Лабораторная работа №4

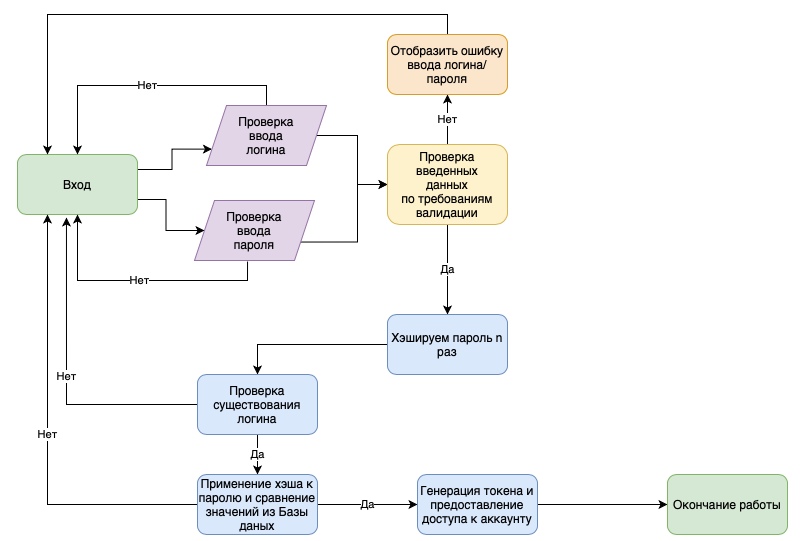
Карпов Алексей

12 группа кафедра ИСУ

Вариант 3

В данной системе для аутентификации применяется логин и пароль, с помощью которых возможен вход в систему в случае наличия пользователя в базе данных с введенными персональными данными. Также представлена двухфакторная аутентификация: генерируется токен на время сессии входа с указанным временем жизни на 60 минут, что позволяет обеспечить дополнительную защиту ввиду ограничения времени использования этого самого токена и невозможности использования аккаунта без него.

Схема процесса аутентификации:



По результату процесса, пользователь также получает и личный токен при доступе к аккаунту. Данный ход позволит избежать нежелательного доступа со стороны злоумышленника - токен всегда выдаётся новый, а также имеет активность 60 минут.

Приведем список возможных атак:

А) Атака на формы ввода логина и пароля.

Б) Небезопасно организованная форма восстановления пароля.

В) Небезопасно организованная форма для сброса пароля.

Г) Атака на пароль (например, по словарю или полный перебор).

Д) Атака на управление выходом.

В разработанной мною системе заметно, цепочка хэшей позволяет защититься от атаки на пароль, атаки на формы ввода логина и пароля, а также от атаки на управление выходом, ибо злоумышленник не обладает информацией о количестве цепочек хэшей.

Поскольку сброс и восстановление пароля не предусмотрены в программе, то единственным вариантом взлома может быть получение личного устройства пользователя. После этого, в случае, если удастся узнать логин и пароль, а также количество цепочек хэшей, злоумышленник сможет осуществить вход.

Итак, реализация цепочки хэшей, а также механизма токенизации позволяет снизить шансы того, что злоумышленник получит доступ к нашеу блокноту.

Таким образом, присутствует несколько уровней защиты:

1) Шифрование текста сессионным ключом перед его отправкой на сервер (это было сделано в лабораторной работе два)

2) Механизм 2-факторной аутентификации в защищённом блокноте. Однако существует ещё один способ получения доступа к тексту - узнать RSA ключ шифрования, который хранится в БД. То есть по сути злоумышленнику достаточно будет взломать доступ к БД. Но стоит помнить, что RSA ключ защищает только ключ для текущей сессии, который каждый раз изменяется, следовательно злоумышленник также не сможет получить полный доступ к зашифрованным текстам.