

MoQ Readiness Checklist

Перед запуском MoQ-пилота — архитектурные, вендорские и операционные вопросы.

1. Соответствие продукту

- ☐ Откроет ли пол задержки в 500 мс конкретную фичу продукта (live-ставки, момент покупки в live-commerce, second-screen-синхрон, интерактивный игровой стрим)? Если нет — MoQ сейчас не нужен.
- ☐ Одновременные зрители — в диапазоне тысяч-миллионов (где WebRTC SFU дорогой, а задержка LL-HLS блокирует фичу)?
- ☐ Аудитория достижима через ваше приложение или embed, куда можно положить vendor MoQ-плеер?
- ☐ Направление вещания — one-to-many или few-to-many (не двусторонний peer-to-peer как в видеозвонке)?
- ☐ Альтернативы LL-HLS, LL-DASH / CMAF и WebRTC delivery исключены с задокументированными причинами?

2. Архитектурные решения

- ☐ Encoder-вендор: подтверждён MoQ-origin 2026 года (Bitmovin, Norsk, Wowza, Ant Media, Broadpeak, Synamedia, Red5, nanocosmos).
- ☐ Relay-уровень: выбрано между Cloudflare MoQ CDN (330+ городов, быстрый пилот) и self-hosted moq-rs (контроль, ops-нагрузка).
- ☐ Зафиксирована конкретная редакция draft-a (draft-ietf-moq-transport-17 или -latest); никаких "follow the head" в production.
- ☐ Streaming format: выбран CMSF (CMAF поверх MoQ) для catalog/timeline; альтернатива LOCMF рассмотрена и зафиксирована.
- ☐ Player: vendor SDK идентифицирован; fallback (LL-HLS или WebRTC) определён для неподдерживаемых устройств (Apple Safari, smart TV, старые Android).
- ☐ Гранулярность GOP/object: один CMAF-чанк на объект, НЕ один сегмент на объект — не повторите "HLS-овский размер объекта".

3. Операционная готовность

- ☐ UDP-путь протестирован в целевых регионах; WebTransport fallback протестирован для корпоративных и мобильных сетей с блокировкой UDP.
- ☐ Модель capacity: память relay $\approx$ 200 байт на активную подписку (проверьте с вашей реализацией); egress смоделирован на edge.
- ☐ Поведение под congestion: subgroup-priority и partial-reliability проверены под потерями (тест 1%, 3%, 5%).
- ☐ Observability: per-track QoE-метрики (startup, latency join, stall rate) собираются на плеере и на relay.
- ☐ DRM и шифрование: подтверждено шифрование QUIC-канала; end-to-end secure objects (draft-ietf-moq-secure-objects) нужны при недоверенном relay.
- ☐ DoS posture: rate-limit на source IP в relay; подписанные ANNOUNCE; согласовано с draft-englishm-moq-relay-dos.

4. Риски вендора и спеки

- ☐ Сроки Working Group Last Call отслежены (RFC через 6–12 мес после WGLC); план апгрейда документирован.
- ☐ SLA вендора согласован под изменения редакции draft-a; пункт о breakage спеки согласован.
- ☐ Bridge на LL-HLS / WebRTC прогрет: если MoQ-пилот падает, можно ли переключить аудиторию на fallback-стек за 24 ч?
- ☐ Авто-обновление плеера: force-refresh / soft-update инфраструктура для изменений catalog и формата сообщений между draft-ами.
- ☐ Внутренняя команда: хотя бы один инженер свободно говорит на QUIC, WebTransport, модели данных MoQ; способен читать IETF draft напрямую.

Правило принятия решения

Если отмечено всё — переходите к MoQ-пилоту на 6–8 недель против определённой фицы продукта. Если в разделах 1–2 не отмечено три и больше пунктов — оставайтесь на текущем протоколе и пересмотрите после следующей редакции moq-transport или после Working Group Last Call. Если неотмеченные пункты сосредоточены в разделах 3–4 — пилотируйте на Cloudflare MoQ CDN, чтобы ограничить операционные и спес-риски первой итерации.