МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова
Математический факультет

УТВЕРЖДАЮ
Декан факультета
_____
"_____"_____2012г.

Программа вступительного экзамена в аспирантуру
по специальности научных работников
05.13.19 Методы и системы защиты информации, информационная безопасность

Ярославль 2012

Программа вступительного экзамена
В аспирантуру по специальности
"05.13.19 – Методы и системы защиты информации, информационная 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) и их применение.
4. Формула Тейлора для действительных функций одного и многих действительных переменных и ее применение. Экстремум действительной функции одного и многих действительных переменных достаточные условия его существования.
5. Числовые ряды. Сходящиеся ряды и их простейшие свойства. Признаки сходимости рядов с положительными членами (признаки сравнения, Даламбера, Коши). Абсолютно и не абсолютно сходящиеся ряды. Признак Лейбница. Переместительное свойство абсолютно сходящихся рядов.
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 и условие разложимости функции в ряд Тейлора.
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.

Раздел 2. ТЕОРИЯ ФУНКЦИЙ КОМПЛЕКСНОГО ПЕРЕМЕННОГО

10. Предел и непрерывность комплекснозначной функции комплексного переменного. Дифференцируемость функции комплексного переменного. Условия Коши-Римана.
11. Ряды комплекснозначных функций комплексного переменного. Равномерно сходящиеся ряды. Признак равномерной сходимости Вейерштрасса. Степенные ряды. Первая теорема Абеля. Радиус сходимости. Равномерная

сходимость ряда. Непрерывность суммы ряда. Ряд Лорана и его область сходимости.

12. Интеграл от функции комплексного переменного. Теорема Коши. Интегральная формула Коши. Теорема о существовании производных любого порядка. Интеграл типа Коши.

13. Разложение функции комплексного переменного в ряды Лорана и Тейлора. Теорема единственности. Классификация изолированных особых точек функций и поведение функции в окрестностях особой точки.

14. Вычеты. Основная теорема о вычетах.

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.

Раздел 4. ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА

21. Вероятностное пространство. Аксиомы теории вероятностей. Свойства вероятностной меры. Дискретное вероятностное пространство. Классическое определение вероятностей.

22. Случайные величины. Функции распределения и их свойства. Абсолютно непрерывные, дискретные распределения. Типовые распределения: биномиальное, равномерное, геометрическое, пуассоновское, нормальное, показательное, распределение Стьюдента, χ-распределение, г-распределение, распределение Коши. Схема Бернулли. Полиномиальная схема.

23. Условные вероятности. Независимость событий. Формула полной вероятности. Формула Бейеса. Независимые случайные величины.

24. Математическое ожидание случайной величины и его свойства. Примеры. Математическое ожидание функции случайной величины. Дисперсия случайной величины и ее свойства. Вычисление математических ожиданий и дисперсий для типовых распределений. Математическое ожидание произведения независимых случайных величин. Неравенство Чебышева. Коэффициент корреляции и его свойства.

25. Определение и свойства характеристической функции. Характеристическая функция суммы независимых случайных величин. Вычисление характеристических функций для типовых распределений. Связь дифференцируемости характеристической функции с наличием моментов распределений. Формула обращения и теорема единственности. Теорема непрерывности для характеристических функций. Примеры и приложения.

26. Виды сходимости последовательности случайных величин. Закон больших чисел. Теорема Чебышева. Теорема Хинчина. Теорема Линдеберга (без доказательства). Теорема Ляпунова. Интегральная предельная теорема Муавра-Лапласа.

27. Основные понятия математической статистики: понятия выборки, вариационного ряда, эмпирической функции распределения, выборочных моментов. Примеры использования этих понятий в практических задачах. Теорема Фишера. Несмещенные оценки, состоятельные оценки. Неравенство Рао-Крамера. Условия обращения его в равенство. Эффективные оценки.

28. Основные методы статистического оценивания. Метод моментов. Метод максимального правдоподобия. Применение к случаю нормального и биномиального распределения.

