С начала 2025 года в России число взломов аккаунтов в ИИ-сервисах, таких как ChatGPT и Grok, выросло на 90% по сравнению с аналогичным периодом прошлого года.

Об этом сообщили эксперты «Информзащиты» и других компаний в сфере кибербезопасности. Основная причина — растущая популярность ИИ-помощников и хранение в чатах конфиденциальной информации.

Пользователи нередко доверяют нейросетям пароли, данные банков и переписки, что делает аккаунты привлекательной целью. Злоумышленники также атакуют через «прослойки» — сторонние сервисы, которые позволяют обойти региональные ограничения.

Кроме того, активизировались атаки с использованием промпт-инъекций, когда ИИ заставляют выполнять вредоносные действия. По данным BI.ZONE, только за первые месяцы 2025 года зарегистрировано более 2100 доменов-двойников популярных ИИ-сервисов, а случаи шантажа с участием ИИ уже фиксируются в реальности.

Эксперты советуют использовать анонимные данные в чатах, выбирать сложные пароли, регулярно их менять и не хранить личную информацию в переписках.