УТВЕРЖДЕН

111.12345678.01234-01 90 01-ЛУ

**НАИМЕНОВАНИЕ СИСТЕМЫ**

**Техническое задание**

**111.12345678.01234-01 90 01**

**Листов 16**

2021

СОДЕРЖАНИЕ

[1. Введение 3](#_Toc72504887)

[1.1. Наименование программы 3](#_Toc72504888)

[1.2. Краткая характеристика области применения 3](#_Toc72504889)

[2. Основания для разработки 4](#_Toc72504890)

[3. Назначение разработки 5](#_Toc72504891)

[3.1. Функциональное назначение 5](#_Toc72504892)

[3.2. Эксплутационное назначение 5](#_Toc72504893)

[4. Требования к программе или программному изделию 6](#_Toc72504894)

[4.1. Требования к функциональным характеристикам 6](#_Toc72504895)

[4.1.1. Требования к составу выполняемых функций 6](#_Toc72504896)

[4.1.2. Требования к организации входных и выходных данных 7](#_Toc72504897)

[4.1.3. Требования к средствам и способам связи для информационного обмена между компонентами системы. 7](#_Toc72504898)

[4.1.4. Требования к защите информации от несанкционированного доступа. 8](#_Toc72504899)

[4.2. Требования к надежности 8](#_Toc72504900)

[4.3. Условия эксплуатации 9](#_Toc72504901)

[4.3.1. Сведения об условиях эксплуатации объекта автоматизации 9](#_Toc72504902)

[4.3.2. Требования по диагностированию системы 10](#_Toc72504903)

[4.4. Требования к составу и параметрам технических средств 10](#_Toc72504904)

[4.5. Требования к информационной и программной совместимости 11](#_Toc72504905)

[4.6. Специальные требования 11](#_Toc72504906)

[5. Требования к программной документации 13](#_Toc72504907)

[6. Технико-экономические показатели 14](#_Toc72504908)

[7. Стадии и этапы разработки 15](#_Toc72504909)

[8. Порядок контроля и приемки 16](#_Toc72504910)

1. Введение
   1. Наименование программы

Программное обеспечение, осуществляющее защищенную передачу сообщений в одной сети криптографическими алгоритмами.

* 1. Краткая характеристика области применения

Передачу конфиденциальной информации между РС необходимо осуществлять только с использованием средств аппаратной, программной и криптографической защиты. Данное ПО предоставит возможность шифрования сообщений несколькими видами алгоритмов, что обеспечит надежность канала связи.

Программное обеспечение по защите системы создается с целью:

1. Обеспечить триаду безопасности Конфиденциальность-Целостность-Доступность (модель CIA)

2. Обеспечить передачу зашифрованной информации без риска их перехвата и дальнейшего взаимодействия.

1. Основания для разработки

Основанием для разработки является задание по дисциплине «Технологии и методы программирования», которое является частью программы направления 10.05.03 «Информационная безопасность автоматизированных систем». Задание утверждено доцентом Будылиной Евгенией Александровной.

Исполнители обязаны разработать и протестировать систему «Программное обеспечение, осуществляющее защищенную передачу сообщений в одной сети криптографическими алгоритмами» не позднее 04.06.2021, предоставить исходные коды и документацию к разработанной системе не позднее 11.06.2021.

Наименование темы разработки – «Программное обеспечение, осуществляющее защищенную передачу сообщений в одной сети криптографическими алгоритмами».

Условное обозначение темы разработки (шифр темы) – «ПО для передачи зашифрованных сообщений в одной сети.».

1. Назначение разработки

Данное ПО предназначено для использования тремя группами пользователей: начальник подразделения, его подчиненные и специалист по сетевым технологиям.

* 1. Функциональное назначение

Для получения доступа к ПО необходимо пройти регистрацию, в зависимости от аккаунта приложение дает возможность принимать или отправлять сообщения. Данное ПО осуществляет симметричное шифрование и предназначено для обеспечения передачи зашифрованных сообщений по открытому каналу криптографическими средствами.

