МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования   
«Гомельский государственный университет имени Франциска Скорины»

Факультет физики и информационных технологий

Кафедра общей физики

Отчёт по теме

**«Защита информации с помощью пароля»**

Студент группы МС-22 : Пилипчук Е.Г.

Проверил: Соколов С.И.

Гомель 2023

Цель работы: Исследовать защиты с применением пароля, а также исследовать методы противодействия атакам на пароль

Проведем атаку перебором (bruteforce attack)

1. Создадим запароленный архив, используя программу WinRar, при этом

длина пароля должна составлять от 1 до 8 символов для различных алфавитов:

А) только английские малые буквы;

Создадим с паролем: asdfghjk

Б) только английские малые буквы и цифры;

Создадим с паролем: asd12er3

В) английские буквы большого и малого регистра и цифры.

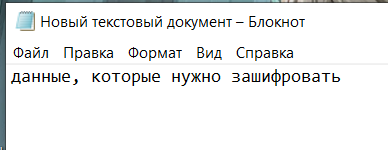
Создадим с паролем: Bs34fK2e

Используя программу для вскрытия паролей произведем атаку на

зашифрованный файл. Область перебора – английские буквы большого и малого

регистра и цифры, длина пароля от 1 до 8 символов.

Проверим правильность определенного пароля, распаковав файл и ознакомившись с его содержимым.



Как мы видим, содержимое не пострадало

2. Выполнив пункт 1, сократим область перебора до фактически

используемого (например, если пароль 6D1A – то выбрать прописные английские

буквы и цифры). Проведем повторное вскрытие и сравним затраченное время.

Время перебора сократилось.

3. Проведем анализ затраченного времени на взлом в зависимости от длины

пароля и алфавита.

Чем длиннее пароль и чем дальше буквы в нем к концу алфавита, тем больше время нужно на его подбор

Проведем атаки по словарю (dictionary attack)

1. Сожмем какой-либо небольшой файл, выбрав в качестве пароля английское

слово длиной до 5 символов (например, love, god, table, admin и т.д.) и проведем

атаку по словарю.

Выберем слово poppy.

2. Попытаем определить пароль методом прямого перебора. Сравним

затраченное время

Время потратили очень много.

Вывод: Исследовали защиты с применением пароля, а также исследовали методы противодействия атакам на пароль