МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

федеральное государственное бюджетное образовательное учреждение высшего образования

**«Вологодский государственный университет»**

**Институт математики, естественных и компьютерных наук**

**Информатика и вычислительная техника**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5**

Количественная оценка стойкости парольной защиты.

Дисциплина: «Защита информации»

Направление подготовки: 09.03.01. Информатика и вычислительная техника

|  |  |
| --- | --- |
| Руководитель | Давыдова.Е.Н |
| Выполнили студенты | Пчелкина О.С. |
| Группа, курс | 4Б09 ВМ-41 4 курс |
| Дата сдачи | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата защиты | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись преподавателя)* |

Вологда

2023 г.

***Цель работы***: реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

**Задание на лабораторную работу**

5 вариант

1. В табл. 3 найти для указанного варианта значения характеристик *P, V, T*.

|  |  |  |  |
| --- | --- | --- | --- |
| Вариант | P | V | T |
| 5 | 10-4 | 100 паролей/день | 12 дней |

T=12/7,V=100\*24\*7=16800

1. Вычислить по формуле (1) нижнюю границу *S\** для заданных *P, V, T*.

S\*=(V\*T)/S=(16800\*12/7)/10^-4=288000000

1. Выбрать некоторый алфавит с мощностью *A* и получить минимальную длину пароля *L*, при котором выполняется условие *S*\* ≤ *S* = *AL*.

Подходит пароль мощностью 25 и длиной 6 символов.

288 000 000< 25^6

1. Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины *L*, при этом должен использоваться алфавит из *A* символов.

#Генератор паролей

import random

import string

сyrillic\_lowercase = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"

сyrillic\_uppercase = "абвгдеёжхийклмнопрстуфхцчшщъыьэюя"

length\_password = 6

power = 25

alf = list(string.ascii\_lowercase + string.ascii\_uppercase + string.digits + string.punctuation + сyrillic\_lowercase + сyrillic\_uppercase)

result = ""

random.shuffle(alf)

''.join(alf)

for i in range(length\_password):

    result += random.choice(alf[0:power])

print(result)

Пример работы



Вывод: в ходе лабораторной работы реализовали генератора паролей, обладающий требуемой стойкостью к взлому.

**Контрольные вопросы**

1. Стойкость подсистемы идентификации и аутентификации зависит от различных факторов, таких как сложность выбора пароля, применение методов шифрования и хэширования, контроль доступа к учетным записям, регулярное обновление паролей и обновление программных и аппаратных средств для обеспечения безопасности.

2. Минимальные требования к выбору пароля могут варьироваться в зависимости от конкретных политик безопасности, но общие требования могут включать в себя использование длинного пароля (не менее 8 символов), использование комбинации букв в верхнем и нижнем регистрах, цифр и специальных символов, и избегание использования личной информации (такой как дата рождения или имя) в пароле.

3. Минимальные требования к подсистеме парольной аутентификации могут включать в себя контроль длины и сложности пароля, контроль срока действия пароля, блокирование учетных записей после нескольких неудачных попыток входа, использование методов шифрования и хэширования для защиты пароля, и установка мер безопасности на уровне приложения и операционной системы для защиты пароля.

4. Вероятность подбора пароля злоумышленником в течение срока его действия зависит от сложности пароля, методов шифрования и хэширования, использованных для защиты пароля, скорости подбора, доступной злоумышленнику, и общего времени, затраченного на подбор пароля. Чем сложнее пароль и чем более безопасны методы шифрования и хэширования, тем меньше вероятность подбора

5.

Длина пароля. Чем длиннее пароль, тем сложнее его подобрать методом перебора. Рекомендуется использовать пароли длиной не менее 12 символов.

Сложность пароля. Пароль должен содержать различные типы символов, такие как заглавные и строчные буквы, цифры и специальные символы. Это усложняет задачу злоумышленнику при подборе пароля.

Использование двухфакторной аутентификации. Дополнительный уровень аутентификации, такой как код, отправляемый на мобильный телефон или использование биометрических данных, может уменьшить вероятность несанкционированного доступа даже в случае компрометации пароля.

Частота изменения пароля. Регулярное изменение пароля может предотвратить компрометацию пароля и уменьшить вероятность подбора пароля злоумышленником.

Использование утилит для генерации паролей. Использование специальных программ для генерации паролей может помочь создать сложные и надежные пароли, которые сложно подобрать методом перебора.