Россиянам рассказали, почему не стоит обсуждать с нейросетью слишком личные вопросы

С ростом популярности нейросетей в повседневной жизни и бизнесе всё чаще поднимается вопрос безопасности личной и корпоративной информации. Пользователи загружают документы, отправляют резюме, указывают контактные данные и даже передают финансовую информацию, не всегда осознавая, какие последствия это может повлечь. В ряде случаев такие данные могут попасть в обучающую выборку ИИ или быть уязвимыми к внешним атакам.

Риски в основном связаны с тем, что многие нейросети работают на базе облачных сервисов и используют информацию для последующего дообучения моделей. Даже при обещаниях обезличивания, существует вероятность восстановления контекста или личности пользователя. Кроме того, под видом известных платформ могут работать фейковые сайты и приложения, целью которых является сбор персональных данных.

Чтобы минимизировать риски, эксперты рекомендуют тщательно проверять политику конфиденциальности сервисов, не передавать чувствительную информацию через открытые ИИ-платформы и использовать корпоративные решения с повышенным уровнем защиты. Также важно обращать внимание на страну размещения серверов, наличие международных сертификатов безопасности у провайдеров и репутацию самой платформы.