**Штатное расписание отдела информационной безопасности**

**(прототип)**

**1. Начальник отдела информационной безопасности**

* **Наименование**: Начальник отдела информационной безопасности
* **Квалификационные требования**:
  + Высшее образование в области информационной безопасности, информационных технологий или смежных областях.
  + Опыт работы в сфере ИБ не менее 5 лет.
  + Знание нормативно-правовых актов (Федеральный закон № 152-ФЗ "О персональных данных", ГОСТ Р 57580, ISO/IEC 27001 и др.).
  + Наличие сертификатов CISSP, CISM или аналогичных.
  + Навыки управления командой и проектами.
* **Должностные обязанности**:
  + Организация и управление работой отдела ИБ.
  + Разработка и внедрение политик и процедур информационной безопасности.
  + Контроль выполнения требований законодательства и стандартов ИБ.
  + Координация реагирования на инциденты информационной безопасности.
  + Взаимодействие с внешними аудиторами и регуляторами.
  + Подготовка отчетов для руководства компании.

**2. Старший специалист по информационной безопасности**

* **Наименование**: Старший специалист по информационной безопасности.
* **Квалификационные требования**:
  + Высшее образование в области ИБ, ИТ или смежных областях.
  + Опыт работы в сфере ИБ не менее 3 лет.
  + Знание стандартов и frameworks (ISO/IEC 27001, NIST, PCI DSS).
  + Наличие сертификатов CEH, CompTIA Security+ или аналогичных.
  + Навыки работы с системами защиты информации (SIEM, DLP, IDS/IPS).
* **Должностные обязанности**:
  + Анализ и оценка рисков информационной безопасности.
  + Разработка и внедрение мер защиты информации.
  + Мониторинг и анализ событий безопасности.
  + Проведение аудитов и тестирования на проникновение.
  + Обучение сотрудников компании по вопросам ИБ.

**3. Специалист по защите персональных данных**

* **Наименование**: Специалист по защите персональных данных.
* **Квалификационные требования**:
  + Высшее образование в области ИБ, юриспруденции или смежных областях.
  + Опыт работы в сфере защиты персональных данных не менее 2 лет.
  + Знание Федерального закона № 152-ФЗ и сопутствующих нормативных актов.
  + Навыки работы с системами защиты персональных данных.
* **Должностные обязанности**:
  + Обеспечение соответствия обработки персональных данных требованиям законодательства.
  + Разработка и актуализация документов по защите персональных данных.
  + Проведение внутренних аудитов.
  + Взаимодействие с Роскомнадзором и другими регуляторами.
  + Консультирование сотрудников по вопросам защиты персональных данных.

**4. Инженер по безопасности сетей**

* **Наименование**: Инженер по безопасности сетей.
* **Квалификационные требования**:
  + Высшее образование в области ИТ или ИБ.
  + Опыт работы в сфере сетевой безопасности не менее 2 лет.
  + Знание сетевых протоколов и технологий (TCP/IP, VPN, Firewall, IDS/IPS).
  + Наличие сертификатов CCNA Security, CCNP Security или аналогичных.
* **Должностные обязанности**:
  + Настройка и поддержка сетевых средств защиты (брандмауэры, VPN, IDS/IPS).
  + Мониторинг сетевой активности на предмет угроз.
  + Расследование инцидентов сетевой безопасности.
  + Разработка и внедрение мер по защите сетевой инфраструктуры.

**5. Аналитик по кибербезопасности**

* **Наименование**: Аналитик по кибербезопасности.
* **Квалификационные требования**:
  + Высшее образование в области ИБ, ИТ или смежных областях.
  + Опыт работы в сфере анализа угроз не менее 2 лет.
  + Знание методов анализа угроз и уязвимостей.
  + Навыки работы с SIEM-системами (Splunk, QRadar, ArcSight).
* **Должностные обязанности**:
  + Анализ угроз и уязвимостей.
  + Мониторинг и анализ событий безопасности.
  + Подготовка отчетов по инцидентам ИБ.
  + Разработка рекомендаций по устранению уязвимостей.

**6. Специалист по реагированию на инциденты**

* **Наименование**: Специалист по реагированию на инциденты.
* **Квалификационные требования**:
  + Высшее образование в области ИБ, ИТ или смежных областях.
  + Опыт работы в сфере реагирования на инциденты не менее 2 лет.
  + Знание методологий реагирования на инциденты (NIST SP 800-61, ISO/IEC 27035).
  + Навыки работы с инструментами анализа (Forensic Tools, SIEM).
* **Должностные обязанности**:
  + Расследование инцидентов информационной безопасности.
  + Разработка и внедрение планов реагирования на инциденты.
  + Восстановление работоспособности систем после инцидентов.
  + Подготовка отчетов и рекомендаций по предотвращению инцидентов.

**7. Администратор средств защиты информации**

* **Наименование**: Администратор средств защиты информации.
* **Квалификационные требования**:
  + Высшее образование в области ИТ или ИБ.
  + Опыт работы с системами защиты информации (DLP, антивирусы, SIEM).
  + Знание принципов работы средств криптографической защиты.
* **Должностные обязанности**:
  + Установка и настройка средств защиты информации.
  + Обновление и поддержка антивирусного ПО.
  + Мониторинг работы систем защиты.
  + Обеспечение резервного копирования данных.