29. Проверка статистических гипотез. Простые и сложные гипотезы. Статистические критерии. Ошибки 1-го II-го родов. Функция мощности. Наиболее мощный и равномерно наиболее мощный критерии. Лемма Неймана-Пирсона. Примеры применения леммы к случаю нормального, биномиального и полиномиального распределений.

30. Критерий согласия. Теорема Пирсона о предельном распределении статистики. Критерий Стьюдента. Примеры.

Раздел 5. АЛГЕБРА

31. Матрицы и операции над ними. Определители матриц и их свойства. Теорема Лапласа. Определитель произведения матриц. Критерий обратимости матриц.

32. Ранг матрицы над полем, способы его вычисления. Ранг произведения матриц. Обратная матрица и способы ее вычисления.

33. Системы линейных уравнений над полем. Критерий Кронекера-Капелли. Алгоритм Гаусса. Фундаментальная система решений однородной системы линейных уравнений. Общее решение системы линейных уравнений.

34. Кольца вычетов. Малая теорема Ферма. Сравнения первой степени. Китайская теорема об остатках.

35. Кольцо многочленов над кольцом с единицей. Делимость многочленов с остатком. Теорема Безу.

36. Делимость многочленов над полем. Наибольший общий делитель (НОД) и наименьшее общее кратное многочленов. Взаимно простые многочлены и их свойства. Неприводимые многочлены и их свойства. Каноническое разложение многочлена и его однозначность.

37. Группы и их основные свойства. Смежные классы по подгруппе, теорема Лагранжа. Циклические группы. Конечные абелевы группы.

38. Подстановки конечных множеств, их четность. Разложение подстановок в произведение независимых циклов. Порождение симметрической группы транспозициями.

39. Нормальные делители группы. Факторгруппа, теорема об эпиморфизме.

40. 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.

41. Линейное преобразование векторного пространства, его матрица в данном базисе, примеры. Критерии обратимости преобразования.

42. Характеристический многочлен линейного преобразования. Собственные значения и собственные векторы преобразования, инвариантные подпространства. Критерий приводимости и разложимости матрицы преобразования.

43. Матрицы над кольцом многочленов над полем, их эквивалентность. Инвариантные делители и множители. Критерий эквивалентности. Критерий подобия матриц над полем. Жорданова нормальная форма матрицы линейного преобразования.

44. Евклидово (унитарное) пространство и его свойства. Существование ортонормированного базиса. Ортогональное дополнение подпространства.

45. Билинейные и квадратичные формы. Квадратичная форма над полем, ее матрица и ранг. Эквивалентность квадратичных форм, канонический вид. Квадратичные формы над полями действительных и комплексных чисел. Положительно определенные квадратичные формы, критерий Сильвестра.

46. Конечные поля, характеристика поля, число элементов, теорема о примитивном элементе. Существование поля с заданным примарным числом элементов. Описание подполей.

47. Неприводимые многочлены над конечными полями. Существование неприводимых многочленов данной степени над конечным полем. Построение конечного поля с заданным числом элементов.

Раздел 6. МАТЕМАТИЧЕСКМАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

48. Булевы функции. Представление булевых функций формулами алгебры высказываний и многочленами Жегалкина. Дизъюнктивные и конъюнктивные нормальные формы.

49. Замкнутые классы функций. Критерии полноты для булевых функций.

50. Исчисления высказываний и предикатов, их полнота и непротиворечивость.

51. Основные подходы к формализации понятия алгоритма: машины Тьюринга, рекурсивные функции, нормальные алгоритмы Маркова.

52. Примеры алгоритмически неразрешимых задач.

53. Понятие сложности алгоритма. Классы сложности.

54. Оценка сложности алгоритмов Гаусса (решения систем линейных уравнений), Штрассена (умножения матриц), Евклида (вычисление НОД).

55. Дискретное преобразование Фурье и его связь с задачами вычисления значений и интерполяции многочленов. Алгоритм быстрого преобразования Фурье (БПФ).

