OpenAI обновила искусственный интеллект, который управляет её цифровым помощником Operator. Этот агент может самостоятельно использовать интернет и программное обеспечение в облачной среде.

Ранее Operator работал на основе версии GPT-4o, но теперь его заменили на более продвинутую модель под названием o3. Эта новая модель лучше справляется с задачами, требующими логики и математических вычислений.

OpenAI подчёркивает, что новая версия была специально дообучена на данных, связанных с безопасным использованием компьютеров. Это помогает «Оператору» точнее понимать, что ему можно делать, а что — нет. Также он стал менее уязвим к попыткам обмануть ИИ с помощью хитрых запросов (так называемая «промт-инъекция»).

Важно отметить, что хоть o3 Operator и умеет программировать, он не имеет прямого доступа к командной строке или кода, что сделано в целях безопасности.