**Полный чек-лист для организации по документам (Указ № 250, Постановление № 1272)**

**I. Организационные меры**

1. **Назначение ответственных лиц**:
   * Назначен заместитель руководителя, ответственный за информационную безопасность.
   * Разработаны и утверждены должностные инструкции для заместителя.
   * Назначены сотрудники для выполнения функций по обеспечению ИБ.
2. **Создание структурного подразделения по ИБ**:
   * Создано подразделение, отвечающее за информационную безопасность.
   * Утверждено положение о подразделении, определены его полномочия и структура.
3. **Привлечение лицензированных организаций**:
   * Заключены договоры с лицензированными ФСТЭК/ФСБ организациями для реализации мер защиты.
4. **Аттестация кадров**:
   * Проведена аттестация сотрудников подразделения на соответствие квалификационным требованиям.
   * Организованы программы обучения и повышения квалификации специалистов.

**II. Политика и планирование ИБ**

1. **Разработка внутренней документации**:
   * Политика информационной безопасности.
   * Положение о защите конфиденциальной информации.
   * Регламенты и инструкции для выполнения требований ИБ.
2. **Планирование мероприятий**:
   * Разработан план мероприятий по обеспечению информационной безопасности.
   * Определены показатели эффективности выполнения мероприятий.
3. **Согласование с ФСБ и ФСТЭК**:
   * Политика и ключевые решения согласованы с уполномоченными органами.
4. **Мониторинг актуальности требований**:
   * Организована система отслеживания новых нормативных актов и рекомендаций от ФСБ/ФСТЭК.

**III. Контроль и мониторинг угроз**

1. **Выявление угроз и управление рисками**:
   * Разработана модель угроз для информационных систем.
   * Проведён анализ рисков с последующим планированием мер их минимизации.
2. **Мониторинг защищённости**:
   * Организован мониторинг ИБ с использованием систем мониторинга (SIEM).
   * Подключены аккредитованные центры ГосСОПКА.
3. **Тестирование защищённости**:
   * Регулярно проводятся пентесты и оценка уязвимостей систем.
4. **Аудит информационных систем**:
   * Проведен аудит существующих систем защиты.
   * Выявленные уязвимости задокументированы, определены меры их устранения.

**IV. Реагирование на инциденты**

1. **Система управления инцидентами**:
   * Разработан и утверждён план реагирования на инциденты.
   * Созданы инструкции по уведомлению руководства и ФСБ о значимых инцидентах.
2. **Журнал инцидентов**:
   * Ведётся учёт всех инцидентов, включая их причины и последствия.
   * Документируются меры по устранению последствий инцидентов.
3. **Взаимодействие с ГосСОПКА**:
   * Налажено взаимодействие с Национальным координационным центром по компьютерным инцидентам.
   * Обеспечена возможность удалённого доступа ФСБ для мониторинга.

**V. Технические меры защиты**

1. **Установка сертифицированных средств защиты**:
   * Используются сертифицированные средства защиты информации.
   * Настроены системы контроля доступа и шифрования данных.
2. **Переход на отечественные технологии**:
   * Проведён аудит используемого иностранного ПО.
   * Разработан план поэтапного перехода на отечественное ПО (до 2025 года).
3. **Резервирование данных**:
   * Организована система резервного копирования и восстановления данных.
   * Проводятся регулярные тесты восстановления.
4. **Журнал событий безопасности**:
   * Ведётся учёт действий пользователей и системных событий.

**VI. Документооборот и отчётность**

1. **Регламент ведения документации**:
   * Разработаны регламенты ведения и хранения документов по ИБ.
   * Организован процесс регулярного обновления документации.
2. **Отчётность**:
   * Подготовка отчетов о состоянии ИБ для руководства.
   * Регулярная передача отчётов в ФСБ и ФСТЭК (при необходимости).
3. **Регистры угроз и мероприятий**:
   * Созданы реестры угроз, уязвимостей и выполненных мероприятий.

**VII. Обучение персонала**

1. **Инструктаж сотрудников**:
   * Проведён инструктаж всех сотрудников, работающих с информацией.
   * Подписаны соглашения о неразглашении конфиденциальной информации.
2. **Программа обучения**:
   * Разработаны и реализованы программы обучения сотрудников по ИБ.
   * Регулярно проводятся тесты на знания сотрудников.
3. **Учебные тревоги**:
   * Организованы симуляции инцидентов и учения для отработки действий.

**VIII. Взаимодействие с подрядчиками**

1. **Соглашения с подрядчиками**:
   * Заключены договоры, включающие требования по защите информации.
   * Проведена проверка соответствия подрядчиков требованиям ИБ.
2. **Контроль деятельности подрядчиков**:
   * Налажен мониторинг выполнения подрядчиками обязательств по ИБ.

