

ВАЖНЫЕ ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ И КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ДЛЯ МЕДИЦИНСКИХ КЛИНИК В 2026 ГОДУ



“ С 2026 года все медицинские организации в России, включая частные клиники, лаборатории, стоматологии и диагностические центры, обязаны соблюдать новые требования по защите персональных данных (ПДн) и критической информационной инфраструктуры (КИИ). Это связано с тем, что сфера здравоохранения официально признана критически важной отраслью, а любая медицинская организация, использующая информационные системы для оказания помощи, автоматически становится субъектом КИИ

Наталья Купкина,
руководитель Медиатора



КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА КЛЮЧЕВЫЕ ТРЕБОВАНИЯ И ШАГИ ДЛЯ КЛИНИК

- » Назначение ответственного за информационную безопасность и создание комиссии по категорированию объектов КИИ
- » Инвентаризация и категорирование всех цифровых систем: медицинские информационные системы (МИС), лабораторные и диагностические сервисы, телемедицина, серверы, сети и др
- » Оформление и подача перечня объектов КИИ и результатов категорирования в ФСТЭК России в установленные сроки.
- » Внедрение технических и организационных мер: использование сертифицированных средств защиты, разработка регламентов, обучение персонала, реагирование на инциденты.
- » Подготовка обязательного пакета документов: акты категорирования, модель угроз, планы защиты, инструкции, журналы учёта инцидентов и др. (всего — более 40 документов).

ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКИХ КЛИНИКАХ В 2026 ГОДУ

В 2026 году медицинские организации обязаны соблюдать строгие требования по защите персональных данных (ПДн) пациентов и сотрудников. Это связано с тем, что клиники работают с специальными категориями ПДн (сведения о здоровье), которые требуют повышенной защиты

и охраняются врачебной тайной. Нарушение этих требований грозит не только штрафами, но и репутационными потерями, а также судебными исками.

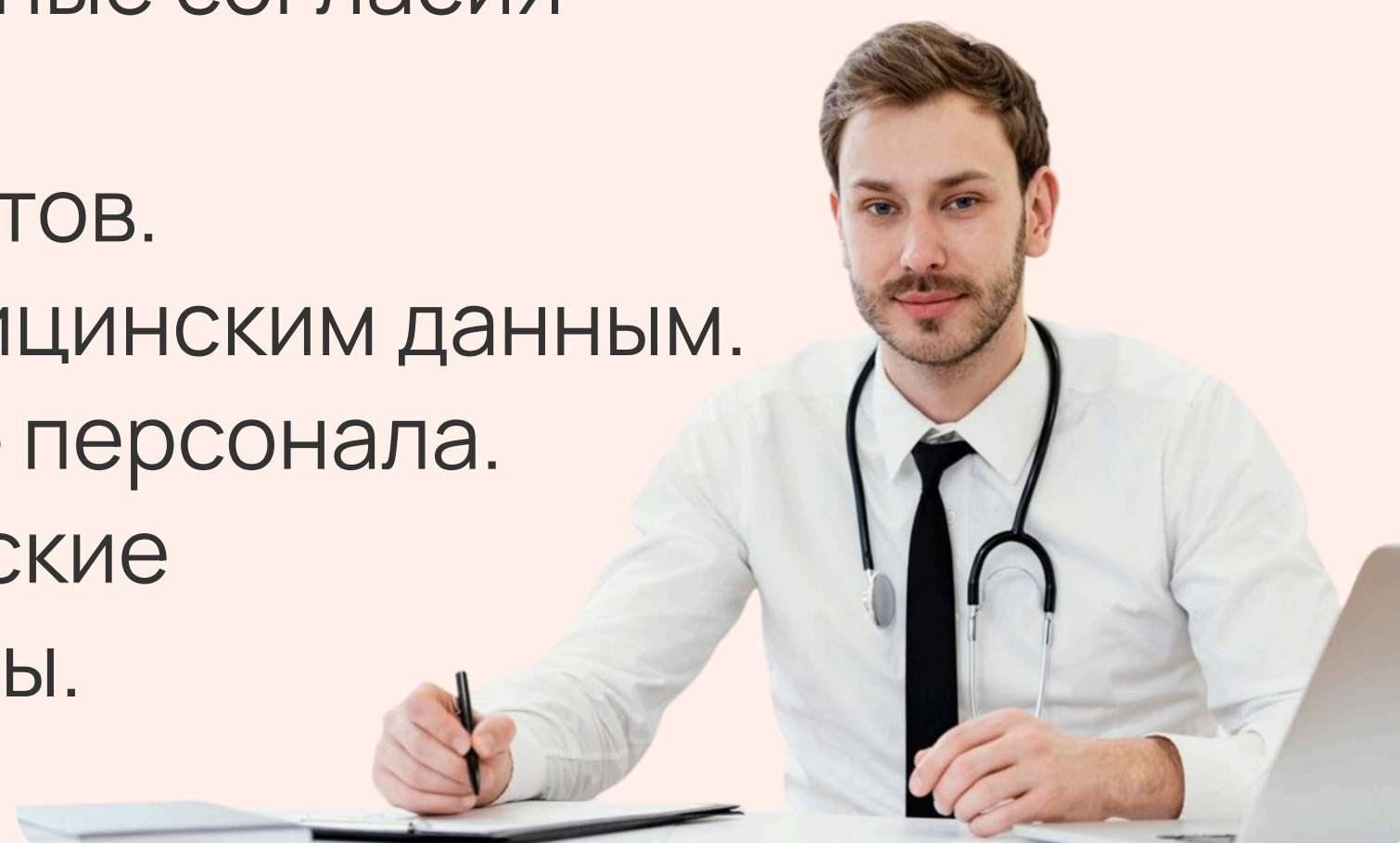
Ключевые требования ФЗ-152 и Роскомнадзора

