**Оценочный материал для промежуточной аттестации по дисциплине «Управление информационной безопасностью» 6 семестр**

| | |
|---|---|
| Квалификация выпускника | **бакалавр** |
| Направление подготовки | **09.03.02** |
| | **Информационные системы и технологии** |
| Направленность (профиль) | **Безопасность информационных систем и технологий** |
| | *наименование* |
| Форма обучения | **очная** |
| Кафедра разработчик | **Информатики и вычислительной техники** |
| | *наименование* |
| Выпускающая кафедра | **Информатики и вычислительной техники** |
| | *наименование* |

# Типовые задания для контрольной работы:

## Практическое задание № 1.

Это практическое задание поможет студентам углубить свои знания о социальной инженерии, анализировать статистические данные, а также разрабатывать рекомендации в области информационной безопасности. Оно также обучит студентов практическим навыкам разработки рекомендаций, основанных на анализе данных

**Цель работы** – *разработка рекомендаций по предотвращению социальной инженерии.*

**Шаги выполнения:**

- Анализ статистических данных: Используя информацию из надежных источников, изучите статистические данные о случаях социальной инженерии, такие как обман и мошенничество, связанные с информационной безопасностью. Определите наиболее распространенные методы и тенденции.
- Изучение случаев: Ознакомьтесь с реальными случаями социальной инженерии, которые получили значительную огласку и имели значимые последствия для компаний или пользователей. Проанализируйте, какими методами и техниками злоумышленники воспользовались, и какая информация была скомпрометирована.
- Составление рекомендаций: Используя полученные знания и анализируя статистические данные, разработайте рекомендации для пользователей по предотвращению проблем, связанных со социальной инженерией. Обращайте внимание на важность обучения персонала, установку надежных паролей, осведомленность о видах атак и подозрительном поведении, а также основные принципы безопасности.
- Представление результатов: Создайте электронный документ или презентацию, в которых подробно изложите свои рекомендации и подкрепите их фактами и статистикой. Объясните простым и понятным языком, почему каждая рекомендация важна и как она поможет предотвратить проблемы социальной инженерии.

## Практическое задание № 2.

Это практическое задание поможет студентам изучить на практике разработку плана реагирования на нарушение информационной безопасности и осознать необходимость готовности к таким событиям для эффективного управления информационной безопасностью

**Цель работы** – *разработка плана реагирования на случай нарушения информационной безопасности для организации.*

**Шаги выполнения:**

- Изучение схемы работы и важных процессов организации: Понимая специфику и основные цели организации, изучите схему работы и важные процессы, связанные с информационной безопасностью. Определите возможные виды нарушений информационной безопасности, которые могут возникнуть.
- Анализ и классификация нарушений: Проанализируйте типичные нарушения, которые могут произойти в организации, и классифицируйте их по уровню серьезности и количеству получаемого ущерба. Определите главного ответственного за каждый вид нарушения.

- Разработка плана реагирования: На основе анализа и классификации нарушений, разработайте план реагирования, включающий основные шаги и процессы, которые необходимо выполнить в случае нарушения безопасности. Установите целевые сроки для каждого шага и определите ответственность. Включите меры предотвращения и меры для устранения последствий нарушения.
- Тестирование плана: Проведите тестирование разработанного плана реагирования с помощью симуляций и ролевых игр. Оцените эффективность плана и произведите необходимые корректировки.
- Представление результатов: Создайте документ или презентацию, в которых подробно изложите разработанный план реагирования на нарушение информационной безопасности. Объясните основные шаги и процессы, а также рекомендуемые меры предотвращения. Обсудите план с ключевыми заинтересованными сторонами и получите их отзыв.

## Типовые вопросы к зачету:

1. Что такое информационная безопасность и какие основные принципы ее обеспечения?
2. Какие основные угрозы информационной безопасности существуют?
3. Что такое уязвимости информационных систем и как их классифицировать?
4. Что такое риск информационной безопасности и как оценивать риски?
5. Какие этапы включает процесс управления рисками в информационной безопасности?
6. Какие меры по защите информации можно использовать для снижения рисков?
7. Что такое политика информационной безопасности и как ее разрабатывать?
8. Какие основные принципы и методы криптографии используются для защиты информации?
9. Что такое аутентификация и какие виды аутентификации существуют?
10. Какие методы защиты информации от сетевых атак и киберугроз существуют?
11. Что такое периметр безопасности и как его обеспечить?
12. Какие меры по обеспечению физической безопасности информационных систем используются?
13. Что такое мониторинг и аудит информационной безопасности и как их проводить?
14. Какие основные этапы включает процесс планирования и восстановления после инцидентов информационной безопасности?
15. Какие методы и инструменты используются для обучения персонала в области информационной безопасности?
16. Что такое социальная инженерия и как ее предотвращать?
17. Какие меры обеспечивают конфиденциальность информации?
18. Какие меры обеспечивают целостность информации?
19. Какие меры обеспечивают доступность информации?
20. Что такое защита от несанкционированного доступа и как ее реализовать?
21. Какие нормативно-правовые акты регулируют информационную безопасность?
22. Что такое стеганография и как она применяется для скрытой передачи информации?
23. Какие основные требования предъявляются к системам управления информационной безопасностью?
24. Какие методы и средства защиты информации применяются в системах хранения данных?
25. Что такое дискреционный и мандатный контроль доступа к информации?
26. Какие меры безопасности применяются в сетях передачи данных?
27. Что такое бекап и как его проводить?
28. Какие методы шифрования информации существуют и как выбрать подходящий метод?
29. Какие методы и инструменты используются для обнаружения и предотвращения вторжений в информационную систему?
30. Какие особенности безопасности сетей Wi-Fi можно выделить и как их обеспечить?
31. Что такое вредоносное программное обеспечение и как его обнаружить и удалить?

32. Какие основные этапы включает процесс реагирования на инциденты информационной безопасности?
33. Какие методы исследования компьютерных преступлений существуют?
34. Что такое этический хакинг и как его применять для повышения безопасности?
35. Какие инструменты и методы используются для проведения анализа рисков в информационной безопасности?
36. Что такое физический анализ безопасности и как его проводить?
37. Какие требования предъявляются к обработке персональных данных с точки зрения информационной безопасности?
38. Что такое программирование с учетом безопасности и как его осуществлять?
39. Какие особенности безопасности имеют мобильные устройства и как их защитить?
40. Какие требования предъявляются к безопасности электронной почты и как ее обеспечить?
41. Что такое системы управления и контроля доступом и как их задействовать для информационной безопасности?
42. Какие методы социальной инженерии используются для атак на информационные системы и как их предотвращать?
43. Какие этапы включает процесс анализа уязвимостей информационных систем?
44. Что такое защита от DDoS-атак и какие методы применяются для защиты?
45. Какие требования предъявляются к безопасности web-приложений и как их обеспечить?
46. Какие меры безопасности можно применить на этапе разработки программного обеспечения?
47. Что такое инцидент информационной безопасности и как им реагировать?
48. Какие требования предъявляются к безопасности в операционных системах и каких методов обеспечения безопасности использовать?