**Чек-лист по Постановлению Правительства РФ № 211 от 21 марта 2012 года**

**I. Организационные меры**

1. **Назначение ответственных лиц**:
   * Назначен ответственный за организацию обработки персональных данных.
   * Утверждены должностные инструкции для сотрудников, работающих с персональными данными.
2. **Создание внутренней нормативной базы**:
   * Разработана политика обработки персональных данных.
   * Утверждены правила внутреннего контроля и аудита обработки данных.
   * Созданы перечни информационных систем и категорий обрабатываемых данных.
3. **Организация процессов обработки данных**:
   * Определены цели, категории данных, сроки обработки и хранения.
   * Утверждены процедуры уничтожения данных по окончании срока их хранения.

**II. Обеспечение безопасности данных**

1. **Технические и организационные меры защиты**:
   * Внедрены сертифицированные средства защиты информации (СЗИ).
   * Реализованы правовые и технические меры для обеспечения безопасности данных в ИСПДн.
2. **Шифрование и контроль доступа**:
   * Настроены системы шифрования для передачи и хранения данных.
   * Реализованы механизмы разграничения прав доступа для сотрудников.
3. **Обезличивание данных**:
   * Организованы процедуры обезличивания персональных данных.
   * Назначены ответственные лица за выполнение операций по обезличиванию.
4. **Защита физических носителей**:
   * Настроен порядок обращения с бумажными документами и физическими носителями (диски, флеш-накопители).
   * Обеспечена их надёжная защита и уничтожение по окончании срока хранения.

**III. Контроль и управление рисками**

1. **Модели угроз и рисков**:
   * Разработана модель угроз для обрабатываемых данных.
   * Проведена оценка рисков и определены меры по их минимизации.
2. **Мониторинг действий сотрудников**:
   * Настроены системы контроля действий сотрудников (DLP-системы, журналы доступа).
   * Проводится регулярный анализ активности пользователей.
3. **Регулярный аудит обработки данных**:
   * Утверждён план регулярных внутренних проверок.
   * Проводятся проверки эффективности мер защиты и выполнения требований.

**IV. Взаимодействие с субъектами данных**

1. **Обеспечение прав субъектов данных**:
   * Утверждены процедуры обработки запросов субъектов данных.
   * Организована возможность для субъектов получать разъяснения о последствиях отказа предоставлять данные.
2. **Публикация политики обработки данных**:
   * Политика обработки данных размещена на официальном сайте или в открытом доступе.

**V. Взаимодействие с государственными органами**

1. **Уведомление Роскомнадзора**:
   * Подано уведомление об обработке персональных данных.
   * Уведомление содержит все необходимые данные:
     + Цели обработки.
     + Категории обрабатываемых данных.
     + Уровень защищённости ИСПДн.
2. **Отчётность и согласование**:
   * Готовятся отчёты для надзорных органов.
   * Документы согласованы с уполномоченными органами.

**VI. Обучение сотрудников**

1. **Ознакомление и инструктаж**:
   * Сотрудники, работающие с данными, ознакомлены с внутренними документами.
   * Проведены инструктажи по основным требованиям законодательства.
2. **Программы обучения**:
   * Разработаны и реализованы программы обучения сотрудников.
   * Проводится регулярное тестирование знаний.

**VII. Реагирование на инциденты**

1. **План реагирования на инциденты**:
   * Утверждены сценарии действий при нарушении безопасности данных.
   * Определены ответственные за устранение последствий.
2. **Документирование инцидентов**:
   * Ведётся журнал инцидентов, включая причины, последствия и принятые меры.

**VIII. Постоянное совершенствование**

1. **Актуализация документации**:
   * Политика, инструкции и регламенты пересматриваются не реже одного раза в год.
   * Учтены изменения в законодательстве и рекомендации надзорных органов.
2. **Модернизация системы защиты**:
   * Проводится регулярное обновление средств защиты данных.
   * Внедряются новые технологии для повышения уровня безопасности.

**Итог**

Чек-лист охватывает ключевые аспекты Постановления № 211, включая организационные, технические и процедурные меры. Если требуется помощь в разработке шаблонов документов или конкретизации шагов, дайте знать!

