Заведующий лабораторией доверенного искусственного интеллекта МИРЭА — Российского технологического университета Юрий Силаев рассказал, что смена паролей не спасёт от утечки данных при использовании публичных ИИ-платформ.

По словам эксперта, публичные ИИ-сервисы обрабатывают информацию на внешних серверах. И сама по себе важная процедура смены паролей не защитит от утечки данных.

По мнению Силаева, лучше для обеспечения защиты использовать не только сложные и разнообразные пароли, двухфакторную защиту, но и специальные приложения для их хранения. Силаев отметил, что основные риски всё же связаны с передачей данных ИИ.

В связи с этим важно следить за доступом ИИ к конфиденциальной информации при принятии пользовательского соглашения. Также важно минимизировать передачу чувствительных данных в публичные ИИ-сервисы и «зашифровывать» данные при работе с такими площадками. К примеру, заменять настоящие инициалы людей на понятные комбинации: «”клиент Иванов” пусть называется “клиент А”, “счёт №12345” — “счёт №XXXXX”».

Также эксперт посоветовал использовать инструменты мониторинга утечек для контроля безопасности данных. Силаев подчеркнул, что ответственность за безопасность данных прежде всего лежит на пользователе, тем более в условиях развития технологий.

«Менять пароли полезно, но этого мало. Лучше использовать сложные и разные пароли для разных сервисов, включать двухфакторную защиту и хранить пароли в специальных приложениях. Однако при работе с ИИ основные риски связаны не с взломом аккаунта, а с тем, куда и как передаются данные. Поэтому важно следить за тем, какой доступ вы даёте ИИ, когда принимаете пользовательское соглашение», — подчеркнул эксперт.