Оценочные материалы для промежуточной аттестации по дисциплине

Методы защиты информации, 7 семестр

Код, направление подготовки	09.03.02 Информационные системы и технологии
Направленность (профиль)	Информационные системы и технологии
Форма обучения	Очная
Кафедра разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

Типовые задания для контрольной работы:

Примерные вопросы для контрольной работы:

1. Актуальность проблемы защиты информации.
2. Основные факторы повышения уязвимости информации.
3. Перечислить риски в промышленности связанные с ИТ.
4. Актуальность защиты информации, связанной с составом и функциональными возможностями современных ИТ.
5. Основные понятия информационной безопасности.
6. Уязвимости вычислительных систем, связанные с физическими процессами, протекающими в них.
7. Уязвимости информационных и вычислительных систем, связанные с спецификой реализации математических и логических вычислений.
8. Информационные ресурсы сбора информации об уязвимостях и рисках информационных и вычислительных систем.
9. Перечислите основные законы РФ связанные с информационной безопасностью.
10. Основные положения Федерального закона №149.
11. Основные положения Федерального закона №152.
12. Способы и подходы к поиску основных законодательных актов РФ в области защиты информации.
13. Перечислить риски возникновения проблем защиты информации при проектировании и разработке информационных и автоматизированных систем.
14. Проблемы сбора, обработки и представления информации с учетом современных требований информационной безопасности на всех уровнях жизненного цикла.
15. Системы защиты от несанкционированного доступа в операционных системах и локальных сетях передачи данных.
16. Политики безопасности.
17. Организация секретного делопроизводства и мероприятий по защите информации.

18. Программно-технические методы и средства защиты информации.
19. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера.
20. Методы и подходы исследования для выявления рисков.

***Типовые вопросы к зачёту*:**

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).