**I. Общие требования информационной безопасности для муниципального управления**

**Таблица требований**

| **Источник (НПА)** | **Формулировка требования** | **Состояние выполнения** |
| --- | --- | --- |
| **ФЗ-152** | Обеспечение конфиденциальности и защиты персональных данных (шифрование, контроль доступа). | Частично выполняется |
| **ФЗ-152, Приказ ФСТЭК №239** | Регулярный аудит ПДн, назначение ответственного за обработку. | Частично выполняется |
| **ФЗ-187** | Категорирование объектов КИИ (АСУГТ). | Выполняется |
| **Приказ ФСТЭК №235** | Создание систем безопасности для значимых объектов (АСУГТ). | Не выполняется |
| **Приказ ФСБ №282** | Информирование о компьютерных инцидентах. | Не выполняется |
| **Приказ ФСТЭК №17** | Использование сертифицированных средств защиты информации (СЗИ). | Не выполняется |
| **ГОСТ Р 56939-2016** | Внедрение системы управления информационной безопасностью (СУИБ). | Не выполняется |
| **Приказ ФСТЭК №21** | Регулярное обновление ПО и устранение уязвимостей. | Выполняется (с задержками) |
| **Постановление Правительства РФ №743** | Подготовка резервных каналов связи для КИИ. | Частично выполняется |
| **ФЗ-152, Приказ ФСТЭК №17** | Резервное копирование данных. | Не выполняется |
| **Приказ ФСТЭК №31** | Разграничение прав доступа на основе ролевой модели. | Выполняется (базовая настройка) |
| **Приказ ФСТЭК №239** | Шифрование данных и двухфакторная аутентификация (для ЭПГ). | Выполняется |

**II. План реализации мер информационной безопасности**

**Таблица плана**

| **Требование** | **Планируемый способ выполнения** | **Источники требований к мерам** | **Сроки реализации** |
| --- | --- | --- | --- |
| **Создание систем безопасности для АСУГТ (Приказ ФСТЭК №235)** | *Технические меры*: Внедрение SIEM-системы (Solar JSOC). | Приказ ФСТЭК №235, ГОСТ Р ИСО/МЭК 27001 | 6 месяцев |
| **Информирование о компьютерных инцидентах (Приказ ФСБ №282)** | *Организационные меры*: Разработка регламента. *Технические*: Интеграция с системами ФСБ. | Приказ ФСБ №282, РД ФСТЭК | 3 месяца |
| **Использование сертифицированных СЗИ (Приказ ФСТЭК №17)** | *Технические меры*: Закупка сертифицированных межсетевых экранов и антивирусов («Киберпротект»). | Реестр сертифицированных СЗИ (ФСТЭК) | 4 месяца |
| **Внедрение СУИБ (ГОСТ Р 56939-2016)** | *Оргмеры*: Разработка политики ИБ. *Технические*: Внедрение SIEM (Solaris). | ГОСТ Р ИСО/МЭК 27001, типовые модели ФСТЭК | 1 год |
| **Резервное копирование данных (ФЗ-152, Приказ ФСТЭК №17)** | *Технические меры*: Настройка автоматического резервного копирования с шифрованием. | РД ФСТЭК, ГОСТ Р 56939-2016 | 2 месяца |
| **Шифрование ПДн (ФЗ-152)** | *Технические меры*: Внедрение сертифицированных СКЗИ («КриптоПро»). | ГОСТ Р 57580.1-2017, Приказ ФСТЭК №239 | 5 месяцев |
| **Регулярный аудит ПДн (ФЗ-152)** | *Организационные меры*: Проведение независимого аудита. | ГОСТ Р 57580-2017, Роскомнадзор №08-04/2018 | Ежегодно |
| **Подготовка резервных каналов связи (Постановление №743)** | *Технические меры*: Организация резервных каналов, тестирование отказоустойчивости. | Постановление Правительства РФ №743 | 3 месяца |
| **Обучение персонала (Приказ ФСТЭК №17)** | *Организационные меры*: Проведение тренингов по ИБ. | Методические рекомендации ФСТЭК | Ежеквартально |
| **Защита от DDoS-атак (ФЗ-187)** | *Технические меры*: Внедрение NGFW. *Организационные*: Пентестинг. | ГОСТ Р 56939-2016, рекомендации ФСТЭК | 4 месяца |