

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра телекоммуникаций и информационных технологий

МАРКОВ

Никита Витальевич

**БЕЗОПАСНОСТЬ МИКРОСЕРВИСНОГО ПРИЛОЖЕНИЯ В СРЕДЕ
«ЦИФРОВОЙ ФАКУЛЬТЕТ»**

Дипломная работа

Научный руководитель:
кандидат физ.-мат. наук,
доцент Ю.И.

Воротницкий

Допущен к защите

«»2021 г.

Зав. кафедрой телекоммуникаций и информационных технологий

кандидат физ.-мат. наук, доцент Ю.И. Воротницкий

Минск, 2021

РЕФЕРАТ

Дипломная работа, 50 страниц, 17 рисунков, 1 таблица, 18 источников.

ВЕБ-ПРИЛОЖЕНИЕ, МИКРОСЕРВИСНАЯ АРХИТЕКТУРА, БЕЗОПАСНОСТЬ, АУТЕНТИФИКАЦИЯ, АВТОРИЗАЦИЯ, МОНИТОР БЕЗОПАСНОСТИ ОБРАЩЕНИЙ.

Объект исследования - информационная система «Цифровой факультет» и связь его микросервисов между собой.

Цель работы - изучение и тщательный анализ существующих проблем в архитектуре приложения «Цифровой факультет», а также реализация варианта защиты веб-приложения, которая позволила бы реализовать базовую защиту от части атак и вытекающих из них последствий, тем самым обеспечить более эффективное и качественное функционирование данного приложения.

В ходе дипломной работы были проанализированы особенности различных архитектур построения веб-приложений, обоснован выбор микросервисной, указаны плюсы и минусы каждой.

Также были обозначены основные требования к защите веб-приложений, и в частности, построенных на микросервисной архитектуре. Были проанализированы и предложены различные варианты защиты такой архитектуры.

Основой безопасности любого веб-приложения смело можно называть монитор безопасности обращений - это некий фильтр, который либо разрешает, либо запрещает доступ к защищенному ресурсу на основе установленных в системе правил разграничения доступа. В дипломной работе были описаны основные требования, которым должен соответствовать монитор безопасности обращений, а также были представлены различные варианты реализации правил разграничения доступа.

Также была разработана система, которая обеспечивает безопасный доступ к защищенным ресурсам. Данная система включает в себя несколько микросервисов, таких как публичный шлюз, сервер регистрации микросервисов, а также сервер авторизации.

РЭФЕРАТ

Дыпломная работа, 50 старонак, 17 малюнкау, 1 таблица, 18 крынц.

ВЭБ-ДАДАТАК, МІКРАСЭРВІСНАЯ АРХІТЭКТУРА, БЯСПЕКА, АУТЭНТЫФІКАЦЫЯ, АУТАРЫЗАЦЫЯ, МАНІТОР БЯСПЕКІ ЗВАРОТАУ.

Аб'ект даследавання - шфармацыйная схэма "лхчбавы факультэт" і сувязь яго мжрасэрв^ау паміж сабой.

Мэта работы - вывучэнне і тльны анатаз існуючы\ праблем у архггэктурцы прыкладання Апчбавы факультэт", а таксама рэатазацыя варыянту абароны вэб-прыкладанш, якая дазволша б рэатазаваць базавую абарону ад часті нападау і вышкаюць з ЦІ\ наступствау, тым самым забяспечыць больш эфектыунае і якаснае функцыянаванне дадзенага прыкладання.

У ходзе дыпломнай працы былі праанатазаваны асаблівасці розных архггэктур пабудовы вэб-прыкладанняу, абгрунтаваны выбар мшрасэрвшнай, пазначаны плюсы і мшусы кожнай.

Таксама былі пазначаны асноуныя патрабаванш да абароны вэб-прыкладанняу, і у прыватнасц, пабудаваных на мжрасэрв^най архыэктурцы. Быта праанатазаваны і прапанаваны розныя варыянты абароны такой архггэктурцы.

Асновай бяспекч любога вэб-прыкладанш смела можна называць Маштор бяспекч зваротау-гэта нейкз фшьтр, якч альбо дазваляе, альбо забараняе доступ да абароненаму рэсурсу на аснове устаноуленых у истэме правшау размежавання доступу. У дыпломнай працы быта ашсаны асноуныя патрабаванш, якГМ павшен адпавядаць Маштор бяспекз зваротау, а таксама быт прадстаулены розныя варыянты рэашзацьп правшау размежавання доступу.

Таксама была распрацавана истэма, якая забяспечвае бяспечны доступ да абароненым рэсурсау. Дадзеная сштэма уключае у сябе некальи мкрасэрв^ау, таих як пуб.тчны шлюз, сервер рэпстрацып мкрасэрв^ау, а таксама сервер аутарызацыг

ABSCTACT

Thesis, 50 pages, 17 images, 1 table, 18 sources.

WEB-APPLICATION, MICROSERVICES ARCHITECTURE,
SECURITY, AUTHENTICATION, AUTHORIZATION, SECURITY
REFERENCE MONITOR.

The *object of the work* is an information system «Цифровой факультет» and it's microservices relationships.

The *purpose of the work* is to study and thoroughly analyze existing problems in the architecture of the "Digital Faculty" application, as well as to implement a web application protection option, which would allow implementing basic protection against some attacks and the resulting consequences, thereby ensuring more efficient and high-quality functioning of this applications.

In the course of the thesis, the features of various architectures for building web applications were analyzed, the choice of microservice was justified, the pros and cons of each were indicated.

The basic requirements for the protection of web applications, and in particular those built on a microservice architecture, were also identified. Various options for protecting such an architecture have been analyzed and proposed.

The security monitor of any web application can be safely called the access security monitor - it is a kind of filter that either allows or denies access to a protected resource based on the access control rules set in the system. In the thesis, the main requirements were described that the access security monitor must meet, and various options for the implementation of access control rules were presented.

A system has also been developed that provides secure access to protected resources. This system includes several microservices, such as a public gateway, a microservices registration server, and an authorization server.