

Министерство образования Республики Беларусь  
Учреждение образования  
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерного проектирования

Кафедра ИПиЭ

Дисциплина: Криптографические технологии

Отчет  
**по Лабораторной работе №5**  
на тему «Исследование методов идентификация и  
аутентификация пользователя. Протоколы рукопожатия и  
идентификации типа запрос-ответ»

Студент гр. 910902

Шпак В.А.

Проверил

Давыдович К.И.

Минск 2022

**Цель работы:** научиться определять время перебора всех паролей, минимальную длину пароля, а также подобрать пароль для архива с помощью специальной программы.

**Ход работы:**

**Задание 1.**

Вариант 5.

1. Определить время перебора всех паролей с параметрами.

$n = 59$  – количество символов алфавита

$k = 5$  – длина пароля

$s = 200$  – скорость перебора пароля в секунду

$m = 0$  – неправильно введенные пароли

$v = 0$  – пауза

Количество вариантов:  $C = 59^5$

Время перебора всех паролей:

$t = C/s = 3\,574\,621\text{с} = 59\,577\text{ мин} = 993\text{ ч} = 41\text{ день}.$

Время перебора всех паролей:

$T = t \cdot 0 = 0$

$T_{\text{итог}} = t + T = 41\text{ день}.$

2. Определить минимальную длину пароля

$n = 59$  - количество символов алфавита

$t = 50$  – время перебора

$s = 200$  – скорость перебора

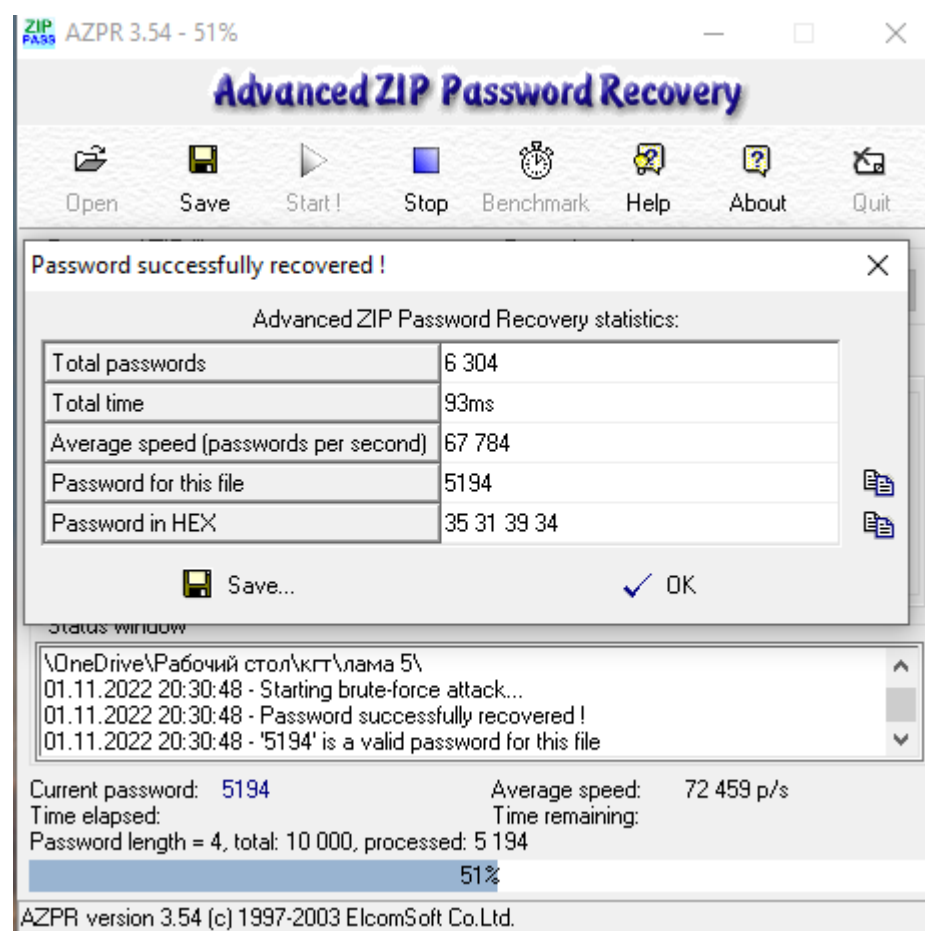
Количество вариантов:  $C = t \cdot s = 50 \cdot 200 = 10\,000 = 3.15 \cdot 10^4$

