**Міністерство освіти і науки України  
Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»  
Факультет інформатики та обчислювальної техніки  
Кафедра обчислювальної техніки**

Лабораторна робота 5

з дисципліни  
«Безпера програмного забезпечення»

Виконав: Перевірив:

студент групи ІП-03 Іваніщев Б.В   
 Янишин Віталій

Київ 2023

**Лабораторна робота 5**

Засвоювання базових навичок роботи з валідацією токенів

**Завдання:**

Розширити **Лабораторну работу 4** перевіркой сігнатури JWT токена. Приклади SDK <https://auth0.com/docs/quickstart/backend>.У випадку асиметричного ключа, public є можливість отримати за посиланням <https://kpi.eu.auth0.com/pem>, aбо за формулою <https://[API_DOMAIN]/pem> Надати код рішення.

Виконання:

Для валідації використаємо метод verify з jsonwebtoken

const validateJwt = async (jwt) => {

  const cert = fs.readFileSync("cert.pem");

  verify(jwt, cert, { algorithms: ["RS256"] }, (error, payload) => {

    if (error) throw new Error(error);

    console.log("jwt validated");

    console.log(payload);

  });

};

app.get("/", async (req, res) => {

  if (req.session.access\_token) {

    validateJwt(req.session.access\_token);

    if (true) {

      const response = await refreshToken(req.session.refresh\_token);

      const responseObj = JSON.parse(response);

      req.session.access\_token = responseObj.access\_token;

      req.session.expires\_at =

        Math.floor(Date.now() / 1000) + responseObj.expires\_in;

      console.log(`token refreshed:

        ${response}

      `);

    }

    return res.json({

      username: req.session.username,

      logout: "http://localhost:3000/logout",

    });

  }

  res.sendFile(path.join(\_\_dirname + "/index.html"));

});

