Гостев Захар Сергеевич, группа 2.1

Лабораторная работа №

Клавиатурный подчерк. Исследование особенностей

**Цель работы**

Исследовать особенности использования клавиатурного подчерка в качестве биометрического метода идентификации личности. Реализовать программное средство, выполнив представленные задания.

**Задание**

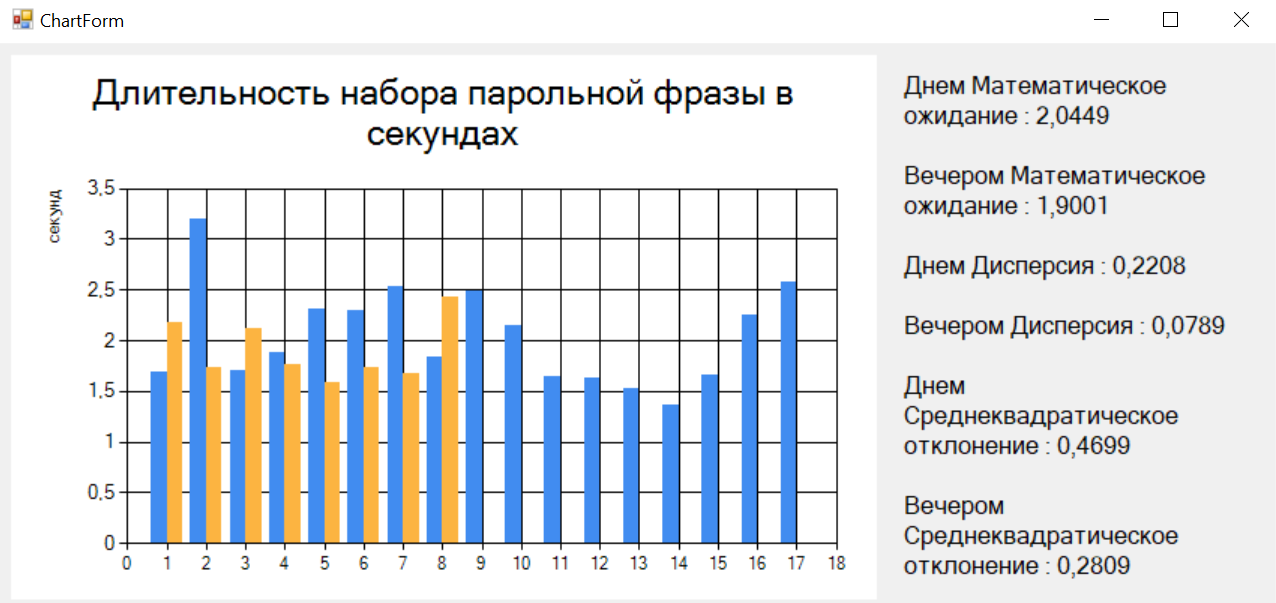
Разработать программу, обладающую следующими возможностями:

