

**ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «РУДЕНА»
(ООО «РУДЕНА»)**

Адрес: 442585, Пензенская область, Сосновоборский район, с. Индерка,
переулок Центральный, здание 2, офис 1 Тел.: 89270912121, 89875293433 | E-
mail: rudenta2023@mail.ru | Сайт: <https://rudena58.ru> ОГРН 1235800000920, ИНН
5826007619, КПП 582601001



«УТВЕРЖДАЮ»

Генеральный директор ООО «Рудена»

Казаева Э. С.

«18» июня 2026 г.

**Сведения о реализуемых требованиях к защите персональных данных в
ООО «Рудена»**

1. Основные понятия и определения

- **Информационная система персональных данных (ИСПДн)** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. В ООО «Рудена» к ИСПДн относятся базы данных программы кадрово-бухгалтерского учета «1С:Бухгалтерия», локальные файлы Word/Excel, используемые для оформления договоров и актов пациентов, а также программное обеспечение «Макс» для ведения записи пациентов.
- **Автоматизированная обработка персональных данных** — обработка персональных данных с помощью средств вычислительной техники.
- **Угроза безопасности персональных данных** — совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в ИСПДн.
- **Уровень защищенности персональных данных** — комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в ИСПДн.

2. Реализуемые мероприятия по обеспечению безопасности

В соответствии с действующим законодательством РФ (Федеральный закон № 152-ФЗ «О персональных данных») в ООО «Рудена» создана необходимая нормативно-правовая база, внедрены организационные меры и реализован следующий комплекс практических мероприятий по защите персональных данных:

- **Назначение ответственных лиц:** Официальным приказом руководителя назначен ответственный сотрудник за организацию обработки персональных данных в клинике — Генеральный директор Казаева Э. С.

- **Разработка локальных нормативных актов:** Изданы и в круговую внедрены внутренние регламенты, положения и инструкции, устанавливающие жесткие процедуры, направленные на предотвращение, выявление нарушений законодательства РФ и оперативное устранение их последствий.
- **Моделирование угроз:** Определены актуальные угрозы безопасности персональных данных с учетом смешанного типа обработки данных и специфики архитектуры ИТ-контура клиники.
- **Установление уровня защищенности:** Исходя из характера обрабатываемых данных (включая специальные сведения о состоянии здоровья пациентов), установлен и технически поддерживается **3-й уровень защищенности (УЗ-3)** персональных данных.
- **Применение сертифицированных средств:** На рабочих станциях сотрудников применяются лицензированные программные средства защиты информации и антивирусное ПО, прошедшие в установленном законодательством порядке процедуру оценки соответствия. Все используемые для защиты информации программные средства имеют соответствующие сертификаты.
- **Контроль съемных носителей:** Организован строгий учет и регулярный антивирусный контроль машинных (съемных) носителей информации (флеш-карт, внешних жестких дисков), периодически используемых сотрудниками в рабочих процессах.
- **Физическая защита и разграничение доступа:** Приняты исчерпывающие меры по защите от несанкционированного физического доступа посторонних лиц к материальным носителям (медицинским картам, кадровым делам). Бумажная документация хранится в строго определенных зонах — «Регистратура (холл)» и «Хозкомната», имеющих четкие границы и запирающихся на ключ. Физический доступ в зону картотеки имеют исключительно уполномоченные сотрудники (медицинские сестры, врачи, администраторы).
- **Резервное копирование:** На регулярной основе осуществляется резервное копирование баз данных программ учета и рабочих файлов, содержащих персональные данные, для обеспечения возможности их незамедлительного восстановления в случае модификации или уничтожения вследствие сбоев или несанкционированного доступа.
- **Внутренний аудит:** Утвержден план и проводятся периодические внутренние проверки (самоаудит) состояния системы защиты и соблюдения сотрудниками правил обработки данных.
- **Оценка потенциального вреда:** Руководством проведена оценка вреда, который может быть причинен субъектам (пациентам и работникам) в случае нарушения законодательства в сфере защиты персональных данных, и установлено его полное соответствие принятым организационно-техническим мерам безопасности.
- **Ознакомление персонала:** Все без исключения сотрудники ООО «Рудена», осуществляющие автоматизированную или ручную обработку персональных данных, ознакомлены под личную роспись с требованиями к защите персональных данных, положениями законодательства РФ и всеми внутренними локальными актами клиники.