Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

Национальный исследовательский ядерный университет «МИФИ»

Обнинский институт атомной энергетики–

Филиал федерального государственного автономного образовательного учреждения высшего образования

«Национальный исследовательский ядерный университет «МИФИ»

(ИАТЭ НИЯУ МИФИ)

Отделение Интеллектуальных кибернетических систем

Направление подготовки: 01.03.02 Прикладная математика и информатика, профиль – Прикладная информатика

УДК 51.37

Утверждаю

Директор ИАТЭ НИЯУ МИФИ

\_\_\_\_\_\_\_\_\_\_\_\_\_Т.А. Осипова

«\_\_\_» \_\_\_\_\_\_\_\_\_2021 г.

ЛАБОРАТОРНАЯ РАБОТА № 1

по теме:

бинарное преобразование файла

Студент гр. М-Б20 \_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.М. Заграевская

Преподаватель,

к.ф.-м.н., доцент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Мышев

Обнинск 2021

СОДЕРЖАНИЕ

I. Введение 3

1.1. Постановка цели 3

1.2. Постановка задачи и этапы выполнения работы 3

1.3. Основные понятия и определения 3

II. Основная часть 6

2.1. Листинг программы 6

2.2. Тестирование 7

III. Заключение 10

**Введение**

**1.1. Постановка цели**

Цель работы: разработка и реализация компьютерных технологий криптографической защиты информации в каналах передачи и хранения в виде готового программного продукта, приобретение базовых знаний построения моделей алгоритма и процедур программных компонент таких технологий, освоение навыков анализа и оценки сложности защиты и надежности технологии продукта.

**1.2. Постановка задач и этапы выполнения работы**

1. Разработка моделей алгоритмов и процедур программного компонента криптографической защиты информации объекта согласно заданию.
2. Разработать программного интерфейса ввода-вывода файловых структур с внешних носителей в ОЗУ и обратно.
3. Разработка и реализация алгоритмов программных компонент обработки файлов на бинарных полях памяти.
4. Отладка программных компонентов.
5. Тестирование и контрольные примеры.
6. Расчеты и анализ. Выводы.
7. Прием-сдача программного компонента в диалоговом режиме.

**1.3.** **Основные понятия и определения**

Для реализации лабораторной работы, необходимо иметь знания в области ввода-вывода файловых структур с внешних устройств в ОЗУ и обратно, определенных и описанных в виде бинарный полей. Выделим следующие термины:

**Бит** – базовая единица измерения информации в каналах хранения и передачи, имеющая в них соответственно логические и физические прототипы.

Логическим прототипом бита является символическое обозначение его образа, т.е. множество символов базового алфавита, в физической среде информационного канала. Например, для булевой логики – это ноль и единица, символические образы которых определяются символами 0 и 1.

**Физическими прототипами бита** в каналах хранения являются физические состояния элементов среды хранения, а в каналах передачи ‒ сигналы определенной длительности и уровня. Например, в полупроводниковом ОЗУ физическим прототипом бита будет триггер, состояние которого (напряжение на выходе) будут соответствовать его логическим прототипам 0 и 1; в НМД (накопитель на магнитном диске) это область на поверхности диска, намагниченность которой будет соответствовать логическим прототипам 0 и 1. Аналогично и на других накопителях информации с другой физической средой.

**Бинарное информационное множество** – это множество элементов базового алфавита, образующих логическую структуру в виде сегмента памяти в физической среде канала хранения или поток логически и функционально связанных данных в канале передачи.

В каналах передачи и хранения любой информационный объект (файлы и другие логические структуры) рассматриваются как бинарные информационные множества, на которых определяются информационные пространства, задаваемые в виде кортежа *<Х,Nm>*, где  *Х* ‒ множество символьных цепочек алфавита *Nm*, который представляет собой множество бинарных цепочек длиной *m* битов.

**Информационное пространство** в виде кортежа *<Х,Nm>*является математической моделью информационного объекта, определенного как бинарное множество. Тогда вероятностно-статистической характеристикой информационного объекта (*IO*) в *<Х,Nm****>*** для заданного алфавита *Nm*  будет таблица информационной насыщенности *IO*, которая представляет собой дискретное распределение вероятностей букв *Nm*в *IO*.