- 01 Назначение ответственного за обработку персональных данных
- 02 Разработка локальных нормативных актов: политика обработки ПДн, положение о защите, регламенты доступа, инструкции.
- 03 Получение корректных согласий пациентов на обработку данных, включая отдельные согласия на специальные категории и передачу третьим лицам.
- 04 Техническая защита: защита медицинских информационных систем, разграничение доступов, резервное копирование, антивирусная защита.
- 05 Обучение персонала правилам работы с ПДн и медицинской тайне.
- 06 Ведение журналов учёта доступа, передачи и уничтожения данных.



ТИПОВЫЕ ОШИБКИ КЛИНИК

- Неправильные или неполные согласия пациентов.
- Отсутствие локальных актов.
- Свободный доступ к медицинским данным.
- Недостаточное обучение персонала.
- Незащищённые медицинские информационные системы.



ОТВЕТСТВЕННОСТЬ И РИСКИ

- » Административные штрафы от 500 000 до нескольких миллионов рублей
- » Приостановка деятельности клиники.
- » Уголовная ответственность (до 10 лет лишения свободы при тяжких последствиях).

✓ Заказать полный комплект обязательных документов по КИИ + подготовка писем во ФСТЭК России можно здесь:

[Узнать подробнее](#)

✓ Заказать полный комплект обязательных документов по персональным данным с изменениями 2026 года можно здесь:

[Узнать подробнее](#)

Обязательное обучение сотрудников по программе повышения квалификации с выдачей удостоверения: «Правила работы с персональными данными в организациях по требованию 152-ФЗ»:

[Узнать подробнее](#)



КИИ. СПИСОК ОБЯЗАТЕЛЬНЫХ ДОКУМЕНТОВ, КОТОРЫЕ ДОЛЖНЫ БЫТЬ В КАЖДОЙ КЛИНИКЕ НИЖЕ:

