1. Планирование мероприятий в сфере информационной безопасности.
2. Реализация мероприятий в сфере информационной безопасности.
3. Контроль мероприятий в сфере информационной безопасности.
4. Обеспечение конфиденциальности, целостности и доступности информации.
5. Защита персональных данных граждан и служебной информации.
6. Предотвращение утечек информации и несанкционированного доступа.
7. Соблюдение требований законодательства РФ в области информационной безопасности.
8. Защита критической информационной инфраструктуры, включая АСУГТ и ЭПГ.

|  |  |
| --- | --- |
| Проекты | Регулярные процессы |
| Установка элементов физической безопасности(камер, электронных замков и прочего) | Пересмотр и обновление политики ИБ |
| Первичная настройка ПО для своевременного обнаружения атак, уязвимостей, а так же контроля за физической безопасностью | Контроль и поддержка киберфизической системы безопасности |
| Организация контролируемого доступа к охраняемым объектам(физический доступ к серверу только после согласования с сотрудником отдела иб, доступ к бд исключительно по паролям и id) | Тестирование системы |
| Настройка систем контроля безопасности АСУГТ и ЭПГ | Постоянное повышение квалификации сотрудников |
| Первичный инструктаж сотрудников по поводу безопасности систем | Борьба с инцидентами |
| Дополнительный инструктаж сотрудников отдела, ответственного за АСУГТ и ЭПГ | Изучение инцидентов |



**Пересмотр и обновление политики ИБ**

Участники:

* Сотрудники ИБ
  + Функции:
    - Анализ текущей политики на соответствие законодательству и требованиям организации.
    - Разработка предложений по изменениям.
  + Права:
    - Запрашивать информацию у других отделов.
    - Инициировать внесение правок.
  + Обязанности:
    - Соблюдать сроки пересмотра.
    - Обеспечивать конфиденциальность документов.
* Руководитель ОИБ
  + Функции:
    - Утверждение обновленной политики.
    - Контроль внедрения изменений.
  + Права:
    - Отклонять/корректировать предложения.
    - Требовать отчёты о выполнении.
  + Обязанности:
    - Гарантировать соответствие политики законодательству РФ.

Ответственные:

* Итоговый результат: Руководитель ОИБ.
* Этапы:
  + Анализ → Сотрудники ИБ.
  + Утверждение → Руководитель ОИБ.

[Анализ] → [Изменения] → [Утверждение] → [Внедрение]

↑ ↑ ↑ ↑

Сотр. ИБ Сотр. ИБ Руководитель Сотр. ИБ/Отделы

**Контроль и поддержка киберфизической системы безопасности**

Участники:

* Сотрудники ИБ
  + Функции:
    - Мониторинг системы в реальном времени.
    - Анализ угроз и инцидентов.
  + Права:
    - Блокировать подозрительные активности.
    - Требовать доступ к логированию.
  + Обязанности:
    - Обеспечивать непрерывность работы системы.
* Администраторы систем
  + Функции:
    - Устранение технических неполадок.
    - Настройка параметров безопасности.
  + Права:
    - Вносить изменения в конфигурацию.
  + Обязанности:
    - Соблюдать регламенты ИБ.

Ответственные:

* Итоговый результат: Сотрудники ИБ.
* Этапы:
  + Устранение неполадок → Администраторы.
  + Составление отчетов → Сотрудники ИБ.

[Мониторинг] → [Выявление] → [Устранение] → [Отчет]

↑ ↑ ↑ ↑

Сотр. ИБ Сотр. ИБ/Адм. Администраторы Сотр. ИБ

**Тестирование системы**

Участники:

* Сотрудники ИБ
  + Функции:
    - Планирование тестовых сценариев.
    - Анализ результатов тестирования.
  + Права:
    - Требовать доступ к тестовым средам.
  + Обязанности:
    - Обеспечивать достоверность результатов.
* Технические специалисты
  + Функции:
    - Проведение нагрузочного и пентест-тестирования.
  + Права:
    - Использовать инструменты для тестирования.
  + Обязанности:
    - Не нарушать работоспособность системы.

Ответственные:

* Итоговый результат: Сотрудники ИБ.
* Этапы:
  + Проведение тестов → Технические специалисты.
  + Корректировка настроек → Техспециалисты + ИБ.

[Планирование] → [Тестирование] → [Анализ] → [Корректировка]

↑ ↑ ↑ ↑

Сотр. ИБ Техспециалисты Сотр. ИБ Техспециалисты

**Постоянное повышение квалификации сотрудников**

Участники:

* Сотрудники ИБ
  + Функции:
    - Формулирование потребностей в обучении.
    - Участие в тренингах.
  + Права:
    - Выбирать курсы/тренинги (по согласованию).
  + Обязанности:
    - Применять полученные знания на практике.
* HR-отдел
  + Функции:
    - Организация обучения (договоры, расписание).
  + Права:
    - Контролировать посещаемость.
  + Обязанности:
    - Соблюдать бюджет на обучение.
* Внешние эксперты
  + Функции:
    - Проведение лекций/воркшопов.
  + Обязанности:
    - Предоставлять актуальные материалы.

