Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Пермский национальный** **исследовательский политехнический университет»**

Факультет: Прикладной математики и механики

Кафедра: Вычислительной математики, механики и биомеханики

Направление: 09.03.02 «Информационные системы и технологии»

Профиль бакалавриата: «Информационные системы и технологии»

**Отчет по лабораторной работе**

по дисциплине

«**Информационная безопасность и защита информации**»

Лабораторная работа

**«АНАЛИЗ УСТОЙЧИВОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ»**

Выполнил студент гр. ИСТ-17-1б

Мальцев К.А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О.)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*(подпись)*

**Принял (преподаватель по дисциплине):**

доцент Труфанов А. Н.

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(должность, ФИО)*

*\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(оценка) (подпись)*

*\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(дата)*

**Пермь, 2020**

**Цель работы:**

1. Изучение парольной системы аутентификации.
2. Получение практических навыков оценки устойчивости парольной защиты к атаке методом "полного перебора".

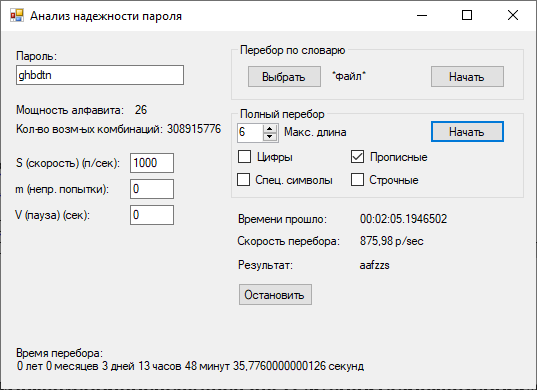


Рис. 1. Внешний вид программы в процессе полного перебора

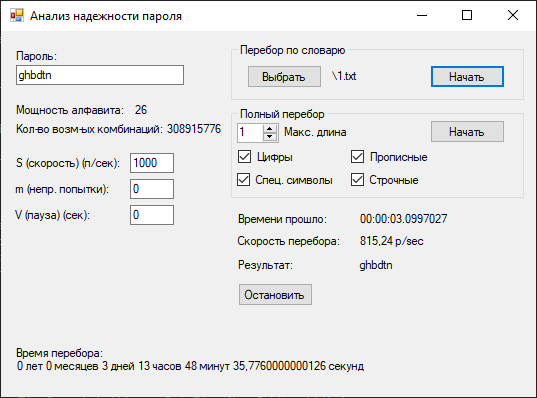


Рис. 2. Внешний вид программы в процессе перебора по словарю

Метод полного перебора осуществляет поиск нового пароля несколько быстрее по сравнению с методом перебора по словарю. Как видно на рисунках выше, в первом случае скорость перебора паролей составляет около 875 паролей в секунду, во втором – 815 паролей в секунду.

В качестве словаря для перебора был выбран частотный словарь русского языка.

Таким образом, если пользователь выбирает пароль символы которого соответствуют буквам часто используемого слова русского языка, метод подберет пароль, причем сделает это довольно быстро.

Метод полного перебора выполняет перебор быстрее, но вариантов паролей при данном переборе гораздо больше.

Исходя из этого, пользователю следует выбирать такой пароль, который не соответствует какому-либо существующему слову, особенно часто используемому, а также не является простым, благодаря чему может находиться в словарях подбора паролей, это поможет защититься от взлома перебором по словарю.

Защититься о метода полного перебора поможет выбор длинного пароля, с максимальной мощностью алфавита.

**Листинг кода**

https://github.com/opp2211/lab5