1. Оценка сложности парольной фразы.
2. Формирование гистограммы скорости ввода парольной фразы.
3. Оценка значения математического ожидания и дисперсии полученной выборки.
4. Исследование зависимости математического ожидания и дисперсии от времени суток.
5. Формирование графика зависимости динамики ввода парольной фразы (интервалы времени между нажатиями соседних символов в парольной фразе).
6. Оценка числа выполненных наложений при вводе парольной фразы (для каждого из типа).
7. Оценка времени удержания клавиш при вводе парольной фразы.
8. Формирование вектора биометрических параметров (с использованием разложения Хаара).
9. БД пользователей на основе полученных биометрических характеристик (удаление, редактирование, добавление, просмотр содержимого БД – отдельно и в совокупности по каждому пользователю).
10. Регистрация пользователя
    1. При регистрации пользователя в БД записывается вся необходимая информации (логин и пароль первостепенны, далее записывается для каждого пользователя информация пунктов 1-8).
    2. После формирования данных и заполнения всех полей БД выводится информационное сообщение, если же не хватает какой либо информации, выводится сообщение о необходимости дополнить данные (с указанием какие именно).
    3. Для того чтобы в БД внести информацию о графиках необходимо ее в виде массива (или другой способ упорядочивании данных).
11. Идентификации пользователя
    1. Для идентификации используется пароль (из которого формируется БХЧ). Проверка происходит как на совпадение пароля, так и на совпадение БХЧ (с некоторой погрешностью).
    2. На выходе система выдает, какой именно пользователь из БД (его ID или имя пользователя)
    3. Если пользователя в БД нет, выдается соответствующее оповещение
12. Верификация пользователя
    1. Для верификации пользователь предоставляет пароль (из которого формируется БХЧ) и ID. Проверка происходит как на совпадение пароля, так и на совпадение БХЧ (с некоторой погрешностью) и ID.
    2. На выходе система выдает, действительно пользователь является тем, за кого себя выдает.
    3. Если пользователя в БД нет, выдается соответствующее оповещение
13. В случаях когда пользователя нет в БД (при верификации и идентификации) необходимо предоставить пользователю возможность зарегистрировать нового пользователя.
14. При работе с БД предусмотреть возможность изменить информацию о пользователе, удалить, редактировать, просмотр (вывод).

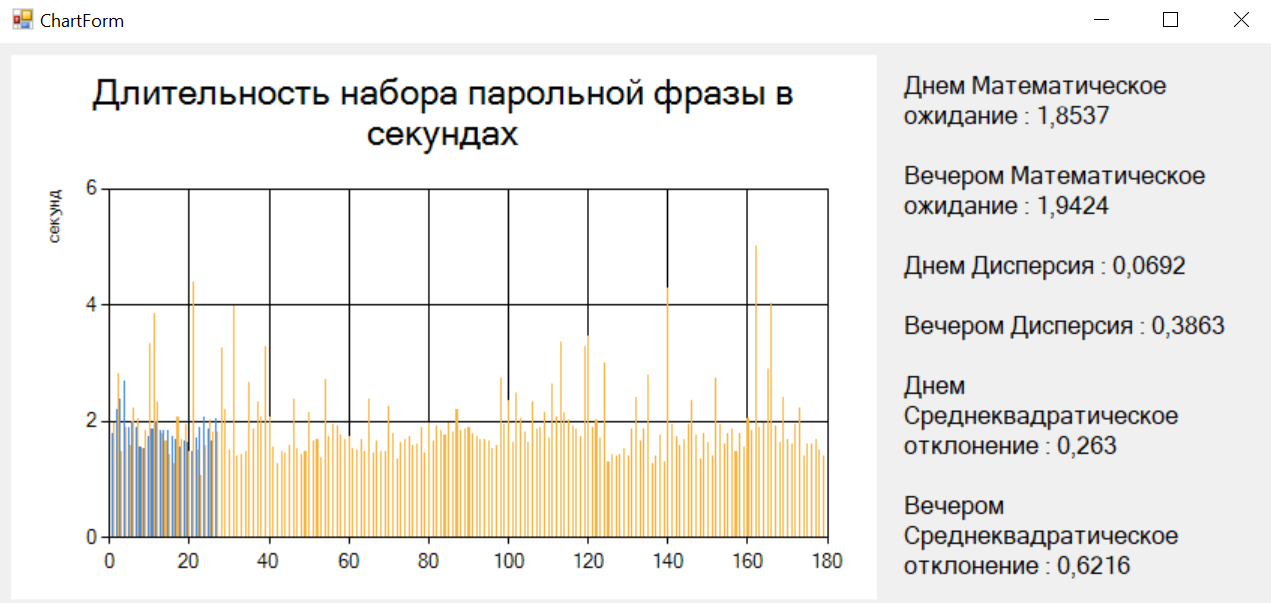
**Результат выполнения задания**

Программа, описанная в отчете по лабораторной работе 2 была модифицирована с учетом задач текущей лабораторной следующим образом:

1. Форма PasswordDurationsChartForm и PasswordVelocityChartForm, отображавшие длительности и скорости ввода паролей, были переработаны следующим образом.

