



AZONE AI

ON-PREMISE ИИ · ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Чек-лист для закупки · PDF

15 пунктов выбора ИИ-подрядчика и 7 красных флагов

Рабочий документ для ИТ-директора, закупки и CISO. Что проверять, какие вопросы задавать и какие документы запрашивать — до того, как подписан договор на пилот.

15

критериев
проверки

7

красных
флагов

9

пунктов в договоре
на пилот

1 15 пунктов проверки

По каждому критерию — зачем проверять, что спросить, какой документ запросить и риск, если критерия нет. Чекбоксы слева — чтобы отмечать прямо в распечатке. Критерии 1, 2, 4, 5 и 8 (лицензии под задачу и работа в закрытом контуре с ИБ) для проектов с чувствительными данными не обсуждаются. Остальное определяет, насколько гладко пройдёт проект.

1 Лицензии ФСТЭК, ФСБ, при необходимости МО РФ

Без них нельзя работать с гостайной, КИИ и СЗИ в ряде проектов.

Что спросить	Номера лицензий и виды работ. Кто конкретно держатель — подрядчик или субподрядчик?
Что запросить	Копии лицензий, проверка по реестру ведомства.
Риск, если нет	Юридическая невозможность проекта; ответственность ложится на заказчика.

2 Опыт on-premise-развёртываний

Облачный опыт не переносится на закрытый контур.

Что спросить	Сколько внедрений «на земле», на каком железе, в каких отраслях?
Что запросить	Референс-лист, обезличенные описания инсталляций.
Риск, если нет	Подрядчик учится за ваш счёт, сроки плывут.

3 Собственные продукты, а не только услуги

Продукт — это накопленная экспертиза и переиспользуемый код.

Что спросить	Что из стека своё, что — чужой open-source? Что вы поддерживаете сами?
Что запросить	Описание продуктовой линейки, демо своих компонентов.
Риск, если нет	Важен не сам «свой продукт» (бывает вендор-лок), а переиспользуемость наработок.

4 Реестр Минцифры / статус подачи

Для госзаказчиков и предпочтений при закупке.

Что спросить	Есть ли запись в реестре отечественного ПО? Номер?
Что запросить	Выписка из реестра или подтверждение статуса подачи.
Риск, если нет	Ограничения по 44-ФЗ / 223-ФЗ для госсектора.

5 Совместимость с Astra Linux, РЕД ОС, Postgres Pro

В госконтуре другого стека часто просто нет.

Что спросить	На каких ОС и СУБД уже разворачивали в проде?
Что запросить	Протоколы испытаний, сертификаты совместимости.
Риск, если нет	Решение не встанет в вашу инфраструктуру.

6 SLA и регламент эксплуатации

ИИ-система требует сопровождения, а не «сдал и забыл».

Что спросить	Время реакции, окна обновления модели, кто дежурит?
Что запросить	Проект SLA, регламент сопровождения.
Риск, если нет	Система деградирует, обновления ломают работу.

7 Методология пилота 4–8 недель

Структурированный пилот даёт измеримый результат.

Что спросить	Как устроен пилот? Какие метрики, точки контроля, критерии go/no-go?
Что запросить	План пилота с этапами и метриками.
Риск, если нет	Пилот без рамок превращается в бесконечную доработку.

8 ИБ-аудит подрядчика, NDA, безопасность поставки

Подрядчик получает доступ к вашим данным.

Что спросить Готовы подписать NDA до получения данных? Как передаются данные?

Что запросить Шаблон NDA, описание процесса передачи и хранения.

Риск, если нет Утечка через сам канал внедрения.

9 Финансовая устойчивость

Проект идёт 6–18 месяцев. Банкротство исполнителя на стадии пилота оставляет заказчика с недостроенной системой.

Что спросить Сколько лет на рынке? Есть ли судебные споры, признаки банкротства?

Что запросить Выписка ЕГРЮЛ, отсутствие в реестрах банкротств.

Риск, если нет Подрядчик исчезает на середине, права на код не переданы.

10 Команда: роли, опыт, сертификаты

За красивой презентацией бывает один человек.

Что спросить Кто конкретно делает проект? Какие роли, какой опыт?

Что запросить CV ключевых ролей, сертификаты.

Риск, если нет Продают сеньоров, работают стажёры.

11 Демо-стенд или живая демонстрация

Слайды о технологии ничего не доказывают.

Что спросить Можете показать систему вживую — хотя бы на синтетике?

Что запросить Доступ к демо-стенду или запись живой демонстрации.

Риск, если нет Платите за то, чего не видели.

12 Прайс-ориентир до старта

Чтобы понимать порядок цифр и защищать бюджет.

Что спросить Какая вилка по пилоту и по промышленному запуску?

Что запросить Предварительная смета или вилка стоимости.

Риск, если нет Сюрприз в смете после подписания.

13 Образцы документов: ТЗ, акт, отчёт пилота

Видно зрелость процессов и качество отчётности.

Что спросить Покажете обезличенные образцы прошлых проектов?

Что запросить Шаблоны ТЗ, акта приёмки, отчёта по пилоту.

Риск, если нет После пилота нечего предъявить на комитете.

14 Опыт с КИИ / отраслевой спецификой

Банк, энергетика, госсектор — разные требования.

