**«Confirmed»**

**by the Head of the Department**

**of «Cryptology»**

**\_\_\_\_\_\_\_\_\_\_\_\_ Khudoykulov Z.T.**

**«\_\_\_\_»\_\_\_\_\_\_\_\_2024 y.**

**Questions of the final control work on the discipline**

**“Access Control”**

1. Describe basic cybersecurity and access control terminology.
2. What is attribute-based access control and how does it work? What are the advantages of this approach and what are the limitations that may arise?
3. What is an ACS? What classes of ACS exist? Give a detailed definition for each with the examples.
4. Describe the types of biometrics in detail with the examples.
5. Describe the structure and process for developing a security policy in detail.
6. Describe in detail the advantages and disadvantages of biometric-based authentication and the attacks that target it with the examples.
7. Describe in detail the advantages and disadvantages of password-based authentication and the attacks that target it with the examples.
8. Describe in detail the advantages and disadvantages of token-based authentication and the attacks that target it with the examples.
9. Write about the application areas of biometric authentication. Describe with the examples.
10. What is an access control and why is it important for information security?
11. What is the authentication based on something you know? Describe in detail with the examples.
12. What are the basic concepts associated with the access control? Describe in detail with the examples.
13. How the passwords are stored? What are password management systems? Explain in detail with the examples.
14. What methods of authentication exist? Explain in detail with the examples.
15. What risks can arise from misusing or not using an information security policy? Explain in detail with the examples.
16. What trust paradigms exist and how can they be used to secure access? Explain in detail with the examples.
17. What identity management models are used for access control and what benefits do they provide? Explain in detail with the examples.
18. What problems can arise when using biometric systems and how can they be solved? Explain in detail with the examples.
19. What is the identity management and why do we need this? What models of identity management do you know? Describe each and provide examples.
20. How does the password-based authentication method work? How are passwords stored in a database? Explain in detail with the examples.
21. What is an information security policy and how is it developed? Explain in detail with the examples.
22. How do software tokens work, what are the advantages of this method, and what are the limitations? Explain in detail with the examples.
23. What are the single-factor multi-factor and contextual authentication? Explain in detail with the examples.
24. How does the method of authentication based on something you have work? Explain in detail with the examples.
25. Describe in detail the specifics of access control in Windows.
26. What is an access control matrix? How is it used in access control models? What other access control models exist? Describe each of them.
27. Compare the advantages and disadvantages of software and hardware tokens and give the examples for each type.
28. What methods can be used to protect passwords and what vulnerabilities exist? Explain in detail with the examples.
29. What trust paradigms exist and how can they be used to secure access? Explain in detail with the examples.
30. What are bimodal biometrics and liveness detection? What types of Liveness detection exist? Explain in detail with the examples.
31. What is Single Sign-on? What protocols are used to implement it? Explain in detail with the examples.
32. Describe in detail the attacks targeting token-based authentication systems and the defenses against such attacks with the examples.
33. Describe in detail attacks that target password-based authentication systems and the defenses against such attacks with the examples.
34. Describe in detail attacks targeting biometric systems and the defenses against such attacks with the examples.
35. Describe in detail the types of smart cards with the examples and how do they differ from each other?
36. What is the “salt” and how is it used to store and compare passwords? How does it help improve security? Explain in detail with the examples.
37. Describe in detail the security policy, hierarchy, and properties of the security policy.
38. Explain how the discretionary access control model works and how it differs from other access control models? Explain in detail with the examples.
39. How important are PIN-based authentication methods in modern access control systems? What security measures should be taken when using PIN-based authentication? Explain in detail with the examples.
40. Explain how the mandatory access control model works and how it differs from other access control models? Explain in detail with the examples.
41. What types of threats can occur when using systems that implement token-based access control? How can they be prevented? Explain in detail with the examples.
42. What basic security principles should be implemented in an organization's information security policy? How do these principles relate to access control in systems? Explain in detail with the examples.
43. What is a trust paradigm? What are the main types of paradigms and how do they differ? Explain in detail with the examples.
44. Describe in detail the specifics of access control in mobile OS with the examples.
45. What devices can be used to identify users and what are the advantages, and disadvantages, of each type? Explain in detail with the examples.
46. What are tokens and what types of tokens are used in access control systems? Explain in detail with the examples.
47. Describe in detail the specifics of access control in Linux with the examples.
48. Describe in detail the security policy, hierarchy, and properties of a security policy.
49. Explain in detail how the role-based access control model works and how it differs from attribute-based access control.
50. Describe in detail the types and factors of authentication with the examples.
51. What are the hardware tokens for authentication? What advantages do they offer over software tokens? Explain in detail with the examples.
52. Write the ACL and C-list for the following access matrix: (here will be the example of access control matrix)
53. Write a query for the following attribute-based access control rule: (here will be the example of the rule like “Access to sensitive data is allowed only from corporate devices”.)

**Written by:**

**the Senior Lecturer of  
the department of “Cryptology”: N.F. Akhmedova**