Раздел 7. ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЯ

56. Энтропия вероятностной схемы и ее свойства. Аксиомы Хинчина и Фаддеева. Условная энтропия. Взаимная информация и ее свойства. Количество информации.

57. Источники информации. Энтропия и избыточность источников. Дискретный источник без памяти. Теоремы Шеннона об источниках. Марковские и эргодические источники. Информационная дивергенция. Граница Симмонса.

58. Математическая модель канала связи. Пропускная способность канала связи.

59. Оптимальное кодирование. Префиксные коды. Неравенство Крафта. Корректирующие свойства кодов.

60. Линейный код и способы его задания. Процесс декодирования линейного кода. Код Хемминга.

61. Корректирующие свойства кодов. Циклические коды. БЧХ-коды. Сверточные коды.

Раздел 8. МЕТОДЫ ПРОГРАММИРОВАНИЯ

62. Алгоритмы на графах. Обход графа в глубину, построение глубинного остовного леса и классификация ребер не вошедших в лес. Алгоритмы нахождения компонент связности, двусвязных компонент неориентированных графов и сильно связных компонент ориентированных графов.

63. Деревья. Алгоритмы построения остовных деревьев минимальной стоимости (алгоритм Крускала). Поиск в ширину и кратчайшие пути в графе. Алгоритм нахождения кратчайших путей от выделенной вершины до всех остальных вершин графа (алгоритм Дейкстры). Оценки сложности.

64. Эйлеровы циклы и эйлеровы графы. Критерий существования эйлеровых путей и циклов в неориентированных и ориентированных графах. Алгоритм Флери построения эйлерова цикла. Гамильтоновы циклы и гамильтоновы графы. Теорема Поша (без доказательства), о достаточных условиях существования гамильтонова цикла.

65. Цикломатическое число графа. Базис циклов графа. Связь между числом элементов любого базиса циклов графа и его цикломатическим числом. Алгоритм построения базиса циклов произвольного графа.

66. Структуры данных для задач, касающихся работы с непересекающимися множествами. Операции с непересекающимися множествами (объединить и найти). Реализация множеств с помощью списков и деревьев. Оценки трудоемкости.

67. Алгоритмы внутренней сортировки. Сортировки сравнениями: сортировка вставками в дерево, пирамидальная сортировка, быстрая сортировка. Лексикографическая сортировка как пример распределяющей сортировки. Оценки трудоемкости.

68. Алгоритмы поиска в последовательно организованных файлах. Бинарный, фибоначчиев, интерполяционный поиск. Поиск в файлах, упорядоченных по вероятности. Самоорганизующиеся файлы. Оценки трудоемкости.

69. Алгоритмы поиска в деревьях. Деревья двоичного поиска, сбалансированные по высоте. Оценка максимальной и средней высоты сбалансированного дерева с n узлами. Алгоритм вставки и удаления элемента в дерево двоичного поиска, сбалансированное по высоте. Красно-черные деревья.

70. Деревья оптимального поиска (построение). Сильно ветвящиеся деревья. B-деревья.

71. Поиск подстроки в строке – линейный, Кнута-Морисса-Пратта, Бойера-Мура. Оценка трудоемкости. Поиск в файлах.

Раздел 9. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

72. 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.

73. Угрозы безопасности информации. Угрозы конфиденциальности, целостности, доступности, раскрытия параметров АС. Понятие политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности.

74. Модель системы безопасности *HRU*. Основные положения модели. Теорема об алгоритмической неразрешимости проблемы безопасности в произвольной системе.

75. 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.

76. Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели. Базовая теорема безопасности (*BST*).

77. Основные положения критериев *TCSEC* («Оранжевая книга»). Фундаментальные требования компьютерной безопасности. Требования классов защиты.

78. Основные положения Руководящих документов Гостехкомиссии в области защиты информации. Определение и классификация НСД. Определение и классификация нарушителя. Классы защищенности АС от НСД к информации.