**Оперативное запоминающее устройство (ОЗУ)** ‒ это компонент, который позволяет компьютеру кратковременно хранить данные и осуществлять быстрый доступ к ним. Компьютер загружает программу или затребованный документ в память из хранилища, а далее обращается к каждой единице информации в оперативной памяти. Многие операции зависят от памяти, поэтому имеющийся объем ОЗУ играет критическую роль в производительности вашей системы.

**Бинарное поле −** некоторое количество бит, расположенных последовательно в памяти, значение которых процессор не способен прочитать из-за особенностей аппаратной реализации.

**Кодирование –** это перевод информации с одного языка на другой (запись в другой системе символов, в другом алфавите). При этом обычно кодированием называют перевод информации с «человеческого» языка на формальный, например, в двоичный код, а декодированием – обратный переход.

**Декодирование** ‒ это процесс восстановления содержания закодированной информации.

**Криптографическая защита информации** – деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности информации с использованием средств криптографической защиты информации.

# Основная часть

# 2.1. Листинг программы

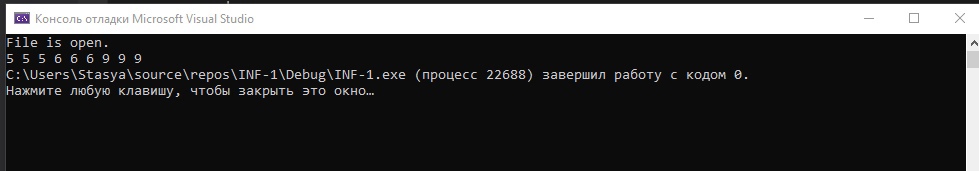
# // laba1.cpp : Этот файл содержит функцию "main". Здесь начинается и заканчивается выполнение программы. // [#include](https://vk.com/im?sel=354876940&st=%23include) <iostream> [#include](https://vk.com/im?sel=354876940&st=%23include) <fstream> using namespace std; int main() { ifstream file1; ofstream file2; [file1.open](https://vk.com/away.php?to=http%3A%2F%2Ffile1.open&cc_key=)("input.txt"); //C:\\Users\\source\\repos\\laba1 [file2.open](https://vk.com/away.php?to=http%3A%2F%2Ffile2.open&cc_key=)("output.txt"); if ([file1.is](https://vk.com/away.php?to=http%3A%2F%2Ffile1.is&cc_key=)\_open() && [file2.is](https://vk.com/away.php?to=http%3A%2F%2Ffile2.is&cc_key=)\_open()) { cout « "File is open." « endl; char ch = 0; while (file1 » ch) //считывает один символ из файла { cout « ch « " "; ch ^= 255; file2 « ch; //записывает один символ в файл } } else { cout « " Error!" « endl; } file1.close(); file2.close(); return 0; }

# 2.2. Тестирование

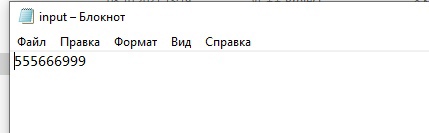
В целях тестирования программы было проведено 3 теста, результаты которых представлены ниже:

