Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Московский государственный университет имени М.В.Ломоносова»
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

УТВЕРЖДАЮ

Декан
механико-математического факультета,

/А.И. Шафаревич/

21 января 2026 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ В АСПИРАНТУРУ

Укрупненная группа научных специальностей:

2.3.Информационные технологии и телекоммуникации

Перечень образовательных программ, на который осуществляется прием по данной программе:
(программы по специальностям 2.3.5 и 2.3.6)

Москва 2026

- **Краткое описание программы.**

Программа вступительного испытания разработана в соответствии с требованиями действующих федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) для уровней специалитета 01.05.01 «Фундаментальная математика и механика», магистратуры 01.04.01 «Математика», 01.04.02 «Прикладная математика и информатика», 01.04.03 «Механика и математическое моделирование», 01.04.04. «Прикладная математика» и 02.04.01 «Математика и компьютерные науки».

Программа вступительного испытания разработана для проведения конкурсного отбора абитуриентов, планирующих обучение по следующим программам высшего образования – программам подготовки научных и научно-педагогических кадров в аспирантуре (далее аспирантура) (программы по специальностям 2.3.5 и 2.3.6).

Вступительное испытание в аспирантуру включает в себя три последовательных этапа. Проведение этапов может быть организовано как в течение одного дня, так и распределено на несколько дней — соответствии с утверждённым расписанием.

Срок проведения вступительного испытания определяется правилами приема в аспирантуру.

В программе описаны формы проведения каждого этапа, их содержательное наполнение, список рекомендуемой литературы, а также методика оценивания результатов.

Для допуска к последующему этапу необходимо успешно пройти предыдущий: абитуриент не может приступить ко второму или третьему этапу, не преодолев порог успешности на предшествующем.

- **Критерии успешности прохождения этапов и вступительного испытания в целом.**

За вступительное испытание в сумме может быть набрано 25 баллов из них:

за первый этап 10 баллов;

за второй этап 10 баллов

за третий этап 5 баллов.

Прохождение вступительного испытания считается успешным если абитуриент набрал в сумме не менее 16 баллов.

Прохождение этапа считается успешным. Если абитуриент набрал не менее:

7 баллов на первом этапе

6 баллов на втором этапе

3 баллов на третьем этапе.

Для абитуриентов, участвовавших в конкурсе научного портфолио в году, соответствующем году поступления, действует следующее правило: победитель конкурса получает максимальный балл за всё вступительное испытание (все три этапа); призёр конкурса проходит все этапы вступительного испытания на общих основаниях, но получает дополнительные 3 балла, которые добавляются к общему результату вступительного испытания.

- **Место проведения вступительного испытания:** Москва, улица Ленинские горы д.1.
- **Форма проведения и содержание этапов вступительного испытания.**

Этап I. Оценка уровня знаний в области фундаментальной и прикладной математики и механики, компьютерных наук и информационной безопасности

Форма проведения этапа: очно в виде ответа на вопросы **из программы государственного экзамена**

Содержание этапа: первый этап состоит в проверке знаний по ключевым областям фундаментальной математики и математической физики. Перечень тем по программе «Фундаментальная математика», «Математика и компьютерные науки», «Математическая физика». *Приложение 1.*

Этап II. Оценка уровня знаний в научной области

Форма проведения этапа: очно в виде ответа на вопрос **по научной специальности**

Содержание этапа: второй этап состоит в проверке знаний в области научных интересов *Приложение 2.*

Основные источники (если применимо) не требуются

Фонд оценочных средств: Оценка от степени осознания и осмысления этой деятельности (осознанная, с четким представлением целей и смыла / отчасти осознанная, но с пониманием целей / слабо осознанная, стереотипная / неосознанная, по наитию / отсутствие каких-либо представлений) и от степени рефлексии (рефлексия деятельности в целом / рефлексия только своей деятельности /рефлексия отдельных действий / рефлексия только отдельных событий /отсутствие рефлексии)

Этап III. Оценка реферата на иностранном языке по научной специальности

Форма проведения этапа: очно в виде собеседования об интересующих абитуриента задачах по научной специальности, о постановке задачи, способах её решения и полученных результатах.

