**I. Перечень требований НПА в области ГИС по информационной безопасности АРМ/мест подключения**

| **Источник (НПА)** | **Формулировка требования** | **Состояние выполнения** |
| --- | --- | --- |
| **Федеральный закон № 149-ФЗ (ст. 16)** | Обеспечение защиты информации от несанкционированного доступа, уничтожения, модификации, блокирования, копирования. | Выполняется (частично) |
| **Федеральный закон № 152-ФЗ (ст. 18, 19)** | Реализация мер по защите персональных данных, включая контроль доступа и шифрование. | Не выполняется (отсутствует шифрование) |
| **Приказ ФСТЭК № 17 (п. 5.1)** | Использование сертифицированных средств защиты информации для АРМ, подключенных к ГИС. | Не выполняется (используются несертифицированные СЗИ) |
| **Приказ ФСТЭК № 21 (п. 14)** | Регулярное обновление ПО и устранение уязвимостей. | Выполняется (частично, обновления проводятся с задержками) |
| **ГОСТ Р 56939-2016** | Внедрение системы управления информационной безопасностью (СУИБ) для контроля инцидентов. | Не выполняется (СУИБ отсутствует) |
| **Приказ ФСТЭК № 31 (п. 9)** | Разграничение прав доступа к информации в ГИС на основе ролевой модели. | Выполняется (базовая настройка прав) |

**Примечание**: Требования, связанные с государственной тайной, исключены, так как муниципальное управление не обрабатывает такие данные.

**II. План выполнения невыполненных требований**

| **Требование** | **Планируемый способ выполнения** | **Источники требований к мерам** |
| --- | --- | --- |
| **Защита персональных данных (152-ФЗ, ст. 19)** | *Технические меры*: Внедрение шифрования данных при передаче и хранении. | ГОСТ Р 57580.1-2017 (шифрование), сертификация СКЗИ по ФСБ/ФСТЭК. |
| **Использование сертифицированных СЗИ (Приказ ФСТЭК № 17)** | *Технические меры*: Закупка и установка сертифицированных межсетевых экранов и антивирусов (например, «Киберпротект»). | Приказ ФСТЭК № 17, Реестр сертифицированных СЗИ (ФСТЭК). |
| **Внедрение СУИБ (ГОСТ Р 56939-2016)** | *Организационные меры*: Разработка политики ИБ, обучение сотрудников. *Технические меры*: Внедрение SIEM-системы. | ГОСТ Р ИСО/МЭК 27001-2022, типовые модели ФСТЭК. |
| **Регулярное обновление ПО (Приказ ФСТЭК № 21)** | *Организационные меры*: Утверждение графика обновлений. *Технические меры*: Настройка автоматических обновлений. | Приказ ФСТЭК № 21, ГОСТ Р 56939-2016. |

**Пояснения:**

1. **Исключенные требования**:
   * Требования к системам с гос. тайной (например, Приказ ФСБ № 378).
   * Требования к критической информационной инфраструктуре (если муниципальный транспорт не относится к КИИ).
2. **Ключевые меры**:
   * Для шифрования данных требуется использовать сертифицированные СКЗИ (например, «КриптоПро»).
   * Внедрение SIEM-системы (например, Solaris) для аудита и анализа событий безопасности.
   * Проведение оценки соответствия ГИС требованиям ФСТЭК (раз в 3 года).
3. **Сроки**:
   * Закупка СЗИ: 6 месяцев.
   * Обучение сотрудников: ежеквартально.
   * Внедрение СУИБ: 1 год.