kaspersky



КиберОктябрь 2026

Тема недели: безопасная работа с ИИ

7 базовых правил безопасной работы с ИИ

1

Не пишите в нейросети то, что не сказали бы незнакомцу

Пароли, номера паспортов и карт, адреса, телефоны, имена сотрудников и клиентов — всё это не должно попадать в переписку с чат-ботом. Нейросеть не различает, где конфиденциальное, а где нет: всё, что вы отправили, сохраняется на её серверах и может быть использовано для обучения модели или выдачи другим людям.

Если данные всё же нужно вставить в запрос — замените их на звёздочки или пометку REDACTED.

2

Не загружайте рабочие документы «чтобы сделать конспект»

Очень соблазнительно отправить в нейросеть отчёт или договор, чтобы получить краткое изложение. Но вместе с документом вы отправляете коммерческую тайну: планы запуска продуктов, зарплаты отдела, условия сделок. А если документ пришёл извне — в нём могут быть спрятаны команды для ИИ, и тогда бот выполнит чужое задание.

3

Проверяйте всё, что сгенерировала нейросеть

Убедительно звучащий ответ не значит правдивый. Нейросеть может перепутать факты, придумать источник, сослаться на несуществующее исследование — это называется «галлюцинация ИИ». Чем важнее вопрос, тем тщательнее проверяйте ответ. Особенно если это код — сгенерированный код может содержать ошибки и уязвимости.

4

Скачивайте ИИ-приложения только из официальных источников

Поддельные приложения «ChatGPT для ПК» и «бесплатные версии ИИ» — это вредоносные программы, которые крадут ваши данные и пароли. В 2026 году «Лаборатория Касперского» выявила почти 100 000 таких атак под видом популярных ИИ-сервисов. В рабочем контексте используйте только те ИИ-инструменты, которые одобрены в вашей компании.

5

Не отправляйте код без проверки и секреты — никогда

Если вы программист и используете ИИ-ассистента — уберите из кода API-ключи, пароли, адреса серверов и всё, что выдаёт структуру вашей инфраструктуры. Эти данные могут украсть или случайно опубликовать. Сгенерированный ИИ код всегда тестируйте как черновик — он может содержать уязвимости.

6

Ограничьте сторонние плагины и надстройки

Плагины для ИИ-чатов создают новые угрозы: часть из них умеет выполнять действия (заказывать билеты, отправлять письма) и может быть использована злоумышленниками (**через промт-инъекцию**). Если плагин нужен — выбирайте те, что существуют давно, регулярно обновляются и имеют много загрузок. Лучше — с открытым исходным кодом.

7

Изучите, что ИИ-сервис делает с данными

Перед использованием сервиса прочитайте политику конфиденциальности: используются ли ваши данные для обучения, как долго хранятся. Многие провайдеры (например, OpenAI) позволяют отключить сохранение истории чатов. А для по-настоящему чувствительных данных лучший выход — локальные модели, которые работают в инфраструктуре без отправки данных в интернет.

КиберОктябрь 2026

Подробнее

www.kaspersky.ru

© 2026, АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее