Государственное учреждение образования

“БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ”

Кафедра: Интеллектуальных информационных технологий

Дисциплина: Средства и методы защиты информации в интеллектуальных системах

**Отчет по лабораторной работе №1**

**“Генерация паролей”**

Вариант 3

Выполнил:

студент гр.121702

Витковская С. И.

Проверил:

Сальников Д.А.

Минск 2023

**Содержание**

[**Цель: 3**](#_10zyi4g1nt1b)

[**Задача: 3**](#_gl8o1xw3chrw)

[**Ход работы: 3**](#)

[**Вывод: 5**](#_y0y3n1dghbe6)

#### **Цель**:

Получить навыки генерации пароля, изучить теоретические сведения о других методах аутентификации.

#### **Задача:**

1) Разработать программу, реализующую следующие функции:

–– генерация строки с заданной пользователем длиной, состоящей из символов алфавита в соответствии с вариантом задания: буквы русского языка строчные;

– поверка равномерности распределения символов путем визуализации частотного распределения;

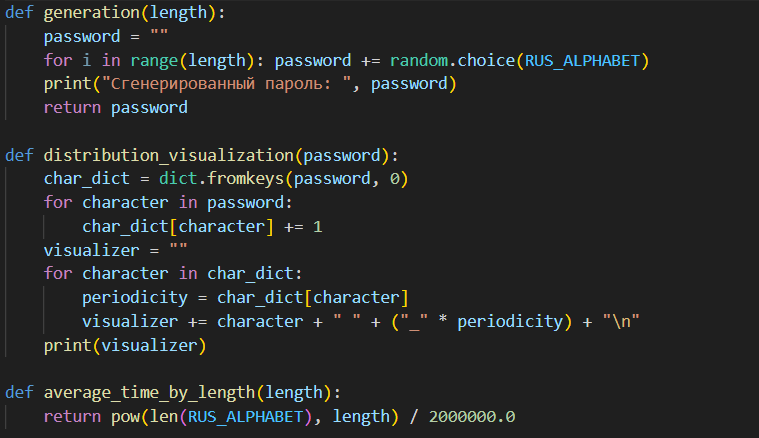
– вычисление среднего времени подбора пароля, выбираемого из сгенерированной строки.

2) Построить график зависимости среднего времени подбора пароля от его длины.

3) Дать практические рекомендации по выбору пароля исходя из предположений об алфавите пароля; ценности информации, доступ к которой защищается с помощью этого пароля; производительности вычислительного средства атакующего и времени атаки.

## **Ход работы:**

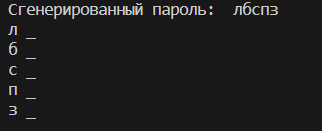
Задание 1:



Метод generation(length) генерирует пароль заданной пользователем длины, используя функцию choice пакета random для выбора символов из заданного алфавита:



Метод distribution\_visualization(password) используется для визуализации частотного распределения символов в пароле:



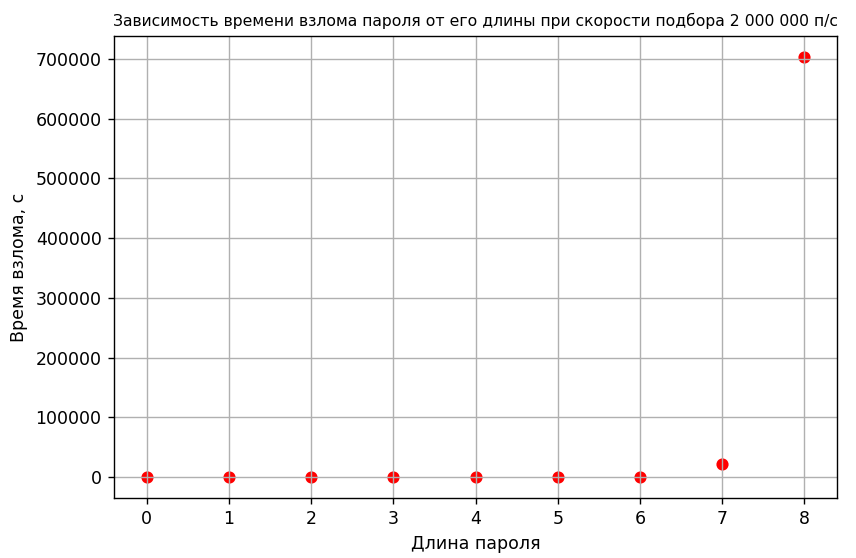
Метод average\_time\_by\_length(length) высчитывает время, которое потребуется для взлома пароля заданной длины, если скорость подбора наборов символов составляет 2 000 000 н/с.



Задание 2:



График строится для значений длины пароля в промежутке между 0 и n, задаваемым пользователем.



Задание 3:

Рекомендуется выбирать пароль с большей длинной символов или более длинным алфавитом, из которого строится пароль. В таком случае количество символов, которое необходимо перебрать злоумышленнику, будет возрастать, однако более высокая производительность оборудования злоумышленника увеличивает и скорость перебора. Так, например, используя алфавит русских строчных букв при скорости подбора паролей 2000000 н/с необходима длина пароля 11 символов для того, чтобы время полного перебора составляло около 800 лет.

Также рекомендуется использовать в качестве пароля рандомный набор символов, чтобы избежать взлома словарной атакой.

При высокой ценности информации следует подбирать гораздо более сложный пароль, а в идеальном случае использовать помимо пароля и другие средства защиты.

#### **Вывод**:

В результате выполнения лабораторной работы была написана программа генерации пароля задаваемой пользователем длины, на алфавите русский строчных букв, и была осуществлена проверка на среднее время взлома такого пароля, построен график данной зависимости на множестве увеличивающихся значений длин пароля. Были даны конкретные рекомендации по выбору пароля с учетом увеличения скорости подбора пароля при больших мощностях оборудования и ее уменьшении при большой длине пароля и(или) используемого алфавита.