

**Аннотация к рабочей программы дисциплины
«Б1.В.ДВ.02.02 Криптография и основы защиты информации»**

Объем трудоемкости: 4 зачетных единицы

Цель дисциплины: Цель освоения дисциплины – рассматривает задачи информатизации и защиты информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Задачи дисциплины: Задачи освоения дисциплины «Криптография и основы защиты информации»: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем

Место дисциплины в структуре образовательной программы

Дисциплина «Криптография и основы защиты информации» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана.

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

| Код и наименование индикатора* достижения компетенции | Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности)) |
|---|--|
| ПК-1 Способен решать актуальные и важные задачи фундаментальной и прикладной математики | |
| ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области ПК-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований | Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа Уметь: Применять основные математические методы, используемые в анализе типовых алгоритмов Владеть навыками: использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений. |
| ПК-4 Способен разрабатывать программное обеспечение для решения прикладных задач в сфере профессиональной деятельности | |
| ПК-4.1 Имеет навыки использования современных языков программирования для разработки программного обеспечения ПК-4.4 Ориентируется в современных алгоритмах компьютерной математики и имеет практический опыт разработки программных модулей на основе математических моделей | Знать: об основных задачах и понятиях теории кодов; о видах информации, подлежащей кодированию; о классификации кодов; о методах защиты компьютерных систем и сетей. Уметь использовать: коды с одной проверкой на четность; линейные коды; циклические коды; групповые коды. Коды Хэмминга; коды Боуза-Чоудхури-Хоквингема; основные математические методы, используемые в анализе типовых алгоритмов. Владеть: алгоритмами решения систем линейных уравнений по разным модулям; методами построения генераторов псевдослучайных последовательностей; алгоритмами построения кодов, исправляющих ошибки |

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

| № | Наименование разделов | Количество часов | | | | |
|---|--|------------------|-------------------|----|----|----------------------|
| | | Всего | Аудиторная работа | | | Внеаудиторная работа |
| | | | Л | ПЗ | ЛР | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Основные понятия и определения теории кодирования. | 22 | 4 | | 8 | 10 |
| 2 | Свойства энтропии. Теорема Шеннона для кодирования в двоичном симметричном канале связи с шумом. | 22 | 4 | | 8 | 10 |
| 3 | Алгебраические методы в теории кодов. | 22 | 4 | | 8 | 10 |
| 4 | Теория кодов и криптография. | 36 | 6 | | 10 | 20 |
| | <i>Итого по разделам дисциплины:</i> | 102 | 18 | | 34 | 50 |
| | Контроль самостоятельной работы (КСР) | 6 | | | | |
| | Промежуточная аттестация (ИКР) | 0,3 | | | | |
| | Подготовка к текущему контролю | 35,7 | | | | |
| | Общая трудоемкость по дисциплине | 144 | | | | |

Курсовые работы: не предусмотрена**Форма проведения аттестации по дисциплине:** экзамен

Автор доктор физ.-мат. наук, проф. Рожков А.В.