КІЛЬКІСНА ОЦІНКА СТІЙКОСТІ ПАРОЛЯ

Мартиць Д.С., *vsp-mk-tdatu@ukr.net*

ВСП «Мелітопольський коледж ТДАТУ»

Стійкість підсистеми ідентифікації та автентифікації користувача в системі захисту інформації (СЗІ) багато в чому визначає стійкість до злому самої СЗІ. Дана стійкість визначається гарантією того, що зловмисник не зможе пройти автентифікацію.

Основним захисним кордоном проти зловмисних атак є система парольного захисту, яка є у всіх сучасних програмних продуктах. Відповідно до встановленої практики, перед початком сеансу роботи з операційною системою користувач зобов'язаний зареєструватися, повідомивши їй своє ім'я та пароль. Ім'я потрібно для ідентифікації користувача, а пароль служить підтвердженням правильності виробленої ідентифікації. Інформація, введена користувачем в діалоговому режимі, порівнюється з тією, що є у розпорядженні операційної системи. Якщо перевірка дає позитивний результат, то користувачеві стають доступні всі ресурси операційної системи, пов'язані з його ім'ям.

Основні вимоги до вибору пароля:

- мінімальна довжина пароля повинна бути не менше 6 символів;
- він має містити з різних груп символів (малі і великі латинські літери, цифри, спеціальні символи '(', ')', '#' та ін.);
- в якості пароля не повинні використовуватися реальні слова, імена, прізвища й т.д.

Основні вимоги до підсистеми парольної автентифікації:

- адміністратор СЗІ повинен встановлювати максимальний термін дії пароля, після чого, він повинен бути змінений;
- у підсистемі парольної автентифікації повинно бути встановлено обмеження числа спроб введення пароля (як правило, не більше 3);
- у підсистемі парольної автентифікації повинна бути встановлена тимчасова затримка при введенні неправильного пароля.

При виконанні перерахованих вимог до паролів і до підсистеми парольної автентифікації єдино можливим методом злому даної підсистеми зловмисником є прямий перебір паролів (brute forcing).

У процесі дослідження систем захисту інформації було визначено основні вимоги щодо парольної автентифікаії. Приведено формулу для розрахунку ймовірності підбору пароля. Згідно основних вимог була розроблена програма, що генерує паролі користувачів. Взаємодія програми з користувачем здійснюється за допомогою графічного інтерфейсу.

Список використаних джерел.

1. Кількісна оцінка стійкості парольного захисту / https://pandia.ru/text/80/242/30241.php.
2. Принципи захисту інформації / https://www.myunivercity.com/SystemPass.html.
3. Ідентифікація та автентифікація / https://sites.google.com/site/ identifikaciata-autentifikacia/ponatta-pro-autentifikaciu/parolna-autentifikacia.

Керівник Бабенко Н.М., викладач