**Алгоритм работы специалиста по информационной безопасности (ИБ) в рамках реализации Распоряжения Правительства РФ № 1189-р**

**I. Подготовительный этап**

1. **Изучение нормативной базы**:
   * Ознакомиться с Концепцией национальной системы управления данными (СУД) и дорожной картой.
   * Анализировать соответствующие федеральные законы:
     + ФЗ № 149 "Об информации".
     + ФЗ № 152 "О персональных данных".
     + ФЗ № 187 "О безопасности критической информационной инфраструктуры".
2. **Аудит текущего состояния**:
   * Провести анализ защищенности существующих информационных систем.
   * Выявить уязвимости в инфраструктуре, подключенной к СУД.
3. **Планирование мер безопасности**:
   * Разработать план мероприятий по защите данных в рамках СУД.
   * Определить требования к техническим средствам защиты.

**II. Реализация технических мер**

1. **Создание системы защиты данных**:
   * Установить сертифицированные средства защиты информации (DLP, SIEM, системы шифрования).
   * Настроить разграничение прав доступа к данным на уровне СУД.
2. **Интеграция с ГосСОПКА**:
   * Подключить инфраструктуру СУД к Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак.
3. **Контроль и управление доступом**:
   * Настроить многофакторную аутентификацию для доступа к государственным данным.
   * Вести журналы регистрации действий пользователей в информационных системах.
4. **Мониторинг безопасности**:
   * Внедрить системы мониторинга активности и выявления инцидентов.

**III. Работа с данными**

1. **Обеспечение качества данных**:
   * Контролировать полноту, точность и актуальность государственных данных.
   * Использовать алгоритмы для выявления несоответствий и ошибок.
2. **Классификация данных**:
   * Разработать регламент классификации данных по уровням конфиденциальности.
   * Установить правила обработки данных разных категорий.
3. **Обеспечение безопасности передачи данных**:
   * Внедрить системы шифрования при передаче данных между участниками СУД.
   * Настроить защиту от утечек данных через каналы передачи.

**IV. Реагирование на инциденты**

1. **План реагирования на инциденты**:
   * Разработать сценарии действий при утечках, сбоях или кибератаках.
2. **Обработка инцидентов**:
   * Вести журнал инцидентов информационной безопасности.
   * Проводить расследования и готовить акты по результатам инцидентов.
3. **Взаимодействие с регуляторами**:
   * Сообщать о выявленных инцидентах в ФСТЭК и Роскомнадзор.
   * Устранять замечания по предписаниям регуляторов.

**V. Обучение сотрудников**

1. **Организация обучения**:
   * Проводить курсы и тренинги по работе с данными и системами СУД.
   * Обучать действиям при инцидентах и защите информации.
2. **Повышение квалификации**:
   * Подготовка специалистов для работы с передовыми технологиями защиты данных.

**VI. Контроль и аудит**

1. **Регулярный аудит безопасности**:
   * Проводить тестирование защищенности систем (включая пентесты).
   * Готовить отчеты по результатам проверок.
2. **Контроль выполнения политики безопасности**:
   * Проверять соблюдение правил сотрудниками.
   * Проводить внутренние расследования при выявлении нарушений.
3. **Оценка эффективности**:
   * Использовать KPI для оценки качества защиты данных (время реакции на инциденты, доля устраненных уязвимостей).

**VII. Документооборот**

1. **Ведение документации**:
   * Разрабатывать и обновлять политики безопасности.
   * Вести журналы доступа, инцидентов и изменений в системах.
2. **Отчеты для руководства**:
   * Предоставлять ежеквартальные отчеты о состоянии ИБ.
   * Готовить отчеты по реализации мероприятий, указанных в дорожной карте.
3. **Взаимодействие с государственными органами**:
   * Регулярно отправлять отчеты в ФСТЭК, ФСБ и Роскомнадзор.
   * Документировать выполнение предписаний и проверок.

**Итог**

Этот алгоритм включает все ключевые этапы работы специалиста по ИБ в рамках создания и функционирования национальной СУД. Если требуется адаптация для специфики вашей организации или разработка шаблонов документов, готов помочь!