|  |  |
| --- | --- |
| **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 №4

**«РАЗРАБОТКА ПОЛИТИКИ 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 №4 «РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ»:**

**Задание**

1. Провести аудит информационных процессов фирмы и оценить риски угроз.
2. Разработать политику безопасности фирмы.
3. Составить матрицу доступа к конфиденциальной информации.
4. Провести аудит безопасности предприятия.

**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. Аудит информационных процессов и оценка рисков угроз

*Шаги:*

* Сбор данных: Провести интервью с сотрудниками для понимания текущих информационных процессов. Просмотр документации и отчетов.
* Идентификация угроз: Определить возможные угрозы, такие как кибератаки, утечка данных, человеческий фактор.
* Оценка рисков: Использовать стандартные методологии (например, STRIDE или PESTLE) для оценки вероятности и влияния каждого риска.

*Пример рисков:*

* Низкая защита от кибератак (например, DDoS).
* Неправильное управление доступом к данным.
* Отсутствие регулярного резервного копирования.

2. Разработка политики безопасности фирмы

Основные элементы политики:

* Цели безопасности: Защита конфиденциальной информации, обеспечение доступности и целостности данных.
* Соблюдение законов: Соответствие GDPR и локальному законодательству.
* Управление доступом: Правила по предоставлению и отзыву доступа.
* Обучение персонала: Обязанности по обучению сотрудников безопасности.
* Реакция на инциденты: Процедуры по реагированию на инциденты безопасности.

3. Матрица доступа к конфиденциальной информации

| Должность | Доступ к проектам | Доступ к данным клиентов | Доступ к финансовым данным | Комментарии |
| --- | --- | --- | --- | --- |
| Разработчик | Часть проектов | Нет | Нет | Ограниченный доступ |
| Менеджер проектов | Полный доступ | Полный доступ | Нет | Ответственен за проекты |
| Финансовый аналитик | Нет | Нет | Полный доступ | Доступ только к финансовым данным |
| Администратор системы | Полный доступ | Полный доступ | Полный доступ | Должен обеспечить безопасность |

4. Аудит безопасности предприятия

Методы аудита:

* Тестирование на проникновение: Оценка уязвимостей в системе.
* Анализ конфигураций: Проверка серверов, сетевых устройств и приложений на наличие безопасных настроек.
* Оценка физической безопасности: Проверка доступа к офисам и серверным.
* Проверка соблюдения политик: Убедиться, что сотрудники следуют установленным правилам безопасности.

Итоговые рекомендации:

* Составить план исправлений для выявленных уязвимостей.
* Регулярные тренировки по безопасности.
* Поддержание актуальности программного обеспечения.

**Контрольные вопросы:**

1. Политика безопасности фирмы

Политика безопасности фирмы — это набор документированных правил, норм и процедур, определяющих, как организация будет защищать свои информационные активы и данные. Эта политика включает в себя стратегии по управлению рисками, контроль доступа, предписание пользователей и установление ответственности, а также реагирование на инциденты.

2. Подготовительный этап при разработке политики безопасности

Подготовительный этап включает в себя:

* Оценку рисков: Анализ потенциальных угроз и уязвимостей информационных систем.
* Определение активов: Идентификация и классификация всех информационных активов компании.
* Сбор информации: Изучение существующих правил и стандартов безопасности, а также анализа опыта других организаций.
* Анализ потребностей и ожиданий: Опрос ключевых сотрудников и заинтересованных сторон для понимания их потребностей в области безопасности.

3. Содержание политики безопасности

Содержание политики безопасности может включать:

* Цели и задачи безопасности.
* Область применения: Определение, какие активы и процессы находятся под защитой.
* Роли и ответственности: Назначение ответственных за политику и исполнение мероприятий безопасности.
* Стандартные процедуры: Описание мер по защите информации, управление инцидентами и реагирование.
* Обучение и повышение осведомленности: Программы обучения сотрудников по вопросам безопасности.
* Мониторинг и аудит: Процедуры контроля за соблюдением политики.

4. Принцип разумной достаточности

Принцип разумной достаточности предполагает, что меры безопасности должны быть пропорциональны уровням риска и стоимости потерь. Это означает, что организация должна реализовывать такие меры безопасности, которые обеспечивают баланс между защитой информации и доступностью ресурсов.

5. Общие рекомендации для обеспечения безопасности компьютерной информации

* Регулярные обновления ПО: Обновляйте операционные системы и приложения для защиты от уязвимостей.
* Управление доступом: Используйте многофакторную аутентификацию и управляйте правами пользователей.
* Шифрование данных: Защищайте важные данные с помощью шифрования.
* Резервное копирование: Регулярно создавайте резервные копии данных и проводите тестирование на восстановление.
* Обучение сотрудников: Повышайте уровень осведомленности сотрудников о возможных угрозах и безопасных практиках.

6. Аудит безопасности

Аудит безопасности — это систематический процесс оценки уровня безопасности информационных систем и соответствия установленным политикам и стандартам. Он проводится с использованием множества методов, таких как:

* Интервью с ключевыми сотрудниками.
* Проверка документации: Анализ политик, процедур и отчетов.
* Тестирование систем: Проводится тестирование на уязвимости и оценка защищенности через пентесты.
* Сравнение с стандартами: Сравнение практик безопасности с принятыми стандартами (например, ISO, NIST).

Результаты аудита, как правило, оформляются в виде отчета с рекомендациями по улучшению системы безопасности.

**Вывод:** в ходе выполнения лабораторной работы: эффективная политика безопасности фирмы основывается на комплексном подходе, который включает аудит информационных процессов, оценку рисков и разработку четких норм и правил для защиты конфиденциальной информации. Важными аспектами являются определение ролей и обязанностей сотрудников, применение принципа разумной достаточности при разработке мер безопасности и обеспечение регулярной проверки безопасности. Это позволит минимизировать риски угроз, повысить уровень защиты данных и создать культуру безопасности в организации.