Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Кафедра компьютерной безопасности и математического обеспечения информационных систем

**Лабораторная работа**

по дисциплине «Технология построения защищенных автоматизированных систем»

УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию

ОГУ 090301.65.3015.006 О

Руководитель работы

канд. техн. наук, доцент

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.В. Влацкая

"\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2017 г.

Исполнитель

студент группы 13КБ(с)РЗПО

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.А. Казакова

"\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2017 г.

**1 Описание угрозы**

Угроза заключается в возможности прохождения нарушителем процедуры авторизации на основе полученной из открытых источников идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» дискредитируемого объекта защиты.  
Данная угроза обусловлена тем, что во множестве программных и программно-аппаратных средств производителями предусмотрены учётные записи «по умолчанию», предназначенные для первичного входа в систему. Более того, на многих устройствах идентификационная и аутентификационная информация может быть возвращена к заданной «по умолчанию» после проведения аппаратного сброса параметров системы (функция Reset).  
Реализация данной угрозы возможна при одном из следующих условий:  
наличие у нарушителя сведений о производителе/модели объекта защиты и наличие в открытых источниках сведений об идентификационной и аутентификационной информации, соответствующей учётной записи «по умолчанию» для объекта защиты;  
успешное завершение нарушителем процедуры выявления данной информации в ходе анализа программного кода дискредитируемого объекта защиты.

Источники угрозы:

* внутренний нарушитель с низким потенциалом;
* внешний нарушитель со средним потенциалом.

Объект воздействия:

* средства защиты информации, системное программное обеспечение;
* сетевое программное обеспечение, микропрограммное обеспечение;
* программно-аппаратные средства со встроенными функциями защиты.

**2 Диаграмма вариантов использования**

На рисунке 1 отображены возможные варианты использования программного продукта.



Рисунок 1 – Диаграмма вариантов использования

**3 Диаграмм последовательностей действий**



Рисунок 2 – Диаграмма последовательности действий

**4 Диаграмма активности**



Рисунок 3 – Диаграмма активности

**5 Примеры работы программы**

Для работы с программой нужно придумать уникальный пароль:

1. Длина пароля (чем больше, тем лучше), для запущенных случаев рекомендуют использовать 15-тисимвольный пароль;
2. Отсутствие словарных слов и частей распространенных паролей в составе пароля;
3. Отсутствие шаблонов при составлении пароля (под шаблоном я понимаю логический алгоритм генерации пароля, например: «Med777ведев», «12@йцу@21» или даже «q1w2e3r4t5»);
4. Стохастические последовательности символов из различных групп (строчные, прописные, цифры, знаки препинания и спец-символы);

На рисунке 4 отображена работа программы с уникальным паролем.

