Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный университет имени М.В. Ломоносова»
механико-математический факультет

«УТВЕРЖДАЮ»
Декан механико-математического факультета,
член- корр. РАН, профессор А.И. Шафаревич
_____
«27» мая 2022 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА

(для осуществления приема на обучение по образовательным программам высшего образования — программам подготовки научных и научно-педагогических кадров в аспирантуре)

2. Технические науки

2.3. Информационные технологии и телекоммуникации

2.3.6. Методы и системы защиты информации, информационная безопасность

(физико-математические науки)

Программа утверждена
Приказом по факультету
№ _ от _____ 2022 г.
/
Ученым советом факультета
(протокол № _ от _____ 2022 г.)

Москва - 2022

I. ОПИСАНИЕ ПРОГРАММЫ

Настоящая программа предназначена для осуществления приема на обучение по образовательным программам высшего образования – программам подготовки научных и научно-педагогических кадров в аспирантуре вступительного экзамена в аспирантуру по специальности 2.3.6 — методы и системы защиты информации, информационная безопасность и содержит основные темы и вопросы к экзамену, список основной и дополнительной литературы и критерии оценивания.

II. ОСНОВНЫЕ РАЗДЕЛЫ И ВОПРОСЫ К ЭКЗАМЕНУ

Раздел 1. Общая часть

1. Непрерывность функций одной переменной, свойства непрерывных функций. Функции многих переменных, полный дифференциал и его геометрический смысл. Достаточные условия дифференцируемости. Градиент.

2. Определенный интеграл. Интегрируемость непрерывной функции. Первообразная непрерывной функции.

3. Неявные функции. Существование, непрерывность и дифференцируемость неявных функций.

4. Числовые ряды. Сходимость рядов. Критерий сходимости Коши. Достаточные признаки сходимости. Абсолютная и условная сходимость ряда. Свойство абсолютно сходящихся рядов. Умножение рядов.

5. Ряды функций Равномерная сходимость. Признак Вейерштрасса. Свойства равномерно сходящихся рядов (непрерывность суммы, почленное интегрирование и дифференцирование).

6. Степенные ряды в действительной и комплексной области. Радиус сходимости, свойства степенных рядов (почленное интегрирование, дифференцирование). Разложение элементарных функций.

7. Несобственные интегралы и их сходимость. Равномерная сходимость интегралов, зависящих от параметра. Свойства равномерно сходящихся интегралов.

8. Ряды Фурье. Достаточные условия представимости функции рядом Фурье.

9. Теоремы Остроградского и Стокса. Дивергенция. Вихрь.

10. 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.

11. Билинейные и квадратичные функции и формы в линейных простран ствах и их матрицы. Приведение к нормальному виду. Закон инерции.

12. Линейные преобразования линейного пространства, их задания матрицами. Характеристический многочлен линейного преобразования. Собственные векторы и собственные значения, связь последних с характеристическими корнями.

13. Евклидово пространство. Ортонормированные базисы. Ортогональные матрицы. Симметрические преобразования. Приведение квадратичной формы к главным осям.

14. Группы, подгруппы, теорема Лагранжа. Порядок элемента. Циклические группы, факторгруппа. Теорема о гомоморфизмах.

15. Аффинная и метрическая классификация кривых и поверхностей второго порядка. Проективная классификация кривых.

16. Дифференциальное уравнение первого порядка. Теорема о существовании и единственности решения.

17. Линейное дифференциальное уравнение второго порядка. Линейное однородное уравнение. Линейная зависимость функций. Фундаментальная система решений. Определитель Вронского. Линейное неоднородное уравнение.

18. Линейное дифференциальное уравнение с постоянными коэффициентами: однородное и неоднородное.

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

20. Элементарные функции комплексного переменного и даваемые ими конформные отображения. Простейшие многозначные функции. Дробно-линейные преобразования.

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

22. Ряд Лорана. Полюс и существенно особая точка. Вычеты.

23. Криволинейные координаты на поверхности. Первая квадратичная форма поверхности.

24. Вторая квадратичная форма поверхности Нормальная кривизна линии на поверхности. Теорема Менье.

25. Главные направления и главные кривизны. Формула Эйлера.

Раздел 2. Специальная часть

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 безопасность 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 (однонаправленные) функции: определение односторонней функции; гипотетические примеры односторонних функций. Криптографические хэш-функции; односторонние семейства хэш-функций; необходимые и достаточные условия существования. Генераторы псевдослучайных

последовательностей в криптографии: два определения псевдослучайных генераторов; необходимые и достаточные условия их существования.

