**Спецификация требований**

**1. Введение**

**1.1. Назначение документа**

Настоящий документ представляет собой спецификацию требований к программному обеспечению для проекта по разработке приложения, реализующего функционал шифрования по методу Виженера, хеширования SHA-512, численного решения уравнений методом деления отрезка пополам (бисекции) и нахождения кратчайшего расстояния между вершинами графа.

Документ предназначен для команды разработчиков, тестировщиков, менеджеров проекта и иных заинтересованных лиц, участвующих в создании, тестировании и сопровождении системы.

**1.2. Область применения**

Разрабатываемое программное обеспечение является клиент-серверным приложением с графическим интерфейсом пользователя. Оно предоставляет пользователям инструменты для криптографических операций, математических вычислений и работы с графами. Система может применяться в учебных целях, для анализа алгоритмов и решения прикладных задач.

**1.3. Определения, акронимы и сокращения**

Шифр Виженера - метод полиалфавитного шифрования текста, использующий ключевое слово для циклического сдвига букв открытого текста.

SHA-512 (Secure Hash Algorithm 512) - криптографическая хеш-функция, входящая в семейство SHA-2, которая генерирует 512-битное (64-байтное) хеш-значение.

Метод деления пополам (бисекции) — численный метод нахождения корня уравнения, основанный на последовательном сужении интервала, содержащего корень.

Граф - совокупность вершин (узлов) и рёбер (связей) между ними.

Кратчайший путь - последовательность вершин графа, соединяющая две заданные вершины, сумма весов рёбер которой минимальна.

GUI (Graphical User Interface) графический пользовательский интерфейс.

**2. Общее описание**

**2.1. Перспективы продукта**

Продукт представляет собой клиент-серверное приложение. Клиентская часть, реализованная с использованием графического интерфейса, обеспечивает удобное взаимодействие пользователя с системой. Серверная часть отвечает за обработку запросов, выполнение алгоритмов и хранение данных в базе данных.

**2.2. Функции продукта**

Ключевой функционал продукта включает:

1. Регистрация и авторизация пользователей.

2. Шифрование и расшифровка текста с использованием шифра Виженера.

3. Хеширование текста с использованием алгоритма SHA-512.

4. Решение нелинейных уравнений методом деления отрезка пополам.

5. Нахождение кратчайшего расстояния между двумя вершинами взвешенного графа.

6. Управление базой данных и просмотр статистики (для администраторов).

**2.3. Характеристики пользователей**

Система определяет три роли пользователей:

1. Гость: Неавторизованный пользователь, который может пройти регистрацию или авторизацию.

2. Пользователь: Авторизованный пользователь, имеющий доступ к основным функциям системы.

3. Администратор: Пользователь с расширенными правами, который может управлять пользователями и просматривать статистику их действий.

**2.4. Ограничения**

1. Система должна быть реализована на языке программирования C++ с использованием фреймворка Qt.

2. Для хранения данных должна использоваться СУБД SQLite.

3. Система должна быть кроссплатформенной и функционировать в операционных системах Windows, Linux и macOS.

4. Пароли пользователей должны храниться в безопасном хешированном виде.

**2.5. Предположения и зависимости**

1. Предполагается, что пользователи обладают базовыми навыками работы с компьютерными приложениями.

2. Для функционирования системы необходимы установленные библиотеки Qt и SQLite.

3. Алгоритмы работы с графами предполагают, что граф является ориентированным или неориентированным с неотрицательными весами рёбер.

**3. Требования к интерфейсам**

**3.1. Пользовательские интерфейсы**

3.1.1.Окно авторизации:

- Поля для ввода логина и пароля.

- Кнопки "Войти" и "Регистрация".

3.1.2. Окно регистрации:

- Поля для ввода логина и пароля.

- Кнопка "Зарегистрироваться".

3.1.3. Главное окно приложения:

- Вкладки или панели для доступа к функциям (Шифр Виженера, SHA-512, Метод деления пополам, Графы).

- Поля ввода для исходных данных (текст, ключ, уравнение, интервал, точность, матрица смежности графа и т.д.).

- Кнопки для выполнения операций ("Зашифровать", "Расшифровать", "Вычислить хеш", "Найти корень", "Найти путь").

- Область для отображения результатов операций.

**3.2. Аппаратные интерфейсы**

Специфических требований к аппаратным интерфейсам не предъявляется. Достаточно стандартных устройств ввода/вывода (клавиатура, мышь, монитор).

**3.3. Программные интерфейсы**

3.3.1. Взаимодействие с СУБД SQLite:

- Создание, обновление схемы базы данных.

- Выполнение операций INSERT, UPDATE, SELECT, DELETE.

3.3.2.Сетевое взаимодействие:

- Обмен данными между клиентом и сервером по протоколу TCP/IP.

**3.4. Коммуникационные интерфейсы**

Система использует стандартные сетевые протоколы (TCP/IP) для обеспечения связи между клиентской и серверной частями.

**4. Функциональные требования**

**4.1. Регистрация и авторизация**

4.1.1.Регистрация пользователя:

* Система должна предоставлять гостю возможность создать учётную запись, указав уникальный логин и пароль.
* Пароль должен храниться в базе данных только в виде хеш-суммы.