1. Сводная (инвентаризационная) таблица всех принадлежащих организации систем: ИС, АСУ, ИТКС (Перечень объектов КИИ, подлежащих категорированию)
2. Реестр бизнес-процессов
3. Реестр информационных систем
4. Результат расчета значений критериев значимости объекта КИИ
5. Перечень объектов КИИ, подлежащих категорированию – направляется во ФСТЭК
6. Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий – направляется во ФСТЭК
7. Состав возможных событий (инцидентов) – направляется во ФСТЭК
8. Перечень возможных действий нарушителей – направляется во ФСТЭК
9. Приказ о создании постоянно действующей комиссии
10. Положение о комиссии
11. Протокол, заключение, акт комиссии
12. План проведения мероприятий по обеспечению безопасности значимых объектов КИИ
13. План реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак
14. Документы по внедрению, приемке и эксплуатации средств
15. Порядок хранения и учета средств
16. План по восстановлению функционирования
17. Правила резервного копирования
18. Приказ о создании системы безопасности, назначении ответственных (подразделений) отвечающих за функции обеспечения безопасности КИИ, определении системы контроля

19. Приказ и положение об отделе информационной безопасности и программно-технического обеспечения
20. Должностная инструкция специалиста по информационной безопасности
21. График проведения обучения персонала
22. Журнал проведения занятий
23. Программа занятий
24. Приказ о назначении ответственного
25. Инструкции для оператора
26. Инструкция для системного администратора
27. Правила обеспечения безопасности объектов КИИ
28. Шаблон отчета (Результаты реализации мероприятий, проводимых для обеспечения безопасности значимого объекта на стадиях (этапах) его жизненного цикла)
29. Модель угроз безопасности информации для объекта КИИ
30. Техническое задание (частное техническое задание).
Технический проект.
31. Правила эксплуатации программных и программно-аппаратных средств
32. Акт установки средств защиты
33. Правила (инструкции) безопасной работы работников, эксплуатирующих значимые объекты, и работников, обеспечивающих функционирование значимых объектов, а также действия работников при возникновении нештатных ситуаций, в том числе вызванных компьютерными инцидентами
34. Порядок доступа к программно-аппаратным средствам
35. Приказ о назначении администратора безопасности значимого объекта
36. Должностная инструкция администратора безопасности
37. Меры обеспечения безопасности
38. Аттестат соответствия

39. Пример проверки функционирования подсистемы безопасности значимого объекта, в том числе реализованных организационных и технических мер
40. ПРИКАЗ О сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них
41. Регламент выявления инцидентов информационной безопасности и реагирование на них
42. Журнал учета нештатных ситуаций

ПЕРСОНАЛЬНЫЕ ДАННЫЕ. ПЕРЕЧЕНЬ ОБЯЗАТЕЛЬНЫХ ДОКУМЕНТОВ

- ☐ Положение об обработке персональных данных
- ☐ Положение «Организация защиты персональных данных», включая утвержденные шаблоны:
 - Перечень персональных данных, обрабатываемых организацией
 - Согласие на обработку персональных данных
 - Обязательство о неразглашении персональных данных
 - Отзыв согласия на обработку персональных данных
 - Форма уведомления об уничтожении ПДн
 - Перечень должностей, имеющих доступ к персональным данным
 - Форма запроса субъекта ПДн на ознакомление с ПДн
 - Форма уведомления об устранении нарушений (уничтожении ПДн) по результатам проверки

- ☐ **Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке, в том числе в информационных системах, включая утвержденные шаблоны:**
- Шаблон запросов субъекта ПДн
 - Шаблон. Запрос на предоставление сведений об операторе
 - Отзыв согласия
 - Требование о блокировании ПДн
 - Требование об уничтожении ПДн
 - Требование об уточнении персональных данных
 - Шаблоны ответов субъекту ПДн
 - Уведомление субъекта об обработке ПДн
 - Отказ в предоставлении сведений
 - Разъяснение порядка принятия решений на основании исключительно автоматизированной обработки ПДн
 - Уведомление субъекта об устранении допущенных нарушений или об уничтожении ПДн
 - Соглашение о конфиденциальности

☐ **Журналы:**

- Журнал поэкземплярного учета средств защиты персональных данных, эксплуатационной и технической документации к ним
- Журнал учета носителей информации, содержащих персональные данные
- Акт классификации ИСПДн
- Журнал учета СКЗИ
- Журнал учета согласий субъектов персональных данных

☐ **Приказ о назначении ответственного за организацию работы с перс.данными, включая утверждение:**

