РЕКОМЕНДАЦИИ
по безопасному взаимодействию с искусственным интеллектом (ИИ)

Рекомендации включают запрет на передачу некоторых категорий данных в ИИ-сервисы. Это связано с рисками утечки информации, несанкционированного использования данных, а также возможными нарушениями требований о конфиденциальности и авторских прав.

Ниже приведены рекомендации по работе с персональными данными, финансовой информацией, медицинской информацией и интеллектуальной собственностью.

Экспресс-проверка перед отправкой в ИИ:

- есть ли в тексте/файле ФИО вместе с телефоном, email или адресом;
- есть ли отдельные телефоны, email-адреса или другие идентификаторы;
- есть ли паспортные данные, ИНН, СНИЛС или сканы документов;
- есть ли финансовые данные (карты, реквизиты, платежи);
- есть ли медицинские сведения;
- есть ли внутренняя информация компании (доступы, схемы безопасности, уязвимости).

Если ответ «да» хотя бы на один пункт - такие материалы нельзя загружать в ИИ без предварительного обезличивания или согласования.

Персональные данные

Не рекомендуется загружать в нейросети:

- ФИО в связке с телефонами, email, адресами и другими идентификаторами;
- паспортные данные, ИНН, СНИЛС и иные государственные идентификаторы;
- сканы/фото паспортов, водительских удостоверений, свидетельств о рождении и других документов, используемых для идентификации личности;
- переписки и документы, содержащие персональные данные клиентов/сотрудников.

Риск возникает не из-за одного имени, а из-за сочетания данных, по которым можно идентифицировать человека.

<u>Рекомендации:</u>

- использовать принцип «очищенных данных»: убирать имена, контакты, точные даты и локации, оставляя только обезличенные факты и показатели;
- не загружать в чат с ИИ целые письма и историю обсуждений - передавать только фрагменты без лишнего контекста;

- если нужен пример, заменять данные на нейтральные обозначения («Клиент_1», «EMAIL_1», «ТЕЛ_1») и добавлять реальные данные уже после получения результата;
- при возможности использовать режимы, где история переписки не сохраняется, а данные не используются для улучшения сервиса (если такие настройки доступны у выбранного провайдера).

Финансовая информация

Не рекомендуется передавать нейросетям:

- банковские реквизиты, данные кредитных и дебетовых карт (включая CVV/CVC и коды подтверждения);
- информацию о транзакциях, инвестициях, задолженностях и иных финансовых операциях.

Даже при защищённой архитектуре сервиса передача финансовых данных через интернет увеличивает риск утечек и мошеннических действий.

Рекомендации:

- использовать для финансовых задач только доверенные (корпоративные) решения и модели ИИ, одобренные компанией;
- регулярно проверять, какие данные используются для работы ИИ, и исключать из них персональные и конфиденциальные сведения;
- не использовать публичные ИИ-сервисы для анализа личных финансовых данных и получения инвестиционных рекомендаций.

Доступы и учетные данные

Запрещено передавать ИИ логины, пароли, коды подтверждения, токены, API-ключи, ссылки для входа и любые сведения, которые открывают доступ к системам и сервисам.

Медицинская информация

Рекомендуем воздерживаться от передачи нейросетям подробной медицинской информации (например: диагнозов, результатов анализов, схем лечения).

ИИ следует использовать только для получения общих справочных сведений без передачи персональных данных и медицинских подробностей.

Интеллектуальная собственность

Не стоит передавать ИИ:

- патентные заявки до подачи;
- незапатентованные изобретения и ноу-хау;
- алгоритмы собственной разработки и внутренние методики;
- черновики проектов, незащищенные идеи, стратегии и планы развития бизнеса;
- схемы безопасности, уязвимости систем и детали внутреннего устройства сервисов.

Рекомендации:

- стараться запрашивать информацию обобщённо, без конкретики и внутренних деталей;
- внимательно изучать условия использования ИИ-сервисов (хранение данных, использование материалов, возможность удаления);
- при создании контента фиксировать процесс (описания запросов, промежуточные версии) - это помогает снижать правовые риски;
- учитывать, что ИИ не гарантирует уникальность результата, возможны совпадения с уже существующими объектами.

Типовые ситуации (безопасный подход)

Если необходимо подготовить письмо, отчет или анализ, сначала попросите ИИ сделать шаблон или структуру без персональных данных, а конкретные сведения добавляйте вручную после получения результата.

Ответственность

Сотрудник несет ответственность за информацию, которую он передает в ИИ-сервисы (тексты, файлы, скриншоты, переписки). При сомнениях рекомендуется не загружать материалы и предварительно согласовать формат данных с ответственным за персональные данные/информационную безопасность.