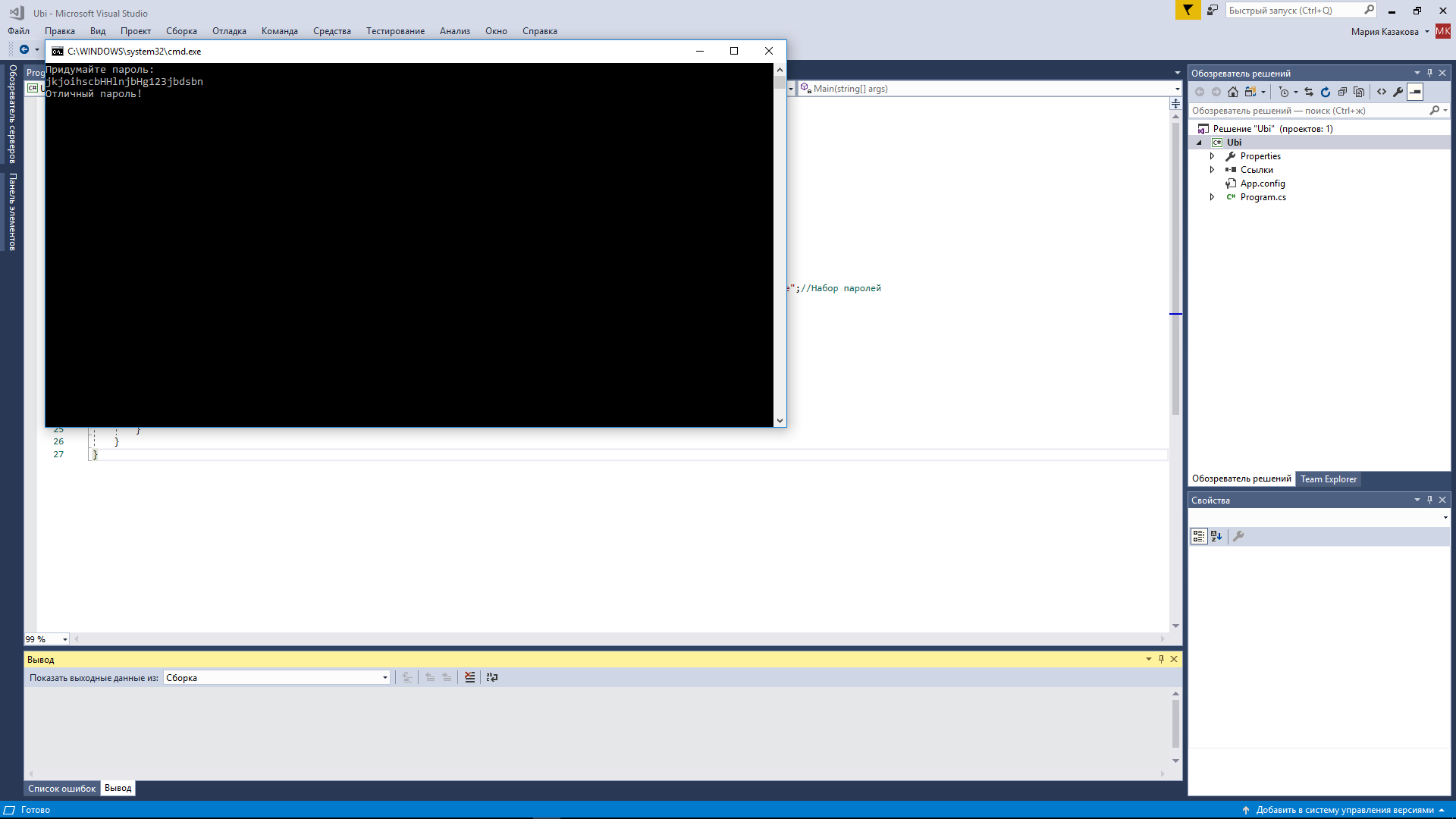


Рисунок 4 – Пример работы программы с уникальным паролем

На рисунке 5 отображена работа программы со стандартным паролем.

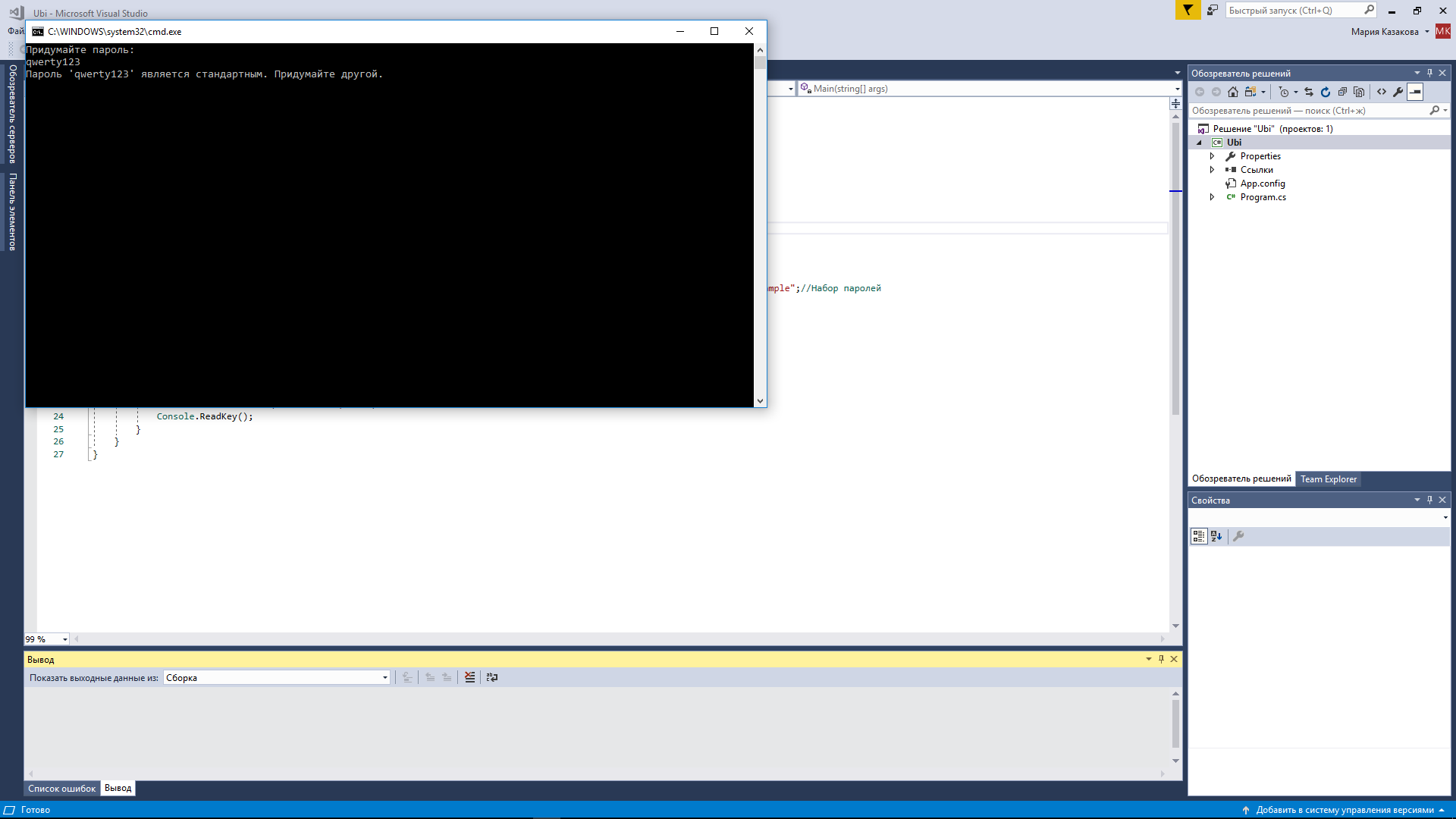


Рисунок 5 – Диаграмма последовательности действий

**6 Вывод**

В данной работе была выполнена защита от угрозы использования информации идентификации/аутентификации, заданной по умолчанию