

Date: 3rd December-2025

МЕТОД ПОСТРОЕНИЯ ЗАЩИЩЁННОГО СЕРВЕРНОГО МЕССЕНДЖЕРА НА BOOST.ASIO

Каримов М.М., Гуломов Ш.Р., Юлдашев Ж.Б.

Ташкентский университет информационных технологий имени Мухаммада
Ал-Хоразмий

Метод основывается на применении библиотеки **Boost.Asio**, которая используется для организации асинхронного обмена данными между сервером и клиентами, обеспечивая высокую производительность и надёжную защиту передаваемой информации. Библиотека обеспечивает асинхронное и неблокирующее взаимодействие, что позволяет обрабатывать тысячи соединений с минимальными задержками и высокой производительностью. Boost.Asio кроссплатформенна, поддерживает встроенные средства шифрования через модуль **SSL/TLS**, легко интегрируется с другими библиотеками Boost и стандартом C++, обеспечивая надёжность и гибкость архитектуры. Однако использование этой библиотеки требует глубокого понимания асинхронного программирования и управления потоками, а также внимательности при отладке, поскольку сложная структура колбэков и шаблонов затрудняет диагностику ошибок. Кроме того, Boost.Asio предоставляет лишь низкоуровневые механизмы работы с сетью, поэтому реализацию таких функций, как маршрутизация сообщений, авторизация или хранение данных, разработчику приходится выполнять самостоятельно. Несмотря на это, Boost.Asio остаётся оптимальным выбором для создания производительных, масштабируемых и безопасных систем обмена сообщениями.

В разработке качестве архитектурного ядра выступает **асинхронная событийная модель**, при которой каждый клиентский сеанс обрабатывается независимо, что предотвращает блокировки потоков и способствует масштабируемости системы. Для защиты данных применяется TLS/SSL-шифрование (через `boost::asio::ssl::stream`), обеспечивающее конфиденциальность и целостность передаваемых сообщений. Дополнительно реализуется аутентификация клиентов с использованием пар токенов, что предотвращает несанкционированный доступ. Основное подключение осуществляется через **WebSocket**, при каждом соединении происходит обновление пары токенов. На сервере предусмотрена возможность подключения нескольких устройств, что обеспечивает удобство и контроль активности каждого из них. Если происходит **кража токена**, его использование с другого устройства блокируется. Токены действительны в течение **15 минут** и не могут одновременно использоваться на двух активных сессиях.

Разработка данного мессенджера ведётся уже более шести месяцев, и за это время реализован полноценный набор функций, необходимых для современного коммуникационного приложения. Система поддерживает чаты между пользователями, возможность поиска контактов, отправку и приём текстовых сообщений и файлов, а также обработку событий в реальном времени, таких как

Date: 3rdDecember-2025

индикатор набора сообщения и статус подключения в сети. Кроме того, реализована функция ответов (reply) на отдельные сообщения, что делает общение более удобным и структурированным. Все эти возможности работают на основе асинхронной архитектуры Boost.Asio, обеспечивающей мгновенную реакцию интерфейса и стабильность соединения. Проект постоянно развивается — оптимизируются алгоритмы обмена данными, улучшается безопасность, добавляются новые функции и расширяются возможности серверной части.

СПИСОК ЛИТЕРАТУРЫ:

1. **Sutter H.** *C++ Concurrency in Action*. — Manning Publications, 2020.
2. **Boost Documentation.** *Boost.Asio C++ Library*. — Официальная документация.
URL: <https://www.boost.org/doc/libs/>
3. **Grimm R.** *Network Programming with Boost.Asio*. — Addison-Wesley, 2019.
4. **Kerrisk M.** *The Linux Programming Interface*. — No Starch Press, 2010.
5. **Rescorla E.** *SSL and TLS: Designing and Building Secure Systems*. — Addison-Wesley, 2001.
6. **Dougherty C.** *Secure Coding in C and C++*. — Addison-Wesley, 2013.
7. **Dierks T., Rescorla E.** *The Transport Layer Security (TLS) Protocol Version 1.3*. — IETF RFC 8446, 2018.
8. **Fielding R.** *Architectural Styles and the Design of Network-based Software Architectures*. — UC Irvine Dissertation, 2000.