ЧЕК-ЛИСТ ДЛЯ ИТ, ИБ, ЮРИСТОВ И ЗАКУПОК

Чек-лист: допустимость LLM для КИИ и госсектора

Три фильтра, вопросы к вендору и таблица для обоснования в техзадании

Единого реестра разрешённых моделей ИИ в России нет. Можно ли поставить конкретную модель в ГИС или на значимый объект КИИ, решают три независимые проверки: защита информации, происхождение ПО и статусы по 243-ФЗ. Документ превращает их в вопросы, на которые можно ответить за одно совещание.

1. **Защита информации**
   Требования к системе, в которой работает модель: аттестация, модель угроз, приказы ФСТЭК № 117 и № 239
2. **Происхождение ПО**
   Указ № 166, 58-ФЗ и национальный режим в закупках: запись в реестре под конкретную редакцию
3. **Статус по 243-ФЗ**
   Суверенная и национальная модель, право Правительства ограничить выбор с 1 марта 2027 года

Шаг 0: статус системы | Три фильтра | 12 вопросов к вендору | Таблица для ТЗ | Календарь норм

По состоянию на 12 октября 2026 года. Данные о записях в реестре российского ПО — на 6 октября 2026 года. Проекты нормативных актов помечены как проекты. Документ не является юридической консультацией: нормы и записи в реестре сверяйте на дату закупки.

Как пользоваться

Вопрос «можно ли нам эту модель» распадается на три самостоятельных. Выдержит ли система, в которой работает модель, требования к защите информации. Подходит ли модель по происхождению ПО, если речь о значимом объекте КИИ или о госзакупке. И что будет с выбором модели, если Правительство ограничит его в вашей сфере по 243-ФЗ.

Заполняйте вместе. ИТ отвечает за архитектуру и сроки ввода, ИБ — за модель угроз и аттестацию, юрист — за применимость норм, закупки — за режим закупки и документы вендора.

Порядок простой. Сначала шаг 0: он показывает, какие фильтры к вашей системе вообще применяются. Затем фильтры по очереди. Вариант, не прошедший фильтр, дальше не проверяйте.

Оценивается всегда пара «модель плюс способ поставки». Одна и та же модель в облаке владельца и в контуре заказчика проходит фильтры по-разному.

Отметка	Что значит	Что делать дальше
Да	Требование выполнено, есть подтверждающий документ	Записать документ и дату
Нет	Требование не выполнено	Сменить способ поставки или вариант, см. последний раздел
Требует уточнения	Ответ должен дать вендор, юрист или владелец системы	Записать, кто отвечает и к какой дате

Шаг 0. Статус системы и режим закупки

Ответы на эти вопросы определяют, какие фильтры действуют. Без них проверка модели превращается в спор о нормах, которые к системе могут не относиться.

Вопрос	Ответ	Где взять
Система — государственная информационная система?	☐ Да, класс ___ ☐ Нет	Акт классификации, аттестат соответствия
Система — объект КИИ?	☐ Да ☐ Нет	Перечень объектов КИИ организации
Объект значимый?	☐ Да, категория ___ ☐ Нет	Акт категорирования
Кто владелец объекта или оператор системы?	☐ Госорган ☐ Заказчик по 223-ФЗ ☐ Иное	Устав, положение о закупке
Обрабатываются ли персональные данные?	☐ Да, УЗ-___ ☐ Нет	Модель угроз, акт определения уровня защищённости
Режим закупки	☐ 44-ФЗ ☐ 223-ФЗ ☐ Собственные правила	План-график, положение о закупке
Плановая дата ввода в промышленную эксплуатацию	_____	План проекта

