# Лабораторная работа

# 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 = AL* – 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 ∙ T*) */ S =* (*V ∙ T*) */ AL*.

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 формуле

*S*\* = [*V ∙ P / T*], (1)

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

После определения нижней границы *S\** необходимо выбрать такие *A* и *L* для формирования *S = AL*, чтобы выполнялось следующее неравенство:

*S*\* ≤ *S* = *AL*. (2)

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

Следует 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 · 60·24·7 = 100800 паролей в неделю. Тогда, S\* = [(10800 ∙ 1) / 10-6] = = 108 ∙ 108.

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

**Задание на лабораторную работу**

1. В табл. 3 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.

5. Оформить отчет по лабораторной работе.

Коды символов:

1. Коды английских символов : «A» = 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. Варианты заданий**

|  |  |  |  |
| --- | --- | --- | --- |
| Вариант | *P* | *V* | *T* |
| 1 | 10-4 | 15 паролей/мин | 2 недели |
| 2 | 10-5 | 3 паролей/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 паролей/мин | 15 дней |
| 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/день | 5 дней |
| 14 | 10-5 | 20 паролей/мин | 6 дней |
| 15 | 10-6 | 15 паролей/мин | 12 дней |
| 16 | 10-7 | 3 паролей/мин | 1 месяц |
| 17 | 10-4 | 10 паролей/мин | 3 недели |
| 18 | 10-5 | 11 паролей/мин | 20 дней |
| 19 | 10-6 | 100 паролей/день | 15 дней |
| 20 | 10-7 | 10 паролей/день | 1 неделя |
| 21 | 10-4 | 20 паролей/мин | 2 недели |
| 22 | 10-5 | 15 паролей/мин | 10 дней |
| 23 | 10-6 | 3 паролей/мин | 5 дней |
| Окончание табл. 3 | | | |
| Вариант | *P* | *V* | *T* |
| 24 | 10-7 | 10 паролей/мин | 6 дней |
| 25 | 10-4 | 11 паролей/мин | 12 дней |
| 26 | 10-5 | 100 паролей/день | 1 месяц |
| 27 | 10-6 | 10 паролей/день | 3 недели |
| 28 | 10-7 | 20 паролей/мин | 20 дней |
| 29 | 10-4 | 15 паролей/мин | 15 дней |
| 30 | 10-5 | 3 паролей/мин | 1 неделя |

**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?