Чек-лист: проверка безопасности видеоконвейера

Пройдите каждый слой до того, как продукт увидит первый пациент. Рядом с каждой мерой – опорная норма: 152-ФЗ, приказ ФСТЭК № 21 (группы мер), приказ ФСБ № 378. Инженерные рекомендации, не юридическая консультация.

А. Шифруйте каждый переход

- [ ] Живой звонок: всё медиа WebRTC идёт через DTLS-SRTP, открытого пути нет (ЗИС)
- [ ] Сигналинг: только wss://; пользователь аутентифицирован до выдачи токена звонка (ИАФ, ЗИС)
- [ ] Релей: учётки TURN короткоживущие, на сессию, каждый запрос журналируется (ИАФ, УПД)
- [ ] Между сервисами: каждый внутренний переход с медданными на TLS 1.3; mTLS для чувствительных связей (ИАФ.2)
- [ ] Где модель угроз закрывает угрозу криптографией – СКЗИ ФСБ нужного класса (ГОСТ-TLS, ГОСТ-VPN); иначе – обоснование

Б. Охраняйте границу медданных

- [ ] SFU, хранилище записей, транскрипция, облако – ваши или по поручению оператора, всё в России
- [ ] Сеть сегментирована: медиаплоскость, управление, данные и корпоративный ИТ – в разных зонах
- [ ] Записи, транскрипты, бэкапы зашифрованы при хранении; ключи хранятся отдельно
- [ ] Записи отдаются только через короткие signed URL; публичных бакетов и вечных ссылок нет
- [ ] Ключи и учётки – в vault или сервисе управления ключами, не в коде и логах; ротация по расписанию

В. Подрядчики и доказательства

- [ ] Ни один SDK аналитики, отчётов о сбоях или ИИ не отправляет медданные без поручения или за рубеж
- [ ] Журналы отвечают, кто, когда и откуда открывал каждую запись (ст. 19 ч. 2 п. 8 152-ФЗ; РСБ)
- [ ] План на случай утечки: Роскомнадзор за 24 и 72 часа; срок уведомления клиники-оператора – в поручении

Г. Один тест перед запуском

- [ ] Мысленный тест: если бакет записей станет публичным, что увидит посторонний – шифртекст или видео пациентов?
- [ ] Спросите: «где лежит ключ?» Если в том же бакете или конфиге – утечка будет полной