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»

**Выполнил:**

Магистрант гр. N42514c

Балданова Юлия Батоевна

Подпись: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Проверил:**

Федоров Иван Романович

Подпись: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Санкт-Петербург,

2020

# Цель работы

Требования к реализации программы:

* необходимо реализовать метод аутентификации в клиент-серверном приложении согласно варианту № 1;
* клиент должен представлять собой веб-страницу с формой авторизации пользователя;
* сервер должен включать в себя две части:
  + таблица идентификаторов (данные о пользователях для аутентификации: логин, хэш пароля (md5), срок действия пароля);
  + процесс с реализованной логикой метода аутентификации.

# Описание выбранных средств реализации и обоснования выбора

Для реализации алгоритма был выбран язык PHP, как один из самых распространенных языков веб-разработки. Он применяется для создания сайтов и веб-приложений любой сложности.

Для реализации клиент-серверной архитектуры был выбран локальный сервер XAMPP, который является самой популярной средой разработки PHP. Он позволяет осуществлять разработку сайтов и работу с БД, не выходя в сеть Интернет. Для верстки был выбран Фреймворк Bootstrap – свободный набор инструментов для создания сайтов и веб-приложений, который включает в себя HTML и CSS-шаблоны оформления для типографики, веб-форм, кнопок и прочих компонентов веб-интерфейса.

# Описание работы алгоритма

В таблице идентификаторов должны храниться: логин, хэш 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 сравниваются не пароли, а результаты MD5.

# Исходный код и демонстрация работы

[Ссылка на исходный код.](https://github.com/yuliaxxx/Cryptography/tree/main/2%20lab%20work)

[Ссылка на демонстрацию работы кода.](https://github.com/yuliaxxx/Cryptography/tree/main/2%20lab%20work)

# Выводы

В ходе Лабораторной работы № 2, была разработана система аутентификации по паролю с хешированием MD5.