**List of questions for the final examination of 4th-year students in the subject "Cybersecurity Policy"**

**For the fall semester of the 2024/2025 academic year.**

1. Explain the role of decision-making in cybersecurity policy.
2. Why is it necessary to consider cyber threats when developing cybersecurity policies?
3. What is the cyber threat assessment process?
4. Provide information about the catalog approach to cybersecurity policy.
5. Please provide information about the cybersecurity policy catalog.
6. List the steps in creating catalogs?
7. What are the challenges of cyber governance?
8. What are the key elements of the structural agile system design process?
9. What are the cyber user problems?
10. Provide information about email policy issues.
11. What are cybercrimes and cyberpolitics?
12. What are the cybersecurity policy issues related to privacy?
13. Provide information about cyber infrastructure issues.
14. Please provide information about the US approach to cybersecurity policy.
15. Provide information about cyber espionage and cyber activities of different countries.
16. Provide information about the cyber policy efforts of the US Congress.
17. Provide information about Russia's approach to cybersecurity policy.
18. What international cooperation is there in the field of information security?
19. Provide information about the international information security system.
20. Provide information about the Russian Federation's approach to cyber issues.
21. Provide information about Uzbekistan's approach to cybersecurity policy.
22. What regulatory and legal documents do you know in the field of information security?
23. Provide information about geopolitics and cybersecurity.
24. What does an antivirus policy consist of?
25. What is a data backup policy?
26. What are cybersecurity policy approaches?
27. Provide information about data backup and recovery policy.
28. What is the concept of cybersecurity and how does it relate to the confidentiality, integrity, and availability of information?
29. Provide information about the types of cybersecurity policies.
30. What regulatory documents are used to create a cybersecurity policy?
31. Provide information about cybersecurity policy, strategy, and standards.
32. What should a cybersecurity policy for businesses and organizations consist of ?
33. What is a problem-solving cybersecurity policy?
34. How to formulate a cybersecurity policy?
35. Provide information about concepts related to cybersecurity policy (cyber threat, cyber attack, vulnerability, cyber law, cyber crime)
36. What is the evolution of cybersecurity?
37. What are the goals of cybersecurity management?
38. Why are cybersecurity metrics needed?
39. What technologies are available to protect the integrity of information in cyberspace?
40. What security technologies are available to prevent or mitigate threats?
41. What factors influence the formation of cybersecurity policies in different countries?
42. What are the cybersecurity responsibilities of individuals in an organization?
43. Provide information about guidelines for creating and protecting passwords.
44. Provide information about the anti-malware policy and its purpose.
45. Provide information about digital forensics and its types.
46. What penetration testing tools do you know?
47. What digital forensics tools do you know?
48. What cybersecurity tools do you know?
49. Provide information about cybersecurity training for employees
50. Provide information about security technology resources.
51. Provide information about cybersecurity training methods.
52. What types of cybersecurity training are available?
53. Provide information about the requirements for developing an effective information security policy.
54. What are the challenges in implementing an effective information security policy?
55. What are the methods for developing a cybersecurity policy?
56. Explain the lifecycle approach to developing a cybersecurity policy.
57. Explain the importance of the risk assessment phase in developing a cybersecurity policy.
58. Explain the importance of the policy development phase in developing a cybersecurity policy.
59. Explain the importance of the policy implementation phase in developing a cybersecurity policy.\
60. Explain the importance of policy monitoring and maintenance phases in cybersecurity policy development.
61. Explain the role of policy support activities in cybersecurity policy development.
62. What is the concept of cybercrime in corporations?
63. What are the main cybersecurity vulnerabilities found in corporations?
64. Describe the types of cybercrime against corporations.
65. Describe cyberattacks on corporations.
66. Provide information on corporate responses to cybercrime.
67. What are the measures to protect against cybercrime and explain them?
68. Explain the role of individuals in ensuring cybersecurity.
69. Explain in detail the process of "Covering" or hiding a problem in corporations
70. List the damages caused by irresponsible employees in corporations.
71. Provide information about the problem of using personal devices in businesses.
72. Provide information about cybersecurity policies in corporations.
73. Explain the role of law enforcement agencies in ensuring cybersecurity.
74. Provide information about the cooperation between law enforcement agencies and cybersecurity experts.
75. Provide an understanding of the information technologies and tools used in cybercrime investigation and digital forensics.
76. Explain in detail the legal framework of cybersecurity.
77. Explain the tasks performed under a policy used in organizations at a low risk level.
78. Explain the tasks performed under the policy used in organizations with a medium level of risk.
79. Explain the important settings for policies that scan for malware protection.
80. Provide information about what is done in the anti-malware policy when the risk is low.
81. Provide information about the actions taken in the anti-malware policy when the risk is medium.
82. Provide information about the actions taken in the anti-malware policy when the risk is high.
83. Explain the authentication policy on the Internet.
84. Provide information about the sections and description of the password policy.
85. Provide information about the sections and description of the data backup policy.
86. Explain how to apply an Internet use policy when the risk is low.
87. Provide information about guidelines for creating and protecting passwords.
88. Describe cyberattacks on corporations.
89. Explain the tasks performed under a policy used in organizations at a low risk level.
90. Provide information about Uzbekistan's approach to cybersecurity policy.
91. What is the evolution of cybersecurity?
92. What factors influence the formation of cybersecurity policies in different countries?
93. Why are cybersecurity metrics needed?
94. What cybersecurity tools do you know?
95. Provide information about the actions taken in the anti-malware policy when the risk is high.
96. What international cooperation is there in the field of information security?
97. Describe cyberattacks on corporations.
98. Why is it necessary to consider cyber threats when developing cybersecurity policies?
99. What are cybersecurity policy approaches?
100. Provide information about Russia's approach to cybersecurity policy.