**Список документов, необходимых для выполнения требований Постановления № 211**

**I. Организационные документы**

1. **Политика обработки персональных данных**
   * Определяет цели, порядок обработки и защиты данных.
2. **Положение о защите персональных данных**
   * Устанавливает принципы работы с данными, обязанности сотрудников и меры безопасности.
3. **Положение о внутреннем контроле обработки персональных данных**
   * Описывает порядок проверок соблюдения требований законодательства.
4. **Перечень персональных данных, подлежащих обработке**
   * Включает данные, которые собираются и обрабатываются организацией.
5. **Положение об обезличивании персональных данных**
   * Регламентирует порядок обезличивания данных и использования обезличенной информации.
6. **Регламент обработки персональных данных**
   * Определяет порядок обработки, хранения и уничтожения данных.
7. **Положение о работе с физическими носителями данных**
   * Устанавливает правила работы с бумажными документами, носителями информации (диски, флешки).
8. **Инструкция по организации защиты информации**
   * Руководство для сотрудников по защите данных на всех этапах работы.

**II. Документы для сотрудников**

1. **Должностные инструкции сотрудников**
   * Описание обязанностей и ответственности сотрудников, работающих с персональными данными.
2. **Программа обучения по защите персональных данных**
   * Курсы и семинары для сотрудников по вопросам защиты данных.
3. **Журнал проведения инструктажей**
   * Учет всех проведённых инструктажей сотрудников.
4. **Соглашения о неразглашении персональных данных**
   * Подписываются всеми сотрудниками, имеющими доступ к данным.

**III. Технические и учетные документы**

1. **Паспорт информационных систем персональных данных (ИСПДн)**
   * Описание используемых систем, их категории и уровня защищённости.
2. **Акт категорирования ИСПДн**
   * Документ, определяющий категории информационных систем в соответствии с требованиями.
3. **Реестр информационных систем, обрабатывающих персональные данные**
   * Полный список систем, где обрабатываются персональные данные.
4. **План мероприятий по защите персональных данных**
   * Меры, направленные на обеспечение защиты данных.
5. **Журнал учёта действий пользователей в ИСПДн**
   * Записи обо всех действиях сотрудников в системах обработки данных.
6. **Журнал инцидентов безопасности**
   * Фиксация всех нарушений и их последствий.
7. **Реестр угроз безопасности персональных данных**
   * Перечень актуальных угроз и мер по их устранению.
8. **План реагирования на инциденты безопасности**
   * Описание действий при обнаружении инцидента.

**IV. Документы для взаимодействия с субъектами данных**

1. **Образцы уведомлений субъектов данных**
   * Шаблоны уведомлений о сборе, обработке и уничтожении данных.
2. **Регламент рассмотрения запросов субъектов данных**
   * Порядок обработки запросов на изменение или удаление данных.
3. **Согласие на обработку персональных данных**
   * Форма для получения согласия субъекта на обработку его данных.
4. **Регламент отзыва согласия на обработку данных**
   * Процедура прекращения обработки данных по запросу субъекта.

**V. Документы для внешнего взаимодействия**

1. **Договоры с подрядчиками и контрагентами**
   * Обязательные пункты о защите персональных данных.
2. **Соглашение о защите данных с подрядчиками**
   * Закрепление ответственности за защиту данных при передаче.
3. **Протоколы проверки подрядчиков**
   * Результаты аудитов подрядчиков на предмет соблюдения требований.

**VI. Отчётность и аудиты**

1. **Уведомление Роскомнадзора об обработке данных**
   * Документ, поданный в Роскомнадзор с описанием целей и методов обработки.
2. **Акт проверки соответствия законодательству**
   * Результаты внутреннего аудита соответствия требованиям законодательства.
3. **Отчёты о выполнении мероприятий по защите данных**
   * Документ для руководства и надзорных органов.

**VII. Документы для обновления и развития**

1. **План модернизации средств защиты данных**
   * Стратегия обновления технологий и процессов защиты.
2. **План улучшения компетенций сотрудников**
   * Программа обучения и повышения квалификации.
3. **Аналитический отчёт по обработке данных**
   * Ежегодный отчёт об эффективности мер защиты и выявленных нарушениях.