**IX. Постоянное совершенствование**

1. **Модернизация систем защиты**:
   * Разработан план модернизации технических средств.
   * Реализуются улучшения на основе новых угроз и технологий.
2. **Актуализация политики и регламентов**:
   * Политика и регламенты пересматриваются ежегодно или при изменении нормативных требований.
3. **Метрики и показатели эффективности**:
   * Установлены KPI для оценки уровня защищённости и эффективности мер ИБ.

**Итог**

Этот чек-лист охватывает ключевые аспекты требований Указа № 250 и Постановления № 1272, включая организационные, технические и процедурные меры. Если требуется помощь в разработке документов или их реализации, дайте знать!

**Дополнения к чек-листу по Указу № 250 и Постановлению № 1272**

**X. Расширенный контроль и мониторинг**

1. **Централизованный сбор и анализ данных**:

* Настроены системы централизованного сбора событий безопасности (SIEM).
* Используются механизмы автоматического анализа для выявления аномалий и угроз.

1. **Реализация искусственного интеллекта в мониторинге**:

* Внедрены системы ИИ для предсказания инцидентов и анализа поведения пользователей (UBA – User Behavior Analytics).

1. **Проверка эффективности защиты данных**:

* Регулярное тестирование механизмов защиты данных, включая резервное копирование и восстановление.

**XI. Интеграция и взаимодействие с государственными органами**

1. **Обеспечение взаимодействия с ГосСОПКА**:

* Установлен прямой контакт с операторами ГосСОПКА.
* Организованы регулярные тренировки по взаимодействию в случае компьютерных атак.

1. **Подготовка отчётности для надзорных органов**:

* Формализованы процессы подготовки отчётов для ФСБ, ФСТЭК и других органов.
* Организован учёт всех выполненных рекомендаций и распоряжений от госорганов.

**XII. Работа с критической информационной инфраструктурой (КИИ)**

1. **Аудит объектов КИИ**:

* Проведена категоризация объектов КИИ, включая определение их значимости.
* Результаты категорирования внесены в реестр ФСТЭК.

1. **Модернизация защиты объектов КИИ**:

* Для объектов с высокой категорией значимости внедрены дополнительные меры защиты.
* Обеспечен постоянный мониторинг состояния объектов КИИ.

1. **Учебные тревоги для объектов КИИ**:

* Регулярно проводятся тренировки по реагированию на инциденты на объектах КИИ.
* Составлены сценарии угроз и проверено взаимодействие с государственными структурами.

**XIII. Техническое совершенствование**

1. **Переход на отечественные средства защиты**:

* Утверждён поэтапный план замены иностранных средств защиты на отечественные.
* Проведены тесты совместимости новых решений с существующими системами.

1. **Внедрение криптографических средств защиты**:

* Реализованы сертифицированные ФСБ криптографические средства для шифрования данных.
* Настроен контроль ключей шифрования.

1. **Миграция с облачных решений недружественных стран**:

* Полностью исключены облачные сервисы, находящиеся под юрисдикцией недружественных стран.
* Настроены локальные хранилища данных или отечественные облачные решения.

**XIV. Усиление работы с персоналом**

1. **Оценка осведомлённости сотрудников**:

* Регулярное проведение тестов на знание актуальных угроз (фишинг, социальная инженерия).
* Проведение курсов по повышению компетенций в сфере ИБ для сотрудников всех уровней.

1. **Система мотивации за соблюдение ИБ**:

* Введены поощрения за предотвращение инцидентов или успешное участие в учениях.

1. **Инструктаж новых сотрудников**:

* Все новые сотрудники проходят обязательный инструктаж по политике ИБ перед началом работы.

**XV. Углубленная работа с подрядчиками**

1. **Оценка рисков от работы с подрядчиками**:

* Проведена оценка рисков, связанных с доступом подрядчиков к информационным системам.
* Разработан перечень ограничений для подрядчиков и партнёров.

1. **Системы мониторинга действий подрядчиков**:

* Настроен контроль действий подрядчиков в информационных системах.
* Логируются и анализируются действия всех внешних пользователей.

**XVI. Постоянное развитие системы безопасности**

1. **Использование метрик эффективности безопасности**:

* Разработаны метрики для оценки состояния ИБ (количество инцидентов, время на реагирование, процент устранённых уязвимостей).
* Проводится регулярный анализ этих метрик для корректировки стратегий.

1. **Обновление внутренней документации**:

* Политики, регламенты и инструкции обновляются не реже одного раза в год.
* Учитываются изменения в законодательстве и рекомендации ФСБ/ФСТЭК.

1. **Внедрение новых технологий защиты**:

* Тестируются и внедряются современные средства защиты, такие как блокчейн, ИИ, биометрия.

**Итоговые дополнения**

Эти дополнения усиливают базовый чек-лист, расширяя его за счёт углублённой работы с КИИ, использования новых технологий, взаимодействия с подрядчиками и управления кадрами. Если требуется уточнение или детальная разработка пунктов, сообщите!