

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования

«Сибирский государственный университет телекоммуникаций и информатики»

(СибГУТИ)

Кафедра (САПР)

09.03.02 (очная форма обучения)

ОТЧЕТ

по лабораторной работе №4.1

«Исследование параметров парольной защиты»

Выполнил:

Института Телекоммуникаций,

гр. ТТМ-21

«__» _____ 2023 г.

_____/ В.Р. Ланин/

(подпись)

Проверил:

Ст. преподаватель каф. САПР

«__» _____ 2023 г.

_____/А.А. Киселев/

(подпись)

Новосибирск 2023

Цель работы: знакомство с основными параметрами паролей, оценка и выбор оптимальных значений параметров.

Задание 1. Определить время перебора всех паролей с параметрами. Алфавит состоит из n символов.

алфавит	$n := 118$
длина пароля	$k := 9$
скорость перебора	$s := 50$
количество неверных паролей перед паузой	$m := 7$
длительность паузы	$v := 12$
количество вариантов	$C := n^k = 4.435 \times 10^{18}$
время перебора паролей	$t := \frac{C}{s} = 8.871 \times 10^{16}$
время перебора всех паролей	$T := \frac{t \cdot v}{m} = 1.521 \times 10^{17}$
Итоговое время	$T1 := t + T = 2.408 \times 10^{17}$
Лет	$T1 := \frac{T1}{3600 \cdot 24 \cdot 365} = 7.635 \times 10^9$

Задание 2. Определить минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет.

алфавит	$n2 := 118$
время перебора паролей	$t2 := 90$
скорость перебора	$s2 := 50$
количество вариантов	$C2 := t2 \cdot s2 \cdot 365 \cdot 24 \cdot 60 \cdot 60 = 1.419 \times 10^{11}$
длина пароля	$k2 := \log(C2, n2) = 5.383$

Задание 3. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет.

длина пароля	$k3 := 11$
время перебора паролей	$t3 := 90$
скорость перебора	$s3 := 50$
алфавит	$n3 := \sqrt[k3]{t3 \cdot s3 \cdot 360 \cdot 24 \cdot 60 \cdot 60} = 10.31$

Задание 4. У меня около 20 паролей, которые считаются сильными, меняю редко. Такая тактика не самая плохая, ведь если пароль сольют, это сильно не поможет для получения доступа к другим ресурсам, но из-за несменяемости могут быть проблемы.