МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Мегафакультет компьютерных технологий и управления**

**Факультет безопасности информационных технологий**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ 1**

«Алгоритмы криптографии и подпись приложений»

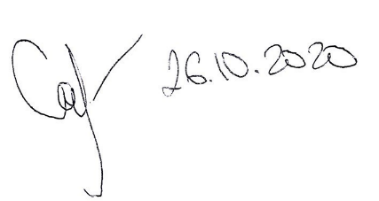
по дисциплине:

«Разработка систем аутентификации и криптографии»

Выполнила:

студент гр. N42514c,

Саенко Александра Игоревна



Проверил:

ассистент ФБИТ

Федоров Иван Романович

Санкт-Петербург

2020

Оглавление

[Цель работы 3](#_Toc58278661)

[Описание выбранных средств реализации и обоснования выбора 3](#_Toc58278662)

[Демонстрация работы программы 3](#_Toc58278663)

[Выводы 5](#_Toc58278664)

**Вариант:** Blowfish

**Цель работы:** реализовать механизм аутентификации в клиент-серверном веб-приложении.

**Задачи:**

- необходимо реализовать метод аутентификации в клиент-серверном приложении согласно варианту 7;

- клиент должен представлять собой веб-страницу с формой авторизации пользователя;

- сервер должен включать в себя две части:

1) таблица идентификаторов (данные о пользователях для аутентификации: логин/пароль/токен/итд в зависимости от метода аутентификации);

2) процесс с реализованной логикой метода аутентификации.

**Ход работы:**

Реализовать аутентификацию по одноразовому паролю с хешированием MD5 (можно использовать функцию из библиотеки). В таблице идентификаторов должны храниться: логин, email, хеш пароля (md5), срок действия пароля. Таблица идентификаторов должна представлять собой таблицу в реляционной БД, данные должны передаваться через SQL-запросы. При истечении срока действия пароля аутентификация не должна проходить. При аутентификации на сервере генерируется пароль для отправки на почту и в таблицу идентификаторов сохраняется его хэш. Сравниваются не пароли, а результаты MD5.

**Работы программы:**

1. Создаем базу данных, где будут храниться логин, пароль, почта пользователя, в моем случае всего один человек в базе данных.

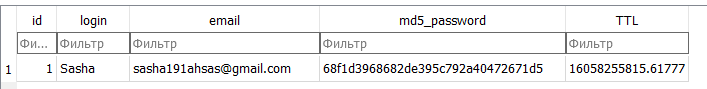


Рисунок 1 – база данных

1. Главная страница, где необходимо ввести логин, после чего нажать на кнопку «отправить пароль на почту».

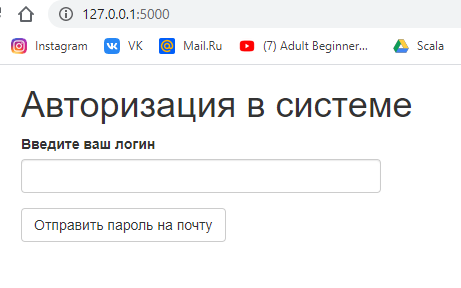


Рисунок 2 – Главная страница

1. В случае неуспешно введенного логина (логина, которого нет в базе данных) высвечивается сообщение «Неправильный логин»

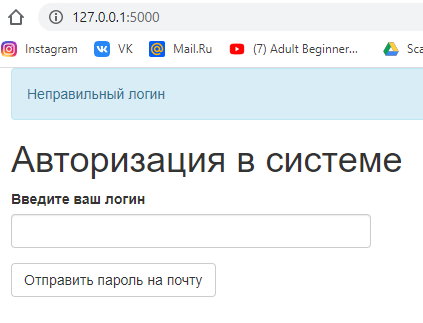


Рисунок 3 – Главная страница в результате неправильного введенного логина

1. Вводим корректный логин и нажимаем на «отправить пароль на почту».

«отправить пароль на почту».

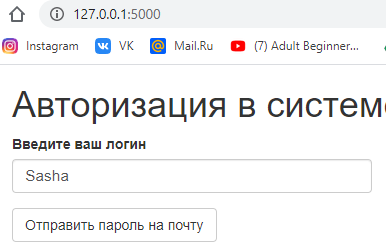


Рисунок 4 – Главная страница и ввод логина пользователя

1. На указанную в базе данных почту этого пользователя отправляется письмо с паролем.

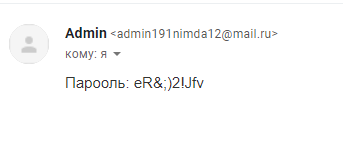


Рисунок 5 – Письмо с паролем

1. Высвечивается графа для ввода пароля.

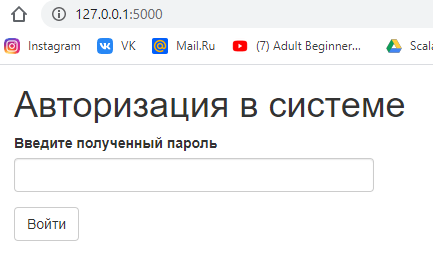


Рисунок 6 – Окно для ввода пароля

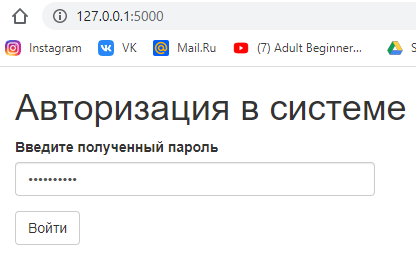


Рисунок 7 – Пароль введен

1. В случае успешно введенного пароля, происходит переход на отдельную страницу где можно видеть надпись: «Вы успешно авторизовались» и имя пользователя.

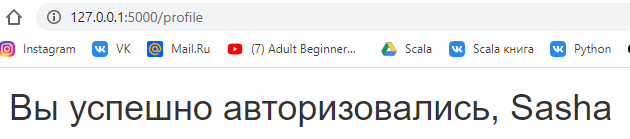


Рисунок 8 – Страница профиля

**Выводы:** в результате выполнения лабораторной работы был реализован метод аутентификации в клиент-серверном приложении по одноразовому паролю с хешированием MD5. Предварительно была создана база данных, в которой хранятся: логин, email, хеш пароля (md5), срок действия пароля. При аутентификации на сервере генерируется пароль для отправки на почту и в таблицу идентификаторов сохраняется его хэш. И в конечном итоге сравниваются результаты MD5, и в случае их равенства пользователя перебрасывает на страницу профиля, где отображается персональное приветствие.