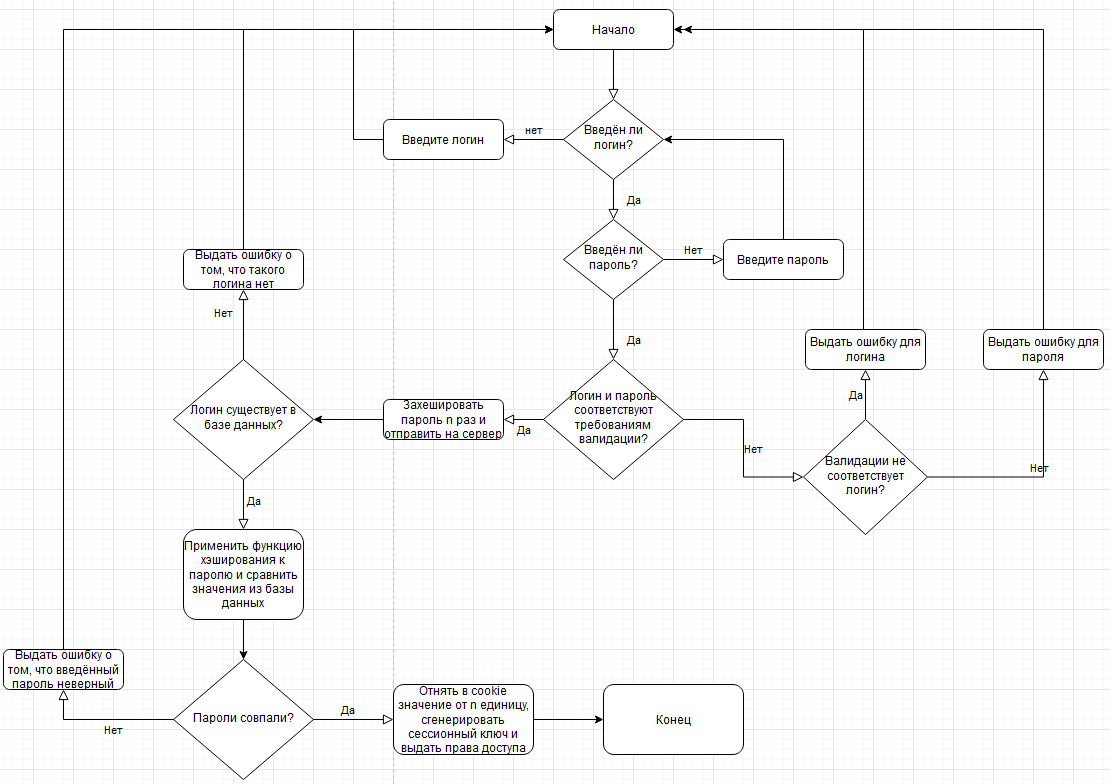
Лабораторная работа №4

Дворяков Максим

12 группа кафедра ИСУ

Вариант 3

Блок-схема



Список возможных атак:

* Обход CAPTCHA
* Атака на функционал восстановления паролей
* Атака на формы входа
* Атака на управление выходом
* Атаки на пароли
* Использование слабых паролей
* Небезопасный сброс пароля
* Использование универсального пароля

Из них применительно к моей системе, не применителен ни один, так как цепочка хэшей делает безопасным аунтификацию. Капчти у меня нет, функционала востановления пароле тоже нет, Атаки на пароли не даст никакого смысла, так как злоумышленнику надо ещё узнать кол-во раз сколько надо захешировать на клиенте, слабый пароль не работает по тем же причинам и универсальный пароль также. Единственный вариант — это получение полного доступа к компьютеру, тогда злоумышленник сможет узнать какой пароль ввёл пользователь и посмотреть сколько раз нужно захешировать пароль на клиенте.

В данной лаб работе были реализована цепочка хешей, механизм токненизации. Текст, который ввёл пользователь шифруется дополнительно паролем, который вводит пользователь перед отправкой текста на сервер, после этого текст шифруется сессионным ключом (aes) и записывается в базу данных. Если злоумышленник получит доступ к бд, то это ничего ему не даст, так как пароль захэширован а текст хранится в зашифрованном виде. А возможность хранить и получать доступ к файлам был реализован ещё во 2 лаб работе. Ключ от RSA хранится в бд, но этот ключ ничего не даст злоумышленнику, так как он защищает только сессионный ключ и его можно в любой момент перегенировать.