

ЧЕК-ЛИСТ ДЛЯ ЮРИДИЧЕСКОЙ СЛУЖБЫ, ИБ И ИТ

Договор с ИИ-подрядчиком: что проверить перед подписанием

Восемь блоков проверки с полем «что просить», три готовые формулировки, переговорные позиции по спорным пунктам и заготовка протокола разногласий

Выбор подрядчика

Чек-лист договора

Формулировки

Переговорные позиции

Разбор инцидента

Протокол разногласий

Закон об ИИ ответственность между участниками не распределил: статья 11 Федерального закона от 26.07.2026 № 243-ФЗ отсылает к общему законодательству, роли разработчика, оператора и пользователя не разведены. Пока специальных норм нет, границу между заказчиком и подрядчиком проводит договор. Документ носит аналитический характер и не заменяет юридическую консультацию.



Как пользоваться

СОДЕРЖАНИЕ

1. Как пользоваться
2. Почему это вообще на вас
3. На этапе выбора подрядчика
4. Если договора ещё нет
5. Чек-лист: восемь блоков
6. Три формулировки
7. Переговорные позиции
8. Первые сутки после инцидента
9. Что зависит от вас, а не от договора
10. Протокол разногласий
11. Если этим некому заняться

Документ рассчитан на один проход по договору перед переговорами: восемь блоков, в каждом — что искать, как выглядит типичная проблема, что просить взамен и три отметки для результата. На реальном договоре это занимает около часа, на коротком — минут двадцать.

Четыре блока помечены как критичные. Это не значит, что остальными можно пренебречь: это значит, что при ограниченном переговорном ресурсе спорить стоит за них в первую очередь.

Заполненный чек-лист переносится в таблицу протокола разногласий на предпоследней полосе: пункт договора, что не устраивает, что предлагаем. С этой таблицей можно идти к подрядчику.

Документ не заменяет юридическую экспертизу и не учитывает специфику вашей сделки: предмет, отраслевые требования, режим обрабатываемых данных. Считайте его картой мест, где договоры с ИИ-подрядчиками чаще всего оказываются пустыми.

Для заполнения от руки используйте печатную версию: светлый фон и увеличенные поля для заметок.



Почему это вообще на вас

Федеральный закон от 26.07.2026 № 243-ФЗ ввёл понятийный аппарат, принципы и статусы моделей: рамочные нормы работают с 1 сентября 2026 года, требования к моделям и обязанности разработчиков включаются с 1 марта 2027-го. Часть будущих требований имеет смысл закладывать в договор уже сейчас, с отложенным сроком исполнения.

Ответственности закон посвятил одну отсылочную статью: участники отношений в сфере искусственного интеллекта отвечают в соответствии с законодательством Российской Федерации. Разделения между разработчиком модели, оператором системы и пользователем в законе нет, специальных составов правонарушений тоже.

Практически это означает, что применяются общие правила: договорные, деликтные, требования 152-ФЗ к обработке персональных данных, отраслевое регулирование. Центр тяжести смещён к тому, кто применяет систему и выпускает решение наружу, — к оператору. Он отвечает первым, а дальше может переложить часть последствий на подрядчика в том объёме, который заранее записан в договоре.

Разбор нормы целиком — в статье «Кто отвечает за ошибку ИИ» на azoneai.ru/blog/33-otvetstvennost-za-oshibku-ii/



На этапе выбора подрядчика

Пять вопросов, которые задаются до того, как появится проект договора. Ответы на них определяют, о чём вообще получится договариваться дальше.

- 1 Кто владеет моделью, которую вам предлагают**
Собственная разработка, открытые веса под конкретной лицензией или доступ к чужому API. Третий вариант означает, что часть условий подрядчик не контролирует и гарантировать не сможет.
- 2 Где выполняется инференс**
В вашем периметре, в его облаке или у стороннего провайдера. От ответа зависит весь блок про данные и половина блока про журналы.
- 3 Есть ли опыт работы в аттестованном контуре**
Развернуть модель в изолированном сегменте и сдать аттестованный объект информатизации — работы разного порядка. Если требования к аттестации у вас есть, спрашивать об этом нужно до конкурса.
- 4 Кто эксплуатирует систему после сдачи**
Ваши инженеры, подрядчик по договору поддержки или никто конкретно. Третий вариант встречается чаще, чем признаётся, и именно он потом порождает споры о качестве.
- 5 Что происходит при смене лицензии на модель или уходе вендора**
Останутся ли у вас веса, конфигурации, промпты и индекс в пригодном для работы виде.

