

## КОЛИЧЕСТВЕННАЯ ОЦЕНКА СТОЙКОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ

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

### Теоретические сведения

Подсистемы идентификации и аутентификации пользователя играют важную роль в системах защиты информации.

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.

Парольные системы идентификации/аутентификации являются одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя, как правило, передний край обороны СЗИ. В связи с этим модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель последнего в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя наиболее просты и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю:

- 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.

К подсистеме парольной аутентификации:

- 1) администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, пароль следует сменить;
- 2) в подсистеме парольной аутентификации необходимо установить ограничение числа попыток ввода пароля (как правило, не более трёх);
- 3) в подсистеме парольной аутентификации требуется установить временную задержку в случае ввода неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

### Количественная оценка стойкости парольной защиты

Пусть  $A$  – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля: 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  $P$  подбора пароля злоумышленником в течение срока его действия  $V$  определяется по следующей формуле:

$$P = (V \cdot T) / S = (V \cdot T) / A^L.$$

Эту формулу можно использовать в обратную сторону для решения следующей задачи.

**Задача.** 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 следующей формуле

$$S^* = \left\lceil \frac{V \cdot T}{P} \right\rceil \quad (1)$$

где  $\lceil \cdot \rceil$  – 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 (2).

$$S^* \leq S = A^L \quad (2)$$

При выборе  $S$ , удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных  $V$  и  $T$ ) будет меньше, чем заданная  $P$ .

Необходимо отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

Пример

Исходные данные –  $P = 10^{-6}$ ,  $T = 7$  дней = 1 неделя,  $V = 10$  паролей / минуту =  $10 \cdot 60 \cdot 24 \cdot 7 = 100800$  паролей в неделю.

$$S^* = \left\lceil \frac{100800 \cdot 1}{10^{-6}} \right\rceil = 1008 \cdot 10^8$$

Тогда,

Условию  $S^* \leq A^L$  удовлетворяют, например, такие комбинации  $A$  и  $L$ , как  $A = 26$ ,  $L = 8$  (пароль состоит из 8 малых символов английского алфавита),  $A = 36$ ,  $L = 6$  (пароль состоит из 6 символов, среди которых могут быть малые латинские буквы и произвольные цифры).

### Задание на лабораторную работу

1. В табл. 3.1 найти для указанного варианта значения характеристик  $P$ ,  $V$ ,  $T$ .
2. Вычислить по формуле (1) нижнюю границу  $S^*$  для заданных  $P$ ,  $V$ ,  $T$ .
3. Выбрать некоторый алфавит с мощностью  $A$  и получить минимальную длину пароля  $L$ , при котором выполняется условие (2).
4. Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины  $L$ , при этом должен использоваться алфавит из  $A$  символов. Параметры  $L$  и  $A$  – могут меняться пользователями в программе, но соблюдается условие (2).
5. Реализовать в программе возможность взлома сгенерированного пароля (с помощью прямого перебора паролей) или любым другим алгоритмом. Оценить время взлома пароля и количество перебранных вариантов пароля. Определить границы времени, при котором пароль считается не взломанным.
6. Оформить отчет по лабораторной работе. Отрастить в отчете зависимость взлома паролей от  $L$  и  $A$ .

Коды символов:

1. Коды английских символов : «А» = 65, ..., «Z» = 90, «a» = 97,..., «z» = 122.
2. Коды цифр : «0» = 48, «9» = 57.
3. «!» = 33, «“» = 34, «#» = 35, «\$» = 36, «%» = 37, «&» = 38, «‘» = 39.
4. Коды русских символов : «А» – 128, ... «Я» – 159, «а» – 160,..., «п» – 175, «р» – 224,..., «я» – 239.

