**2.3 Перечень тем лабораторных занятий по дисциплине**

**Методы защиты информации**

Основная цель проведения лабораторных занятий состоит в закреплении теоретического материала курса, приобретении навыков выполнения эксперимента, обработки экспериментальных данных, анализа результатов, грамотного оформления отчетов.

|  |  |  |
| --- | --- | --- |
| №  темы  по п.1 | Наименование  лабораторной работы | Содержание |
| 3 | Лабораторная работа № 1  Симметричная криптография. Стандарт шифрования ГОСТ 28147-89 | Реализовать программные средства шифрования и дешифрования текстовых файлов при помощи стандарта шифрования ГОСТ 28147-89 в следующих режимах:   1. Простой замены 2. Гаммирования 3. Гаммирования с обратной связью 4. Генерации имитоприставок |
| 3 | Лабораторная работа № 2  Симметричная криптография. СТБ 34.101.31-2011 | Реализовать программные средства шифрования и дешифрования текстовых файлов при помощи алгоритма СТБ 34.101.31-2011 в различных режимах |
| 4 | Лабораторная работа № 3  Асимметричная криптография. Криптосистема Рабина | Реализовать криптостойкое программное средство шифрования и дешифрования текстовых файлов при помощи Криптосистемы Рабина |
| 4 | Лабораторная работа № 4  Асимметричная криптография. Алгоритм Мак-Элиса | Реализовать программные средства шифрования и дешифрования текстовых файлов при помощи алгоритма Мак-Элиса для криптостойких размеров порождающей матрицы |
| 5 | Лабораторная работа № 5  Хэш-функции | Реализовать программное средство контроля целостности сообщений с помощью вычисления хэш-функции и алгоритма ГОСТ 34.11 |
| 6 | Лабораторная работа № 6  Цифровая подпись | Реализовать программное средство формирования и проверки ЭЦП на базе алгоритма ГОСТ 34.10 |
| 7 | Лабораторная работа № 7  Криптография с ис­пользованием эллипти­ческих кривых | Реализовать схему шифрования (дешифрования) для аналога алгоритма Эль-Гамаля на основе эллиптических кривых |
| 8 | Лабораторная работа № 8  Стеганографические методы | Реализовать программное средство, сокрытия (извлечения) текстового сообщения в (из) JPEG изображение(я) на основе метода сокрытия в частотной области изображения |

По результатам работы студентом должен быть представлен и защищен отчет. Содержание отчета включает:

1. Титульный лист, подписанный студентом и преподавателем с оценкой после защиты работы
2. Введение, содержащее общие теоретические сведения и индивидуальную постановку задачи.
3. Полную блок – схему разработанного алгоритма.
4. Распечатку скриншотов результатов ввода данных и исполнения программы.
5. Распечатку программного кода.
6. Вывод о решении поставленной задачи и иные сведения, относящиеся к процессу ее решения.