**Определение задач для каждой роли в организации, связанной с информационной безопасностью**

**I. Стратегические роли**

**1. Директор по информационной безопасности (CISO)**

* **Функции**:
  + Разработка стратегии информационной безопасности (ИБ).
  + Внедрение политики безопасности на уровне всей организации.
  + Координация работы подразделений, связанных с ИБ.
* **Задачи**:
  + Определить ключевые риски в области ИБ.
  + Контролировать соответствие законодательства и стандартам (ФЗ-152, ISO 27001).
  + Отчитываться перед высшим руководством о состоянии ИБ.

**2. Менеджер по информационной безопасности**

* **Функции**:
  + Организация выполнения политики ИБ.
  + Обучение сотрудников.
* **Задачи**:
  + Разработать инструкции и процедуры по ИБ.
  + Координировать работу сотрудников, связанных с ИБ.

**II. Технические роли**

**3. Инженер по информационной безопасности**

* **Функции**:
  + Настройка и управление техническими средствами защиты.
* **Задачи**:
  + Установка и настройка межсетевых экранов, IDS/IPS.
  + Реализация защиты данных (шифрование, резервное копирование).

**4. Сетевой инженер по безопасности**

* **Функции**:
  + Обеспечение безопасности сетевой инфраструктуры.
* **Задачи**:
  + Настройка VPN, защитных шлюзов.
  + Мониторинг сетевого трафика для выявления угроз.

**5. Специалист по криптографии**

* **Функции**:
  + Внедрение и поддержка средств криптографической защиты.
* **Задачи**:
  + Обеспечение шифрования данных.
  + Управление ключами шифрования.

**III. Оперативные роли**

**6. Аналитик SOC (оператор центра мониторинга безопасности)**

* **Функции**:
  + Мониторинг событий безопасности.
* **Задачи**:
  + Анализ событий в SIEM.
  + Выявление аномалий и угроз.

**7. Специалист по реагированию на инциденты**

* **Функции**:
  + Реакция на кибератаки и инциденты.
* **Задачи**:
  + Разработка плана реагирования.
  + Устранение последствий инцидентов.

**8. Специалист по управлению доступом (IAM Specialist)**

* **Функции**:
  + Контроль доступа пользователей.
* **Задачи**:
  + Управление учетными записями.
  + Регулярная проверка прав доступа.

**IV. Роли в области аудита и соответствия**

**9. Аудитор по информационной безопасности**

* **Функции**:
  + Проверка соблюдения требований стандартов и законодательства.
* **Задачи**:
  + Проведение регулярных проверок.
  + Формирование отчетов о выявленных несоответствиях.

**10. Специалист по соответствию (Compliance Specialist)**

* **Функции**:
  + Контроль выполнения требований нормативов.
* **Задачи**:
  + Проверка соответствия ФЗ-152, ФЗ-187, ISO/IEC.
  + Разработка рекомендаций по устранению нарушений.

**V. Роли в области тестирования и анализа**

**11. Пентестер (Penetration Tester)**

* **Функции**:
  + Тестирование систем на наличие уязвимостей.
* **Задачи**:
  + Проведение тестов на проникновение.
  + Документирование обнаруженных уязвимостей.

**12. Форензик-аналитик**

* **Функции**:
  + Расследование цифровых инцидентов.
* **Задачи**:
  + Анализ цифровых следов атак.
  + Восстановление данных и построение временной линии событий.

**VI. Обучение и поддержка**

**13. Тренер по информационной безопасности**

* **Функции**:
  + Обучение сотрудников.
* **Задачи**:
  + Проведение семинаров и тренингов.
  + Разработка обучающих материалов.

**14. Менеджер по рискам**

* **Функции**:
  + Управление рисками ИБ.
* **Задачи**:
  + Оценка вероятности инцидентов.
  + Формирование плана по минимизации рисков.

**VII. Поддерживающие роли**

**15. Системный администратор с функциями ИБ**

* **Функции**:
  + Администрирование серверов и сетей.
* **Задачи**:
  + Настройка серверов в соответствии с требованиями ИБ.
  + Контроль резервного копирования данных.

**16. Архивариус данных**

* **Функции**:
  + Управление архивами информации.
* **Задачи**:
  + Обеспечение безопасного хранения данных.

**VIII. Общие задачи для всех ролей**

1. Обеспечение соблюдения законодательных и нормативных требований.
2. Снижение рисков утечки данных и сбоев систем.
3. Повышение осведомленности сотрудников об угрозах ИБ.

Эти функции и задачи помогут определить, как организовать работу GPT-агента для каждой роли и бизнеса в целом.

4o

**Вы сказали:**

добавь проектировщика информационной безопасности

**ChatGPT сказал:**

ChatGPT

**Роль: Проектировщик информационной безопасности**

**Функции:**

1. **Разработка архитектуры систем ИБ**:
   * Создание архитектуры информационных систем с учетом требований безопасности.
   * Определение технических и организационных мер защиты информации.
2. **Интеграция безопасности в процессы проектирования**:
   * Внедрение принципов "безопасность по умолчанию" и "безопасность с самого начала" (Security by Design).
   * Учет требований законодательства (ФЗ-152, ФЗ-187) и стандартов (ГОСТ, ISO 27001) на этапе проектирования.
3. **Подбор технических решений**:
   * Выбор и обоснование использования средств защиты (межсетевые экраны, системы шифрования, IDS/IPS).
   * Оптимизация затрат на безопасность при сохранении высокого уровня защиты.
4. **Оценка рисков проектируемой системы**:
   * Анализ потенциальных угроз и уязвимостей архитектуры системы.
   * Рекомендации по минимизации рисков на этапе проектирования.
5. **Сопровождение внедрения**:
   * Контроль реализации проектных решений.
   * Тестирование систем после внедрения для проверки их соответствия требованиям безопасности.