**Практика 12**

**Цель работы**: получение навыков формирования компонентов процесса управления инцидентами ИБ в организации

Задание выполняется **в группах,** объекты – те же организации, что и на практике №1 на основе результатов предыдущей работы (практики).

1. Определите требования НПА к управлению инцидентами и реагированию на них в вашей организации.
2. Разработайте схему процесса управления инцидентами информационной безопасности в рассматриваемой организации. Учтите требования НПА.
3. Определите ответственных на каждом этапе процесса. Учтите требования НПА.
4. Определите перечень действий на каждом этапе процесса для каждого участника. Учтите требования НПА.
5. Разработайте необходимую организационно – распорядительную документацию:
   1. Составьте список ОРД (организационно – распорядительной документации) для обеспечения процесса управления инцидентами.
   2. Разработайте политику управления инцидентами (скорректируйте, если политика была разработана ранее)
   3. Разработайте фрагменты должностных инструкций для участников процесса управления инцидентами.
   4. Разработайте прочие необходимые ОРД.

**Оформить результат в виде:**

1. Презентации для рассказа (при необходимости)
2. Файла в формате doc/docx/odt - по одному отдельному файлу на каждый с
3. **Требования НПА к управлению инцидентами и реагированию на них в нашей организации**

**1. Обязательные требования для всех типов дронов**

**1.1. Федеральный закон № 187-ФЗ «О безопасности КИИ»:**

**- Классификация предприятия как субъекта КИИ при наличии критически важных объектов**

**- Обязательное внедрение системы мониторинга инцидентов ИБ**

**- Уведомление ФСТЭК/ФСБ о значимых инцидентах в течение 24 часов**

**- Проведение расследований с оформлением актов по установленной форме**

**1.2. Приказ ФСТЭК № 239 (2021):**

**- Ведение журнала инцидентов ИБ с хранением данных не менее 5 лет**

**- Назначение ответственных за обработку инцидентов ИБ**

**- Разработка регламентов реагирования на инциденты**

**1.3. ГОСТ Р 57580.1-2017:**

**- Создание центра реагирования на инциденты (SOC/SIEM)**

**- Регулярное тестирование процедур реагирования (не реже 1 раза в год)**

**2. Дополнительные требования для военных дронов**

**2.1. Постановление Правительства № 1279 (2021):**

**- Специальные требования к защите сведений, составляющих гостайну**

**- Обязательное использование сертифицированных средств защиты (СЗИ)**

**- Дополнительные формы отчетности в Минобороны**

**2.2. Приказ ФСБ № 66 (2020):**

**- Особый порядок расследования инцидентов с утечкой секретных данных**

**- Обязательное участие представителей ФСБ в расследовании критических инцидентов**

**- Использование защищенных каналов связи при передаче данных об инцидентах**

**3. Требования для гражданских дронов**

**3.1. Приказ Минцифры № 766 (2022):**

**- Уведомление Роскомнадзора об утечках персональных данных**

**- Соблюдение требований к защите облачных систем**

**- Обязательное резервное копирование данных**

**3.2. Технический регламент ЕАЭС 037/2016:**

**- Ведение реестра инцидентов с программным обеспечением**

**- Отзыв продукции при выявлении уязвимостей**

**4. Процедурные требования**

**1. Регистрация инцидентов:**

**- Фиксация всех событий ИБ в едином журнале**

**- Присвоение категории критичности (по методике ФСТЭК)**

**2. Расследование:**

**- Срок проведения - не более 30 дней**

**- Обязательное документирование результатов**

**3. Устранение последствий:**

**- Разработка корректирующих мер**

**- Контроль исполнения**

**4. Отчетность:**

**- Ежеквартальные отчеты в ФСТЭК**

**- Экстренные уведомления при критических инцидентах**

1. **Схема процесса управления инцидентами ИБ**

Изображение выглядит как текст, диаграмма, линия, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Порядок приоритета реагирования: Экстренное – срочное – плановое (возможно лучше заменить на «несрочное»)

