МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

Факультет вычислительной математики и кибернетики

ПРОГРАММА

вступительного экзамена в аспирантуру
по направлению 10.06.01 – информационная безопасность,
направленность 05.13.19 – «методы и системы защиты информации, информационная безопасность»

От экзаменующегося требуется: знание материала, предусмотренного в общей и дополнительной частях; умение кратко изложить содержание работы, представленной в качестве реферата, и владение всем кругом вопросов связанных с узкой областью, к которой относится реферат.

1. Общая часть.

1. Непрерывные функции одной переменной и их свойства. Равномерная непрерывность. Равностепенная непрерывность семейства функций. Теорема Арцела.
2. Функции многих переменных. Полный дифференциал, и его геометрический смысл. Достаточные условия дифференцируемости. Градиент.
3. Определенный интеграл. Интегрируемость непрерывной функции. Первообразная непрерывной функции. Приближенное вычисление определенных интегралов. Формулы трапеций и Симпсона, оценки погрешностей. Понятие о методе Гаусса.
4. Числовые ряды. Сходимость рядов. Критерий Коши. Достаточные признаки сходимости (Коши, Деламбера, интегральный, Лейбница).
5. Абсолютная и условная сходимость ряда. Свойства абсолютно сходящихся рядов. Перестановка членов ряда. Теорема Римана. Умножение рядов.
6. Ряды и последовательности функций. Равномерная сходимость. Признак Вейерштрасса. Свойства равномерно сходящихся рядов (непрерывность суммы, почленное интегрирование и дифференцирование).
7. Собственные и несобственные интегралы, зависящие от параметра. Равномерная сходимость по параметрам и ее признаки. Непрерывность, интегрирование и дифференцирование интегралов по параметру.

8. Мера множества. Измеримые функции. Интеграл Лебега и его основные свойства.

9. Степенные ряды в действительной и комплексной области. Радиус сходимости. Теорема Коши-Адамара. Теорема Абеля. Свойства степенных рядов (почленное интегрирование и дифференцирование). Разложение элементарных функций.

10. Функции комплексного переменного. Условия Коши-Римана. Геометрический смысл аргумента и модуля производной.

11. Элементарные функции комплексного переменного z^n, e^z, $\frac{az+b}{ez+d}$, и даваемые ими конформные отображения. Простейшие многозначные функции $\sqrt{z}$, $Ln(z)$.

12. Теорема Коши об интеграле по замкнутому контуру. Интеграл Коши. Ряд Тейлора.

13. Ряд Лорана. Полюс и существенно особая точка. Вычеты. Основная теорема о вычетах и ее применение.

14. Линейные преобразования. Квадратичные формы. Приведение их к каноническому виду линейными преобразованиями в комплексной и действительной областях. Закон инерции.

15. Линейная зависимость и независимость векторов. Ранг матрицы. Системы линейных алгебраических уравнений, теорема Кронекера-Капелли. Общее решение системы линейных алгебраических уравнений.

16. Ортогональные преобразования в евклидовом пространстве и ортогональные матрицы. Свойства ортогональных матриц.

17. Характеристический многочлен линейного преобразования векторного пространства. Собственные числа и собственные векторы. Свойства собственных чисел и векторов симметрических матриц. Понятие о методе ортогональных вращений решения полной проблемы собственных значений.

18. Итерационные методы решения уравнения $f(x)=0$ (хорд, Ньютона). Принцип сжатых отображений в полных метрических пространствах и его применение.

19. Линейные операторы, норма линейного оператора. Итерационные методы решения систем линейных алгебраических уравнений (методы простой итерации и Зейделя).

20. Гильбертово пространство. Линейные и билинейные функционалы в гильбертовом пространстве. Линейные уравнения с вполне непрерывным оператором.

21. Интегральные уравнения Фредгольма 2-ого рода. Теорема Фредгольма. Интегральные уравнения с симметричным ядром.

22. Ортогональные системы функций. Ряды Фурье по ортогональной системе функций, неравенство Бесселя, сходимость ряда Фурье. Достаточные условия равномерной сходимости рядов Фурье по тригонометрической системе функций. Влияние гладкости функции на порядок коэффициентов Фурье.

23. Теорема существования и единственности решения задачи Коши для уравнения, системы уравнений первого порядка и уравнения n-ого порядка.

24. Линейные дифференциальные уравнения n-ого порядка. Линейное однородное уравнение. Линейная независимость функций. Фундаментальная система решений. Определитель Вронского. Общее решение неоднородного уравнения.