Какие фильтры действуют для вашей системы

Тип системы	Защита информации	Происхождение ПО	Закупка	Статус по 243-ФЗ
ГИС госоргана	Действует: аттестация, приказ ФСТЭК № 117	Если ГИС — значимый объект КИИ: указ № 166	44-ФЗ: запрет иностранного ПО по ПП № 1875	С 1 марта 2027 — если сфера попадёт в перечень
Значимый объект госоргана или заказчика по 223-ФЗ	Действует: приказ ФСТЭК № 239	Действует: указ № 166, 58-ФЗ	44-ФЗ или положение о закупке по 223-ФЗ	С 1 марта 2027 — если сфера попадёт в перечень
Значимый объект иного владельца	Действует: приказ ФСТЭК № 239	Действует с графиком 58-ФЗ	Собственные правила	С 1 марта 2027 — если сфера попадёт в перечень
Незначимый объект КИИ	Модель угроз; 152-ФЗ при обработке ПДн	Не действует	По режиму закупки	С 1 марта 2027 — если сфера попадёт в перечень
Коммерческая система без КИИ	Модель угроз; 152-ФЗ при обработке ПДн; аттестация обычно не нужна	Не действует	По режиму закупки	С 1 марта 2027 — если сфера попадёт в перечень

Закупка по 44-ФЗ включает запрет на иностранное ПО независимо от того, относится ли система к КИИ. **По 223-ФЗ** национальный режим применяется через положение о закупке конкретного заказчика.

Фильтр 1. Защита информации

Требования по защите информации предъявляются к системе, в которой работает модель: к классу защищённости ГИС, категории значимости объекта КИИ, уровню защищённости персональных данных. Модель внутри аттестованной среды наследует её защиту при одном условии — её включили в модель угроз и в проект системы защиты.

Для любой системы

- [ ] **Модель, движок генерации и векторная база включены в модель угроз.** Угрозы для ИИ — подмена весов, утечка через ответы, внедрение инструкций в документы базы знаний — описаны явно.
- [ ] **Компоненты ИИ отражены в проекте системы защиты.** Стенд «на пробу» рядом с аттестованной системой её защиту не наследует.
- [ ] **Ответ генерируется на серверах внутри вашего периметра.** При генерации во внешнем сервисе запросы, фрагменты документов и история диалогов уходят к владельцу сервиса.
- [ ] **Журналы запросов и ответов хранятся внутри периметра.** Зафиксируйте систему хранения и срок.
- [ ] **Определён круг лиц с доступом к журналам.** В журналах — содержание запросов, то есть те же данные, что в документах.
- [ ] **Модель и движок работают без внешних соединений.** Проверьте обновления, телеметрию и проверку лицензий.
- [ ] **Веса заносятся в контур на согласованном носителе и сверяются по контрольным суммам.** Контрольные суммы берут у правообладателя.
- [ ] **Доступ к базе документов для RAG повторяет права пользователей.** Модель не должна выдавать фрагмент документа, который пользователь не может открыть сам.

Для ГИС и систем госорганов, госучреждений, ГУП — приказ ФСТЭК № 117

Действует с 1 марта 2026 года вместо приказа № 17.

- [ ] **Определены шаблоны запросов или допустимые тематики, контроль их соблюдения настроен.** Ограничения проще задать в интерфейсе, чем полагаться на дисциплину пользователей.
- [ ] **Есть механизм контроля недостоверных ответов.** Ссылка на источник в каждом ответе показывает проверяющему, что именно проверять.
- [ ] **Исключено нерегламентированное влияние ИИ на работу системы.** Модель не меняет данные и настройки системы без участия человека.

Рекомендуется закладывать уже сейчас — проект поправок к приказу № 117

Проект вынесен на обсуждение 24 августа 2026 года, планируемое вступление — 1 марта 2027 года. Это проект, но новую систему разумно проектировать уже под него.

- [ ] **Модели выделены в отдельный сегмент инфраструктуры.**
- [ ] **Доступ в сегмент — с усиленной многофакторной аутентификацией и минимальными правами.**

- ☐ **Действия пользователей в сегменте регистрируются и анализируются.**
- ☐ **Для моделей, работающих с информацией ограниченного доступа, настроены контроль доступа к моделям, фильтрация входных и выходных данных и квоты на запросы.**
- ☐ **Права ИИ-агентов описаны во внутренних стандартах и контролируются.** Это касается и автономных агентов.