**Таблица 3.1. Варианты заданий**

Вариант	$P$	$V$	$T$	Используемые группы символов пароля
1	$10^{-4}$	15 паролей/мин	2 недели	1. Цифры (0-9) 2. Латинские строчные буквы (a-z)
2	$10^{-5}$	3 паролей/мин	10 дней	1. Латинские прописные буквы (A-Z) 2. Русские строчные буквы (а-я)
3	$10^{-6}$	10 паролей/мин	5 дней	1. Русские прописные буквы (А-Я) 2. Специальные символы.
4	$10^{-7}$	11 паролей/мин	6 дней	1. Цифры (0-9) 2. Латинские прописные буквы (A-Z)
5	$10^{-4}$	100 паролей/день	12 дней	1. Русские прописные буквы (А-Я) 2. Латинские строчные буквы (a-z)
6	$10^{-5}$	10 паролей/день	1 месяц	1. Русские строчные буквы (а-я) 2. Специальные символы.
7	$10^{-6}$	20 паролей/мин	3 недели	1. Цифры (0-9) 2. Русские строчные буквы (а-я)
8	$10^{-7}$	15 паролей/мин	20 дней	1. Латинские строчные буквы (a-z) 2. Латинские прописные буквы (A-Z)
9	$10^{-4}$	3 паролей/мин	15 дней	1. Русские прописные буквы (А-Я) 2. Русские строчные буквы (а-я)
10	$10^{-5}$	10 паролей/мин	1 неделя	1. Цифры (0-9) 2. Специальные символы.
11	$10^{-6}$	11 паролей/мин	2 недели	1. Цифры (0-9) 2. Русские прописные буквы (А-Я)
12	$10^{-7}$	100 паролей/день	10 дней	1. Латинские строчные буквы (a-z) 2. Русские прописные буквы (А-Я)
13	$10^{-4}$	10 паролей/день	5 дней	1. Цифры (0-9) 2. Латинские строчные буквы (a-z)
14	$10^{-5}$	20 паролей/мин	6 дней	1. Латинские прописные буквы (A-Z) 2. Русские строчные буквы (а-я)
15	$10^{-6}$	15 паролей/мин	12 дней	1. Русские прописные буквы (А-Я) 2. Специальные символы.
16	$10^{-7}$	3 паролей/мин	1 месяц	1. Цифры (0-9) 2. Латинские прописные буквы (A-Z)
17	$10^{-4}$	10 паролей/мин	3 недели	1. Русские прописные буквы (А-Я) 2. Латинские строчные буквы (a-z)
18	$10^{-5}$	11 паролей/мин	20 дней	1. Русские строчные буквы (а-я) 2. Специальные символы.
19	$10^{-6}$	100 паролей/день	15 дней	1. Цифры (0-9) 2. Русские строчные буквы (а-я)
20	$10^{-7}$	10 паролей/день	1 неделя	1. Латинские строчные буквы (a-z) 2. Латинские прописные буквы (A-Z)
21	$10^{-4}$	20 паролей/мин	2 недели	1. Русские прописные буквы (А-Я) 2. Русские строчные буквы (а-я)
22	$10^{-5}$	15 паролей/мин	10 дней	1. Цифры (0-9) 2. Специальные символы.
23	$10^{-6}$	3 паролей/мин	5 дней	1. Цифры (0-9) 2. Русские прописные буквы (А-Я)
24	$10^{-7}$	10 паролей/мин	6 дней	1. Латинские строчные буквы (a-z) 2. Русские прописные буквы (А-Я)
25	$10^{-4}$	11 паролей/мин	12 дней	1. Цифры (0-9) 2. Латинские строчные буквы (a-z)
26	$10^{-5}$	100 паролей/день	1 месяц	1. Латинские прописные буквы (A-Z)

				2. Русские строчные буквы (а-я)
27	$10^{-6}$	10 паролей/день	3 недели	1. Русские прописные буквы (А-Я) 2. Специальные символы.
28	$10^{-7}$	20 паролей/мин	20 дней	1. Цифры (0-9) 2. Латинские прописные буквы (А-Z)
29	$10^{-4}$	15 паролей/мин	15 дней	1. Русские прописные буквы (А-Я) 2. Латинские строчные буквы (а-z)
30	$10^{-5}$	3 паролей/мин	1 неделя	1. Русские строчные буквы (а-я) 2. Специальные символы.

### Контрольные вопросы

1. Чем определяется стойкость подсистемы идентификации и аутентификации?
2. Перечислить минимальные требования к выбору пароля.
3. Перечислить минимальные требования к подсистеме парольной аутентификации.
4. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?
5. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?