

Министерство науки и высшего образования Российской Федерации  
Санкт-Петербургский политехнический университет Петра Великого  
Институт компьютерных наук и кибербезопасности

Работа допущена к защите  
Руководитель ОП  
\_\_\_\_\_ И.О. Фамилия  
«\_\_\_\_\_» \_\_\_\_\_ 202\_ г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**  
**РАБОТА БАКАЛАВРА**  
**РАЗРАБОТКА КОМПОНЕНТОВ АУТЕНТИФИКАЦИИ, АВТОРИЗАЦИИ**  
**И УЧЕТА В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ**

по направлению подготовки 09.03.03 Прикладная информатика  
Направленность (профиль) 09.03.03\_03 Интеллектуальные инфокоммуникацион-  
ные технологии

Выполнил  
студент гр. 5130903/20302

Н.Ю. Каралюс

Руководитель  
должность,  
степень, звание<sup>1</sup>

И.О. Фамилия

Консультант<sup>2</sup>  
должность, степень

И.О. Фамилия

Консультант  
по нормоконтролю<sup>3</sup>

И.О. Фамилия

Санкт-Петербург  
2026

---

<sup>1</sup> Должность указывают сокращенно, учёную степень и звание — при наличии, а подразделения — аббревиатурами. «СПбПУ» и аббревиатуры институтов не добавляют.

<sup>2</sup> Оформляется по решению руководителя ОП или подразделения. Только 1 категория: «Консультант». В исключительных случаях можно указать «Научный консультант» (должен иметь степень). Без печати и заверения подписи.

<sup>3</sup> Обязателен, из числа ППС по решению руководителя ОП или подразделения. Должность и степень не указываются. Сведения помещаются в последнюю строчку по порядку. Рецензенты не указываются.

## СОДЕРЖАНИЕ

Введение .....	3
Список использованных источников.....	5

## ВВЕДЕНИЕ

Современные программные системы всё чаще используют микросервисную архитектуру и облачную оркестрацию [6]. Это подход даёт преимущества в масштабируемости и независимом развитии компонентов, но одновременно увеличивает сложность управления безопасностью: дробление приложения на множество компонентов расширяет поверхность атаки и усложняет гарантирование корректной идентификации и разграничения прав как для пользователей, так и для самих сервисов [3; 4; 7]. В распределённых средах особенно актуальны вопросы надёжной пользовательской аутентификации и авторизации, безопасной межсервисной коммуникации и организации централизованного аудита и логирования для обнаружения инцидентов [2; 8]. Низкая степень унификации и ограниченная доступность готовых Open Source решений, полностью покрывающих требования по AAA (Authentication, Authorization, Accounting) создаёт потребность в исследованиях и разработке собственных решений, пригодных для промышленного использования [1; 5].

Предметом исследования данной работы является проектирование и реализация AAA подсистемы для распределённой микросервисной Continuous Delivery платформы с открытым исходным кодом, развёрнутой в Kubernetes. В рамках предметной области изучаются архитектурные подходы обеспечения доверенной межсервисной коммуникации, протоколы и механизмы пользовательской аутентификации и авторизации, архитектура и практики сбора, передачи и индексирования продуктовых логов и событий аудита. Особая практическая задача — обеспечить, чтобы разработанная AAA-подсистема была естественно интегрирована в архитектуру Continuous Delivery платформы, и обслуживала исключительно микросервисы и потоки данных внутри данной системы при сохранении возможности расширения в будущем.

Разработанный проект AAA представляет собой прикладную реализацию рекомендаций по безопасной межсервисной аутентификации и управлению доступом, предоставляя команде платформы готовый модуль для обеспечения доверенного взаимодействия её компонентов. Сформулированные архитектурные решения и практические рекомендации могут служить основой для дальнейших исследований и эволюции системы, в том числе для расширения поддержки внешних провайдеров аутентификации, уточнения политик доступа и интеграции с системами аналитики и безопасности. Наконец, разработанная подсистема обеспечит решение

практических задач безопасности и аудита в пределах микросервисной экосистемы разрабатываемой open-source платформы непрерывной доставки, будучи ориентированной на внутренние процессы проекта и его инфраструктуру.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Almeida M. G. de, Canedo E. D.* Authentication and Authorization in Microservices Architecture: A Systematic Literature Review // *Applied Sciences*. — 2022. — Т. 12, № 6. — С. 3023. — DOI 10.3390/app12063023.
2. *Barabanov A. I., Makrushin D.* Security Audit Logging in Microservice-Based Systems: Survey of Architecture Patterns // *Вопросы кибербезопасности*. — 2021. — № 2. — С. 71—80. — DOI 10.21681/2311-3456-2021-2-71-80.
3. *Blog P. S.* Как мы строили безопасную микросервисную архитектуру с Service Mesh: взгляд изнутри. — URL: <https://platformv.sbertech.ru/blog/kak-my-stroili-bezopasnuyu-mikroservisnuyu-arhitekturu-s-service-mesh-vzglyad-iznutri> (дата обращения: 25.10.2025).
4. *Glumov K. S.* Безопасность микросервисов: управление секретами и безопасная аутентификация // *Актуальные исследования*. — 2024. — 45 (227). — С. 23—29. — DOI 10.5281/zenodo.14029864.
5. Listening to what the system tells us: Innovative auditing for distributed systems / P. Di Pilla [и др.] // *Frontiers in Computer Science*. — 2023. — Т. 4. — С. 1020946. — DOI 10.3389/fcomp.2022.1020946.
6. Research Trends and Recommendations for Future Microservices Research / Z. Stojanov [и др.] // *Trudy ISP RAN/Proc. ISP RAS*. — 2024. — Т. 36, № 1. — С. 105—130. — DOI 10.15514/ISPRAS-2024-36(1)-7.
7. *Sikha G., Dorai V.* End-to-End Security and Operations for Kubernetes-Based Microservices // *International Research Journal of Modernization in Engineering Technology and Science*. — 2025. — Т. 7, № 8. — С. 2582—5208. — DOI 10.56726/IRJMETS82304.
8. *Zimina K. I., Laponina O. R.* Механизмы межсервисной аутентификации в приложениях с микросервисной архитектурой // *International Journal of Open Information Technologies*. — 2023. — Т. 11, № 5. — С. 146—154. — URL: <https://cyberleninka.ru/article/n/mehanizmy-mezhservisnoy-autentifikatsii-v-prilozheniyah-s-mikroservisnoy-arhitekturoy> (дата обращения: 25.10.2025).