Содержание этапа: экспертная оценка наличия понимания смысла научно-исследовательской деятельности. Осуществляется посредством диалога с ответом на вопросы на иностранном языке, какие проблемы абитуриент видит при решении поставленной задачи и о его научных результатах.

Реферат по избранному направлению подготовки представляет собой обзор литературы по теме будущего научного исследования и позволяет понять основные задачи и перспективы развития темы будущей диссертационной работы. Реферат включает титульный лист, содержательную часть, выводы и список литературных источников. Объем реферата 10-15 страниц машинописного текста. В отзыве к реферату предполагаемый научный руководитель дает характеристику работы.

Основные источники (если применимо) не требуются

Фонд оценочных средств: оценка осуществляется в зависимости от степени понимания задаваемых вопросов и ясности и четкости ответа на них на иностранном языке.

Приложение 1
К программе вступительного испытания
механико-математического факультета
Утвержденного приказом

№1/101-ОСН от 21января 2026 г.

ОБЩИЕ ВОПРОСЫ ФУНДАМЕНТАЛЬНОЙ МАТЕМАТИКИ

1. Непрерывность функций одной переменной, свойства непрерывных функций.
2. Функции многих переменных, полный дифференциал и его геометрический смысл. Достаточные условия дифференцируемости. Градиент.
3. Определенный интеграл. Интегрируемость непрерывной функции. Первообразная непрерывной функции.
4. Неявные функции. Существование, непрерывность и дифференцируемость неявных функций.
5. Числовые ряды. Сходимость рядов. Критерий сходимости Коши. Достаточные признаки сходимости.
6. Абсолютная и условная сходимость ряда. Свойство абсолютно сходящихся рядов. Умножение рядов.
7. Ряды функций. Равномерная сходимость. Признак Вейерштрасса. Свойства равномерно сходящихся рядов (непрерывность суммы, почленное интегрирование и дифференцирование).
8. Степенные ряды в действительной и комплексной области. Радиус сходимости, свойства степенных рядов (почленное интегрирование, дифференцирование). Разложение элементарных функций.
9. Несобственные интегралы и их сходимость. Равномерная сходимость интегралов, зависящих от параметра. Свойства равномерно сходящихся интегралов.
10. Ряды Фурье. Достаточные условия представимости функции рядом Фурье.
11. Теоремы Остроградского и Стокса. Дивергенция. Вихрь.
12. Линейные пространства, их подпространства. Базис. Размерность. Теорема о ранге матрицы. Система линейных уравнений. Геометрическая интерпретация системы линейных уравнений. Фундаментальная система решений системы однородных линейных уравнений. Теорема Кронекера - Капелли.
13. Билинейные и квадратичные функции и формы в линейных пространствах и их матрицы. Приведение к нормальному виду. Закон инерции.
14. Линейные преобразования линейного пространства, их задание матрицами. Характеристический многочлен линейного преобразования. Собственные векторы и собственные значения, связь последних с характеристическими корнями.
15. Евклидово пространство. Ортонормированные базисы. Ортогональные матрицы. Симметрические преобразования. Приведение квадратичной формы к главным осям.
16. Группы, подгруппы, теорема Лагранжа. Порядок элемента. Циклические группы, факторгруппа. Теорема о гомоморфизмах.
17. Аффинная и метрическая классификация кривых и поверхностей второго порядка. Проективная классификация кривых.
18. Дифференциальное уравнение первого порядка. Теорема о существовании и единственности решения.
19. Линейное дифференциальное уравнение второго порядка. Линейное однородное уравнение. Линейная зависимость функций. Фундаментальная система решений. Определитель Вронского. Линейное неоднородное уравнение.

20. Линейное дифференциальное уравнение с постоянными коэффициентами: однородное и неоднородное.
21. Функции комплексного переменного. Условия Коши - Римана. Геометрический смысл аргумента и модуля производной.
22. Элементарные функции комплексного переменного и даваемые ими конформные отображения. Простейшие многозначные функции. Дробно-линейные преобразования.
23. Теорема Коши об интеграле по замкнутому контуру. Интеграл Коши. Ряд Тейлора.
24. Ряд Лорана. Полюс и существенно особая точка. Вычеты.
25. Криволинейные координаты на поверхности. Первая квадратичная форма поверхности.
26. Вторая квадратичная форма поверхности. Нормальная кривизна линии на поверхности. Теорема Менье.
27. Главные направления и главные кривизны. Формула Эйлера.

