МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение
высшего образования
«Самарский национальный исследовательский университет
имени академика С.П. Королева»
Механико-математический факультет

УТВЕРЖДАЮ
Декан _____ М.Е. Федина
«___» _____ 2024г.

ПРОГРАММА КОМПЛЕКСНОГО ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

для поступающих в магистратуру

Направление подготовки

10.04.01 Информационная безопасность

Форма обучения

Очная

Самара

2024

Аннотация программы

Программа включает в себя основные разделы, связанные с организацией защиты информации. В каждом разделе выделены базовые понятия и методы, которые являются важными для освоения магистерской программы согласно федерального государственного стандарта. Ключевые вопросы в каждом блоке вопросов предполагают владение теоретическим материалом и должны сопровождаться практическими примерами и иллюстрироваться решением задач на основе излагаемой теории.

Тема 1. Математические основы

Непрерывность действительных функций одной действительной переменной. Классификация точек разрыва. Свойства функций непрерывных на отрезке. Дифференцируемость функций одной и нескольких действительных переменных. Дифференциал функции. Первообразная и неопределенный интеграл. Определенный интеграл и его свойства. Ряды Фурье. Матрицы и операции над ними. Определители матриц и их свойства. Ранг матрицы. Критерий обратимости матриц (с доказательством). Способы вычисления обратной матрицы. Системы линейных уравнений. Теорема о структуре общего решения системы линейных уравнений. Векторные пространства, их базисы и размерность. Координаты векторов в базисе и их изменение при переходе к другому базису. Дифференциальные уравнения первого порядка. Линейные дифференциальные уравнения.

Тема 2. Дискретная математика

Алгебра множеств и отношений. Представление алгебр множеств и отношений матричными алгебрами.

Функциональные отношения. Отношения эквивалентности и порядка на конечных множествах, свойства их матриц.

Тема 3. Математическая логика и теория алгоритмов

Булевы функции. Представление булевых функций формулами алгебры.

Исчисления высказываний и предикатов, их полнота и непротиворечивость.

Тема 4. Теория вероятностей и математическая статистика

Вероятностное пространство. Аксиоматика А.Н. Колмогорова. Свойства вероятностной меры. Классическое определение вероятности.

Условные вероятности. Независимость событий. Формула полной вероятности и формула Байеса.

Случайные величины. Функции распределения случайных величин и их свойства. Плотности распределения. Типовые распределения: биномиальное, пуассоновское, равномерное, гауссовское (нормальное).

Тема 5. Компьютерные сети

Сравнительная характеристика сетей различных типов. Особенности протокола TCP/IP. Виды атак в IP сетях. Причины уязвимости IP сетей. Модель информационной безопасности систем. Типовые виды угроз безопасности. Классификация способов и средств защиты информации в сетях. Защита от вирусов. Стандартные методы защиты сетей, МСЭ. Защита доверительной сети, VPN. Требования к системе безопасности сетей. Принципы построения системы обеспечения безопасности корпоративной сети.

Тема 6. Структуры данных и алгоритмы

Понятие базы данных и СУБД. Основные функции СУБД. Иерархическая, сетевая и реляционная модели баз данных. Алгоритмы внутренней сортировки. Оценка трудоемкости. Алгоритмы поиска в последовательно организованных файлах. Оценка трудоемкости. Алгоритмы поиска в деревьях.

Тема 7. Защита информации

Основные понятия защиты информации. Государственная система обеспечения информационной безопасности. Система нормативно-правовых актов, регулирующих обеспечение информационной безопасности в РФ. Правовые основы защиты информации. Организационные основы информационной безопасности. Каналы утечки информации. Основные положения Руководящих

документов ФСТЭК и ФСБ в области защиты информации. Лицензирование и сертификация в области защиты информации. Угрозы безопасности информации. Понятие политики безопасности. Модели системы безопасности, примеры моделей. Криптография и криптоанализ. Конфиденциальность, целостность, доступность информации. Теоретическая и практическая стойкость шифра. Классификация криптографических систем. Шифры простой и сложной замены, перестановки, гаммирования. Криптосистемы с секретным ключом. Поточные криптосистемы. Шифрование методом гаммирования. Криптосистемы с секретным ключом. Блочные шифры. Сеть Фейстеля. Стандарт шифрования DES. Российский стандарт шифрования. Основные режимы работы блочных шифров. Криптосистемы с открытым ключом. Односторонние функции, односторонние функции с секретом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптографические хэш-функции. Однонаправленные хэш-функции. Алгоритм безопасного хеширования SHA. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Электронная подпись.

