Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Кубанский государственный технологический университет»

(ФГБОУ ВО «КубГТУ»)

Многоотраслевой институт подготовки и переподготовки специалистов (МИППС)

Факультет: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кафедра: информационных систем и программирования

Направление подготовки: 09.03.04 программная инженерия

Профиль: беспрофильный

Отчет к лабораторной работе №1

по дисциплине «Информационная безопасность»

Выполнила студентка

группы 16-ЗКБ-ПР1

Бочинский А.С.

Шифр: 13-КБ-ПРк-105

Краснодар

2020 г.

# Лабораторная работа № 1.

# Тема: «Защита информации с помощью пароля»

**Цель работы:**

1) Изучить виды атак на пароль и защиту ПО с применением пароля.

2) Приобрести умения и навыки противодействия атакам на пароль.

**Постановка задачи:**

**Проведение атаки перебором (bruteforce attack)**

1. Используя программу для вскрытия паролей произвести атаку на зашифрованный файл try\_me.rar (try\_me.arj, try\_me.zip – в зависимости от варианта). Область перебора – все печатаемые символы, длина пароля от 1 до 4 символов. Время выполнения на компьютере класса Pentium примерно 3-4 минуты. На компьютере класса Pentium II – 50 секунд. Проверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым.

2. Выполнив пункт 1, сократить область перебора до фактически используемого (например, если пароль 6D1A – то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

**Проведение атаки по словарю (dictionary attack)**

1. Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например, love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

2. Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.

**Результаты выполнения:**

Для выполнения поставленной задачи установим программу Advanced

ZIP Password Recovery. Главное окно программы изображено на Рисунке 1.

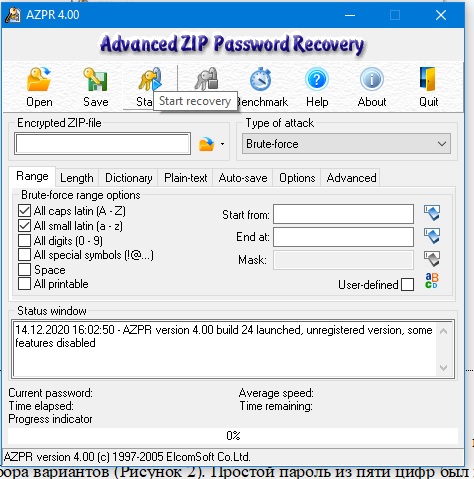


Рисунок 1 – Главное окно программы

Произведем подбор пароля к созданному rar архиву с помощью перебора вариантов (Рисунок 2). Простой пароль «alex» был вычислен за 178 мс.

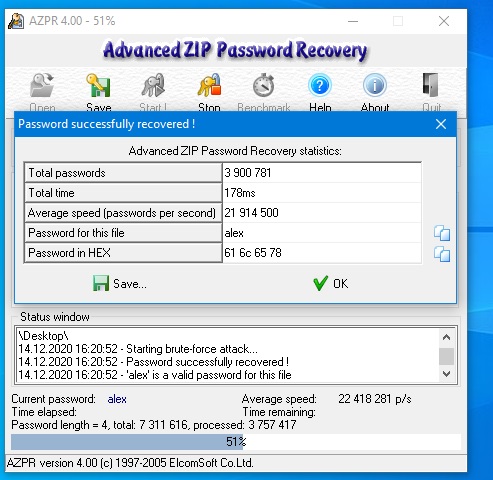


Рисунок 2 – Подбор пароля из пяти чисел

Для проверки попробуем использовать пароль из букв латинского алфавита, используя также цифры – «alex1988» - тем самым увеличив длину пароля на 4 символа. (Рисунок 3). Поиск занял больше времени, следовательно можно сделать вывод, что сложность пароля напрямую зависит от кол-ва символов.



Рисунок 3 – Подбор пароля из латинских букв с помощью перебора

Согласно второй части лабораторной работы, произведем подбор пароля к архиву с помощью метода атаки по словарю. В качестве слова-пароля выберем также слово «alex» (Рисунок 4). Как видно из рисунка, популярные слова так же не подходят в качестве пароля, так как подбор такого пароля занял ничтожные 9 мс.

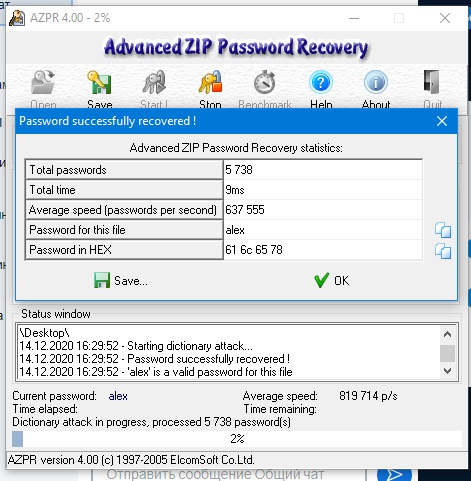


Рисунок 4 – Подбор пароля с помощью словаря

Вывод:

В результате выполнения данной лабораторной работы были изучены два вида атак на пароль, а также выявлены основные требования к созданию паролей.