**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

**«**Разработка систем аутентификации и криптографии**»**

**Лабораторная работа 2** на тему

«Методы аутентификации»

Вариант 8

**Выполнил:**

магистрант гр. N42514c

Самоследов Г.А.

**Проверил:**

Фёдоров И. Р.

Санкт-Петербург

2020

**Цель работы:** получить навыки реализации механизма аутентификации в клиент-серверном веб-приложении.

**Задача:** реализовать механизм аутентификации согласно варианту задания.

**Вариант задания:**

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 файл .JSON. 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.

**Средства реализации:**

IDE: PyCharm Community 2020.1.1.

Язык: Python 3.

Операционная система: Windows 10.

**Краткое описание работы:**

Аутентификация используется для подтверждения подлинности владельца идентификатора. Самый распространённый метод аутентификации — вход по паролю, использующийся в подавляющем большинстве компьютерных систем. Менее распространённым способом является использование аппаратных идентификаторов, на которые записываются ключи доступа или пользовательские пароли.

Также в корпоративном секторе популярна двухфакторная аутентификация. Как правило, под этим понимается связка из е-токена и пин-кода вводимого пользователем, но встречаются и более экзотические сочетания, состоящие из биометрического сканера и аппаратного идентификатора или пользовательского пароля.

В данной работе производится аутентификация по случайно сгенерированному одноразовому паролю, который отправляется на электронную почту.

В качестве веб-фреймворка использован bottle. Он был выбран за счет крайней простоты создания и настройки, а также достаточности функционала для данной лабораторной работы. Нужно всего лишь скачать библиотеку bottle с помощью pip. Других библиотек для работы данного сервера устанавливать не требуется.

Хэш-функция md5 взята из библиотеки hashlib. Также использованы библиотеки: random для генерации пароля, smtplib для отправки почты по протоколу smtp, datetime для вычисления срока действия пароля, json для работы с файлами формата json, а также string для получения готовой строки со всеми возможными латинскими буквами.

Json файл играет роль базы данных. В нем имеются несколько пользователей, каждый из них имеет имя, адрес электронной почты, хэш одноразового пароля и срок действия пароля с момента генерации (в секундах).

**Ссылка на репозиторий:**

<https://github.com/4444gleb/Cryptography/tree/main/2>

**Выводы:**

В ходе работы получены навыки реализации механизма аутентификации в клиент-серверном веб-приложении.. Был реализован механизм аутентификации согласно варианту.