Омский государственный университет им. Ф.М. Достоевского

Факультет компьютерных наук

Утверждено ученым советом
факультета компьютерных наук
«17» октября 2008 г.

Программа государственного экзамена

по специальности 075200 – «Компьютерная безопасность»

Раздел 1. МАТЕМАТИЧЕСКИЙ АНАЛИЗ

1. Непрерывность действительных функций одного и многих действительных переменных. Свойства непрерывных функций.
2. Дифференцируемость функций одного и многих действительных переменных в точке и на множестве. Достаточные условия дифференцируемости. Производные и дифференциалы высших порядков.
3. Теоремы о среднем для действительных функций одного действительного переменного (Ролля, Лагранжа, Коши).
4. Формула Тейлора для действительных функций одного и многих действительных переменных. Экстремум действительной функции одного и многих действительных переменных достаточные условия его существования.
5. Числовой ряд. Сходящиеся ряды и их простейшие свойства. Признаки сходимости рядов с положительными членами (признаки сравнения, Даламбера, Коши). Абсолютно и не абсолютно сходящиеся ряды. Признак Лейбница.
6. Функциональные ряды. Равномерно сходящиеся ряды. Критерий Коши равномерной сходимости ряда. Непрерывность суммы равномерно сходящегося ряда непрерывных функций. Теорема о почленном дифференцировании ряда.
7. Степенные ряды. Первая теорема Абеля. Область и радиус сходимости степенного ряда. Равномерная сходимость степенного ряда. Непрерывность суммы, почленная дифференцируемость. Ряд Тейлора для функции одного действительного переменного.
8. Элементарная теория интеграла. Первообразная и неопределенный интеграл. Существование первообразной для непрерывной функции. Определенный интеграл и его свойства. Формула Ньютона-Лейбница.
9. Ряды Фурье и их сходимость. Неравенство Бесселя и равенство Парсеваля. Свойство рядов Фурье. Интеграл и преобразования Фурье.

ЛИТЕРАТУРА

1. Фихтенгольц Г.М. Основы математического анализа. В 2-х тт. М., 2002
2. Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления. Т.1-3. М., 1970
3. Архипов Г.И., Садовничий В.А., Чубариков В.Н. Лекции по математическому анализу. М.: Высшая школа, 2000.
4. Зорич В.А. Математический анализ. Т.1-2. М., 1981
5. Никольский С.М. Курс математического анализа. Т. 1-2. М.: Наука, 1973.
6. Рудин У. Основы математического анализа. СПб., 2002.
7. Файзуллин Р.Т. Основы математического анализа. Омск, 2002.

Раздел 2. ТЕОРИЯ ФУНКЦИЙ КОМПЛЕКСНОГО ПЕРЕМЕННОГО

10. Предел и непрерывность комплекснозначной функции комплексного переменного. Дифференцируемость функции комплексного переменного. Условия Коши-Римана.
11. Степенные ряды. Радиус сходимости. Ряд Лорана и его область сходимости.
12. Интеграл от функции комплексного переменного. Теорема Коши. Интегральная формула Коши.
13. Разложение функции комплексного переменного в ряды Лорана и Тейлора. Классификация изолированных особых точек функций и поведение функции в окрестностях особой точки.
14. Вычеты. Основная теорема о вычетах.

ЛИТЕРАТУРА

1. Гуц А.К. Комплексный анализ и информатика. Омск: ОмГУ, 2002.
2. Бицадзе А.В. Основы теории аналитических функций комплексного переменного. М.: Наука, 1969.
3. Волковыский Л.И., Лунц Г.Л., Араманович И.Г. Сборник задач по теории функций комплексного переменного. М.: Наука, 1975.
4. Гичев В.М. Основы комплексного анализа. Часть I. Омск: изд-во ОмГУ, 2000.
5. Сидоров Ю.В., Федорюк М.В., Шабунин М.И. Лекции по теории функций комплексного переменного. М.: Наука, 1989.

