**Лабораторная работа №1**

**На тему: система защиты компьютера с использованием паролей и средств не парольной защиты.**

**Студент:** Артюшов Андрей Геннадьевич

**Группа**: 3221

**Позиция в группе:** 1

**Задание 1. Ознакомление с теоретическим материалом и подготовка ответов на вопросы.**

**Перечислить минимальные требования к выбору пароля.**

* Пароль должен быть длинным
* Пароль должен быть трудно угадываемым
* Пароль не должен представлять собой распространенные слова, имена, названия и тп
* Пароль должен быть сложным
* Пароль должен значительно отменяться от паролей, использованных ранее
* Пароль должен быть уникальным

**Как определить вероятность подбора пароля злоумышленником в течение срока его действия?**

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;   
- 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 течении срока его действия V определяется по следующей формуле:

.

**Как можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?**

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

 (1)

где  - целая часть числа, взятая с округлением вверх.

После нахождения нижней границы *S\** необходимо выбрать такие *A* и *L* для формирования *S=AL*, чтобы выполнялось неравенство (2).

 (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.

В том случае, если значение *А* известно или задано, длину пароля можно определить как *L=LnS/LnA.* (3)

**Задание 2. Определение необходимой длины пароля при заданных исходных данных**

Пусть *A* – мощность алфавита паролей - количество символов, которые могут быть использованы при составлении пароля.

*L* – Длина пароля;

 - 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 течении срока его действия *V* определяется по следующей формуле:

.

В том случае, если значение А известно или задано, длину пароля можно определить по формуле:

Получив исходные данные посчитаем:

;

;

;

;

Минимальная длина пароля составляет 6 знаков, при заданных условиях.

**Задание 3. Изменение пароля при входе в операционную систему Windows**

Для изменения пароля при входе в систему в Windows 10 откройте «Параметры» и перейдите в «Учётные записи»

