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

**ВОПРОСЫ К ЗАЧЕТУ**

**по дисциплине**

**«Методы и технические средства обеспечения безопасности»**

**Осенний семестр 2022-2023 учебного года**

**Специальность 1-39 03 01 «Электронные системы безопасности»**

**(группы 013301, 083371, 083372)**

**Часть 1. Методы и технические средства обеспечения безопасности информации**

1. Понятие информации. Виды представления и классификация информации.
2. Понятия безопасности и системы безопасности информации. Фрагментарный и системный подход к защите информации.
3. Требования к защите информации. Виды обеспечения системы защиты информации.
4. Концептуальная модель информационной безопасности и ее компоненты.
5. Модель построения системы информационной безопасности предприятия.
6. Угрозы конфиденциальной информации и их классификация.
7. Источники угроз безопасности информации, их классификация и ранжирование.
8. Уязвимости безопасности информации, их классификация и ранжирование.
9. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
10. Правовая и организационная защита информации.
11. Инженерно-техническая защита информации.
12. Классификация и общая характеристика каналов утечки информации.
13. Технические каналы утечки информации, причины и источники их образования.
14. Классификация и характеристика каналов утечки речевой информации.
15. Технические каналы утечки речевой информации и методы ее съема.
16. Методы дистанционного проникновения в помещение для скрытого съема аудио- и видеоинформации.
17. Технические средства съема аудиоинформации: малогабаритные проводные, радио- и стетоскопные микрофоны.
18. Технические средства съема аудиоинформации: направленные, лазерные и ИК микрофоны.
19. Технические средства съема аудиоинформации: эндовибраторы, аудиотранспондеры и вторичные микрофоны.
20. Технические средства съема аудиоинформации: устройства ВЧ навязывания, устройства с перемодуляцией радиоизлучений на нелинейных элементах, устройства с двойной модуляцией, устройства с питанием и передачей информации по сети, диктофоны.
21. Методы съема информации в телефонных линиях связи: способы несанкционированного подключения.
22. Методы съема информации в телефонных линиях связи: контактное и бесконтактное подключение, ВЧ навязывание, междугородная закладка.
23. Технические средства съема видеоинформации и их общая характеристика.
24. Виды электромагнитных излучений, электромагнитные и электрические каналы утечки информации.
25. Методы и средства съема информации по радиоканалу.
26. Электромагнитные излучения и съем информации, обрабатываемой средствами вычислительной техники.
27. Съем информации с помощью технологи Bluetooth и в Wi-Fi-сетях.
28. Методы и средства съема информации в высокочастотных и волоконно-оптических кабелях.
29. Методы защиты речевой информации. Защита речевой информации с помощью маскирующих сигналов.
30. Системы виброакустического зашумления.
31. Подавители диктофонов.
32. Блокираторы сотовых телефонов.
33. Защита речевой информации от узконаправленных микрофонов и лазерного съема.
34. Методы и средства обнаружения радиозакладных устройств: индикаторы поля, панорамные сканирующие приемники, аппаратно-программные комплексы, аппаратура для измерения параметров сигналов.
35. Методы и средства обнаружения радиозакладных устройств: обнаружители диктофонов и нелинейные локаторы.
36. Прозрачные переговорные кабины.
37. Звукоизоляция помещений.
38. Общие принципы защиты телефонных линий связи. Методы и средства пассивной защиты.
39. Методы подавления телефонных закладных устройств.
40. Применение маскираторов и средств постановки активных помех для защиты информации в телефонных линиях связи.
41. Применение скремблеров и вокодеров для защиты информации в телефонных линиях связи.
42. Методы и средства обнаружения и противодействия в телефонных линиях связи.
43. Общая характеристика методов защиты информации от утечки по электромагнитным каналам.
44. Защита информации от утечки за счет микрофонного эффекта.
45. Защита информации от утечки за счет электромагнитного излучения.
46. Защита информации от утечки за счет паразитной генерации, по цепям питания и по цепям заземления.
47. Защита информации от утечки за счет взаимного влияния проводов и линий связи и высокочастотного навязывания.
48. Защита линий связи. Защита информации от утечки в волоконно-оптических линиях связи.
49. Детекторы видеокамер.
50. Экранирование технических средств и помещений.
51. Использование металлизированных пленок, тканей, электропроводных эмалей и ферритовых фильтров для защиты информации от утечки по электромагнитному каналу.
52. Применение радиоэлектронных помех для защиты информации от утечки по электромагнитному каналу.
53. Программные и аппаратно-программные методы защиты информации в персональных компьютерах.
54. Защита от компьютерных вирусов.
55. Способы уничтожения информации на магнитных носителях.
56. Защита информации в персональных компьютерах от перехвата по электромагнитному каналу.
57. Защита компьютерной сети с использованием межсетевых экранов.
58. Обеспечение безопасности информации в сетях ЭВМ.
59. Методы криптографии с секретными ключами.
60. Методы криптографии с открытыми ключами.
61. Поточное и блочное шифрование.
62. Методы компьютерной стеганографии.
63. Компьютерная стеганофония.
64. Применение электронной цифровой подписи для защиты электронных документов.

Вопросы разработал

АЛЕФИРЕНКО Виктор Михайлович – канд. техн. наук, доцент