

Отчет по лабораторной работе №1 по дисциплине «Защита программ и данных»

Работу выполнил Алексеев К.П.

Студент СКБ-172

13.12.2021

Задание:

Реализовать программу на языке C\C++, которая должна включать следующую последовательность действий:

1. Запрос какой-либо информации от пользователя (логин, номер телефона, номер какого-либо документа, ключ любого вида и т.д.)
2. Произведение манипуляций по разработанному алгоритму с введённой пользователем информацией для генерации ответа на ключевой вопрос
3. Запрос ключа от пользователя и сравнение его со сгенерированным ключом на этапе 2.
4. Выдача результата по принципу:
 - Сгенерированный алгоритмом и введённый пользователем ключи совпадают – TRUE -> поздравление или доступ к какой-либо информации
 - Не совпадают – ошибка

При реализации программы должны быть соблюдены условия:

1. Внутри программы должен быть какой-либо алгоритм преобразования данных для генерации ключевой информации.
2. Должны быть реализованы меры защиты от отладки: специальные функции языка, искусственное усложнение кода, директивы препроцессора, условия сборки компилятора, упаковщики и т. д.

Ход работы:

1) Описание алгоритма

Программа запрашивает логин от пользователя. Принимается строка, у которой считается сумма ASCII-кодов каждого ее символа. Эта сумма умножается на 2021 (обозначим за Sum). Далее программа запрашивает пароль у пользователя, если сумма ASCII-кодов его символов совпадает с Sum, то программа выводит сообщение о верном пароле, в противном случае – о неверном пароле.

2) Использованные защитные меры

Были применены следующие меры защиты от отладочного процесса:

- Замена числовых выражений на эквивалентные им в шестнадцатеричном виде;
- Хэширование имен переменных и функций алгоритмом MD5;
- Добавление фиктивных частей кода (циклов);
- Отсутствие комментариев в коде.

Выводы о проделанной работе:

Обфускация достаточно сложный процесс для выполнения, который совмещает в себе и некоторые риски. Например, могут повредиться стек трейсы в логах. Чтобы этого избежать, можно использовать «биективные» методы обфускации, которые позволяют вернуть код к оригинальному виду, что, впрочем, снижает целесообразность использования обфускации, поскольку такие методы облегчают анализ кода.