Что спросить Есть кейсы в нашей отрасли? Знаете её регуляторику?

Что запросить Кейсы по отрасли, понимание профильных норм.

Риск, если нет Подрядчик не знает ваших ограничений.

15 Карта эскалации и ответственность

Когда что-то сломается, нужно знать, к кому идти.

Что спросить Кто отвечает за инцидент? Какие сроки и ответственность в договоре?

Что запросить Карта эскалации, раздел об ответственности в договоре.

Риск, если нет В критический момент никого не найти.

2 7 красных флагов

Любой из этих признаков — повод насторожиться. Два и больше — повод не подписывать. Почти все они проявляются на пресейле, до денег.

1 Нет лицензий ФСТЭК/ФСБ там, где они нужны

Берётся за проект с КИИ или гостайной без лицензий: «привлечём субподрядчика». Ответственность останется на вас.

2 Нет NDA на предварительном этапе

Просит выгрузить документы «чтобы оценить объём», но соглашение о конфиденциальности подписать не предлагает.

3 Нет демонстрации технологии

На просьбу показать систему — уход в слайды и «коммерческую тайну». Зрелый подрядчик показывает стенд хотя бы на синтетике; полный отказ — сигнал.

4 Расплывчатые сроки и стоимость

«Сделаем за пару месяцев, бюджет по ходу». Нет вилки до старта — либо не понимает объём, либо добирает на допработах.

5 «Дообучим под вас», но без метрик

Fine-tuning как волшебная кнопка. На сотне разнородных документов дообучение чаще ухудшает ответы; проверить эффект без замера до/после нельзя.

6 Нет плана перехода пилот → промышленная эксплуатация

Про пилот — с энтузиазмом, про «как это поедет в прод и кто сопровождает» — уклончиво. Пилот без продолжения — это демо за ваши деньги.

7 Готовность подписать всё без уточнений

Соглашается на любые формулировки, не спросив про данные, доступы и ответственность. Выглядит как гибкость, на деле — безразличие.

3 Зрелый и незрелый подрядчик

Короткий тест по поведению, а не по презентации.

Зрелый подрядчик	Незрелый подрядчик
Спрашивает про данные и ИБ на первой встрече	Сразу показывает демо и называет цену
Предлагает измеримый пилот с метриками	Предлагает сразу промышленный контракт
Честно называет, что ИИ не закроет	Обещает решить любую задачу
Подписывает NDA до получения данных	Просит данные «чтобы оценить» без NDA
Фиксирует критерии приёмки в договоре	Оставляет приёмку «на усмотрение»
Показывает план перехода пилот → пром	Про эксплуатацию — «потом разберёмся»

4 Что должно быть в договоре на пилот

Договор на пилот защищает не юриста, а сам проект — от того, чтобы «успех» каждая сторона понимала по-своему.

Цель пилота

Одной проверяемой фразой. Не «внедрить ИИ», а «сократить время поиска документа с N минут до M».

Порядок приёмки

Кто, по каким критериям и в какие сроки принимает результат.

Метрики успеха

Конкретные числа и способ замера. Иначе приёмка — спор «нравится / не нравится».

Ограничения результата

Честная фиксация: пилот проверяет гипотезу, а не гарантирует промышленный результат.

Состав и объём данных

Что передаётся, в каком формате, кто отвечает за подготовку.

Права на доработки

Кому принадлежит код и настройки, можно ли продолжить с другим подрядчиком.

Ответственность сторон

Что делает подрядчик, что остаётся на заказчике (подготовка данных и доступы — всегда на заказчике).

Условия перехода в пром

Хотя бы рамочно — чтобы успешный пилот не упёрся в переговоры с нуля.

ИБ-требования

Где обрабатываются данные, кто имеет доступ, что происходит с ними после пилота.

5 Подготовка к встрече с подрядчиком

Часть неудачных пилотов срывается не на стороне подрядчика: заказчик приходит на встречу без данных и без сформулированной цели. Соберите до разговора:

Р Описание процесса, который хотите автоматизировать, — как он работает сейчас.

Р Набор данных или понимание, где они лежат, в каком объёме и состоянии.

Р ИБ-ограничения: что можно выгружать, что нельзя, требования к контуру.

Р Ожидаемый эффект: в чём измеряете успех (время, деньги, ошибки).

Р Текущие системы, с которыми решение должно интегрироваться.

Р Бюджетный коридор — хотя бы порядок цифр.

Р Сроки: когда нужен результат и от чего зависит дедлайн.

Чем конкретнее этот набор, тем точнее любой подрядчик оценит проект — и тем меньше сюрпризов в смете и сроках.



Проверьте AZONE AI по этому же чек-листу

On-premise ИИ в закрытом контуре, лицензии ФСТЭК, ФСБ и МО РФ, работа от пилота с согласованными метриками. Опишите задачу, данные и ограничения — оценим объём пилота и пришлём ориентир по срокам и стоимости.

azoneai.ru/contact · полный разбор — статья «Как выбрать ИИ-подрядчика в 2026» на azoneai.ru/blog

Документ носит методический характер и подготовлен по состоянию на июнь 2026 года. Конкретные требования к лицензированию, реестрам и закупочным процедурам следует сверять с действующими нормами и профильными специалистами. Сведения о лицензиях и статусах AZONE AI / АЗОН проверяйте по официальным реестрам.