

Можно ли внедрить ИИ, не словив проблем?



Спикер

Македошин Максим

- IT-юрист команды AG-LEGAL
- вошел в региональный рейтинг лучших юристов «Коммерсантъ»
- включил более 60 ПО в РРПО
- оформляю внедрение ИИ в разработки



Источник: Macintosh HD

Кто мы?

Юридический консалтинг для IT

- 6 лет на рынке
- 800+ клиентов
- 100% успешных регистраций в Реестре российского ПО



Источник: Macintosh HD



Зачем обсуждать ИИ с юристом?

• Практика уже есть

Решение по делу № 02-1545/2026 от 13.07.2026 г.

ИБ зафиксировало как директор по продажам загружает в DeerpSeek коммерческую тайну.
Последовало увольнение за ее разглашение.

Бабушкинский районный суд г. Москвы признал увольнение законным.



О чем поговорим сегодня?

1	Нет регламента по ИИ в компании, что делать? Как выбрать ИИ ?
2	Какие могут быть риски у разных моделей использования ИИ ?
3	Как уже сейчас наказывают за нарушение авторских прав ?
4	Когда ИИ все-таки виноват ?
5	Кому принадлежит дообученная ИИ-модель ?
6	Формируем список рабочих задач и сводим риски на нет.

Нет регламента по ИИ в компании?

• Это база

Принципы, чтобы не стать крайним:

- читайте *пользовательское соглашение*;
- отключайте *дообучение на диалогах*;
- обезличивайте *все передаваемые данные*;
- фиксируйте себе *след ИИ в коде*;
- не используйте *генерацию как готовое решение*.



Как выбрать ИИ?

Реализация	Преимущества	Недостатки
Зарубежная	- Качество ответов - Скорость обработки - Передовые технологии	- Враждебный провайдер и утечки - Отсутствие гарантий - Ограничения использования
Отечественная	- Локализация техники - Легальность использования - Доступ к провайдеру	- Надзор и доступ государства - Сравнительно низкое качество - Небольшой выбор
Локальная	- Максимальный контроль - Подходит для NDA и т.п.	- Стоимость содержания - Трата ресурсов команды

Кейс проекта «Рыбарь»

• Вам могут быть не рады

OpenAI в феврале 2026 г. отчиталась о блокировке связанных с проектом **«Рыбарь»** аккаунтов.

По мнению компании, **часть аккаунтов была создана в РФ**. ИИ использовался для многоязычных кампаний влияния на сайтах и в соц. сетях.

В октябре 2026 г. команду задержала и досмотрела полиция Черногории, после чего депортировали.



Отчет Open AI

Риски по моделям использования

Главный страх трипофоба



ИИ как инструмент разработки

• Бойкот внешним моделям

Условия использования ИИ от Теодора Христакиса:

1. Отсутствие приватности – обучение, анализ и реклама.
2. Непрозрачность обработки – переписка читается и долго хранится.
3. Риск воспроизведения – модель может украсть ваш код или идею.

Утечки неизбежны

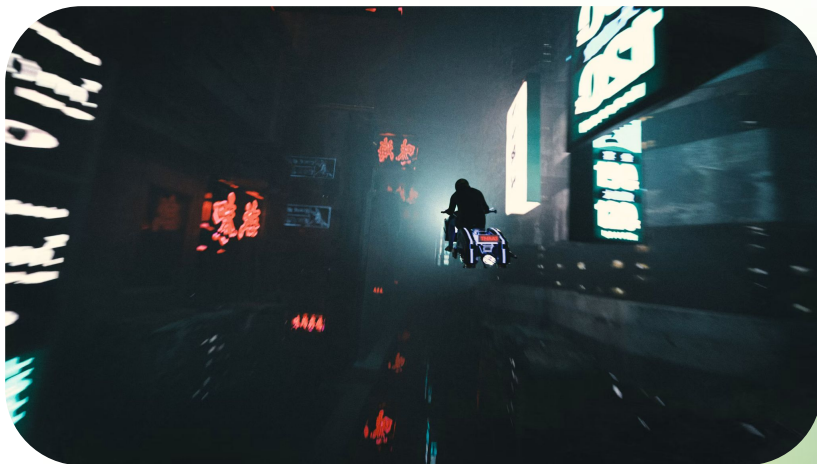


ИИ как инструмент разработки

• **Мировая практика**

Утечки коммерческой тайны привели к запрету использования ИИ в:

- Samsung;
- Apple;
- Amazon.



