

Защита контента — рабочий лист решения

Fora Soft Learn

Решите, сколько защиты реально нужно каталогу, до подписания контентной сделки или контракта на DRM. Подбирайте слой под угрозу — DRM сердце стека, но не весь стек. Инженерное руководство; числа вендоров сверяйте вживую, они меняются.

1 · НАЗОВИТЕ УГРОЗУ (от чего вы на самом деле защищаетесь?)

- ☐ **Запишите, во что обходится одна утечка.** «Конкурент бесплатно получит наш оригинал за \$20M» — это территория DRM; «кто-то посмотрел вебинар без регистрации» — нет.
- ☐ **Классифицируйте контент:** публичный / малоценный · приватный, но не премиум · премиум или лицензированный · 4K или раннее окно.
- ☐ **Проверьте лицензию.** Если вы лицензируете студийный контент, защиту задаёт контракт — выбирать не вам.

2 · ПОДБЕРИТЕ СЛОЙ ПОД УГРОЗУ (каждый ловит своего атакующего)

- ☐ **Контроль доступа (token auth / signed URL)** — решает, кто вообще может запросить манифест и сегменты.
- ☐ **Шифрование транспорта (AES-128, HLS)** — шифрует байты; надёжно ровно настолько, насколько защищён запрос ключа.
- ☐ **DRM (Widevine / PlayReady / FairPlay)** — защищает КЛЮЧ и РАСШИФРОВАННЫЕ БАЙТЫ в доверенном модуле.
- ☐ **Защита вывода (HDCP 2.2+) + forensic watermarking** — стерегут кабель; отслеживают утечку, которую DRM не предотвратит.

ОДНА ПРОВЕРКА ПЕРЕД ПОДПИСАНИЕМ

Всё решают два вопроса. (1) Что требует лицензия? Если вы лицензируете контент, ответ записан и выбирать не вам — премиум 4K обычно обязывает к hardware DRM + HDCP 2.2 + forensic watermarking. (2) Во что реально обходится одна утечка? DRM дешёв относительно того, что он открывает: при типичных \$0,30 за 1 000 запросов лицензий 100 000 подписчиков × 50 сессий/мес = 5 000 000 запросов ≈ \$1 500/мес — около 0,125% от каталога на \$1,2M/мес, который без DRM просто не лицензируется. Реальная стоимость — интеграция multi-DRM и работа плеера под устройства, а не плата за лицензию. Помните, чего DRM не может: он защищает ключ и расшифрованные байты, но не камеру у экрана — для этого есть watermarking.

3 · ПРИМИТЕ РЕШЕНИЕ ПО DRM (не пере- и не недозащищайте)

- ☐ **Публичный / малоценный?** Хватит контроля доступа — без DRM. Ваше решение: _____
- ☐ **Приватный, но не премиум?** Token auth + AES-128 с ЗАЩИЩЁННЫМ key server часто достаточно.
- ☐ **Премиум или лицензированный?** Multi-DRM: шифруем один раз через cbcs, лицензии Widevine + PlayReady + FairPlay.
- ☐ **4K или раннее окно?** Hardware DRM (Widevine L1 / SL3000) + HDCP 2.2 + forensic watermarking.

4 · ИЗБЕГАЙТЕ ЧЕТЫРЁХ КЛАССИЧЕСКИХ ОШИБОК

- ☐ **Шифрование только cbcs** молча ломает Apple — FairPlay нужен cbcs. Стандартизируйтесь на cbcs с первого дня.
- ☐ **«DRM останавливает запись экрана»** — нет. Analog hole закрывает watermarking, а не «лучший» DRM.
- ☐ **Открытый key server AES-128** — ключ лежит в манифесте; без token auth шифрование как москитная сетка.
- ☐ **Перезащита малоценного** при недозащите единственного тайтла с контрактными обязательствами.