Вопросы к собеседованию

1. Непрерывность действительных функций одной действительной переменной. Классификация точек разрыва. Свойства функций непрерывных на отрезке.
2. Дифференцируемость функций одной и нескольких действительных переменных.
3. Первообразная, неопределенный и определенный интеграл.
4. Ряды Фурье.
5. Матрицы и операции над ними.
6. Дифференциальные уравнения.
7. Алгебра множеств и отношений. Представление алгебр множеств и отношений матричными алгебрами.
8. Булевы функции. Представление булевых функций формулами алгебры.
9. Вероятностное пространство. Аксиоматика А.Н. Колмогорова. Свойства вероятностной меры. Классическое определение вероятности.
10. Случайные величины. Функции распределения случайных величин и их

свойства.

11. Государственная система обеспечения информационной безопасности.
12. Система нормативно-правовых актов, регулирующих обеспечение информационной безопасности в РФ.
13. Каналы утечки информации.
14. Основные положения Руководящих документов ФСТЭК и ФСБ в области защиты информации.
15. Сравнительная характеристика сетей различных типов.
16. Конфиденциальность, целостность, доступность информации.
17. Понятие базы данных и СУБД. Основные функции СУБД.
18. Иерархическая, сетевая и реляционная модели баз данных.
19. Особенности протокола TCP/IP. Виды атак в IP сетях. Причины уязвимости IP сетей.
20. Модель информационной безопасности систем. Типовые виды угроз безопасности.
21. Стандартные методы защиты сетей, МСЭ.
22. Принципы построения системы обеспечения безопасности корпоративной сети.
23. Понятие политики безопасности. Модели системы безопасности, примеры моделей.
24. Классификация криптографических систем. Теоретическая и практическая стойкость шифра.
25. Шифры простой и сложной замены, перестановки, гаммирования.
26. Стандарт шифрования DES. Российский стандарт шифрования.
27. Криптосистема RSA. Криптосистема Эль Гамаля.
28. Криптографические хэш-функции.
29. Электронная подпись.
30. Лицензирование и сертификация в области защиты информации.

Список рекомендуемой литературы

1. Кудрявцев Л.Д. Краткий курс математического анализа. Тт. 1, 2. М.: Физматлит, 2002.

2. Зорич В.А. Математический анализ. Ч. 1, 2. М.: МЦНМО, 2002.
3. Фихтенгольц Г.М. Основы математического анализа. Ч. 1, 2. Лань, 2008.
4. Тихонов А.Н. Обыкновенные дифференциальные уравнения. М.: Физматлит, 2005.
5. Бибиков Ю.Н. Курс обыкновенных дифференциальных уравнений. М.: Лань, 2011.
6. Петровский И.Г. Лекции по теории обыкновенных дифференциальных уравнений. М.: Физматлит, 2009.
7. Владимиров В.С., Жаринов В.В. Уравнения математической физики. М.: Физматлит, 2008.
8. Ефимов Н.В., Розендорн Э.Р. Линейная алгебра и многомерная геометрия. М.: Физматлит, 2005.
9. Свешников А.Г. , Тихонов А.Н. Теория функций комплексной переменной. М.: Физматлит, 2010.
10. Кострикин А.И. Основы алгебры. М.: МЦНМО, 2009.
11. Кострикин А.И., Манин Ю.И. Линейная алгебра и геометрия. М.: Лань, 2008.
12. Ильин В.А., Позняк Э.Г. Аналитическая геометрия. М.: Физматлит, 2004.
13. 15. Мальцев И. А. Дискретная математика. М.: Лань, 2011.
14. Кремер Н.Ш. Теория вероятностей и математическая статистика: учебник для вузов. -2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА, 2004. – 573с.
15. Гусева Е.Н. Теория вероятностей и математическая статистика: [Электронный ресурс] учеб. пособие /Е.Н. Гусева. -5-е изд., стер. – М.: ФЛИНТА, 2011. -210с. URL:http://www.biblioclub.ru
16. Калинина В.Н. Теория вероятностей и математическая статистика. Компьютерно-ориентированный курс: [Электронный ресурс] учеб. пособие для вузов /В.Н. Калинина. – М.: Дрофа, 2008. -471с. URL:http://www.biblioclub.ru
17. Акимов О.Е. Дискретная математика: логика, группы, графы. – М.: Лаборатория Базовых Знаний, 2001. – 352 с.: ил.
18. Верещагин Н.К., Шень А. Лекции по математической логике и теории алгоритмов. Часть 2. Языки и исчисления. М.: МЦНМО, 2000. – 288 с. (Серия «Современные лекционные курсы»).
19. Сети под управлением Windows XP / Каки Коэн, Эндрю Дэниелс; Пер. с англ. В. А. Вет ских. - М. : НТ Пресс, 2005. - 504 с. : ил. - (Защита и администрирование).
20. Проектирование инфраструктуры Active Directory и сети на основе Microsoft Windows Server 2003. Учебный курс Microsoft/пер. с англ - М.: Издательско-торговыи дом «Русская Редакция»; СПб.: Питер, 2006. - 364 стр.: ил.
21. TCP/IP. Для профессионалов. 3-е изд. / Т. Паркер, К. Сиян. — СПб.: Питер, 2004.—

