Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Уфимский государственный нефтяной технический университет»

Кафедра вычислительной техники и инженерной кибернетики

Лабораторная работа №1

по дисциплине Информационная безопасность

Количественная оценка стойкости парольной защиты

Вариант 25

Выполнил: студент гр. БПОи-16-01 Камалов К.И.

Проверил: кандидат технических наук, доцент Агишев Т.Х.

Уфа, 2019

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

**Порядок выполнения работы:**

1. Язык программирования – JavaScript
2. Исходные данные: паролей/мин дней.
3. По формуле вычислим нижнюю границу числа всевозможных паролей: паролей.
4. При формировании пароля могут быть использованы заглавные латинские буквы(заглавные), то есть мощность алфавита А=26

Рассчитаем минимальную длину пароля, исходя из следующего условия: .

, значит, минимальная длина пароля, удовлетворяющая условию равна 8.

Программа – генератор паролей пользователя:

var T = 12;

document.getElementById('T').innerHTML = T;

var V = 11 \* 60 \* 24 \* T;

document.getElementById('V').innerHTML = V;

var P = Math.pow(10, -4);

document.getElementById('P').innerHTML = P;

var S\_aster = Math.ceil(V \* T / P);

document.getElementById('S\*').innerHTML = S\_aster;

var A = 26;

document.getElementById('A').innerHTML = A;

var L = Math.ceil(Math.log(S\_aster)/Math.log(A));

document.getElementById('L').innerHTML = L;

var S = Math.pow(A, L);

document.getElementById('S').innerHTML = S;

document.getElementById('S\*<S').innerHTML = S\_aster <= S;

var password = "";

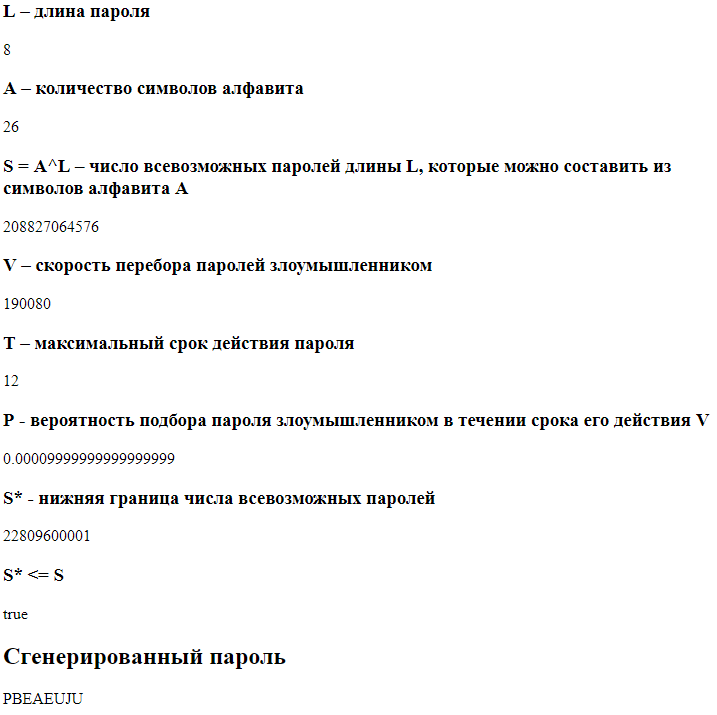
for (var i = 1; i <= L; i++) {

password += String.fromCharCode(randomIntFromInterval(65, 90));

}

document.getElementById('password').innerHTML = password;

Результаты работы программы:



**Ответы на контрольные вопросы:**

1. Чем определяется стойкость подсистемы идентификации и аутентификации?

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

1. Перечислить минимальные требования к выбору пароля.
   1. Минимальная длина пароля должна быть не менее 6 символов.
   2. Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.).
   3. В качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.
2. Перечислить минимальные требования к подсистеме парольной аутентификации.

3.1. Администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, он должен быть сменен.

3.2. В подсистеме парольной аутентификации должно быть установлено ограничение числа попыток ввода пароля (как правило, не более 3).

3.3. В подсистеме парольной аутентификации должна быть установлена временная задержка при вводе неправильного пароля.

1. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?

Вероятность *P* подбора пароля злоумышленником в течении срока его действия *V* определяется по следующей формуле:

где - длина пароля, – число возможных паролей длины , которые можно составить из символов алфавита , - скорость перебора паролей злоумышленником, – максимальный срок действия пароля.

1. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

Для уменьшения вероятности подбора пароля злоумышленником можно изменять длину пароля и используемый алфавит, то есть необходимо подобрать такие и , при которых следующее неравенство будет выполняться: .

**Выводы по работе:**

В ходе выполнения данной лабораторной работы были изучены подсистемы идентификации и аутентификации, также был создан генератор паролей, обладающий требуемой стойкостью к взлому.