С. Е. Иванов, А. А. Оленников
Тюменский государственный университет, г. Тюмень
УДК 004.056.5

РАЗРАБОТКА ЗАЩИЩЕННОГО ОБЛАЧНОГО СЕРВИСА ДЛЯ ПРОЕКТИРОВАНИЯ СХЕМ ЭНЕРГОУТИЛИЗАЦИИ МЕТАЛЛУРГИЧЕСКИХ АГРЕГАТОВ

Аннотация. В статье рассматривается разработка облачного сервиса, обеспечивающего безопасное выполнение сложных инженерных расчетов при проектировании схем энергоутилизации металлургических агрегатов. Представлена архитектура защищенного облачного кластера, на котором развернут программный комплекс для моделирования и оптимизации схем утилизации тепловой энергии. Описаны примененные методы обеспечения информационной безопасности: защищенное хранение данных, аутентификация и авторизация пользователей, механизм разграничения доступа и другие меры. Сделаны выводы об эффективности предложенного решения для повышения энергоэффективности металлургических производств за счет использования облачных технологий.

Ключевые слова: облачные вычисления, энергоутилизация, металлургические агрегаты, информационная безопасность, высокодоступный кластер, веб-сервис, RBAC.

Введение. Металлургическая отрасль характеризуется высоким энергопотреблением и значительными потерями тепла с отходящими газами и другими теплоносителями [1]. По данным современных российских исследований, до 30% тепловой энергии в ряде технологических процессов металлургии теряется и не используется вторично [2], что формирует значительный резерв для повышения энергоэффективности производства. В современных металлургических агрегатах (доменных печах, сталеплавильных конвертерах и др.) имеются большие резервы для вторичного использования тепловой энергии, например посредством установки теплообменников, парогенераторов и газотурбинных установок [3]. Проектирование комплексной схемы энергоутилизации, пример которой показан на рис. 1 — является сложной инженерной задачей, требующей учета термодинамики, газодинамики, теплообмена и экономических показателей.

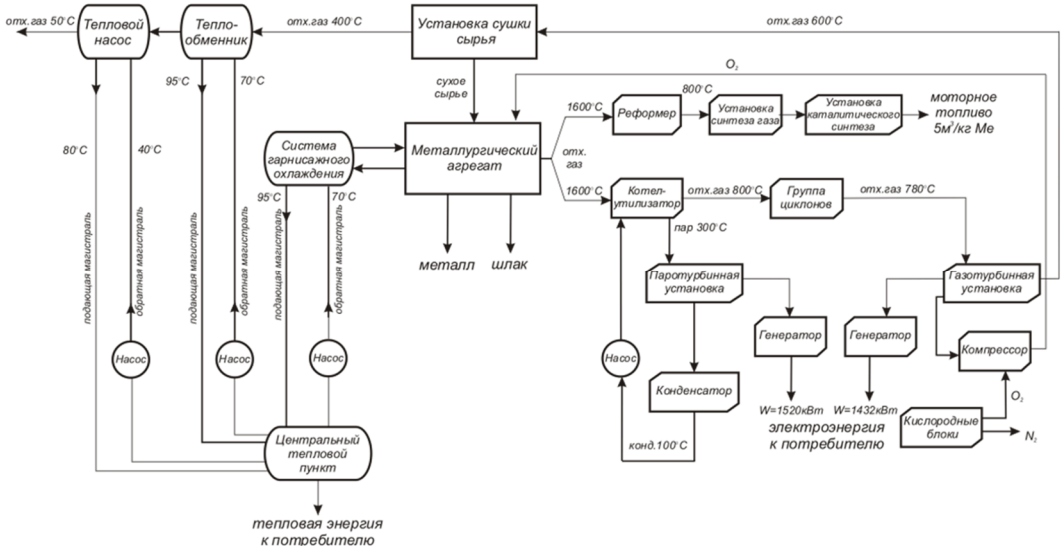

Рис. 1. Пример схемы энергоутилизации для металлургического агрегата (утилизация тепла отходящих газов и охлаждающей системы с выработкой пара, и электроэнергии)

Разработка подобных схем традиционно осуществлялась с использованием специализированных расчетных программ на рабочих станциях инженеров [4]. Однако локальные вычислительные ресурсы могут быть недостаточны для быстрого проведения многовариантных расчетов, особенно при оптимизации больших систем утилизации. В последнее время наблюдается тенденция перехода к облачным вычислениям в инженерных задачах: специалисты получают возможность выполнять ресурсоемкие симуляции на удаленных высокопроизводительных кластерах через веб-интерфейсы [5]. Это ускоряет расчеты и позволяет нескольким инженерам совместно работать над проектом в режиме онлайн.

