Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение

высшего образования

**«Пермский национальный исследовательский**

**политехнический университет»**

Факультет прикладной математики и механики

Кафедра «Вычислительная математика, механика и биомеханика»

Направление подготовки: 09.03.02 «Информационные системы и технологии»

**О Т Ч Е Т**

**по преддипломной практике**

(практике для выполнения выпускной квалификационной работы)

Выполнил студент гр.ИСТ-19-2б

\_\_\_\_\_\_\_\_\_\_Рачев Р.И.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(Фамилия, имя, отчество)*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_

*(подпись)*

**Проверили:**

cт. препод. Банников Р.Ю.

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(должность, Ф.И.О. руководителя от принимающей организации)*

*\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(оценка) (подпись)*

*\_\_\_\_\_\_\_\_\_\_\_\_\_*

МП *(дата)*

ст. препод. Горохов А.Ю.

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(должность, Ф.И.О. руководителя от кафедры)*

*\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(оценка) (подпись)*

*\_\_\_\_\_\_\_\_\_\_\_\_\_*

*(дата)*

**Пермь 2023**

Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение

высшего образования

**«Пермский национальный исследовательский**

**политехнический университет»**

Факультет прикладной математики и механики

Кафедра «Вычислительная математика, механика и биомеханика»

Направление подготовки: 09.03.02 «Информационные системы и технологии»

УТВЕРЖДАЮ

Зав. кафедрой ВММБ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_)

«\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ**

на преддипломную практику

студента группы ИСТ-19-2б

Рачева Руслана Игоревича

*(Фамилия, Имя, Отчество)*

**1. Тема индивидуального задания**: Разработка системы управления проектами и задачами

**2. ЦЕЛЬ: *Формирование компетенций в соответствии с требованиями программы практики:***

ПК-4.Б2.В.05 – способность проводить выбор исходных данных для проектирования;

ПК-22.Б2.В.05 – способность проводить сбор, анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования;.

**3. Календарный план проведения преддипломной практики**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Наименование этапа** | **Наименование работ** | **Сроки** | | **Отчетный**  **документ** | **Формируемые**  **компоненты**  **компетенций** |
| **начало** | **окон-чание** |
| 1 | **1 этап (подготовительный)** | Сбор информации о существующих решениях | 17.04 | 01.05 | Отчет по практике | ПК-4.Б2.В.05-з1 - знать основные методы и средства систематизации и внедрения исходных данных при проектировании.  ПК-22.Б2.В.05-з1 - знать основные методы и средства применения научно-технической информации в рамках научного исследования. |
| 2 | **2 этап (основной)** | Проведение обзора технологий для написания веб-приложения | 01.05 | 15.05 | Отчет по практике | ПК-4.Б2.В.05-у1 - уметь применять современные научно-технические разработки в рамках научно-исследовательской работы.  ПК-22.Б2.В.05-у1 – уметь применять современные научно-технические разработки при проектировании информационных систем и технологий.  ПК-22.Б2.В.05-в1 - владеть современными компьютерными и информационными средствами и технологиями анализа научно-технической информации. |
| 3 | **3 этап (итоговый)** | Разработка компонентов веб-приложения для автоматизации процесса учета сотрудников. Написание и сдача отчета по практике. | 30.04 | 08.05 | Отчет по практике | ПК-4.Б2.В.05-в1 – владеть навыками проектирования научно-технических систем на основе технического задания. |

**4. Место прохождения практики: \_\_\_**Кафедра ВММБ

**5. Срок сдачи студентом отчёта по преддипломной практике и отзыва руководителя практики от принимающей организации руководителю практики от кафедры:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_15.05.2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**6. Содержание отчёта**

\_\_\_В отчете представлена информация о важности авторизации в веб-приложениях, рассмотрен один из современных методов авторизации в микросервисных веб-приложения – использование JWT-токенов. Рассмотренный метод был реализован для поставленной задачи в рамках преддипломной работы.