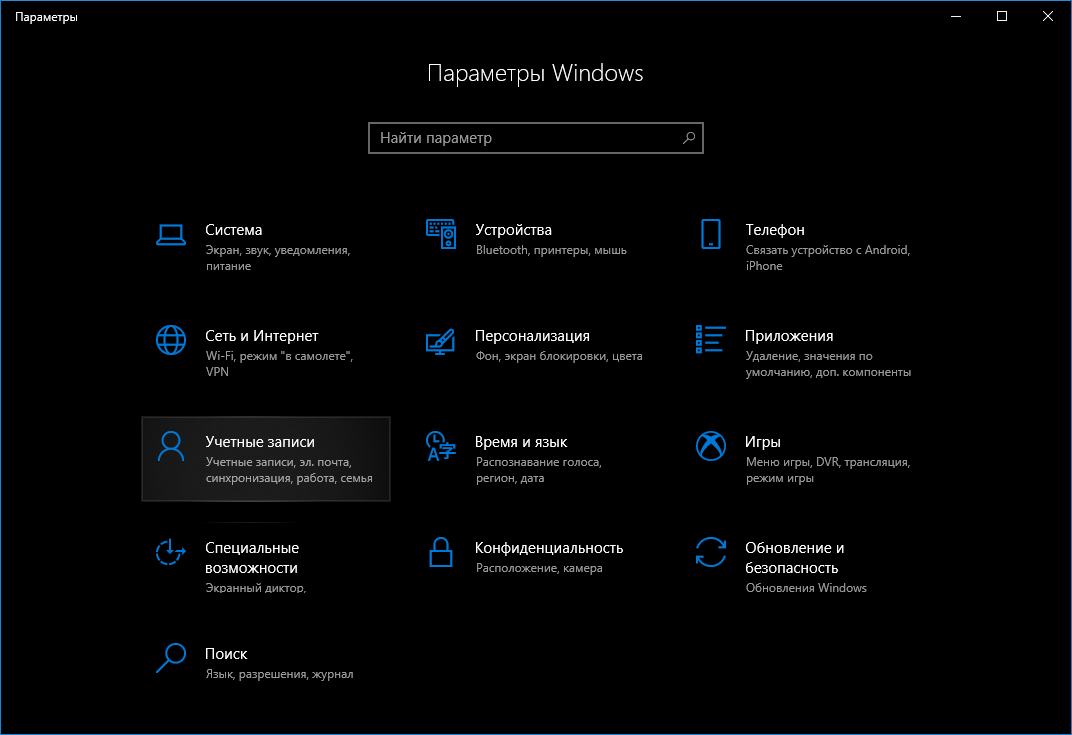


Рис. 1 Параметры компьютера

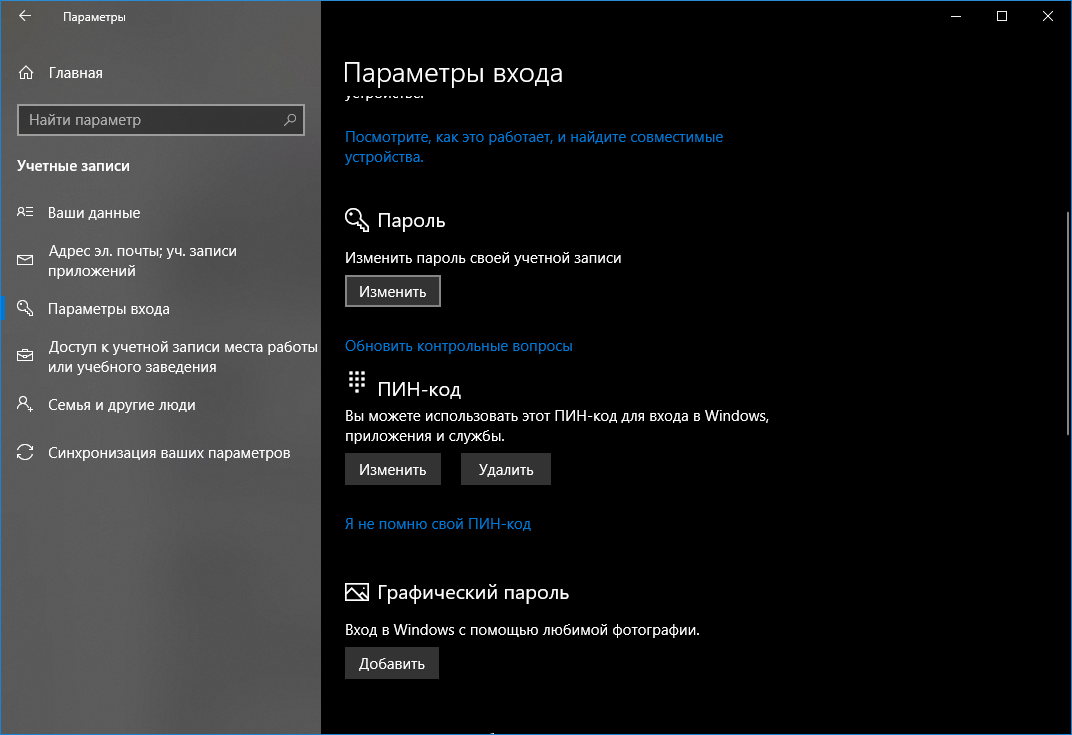
Далее перейдите в «Параметры входа» и нажмите на кнопку «Изменить»

Рис. 2 Параметры входа

Пароли хранятся в файле SAM который находится в «C:\Windows\System32\config»

**Задание 4. Исследование программного обеспечения для хранения паролей**

Для ознакомления с принципами работы хранения паролей была взята программа *LastPass.* Это достаточно простая и понятная в обращении программа. Онапоможет создать для каждой учетной записи свой пароль, а самое главное, что пароли будут храниться в закодированном виде, закрытой одним главным ключом или специальным файлом.

Основные функции и особенности *LastPass:*

* Использование алгоритмов для шифрования баз данных паролей;
* Программа защищена от клавиатурных шпионов;
* Программа в автоматическом режиме очищает буфер обмена после работы;
* Также программа имеет свой собственный алгоритм генерации паролей.

Из недостатков программы *LastPass:*

* Как и любого другого менеджера хранения паролей есть вероятность взлома;
* Программа имеет закрытый код, что не дает подробно изучить механизм ее работы.

**Задание 5. Разработка генератора паролей**

Программа для генерации паролей была разработана на языке программирования *Python*. Программа обладает возможностью выбора длины пароля и символов из которых он будет состоять.

**Задание 6. Использование методов не парольной защиты**

Исследования методов не парольный защиты были проведены на примере программы *Rohos Logon Key*, разработанной для хранения паролей. Программа позволяет защитить ОС, используя двухфакторную аутентификацию с помощью паролей, которые используются один раз.

Преимущества защиты с помощью электронного Ключа:

* Замена слабой парольной авторизации на физический Ключ.
* Повышенная безопасность Windows посредством более сложного пароля, чем обычно вы используете.
* Пароль автоматически передается в систему с Ключа.
* Удобная автоблокировка компьютера при отключении Ключа. Вернулись, подключили Ключ и вы снова в работе, не отвлекаясь на ввод пароля.
* Двухфакторная авторизация: физический USB-Ключ + PIN код либо Windows пароль.
* Используете один USB-Ключ для доступа к домашнему и к рабочему компьютеру.
* Возможность запретить доступ к компьютеру по обычному паролю (только при помощи USB-Ключа).
* Windows защищен даже в Безопасном Режиме.
* Использование USB-Ключа обеспечивает защиту также в Спящем Режиме.

За время изучения работы программы недостатков не было обнаружено.

На данный момент существует множество различных способов не парольной защиты, например, по скану отпечатка пальца, скан сетчатки глаза, по анализу лица и т.д.