Entrance tests

1. A theorem on the existence and uniqueness of the greatest common divisor (GCD0 of two polynomials.

2. A theorem on the dimension of the space of solutions of a homogeneous system of linear equations.

3. A theorem on the dimension of the sum of two subspaces.

4. A theorem on the rank of a matrix.

5. A theorem on the dimension of the space of solutions for a homogeneous system of linear equations.

6. Sylvester's criterion for the positive definiteness of a real quadratic form.

7. A theorem on the connection between the eigenvalues of the linear transformation with the roots of its characteristic polynomial.

8. A theorem on the connection between the dimensions of a kernel and the linear mapping image.

9. A theorem on the orthogonalisation of a linearly independent sequence of elements of the Euclidean space.

10. Normal divisors and factor groups, the first theorem on homomorphisms for groups.

11. Continuous functions. The Bolzano-Cauchy theorem on the intermediate values for functions that are continuous on an interval. Weierstrass's theorems on functions that are continuous on an interval (or, more generally, on a bounded closed set).

12. Rolle and Lagrange's theorems for differentiable functions. The Taylor formula with the remainder term in the form of Lagrange.

13. The definite Riemann integral over an interval. The existence theorem for a definite integral of a continuous function. Properties of an integral with variable upper limit: continuity and differentiability. The Newton-Leibniz formula.

14. Power series on a number line and in the complex plane. The circle and the radius of convergence of the power series; Calculating the radius of convergence of a power series.

Infinite differentiability of the sum of a power series.

15. Differentiability of a complex function of several variables; Derivative in the direction; gradient.

16. A theorem on the general solution of a linear homogeneous differential equation with constant coefficients (with proof for the case of simple roots).

17. A scheme of independent tests. Bernoulli's formula. Poisson's theorem.

18. The mathematical expectation of a random variable and its properties.

19. The law of large numbers (Chebyshev's inequality, Chebyshev's, Markov's and Bernoulli's theorems).

20. The representation of Boolean functions by formulas of the propositional algebra and Zhegalkin polynomials.

21. The closed classes of Boolean functions, the completeness criterion for Boolean functions.

22. The problem of the minimal skeleton and the Boruvka-Kraskal algorithm.

23. Dijkstra's algorithm for finding the shortest distances from the selected vertex to the remaining vertices of the graph.

24. Linear codes, the generating matrix, the Singleton boundary, the Plotkin boundary.

25. The control matrix, Hamming code, characterisation of the minimum distance in terms of the control matrix, the Hilbert-Varshamov boundary.

26. Cyclic codes. Codes that fix error packets, the Rager's boundary, an algorithm for fixing error packets.

27. The main parameters of error correcting codes, i.e. length, speed and minimum distance. The relationship between the minimum distance and the corrective capabilities of the code. The Hamming boundary.

28. Substitution and permutation ciphers (general definitions and specific examples). Absolutely persistent cipher of Vernam.

29. Symmetric (single-key) cryptosystems. The basic modes for encrypting long messages.

30. The RSA cryptosystem.

31. Information properties as a protection object.

32. Information protection strategies and models built on their basis.

33. The classification and definition of technical channels of information leakage. The main means and methods of protecting acoustic information from leakage via technical channels. Organizational and instrumental methods of detecting means of secret eavesdropping.

34. Principles of operation of signaling sensors of the infrared and radio engineering types. The construction of sensitive elements and paths of processing of alarm information. Requirements for the placement of sensors at the facility.

35. The general characteristics of control systems for physical and logical access to information objects. Password systems. The physical media of key information. Biometric systems. The comparative characteristics of the identification and authentication methods.

36. The principles of protection of the computer information stored on external computer media. The procedure for registration, issuance, storage, transfer and destruction of computer media with confidential data. Hardware-software tools for the guaranteed deletion of information. Methods for restoring information on magnetic media.

37. The main properties of the NTFS file system. The MFT concept. The MFT recording structure. The organisation of resident and non-resident files in NTFS. The EFS concept. The structure of the encrypted file.

38. Implementing the protection of computer information in Linux file systems. Features of EXT * FS file systems. The structure of metadata and their placement on the disk space. Access rights. Work with filesystem objects.

39. The security audit of computer systems. Goals, standards and approaches. Tools for auditing the security of computer systems, their capabilities and disadvantages.

40. Application of the dedicated software for information protection (GIS), their advantages and disadvantages. Requirements for the specialised means of protecting information from any unauthorised access. The organisation of virtual protected logical disks. The control of 'technological' debris. Mechanisms for organising access control before the operating system (OS) is loaded. Mechanisms of trusted OS downloads implemented in the Information Security System.

41. Implementation of access control policy in the operating systems MS Windows 2000, XP. Implementation of authentication and authentication mechanisms in OS MS Windows 2000, XP. Storage of password information in the operating system.

42. The classification of network attacks. Scanning the network and exploring its topology. The ability of intruders to intercept and redirect information transmitted in computer networks. Methods of malicious blocking of network nodes and communication channels.

43. Firewalling concepts. The Network Security Policy. The packet filtering criteria. The basic schemes of computer information protection based on firewalls.

44. The organisation of VPN-networks. Tasks solved by VPN. Tunneling to VPN. Protocols and means of organizing a VPN at the network level. The purpose, scope, authentication and encryption of data in the protocols SKIP and IPSec.

45. PPTP, SSL protocols. The purpose, scope, authentication and data encryption. Electronic certificates. The concept of a public key infrastructure. X.509 standard.

36. The conditions for the lawful use of computer programmes and databases. The responsibility for copyright violation.

47. Criminally-legal characteristic of crimes in the sphere of computer information. The characteristics of the objective side of the crimes provided for in Art. 272-274 of the Criminal Code. The definition of key concepts, such as malicious deletion, copying, blocking and modification of computer information, types of computer malfunction. Subjects of crimes. Sanctions for committing criminal acts.

48. Typical conflict situations arising between the administrator of a computer network and the organisation’s management regarding the provision of information security, and methods for their resolution.

49. Typical conflict situations arising between the administrator of a computer network and computer users regarding the provision of information security, and options for their resolution.

50. The procedure for the interaction of the telecommunications operator and the administration of computer networks with representatives of law enforcement bodies on issues stipulated by the federal law.

51. The definition and classification of malware for computers. Destructive possibilities of computer programmes. Software methods for malicious deletion, copying, blocking, modification of computer information and computer malfunctions.

52. The organisational and software tools and methods of antivirus protection, evaluation of their effectiveness.

53. The implementation of mechanisms for protecting computer information at the level of client applications (on the examples of the Microsoft Word word processor and the Microsoft Internet Explorer browser).

54. The concept and classification (taxonomy) of threats to the security of computer information. GOST R 51275-99. Losses and damage from the implementation of threats. The concept of security policies and models in computer systems.