ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

(повне найменування вищого навчального закладу)

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

(повне найменування інституту, назва факультету (відділення))

КАФЕДРА ПРОГРАМНИХ ЗАСОБІВ І ТЕХНОЛОГІЙ

(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістра

(освітній рівень)

на тему: «Дослідження та розробка архітектури захищеного клієнт-серверного застосунку реального часу на основі транспортних протоколів»

Виконав: студент 6 курсу, групи 6ПР2

спеціальності

121 - «Інженерія програмного забезпечення» (шифр і назва спеціальності)

Юдін Дмитро Федорович

(прізвище та ініціали)

Керівник к.т.н., доцент Вишемирська С.В.

(прізвище та ініціали)

Рецензент _____

(прізвище та ініціали)

Хмельницький - 2025

Херсонський національний технічний університет

(повне найменування вищого навчального закладу)

Факультет, відділення Інформаційних технологій та дизайну

Кафедра Програмних засобів і технологій

Освітній рівень магістр

Спеціальність 121 – Інженерія програмного забезпечення

(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Програмних засобів і технологій

к.т.н. доцент О.Є. Огнєва

“___” _____ 2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Юдін Дмитро Федорович

(прізвище, ім’я, по батькові)

Тема роботи «Дослідження та розробка архітектури захищеного клієнт-серверного застосунку реального часу на основі транспортних протоколів»

керівник роботи к.т.н., доцент Вишемирська С.В.

(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджена наказом вищого навчального закладу від 15 . 09 .2025 р. № 417 -с

2. Строк подання студентом роботи

3. Вихідні дані до роботи літературні та періодичні джерела, матеріали переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1. Аналіз сучасних систем миттєвого обміну повідомленнями

2. Визначення вимог до системи

3. Вибір технологій та інструментів .

4. Проєктування архітектури та криптографічного протоколу

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 12.10.2025

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів виконання роботи	Термін виконання етапів роботи	Примітки
1	Отримання завдання	12.10.2025	Виконано
2	Підбір літератури, аналіз сучасних систем	13.10.2025-20.10.2025	Виконано
3	Аналіз предметної області та протоколів	21.10.2025-28.10.2025	Виконано
4	Розробка та обґрунтування завдання	29.10.2025-07.11.2025	Виконано
5	Розробка концептуальної моделі та криптопротоколу	08.11.2025-17.11.2025	Виконано
6	Моделювання та проєктування системи (архітектура, транспортні протоколи)	18.11.2025-30.11.2025	Виконано
7	Моделювання та проєктування бази даних	01.12.2025-05.12.2025	Виконано
8	Розробка інтерфейсу клієнтської частини	06.12.2025-12.12.2025	Виконано

9	Реалізація серверної частини та криптографічного протоколу	13.12.2025-18.12.2025	Виконано
10	Тестування системи та аналіз ефективності WebSocket/WebRTC	19.12.2025-22.12.2025	Виконано
11	Оформлення пояснювальної записки	23.12.2025-25.12.2025	Виконано
12	Захист кваліфікаційної роботи		Виконано

Студент _____ Д.Ф. Юдін .

(підпис) (прізвище та ініціали)

Керівник роботи _____ С.В. Вишемирська

(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка до комплексної курсової роботи: 94 с., 40 рис., 2 додатки, 15 джерел.

Об’єкт дослідження – клієнт-серверна система миттєвого обміну повідомленнями.

Предмет дослідження – методи та алгоритми забезпечення безпеки обміну повідомленнями та ефективності роботи транспортних протоколів WebSocket і WebRTC у реальних мережевих умовах.

Мета роботи – розробка захищеного клієнт-серверного месенджера із власним криптографічним протоколом та проведення аналізу ефективності сучасних транспортних протоколів реального часу.

Методи розробки – стек технологій React, NestJS, PostgreSQL, WebSocket, WebRTC; власний криптографічний протокол на основі X3DH і Double Ratchet з використанням AES-256-GCM, Curve25519, SHA-512.

У процесі виконання роботи проведено аналіз сучасних систем обміну повідомленнями, огляд криптографічних і транспортних протоколів, спроєктовано архітектуру системи, реалізовано прототип клієнтської та серверної частини месенджера, а також виконано тестування ефективності передачі даних і стійкості протоколу до атак.

Отримані результати підтвердили, що розроблений месенджер забезпечує високий рівень конфіденційності, цілісності та автентичності переданих даних, стабільну роботу в умовах різної якості з’єднання, а також мінімальні затримки при передачі повідомлень і мультимедіа.

Ключові слова: МЕСЕНДЖЕР, КЛІЄНТ-СЕРВЕРНА СИСТЕМА, КРИПТОГРАФІЧНИЙ ПРОТОКОЛ, WEBSOCKET, WEBRTC, X3DH, DOUBLE RATCHET, БЕЗПЕКА, ШИФРУВАННЯ, МИТТЄВИЙ ОБМІН ПОВІДОМЛЕННЯМИ.

