**Аннотация к рабочей программы дисциплины**

# «Б1.В.02 ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ»

**Объем трудоемкости**: 2 зачетных единицы

**Цель дисциплины**: рассматривает задачи защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

**Задачи дисциплины**: Задачи освоения дисциплины «Теоретико-числовые методы криптографии»: 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 «Теоретико-числовые методы криптографии» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана.

Изучение теоретических основ предмета: Числовые функции, основные теоремы о евклидовых кольцах, алгоритмы решения линейных и квадратных уравнений в конечных полях, кольцах вычетов, алгоритмы нахождения наибольших общих делителей, алгоритмов проверки простоты чисел

**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 формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики | |
| ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач<br>ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области | Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации;<br>Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;<br>Владеть: анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем. |
| **ПК-2** Способен активно участвовать в исследовании новых математических моделей в естественных науках | |
| ПК-2.1 Умеет использовать математические модели и применять численные методы решения задач в естественных науках<br>ПК-2.3 Владеет навыками математической обработки результатов экспериментальных исследований составленных | Знать: основные педагогические методы и идеи<br>Уметь: выделять сущности и связи предметной области;<br>Владеть навыками: работы с педагогической литературой и колллективом учащихся . |

| Код и наименование индикатора* достижения компетенции | Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности)) |
|---|---|
| математических моделей | |

**Содержание дисциплины:**

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 7 семестре

| № раздела | Наименование разделов | Количество часов | | | |
|---|---|---|---|---|---|
| | | Всего | Аудиторная работа | | Самостоятельная работа |
| | | | Л | ЛЗ | |
| **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | Модели шифров. | 15 | 4 | 4 | 7 |
| 2 | Мультипликативные функции. | 16 | 4 | 4 | 8 |
| 3 | Табличное и модульное гаммирование. | 18 | 4 | 4 | 10 |
| 4 | Построение больших простых чисел. | 20,8 | 4 | 6 | 10,8 |
| | **Итого:** | | 16 | 18 | 35,8 |
| | *ИТОГО по разделам дисциплины* | | | | |
| | Контроль самостоятельной работы (КСР) | 2 | | | |
| | Промежуточная аттестация (ИКР) | 0,2 | | | |
| | Подготовка к текущему контролю | | | | |
| | Общая трудоемкость по дисциплине | 72 | | | |

**Курсовые работы**: не предусмотрена.

**Форма проведения аттестации по дисциплине:** зачет.

Автор А.В. Рожков, профессор, д.ф.-м.н., профессор