ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ

(МТУСИ)



Кафедра Информационной безопасности

Лабораторная работа №1

Выполнили студенты группы БВТ1904:

Игнатов Д.В.

Баскаева М.А.

Игнатенко Я.И.

Проверила:

Магомедова Д.И.­

*Москва,2020*

**Цель работы**

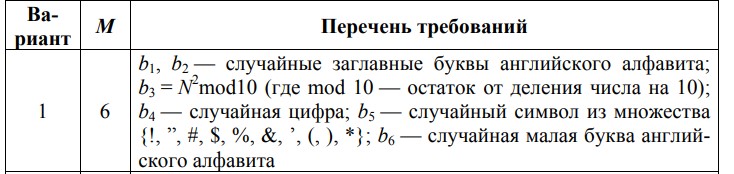
Получение основных теоретических сведений и практических навыков, по оценке стойкости парольной защиты.

**Постановка задачи**

Реализовать простейший генератор паролей, обладающий основными требованиями к парольным генераторам.

Программа должна выполнять следующие действия.

1. Ввод идентификатора пользователя с клавиатуры. Данный идентификатор представляет собой последовательность символов a1, a2, ..., aN, где N — количество символов идентификатора (может быть любым), ai — i-й символ идентификатора пользователя.
2. Формирование пароля пользователя b1, b2, ..., bM для данного идентификатора, где M — количество символов пароля, соответствующее вашему варианту и вывод его на экран. Алгоритм получения символов пароля bi указан в перечне требований для вашего варианта



**Листинг программы**

Random rnd = new Random();

string alphabet = "!\"#$%&\'()\*";

result\_pass.Text = ""+   
((char)rnd.Next('\u0041', '\u005A')) +   
((char)rnd.Next('\u0041', '\u005A')) + Convert.ToString((id\_tb.Text.Length\* id\_tb.Text.Length) % 10) + Convert.ToString(rnd.Next(10)) +   
alphabet[rnd.Next(alphabet.Length)] + (char)rnd.Next('\u0061', '\u007A');

**Результаты выполнения программы**

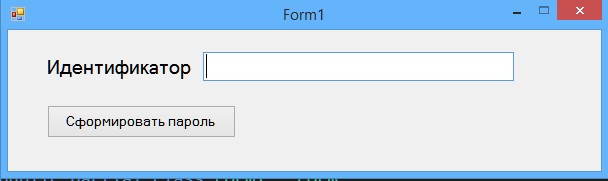


Рис 1. Финальный вид программы

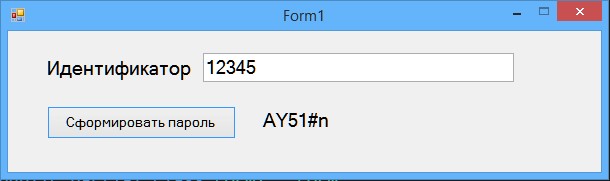


Рис 2. Генерация пароля

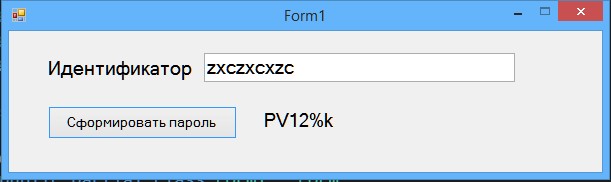


Рис 3. Генерация пароля

**Контрольные вопросы**

**1) Дать определение стойкости пароля к взлому. Написать формулу.**

1. Стойкость пароля — мера оценки времени, которое необходимо затратить на угадывание пароля или его подбор каким-либо методом, например, методом полного перебора. Оценка того, как много попыток (времени) в среднем потребуется взломщику для угадывания пароля.  
Оценка стойкости парольных систем осуществляется по формуле:  
P = V\*T/S, S = A^L, где Здесь А - мощность алфавита паролей; L - длина пароля; S - мощность пространства паролей; V - скорость подбора паролей; T - срок действия пароля; Р - вероятность подбора пароля в течение его срока действия.

**2) Дать определение мощности алфавита паролей.**

Мощность алфавита паролей - количество символов, которые могут быть использованы при составлении пароля. Например, если пароль состоит только из малых английских букв, то A = 26.

**3) Перечислить основные задачи, которые могут решаться с использованием определения стойкости пароля.**

**4)Перечислить основные требования к выбору пароля.**

1. Минимальная длина пароля должна быть не менее 6 символов. Сокращение длины пароля во многом повышает вероятность успешной атаки полным их перебором.

2. Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы «(», «)», «#» и т. д.). Использование одной конкретной группы символов при формировании пароля в значительной степени повышает вероятность успешной атаки по маске.

3. В качестве пароля не должны использоваться реальные слова, имена, фамилии и т. д. Использование в качестве паролей конкретных слов, имен в значительной степени повышает вероятность успешной атаки по словарю.

**Заключение**

Итак, опираясь на результаты тестирования, можно сделать вывод что мы получили основные теоретические сведения и практические навыки, по оценке стойкости парольной защиты.