Questions for the exam on the subject
"Protection of Operating Systems and Software" (8th semester)

1. Software classification. Definition, purpose and types of operating systems.
2. Principles of building operating systems.
3. Classification of operating systems.
4. The main vulnerabilities of operating systems of the Windows family.
5. Implementation of measures to ensure the security of operating systems of the Windows family.
6. Security model of operating systems of the Windows family.
7. Auditing events in operating systems of the Windows family.
8. Authentication and authorization in operating systems of the Windows family.
9. Encryption in operating systems of the Windows family.
10. Means of network protection in operating systems of the Windows family.
11. The structure of the security settings of operating systems of the Windows family.
12. Computer policy settings. Categories of audit.
13. Computer policy settings. Security settings.
14. Anti-malware technologies in operating systems of the Windows family.
15. Technologies for protecting confidential data in operating systems of the Windows family.
16. Model of applications of operating systems of the Windows family.
17. A set of tools for ensuring application compatibility in operating systems of the Windows family.
18. The mode of operating systems of the Windows family of an earlier version.
19. Security mechanisms that affect application compatibility in operating systems of the Windows family.
20. Solutions related to enhancements to the Windows operating systems that affect application compatibility.
21. Programs for improving the protection system of operating systems of the Windows family. security scanners.
22. Programs for improving the protection system of operating systems of the Windows family. Antivirus software.
23. Programs for improving the protection system of operating systems of the Windows family. Ensuring security in a virtual infrastructure.
24. Programs for improving the protection system of operating systems of the Windows family. Programs for backing up system resources of operating systems of the Windows family.
25. Setting the basic BIOS settings.
26. The basic concept of operating systems of the Unix family.
27. Vulnerabilities of operating systems of the Unix family.
28. Security model of operating systems of the UNIX family. Users and groups.

29. Security model of operating systems of the UNIX family. Superusers.
30. Security model of operating systems of the UNIX family. Access rights.
31. Restrictions and extensions of the basic access model in operating systems of the UNIX family.
32. Security model of operating systems of the UNIX family. User authentication.
33. Security model of operating systems of the UNIX family. Database of system users.
34. Security model of operating systems of the UNIX family. User session restriction.
35. Security model of operating systems of the UNIX family. Audit.
36. Approaches to ensuring the security of operating systems of the UNIX family.
37. Improving the security system of the Unix OS family. Loadable authentication modules.
38. Improving the security system of the Unix OS family. Intrusion detection systems.
39. Improving the protection system of the OS of the UNIX family. Extended environment for intrusion detection systems.
40. Purpose, application features, classification and distinctive features of real-time operating systems.
41. Vulnerabilities in real-time operating systems.
42. Security model of real-time operating systems.
43. Ensuring the security of real-time operating systems.
44. Purpose, application features, classification, distinguishing features of operating systems for mobile devices.
45. Vulnerabilities of operating systems for mobile devices.
46. Ensuring the security of operating systems for mobile devices.