Программа междисциплинарного государственного экзамена по специальности 090102 – Компьютерная безопасность

БЛОК 1

Раздел 1. Математический анализ

1. Непрерывность действительных функций одной действительной переменной. Классификация точек разрыва. Свойства функций непрерывных на отрезке. Доказательство теоремы о промежуточном значении непрерывной функции.
2. Дифференцируемость функций одной и нескольких действительных переменных. Дифференциал функции. Достаточные условия дифференцируемости (без доказательства). Основные теоремы дифференциального исчисления функций одной переменной: теорема Ферма (с доказательством), теоремы Роля, Лагранжа, Коши (без доказательства).
3. Вывод формулы Тейлора для функций одной действительной переменной. Экстремумы функций одной переменной. Достаточное условие существования экстремума (с доказательством).
4. Абсолютно и условно сходящиеся числовые ряды: признаки сравнения и Даламбера (с доказательством), признаки Коши и Лейбница (без доказательства.)
5. Степенные ряды: теорема Абеля (без доказательства). Область и радиус сходимости степенного ряда. Ряды Тейлора и Маклорена. Достаточное условие разложимости функции в ряд Тейлора (с доказательством).
6. Первообразная и неопределенный интеграл. Определенный интеграл и его свойства. Существование первообразной для непрерывной функции (без доказательства). Интеграл с переменным верхним пределом, формула Ньютона-Лейбница (с доказательством).
7. Ряды Фурье. Признак Дини поточечной сходимости рядов Фурье (с доказательством).

Раздел 2. Алгебра

8. Матрицы и операции над ними. Определители матриц и их свойства. Ранг матрицы. Критерий обратимости матриц (с доказательством). Способы вычисления обратной матрицы.
9. Системы линейных уравнений. Критерий Кронекера–Капелли (с доказательством). Теорема о структуре общего решения системы линейных уравнений (без доказательства).
10. Кольцо вычетов. Сравнения и их основные свойства. Малая теорема Ферма (с доказательством).
11. Кольцо многочленов. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида.
12. Группы и их основные свойства. Примеры: циклические группы, конечные абелевые группы. Смежные классы по подгруппе. Теорема Лагранжа (с доказательством).
13. Векторные пространства их базисы и размерность. Координаты векторов в базисе и их изменение при переходе к другому базису.
14. Линейные преобразования векторного пространства и их матрицы. Характеристический многочлен линейного преобразования. Собственные значения и собственные векторы.
15. Квадратичные формы, их матрицы и ранг. Эквивалентность квадратичных форм, приведение к каноническому виду (с доказательством). Положительно определенные квадратичные формы, критерий Сильвестра (без доказательства).
16. Конечные поля. Характеристика поля. Построение конечного поля с заданным числом элементов.

Раздел 3. Теория вероятностей и математическая статистика

17. Вероятностное пространство. Аксиоматика А.Н. Колмогорова. Свойства вероятностной меры. Классическое определение вероятности.

18. Условные вероятности. Независимость событий. Формула полной вероятности и формула Байеса.
19. Случайные величины. Функции распределения случайных величин и их свойства. Плотности распределения. Типовые распределения: биномиальное, пуассоновское, равномерное, гауссовское (нормальное). Многомерные функции распределения. Многомерное нормальное Распределение. Независимые случайные величины.
20. Определение математического ожидания случайной величины, как интеграла Лебега по вероятностной мере. Формулы вычисления математических ожидания для дискретных и абсолютно непрерывных случайных величин. Дисперсия случайной величины и ее свойства. Коэффициент ковариации случайных величин. Вычисление математических ожиданий и дисперсий случайных величин имеющих типовые распределения.
21. Неравенство П.Л. Чебышева (с доказательством). Закон больших чисел в форме Чебышева (с доказательством).
22. Определение характеристических функций случайных величин. Вычисление характеристических функций случайных величин имеющих типовые распределения. Свойства характеристических функций (без доказательства). Метод характеристических функций в доказательстве предельных теорем. Центральная предельная теорема для независимых одинаково распределенных случайных величин с ограниченной дисперсией (с доказательством). Следствие: теорема Муавра-Лапласа.

Раздел 4. Теория функций комплексного переменного

23. Дифференцируемость функции комплексного переменного. Вывод условий Коши-Римана.
24. Интеграл от функции комплексного переменного. Теорема Коши об интеграле от аналитической функции по замкнутому контуру (с доказательством). Интегральная формула Коши (с доказательством).

