**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное ГОСУДАРСТВЕННОЕ бюджетное ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информатики

и вычислительной техники

Кафедра информационной

безопасности

**Отчет к лабораторной работе №1 по дисциплине «Теоретические основы компьютерной безопасности»**

Тема лабораторной работы: «Запрос на идентификацию/аутентификацию»

Выполнила: студент БИс-32\_\_\_\_\_\_\_Мустаев Д. В.\_\_\_\_\_\_\_,

подпись дата

Проверил: ассистент кафедры ИБ \_\_\_\_\_\_\_Ситников И.В. \_\_\_\_\_\_\_

подпись дата

Йошкар-Ола

2017 г.

# **Цель работы**

Цель работы - написать на любом известном языке программирования программу, реализующую интерфейсную систему как составляющую парольной системы с применением механизмов парольной защиты; методов аутентификации; алгоритмов шифрования различной сложности.

# **Техническое задание**

Используя объектно-ориентированный подход, разработать упрощенную парольную систему, которая отвечает следующим требованиям:

1. Приложение должно быть реализовано на Windows Forms
2. Пользователь может осуществлять ввод некоторых данных (пароль, ключ) с клавиатуры
3. Приложение должно иметь следующий функционал

3.1 При запуске программы пользователю выводится окно ввода пароля. Затем в текстовое поле вводится пароль. Текстовое значение пароля хранится в текстовом файле в любом каталоге. Если файла нет, то пароль записывается в файл. Переходим к пункту 3.2. Иначе программа сравнивает пароль и переходит к пункту 3.3.

3.2 Программа открывает форму, где в текстовом поле случайным образом генерируется ключ. По этому ключу шифруется пароль. А также появляется возможность сменить пароль, пункт 3.4.

3.3 Программа открывает форму, где в текстовое поле пользователем вводится сгенерированный ранее ключ. Если ключ и пароль введены верно, то переходим к пункту 3.2, если нет, то допускаются еще две попытки ввода пароля, а в случае неудачи –вывод сообщения об ошибке и закрытие программы.

3.4 Программа показывает следующую форму с кнопкой «сменить пароль». При вводе старого пароля программа зашифровывает его, затем записывает и сравнивает с содержимым файла. Если они совпадают, то программа дает разрешение на переписывание пароля, если нет, то выдается сообщение об ошибке. Перед записью в файл новый пароль предварительно шифруется и записывается уже в зашифрованном виде.

**Ссылка на GitHub**: https://github.com/ilyapasynkov/WindowsFormsApp1

# **Блок-схема программы**



**Блок-схема алгоритма шифрования Виженера**



# **Выводы**

В результате лабораторной работы была написана программа, реализующая парольную систему с применением механизмов парольной защиты на языке С#. Приложение было реализовано на Windows Forms. В программе был использован алгоритм шифрования Виженера.