**Техническое задание**

**на Защищенный месседжер**

**Содержание**

**Перечень сокращений и условных обозначений**

# 1 Общие сведения

## 1.1 Полное наименование системы

Полное наименование системы: Защищенный чат на основе криптографических алгоритмов.

## 1.2 Основания разработки

Основание для выполнения работ, являются документы:

* Техническое задание;
* Задание на курсовую работу;

## 1.3 Сроки исполнения работ

Начало разработки: 06.02.2017

Окончание разработки: 31.05.2017

# 2 Характеристика объекта реализации

## 2.1 Краткое описание объекта

Проект представляет собой клиент-серверное приложение, реализующее создание защищенного P2P чата между двумя клиентами, с хранением пользовательской информации в базе данных пользователей.

Основное назначение приложения, реализация защищенного корпоративного чата, с возможностью общения из внешней сети организации.

## 2.2 Краткое описание серверной части приложения

Сервер должен реализовывать следующие режимы работы:

* Режим регистрации пользователей;
* Режим авторизации пользователей;
* Режим поиска собеседника;
* Режим создания P2P соединения в рамках LAN;
* Режим STUN-сервера при работе через NAT.

Сервер должен реализовывать следующий функционал:

* Регистрация пользователей и генерация ключевой информации, с занесением данных пользователя в БД;
* Авторизация пользователей на сервере, на основе защищенных алгоритмов идентификации и аутентификации;
* Создание защищенного P2P соединения между пользователями при их нахождении в рамках одной корпоративной сети;
* Создание защищенного обмена сообщениями между пользователями, при нахождении одного из них за NAT.

## 2.3 Краткое описание клиентской части приложения

Клиентское приложение должно реализовывать следующие функции:

* Интерфейс взаимодействия;
* Сохранение ключевой информации и организация доступа к ней на основе ключевой фразы;
* Поддержка алгоритмов аутентификации используемых для авторизации на сервере;
* Поддержка алгоритмов генерации сессионных ключей;
* Поддержка алгоритмов симметричного шифрования, используемых на сервере, на основе сессионных ключей;
* Сохранение истории сообщений, зашифрованной на основе ключевой фразы.
* Работы в режиме P2P соединения;
* Работа через STUN сервер.

## 2.4 Краткое описание базы данных пользователей

База данных должна обеспечивать:

* Хранение аутентификационных данных пользователей;
* Хранение данных последней активности пользователя.

# 3 Требования к серверной части

## 3.1 Требования к размещению серверной части

Серверная часть должна быть установлена внутри корпоративной сети организации, при необходимости подключения из внешней сети организации требуется произвести проброс портов сервера во внешнею сеть.

## 3.2 Требование к режиму регистрации пользователей

Сервер в режиме регистрации пользователей должен реализовывать следующее:

* Генерация ключевой информации;
* Защищенная передача ключевой информации;
* Сохранение пользовательских данных в БД:
  + Логин пользователя;
  + Ключевая информация требуемая для аутентификации пользователя;
  + ID пользователя в системе.

## 3.3 Требования к режиму авторизации пользователей

Сервер в режиме авторизации пользователей должен реализовывать следующее:

* Идентификация пользователя;
* Аутентификация пользователя;
* Предоставление пользователю доступа к функциям системы.

Идентификация и аутентификация должны соответствовать требования *Главы 5 Требования по обеспечению защиты информации*.

## 3.4 Требования к режиму поиска собеседника

Доступ к режиму поиска собеседника должен предоставляться только авторизованным пользователям.

## 3.5 Требования к режиму создания P2P в рамках LAN

Сервер должен определять, находится ли пользователь за NAT или пользователь находятся внутри корпоративной сети.

При нахождении обоих пользователей в рамках одной корпоративной сети, сервер должен отправить адрес собеседника пользователям, для создания защищенного P2P соединения.

После создания соединения сервер продолжает обмен сообщениями с клиентским приложением, для возможности создания нескольких чатов.

## 3.6 Требования к режиму STUN-сервера

При нахождении одного из пользователя за NAT, сервер инициирует создание соединения пользователей через самого себя.

Сервер производит пересылку сообщений от пользователей друг другу.

Шифрование сообщений должно происходить на стороне клиента.

Сервер не должен производить модификации пакетов во время их пересылки между пользователями.