МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра высшей алгебры и защиты информации

Сидорович Дмитрий Андреевич

Аннотация к дипломной работе:

**РАЗРАБОТКА БЕЗОПАСНОЙ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ В ВЕБ-ПРИЛОЖЕНИЯХ С ИСПОЛЬЗОВАНИЕМ КРИПТОГРАФИИ**

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

Минск, 2024

# АННОТАЦИЯ

Дипломная работа состоит из 56 страниц, 18 рисунков, 2 приложения, список цитируемых литературных источников в количестве 13 наименований.

Ключевые слова: БЕЗОПАСНАЯ АУТЕНТИФИКАЦИЯ, ВЕБ-ПРИЛОЖЕНИЯ, КРИПТОГРАФИЯ, JWT, OAuth, ZKP, Node.js, Angular, TypeScript.

*Объектами исследования* являются методы аутентификации и авторизации в веб-приложениях с использованием криптографических методов.

*Предмет исследования* – разработка и внедрение системы безопасной аутентификации и авторизации на базе современных криптографических алгоритмов и протоколов.

*Целью* дипломной работы является создание системы безопасной аутентификации и авторизации для веб-приложений с использованием криптографических методов.

В результате работы была разработана система безопасной аутентификации и авторизации для веб-приложений с использованием современных криптографических методов. Проведено исследование и внедрение методов аутентификации JWT, OAuth и ZKP, а также методов авторизации RBAC и ABAC. Использование криптографических алгоритмов HMAC и RSA обеспечило высокий уровень защиты данных. Разработанная система обеспечивает гибкую настройку доступа к ресурсам, что делает ее безопасной и удобной для пользователей.

*Практическая ценность* этой работы в том, что её можно использовать для создания защищенных веб-приложений. Это особенно важно для таких областей, как образование, здравоохранение и финансы.

*Обоснованность и достоверность* полученных результатов подтверждаются использованием проверенных криптографических методов и стандартов, а также проведением тестирования и анализа безопасности системы.

Дипломная работа выполнена автором *самостоятельно*.

# АНАТАЦЫЯ

Дыпломная праца складаецца з 56 старонак, 18 малюнкаў, 2 дадаткі, спіс цытуемых літаратурных крыніц у колькасці 13 найменняў.

Ключавыя словы: БЯСПЕЧНАЯ АЎТЭНТЫФІКАЦЫЯ, ВЭБ-ДАДАТКІ, КРЫПТАГРАФІЯ, JWT, OAuth, ZKP, Node.js, Angular, TypeScript.

Аб'ектамі даследавання з'яўляюцца метады аўтэнтыфікацыі і аўтарызацыі ў вэб-прыкладаннях з выкарыстаннем крыптаграфічных метадаў.

Прадмет даследавання - распрацоўка і ўкараненне сістэмы бяспечнай аўтэнтыфікацыі і аўтарызацыі на базе сучасных крыптаграфічных алгарытмаў і пратаколаў.

Мэтай дыпломнай працы з'яўляецца стварэнне сістэмы бяспечнай аўтэнтыфікацыі і аўтарызацыі для вэб-прыкладанняў з выкарыстаннем крыптаграфічных метадаў.

У выніку працы была распрацавана сістэма бяспечнай аўтэнтыфікацыі і аўтарызацыі для вэб-прыкладанняў з выкарыстаннем сучасных крыптаграфічных метадаў. Праведзена даследаванне і ўкараненне метадаў аўтэнтыфікацыі JWT, OAuth і ZKP, а таксама метадаў аўтарызацыі RBAC і ABAC. Выкарыстанне крыптаграфічных алгарытмаў HMAC і RSA забяспечыла высокі ўзровень абароны дадзеных. Распрацаваная сістэма дазваляе гнутка наладжваць доступ да рэсурсаў, забяспечваючы высокі ўзровень бяспекі і зручнасці для карыстальнікаў.

Практычная значнасць дадзенай працы заключаецца ў магчымасці выкарыстання распрацаванай сістэмы для стварэння бяспечных вэб-прыкладанняў, што актуальна для розных сфер дзейнасці, уключаючы адукацыю, ахову здароўя і фінансы.

Абгрунтаванасць і дакладнасць атрыманых вынікаў пацвярджаюцца выкарыстаннем правераных крыптаграфічных метадаў і стандартаў, а таксама правядзеннем тэсціравання і аналізу бяспекі сістэмы.

Дыпломная праца выканана аўтарам самастойна.

# ANNOTATION

The thesis consists of 56 pages, 18 figures, 2 appendices, a list of cited literary sources of 13 titles.

Keywords: SAFE AUTHENTIFICATION, WEB APPLICATIONS, CRYPTOGRAPHY, JWT, OAuth, ZKP, Node.js, Angular, TypeScript.

The research focuses on methods of authentication and authorization in web applications using cryptographic techniques.

The subject of the study is the development and implementation of a secure authentication and authorization system based on modern cryptographic algorithms and protocols.

The purpose of the thesis is to create a system of secure authentication and authorization for web applications using cryptographic methods.

As a result of the work was developed a system of secure authentication and authorization for web applications using modern cryptographic methods. JWT, OAuth and ZKP authentication methods and RBAC and ABAC authorization methods have been investigated and implemented. The use of HMAC and RSA cryptographic algorithms provided a high level of data protection. The developed system allows flexible customization of access to resources, providing a high level of security and convenience for users.

The practical significance of this work lies in the possibility of using the developed system to create secure web applications, which is relevant for various spheres of activity, including education, health care and finance.

The validity and reliability of the obtained results are confirmed by the use of proven cryptographic methods and standards, as well as by testing and analyzing the security of the system.

The thesis is independently performed by the author.