Раздел 5. Дифференциальные уравнения

25. Основные типы дифференциальных уравнений первого порядка и методы их решения. Теорема существования и единственности решения дифференциального уравнения первого порядка (без доказательства).
26. Линейные дифференциальные уравнения n-го порядка, структура общего решения (без доказательства). Решение линейных дифференциальных уравнений n-го порядка с постоянными коэффициентами.

БЛОК II

Раздел 6. ДИСКРЕТНАЯ МАТЕМАТИКА

27. Алгебра множеств и отношений. Представление алгебр множеств и отношений матричными алгебрами.
28. Функциональные отношения. Отношения эквивалентности и порядка на конечных множествах, свойства их матриц.
29. Универсальные алгебры с конечным носителем. Представление операций многомерными двоичными массивами.

Раздел 7. МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

30. Булевы функции. Представление булевых функций формулами алгебры.
31. Исчисления высказываний и предикатов, их полнота и непротиворечивость.

Раздел 8. ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЯ

32. Мера количества информации. Энтропия и ее свойства.
33. Теорема Шеннона о пропускной способности канала связи.
34. Линейные блоковые коды. Корректирующие свойства кодов. Код Хемминга.
35. Определение циклического кода. Сверточный код. Алгоритм Витерби.

Раздел 9. КОМПЬЮТЕРНЫЕ СЕТИ

36. Виды атак в IP сетях. Причины уязвимости IP сетей.
37. Модель информационной безопасности систем. Типовые виды угроз безопасности.
38. Классификация способов и средств защиты информации в сетях.
39. Защита от вирусов.
40. Стандартные методы защиты сетей, МСЭ. Защита доверительной сети, VPN.
41. Требования к системе безопасности сетей. Принципы построения системы обеспечения безопасности корпоративной сети.

Раздел 9. СТРУКТУРЫ ДАННЫХ И АЛГОРИТМЫ

42. Понятие базы данных и СУБД. Основные функции СУБД. Иерархическая, сетевая и реляционная модели данных.
43. Алгоритмы на графах. Алгоритм Крускала. Алгоритм Дейкстры. Оценка сложности.
44. Алгоритмы внутренней сортировки. Оценка трудоемкости.
45. Алгоритмы поиска в последовательно организованных файлах. Оценка трудоемкости.
46. Алгоритмы поиска в деревьях.

Раздел 10. ЗАЩИТА ИНФОРМАЦИИ

47. Основные понятия защиты информации. Построение защищенной автоматизированной системы.
48. Угрозы безопасности информации. Понятие политики безопасности.
49. Модели системы безопасности, примеры моделей.
50. Основные положения критериев TCSEC ("Оранжевая книга").
51. Основные положения Руководящих документов ГТК в области защиты информации.
52. Основные положения CCITSE ("Единые критерии").
53. Криптография и криптоанализ. Конфиденциальность, целостность, имитостойкость. Теоретическая и практическая стойкость шифра.
54. Классификация криптографических систем. Шифры простой и сложной замены, перестановки, гаммирования.
55. Криптосистемы с секретным ключом. Поточные криптосистемы. Шифрование методом гаммирования.
56. Криптосистемы с секретным ключом. Блочные шифры. Сеть Фейстеля. Стандарт шифрования DES. Российский стандарт шифрования ГОСТ 28147-89. Основные режимы работы блочных шифров.
57. Криптосистемы с открытым ключом. Односторонние функции, односторонние функции с секретом. Криптосистема RSA. Криптосистема Эль Гамаля.
58. Криптографические хэш-функции. Однонаправленные хэш-функции. Алгоритм безопасного хеширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции ГОСТ Р 34.11-94.
59. Электронная цифровая подпись. Схемы ЭЦП
60. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.
61. Правовые основы защиты информации с использованием технических средств.
62. Организация и обеспечение режима секретности.
63. Лицензирование и сертификация в области защиты информации.

Рекомендуемая литература для подготовки к экзамену

Раздел 1. МАТЕМАТИЧЕСКИЙ АНАЛИЗ

Основная:

1. Зорич В.А., Математический анализ. Ч.1.-М.: Наука. - Ч.2.-М.: Наука. 1984
2. Кудрявцев Л.Д. Курс математического анализа. - Т.1,2.-М.: ВШ, 1981
3. Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления. - Т.1,2,3.-М.: Наука,1961
4. Демидович Б.Н. Сборник задач и упражнений по математическому анализу (любое издание)
5. Колмогоров А.Н., Фомин С.В. Элементы теории функций и функционального анализа. М.: Наука,1978

Дополнительная:

1. Никольский С.М. Курс математического анализа. - Т.1,2.-М.: Наука,1973
2. Рудин У. Основы математического анализа. М.: Наука,1976
3. Толстов Г.П. Мера и интеграл. - М.: Наука,1976