АНОТАЦІЯ

У магістерській роботі досліджено підходи до проєктування та реалізації захищених клієнт-серверних застосунків реального часу на прикладі системи миттєвого обміну повідомленнями. Проаналізовано сучасні месенджери, їх архітектурні рішення, криптографічні механізми та транспортні протоколи передавання даних. Особливу увагу приділено питанням забезпечення конфіденційності, цілісності та автентичності інформації в умовах зростання кіберзагроз.

У роботі сформульовано вимоги до захищеного месенджера, обґрунтовано вибір стеку технологій та спроєктовано архітектуру клієнт-серверної системи. Розроблено власний криптографічний протокол на основі сучасних алгоритмів і принципів наскрізного шифрування, що забезпечує стійкість до поширених атак, зокрема MITM та повторного відтворення повідомлень. Реалізовано прототип клієнтської та серверної частин застосунку з підтримкою текстового і мультимедійного обміну.

Проведено експериментальне порівняння транспортних протоколів WebSocket і WebRTC за критеріями затримки, стабільності та ефективності передачі даних у реальному часі. Отримані результати підтверджують доцільність використання комбінованого підходу до організації транспортного рівня залежно від типу передаваних даних.

Практичне значення роботи полягає у можливості використання розроблених архітектурних і криптографічних рішень під час створення захищених вебзастосунків реального часу.

Ключові слова: клієнт-серверна система, месенджер, захист інформації, криптографічний протокол, WebSocket, WebRTC, шифрування, реальний час.

ABSTRACT

This master’s thesis focuses on the research and development of a secure client-server real-time application architecture, using an instant messaging system as a case study. Modern messaging platforms, their architectural approaches, cryptographic mechanisms, and data transport protocols are analyzed. Special attention is given to ensuring confidentiality, integrity, and authenticity of information in the context of increasing cybersecurity threats.

The system requirements for a secure messenger are defined, the technology stack is justified, and a client-server architecture is designed. A custom cryptographic protocol based on modern algorithms and end-to-end encryption principles is developed, providing resistance to common attacks such as man-in-the-middle and replay attacks. A functional prototype of the client and server components supporting text and multimedia communication is implemented.

An experimental comparison of WebSocket and WebRTC transport protocols is conducted, focusing on latency, stability, and data transmission efficiency in real-time environments. The results demonstrate the effectiveness of a hybrid transport approach depending on the type of transmitted data.

The practical value of the research lies in the applicability of the proposed architectural and cryptographic solutions for developing secure real-time web applications.

Keywords: client-server system, messenger, information security, cryptographic protocol, WebSocket, WebRTC, encryption, real-time communication.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

API – програмний інтерфейс прикладного програмування

AES – стандарт симетричного блочного шифру

E2EE – наскрізне шифрування

MITM – атака «людина посередині»

PFS – принцип проспективної секретності

SHA – алгоритм криптографічного хешування

UI – користувацький інтерфейс

WebRTC – вебтехнологія реального часу

WebSocket – мережевий протокол двонапрямленого обміну даними в реальному часі

X3DH – розширений протокол обміну ключами

СУБД – система управління базами даних

ID – ідентифікатор користувача або об’єкта

MSG – повідомлення

PK – публічний ключ

SK – секретний (приватний) ключ

ВСТУП

Миттєвий обмін повідомленнями є невід’ємною складовою сучасної цифрової комунікації. Зростання обсягів переданих даних, необхідність підтримки високої швидкості та захисту інформації обумовлюють потребу у створенні нових рішень, здатних забезпечити надійність і конфіденційність передавання. Зважаючи на зростаючу кількість кіберзагроз, ключовим завданням стає впровадження сучасних криптографічних методів та оптимізація транспортних протоколів для роботи в реальному часі.

Більшість наявних месенджерів використовують стандартні протоколи та архітектурні підходи, які не завжди дозволяють адаптувати систему під специфічні вимоги. Це зумовлює актуальність розробки індивідуальних рішень, що поєднують високий рівень безпеки, продуктивність і масштабованість.

Мета роботи – створення захищеного клієнт-серверного месенджера з власним криптографічним протоколом і проведення аналізу ефективності сучасних транспортних протоколів реального часу.

Об’єкт дослідження – клієнт-серверні системи миттєвого обміну повідомленнями.

Предмет дослідження – методи та алгоритми захисту комунікацій і підвищення ефективності транспортних протоколів WebSocket та WebRTC.

Для досягнення мети передбачено:

- проаналізувати сучасні рішення у сфері захищеного обміну повідомленнями;
- обґрунтувати вибір технологій для клієнтської та серверної частин;
- розробити власний криптографічний протокол;
- реалізувати прототип месенджера з підтримкою текстового та мультимедійного обміну;
- протестувати та порівняти роботу WebSocket і WebRTC.

Розроблена система має забезпечити конфіденційність, цілісність і автентичність переданих даних, стабільну роботу за різних мережевих умов і низькі затримки при передачі повідомлень та мультимедіа.