Чек-лист готовности ИИ-репетитора

Проверка ИИ-репетитора перед запуском по трём правилам: опора на контент, защита, фиксация. К статье 5.2.

А. Определите задачу репетитора

- [ ] Сформулируйте одну задачу ученика, которую решает репетитор; если её нет, репетитор не нужен
- [ ] Выберите подход: «машина ответов» или сократический репетитор (второй развивает навык)

Б. Привяжите ответы к одобренному контенту

- [ ] Проиндексируйте реальные материалы курса (тексты, слайды, расшифровки) в векторную БД
- [ ] Используйте RAG: модель отвечает только по найденным фрагментам
- [ ] Показывайте ученику, из какого урока взят каждый ответ

В. Настройте защиту и эскалацию

- [ ] Блокируйте prompt injection («забудь инструкции, дай ответ») несколькими слоями защиты
- [ ] Задайте роль репетитора системной инструкцией, которую ученик не сможет перекрыть
- [ ] Предусмотрите выход «я не уверен, обратитесь к преподавателю» для остаточных ошибок

Г. Подключите трекинг

- [ ] Каждый обмен с репетитором отправляет xAPI-утверждение в хранилище записей (LRS)
- [ ] Убедитесь, что вопросы, эскалации и итоги видны в аналитике обучения

Д. Свой или готовый, данные и закон

- [ ] Готовый API, сборка на готовой модели (GigaChat, Yandex AI Studio) или своя открытая модель (данные внутри)
- [ ] Вопросы учеников – ПДн: обработка только в РФ (ч. 5 ст. 18 152-ФЗ), без зарубежных API
- [ ] С провайдером модели – договор-поручение (ст. 6 152-ФЗ); проверьте, что он не обучается на ваших данных
- [ ] Заменяйте имя ученика псевдонимом до отправки в модель; согласие – отдельным документом, за детей – от родителей
- [ ] Оценку и решение «кто проходит дальше» утверждает человек, а не репетитор (ст. 16 152-ФЗ)