**Полный список документов для реализации Указа Президента РФ № 400 "О Стратегии национальной безопасности Российской Федерации"**

**I. Организационные документы**

1. **Стратегия информационной безопасности организации**
   * Адаптированный локальный документ, основанный на положениях Стратегии национальной безопасности РФ.
2. **Положение о защите информации**
   * Основные подходы к защите информации, включая персональные и конфиденциальные данные.
3. **Политика информационной безопасности (ИБ)**
   * Устанавливает правила, обязанности и процессы защиты информации в организации.
4. **Положение о критической информационной инфраструктуре (КИИ)**
   * Определяет перечень объектов КИИ, меры их защиты и порядок взаимодействия с регуляторами.
5. **Регламент обработки персональных данных**
   * Устанавливает правила работы с персональными данными, их хранения и уничтожения.
6. **Положение о классификации информации**
   * Регламентирует уровни конфиденциальности данных и порядок их обработки.

**II. Документы по управлению доступом**

1. **Матрица распределения прав доступа**
   * Указывает, какие сотрудники имеют доступ к определённым данным и системам.
2. **Регламент управления доступом к информационным системам**
   * Порядок предоставления, изменения и отзыва доступа.
3. **Журнал регистрации доступа**
   * Учет предоставления, изменения и закрытия доступа к критически важным системам.
4. **Акты разграничения прав доступа**
   * Утверждает права доступа для каждого сотрудника или группы.

**III. Документы по реагированию на инциденты**

1. **План реагирования на инциденты информационной безопасности**
   * Детализирует действия при утечках данных, кибератаках и сбоях.
2. **Журнал регистрации инцидентов**
   * Учитывает все случаи инцидентов безопасности.
3. **Акт расследования инцидентов**
   * Документирует причины, ход и результаты расследований инцидентов.
4. **Отчет по результатам реагирования на инциденты**
   * Включает выводы и рекомендации для предотвращения повторений.
5. **Регламент работы с ГосСОПКА**
   * Порядок взаимодействия с государственной системой обнаружения и предотвращения кибератак.

**IV. Документы по обучению сотрудников**

1. **Программа обучения по информационной безопасности**
   * Включает теоретические и практические модули для всех уровней сотрудников.
2. **Журнал проведения инструктажей**
   * Учет всех инструктажей по ИБ.
3. **Тесты для проверки знаний сотрудников**
   * Наборы вопросов для оценки компетенций в области ИБ.
4. **Памятки по защите информации**
   * Краткие инструкции для сотрудников по защите данных и реагированию на угрозы.

**V. Документы по технической защите**

1. **Паспорт информационных систем**
   * Подробное описание всех информационных систем, включая их защиту.
2. **Реестр критической информационной инфраструктуры (КИИ)**
   * Перечень объектов КИИ с их характеристиками.
3. **План модернизации технических средств защиты**
   * Описание этапов обновления ИТ-инфраструктуры.
4. **Акт об установке и настройке средств защиты информации**
   * Документирование установки сертифицированных систем защиты.
5. **Отчет по аудиту информационной безопасности**
   * Результаты внутреннего и внешнего аудита.

**VI. Документы по управлению рисками**

1. **Карта рисков информационной безопасности**
   * Сценарии угроз, их вероятность и меры по минимизации.
2. **План управления рисками**
   * Конкретные мероприятия по предотвращению и снижению рисков.
3. **Журнал учета выполненных мероприятий по снижению рисков**
   * Учет действий по управлению рисками.

**VII. Взаимодействие с государственными органами**

1. **Регламент взаимодействия с ФСТЭК, ФСБ и Роскомнадзором**
   * Устанавливает порядок взаимодействия с регуляторами.
2. **Отчеты в государственные органы**
   * Регулярные отчеты о состоянии информационной безопасности.
3. **Журнал проверок регуляторов**
   * Учет всех проверок и предписаний государственных органов.
4. **Акты выполнения предписаний регуляторов**
   * Документы, подтверждающие устранение нарушений.

**VIII. Документы по физической безопасности**

1. **Положение о защите серверных помещений**
   * Правила физической защиты серверов и оборудования.
2. **Журнал учета физического доступа в серверные помещения**
   * Учет сотрудников и посетителей, имеющих доступ.

**IX. Расширенные документы**

1. **Программа импортозамещения ПО и оборудования**
   * План перехода на отечественные технологии.
2. **Методика оценки эффективности мер ИБ**
   * Определяет показатели эффективности системы защиты.
3. **Отчетность о достижении показателей эффективности**
   * Анализ выполненных мероприятий и их результатов.
4. **План действий при чрезвычайных ситуациях (Disaster Recovery Plan)**
   * Мероприятия по восстановлению работы после катастрофических событий.

**Итог**

**Всего: 37 документов**. Этот перечень покрывает организационные, технические и процедурные аспекты выполнения требований Указа № 400 и обеспечения информационной безопасности. Если требуется помощь в разработке конкретных документов, обращайтесь!