**Чек-лист для организации по обеспечению безопасности в соответствии с ФЗ № 390-ФЗ "О безопасности"**

**I. Организационные меры**

1. **Создание структуры обеспечения безопасности:**
   * Разработать и утвердить структуру, отвечающую за безопасность организации.
   * Назначить ответственного за реализацию мер безопасности.
2. **Разработка внутренних документов:**
   * Утвердить политику безопасности организации.
   * Составить план мероприятий по обеспечению безопасности.
   * Разработать инструкции для сотрудников, описывающие их обязанности по защите информации.
3. **Обучение персонала:**
   * Провести регулярное обучение сотрудников по вопросам безопасности.
   * Организовать тестирование сотрудников на знание процедур безопасности.

**II. Информационная безопасность**

1. **Защита информации:**
   * Обеспечить конфиденциальность, целостность и доступность информации.
   * Использовать сертифицированные средства защиты информации.
2. **Модели угроз:**
   * Разработать модель угроз, актуальную для организации.
   * Обновлять модель при изменении инфраструктуры или выявлении новых рисков.
3. **Мониторинг событий:**
   * Внедрить систему мониторинга инцидентов информационной безопасности (например, SIEM).
   * Вести журнал инцидентов для анализа и реагирования.

**III. Технические меры**

1. **Контроль доступа:**
   * Установить системы контроля и управления доступом (СКУД).
   * Ограничить доступ сотрудников только к необходимым данным и ресурсам.
2. **Резервное копирование:**
   * Настроить регулярное резервное копирование данных.
   * Проверять целостность резервных копий.
3. **Обновление инфраструктуры:**
   * Обеспечить своевременное обновление программного обеспечения и оборудования.
   * Устранять уязвимости, выявленные в системах.
4. **Физическая защита:**
   * Обеспечить контроль доступа к помещениям, где размещены критические системы.
   * Установить видеонаблюдение и системы сигнализации.

**IV. Управление рисками**

1. **Идентификация рисков:**
   * Регулярно проводить оценку рисков безопасности.
   * Создать реестр рисков с описанием угроз, их вероятности и последствий.
2. **Планирование реагирования:**
   * Разработать планы реагирования на инциденты и чрезвычайные ситуации.
   * Регулярно тестировать планы на предмет их эффективности.
3. **Меры по минимизации рисков:**
   * Реализовать технические и организационные меры для снижения вероятности реализации угроз.
   * Обеспечить страхование критически важных рисков.

**V. Взаимодействие с государственными органами**

1. **Уведомление о критических инцидентах:**
   * Наладить процесс уведомления уполномоченных органов о нарушениях безопасности (если применимо).
   * Вести учет переданных отчетов.
2. **Сотрудничество с регуляторами:**
   * Подготовить документы для взаимодействия с проверяющими органами.
   * Регулярно проверять соответствие требованиям законодательства.

**VI. Проверки и аудит**

1. **Внутренний аудит:**
   * Проводить регулярные проверки соблюдения мер безопасности.
   * Составлять отчеты о выявленных несоответствиях и мерах по их устранению.
2. **Аудит со стороны третьих лиц:**
   * Привлекать внешних экспертов для проверки соответствия стандартам безопасности.
   * Учитывать рекомендации аудита при планировании дальнейших мероприятий.

**VII. Документооборот**

1. **Ведение документации:**
   * Утвердить реестр документов по безопасности.
   * Регулярно актуализировать локальные акты, планы и политики.
2. **Хранение и уничтожение документов:**
   * Обеспечить безопасное хранение и уничтожение конфиденциальных документов.
   * Внедрить процедуры контроля за обращением с документацией.

**VIII. Отчетность и обновление**

1. **Обновление мер безопасности:**
   * Актуализировать планы и процедуры безопасности в случае изменений в законодательстве или инфраструктуре.
   * Проводить регулярные брифинги с руководством по текущему состоянию безопасности.
2. **Отчетность руководству:**
   * Составлять периодические отчеты о выполнении мероприятий по безопасности.
   * Предоставлять руководству рекомендации по улучшению систем безопасности.

Этот чек-лист поможет специалисту по ИБ организовать эффективную систему безопасности в организации в соответствии с ФЗ-390. Если нужна детальная разработка инструкций, шаблонов или другой документации, могу помочь!

**Дополнения к чек-листу по обеспечению безопасности в соответствии с ФЗ-390**

**IX. Кибербезопасность и реагирование на инциденты**

1. **Проактивная защита:**

* Внедрить системы обнаружения и предотвращения атак (IDS/IPS).
* Реализовать механизм защиты от фишинга и вредоносного ПО.

1. **Сбор и анализ логов:**

* Настроить централизованный сбор логов с ключевых систем.
* Использовать аналитику для выявления аномальной активности.

1. **План восстановления:**

* Разработать детальный план восстановления после атак.
* Периодически тестировать его реализацию.