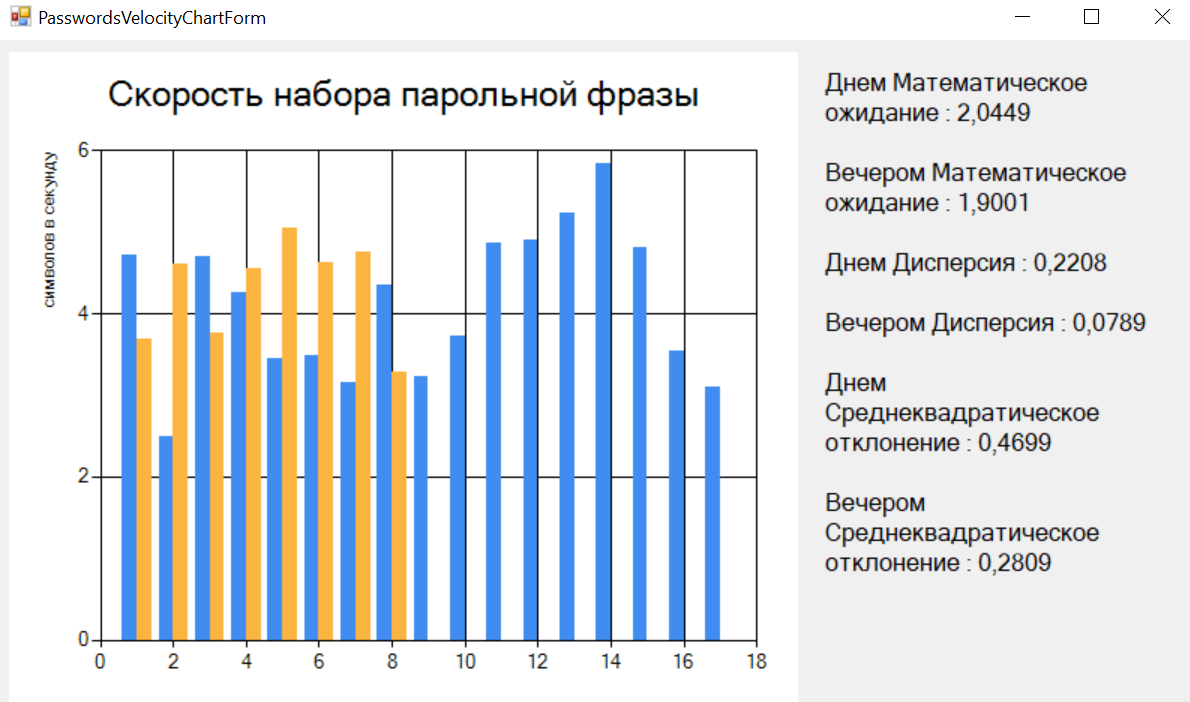


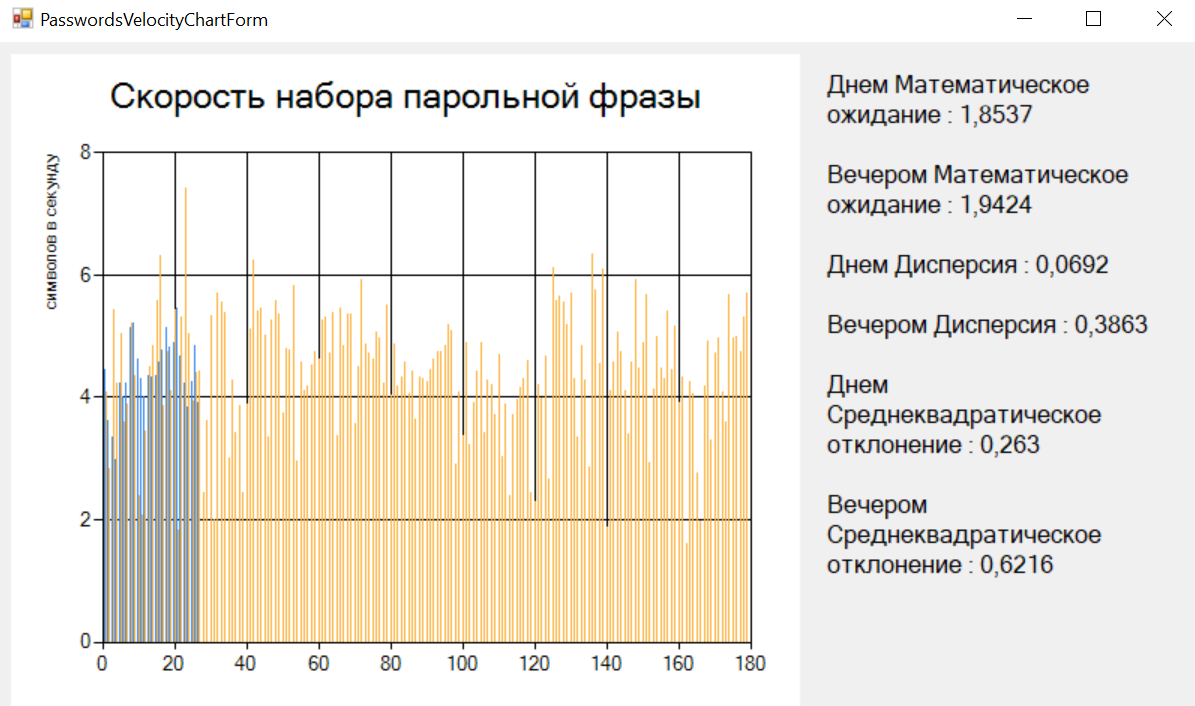
Теперь на форме отображаются данные вводов паролей в дневное и вечернее время, так же математическое ожидание, дисперсия и среднеквадратическое отклонение для каждого набора данных.