В то же время перенос инженерного программного комплекса в облако требует особого внимания к вопросам информационной безопасности. Необходимо защитить ценные алгоритмы и данные расчетов от несанкционированного доступа, обеспечить сохранность результатов и персональных данных пользователей, а также гарантировать надежную работу сервиса при сетевых сбоях и попытках атак. Таким образом, актуальной является задача создания защищенного облачного сервиса для проектирования схем энергоутилизации — платформы, обеспечивающей удаленный доступ к мощным вычислительным ресурсам для расчета тепловых схем при строгом соблюдении мер безопасности.

Цель данной работы — разработать и внедрить облачный сервис (в виде кластера виртуальных серверов), на котором развернут программный комплекс для проектных расчетов схем энергоутилизации металлургических агрегатов, с обеспечением требуемого уровня информационной безопасности. Для достижения поставленной цели необходимо было решить следующие задачи:

1. проанализировать архитектуру и функциональные возможности исходного расчетного программного комплекса;
2. изучить существующие подходы к защите программного обеспечения и данных в облаке;
3. разработать модель нарушителя и модель угроз для данного сервиса;
4. спроектировать архитектуру облачного кластера, обеспечивающую отказоустойчивость и масштабируемость;
5. реализовать облачный сервис — собрать кластер и развернуть на нем программный комплекс;
6. разработать и интегрировать подсистемы безопасности (аутентификация, авторизация, защита данных);
7. провести тестирование работоспособности и безопасности сервиса в режиме онлайн.

Постановка задачи проектирования. Необходимо обеспечить возможность удаленного доступа пользователей (инженеров-проектировщиков) к программному комплексу расчета схем энергоутилизации. Сервис должен позволять загружать исходные данные технологического процесса (параметры отходящих потоков тепла, характеристики оборудования и др.), выполнять серии вычислительных экспериментов (моделирование тепловых процессов, оптимизация конфигурации оборудования) и предоставлять результаты в виде, пригодном для последующего использования в проектной документации. При этом сервис предназначен для

многопользовательской работы: предполагается, что разные организации (заводы) могут эксплуатировать систему для своих задач, поэтому нужна поддержка нескольких аккаунтов с разграничением прав доступа (обычные пользователи и администраторы).

Требования к производительности и масштабируемости. Программный комплекс SKV_Sapr включает в себя модули расчета термодинамических параметров, аэродинамики газовых потоков, сложного теплообмена, оптимизационного подбора размеров аппаратов и др. (см. рис. 2). Совокупная вычислительная нагрузка при моделировании большой схемы может быть очень высокой, поэтому сервис должен обладать достаточной производительностью. Заложено требование горизонтального масштабирования: архитектура должна допускать добавление новых вычислительных узлов для повышения производительности по мере роста числа пользователей или сложности моделей. Применение кластерного решения обеспечивает и высокий уровень доступности сервиса — при выходе из строя одного узла его задачи должны автоматически перенаправляться на другие узлы без остановки сервиса.

Требования к безопасности. Разрабатываемый сервис должен удовлетворять современным требованиям информационной безопасности. Это включает: защиту веб-приложения от наиболее распространенных уязвимостей (SQL-инъекции, межсайтовый скриптинг и пр.), безопасное хранение аутентификационных данных пользователей (паролей), шифрование конфиденциальной информации при передаче и хранении, а также надежную аутентификацию и авторизацию. Следует реализовать систему разграничения доступа на основе ролей (role-based access control, RBAC), чтобы исключить несанкционированные операции пользователей.

Таким образом, в рамках работы решается комплексная задача: создание облачной платформы для ресурсоемких инженерных расчетов с многоуровневой системой безопасности. Для ее решения выбрана стратегия развертывания программного комплекса в виде набора взаимодействующих сервисов в виртуальном кластере под управлением специализированной платформы виртуализации. Ниже описаны методы и архитектурные решения, использованные для реализации поставленной задачи.

