**Распределение обязанностей по чек-листу на роли в отделе информационной безопасности и руководителя организации**

**I. Роль: Руководитель организации**

**Основные задачи:**

1. **Назначение ответственных лиц:**
   * Назначить заместителя руководителя, ответственного за информационную безопасность.
   * Утвердить создание подразделения ИБ или возложить функции на существующее.
   * Утвердить основные политики и положения по ИБ.
2. **Контроль выполнения требований:**
   * Утверждать планы мероприятий по ИБ и контролировать их выполнение.
   * Получать регулярные отчёты о состоянии ИБ.
3. **Работа с государственными органами:**
   * Организовать взаимодействие с ФСБ, ФСТЭК, ГосСОПКА.
   * Утверждать отчёты для передачи в надзорные органы.
4. **Ресурсное обеспечение:**
   * Обеспечить финансирование мероприятий по ИБ.
   * Поддерживать обновление технологий и обучение сотрудников.

**II. Роль: Заместитель руководителя по ИБ**

**Основные задачи:**

1. **Руководство подразделением ИБ:**
   * Координировать деятельность сотрудников подразделения ИБ.
   * Утверждать регламенты, процедуры и планы работы.
2. **Мониторинг и контроль:**
   * Контролировать выполнение мер защиты информации.
   * Анализировать отчёты об инцидентах и результатах аудитов.
3. **Реализация политики ИБ:**
   * Обеспечивать внедрение утверждённой руководителем политики ИБ.
   * Следить за выполнением обязательств перед государственными органами.
4. **Взаимодействие с внешними организациями:**
   * Участвовать в проверках ФСБ и ФСТЭК.
   * Контролировать деятельность подрядчиков.

**III. Роль: Руководитель подразделения информационной безопасности**

**Основные задачи:**

1. **Разработка внутренней документации:**
   * Разработать политики, регламенты и инструкции по ИБ.
   * Обновлять документы в соответствии с изменениями законодательства.
2. **Организация мониторинга:**
   * Настроить системы мониторинга (SIEM, UBA).
   * Организовать регулярный сбор данных о событиях безопасности.
3. **Управление инцидентами:**
   * Разработать сценарии реагирования на инциденты.
   * Координировать действия сотрудников при устранении инцидентов.
4. **Работа с рисками:**
   * Проводить регулярную оценку рисков.
   * Вносить изменения в планы защиты на основании результатов анализа.

**IV. Роль: Специалист по мониторингу и реагированию**

**Основные задачи:**

1. **Мониторинг событий безопасности:**
   * Настроить и управлять SIEM-системами.
   * Проводить анализ логов и выявлять аномалии.
2. **Реагирование на инциденты:**
   * Следовать утверждённым сценариям реагирования.
   * Документировать действия по устранению инцидентов и их последствия.
3. **Взаимодействие с ГосСОПКА:**
   * Передавать данные о выявленных инцидентах в аккредитованные центры.
   * Обеспечивать выполнение требований ГосСОПКА.

**V. Роль: Специалист по технической защите информации**

**Основные задачи:**

1. **Установка и настройка средств защиты:**
   * Настроить межсетевые экраны, DLP, антивирусные и криптографические системы.
   * Обеспечить резервное копирование и восстановление данных.
2. **Контроль технической инфраструктуры:**
   * Проводить регулярное тестирование на уязвимости.
   * Вести журнал событий информационной безопасности.
3. **Переход на отечественные технологии:**
   * Реализовать план поэтапной замены иностранных средств на отечественные.
   * Проверить совместимость новых решений.

**VI. Роль: Специалист по обучению и работе с персоналом**

**Основные задачи:**

1. **Организация инструктажей:**
   * Проводить обучение новых сотрудников правилам ИБ.
   * Разрабатывать памятки по предотвращению инцидентов (фишинг, социальная инженерия).
2. **Оценка компетенций:**
   * Проводить тестирование знаний сотрудников.
   * Организовывать учебные тревоги и тренировки.
3. **Мотивация сотрудников:**
   * Разрабатывать и внедрять программы поощрения за соблюдение ИБ.
   * Анализировать результаты участия сотрудников в учениях.

**VII. Роль: Специалист по работе с подрядчиками**

**Основные задачи:**

1. **Контроль подрядчиков:**
   * Проверять выполнение подрядчиками требований по защите информации.
   * Вести документацию о взаимодействии с подрядчиками.
2. **Заключение соглашений:**
   * Подготавливать договоры, включающие требования по ИБ.
   * Контролировать выполнение обязательств подрядчиками.

**VIII. Итоговые метрики и отчетность**

**Руководитель организации:**

* Получение итоговых отчётов о состоянии ИБ.
* Принятие стратегических решений по ресурсам и модернизации.

**Заместитель руководителя по ИБ:**

* Анализ эффективности подразделения.
* Формирование предложений по улучшению мер защиты.

**Руководитель подразделения ИБ и сотрудники:**

* Предоставление метрик и аналитических данных (количество инцидентов, время на реагирование, статус обновления ПО).
* Участие в разработке новых инициатив и планов.

**Распределение обязанностей позволяет обеспечить системный подход к выполнению требований, снизить риски и повысить уровень защищённости организации. Если нужно детализировать какую-либо роль, сообщите!**