Компания Google в своих комментариях, направленных в Национальное управление по телекоммуникациям и информации (NTIA), признала растущую угрозу сбоев и краж, направленных на их модели. Они подчеркнули, что у них есть «надежная команда по обеспечению безопасности», а также предпринимаются усилия по «созданию экспертного комитета для управления доступом к моделям».

Аналогичным образом OpenAI подчеркнула необходимость как открытых, так и закрытых моделей и объявила о создании комитета по безопасности при своем совете директоров. Недавно они опубликовали в своем блоге подробную информацию о мерах безопасности, применяемых в их технологии обучения, стремясь побудить другие лаборатории к принятию аналогичных мер защиты.

Генеральный директор RAND Джейсон Мэтини, выступая в Стэнфорде, подчеркнул государственную важность усиления защиты от кибератак и шпионажа. Недавний случай подчеркивает эти опасения: инженер Google Линвэй Динг якобы украл конфиденциальные секреты чипов ИИ для китайского ИИ-стартапа.