* 1. Эксплутационное назначение

Данное ПО используется во многих подразделениях автоматизированных систем, где есть риск потерять необходимые данные (персональные данные, базы данных, реестр данных, общие сведения предприятий).

1. Требования к программе или программному изделию
   1. Требования к функциональным характеристикам
      1. Требования к составу выполняемых функций

ПО для передачи зашифрованных сообщений в одной сети должно представлять собой систему, включающую в себя подсистемы:

* авторизацию
* поиск пользователя в защищенной БД
* шифрование/расшифрование сообщений
* отправка/прием сообщений

1. Авторизация:

* Для доступа к программе пользователю необходимо зарегистрироваться, после этого его логин и пароль появляются в базе данных, и он сможет авторизоваться в системе
* Для авторизации пользователь должен ввести логин и пароль, в случае, если логин и пароль совпадают с теми, что находятся в базе данных, авторизация проходит успешно, и пользователь получает доступ к программе. В случае, если логин и/или пароль не совпадают с теми, что находятся в базе данных, авторизация завершается ошибкой

1. Поиск пользователя в защищенной БД:

* После прохождения регистрации пользователем введенные им логин и пароль попадают в базу данных
* Алгоритм ищет совпадение с логином и паролем, которые находятся в базе данных посредством сверки каждого символа

1. Ключ шифрования:

* Ключ шифрования выбирается администратором и сообщается пользователям. Смена ключа производится минимум один раз в 30 дней

1. Шифрование/расшифрование сообщений:

* Шифрование осуществляется тремя алгоритмами шифрования на выбор субъекта, осуществляющего отправку сообщений, с помощью ключа
* Расшифрование осуществляется с помощью ключа тем алгоритмом, на котором сообщение зашифровано принимающей стороной

1. Отправка/прием сообщений:

* Для отправки сообщений нужно авторизоваться под аккаунтом администратора, так как только администратор может отправлять сообщения
* Для получения сообщений нужно авторизоваться под аккаунтом пользователя
* Администратор загружает текст для шифрования из файла или же собственноручно, вводит ключ и отправляет сообщение
* Пользователь получает уведомление о новом сообщении и нажимает «Принять сообщение», после копирует его в поле для сообщения, вводит ключ и получает расшифрованное сообщение
  + 1. Требования к организации входных и выходных данных

Входные данные должны представлять собой осмысленные слова, словосочетания и предложения на русском языке.

Выходными данными является зашифрованный текст, который прошел шифрование в соответствие с выбранными алгоритмами шифрования или же расшифрованный текст, который прошел дешифрование в соответствие с выбранным алгоритмом.

* + 1. Требования к средствам и способам связи для информационного обмена между компонентами системы.

Для информационного обмена между компонентами системы должна быть организована локальная сеть. ПО для передачи зашифрованных сообщений функционирует на сервере, к которому имеют доступ пользователи этой программой по средствам локальной сети.

* + 1. Требования к защите информации от несанкционированного доступа.

ПО для передачи зашифрованных сообщений в одной сети нуждается в защите информации от несанкционированного доступа. ПО защищается паролем. Существует три вида доступа:

1. доступ пользователям – адресат (регистрироваться и авторизовываться под аккаунтом пользователя, получать сообщения и расшифровывать их);
2. доступ администратора – адресант (авторизовываться под аккаунтом администратора, получать сообщения и зашифровывать их);
3. доступ специалист по сетевым технологиям – регистрировать аккаунт администратора, заполнять, вносить изменения в подсистему программы связанную с защитой и подготовкой отчетности, вести профилактические мероприятия, следить за правильностью ведения БД;
   1. Требования к надежности

Необходимо, чтобы система обладала устойчивостью к отказам оборудования и программных систем, а также электропитания. Для надежной работы комплекса необходимы высоконадежные аппаратные и программные системы. Требования надежности должны быть регламентированы для следующих аварийных ситуаций:

* выход из строя аппаратных средств системы;
* отсутствие электроэнергии;
* выход из строя программных средств системы;
* неверные действия персонала компании;
* пожар, взрыв и т.п.

