Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет   
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

ОТЧЁТ

к лабораторной работе №3

на тему

**ИДЕНТИФИКАЦИЯ И АУТЕНТИЦИФКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ. ПРОТОКОЛ KERBEROS**

Выполнил: студент гр.253504 Давыдовский Д.В.

Проверил: ассистент кафедры информатики Герчик А.В.

Минск 2025

**СОДЕРЖАНИЕ**

[1 Цель работы 3](#_Toc188986632)

[2 Ход работы 4](#_Toc188986633)

[Заключение 6](#_Toc188986634)

# 1 ЦЕЛЬ РАБОТЫ

Цель работы – реализовать программные средства для идентификации и аутентификации пользователей с использованием протокола *Kerberos*, а также разработать удобный интерфейс для тестирования пользователем.

*Kerberos* – это система, которая позволяет компьютерам в сети проверять, кто есть кто, без передачи паролей. Работает она как паспортный контроль в аэропорту: один раз показываешь документы, получаешь пропуск, а дальше используешь его, чтобы проходить проверки без повторного предъявления паспорта.

Когда вы включаете компьютер и вводите логин с паролем, ваш компьютер не отправляет пароль на сервер, а создаёт зашифрованный запрос и отправляет его в центр аутентификации *Kerberos*. Этот центр проверяет, есть ли такой пользователь, и если всё в порядке, отправляет обратно специальный билет, который называется *Ticket Granting Ticket* или просто *TGT*. Он зашифрован и доказывает, что вы прошли аутентификацию, но сам по себе не даёт доступ к конкретным сервисам. Компьютер сохраняет этот билет, чтобы больше не спрашивать пароль.

Когда вам нужно подключиться к какому-то сервису, например к почте или файлам на сервере, ваш компьютер берёт этот билет и отправляет его в центр *Kerberos*, запрашивая разрешение на доступ. Центр проверяет билет, убеждается, что он действителен, и выдаёт новый билет, но уже специально для этого сервиса. Этот билет тоже зашифрован, но теперь предназначен для сервера, к которому вы подключаетесь.

После этого компьютер отправляет новый билет на сервер, сервер проверяет его, видит, что всё в порядке, и разрешает вам доступ. Всё это происходит автоматически, без необходимости вводить пароль ещё раз. Так как билеты зашифрованы и действуют только ограниченное время, никто не сможет перехватить или подделать их, что делает систему безопасной.

# 2 ХОД РАБОТЫ

В ходе выполнения поставленной задачи было реализовано веб-приложение для идентификации и аутентификации пользователей с использованием протокола *Kerberos*. Программа включает в себя механизмы регистрации пользователей, входа в систему и проверки валидности сессии.

Для демонстрации был разработан веб-сайт. На рисунке 1 представлена страница авторизации.

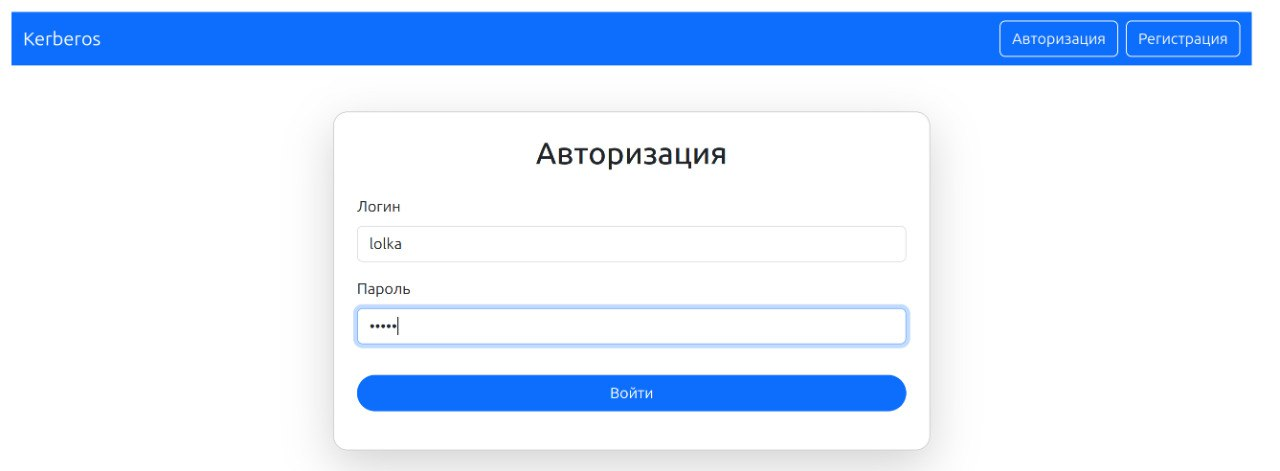


Рисунок 1 – Страница авторизации

Также для удобства пользователя была разработана страница регистрации, которая выглядит идентично странице авторизации за исключением кнопки. Вместо кнопки входа, на странице регистрации, кнопка регистрации.

