

АННОТАЦИЯ ДИСЦИПЛИНЫ

«Математика, специальные главы»

Дисциплина «Математика, специальные главы» является частью программы специалитета «Безопасность открытых информационных систем (СУОС)» по направлению «10.05.03 Информационная безопасность автоматизированных систем».

Цели и задачи дисциплины

Цель дисциплины - ознакомить обучающихся со специальными разделами высшей математики. В процессе изучения дисциплины студент осваивает следующие компетенции: способностью совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности; способен проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента. Задачи дисциплины: привить обучающимся навыки использования рассматриваемого математического аппарата в профессиональной деятельности и воспитать у обучаемых высокую культуру мышления, т.е. строгость, последовательность, непротиворечивость и основательность в суждениях, в том числе и в повседневной жизни; знать понятие стохастического интеграла и области его применения; изучение построения спектральных представлений случайных процессов; формирование навыков решения задачи прогнозирования и фильтрации с помощью условного математического ожидания; освоить методику оценки сложности и вероятностной оценки базовых вероятностных тестов простоты..

Изучаемые объекты дисциплины

Предметом освоения дисциплины являются следующие объекты: случайные процессы в линейных системах; процессы дробового эффекта; стохастический интеграл; интеграл Ито; прогнозирование и фильтрация; порядок и принципы засекречивания и рассекречивания информации; условные математические ожидания; организация работы с персоналом по вопросам защиты информации; апостериорные вероятности; субэкспоненциальные алгоритмы; алгоритмы проверки простоты и факторизации с помощью эллиптических кривых; аддитивный и мультипликативный характеры конечного поля вычетов..

Объем и виды учебной работы

| Вид учебной работы | Всего часов | Распределение по семестрам в часах | |
|--|-------------|------------------------------------|--|
| | | Номер семестра | |
| | | 5 | |
| 1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: | 45 | 45 | |
| 1.1. Контактная аудиторная работа, из них: | | | |
| - лекции (Л) | 16 | 16 | |
| - лабораторные работы (ЛР) | | | |
| - практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ) | 27 | 27 | |
| - контроль самостоятельной работы (КСР) | 2 | 2 | |
| - контрольная работа | | | |
| 1.2. Самостоятельная работа студентов (СРС) | 63 | 63 | |
| 2. Промежуточная аттестация | | | |
| Экзамен | | | |
| Дифференцированный зачет | | | |
| Зачет | 9 | 9 | |
| Курсовой проект (КП) | | | |
| Курсовая работа (КР) | | | |
| Общая трудоемкость дисциплины | 108 | 108 | |

Краткое содержание дисциплины

| Наименование разделов дисциплины с кратким содержанием | Объем аудиторных занятий по видам в часах | | | Объем внеаудиторных занятий по видам в часах |
|--|---|----|----|--|
| | Л | ЛР | ПЗ | СРС |
| 5-й семестр | | | | |

| Наименование разделов дисциплины с кратким содержанием | Объем аудиторных занятий по видам в часах | | | Объем внеаудиторных занятий по видам в часах |
|--|---|----|----|--|
| | Л | ЛР | ПЗ | СРС |
| Теоретико-числовые методы в криптографии | 4 | 0 | 7 | 10 |
| Тема 2.1. Проверка простоты натуральных чисел. Сложность и вероятностная оценка базовых вероятностных тестов простоты. Детерминированный полиномиальный тест простоты. Тема 2.2. Факторизация целых чисел. Основные идеи субэкспоненциальных алгоритмов факторизации. Схема методов решета числового поля. Тема 2.3. Применение эллиптических кривых для проверки простоты и факторизации. Алгоритм Шуфа вычисления порядка группы точек эллиптической кривой над конечным полем. Алгоритмы проверки простоты и факторизации с помощью эллиптических кривых. Тема 2.4. Характеры конечных полей. Аддитивный и мультипликативный характеры поля. Оценки сумм характеров и их приложения. | | | | |
| Некоторые задачи прогнозирования, фильтрации и регулирования случайных процессов | 4 | 0 | 8 | 23 |
| Тема 1.4. Общая задача о наилучшем приближении. Лемма о перпендикуляре. Задача о комплексе приборов. Примеры. Тема 1.5. Прогнозирование и фильтрация стационарных случайных процессов. Задача линейного прогнозирования. Линейная фильтрация (оценивание среднего значения). Тема 1.6. Условные математические ожидания и некоторые задачи прогнозирования и фильтрации. Об условных математических ожиданиях. Роль апостериорных вероятностей в некоторых задачах прогнозирования и фильтрации. | | | | |
| Специальные разделы теории случайных процессов. | 8 | 0 | 12 | 30 |
| Некоторые модели случайных процессов АРС Тема 1.1 Случайные процессы в линейных системах. Вводные замечания. Стохастический интеграл. Сходимость к стационарному процессу. Процессы дробового | | | | |

| Наименование разделов дисциплины с кратким содержанием | Объем аудиторных занятий по видам в часах | | | Объем внеаудиторных занятий по видам в часах |
|---|---|----|----|--|
| | Л | ЛР | ПЗ | СРС |
| <p>эффекта.</p> <p>Тема 1.2. Стационарные случайные процессы. Спектральное представление стационарных процессов и преобразование Фурье. Линейные преобразования. Примеры.</p> <p>Тема 1.3. Диффузионные процессы. Случайные процессы, представимые стохастическим интегралом Ито. Дифференциальные уравнения Колмогорова.</p> | | | | |
| ИТОГО по 5-му семестру | 16 | 0 | 27 | 63 |
| ИТОГО по дисциплине | 16 | 0 | 27 | 63 |