**Перечень документов, которые необходимо завести в организации для соблюдения требований Федерального закона № 152-ФЗ "О персональных данных"**

**I. Организационные документы**

1. **Политика обработки персональных данных**:
   * Основной документ, описывающий цели, принципы и условия обработки персональных данных.
   * Утверждается руководством организации и предоставляется для ознакомления субъектам данных.
2. **Положение об обработке и защите персональных данных**:
   * Детализирует порядок обработки, включая меры защиты.
   * Утверждается на уровне локального нормативного акта.
3. **Приказ о назначении ответственного за обработку персональных данных**:
   * Документ, назначающий сотрудника, ответственного за организацию обработки и защиту персональных данных.
4. **Приказ о назначении ответственного за обеспечение безопасности персональных данных**:
   * Утверждает лицо, которое организует меры защиты данных и мониторит их выполнение.

**II. Документы для обеспечения защиты данных**

1. **Модель угроз безопасности персональных данных**:
   * Документ, в котором анализируются потенциальные угрозы, связанные с обработкой данных.
2. **План мероприятий по защите персональных данных**:
   * Содержит список организационных и технических мер, направленных на обеспечение безопасности данных.
3. **Журнал учета инцидентов информационной безопасности**:
   * Регистрирует все инциденты, связанные с утечкой, утратой или иным нарушением обработки персональных данных.
4. **Акты категорирования информационных систем персональных данных (ИСПДн)**:
   * Устанавливают категории ИСПДн в зависимости от типа обрабатываемых данных и их значимости.

**III. Документы по обработке персональных данных**

1. **Соглашение о конфиденциальности с сотрудниками**:
   * Обязательство сотрудников о неразглашении персональных данных, доступ к которым они получили в процессе работы.
2. **Согласие на обработку персональных данных**:
   * Подписывается субъектом данных, предоставляющим свои данные для обработки.
3. **Реестр обработки персональных данных**:
   * Включает перечень операций по обработке данных, цели, объемы, сроки хранения и лица, ответственные за обработку.
4. **Акт об уничтожении персональных данных**:
   * Фиксирует уничтожение данных, которые более не нужны для достижения целей обработки.

**IV. Документы для сотрудников**

1. **Инструкция по обработке персональных данных**:
   * Руководство для сотрудников, работающих с персональными данными, о правилах обработки и защиты данных.
2. **Памятка для сотрудников**:
   * Содержит краткие правила работы с персональными данными и меры предосторожности.
3. **Протокол обучения сотрудников**:
   * Удостоверяет, что сотрудники прошли инструктаж или обучение по работе с персональными данными.

**V. Взаимодействие с третьими лицами**

1. **Договор о поручении обработки персональных данных**:
   * Подписывается с контрагентами, если они обрабатывают данные по поручению организации (например, бухгалтерия, колл-центры).
2. **Соглашение об ответственности за защиту персональных данных**:
   * Содержит обязательства контрагентов соблюдать меры защиты данных.

**VI. Документы для уведомления Роскомнадзора**

1. **Уведомление о начале обработки персональных данных**:
   * Направляется в Роскомнадзор с указанием целей, категорий данных и мер защиты.
2. **Отчет о выполнении требований Роскомнадзора**:
   * Подготавливается при проверке или по запросу регулятора.

**VII. Технические документы**

1. **Паспорт информационной системы персональных данных**:
   * Описывает архитектуру и состав ИСПДн, включая технические средства защиты.
2. **Руководство пользователя информационной системы**:
   * Описывает, как работать с системой при обработке персональных данных.
3. **Протокол тестирования систем защиты данных**:
   * Документирует результаты проверки безопасности систем.

**VIII. Отчеты и акты**

1. **Акт проверки соответствия обработки данных требованиям ФЗ-152**:
   * Подтверждает, что организация соблюдает требования закона.
2. **Отчет об инцидентах персональных данных**:
   * Анализирует причины и последствия инцидентов, а также меры, предпринятые для их устранения.
3. **Акт об утверждении сроков хранения персональных данных**:
   * Определяет временные рамки хранения данных в зависимости от целей обработки.

**IX. Регулярные аудиты**

1. **Протокол внутреннего аудита обработки данных**:
   * Результаты регулярных проверок соответствия обработок данных требованиям закона.
2. **Протокол анализа эффективности мер защиты**:
   * Отчет о проведенных мероприятиях по проверке уровня защиты данных.