Если договора ещё нет

Часто на руках только коммерческое предложение и техническое задание. Проверять в этом случае нужно то же самое, но раньше и в другом документе.

В техническом задании должны появиться: состав журналирования, порядок приёмки с методикой, требование к фиксации версии модели. Всё это потом попадёт в договор автоматически, а вписать в готовый договор будет уже труднее.

В коммерческом предложении стоит обратить внимание на то, чего в нём нет: юрисдикции обработки данных, судьбы производных, условий поддержки после сдачи. Молчание на этом этапе почти всегда означает, что вопрос не проработан.



Чек-лист: восемь блоков

Отметьте по каждому блоку своё положение дел. Пустая отметка честнее оценки на глаз: на переговорах видно, где вы не проверяли, а где условие действительно отсутствует.

1 Границы предмета

Что проверяем. За что подрядчик отвечает: за работоспособность системы или за корректность каждого ответа модели. Второго не гарантирует никто — генеративная модель по своей природе даёт вероятностный результат, и обещание обратного само по себе повод насторожиться. Важнее другое: записано ли, что система формирует рекомендацию, а решение принимает сотрудник заказчика.

Как выглядит проблема. Предмет описан как «внедрение ИИ-системы» без указания, что считается результатом работы и что — решением. При инциденте спор смещается с фактов на вопрос, чью ошибку вообще разбирают.

Что просить. Разделение в тексте договора: результат работ — работающая система с описанными характеристиками; выходные данные системы носят рекомендательный характер; решение по ним принимает уполномоченный работник заказчика.

☐ есть ☐ нет ☐ формулировка слабая

Заметка: _____

2 Права на модель и лицензия весов

Что проверяем. Подтверждает ли подрядчик правомерность использования весов модели, указана ли редакция лицензии на дату поставки, обязан ли он уведомить об её изменении, есть ли возмещение при претензиях правообладателей.

Как выглядит проблема. Модель развёрнута из открытого репозитория, лицензия в договоре не названа вовсе. Через год условия использования меняются, а обязанности сообщить об этом у подрядчика нет.

Что просить. Приложение с перечнем компонентов и лицензий на дату подписания, гарантия правомерности использования, уведомление об изменении лицензионных условий в разумный срок, возмещение расходов заказчика при претензиях третьих лиц.

☐ есть ☐ нет ☐ формулировка слабая

Заметка: _____

3 Юрисдикция обработки и хранения, включая производные

КРИТИЧНО

Что проверяем. Где выполняется инференс, где физически лежат данные и что происходит с производными: журналами запросов и ответов, векторными представлениями корпуса, кэшем генераций.

Как выглядит проблема. Про основные данные написано подробно, про производные — ни слова. Между тем в журналах оседают фрагменты документов, а из векторного индекса, по опубликованным исследованиям, при определённых условиях частично восстанавливается исходный текст: насколько именно — зависит от модели эмбеддингов и объёма корпуса.

Что просить. Формулировка про данные и производные из раздела «Три формулировки», плюс указание конкретной площадки размещения и порядка удаления данных и производных при расторжении.

☐ есть ☐ нет ☐ формулировка слабая

Заметка: _____

4 Методика приёмки вместо процента точности

Что проверяем. Как измеряется качество. Проверяемая конструкция — согласованный набор кейсов, описанная процедура прогона и критерий приёмки по результатам.

Как выглядит проблема. В договоре стоит формулировка вида «точность ответов не менее 95%» без методики измерения. Такую цифру нельзя ни подтвердить, ни оспорить, и в споре она работает против обеих сторон.

Что просить. Приложение «Методика приёмочных испытаний»: набор согласованных кейсов с эталонными ответами, порядок прогона, кто оценивает результат и по каким критериям, что считается устранимым замечанием.

☐ есть ☐ нет ☐ формулировка слабая

Заметка: _____

5 Журналы и порядок разбора инцидента

КРИТИЧНО

Что проверяем. Кто ведёт журналы, что в них попадает, сколько они хранятся, у кого доступ. Отдельно — порядок совместного разбора с воспроизведением запроса на зафиксированной версии.