Общий подход. Учитывая перечисленные требования, была спроектирована модульная архитектура программного решения, в которой различные функциональные компоненты отделены друг от друга. Ядром системы является существующий расчетный **программный комплекс** *SKV_Sapr* для теплотехнического моделирования. Он включает набор математических моделей: модели теплопередачи, газодинамики, расчета эффективности использования энергии и экономических показателей (капитальных затрат) — см. структурную схему на рис. 2.

Вокруг этого ядра разработана облачная оболочка, предоставляющая веб-интерфейс, управление задачами и средства обеспечения безопасности. Для реализации сервиса выбран кластерный подход: программные компоненты размещены на нескольких виртуальных машинах, объединенных в единый кластер. В качестве платформы виртуализации использовано решение Proxmox VE [6] — оно позволяет создавать кластер из нескольких физических узлов с централизованным управлением и автоматизацией развертывания виртуальных серверов.

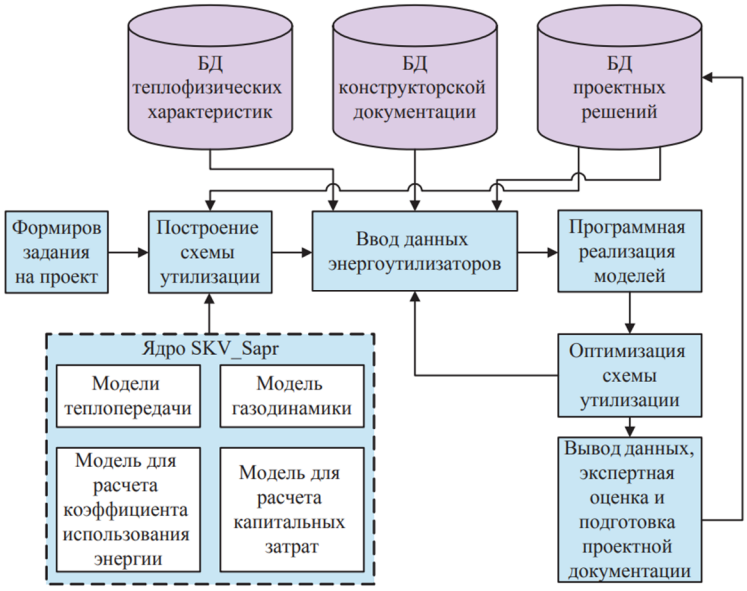

Рис. 2. Структура программного комплекса и данных для проектирования схем энергоутилизации (ядро SKV_Sapr и связанные модули)

Анализ угроз и выбор средств защиты. На этапе проектирования проведен анализ возможных угроз безопасности облачного сервиса. Выделены следующие потенциальные векторы атак: 1) попытки SQL-инъекций через веб-формы ввода исходных данных; 2) подбор или компрометация паролей учетных записей; 3) эскалация привилегий (попытка обычного пользователя получить доступ к административным функциям); 4) атаки типа DoS на сервис; 5) несанкционированный доступ к данным при передаче по сети. Для нейтрализации выявленных угроз в архитектуру решения включены соответствующие меры.

Во-первых, для предотвращения SQL-инъекций все обращения к базе данных реализованы с использованием параметризированных запросов (prepared statements) вместо конкатенации строк SQL [7]. Такой подход заставляет разделять текст SQL-запроса и параметры и исключает исполнение вставляемых данных как кода. Во-вторых, для защиты паролей применен алгоритм криптостойкого хеширования BCrypt с солью. При создании нового пользователя вводимый пароль сразу проходит через функцию хеширования BCrypt, которая автоматически добавляет криптографическую соль и многократно (с заданным work factor) вычисляет хеш. В результате в базе данных хранится только хеш пароля, и даже в случае утечки базы восстановить исходные пароли практически невозможно. Данный метод полностью соответствует рекомендациям OWASP по хранению паролей и защищает от атак с использованием радужных таблиц и перебора паролей.