**7. Требования к разрабатываемой отчётной документации**

Результаты преддипломной практики должны быть оформлены в форме отчёта по практике в соответствии с требованиями ГОСТ 7.32–2001 «Система стандартов по информации, библиотечному и издательскому делу. Отчёт о научно-исследовательской работе. Структура и правила оформления».

Страницы не обводятся в рамках, поля не отделяются чертой. Размеры полей не менее: левого – 30 мм, правого – 10 мм, верхнего – 20 мм и нижнего – 20 мм. Нумерация страниц отчёта - сквозная: от титульного листа до последнего листа приложений. Номер страницы на титульном листе не проставляют. Номер страницы ставят в центре нижней части листа, точка после номера не ставится. Страницы, занятые таблицами и иллюстрациями, включают в сквозную нумерацию.

Объём отчёта по преддипломной практике должен быть не менее 10 страниц (без учёта приложений) машинописного текста (шрифт 14пт, TimesNewRoman, через 1 интервал). Отчёт должен быть отпечатан на формате А4 и подшит в папку. Описания должны быть сжатыми. Объём приложений не регламентируется.

Титульный лист является первым листом отчёта, после которого помещается индивидуальное задание на практику, содержащее календарный план выполнения преддипломной практики. Титульный лист и задание не нумеруются, но входят в общее количество страниц. Титульный лист отчёта оформляется по установленной единой форме, приводимой в приложении. За индивидуальным заданием в отчёте помещается содержание, основная часть, заключение, список литературы, приложения. Основная часть включает 2–3 главы и разбивку на параграфы. К основному разделу отчёта прикладываются дневник по преддипломной практике (при необходимости) и отзыв руководителя практики от принимающей орга­низации*.*

Разделы отчёта нумеруют арабскими цифрами в пределах всего отчёта. Наименования разделов должны быть краткими и отражать содержание раздела. Переносы слов в заголовке не допускаются.

Цифровой материал необходимо оформлять в виде таблиц. Каждая таблица должна иметь номер и тематическое название. Таблицу следует помещать после первого упоминания о ней в тексте.

Приложения оформляют как продолжение отчёта. В приложении помещают материалы, не вошедшие в основной текст отчёта.

Руководитель практики

от кафедры ВММБ \_\_\_\_\_\_\_\_\_\_\_\_\_ ( )

*(Ф.И.О.)*

Руководитель практики

от принимающей организации

(структурного подразделения

ПНИПУ) \_\_\_\_\_\_\_\_\_\_\_\_\_ ( )

*(Ф.И.О.)*

Руководитель бакалавриата \_\_\_\_\_\_\_\_\_\_\_\_\_ ( )

*(Ф.И.О.)*

Задание принял к исполнению \_\_\_\_\_\_\_\_\_\_\_\_\_ ( )

*(Ф.И.О. студента)*

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**СОДЕРЖАНИЕ**

[Введение 1](#_Toc135298419)

[1. Авторизация с помощью JWT-токенов 2](#_Toc135298420)

[3. Разработка серверной части JWT-авторизации 4](#_Toc135298421)

[4. Разработка клиентской части JWT-авторизации 6](#_Toc135298422)

[Заключение 8](#_Toc135298423)

[Список литературы 9](#_Toc135298424)

Введение

В наше время, когда технологии проникают во все сферы нашей жизни, вопрос безопасности становится критически важным [1]. Виртуальный мир стал средой, где хранятся и обрабатываются большие объемы чувствительной информации.

Безопасность является неотъемлемой частью современного мира, а авторизация – основной аспект обеспечения безопасности в сетевых приложениях и системах.

Авторизация выполняет следующие функции:

1. Защита конфиденциальности данных. Системы авторизации обеспечивают конфиденциальность данных, позволяя ограничить доступ только уполномоченным пользователям. Они гарантируют, что только те лица, которым разрешен доступ, смогут просматривать, изменять или удалять информацию.
2. Защита от несанкционированного доступа. Авторизация помогает обнаруживать и блокировать попытки вторжения, а также пресекает несанкционированное использование привилегий и ресурсов.
3. Предотвращение мошенничества и кражи идентичности. Путем проверки подлинности пользовательских данных и учетных записей, системы авторизации обнаруживают попытки подделки или использования чужих данных.
4. Обеспечение целостности данных. Информация остается неизменной и неповрежденной, и только уполномоченные пользователи могут вносить изменения.
5. Управление правами доступа. С помощью различных уровней авторизации и ролей можно определить, какой доступ предоставляется каждому пользователю, основываясь на его роли, обязанностях или других факторах.

