

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІН-
ЖЕНЕРІЇ

АНДРІЙЧУК ЯРОСЛАВ ВАСИЛЬОВИЧ

УДК 004.415.5

**РЕАЛІЗАЦІЯ ПРОТОКОЛІВ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ВЕБ-ОРІ-
ЄНТОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ**

123 «Комп'ютерна інженерія»

Автореферат

дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2018

Роботу виконано на кафедрі комп'ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: доктор технічних наук, доцент кафедри електротехніки
Лупенко Анатолій Миколайович,
Тернопільський національний технічний університет
імені Івана Пулюя,

Рецензент: кандидат технічних наук, доцент кафедри інформатики і
математичного моделювання
Гашин Надія Богданівна,
Тернопільський національний технічний університет
імені Івана Пулюя,

Захист відбудеться 27 грудня 2018 р. о 9⁰⁰ годині на засіданні експертної комісії № 34 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 1-603

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. На даний момент існує безліч методів авторизації та аутентифікації користувача: від найпростіших - як введення логіна і пароля, до найскладніших, що включають в себе багатоетапну систему підтвердження аутентичності.

Всі вони розрізняються використовуваними протоколами передачі даних, складністю реалізації, вартістю підтримки працездатності системи і т.д. Також вибір методик залежить від ступеня важливості інформації, що зберігається, або ступеня шкоди, який може бути викликаний при несанкціонованому доступі.

Проаналізувавши останні публікації і дослідження, стає зрозуміло, що значну увагу проблемам аутентифікації користувачів веб-орієнтованих комп'ютерних систем та аналізу протоколів аутентифікації приділяли такі провідні вітчизняні та зарубіжні науковці, як Л. Адлеман, А.І. Березовський, Л.Ю. Боков, А.М. Боровиков, Л.А. Завадська, В.К. Задирака, Р.Є. Сміт, А.М. Фаль, Л.Б. Шевчук та інші. Проте, у працях цих дослідників недостатньо вичерпно висвітлені питання різноманітних підходів до протоколів аутентифікації. Мало уваги приділено вибору протоколу для конкретної інформаційної системи. Беручи до уваги вище зазначені проблеми, дослідження аналізів протоколів аутентифікації користувачів web-сервісів є актуальним науковим завданням.

Відомі методи аутентифікації особи характеризуються значними величинами похибок першого та другого родів, що ускладнює їх використання в інформаційних системах аутентифікації особи.

Метою є дослідження протоколів та реалізація протоколу аутентифікації користувачів для веб-орієнтованих комп'ютерних систем.

Задачі, які необхідно вирішити у магістерській роботі полягають у наступному:

- проаналізувати сучасні методи протоколів аутентифікації;
- проаналізувати технології аутентифікації у веб-орієнтованих комп'ютерних системах;
- розробити систему аутентифікації для веб-платформи.

Об'єктом досліджень є процес аутентифікації людини у веб-орієнтованих комп'ютерних системах.

Предметом досліджень є види протоколів аутентифікації, реалізація протоколу аутентифікації користувачів веб-орієнтованих комп'ютерних систем.

Наукова новизна отриманих результатів:

- уперше проведено аналіз протоколів призначених для аутентифікації особи у web-сервісах;
- запропоновано протоколи та стандарти які дозволяють покращити захищеність та зручність web-сервісів
- показано доцільність використання методів та моделей біометричної аутентифікації.

Практичне значення отриманих результатів. Спроектowana система аутентифікації особи веб-орієнтованих комп'ютерних систем дає змогу підвищити конфіденційність особистої інформації.

Апробація результатів дипломної роботи. Результати роботи апробовано на VI Міжнародної науково-технічної конференції молодих учених та студентів «Інформаційні моделі, системи та технології» м. Тернопіль 12-13 грудня 2018 року

Публікації. Лупенко С.А., Андрійчук Я.В Реалізація протоколів аутентифікації користувачів веб-орієнтованих комп'ютерних систем. VI науково-технічній конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології». 12-13 грудня 2018 р.: тези доп. – Тернопіль, 2018. – С. 57.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 6 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 115 арк. формату А4, графічна частина – 8 аркушів формату А1

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність дослідження, мету роботи, задачі, об'єкт, предмет, наукова новизна, практичне значення, апробація та публікації дипломних досліджень.

У першому розділі роботи «Дослідження предметної області протоколів аутентифікації» проаналізовано основні рівні загроз, і розглянуто рівні аутентифікації до сервісу. Досліджено сучасні методи аутентифікації та виокремлено актуальні методи аутентифікації користувачів веб-орієнтованих комп'ютерних систем.

У другому розділі «Аналіз протоколів аутентифікації користувачів веб-орієнтованих комп'ютерних систем» розглянуто декілька протоколів в цілому та наведені їхні недоліки. Зроблено огляд протоколів аутентифікації особи та обґрунтовано вибрано найактуальніший. Розглянуто інтеграцію протоколу аутентифікації OpenID Connect у веб-орієнтованих комп'ютерних системах та наведено приклади.

