ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ

(МТУСИ)



Кафедра Информационной безопасности

Лабораторная работа №3

Выполнили студенты группы БВТ1904:

Игнатов Д.В.

Баскаева М.А.

Игнатенко Я.И.

Проверила:

Магомедова Д.И.­

*Москва,2020*

**Цель работы**

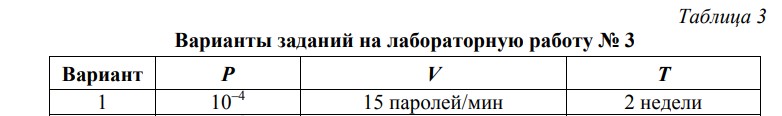
Получение основных теоретических сведений и практических навыков, по оценке стойкости парольной защиты.

**Постановка задачи**

В таблице 3 найти для вашего варианта значения характеристик

P, V, T.

1. Вычислить по формуле (2) нижнюю границу S\* для заданных P, V, T.
2. Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L, при котором выполняется условие (3).
3. Реализовать программу-генератор паролей пользователей. Программа должна формировать случайную последовательность символов длины L, при этом должен использоваться алфавит из A символов.



**Листинг программы**

double P, V, T;

try

{

P = Convert.ToDouble(P\_tb.Text);

V = Convert.ToDouble(V\_tb.Text);

T = Convert.ToDouble(T\_tb.Text);

}

catch (Exception e1) {

MessageBox.Show("Введены некоректные данные!");

return;

}

string engUP = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";

string englow = engUP.ToLower();

string rusUP = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

string ruslow = rusUP.ToLower();

string chars= "!\"#$%&\'()\*";

string numbers= "0123456789";

string alphabet = "";

int S = (int)Math.Ceiling(V \* T / P);

double A = 0, L = 0;

if (checkBox1.Checked) alphabet += engUP;

if (checkBox2.Checked) alphabet += englow;

if (checkBox3.Checked) alphabet += rusUP;

if (checkBox4.Checked) alphabet += ruslow;

if (checkBox5.Checked) alphabet += chars;

if (checkBox6.Checked) alphabet += numbers;

A = alphabet.Length;

if (A == 0) {

MessageBox.Show("Выбирете символы из которых должен состоять пароль!");

return;

}

while (S > Math.Pow(A, L)) {

L++;

}

S\_tb.Text = Convert.ToString(S);

A\_tb.Text = Convert.ToString(A);

L\_tb.Text = Convert.ToString(L);

string password = "";

Random rnd = new Random();

for (int i = 0; i < L; i++) {

password += alphabet[rnd.Next(alphabet.Length)];

}

password\_lb.Text = password;

