**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\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.О. Николаев

подпись, дата

Владимир 2017

**Содержание**

[1. Введение 3](#_Toc477989622)

[1.1. Название программы 3](#_Toc477989623)

[1.2. Назначение и область применения 3](#_Toc477989624)

[1.3. Общее описание 3](#_Toc477989625)

[2. Требования к программе 3](#_Toc477989626)

[2.1. Требование к представлению информации 3](#_Toc477989627)

[2.2. Требования к функциональным характеристикам 3](#_Toc477989628)

[2.3. Требования к надежности 4](#_Toc477989629)

[2.4. Модель нарушителя 4](#_Toc477989630)

[3. Процесс эксплуатации 4](#_Toc477989631)

[4. Сроки и этапы разработки 5](#_Toc477989632)

[5. Цены разработки, порядок контроля и приемки 5](#_Toc477989633)

## Введение

## Название программы

Название программы: «Защищенный чат».

## Назначение и область применения

Программа предназначена для защищенного обмена сообщениями между двумя пользователями. Область применения – личное, некоммерческое использование, использование в бизнесе для обмена конфиденциальной информацией

## Общее описание

Программа представляет собой приложение для персонального компьютера с возможностью отправки сообщений другой копии программы в локальной сети и в сети Интернет, и получение сообщений от него в зашифрованном виде. Приложение разрабатывается для компьютеров, работающих на операционной системе Windows 10.

## Требования к программе

## Требование к представлению информации

Информация, получаемая одним пользователем от другого пользователя, должна быть представлена в виде последовательности символов, отправляемой другой пользователем. Сообщения не могут содержать файлы, картинки, аудио или видео.

## Требования к функциональным характеристикам

Программа должна обеспечивать выполнение следующих свойств:

1. Безопасность и конфиденциальность. Для получения доступа в программу, пользователь должен установить сложный пароль, при первом включении программы. Пароль должен содержать от 16 до 40 символов, среди которых буквы латинского алфавита верхнего и нижнего регистра, арабские цифры, служебные знаки. Пароль хранится на персональном компьютере пользователя в зашифрованном виде. Для обмена сообщений используется протокол, шифрующий сообщения на основе открытого и закрытого ключа. Открытый ключ передается по каналу связи, закрытый ключ хранится в зашифрованном виде на компьютере пользователя. Сообщения должны передаваться по каналу связи в зашифрованном виде. Для шифрования используются крипто стойкие алгоритмы.
2. Доступность. Пользователи должны иметь возможность начать обмен сообщениями в любое время.
3. Целостность. Сообщения, передаваемые пользователем, на этапе шифрования и дешифрования должны совпадать.

## Требования к надежности

Программа должна надежно работать без каких-либо ошибок: устанавливать соединение между пользователями, должны выполняться требования безопасности, доступности и целостности.

## Модель нарушителя

## Процесс эксплуатации

При первом включении программы, от пользователя требуется ввести сложный пароль, содержащий от 16 до 40 символов, среди которых буквы латинского алфавита верхнего и нижнего регистра, арабские цифры, служебные знаки. Пароль сохраняется в зашифрованном виде на компьютере пользователя в директории с программой. Для каждого последующего включения пользователю требуется ввести пароль.

Пользователь указывает ip адрес и порт собеседника, о которых они договариваются заранее.

В процессе установки соединения создается пара: открытый и закрытый ключ. Открытый ключ передается в зашифрованном виде другой стороне. Далее, следуя крипто алгоритму, если ключи подходят, устанавливается соединение

Все сообщения, которыми обмениваются пользователи, шифруются с помощью крипто стойкого алгоритма.

Для окончания чата, пользователь закрывает программу, соединение прерывается.

## Сроки и этапы разработки

Начало разработки: 06.02.2017

Окончание разработки: 31.05.2017