

**Final control questions for the subject “*Open Source Operating System Security*” for fourth-year students of the educational program
5330300 - Information Security (by field)**

1. Does the OS provide tools for incident response, such as isolation of compromised systems or rollback capabilities?
2. What is the cross-sectional screen and its main function?
3. XFS file system classification?
4. What is included in the software level of the input/output subsystem?
5. How many protective systems are there according to the functional principle?
6. What does the /sbin directory include?
7. Does the OS support secure file permissions, auditing, and monitoring for sensitive data?
8. What is a root user and what are its rights?
9. Storage management. What are the reasons for their use, and what are they?
10. Are there logging and monitoring features to detect unauthorized access attempts?
11. What is fragmentation? Classify its types.
12. Is there support for least privilege principles, ensuring users and processes have only necessary permissions?
13. What is the subsystem of operating system protection when applying the fragmentation approach?
14. Does the OS support secure software installation (e.g., sandboxing, checking for malware)?
15. What does the /bin directory include? What other directories do you know and what are their functions?
16. Does the OS have logging and auditing capabilities for security-relevant events?
17. The main components of an operating system security strategy.
18. Security in communication networks and systems
19. Does the OS come with a security configuration tool or settings that allow users to easily enable/disable security features?
20. Ext2/3 file system classification?
21. Are logs easily accessible for review and analysis?
22. The ext3 (third extended file system) classification, when and by whom was it developed?
23. What are the tools that can be used to ensure secure communication?
24. What is the classification of ext (extended file system), and when and by whom was it developed?
25. Describe the /mnt directory and what it contains.
26. Vulnerabilities of open source operating systems.
27. Does the OS implement strong authentication mechanisms (e.g., multi-factor authentication, strong password policies)?
28. Symbian OS features?
29. What do file access attributions include?
30. How many different classifications of security threats are there?

31. Specify a rule that Apple App Store applications must comply with.
32. What options do you know where file permissions are provided?
33. Classification of the SWAPFS file system?
34. When and by whom was ext2 (the second extended file system) developed?
35. What is exchanging? How many types of loads are there?
36. Can the OS protect against hardware-based attacks like DMA or cold boot attacks?
37. Describe the concepts of process and flow.
38. Are there security hardening guides or best practices for configuring the OS securely?
39. Does the OS support regular backups and recovery processes?
40. Existing software protection systems can be classified according to a number of characteristics, which are they?
41. According to the functional principle, how can memory provision be categorized?
42. High Memory?
43. Are firmware updates for hardware devices and components handled securely?
44. How often are security audits and penetration tests conducted on the OS?
45. What is a process resource?
46. What are the functions of the file system in the Linux operating system?
47. Is the OS capable of securely configuring and managing network services, such as SSH, FTP, or HTTP?
48. OS features for mobile devices
49. What is the system kernel?
50. How often are security audits and penetration tests conducted on the OS?
51. Can you provide examples of security requirements for operating systems?
52. Are there built-in features for network segmentation and isolation?
53. Are there firewall capabilities for both inbound and outbound traffic?
54. Does the OS support secure development practices such as static analysis, fuzz testing, and vulnerability scanning?
55. What are the management measures?
56. Does the OS provide tools for incident response, such as isolation of compromised systems or rollback capabilities?
57. Is role-based access control (RBAC) available for fine-grained permissions?
58. Does the OS implement secure DNS (DNSSEC) and prevent DNS-based attacks?
59. Are vulnerabilities tracked and published in a publicly accessible database (e.g., CVE)?
60. How many storage management methods are there, and what are they?
61. Write about the concept of "operating system kernel"
62. What is the protocol and mission?.
63. Does the OS have the ability to configure secure tunneling protocols like VPN or Tor?
64. Does the OS include features for securing network communications (e.g., firewall, VPN, IP filtering)?

65. How quickly are security vulnerabilities patched and updated in the OS?
66. What variants of kernel implementation in operating systems do you know?
67. What is multitasking and what types of multitasking do you know?
68. What is the need for auditing when working with operating systems?
69. Give a description of each of the attacks presented in the STRIDE methodology.
70. What is journaling and what is the role of this process in information security?
71. Common OS attacks: backdoors and their advantages.
72. Interactive login to the operating system. Authentication methods: local logon and domain logon (Active Directory).
73. Software and hardware means of protecting operating systems.
74. Explain the role of penetration testing in assessing the security level of operating systems.
75. What is the role of information forums and mailing lists in the development and maintenance of open source applications?
76. Functional components and architecture of active auditing tools.
77. Give definitions of these types of algorithms: data encryption algorithms, entanglement algorithms, mutation algorithms, data compression algorithms.
78. What are the positive aspects of password protection systems in the OS user authentication process?
79. Characteristic features of logging and auditing process.
80. The concept of active auditing in an operating system.
81. Functional components of active auditing.
82. Main tasks of logging and auditing in OS.
83. What open source operating systems are used in mobile devices? What are their features?
84. What are the differences between defragmentation and fragmentation processes?
85. What do you know about such an attack as “garbage collection”?
86. Advantages and disadvantages of open source operating systems.
87. Attacks aimed at total or partial disabling of the operating system.
88. Types of OS multitasking.
89. Types of process state in OS. Give examples.
90. In what state can a process be blocked due to external reasons, at the initiative of the operating system? Give examples.
91. What is the state in which a process is blocked and cannot execute due to its internal reasons? Give examples.
92. Why is a memory management process necessary as part of OS functioning?
93. In what case does the kernel create a new virtual address space?
94. Resident memory and its use in an open source OS?
95. What is a memory address trap? Give examples.
96. What attributes can be used to classify existing software protection systems?
97. Types of file systems, their purpose and differences.
98. Common attacks on operating systems.
99. Program means of ensuring the security of information resources.

100. Comparison of open source and proprietary operating systems: advantages and disadvantages.