МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**
Кафедра информатики и программирования

# ИНТЕГРАЦИЯ СЕРВИСА ЕДИНОЙ АВТОРИЗАЦИИ KEYCLOAK В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ФАКТОРИНГ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 441 группы
направления 02.03.03 — Математическое обеспечение и
администрирование информационных систем
факультета КНиИТ
Бурчуладзе Леван Александрович

Научный руководитель
к. ф.-м. н, доцент _____ М. В. Огнева
Заведующий кафедрой
к. ф.-м. н, доцент _____ М. В. Огнева

Саратов 2023

# ВВЕДЕНИЕ

**Актуальность темы.**

В настоящее время использование информационных технологий становится все более распространенным в различных сферах деятельности. Вместе с растущим рынком информационных технологий, растет и количество продуктов, в рамках которых используются аутентификация и авторизация пользователей в данные продукты. Вследствие чего пользователь должен запоминать или записывать логин и пароль, и, возможно, еще и секретный код, для каждого продукта. В следствие чего, многие компании, у которых есть несколько продуктов, начали использовать свои сервисы единой авторизации.

Сервис единой авторизации (Single Sign-On, SSO) позволяет пользователям использовать один и тот же логин и пароль для доступа к нескольким продуктам компании. При использовании SSO пользователь вводит свои учетные данные только один раз, после чего система авторизует его на всех связанных с аккаунтом сервисах. Это значительно упрощает процесс авторизации и облегчает работу пользователя. [1]

Для компаний SSO также представляет множество преимуществ. Во-первых, это позволяет существенно сократить затраты на разработку и поддержку системы авторизации для каждого продукта. Вместо того, чтобы создавать и поддерживать отдельные системы авторизации для каждого приложения, компания может использовать единую систему SSO, что упрощает процесс управления пользователями и повышает безопасность.

Во-вторых, использование единой системы авторизации позволяет компании повысить уровень безопасности своих продуктов и сервисов. Это происходит благодаря тому, что SSO позволяет управлять политиками безопасности и авторизации в централизованном режиме, что уменьшает вероятность возникновения ошибок.

Кроме того, использование единой системы авторизации может улучшить производительность и эффективность работы сотрудников, так как они не будут тратить время на повторный ввод учетных данных при переключении между приложениями. Это особенно важно для компаний, которые используют множество внутренних приложений и систем.

Наконец, использование SSO может помочь компаниям повысить лояльность и удовлетворенность пользователей. Пользователи ценят удобство и простоту. SSO позволяет им не запоминать множество логинов и паролей для доступа к различным сервисам, что делает процесс авторизации более привлекательным. Кроме того, SSO может ускоряет работу пользователя, так как пользователи могут более быстро и удобно переключаться между различными приложениями и сервисами компании.

В целом, использование единой системы авторизации является актуальным и ценным решением для компаний, которые разрабатывают и поддерживают множество приложений и сервисов. Это позволяет сократить затраты на разработку и поддержку, улучшить безопасность и производительность, а также дает удовлетворенность и простоту использования продуктов с единой системой авторизации пользователю.

**Цель бакалаврской работы** — интегрировать единую систему авторизации и аутентификации платформы Keycloak для автоматизированной системы факторинга «Факторинг Плюс».

**Задачи:**

- Рассмотреть основные понятия и определения
- Дать определение сервису единой авторизации и проанализировать готовые решения.
- Рассказать про автоматизированную систему факторинга.
- Интегрировать систему единой авторизации в “Факторинг Плюс”.

- Провести тестирование и оценить эффективность использования разработанной системы.

**Методологические основы.**

Аутентификация, авторизация и сервисы единой авторизаций, и сам факторинг представлены в работах: Барабанов А., Белова Е.П., Леднев М.В., Charles Bihis,

**Практическая значимость бакалаврской работы.**

Практическая значимость бакалаврской работы заключается в интеграции системы единой авторизации Keycloak в различные продукты компании для сокращения затрат на разработку и поддержку, улучшить безопасность и производительность, а также дает удовлетворенность и простоту использования продуктов пользователю.

**Структура и объём работы.**

Бакалаврская работа состоит из введения, 4 разделов, заключения, списка источников и 20 приложений. Общий объём работы — 86 страниц, из них 42 страницы — основное содержание, включая 9 рисунков, цифровой носитель в качестве приложения, список использованных источников информации — 23 наименований.

## КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

**Первый раздел «Теоретические основы авторизации и аутентификации»** посвящен концепции авторизации и аутентификации в контексте компьютерной безопасности. С развитием компьютерных технологий и распространением компьютерных сетей стало необходимо обеспечить защиту информации от несанкционированного доступа, перечислим основные термины.

Аутентификация — это процесс проверки подлинности пользователя, который позволяет убедиться в том, что пользователь является тем, за кого себя выдает. Для этого пользователь должен предоставить некоторые уникальные данные, такие как логин и пароль, отпечаток пальца или другие биометрические данные.

Существует несколько методов аутентификации: Парольная аутентификация, биометрическая аутентификация, аутентификация с помощью токена, аутентификация с помощью сертификатов - пользователь использует цифровой сертификат, который подтверждает его личность, аутентификация с помощью социальных сетей, аутентификация с помощью двухфакторной аутентификации.

Авторизация — это процесс проверки прав доступа пользователя к определенным ресурсам или функциям системы. После успешной аутентификации пользователь получает определенный уровень доступа, который определяется его ролями и правами.

Методы авторизации используются для проверки подлинности пользователя и предоставления ему доступа к защищенным ресурсам.

Некоторые из наиболее распространенных методов авторизации включают в себя: Логин и пароль, по смарт-карте, по SMS, по двухфакторной аутентификации.

Технология единого входа (Single Sign-On, SSO) — это метод авторизации, который позволяет пользователю получить доступ к нескольким приложениям и сервисам, используя только одно имя пользователя и пароль. Вместо того чтобы каждый раз вводить учетные данные при входе в различные приложения, пользователь вводит их только один раз, после чего система авторизует его на всех связанных с аккаунтом сервисах.

В настоящее время существует множество различных реализаций системы единого входа: IdentityServer, Auth0, Okta, Ping Identity, Keycloak.

При выборе из доступных сервисов единой авторизации, важными пунктами было: открытый исходный код, поддержка множества протоколов и стандартов, полностью бесплатный сервис, расширяемость с помощью плагинов и расширений, что дает возможность настроить сервис под свои конкретные потребности, наличие поддержки для Kubernetes, наличие поддержки для DevOps, предоставление инструментов для автоматизации настройки и развертывания, развитое русскоязычное и международное комьюнити, не сложный порог входа в данный сервис.

Исходя из вышенаписанных пунктов, больше всего подходит сервис единой авторизации – Keycloak, который представляет собой мощный и гибкий сервис единой авторизации, обладающий множеством преимуществ, включая открытый исходный код, гибкость, наличие бесплатной версии, расширяемость и совместимость с Java и Kubernetes и порог входа довольно легкий, его можно запустить сразу из коробки.

**Второй раздел «Теоретические основы системы факторинг»** включает в себя обзор факторинга и самого продукта «Факторинг Плюс», а именно, что факторинг — это финансовый инструмент, который позволяет компаниям получать финансирование путем продажи своих дебиторских задолженностей (т.е. неоплаченных счетов) третьей стороне -

факторинговой компании. Факторинговая компания предоставляет компании деньги в обмен на право получения денег от ее дебиторов.

А также о самой архитектуре проекта “Факторинг Плюс”, который является уже долгоживущим проектом, который постоянно меняется, развивается и переделывается, в настоящий момент проект разбит на две составляющие: Back-End часть и Front-End часть.

Back-End написан на языке программирования C# на платформе ASP.NET с интерфейсом программирования Web API, которое облегчают разработку и управление приложением.

Front-End — это часть веб-приложения, которая отвечает за отображение данных пользователю и взаимодействие с ним. Front-End выполняется в браузере пользователя и написан с помощью фреймворка VUE 3, где используется HTML, CSS и JavaScript.

**Третий раздел «Практическая часть»** посвящен интеграции нового сервиса единой авторизации в проект «Факторинг Плюс». Она должна была проводиться поэтапно, с одновременной работой старого сервиса единой авторизации по причине того, что проект в данное время уже работает с клиентами и прекращение работы автоматически означало потерю клиентов.