Важность авторизации в современном мире трудно переоценить. Недостаточная защита данных может привести к серьезным последствиям, включая утечку конфиденциальной информации, финансовые потери и утрату доверия клиентов [2]. Поэтому эффективная система авторизации является неотъемлемой частью разработки приложений и систем, обеспечивая безопасность, конфиденциальность и надежность.

1. Авторизация с помощью JWT-токенов

Авторизация с использованием JWT-токенов (JSON Web Tokens) является распространенным методом аутентификации и авторизации в веб-приложениях. JWT-токены представляют собой компактные и самодостаточные сущности, которые могут передаваться между клиентом и сервером в зашифрованном виде [3].

JWT-токен состоит из трех частей, разделенных точками (рис.1):

1. Заголовок (Header): Заголовок содержит информацию о типе токена и алгоритме шифрования, используемом для его подписи. Обычно это JSON-объект, содержащий два поля: "alg" (алгоритм) и "typ" (тип токена).
2. Полезная нагрузка (Payload): Полезная нагрузка содержит информацию о пользователе или другие данные, которые могут быть полезными для приложения. Это JSON-объект, который может содержать произвольные поля. Некоторые из стандартных полей включают "sub" (субъект) – идентификатор пользователя, "iss" (издатель) – идентификатор сервера, выдавшего токен, "exp" (срок годности) – время истечения токена и другие.
3. Подпись (Signature): Подпись используется для проверки подлинности токена и обеспечения целостности данных. Она создается путем кодирования заголовка и полезной нагрузки с использованием секретного ключа сервера (или публичного/приватного ключевой пары в случае использования асимметричного шифрования). Полученная подпись добавляется к токену. Подпись может быть проверена сервером при получении токена для удостоверения его подлинности.

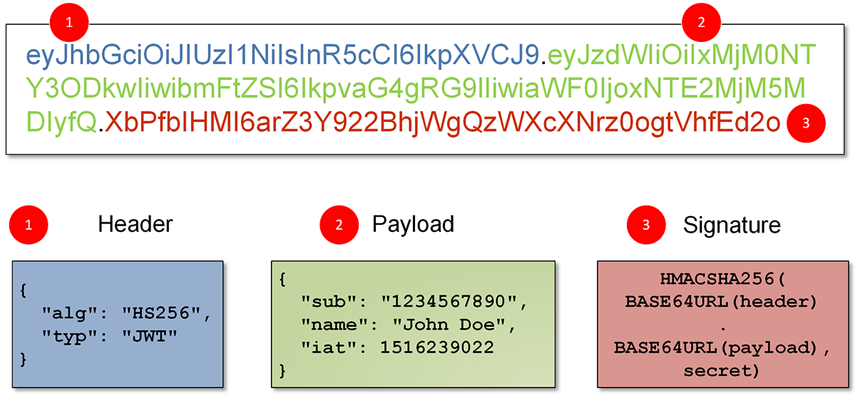


Рис.1 – Структура JWT-токена

Преимущества использования JWT-токенов для авторизации заключаются в их масштабируемости, удобстве и безопасности. Токены содержат всю необходимую информацию, что исключает необходимость обращения к базе данных для проверки подлинности на каждый запрос. Кроме того, так как токены шифруются и подписываются, они сложны для подделки, что повышает безопасность приложения.

Подобные токены не используются для хранения конфиденциальных данных. Их следует использовать только для проверки подлинности и авторизации пользователей.

JWT-авторизация предоставляет удобный и безопасный механизм для контроля доступа в веб-приложениях.