Раздел 3. ДИФФЕРЕНЦИАЛЬНЫЕ УРАВНЕНИЯ

15. Основные типы дифференциальных уравнений 1-го порядка и методы их решения.
16. Теорема существования и единственности решения уравнения первого порядка.
17. Линейные уравнения *n*-го порядка. Структура его общего решения.
18. Линейные уравнения *n*-го порядка с постоянными коэффициентами.
19. Системы линейных дифференциальных уравнений с постоянными коэффициентами.
20. Структура общего решения линейной системы уравнений.

ЛИТЕРАТУРА

1. Петровский И.Г. Лекции по теории обыкновенных дифференциальных уравнений. М.:Наука, 1970.
2. Понтрягин Л.С. Обыкновенные дифференциальные уравнения. М.: Наука, 1970.
3. Филиппов А.Ф. Сборник задач по дифференциальным уравнениям. М.: Наука, 1992.

Раздел 4. ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА

21. Вероятностное пространство. Аксиомы теории вероятностей. Свойства вероятностной меры. Условные вероятности. Независимость случайных событий.
22. Классическая схема. Схема Бернулли.
23. Случайные величины, распределения случайных величин. Функции распределения и их свойства. Типы распределений. Случайные векторы.
24. Математическое ожидание случайной величины и его свойства. Дисперсия случайной величины и ее свойства. Коэффициент корреляции и его свойства. Неравенства Иенсена, Чебышева и Маркова.
25. Определение и свойства характеристических функций. Теорема непрерывности для характеристических функций.
26. Сходимость по вероятности и почти наверное. Слабая сходимость распределений и сходимость по распределению. Теорема о слабой сходимости.
27. Законы больших чисел. Неравенство Колмогорова. Сильный закон больших чисел для последовательности независимых неодинаково распределенных величин (теорема Колмогорова).

28. Центральная предельная теорема для стандартной схемы серий. Теоремы Линдебегра-Феллера и Ляпунова.
29. Дискретные цепи Маркова. Примеры цепей Маркова. Классификация состояний цепи Маркова. Эргодические теоремы для цепей Маркова
30. Определение случайного процесса. Теорема Колмогорова о согласованных распределениях (без доказательства). Классификация случайных процессов. Пуассоновский случайный процесс. Винеровский процесс.
31. Марковские цепи с непрерывным временем. Прямые и обратные дифференциальные уравнения Колмогорова.
32. Основные понятия математической статистики: статистические модели, стратегии, функции риска. Эмпирическое распределение и эмпирическая функция распределения. Теорема Гливенко-Кантелли. Метод моментов и метод максимального правдоподобия. Несмещенные оценки, состоятельные оценки. Достаточные статистики. Факторизационная теорема Неймана-Фишера. Эффективные оценки. Неравенство Рао-Крамера.
33. Проверка статистических гипотез. Наиболее мощный и равномерно наиболее мощный критерии. Лемма Неймана-Пирсона. Понятие о непараметрических критериях. Критерий хи-квадрат.

ЛИТЕРАТУРА

1. Боровков А. А. Теория вероятностей. М: Наука, 1986
2. Боровков А. А. Теория вероятностей. М: Наука, 2003
3. Ширяев А.Н. Вероятность. М: Наука, 1989
4. Ивченко Г. И., Медведев Ю.И. Математическая статистика. М: Высшая школа, 1984
5. Боровков А. А. Математическая статистика. Наука, 1984

