3. ЛАБОРАТОРНАЯ РАБОТА № 3. КОЛИЧЕСТВЕННАЯ ОЦЕНКА СТОЙКОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ

Цель работы: получение основных теоретических сведений и практических навыков по оценке стойкости парольной защиты.

3.1. Ход работы

1. Ознакомиться с теоретической частью данной работы.
2. Реализовать простейший генератор паролей, обладающий требуемой стойкостью к взлому.
3. Составить отчет по проделанной работе.
4. Защитить работу.

3.2. Содержание отчета

1. Тема.
2. Цель работы.
3. Ход работы.
4. Постановка задачи.
5. Листинг программы.
6. Результат выполнения программы.

3.3. Теоретическая справка

Пусть A — мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля. Например, если пароль состоит только из малых английских букв, то $A = 26$).

L — длина пароля, $S = A^L$ — число всевозможных паролей длины L, которые можно составить из символов алфавита A, V — скорость перебора паролей злоумышленником, T — максимальный срок действия пароля.

Тогда вероятность подбора пароля P злоумышленником в течении срока его действия V определяется по формуле

$$P = \frac{VT}{S} = \frac{VT}{A^L}. \quad (1)$$

Эту формулу можно использовать в обратную сторону для решения следующей задачи: определить минимальные мощность алфавита паролей A и длину паролей L , обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Данная задача имеет неоднозначное решение. При исходных данных *V, T, P* однозначно можно определить лишь нижнюю границу S^* числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле

$$S^* = \left\lceil \frac{VT}{P} \right\rceil, \quad (2)$$

где [] — целая часть числа, взятая с округлением вверх.

После нахождения нижней границы S^* необходимо выбрать такие *A* и *L* для формирования $S = A^L$, чтобы выполнялось неравенство

$$S^* \le S = A^L. \quad (3)$$

При выборе *S*, удовлетворяющего неравенству (3), вероятность подбора пароля злоумышленника (при заданных *V* и *T*) будет меньше, чем заданная *P*.

Необходимо отметить, что при осуществлении вычислений по формулам (2) и (3), величины должны быть приведены к одним размерностям.

3.4. Задание к лабораторной работе № 3

В таблице 3 найти для вашего варианта значения характеристик *P, V, T*.

1. Вычислить по формуле (2) нижнюю границу S^* для заданных *P, V, T*.

2. Выбрать некоторый алфавит с мощностью *A* и получить минимальную длину пароля *L*, при котором выполняется условие (3).

3. Реализовать программу-генератор паролей пользователей. Программа должна формировать случайную последовательность символов длины *L*, при этом должен использоваться алфавит из *A* символов.

Таблица 3

Варианты заданий на лабораторную работу № 3

Вариант	*P*	*V*	*T*
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 пароля/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10^{-4}	3 пароля/мин	15 дней

Продолжение табл. 3

Вариант	*P*	*V*	*T*
10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
13	10^{-4}	10 паролей/мин	3 недели
14	10^{-5}	11 паролей/мин	20 дней
15	10^{-6}	100 паролей/день	15 дней
16	10^{-7}	10 паролей/день	1 неделя
17	10^{-4}	20 паролей/мин	2 недели
18	10^{-5}	15 паролей/мин	10 дней
19	10^{-6}	3 пароля/мин	5 дней
20	10^{-7}	10 паролей/мин	6 дней
21	10^{-4}	11 паролей/мин	12 дней
22	10^{-5}	100 паролей/день	1 месяц
23	10^{-6}	10 паролей/день	3 недели
24	10^{-7}	20 паролей/мин	20 дней
25	10^{-4}	15 паролей/мин	15 дней
26	10^{-5}	3 пароля/мин	1 неделя

3.5. Пример реализации лабораторной работы

На рисунке 5 показан пример реализации программы по генерированию паролей с заданными требованиями. Входными параметрами являются:

— вероятность подбора пароля злоумышленником;
— скорость перебора паролей;
— срок действия пароля;
— используемый алфавит.

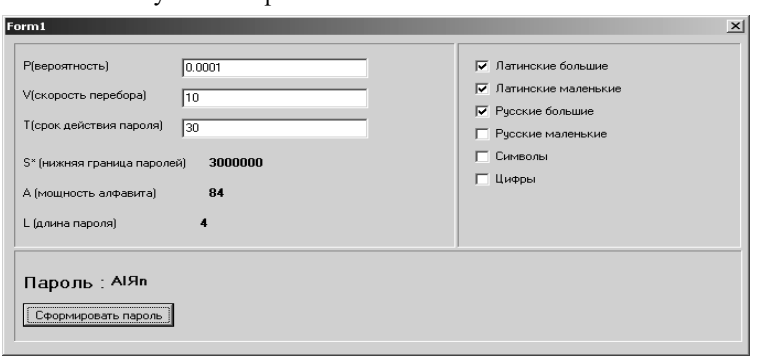

Рис. 5

Результат работы программы, реализующей простейший генератор с заданными требованиями

На выходе получаем сгенерированный пароль, обладающий требуемой стойкостью к взлому.

Контрольные вопросы

1. Дать определение стойкости пароля к взлому. Написать формулу.
2. Дать определение мощности алфавита паролей.
3. Перечислить основные задачи, которые могут решаться с использованием определения стойкости пароля.
4. Перечислить основные требования к выбору пароля.