники. Это особенно актуально в регионах, где не хватает кадров. Государственные услуги: ИИ используется для анализа данных и улучшения качества предоставления услуг. Однако эксперты подчёркивают, что необходимо обеспечить прозрачность его применения.

Так почему же некоторые так боятся ИИ?

Главные страхи, связанные с ИИ, часто основаны на рисках, которые он несёт. Это и массовое наблюдение, когда есть возможность анализа каждого человека, если системы наблюдения, используемые внутри компаний, будут масштабированы на уровень всей страны. Это и дипфейки, и манипуляции. К слову, генеративный ИИ может создавать поддельный контент, что представляет угрозу для безопасности и правды. Также многие остерегаются и «потери контроля». В мире уже были случаи, когда ИИ вместо помощи людям предлагал им опасные решения. Например, в США несколько громких эпизодов привели к печальным последствиям.

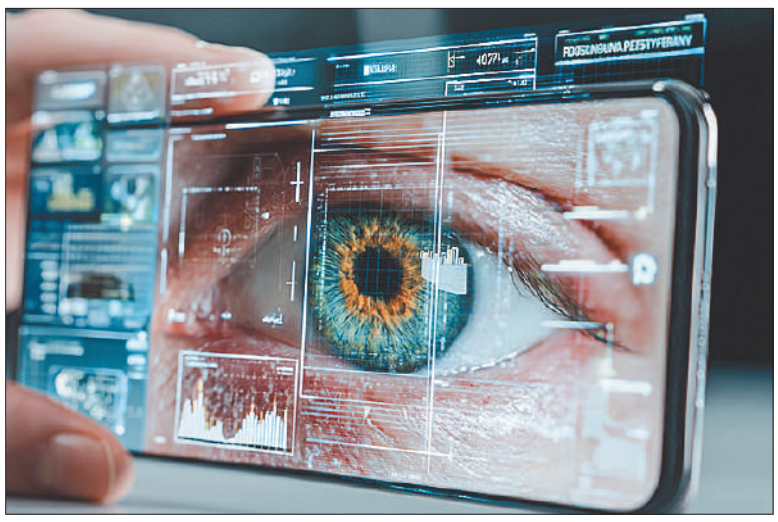
Однако, несмотря на все страхи, ИИ продолжает активно внедряться по нескольким причинам: например, когда видна экономическая эффективность, когда компании получают значительную экономию от внедрения ИИ. Ведь только в банковском секторе средняя экономия составляет 15–20% операционных расходов. Это и автоматизация процессов, когда ИИ позволяет автоматизировать сложные бизнес-процессы, что особенно важно в условиях нехватки кадров. Это и инновационный потенциал, когда развитие ИИ открывает новые возможности для создания продуктов и услуг, которые ранее были невозможны. Стоит сказать, что национальная стратегия развития ИИ до 2030 года и федеральный проект «Искусственный интеллект» предусматривают финансовую и регулятивную поддержку отрасли.

Поэтому в ближайшее время Госдума планирует обсудить вопросы регулирования ИИ, и от того, какие решения будут приняты, зависит не только технологическое лидерство России, но и безопасность её граждан.

Мария Климанова
по материалам СМИ

MAX: Первое впечатление можно произвести только раз...

Как стало известно, в сентябре текущего года все продаваемые в России смартфоны и планшеты должны предустанавливать мессенджер MAX от VK.



MAX задумывался как российский аналог WeChat — единая платформа для решения повседневных задач. В перспективе в нём должны быть интегрированы умные ассистенты, инструменты для бизнеса, обращения в госорганы, оплата услуг и медицинские карты.