79. Основные положения *CCITSE* («Единые критерии»). Структура профиля и проекта защиты. Структура и ранжирование функциональных требований. Структура требований адекватности и уровни адекватности.

Раздел 10. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

80. Основные положения теории секретности Шеннона. Расстояние единственности.

81. Протоколы шифрования с открытым ключом *RSA*, Эль-Гамаля, на основе задачи о рюкзаке. Понятие сертификата.

82. Выбор параметров системы шифрования *RSA*.

83. Криптографические ключевые хэш-функции и предъявляемые к ним требования. Коды аутентификации и их свойства.

84. Криптографические бесключевые хэш-функции и предъявляемые к ним требования. Стандарты.

85. Цифровая подпись. Схемы цифровой подписи RSA и Эль-Гамаля. Стандарты цифровой подписи.

86. Схема предварительного распределения ключей Блома и ее безусловная стойкость.

87. Криптографические протоколы выработки ключей. Протокол Диффи–Хеллмана и его модификации.

88. Протоколы идентификации Шнорра и Окамото. Их полнота и корректность.

89. Совершенная схема разделения секрета Шамира.

Раздел 11. ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

90. Структура и состав системы нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.

91. Правовой режим защиты государственной тайны.

92. Правовой режим защиты конфиденциальной информации.

93. Структура системы обеспечения информационной безопасности.

94. Правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.).

95. Организация и обеспечение режима секретности.

96. Лицензирование и сертификация в области защиты информации

Раздел 12. ЯЗЫКИ ПРОГРАММИРОВАНИЯ

97. Жизненный цикл программ. Оптимизация программ. Алгоритмическая, машинно-зависимая, машинно-независимая оптимизация. Виды оптимизаций, выполняемые компиляторами. Профилирование программ. Оптимизация в современных процессорах. Влияние оптимизации на переносимость. Способы написания переносимых программ. Тестирование программ. Функциональное и структурное тестирование.

98. Методологии программирования. Структурное программирование. Модульное программирование. Объектно-ориентированное программирование (ООП). Концепции ООП – инкапсуляция, наследование, полиморфизм, абстрагирование. Абстрактные типы данных. Классы, объекты и методы. Распределение динамической памяти и обработка ошибок в современных ООП-языках.

Раздел 13. ОПЕРАЦИОННЫЕ СИСТЕМЫ И ИХ ЗАЩИТА

99. Процессы и потоки. Межпроцессное взаимодействие. Распределение времени процессора.

100. Управление памятью. Сегментация и страничная организация памяти. Виртуальная память. Адресное пространство задачи. Ресурсы. Совместное использование ресурсов.

101. Защита в операционной системе. Проблемы внедрения политики безопасности. Требования к подсистеме взаимодействия с ресурсами для корректного внедрения абстрактной модели безопасности.

102. Состав и правила взаимодействия компонент в подсистеме обеспечения безопасности.

103. Современные типы операционных систем. Преимущества и недостатки различных подходов к построению ОС.

104. Типовая структура подсистемы безопасности ОС и выполняемые ей функции. Идентификация и аутентификация, разграничение доступа, аудит, подотчетность действий, повторное использование объектов. Точность и надежность обслуживания. Защита обмена данных. Реализация подсистем безопасности. Средства обеспечения безопасности ОС семейств UNIX, Windows и Linux. Домены безопасности. Критерии защищенности ОС.

Раздел 14. ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ И ИХ ЗАЩИТА

105. Эталонная модель взаимодействия открытых систем. Основные службы и протоколы вычислительных сетей.

106. Общие вопросы построения сетей. Проблемы распределенной обработки данных; классификация сетей по различным признакам. Сравнительная характеристика сетей различных типов. Основы организации и функционирования сетей Основные сетевые стандарты и стандартизирующие организации. Топологии сетей; иерархические модели сетей.