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: примеры протоколов; необходимые и достаточные условия существования стойких протоколов электронной подписи. Доказательства с нулевым разглашением: понятие протокола интерактивного доказательства; свойство нулевого разглашения; примеры; протоколы интерактивной аутентификации.
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. Совместное использование криптосистем с открытым ключом и симметричных криптосистем. 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 доменных имен, источников отсылки сообщений. Использование подмены в проведении атак «человек посередине» и организации фишинга. Атаки на основные сетевые протоколы: IP; TCP; HTTP. Методы защиты от сетевых атак. Варианты защищенных сетевых проколов: IPsec; SSL/TLS; HTTPS. Инфраструктура открытых ключей, удостоверяющий центр, сертификат, путь доверия. Методы защиты от сетевых атак с использованием

инфраструктуры открытых ключей или альтернативных моделей доверия (PGP).

5. Протоколирование и аудит. Понятие о протоколировании, аудите, активном аудите. Подходы к организации архитектуры систем активного аудита. Методы мониторинга и обнаружения вторжений в распределенных информационно-вычислительных системах. Основные методы анализа регистрационной информации. Сигнатурные методы обнаружения вторжений и аномальной активности; использование регулярных выражений. Алгоритмы статистического анализа регистрационной информации.
6. Защита от вредоносного программного обеспечения. Понятие о вредоносном программном обеспечении. Подходы к классификации вредоносного программного обеспечения. Программные закладки. Троянские программы. Вирусы и черви. Способы внедрения вредоносного программного обеспечения в компьютерные системы. Воздействие вредоносного программного обеспечения на компьютерные системы. Взаимодействие компонентов вредоносного программного обеспечения. Вредоносное программное обеспечение и бот-сети. Методы защиты от вредоносного программного обеспечения. Обеспечение целостности. Изолированные программные среды. Методы антивирусной защиты. Алгоритмическая неразрешимость задачи выявления вируса. Существование вирусов, не выявляемых алгоритмически.
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. Примеры атак с использованием распространенных уязвимостей программных средств (переполнение буфера, состояние гонки, арифметическое переполнение, инъекции интерпретируемого кода). Подходы к предотвращению возникновения уязвимостей. Методы тестирования программных средств, методы верификации программных средств. Использование автоматических анализаторов исходного кода.

III. РЕФЕРАТ ПО ИЗБРАННОМУ НАПРАВЛЕНИЮ ПОДГОТОВКИ

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 и рекомендуемую оценку, входящую в общий экзаменационный балл.

IV. ПРИМЕР ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Вопрос 1. Теорема Коши об интеграле по замкнутому контуру. Интеграл Коши. Ряд Тейлора.

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).

V. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. ОСНОВНАЯ

Общая часть:

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

Специальная часть:

1. Основы информационной безопасности: курс лекций / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина — 4-е изд. — М.: Интернет-университет информационных технологий; БИНОМ. Лаборатория знаний, 2008. — 205 с. : ил. — (Серия «Основы информационных технологий»).
2. Теоретические основы защиты информации : учеб. пособие для студентов высш. учеб. заведений / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. — М.: Издательский центр «Академия», 2009. — 272 с.
3. Стандарты информационной безопасности : курс лекций : учеб. пособие / Второе издание / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина — М.: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2006. — 264 с.
4. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия. / О. О. Андреев и др. Под ред. В. А. Васенина. — М.: МЦНМО, 2008. — 398 с.
5. Критически важные объекты и кибертерроризм. Часть 2. Аспекты программной реализации средств противодействия. / О. О. Андреев и др. Под ред. В. А. Васенина. — М.: МЦНМО, 2008. — 607 с.
6. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П. Н. Девянин. – М.: Радио и связь, 2006. — 176 с.
7. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / П. Н. Девянин. — М.: Издательский центр «Академия», 2005. — 144 с.
8. Информационные компьютерные преступления: учебное пособие / В. В. Крылов. — М.: Изд-во РАГС, 2004. — 221 с.
9. Введение в криптографию. Издание 4-е, дополненное / Под общей редакцией В. В. Ященко. — М.: МЦНМО, 2012. — 352 с.
10. Методы дискретной математики в криптологии / В. М. Фомичев. — М.: Диалог-МИФИ, 2010. — 424 с.
11. Введение в дискретную математику / С. В. Яблонский. — М.: Высшая школа, 2010. — 384 с.
12. Введение в теорию автоматов / В. Б. Кудрявцев, С. В. Алешин, А. С. Подколзин. — М.: Наука. Гл. ред. физ.-мат. лит., 1985. — 320 с.
13. Дискретная математика для инженера / О. П. Кузнецов, Г. М. Адельсон-Вельский — 2-е изд., перераб. и доп. — М.: Энергоатомиздат, 1988. — 480 с.
14. Вычислительные машины и труднорешаемые задачи / М. Гэри, Д. Джонсон. — М.: «Мир», 1982. — 419 с.
15. Классические и квантовые вычисления / А. Китаев, А. Шень, М. Вялый. М.: МЦНМО, 1999. — 192 с.