**X. Обновление документов**

1. **План актуализации локальных нормативных актов**:
   * Указывает сроки и порядок обновления документов в зависимости от изменений законодательства.
2. **Протокол об обновлении технических средств защиты данных**:
   * Подтверждает модернизацию технических решений для защиты персональных данных.

Да, дополнения к перечню документов могут быть связаны с более глубокой интеграцией информационной безопасности, учетом специфики организации и современных требований:

**XI. Документы по управлению рисками**

1. **Реестр рисков обработки персональных данных**:
   * Содержит перечень потенциальных угроз, их вероятности и последствий, а также меры по минимизации.
2. **План управления рисками**:
   * Устанавливает порядок реагирования на возможные риски, связанные с обработкой данных.
3. **Отчет о регулярной оценке рисков**:
   * Отражает результаты анализа угроз и эффективности мер защиты.

**XII. Документы для внешних проверок**

1. **Протокол взаимодействия с проверяющими органами**:
   * Описывает порядок предоставления информации Роскомнадзору, взаимодействие с проверяющими и защиту конфиденциальных данных при проверке.
2. **План подготовки к проверке**:
   * Содержит перечень действий по подготовке к проверке (проверка соответствия документов, состояния систем, обучение персонала).
3. **Документы о соблюдении GDPR (если применимо)**:
   * Политика защиты данных для международных клиентов.
   * Регламент выполнения запросов субъектов данных (право на удаление, ограничение обработки и т.д.).

**XIII. Внедрение современных технологий**

1. **Руководство по работе с автоматизированными системами обработки данных**:
   * Для систем, использующих ИИ, Big Data или другие технологии.
2. **Процедура обработки обезличенных данных**:
   * Описание методик анонимизации и проверки их эффективности.

**XIV. Обеспечение прозрачности**

1. **Публичная политика обработки данных**:
   * Документ, доступный для ознакомления клиентам и партнерам через сайт или иные каналы.
2. **Форма для запросов субъектов данных**:
   * Стандартный шаблон, который субъект может использовать для обращения в организацию (запрос об удалении, исправлении, предоставлении данных).

**XV. Для модернизации защиты**

1. **План обновления систем защиты персональных данных**:
   * Сроки и действия по улучшению технических и организационных мер.
2. **Протокол об оценке новых технологий защиты данных**:
   * Описание внедряемых решений (например, SIEM, DLP-системы).

**XVI. Управление доступом**

1. **Реестр привилегированных учетных записей**:
   * Учет учетных записей с повышенными правами доступа.
2. **Политика управления доступом**:
   * Правила назначения, изменения и отзыва доступа для пользователей.
3. **Журнал временного доступа**:
   * Учет временных прав, предоставленных сотрудникам или партнерам.

**XVII. Мониторинг и реагирование**

1. **Инструкция по реагированию на инциденты**:
   * Подробное руководство для сотрудников, описывающее порядок действий при утечке данных или кибератаке.
2. **Протокол о завершении инцидента**:
   * Документ, фиксирующий результаты анализа инцидента, его последствия и меры по устранению.
3. **Журнал уведомлений о нарушениях**:
   * Учет уведомлений субъектов данных или контролирующих органов о нарушениях обработки данных.

**XVIII. Обучение персонала**

1. **Программа обучения по защите персональных данных**:
   * Описание регулярных курсов, тренингов и тестирований.
2. **Отчет о результатах обучения сотрудников**:
   * Итоги проведенных курсов, охват сотрудников, результаты тестов.

**XIX. Контроль за подрядчиками**

1. **Акт проверки подрядчиков**:
   * Документ, подтверждающий, что сторонние организации соблюдают требования закона (например, при аутсорсинге обработки данных).
2. **Политика взаимодействия с подрядчиками**:
   * Регламент работы с третьими лицами, включая требования к обработке данных и мерам защиты.

**XX. Регулярный пересмотр**

1. **План пересмотра локальных нормативных актов**:
   * Устанавливает сроки обновления документов и ответственных лиц.
2. **Отчет о соответствии новым законодательным требованиям**:
   * Подтверждает, что документы и процессы адаптированы к изменениям законодательства.