Ответственные:

* Итоговый результат: Руководитель ОИБ.
* Этапы:
  + Организация → HR-отдел.
  + Проведение → Внешние эксперты.

[Оценка] → [Организация] → [Обучение] → [Оценка]

↑ ↑ ↑ ↑

Сотр. ИБ HR-отдел Внешние эксперты Руководитель

**Борьба с инцидентами**

Участники:

* Специалисты ИБ
  + Функции:
    - Мониторинг систем на предмет аномалий.
    - Классификация инцидентов по уровню угрозы.
    - Координация действий участников.
  + Права:
    - Полный доступ к данным мониторинга и журналам событий.
    - Требовать срочных мер от администраторов.
  + Обязанности:
    - Оперативное информирование о выявленных угрозах.
    - Соблюдение регламентов реагирования.
* Администраторы систем
  + Функции:
    - Изоляция зараженных или уязвимых систем.
    - Восстановление работоспособности инфраструктуры.
  + Права:
    - Вносить изменения в конфигурацию сетевого оборудования.
    - Блокировать подозрительные IP-адреса или пользователей.
  + Обязанности:
    - Минимизация времени простоя систем.
    - Согласование действий с ИБ-специалистами.
* Юрист
  + Функции:
    - Документирование инцидентов для отчётности.
    - Проверка соответствия действий законодательству РФ.
  + Права:
    - Запрашивать данные о ходе расследования.
    - Участвовать в разборе инцидента.
  + Обязанности:
    - Обеспечение юридической чистоты процессов.
* Руководитель ОИБ
  + Функции:
    - Утверждение плана действий.
    - Контроль выполнения этапов.
    - Отчёт перед высшим руководством.
  + Права:
    - Принимать решения об эскалации инцидента.
    - Назначать ответственных за этапы.
  + Обязанности:
    - Обеспечение ресурсов для устранения угроз.

Ответственные:

* Итоговый результат: Руководитель ОИБ.
* Этапы:
  1. Обнаружение и классификация:
     + Ответственные: Специалисты ИБ.
  2. Изоляция систем:
     + Ответственные: Администраторы систем.
  3. Восстановление:
     + Ответственные: Администраторы систем + Специалисты ИБ.
  4. Анализ причин:
     + Ответственные: Юрист + Руководитель ОИБ.

[Обнаружение] → [Изоляция] → [Восстановление] → [Анализ]

↑ ↑ ↑ ↑

Спец. ИБ Администраторы Администраторы Юрист/Руководитель

**Изучение инцидентов**

Участники:

* Специалисты ИБ
  + Функции:
    - Сбор данных: логи, метаданные, информация о событиях.
    - Первичный анализ для определения масштаба инцидента.
    - Подготовка материалов для углубленного исследования.
  + Права:
    - Доступ к системам мониторинга и базам данных.
    - Запрос дополнительной информации у сотрудников.
  + Обязанности:
    - Обеспечение сохранности и конфиденциальности собранных данных.
    - Своевременная передача материалов экспертам.
* Эксперты по кибербезопасности
  + Функции:
    - Углубленный анализ причин инцидента.
    - Выявление уязвимостей в системах и процессах.
    - Разработка рекомендаций по предотвращению повторных инцидентов.
  + Права:
    - Использование специализированных инструментов для анализа.
    - Внесение предложений по изменению политик безопасности.
  + Обязанности:
    - Объективность и точность в оценке уязвимостей.
    - Согласование рекомендаций с ИБ-специалистами.
* Руководитель ОИБ
  + Функции:
    - Утверждение плана анализа и рекомендаций.
    - Контроль сроков выполнения этапов.
    - Организация ресурсов для реализации изменений.
  + Права:
    - Приостановка процесса при выявлении критических ошибок.
    - Требование пересмотра рекомендаций.
  + Обязанности:
    - Обеспечение взаимодействия между участниками.
    - Отчет перед руководством о результатах исследования.

Ответственные:

* Итоговый результат: Руководитель ОИБ.
* Этапы:
  1. Сбор данных:
     + Ответственные: Специалисты ИБ.
  2. Анализ уязвимостей:
     + Ответственные: Эксперты по кибербезопасности.
  3. Разработка рекомендаций:
     + Ответственные: Эксперты + Специалисты ИБ.
  4. Утверждение плана действий:
     + Ответственные: Руководитель ОИБ.

[Сбор данных] → [Анализ] → [Рекомендации] → [Утверждение]

↑ ↑ ↑ ↑

Спец. ИБ Эксперты Эксперты/ИБ Руководитель