У третьому розділі «Проектування веб-додадку на основі протоколу OpenIDConnect та фреймворку Laravel» представлено проектування системи онлайн-чату та аутентифікації особи. Спроектowano програмний код програми та проведено повне тестування системи на перевірку коректної та стабільної роботи. Розроблена система дозволяє забезпечити цілісність та конфіденційність даних та унеможливило попаданню особистих даних в руки злоумисників.

У четвертому розділі «Обґрунтування економічної ефективності» зроблено обчислення показників економічної ефективності від застосування методу вибору оптимального рішення при реалізації програмних проектів, що дало можливість зробити висновок про доцільність проведення НДР.

П'ятий розділ роботи «Охорона праці та безпека в надзвичайних ситуаціях» проведено аналіз вимог з охорони праці і техніки безпеки при використанні комп'ютерної техніки, зокрема при дослідженні та експлуатації методів та засобів

розпізнавання зображень, також проаналізовано електробезпеку користувачів персональних комп'ютерів.

Шостий розділ роботи «Екологія» містить дослідження питання становлення екологічних знань у різних суспільних галузях та розглянуто зведення та первинне опрацювання статистичних даних екологічної інформації.

ВИСНОВКИ

В результаті виконання дипломної роботи було виконано наступні кроки для вирішення поставлених задач:

- проаналізовано сучасні методи і засоби аутентифікації;
- досліджено технології аутентифікації користувачів веб-орієнтованих комп'ютерних систем;
- розроблено систему аутентифікації онлайн-чату для користувачів веб-орієнтованих комп'ютерних систем.

Спроектвана система є досить гнучкою і легко піддається модернізації. Проаналізувавши сучасні методи та засоби аутентифікації можна зробити висновок, що розробка даної системи є актуальною, оскільки кожного дня стає все більше і більше різноманітних додатків в яких користувачі зберігатимуть свою особисту інформацію та матимуть бажання з мінімальними витратами часу реєструватися чи створювати вхід у веб-сервіс. Це призводить до задачі їх захисту та забезпечення конфіденційності, а розроблена система вирішує поставлену задачу. Також розглянуто і протестовано систему аутентифікації користувачів веб-орієнтованих комп'ютерних систем.

Здійснено економічні розрахунки, спрямовані на визначення економічної ефективності та вартості системи біометричної аутентифікації для мобільних пристроїв.

Розглянуто та описано вимоги з охорони праці та техніки безпеки відповідно до нормативних документів щодо: організації робочого місця, електробезпеки, шуму та вібрації, освітленості, мікроклімату та пожежної безпеки.

Ознайомлено з поставленими питаннями екології які стосуються дипломної роботи.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Андрійчук Я. Реалізація протоколів аутентифікації користувачів веб-орієнтованих комп'ютерних систем. [Електронний ресурс] / Ярослав Андрійчук // VI Науково-технічній конференції «Інформаційні моделі, системи та технології». – 2018. – Режим доступу до ресурсу: http://elartu.tntu.edu.ua/bitstream/lib/23329/2/ZBIRNYK_MAT_1-1.pdf.
2. Андрійчук Я. Проектування веб-додатку на основі фреймворку Laravel. [Електронний ресурс] / Ярослав Андрійчук // Міжнародній науково-практичній конференції «Актуальні питання в контексті розвитку сучасних наук». – Режим доступу до ресурсу: https://ukrlogos.in.ua/scientific_journal_ua.php

АНОТАЦІЯ

Андрійчук Я.В. Реалізація протоколів аутентифікації користувачів веб-орієнтованих комп'ютерних систем.

Дипломна робота на здобуття освітнього ступеня магістра 123 – Комп'ютерні системи та мережі. – Тернопільський національний технічний університет імені Івана Пулюя 2018.

У дипломній роботі проведено комплексне дослідження методів та засобів аутентифікації особи та наведено сфери їх застосування.

На основі проведених досліджень було проаналізовано сучасні методи аутентифікації користувачів веб-орієнтованих комп'ютерних систем. Досліджено технології аутентифікації користувачів веб-орієнтованих комп'ютерних систем. Було обрано та розглянуто середовище проектування системи.

На основі обраної моделі протоколу аутентифікації розроблено алгоритми роботи та спроектовано систему аутентифікації користувачів веб-орієнтованих комп'ютерних систем. На базі програмної реалізації проведено тестування та дослідження ефективності та стабільності роботи.

Ключові слова: аутентифікація, протокол, веб-сервіси, OpenID Connect, OAuth, стандартизація, Laravel.

ANNOTATION

Andriichuk Y.V. Implementation of authentication protocols of web-oriented computer systems users.

The diploma paper for obtaining the Master's degree 123 – Computer systems and network – Ternopil Ivan Puluj National Technical University 2018.

In the thesis the complex research of methods and means of authentication of the person is carried out and the areas of their application are given.

On the basis of the conducted researches, modern methods of authentication of users of web-oriented computer systems were analyzed. The technologies of authentication of users of web-oriented computer systems are investigated. The system design environment was selected and considered.

Based on the selected authentication protocol model, algorithms were developed and a user authentication system for user-oriented web-based computer systems was designed. On the basis of the program implementation, the testing and research of efficiency and stability of work has been conducted.

Keywords: authentication, protocol, web-services, OpenID Connect, OAuth, standardization, Laravel.