1. Анализ основных угроз информационной безопасности в компании/организации. Рассмотрите различные виды угроз, такие как взломы, фишинг, DoS-атаки и т.д., и опишите, какие меры безопасности можно применить для предотвращения таких угроз.

2. Изучение методов криптографии и их применение в информационной безопасности. Рассмотрите различные алгоритмы шифрования, такие как AES, RSA, и описывающие их принципы работы. Также рассмотрите примеры применения криптографии в реальном мире.

3. Исследование техник обнаружения и предотвращения вторжений (Intrusion Detection and Prevention Systems, IDS/IPS). Изучите различные методы обнаружения и предотвращения атак, такие как подписей, эвристические методы и анализ поведения. Опишите, как эти системы могут быть настроены для эффективного обнаружения и предотвращения атак.

4. Анализ социальной инженерии и ее влияния на информационную безопасность. Рассмотрите различные методы использования социальной инженерии для получения несанкционированного доступа к информации. Опишите, какие меры могут быть приняты для предотвращения таких атак.

5. Изучение методов обеспечения безопасности на сетевом уровне. Рассмотрите различные технологии, такие как фаерволлы, виртуальные частные сети (VPN) и безопасные протоколы передачи данных (HTTPS), и описывающие их механизмы безопасности.