List of questions for preparing for the exam in the academic discipline:
«SYMMETRICAL AND ASSYMETRIC CRYPTOSYSTEMS. Part 2»

1. Asymmetric cryptosystems: design features and information security.
2. One-way encryption functions based on discrete logarithm and factorization of large numbers. Irreversible trapdoor functions. One-way hash functions based on symmetric block-type encryption algorithms.
3. Schemes for using one-way encryption functions to control data integrity.
4. RSA algorithm: structural diagram of the cryptosystem, implementation stages, performance and level of information security.
5. Attacks on RSA cryptosystems.
6. Rabin's algorithm: structural diagram of the cryptosystem, stages of implementation, performance and level of information security.
7. Pohlig-Hellman algorithm: structural diagram of the cryptosystem, implementation stages, performance and level of information security.
8. El Gamal algorithm: structural diagram of the cryptosystem, stages of implementation, performance and level of information security.
9. Comparative analysis of asymmetric and symmetric cryptosystems.
10. Information security assessment of RSA, Rabin, Pohlig-Hellman and El Gamal algorithms.
11. Typical user identification and authentication schemes. Using a password to authenticate users. Simple authentication scheme. Authentication scheme using an identification table.
12. Authentication of the author of the document and the document itself using an electronic digital signature.
13. Formation of an electronic digital signature.
14. Ensuring the confidentiality of a document with an electronic digital signature.
15. RSA electronic digital signature algorithm.
16. El Gamal electronic digital signature algorithm.
17. Electronic digital signature algorithm DSA.
18. Mutual user authentication. Handshake procedure diagram.
19. Mutual user authentication. Continuous sender authentication scheme.
20. Simplified identification protocol with zero knowledge transfer Feige-Fiat-Shamir.
21. Parallel identification protocol with zero knowledge transfer.
22. Modified parallel identification protocol with zero knowledge transfer.
23. Gillow-Quiswater's zero knowledge transfer identification protocol.
24. User authentication using a reusable password in the CHAP protocol.
25. Key generation.
26. Key storage.
27. Key hierarchy concept.
28. Calculation of the main parameters of the RSA, Rabin, Pohlig-Hellman and El Gamal algorithms when encrypting data and decrypting ciphertexts: calculating keys, ciphertexts and messages.
29. Calculation of the main parameters of the RSA, El Gamal and DSA electronic digital signature algorithms: calculation of keys, digital signatures and verification equations.
30. Calculation of the main parameters of the Feige-Fiat-Shamir, parallel identification and Gillow-Quiswater identification protocols with zero knowledge transfer: calculation of secret keys.