Ранбук реагирования на утечку – шаблон

Заполните до запуска, а не во время инцидента. Сроки 152-ФЗ считаются с момента выявления, включая ночи и выходные. Инженерные рекомендации, а не юридическая консультация – детали подтверждайте у юриста.

А. Подготовка (до инцидента)

- [ ] Названы дежурный, замена и порядок эскалации к ответственному за защиту ПДн.
- [ ] ЕСИА и электронная подпись для портала Роскомнадзора – у двух человек, доступ проверен.
- [ ] Известно, есть ли соглашение с НКЦКИ и является ли система объектом КИИ.
- [ ] В каждом поручении срок уведомления оператора – в часах, состав сведений перечислен.
- [ ] Алерты, ящик поддержки и адрес для сообщений об уязвимостях читаются круглосуточно.
- [ ] Шаблоны уведомлений РКН (24 и 72 часа) и сообщения пациентам подготовлены заранее.

Б. Первый час (любой инцидент)

- [ ] Запишите момент выявления: кто, когда, откуда (алерт, письмо, жалоба).
- [ ] Сдержите: изолируйте системы, отзовите ключи и токены, закройте путь доступа.
- [ ] До изменений сохраните журналы доступа, хранилища и ключевой системы.
- [ ] Значимый объект КИИ? НКЦКИ – не позднее 3 часов с обнаружения (приказ ФСБ № 547).
- [ ] Вы подрядчик? Уведомите оператора в срок из поручения – у него уже идут 24 часа.

В. Первые 24 часа (если затронуты ПДн)

- [ ] Четыре вопроса: какие данные и сколько; кто получил; был ли доступ; что сделано.
- [ ] Роскомнадзор: факт, причины, вред, меры, контактное лицо (ст. 21 ч. 3.1 152-ФЗ).
- [ ] ГосСОПКА – в НКЦКИ при соглашении или через РКН; запросы НКЦКИ – за 24 часа.
- [ ] «Не уведомлять» решает оператор с юристом; факты и основания – в журнал.

Г. До 72 часов и после

- [ ] Роскомнадзор: итоги внутреннего расследования и сведения о виновных, если установлены.
- [ ] Пациентам – по решению оператора с юристом, по готовому шаблону на простом языке.
- [ ] Разбор: модель угроз, ранбук, сроки в договорах; учение по восстановлению из копии.
- [ ] Неуведомление РКН – 1–3 млн ₽ (ч. 11 ст. 13.11 КоАП); утечка данных о здоровье – 10–15 млн ₽.