ОЦЕНОЧНЫЕ СРЕДСТВА

Сформированности профессиональных компетенций

по учебной по дисциплине

«Введение в информационную безопасность»

Квалификация выпускника – магистр

Нормативный срок обучения – 2 года

Форма обучения – очная

2016 г.

Оценочные средства составляются преподавателем самостоятельно при ежегодном обновлении банка средств. Количество вариантов зависит от числа обучающихся.

Перечень контрольных вопросов, выносимых на ЗАЧЁТ / ЭКЗАМЕН:

1. Граф «угроза - объект» - как базовая модель СЗИ
2. Основные функции и методы реализации СЗИ
3. Угрозы безопасности КС
4. Процедуры подтверждения подлинности (идентификация и аутентификация)
5. Статические биометричесие методы идентификации и их характеристики
6. Динамические биометричесие методы идентификации и их характеристики
7. Методы взлома парольной защиты и модификации схемы «простой пароль»
8. Методы парольной аутентификации PAP, CHAP, MsChap
9. ЭЦП как средство аутентификации любых цифровых данных
10. Субъектно-объектная модель компьютерной системы. Монитор безопасности
11. Модели (политики) безопасности в субъектно-объектной модели КС
12. Модели на основе матрицы доступа (варианты принудительного и добровольного управления доступом, проблема «троянских коней»)
13. Модель Харрисона-Руззо-Ульмана (модель HRU). Критерий безопасности и основные теоремы модели HRU
14. Расширения модели HRU
15. Теоретико-графовая модель «take-grant». Распространение (утечка) прав доступа в графе модели «take-grant», состоящем из субъектов
16. Теоретико-графовая модель «take-grant». Распространение (утечка) прав доступа в графе модели «take-grant», состоящем из субъектов и объектов
17. Критерий безопасности и основная теорема модели «take-grant»
18. Расширенная модель Take–Grant, “неявные” информационные потоки.
19. Достоинства и недостатки дискреционных моделей
20. Основные положения моделей мандатного доступа. Решетка уровней и функции безопасности. MLS решетка.
21. Модель Белла-ЛаПадулы. Критерий безопасности модели Белла-ЛаПадулы.
22. Достоинства и недостатки модели Белла-ЛаПадулы
23. Модификации модели Белла-ЛаПадулы (Мак-Лин, LWM)
24. Основные ограничения моделей мандатного доступа.
25. Модели безопасности на основе тематической политики доступа
26. Дескрипторная тематическая классификация в модели тематической политики доступа
27. Иерархическая тематическая классификация в модели тематической политики доступа
28. Тематические решетки в модели тематической политики доступа
29. Решетка мультирубрик в модели тематической политики доступа
30. Модели ролевого доступа
31. Модели индивидуально-группового доступа
32. Политики безопасности в Windows и Linux.
33. Понятие скрытых каналов утечки информации в моделях разграничения доступа. Виды скрытых каналов утечки информации. Понятие скрытых каналов по памяти и скрытых каналов по времени.
34. Статистический скрытый канал передачи информации
35. Автоматная модель невлияния Гогена-Месигера (GM-модель)

36. Понятие целостности данных. Мандатная модель целостности Биба.
37. Модели комплексной оценки защищенности КС
38. Угрозы сети традиционные и «типично сетевые»
39. Оценка рисков нарушения ИБ
40. Стандарты в сфере безопасности ИТ (типы объектов, шкалы)
41. Развитие стандартов, ГОСТ и РД.
42. Защищенные протоколы. Уязвимости протоколов интернет.
43. Анонимность в интернет.
44. Анонимные сети
45. Защищенные протоколы.
46. Сертификаты и ЭЦП. Иерархия сертификатов.
47. Аутентификация и авторизация.
48. Протокол аутентификации Kerberos
49. Управление доступом. Межсетевые экраны. DMZ.
50. Сканирование сетей.
51. Перехват данных. Снифинг. Включение в разрыв сети. Методы защиты.
52. Перехват данных. Ложные запросы. Перехват TCP-соединения. Методы защиты.
53. Атаки на отказ в обслуживании. Цели и основные методы атак.Методы защиты

Перечень контрольных вопросов, выносимых на ЭКЗАМЕН:

54. Эволюция подхода к управлению ИБ: реактивный, системно-сервисный, архитектурный, развитие пространства критериев ИБ, принципиально процессный характер управления ИБ, содержание этапов жизненного цикла управления.
55. Содержание и инструменты уровней управления ИБ, концептуальные принципы безопасности, основания дифференциации защищаемых информационных активов, диалектика и компоненты понятия угрозы, методы формирования модели угроз, виды политик ИБ.
56. Иерархическая классификация объектов защиты и требований безопасности в традиционной идеологии управления ИБ, ограничения традиционной идеологии, стандартизация управления ИБ, система стандартов 27-го подкомитета ISO.
57. Идеология анализа и управления информационными рисками, исчисляемые факторы при двух-, трех- и четырехфакторном анализе рисков, вероятностное расширение модели Клементса, проблемы экспертного оценивания и количественной интерпретации качественных шкал.
58. Модель высокоуровневых понятий в идеологии общих критериев, диалектика взаимодействия угроз, политик, предположений и целей безопасности в профиле защиты, функциональные требования безопасности и требования доверия, оценочные уровни доверия.
59. Управление специальными методами безопасности, безопасность критических объектов информационной инфраструктуры, привлечение фактора необратимости, делегирование управления ИБ, динамические политики ИБ.
60. Управление защитой от угроз инсайдера, принципиальная избыточность полномочий, факторы избыточности, ограниченность мониторинга событий безопасности и традиционных методов защиты, методы компенсации потенциала угроз инсайдера.