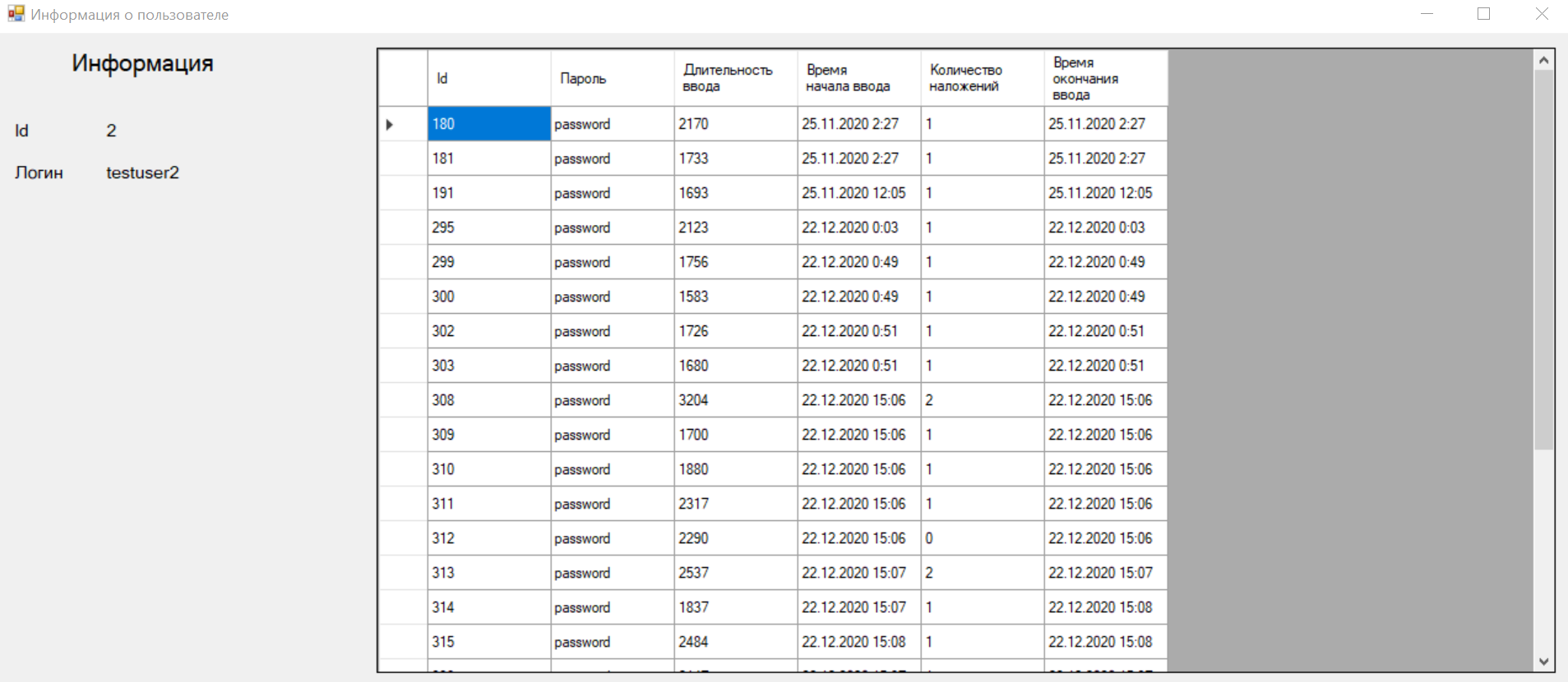
Как наглядно видно по результатам исследования более чем на 200 вводах паролей, математическое ожидание вводов паролей в дневное время меньше, чем в вечернее на 0.1 секунду. Дисперсия и среднеквадратическое отклонение также меньше для дневного времени.