Рекомендуемая литература для подготовки:

1. Кострикин А.И. Введение в алгебру.
2. Зорич В.А. Математический анализ, тт. 1, 2.
3. Филиппов А.Ф. Введение в теорию дифференциальных уравнений.
4. Лаврентьев М.А., Шабат Б.В. Методы теории функций комплексного переменного.
5. Тихонов А.Н., Самарский В.А. Уравнения математической физики.
6. Маркеев А.П. Теоретическая механика.
7. Голубев Ю.В. Основы теоретической механики.
8. Александров В.В., Болтянский В.Г., Лемак С.С., Парусников Н.А., Тихомиров В.М. Оптимальное управление движением.
9. Седов Л.И. Механика сплошной среды, тт. 1, 2.
10. Ильюшин А.А. Механика сплошной среды.
11. Кочин Н.Е., Кибель И.А., Розе Н.В. Теоретическая гидромеханика, тт.1, 2.
12. Черный Г.Г. Газовая динамика.
13. Победря Б.Е., Георгиевский Д.В. Основы механики сплошной среды.
14. Галин Г.Я., Голубятников А.Н., Каменярж Я.А., Карликов В.П., Куликовский А.Г., Петров А.Г., Свешникова Е.И., Шикина И.С., Эглит М.Э. Механика сплошных сред в задачах, тт. 1, 2.
15. Новацкий В. Теория упругости.
16. Моисеев Н.Д. Очерки развития механики.17. Крутецкий, В.А. Психология математических способностей школьников. - М.: Институт практической психологии; Воронеж, НПО МОДЕК, 1998.

Приложение 2
К программе вступительного испытания
механико-математического факультета
Утвержденного приказом

№1/101-ОСН от 21января 2026 г.

СПЕЦИАЛЬНЫЕ ВОПРОСЫ ПО НАУЧНОЙ СПЕЦИАЛЬНОСТИ

2.3.5. Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

1. Динамические структуры данных: стек, дек, очередь, последовательность, список, дерево, множество. Непрерывные и ссылочные реализации структур данных.
2. Реализации множеств. Хэширование. Совершенные, минимальные хеш-функции. Различные варианты хэш-реализаций множеств. Эффективность процедур поиска, включения и исключения элементов при различных реализациях.
3. Бинарные деревья. Процедуры восходящего, нисходящего, горизонтального обхода бинарного дерева. Деревья поиска. Добавление и удаление элементов в дерево поиска. Сбалансированные бинарные деревья. Алгоритмы балансировки дерева. Теорема о глубине сбалансированного дерева.
4. Красно-черные деревья. Сравнение эффективности поиска со сбалансированным деревом. Процедуры добавления и удаления элементов. Оценки их эффективности. Теорема о глубине красно-черного дерева.
5. B-деревья. Процедуры добавления и удаления элементов. Оценки их эффективности.
6. Контейнеры данных переменного и фиксированного размера. Методы реализации функций динамического выделения памяти.
7. Сортировки обменом, линейной вставкой, выбором, слиянием (Неймана). Сортировка Шелла. Сортировка с помощью дерева (heapsort). Быстрая сортировка. Теоремы об оценке снизу для трудоемкости сортировок. Теоремы о средней трудоемкости быстрой сортировки. Алгоритм сортировки с линейной оценкой трудоемкости.
8. Алгоритмы сжатия данных: RLE, Хаффмена, LZW, арифметического кодирования. Адаптивные алгоритмы. Теоремы об оптимальности кода Хаффмена. Теоремы о сжатии в методе арифметического кодирования.
9. Формальные грамматики. LR(1) разбор для арифметического выражения. Рекурсивный алгоритм построения дерева разбора арифметического выражения. Компилятор модельного языка программирования: проектирование системы команд стекового процессора, реализация операторов перехода в программе, организация вызовов подпрограмм и функций, передача параметров в функции.
10. Операционные системы (ОС). Определения операционных систем реального времени (ОСРВ). Определения основных объектов ОС. Программа, процессор, процесс. Основные составляющие процесса, состояния процесса. Стек, виртуальная память, механизмы трансляции адреса.