Раздел 5. АЛГЕБРА

34. Матрицы и операции над ними. Определители матриц и их свойства. Теорема Лапласа. Определитель произведения матриц. Критерий обратимости матриц.
35. Ранг матрицы над полем, способы его вычисления. Ранг произведения матриц. Обратная матрица и способы ее вычисления.
36. Системы линейных уравнений над полем. Критерий Кронекера-Капелли. Алгоритм Гаусса. Фундаментальная система решений однородной системы линейных уравнений. Общее решение системы линейных уравнений.
37. Нормальные делители группы. Факторгруппа, теорема о гоморфизме групп..
38. Векторные пространства над полем, их базисы и размерность. Координаты векторов в базисе и их изменение при переходе к другому базису. Свойства конечномерных векторных пространств. Подпространства векторного пространства, операции над ними. Размерности суммы и пересечения подпространств.
39. Линейное преобразование векторного пространства, его матрица в данном базисе, примеры. Критерии обратимости преобразования.
40. Характеристический многочлен линейного преобразования. Собственные значения и собственные векторы преобразования, инвариантные подпространства.
41. Подобные матрицы. Теорема о приведении матрицы к жордановой нормальной форме.
42. Евклидово (унитарное) пространство и его свойства. Существование ортонормированного базиса. Ортогональное дополнение подпространства.
43. Квадратичная форма над полем, ее матрица и ранг. Эквивалентность квадратичных форм, канонический вид. Квадратичные формы над полями действительных и комплексных чисел. Закон инерции.
44. Кольца и их идеалы. Фактор-кольца, поля. Простые поля, расширения полей.
45. Конечные поля, характеристика поля, число элементов, теорема о примитивном элементе. Описание подполей.
46. Неприводимые многочлены над конечными полями. Построение конечного поля с заданным числом элементов.

ЛИТЕРАТУРА

1. Курош А.Г. Курс высшей алгебры. М.: Наука, 1975.
2. Ван дер Варден Б.Л. Алгебра. М.: Наука, 1979.
3. Кострикин А.И. Введение в алгебру. Часть I.: Основы алгебры. М.: Физико-математическая литература, 2000.
4. Кострикин А.И. Введение в алгебру. Часть II.: Линейная алгебра. М.: Физико-математическая литература, 2000.
5. Кострикин А.И. Введение в алгебру. Часть III.: Основные структуры алгебры. М.: Физико-математическая литература, 2000.
6. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра. Т. I, II. М.: Гелиос АРВ, 2003.

Раздел 6. МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

47. Исчисления высказываний и предикатов, их полнота и непротиворечивость.
48. Теорема Гёделя о неполноте.
49. Основные подходы к формализации понятия алгоритма: машины Тьюринга, рекурсивные функции.
50. Понятие сложности алгоритма. Классы сложности. Эффективный алгоритм.

ЛИТЕРАТУРА

1. Гуц А.К. Математическая логика и теория алгоритмов. Омск: Наследие. Диалог-Сибирь, 2003.
2. Мальцев А.И. Алгоримы и рекурсивные функции. М.: Наука, 1986.
3. Ершов Ю.Л. Палютин Е.А. Математическая логика. М., 2004.
4. Лавров И.А. и др. Задачи по теории множеств, математической логике и теории алгоритмов. М., 2003.

Раздел 7. ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЯ

51. Энтропия и ее свойства. Количество информации. Общая схема линии связи.
52. Источник сообщения, его энтропия и избыточность.
53. Поток информации и пропускная способность канала связи.
54. Оптимальное кодирование. Корректирующие свойства кодов.
55. Линейный код и способы его задания. Процесс декодирования линейного кода. БЧХ-коды. Код Хемминга.

ЛИТЕРАТУРА

1. Самсонов Б.Б., Плохов Е.М., Филоненков А.И. Теория информации и кодирование. М., 2002.
1. Галлагер Р. Теория информации и надежная связь. М.: Сов.радио, 1974.
2. Колесник В.Д., Полтырев Г.Ш. Курс теории информации. М.: Наука, 1982.
3. Кричевский Р.Е. Сжатие и поиск информации. М.: Радио и связь, 1989.
4. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.Л. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М.:Мир, 1976.
6. Шеннон К. Работы по теории информации и кибернетике. М.: ИЛ, 1963.

Раздел 8. ЗАЩИТА ИНФОРМАЦИИ

Модели безопасности

56. Основные понятия защиты информации (субъекты, объекты, доступ, граф доступов, информационные потоки). Постановка задачи построения защищенной автоматизированной системы (АС). Модели ценности информации. Аддитивная модель. Порядковая шкала. Модель решетки ценности. *MLS* решетка.
57. Угрозы безопасности информации. Угрозы конфиденциальности, целостности, доступности, раскрытия параметров АС. Понятие политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности.

