

Чек-лист проверок медицинских компаний на соответствие 152/323-ФЗ

Соблюдение требований Федерального закона №152-ФЗ «О персональных данных», №323-ФЗ «Об основах охраны здоровья граждан» и смежного законодательства является критически важным для медицинских организаций. Несоблюдение установленных норм влечет административную ответственность с штрафными санкциями до 18 млн рублей, а в отдельных случаях (например, при нарушении порядка обработки медицинской информации несовершеннолетних) — уголовную ответственность.

Данный чек-лист представляет собой комплексный инструмент оценки соответствия медицинского учреждения действующим требованиям в области защиты персональных данных и позволяет выявить потенциальные риски нарушения законодательства.

Коммуникации и мессенджеры

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
WhatsApp/Telegram не используются даже с согласия пациентов		Штраф до 500 000 Р + блокировка аккаунта	Перевести пациентов на VK Мессенджер или СБЕР Чаты
Чат Авито - только для общих вопросов, сбор ПДн через перенаправление		Штраф до 6 млн Р за локализацию	Внедрить автоответ: "Для записи перейдите на [ссылка]"
Виджеты JivoSite/LiveChat заменены на российские аналоги		Трансграничная передача → штраф до 18 млн Р	Внедрить VK Консультант или Roistat с DPA

Обработка ПДн и согласия

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Согласие оформляется через ЭЦП-формы с явным указанием ИНН клиники		Недействительность согласия → штраф 500 000 Р	Добавить: "Оператор: ООО «Клиника», ИНН 1234567890" над чекбоксом
Номера телефонов (даже без ФИО) не собираются через Telegram/Авито		Косвенная идентификация → штраф 300 000 Р	Удалить номера из чатов, вносить только после ЭЦП-согласия
Отдельная форма для биометрии с аккредитованным шифрованием		Штраф 20 млн Р + уголовная ответственность	Внедрить КриптоПРО + подписание через Госуслуги

Иностранные операторы и облака

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Для иностранных сервисов (AWS, Google Cloud) подписан DPA с требованиями 152-ФЗ		Незаконная передача → штраф 6-18 млн ₽	Скачать шаблон DPA: https://rkn.gov.ru/docs/dpa_foreign_template.docx
Google Forms/Google Docs полностью заменены российскими аналогами		Нелегальный сбор ПДн → штраф 15 млн ₽	Перенести на Tilda (с опцией РФ) или Р7-Офис
Резервные копии не хранятся на Google Drive/Dropbox		Нарушение локализации → штраф 6 млн ₽	Использовать VK Диск или СберОблако с геоограничением

Сайт и аналитика

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Отсутствие Google Analytics/Meta Pixel/Facebook виджетов		Блокировка сайта + штраф 1 млн ₽	Удалить скрипты через BuiltWith, внедрить Яндекс.Метрику
Cookie-баннер блокирует скрипты до согласия с кнопкой "Отклонить всё"		Штраф 500 000 ₽	Проверить через Cookiebot: https://www.cookiebot.com/ru/
Отсутствие скрытых скриптов (Google Fonts, CDN)		Передача IP за рубеж → штраф 300 000 ₽	Заменить на local-шрифты и российский CDN (cdnvideo.ru)

Хранение данных

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Все базы ПДн пациентов на серверах в РФ (проверить ИНН поставщика в реестре РКН)		Штраф 18 млн ₽ + аннулирование лицензии	Запросить акт локализации, перейти на Selectel/SberCloud при нарушениях
Медданные передаются только в зашифрованном виде (ГОСТ)		Утечка → штраф 15 млн ₽ + уголовное дело	Внедрить КристоПРО для всех вложений с медданными

Документация

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Подано уведомление в РКН о трансграничной передаче (если используются иностранные API)		Штраф 3 млн ₽	Подать через Госуслуги в течение 3 дней
Политика конфиденциальности содержит ИНН всех операторов		Штраф 300 000 ₽	Обновить по шаблону: https://rkn.gov.ru/docs/policy_template_med.docx
Регламент реагирования на утечки (уведомление РКН в течение 24 часов)		Увеличение штрафа на 50% при задержке	Скачать шаблон: https://rkn.gov.ru/docs/PD_Incident_Response_2025.docx

