Оценочные материалы для промежуточной аттестации по дисциплине

Управление корпоративной информационной безопасности,
3 семестр

Код, направление подготовки	09.04.02 Информационные системы и технологии
Направленность (профиль)	Управление данными
Форма обучения	Очная
Кафедра разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

Типовые задания для контрольной работы:

Примерные задания для контрольной работы:

1. Расположите события в порядке уменьшения вероятности: 1) Угадать случайный 128-битный AES-ключ с первой попытки. 2) Выиграть в лотерею с 1 000 000 участников (вероятность одна миллионная) 3) Выиграть в такую лотерею 5 раз подряд 4) Выиграть в такую лотерею 6 раз подряд. 5) Выиграть в такую лотерею 7 раз подряд.

2. Предположим, что за $200 можно собрать компьютер, который перебирает около 1 млрд. AES-ключей в секунду. Предположим, одна организация хочет запустить полный перебор для поиска одного AES-ключа(128бит) и может потратить 4 триллиона долларов ($4*10^12). Сколько времени потребуется для подбора этого ключа с помощью таких компьютеров? Доп. расходы не учитывать.

3. Сжатие часто используется при хранении и передаче данных. Предположим вы хотите совместить сжатие и шифрование. Какая последовательность имеет больший смысл?

4. Используя шифр Цезаря (сдвига) зашифруйте сообщение. Проведите криптоанализ сообщения.

5. Используя шифр табличной перестановки зашифруйте сообщение. Проведите криптоанализ сообщения.

6. Для шифрования использовался одноразовый ключ (метод одноразового блокнота).Каждый символ исходного сообщения был представлен в 16-ричном виде по таблице ASCII. Зашифрованное сообщение получено операцией XOR символов исходного текста и ключа. Исходное сообщение: "attack at dawn", зашифрованное сообщение: "09 e1 c5 f7 0a 65 ac 51 94 58 e7 e5 3f 36". Подмените исходное

сообщение на "attack at dusk". Какое будет зашифрованное сообщение при использовании того же ключа? Восстановите ключ шифрования целиком.

7. Выработать общий секретный ключ по алгоритму Диффи-Хэллмана.

8. Используя статистические закономерности, расшифруйте предложенный текст, зашифрованный методом замены «ЁЫДЖ ТВЁЁЯЪЖ,….. ОХЮФХЧДЖЛЖЪП»

***Типовые вопросы к экзамену*:**

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. Генерация псевдослучайных последовательностей чисел в системах защиты информации.
11. Американский стандарт шифрования данных DES.
12. Отечественный стандарт шифрования данных (ГОСТ 28147-89).
13. Алгоритм шифрования Диффи-Хеллмана.
14. Однонаправленные хэш-функции.
15. Электронная цифровая подпись
16. Применение функций хеширования в идентификации и проверке подлинности.
17. Алгоритмы MD5, SSH.
18. Основные функций межсетевых экранов для фильтрации сообщений и защиты информации.
19. Защита от отладок и дизассемблирования.
20. Способы встраивания защитных механизмов в программное обеспечение.
21. Методы перехвата и навязывания информации.
22. Методы внедрения программных закладок.
23. Компьютерные вирусы как особый класс разрушающих программных воздействий.
24. Защита от разрушающих программных воздействий.
25. Классификация систем защиты носителей информации.
26. Методы и средства защиты носителей информации.
27. Виды информационных ресурсов. Способы защиты информационных ресурсов от несанкционированного доступа.
28. Способы защиты информационных ресурсов от несанкционированного доступа.
29. Основные виды атак на протоколы аутентификации.
30. Основные приемы предотвращения атак.
31. Вопросы защиты авторского права (имущественные и неимущественные права).