Анализ требований НПА для ИСПДн муниципалитета поселка

# Система электронной приемки граждан

* 1. **Перечень требований НПА**

|  |  |  |
| --- | --- | --- |
| **Источник (НПА)** | **Формулировка требования** | **Состояние выполнения** |
| ФЗ-152 “О  персональных данных” | Назначение ответственного за обработку ПДн | Выполняется |
| Приказ ФСТЭК №17 | Проведение классификации ИСПДн | Не выполняется |
| Приказ ФСТЭК №17 | Разработка политики безопасности | Выполняется |
| ФЗ-152 | Информирование субъектов ПДн о целях обработки | Выполняется |
| Приказ ФСТЭК №17 | Регулярный аудит безопасности | Не выполняется |
| ФЗ-152 | Получение согласия на обработку ПДн | Выполняется |
| Приказ ФСТЭК №17 | Ограничение доступа к ПДн | Частично выполняется |
| ФЗ-152 | Обеспечение права субъектов на доступ к своим ПДн | Частично выполняется |
| Приказ ФСТЭК №17 | Защита от несанкционированного доступа | Частично выполняется |
| ФЗ-152 | Уведомление Роскомнадзора об обработке ПДн | Выполняется |
| Приказ ФСТЭК №17 | Резервное копирование данных | Не выполняется |

* 1. **План выполнения требований**

|  |  |  |
| --- | --- | --- |
| **Требование** | **Способ выполнения** | **Источники требований** |
| Классификация ИСПДн | Проведение оценки угроз и рисков, составление акта классификации | ГОСТ Р ИСО/МЭК 27005- 2010 |
| Аудит безопасности | Привлечение аккредитованной организации для проведения | Федеральный закон №187- ФЗ |

|  |  |  |
| --- | --- | --- |
| **Требование** | **Способ выполнения** | **Источники требований** |
|  | аудита |  |
| Ограничение доступа | Внедрение системы  разграничения доступа на основе ролей | ГОСТ Р ИСО/МЭК 27001- 2021 |
| Резервное копирование | Настройка автоматического резервного копирования с хранением копий | РД ФСТЭК |
| Защита от НСД | Установка межсетевого экрана, антивирусной защиты | Реестр сертифицированных средств защиты |

# База данных жителей поселка

* 1. **Перечень требований НПА**

|  |  |  |
| --- | --- | --- |
| **Источник (НПА)** | **Формулировка требования** | **Состояние выполнения** |
| ФЗ-152 | Обеспечение конфиденциальности ПДн | Частично выполняется |
| Приказ ФСТЭК  №17 | Применение средств защиты информации | Частично выполняется |
| ФЗ-152 | Хранение ПДн в течение установленного срока | Выполняется |
| Приказ ФСТЭК  №17 | Регулярное обучение персонала | Не выполняется |
| ФЗ-152 | Уведомление Роскомнадзора об обработке ПДн | Выполняется |
| Приказ ФСТЭК  №17 | Физическая защита помещений | Частично выполняется |
| ФЗ-152 | Уничтожение ПДн при прекращении обработки | Не выполняется |
| Приказ ФСТЭК  №17 | Контроль доступа в информационные системы | Частично выполняется |
| ФЗ-152 | Обеспечение безопасности при передаче ПДн | Частично выполняется |
| Приказ ФСТЭК  №17 | Защита от вредоносного ПО | Частично выполняется |

* 1. **План выполнения требований**

|  |  |  |
| --- | --- | --- |
| **Требование** | **Способ выполнения** | **Источники требований** |
| Конфиденциальность | Внедрение системы разграничения доступа, шифрование данных | ГОСТ 34.10-2018 |
| Средства защиты | Установка сертифицированных межсетевых экранов и антивирусов | Реестр сертифицированных средств защиты |
| Обучение персонала | Организация регулярных тренингов по ИБ | Методические рекомендации ФСТЭК |
| Физическая защита | Установка систем контроля и управления доступом | ГОСТ Р 51241-2008 |
| Уничтожение данных | Внедрение специализированного ПО для безопасного уничтожения данных | РД ФСТЭК |
| Контроль доступа | Внедрение двухфакторной аутентификации | ГОСТ Р ИСО/МЭК 27001- 2021 |

# Общие рекомендации:

Провести полный аудит текущей системы защиты информации Разработать план-график внедрения недостающих мер защиты Организовать процедуру регулярного мониторинга выполнения требований Обеспечить документирование всех процессов обработки ПДн

Провести инвентаризацию всех ИСПДн в организации Разработать регламент реагирования на инциденты Организовать систему учета и контроля доступа к ПДн