Раздел 2. АЛГЕБРА

Основная:

1. Кострикин А.И. Введение в алгебру. - М.: Наука, учебник, 1977
2. Фаддев Д.К., Соминский И.С. Сборник задач по высшей алгебре. - М.: Наука, 1977
3. Сборник задач по алгебре (под ред. А.И. Кострикина). - М.: Наука, 1995

Дополнительная:

1. Курош А.Г. Курс высшей алгебры. - М.: Наука,1965
2. Скорняков Л.А. Элементы общей алгебры. - М.: Наука, 1983
3. Фаддеев Д.К. Лекции по алгебре. - М.: Наука, 1984
4. Куликов Л.Я. Алгебра и теория чисел. - М.: Высшая школа, 1979

Раздел 3. ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА.

Основная:

1. Ширяев А. Н. *Вероятность*. М.: Наука, 1989.
2. Боровков А. А. *Теория вероятностей*. М.: Наука, 1986.
3. Гнеденко Б. В. *Курс теории вероятностей*. М.: Наука, 1969.
4. Боровков А. А. *Математическая статистика.* М.: Наука, 1984.
5. Козлов М. В., Прохоров А. В. *Введение в математическую статистику.* М.: МГУ, 1987.
6. Розанов Ю. А. *Случайные процессы*. М.: Наука, 1971, 1979.
7. Розанов Ю. А. *Теория вероятностей, случайные процессы и математическая статистика*. М.: Наука, 1985.

Дополнительная:

1. Феллер В. *Введение в теорию вероятностей и её приложения*. Т. 1, 2. М.: Мир, 1967, 1983.
2. Чистяков В. П. *Курс теории вероятностей*. М.: Наука, 1978.
3. Ван дер Варден Б. Л. *Математическая статистика.* М.: ИЛ, 1960.
4. Боровков А. А. Математическая статистика: дополнительные главы. М.: Наука, 1984.
5. Вентцель А. Д. *Курс теории случайных процессов*. М.: Наука, 1975.
6. Гихман И. И., Скороход А. В. *Введение в теорию случайных процессов*. М.: Наука, 1977.
7. Розанов Ю. А. *Введение в теорию случайных процессов*. М.: Наука, 1982.

Раздел 4. ТЕОРИЯ ФУНКЦИЙ КОМПЛЕКСНОГО ПЕРЕМЕННОГО

Основная:

1. Привалов И.И., Введение в теорию функций комплексного переменного. - М.: Наука, 1967
2. Маркушевич А.И. Краткий курс теории аналитических функций. - М.: Наука, 1966
3. Сидоров Ю.В., Федорюк М.В., Шабунин М.И. Лекции по теории функций комплексного переменного. - М.: Наука, 1976

4. Сборник задач по теории аналитических функций под редакцией М.А. Евграфова. - М.: Наука, 1972

Дополнительная:

1. Александров И.А., Соболев В.в. Аналитические функции комплексного переменного**. -** М.: Высшая школа, 1984
2. Лаврентьев М.А., Шабат Б.В. Методы теории функций комплексного переменного**. -** М.: Наука, 1973

Раздел 6. ДИСКРЕТНАЯ МАТЕМАТИКА

1. Акимов О.Е. Дискретная математика: логика, группы, графы. – М.: Лаборатория Базовых Знаний, 2001. – 352 с.: ил.
2. Андерсон, Джеймс А. Дискретная математика и комбинаторика: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 960 с.: ил.
3. Белоусов А.И., Ткачев С.Б. Дискретная математика. Учеб для вузов / Под ред. В.С. Зарубина, А.П. Крищенко. – М.: Издательство МГТУ им. Н.Э. Баумана, 2001. – 744 с. (Сер. Математика в техническом университете; Вып. XIX).
4. Горбатов В.А. Фундаментальные основы дискретной математики. Информационная математика. – М.: Наука. Физматлит, 1999. – 544 с., ил.
5. Грэхем Р., Кнут Д., Поташник О. Конкретная математика. Основание информатики: Пер. с англ. – М.: Мир, 1998. – 703 с., ил.
6. Ерусалимский Я.М. Дискретная математика: Теория, задачи, приложения. – 5-е изд. перераб. и дополн. – М.: Вузовская книга, 2002. – 268 с.: ил.
7. Иванов Б.Н. Дискретная математика. Алгоритмы и программы: Учеб. пособие. – М.: Лаборатория Базовых Знаний, 2001. – 288 с.: ил.
8. Нефедов В.Н., Осипова В.А. Курс дискретной математики: Учеб. пособие. – М.: Издательство МАИ, 1992. – 264 с.: ил.
9. Романовский И.В. Дискретный анализ. Учебное пособие для студентов, специализирующихся по прикладной математике и информатике. – Издание 2-е, исправленное. – СПб.: Невский диалект, 2000. – 240 с., ил.

