Чек – лист На основании анализа **Указа Президента РФ № 250 от 1 мая 2022 года "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"**, ниже представлен чек-лист для выполнения требований указа в организации:

**I. Организационные меры**

1. **Назначение ответственных лиц**:
   * Назначен заместитель руководителя, ответственный за информационную безопасность.
   * Определены полномочия по обнаружению, предупреждению и ликвидации последствий компьютерных атак.
2. **Создание структурного подразделения**:
   * Создано подразделение, ответственное за обеспечение информационной безопасности.
   * Либо эти функции возложены на существующее подразделение.
3. **Привлечение лицензированных организаций**:
   * Привлечены организации, имеющие лицензии ФСТЭК или ФСБ, для реализации мер защиты (при необходимости).
4. **Обеспечение доступа ФСБ**:
   * Обеспечен доступ ФСБ (включая удалённый) к информационным ресурсам организации для мониторинга защищенности.

**II. Технические и организационные меры**

1. **Реализация мер по указаниям ФСБ и ФСТЭК**:
   * Мгновенно реализуются меры, рекомендованные ФСБ и ФСТЭК в случае обнаружения угроз.
2. **Переход на отечественные средства защиты**:
   * Исключены иностранные средства защиты информации и сервисы, связанные с недружественными государствами (вступает в силу с 1 января 2025 года).

**III. Оценка защищенности информационных систем**

1. **Оценка уровня защищенности**:
   * Проведена оценка уровня защищенности информационных систем.
   * Результаты представлены в Правительство РФ (для организаций, включённых в соответствующий перечень).
2. **Мониторинг защищенности**:
   * Настроен мониторинг защищенности ресурсов с использованием аккредитованных центров ГосСОПКА.

**IV. Взаимодействие с аккредитованными центрами**

1. **Работа с аккредитованными центрами**:
   * Заключены соглашения с аккредитованными центрами для обнаружения и ликвидации последствий компьютерных атак.
   * Центры аккредитованы в ГосСОПКА.
2. **Контроль деятельности центров**:
   * Убедились, что деятельность аккредитованных центров соответствует требованиям ФСБ.

**V. Документооборот и отчётность**

1. **Документация по информационной безопасности**:
   * Разработано и утверждено положение о структурном подразделении по информационной безопасности.
   * Разработаны типовые регламенты и инструкции для реализации требований Указа.
2. **Отчётность перед контролирующими органами**:
   * Организована система регулярного предоставления отчётов в правительство и ФСБ.

**VI. Постоянное совершенствование**

1. **Актуализация мер безопасности**:
   * Внедряются меры по обновлению систем защиты в соответствии с новыми угрозами.
   * Проводятся регулярные тренировки по реагированию на компьютерные инциденты.

**Итог**

Этот чек-лист позволяет обеспечить выполнение требований Указа № 250 в рамках организации. Если необходимо разработать шаблоны документов, инструкции или детализировать пункты, сообщите!

**Дополнения к чек-листу по Указу Президента РФ № 250 от 1 мая 2022 года**

**VII. Усиленные меры по переходу на отечественные технологии**

1. **Переход на отечественное программное обеспечение**:

* Разработан план поэтапного перехода на отечественное ПО.
* Ведётся аудит используемого иностранного ПО с целью его замены.

1. **Проверка совместимости отечественных решений**:

* Проведены тестирования совместимости отечественных средств защиты с информационными системами организации.
* Внедрены решения для устранения проблем совместимости.

1. **Отказ от облачных решений недружественных государств**:

* Исключено использование облачных сервисов, находящихся под юрисдикцией недружественных государств.

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

1. **Идентификация объектов КИИ**:

* Проведена категоризация объектов, входящих в состав КИИ.
* Внесены данные об объектах КИИ в реестр ФСТЭК.

1. **Повышение защищённости объектов КИИ**:

* Реализованы дополнительные меры защиты для объектов с высокой категорией значимости.
* Ведётся мониторинг работоспособности объектов КИИ в режиме реального времени.

1. **Аудит готовности к угрозам**:

* Проведены учения по реагированию на инциденты в системе КИИ.
* Выявленные уязвимости устранены в установленные сроки.

**IX. Усиленный мониторинг и реагирование**

1. **Проведение регулярных тестов защищённости**:

* Проводится регулярное тестирование систем на уязвимости (пентесты).
* Реализованы сценарии эмуляции кибератак для оценки готовности к инцидентам.

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

* Настроен централизованный сбор логов с критически важных систем.
* Используются системы искусственного интеллекта (ИИ) для анализа логов и обнаружения аномалий.

1. **Контроль за третьими лицами**:

* Проверяется выполнение подрядчиками требований безопасности.
* Заключены соглашения с подрядчиками, включающие ответственность за нарушения.

**X. Работа с кадрами**

1. **Аттестация персонала по безопасности**:

* Проведена аттестация сотрудников, работающих с критически важными системами.
* Организовано повышение квалификации специалистов ИБ.

1. **Повышение осведомлённости сотрудников**:

* Реализована программа повышения осведомлённости сотрудников о киберугрозах.
* Регулярно проводятся тесты на фишинг и социальную инженерию.

1. **Мотивация персонала**:

* Внедрена система поощрений за предотвращение инцидентов и внедрение эффективных мер защиты.

**XI. Регулярный контроль и совершенствование**

1. **Актуализация внутренней документации**:

* Политики и регламенты обновляются ежегодно или при изменении законодательства.
* Актуализация осуществляется с учётом новых указаний ФСБ и ФСТЭК.

1. **Внедрение метрик и KPI по безопасности**:

* Установлены ключевые показатели эффективности (например, время реагирования на инциденты, число устранённых уязвимостей).
* Показатели регулярно анализируются и используются для совершенствования системы безопасности.

**XII. Интеграция с госструктурами и мониторинг законодательства**

1. **Мониторинг новых указаний**:

* Организована система отслеживания новых требований и указаний ФСБ, ФСТЭК и других органов.

1. **Взаимодействие с ГосСОПКА**:

* Установлен постоянный контакт с операторами ГосСОПКА для оперативного обмена данными.
* Регулярно предоставляются отчёты о выполнении требований.

**Итог**

Эти дополнения расширяют базовый чек-лист, усиливая акцент на кадрах, интеграции с государственными органами, использовании отечественных технологий и защите КИИ. Если требуется детализировать конкретные пункты или разработать соответствующие шаблоны, сообщите!