**БАЛТИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ «ВОЕНМЕХ» им. Д.Ф. Устинова**

**Кафедра O7**

**ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ № 1**

по учебной дисциплине **МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

на тему "Защита информации с помощью пароля "

Студент: Рахимбердиев Т. А.

Группа: И594

**ПРЕПОДАВАТЕЛЬ**

\_\_\_\_\_\_\_\_\_/Князьков А.В./

"\_\_\_\_"\_\_\_\_\_\_\_\_\_2022 г.

Санкт-Петербург  
2022 г.

Цель работы: исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль.

**Ход работы:**

Производим установку демоверсии программы **ARCHPR** на персональный компьютер.

**Проведение атаки с помощью перебора.**

1) Создаем текстовый файл, например, с именем «Name.doc», сохраняем его и архивируем в архив **ZIP**. В качестве пароля выбираем символы **veg1**.

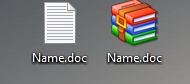


Рисунок 1- Создание файла и его архива

2) Установка пароли на архив

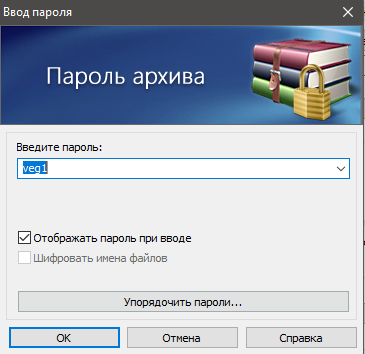


Рисунок 2 – Установка пароли “veg1” для архива

3) Проведение атаки на зашифрованный файл «Name.zip» с программой **ARCHPR**. С областью перебора «Все печатаемые символы».

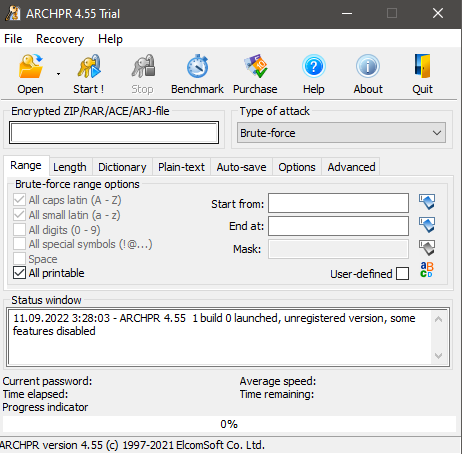


Рисунок 3 – установка области перебора «Все печатаемые символы»

4) Время выполнения атаки (для моего ПС) - 33 миллисекунд. Определен пароль ‘B@’.

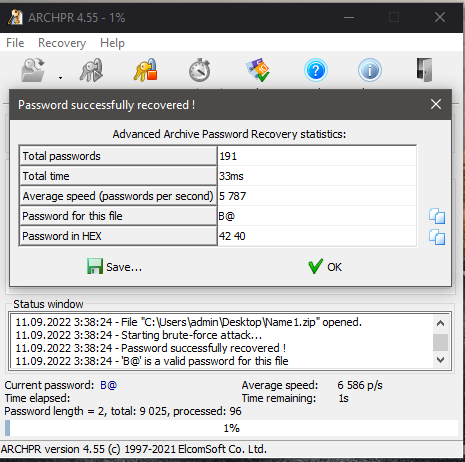


Рисунок 4 – Результат поиска

5) Открыт защищенный файл с помощью найденного программой пароля ‘B@’. Программа определила пароль правильно.

6) Сокращение области перебора до фактически используемого т.е. «Строчные латинские» и «Все цифры».

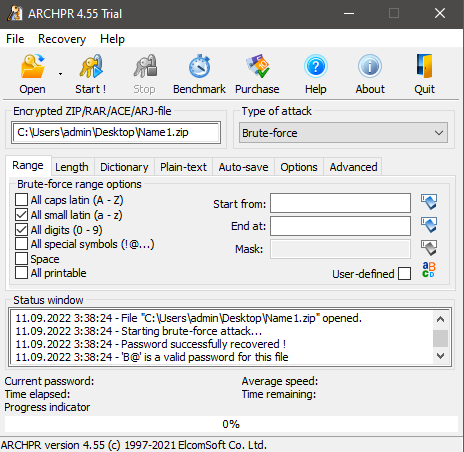


Рисунок 5 - установка области перебора «Строчные латинские» и «Все цифры»

7) Время выполнения атаки (для моего ПС) - 9 миллисекунд. Определен пароль ‘el’.

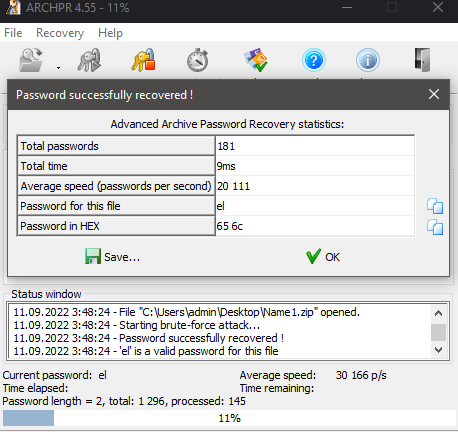


Рисунок 6 – Результат поиска

8) Открыт защищенный файл с помощью найденного программой за 9 миллисекунд с паролем ‘el’. Программа определила пароль правильно.

**Проведение атаки по словарю.**

9) Создание нового текстового файла «Name1.doc», с архивацией его в **ZIP**, с паролем **bear** и проведение атаки.

