**Лабораторные работы по предмету**

**«Методам и средствам защиты информации»**

**Требования к отчету по лабораторным работам**

Содержание отчета:

1. Титульный лист взять на сайте кафедры ИСУ
2. Текст задания
3. Описание алгоритма
4. Два примера шифрования и расшифровывания

4.1 Нижегородский государственный технический университет

4.2 Ваши Ф.И.О.

1. Текст программы с **комментариями**
2. Принтскрины экранов с входными и выходными данными.

**Лабораторная работа № 1 КЛАССИЧЕСКИЕ КРИПТОСИСТЕМЫ (Шифры замены)**

**Задание №1.1**

Реализовать алгоритм шифрования данных «**Шифр Вижинера**».

**Задание №1.2**

Реализовать алгоритм шифрования данных «**Биграммный шифр Плейфейра**».

**Задание №1.3**

Реализовать алгоритм шифрования данных «**Шифр *"двойной квадрат"* Уитстона**».

**Лабораторная работа № 2 (Шифрование методом гаммирования)**

**Задание №2**

Реализовать алгоритм шифрования данных «Шифрование методом гаммирования»

**По модулю N**.

**Лабораторная работа № 3 АЛГОРИТМЫ СИММЕТРИЧНОГО БЛОЧНОГО ШИФРОВАНИЯ (Шифр DES и его режимы)**

**Задание №3.1**

Реализовать стандарт шифрования данных **DES** в режиме «Электронная кодовая книга».

**Задание №3.2**

Реализовать стандарт шифрования данных **DES** в режиме «Сцепление блоков шифрованного текста».

**\*Задание №3.3**

Реализовать стандарт шифрования данных **DES** в режиме «Обратная связь по шифру».

**Задание №3.4**

Реализовать стандарт шифрования данных **DES** в режиме в режиме «Обратная связь по выходу».