Методы оценки и контроля показателей надежности на разных стадиях создания системы должны отвечать следующим особенностям:

* многофункциональность;
* сложные формы взаимосвязи систем комплекса;
* существенная роль временных соотношений отказов отдельных систем комплекса;
* разнообразные законы распределения среднего времени безотказной работы и восстановления.

Сохранность информации должна быть обеспечена в следующих случаях:

* выход из строя аппаратных систем комплекса;
* стихийные бедствия (пожар, наводнение, взрыв, землетрясение и т.п.);
* хищение носителей информации, других систем комплекса;
* ошибки в программных средствах;
* неверные действия сотрудников.

Для сохранности информации необходимо предусмотреть использование блоков бесперебойного питания для защиты данных от повреждения в случае отключения питания, для надёжного хранения данных необходимо производить еженедельное резервное копирование БД на несколько дисков.

Для выполнения операции отката и повышения надёжности хранения базы данных предусмотреть раздельное хранение двух дополнительных копий (с возможностью сохранения на различных физических носителях).

* 1. Условия эксплуатации
     1. Сведения об условиях эксплуатации объекта автоматизации

Данное ПО используется для передачи зашифрованных сообщений между руководителем организации/филиала/отдела и его подчиненными**.**

Документация, связанная с ПО разрабатывается и дополняется каждую неделю:

* техническое задание дополняется каждую неделю, а также вносятся правки в случае изменения или увеличения функционала ПО;
* техническая документация будет создана по окончанию написания кода с помощью автоматизированного сервиса.

Функционирование системы должно происходить в требуемых условиях:

* при конструктивной температуре, давлении и допустимом уровне запыленности. «Гигиенические требования к микроклимату производственных помещений». Специалист выполняет соответствующие ему функции ежедневно (кроме субботы и воскресения) с 9.00 до 18.00 часов.
* сеть энергоснабжения должна иметь следующие параметры: напряжение – 220В; частота – 50Гц.
  + 1. Требования по диагностированию системы

Диагностика и профилактика технических средств проводится раз в месяц. Проверка целостности данных и нарушений проводится по мере необходимости. Проверка программного и аппаратного обеспечения проводится по мере необходимости.

* 1. Требования к составу и параметрам технических средств

ПО для передачи зашифрованных сообщений в одной сети

требует для своей работы установки следующего ПО:

1. На сервере ПО для передачи зашифрованных сообщений в одной сети должны быть установлены:
   * + - Операционная система: Microsoft Windows 10,
       - СУБД Microsoft Access 10 (БД аккаунтов пользователей)
2. На рабочей станции пользователя необходимо установить:
   * + - Операционная система: Microsoft Windows 10;
       - ПО для передачи зашифрованных сообщений в одной сети.

Для функционирования ИС необходимо:

* локальная вычислительная сеть на основе протокола TCP/IP с пропускной способностью 10/100 Мбит/с.

Сервер должен удовлетворять следующим минимальным требованиям:

* процессор Celeron-500MHz или аналогичный,
* 1 Gb и более оперативной памяти;
* 80 Gb – жесткий диск
* Монитор – SVGA;
* Клавиатура - 101/102 клавиши;
* Манипулятор типа «мышь».

Требования, предъявляемые к конфигурации клиентских станций:

* процессор, с тактовой частотой не менее 400 MHz,
* 256 Mb оперативной памяти;
* Монитор – SVGA;
* Клавиатура - 101/102 клавиши;
* Манипулятор типа «мышь».
  1. Требования к информационной и программной совместимости

Программы пользователя и администратора обмениваются с СУБД сообщениями по локальной сети. Должно быть исключено появление посторонних устройств в сети.

* 1. Специальные требования

Для работы с ПО необходимо разделение пользователей на:

1. пользователь – сотрудник организации, который не имеет прав администратора (имеет возможность осуществлять регистрацию и авторизацию пользователя, получать и расшифровывать сообщения с помощью ключа);
2. администратор – сотрудник организации, который имеет права администратора (имеет возможность осуществлять авторизацию администратора, отправлять и зашифровывать/расшифровывать сообщения с помощью ключа).
3. специалист по сетевым технологиям – сотрудник организации, который имеет возможность корректировки информации в БД, вести профилактические мероприятия, следить за правильностью ведения БД, осуществлять регистрацию администратора.

