**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Разработка систем аутентификации и криптографии»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2**

**Методы аутентификации**

**7 вариант**

**Выполнила:**

Студенты гр. N42514c

Родиманова Е.С.

**Проверил:**

Фёдоров И.Р.

Санкт-Петербург

2020 г.

Оглавление

[Цель работы 3](#_Toc58278661)

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

[Демонстрация работы программы 3](#_Toc58278663)

[Выводы 5](#_Toc58278664)

# Цель работы

**-** реализовать механизм аутентификации в клиент-серверном веб-приложении.

**Требования к реализации:**

* 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.

* программа не должна разрешать переход на страницу-заглушку без успешной аутентификации (напрямую по URL).

**Вариант 7:**

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.

# Описание выбранных средств реализации и обоснования выбора

Для реализации алгоритма был выбран язык Python 3.9.0, так как это понятный и простой язык программирования.

В качестве среды разработки использовался **Visual Studio Code (VS Code)**.

Использовался фреймворк **Flask**, который позволяет создавать сайты самых разных типов с использованием языка Python. Flask относится к разряду микрофреймворков, то есть, он предоставляет лишь базовый инструментарий для построения сайтов, все по минимуму – ничего лишнего. Однако, этого вполне достаточно, чтобы создавать большинство типовых сайтов с поддержкой шаблонов страниц, баз данных и прочими стандартными возможностями. И, кроме того, простота и достаточность функционала для типовых решений позволяют достаточно быстро разобраться в этом пакете и начать сразу его применять.

Также использовался **Bootstrap** — бесплатный HTML/CSS/JavaScript фреймворк для быстрого создания адаптивного дизайна сайта. Bootstrap позволяет с минимальными знаниями создавать интерфейсы, которые работают во всех популярных браузерах и не ломаются при изменении разрешения экрана.

# Демонстрация работы программы

Перед тем как начать работу, необходимо создать базу данных, в которой будут храниться данные о пользователях – логин, пароль, e-mail. Эти данные представлены в виде таблицы, приведенной на Рисунке 1.

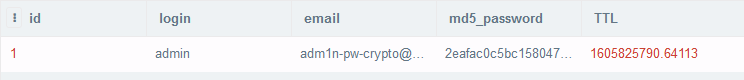


Рисунок 1 – Таблица Users, в которой находятся данные о зарегистрированных пользователях

На странице входа (Рисунок 2) необходимо ввести логин пользователя и нажать кнопку «Получить пароль». После этого на адрес, который хранится в базе данных этого пользователя, отправится пароль.

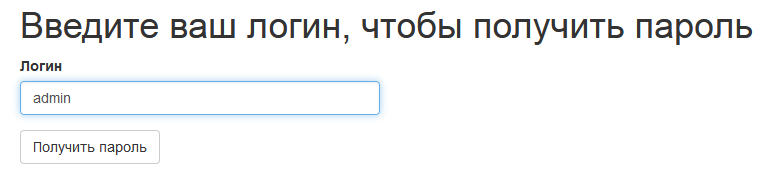


Рисунок 2 – Ввод логина пользователя

После того, как на почту пришло письмо с паролем (Рисунок 3), этот пароль необходимо ввести в поле, которое появится на сайте (Рисунок 4).

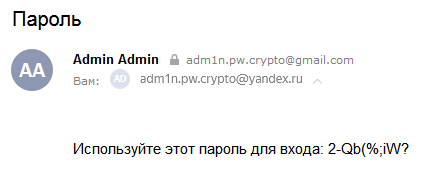


Рисунок 3 – Письмо с паролем

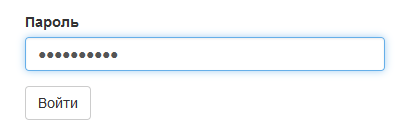


Рисунок 4 – Ввод пароля

После ввода пароля на сайте появится приветственное сообщение (Рисунок 5).

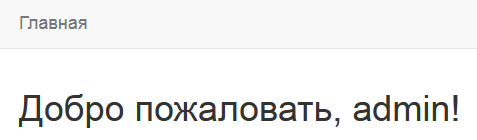


Рисунок 5 – Приветственное сообщение

# Выводы

В ходе работы был реализован метод аутентификации в клиент-серверном приложении в соответствии с выбранным вариантом.