**Жизненный цикл программного продукта:**

**1. Формирование требований к программному продукту (далее —ПП)**

ПП должен быть разработан для обмена защищенными сообщениями между пользователями.

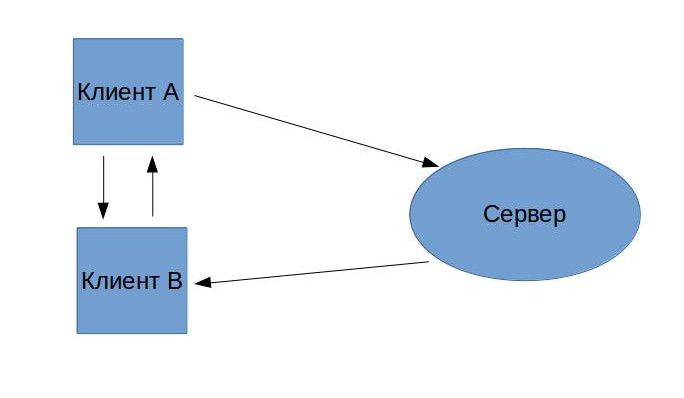
ПП должен отработать без сбоев от начала и до конца всего

процесса обмена сообщениями.

Система защиты (далее СЗИ) ПП должна учитывать реальные угрозы нарушения конфиденциальности пользователей и вскрытию сообщений.

**2. Разработка концепции.**

Рассмотрим концепцию ПП, состоящего из 2 клиентов и 1 сервера.



Клиент А направляет запрос серверу для инициации процесса обмена с клиентом В, после удачного соединения клиента А и В начинается обмен сообщениями между этими клиентами.

**3. Техническое задание**

***1. Введение***

1.1 Наименование программного продукта

Наименование программного продукта (далее - ПП) «программа для обмена защищенными сообщениями (ПОЗС)».

1.2 Назначение и область применения

ПП должен быть разработан для обмена защищенными сообщениями между пользователями.

1.3 Общее описание

ПП состоит из клиентской программы (далее — КП) и серверной программы (далее — СП).

***2. Требования к ПП***

2.1 Требования к функциональным характеристикам

ПП должна обеспечивать возможность выполнения перечисленных ниже функций:

2.1.1 Сообщения должны быть зашифрованы.

2.1.2 КП обмениваются обмениваются сообщениями, при этом сообщения отправляются напрямую между КП.

2.1.3 СП должен обеспечивать авторизацию между КП готовых к обмену сообщений.

2.1.4 В КП должен быть реализован протокол удостоверения подлинности и обмена ключей.

2.1.5 СП должен выступать в качестве доверенной стороны для осуществления обмена сеансовыми ключами между КП.

2.1.6 СП должен производить регистрацию пользователей.  
 2.2. Требования к надежности

### 2.2.1 Требования к обеспечению надежного функционирования программы

Надежное (устойчивое) функционирование программы должно быть обеспечено выполнением Заказчиком совокупности организационно-технических мероприятий, перечень которых приведен ниже:   
а) организацией бесперебойного питания технических средств;   
б) использованием лицензионного программного обеспечения;   
в) регулярным выполнением рекомендаций Министерства труда и социального развития РФ, изложенных в Постановлении от 23 июля 1998 г. Об утверждении межотраслевых типовых норм времени на работы по сервисному обслуживанию ПЭВМ и оргтехники и сопровождению программных средств»;   
г) регулярным выполнением требований ГОСТ 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов

### 2.2.2. Время восстановления после отказа

Время восстановления после отказа, вызванного сбоем электропитания технических средств (иными внешними факторами), не фатальным сбоем (не крахом) операционной системы, не должно превышать 30-ти минут при условии соблюдения условий эксплуатации технических и программных средств.   
Время восстановления после отказа, вызванного неисправностью технических средств, фатальным сбоем (крахом) операционной системы, не должно превышать времени, требуемого на устранение неисправностей технических средств и переустановки программных средств.