Раздел 7. МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

1. Акимов О.Е. Дискретная математика: логика, группы, графы. – М.: Лаборатория Базовых Знаний, 2001. – 352 с.: ил.
2. Верещагин Н.К., Шень А. Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления. М.: МЦНМО, 2000. – 288 с. (Серия «Современные лекционные курсы»).
3. Гиндикин С.Г. Алгебра логики в задачах. – М.: Наука, 1972. – 288 с., ил.
4. Гладкий А.В. Математическая логика. – М.: Российск.гос.гуманит.ун-т, 1998. – 479 с.
5. Горбатов В.А. Фундаментальные основы дискретной математики. Информационная математика. – М.: Наука. Физматлит, 1999. – 544 с., ил.
6. Грей П. Логика, алгебра и базы данных / Пер. с англ. Х.И. Килова, Г.Е. Минца; Под ред. Г.В. Орловского, А.О. Слисенко. – М.: Машиностроение, 1989. – 368 с.: ил.
7. Ерусалимский Я.М. Дискретная математика: Теория, задачи, приложения. – 5-е изд. перераб. и дополн. – М.: Вузовская книга, 2002. – 268 с.: ил.
8. Лавров И.А. Максимова Л.Л. Задачи по теории множеств, математической логике и теории алгоритмов / Под ред. Н.В. Белякина, В.В. Донченко. – М.: Наука, 1975. – 240 с.
9. Лихтарников Л.М., Сукачева Т.Г. Математическая логика. Курс лекций. Задачник-практикум и решения. Серия «Учебники для вузов, специальная литература». – СПб.: Издательство «Лань». – 1999. – 288 с.
10. Мощенский В.А. Лекции по математической логике. – Минск, Издателство БГУ, 1973. – 160 с.

Раздел 8. ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЯ

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки, М.: «Мир», 1986. – 576с.

2. Теория электрической связи // под ред. Д.Д. Кловского, М.: Радио и связь, 1998. – 432с.

3. Стратанович Р.Л. Теория информации. М.: «Сов. радио», 1975. – 424с.

Раздел 9. СТРУКТУРЫ ДАННЫХ И АЛГОРИТМЫ

1. Базы данных и СУБД.

1.1. Карпова Т. С. Базы данных: модели, разработка, реализация.- СПб.: Питер,2001..
1.2. Конноли Т., Бегг К., Страчан А. Базы данных: проектирование, реализация и сопровождение.-М: Вильямс,2001
1.3. Дейт К.Дж. Введение в системы баз данных. -М.: Вильямс, 1998

2. Структуры данных.

2.1. Макконел Дж. Анализ алгоритмов. Вводный курс. – М.: Техносфера, 2002.
2.2. Вирт Н. Алгоритмы + структуры данных = программы. М.: Мир, 1985.
2.3. Кук Д., Бейз Г. Компьютерная математика. - М.: Наука, 1190.
2.4. Новиков Ф. А. Дискретная математика для программистов. – СПб.: Питер, 2001.
2.5. Кнут Д. Искусство программирования. т 1. Основные алгоритмы.
2.6. Кнут Д. Искусство программирования. т 3. Сортировка и поиск.
2.7. Кормен Т. и др. Алгоритмы: построение и анализ. –М. : МЦНМЩ, 2001.

Раздел 10. ЗАЩИТА ИНФОРМАЦИИ

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. М.: ГЕЛИОС АРВ, 2002.
2. Бабаш А.В., Шанкин Г.П. Криптография. Аспекты защиты. М.: Солон-Р, 2002.
3. Введение в криптографию (под ред. В.В. Ященко). М.: МЦНМО-ЧеРо, 1998.
4. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001.
5. Столингс В. Криптография и защита сетей. Принципы и практика. М.: Издательский дом “Вильямс”, 2001.
6. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999.
7. Чмора А. Современная прикладная криптография. М.: ГЕЛИОС АРВ, 2002.
8. Шнайер Б. Прикладная криптография. М.: Триумф, 2002.
9. Пазизин С.В. Основы защиты информации в компьютерных системах. М.: ТВП, 2003.
10. Стрельцов А.А. Обеспечение информационной безопасности России. М.: МЦНМО, 2002.
11. Герасименко В.А., Малюк А.А. Основы защиты информации. М., 1997.
12. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. М., 1996.
13. Галатенко В.А. Основы информационной безопасности. М.: ИНТУИТ, 2003.