|  |  |
| --- | --- |
| **лого для документов 2022** | ***Федеральное агентство по рыболовству***  ***Федеральное государственное бюджетное образовательное***  ***учреждение высшего образования***  ***«Астраханский государственный технический университет»***  **Система менеджмента качества в области образования, воспитания, науки и инноваций**  **ООО «ДКС РУС» по международному стандарту ISO 9001:2015** |

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ

**КАФЕДРА АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ И УПРАВЛЕНИЯ**

**ОРГАНИЗАЦИОННЫЕ МЕТОДЫ**

**ЗАЩИТЫ ИНФОРМАЦИИ**

(*наименование дисциплины*)

**ОТЧЕТ**

о выполнении заданий к лабораторной работе №2

**«СОЗДАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ»**

*(название лабораторной работы)*

|  |  |
| --- | --- |
|  | Выполнила:  студент гр. ДИНРБ-41 |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Кузургалиев Р.А. |
|  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2024 г. |
|  | Максимальное количеству баллов \_\_\_\_\_  ЗАЩИЩЕНО:  Получено баллов \_\_\_\_\_\_ |
|  | Преподаватель: \_\_\_\_\_\_\_Сахипова Ж.Ш. |
|  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2024 г. |

**Астрахань – 2024**

**Лабораторная работа №1 «СОЗДАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ»:**

1. Указать цель обеспечения информационной безопасности предприятия. Задать величину степени защищенности (в процентах) создаваемой на объекте системы защиты информации и стоимость (S) используемых активов АС.
2. Выбрать и обосновать стратегические принципы безопасности АС.
3. Оценить величину ущерба (V) активам АС при реализации угроз.
4. Рассчитать ожидаемые потери (E) после создания системы информационной безопасности (заполнить таблицу).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Категории активов | S [руб.] | V [руб.] | P | E [руб.] |
| Аппаратное обеспечение | 5 000 000 | 200 000 | 0,5 | 100 000 |
| Программное обеспечение | 1 000 000 | 1 000 000 | 0,5 | 500 000 |
| Информационное обеспечение | 500 000 | 10 000 000 | 0,5 | 5 000 000 |
| Персонал | 1 200 000 | ----- | 0,5 | ----- |
| Документация | 100 000 | 100 000 | 0,5 | 50 000 |
| Расходные материалы | 200 000 | ----- | 0,5 | ----- |

Примечание. Вероятность возникновения угроз (P) взять из известных в литературе данных или принять среднее значение – 0,5.

**Ход работы:**

Название: "ИнноваТек"

Вид деятельности: Разработка программного обеспечения

Область деятельности: IT-услуги для бизнеса, включая создание программного обеспечения на заказ и хранилище данных.

**1. Цель:** Обеспечение конфиденциальности, целостности и доступности информации, а также защита интеллектуальной собственности компании «ИнноваТек». **Степень защищенности:** 90% (это значение предполагает, что система защиты информации достаточно надежна для mitigating большинства угроз, но оставляет возможность для возможных инцидентов). **Стоимость используемых активов (S):** 5,000,000 рублей( стоимость 10 рабочих мест(исключительно аппаратура: ПК, монитор, прочие устройства, а также системная часть: роутеры, маршрутиризаторы)) стоимость ПО равняется 1 000 000 рублей, в эту сумму входит приобретение лицензий на антивирус, ОС, а также ПО, с помощью которой компания ведёт свою коммерческую деятельность. 200 000 рублей выделены на расходные материалы: бумага, картриджы, тонеры , а также на комплектующие ПК в случае его поломки. На разработку документации и консультации с юристами выделено 100 000 рублей. На информационное обеспечение и первонал выделено 500 000 и 1 200 000 рублей соответственно.

### 2. Стратегические принципы безопасности АС

**Принципы:**

1. **Комплексный подход:** Информационная безопасность должна охватывать все уровни организации, включить управление рисками, физическую безопасность, обучение сотрудников и технические меры.
2. **Система управления безопасностью:** Разработка и внедрение системы управления информационной безопасностью (СУИБ) с четким учетом бизнес-процессов компании.
3. **Политика минимальных привилегий:** Доступ к системам и данным должен предоставляться на основании необходимости, чтобы ограничить потенциальные риски от внутренних угроз.
4. **Обучение и повышение осведомленности:** Регулярные тренинги для сотрудников по вопросам информационной безопасности для уменьшения рисков, связанных с человеческим фактором.
5. **Регулярный аудит и мониторинг:** Постоянное отслеживание и аудит систем и процессов для быстрого выявления и устранения уязвимостей.