1. **Ответственных на каждом этапе процесса и их действия**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Этап процесса | Уровень критичности | Ответственные | Действия | Требования НПА | Сроки |
| 1 | **Обнаружение** | Все | SOC-оператор, Отдел ИБ | - Фиксация в SIEM - Первичный анализ | ФЗ-187 ст.10, Приказ ФСТЭК №239 | Непрерывно |
| 2 | **Классификация** | Все | Руководитель ИБ, CISO | - Определение уровня (низкий/высокий/критичный) - Назначение ответственных | ГОСТ Р 57580.1-2017 | До 1 часа |
| 3 | **Уведомление** | Критический/Высокий | Юр.отдел, CISO | - Форма КИИ-1 в ФСТЭК/ФСБ - Уведомление Роскомнадзора (для ПДн) | ФЗ-187 ст.10, 152-ФЗ ст.19.7 | До 24 часов |
| 5 | **Устранение** | Все | ИТ-отдел, Разработчики | - Патчинг уязвимостей - Восстановление данных | Техрегламент ЕАЭС 037/2016 | По плану |
| 6 | **Корректирующие меры** | Все | CISO, HR, Руководство | - Обновление политик ИБ - Проверка персонала | Приказ ФСТЭК №239 п.18 | До 30 дней |
| 7 | **Отчётность** | Все | Служба контроля, Секретариат | - Отчёт регуляторам - Внутренний аудит | ФЗ-187 ст.12 | До 10 дней |
| 8 | **Архивация** | Все | Архивариус, Отдел ИБ | - Внесение в журнал - Передача в спецархив (для гостайны) | Приказ ФСТЭК №239 п.8 | 5 лет |

Состав комиссий по типам инцидентов:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Тип инцидента | Обязательные участники | Дополнительные требования | Тип инцидента | Обязательные участники | Дополнительные требования |
| Утечка гостайны | Представитель ФСБ, Руководитель ОПК, Архивариус | Использование СЗИ класса КС2 | Утечка гостайны | Представитель ФСБ, Руководитель ОПК, Архивариус | Использование СЗИ класса КС2 |
| Кибератака на КИИ | Специалист ФСТЭК, ИТ-директор | Форма КИИ-1 + приложение с цифр.доказат. | Кибератака на КИИ | Специалист ФСТЭК, ИТ-директор | Форма КИИ-1 + приложение с цифр.доказат. |
| Утечка ПДн | DPO, Юрист, ИТ-специалист | Уведомление Роскомнадзора по форме | Утечка ПДн | DPO, Юрист | Уведомление Роскомнадзора по форме |

1. **Порядок действий**

1. Обнаружение инцидента

SOC-оператор:

Мониторинг событий в SIEM/SOC.

Фиксация инцидента в журнале (Приказ ФСТЭК №239, п.8).

Первичный анализ (определение типа: атака, утечка, сбой).

Сотрудники:

Сообщение о подозрительных событиях в SOC (через установленные каналы).

2. Классификация инцидента

Определение уровня критичности:

Низкий (не влияет на КИИ/ПДн).

Высокий (риск для бизнеса).

Критичный (угроза КИИ, гостайне, массовая утечка ПДн).

Назначение ответственных за расследование.

3. Уведомление регуляторов

Заполнение формы КИИ-1 (ФСТЭК/ФСБ) в течение 24 часов (ФЗ-187).

Уведомление Роскомнадзора (для утечек ПДн по 152-ФЗ).

Использование защищённых каналов связи (Приказ ФСБ №66).

4. Расследование

Сбор доказательств (логи, скриншоты, дампы памяти).

Заполнение Акта расследования (Приказ ФСТЭК №239).

Определение root-cause.

5. Устранение последствий

Патчинг уязвимостей.

Восстановление данных из резервных копий (Приказ Минцифры №766).

Блокировка компрометированных учётных записей.

6. Корректирующие меры

Обновление политик ИБ.

Дополнительное обучение сотрудников.

Внедрение новых средств защиты (СЗИ).

7. Отчётность

Подготовка отчёта для регуляторов (ФСТЭК, ФСБ, Роскомнадзор).

Внутренний аудит эффективности мер.

