

## **РАЗРАБОТКА СИСТЕМЫ РОЛЕЙ И КОНТРОЛЯ ДОСТУПА К ТРЕНАЖЁРУ УПРАВЛЕНИЯ УЧЕБНЫМИ ПРОЕКТАМИ EDUFLOW**

Плешнев А. В., Москалец Д. А., Карагулов М. Р.  
(Университет ИТМО)

Научные руководители – к.т.н., доцент Горлушкина Н.Н., аспирант Афанасьев А.В.  
(Университет ИТМО)

### **Введение**

В рамках факультета ФПИИ используется система – тренажер для управления учебными проектами на базе Odoo [1]. Odoo стало узким местом для дальнейшего развития системы. Разработка представляет собой эволюционное развитие существующей, успешно апробированной системы в полноценный тренажер проектной деятельности. Система за три года эксплуатации доказала свою востребованность – она была использована для организации проектной деятельности одновременно более 250 студентов.

В тренажере EDUFlow большое количество функций. Рассмотрим функцию контроля доступа.

Цель работы – создать модуль ролевого контроля доступа [2], интегрированный в существующую инфраструктуру EDUflow, который обеспечит:

- определение и гибкое конфигурирование ролей пользователей (студент, магистрант-руководитель, преподаватель, администратор);
- авторизацию через OAuth 2.0 / OpenID Connect [X] с выдачей JWT-токена и проверкой его Auth-guard-ом в SPA (React);
- политику прав на уровне функций (просмотр, создание, редактирование, удаление) с динамическим отображением UI-компонентов в зависимости от роли;
- логирование всех действий в таблице access\_logs для последующего аудита;
- список сессий пользователя.

### **Основная часть**

Система управления учебными проектами, подробно ее структура была изложена на конференции Научно и учебно-методической конференции ИТМО [X], позволяет: студентам (бакалаврам - участникам проекта) увидеть предложения по разным проектам, после создания резюме, и подать заявку на участие в выбранном проекте, с возможностью выбора приоритетов; студентам (магистрантам - руководителям) представлять свои проекты, выбирать в свою команду кандидатов, управлять задачами и их выполнением в команде на канбан-доске. Работа в системе позволяет улучшить коммуникацию между участниками и повысить заинтересованность выполнения проекта, так как происходит знакомство с инструментами коллективной проектной работы.

Разработанная функция контроля доступа пользователя позволяет гибко определять разрешения для каждого пользователя: на основании роли, которая присвоена пользователю администратором, а также на основании индивидуальных пользовательских разрешений.

Реализована система сессий, благодаря которой пользователь может контролировать все активные подключения к тренажеру через его аккаунт.

Модуль ролевого контроля построена на модульной архитектуре. Backend используется базу данных, включающую таблицы: user, role, user\_permission, role\_permission, access\_logs (журнал действий). Каждой роли ставится в соответствие набор разрешений, определяющих допустимые операции над ресурсами системы.

Разграничение ролей реализовано следующим образом. Студенты-бакалавры получают доступ к просмотру задач, загрузке материалов и фиксации прогресса в рамках своего проекта. Магистранты-руководители дополнительно могут создавать задачи, назначать их участникам команды и отслеживать общий прогресс. Преподаватели обладают правами просмотра и оценивания всех проектов, а также управления составом команд. Администраторы имеют полный доступ к системе, включая управление учетными записями, назначение ролей и просмотр журнала аудита.

Frontend взаимодействует с backend-ом через OAuth 2.0 / OpenID Connect: при входе в систему пользователь получает JWT-токен, содержащий информацию о его роли. Auth-guard на стороне frontend проверяет токен и динамически отображает или скрывает UI-компоненты в соответствии с правами пользователя.


Тестирование охватывает unit-тесты бизнес-логики разграничения прав (pytest, покрытие  $\geq 80\%$ ) и security-тесты на устойчивость к несанкционированному повышению привилегий. Что будет рассмотрено в рамках КМУ Никиты [X] Система развернута в Docker Compose с контейнерами backend, frontend и базы данных.


### Выводы

Разработанный модуль ролевого контроля доступа успешно интегрирован в EDUflow, обеспечивая гибкое разграничение прав четырёх ролей пользователей и полное аудирование действий. Реализованная модель RBAC позволяет администраторам оперативно добавлять новые роли и перераспределять разрешения без изменения кода. Проведённые тесты подтвердили корректность работы и безопасность решения. В дальнейшем планируется добавить поддержку составных ролей, интеграцию с системой уведомлений об изменении прав, а также расширенную аналитику по журналам доступа.

### Список использованных источников

1. Open source ERP and CRM [Электронный ресурс] URL: <https://www.odoo.com/> (дата обращения: 24.02.2026).
2. Управление доступом на основе ролей [Электронный ресурс] URL: [https://en.wikipedia.org/wiki/Role-based\\_access\\_control](https://en.wikipedia.org/wiki/Role-based_access_control) (дата обращения: 21.02.2026).
3. Афанасьев А.В., Горлушкина Н.Н., Шутов Д.Э. Разработка информационного обеспечения системы управления проектной деятельностью студентов. Экономика. Право. Инновации. 2023. № 2. С. 92–101. URL: <https://books.ifmo.ru/file/pdf/3256.pdf> (дата обращения: 20.02.2026).
4. Ferraiolo D., Kuhn R. Role-Based Access Controls // Proceedings of the 15th National Computer Security Conference. 1992. P. 554–563.
5. Docker Documentation. [Электронный ресурс] URL: <https://docs.docker.com/> (дата обращения: 21.02.2026).
6. OpenID Connect Core 1.0. [Электронный ресурс] URL: [https://openid.net/specs/openid-connect-core-1\\_0.html](https://openid.net/specs/openid-connect-core-1_0.html) (дата обращения: 21.02.2026).

 / Горлушкина Н.Н. /  
(подпись)

 / Карагулов М. Р. /  
(подпись)