25. Линейные обыкновенные дифференциальные уравнения с постоянными коэффициентами (однородные и неоднородные).

26. Устойчивость по Ляпунову решений обыкновенных дифференциальных уравнений. Теорема об устойчивости по первому приближению. Второй метод Ляпунова.

27. Простейшая задача вариационного исчисления. Уравнение Эйлера. Вариационная задача с подвижными концами. Условия трансверсальности.

28. Градиентные методы поиска экстремума.

29. Формализация понятия алгоритма (машины Тьюринга, нормальные алгоритмы Маркова). Алгоритмическая неразрешимость.

30. Структура и состав вычислительной системы (аппаратура + программное обеспечение). Физические и виртуальные ресурсы. Управление ресурсами в вычислительной системе. Потоки управляющей информации и данных в вычислительной системе. Проблемы дисбаланса производительности компонентов вычислительной системы и аппаратно-программные решения, предназначенные для сглаживания этого дисбаланса. Кеширование информационных потоков в вычислительной системе.

31. Архитектура многопроцессорных вычислительных систем. Графовая модель представления параллельных алгоритмов. Принципы построения

параллельных программ с использованием технологий MPI и OpenMP. Показатели качества параллельных программ. Закон Амдала, его следствия.

32. Операционные системы, основные функции. Типы операционных систем. Организация управления и взаимодействия процессов в Операционной системе. Модели и средства синхронизации. Программирование взаимодействующих процессов. Модели организации и управления ОЗУ.

33. Парадигмы программирования (функциональное, императивное, объектно-ориентированное программирование).

34. Базы данных. Основные понятия реляционной модели данных. Реляционная алгебра. Средства языка запросов SQL.

35. Функции алгебры логики. Реализация их формулами. Совершенная дизъюнктивная нормальная форма.

36. Схемы из функциональных элементов и простейшие алгоритмы их синтеза. Оценка сложности схем, получаемых по методу Шеннона.

ЛИТЕРАТУРА

1. Ильин В.А., Поздняк Э.Г. Основы математического анализа, часть 1 и часть 2. М.: Физматлит, 2005 (часть 1) и 2002 (часть 2).
2. Кудрявцев Л.Д. Математический анализ, часть 1 и часть 2. М.: Дрофа, 2003 (часть 1) и 2004 (часть 2).
3. Александров П.С. Лекции по аналитической геометрии. М.: Наука, 1968.
4. Воеводин В.В. Линейная алгебра. М.: Наука, 1980.
5. Привалов И.И. Введение в теорию функций комплексного переменного. СПб.: Лань, 2009.
6. Свешников А.Г., Тихонов А.Н. Теория функций комплексного переменного. М.: Физматлит, 2008.
7. Гельфанд И.М. Лекции по линейной алгебре. Изд-во МЦНМО, 1998.
8. Курош А.Г. Курс высшей алгебры. СПб.: Лань, 2006.
9. Колмолгоров А.Н., Фомин С.В. Элементы теории функций и функционального анализа. М.: Физматлит, 2004.
10. Шилов Г.Е. Введение в теорию линейных пространств. М.: ГИТТЛ, 1956.
11. Понтрягин Л.С. Обыкновенные дифференциальные уравнения. М.: Наука, 1982.
12. Степанов В.В. Курс дифференциальных уравнений. М.: Эдиториал УРСС, 2004.
13. Петровский И.Г. Лекции по обыкновенным дифференциальным уравнениям. М.: Физматлит, 2009.
14. Эльсгольц Л.Э. Дифференциальные уравнения и вариационное исчисление. М.: Наука, 1969.

