**«ПОДТВЕРЖДАЮ»**

**Заведующей кафедрой**

**«Криптология»**

**\_\_\_\_\_\_\_\_\_\_\_\_ Худойкулов З.Т.**

**«\_\_\_\_»\_\_\_\_\_\_\_\_2024 год**

**Вопросы для итогового контроля**

**по дисциплине «Управление доступом»**

1. Подробно опишите базовую терминологию кибербезопасности и управления доступом.
2. Что такое управление доступом на основе атрибутов и как оно работает? Какие преимущества у такого подхода и какие ограничения могут возникнуть?
3. Что такое СКУД? Какие классы СКУД существуют? Подробно опишите каждый с примерами.
4. Подробно опишите виды биометрии с примерами.
5. Подробно опишите структуру и процесс разработки политики безопасности.
6. Подробно опишите преимущества и недостатки аутентификации на основе биометрических параметров, а также атаки, направленные на неё с примерами.
7. Подробно опишите преимущества и недостатки аутентификации на основе пароля, а также атаки, направленные на неё с примерами.
8. Подробно опишите преимущества и недостатки аутентификации на основе токенов, а также атаки, направленные на неё с примерами.
9. Напишите про области применения биометрической аутентификации. Приведите примеры.
10. Что такое управление доступом, и почему оно важно для информационной безопасности?
11. Что такое аутентификация на основе знания чего-то? Подробно опишите с примерами.
12. Какие основные понятия связаны с управлением доступом? Подробно опишите с примерами.
13. Как хранить пароли? Что такое системы управления паролями? Подробно объясните с примерами.
14. Какие методы аутентификации существуют? Подробно опишите с примерами.
15. Какие риски могут возникнуть при неправильном использовании или не использовании политики информационной безопасности? Подробно объясните с примерами.
16. Какие парадигмы доверия существуют и как они могут быть использованы для обеспечения безопасности доступа? Подробно объясните с примерами.
17. Какие модели управления идентификаторами используются для управления доступом и какие преимущества они предоставляют? Подробно объясните с примерами.
18. Какие проблемы могут возникнуть при использовании биометрических систем и как их можно решить? Подробно объясните с примерами.
19. Что такое управление идентификаторами, для чего это нужно? Какие модели управления идентификаторами вы знаете? Подробно опишите каждое и приведите примеры.
20. Как работает метод аутентификации на основе пароля? Как хранятся пароли в базе данных? Подробно объясните с примерами.
21. Что такое политика информационной безопасности и как она разрабатывается? Подробно объясните с примерами.
22. Как работают программные токены, какие преимущества у этого метода, и какие ограничения? Подробно объясните с примерами.
23. Что такое однофакторная многофакторная и контекстная аутентификация? Подробно объясните с примерами.
24. Как работает метод аутентификации на основе владения чем то? Подробно объясните с примерами.
25. Подробно опишите специфику управления доступом в ОС Windows.
26. Что такое матрица управления доступом? Как она используется в моделях управления доступом? Какие другие модели управления доступом существуют? Подробно опишите каждую из них.
27. Сравните преимущества и недостатки программных и аппаратных токенов и приведите примеры каждому виду.
28. Какие методы можно использовать для защиты паролей и какие уязвимости существуют? Подробно объясните с примерами.
29. Какие парадигмы доверия существуют и как они могут быть использованы для обеспечения безопасности доступа? Подробно объясните с примерами.
30. Что такое бимодальная биометрия и детектор живого пользователя? Какие виды “Liveness detection” существуют? Подробно объясните с примерами.
31. Что такое Single Sign-on? Какими протоколами оно реализуется? Подробно объясните с примерами.
32. Подробно опишите атаки направленные на системы аутентификации на основе токена и меры защиты от таких атак с примерами.
33. Подробно опишите атаки направленные на системы аутентификации на основе пароля и меры защиты от таких атак с примерами.
34. Подробно опишите атаки направленные на биометрические системы и меры защиты от таких атак с примерами.
35. Подробно опишите виды смарт карт с примерами и чем они отличаются друг от друга?
36. Что такое "соль", и как она используется для хранения и сравнения паролей? Как она помогает повысить безопасность? Подробно объясните с примерами.
37. Подробно опишите политику безопасности, иерархию и свойства политики безопасности.
38. Объясните, как работает дискреционная модель управления доступом и как она отличается от других моделей управления доступом? Подробно объясните с примерами.
39. Как важны методы аутентификации на основе PIN-кода в современных системах управления доступом? Какие меры безопасности необходимо принимать при использовании PIN-кода? Подробно объясните с примерами.
40. Объясните, как работает мандатная модель управления доступом и как она отличается от других моделей управления доступом? Подробно объясните с примерами.
41. Какие типы угроз могут возникнуть при использовании систем, которые осуществляют управление доступом на основе токенов? Как их можно предотвратить? Подробно объясните с примерами.
42. Какие основные принципы безопасности должны быть реализованы в политике информационной безопасности организации? Как эти принципы связаны с управлением доступом в системах? Подробно объясните с примерами.
43. Что такое парадигма доверия? Какие основные типы парадигм существуют и как они различаются? Подробно объясните с примерами.
44. Подробно опишите специфику управления доступом в мобильных ОС с примерами.
45. Какие устройства могут использоваться для идентификации пользователей и какие преимущества, и недостатки у каждого типа? Подробно объясните с примерами.
46. Что такое токены и какие виды токенов используются в системах управления доступом? Подробно объясните с примерами.
47. Подробно опишите специфику управления доступом в ОС Linux с примерами.
48. Подробно опишите политику безопасности, иерархию и свойства политики безопасности.
49. Подробно объясните, как работает ролевая модель управления доступом и как она отличается от управления доступом на основе атрибутов.
50. Подробно опишите виды и факторы аутентификации с примерами.
51. Что такое аппаратные токены для аутентификации? Какие преимущества они предоставляют по сравнению с программными токенами? Подробно объясните с примерами.
52. Напишите ACL и C-list для следующей матрицы доступа: (тут будет пример матрицы доступа).
53. Напишите запрос следующего правила управления доступом на основе аттрибутов: (тут будет пример правила)

**Составитель:**

**Старший преподаватель**

**кафедры, «Криптология»: Ахмедова Н.Ф.**