**Дополнения к чек-листу по Постановлению № 211**

**IX. Дополнительные технические меры**

1. **Управление учётными записями**:

* Внедрена система управления учётными записями (IAM) для контроля доступа сотрудников к ИСПДн.
* Настроены временные права доступа для выполнения разовых задач.

1. **Резервирование и восстановление данных**:

* Настроена система автоматического резервного копирования персональных данных.
* Регулярно тестируется возможность восстановления данных из резервных копий.

1. **Сегментация сети**:

* Информационные системы разделены на сегменты для предотвращения распространения угроз.
* Настроены межсетевые экраны и системы контроля доступа на уровне сети.

1. **Защита от внешних угроз**:

* Используются системы обнаружения и предотвращения атак (IDS/IPS).
* Настроена защита от DDoS-атак (если это применимо).

**X. Расширенный контроль обработки персональных данных**

1. **Журналирование событий**:

* Ведётся журналирование всех событий, связанных с доступом к персональным данным (изменение, копирование, удаление).
* Настроены автоматические уведомления о подозрительной активности.

1. **Управление инцидентами безопасности**:

* Разработаны детализированные планы реагирования на инциденты.
* Проводится анализ инцидентов для выявления корневых причин.

1. **Внедрение DLP-систем**:

* Используются системы предотвращения утечек данных (DLP) для мониторинга и контроля операций с данными.
* Настроены правила и политики для предотвращения несанкционированного доступа или передачи данных.

**XI. Расширение взаимодействия с субъектами данных**

1. **Процедуры отзыва согласия на обработку данных**:

* Разработан и утверждён регламент отзыва субъектами согласия на обработку их данных.
* Организована система уведомления о прекращении обработки данных по требованию.

1. **Обеспечение доступа субъектов к данным**:

* Субъекты данных имеют доступ к информации о том, какие данные обрабатываются и для каких целей.
* Реализована возможность вносить изменения в данные по запросу субъектов.

1. **Обратная связь**:

* Организована служба поддержки для ответов на запросы субъектов данных.
* Внедрён механизм регистрации и обработки жалоб.

**XII. Работа с подрядчиками и внешними организациями**

1. **Оценка соответствия подрядчиков**:

* Проведена проверка соответствия подрядчиков требованиям законодательства о персональных данных.
* Заключены соглашения, закрепляющие обязательства подрядчиков по защите данных.

1. **Уведомление о нарушениях безопасности**:

* Разработаны процедуры уведомления подрядчиков в случае инцидентов.
* Определены сроки устранения нарушений и отчётности подрядчиков.

1. **Контроль передачи данных**:

* Внедрены правила передачи данных между организацией и третьими лицами.
* Настроены каналы защищённой передачи данных (VPN, TLS).

**XIII. Углублённый аудит и совершенствование**

1. **Независимые аудиты**:

* Привлекаются внешние специалисты для аудита системы защиты персональных данных.
* Результаты аудитов используются для разработки улучшений.

1. **Обратная связь с сотрудниками**:

* Сотрудники могут анонимно сообщать о нарушениях в области обработки данных.
* Разработаны меры защиты для информаторов.

1. **Оценка эффективности мер защиты**:

* Внедрены KPI для измерения эффективности защиты данных.
* Анализируются показатели, такие как количество инцидентов и время их устранения.

**XIV. Постоянное развитие и обучение**

1. **Индивидуальные планы обучения**:

* Для ключевых сотрудников разрабатываются индивидуальные программы повышения квалификации.
* В обучение включаются кейсы реальных инцидентов.

1. **Обновление знаний сотрудников**:

* Организуются семинары с приглашением экспертов.
* Рассылаются актуальные информационные бюллетени по изменениям в законодательстве и новым угрозам.

**Итог**

Эти дополнения усиливают базовый чек-лист за счёт расширения работы с техническими средствами, взаимодействия с подрядчиками, субъектами данных и внешними аудиторами, а также акцентируют внимание на развитии персонала и систем защиты. Если нужно детализировать или разработать конкретные процедуры, сообщите!