Аналогичные изменения были произведены со скоростями вводов паролей

.



1. Добавлено отображение информации о текущем пользователе.



Наиболее важная информация о пользователе отображается на форме UserForm.

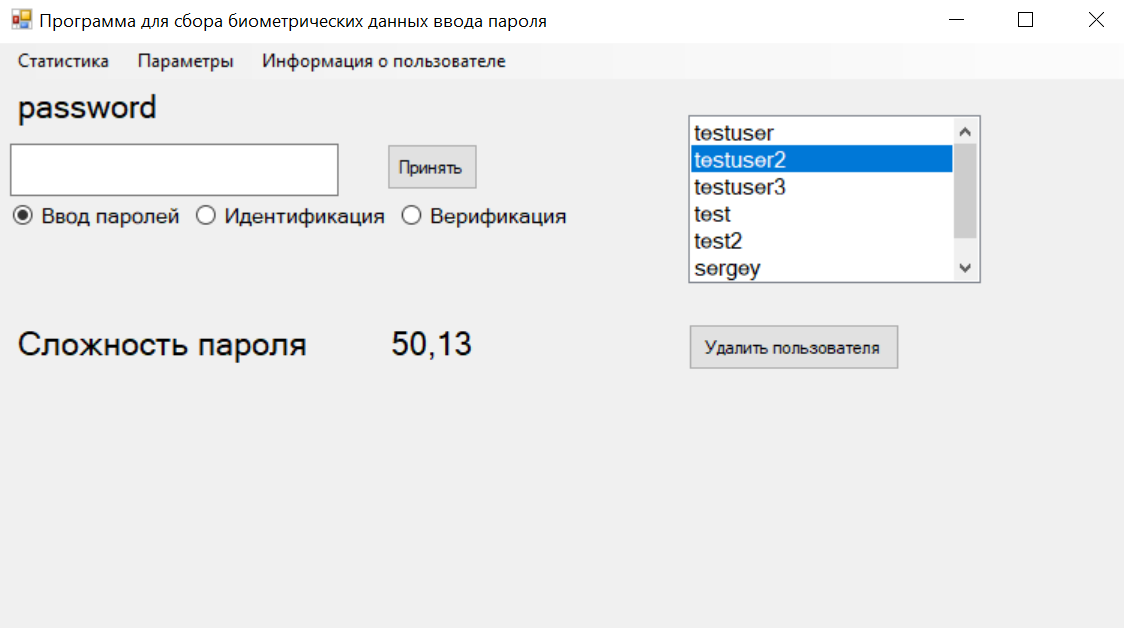
Это Id, логин пользователя, а также история всех его вводов паролей за все время, данные этих вводов пароля.