Длина пароля:  $k = \lg C = \lg(3.15 \cdot 10^4) = 4.5$

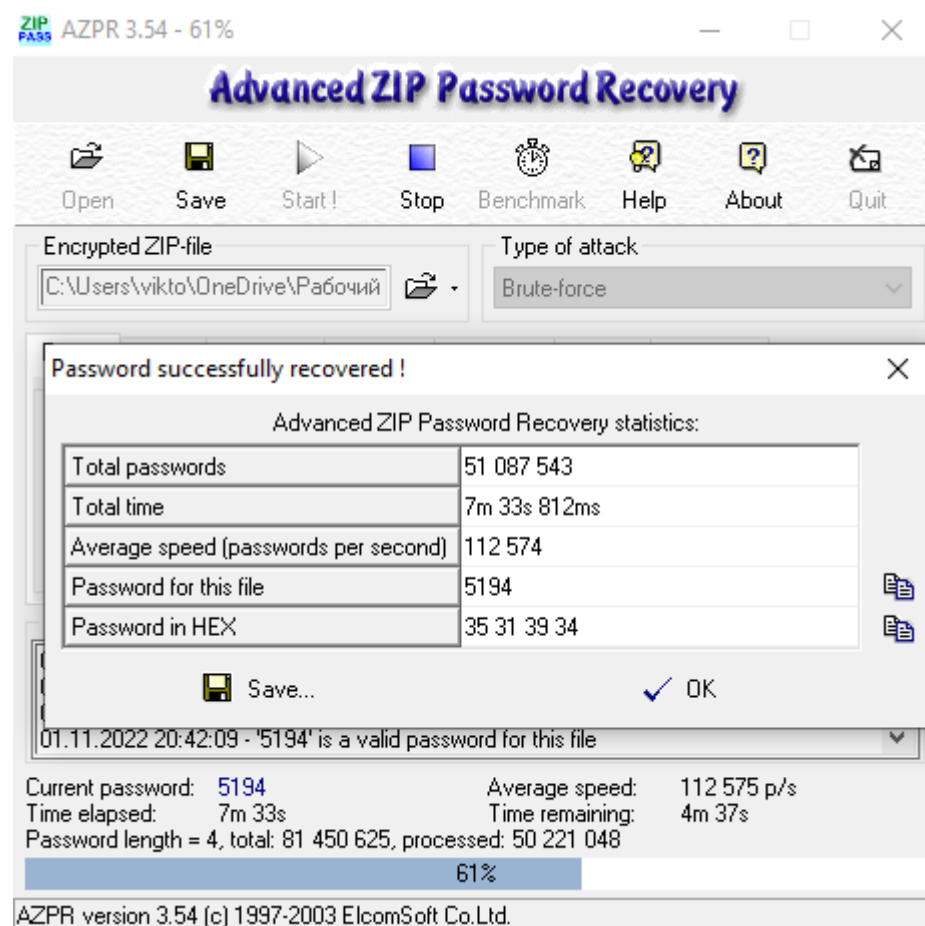
Длина пароля должна быть не менее 11 символов.

**Задание 2.**

Все цифры, длина 1-4



Все печатаемые.



## Перебор по маске.

ZIP PASS AZPR 3.54 - 61%

**Advanced ZIP Password Recovery**

Open Save Start! Stop Benchmark Help About Quit

Encrypted ZIP-file: C:\Users\wikto\OneDrive\Рабочий  
Type of attack: Mask

**Password successfully recovered !**

Advanced ZIP Password Recovery statistics:

Total passwords	50 221 048
Total time	8m 23s 305ms
Average speed (passwords per second)	99 782
Password for this file	5194
Password in HEX	35 31 39 34

Save... OK

01.11.2022 20:56:47 - Password successfully recovered !  
01.11.2022 20:56:47 - '5194' is a valid password for this file

Current password: 5194 Average speed: 99 784 p/s  
Time elapsed: 8m 23s Time remaining: 5m 12s  
Password length = 4, total: 81 450 625, processed: 50 221 048

61%

AZPR version 3.54 (c) 1997-2003 ElcomSoft Co.Ltd.

## Перебор по словарю.

ZIP PASS AZPR 3.54 - 100%

**Advanced ZIP Password Recovery**

Open Save Start! Stop Benchmark Help About Quit

Encrypted ZIP-file: C:\Users\wikto\OneDrive\Рабочий  
Type of attack: Dictionary

**Password not found**

Advanced ZIP Password Recovery statistics:

Total passwords	26 810
Total time	362ms
Average speed (passwords per second)	74 060
Password for this file	Not found
Password in HEX	Not found

Save... OK

01.11.2022 20:57:57 - Starting dictionary attack...  
01.11.2022 20:57:57 - Password not found

Current password: zygot Average speed: 76 381 p/s  
Time elapsed: Time remaining: 0s  
Dictionary attack in progress, processed 26 810 password(s)

100%

AZPR version 3.54 (c) 1997-2003 ElcomSoft Co.Ltd.

**Вывод:** таким образом, в ходе лабораторной работы мы научились определять время перебора всех паролей, минимальную длину пароля, а также подобрали пароль для архива с помощью специальной программы.