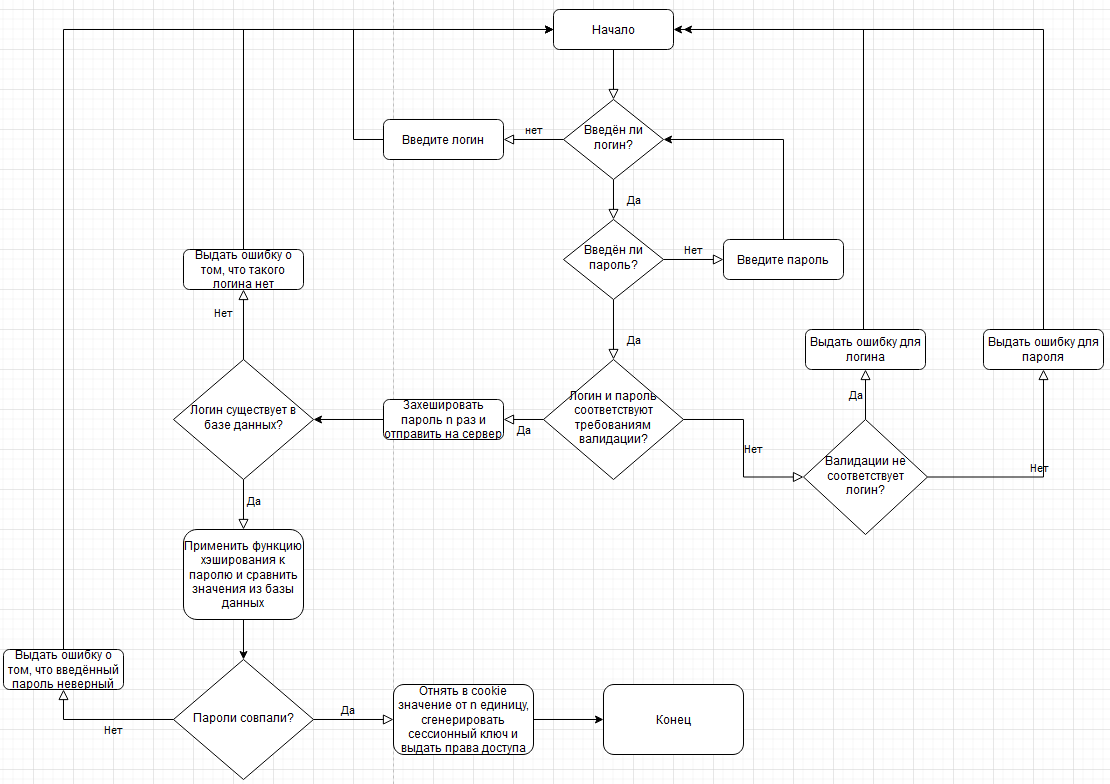
Лабораторная работа №4

Веренич Владислав,

Поживилко Фёдор

12 группа кафедра ИСУ

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 пароль + ПИН делает безопасным аутентификацию. Капчи у меня нет, функционала восстановления пароля тоже нет. Атаки на пароли не дадут никакого смысла. Единственный вариант — это получение полного доступа к компьютеру, тогда злоумышленник сможет узнать какой пароль ввёл пользователь и посмотреть какой введен ПИН.

В данной лабораторной работе была реализована двухфакторная аутентификация. Текст, который ввел 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 перегенерировать.