Посредством этого был выстроен такой план:

- Создать модуль с новым сервисом единой авторизации (Keycloak) с теми же интерфейсами и моделями, которые есть у старого SSO (identity server).
- Реализовать данные интерфейсы и модели с подключением к Keycloak, а также сделать переключение между сервисами единой авторизации.
- После интеграционного тестирования, которое подтвердит полноценную работу на новом сервисе – удалить реализацию с identity Server.

После полной интеграции сервиса единой авторизации Keycloak, нужно было удалить старый сервис Identity Server, обновить имена файлов с модулем Keycloak, и удалить переключатель.

**Четвертый раздел «Тестирование интеграции Keycloak»** посвящен тестирование нового сервиса единой авторизации. Тестирование проводилось регрессионного и интеграционного тестирования.

Регрессионное тестирование — это процесс тестирования программного обеспечения, который выполняется чтобы обеспечить стабильность работы программного обеспечения после внесения изменений. При этом проверяются функциональность и надежность системы, а также ее соответствие требованиям. Проводится путем запуска тестов, которые были выполнены ранее, для проверки, что они продолжают работать корректно после внесения изменений. Если тесты не проходят или происходят ошибки, то это указывает на то, что внесенные изменения повлияли на работу системы.

Интеграционное тестирование (Integration Testing) – это процесс проверки взаимодействия различных компонентов или модулей системы в единой интегрированной среде. Основная цель интеграционного тестирования – обнаружение ошибок взаимодействия между компонентами системы и проверка их работоспособности в целом.

При переходе с IdentityServer на Keycloak во всем проекте в ходе тестирования было обнаружено порядка 60 новых багов, с разными приоритетами и серьезностью. Основная масса багов была связана с сетевыми ошибками, другая часть багов была связана с Front-end частью проекта. Сложность в тестировании вышеуказанного перехода заключалась в том, что в ходе исправления одной части багов, возникали ошибки в другой части проекта, соответственно, постоянно проводилось регрессионное и интеграционное тестирование.

## ЗАКЛЮЧЕНИЕ

В ходе данной работы была рассмотрена тема интеграции системы единой авторизации в автоматизированную систему факторинга с использованием технологии Keycloak.

В итоге интеграция системы единой авторизации Keycloak в «Факторинг Плюс» позволила упростить процесс авторизации для пользователей и повысить безопасность системы. Разработанная система показала хорошие результаты в ускорении процесса авторизации и сокращении времени, затрачиваемого на управление учетными данными пользователей. Это является важным шагом в развитии и совершенствовании автоматизированной системы факторинга и может быть использовано в качестве примера для других компаний, которые также ищут решения для упрощения и улучшения процесса авторизации.

Данная работа может быть использована в качестве руководства по интеграции системы единой авторизации в другие продукты или системы, а также может быть полезна разработчикам, администраторам и архитекторам, которые работают с системами авторизации и аутентификации.

**Основные источники информации:**


1. Барабанов А. Authentication and authorization in microservice-based systems: survey of architecture patterns / А. Барабанов, Д. Макрушин // вопросы кибербезопасности. 2020. № 4(38). с. 32-43
2. Белова Е.П. Классификация методов аутентификации пользователей в автоматизированных системах // материалы МСНК "Студенческий научный форум 2023". – 2020. – № 4. – с. 85-87
3. Charles Bihis Mastering OAuth 2.0 / Charles Bihis — PACKT Publishing, 2015 — 238 с.

4. Рихтер Дж. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C# / Дж. Рихтер; 4-е изд. — СПб.: Питер, 2013. — 896 с.
5. ASP.NET Core Identity [Электронный ресурс] URL: learn.microsoft.com/ru-ru/dotnet/architecture/microservices/secure-net-microservices-web-applications (Дата обращения 22.01.2023)
6. Aauth0 docs [Электронный ресурс] URL: auth0.com/docs (Дата обращения 24.01.2023)
7. Okta Docs [Электронный ресурс] URL: developer.okta.com (Дата обращения 24.01.2023)
8. Ping identity Docs [Электронный ресурс] URL: docs.pingidentity.com/ (Дата обращения 24.01.2023)
9. Keycloak Admin REST API [Электронный ресурс] URL: keycloak.org/docs-api/18.0/rest-api/index.html (Дата обращения 15.01.2023)
10. Леднев М.В. Факторинг / М.В. Леднев, И.Е. Покаместов – СПБ: БХВ, 2021. – 272 с.