**Практическийраздел**

ИНДИВИДУАЛЬНЫЕ ПРАКТИЧЕСКИЕ РАБОТЫ, ИХ ХАРАКТЕРИСТИКА

**Введение**

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

1. Титульный лист
2. Введение, содержащее постановку задачи.
3. Блок – схему алгоритма.
4. Распечатку скриншотов результатов ввода данных и исполнения программы.
5. Распечатку программного кода.
6. Вывод.

**ИПР №1**

**Часть 1.1 Шифрование файлов**

**Изучите теоретические сведения**

**Цель:**Реализуйте программное средство шифрования и дешифрования текстовых файлов при помощи Шифра Цезаря, (шифра сдвига, кода Цезаря).

**Результат:** Программа шифрования, осуществляющая криптографическое преобразование введенного текста с помощью Шифра Цезаря, (шифра сдвига, кода Цезаря).

**Общая постановка задачи:**  Создать программу, читающую данные из файла и шифрующие (дешифрующие) их с помощью с помощью Шифра Цезаря.

**ИПР №2**

**Часть 2.1. 2. Блочные шифры. AES.**

**Изучите теоретические сведения, содержащие требования к реализации блочных шифров.**

**Цель:** реализовать на языке программирования C++ алгоритм блочного шифрования AES.

**Результат:** Программа шифрования, осуществляющая криптографическое преобразование введенного текста с помощью алгоритма блочного шифрования AES.

**Общая постановка задачи:**  Создать программу, читающую данные из файла, шифрующие и дешифрующие их с помощью алгоритма блочного шифрования AES.

**КОНТРОЛЬНЫЕ РАБОТЫ**

***Контрольная работа №1***

**Указания по выбору варианта**

Рабочей программой дисциплины «Методы защиты информации» предусмотрено выполнение двух контрольных работ. Контрольная работа № 1 подразумевает изучение и программную реализацию (на языке высокого уровня) алгоритма формирования Хэш-функции **MD5**. В качестве отчета по контрольной работе высылается листинг программной реализации, представленный в виде теста и исполняемый файл. В контрольной работе № 1 используется **один вариант** (для всех номеров зачетных книжек).

**Теоретическая часть**

1. Изучить алгоритм формирования Хэш-функции **MD5**.
2. Создать и протестировать алгоритм формирования Хэш-функции **MD5** на языке высокого уровня.

***Контрольная работа №2***

**Криптография с использованием эллиптических кривых.**

**Указания по выбору варианта**

Рабочей программой дисциплины «Методы защиты информации» предусмотрено выполнение двух контрольных работ. Контрольная работа № 2 подразумевает изучение и программную реализацию (на языке высокого уровня) алгоритма шифрования/дешифрования на основе эллиптических кривых. В качестве отчета по контрольной работе высылается листинг программной реализации, представленный в виде теста и исполняемый файл. В контрольной работе № 2 используется **один вариант** (для всех номеров зачетных книжек).

**Теоретическая часть**

1. Изучить
2. Аналог алгоритма Диффи-Хеллмана обмена ключами;
3. Алгоритм цифровой подписи на основе эллиптических кривых ECDSA;
4. Шифрование/дешифрование с использованием эллиптических кривых.
5. Создать и протестировать алгоритм шифрования/дешифрования на основе эллиптических кривых на языке высокого уровня.