Как выглядит проблема. Логирование формально включено, но ротация настроена на неделю, а версия модели в записи не попадает. Восстановить картину инцидента по таким журналам невозможно.

Что просить. Состав записи: запрос, извлечённый контекст, версия модели, ответ, кто утвердил результат. Срок хранения не менее 12 месяцев, выгрузка по требованию заказчика в течение 3 рабочих дней, совместный разбор с воспроизведением на зафиксированной версии.

☐ есть ☐ нет ☐ формулировка слабая

Заметка: _____

6 Управление версиями

Что проверяем. Порядок замены базовой модели, весов и системных инструкций: уведомление, согласование, фиксация версии как объекта приёмки. Для аттестованного сегмента — оценка влияния на аттестованную конфигурацию.

Как выглядит проблема. Подрядчик оставляет за собой право обновлять модель по своему усмотрению. После планового обновления система начинает вести себя иначе, а сравнить поведение с приёмочной версией нечем.

Что просить. Формулировка про смену версии из раздела «Три формулировки», плюс фиксация версии модели и системных инструкций в акте приёмки как характеристики результата работ.

☐ есть ☐ нет ☐ формулировка слабая

Заметка: _____

7 Пределы ответственности и исключения из них

КРИТИЧНО

Что проверяем. Ограничение суммой договора обсуждается всегда, и спорить о проценте менее продуктивно, чем о списке исключений: утечка персональных данных, нарушение прав третьих лиц, умысел, грубая неосторожность. Последнюю подрядчики вычёркивают первой.

Как выглядит проблема. Ограничение есть, исключений нет, косвенные убытки исключены целиком. При утечке возмещение упирается в потолок, который к масштабу последствий отношения не имеет.

Что просить. Формулировка про исключения из предела ответственности из раздела «Три формулировки». Отдельный предмет торга — размер самого предела: цена договора или годового вознаграждения вместо доли от них.

☐ есть ☐ нет ☐ формулировка слабая

Заметка: _____

8 Персональные данные и поручение на обработку

КРИТИЧНО

Что проверяем. Получает ли подрядчик доступ к данным при поддержке, дообучении или разборе инцидентов. Если да — нужно поручение на обработку по правилам 152-ФЗ с распределением ролей оператора и обработчика, перечнем действий и требованиями к защите.

Как выглядит проблема. Доступ фактически есть — инженеры подключаются к контуру для диагностики, — а поручения нет, потому что «данные не передаются».

Что просить. Поручение на обработку отдельным приложением: перечень действий, цели, категории данных и субъектов, требования к мерам защиты, запрет привлечения соисполнителей без согласия, журналирование каждого подключения инженеров подрядчика к контуру.

☐ есть ☐ нет ☐ формулировка слабая

Заметка: _____

Три формулировки

Заготовки к блокам 3, 6 и 7. Формулировки написаны так, чтобы их можно было перенести в протокол разногласий и обсуждать предметно.

Исключения из предела ответственности

«Ограничение ответственности, установленное настоящим пунктом, не применяется к убыткам, возникшим вследствие разглашения или утраты персональных данных, нарушения прав третьих лиц на результаты интеллектуальной деятельности, а также умышленных действий Исполнителя».

Данные заказчика и производные

«Исполнитель не вправе использовать данные Заказчика, включая журналы запросов и ответов, векторные представления корпуса и кэш генераций, для обучения или дообучения моделей, а также передавать их третьим лицам».

Смена версии

«Замена базовой модели, её весов или системных инструкций производится по предварительному письменному согласованию с Заказчиком; для сегмента, прошедшего аттестацию, — после оценки влияния на аттестованную конфигурацию».

Это заготовки для разговора с юристом. Готовым текстом договора они не являются: ни предмет вашей сделки, ни применимое к ней регулирование здесь не учтены.

Переговорные позиции

Левая колонка описывает то, что чаще всего оказывается в присланной редакции, — по нашей договорной практике, без претензии на рыночную статистику. Правая колонка — позиция для входа в переговоры; нормативом она не является.