107. Функционирование локальных сетей. Способы передачи информации. Уровни и методы кодирования информации. Методы получения доступа к среде; сравнение эффективности различных методов получения доступа к среде. Сети Ethernet (10/100/1000 Mbps), Token Ring, FDDI, ATM; беспроводные сети WiFi и Bluetooth.

108. Функционирование глобальных сетей. Проблемы связывания узлов глобальной гетерогенной сети. Стек протоколов TCP/IP, включая протоколы: IP, ARP, ICMP, IGMP, RIP, TCP, UDP, SNMP, SMTP, POP3, IMAP, HTTP, FTP. Протоколы и алгоритмы функционирования файлообменных сетей и сетей моментального обмена сообщениями.

109. Безопасность вычислительных сетей. Проблемы безопасности при взаимодействии в сети. Методы и протоколы аутентификации пользователей и узлов сети.

110. Достоинства и недостатки основных технологий межсетевых экранов.

111. Сравнительный анализ сетевых и хостовых систем обнаружения вторжений.

112. Протоколы и алгоритмы построения виртуальных сетей. Защитные функции туннельного и транспортного режимов при построении VPN.

Раздел 15. ЗАЩИТА В СУБД

113. Средства обеспечения защиты информации в СУБД. Средства идентификации и аутентификации объектов баз данных, управление доступом. Средства контроля целостности информации. Организация аудита. Типы контроля безопасности: потоковый, контроль вывода, контроль доступа. Многоуровневая защита.

114. Модели безопасности, применяемые при построении защиты в СУБД. Использование транзакции для изолирования действий пользователей. Блокировки; ссылочная целостность; триггерная и событийная реализация правил безопасности.

115. Причины, виды, основные методы нарушения конфиденциальности в СУБД. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов.

Раздел 16. ДИСЦИПЛИНЫ СПЕЦИАЛИЗАЦИИ

Криптографические протоколы

1. Примитивные протоколы (подбрасывания монеты и закрытия бита).
2. Схема идентификации Гиллу-Кискате.
3. Схема слепой подписи.
4. Протоколы с нулевым разглашением.
5. Схемы разделения секрета.
6. Рюкзачная криптосистема Меркля-Хеллмана.

Теоретико-числовые методы в криптографии

1. Расширенный алгоритм Евклида.
2. Дихотомический алгоритм возведения в степень.
3. Алгоритмы проверки чисел на простоту.
4. Построение больших простых чисел.
5. Алгоритмы факторизации целых чисел.

Алгебраическая алгоритмика

1.Факториальность кольца многочленов над полем.
2. Примитивные элементы в конечных полях.
3. Линейные рекуррентные последовательности максимального периода.
4. Китайская теорема об остатках для чисел и многочленов. Модульная арифметика.

Теория кодирования

1. Квадратично-вычетные коды.
2. Коды Рида-Миллера.
3. Циклические коды, исправляющие две ошибки.
4. Декодер Питерсона-Горенстейна.

Общая алгебра

1. Евклидовы и факториальные кольца.
2. Модули, подмодули и фактормодули. Гомоморфизмы модулей.
3. Нетеровы модули и кольца. Теорема Д. Гильберта о базисе.

Теория автоматов

1. Детерминированные и недетерминированные конечные автоматы и автоматные языки.
2. Регулярные выражения и регулярные языки. Теорема С. Клини.
3. Алгоритмические проблемы для регулярных языков.

Теория чисел

1. Кольца вычетов. Малая теорема Ферма и теорема Эйлера. Сравнения первой степени. Китайская теорема об остатках.
2. Квадратичные вычеты. Символы Лежандра и Якоби, их свойства. Квадратичный закон взаимности.
3. Непрерывные дроби и их свойства. Диофантовы уравнения. Уравнение Пелля.
4. Теорема Евклида о бесконечности множества простых чисел. Распределение простых чисел, теорема Чебышева. Оценка величины *n*-го простого числа.

Заведующий кафедрой компьютерной безопасности
И математических методов обработки информации, профессор

В.Г. Дурнев