11. Ресурсы, приоритеты. Виды ресурсов: аппаратные, программные, активные, пассивные, локальные, разделяемые, постоянные, временные, не критичные, критичные.
12. Параллельные процессы. Многозадачные ОС. Типы взаимодействия процессов: сотрудничающие и конкурирующие процессы, взаимное исключение процессов. Проблемы, возникающие при синхронизации процессов и идеи их разрешения. Связывание. Статическое и динамическое связывание. Особенности реализации для ОСРВ.
13. Определение потока исполнения (thread). Сравнение с процессами: создание, планирование, управление. Состояния процесса, потока исполнения и механизмы перехода из одного состояния в другое.
14. Типы архитектур операционных систем. Монолитная и модульная архитектура. Общее строение ОС. Роли отдельных компонент: планировщика, диспетчера.
15. Механизмы взаимодействия процессов: разделяемая память. Примитивные операции. Особенности реализации для систем с виртуальной памятью. Особенности реализации для ОСРВ.
16. Механизмы взаимодействия процессов: семафоры. Примитивные операции. Особенности реализации для ОСРВ.
17. Механизмы взаимодействия процессов: сигналы, события, критические секции. Примитивные операции. Особенности реализации для ОСРВ.
18. Механизмы взаимодействия процессов: очереди сообщений (почтовые ящики). Примитивные операции. Особенности реализации для ОСРВ.
19. Синхронизация и взаимодействие потоков исполнения. Объекты типа mutex. Примитивные операции. Виды mutex. Особенности реализации для ОСРВ.
20. Синхронизация и взаимодействие потоков исполнения. Объекты типа condvar. Примитивные операции. Виды condvar. Особенности реализации для ОСРВ.
21. Планирование задач в ОС. Цели планирования в ОСРВ. Требования к планировщику задач в ОСРВ, его роль в ОСРВ.
22. Приоритеты. Схемы назначения приоритетов. Инверсия приоритетов и методы борьбы с ней. Стратегии планирования задач. Типичные схемы планирования в UNIX системах и ОСРВ.
23. Контекст задачи. Переключение контекста. Роль и задачи диспетчера. Прерывания. Процессы обработки прерывания и вызова подпрограмм. Время реакции на прерывание.
24. Файловые системы. Принципы организации хранения файлов на диске. Логическая структура диска. Базовые функции файловой системы. Принципы организации древовидной файловой системы. Организация файловых систем FAT, ext, NTFS. Процедуры поиска всех блоков файла, поиска свободного места, создания и удаления файла.
25. Внутренняя организация процессоров. Выделение независимо работающих устройств: IU, FPU, MMU, BU. CISC и RISC процессоры. Повышение производительности процессоров за счет конвейеризации. Условия оптимального функционирования конвейера. Суперконвейерные и суперскалярные процессоры. Методы уменьшения негативного влияния инструкций перехода на производительность процессора. Исполнение инструкций не по порядку.
26. Повышение производительности процессоров за счет введения кэш памяти. Кэши: единый, Гарвардский, с прямой записью, с обратной записью. Организация кэш-памяти. Алгоритмы замены данных в кэш памяти. Специальные кэши. Согласование кэшей в мультипроцессорных системах с общей памятью. Методы уменьшения времени реакции на прерывание.
27. Архитектуры системных шин. Синхронные и асинхронные шины. Мультиплексирование шины. Отображение ресурсов на память и пространство ввода-вывода. Мосты между шинами. Архитектуры шин PCI, VME, CompactPCI.