В-третьих, реализована строгая система аутентификации и авторизации на основе JWT-токенов (JSON Web Token) [8]. При входе пользователя в систему после проверки его учетных данных сервер генерирует JWT-токен, подписанный алгоритмом HMAC-SHA256 с секретным ключом. Токен содержит в полезной нагрузке (payload) информацию о пользователе, в том числе его роль (обычный пользователь или администратор). Все последующие запросы клиента к сервису должны содержать этот токен в заголовке авторизации. Сервер при получении запроса сначала проверяет подпись JWT, убеждаясь в его подлинности и неизменности, а затем извлекает роль пользователя. Если токен отсутствует, недействителен или пользователь

пытается выполнить действие, не соответствующее его роли, доступ запрещается (возвращаются коды ошибок 401 Unauthorized или 403 Forbidden). Благодаря включению роли пользователя непосредственно в токен JWT, система может быстро проверять права доступа без дополнительного обращения к базе данных для каждого запроса. Это повышает производительность и упрощает масштабирование сервиса при росте числа пользователей.

В-четвертых, для защиты от отказов и обеспечения доступности сервис развернут в виде кластера с избыточными компонентами. Были выбраны методы виртуализации, позволяющие переносить выполняющиеся задачи между узлами кластера. В данной работе применена кластеризация на уровне гипервизора (Proxmox) с использованием keepalived внутри виртуальных машин. Два физических узла объединены в кластер, и на каждом узле запущены экземпляры основных сервисов (балансировка, веб-интерфейс, база данных, вычислительные модули). Между узлами настроено дублирование функций: отказ одного из узлов не приводит к недоступности системы, так как второй узел продолжает обработку запросов. Также настроено регулярное резервное копирование виртуальных машин кластера для восстановления в случае сбоя оборудования.

Облачный кластер и его компоненты. Разработанный облачный сервис развернут на кластере из двух физических серверов, соединенных локальной сетью. На каждом сервере установлено ПО Proxmox VE, образуя единый кластер виртуализации. Поверх гипервизора на каждом узле запущены несколько виртуальных машин, отвечающих за разные роли (см. рис. 3). Выделены следующие основные компоненты системы:

- **Балансировщик нагрузки и DNS:** на отдельной VM установлен HAProxy, распределяющий входящие сетевые запросы между узлами, а также DNS-сервер (Dnsmasq) для внутреннего именования сервисов. HAProxy обеспечивает равномерную загрузку вычислительных модулей и выполняет проверку доступности узлов (health-checks), перенаправляя трафик при отказе одного из них.
- **Веб-сервер и база данных:** еще одна виртуальная машина на каждом узле запускает веб-сервис и СУБД. В качестве веб-сервера используется связка Nginx + FastAPI (Python) — Nginx работает как обратный прокси, раздавая статические файлы интерфейса и перенаправляя API-запросы на приложение FastAPI. Последнее реализует REST API для взаимодействия с расчетным ядром. СУБД PostgreSQL хранит данные пользователей, проектов и результаты. Используется тип данных JSONB для гибкого хранения сложных структур (например, параметров схем и полученных полей результатов), что позволяет легко добавлять новые виды данных без изменения схемы БД.
- **Вычислительный модуль:** основной расчетный комплекс (SKV_Sapr) запускается на отдельной виртуальной машине на каждом узле. Он взаимодействует с веб-приложением через API. В реализации, описанной в данной работе, использована модель, при которой веб-приложение вызывает вычислительный модуль напрямую через HTTP-запросы (асинхронно, используя HTTPX), что упростило архитектуру.

Сетевая структура и безопасность. Внешний доступ к кластеру осуществляется через двухмаршрутный Интернет-шлюз. Каждый физический узел имеет подключение к двум независимым интернет-провайдерам (две подсети WAN1 и WAN2 на рис. 3) через сетевой экран (межсетевой экран DFL860E). Это повышает отказоустойчивость внешнего соединения. Внутри кластера организована отдельная управляемая сеть для служебного трафика Proxmox

(синхронизация узлов, миграция виртуальных машин) и для обмена данными между сервисами. На рис. 3 различными цветами показаны сегменты трафика: желтый — управление кластером, зеленый — взаимодействие сервисов (между веб, БД и вычислительными модулями), синий — трафик балансировки и DNS, красный — пользовательские обращения. Коммутация внутри кластера осуществляется через управляемый коммутатор (Cisco Catalyst). Каждый виртуальный узел имеет свой внутренний IP-адрес; при этом HAProxy принимает внешние запросы и перенаправляет их на внутренние адреса сервисов. Такая многослойная топология (DMZ с балансировщиком, отдельная сеть для внутренних сервисов) укрепляет безопасность: напрямую до вычислительных узлов внешний трафик не доходит, сначала проходя через узел с ограниченной функциональностью (HAProxy).

