**Прототип штатного расписания отдела информационной безопасности**

**1. Глава отдела информационной безопасности**

Наименование должности: Глава отдела информационной безопасности

Квалификационные требования:

1. Высшее образование в области информационных технологий, информационной безопасности или смежных областях.
2. Опыт работы в сфере информационной безопасности не менее 5 лет.
3. Знание международных стандартов ISO/IEC 27000, российского законодательства (ФЗ № 149-ФЗ, ФЗ № 152-ФЗ, ФЗ № 187-ФЗ).
4. Сертификаты в области информационной безопасности (например, CISSP, CISM, ISO 27001 Lead Auditor).
5. Навыки управления командой и проектами.

Должностные обязанности:

1. Разработка и контроль выполнения политики информационной безопасности.
2. Организация и координация работы отдела по защите информации.
3. Управление инцидентами информационной безопасности (выявление, локализация, устранение последствий).
4. Взаимодействие с руководством муниципалитета по вопросам ИБ.
5. Проведение аудитов и проверок на соответствие требованиям законодательства и стандартов.
6. Разработка и актуализация нормативных документов по ИБ.
7. Организация обучения сотрудников по вопросам информационной безопасности.
8. Контроль за выполнением мер по защите персональных данных и критической информационной инфраструктуры (КИИ).

**2. Специалист по информационной безопасности**

Наименование должности: Специалист по информационной безопасности

Квалификационные требования:

1. Высшее образование в области информационных технологий, информационной безопасности или смежных областях.
2. Опыт работы в сфере информационной безопасности не менее 3 лет.
3. Знание основ защиты персональных данных (ФЗ № 152-ФЗ), требований к КИИ (ФЗ № 187-ФЗ).
4. Навыки работы с системами защиты информации (антивирусы, межсетевые экраны, IDS/IPS).
5. Знание СУБД (MySQL, PostgreSQL) и основ шифрования данных.
6. Сертификаты в области информационной безопасности (например, CEH, CompTIA Security+).

Должностные обязанности:

1. Мониторинг и анализ угроз информационной безопасности.
2. Настройка и поддержка систем защиты информации (антивирусы, межсетевые экраны, системы обнаружения вторжений).
3. Проведение резервного копирования данных и восстановление после сбоев.
4. Контроль за обработкой и защитой персональных данных сотрудников и граждан.
5. Устранение уязвимостей в информационных системах.
6. Проведение аудитов безопасности и тестирования на проникновение.
7. Обучение сотрудников по вопросам информационной безопасности.
8. Поддержка работоспособности систем шифрования данных.
9. Обеспечение защиты от DDoS-атак и других киберугроз.
10. Мониторинг и защита критической информационной инфраструктуры (КИИ).

**Распределение обязанностей между должностями**

Глава отдела информационной безопасности**:**

1. Стратегическое планирование и управление.
2. Координация работы специалиста.
3. Взаимодействие с руководством и внешними организациями.
4. Контроль за выполнением политики безопасности.
5. Проведение аудитов и отчетность.

Специалист по информационной безопасности**:**

1. Оперативная работа по защите информации.
2. Настройка и поддержка технических средств защиты.
3. Мониторинг угроз и реагирование на инциденты.
4. Обучение сотрудников и контроль за обработкой ПДн.
5. Поддержка защиты КИИ.