**Техническое задание**

**на Защищенный месседжер**

**Содержание**

[1 Общие сведения 4](#_Toc477445903)

[1.1 Полное наименование системы 4](#_Toc477445904)

[1.2 Основания разработки 4](#_Toc477445905)

[1.3 Сроки исполнения работ 4](#_Toc477445906)

[2 Характеристика объекта реализации 5](#_Toc477445907)

[2.1 Краткое описание объекта 5](#_Toc477445908)

[2.2 Краткое описание серверной части приложения 5](#_Toc477445909)

[2.3 Краткое описание клиентской части приложения 5](#_Toc477445910)

[2.4 Краткое описание базы данных пользователей 6](#_Toc477445911)

[3 Требования к серверной части 7](#_Toc477445912)

[3.1 Требования к размещению серверной части 7](#_Toc477445913)

[3.2 Требование к режиму регистрации пользователей 7](#_Toc477445914)

[3.3 Требования к режиму авторизации пользователей 7](#_Toc477445915)

[3.4 Требования к режиму поиска собеседника 7](#_Toc477445916)

[3.5 Требования к режиму создания P2P в рамках LAN 8](#_Toc477445917)

[3.6 Требования к режиму STUN-сервера 8](#_Toc477445918)

**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.

Сервер должен однозначно определять нахождения пользователя за NAT или в рамках LAN в автоматическом режиме.

## 3.7 Требования к организации базы данных

База данных клиентов должна обеспечивать хранение следующих данных пользователей:

* Логин;
* Хеш для аутентификации пользователя;
* Дату последней авторизации;
* ID пользователя;
* Имя пользователя;

# 4 Требования к клиентской части

## 4.1 Требования к интерфейсу взаимодействия

Интерфейс приложения должен:

* Форму регистрации;
* Форму авторизации;
* Форму выбора собеседника;
* Окно чата, состоящие из поля ввода сообщений; поля отображения сообщений собеседника;

## 4.2 Требования к криптографическим системам

Клиентское приложение должно реализовывать используемые алгоритмы аутентификации, шифрования и т.д. используемые серверным приложением.

Данные алгоритмы должны использоваться в следующих функциях системы:

* В режиме регистрации, поддержка алгоритмов распределения ключей, сохранение полученной ключевой информации по ключевой фразе;
* В режиме аутентификации, поддержка алгоритмов аутентификации и алгоритмов доступа к ключевой информации на основе ключевой фразы;
* В режиме работы чата, обеспечивать поддержку создания сессионного ключа и реализовывать требуемое симметричное шифрование на основе сессионного ключа;
* Сохранение истории сообщений на основе ключевой фразы;

Выбор алгоритмов для реализации системы описан в *Главы 5 Требования по обеспечению защиты информации*.

## 4.3 Требования к сетевому взаимодействую

Клиентское приложение должно обеспечивать такие режимы работы:

* Создание P2P соединения с собеседников в рамках одной корпоративной сети;
* Создание соединения с собеседников через STUN-сервер;

# 5 Требования по обеспечению защиты информации

Данная глава направлена на определение основных функций по защите информации

Составим модель угроз на основании которой будем строить защиту.

Для построения модели угроз, составим модель нарушителей.

## 5.1 Модель нарушителей

В нашей системе предполагается работа как из внутренней корпоративной сети, так и из внешней сети Интерне, основываясь на этой информации выделим 2 типа нарушителей:

* Внутренние нарушители;
* Внешние нарушители;

Выделим уровень подготовки нарушителей разного типа:

* Внутренний нарушитель имеет доступ с корпоративной сети, может создавать P2P соединения;  
  Имеет возможность прослушивать и модифицировать канал связи, имеет возможность читать, но не имеет возможности модифицировать информацию на локальном ПК собеседника;
* Внешний нарушитель обладает средней квалификацией в сфере информационной безопасности, имеет возможность прослушивать и модифицировать канал связи, не имеет возможности читать и модифицировать информацию на локальном ПК собеседника.

## 5.2 Модель угроз информационной безопасности системы

На основе составленной модели нарушителей и целей разработки данной системы выделим угрозы, от которых наша система будем защищена.

Произведем классификацию угроз:

* По виду нарушаемого свойства информации:
  + Угрозы конфиденциальности информации (утечка, перехват, съем, копирование, хищение информации);
  + Угрозы целостности информации (утраты, модификации информации);
* Угрозы несанкционированного доступа:
  + Угрозы, реализуемые с применением программных средств в операционной системы.

## 5.3 Выбор механизмов для закрытия выявленных угроз в соответствии с моделью

В соответствии с составленной моделью угроз, требуется реализовать следующие механизмы защиты:

* Защищенная регистрация пользователей в системе.   
  Алгоритмы регистрации должны обеспечивать безопасное распределение ключевой информации; Так же сохранение ключевой информации на локальном ПК в зашифрованном виде, на основе ключевой фразы; Закрываемые угрозы: конфиденциальности, целостности, НСД;
* Алгоритмы аутентификации должны обеспечивать, аутентификацию на сервере на основе алгоритмов с нулевым разглашением; Закрываемые угрозы: конфиденциальности, целостности;
* Создание сессионного ключа на основе алгоритмов с нулевым разглашением; Использование ключа длинной не менее 256-бит. Использование симметричного шифрования. Закрываемые угрозы: конфиденциальности, целостности.