ИИ как инструмент разработки

• Российская практика

**Определение от 05.08.2025
N 88-10958/2025**

Работодатель **vs** работник

Аналогично: Постановление Конституционного Суда РФ от 26.10.2017 N° 25-П по делу А.И. Сушкова

Работник пересылал себе же рабочие материалы с конфиденциальной информацией в Telegram.

Его уволили за разглашение коммерческой тайны, зафиксировав нарушение ЛНА.

Факт ознакомления третьих лиц с данными суду оказался не важен.

ИИ как функция ПО

• Неприятные вопросы

Найдите **ответы** на вопросы:

- чья эта модель?
- какие данные собираются?
- куда они уходят?
- где хранятся?

Например, у вас есть чат-бот.



ИИ как функция ПО

• Базовые штрафы из сферы ПДн

Статья 13.11 КоАП РФ	Правонарушение	Штраф
ч. 1	Обработка ПДн <u>вне заявленных целей</u>	до 300 тыс. руб.
ч. 2	Обработка ПДн <u>без согласия субъекта</u>	до 700 тыс. руб.
ч. 3	Отсутствуют <u>обязательные документы</u>	до 60 тыс. руб.
ч. 10	<u>Неуведомление</u> РКН об обработке ПДн	до 300 тыс. руб.
ч. 11	Неуведомление РКН об обработке ПДн, повлекшее <u>нарушение прав субъектов</u>	до 3 млн. руб.

ИИ как функция ПО

• Судебная практика по ПДн

**Определение Второго
кассационного суда общей
юрисдикции от 14.11.2023 по
делу N 88-29002/2023**

Клиент **vs** Компания

Пользователь сервиса «Яндекс.Еда» взыскал с компании компенсацию морального вреда после утечки ПДн (имя, телефон, адрес) в открытый доступ.

Суд указал, что оператор несет ответственность за сохранность ПДн независимо от того, кто конкретно совершил утечку, если им не было предприняты все меры безопасности.

Авторские права и ИИ

Преступление и наказание



Нарушение ИИ авторских прав

• **Общая проблема**

Распространенные сценарии:

- в вашу генерацию включены чужие охраняемые РИДы;
- вы обучили ИИ на чужих РИДах;
- результат генерации принадлежит провайдеру.

Выход:

- проверка и переработка материалов;
- заключение лицензионных договоров с авторами;
- изучение пользовательского соглашения.

Нарушение ИИ авторских прав

• **Doe v. GitHub (Copilot litigation)**

Дело Окружного суда США (Северный округ Калифорнии):

- Разработчики **open source** подали иски к GitHub, Microsoft, OpenAI.
- ИИ «GitHub Copilot» **воспроизводил их код** после обучения на нем, **не соблюдая условия лицензий** и не упоминая авторов.
- Суд еще рассматривает дело, но уже:
 - указал на отсутствие намерения нарушить авторские права;
 - допустил наличие **нарушений лицензионных условий**.

Нарушение ИИ авторских прав

• ФЗ от 26.07.2026 N 243-ФЗ

1. Провайдер большой фундаментальной модели **обязан извещать** пользователя о распределении о прав.
2. Провайдер суверенной / национальной большой фундаментальной модели **вправе обучать ИИ** на законно полученном экземпляре произведения **без согласия автора**.

