Чек-лист WebRTC Security Pre-Flight

28 пунктов перед релизом WebRTC-продукта — DTLS, SRTP, fingerprints, сигнал, SFrame

1. Сигнальный канал

- [ ] Сигнальный эндпоинт — wss:// (или HTTPS), никогда не plain ws:// или http://.
- [ ] TLS-сертификат сигнального сервера проходит public-CA цепочку — без self-signed в проде.
- [ ] WebSocket origin ограничен серверно доменом приложения — блокируем cross-origin-клиентов.
- [ ] Аутентификация на коннект: короткоживущий bearer-токен (JWT или эквивалент), проверка на сервере до релея SDP.

2. DTLS-хендшейк

- [ ] Браузер поддерживает DTLS 1.3 (RFC 9147) — проверяем в chrome://webrtc-internals или about:webrtc.
- [ ] DTLS 1.0 / 1.1 выключены на SFU; принимаем только 1.2 и 1.3.
- [ ] Список cipher suite исключает слабые AES-CBC; только AEAD.
- [ ] Срок жизни self-signed-сертификата равен жизни PeerConnection — генерируется каждый раз заново.

3. Профиль SRTP

- [ ] AEAD-AES-128-GCM согласован как предпочтительный SRTP-профиль (RFC 7714).
- [ ] Legacy AES-CM-HMAC-SHA1-80 — только fallback; логи помечают такие случаи.
- [ ] Replay window — дефолт (64 пакета) или больше; не отключён.
- [ ] Теги аутентификации на каждом медиа-пакете — проверяем выборкой в Wireshark.

4. SDP fingerprint

- [ ] a=fingerprint:sha-256 присутствует в каждом offer и каждом answer.
- [ ] SHA-1 fingerprint отвергается приложением — логируем и роняем согласование.
- [ ] Несовпадение fingerprint — разрыв соединения, ошибка пользователю.

5. ICE и приватность

- [ ] mDNS host-кандидаты используются клиентом (дефолт в Chromium / Edge / Opera).
- [ ] TURN-сервер требует короткоживущих эфемерных credentials (REST-over-HTTPS, < 1 часа).
- [ ] Доля TURN-relay измеряется в продакшен-телеметрии — норма 10-15%; всплески алертятся.
- [ ] Экспозиция публичного IP задокументирована и раскрыта в privacy policy.

6. Identity и авторизация

- [ ] SFU контролирует доступ к комнате токеном — токены publisher и subscriber проверены до медиа.
- [ ] Право публиковать или подписываться на трек решает сервер, а не клиент.
- [ ] Срок жизни токена короткий, чтобы ограничить replay (15-60 минут типично).
- [ ] Политика ротации задокументирована для API-ключей SFU и подписи JWT.

7. E2EE (если заявляем)

- [ ] SFrame (RFC 9605) поверх Insertable Streams, если продукт заявляет E2EE через SFU.
- [ ] Управление групповыми ключами задокументировано — MLS, кастомное или от вендора.
- [ ] Ротация ключей при join/leave протестирована хотя бы одним сценарием хаос-теста.
- [ ] Границы браузерной поддержки задокументированы (пробелы Insertable Streams в Safari/FF 2026).

8. Observability

- [ ] Ошибки DTLS-хендшейка алертятся с reason code (cert mismatch, версия, cipher suite).
- [ ] События SDP-fingerprint-mismatch идут в security-лог и в дашборд.
- [ ] RTT и доля TURN-relay по сессии хранятся минимум 30 дней для форензики.