МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования

«Гомельский государственный университет

имени Франциска Скорины»

Факультет физики и информационных технологий

Кафедра общей физики

Отчет по теме

**«ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ПАРОЛЯ»**

Студент группы МС-22 Перникова Ю.С.

Проверил:

Старший преподаватель

кафедры общей физики Соколов С. И.

Гомель, 2023

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

**Выполнение задания:**

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:

* Только английские буквы

Создадим пароль: jiklgvfq

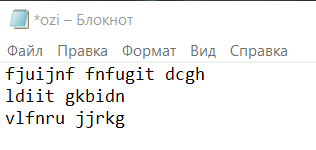
* Только английские малые буквы и цифры

Создадим пароль: bd4nk9lq

* английские буквы большого и малого регистра и цифры

Создадим пароль: gO7Vlk4x

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.



В. Выполнив пункт А, сократим область перебора до фактически используемого (например, если пароль H67E – то выбрать прописные английские буквы и цифры). Проведем повторное вскрытие и сравним затраченное время. Время перебора сократилось.

С. Проведем анализ затраченного времени на взлом в зависимости от длины пароля и алфавита. Чем длиннее пароль и чем буквы в нем ближе к концу алфавита, тем больше время нужно на его подбор.

Проведем атаки по словарю (dictionary attack)

А. Сожмем какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например, love, god, user, admin и т.д.) и проведем атаку по словарю. Выберем слово summa.

В. Попытаемся определить пароль методом прямого перебора. Сравним затраченное время. С помощью этого метода мы подобрали пароль намного быстрее чем через перебор.

**Вывод:** в ходе лабораторной работы мы исследовали защиты с применением пароля, а также исследовали методы противодействия атакам на пароль.