**Результаты выполнения программы**

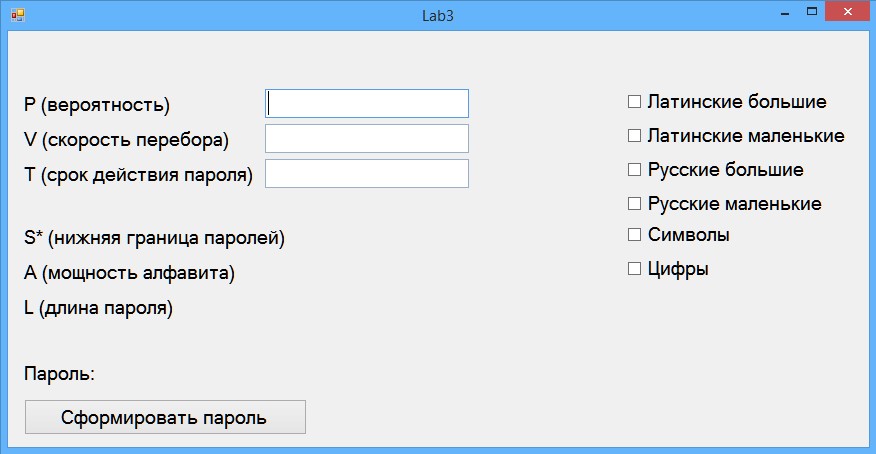


Рис 1. Финальный вид программы

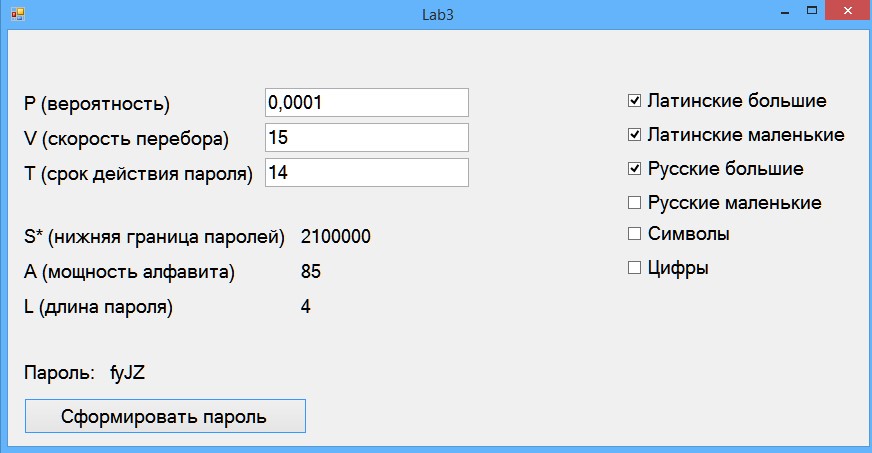


Рис 2. Генерация пароля

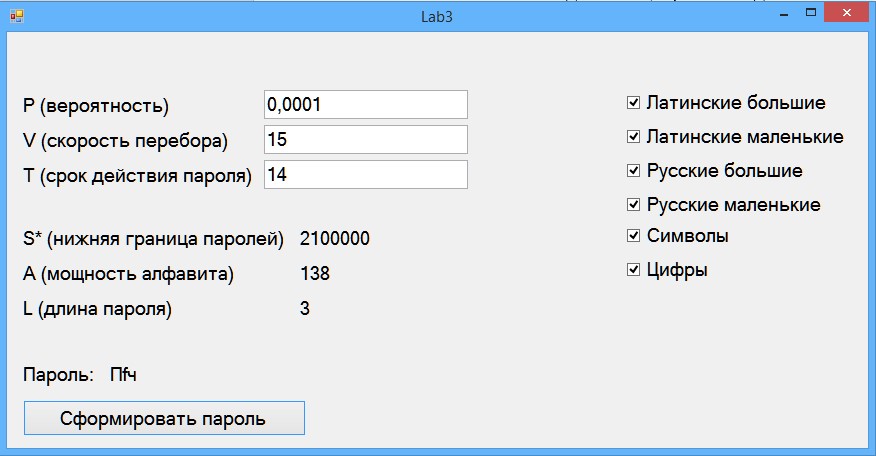


Рис 3. Генерация пароля с использованием большой мощности алфавита

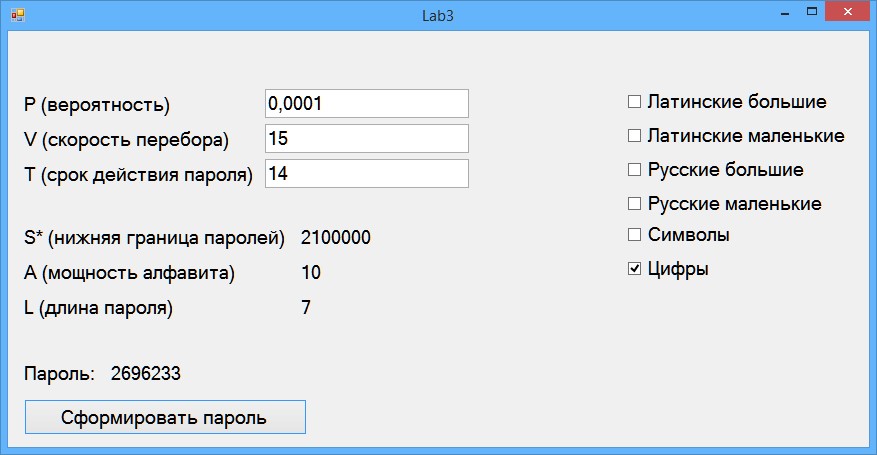


Рис 4. Генерация пароля только из цифр

**Контрольные вопросы**

**1) Дать определение стойкости пароля к взлому. Написать формулу.**

1. Стойкость пароля — мера оценки времени, которое необходимо затратить на угадывание пароля или его подбор каким-либо методом, например, методом полного перебора. Оценка того, как много попыток (времени) в среднем потребуется взломщику для угадывания пароля.  
Оценка стойкости парольных систем осуществляется по формуле:  
P = V\*T/S, S = A^L, где Здесь А - мощность алфавита паролей; L - длина пароля; S - мощность пространства паролей; V - скорость подбора паролей; T - срок действия пароля; Р - вероятность подбора пароля в течение его срока действия.

**2) Дать определение мощности алфавита паролей.**

Мощность алфавита паролей - количество символов, которые могут быть использованы при составлении пароля. Например, если пароль состоит только из малых английских букв, то A = 26.

**3) Перечислить основные задачи, которые могут решаться с использованием определения стойкости пароля.**

**4)Перечислить основные требования к выбору пароля.**

1. Минимальная длина пароля должна быть не менее 6 символов. Сокращение длины пароля во многом повышает вероятность успешной атаки полным их перебором.

2. Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы «(», «)», «#» и т. д.). Использование одной конкретной группы символов при формировании пароля в значительной степени повышает вероятность успешной атаки по маске.

3. В качестве пароля не должны использоваться реальные слова, имена, фамилии и т. д. Использование в качестве паролей конкретных слов, имен в значительной степени повышает вероятность успешной атаки по словарю.

**Заключение**

Итак, опираясь на результаты тестирования, можно сделать вывод что я получил основные теоретические сведения и практические навыки, по оценке стойкости парольной защиты.