**Алгоритм работы специалиста по информационной безопасности в организации в соответствии с ФЗ № 390-ФЗ "О безопасности"**

**1. Подготовительный этап**

1. **Изучение нормативных требований**:
   * Ознакомиться с положениями ФЗ № 390-ФЗ, другими профильными законами (например, ФЗ № 187-ФЗ, ФЗ № 152-ФЗ) и внутренними стандартами организации.
   * Определить требования, относящиеся к специфике организации (например, критическая информационная инфраструктура, государственная тайна).
2. **Анализ текущего состояния безопасности**:
   * Провести аудит существующей системы безопасности.
   * Составить перечень объектов защиты (информационные системы, помещения, сотрудники, оборудование).
3. **Идентификация угроз**:
   * Разработать модель угроз, исходя из анализа инфраструктуры и внешних факторов.
   * Определить вероятные риски и сценарии атак.

**2. Разработка и внедрение мер безопасности**

1. **Создание системы организационных мер**:
   * Разработать и утвердить Политику безопасности организации.
   * Подготовить внутренние документы: инструкции, планы мероприятий, регламенты, модели угроз.
2. **Назначение ответственных лиц**:
   * Утвердить приказ о назначении ответственных за различные аспекты безопасности (физическая, информационная, экономическая).
3. **Интеграция технических мер**:
   * Настроить системы мониторинга и предотвращения инцидентов (IDS/IPS, SIEM).
   * Установить системы резервного копирования и шифрования данных.
4. **Физическая защита объектов**:
   * Организовать контроль доступа на территорию и в помещения.
   * Установить системы видеонаблюдения, сигнализации, пожарной безопасности.

**3. Обучение и работа с персоналом**

1. **Проведение инструктажей и обучения**:
   * Ознакомить сотрудников с правилами безопасности, обязанностями и мерами ответственности.
   * Организовать обучение по действиям в чрезвычайных ситуациях и при инцидентах.
2. **Актуализация знаний сотрудников**:
   * Проводить регулярные тестирования и обновление инструкций.
   * Информировать о новых угрозах и изменениях в политике безопасности.

**4. Мониторинг и реагирование**

1. **Постоянный мониторинг безопасности**:
   * Вести наблюдение за состоянием объектов безопасности и анализировать логи систем.
   * Оперативно выявлять и фиксировать инциденты.
2. **Реагирование на инциденты**:
   * Разработать и утвердить план реагирования на инциденты.
   * При выявлении инцидента — следовать утвержденному протоколу:
     + Изоляция объекта.
     + Устранение угрозы.
     + Документирование инцидента.
3. **Уведомление о критических инцидентах**:
   * В случае необходимости информировать руководство и уполномоченные органы (например, Роскомнадзор, ФСТЭК, ФСБ).

**5. Управление рисками**

1. **Проведение оценки рисков**:
   * Регулярно анализировать текущие риски и их влияние на деятельность организации.
   * Обновлять реестр рисков и определять меры по их минимизации.
2. **Разработка плана управления рисками**:
   * Определить приоритетные направления и ресурсы для устранения выявленных рисков.
   * Внедрить меры по снижению уязвимостей (например, обновление ПО, усиление контроля доступа).

**6. Документооборот и отчетность**

1. **Ведение документации**:
   * Составлять и обновлять следующие документы:
     + Политики и инструкции.
     + Журнал инцидентов безопасности.
     + Акты проверок и аудитов.
   * Утверждать документы руководством.
2. **Отчетность и взаимодействие с органами**:
   * Готовить отчеты для руководства о состоянии безопасности.
   * Своевременно предоставлять информацию контролирующим органам.

**7. Регулярный аудит и улучшение**

1. **Проведение внутренних проверок**:
   * Оценивать эффективность мер безопасности.
   * Проверять соответствие системы безопасности требованиям законодательства и внутренних документов.
2. **Привлечение внешних экспертов**:
   * При необходимости организовать независимый аудит системы безопасности.
3. **Обновление системы безопасности**:
   * Вносить изменения в меры безопасности при изменении законодательства, выявлении новых угроз или расширении инфраструктуры.

**8. Подготовка к чрезвычайным ситуациям**

1. **Тренировки и тесты**:
   * Проводить регулярные учебные тревоги для отработки действий в кризисных ситуациях.
   * Тестировать планы восстановления и антикризисного управления.
2. **Обеспечение непрерывности работы**:
   * Разработать планы восстановления после ЧС.
   * Убедиться, что критические функции организации будут восстановлены в кратчайшие сроки.