Уже сейчас коммуникацию с россиянами предлагают перевести в MAX Госуслуги, «Авито», РЖД, маркетплейсы, мобильные операторы, «Почта России». Приложение можно установить на Android и iOS, а также воспользоваться его веб-версией. Ссылки на загрузку размещены на официальном сайте мессенджера, а также в Google Play, App Store или RuStore. Сейчас регистрация в MAX проходит только по номеру телефона и только через смартфон (пользоваться браузерной версией можно после первого входа на мобильном). Разработчики из VK заверяют, что все чаты в мессенджере защищены сквозным шифрованием (end-to-end). Это значит, что расшифровать сообщения могут только отправитель и получатель — даже разработчики не имеют доступа к содержимому.

Мера же предустановки, задуманная как шаг к технологическому новшеству, вызывает у пользователей смешанные чувства — от надежды на появление отечественного аналога китайской социальной сети до опасений тотальной слежки и утечек данных.

Есть и информация, что за нарушение требований о предустановке предусмотрены штрафы: должностным лицам — 30–50 тысяч рублей, компаниям — 50–200 тысяч рублей.

Как отмечает ряд экспертов, идея запуска MAX, бесспорно, масштабная – создать многофункциональную платформу для общения, платежей, государственных и бизнес-сервисов. Однако уже в первые недели её работы выявились серьёзные проблемы.

Например, не успел мессенджер набрать первые миллионы пользователей, как в Forbes появилось расследование, основанное на техническом анализе приложения. Cybersecurity-исследователи заявили, что MAX постоянно отслеживает активность пользователей с помощью «избыточного трекинга».

«Это приложение просто собирает все данные и логирует их. Я не помню, чтобы видел подобное в каких-либо других мессенджерах», — приводит издание слова анонимного исследователя. Кроме этого, бывший аналитик АНБ Патрик Уордл подтвердил данные выводы, добавив, что код MAX указывает на встроенный фоновый трекинг местоположения с высокой точностью. К слову, пользователи десктопной версии заметили ещё более тревожную деталь: индикатор работы веб-камеры загорается каждые 5–10 минут, даже когда приложение свернуто и не используется для звонков. В пресс-службе MAX эту информацию опровергли, заявив, что платформа не запрашивает доступ к камере.

Например, Эльдар Муртазин, ведущий аналитик Mobile Research Group, объяснил это явление некачественным кодом: «Мессенджер написан немного неудачно. Некачественный код вызывает функцию, которая стучится к камере, но не получает к ней доступ».

Парадоксально, но приложение, призванное повысить безопасность коммуникаций, уже стало платформой для мошенничества.

Так, 70-летняя жительница Санкт-Петербурга потеряла 2,5 миллиона рублей после звонка от человека, представившегося сотрудником Росфинмониторинга. Мошенник убедил её установить MAX и затем перезвонил «от имени ФСБ», после чего женщина передала свои сбережения курьерам.

Аналогичная история произошла с жительницей Курской области, которую обманули на 444 тысячи рублей через тот же мессенджер.

По словам Эльдара Муртазина, проблема в том, что MAX обязан передавать переписку правоохранительным органам по умолчанию – это автоматический процесс. При этом мессенджер не обеспечивает заявленной защиты от мошенников – большинство мошеннических аккаунтов блокируются вручную сотрудниками службы безопасности.

Одной из самых неоднозначных особенностей MAX стало ограничение на регистрацию — для неё требуется российская или белорусская SIM-карта. Это создаёт серьёзные проблемы для россиян, проживающих за границей.

В Индии, где сосредоточена значительная диаспора российских экспатов, приложение недоступно для скачивания. Те, кто уже установил его, могут совершать звонки, но новые пользователи зарегистрироваться не могут. На Кубе ситуация ещё сложнее — из-за санкций официальные магазины приложений Google Play и AppStore не работают, что делает установку MAX крайне затруднительной.

В целом же, чтобы этому новому продукту утвердиться на рынке «мессенджеров», ещё нужно время. И скорее всего, потребуются не только технические доработки, но и полная прозрачность в вопросах сбора и использования данных пользователей.

Да и создатели MAX уверяют: если пользователь опасается за сохранность своих личных данных, он может прекратить пользоваться им. Платформа безвозвратно удалит страницу через 30 дней.