**X. Интеграция новых технологий**

1. **Анализ новых решений:**

* Оценивать безопасность при внедрении новых технологий (облачные сервисы, IoT).
* Проводить предварительный аудит решений перед их использованием.

1. **Автоматизация процессов:**

* Внедрить системы автоматизации мониторинга и отчетности по безопасности.
* Использовать решения на базе ИИ для выявления угроз.

**XI. Комплаенс и стандарты**

1. **Сертификация:**

* При необходимости пройти сертификацию по стандартам (например, ISO/IEC 27001).
* Вести документацию, подтверждающую выполнение требований сертификации.

1. **Международные стандарты:**

* Если организация работает за рубежом, соблюдать требования международных стандартов и законов, таких как GDPR.

1. **Сопоставление с требованиями КИИ:**

* Если организация относится к критической информационной инфраструктуре (КИИ), проверить соответствие требованиям ФЗ-187.

**XII. Работа с подрядчиками и третьими лицами**

1. **Аудит подрядчиков:**

* Проверять меры безопасности подрядчиков перед заключением договора.
* Регулярно проводить аудит их соответствия установленным требованиям.

1. **Управление аутсорсингом:**

* Убедиться, что контракты с аутсорсерами включают положения о защите данных и ответственности за инциденты.

**XIII. Защита критической инфраструктуры**

1. **Обеспечение физической безопасности:**

* Установить дополнительные меры защиты для помещений с критическими системами.
* Реализовать резервные системы питания и связи.

1. **Резервирование и дублирование:**

* Настроить резервирование ключевых систем.
* Проводить регулярные тесты на отказоустойчивость.

**XIV. Культура безопасности**

1. **Мотивация сотрудников:**

* Разработать программы поощрения сотрудников за активное участие в обеспечении безопасности.
* Внедрить программы повышения осведомленности о безопасности.

1. **Обратная связь:**

* Организовать механизм анонимного сообщения о проблемах или нарушениях безопасности.
* Проводить регулярные опросы сотрудников по вопросам безопасности.

**XV. Специфические требования для государственных организаций**

1. **Соблюдение Доктрины информационной безопасности РФ:**

* Убедиться, что меры безопасности соответствуют положениям Доктрины.

1. **Интеграция с системами государственного мониторинга:**

* Настроить взаимодействие с государственными системами мониторинга инцидентов (например, ГосСОПКА).

**XVI. Обеспечение непрерывности бизнеса**

1. **План управления кризисными ситуациями:**

* Разработать и утвердить планы действий при чрезвычайных ситуациях.
* Назначить ответственных за реализацию каждого этапа плана.

1. **Тренировки и симуляции:**

* Проводить симуляции кибератак, чрезвычайных ситуаций и тестирование плана восстановления.

**XVII. Регулярное обновление**

1. **Актуализация политики безопасности:**

* Регулярно пересматривать политику безопасности и другие документы с учетом новых угроз.
* Внедрять изменения в процессах после обновления законодательства.

Эти дополнения направлены на повышение уровня безопасности и гибкости организации в условиях современных угроз. Если требуется детализировать какой-либо пункт, сообщите!

В соответствии с Федеральным законом № 390-ФЗ «О безопасности» организациям рекомендуется разработать и внедрить следующие документы для обеспечения комплексной системы безопасности:

1. **Политика безопасности организации**: определяет общие принципы и подходы к обеспечению безопасности в организации.
2. **Положение об обеспечении безопасности**: детализирует меры и процедуры, направленные на защиту различных аспектов деятельности организации.
3. **План мероприятий по обеспечению безопасности**: содержит конкретные действия, сроки и ответственных лиц за реализацию мер безопасности.
4. **Приказы о назначении ответственных за безопасность**: документы, назначающие сотрудников, ответственных за различные направления безопасности (информационная, физическая, экономическая и т.д.).
5. **Инструкции для сотрудников по вопросам безопасности**: руководства, описывающие обязанности и действия сотрудников в различных ситуациях, связанных с безопасностью.
6. **План реагирования на чрезвычайные ситуации**: определяет порядок действий при возникновении инцидентов, угрожающих безопасности организации.
7. **Отчеты и акты по результатам проверок и аудитов безопасности**: документы, фиксирующие результаты внутренних и внешних проверок системы безопасности.
8. **Журналы учета инцидентов безопасности**: регистрация всех происшествий, связанных с нарушением безопасности, и принятых мер по их устранению.
9. **Планы обучения и повышения квалификации сотрудников в области безопасности**: программы, направленные на повышение осведомленности и компетентности персонала в вопросах безопасности.
10. **Договоры с контрагентами, содержащие требования по обеспечению безопасности**: соглашения, включающие обязательства сторон по соблюдению мер безопасности при взаимодействии.

Эти документы помогут организации соответствовать требованиям законодательства и обеспечить эффективную защиту от различных угроз.