Процесс авторизации с помощью JWT-токенов состоит из нескольких шагов. Вот общий обзор этого процесса:

* Аутентификация: Пользователь предоставляет свои учетные данные, такие как имя пользователя и пароль, на сервере. Сервер проверяет правильность предоставленных данных.
* Выдача токена: Если аутентификация прошла успешно, сервер создает JWT-токен. Данный токен будет содержать всю необходимую информацию, используемую при авторизации в веб-приложении.
* Передача токена клиенту: JWT-токен передается клиенту, обычно в виде HTTP-заголовка "Authorization". Клиент может сохранить токен в памяти, в cookie или в локальном хранилище браузера.
* Проверка токена: Когда клиент отправляет запрос на защищенный маршрут, он включает токен в заголовок "Authorization". Сервер получает токен и проверяет его подлинность и целостность. Это включает проверку подписи, срока действия токена и других механизмов безопасности.
* Авторизация: После успешной проверки токена сервер устанавливает контекст авторизации для текущего пользователя, основываясь на информации в токене. Это позволяет приложению принимать решения о доступе пользователя к определенным ресурсам или операциям.

1. Разработка серверной части JWT-авторизации

Для разработки серверной части JWT-авторизации в веб-приложении в проект были добавлены следующие зависимости: Spring Security[4-5], Spring Web и jjwt.

При работе с JWT-авторизацией пользователю обычно выдается два вида токенов: AccessToken и RefreshToken [6].

Access токен (JWT-токен доступа) – это токен, который предоставляет авторизованному пользователю доступ к защищенным ресурсам на сервере. Он имеет ограниченный срок действия (например, несколько минут или часов) и может быть использован для проверки подлинности пользователя. При успешной аутентификации сервер генерирует Access токен и отправляет его клиенту, который затем включает его в заголовок авторизации при каждом запросе к защищенным ресурсам на сервере.

Refresh токен (JWT-токен обновления) имеет долгосрочный срок действия и используется для безопасного обновления Access токена без необходимости повторной аутентификации пользователя при каждом запросе.

Для генерации новых токенов пользователю были написаны следующие методы (рис.2):

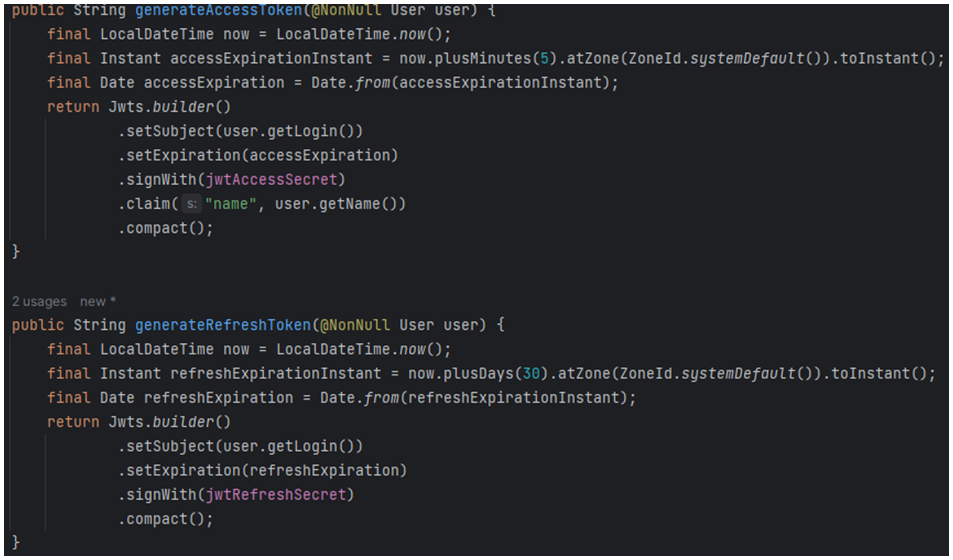


Рис.2 – Методы генерации токенов

А также метод проверки токенов, отправляемых пользователями на сервер (рис.3).