Оценка ущерба:

Величина ущерба при реализации угроз может варьироваться в зависимости от характера инцидента. Например:

* В случае кибератаки может пострадать аппаратура: в частности ПК, а именно носители информации, в данном случае нанесённый ущерб может составить 200 000 рублей.
* В случае несанкционированного доступа может произойти утечка приобретённых лицензий, разрабатываемых продуктов и данных , составляющих коммерческую тайну. В таком случае максимальный ущерб составит 1 000 000 и 10 000 000 рублей

**Контрольные вопросы:**

### 1. Этапы создания системы информационной безопасности предприятия

1. **Анализ текущей инфраструктуры:** Оценка существующих процессов и систем безопасности.
2. **Определение рисков:** Идентификация и анализ угроз и уязвимостей.
3. **Разработка политики безопасности:** Формирование документов, описывающих подход к безопасности.
4. **Проектирование системы защиты:** Создание архитектуры системы безопасности.
5. **Имплементация мер безопасности:** Установка и настройка технических решений.
6. **Обучение персонала:** Проведение тренингов и семинаров для сотрудников.
7. **Мониторинг и аудит:** Регулярная проверка эффективности системы безопасности.

### 2. Реализация на практике концепции ИБП

* **Определение целей:** Уточнение бизнес-целей и соответствующих им требований к безопасности.
* **Настройка систем и процессов:** Интеграция мер безопасности в бизнес-процессы.
* **Производство и тестирование:** Проведение тестов систем безопасности, обучение сотрудников.
* **Контроль и доработка:** Изучение инцидентов и внесение корректировок в систему.

### 3. На основе каких документов разрабатывается политика безопасности?

* **Законодательные и нормативные документы:** Такие как российские законы о защите информации.
* **Стандарты информационной безопасности:** ISO/IEC 27001, NIST и другие.
* **Внутренние корпоративные документы:** Устав, кодекс поведения и другие внутренние регламенты.

### 4. Исходя из чего выбирают стратегические принципы безопасности?

* **Анализ рисков:** На основе результатов анализа выявляемых угроз и уязвимостей.
* **Бизнес-цели:** Учет целей и стратегий бизнеса, чтобы гарантировать соответствие.
* **Лучшая практика:** Оценка стандартов и рекомендаций в области информационной безопасности.

### 5. Уровни политики безопасности и ответственные за них

1. **Стратегический уровень:** Генеральный директор или совет директоров.
2. **Тактический уровень:** Директор по информационной безопасности.
3. **Оперативный уровень:** ИТ-отдел, специалисты по безопасности.
4. **Исполнительный уровень:** Все сотрудники компании, ответственные за соблюдение политик.

### 6. Зачем проводится анализ риска? Методы оценки рисков.

**Зачем:** Анализ риска позволяет выявить уязвимости и угрозы, оценить последствия и сформулировать меры по защите.

**Методы оценки рисков:**

* **Качественный анализ:** Оценка рисков на основе экспертных мнений.
* **Количественный анализ:** Использование статистики и моделей для понимания вероятности и величины ущерба.
* **Методы SWOT:** Анализ сильных и слабых сторон, возможностей и угроз.

### 7. Категории защищаемых активов АС, классификация угроз

**Категории защищаемых активов:**

* **Физические активы:** Серверы, компьютеры, сети.
* **Информационные активы:** Данные, программы, базы данных.
* **Человеческие активы:** Сотрудники, их знания и навыки.

**Классификация угроз:**

* **Внешние угрозы:** Хакерские атаки, вирусы, кибершпионаж.
* **Внутренние угрозы:** Ошибки сотрудников, злоупотребления.
* **Природные угрозы:** Пожары, наводнения, аварии.

### 8. Содержание плана защиты АС

* **Обзор ситуации**: Описание текущего состояния безопасности.
* **Цели и задачи защиты**: Обоснование необходимости защиты активов.
* **Меры защиты**: Установление конкретных технических и организационных мер.
* **Подразделения и ответственности**: Назначение ответственных за реализацию плана.
* **Методы оценки эффективности**: Периодическая проверка и аудиты.

### 9. Содержание плана обеспечения непрерывной работы АС

* **Оценка критических процессов**: Определение ключевых бизнес-функций.
* **Стратегии восстановления**: Разработка сценариев восстановления системы после сбоев.
* **Распределение ресурсов**: Определение ресурсов для обеспечения непрерывности работы.
* **Обучение и тренировки персонала**: Подготовка сотрудников к действиям в чрезвычайных ситуациях.
* **Мониторинг и обновление**: Регулярное обновление плана в соответствии с изменениями в бизнесе.

Вывод: В ходе работы была рассмотрена система этапов разработки концепции и создания системы информационной безопасности (ИБ) в автоматизированных системах (АС) предприятия. Основное внимание уделялось ключевым шагам, необходимым для формирования эффективной системы защиты информации. Освоение этапов, таких как анализ текущей инфраструктуры, определение рисков, разработка политики безопасности и реализация технических мер, подтверждает необходимость комплексного подхода к обеспечению информационной безопасности.

Важно отметить, что успешная реализация концепции ИБ требует не только применения технологий, но и вовлечения всего персонала, что обеспечивает интеграцию политики безопасности на всех уровнях предприятия. Кроме того, регулярный мониторинг и аудит системы безопасности способствуют ее адаптации к изменяющимся угрозам и условиям.

Таким образом, освоение этапов разработки концепции и создания системы ИБ позволяет обеспечить защиту информационных активов, минимизировать риски и гарантировать непрерывность бизнес-процессов, что является важной задачей для любого предприятия в условиях быстро меняющейся информационной среды.