28. Виды многопроцессорных архитектур. Системы с общей и распределенной памятью. Поддержка многозадачности и многопроцессорности специальными инструкциями процессора. Организация данных во внешней памяти. Механизмы преобразования данных при обменах.
29. Программирование систем с распределенной памятью. Message Passing Interface (MPI). Общая структура MPI-программы. Сообщения и их виды. Группы и коммуникаторы. Попарный обмен сообщениями. Операции ввода-вывода в MPI программах.
30. Коллективный обмен сообщениями. Учет архитектуры параллельной ЭВМ. Ограничение коллективного обмена на подмножество процессов. Время в MPI программах.
31. Пересылка структур данных. Создание нового MPI типа данных. Упаковка/распаковка разнородных данных. Пересылка структур данных в однородных параллельных ЭВМ. Пересылки строк и столбцов матриц.
32. Объектно-ориентированный подход в программировании. Объекты, их информационная структура, отношения между объектами. Инкапсуляция, сокрытие информации. Абстрактные типы данных. Классы и представители. Полиморфизм.
33. Объектно-ориентированный подход в программировании. Наследование. Переопределение информационных и/или поведенческих структур при наследовании. Цели использования наследования. Классический и объектно-ориентированный подходы к построению программ.
34. Понятие о сетях с коммутацией каналов и пакетов. Достоинства и недостатки каждого из подходов. Базовые топологии локальных сетей: линия, кольцо, звезда. Структурные элементы локальных и глобальных сетей. Повторитель, разветвитель, мост, шлюз.
35. Логика функционирования сетей Ethernet. Адресация. Дисциплина передачи данных. Разрешение коллизий.
36. Иерархия сетевых протоколов в модели TCP/IP. IP адресация. Классы адресов. Широковещательные и другие специальные адреса. Маска подсети. Протоколы ARP, RARP, ICMP, назначение, принципы работы.
37. Протокол IP, назначение, принципы работы. Функции IP протокола, фрагментация и сборка. Уничтожение пакетов. Маршрутизация.
38. Протокол UDP, назначение, принципы работы. Адресация транспортного уровня. Протокол TCP, назначение, принципы работы. Обеспечение надежности передачи. Сегментация данных при отправлении и сборка при получении. Процедуры установления и разрыва соединения. Механизм подтверждений. Таймеры.
39. Протокол и система DNS, назначение, принципы работы. Структура доменных имен. Классификация DNS серверов. Формат запроса и ответа. Ресурсная запись. Итеративная, рекурсивная и смешанная процедуры.
40. Протокол FTP, назначение, принципы работы. Вид запроса и отклика. Процесс передачи файлов. Классификация кодов откликов.
41. Протокол HTTP, назначение, принципы работы. Формат запроса и отклика. Структура и назначение строк-заголовков (header-lines). Виды соединений. Отличие HTTP/1.0 и HTTP/1.1. Классификация кодов откликов.
42. Socket-интерфейс. Основные функции и их назначение. Последовательность действий программы-клиента и программы-сервера.

ПРИМЕР ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ:
Вопрос 1. Ряды Фурье. Достаточные условия представимости функции рядом Фурье.
Вопрос 2. Определение потока исполнения (thread). Сравнение с процессами: создание, планирование, управление. Состояния процесса, потока исполнения и механизмы перехода из одного состояния в другое.
Вопрос 3. Содержание реферата по теме диссертационного исследования (с приложением реферата и отзыва на реферат с отметкой предполагаемого научного руководителя).

Рекомендуемая литература для подготовки:

ОСНОВНАЯ:
1. Кострикин А.И. Введение в алгебру, ч. I,II,III Основы алгебры.
2. Курош А.Г. Курс высшей алгебры.
3. Александров П.С. Курс по аналитической геометрии и линейной алгебре.
4. Гельфанд И.И. Лекции по линейной алгебре.
5. Кудрявцев Л.Д. Математический анализ.
6. Фихтенгольц Г.И. Основы математического анализа, тт. 1,2,3.
7. Степанов В.В. Курс дифференциальных уравнений.
8. Арнольд В.И. Обыкновенные дифференциальные уравнения.
9. Привалов Н.Н. Введение в теорию функции комплексных переменных.
10. Шабат Б.В. Введение в комплексный анализ.
11. Гнеденко Б.В. Очерк по истории математики в России и СССР.
12. Рыбников К.А. История математики.

ДОПОЛНИТЕЛЬНАЯ:
1. Валединский В.Д., Пронкин Ю.Н. Вычислительные системы и программирование. Системы хранения данных. М.: ЦПИ МГУ, 2006.
2. Валединский В.Д., Пронкин Ю.Н. Вычислительные системы и программирование. Организация вычислительных систем. М.: ЦПИ МГУ, 2006.
3. Богачев К.Ю. Операционные системы реального времени. М.: ЦПИ МГУ, 2001.
4. Богачев К.Ю. Основы параллельных вычислений. Том 1. М.: ЦПИ МГУ, 2002.
5. Богачев К.Ю. Основы параллельных вычислений. Том 2. М.: ЦПИ МГУ, 2002.

