Согласно исследованию Work Trend Index за 2024 год, 75% сотрудников по всему миру применяют инструменты генеративного искусственного интеллекта в работе. Их используют для написания текстов, программирования и решения других повседневных задач. Однако с активным внедрением ИИ возрастает риск утечки корпоративных данных. О том, как защитить информацию компании, рассказал Иван Башарин, руководитель ИИ-лаборатории VESNA.

Основная угроза кроется в том, что чат-боты и другие ИИ-системы могут сохранять пользовательские запросы в облачных хранилищах. Например, если сотрудник попросит нейросеть подготовить презентацию, загрузив в нее финансовые показатели или информацию о клиентах, эти данные могут остаться в системе. В дальнейшем из-за уязвимостей или ошибок алгоритма они могут стать доступными третьим лицам.

Чтобы минимизировать риски, Башарин советует соблюдать три ключевых правила. Первое — не использовать реальные данные при взаимодействии с ИИ.

> В случае острой необходимости внедрения ИИ, требующего ввода данных, организация может установить политику использования исключительно вымышленной информации. Это предполагает применение нереальных имен, фамилий, электронных адресов и прочей подобной информации.

Иван Башарин
Руководитель ИИ-лаборатории VESNA

Второй важный принцип — не применять нейросети для хранения конфиденциальной информации. Если использование ИИ неизбежно, следует внимательно изучить политику конфиденциальности сервиса. Во многих случаях есть возможность отключить сохранение истории запросов, использовать временные аккаунты или локальные решения без подключения к интернету.

Наконец, организации стоит отдавать предпочтение только лицензированным корпоративным версиям ИИ.

> Эти версии могут подвергаться значительным рискам утечек данных, так как их проще взломать. В отличие от них, бизнес-лицензии разрабатываются с учетом требований корпоративного уровня и обеспечивают регулярные обновления, поддержку со стороны разработчиков и доступ к последним технологическим достижениям в области безопасности.

Иван Башарин
Руководитель ИИ-лаборатории VESNA