8. Архивация

Внесение данных в журнал инцидентов (хранение 5 лет).

Передача документов в спецархив (для гостайны).

1. **Список ОРД (организационно – распорядительной документации) для обеспечения процесса управления инцидентами**

* Политика управления инцидентами
* Регламент классификации инцидентов
* Журнал учета инцидентов ИБ или Форма КИИ-1
* Должностные инструкции участников процесса управления инцидентами

**Фрагменты должностных инструкций для участников процесса управления инцидентами ИБ**

**1. Должностная инструкция SOC-аналитика**

**1.2. Обязанности**

* **Мониторинг**:
  + Выявление подозрительных событий в SIEM.
  + Анализ логов (Firewall, IDS/IPS, EDR).
* **Реагирование**:
  + Первичная классификация инцидентов (низкий/высокий/критичный).
  + Эскалация инцидентов CISO (для высокого/критичного уровня).
  + При выявлении инцидента, связанного с гостайной, немедленно уведомлять сотрудника по работе с ФСБ и CISO. Не предпринимать действий по удалению/изменению данных до их фиксации ФСБ
* **Документирование**:
  + Заполнение Журнала инцидентов ИБ.
  + Фиксация доказательств (скриншоты, дампы трафика).

**1.3. Права**

* Требовать устранения нарушений ИБ от сотрудников.
* Получать доступ к системным логам и данным.

**1.4. Ответственность**

* За несвоевременное выявление/эскалацию инцидентов.
* За нарушение конфиденциальности данных.

**2. Должностная инструкция CISO (Руководителя ИБ)**

**2.2. Обязанности**

* **Управление процессом**:
  + Координация расследований инцидентов.
  + Утверждение корректирующих мер.
* **Отчётность**:
  + Подготовка отчётов для ФСТЭК/ФСБ (форма КИИ-1).
  + Информирование руководства о рисках.
* **Развитие ИБ**:
  + Внедрение новых средств защиты (SOC, DLP).
  + Обучение сотрудников.
* **Взаимодействие с ФСБ:**
  + Организация участия представителей ФСБ в расследованиях инцидентов, связанных с гостайной.
  + Передача данных об инцидентах через защищённые каналы связи (СЗИ класса КС2/КС3).
  + Заполнение спецформ отчётности (например, форма «ИБ-ГТ»).
* **Контроль соблюдения режима:**
  + Проверка журналов учёта носителей гостайны после инцидента.
  + Мониторинг использования криптосредств (например, «КриптоПро»).

**2.3. Права**

* Приостанавливать работу систем при угрозе КИИ.
* Требовать участия юристов/ФСБ в расследованиях.

**2.4. Ответственность**

* За несоблюдение сроков уведомления регуляторов.
* За неэффективность мер реагирования.

**3. Должностная инструкция ИТ-специалиста (участника комиссии по расследованию)**

**3.2. Обязанности**

* **Анализ**:
  + Исследование логов, метаданных, памяти систем.
  + Выявление root-cause инцидента.
* **Устранение**:
  + Патчинг уязвимостей.
  + Восстановление данных.
* **Документирование**:
  + Заполнение *Акта расследования*.

**3.3. Права**

* Требовать доступ к оборудованию/софту.
* Привлекать сторонних экспертов (по согласованию с CISO).

**3.4. Ответственность**

* За недостоверность выводов расследования.

**4. Должностная инструкция специалиста по работе с данными (здесь про ПДн)**

**4.2. Обязанности**

* **Реагирование**:
  + Уведомление Роскомнадзора об утечках ПДн (в течение 72 часов).
  + Оценка масштаба инцидента.
* **Профилактика**:
  + Контроль соблюдения политик обработки ПДн.
  + Обучение сотрудников.
* **Расследование:**
  + Использовать только сертифицированные ФСБ средства для сбора доказательств (например, «Мобильный криминалист»). Передавать данные исключительно через СЗИ класса КС2

**4.3. Права**

* Блокировать обработку ПДн при нарушениях.

**4.4. Ответственность**

* За несвоевременное уведомление регуляторов.