Для значимых объектов КИИ

- ☐ **Компоненты ИИ учтены в мерах защиты объекта по приказу ФСТЭК № 239.** Приказ применяется к значимым объектам; к незначимым — нет.

Локальная установка ещё не аттестация. Для ГИС аттестация обязательна до ввода в эксплуатацию, и модель становится частью аттестуемой системы. Коммерческой системе без статуса ГИС и без значимых объектов КИИ аттестация обычно не требуется: достаточно модели угроз и выполнения 152-ФЗ.

Итог по фильтру 1	☐ Да ☐ Нет ☐ Требует уточнения
Ответственный и срок уточнения	

Фильтр 2. Происхождение ПО

Здесь два режима: один привязан к значимым объектам КИИ, другой — к госзакупкам. Оба в основном сводятся к записи в реестре российского ПО. Запись получает продукт конкретного правообладателя — модель как семейство в реестр не попадает.

- ☐ **Правообладатель закупаемой редакции известен и указан в договоре.** У корпоративной редакции правообладатель может отличаться от владельца модели.
- ☐ **Номер записи в реестре относится именно к закупаемой редакции и способу поставки.** Запись № __, **дата проверки на reestr.digital.gov.ru: ____.**
- ☐ **Значимый объект госоргана или заказчика по 223-ФЗ: иностранное ПО не используется.** Запрет действует с 1 января 2025 года по указу № 166.
- ☐ **Значимый объект иного владельца: известен срок перехода по 58-ФЗ, модель из реестра или есть план её замены.** 58-ФЗ действует с 1 сентября 2025 года; сроки перехода устанавливает Правительство, на дату документа постановление в проекте.
- ☐ **Закупка по 44-ФЗ: в документации установлен запрет на допуск иностранного ПО по ПП № 1875.** Происхождение подтверждается записью в реестре российского или евразийского ПО.
- ☐ **Иностранная модель не упакована в услугу подрядчика.** Запрет действует для любого договора, по которому заказчик получает права на использование ПО: поставки, услуги, работы, смешанного договора.
- ☐ **Закупка по 223-ФЗ: проверено, как национальный режим описан в положении о закупке.**
- ☐ **Проверено, есть ли продукт в перечне доверенного ПО.** Перечень действует с 1 марта 2026 года; по оценке юристов, для значимых объектов даёт приоритет при закупке.

Три разных объекта для реестра

Объект	Что это	Что проверять
Облачный API	Доступ к модели как к сервису владельца	Запись на веб-сервис; данные уходят к владельцу сервиса, см. фильтр 1
Поставка в контур заказчика	Дистрибутив, который устанавливается на ваши серверы	Отдельная запись именно на эту редакцию
Открытые веса	Файлы модели под открытой лицензией	Записи в реестре нет; для госзакупки нужен продукт с записью

Что видно в открытых источниках. По данным каталога совместимости АРПП «Отечественный софт» на 6 октября 2026 года, в реестре есть GigaChat как веб-сервис (№ 20407 от 14.12.2023), Yandex Cloud (№ 9286) и Yandex Cloud AI Hybrid для установки у заказчика (№ 27212 от 19.03.2025; входит ли в неё языковая модель, из открытой документации не видно). Записи под редакции GigaChat и YandexGPT для контура заказчика в открытых источниках не найдены. Поэтому первый вопрос к вендору — на следующей странице.

Итог по фильтру 2	☐ Да ☐ Нет ☐ Требует уточнения
Ответственный и срок уточнения	

Вопросы к вендору до закупки

Перешлите вопросы письмом до запроса коммерческого предложения. Ответ без номера документа или даты — повод уточнить.