### 2.2.3. Отказы из-за некорректных действий пользователей системы

Отказы программы вследствие некорректных действий пользователя при взаимодействии с программой недопустимы.

# ***3. Условия эксплуатации***

## 3.1. Климатические условия эксплуатации

Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики, должны удовлетворять требованиям, предъявляемым к техническим средствам в части условий их эксплуатации

3.2. Требования к квалификации и численности персонала

Требования к квалификации и численности персонала не устанавливаются.

## 3.3. Требования к составу и параметрам технических средств

## 3.3.1. В состав технических средств должен входить персональный компьютер, выполняющий роль сервера, включающий в себя:

## 3.3.1.1. процессор Pentium-2.0Hz, не менее; 3.3.1.2. оперативную память объемом, 1Гигабайт, не менее; 3.3.1.3. HDD, 40 Гигабайт, не менее; 3.3.1.4. предустановленный Python 3.0, не менее.

3.3.1.5. предустановленная операционная система, совместимая с высокоуровневым языком программирования Python 3.

3.3.2. В состав технических средств должен входить персональный компьютер, выполняющий роль клиента, включающий в себя:

3.3.1.1. процессор Pentium-2.0Hz, не менее;   
3.3.1.2. оперативную память объемом, 1Гигабайт, не менее;   
3.3.1.3. HDD, 40 Гигабайт, не менее;   
3.3.1.4. предустановленный Python 3.0, не менее.

3.3.1.5. предустановленная операционная система, совместимая с высокоуровневым языком программирования Python 3.

### 3.4.2. Требования к исходным кодам и языкам программирования

ПП должен быть написан на высокоуровневом языке программирования Python 3.

### 3.4.3. Требования к защите информации и программ

ПП должен учитывать все возможные угрозы безопасности при обмене сообщениями, для чего необходимо составить список защищаемых ресурсов и потоков, а так же модель потенциального нарушителя.

При обмене сообщениями пользователи должны быть уверены в подлинности своего собеседника.

ПП должен производить обмен сообщениями напрямую между пользователями, что бы данные обмена сохранялись в секрете.

Сообщения при обмене должны иметь зашифрованный вид.

## 3.5. Специальные требования

Взаимодействие между КП может осуществляться через консоль, без использования графического интерфейса.

## ***4. Требования к программной документации***

## 4.1. Предварительный состав программной документации

Состав программной документации должен включать в себя:   
4.1.1. техническое задание;  
4.1.2. программу и методики испытаний.

4.1.3. Список защищаемых ресурсов и потоков;

4.1.4. Модель потенциального нарушителя.

# ***5. Технико-экономические показатели***

## 5.1. Экономические преимущества разработки

Ориентировочная экономическая эффективность не рассчитываются. Аналогия не проводится ввиду уникальности предъявляемых требований к разработке.

# ***6. Стадии и этапы разработки***

## 6.1. Стадии разработки

Разработка должна быть проведена в три стадии:   
1. разработка технического задания;   
2. рабочее проектирование;   
3. внедрение.

6.2. Этапы разработки

На стадии разработки технического задания должен быть выполнен этап разработки, согласования и утверждения настоящего технического задания.   
На стадии рабочего проектирования должны быть выполнены перечисленные ниже этапы работ:

1. разработка программы;   
2. разработка программной документации;   
3. испытания программы.

На стадии внедрения должен быть выполнен этап разработки подготовка и передача программы.

## 6.3. Содержание работ по этапам

На этапе разработки технического задания должны быть выполнены перечисленные ниже работы:   
1. постановка задачи;   
2. определение и уточнение требований к техническим средствам;   
3. определение требований к программе;  
4. определение стадий, этапов и сроков разработки программы и документации на неё;   
5. согласование и утверждение технического задания.   
На этапе разработки программы должна быть выполнена работа по программированию (кодированию) и отладке программы.   
На этапе разработки программной документации должна быть выполнена разработка программных документов в соответствии с требованиями к составу документации.   
На этапе испытаний программы должны быть выполнены перечисленные ниже виды работ:   
1. разработка, согласование и утверждение и методики испытаний;   
2. проведение приемо-сдаточных испытаний;   
3. корректировка программы и программной документации по результатам испытаний.   
На этапе подготовки и передачи программы должна быть выполнена работа по подготовке и передаче программы и программной документации в эксплуатацию на объектах Заказчика.

