**1. Специалист по информационной безопасности (ИБ):**

* Основной профессионал, отвечающий за защиту информации в организации, разрабатывающий и внедряющий политику безопасности данных.

**2. Аналитик информационной безопасности:**

* Занимается анализом угроз, уязвимостей и разработкой рекомендаций по их устранению.

**3. Операционный аналитик кибербезопасности (SOC Analyst):**

* Работает в центре управления безопасностью (SOC), занимается мониторингом событий, реагированием на инциденты.

**4. Специалист по киберразведке (Threat Intelligence Analyst):**

* Анализирует данные о киберугрозах и предоставляет информацию о возможных атаках для предотвращения инцидентов.

**5. Пенетратор (Pentester):**

* Осуществляет тестирование на проникновение, выявляя уязвимости в системах безопасности через симулированные атаки.

**6. Инженер по безопасности сетей (Network Security Engineer):**

* Защищает сетевые инфраструктуры, внедряя брандмауэры, системы обнаружения и предотвращения атак, VPN и другие технологии.

**7. Аудитор информационной безопасности:**

* Проводит аудит систем безопасности, выявляет несоответствия и уязвимости, делает отчеты и рекомендации по улучшению защиты.

**8. Офицер по информационной безопасности (CISO – Chief Information Security Officer):**

* Руководитель службы ИБ, отвечающий за разработку и реализацию стратегии безопасности в компании.

**9. Инженер по безопасности приложений (Application Security Engineer):**

* Занимается защитой программного обеспечения от уязвимостей, работает с разработчиками для интеграции безопасности в процессе разработки.

**10. Криптограф:**

* Специалист по шифрованию и защите данных через криптографические методы, использует сложные математические модели для защиты информации.

**11. Инженер по безопасности облачных систем (Cloud Security Engineer):**

* Отвечает за защиту данных и сервисов, расположенных в облачных инфраструктурах (например, AWS, Azure).

**12. Специалист по управлению инцидентами:**

* Организует работу при возникновении инцидентов безопасности, разрабатывает планы по реагированию и минимизации последствий.

**13. Специалист по управлению доступом (Identity and Access Management - IAM):**

* Обеспечивает правильное управление правами доступа сотрудников к информационным системам и данным.

**14. Разработчик защитных решений (Security Software Developer):**

* Разрабатывает и поддерживает программные решения для защиты информации, такие как антивирусы, системы шифрования.

**15. Форензик-аналитик (Digital Forensic Analyst):**

* Специалист по расследованию киберпреступлений, занимается анализом данных, восстановлением информации и поиском источников атак.

**16. Консультант по информационной безопасности:**

* Консультирует компании по вопросам построения систем безопасности, предоставляет рекомендации и помогает внедрять решения.

**17. Оценщик рисков (Risk Assessor):**

* Оценивает возможные риски, связанные с информационной безопасностью, разрабатывает методы минимизации этих рисков.

**18. Эксперт по защите данных (Data Protection Officer - DPO):**

* Специалист, отвечающий за соответствие компании нормам защиты данных (например, GDPR).

**19. Администратор безопасности баз данных (Database Security Administrator):**

* Отвечает за защиту баз данных, управление доступом к данным, предотвращение их утечек.

**20. Архитектор информационной безопасности:**

* Разрабатывает стратегические и технические решения для построения безопасной ИТ-инфраструктуры компании.