Kafedranın adı: _Информатика_

Fənnin adı:Информационная безопасность_

Kurs:__3_

Bölmə:_русский_

Bakalavriat

İMTAHAN SUALLARI

1. Основные понятия информационной безопасности.
2. Понятие информационных угроз.
3. Виды информационных угроз и их причины.
4. Отказоустойчивые ИТ-системы: принципы построения.
5. Блокчейн.
6. Decimal – Валидаторы.
7. Что такое Stellar: обзор криптовалюты Lumens (XLM).
8. Содержание и структура понятия компьютерной безопасности.
9. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности.
10. Место межсетевых экранов в системе защиты СПД.
11. Классификация межсетевых экранов.
12. Основные понятия и определения шифрования.
13. Симметричного шифрования.
14. Асимметричное шифрование.
15. Контроль целостности данных . Электронная цифровая подпись (ЭЦП).
16. Криптография. Основные методы и проблемы. Современные тенденции криптографии.
17. Криптографические протоколы
18. Понятие «информационная война».
19. Информационно-сетевая война
20. Методы ведения информационной войны
21. Цели информационной войны.
22. Криптографические средства защиты информации: Простые криптосистемы.
23. Классификация основных методов криптографического закрытия информации.
24. Шифр гаммирования.
25. Стандарты и спецификации в области информационной безопасности.
26. Основные положения теории информационной безопасности информационных систем.
27. Основные понятия программно-технического уровня информационной безопасности.
28. Идентификация и аутентификация.
29. Модели управления доступом .
30. Модели управления доступом . Цели и область применения.
31. Методы управления доступом.

32. Таксономия нарушений информационной безопасности вычислительной системы и причины, обусловливающие их существование
33. Таксономия нарушений информационной безопасности по размещению в вычислительных сетях
34. Классификация нарушений информационной безопасности по этапам возникновения и внедрения
35. Непреднамеренные (неумышленные) ошибки и нарушения информационной безопасности.
36. Аудит в системе менеджмента информационной безопасности
37. Шифрование. Простые криптосистемы. Классификация основных методов криптографического закрытия информации
38. Шифрование методом замены (подстановки)-одноалфавитная и многоалфавитная.
39. Шифрование методом перестановки
40. Шифрование методом гаммирования
41. Комбинированные (составные) шифры.
42. Информационная безопасность в Интернете. DoS-атака (отказ в обслуживании).
43. 4Информационная безопасность в Интернете. Атаки на пароли.
44. Компьютерные вирусы и средства борьбы с ними.
45. Классификация компьютерных вирусов.
46. Классификация антивирусных программ.
47. Средства создания и распространения вирусов.
48. Классификация сетевых атак.
49. бщие сведения об информационной безопасности в Интернете.
50. Информационная безопасность в Интернете. Фишинг (Fishing) и farming.
51. Информационная безопасность в Интернете. Sniffing- Вид атаки сетевой, осуществляемой посредством пассивного прослушивания сети специальным средством программным перехвата сетевых пакетов (сниффером пакетным).
52. Информационная безопасность в Интернете. Атаки на пароли.
53. Методы обеспечения информационной безопасности.
54. Пути решения проблемы защиты информации в сетях
55. Идентификация одноразового пароля с помощью электронного токена.
56. Средства защиты сети. Брандмауэры.
57. Метод шифрования с секретным ключом. Пароль Цезаря.
58. Модели безопасности. Модель DAC (Diskresion)).
59. Модели безопасности. MAC (Bella-LaPadula).
60. .Модели безопасности. Модель RBAC (Rol).