|  |  |
| --- | --- |
| **E:\!Кафедра ПИКС\Логотип БГУИР\Символика.jpg** | **E:\!Кафедра ПИКС\Логотип ПИКС\17 мая 2013\Логотип ПИКС_3.jpg** |

**ВОПРОСЫ К ЭКЗАМЕНУ**

**по дисциплине**

**«БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНЫХ СЕТЯХ»**

**Осенний семестр 2023-2024 учебного года**

**Специальность 1-39 03 02 «Программируемые мобильные системы»**

**(группы 013801-013802, 013831-013834)**

1. Опишите наиболее эффективных метода защиты от вредоносного ПО.
2. Приведите примеры технологий хеширования и их свойства.
3. Что такое многофакторная аутентификацию и ее применение.
4. Перечислите и дайте краткую характеристику к подходам по обеспечению доступности.
5. Для чего используется аутентификации и ее свойства.
6. Перечислите нетехнические методы получения конфиденциальной информации.
7. Какие технологии идентификации можно использовать в составе системы аутентификации сотрудников.
8. Многоуровневый подход защиты сетевой инфраструктуры.
9. Приведите примеры протоколов, которые могут представлять угрозу для коммутируемой среды.
10. Опишите метод «Перебора по словарю».
11. Опишите метод «Грубой силы».
12. Приведите примеры симметричных алгоритмов шифрования данных. Дайте им краткую характеристику
13. Приведите примеры асимметричных алгоритмов шифрования данных. Дайте им краткую характеристику
14. Приведите примеры категорий злоумышленников и дайте краткую характеристику каждой категории.
15. Модель ISO/OSI
16. Документ ISO 27000, ISO 27001, ISO 27002.
17. Назовите три состояния данных. Приведите практические примеры.
18. Что означает термин «Точка баланса вероятностей ошибок»
19. Какие инструменты могут использоваться для сканирования сети в целях выявления угроз безопасности.
20. Системы обнаружения вторжений. Примеры использования и принцип работы.
21. Системы предотвращения вторжений. Примеры использования и принцип работы.
22. Алгоритм шифрования с открытым ключом.
23. Алгоритм шифрования с закрытым ключом.
24. Что означает термин «Уязвимость»
25. Перечислите меры эффективные в борьбе с киберпреступниками?
26. Что означает аббревиатура IoE. Информационная защита IoE.
27. DDoS-атака. DoS-атака. Различие между DDoS и DoS.
28. Какие три основных принципа кибербезопасности.
29. Для чего используется резервное копирование данных. Способы организации резервного копирования данных.
30. Перечислите и дайте краткую характеристику средств контроля доступа.
31. Перечислите и дайте краткую характеристику категориям конфиденциальной информации.
32. Приведите примеры вредоносного ПО и дайте краткую характеристику каждому типу.
33. Протоколы WEP, WPA, WPA-2: характеристики, различие и область использования.
34. Приведите способа защиты компьютера от вредоносного ПО.
35. Опишите тактики социальной инженерии.
36. Вида устройств, которые относятся к категории физических средств контроля доступа.
37. Приведите примеры административных средств контроля доступа.
38. Что такое цифровой подписи и область ее применения.
39. Дайте определение криптографически стойкому генератору псевдослучайных чисел и область его применения.
40. Назовите наиболее распространенные хеш-функции.
41. Назовите главные свойства криптографической хеш-функции.
42. Для чего используется «Соль» в хеш-функциях. Пример использования.
43. Хеш-функция. Приведите примеры применения хеш-функции.
44. Опишите концепцию «пять девяток»
45. В каких сферах необходимо гарантировать доступность систем на уровне «пять девяток».
46. В чем разница между системой обнаружения вторжений на базе хостов (HIDS) и межсетевым экраном?

Вопросы разработали:

ФЕЩЕНКО Артем Александрович – кандидат технических наук, доцент

КОТУХОВ Алексей Валерьевич – старший преподаватель