List of questions for preparing for the exam in the academic discipline:
«SYMMETRICAL AND ASSYMETRIC CRYPTOSYSTEMS. Part 1»

1. Generalized cryptographic communication system.
2. Generalized scheme of a symmetric cryptosystem.
3. Requirements for ciphers.
4. Requirements for a cryptographically secure pseudo-random number sequence generator.
5. Standard DES: general information, data encryption schemes, decryption of ciphertexts and calculation of encryption functions *f*.
6. Schemes for calculating keys of the DES algorithm based on cyclic left and right shift blocks.
7. Operating modes of the DES algorithm. ECB mode.
8. Operating modes of the DES algorithm. CBC mode.
9. Operating modes of the DES algorithm. PCBC mode.
10. Operating modes of the DES algorithm. CFB mode.
11. Operating modes of the DES algorithm. OFB mode.
12. Operating modes of the DES algorithm. CTR mode.
13. Operating modes of the DES algorithm. DESX mode.
14. Operating modes of the DES algorithm. 3DES EDE2 mode.
15. Areas of application of the DES algorithm.
16. Standard IDEA: data encryption and ciphertext decryption schemes, advantages and disadvantages of the algorithm.
17. Standard GOST 28147-89: data encryption and ciphertext decryption in simple replacement mode.
18. Standard GOST 28147-89: data encryption and ciphertext decryption in gamma mode.
19. Standard GOST 28147-89: data encryption and ciphertext decryption in gamma mode with feedback.
20. Production mode of imitation insert GOST 28147-89.
21. The belt-block(X, K) algorithm of the STB 34.101.31-2020 standard when encrypting data.
22. The belt-block^{-1}(Y, K) algorithm of the STB 34.101.31-2020 standard when decrypting ciphertexts.
23. Block and stream ciphers.
24. Block encryption of data with feedback.
25. Comparative analysis of DES, IDEA, GOST 28147-89 and STB 34.101.31-2020 standards.
26. Combining block algorithms.
27. Calculation of the main parameters of the DES algorithm when encrypting data and decrypting ciphertexts: calculating matrices IP, IP^{-1}, functions E, S, P, PC–1 (G) and PC–2 (H).
28. Calculation of the main parameters of the GOST 28147-89 standard: calculation of results at the outputs CM_1, CM_2, CM_3, CM_4, CM_5 and R and in the corresponding modes (simple replacement, gamming, gamming with feedback and generating a simulation insert).
29. Calculation of the main parameters of the GOST 28147-89 standard: calculation of ciphertexts and plaintexts in gamma modes and gamma with feedback.
30. Calculation of the main parameters of the belt-block(X, K) block encryption and belt-block^{-1}(Y, K) block decryption algorithms of the STB 34.101.31-2020 standard.