58. Модель системы безопасности *HRU*. Основные положения модели. Теорема об алгоритмической неразрешимости проблемы безопасности в произвольной системе.
59. Модель распространения прав доступа *Take-Grant*. Теоремы о передаче прав в графе доступов, состоящем из субъектов, и произвольном графе доступов. Расширенная модель *Take-Grant* и ее применение для анализа информационных потоков в АС.
60. Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели. Базовая теорема безопасности (*BST*).

Криптографические методы защиты информации

61. Блочные шифры DES, ГОСТ, режимы шифрования.
62. Криптосистемы с открытым ключом. Криптосистема *RSA*. Выбор параметров.

Организационно-правовое обеспечение информационной безопасности

63. Основные положения критериев *TCSEC* (“Оранжевая книга”). Фундаментальные требования компьютерной безопасности. Требования классов защиты.
64. Структура и состав системы нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.
65. Правовой режим защиты государственной тайны.
66. Правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.);
67. Организация и обеспечение режима секретности.
68. Лицензирование и сертификация в области защиты информации

Защита в сетях и Интернет

69. Возможные атаки против хоста сети в Интернете. Протоколы и сервисы Интернета,и их подверженность атакам.
70. Аутентификация в Интернете. Протоколы стека TCP/IP. Соединение по протоколу TCP. Состояния соединения.
71. Хэш-функции. Модель итеративной хэш-функции. Использование хэш-функций для обеспечения контроля целостности данных и аутентификации сообщений. MAC-код (Message Authentication Code). Свойства хэш-функций.
72. Цифровые подписи. Цифровая подпись. Цифровая подпись с добавлением.

Криптографические протоколы.

73. Протоколы совместного вычисления ключей (протокол Диффи-Хелмана, протокол Хьюза).
74. Протоколы разделения секрета (схема Блэкли, схема Шамира).
75. Доказательство с нулевым разглашением (протокол «Изоморфизм графов», протокол Фиата-Шамира).
76. Протоколы «честной игры» (электронная ставка, электронный покер).
77. Протокол Kerberos.

ЛИТЕРАТУРА

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. М.: Гелиос АРВ, 2001.
2. Зегжда Д.П. Ивашко А.М. Основы безопасности информационных систем. М., 2000.
3. Лавров Д.Н. Элементы теории чисел и криптографии. Омск, 2003.
4. Введение в криптографию / Под общ. Ред. В.В. Ященко. М.: МЦНМО, «ЧеРо», 1998.
5. Анохин М. А., Варновский Н. П., Сидельников В. М., Ященко В.В. Криптография в банковском деле, МИФИ, 1997.
6. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб.: Изд-во «Лань», 2000.

7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2003
8. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
9. Саломаа А. Криптография с открытым ключом. М.: Мир, 1996.
10. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. М.: ДМК Пресс, 2002
11. Девянин П.Н. Модели безопасности компьютерных систем. М.:ACADEMIA, 2005
12. Копылов В.А. Информационное право: Учебное пособие. – М.: Юристъ, 1997. – 472 с.

Раздел 9. ДИСКРЕТНАЯ МАТЕМАТИКА

78. Представление булевых функций совершенными дизъюнктивными и конъюнктивными нормальными формами и полиномами Жегалкина.
79. Постовские классы. Теорема Поста о функциональной полноте.
80. Построение кратчайших остовных деревьев: алгоритм Краскала и алгоритм Прима.
81. Эйлеров цикл: критерий существования и алгоритм поиска.
82. Гамильтонов цикл: достаточные условия существования. Задача коммивояжера.
83. Поиск кратчайших путей: алгоритм Флойда, алгоритм Дейкстры.
84. Планарные графы: теорема о пяти красках, алгоритмы раскрашивания.

ЛИТЕРАТУРА

1.Новиков Ф.А. Дискретная математика для программистов. С.-П.: Питер, 2001.
2. Яблонский С.В. Введение в дискретную математику. М.: Высшая школа, 2001.
3. Горбатов В.А. Дискретная математика. М.,2000.

Программа принята на ученом совете ФКН 17 октября 2008 г. (Протокол № 2).

Председатель ученого совета А.К. Гуц