15. Тихонов А.Н., Самарский А.А. Уравнения математической физики. М.: Наука, 2004.
16. Соболев С.Л. Уравнения математической физики. М.: Наука, 1966.
17. Петровский И.Г. Лекции об уравнениях с частными производными. М.: Физматлит, 2009.
18. Березин И.С., Жидков Н.П. Методы вычислений, том 1 и том 2. М.: ГИФМЛ, 1962 (том 1) и 1959 (том 2).
19. Бахвалов Н.С. Численные методы. М.: Наука, 1975.
20. Самарский А.А. Введение в теорию разностных схем. М.: Наука, 1971.
21. Феллер В. Введение в теорию вероятностей и ее приложения, том 1 и том 2. М.: Мир, 1964 (том 1) и 1967 (том 2).
22 Крамер Г. Математические методы статистики. М.: Мир, 1975.
23. Яблонский С.В. Введение в дискретную математику. М.: Высшая Школа, 2010.
24. Алексеев В.Б. Лекции по дискретной математике. М.: Инфра-М, 2012.
25. Ложкин С.А. Лекции по основам кибернетики. М.: Издательский отдел ф-та ВМК МГУ, 2004.
26. Мальцев А.И. Алгоритмы и вычислимые функции. М.: Наука, 1986.
27. Карлин С. Математические методы в теории игр, программировании и экономике. М.: Мир, 1964.
28. Васильев Ф.П. Методы оптимизации. М.: Факториал пресс, 2002.
29. Гермейер Ю.Б. Введение в теорию исследования операций. М.: Наука, 1971.
30. Корухова Л.С., Шура-Бура М.Р. Введение в алгоритмы. Учебное пособие для студентов I курса, 2-е исправленное издание. — М. Издательский отдел факультета ВМиК МГУ (лицензия ИД № 05899 от 24.09.2001 г.); МАКС Пресс, 2010, http://sp.cmc.msu.ru/info/1/vvedalg.pdf
31. Э. Таненбаум, Т. Остин, Архитектура компьютера. 6-е издание, СПб: Питер, 2013.
32. Операционные системы. У. Столингс. Вильямс. 2002.
33. Э. Таненбаум, Х. Бос Современные операционные системы. 4-е издание, СПб: Питер, 2015.
34. Т. Пратт. М. Зелкович. Языки программирования. Разработка и реализация 4-е издание, СПб: Питер, 2002.
35. В. Ш. Кауфман. Языки программирования. Концепции и принципы. - М.: ДМК-Пресс, 2010.
36. К. Дейт. Введение в системы баз данных. М: Вильямс, 2006.
37. В.В.Воеводин, Вл.В.Воеводин "Параллельные вычисления", БХВ-Петербург, 2002, 608с.
38. А.С. Антонов Технологии параллельного программирования MPI и OpenMP: Учеб пособие. Предисл. : В.А. Садовничий - М.: Изд-во Моск. ун-та, 2012. – 344 с. - (Серия "Суперкомпьютерное образование").

2. Дополнительная часть.

a. Теорема о полноте для P_2. ([1]:30-41). Теорема Кузнецова. Алгоритм распознавания полноты в P_k. ([1]:48-56)

b. Теорема Слупецкого. ([1]:56 64) Особенности k-значных логик. ([1]:65-72)

c. Упрощение дизъюнктивных нормальных форм. ([1]:297-336)

d. Асимптотически оптимальные методы синтеза схем. Методы получения нижних оценок. ([1]:336-366)

e. Логика 1-го порядка. Выполнимость и общезначимость. Общая схема метода резолюций. ([19]:35-100)

f. Автоматы и машины Тьюринга. Классы рекурсивных функций. Эквивалентность понятий частично рекурсивная функция и функция, вычислимая по Тьюрингу. ([1]:113-121, 129-170).

g. Классы P и NP. NP-полные задачи. Теорема Кука. NP-полные задачи на графах. ([2]:46-64). NP-полнота задачи о хроматическом числе графа. ([9]: 95, 99)

h. Вероятностная машина Тьюринга. Классы RP и BPP. Класс P/Po1y. ([3]; [7]: 12-19) Сильные и слабые односторонние функции. ([5]: 30-32; [7]: 31-35, 43-48)

i. Трудные предикаты. ([7]: 64-70) Псевдослучайные генераторы. ([5]: 32-34; [7]: 112-113, 120- 121,123-124)

j. Основные понятия теории групп. ([12]:11-27) Свойства конечных абелевых групп. ([12]: 160- 166) Основные свойства конечных полей. ([12]: 37-42)

k. Минимальные многочлены и их свойства, расширение полей. ([12]: 113-124) Рекуррентные последовательности над конечными полями и регистры сдвига максимального периода. ([12]: 126-134)

l. Спектральные характеристики булевых функций и их основные свойства. Основные криптографические свойства булевых функций: максимальная нелинейность, корреляционная иммунность и устойчивость, совершенная уравновешенность, алгебраическая иммунность. ([4]:74-78. 80-81, 235-238, 272-278, 419-425. [11]: 90-94)