Параметр	Что обычно в первой редакции	Куда двигаться
Предел ответственности	Ограничение процентом от цены договора, косвенные убытки исключены	Цена договора или годового вознаграждения; из-под предела выведены утечка ПДн, права третьих лиц, умысел, грубая неосторожность
Хранение журналов	Короткий срок либо условие отсутствия	Не менее 12 месяцев, с выгрузкой по требованию заказчика
Разбор инцидента	Общий срок ответа на обращение	Фиксация в течение суток, совместный разбор с воспроизведением — 5 рабочих дней
Смена версии модели	Право подрядчика без уведомления	Уведомление за 30 дней, для аттестованного сегмента — предварительное согласование
Данные для дообучения	Не оговорено	Прямой запрет, включая производные
Доступ к данным при поддержке	Общая фраза о технической поддержке	Перечень действий, поручение на обработку, журналирование доступа

Конкретные сроки и пределы зависят от предмета сделки и переговорной силы сторон. Полезнее относиться к таблице как к списку пунктов, которые обязательно должны быть проговорены.



Первые сутки после инцидента

Получив претензию или обнаружив ошибочное решение, сначала фиксируют доказательства, потом разбираются в причинах. Порядок обратный привычному, потому что журналы стираются сами.

Что выгружается и сохраняется отдельно от рабочей системы: журналы за спорный период целиком; текущая версия модели и её весов; системные инструкции и шаблоны промптов в редакции на момент события; состав корпуса и права доступа, под которыми выполнялся запрос; запись о том, кто утвердил результат.

Отдельно останавливается плановое обновление модели до окончания разбора. Обновление, прошедшее через сутки после инцидента, уничтожает возможность воспроизвести спорный ответ.

Кто отвечает за фиксацию: _____

Где хранится выгрузка: _____



Что зависит от вас, а не от договора

Часть рисков договором не закрывается в принципе. Нужен перечень ИИ-сценариев с указанием владельца решения по каждому. Нужен регламент проверки ответов человеком — хотя бы на тех сценариях, где результат уходит наружу. Нужен приказ о владельце системы и определение того, что в вашей компании считается решением системы. Всё это внутренние документы: они стоят дешевле любой договорной конструкции и начинают работать раньше неё.

Проверьте заодно, что журналы действительно пишутся: включённое логирование и хранимые журналы — разные состояния, и расходятся они чаще, чем кажется.



Протокол разногласий

Перенесите сюда пункты, отмеченные как «нет» или «формулировка слабая».

Пункт договора	Что не устраивает	Что предлагаем

Если в таблице оказалось три и более критичных блока, вопрос уже не к формулировкам: стоит вернуться к архитектуре решения и составу работ, пока договор не подписан.

Если этим некому заняться

Проверка договора не требует подрядчика: всё описанное здесь делается силами юридической службы вместе с ИТ и ИБ. Методику мы выложили целиком именно поэтому.

Но если разбирать нужно не один договор, а портфель, или требуется техническая сторона аргументации — что технически возможно журналировать, какой срок хранения реалистичен, что меняется при смене версии модели, — AZONE-AI может пройти этот путь вместе с вашей командой в рамках пилотного проекта.

Развёртывание идёт на инфраструктуре заказчика: модель, векторное хранилище и документы не покидают периметр. Для аттестованных сегментов это условие обязательное, и обсуждать его лучше до подписания договора.

Обсудить пилот и юридическую рамку

Подробный разбор нормы: статья «Кто отвечает за ошибку ИИ: что на самом деле сказано в 243-ФЗ» на сайте AZONE-AI

azoneai.ru/services/ai-pilot/ · ContractGuard для ревизии портфеля договоров · лицензии ФСТЭК, ФСБ, МО РФ · статья: azoneai.ru/blog/33-otvetstvennost-za-oshibku-ii

AZONE-AI · направление компании АЗОН. Корпоративные AI/LLM-решения в закрытых контурах: on-premise развёртывание, RAG-системы, ИИ для информационной безопасности.

Документ подготовлен в сентябре 2026 года и отражает состояние регулирования на эту дату: подзаконных актов и правоприменительной практики по 243-ФЗ нет. AZONE-AI не является юридической фирмой; материал содержит в том числе экспертные трактовки и не заменяет юридическую консультацию. Формулировки статьи 11 сверяйте с официальной публикацией: publication.pravo.gov.ru, номер опубликования 0001202607260003.