**Список документов, необходимых для выполнения требований Указа Президента РФ № 585**

**I. Организационные документы**

1. **Политика информационной безопасности**
   * Определяет общие подходы к защите информации в рамках ядерной и радиационной безопасности.
2. **Положение о защите информации на объектах атомной отрасли**
   * Устанавливает порядок работы с данными, правила обработки и хранения информации.
3. **Положение о классификации информации**
   * Регламентирует классификацию данных на уровни конфиденциальности (государственная тайна, служебная, общедоступная информация).
4. **Инструкция по работе с конфиденциальной информацией**
   * Уточняет порядок обращения с документами и электронными данными ограниченного доступа.
5. **Положение о предотвращении утечек данных**
   * Описывает правила работы с системами предотвращения утечек данных (DLP).

**II. Документы по управлению доступом**

1. **Регламент управления доступом к информации**
   * Устанавливает порядок предоставления, ограничения и отзыва доступа сотрудников к данным.
2. **Матрица ответственности и доступа**
   * Документ, фиксирующий доступ сотрудников к критически важной информации.
3. **Журнал регистрации доступа к данным**
   * Учет всех операций доступа к конфиденциальной информации.
4. **Акты разграничения доступа**
   * Документы, утверждающие уровни доступа для каждого сотрудника.

**III. Документы по реагированию на инциденты**

1. **План реагирования на инциденты информационной безопасности**
   * Включает сценарии действий при кибератаках, утечке данных, авариях и иных угрозах.
2. **Журнал регистрации инцидентов безопасности**
   * Учет всех случаев нарушений информационной безопасности.
3. **Акт расследования инцидента**
   * Документ, фиксирующий результаты расследования и меры по устранению последствий.
4. **Отчёт по анализу инцидентов и уязвимостей**
   * Рекомендации по устранению выявленных проблем.

**IV. Документы по обучению сотрудников**

1. **Программа обучения сотрудников по защите информации**
   * Курсы, семинары и тесты для работников, связанных с обработкой критически важной информации.
2. **Журнал проведения инструктажей по информационной безопасности**
   * Учет проведённых инструктажей.
3. **Тесты на знание правил информационной безопасности**
   * Для проверки компетенций сотрудников.

**V. Технические документы**

1. **Паспорт информационной системы объектов атомной отрасли**
   * Описание всех информационных систем, включая их защищенность и доступ.
2. **Реестр информационных систем, обрабатывающих критически важные данные**
   * Полный список систем, где осуществляется работа с важной информацией.
3. **План модернизации технических средств защиты**
   * Стратегия обновления ИТ-инфраструктуры и программного обеспечения.
4. **Отчёт по результатам аудита информационной безопасности**
   * Документ, подтверждающий соответствие систем нормативным требованиям.
5. **Акт об установке и настройке средств криптографической защиты**
   * Учет установки сертифицированных криптографических систем.

**VI. Документы для взаимодействия с регуляторами**

1. **Отчётность в Росатом и другие контролирующие органы**
   * Регулярные отчёты о состоянии информационной безопасности.
2. **Журнал проверок со стороны надзорных органов**
   * Учет проверок и их результатов.
3. **Акты соответствия стандартам и требованиям**
   * Документы, подтверждающие выполнение обязательных норм.

**VII. Документы по управлению рисками**

1. **Карта рисков информационной безопасности**
   * Анализ угроз и уязвимостей с рекомендациями по их устранению.
2. **План мероприятий по минимизации рисков**
   * Документ с описанием действий для снижения вероятности возникновения угроз.

**Итог**

**Итого: 26 документов**, охватывающих ключевые аспекты реализации Указа № 585 в части защиты информации. Если требуется помощь в разработке или адаптации этих документов, дайте знать!