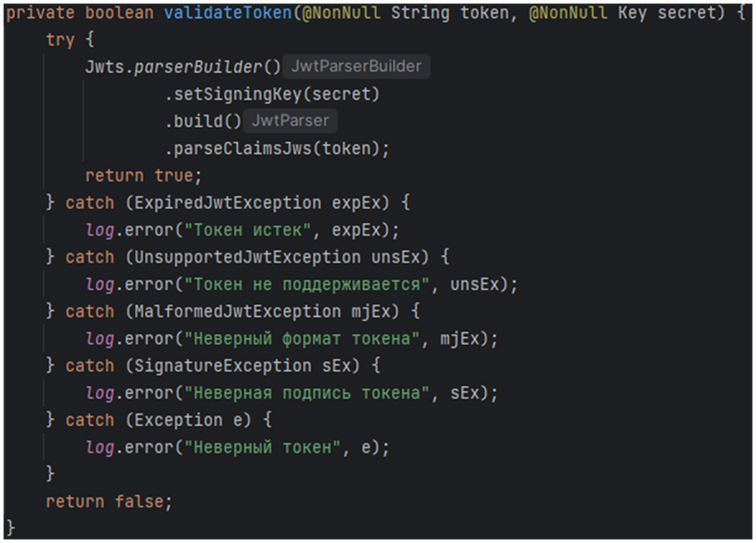


Рис.3 – Метод проверки токенов

Далее были написаны методы для поиска пользователя в базе, проверки его данных для входа, и в случае если они верны, возвращающие сгенерированные токены.

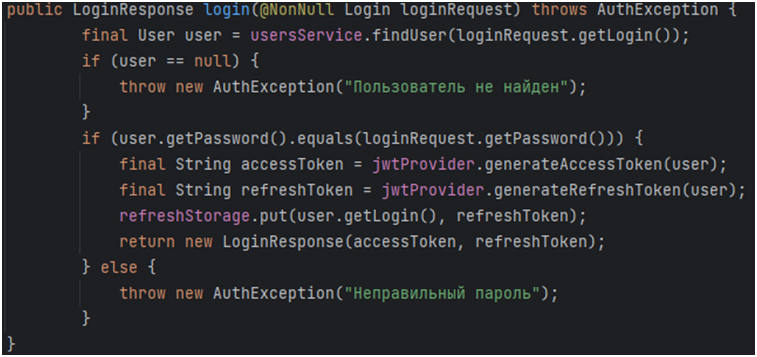


Рис.4 – Метод для проверки данных авторизации

В итоге был разработан контроллер, который будет принимать и обрабатывать запросы авторизации от клиентской части приложения. Он получает введенные пользователем данные, после чего проверяет их, с помощью описанных выше методов. После успешной проверки сгенерированные токены отправляются клиенту, и пользователь получает доступ к приложению.

1. Разработка клиентской части JWT-авторизации

Перед разработкой авторизации с использованием JWT-токенов на клиентской части веб-приложения предварительно необходимо было установить библиотеку для отправки запросов на сервер, в частности axios[7]. Данная библиотека позволяет перехватывать, а также обрабатывать все запросы и ответы перед их отправкой или после получения. Для достижения этого используются перехватчики (interceptors).

Перехватчики Axios предоставляют два метода: axios.interceptors.request и axios.interceptors.response.

Метод axios.interceptors.request позволяет добавлять перехватчик для всех исходящих запросов (рис.2). Он используется для того, чтобы модифицировать заголовки запроса, добавлять авторизационные данные, устанавливать общие параметры и т. д.

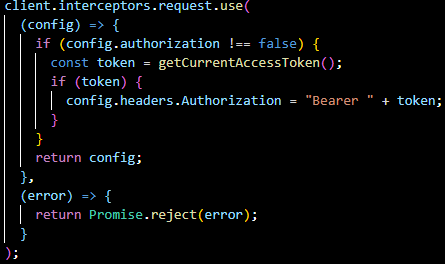


Рис.2 – Пример использования перехватчика запросов

Метод axios.interceptors.response позволяет добавлять перехватчик для всех входящих ответов (рис.3). Он используется для обработки успешных ответов, обработки ошибок, преобразования данных и т. д.