АВТОРЫ

д.ф.-м.н. профессор Г.М. Кобельков
д.ф.-м.н. профессор К.Ю. Богачев
к.ф.-м.н. доцент А.В. Попов
младший научный сотрудник Б.М. Сиротич

2.3.6. Методы и системы защиты информации, информационная безопасность

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Алгебра логики. Функции алгебры логики. Задание функций таблицами истинности и формулами. Операция суперпозиции. Замыкание и замкнутые классы. Теорема Поста о полноте.
2. Теория автоматов. Понятие конечного абстрактного автомата. Отличимость состояний. Теоремы Мура об отличимости состояний. Регулярные и представимые множества. Теорема Клини. Связь сложности регулярных выражений и автоматов. Проблема экспоненциального взрыва. Понятие структурного автомата. Конечные полные системы относительно операции суперпозиции.
3. Схемы из функциональных элементов. Понятие схемы из функциональных элементов. Сложность и глубина схемы. Необходимое и достаточное условие полноты. Асимптотика функции Шеннона сложности и глубины схемы.
4. Теория алгоритмов. Понятие машины Тьюринга. Тезис Тьюринга. Существование универсальной машины Тьюринга. Теорема о структурном программировании. Теорема Райса. Понятие сложности вычисления. Классы сложности P, NP, BPP. Понятия сводимости и полноты. NP-полные задачи. Теорема Кука. Тезис Эдмондса (полиномиальный тезис Тьюринга).

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Законодательные и правовые основы информационной безопасности. Содержание и роль законодательного уровня. Анализ российского законодательства в области информационной безопасности.
2. Основные понятия административного уровня обеспечения информационной безопасности. Политика безопасности. Программа безопасности. Обеспечение информационной безопасности и жизненный цикл информационной системы. Особенности управления рисками информационной безопасности на административном уровне. Понятие об анализе защищенности.
3. Основные понятия процедурного уровня обеспечения безопасности. Меры процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.
4. Основные понятия программно-технического уровня обеспечения безопасности. Состав основных программно-технических мер, методов и средств защиты информации. Понятие об архитектурной безопасности.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

1. Математические основы криптографии. Теория информации. Энтропия по Шеннону. Понятия информации, взаимной информации, условной энтропии.
2. Основные понятия криптографии. Три задачи криптографии: конфиденциальность, целостность, неотслеживаемость (на примерах). Понятие о криптографических системах, криптографических протоколах и криптографических примитивах. Модель противника. Атаки, угрозы, стойкость (на примерах).
3. Теоретическая криптография. Теория Шеннона секретной связи. Модель системы секретной связи. Неоднозначность ключа. Расстояние единственности. Идеальный шифр. Совершенная секретность. Шифр Вернама. Теория Симмонса аутентификации. Модель протокола аутентификации. Имитация и подмена. Безусловная целостность.

4. Элементы криптографических систем и протоколов. Односторонние функции: определение; гипотетические примеры. Криптографические хэш-функции; односторонние семейства хэш-функций; необходимые и достаточные условия существования. Генераторы псевдослучайных последовательностей в криптографии.
5. Криптографические системы. Принципы построения криптосистем с секретным ключом (симметричных криптосистем). Сети Файстеля и подстановочно-перестановочные сети (SP-сети). Криптосистемы с открытым ключом. Семейства функций с секретом. Криптосистема RSA. Криптосистемы на основе эллиптических кривых. Схемы разделения секрета: структуры доступа; доли секрета; пороговые схемы; схема Шамира.
6. Криптографические протоколы. Протоколы генерации ключей на примере протокола Диффи-Хеллмана. Протоколы электронной подписи. Доказательства с нулевым разглашением.
7. Криптографические стандарты. Отечественные и международные стандарты криптографических примитивов и криптографических протоколов.