859 с: ил.

22. Камышников В.В., Основы сетевой архитектуры Internet, – Самара, Изд-во. СамГУ, 2001, 106 с.
23. Родичев Ю.А., Компьютерные сети: архитектура, технологии, защита – Самара, Изд-во. СамГУ, 2006, 468 с.
24. Администрирование Novell NetWare 6.0/6.5: Пер. с англ. – СПб.: БХВ-Петербург, 2003. – 1056 с.: ил.
25. Карпова Т.С. Базы данных: модели, разработка, реализация.- СПб.: Питер,2001.
26. Конноли Т., Бегг К., Страчан А. Базы данных: проектирование, реализация и сопровождение.-М: Вильямс,2001
27. Дейт К. Введение в системы баз данных. 6-е издание: Пер. с англ. – М., СПб, Киев: Вильямс, 2000. – 848 с.
28. Родичев Ю.А., Компьютерные сети. Нормативно-правовые аспекты информационной безопасности – Самара, Изд-во. СамГУ, 2007, 344 с.
29. Родичев Ю.А., Информационная безопасность: нормативно-правовые аспекты. – Изд-во. Питер, 2008, 272 с.
30. Родичев Ю.А., Правовая защита персональных данных – Самара, Изд-во. СамГУ, 2009, 449 с.
31. Рощупкин В.Г., Основы информационно-аналитической деятельности – Самара, Изд-во. СамГУ, 2012, 149 с.
32. Давыдов А.Е., Максимов Р.В., Савицкий О.К., Защита и безопасность ведомственных интегрированных инфокоммуникационных систем – Москва: Изд-во. ОАО «Воентелеком», 2015. 520 с.
33. Информационная безопасность и защита информации : Учеб. пособие для вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков; Под ред. С.А. Клейменова. - М. : Академия, 2006. - 336с. - (Высшее профессиональное образование).
34. Зайцев А.П. Технические средства и методы защиты информации: Учеб. пособие для вузов Издательство: "Горячая линия - Телеком", 2009; 616 стр.
35. Теоретические основы защиты информации : Учеб. пособие для вузов / С.С. Корт. - М. : Гелиос АРВ, 2004. - 240 с. : ил.
36. Защита от утечки информации по техническим каналам / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев Горячая линия-Телеком: 2005.
37. Стрельцов А.А. Обеспечение информационной безопасности России. М.: МЦНМО, 2002.
38. Галатенко В.А. Основы информационной безопасности. М.: ИНТУИТ, 2003.

39. Пазизин С.В. Основы защиты информации в компьютерных системах. М.: ТВП, 2003.
40. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2005.
41. Зензин О.С., Иванов М.А. Стандарт криптографической защиты AES. Конечные поля. М.: КУДИЦ-ОБРАЗ, 2002.
42. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003.
43. Фомичев В.М. Дискретная математика и криптология. М.: "ДИАЛОГ· МИФИ", 2003..
44. Бабаш А.В., Шанкин Г.П. Криптография. Аспекты защиты. М.: Солон-Р, 2002.
45. Введение в криптографию (под ред. В.В. Ященко). М.: МЦНМО-ЧеРо, 1998.
46. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001.
47. Столингс В. Криптография и защита сетей. Принципы и практика. М.: Издательский дом "Вильямс", 2001.
48. Чмора А. Современная прикладная криптография. М.: ГЕЛИОС АРВ, 2002.
49. Шнайер Б. Прикладная криптография. М.: Триумф, 2002.