**9. Постоянное совершенствование**

1. **Обновление политики безопасности**:
   * Пересматривать Политику безопасности не реже одного раза в год или при изменении законодательства.
2. **Мониторинг законодательства**:
   * Следить за изменениями в нормативной базе и своевременно вносить корректировки в меры безопасности.

Этот алгоритм помогает специалисту по ИБ организовать системный подход к безопасности в соответствии с ФЗ № 390-ФЗ. Если нужны уточнения или конкретизация, сообщите!

**Дополнения к алгоритму работы специалиста по ИБ в соответствии с ФЗ № 390-ФЗ "О безопасности"**

**10. Интеграция безопасности в бизнес-процессы**

1. **Оценка безопасности новых проектов и инициатив**:

* Проверять все новые проекты, IT-системы и бизнес-процессы на соответствие требованиям безопасности перед запуском.
* Создавать чек-листы для оценки их безопасности.

1. **Включение безопасности в разработку**:

* Интегрировать принципы безопасной разработки (Security by Design) на всех этапах создания информационных систем.

1. **Контроль взаимодействия с контрагентами**:

* Проверять соблюдение мер безопасности при заключении контрактов с подрядчиками.
* Включать требования по безопасности в договоры и соглашения.

**11. Защита критической информационной инфраструктуры (КИИ) *(при наличии)***

1. **Категорирование объектов КИИ**:

* Проводить категорирование информационных систем в соответствии с ФЗ № 187-ФЗ.
* Утверждать акты категорирования объектов и обновлять их по мере необходимости.

1. **Взаимодействие с ГосСОПКА**:

* Настроить взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).
* Своевременно передавать информацию об инцидентах.

1. **Анализ критических зависимостей**:

* Оценивать зависимость организации от внешних систем и поставщиков услуг.
* Разрабатывать меры на случай отказа сторонних поставщиков или систем.

**12. Углубленный анализ инцидентов**

1. **Расследование инцидентов**:

* Использовать форензик-методы (digital forensic) для анализа инцидентов.
* Создавать подробные отчеты о причинах, последствиях и мерах по предотвращению повторных случаев.

1. **Автоматизация управления инцидентами**:

* Внедрять системы управления инцидентами (SOAR), чтобы ускорить обнаружение и реагирование на угрозы.

1. **Обучение на инцидентах**:

* Проводить пост-инцидентное обучение для повышения уровня готовности сотрудников.

**13. Инновационные подходы**

1. **Внедрение современных технологий защиты**:

* Рассматривать и тестировать использование ИИ и машинного обучения для предсказания угроз.
* Интегрировать блокчейн для защиты критически важных данных.

1. **Использование системы раннего предупреждения**:

* Настроить мониторинг Dark Web и других источников для выявления утечек данных.

**14. Углубленная работа с кадрами**

1. **Система внутреннего контроля сотрудников**:

* Внедрить мониторинг действий привилегированных пользователей (Privileged Access Management).
* Обеспечить проверку сотрудников, имеющих доступ к критически важным данным.

1. **Оценка лояльности сотрудников**:

* Проводить периодическую проверку сотрудников, работающих с конфиденциальной информацией.

**15. Регулярные тестирования**

1. **Тестирование резервных копий**:

* Проводить тесты восстановления данных из резервных копий для проверки их актуальности и целостности.

1. **Имитация реальных атак**:

* Проводить регулярные пентесты для оценки защищенности системы.
* Организовывать Red Team/Blue Team тренировки для подготовки команды реагирования.

1. **Тестирование антикризисного плана**:

* Ежегодно тестировать планы восстановления и реагирования на чрезвычайные ситуации.

**16. Работа с физической безопасностью**

1. **Интеграция с экстренными службами**:

* Установить контакт с местными подразделениями полиции, пожарной охраны и службами МЧС.
* Разработать протоколы совместных действий в случае ЧС.

1. **Проверка резервных путей доступа и эвакуации**:

* Убедиться в наличии и исправности всех путей эвакуации и резервного доступа.

**17. Повышение уровня безопасности**

1. **Регулярное обновление базы знаний**:

* Создавать и обновлять внутреннюю базу знаний об угрозах, инцидентах и лучших практиках.

1. **Сравнение с лучшими практиками**:

* Периодически оценивать соответствие системы безопасности международным стандартам (например, ISO/IEC 27001).

**Итоговые дополнения**

Эти пункты позволяют углубить алгоритм работы специалиста по ИБ, обеспечивая не только соответствие требованиям ФЗ-390, но и внедрение современных подходов для защиты организации от угроз. Если требуется более детальная проработка, например, инструкции или шаблоны документов, сообщите!