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Математические модели гарантированно защищенных систем. Примеры. Алгоритмическая разрешимость свойства безопасности. Теоремы раскрутки.
2. Логическое разграничение доступа. Подход к определению безопасности в терминах доступов. Понятие о логическом разграничении доступа. Связь с идентификацией и аутентификацией. Модели логического разграничения доступа: дискреционные модели; мандатные многоуровневые модели; ролевые модели логического разграничения доступа. Анализ информационных потоков. Механизмы логического разграничения доступа в современных операционных системах.
3. Принципы реализации криптографических систем. Реализация симметричных криптосистем. Примеры режимов блочного шифрования. Примеры реализации потоковых криптосистем с секретным ключом. Принципы реализации алгоритма шифрования AES. Реализация криптосистем с открытым ключом. Выбор длины ключа; функции формирования ключей; удлинение ключей. Отечественные криптосистемы.
4. Методы защиты от сетевых атак. Примеры сетевых атак. Подмена сетевых адресов, подмена доменных имен и «отравление» кэша. Атаки на основные сетевые протоколы: IP; TCP; HTTP. Варианты защищенных сетевых протоколов: IPsec; SSL/TLS; HTTPS. Инфраструктура открытых ключей, удостоверяющий центр, сертификат, путь доверия.
5. Протоколирование и аудит. Понятие о протоколировании, аудите, активном аудите. Подходы к организации архитектуры систем активного аудита. Методы мониторинга и обнаружения вторжений. Основные методы анализа регистрационной информации. Сигнатурные методы обнаружения вторжений и аномальной активности. Алгоритмы статистического анализа регистрационной информации.
6. Защита от вредоносного программного обеспечения. Понятие о вредоносном программном обеспечении. Подходы к классификации. Программные закладки. Троянские программы. Вирусы и черви. Методы защиты от вредоносного программного обеспечения. Обеспечение целостности. Изолированные программные среды. Методы антивирусной защиты. Алгоритмическая неразрешимость задачи выявления вируса.
7. Защита информации с точки зрения технологий программирования. Основные классы уязвимостей программных средств: ошибки типа «переполнение буфера» и ошибки управления памятью, ошибки типа «состояние гонки», арифметические переполнения, инъекции интерпретируемого кода. Подходы к предотвращению возникновения уязвимостей. Методы

тестирования и верификации программных средств. Использование автоматических анализаторов исходного кода.

ПРИМЕР ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ:

Вопрос 1. Ряды Фурье. Достаточные условия представимости функции рядом Фурье.
Вопрос 2. Сигнатурные методы обнаружения вторжений и аномальной активности; использование регулярных выражений. Алгоритмы статистического анализа регистрационной информации.
Вопрос 3. Содержание реферата по теме диссертационного исследования (с приложением реферата и отзыва на реферат с отметкой предполагаемого научного руководителя).

Рекомендуемая литература для подготовки:

ОСНОВНАЯ:

1. Кострикин А.И. Введение в алгебру, ч. I, II, III.
2. Кострикин А.И. Введение в алгебру, ч. II. Линейная алгебра.
3. Александров П.С. Курс по аналитической геометрии и линейной алгебре.
4. Гельфанд И.М. Лекции по линейной алгебре.
5. Фихтенгольц Г.И. Основы математического анализа, тт. 1,2,3.
6. Степанов В.В. Курс дифференциальных уравнений.
7. Арнольд В.И. Обыкновенные дифференциальные уравнения.
8. Привалов Н.Н. Введение в теорию функции комплексных переменных.
9. Шабат Б.В. Введение в комплексный анализ.
10. Дубровин Б.А., Новиков С.П., Фоменко А.Т. Современная геометрия.

ДОПОЛНТЕЛЬНАЯ:

1. Яблонский С.В. Введение в дискретную математику. М.: Наука, 1986.
2. Кудрявцев В.Б., Алешин С.В., Подколзин А.С. Введение в теорию автоматов. М.: Наука, 1985.
3. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети. М.: ДМК Пресс, 2004.
4. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. М.: ГЛТ, 2006.
5. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб.: Лань, 2001.
6. Мао В. Современная криптография: теория и практика. М.: Вильямс, 2005.
7. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003.

АВТОРЫ

д.ф.-м.н. профессор В.А. Васенин
д.ф.-м.н. профессор Э.Э. Гасанов
к.ф.-м.н. доцент С.Т. Главацкий
к.ф.-м.н. доцент А.В. Галатенко
к.ф.-м.н. доцент Д.В. Алексеев
к.ф.-м.н. ведущий научный сотрудник С.А. Афонин
к.ф.-м.н. ведущий научный сотрудник. А.С. Шундеев