Спецтребования для медицины

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Данные несовершеннолетних с двойным шифрованием и ограниченным доступом		Штраф 20 млн ₽ + ст. 137 УК РФ	Настроить AES-256 + ГОСТ, доступ только лечащему врачу
Генетические данные - отдельное согласие с ЭЦП		Лишение лицензии	Внедрить подписание через Госуслуги с

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
			указанием целей исследования

Организационные меры защиты

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Издан приказ о назначении ответственного за обработку ПДн с четким описанием обязанностей		Отсутствие ответственного → штраф 500 000 Р	Назначить ответственного приказом, разработать должностную инструкцию
Весь персонал обучен требованиям 152-ФЗ с документированием (программа, журналы, тесты)		Необученный персонал → штраф 1 млн Р	Провести обучение, вести журналы, тестировать знания
Все сотрудники ознакомлены под подпись с политикой конфиденциальности и регламентами		Нарушения из-за незнания → штраф 300 000 Р	Ознакомить всех под роспись, хранить журналы ознакомления
Проводятся регулярные внутренние аудиты соблюдения требований ПДн (не реже 1 раза в год)		Накопление нарушений → штраф 3 млн Р	Утвердить график аудитов, назначить аудиторов

Технические меры защиты

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Доступ к ПДн разграничен по ролям - каждый видит только необходимые для работы данные		Избыточный доступ → штраф 1 млн Р	Настроить ролевую модель доступа в МИС
Ведется полное журналирование всех операций с ПДн (кто, когда, какие данные, какие действия)		Невозможность расследования → штраф 6 млн Р	Включить логирование всех операций с ПДн
Установлено и обновляется антивирусное ПО, ведется контроль целостности медданных		Заражение/повреждение → штраф 15 млн Р	Внедрить корпоративный антивирус с централизованным управлением

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Настроено автоматическое резервное копирование ПДн с шифрованием и контролем восстановления		Потеря данных → штраф 20 млн ₽ + иски	Настроить ежедневное резервирование с тестами восстановления
Парольная политика требует сложные пароли, смену каждые 90 дней, блокировку после неудачных попыток		Несанкционированный доступ → штраф 6 млн ₽	Внедрить Active Directory с политиками паролей
Рабочие места с ПДн защищены от несанкционированного доступа (блокировка экрана, физическая защита)		Утечка через рабочие места → штраф 1 млн ₽	Настроить автоблокировку, обеспечить физическую безопасность

Управление инцидентами и нарушениями

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Ведется журнал учета всех инцидентов с ПДн (утечки, нарушения доступа, сбои)		Неучтенные инциденты → штраф 3 млн ₽	Завести журнал инцидентов, назначить ответственного
Утвержден регламент расследования инцидентов с ПДн со сроками и ответственными		Неправильное расследование → штраф 1 млн ₽	Разработать и утвердить регламент расследований
Определен порядок уведомления РКН об утечках ПДн в течение 24 часов		Несвоевременное уведомление → штраф +50% к основному	Подготовить шаблоны уведомлений, назначить ответственного
Разработан план восстановления после инцидентов с тестированием процедур		Долгое восстановление → дополнительные ущербы	Разработать план, провести учебные тревоги
Настроена система мониторинга подозрительной активности с ПДн в режиме реального времени		Позднее обнаружение утечек → штраф 15 млн ₽	Внедрить SIEM-систему или аналог для мониторинга

Дополнительные технические требования

Что проверить (Как должно быть)	Есть ли проблема?	Риски	Рекомендации
Сетевая инфраструктура сегментирована - медданные в отдельной защищенной сети		Латеральное движение атакующих → штраф 18 млн ₽	Настроить VLAN для медицинских данных
Удаленный доступ к ПДн осуществляется только через VPN с двухфакторной аутентификацией		Компрометация удаленного доступа → штраф 6 млн ₽	Внедрить корпоративный VPN с 2FA
Все съемные носители зашифрованы или заблокированы для подключения к системам с ПДн		Утечка через USB → штраф 3 млн ₽	Настроить групповые политики блокировки USB
Принтеры и МФУ настроены для защищенной печати медицинских документов		Утечка через принтеры → штраф 1 млн ₽	Настроить аутентификацию перед печатью
Системы видеонаблюдения не фиксируют экраны с медицинской информацией		Видеозапись ПДн → штраф 500 000 ₽	Настроить зоны приватности в камерах