Перечень вопросов для подготовки к экзамену по учебной дисциплине:

«СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ. Часть 1»

1. Обобщенная система криптографической связи.
2. Обобщенная схема симметричной криптосистемы.
3. Требования, предъявляемые к шифрам.
4. Требования, предъявляемые к криптографически стойкому генератору псевдослучайной последовательности чисел.
5. Американский стандарт шифрования данных DES: общие сведения, схемы шифрования данных, расшифрования шифртекстов и вычисления функции шифрования *f*.
6. Схемы вычисления ключей алгоритма DES на базе блоков циклического сдвига влево и вправо.
7. Режимы работы алгоритма DES. Электронная кодовая книга ECB.
8. Режимы работы алгоритма DES. Сцепление блоков шифра CBC.
9. Режимы работы алгоритма DES. Распространяющееся сцепление блоков шифра PCBC.
10. Режимы работы алгоритма DES. Обратная связь по шифртексту CFB.
11. Режимы работы алгоритма DES. Обратная связь по выходу OFB.
12. Режимы работы алгоритма DES. Режим счетчика CTR.
13. Режимы работы алгоритма DES. Режим DESX.
14. Режимы работы алгоритма DES. Режим 3DES EDE2.
15. Области применения алгоритма DES.
16. Алгоритм шифрования данных IDEA: схемы зашифрования данных и расшифрования шифртекстов, преимущества и недостатки алгоритма.
17. Зашифрование данных и расшифрование шифртекстов ГОСТ 28147-89 в режиме простой замены.
18. Зашифрование данных и расшифрование шифртекстов ГОСТ 28147-89 в режиме гаммирования.
19. Зашифрование данных и расшифрование шифртекстов ГОСТ 28147-89 в режиме гаммирования с обратной связью.
20. Режим выработки имитовставки ГОСТ 28147-89.
21. Алгоритм belt-block(X, K) стандарта СТБ 34.101.31-2020 при зашифровании данных.
22. Алгоритм belt-block^{-1}(Y, K) стандарта СТБ 34.101.31-2020 при расшифровании шифртекстов.
23. Блочные и поточные шифры.
24. Блочное шифрование данных с обратной связью.
25. Сопоставительный анализ стандартов DES, IDEA, ГОСТ 28147-89 и СТБ 34.101.31-2020.
26. Комбинирование блочных алгоритмов.
27. Расчет основных параметров алгоритма DES при зашифровании данных и расшифровании шифртекстов: вычисление матриц IP, IP^{-1}, функций E, S, P, PC–1 (G) и PC–2 (H).
28. Расчет основных параметров стандарта ГОСТ 28147-89: вычисление результатов на выходах CM_1, CM_2, CM_3, CM_4, CM_5 и R в соответствующих режимах (простой замены, гаммирования, гаммирования с обратной связью и выработки имитовставки).
29. Расчет основных параметров стандарта ГОСТ 28147-89: вычисление шифртекстов и открытых текстов в режимах гаммирования и гаммирования с обратной связью.
30. Расчет основных параметров алгоритмов зашифрования блока belt-block(X, K) и расшифрования блока belt-block^{-1}(Y, K) стандарта СТБ 34.101.31-2020.