

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ,
МЕХАНИКИ И ОПТИКИ»**

Факультет информатики и вычислительной техники

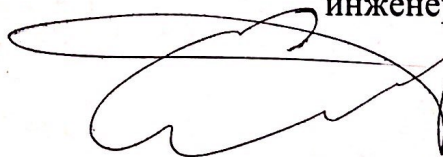
Дисциплина:
«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

Выполнил:
Студент гр. Р3231
Кислицин Алексей Андреевич



Проверил:
Есипов Дмитрий Андреевич,
инженер ФБИТ



Санкт-Петербург
2022г.

Цель: разработка подсистемы идентификации и аутентификации субъектов.

Задачи:

1. Составить алгоритм для реализации выбранной подсистемы.
2. Составить полную схему компьютерной системы со встроенной в неё подсистемой идентификации и аутентификации.

Конспект:

В парольных системах идентификации и аутентификации пользователей, информацией, аутентифицирующей пользователя, является его личный секретный пароль.

Так как парольные системы могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику, то парольные системы являются самыми привлекательными объектами атаки.

Основные типы угроз:

1. Перебор паролей в интерактивном режиме
2. Подсмотр пароля
3. Преднамеренная передача пароля его владельцем другому лицу.
4. Кража базы данных учётных записей с дальнейшим её анализом, подбором пароля.
5. Перехват вводимого пароля путём внедрения в КС программных закладок (клавиатурных шпионов); перехват пароля, передаваемого по сети.
6. Социальная инженерия.

Чтобы минимизировать влияние человеческого фактора необходимо установить правила для выбора пароля. Эти правила:

1. Задание минимальной длины пароля
2. Использование в пароле различных групп символов
3. Проверка и отбраковка пароля по словарю
4. Установление максимального срока действия пароля
5. Применение эвристического алгоритма, бракующего «плохие» пароли
6. Ограничение числа попыток ввода пароля
7. Использование задержки при вводе неправильного пароля
8. Поддержка режима принудительной смены пароля пользователя
9. Запрет на выбор пароля самим пользователем и автоматическая генерация паролей

Количественная оценка стойкости парольных систем:

Вероятность P подбора пароля злоумышленником в течение срока его действия T определяется по следующей формуле.

$$P = \frac{V * T}{S} = \frac{V * T}{A^L}$$

A – количество символов, которые могут быть использованы при составлении пароля.

L – длина пароля.

S = число всевозможных паролей длины L , которые можно составить из символов алфавита A .

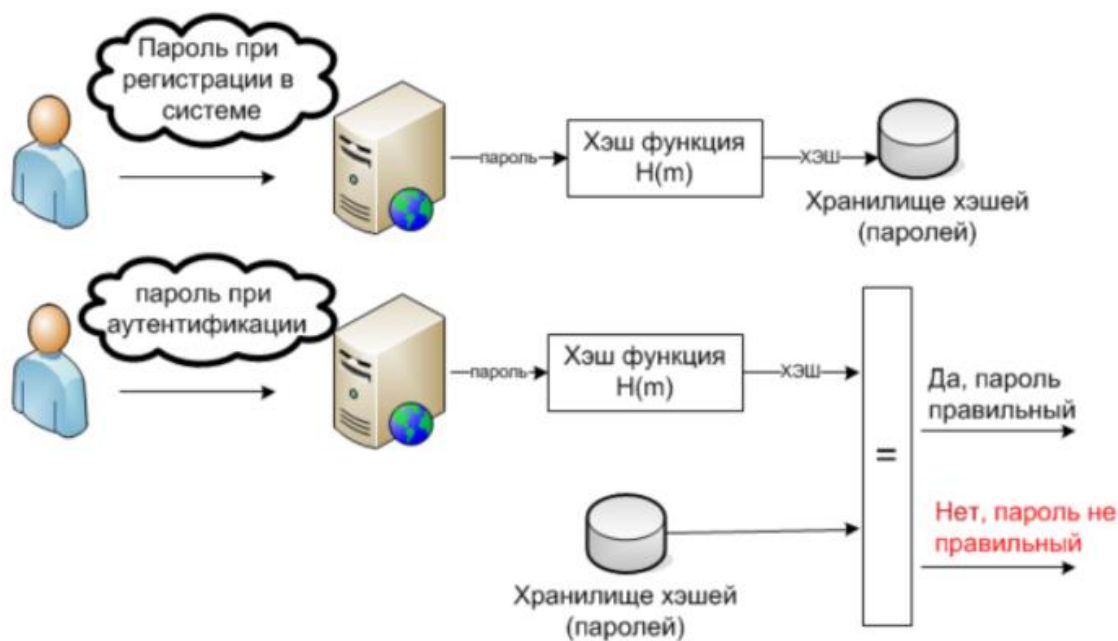
V – скорость перебора паролей злоумышленником.

T – максимальный срок действия пароля.

Блок-схема



Схема компьютерной системы:



Вывод:

При правильном направлении пользователей к выбору своего пароля возможно минимизировать способы проникнуть в чужую учётную запись от злоумышленников. Также в целях безопасности учётных записей стоит повысить защиту баз данных паролей. Также рекомендуется использовать двухфакторную аутентификацию - метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения.