Оценочный материал для промежуточной аттестации по дисциплине «Разработка и эксплуатация защищенных информационных систем»

Квалификация выпускника: **бакалавр**

Направление подготовки: **09.03.02**

Информационные системы и технологии

Направленность (профиль): **Информационные системы и технологии**

наименование

Форма обучения: **очная**

Кафедра разработчик: **Информатики и вычислительной техники**

наименование

Выпускающая кафедра: **Информатики и вычислительной техники**

наименование

Типовое задания для контрольной работы:

Практическое задание № 1.

Цель работы – *разработать и протестировать защиту информационной системы*.

Необходимое оборудование:

- Компьютер со специализированным программным обеспечением для разработки информационных систем.
- Сервер для размещения защищенных информационных систем.
- Сетевое оборудование для создания и поддержки сетевой инфраструктуры.
- Защитные системы и программы, такие как антивирусное программное обеспечение, брандмауэры и т.д.

Шаги выполнения:

- Исследование требований к защищенной информационной системе. Определение основных функциональных требований.
- Проектирование архитектуры защищенной информационной системы. Разработка диаграмм, описание логики работы системы, определение используемых технологий и протоколов.
- Разработка и тестирование программного кода для защищенной информационной системы. Реализация функциональности системы, включая механизмы безопасности (аутентификация, авторизация, шифрование данных и т.д.).
- Установка и настройка оборудования. Развертывание сервера, настройка сетевого оборудования и приложений.
- Тестирование и анализ системы на безопасность. Проведение тестов на проникновение, анализ уязвимостей и исправление обнаруженных ошибок.
- Запуск и эксплуатация защищенной информационной системы. Поддержка и сопровождение работы системы, обновление компонентов безопасности в соответствии с требованиями.

Типовые вопросы к зачету:

1. Что такое защищенная информационная система?
2. Какие основные принципы безопасности необходимо учитывать при разработке защищенных информационных систем?
3. Какую роль играет аутентификация в защищенных информационных системах?
4. Что такое атаки на информационные системы и какие виды атак существуют?
5. Каким образом можно защитить информационные системы от вредоносного программного обеспечения?
6. Что такое шифрование информации и для чего оно используется в защищенных информационных системах?
7. Какие методы можно применять для обеспечения безопасности данных в защищенных информационных системах?
8. Что такое брандмауэр и какую роль он играет в защите информационных систем?
9. Что такое аудит безопасности информационной системы и какие задачи он решает?
10. Какие методы могут использоваться для защиты от DDoS-атак?
11. Что такое уязвимости информационных систем и какие виды уязвимостей существуют?
12. Какие основные принципы следует соблюдать при проектировании сетевой инфраструктуры для защищенных информационных систем?
13. Что такое многофакторная аутентификация и как она обеспечивает безопасность?
14. Какие методы можно использовать для обеспечения конфиденциальности данных в защищенных информационных системах?
15. Каковы основные этапы жизненного цикла защищенной информационной системы?
16. Какие политики безопасности обычно применяются в защищенных информационных системах?
17. Что такое атаки на службу аутентификации и какие методы могут быть использованы для предотвращения таких атак?
18. Какие методы можно применять для предотвращения атак на переполнение буфера?
19. Что такое системы обнаружения вторжений и какую роль они играют в защищенных информационных системах?
20. Каким образом можно защитить информационные системы от социальной инженерии?
21. Что такое резервное копирование данных и какое значение оно имеет для защищенных информационных систем?
22. Какие механизмы могут использоваться для обнаружения и предотвращения атак на защищенные информационные системы?
23. Что такое атаки на отказ в обслуживании и какие методы можно использовать для защиты?
24. Что такое системы контроля доступа и какую роль они играют в защищенных информационных системах?
25. Какие методы можно использовать для обнаружения скрытого программного обеспечения в информационных системах?
26. Что такое методы идентификации и аутентификации пользователей в защищенных информационных системах?
27. Какие методы можно использовать для защиты от фишинг-атак?
28. Что такое взлом паролей и как можно предотвратить такие атаки?
29. Каким образом можно организовать контроль целостности данных в защищенных информационных системах?
30. Что такое атаки на службу авторизации и какие методы можно применять для их предотвращения?
31. Какие методы могут использоваться для обеспечения безопасности беспроводных сетей в защищенных информационных системах?
32. Что такое системы мониторинга безопасности и какую роль они играют в защищенных информационных системах?
33. Каким образом можно защитить информационные системы от перехвата и подмены данных?
34. Что такое межсетевые экраны и какую роль они играют в защите информационных систем?
35. Каким образом можно защитить информационные системы от атак через веб-приложения?

36. Что такое защита от входной атаки и какую роль она играет в защищенных информационных системах?
37. Какие методы могут использоваться для защиты информации от несанкционированного доступа?
38. Что такое системы аварийного восстановления и какое значение они имеют для защищенных информационных систем?
39. Каким образом можно защитить информационные системы от внутренних угроз?
40. Что такое методы шифрования данных и как они могут быть применены для обеспечения безопасности информационных систем?
41. Какие методы могут использоваться для обнаружения и предотвращения атак на сетевую инфраструктуру защищенных информационных систем?
42. Что такое атаки на службу хранения данных и какие методы можно использовать для их предотвращения?
43. Каким образом можно обеспечить безопасность при передаче данных в защищенных информационных системах?
44. Что такое методы слежения за информационной системой и какие есть способы их реализации?
45. Каким образом можно защитить информационные системы от внутренней неряшливости?
46. Что такое защита информации от утери и какую роль она играет в защищенных информационных системах?
47. Какие методы могут использоваться для предотвращения атак на защищенную информационную систему с помощью перехвата данных?
48. Что такое методы скрытия информации и как можно применять их в защищенных информационных системах?
49. Каким образом можно защитить информационные системы от атак на службу классификации данных?
50. Что такое постоянный анализ безопасности и какую роль он играет в защищенных информационных системах?