Рабочий лист: модель угроз телемед-платформы

Пройдите цикл для каждого потока данных. STRIDE даёт содержание, методика ФСТЭК 2021 года – структуру документа. Инженерные рекомендации, не юридическая консультация.

А. Цикл из четырёх шагов

- [ ] Опишите систему: диаграмма потоков данных, граница медданных (ваши хосты в РФ + обработчики по поручению)
- [ ] Найдите угрозы: шесть подсказок STRIDE к каждому элементу и каждому пересечению границы; LINDDUN – для психиатрии и других чувствительных сервисов
- [ ] Ранжируйте: вероятность × ущерб по шкале 1–5, балл 1–25; правый верхний угол – работа на этот квартал
- [ ] Снизьте и проверьте: снизить, передать, принять или избежать – затем протестируйте меру

Б. STRIDE – к каждому элементу

- [ ] S – выдать себя за другого: фишинг логина врача открывает карты
- [ ] T – подмена: результат анализа или дозировка изменены по пути в МИС
- [ ] R – отрицание: нет журнала, кто открывал запись (ст. 19 ч. 2 п. 8 152-ФЗ)
- [ ] I – раскрытие: публичный бакет; SDK аналитики шлёт медданные без поручения или за рубеж
- [ ] D – отказ в обслуживании: флуд выводит платформу из строя во время приёмов
- [ ] E – повышение прав: аккаунт пациента получает доступ к админ-эндпоинту

В. Поверхность атаки – шесть зон

- [ ] Устройства пациента и врача; живой звонок (сигналинг, TURN, SFU видит открытое видео)
- [ ] Сигналинг и API; записи и хранилище – самая ценная цель (записи консультаций хранятся год)
- [ ] Интеграции с МИС, ЕГИСЗ, лабораториями, оплатой; сторонний код – зашифрованное ≠ законное

Г. От модели – к документам

- [ ] Тип актуальных угроз (1, 2 или 3) определён и обоснован (п. 6–7 ПП 1119)
- [ ] Уровень защищённости посчитан: медданные, угрозы 3-го типа – УЗ-3 до 100 000 пациентов, УЗ-2 свыше
- [ ] Базовый набор мер приказа ФСТЭК № 21 адаптирован, уточнён под актуальные угрозы и дополнен (п. 9)
- [ ] Где угрозы закрыты шифрованием – СКЗИ ФСБ нужного класса (приказ № 378); иначе – обоснование
- [ ] Перечень сверен с БДУ ФСТЭК; модель пересматривается при каждом изменении системы