При изменении пользователя эта информация обновляется.

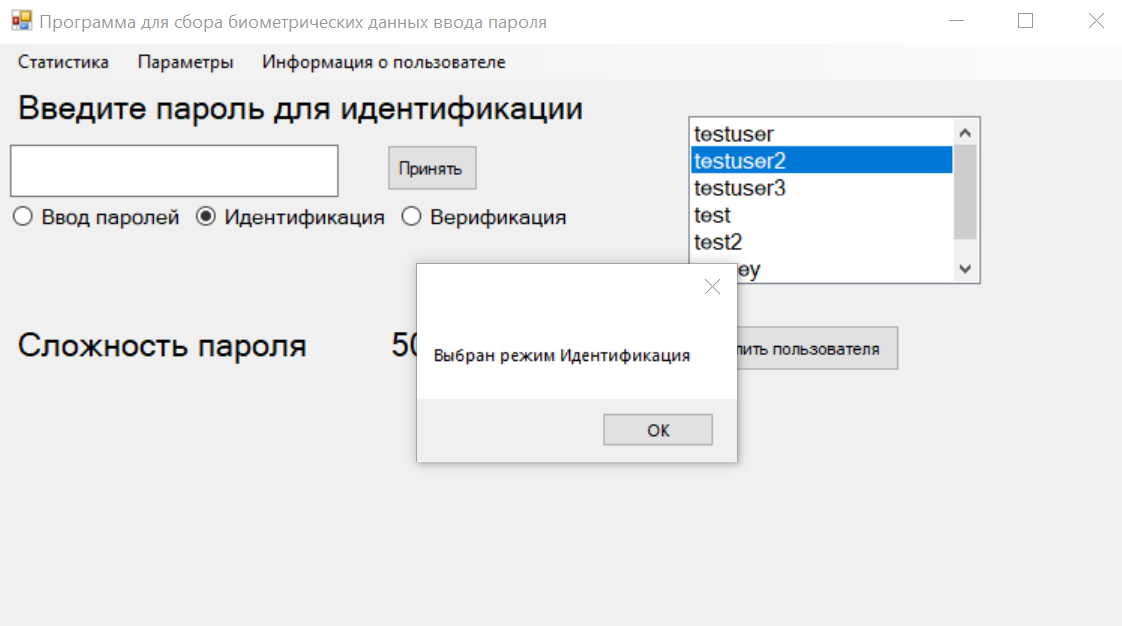
1. Добавлены идентификация и верификация пользователя.

На главном экране пользователь имеет возможность выбрать режим работы.

* Ввод паролей
* Идентификация
* Верификация

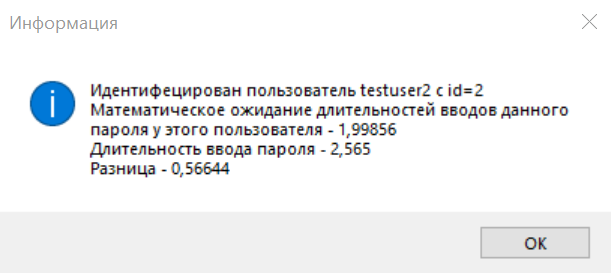


При выборе режима «Ввод паролей» все введенные пароли будут сохраняться в базу данных, а также изменяться вся статистка по вводам паролей.