m. Основные понятия теории кодирования. Коды Рида-Маллера. Декодирование кода Рида-Маллера порядка 1. Алгоритм декодирования Рида кодов Рида-Маллера высших порядков. ([4]:158-161, 173-175, 200-203, 210-213, 215-218)

n. Псевдослучайные функции и псевдослучайные перестановки. ([7]: 148-156) IND-CPA стойкая криптосистема с секретным ключом. ([7]: 408-411)

o. Системы блокового шифрования DES, ГОСТ 28147-89 и AES. Режимы ECB, CFB, CBC, OFB работы систем блокового шифрования, выработка имитовставки. ([8]:224-233, 250-256; [13]:1-16; [14]: 1-24)

p. Понятие криптосистемы с открытым ключом. ([7]:413-415) Описание и доказательство корректности криптосистем RSA, Рабина, Эль-Гамаля, МакЭлиса. ([8]: 283-287, 292-299) Задача выработки сессионного ключа. ([8]: 489-496) Описание и доказательство корректности протокола Диффи-Хеллмана. ([8]: 515-517)

q. Криптографические хэш-функции и их приложения ([15]: 15-39). Основные методы криптоанализа хэш-функций, парадокс задачи о днях рождения ([15]: 40-52; [16]: 328-333).

r. Построение итерационных хэш-функций на основе блоковых шифров, криптоанализ общей схемы ([15]: 100-106). Российский стандарт функции хэширования ГОСТ Р 34,11-94 ([17]). Американский стандарт функции хэширования SHA-2 ([18]).

s. Протоколы идентификации и аутентификации. Схемы аутентификации на постоянных паролях. Схема Лэмпорта использования одноразовых паролей. Схемы аутентификации на основе симметричных криптосистем и криптосистем с открытым ключом. ([8]: 385-405)

t. Интерактивные доказательства и доказательства с нулевым разглашением. ([5]: 35-40; [7]: 184-194, 200-203,223-230)

u. Схемы электронно-цифровой подписи. Схема электронно-цифровой подписи RSA: описание и доказательство корректности. ([8]: 425-434) Схемы разделения секрета. ([5]: 72-75) Электронная монета, неотслеживаемость. ([7]: 60-67)

v. Определение политики безопасности. Дискреционная политика. Политика MLS. Математические методы анализа политики безопасности. Модель «take-grant», модель Белла-Лападула, модель LWM, модель невлияния и автоматный подход. ([10]: 75-86, 115- 132)

Литература:

i. Яблонский С.В. Введение в дискретную математику. М.: Наука, 1986.

ii. Алексеев В.Б. Введение в теорию сложности алгоритмов. Изд. отдел ф-та ВМиК МГУ, 2002.

iii. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир. 1982.

iv. Логачев О.А, Сальников *А*.А, Ященко В.В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

v. Ященко В.В. (ред.). Введение в криптографию (2-е изд.). М:. МЦНМО, 2000.

vi. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.

vii. Oded Goldreich. Foundations of Cryptography. Cambridge University Press, 2001.

viii. Menezes A.J., van Oorschot P C., Vanstone S.A. Handbook of Apllied Cryptography. CRC Press, 1997.

ix. Richard M. Karp. Reducibility Among Combinatorial Problems. In: R.E. Miller and J.W. Thatcher (eds), Complexity of Computer Computations, Plenum Press, New York, 85-103. 1972.

x. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. Изд. центр «Академия», 2009.

xi. Логачев О.А. Криптографические свойства булевых функций. М: «МАКС-пресс», 2007.

xii. Применко Э.А. Алгебраические основы криптографии. М: «МАКС-пресс», 2007.

xiii. ГОСТ 28147-89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

xiv. FIPS 197. Specification for the Advanced Encryption Standard.

xv. Preneel B. Analysis and Design of Cryptographic Hash Functions, PhD Thesis, 1993, http://www.esat.kuleuven.ac.be/~pretieel/phd_preneel_febl993.pdf

xvi. Столлингс В. Криптография и защита сетей. Принципы и практика. Москва, Санкт- Петербург, Киев: Издательский дом «Вильяме», 2-е издание, 2001.

xvii. ГОСТ Р 34.11-94 Криптографическая защита информации. Функция хэширования. М.: Госстандарт России, 1994, http://protect.gost.ru/document.aspx?control=7&id=l 34550

xviii. FIPS 180-3. Secure Hash Standard (SHS), October 2008.

xix. Чень Ч., Ли Р. Математическая логика и автоматическое доказательство теорем. М.: Мир. 1983.