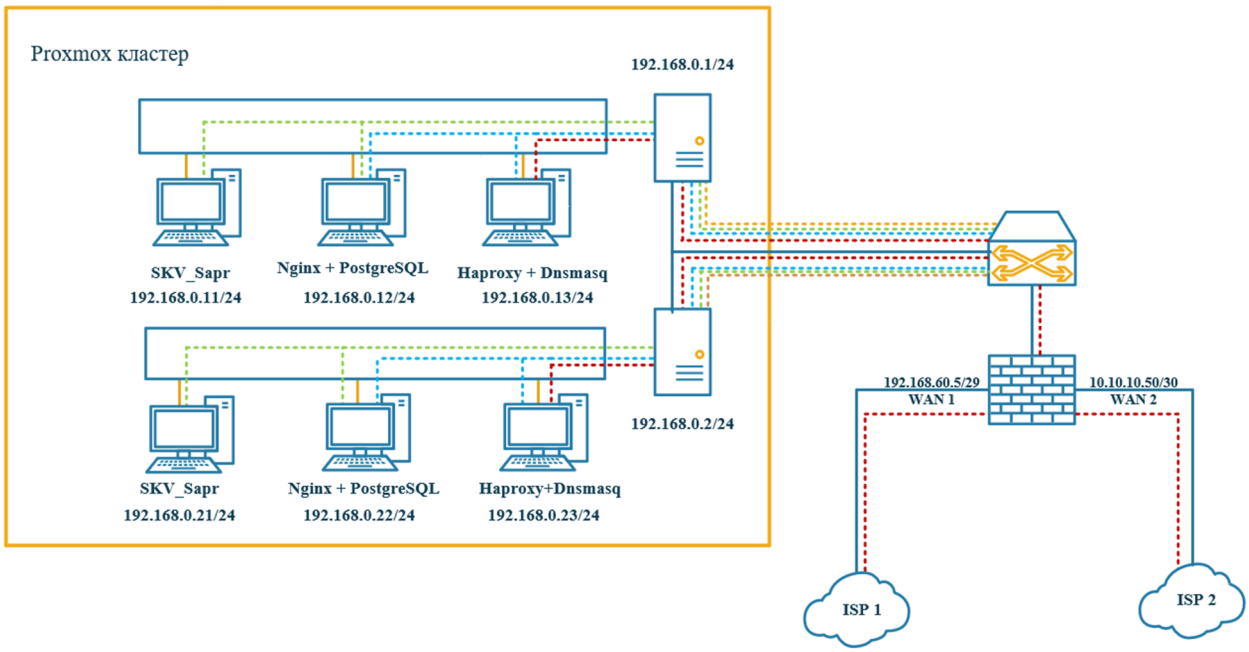

Рис. 3. Логическая топология защищенного облачного кластера (двухузловой кластер Proxmox с дублированием сервисов, балансировщик нагрузки, файервол и резервирование интернет-каналов)

Кроме того, реализован межсетевой экран, фильтрующий входящие соединения: открыт только необходимый порт для веб-доступа (HTTPS) доступ возможен только с определенных IP-адресов, согласованных при заключении контракта о предоставлении услуг.

Важно отметить, что архитектура решения носит черты микросервисного подхода — функциональные компоненты (балансировка, веб-интерфейс, расчет, БД) разделены и могут масштабироваться независимо. Подобный подход повышает гибкость системы и упрощает ее сопровождение. Например, при возрастании нагрузки можно запустить дополнительный экземпляр вычислительного модуля на новом узле, не затрагивая работу остальных частей. В микросервисной архитектуре отдельные сервисы легко масштабировать горизонтально и отказы отдельных компонентов не выводят из строя всю систему. В данной реализации независимое масштабирование ограничено рамками кластера из двух узлов, но заложенные принципы позволят расширить систему до большего числа узлов при развертывании в промышленной эксплуатации.

Заключение. В ходе выполнения данной работы создан защищенный облачный сервис для проектирования схем энергоутилизации металлургических агрегатов. Сервис представляет собой кластер виртуальных серверов, на которых развернут программный комплекс теплотехнического моделирования. В архитектуре решения применены современные технологии облачной инфраструктуры и реализованы необходимые механизмы информационной безопасности. Благодаря использованию кластерного подхода достигнута высокая отказоустойчивость и возможность масштабирования системы — добавление новых узлов позволяет нарастить вычислительную мощность под увеличивающуюся нагрузку пользователей.

