Минобрнауки Российской Федерации

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»

УТВЕРЖДАЮ
Председатель
Приемной комиссии ЮЗГУ
С.Г. Емельянов
«15» сентября 2020 г.

Вопросы к вступительному экзамену в аспирантуру

Направление подготовки: 10.06.01 – информационная безопасность
Профиль Методы и системы защиты информации, информационная безопасность

Курск 2020

1. Понятия группы, кольца, поля, их основные свойства. Основы теории конечных полей.
2. Кольца вычетов. Кольцо многочленов над конечным полем. Поля Галуа.
3. Условная вероятность и независимость. Последовательность независимых испытаний.
4. Цепи Маркова.
5. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
6. Сходимость последовательностей случайных величин и сходимость распределений.
7. Закон больших чисел. Центральная предельная теорема.
8. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
9. Конечные автоматы. Граф перехода автомата.
10. Графы и орграфы. Перечисление графов и отображений.
11. Алгоритмические задачи на графах.
12. Поля Галуа.
13. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
14. Основные понятия теории вероятностей и математической статистики.
15. Графы и орграфы. Перечисление графов и отображений.
16. Понятия группы, кольца, поля, их основные свойства. Основы теории конечных полей.
17. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
18. Конечные автоматы. Граф перехода автомата.
19. Архитектура современной ЭВМ. Основные принципы работы ее отдельных компонент.
20. Устройство персонального компьютера: центральный процессор, структура памяти, структура ввода-вывода.
21. Программный интерфейс вычислительной системы. Языки программирования низкого и высокого уровня. Компиляторы и интерпретаторы.
22. Технология объектно-ориентированного программирования.
23. Операционные системы. Функции ядра операционной системы.
24. Функции защиты информации.
25. Однопользовательская и многопользовательские многозадачные операционные системы.
26. Локальные и глобальные вычислительные сети. Типовые конфигурации сети.
27. Протоколы обмена данными.
28. Маршрутизация сообщений в сети.
29. Системы управления базами данных.

30. Реляционная, иерархическая и сетевая модели.
31. Распределенные базы данных в сетях ЭВМ.
32. Операционные системы. Функции ядра операционной системы.
33. Программный интерфейс вычислительной системы. Языки программирования низкого и высокого уровня.
34. Устройство персонального компьютера: центральный процессор, структура памяти, структура ввода-вывода.
35. Языки программирования низкого и высокого уровня. Компиляторы и интерпретаторы.
36. Функции защиты информации. Однопользовательская и многопользовательские многозадачные операционные системы.
37. Основные принципы современной концепции обеспечения защиты информации. Требования к защите с позиции пользователя.
38. Основные методы защиты информации. Методология организации и проведении работ по разработке и анализу средств защиты информации.
39. Основные положения государственной политики обеспечения информационной безопасности. Современная нормативно-правовая база в области защиты информации, защиты информации.
40. Понятие информации с ограниченным доступом. Цели защиты информации и степени секретности.
41. Лицензирование в области защиты информации. Сертификации средств защиты информации. Аттестации объектов информатики. Правовая основа сертификации.
42. Понятие угрозы информационной безопасности системы. Классификация угроз информационной безопасности. Угрозы нарушения конфиденциальности, целостности информации, отказа служб, разведки параметров системы. Понятия непосредственных и опосредованных угроз.
43. Основные уровни защиты информации в автоматизированных системах. Основные направления и методы реализации информационных угроз.
44. Понятие политики информационной безопасности. Каноническая модель управления доступом. Классификация каналов взаимодействия субъектов доступа. Основные модели управления доступом с взаимодействием субъектов доступа. Понятия дискреционного и мандатного механизмов управления доступом. Метки безопасности.
45. Метки безопасности. Их назначение в разграничении прав доступа при реализации мандатной модели доступа. Правила разграничения доступа для полномочной модели управления доступом. Особенности использования мандатного механизма управления доступом при разграничении прав доступа субъектов. Правила назначения меток безопасности иерархическим объектам доступа.
46. Анализ возможностей корректной реализации моделей управления доступом с каналом взаимодействия субъектов доступа для ОС UNIX.

Исключение субъектов и объектов из схемы мандатного управления доступом. Принципы организации мандатного управления доступом к устройствам.

47. Возможности разграничения доступа к системному диску для ОС Windows NT/2000/XP и Unix. Привилегированные процессы. Механизм обеспечения замкнутости программной среды и его роль в системе защиты. Реализация механизмов парольной защиты. Процедуры идентификации пользователя на рабочей станции и взаимной идентификации удаленных рабочих станций.
48. Контроль целостности информации, основные схемы контроля. Аутентификация информации. Угрозы преодоления парольной защиты. Усиление парольной защиты. Стандарты в области защиты информации в вычислительной системе, "Оранжевая книга" США, российские стандарты.
49. Основные понятия криптографии. Понятие симметричной и ассиметричной криптосистем. Основные типы криптоаналитических атак. Шифрование методом простой замены. Алгоритм простой замены. Шифрование методом полиалфавитной замены. Алгоритм полиалфавитной замены с использованием таблицы Вижинера.
50. Аддитивные методы шифрования. Шифрование методом перестановки. Карты Гамильтона. Аналитические методы шифрования.
51. Система открытого распространения ключей. Использование схемы открытого шифрования для создания цифровых подписей. Применение хэш-функции для создания цифровых подписей. Алгоритм цифровой подписи с использованием хэш-функции.
52. Защита информации от технической разведки. Основные физические каналы утечки информации о функционировании информационной системы. Узлы и блоки оборудования информационной системы, уязвимые для технической разведки. Технические параметры современных средств перехвата побочных сигналов. Меры и средства зашиты от инженерно-технической разведки. Методика оценки качества инженерно-технической защиты.
53. Разрушающие программные воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействий. Классификация вирусов. Методы выявления и защиты от вирусов.
54. Методика анализа алгоритмов защиты программных реализаций информационных систем. Методы восстановления алгоритмов защиты в программных продуктах. Оценка уровня криптографической защиты типовых программных продуктов.

Д.ф.-м.н., проф., проф. каф. ИБ Добрица В.П.