**Алгоритм работы специалиста по информационной безопасности (ИБ) в рамках Указа Президента РФ № 490 и связанных документов**

**I. Подготовительный этап**

1. **Изучение нормативной базы**:
   * Ознакомиться с Национальной стратегией развития искусственного интеллекта до 2030 года.
   * Проанализировать изменения, внесённые в стратегию Указом № 124 от 2024 года.
2. **Аудит текущего состояния**:
   * Провести анализ инфраструктуры, где применяются технологии искусственного интеллекта (ИИ).
   * Оценить соответствие текущих мер защиты информации требованиям стратегии.
3. **Идентификация объектов защиты**:
   * Выделить наборы данных, системы и алгоритмы, требующие особой защиты.
   * Определить критически важные элементы инфраструктуры.

**II. Реализация мероприятий**

1. **Внедрение мер защиты данных**:
   * Настроить механизмы шифрования данных, особенно больших массивов для обучения ИИ.
   * Обеспечить безопасность передачи данных между участниками системы.
2. **Модернизация технологий**:
   * Внедрить отказоустойчивые системы и решения.
   * Обеспечить переход на отечественное оборудование и ПО.
3. **Управление доступом**:
   * Установить многофакторную аутентификацию для всех пользователей систем ИИ.
   * Регламентировать права доступа в соответствии с классификацией данных.
4. **Мониторинг и управление рисками**:
   * Разработать сценарии возможных угроз, включая утечку данных и несанкционированный доступ.
   * Установить системы мониторинга событий безопасности.

**III. Работа с кадрами**

1. **Обучение сотрудников**:
   * Организовать тренинги по использованию систем ИИ и защите информации.
   * Провести ознакомление с нормативной базой и принципами безопасности данных.
2. **Формирование кадрового резерва**:
   * Подготовить специалистов для работы с моделями ИИ, включая их обучение и адаптацию.

**IV. Реагирование на инциденты**

1. **Планирование реагирования**:
   * Разработать план действий на случай инцидентов, связанных с системами ИИ.
   * Включить процедуры восстановления данных и обеспечения непрерывности бизнеса.
2. **Расследование инцидентов**:
   * Вести учёт всех происшествий.
   * Анализировать причины инцидентов и разрабатывать меры для их предотвращения.

**V. Документооборот и отчётность**

1. **Разработка внутренних документов**:
   * Политики по управлению доступом к данным и защите алгоритмов ИИ.
   * Планы мероприятий по снижению рисков.
2. **Ведение отчётности**:
   * Представлять регулярные отчёты о выполнении мероприятий.
   * Подготавливать документацию для проверок регуляторов.
3. **Взаимодействие с органами власти**:
   * Отчитываться о реализации стратегии и выполнении требований указов.
   * Участвовать в государственных проектах по развитию ИИ.

**Итог**

Эти шаги помогут интегрировать требования Указа № 490 и связанных нормативных документов в деятельность специалиста по ИБ. Если требуется подробная детализация по конкретным документам или мероприятиям, сообщите!