Углубимся в принцип работы. Для использования веб-сайта был разработан сервер, который реализует упрощённую версию протокола *Kerberos*. Для удобства и ускорения разработки, на стороне клиента шифрование не применяется, но на стороне сервера задействуется. Также была подключена база данных *PostgreSQL* для хранения пользователей, билетов и сессий.

При регистрации никаких сложных манипуляций не происходит, за исключением шифрования и сохранения пользователя в базе данных, поэтому мы подробнее рассмотрим авторизацию пользователя на веб-сайте и то, что происходит после.

При успешной регистрации пользователь получает билет*,* который будет использоваться далее. При попытке перейти на страницу профиля, задействуется, полученный ранее билет. При переходе на страницу билет отправляется на проверку, в ходе которой проверяется действительность билета, а также срок его действия, если срок действия билета истёк, пользователю будет предложено повторно авторизироваться на веб-сайте. В ином случае, данный билет используется для получения сервисного билета. Для получения сервисного билета, на сервер отправляется временный билет и название сервиса, к которому пользователь хочет получить доступ, в нашем случае профиль. Далее сервер проверяет валидность и существование данного временного билета. При успешной проверке в таблице с сервисными билета ищется запись, которая покажет, что пользователь уже обращался с этим сервисным билетом к сервису. В случае нахождения такой записи, сервисный билет проверяется на валидность и при успехе высылается пользователю, что позволяет получить доступ к сервису, в ином случае создаётся новый сервисный билет, что в свою очередь также позволяет получить доступ к запрашиваемому сервису. На рисунке 2 представлен результат успешной авторизации пользователя.

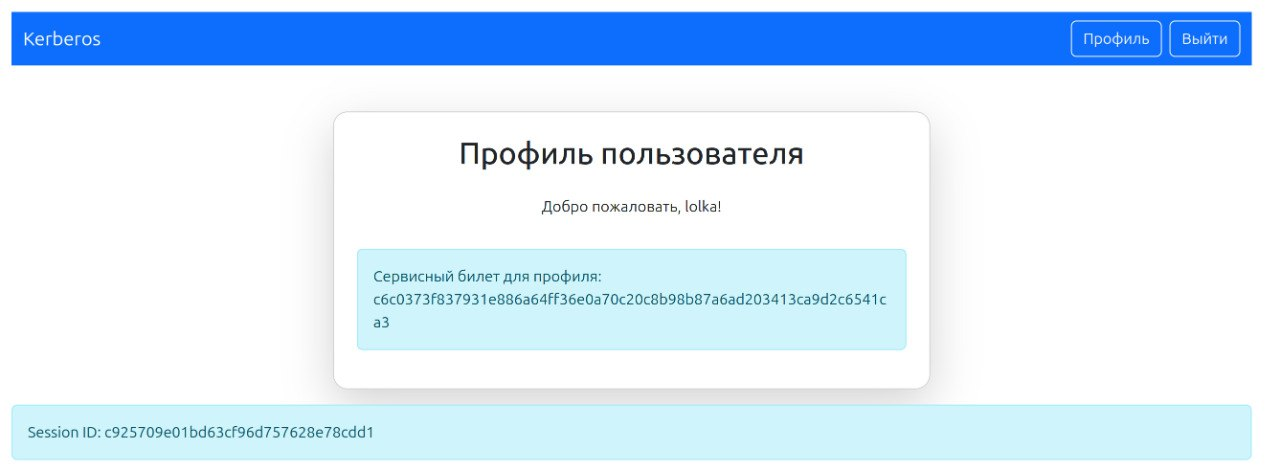


Рисунок 2 – Результат работы программы

# ЗАКЛЮЧЕНИЕ

Таким образом, в ходе выполнения работы было создано веб-приложение, обеспечивающее безопасную идентификацию и аутентификацию пользователей с использованием протокола *Kerberos*. Реализованные механизмы регистрации, входа и проверки сессии гарантируют защиту данных и контроль доступа к ресурсам.

Приложение обладает удобным интерфейсом, поддерживает работу с *PostgreSQL*, использует *Express.js* для обработки *HTTP*-запросов.

Для наглядной демонстрации работы протокола был разработан веб-сайт, который позволяет пользователям регистрироваться, входить в систему и получать доступ к ресурсам сайта. Это делает взаимодействие с системой интуитивно понятным даже для пользователей без глубоких технических знаний.