Нарушение ИИ авторских прав

• Российская практика

Дело N A32-40085/2024

Правообладатель **vs** ИП

Компания привлекла к ответственности ИП за использование сгенерированных ИИ изображений, схожих с рисунками истца.

Дело N A56-52652/2024

Правообладатель **vs** автор

Компания привлекла к ответственности фотографа за незаконное использование фотографий, которые он ей сгенерировал и передал. Суд признал фотографа автором.

Когда и кто виноват в ошибках?

Вечная борьба



AG-LEGAL®

✉ @aglegal

Источник: <https://unsplash.com/>
Тип лицензии: royalty free CC0

Ответственность работников за ИИ

• Кто же станет крайним?

1. **Работник** (ст. 241, 243 ТК РФ): материальная ответственность (коммерческая тайна).
2. **ИП-разработчик**: отвечает всем имуществом без ограничений.
3. **СЕО** (ст. 53.1 ГК РФ):
 - отвечает за убытки компании при виновных действиях;
 - субсидиарная ответственность при банкротстве.

Когда же ИИ все-таки виноват?

• Ответственность на провайдере

Провайдер виноват за ответы ИИ, если он:

- призывает к преступным действиям;
- вводит в заблуждение;
- порочит чью-то честь и достоинство;
- создает противоправный контент.



Когда же ИИ все-таки виноват?

• Зарубежная практика

Дело N 26 O 869/26

Landgericht München I

Издательство **vs** Google

Издательские компании подали иск к Google из-за AI Overviews, которые при поиске связывали их с «мошенническими схемами».

Google утверждал, что это автоматически сгенерированный контент из третьих источников.

Суд признал, что такие AI-ответы воспринимаются как собственные высказывания сервиса, и возложил ответственность на провайдера.

Кому принадлежит ИИ-модель?

Простой вопрос, плохой ответ



Вы дообучили чужой ИИ, но...

• он по-прежнему не ваш

1. Open AI в январе 2024 года прекратило поддержку модели text-davinci-003. Компании, дообучившие модели на этой базе, **потеряли к ним доступ**.
2. Google Gemini в феврале 2026 года массово блокировала платные аккаунты за использование OpenClaw, что **привело к потере времени и денег** инвестировавших в дообучение.

Возможные решения

Просто попробуйте



Решения

• Ликвидируем утечки

1. Проведите опрос (**какими ИИ пользуются работники**).
2. Иницилируйте создание регламента использования ИИ:
 - допустимые сервисы;
 - наличие корпоративных аккаунтов;
 - перечень и объем данных, допускаемых и не допускаемых к ИИ;
 - ответственность работников за нарушения.

Решения

• Следим за авторскими правами

1. Введите **правило недоверия** к коду от ИИ (запрещено копировать в прод без ревью и доработки).
2. Внедрите запрет на использование **цельных кусков** от ИИ (human in the loop).
3. **Помечайте использование** ИИ в проде (короткий тег: AI-assisted) для точечной редакции.

Решения

• Грамотно обрабатываем ПДн

1. Согласуйте с юристом **минимальный объем** ПДн.
2. Иницируйте повторную проверку соглашения с провайдеров для установки **запрета на дообучение** ИИ.
3. Введите технически явное информированное согласие для функций, где требуется передача ПДн.

Решения

• Дообучаем, но бережем ресурсы

1. Храните все, что вы создаете вокруг модели:
 - промпты, параметры, пайплайны обработки, метрики качества.
2. Имейте в запасе другие модели на «черный день».
3. Иницилируйте создание локальной ИИ-модели.
4. Обеспечьте низкую зависимость проекта от конкретной ИИ-модели.

Итоги

1. Риски везде, так всегда было и будет.
2. Темы для размышления и инструменты даны.
3. Решение за вами.



Остаемся на связи



Максим Македошин
@Maximillus

Команда **AG-LEGAL**



Наш **чат IT-тусовки**



AG-LEGAL®

📩 @aglegal