***7. Порядок контроля и приемки***

## 7.1. Виды испытаний

Приемо-сдаточные испытания должны проводиться на объекте Заказчика в оговоренные сроки.   
Приемо-сдаточные испытания программы должны проводиться согласно разработанной Исполнителем и согласованной Заказчиком Программы и методик испытаний.   
Ход проведения приемо-сдаточных испытаний Заказчик и Исполнитель документируют в Протоколе проведения испытаний.

## 7.2. Общие требования к приемке работы

На основании Протокола проведения испытаний Исполнитель совместно с Заказчиком подписывает Акт приемки-сдачи программы в эксплуатацию.

**4. Эскизный проект.**

ПП будет написан на языке программирования Python и будет состоять из 2 частей, 1 часть — клиент, 2 часть — сервер.

Описание клиентского приложения (далее - КП).

КП предназначен для отправки зашифрованных сообщений между разными КП. Шифрование основывается на принципе разделения секрета.

Сервер отвечает за установку соединения между КП, при этом на сервере должны храниться только имена клиентов. Через сервер не должно происходить обмена сообщениями.

**5. Технический проект.**

Рассмотрев предъявленные требования, а так же учитывая что это приложение для обмена сообщениями, что подразумевает, что все операции по зашифровки и расшифровки сообщений должно происходить быстро, было принято решение реализовать схему Fiat-Shamir. Данная схема представляет интерес и в том, что сервер должен выступать в роли доверенной стороны, которая в свою очередь отвечает за коммутацию между клиентами, но при это не должен участвовать в обмене сообщениями.

Список защищаемых ресурсов и потоков.

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование ресурса или потока | Расположение |
|  | База данных зарегистрированных пользователей | Сервер |
|  | Сеансовый ключ | Клиент |
|  | Зашифрованные сообщения | Клиент |
|  | Расшифрованные сообщения | Клиент |
|  | Трафик между пользователями | Сеть |
|  | Сертификаты клиентов | Сервер |

Модель угроз потенциального нарушителя

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование ресурса или потока | Угрозы со стороны потенциального нарушителя |
|  | База данных зарегистрированных пользователей | В том случае, если нарушитель завладеет базой данных зарегистрированных пользователей, он сможет выдать себя за любого зарегистрированного пользователя, что будет означать утрату доверия к серверу. |
|  | Сеансовый ключ | В том случае, если нарушитель завладеет сеансовым ключем, у него появится возможность обмениваться зашифрованными сообщениями с другим пользователем, без подмены в базе данных зарегистрированных пользователей, нарушитель не сможет выдавать себя за другого пользователя |
|  | Зашифрованные сообщения | В том случае, если нарушитель завладеет зашифрованными сообщениями, без знания сеансового ключа, он не сможет прочитать открытый текст сообщения |
|  | Расшифрованные сообщения | Нарушитель может получить открытый текст сообщения, в случае если как минимум на одном из двух клиентов будет установлена программа считывающая ввод с клавиатуры, либо выгружающая информацию из оперативной памяти компьютера. |
|  | Трафик между пользователями | В том случае, если нарушитель будет прослушивать трафик между двумя клиентами, обменивающимися зашифрованными сообщениями, без знания сеансового ключа он не сможет прочитать открытые сообщения. |
|  | Сертификаты клиентов | В том случае, если нарушитель завладеет полным списком сертификатов клиентов, он сможет доказать факты обмена зашифрованными сообщениями. |

В данной системе, нарушитель может быть как внешним, так и внутренним, с разным уровнем образования и мотивации. Другие угрозы со стороны потенциального нарушителя не рассматриваются, т. к. являются экономически не целесообразными, либо мало вероятными.