**Итог:**

**Итого: 33 документа**. Этот список охватывает ключевые аспекты выполнения требований Постановления № 211, включая организационные, технические и процедурные меры. Если требуется помощь в разработке шаблонов, обращайтесь!

**Дополнительные документы для выполнения требований Постановления № 211**

**VIII. Расширенные организационные и контрольные документы**

1. **Матрица ответственности сотрудников**
   * Документ, описывающий распределение обязанностей по защите данных между сотрудниками.
2. **Положение о внутреннем аудите обработки персональных данных**
   * Регламентирует порядок проведения внутренних проверок на соответствие требованиям ИБ.
3. **Регламент взаимодействия с контролирующими органами**
   * Описание процедур взаимодействия с Роскомнадзором, ФСБ и ФСТЭК.
4. **Акт о назначении ответственных за ИБ**
   * Документ, фиксирующий назначение сотрудников, ответственных за защиту данных.
5. **Инструкция по классификации и уничтожению данных**
   * Определяет категории данных и процедуры их уничтожения.
6. **Регламент работы с данными в условиях удалённого доступа**
   * Устанавливает требования и ограничения при обработке данных вне офиса.
7. **Перечень документов, содержащих персональные данные**
   * Указание всех документов, хранящих персональные данные (например, анкеты, договора, заявки).

**IX. Документы для мониторинга и реагирования**

1. **План проверки системы обработки данных**
   * Содержит график и методику проверки эффективности защиты данных.
2. **Журнал инцидентов обработки данных**
   * Учитывает любые случаи, связанные с обработкой, включая ошибки, сбои или нарушения.
3. **Протокол расследования инцидента**
   * Документ, фиксирующий результаты расследования инцидентов и предложенные меры по их устранению.
4. **Инструкция по действиям при утечке данных**
   * Детализированный план действий при выявлении инцидентов с утечкой информации.

**X. Документы для работы с подрядчиками и партнёрами**

1. **Регламент оценки подрядчиков**
   * Описание методик проверки соответствия подрядчиков требованиям ИБ.
2. **Акт передачи данных подрядчику**
   * Документ, подтверждающий передачу персональных данных подрядчику с указанием объёма и целей обработки.
3. **Журнал взаимодействия с подрядчиками**
   * Фиксация всех операций, связанных с передачей и обработкой данных.

**XI. Документы для обучения сотрудников**

1. **План проведения обучающих мероприятий по ИБ**
   * График семинаров, тренингов и проверок знаний.
2. **Тесты для проверки знаний сотрудников**
   * Набор вопросов для оценки понимания сотрудниками требований по защите данных.
3. **Журнал аттестации сотрудников**
   * Фиксация результатов проверки знаний сотрудников в области ИБ.

**XII. Документы по защите физической инфраструктуры**

1. **Паспорт помещений, где обрабатываются данные**
   * Описание всех помещений, где ведётся работа с данными, и применяемых мер защиты.
2. **Положение о пропускном режиме в помещениях**
   * Регламент контроля доступа в офисы и серверные комнаты.
3. **Инструкция по действиям при несанкционированном доступе**
   * План действий при выявлении попыток физического проникновения или утраты носителей данных.
4. **Журнал учета доступа к серверным помещениям**
   * Учет всех сотрудников и посетителей, имевших доступ к серверным помещениям.

**XIII. Расширенные технические документы**

1. **Регламент использования шифрования данных**
   * Определяет порядок работы с криптографическими средствами защиты.
2. **Регламент обновления средств защиты информации**
   * Описание процедур регулярного обновления программного обеспечения и оборудования.
3. **Реестр сертификатов используемых средств защиты**
   * Список сертифицированных средств защиты, используемых в организации.

**XIV. Отчётность и развитие системы защиты**

1. **Ежегодный отчёт об инцидентах и уязвимостях**
   * Детализированный анализ всех выявленных инцидентов и уязвимостей за год.
2. **План по улучшению системы ИБ**
   * Стратегия развития технической и организационной защиты данных.
3. **Акт об эффективности мер защиты данных**
   * Документ, фиксирующий результаты анализа защищённости данных и рекомендации по улучшению.

**Итог**

**Итого: 60 документов**, включая обязательные и расширенные. Этот список покрывает все ключевые аспекты обработки и защиты персональных данных в рамках Постановления № 211. Если необходимо помочь с шаблонами, разработкой или адаптацией этих документов, обращайтесь!