Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 19.06.2024 06:15:49
Уникальный программный ключ:
e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

Оценочные материалы для промежуточной аттестации по дисциплине

Риски и безопасность, 3 семестр

Код, направление подготовки	09.04.01 Информатика и вычислительная техника
Направленность (профиль)	Информационное и программное обеспечение
Форма обучения	Очная
Кафедра разработчик	Автоматизированных систем обработки информации и управления
Выпускающая кафедра	Автоматизированных систем обработки информации и управления

Типовые задания для контрольной работы:

Примерные вопросы для контрольной работы:

1. Актуальности проблемы защиты информации. Основные факторы повышения уязвимости информации. Риски в промышленности.
2. Основные понятия информационной безопасности. Российское и международное законодательство.
3. Российское законодательство по защите информационных технологий. Нормативно-правовая информация.
4. Системы защиты от несанкционированного доступа в операционных системах и локальных сетях передачи данных.
5. Методы и средства защиты информации в Internet.
6. Политики безопасности.
7. Организация секретного делопроизводства и мероприятий по защите информации.
8. Программно-технические методы и средства защиты информации.
9. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера.
10. Разработка программного макета системы шифрования информации методом Вернама.
11. Генерация псевдослучайных последовательностей чисел в системах защиты информации.
12. Американский стандарт шифрования данных DES.
13. Отечественный стандарт шифрования данных (ГОСТ 28147-89).
14. Алгоритм шифрования Диффи-Хеллмана.
15. Однонаправленные хэш-функции.
16. Электронная цифровая подпись
17. Применение функций хеширования в идентификации и проверке подлинности.
18. Алгоритмы MD5, SSH.
19. Основные функций межсетевых экранов для фильтрации сообщений и защиты информации.
20. Защита от отладок и дизассемблирования.
21. Способы встраивания защитных механизмов в программное обеспечение.

22. Методы перехвата и навязывания информации.
23. Методы внедрения программных закладок.
24. Компьютерные вирусы как особый класс разрушающих программных воздействий.
25. Защита от разрушающих программных воздействий.
26. Классификация систем защиты носителей информации.
27. Методы и средства защиты носителей информации.
28. Виды информационных ресурсов. Способы защиты информационных ресурсов от несанкционированного доступа.
29. Способы защиты информационных ресурсов от несанкционированного доступа.
30. Основные виды атак на протоколы аутентификации.
31. Основные приемы предотвращения атак.
32. Вопросы защиты авторского права (имущественные и неимущественные права).

***Типовые вопросы к экзамену*:**

1. Актуальности проблемы защиты информации.
2. Основные факторы повышения рисков, связанных со способами сбора, обработки, представления информации.
3. Актуальность угроз и рисков связанных с составом и функциональными возможностями современных информационных технологий и программных средств
4. Перечислить риски в промышленности.
5. Основные понятия информационной безопасности.
6. Российское и международное законодательство.
7. Российское законодательство по защите информационных технологий.
8. Основные законы связанные с защитой информации.
9. Принципы использования законодательных норм.
10. Перечислите основные законы РФ связанные с информационной безопасностью.
11. Основные положения Федерального закона №149.
12. Основные положения Федерального закона №152.
13. Способы и подходы к поиску основных законодательных актов РФ в области защиты информации.
14. Проблемы защиты информации в информационных системах.
15. Риски возникновения проблем защиты информации при проектировании и разработке информационных и автоматизированных систем.
16. Способы сбора, обработки и представления информации с учетом современных требований информационной безопасности.
17. Системы защиты от несанкционированного доступа в операционных системах и локальных сетях передачи данных.
18. Политики безопасности.
19. Содержание системы средств защиты компьютерной информации в информационных системах.
20. Компоненты средств защиты в информационных системах.
21. Методы и подходы к анализу средств защиты информации при проектировании информационных и автоматизированных систем.
22. Методы и подходы к анализу средств защиты информации при разработке информационных и автоматизированных систем.
23. Подходы к проведению теоретического исследования для выявления рисков.
24. Подходы к проведению экспериментального исследования для выявления рисков.

25. Риски использования сети Internet.
26. Подходы к оценке рисков в сети Internet.
27. Методы и средства защиты информации в Internet.
28. Политики безопасности в сети Internet.
29. Программно-технические методы и средства защиты информации в сети Internet.
30. Виды информационных ресурсов в сети Internet.
31. Способы защиты информационных ресурсов от несанкционированного доступа в сети Internet.
32. Методы идентификации и проверки подлинности пользователей компьютерных систем сети Internet.
33. Основные функций межсетевых экранов для фильтрации сообщений и защиты информации.
34. Методы перехвата и навязывания информации.
35. Компьютерные вирусы как особый класс разрушающих программных воздействий.
36. Виды вредоносных программ.
37. Защита от разрушающих программных воздействий.
38. Защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.
39. Программные и технические средства противодействия вредоносному ПО.
40. Технологии и методы борьбы с угрозами от воздействия вредоносного ПО.
41. Способы встраивания защитных механизмов в программное обеспечение.
42. Защита программы от отладок и дизассемблирования
43. Методы расчёта рисков.
44. Методы оценки и анализа рисков.
45. Подходы к формированию комплексной защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.
46. Защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.
47. Способы встраивания защитных механизмов в программное обеспечение.
48. Классификация систем защиты носителей информации.
49. Методы и средства защиты носителей информации.
50. Виды информационных ресурсов. Способы защиты информационных ресурсов от несанкционированного доступа.
51. Классификация систем защиты носителей информации.
52. Методы защиты носителей информации.
53. Средства защиты носителей информации. Способы защиты информационных ресурсов от несанкционированного доступа.