Перечень экзаменационных вопросов и задач

Дисциплина	МДК.02.02 Криптографические средства защиты информации
Преподаватели	Голубев Дмитрий Дмитриевич Асейкина Ксения Романовна
Группы	БИ50-1-23, БИ50-11/1-24 БИ50-2-23, БИ50-11/2-24 БИ50-3-23, БИ50-11/3-24 БИ50-4-23 БИ50-5-23
Специальность	10.02.05 Обеспечение информационной безопасности автоматизированных систем
Семестр	6(4)
Форма контроля	экзамен

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Модуль 1. Асейкина Ксения Романовна

1. Дайте определение криптологии и охарактеризуйте две её основные составляющие: криптографию и криптоанализ. В чём разница между их задачами?

2. Что такое криптографическая стойкость? Какие факторы её определяют и чем она отличается от простой сложности алгоритма?

3. Опишите базовую терминологию шифрования: алфавит, открытый текст, шифр (шифротекст), алгоритм шифрования. Каково назначение каждого элемента?

4. Что такое ключ в криптографии? Какие существуют стандарты размера ключей?

5. Дайте определения шифрованию, дешифрованию и кодированию. В чём принципиальная разница между шифрованием и кодированием?

6. Опишите симметричные и асимметричные криптосистемы. В чём их принципиальное отличие? Приведите примеры использования каждой.

7. Что такое открытый и закрытый ключи в асимметричной криптографии? Как они связаны между собой и для чего используется каждый из них?

8. Дайте определения блочного и поточного (потокового) шифрования. В чём состоят фундаментальные отличия их алгоритмических принципов?

9. Что такое аутентичность в криптографии? Какими механизмами она обеспечивается и как связана с ЭЦП и ПЭП?

10. Дайте определения КЭП, НЭП и ПЭП. В чём их различия по юридической силе и технической реализации?

11. Что такое сертификат, центр сертификации и самоподписанный сертификат? Опишите их роль в инфраструктуре открытых ключей (PKI).

12. Что такое ГПСЧ? В каких криптографических задачах он применяется и каким требованиям должен отвечать?

13. Дайте определение криптографической хеш-функции, хеша и процесса хеширования. Перечислите основные свойства криптографических хеш-функций.

14. Опишите атаку «дней рождения» и парадокс дней рождения. Как они связаны с поиском коллизий в хеш-функциях? Что такое радужные таблицы и для чего они используются?

15. Что такое стеганография? Перечислите основные виды стеганографии и объясните, чем она принципиально отличается от криптографии.

Модуль 2. Голубев Дмитрий Дмитриевич

16. Перечислите основные виды чисел. Сформулируйте основную теорему арифметики.

17. Дайте определения обратных чисел по сложению и по умножению для обычной арифметики. Приведите примеры.

18. Дайте определения обратных элементов по сложению и по умножению по модулю числа. Как они вычисляются?

19. Опишите алгоритм разложения числа на простые множители. Каковы назначение и принцип работы расширенного алгоритма Евклида в контексте работы с модулярной арифметикой?

20. Что такое функция Эйлера? Как она вычисляется? Дайте определение взаимно-простым числам и приведите примеры.

21. Дайте определение вычета, класса вычетов, полной системы вычетов и приведённой системы вычетов. В чём разница между полной и приведённой системами?

22. Опишите моноалфавитные и полиалфавитные шифры. В чём их принципиальное различие и как это влияет на криптостойкость?

23. Что такое частотный анализ и против каких шифров он эффективен? Почему полиалфавитные шифры устойчивее к этому методу?

24. Перечислите 5 основных операций алгебры логики и объясните принцип их работы. Что такое элементарные высказывания?

25. Дайте определения тождественно-истинных и тождественно-ложных функций. Что такое нормальная форма в алгебре логики?

26. Объясните, что такое СДНФ и СКНФ. В чём их отличие от обычных ДНФ и КНФ?

27. Что такое гамма в криптографии? Опишите процесс генерации гаммы и её основные свойства.

28. В чём отличие гаммы от ключа? Почему эти понятия не являются синонимами?

29. Опишите процесс гаммирования (шифрование и дешифрование). Какую роль в этом процессе играет операция XOR и почему она обратима?

30. Что такое ИСЧ и ПСЧ? В чём их разница, преимущества и недостатки? Как они связаны с гаммой?

31. Объясните принцип работы One-Time Pad (шифр Вернама). Почему он теоретически абсолютно стоек и каково его главное ограничение на практике?

ПРАКТИЧЕСКАЯ ЧАСТЬ

1. Решение системы Китайской теоремы об остатках (КТО) из n уравнений

2. Решение одного случайного задания из следующего списка:
   - Сравнения первой степени
   - Возведение в степень по модулю
   - Линейные диофантовы уравнения