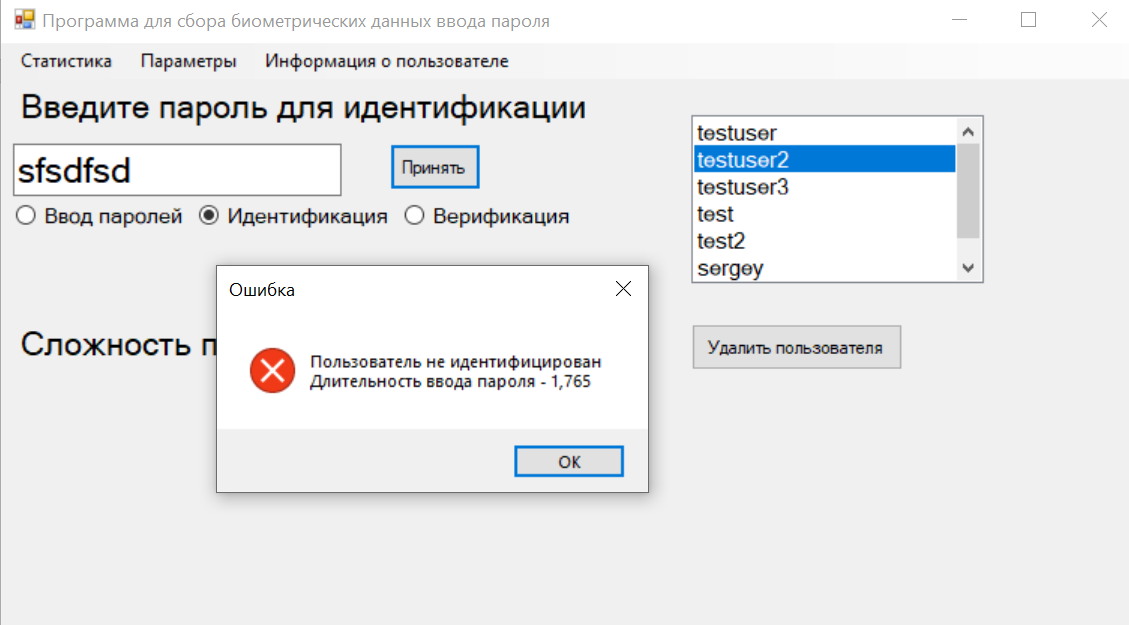


При выборе режима «Идентификация» введенный пароль будет сохранен в памяти программы, после чего проанализируется модулем AuthorizationController.

Все пользователи, имеющие в базе данных вводы паролей с паролем, совпадающим с полученным в ходе идентификационного ввода попадут в выборку. Далее, будут получены статистические данные для каждого пользователя (математическое ожидание времени ввода пароля), после чего будет выбран пользователь с наименьшим отклонением математического ожидания времени ввода пароля от идентификационного ввода.

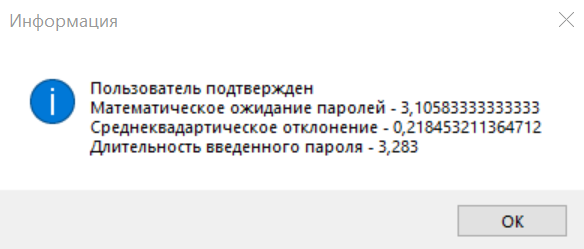


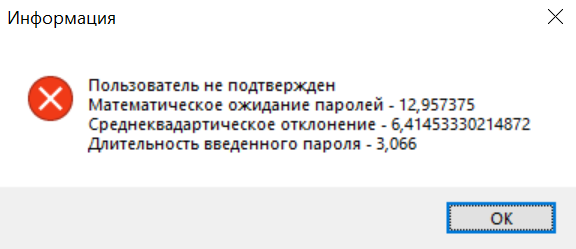
В случае, если пользователя с таким паролем нет, то будет выдана ошибка.



При выборе режима «Верификация» введенный пароль будет сохранен в памяти программы, после чего проанализируется модулем AuthorizationController.

В случае, если модуль разницы времени верификационного ввода пароля и математического ожидания всех вводов пароля пользователя меньше среднеквадратического отклонения, то пользователь будет подтвержден, иначе – нет.





# Вывод

В ходе выполнения работы были исследованы особенности использования клавиатурного подчерка в качестве биометрического метода идентификации личности. Также был осуществлен третий этап создания программного средства, выполнены представленные задания.