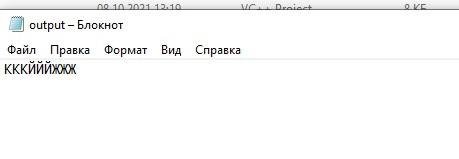
*Тест 1*

Таблица 1 ‒ Результат теста 1



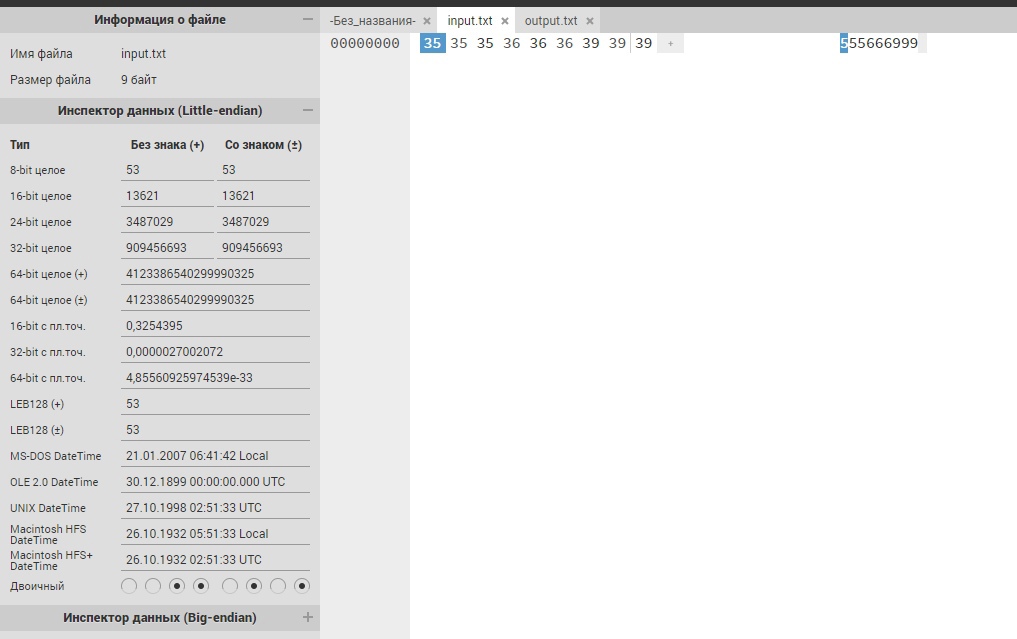
*Тест 2*

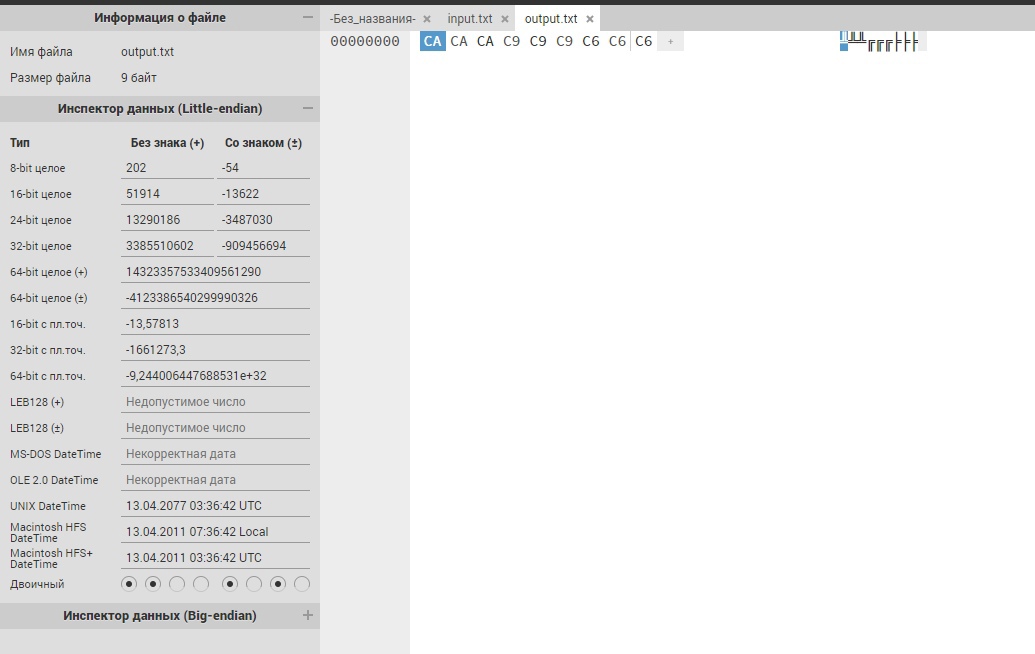




*Тест 3*

На этом этапе тестирование проводилось в HedEd.it ‒ Browser-based Online and Offline Hex Editing:





Программа отработала верно.

**ЗАКЛЮЧЕНИЕ**

Результатом данной лабораторно работы явилось создание программы на языке программирования С++, реализующей следующие функции:

* ввод-вывод файловых структур с внешних устройств в ОЗУ и обратно, определенных и описанных в виде бинарных полей;
* преобразование информационного объекта на бинарном поле ОЗУ;
* кодирование файла и его запись на внешнее устройство;
* декодирование файла и его запись на внешнее устройство.

Через решение поставленной задачи были изучены и апробированы методами криптографической защиты информации в каналах хранения и передачи, приобретены навыки разработки алгоритмов процедур технологий криптографической защиты в информационных каналах, навыки разработки и реализации программных компонентов компьютерных технологий криптографической защиты информации, навыки анализа и оценки сложности защиты и надежности продукта.