

Чек-лист готовности контроля доступа — справочник на одну страницу

Fora Soft Learn

Paywall — это экран; контроль доступа — система, которая решает и исполняет каждый запуск. Осознанно выберите форму paywall, затем исполняйте в четырёх серверных слоях. Инженерное руководство; лимиты вендоров и судебная практика в 2026 меняются — сверяйте вживую.

1 • ВЫБЕРИТЕ ФОРМУ PAYWALL (ОСОЗНАННО)

- ☐ **Hard** — платишь — смотришь всё; макс. доход с юзера, тяжелейшее первое впечатление. Премиум-каталоги.
- ☐ **Metered / soft** — бесплатная квота (напр. 3/мес), затем оплата; даёт привычку, охват и SEO.
- ☐ **Freemium** — постоянный бесплатный уровень как маркетинг платного; идёт в паре с регистрационной стеной.
- ☐ **Регистрационная стена** — email/аккаунт — это цена; сбор first-party данных (помните о VPPA, кол. 4).

2 • ИСПОЛНЯЙТЕ В ЧЕТЫРЁХ СЕРВЕРНЫХ СЛОЯХ

- ☐ **Проверка entitlement** — на каждом запуске: можно ли аккаунту смотреть этот тайтл, в этом регионе, сейчас?
- ☐ **Подписанный токен (JWT)** — доказывает решение; несёт claims user/asset/region + короткий expiry.
- ☐ **Подписанный URL** — CDN отдаёт байты только при валидной подписи; жизнь сегмента 60-300 с.
- ☐ **Лицензия DRM** — шифрует контент; единственный слой, защищающий расшифрованное видео.

ПОРЯДОК СБОРКИ — ТОЛЬКО СЕРВЕР РЕШАЕТ, ЧТО ОТДАВАТЬ

Никогда не исполняйте гейт на клиенте: проверка в приложении — это одна строка, правимая в консоли, а видеофайлы лежат на CDN за URL, которые любой скачает, если они без подписи. Клиент может прятать кнопку Play ради удобства, но проверка entitlement, подписанный токен (JWT, RFC 7519), подписанный URL доставки и лицензия DRM должны исполняться на сервере и на edge, вне досягаемости пользователя. Держите токены короткими (60-300 с для URL сегментов), чтобы утёкший URL умер раньше, чем им поделятся. Тест: представьте, что у самого враждебного юзера есть ваши сырые URL сегментов, пропатченное приложение и VPN — если выручка держится, гейт настоящий. Сверяйте лимиты concurrency по сервисам и практику VPPA перед запуском; в 2026 и то и другое меняется.

3 • ГЕО-ГЕЙТИНГ + CONCURRENCY

- ☐ **Гео-гейт** — определите страну по IP; исполняйте территориальную лицензию тайтла на edge.
- ☐ **EU portability** ((EU) 2017/1128) — дайте платящему подписчику смотреть домашний контент в поездке по ЕС.
- ☐ **Устройство ≠ резидентство** — portability считается от домашнего рынка, не от текущего места.
- ☐ **Concurrency** — heartbeat каждые 30-60 с; отклоняйте запуски сверх лимита; освобождайте слоты упавших.

4 • ЧЕК-ЛИСТ VPPA / СОГЛАСИЯ (рег. стены)

- ☐ **Отдельное согласие** — явное, информированное согласие на ПЕРЕДАЧУ данных просмотра; баннер cookie не годится.
- ☐ **Без утечек через пиксели** — держите события просмотра вне рекламных пикселей (Meta/Google) вне вашего контроля.
- ☐ **Аудируемая запись** — храните согласие как запрашиваемые данные; от \$2 500 ущерба за нарушение.
- ☐ **Следите за практикой** — Salazar v. Paramount в Верховном суде США (2026); сверяйте перед запуском.