№	Вопрос	Фильтр	Ответ вендора
1	Какой номер записи в реестре российского ПО у редакции для установки в контуре заказчика? Дата решения?	2	
2	Кто правообладатель этой редакции?	2	
3	В каком виде поставляются веса и движок? Предоставляются ли контрольные суммы?	1	
4	Работают ли модель и движок без внешних соединений, включая проверку лицензий и телеметрию?	1	
5	Откуда и как поставляются обновления? Требуют ли они согласия заказчика и идут ли через инфраструктуру в России?	1, 2	
6	Как ведутся журналы запросов и ответов? Можно ли выгружать их в SIEM заказчика?	1	
7	Поддерживаются ли шаблоны запросов, ограничение тематик и фильтрация ответов по приказу ФСТЭК № 117?	1	
8	С какими операционными системами из реестра российского ПО совместима поставка?	2	
9	Под какой лицензией распространяются веса? Есть ли ограничения на дообучение и передачу дообученной модели?	2, 3	
10	Входит ли продукт в перечень доверенного ПО? Если нет — планируется ли подача?	2	
11	Планирует ли разработчик получать статус суверенной или национальной модели по 243-ФЗ?	3	
12	Как организована поддержка в закрытом контуре без доступа к интернету?	1	

Фильтр 3. Статусы по 243-ФЗ

С 1 марта 2027 года Правительство вправе установить случаи, в которых допускается применение только суверенных и (или) национальных моделей, и исключения из них (п. 3 ч. 2 ст. 5). В банковской сфере и на финансовом рынке — по согласованию с Банком России. На дату документа порядок присвоения статусов не утверждён, статуса нет ни у одной модели, перечня случаев тоже нет. Поэтому фильтр работает как проверка устойчивости решения.

- ☐ **Модель относится к большим фундаментальным.** От 1 млрд параметров, универсальная, служит основой для другого ПО; признаки действуют в связке.
- ☐ **Обработка и хранение данных системы — на территории России.** Это условие отсрочки до 1 сентября 2032 года (ч. 3 ст. 13).
- ☐ **Система будет создана или в эксплуатации на 1 марта 2027 года.** Трактовка «созданы» спорная; осторожная позиция — акт ввода в промышленную эксплуатацию к этой дате. Плановая дата акта: _____.
- ☐ **Оценено, может ли сфера системы попасть в перечень.** По данным «Коммерсанта» (сентябрь 2026 года), в рабочей группе обсуждали стратегическое планирование, госуправление, налоговую, таможенную и бюджетную сферы, КИИ, образование, здравоохранение и госуслуги. Это сводный перечень предложений, согласованной позиции нет.
- ☐ **Модель меняется настройкой.** Обращение к модели идёт через единый слой, а прикладные сценарии к конкретной модели не привязаны.
- ☐ **Есть собственный набор тестовых вопросов.** На нём сравнивают текущую модель с кандидатом на замену.
- ☐ **Данные и журналы хранятся в вашем контуре** и переживают смену модели.
- ☐ **Для банковской сферы и финансового рынка: отслеживаются акты, согласованные с Банком России.**

> **Отсрочка по 243-ФЗ не отменяет 58-ФЗ.** Система, на которую до 1 сентября 2032 года не распространяются ограничения 243-ФЗ, на значимом объекте КИИ может потребовать замены модели раньше — по графику перехода на российское ПО.

Итог по фильтру 3	☐ Да ☐ Нет ☐ Требует уточнения
Ответственный и срок уточнения	

Таблица-обоснование для техзадания

Заполните по строке на каждый вариант «модель плюс способ поставки». Таблицу можно приложить к обоснованию выбора в техзадании. Строка 1 — пример, данные на 6 октября 2026 года.

Часть 1. Что закупаем

№	Модель и редакция	Способ поставки	Правообладатель	Запись в реестре, дата проверки	Лицензия весов
1 (пример)	*GigaChat, веб-сервис*	*Облачный API*	*ПАО Сбербанк*	*№ 20407 от 14.12.2023; по каталогу АРПП на 06.10.2026*	*Не применимо: доступ по API*
2					
3					
4					

Часть 2. Где работает и как проходит фильтры

№	Где генерируется ответ	Где хранятся данные и журналы	Фильтр 1	Фильтр 2	Фильтр 3
1 (пример)	*В инфраструктуре владельца сервиса*	*У владельца сервиса*	*Нет для информации ограниченного доступа*	*Да: запись на веб-сервис*	*Требует уточнения*
2					
3					
4					