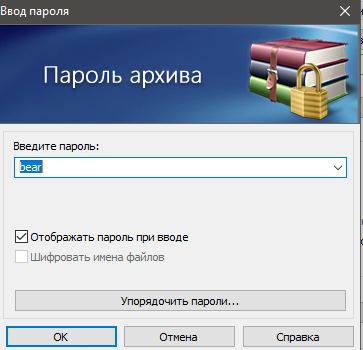


Рисунок 7 – дача пароля архиву

10) Время выполнения атаки (для моего ПС) – 11 миллисекунд.

Определен пароль **Gv**.

При проверке правильности пароля файл открылся, следовательно, пароль верный.

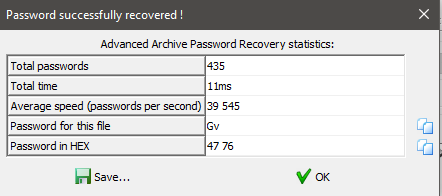


Рисунок 8 – результат поиска по словарю

**Сравнение атаки по словарю и с помощью перебора.**

11) Проведем атаку на файл «Name1.zip», в котором пароль все еще **bear**, с помощью перебора символов, выбрав «Все печатаемые» символы».

Время проведения атаки (для моего ПС) – 10 миллисекунд.

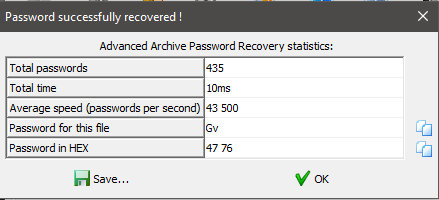


Рисунок 9 – результат поиска по всем печатаемым символам

12) Ограничение области перебора только «строчными латинскими».

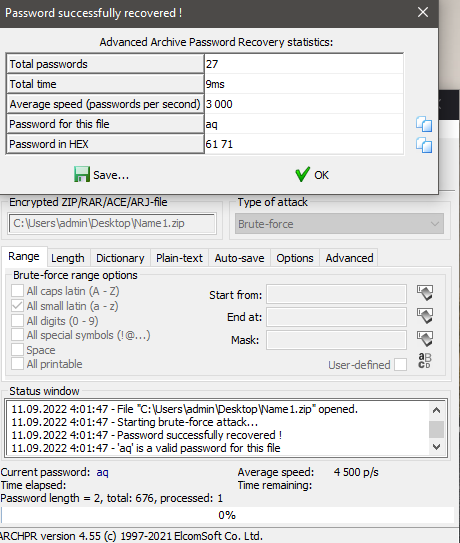


Рисунок 10 – результат поиска по всем строчным символам

Время проведения атаки (для моего ПС) – 9 миллисекунд.

**Создание более надежного пароля**

13) Создаем пароль, в котором нет слов, имеющихся в словаре, а также присутствуют цифры и различные символы (например – @, &, %, $ и др.) и используем и заглавные и строчные символы.

Область перебора устанавливаем «Все печатаемые символы» и «Все цифры».

Время выполнения атаки – (12 миллисекунд пароль: CW).

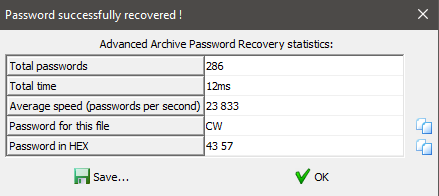
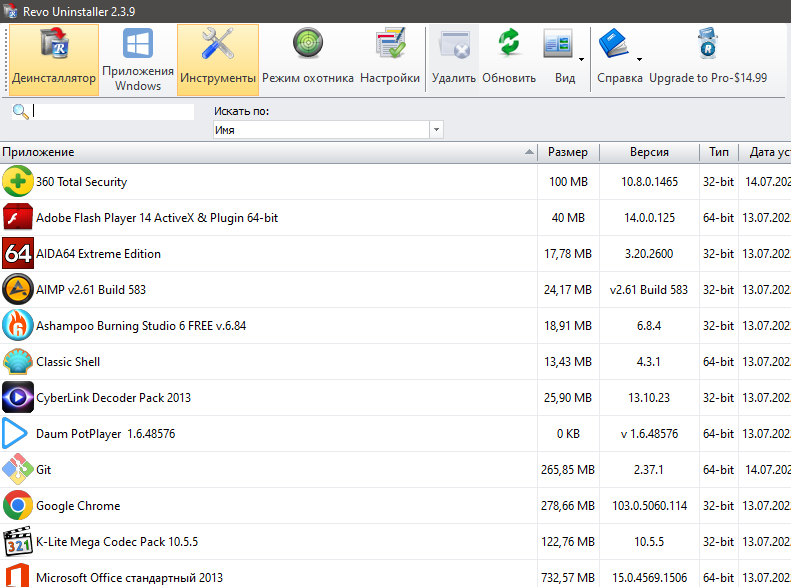


Рисунок 11 – результат поиска по всем строчным символам

Удаляем созданные в процессе работы файлы и архивы. Производим деинсталляцию программы **ARCHPR**.



**Выводы**

В данной практической работе была произведена атака на запароленый архив ZIP двумя способами – с помощью перебора и с помощью словаря.

Результат работы показал, что определение пароля с помощью словаря является более быстрым, чем перебором, если, конечно же, пароль является словом из словаря. Однако, перебирать слова только «строчными латинскими» оказалось быстрее, но для этого необходимо быть уверенным, что пароль включает в себя только таковые.

В конце работы становится очевидно, что для хорошей защиты информации следует использовать пароль, в котором нет слов, имеющихся в словаре, а также должны присутствовать цифры и различные символы (например – @, &, %, $ и др.). Для еще более безопасного пароля нужно использовать и заглавные и строчные символы.