*Чтоб мысль врага узнать,*
*ему вскрывают сердце.*
*А письма — и подавно...*

**Шекспир , "Король Лир"**

# Математические основы криптологии

# Форма отчетности

- Форма отчетности – **зачет**.

Для получения оценки необходимо набрать за семестр от **60** до **100** баллов:

| | **Кол-во** | **баллы** | **сумма** |
|---|---|---|---|
| **ЛК** | 18 | 1,5п*18 | 27 |
| **ПЗ** | 7+2 к/р | 2*7 | 14 |
| **ЛР** | 4 | (5з*1,5)*4 | 30 |
| **КР** | 2 | 15 | 30 |
| **итог** | - | - | **101** |

**П** – посещение; **З** – защита ЛР

# Литература:


1. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. – С.Пб: ИТМО, 2004. – 109 с.

2. Математические и компьютерные основы криптологии: Учебное пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003. – 382 с.

3. Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство. – М.: Мир, 2006. – 471 с.

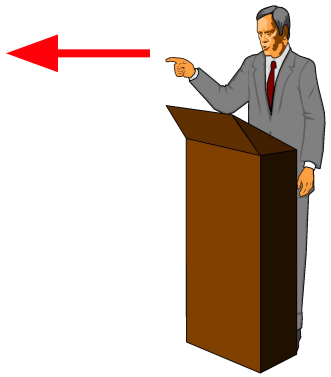
4. Галуев Г.А. Математические основы криптологии. Таганрог: ТРТУ, 2003. – 120 с.

5. Поповский В.В., Персиков А.В. Основы криптографической защиты информации в телекоммуникационных системах. Том 1: Учебник. – ООО «Компания СМИТ», 2010. – 352 с.

# Основные задачи дисциплины

**ЗНАТЬ:**

- основные операции математической логики;
- основные методы, используемые криптологией;
- свойства специальных последовательностей чисел;
- основные понятия теории групп, колец, полей и многочленов;
- основные понятия теории вероятности;
- основные задачи и методы математической статистики;
- способы представления информации в криптосистемах.



**УМЕТЬ:**

- классифицировать криптосистемы по нескольким критериям;
- использовать основные алгебраические структуры для криптопреобразований;
- анализировать вычислительную сложность алгоритмов криптопреобразований;
- находить вероятности сложных событий;
- проводить исследования свойств последовательностей чисел;
- строить генераторы псевдослучайных последовательностей чисел;
- рассчитывать криптосистемы, построенные на основе дискретного логарифма.

# Содержание

1. **Базовые элементы теории чисел.**
   - Операции по модулю
   - НОД, НОК чисел. Алгоритм Эвклида
2. **Основные определения и термины криптографии. Классификация систем шифрования.**
3. **Исторические этапы развития криптографии.**
   - Этапы развития
   - Шифры перестановок
   - Шифры подстановок
   - Шифры гаммирования
4. **Способы представления информации в криптологии**
   - Двоичный код, 16-ричный, ASCII, Unicod.
5. **Основы математической логики. Стойкость криптосистем.**
   - Случайные события. Формула Байеса. Формула Бернулли.
6. **Основы теории информации и кодирования источника**
7. **Основы теории чисел. Группы. Кольца. Поля. Многочлены.**
8. **Математические преобразования в симметричных криптосистемах**
   - Классификация современных шифров
   - Математические операции в современных симметричных шифрах: примеры, достоинства, недостатки
9. **Модульная арифметика. Теория вычетов.**
   - Функция Эйлера.
   - Нахождение обратных элементов: Цепные дроби. Расширенный алгоритм Эвклида.
   - Китайская теорема об остатках.
   - Квадратичные вычеты
   - Современные асимметричные шифры: примеры (RSA, El-Gamal, Polig-Hellman), достоинства, недостатки
   - Гибридные шифры
10. **Математические преобразования в асимметричных криптосистемах**
    - Математические операции в современных асимметричных шифрах: примеры, достоинства, недостатки
    - Криптосистемы на эллиптических кривых.