**Алгоритм работы специалиста по информационной безопасности при начале работы с персональными данными**

**1. Подготовительный этап**

1. **Анализ требований законодательства**:
   * Изучить положения Федерального закона № 152-ФЗ "О персональных данных".
   * Ознакомиться с требованиями Роскомнадзора и нормативными актами.
2. **Определение целей обработки данных**:
   * Уточнить, зачем и для каких целей будут обрабатываться персональные данные.
   * Описать эти цели в политике обработки данных.
3. **Классификация данных**:
   * Определить категории персональных данных: общие (ФИО, телефон) и особые (расовая принадлежность, здоровье).
   * Провести анализ объема и характера данных, необходимых для достижения целей обработки.

**2. Разработка организационных мер**

1. **Назначение ответственных лиц**:
   * Назначить оператора, ответственного за обработку данных.
   * Определить ответственного за защиту персональных данных (может быть специалист ИБ).
2. **Разработка локальных актов**:
   * Составить и утвердить Политику обработки персональных данных.
   * Разработать инструкции для сотрудников, работающих с персональными данными.
   * Утвердить план реагирования на инциденты, связанные с утечкой данных.
3. **Уведомление Роскомнадзора**:
   * Заполнить форму уведомления на сайте Роскомнадзора.
   * Указать цели обработки, категории данных, оператора и меры защиты.
   * Отправить уведомление и получить подтверждение о постановке на учет.

**3. Разработка технических мер защиты**

1. **Обеспечение конфиденциальности**:
   * Настроить ограничение доступа к персональным данным на основе ролей.
   * Внедрить системы идентификации и аутентификации пользователей.
2. **Применение сертифицированных средств защиты**:
   * Установить антивирусное ПО, межсетевые экраны, системы контроля доступа.
   * Использовать шифрование данных при передаче через открытые сети.
3. **Резервное копирование**:
   * Настроить регулярное резервное копирование персональных данных.
   * Обеспечить защиту резервных копий.
4. **Логирование операций**:
   * Настроить журналы учета операций с персональными данными.
   * Обеспечить мониторинг действий пользователей с доступом к данным.

**4. Оценка рисков**

1. **Анализ угроз**:
   * Провести анализ потенциальных угроз и уязвимостей.
   * Составить модель угроз для защищаемых данных.
2. **Разработка плана минимизации рисков**:
   * Установить меры по устранению выявленных рисков.
   * Внедрить постоянный мониторинг состояния защиты.

**5. Информирование сотрудников**

1. **Обучение персонала**:
   * Организовать обучение сотрудников требованиям ФЗ-152.
   * Провести инструктаж по безопасной работе с персональными данными.
2. **Закрепление ответственности**:
   * Ознакомить сотрудников с правилами обработки данных под подпись.
   * Заключить соглашения о неразглашении данных.

**6. Контроль и аудит**

1. **Тестирование системы защиты**:
   * Провести внутренний аудит соответствия защиты данных требованиям ФЗ-152.
   * Провести тестирование технических мер защиты (пентест, анализ логов).
2. **Подготовка к проверке Роскомнадзора**:
   * Убедиться, что все документы и меры соответствуют законодательству.
   * Сформировать пакет отчетности (политика, инструкции, реестры).

**7. Начало обработки персональных данных**

1. **Регистрация операций**:
   * Вести реестр обработки персональных данных (цели, объемы, сроки хранения).
   * Регулярно обновлять реестр в случае изменений.
2. **Мониторинг и обновление защиты**:
   * Постоянно контролировать состояние защиты данных.
   * Обновлять технические и организационные меры при изменении законодательных требований или выявлении новых угроз.

**8. Ведение отчетности**

1. **Формирование регулярных отчетов**:
   * Отчет о проведенных мерах защиты.
   * Отчет о выявленных инцидентах и принятых мерах.
2. **Соблюдение сроков хранения**:
   * Уничтожать данные после окончания срока обработки, если они больше не требуются для достижения целей.