Реализованный комплекс мер безопасности (защита от SQL-инъекций, хеширование паролей, JWT-аутентификация с RBAC и др.) обеспечивает надежную защиту программного комплекса и данных пользователей при его облачном развертывании. Предложенный подход позволяет предприятиям использовать сложные инженерные расчеты в формате облачного сервиса, не инвестируя средства в собственные вычислительные мощности и их поддержку.

Работа показала, что критически важные приложения, такие как системы расчета энергоутилизации, могут быть успешно перенесены в облачную среду без компромиссов в безопасности и с выигрышем в эффективности. В будущем планируется дальнейшее развитие сервиса: интеграция дополнительных модулей расчета (например, моделирование процессов горения, анализ выбросов), расширение функционала пользовательского интерфейса, а также аттестация системы на соответствие государственным стандартам защиты информации. Полученные результаты могут быть использованы при создании аналогичных защищенных облачных решений в области промышленной энергетики и инженерного анализа.

СПИСОК ЛИТЕРАТУРЫ

1. Тахеци И., Коробейников В. В., Ткаченко С. С. Снижение тепловых потерь жидкого метала — залог эффективности литейного производства // Литье и металлургия. — 2022. — № 2. — URL: https://cyberleninka.ru/article/n/snizhenie-teplovyh-poter-zhidkogo-metala-zalog-effektivnosti-liteynogo-proizvodstva (дата обращения: 20.04.2025).
2. Казачков Е. А., Исайчикова С. Г. Исследование тепловых потерь в 350 — т сталеразливочном ковше // ГВУЗ «Приазовский государственный технический университет». — 2000. — № 9. — URL: https://cyberleninka.ru/article/n/issledovanie-teplovyh-poter-v-350-t-stalerazlivochnom-kovshe (дата обращения: 22.04.2025).
3. Бушуев А. Н., Картавцев С. В. Об энергоэффективности теплового генерирующего источника на базе паротурбинного цикла для сталеплавильного производства // Энергобезопасность и энергосбережение. — 2012. — № 5. — URL: https://cyberleninka.ru/article/n/ob-energoeffektivnosti-teplovogo-generiruyuschego-istochnika-na-baze-paroturbinnogo-tsikla-dlya-staleplavilnogo-proizvodstva (дата обращения: 24.04.2025).
4. Вахтин А. А., Видикер В. Г. Математическое моделирование на ЭВМ теплоэнергетических процессов при переделе слитков в металлургическом производстве // ГВУЗ «Приазовский государственный технический университет». — 2000. — № 9. — URL: https://cyberleninka.ru/article/n/matematicheskoe-modelirovanie-na-evm-teploenergeticheskih-protsessov-pri-peredele-slitkov-v-metallurgicheskom-proizvodstve (дата обращения: 26.05.2025).

5. Сухорослов О. В. Интеграция вычислительных приложений и распределенных ресурсов на базе облачной программной платформы // Программные системы: теория и приложения. — 2014. — № 4 (22). — URL: https://cyberleninka.ru/article/n/integratsiya-vychislitelnyh-prilozheniy-i-raspredelennyh-resursov-na-baze-oblachnoy-programmnoy-platformy (дата обращения: 01.05.2025).
6. Баранов А. В., Киселев Е. А. Облачные сервисы для научных высокопроизводительных вычислений на базе платформы proxmox // ЖВТ. — 2019. — № 6. — URL: https://cyberleninka.ru/article/n/oblachnye-servisy-dlya-nauchnyh-vysokoproizvoditelnyh-vychisleniy-na-baze-platformy-proxmox (дата обращения: 02.05.2025).
7. Алиева Е. М. К., Ширинова Ш. З. К. Актуальность атак с использованием sql-инъекций // In The World Of Science and Education. — 2025. — № 15 март ELB. — URL: https://cyberleninka.ru/article/n/aktualnost-atak-s-ispolzovaniem-sql-inektsiy (дата обращения: 04.05.2025).
8. Макаров Д. А. Механизм авторизации с использованием технологии JWT // Теория и практика современной науки. — 2020. — № 1 (55). — URL: https://cyberleninka.ru/article/n/mehanizm-avtorizatsii-s-ispolzovaniem-tehnologii-jwt (дата обращения: 05.05.2025).