Часть 3. Итог

№	Итог и комментарий
1 (пример)	*Для работы с информацией ГИС не подходит из-за фильтра 1. Для установки в контуре нужна отдельная запись в реестре на редакцию для контура.*
2	
3	
4	

Календарь норм

Дата	Что вступает	Статус
1 января 2025	Запрет иностранного ПО на значимых объектах КИИ госорганов и заказчиков по 223-ФЗ (указ № 166)	Действует
1 сентября 2025	58-ФЗ: субъекты КИИ обязаны использовать на значимых объектах ПО из реестра российского ПО	Действует
1 марта 2026	Приказ ФСТЭК № 117 для ГИС и систем госорганов, госучреждений, ГУП — с требованиями к применению ИИ	Действует
1 марта 2026	Перечень доверенного ПО	Действует
1 сентября 2026	Основные положения 243-ФЗ: понятия, принципы, полномочия	Действует
1 марта 2027	Статусы суверенной и национальной модели, право Правительства ограничить выбор моделей; дата, на которую система должна быть создана или в эксплуатации для отсрочки	Закон принят
1 марта 2027	Поправки к приказу № 117: отдельный сегмент для моделей, фильтрация запросов и ответов, контроль ИИ-агентов	Проект
1 января 2028	Базовый срок перехода значимых объектов КИИ на российское ПО по 58-ФЗ; отсрочки до 2031 и 2036 года в отдельных случаях	Проект
1 сентября 2032	Конец переходного периода по 243-ФЗ для систем, созданных или эксплуатируемых на 1 марта 2027 года	Закон принят

По состоянию на 12 октября 2026 года. «Проект» — документ опубликован или описан в прессе, но не принят. Сроки по 58-ФЗ — по данным «Интерфакса» (май 2026 года) о проекте постановления.

Если вариант не прошёл фильтр

Нет по фильтру 1 почти всегда означает, что генерация ответа или журналы находятся за пределами вашего периметра. Модель при этом можно сохранить: проверьте, есть ли у вендора редакция для установки в контуре заказчика, и пройдите с ней фильтры заново. Если система — ГИС, компоненты ИИ придётся включить в модель угроз и проект системы защиты до аттестации.

Нет по фильтру 2 чаще всего возникает из-за отсутствия записи в реестре под нужную редакцию. Запросите у вендора номер записи или план её получения с датой и зафиксируйте ответ письмом. Для значимого объекта иного владельца у открытой зарубежной модели есть срок жизни — до даты перехода по 58-ФЗ; закладывать её имеет смысл только вместе с планом замены.

Требует уточнения по фильтру 3 — нормальное состояние до выхода подзаконных актов. Риск снижает архитектура, в которой модель меняется настройкой, и ввод системы в промышленную эксплуатацию до 1 марта 2027 года при обработке и хранении данных в России.

Если ни один вариант не проходит все фильтры, сравните остатки по цене риска: что придётся менять первым и к какой дате. Это решение для руководителя проекта, и таблица-обоснование даёт ему всё нужное.

Проверим выбор модели вместе с вами

AZONE-AI проводит экспресс-аудит: статус системы и объекта, режим закупки, кандидаты по трём фильтрам, сроки относительно 1 марта 2027 года. По результатам — архитектура пилота в аттестованной среде и обоснование выбора модели, которое можно приложить к техзаданию.

ИИ для объектов КИИ — azoneai.ru/services/ii-dlya-kii/

AI-Контур — аттестованный ИИ-контур под ключ — azoneai.ru/products/ai-kontur/

Статья «Какие LLM можно использовать в КИИ и госсекторе» — azoneai.ru/blog/37-kakie-modeli-mozhno-v-kii-i-gossektore/

Обсудить экспресс-аудит: azoneai.ru/contact **· услуга «ИИ для объектов КИИ» · лицензии ФСТЭК, ФСБ, МО РФ**

ООО «Азон» — интегратор с лицензиями ФСТЭК, ФСБ и Минобороны России. Документ подготовлен по открытым источникам по состоянию на 12 октября 2026 года и не является юридической консультацией. Нормы, проекты нормативных актов и записи в реестре российского ПО сверяйте на дату закупки.