**Министерство образования и науки РФ**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»**

**(ВлГУ)**

**Кафедра информатики и защиты информации**

**Техническое задание для программы «Защищенный чат»**

**по дисциплине:**

**«Защита информационных систем»**

Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ к.т.н. Монахов Ю.М.

подпись, дата

Студент гр. ИБм-116\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.А. Шибнев

подпись, дата

Владимир 2017

**Содержание**

[1 Общие сведения 4](#_Toc478032590)

[1.1 Полное наименование системы 4](#_Toc478032591)

[1.2 Основания разработки 4](#_Toc478032592)

[1.3 Сроки исполнения работ 4](#_Toc478032593)

[2 Характеристика объекта реализации 5](#_Toc478032594)

[2.1 Краткое описание объекта 5](#_Toc478032595)

[2.2 Краткое описание серверной части приложения 5](#_Toc478032596)

[2.3 Краткое описание клиентской части приложения 5](#_Toc478032597)

[2.4 Краткое описание базы данных пользователей 6](#_Toc478032598)

[3 Требования к серверной части 7](#_Toc478032599)

[3.1 Требования к размещению серверной части 7](#_Toc478032600)

[3.2 Требование к режиму регистрации пользователей 7](#_Toc478032601)

[3.3 Требования к режиму авторизации пользователей 7](#_Toc478032602)

[3.4 Требования к режиму защищенного обмена сообщениями между клиентами 7](#_Toc478032603)

**Перечень сокращений и условных обозначений**

БД – база данных

ID – идентификатор клиента

# 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 чата между двумя клиентами, с хранением пользовательской информации в базе данных пользователей.

Основное назначение приложения, реализация защищенного корпоративного чата.

## 2.2 Краткое описание серверной части приложения

Сервер должен реализовывать следующие режимы работы:

* Режим регистрации пользователей;
* Режим авторизации пользователей;
* Режим защищенного обмена сообщениями

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 обмена сообщениями между пользователями.

## 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;

## 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.

## 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.
  + Ключевая информация, требуемая для защищенного обмена сообщениями.

## 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.

## 3.4 Требования к режиму защищенного обмена сообщениями между клиентами

* Шифрование каждого сообщения между клиентами;
* Сбрасывать соединение после 5 минут бездействия.

## 3.5 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;

## 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 регистрации, 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;

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

## 5 Требования по обеспечению защиты информации

Данная глава направлена на определение основных функций по защите информации

Для построения модели угроз, составим модель нарушителей.

## 5.1 Модель нарушителей

В нашей системе предполагается работа из внутренней корпоративной сети, основываясь на этой информации выделим тип нарушителей:

* Внутренние нарушители;

Выделим уровень подготовки нарушителей разного типа:

* Внутренний нарушитель имеет доступ к корпоративной сети;  
  Имеет возможность прослушивать и модифицировать канал связи;
* Имеет возможность читать, но не имеет возможности 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.