Перечень вопросов для подготовки к экзамену по учебной дисциплине:

«ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ В ОТКРЫТЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ»

1. Свойства алгебраических структур групп < G = {…}, ·>. Конечные и бесконечные группы. Порядок группы.
2. Алгебраические структуры подгруппы H.
3. Алгебраические структуры циклические подгруппы (<*a*>).
4. Получение циклических подгрупп из групп < *Zn*, +> алгебраических структур.
5. Получение циклических подгрупп из групп < *Zn**, ×> алгебраических структур.
6. Алгебраические структуры циклические группы.
7. Использование теоремы Лагранжа для быстрого определения порядков потенциальных подгрупп алгебраических структур.
8. Алгебраическая структура кольцо <R = {…}, ·, □>. Коммутативное кольцо.
9. Алгебраическая структура поле <F = {…}, ·, □>. Конечное и бесконечное поле.
10. Алгебраическая структура поле Галуа GF (p^n).
11. Сопоставительный анализ алгебраических структур групп, колец и полей по операциям, используемым для систем шифрования данных.
12. Алгебраические структуры полей Галуа GF (p) для n-битовых слов.
13. Алгебраические структуры полей Галуа GF (2^n) для n-битовых слов.
14. Представление n-битовых слов в алгебраических структурах на основе полиномиального выражения степени (n – 1). Первое и второе упрощения. Расширенный полином.
15. Неприводимые полиномы.
16. Сложение полиномов в поле Галуа GF (2^n) для n-битовых слов.
17. Умножение полиномов в поле Галуа GF (2^n) для n-битовых слов.
18. Аддитивная и мультипликативная инверсия полинома с коэффициентами в поле Галуа GF (2^n) для n-битовых слов.
19. Нахождение мультипликативной инверсии в поле Галуа GF (2^n) для n-битовых слов.
20. Эффективный алгоритм умножения полиномов в полях Галуа GF (2^n) для n-битовых слов.
21. Спецификации стандарта AES. Криптостойкость алгоритма AES.
22. Схема шифрования данных стандарта AES.
23. Схема расшифрования шифртекстов стандарта AES.
24. Процедура Key Expansion() стандарта AES.
25. Атаки по сторонним (или побочным) каналам.
26. Алгоритмы IDEA, DES и ГОСТ 28147-89.
27. Режимы работы алгоритмов блочного шифрования.
28. Алгоритмы асимметричного шифрования данных.
29. Обеспечение конфиденциальности документа с ЭЦП.
30. Нормативно-правовая база РБ в области криптографической защиты информации.