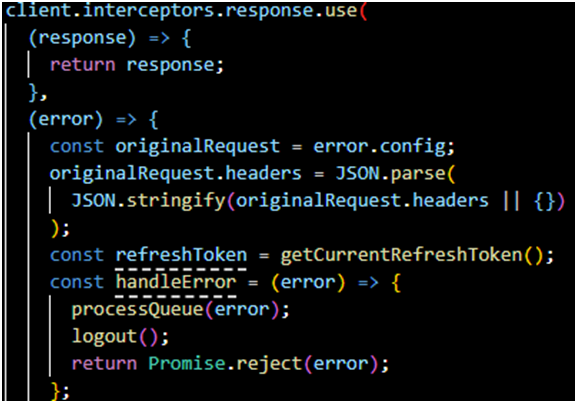


Рис.3 – Пример использования перехватчика ответов

Данные методы являются основными при разработке авторизации на клиентской части веб-приложения . Они позволяют получать и сохранять JWT-токены отправленные пользователю при авторизации, а также запрашивать новые токены, если срок действия старых истек [8-9].

Заключение

Авторизация играет ключевую роль в обеспечении безопасности информации и систем, предотвращая несанкционированный доступ и защищая конфиденциальность данных.

Системы авторизации позволяют ограничить доступ к чувствительным данным только уполномоченным пользователям, предотвращая утечку информации и кражу идентичности. Они обеспечивают целостность данных и позволяют эффективно управлять правами доступа, обеспечивая гибкость и контроль над тем, какие ресурсы и функциональности могут быть использованы.

Важность авторизации простирается на множество сфер, включая банковское дело, электронную коммерцию, здравоохранение, социальные сети и многие другие. Недостаточная защита данных может привести к серьезным последствиям.

Разработка и реализация надежных систем авторизации должны стать приоритетом для организаций и разработчиков. Это включает использование современных методов аутентификации, таких как JWT-токены. Данный метод был подробно рассмотрен и разобран в работе. Была описана структура JWT-токенов и принцип работы с ними. Также метод был использован в ходе разработки системы управления проектами и задачами.

Важность авторизации в наше время неразрывно связаны с обеспечением конфиденциальности, целостности и доступности информации. Системы авторизации играют решающую роль в защите данных и обеспечении доверия пользователей. Только с надежными и эффективными механизмами авторизации возможно строить безопасное и устойчивое цифровое общество.

Список литературы

1. Капитонов В.В. Информационная безопасность и ее важность в современных реалиях. // Актуальные вопросы современной науки и практики. –2019. –C. 61-65.
2. Камалов М.К., Окас А.Е. Важность защищенной системы обработки информации на основе актуальных проблем информационной безопасности. // Актуальные научные исследования в современном мире. –2019. –№5-7(49). –C. 22-25.
3. Бетелин А.Б., Егорычев И.Б., Прилипко А.А., Прилипко Г.А., Романюк С.Г., Самборский Д.В. О некоторых особенностях JWT аутентификации в веб-приложениях. // Труды Научно-исследовательского института системных исследований Российской академии наук. –2021. –№1. –C. 4-10.
4. Spring Security [Электронный ресурс]. // Spring. URL : https://spring.io/projects/spring-security (дата обращения: 13.05.23).
5. Абдурайимов Л.Н. Аутентификация в Rest-приложениях с использованием Spring Security и JWT. // Информационно-компьютерные технологии в экономике, образовании и социальной сфере. –2021. –№4(34). –С. 5-13.
6. Матюшин Д.С., Богорадникова А.В. Генерация токена авторизации посредством библиотеки JWT // Актуальные вопросы в науке и практике. –2018. –С. 91-94.
7. Getting Started | Axios Docs [Электронный ресурс]. // Axios. URL : https://axios-http.com/docs/intro (дата обращения: 13.05.23).
8. Козлов С.В., Воробьев М.С. Реализация аутентификации пользователя в Web-приложении с использованием стандарта JWT. // Системы компьютерной математики и их приложения. –2022. –№23 –C. 362-366.
9. Васильев П.А. Технология JWT языка программирования Node JS. // Бизнес-образование в экономике знаний. –2016. –№ 8(20). –С. 32-33.