2. ДОПОЛНИТЕЛЬНАЯ

1. Основы теории информации / А. Файнстейн ; пер. с англ. Коваленко И. Н., Ницкой Э. Р. ; под ред. Гихмана И. И. — М.: Издательство иностранной

литературы, 1960. — Перевод изд.: Feinstein, Amiel. Foundations of Information Theory. New York: McGraw-Hill, 1958.
2. Математическая теория связи / К. Шеннон. // Работы по теории информации и кибернетике / К. Шеннон. — М.: Издательство иностранной литературы, 1963. — 832 с. — с. 243-332. — Перевод изд.: A Mathematical Theory of Communication / C. E. Shannon // The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.
3. Теория связи в секретных системах / К. Шеннон. // Работы по теории информации и кибернетике / К. Шеннон. — М.: Издательство иностранной литературы, 1963. — 832 с. — с. 333-402. — Перевод изд.: Communication Theory of Secrecy Systems / C. E. Shannon // Bell System Technical Journal, Vol. 28, Issue 4, pp. 656–715, October 1949.
4. Обзор методов аутентификации информации / Г. Дж. Симмонс : пер. с англ. // Труды ИИЭР, 1988. — Т. 76, № 5. — Перевод изд.: Authentication Theory/Coding Theory / Gustavus J. Simmons // Proceedings of CRYPTO 84 on Advances in cryptology. — Springer-Verlag New York, Inc., New York, NY, USA, 1985. — Pages 411-431.
5. Foundations of cryptography. Volume 1 (Basic tools) / O. Goldreich. — Cambridge University Press, Cambridge, United Kingdom, 2001.
6. Foundations of cryptography. Volume 2 (Basic applications) / O. Goldreich. — Cambridge University Press, Cambridge, United Kingdom, 2004.
7. Pseudorandomness and cryptographic applications / M. Luby. — Princeton University Press, Princeton, New Jersey, USA, 1996.
8. Computational Complexity: A Modern Approach / S. Arora, B. Barak. — Cambridge University Press, New York, NY, USA, 2009.
9. О существовании скрытых каналов / А. А. Грушо. // Дискретная математика, т. 11, вып. 1, (1999). — с. 24-28.
10. О скрытых каналах и не только / А. В. Галатенко. // JetInfo, № 11, 2002. — с. 12-20.
11. Скрытые каналы / Е. Е. Тимонина. //JetInfo, № 11, 2002. — с. 2-11.
12. Активный аудит / А. В. Галатенко. // JetInfo, № 8, 1999. — с. 2-28.
13. The NIDES statistical component description and justification / H.S. Javitz, A. Valdes // Technical report, Computer Science Laboratory, SRI International, 1994. — URL: http://www.sdl.sri.com/papers/statreport
14. Computer Viruses / Cohen F. // Ph.D. Thesis, 1985.
15. An undetectable computer virus / D.M. Chess, S.R. White // Proceedings of Virus Bulletin Conference, 2000.

V. КРИТЕРИИ ОЦЕНИВАНИЯ

Уровень знаний поступающих в аспирантуру МГУ оценивается по десятибалльной шкале. При отсутствии поступающего на вступительном экзамене в качестве оценки проставляется неявка. Результаты сдачи вступительных экзаменов сообщаются поступающим в течение трех дней со дня экзамена путем их размещения на сайте и информационном стенде структурного подразделения. Вступительное испытание считается пройденным, если абитуриент получил семь баллов и выше.

VI. АВТОРЫ

1. д.ф.-м.н., профессор В.А. Васенин
2. к.ф.-м.н., ст.н.с. А.В. Галатенко