Квалификация пользователя программы:

Пользователь программы должен владеть навыками работы с операционной системой Microsoft Windows 10.

1. Требования к программной документации

Проектная документация должна быть разработана в соответствии с ГОСТ 19.201-78 и ГОСТ ЕСПД.

Отчетные материалы должны включать в себя текстовые материалы (представленные в виде бумажной копии и на цифровом носителе в формате MS Word) и электронные материалы (доска Trello, Github, Docker, сайт, код ПО).

Предварительный состав программной документации:

* техническое задание (включает описание применения);
* проектная документация;
* документация по тестированию;
* руководство пользователя ПО для передачи зашифрованных сообщений в одной сети
* руководство администратора ПО для передачи зашифрованных сообщений в одной сети
* руководство для специалиста по сетевым технологиям ПО для передачи зашифрованных сообщений в одной сети

1. Технико-экономические показатели

ПО для передачи зашифрованных сообщений в одной сети будет использоваться руководителями и сотрудниками предприятия, работающего с персональными данными и конфиденциальной информацией. Обмен информацией между компонентами системы и руководителями/сотрудниками предприятия должен производиться путем передачи зашифрованных электронных документов и иной информации.

ПО не требует высоких требований технического обеспечения организации и удобна в использовании. Использование ПО и поддержка его функционирования не требует высокой квалификации персонала и дальнейшего сопровождения разработчиков, поэтому при невысокой рыночной цене, ПО сможет выйти на рынок и составит достойную конкуренцию своим конкурентам. Экономический эффект может быть обеспечен за счет продажи ПО и платной установки.

1. Стадии и этапы разработки

Перечень документов, предъявляемых по окончании соответствующих стадий по созданию системы, представлен в таблице 1.

Разработка системы предполагается по укрупненному календарному плану, приведенному в таблице 1.1.

Таблица 1 – Календарный план работ по созданию

|  |  |  |
| --- | --- | --- |
| Наименование стадий и этапов создания системы | Сроки выполнения работ | Результаты работ |
| 1. Выбор проекта и начало разработки  1.1. Разработка предварительных проектных решений ПО, сайта, создание Github, разработка ТЗ.  1.2. Распределение задач с помощью доски Trello. | 19.02.21 – 19.03.21 | Описание системы и ее функций, предварительная версия сайта, утвержденная структура Github и ТЗ. Назначение ответственных за определенные задачи. |
| 2. Работа над кодом ПО, доработка сайта, работа с Docker и Github, построение UseCase и диаграммы классов. | 20.03.21 – 18.04.21 | Описание ПО, информационной базы, интерфейса, упаковка программы в Docker, диаграммы для ПО. |
| 3. Рабочая документация  3.1. Разработка рабочей документации для ПО.  3.2. Разработка стратегии тестирования ПО | 19.04.21 - 31.05.21 | Готовая версия ПО. Документация для ПО.  Стратегия тестирования. |
| 4. Ввод в действие.  4.1 Проведение UnitTest. | 01.06.21 – 21.06.21 | Протокол испытаний.  Устранение неполадок.  Внесение изменений в документацию. |

1. Порядок контроля и приемки

Нужно установить контроль и приемку результатов работ на каждой стадии создания ПО в соответствии с разделом 7.

На стадии 3 принимается готовая версия программного продукта.

Остальные результаты работ передаются в виде документов (согласно табл. 1).

Приемка этапа заключается в рассмотрении и оценке проведенного объема работ и предъявленной технической документации в соответствии с требованиями настоящего технического задания.

Ответственность за организацию и проведение приемки системы должен нести преподаватель. Приемка системы должна производиться по завершению приемки всех задач системы. При этом необходимо предоставить обеспечение материальной частью (технические средства), проектной документацией и специально выделенным персоналом.

Завершающим этапом при приемке системы должно быть составление акта приемки.