- Перечень должностей, доступ которых к персональным данным необходим для выполнения ими должностных обязанностей
- Перечень должностей, ведущих обработку персональных данных без использования средств автоматизации
- Перечень должностей, ведущих обработку персональных данных с использованием средств автоматизации
- Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных
- Перечень должностей, замещение которых предусматривает проведение работ по обезличиванию персональных данных
- Порядок доступа работников в помещения, в которых ведётся обработка персональных данных
- Инструкцию ответственного за организацию обработки персональных данных
- Инструкцию по обработке персональных данных без использования средств автоматизации
- Инструкция ответственного за эксплуатацию информационных систем персональных данных
- Инструкцию по обработке персональных данных без использования средств автоматизации
- Правила рассмотрения запросов субъектов персональных данных или их представителей
- Правила работы лиц, доступ которых к персональным данным необходим для выполнения ими трудовых обязанностей

- Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований
- Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
- Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований

☐ Модель угроз безопасности

✓ Заказать полный комплект обязательных документов по КИИ + подготовка писем во ФСТЭК России можно [здесь](#):

[Узнать подробнее](#)

✓ Заказать полный комплект обязательных документов по персональным данным с изменениями 2026 года можно [здесь](#):

[Узнать подробнее](#)

✓ Обязательное обучение сотрудников по программе повышения квалификации с выдачей удостоверения: «Правила работы с персональными данными в организациях по требованию 152-ФЗ»:

[Узнать подробнее](#)

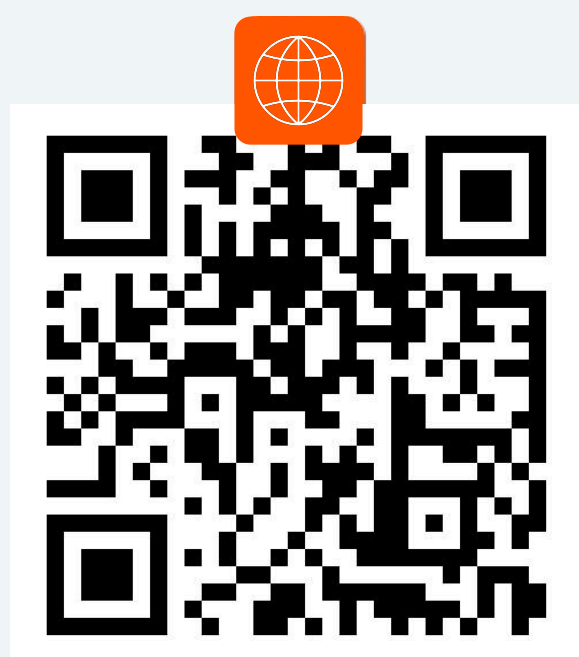


Горячая линия по юридическим вопросам
и вопросам документального сопровождения
и обучения



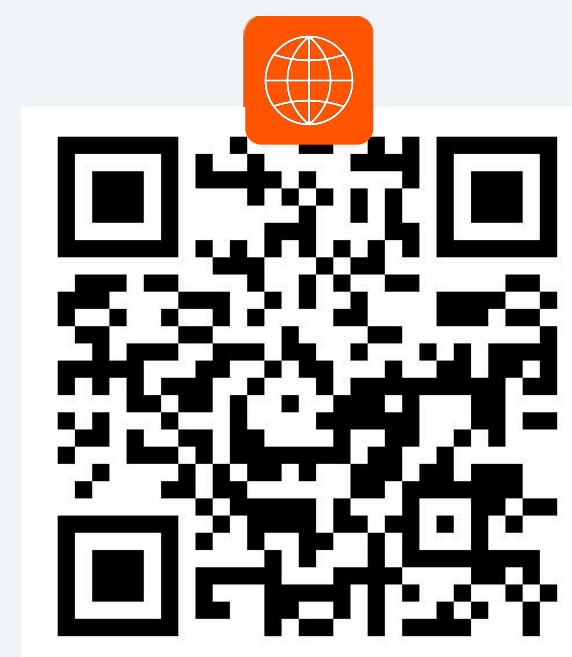
Телефон

[8 \(800\) 100-7226](tel:8(800)100-7226)



Сайт

www.mediator-pravo.ru



Сайт

www.mediator-dpo.ru