4.1.2. Авторизация пользователя:

* Система должна проверять аутентификационные данные (логин и пароль) при входе в систему.
* Доступ к функционалу предоставляется только после успешной авторизации.

**4.2. Шифрование и расшифровка текста (Шифр Виженера)**

4.2.1. Шифрование текста:

* Система должна предоставлять интерфейс для ввода открытого текста и ключевого слова.
* Система должна выполнять шифрование введённого текста по алгоритму Виженера.
* Результат (шифртекст) должен отображаться пользователю.

4.2.2. Расшифровка текста:

* Система должна предоставлять интерфейс для ввода шифртекста и ключевого слова.
* Система должна выполнять расшифровку текста по алгоритму Виженера.
* Результат (открытый текст) должен отображаться пользователю.

**4.3. Хеширование текста SHA-512**

4.3.1. Создание хеша:

* Система должна предоставлять возможность ввода текста для хеширования.
* Система должна вычислять хеш-сумму введённого текста по алгоритму SHA-512.
* Полученное хеш-значение должно отображаться пользователю.

4.3.2. Проверка хеша:

* Система должна позволять пользователю вводить исходный текст и хеш-сумму для проверки.
* Система должна вычислять хеш от введённого текста и сравнивать его с предоставленной хеш-суммой.
* Должен отображаться результат проверки (совпадение/несовпадение).

**4.4. Решение уравнений методом деления пополам**

4.4.1. Ввод данных:

* Система должна предоставлять интерфейс для ввода уравнения, интервала поиска [a, b] и требуемой точности.

4.4.2. Решение уравнения:

* Система должна реализовывать алгоритм метода бисекции для нахождения корня уравнения на заданном интервале.
* Система должна отображать найденный корень (если он существует) и количество итераций.
* Система должна обрабатывать случаи, когда на интервале нет корня или нарушены условия применимости метода.

**4.5. Поиск кратчайшего расстояния между вершинами графа**

4.5.1.Ввод графа:

* Система должна предоставлять интерфейс для ввода графа (например, через матрицу смежности или список рёбер).
* Система должна позволять пользователю указывать начальную и конечную вершины.

4.5.2. Вычисление кратчайшего пути:

* Система должна реализовывать алгоритм поиска кратчайшего пути (например, алгоритм Дейкстры) для взвешенного графа.
* Система должна отображать кратчайшее расстояние между вершинами и, если возможно, сам путь.
* Система должна обрабатывать случаи, когда путь между вершинами отсутствует.

**4.6. Администрирование**

4.6.1. Управление базой данных:

* Система должна предоставлять администратору интерфейс для выполнения базовых операций с БД (очистка таблиц, сброс данных).

4.6.2. Просмотр статистики:

* Система должна позволять администратору запрашивать и просматривать статистику по действиям пользователей (частота использования функций, активность и т.д.).
* Статистика должна отображаться в удобочитаемом виде (таблицы, списки).

**5. Нефункциональные требования**

**5.1. Требования к производительности**

* Время отклика системы на стандартные пользовательские действия (шифрование, хеширование, решение уравнения) не должно превышать 3 секунд.
* Время вычисления кратчайшего пути для графа с количеством вершин до 100 должно быть приемлемым для интерактивной работы (до 5 секунд).
* Система рассчитана на работу с ограниченным числом одновременных пользователей (до 10-20).
* Производительность зависит от вычислительной мощности клиентского устройства и скорости сетевого соединения.

**5.2. Требования к безопасности**

* Пароли пользователей должны храниться в БД в виде хеш-сумм, полученных с использованием стойкого алгоритма хеширования (например, bcrypt).
* Аутентификация должна производиться путем сравнения хешей, а не хранения паролей в открытом виде.
* На текущем этапе система не реализует защиту от сложных сетевых атак (например, MITM) и SQL-инъекций, так как предназначена для использования в контролируемой среде.

**5.3. Требования к надежности**

* Система должна гарантировать сохранность пользовательских данных и их целостность в БД при штатной работе.
* Приложение должно корректно обрабатывать ошибки ввода (неверный формат уравнения, некорректный граф) без аварийного завершения.
* Ведение детальных логов ошибок не предусмотрено, но может быть добавлено в будущих версиях.

**5.4. Требования к удобству использования**

* Интерфейс должен быть интуитивно понятным, с четким разделением функций и простой навигацией.
* Все основные операции должны быть доступны с помощью мыши и клавиатуры.

**5.5. Требования к сопровождаемости**

* Архитектура системы должна быть модульной, что позволит относительно легко вносить изменения в отдельные компоненты (например, заменять алгоритм поиска пути).
* Исходный код должен быть достаточно документирован для понимания его разработчиками.
* Обновление системы должно производиться путем замены исполняемых файлов и файлов БД (при необходимости миграции схемы).

**5.6 Требования к переносимости**

* Система должна быть полностью кроссплатформенной и функционировать под управлением ОС семейств Windows, Linux и macOS.
* База данных SQLite обеспечивает переносимость данных между разными операционными системами.

**6. Другие требования**

**6.1. Требования к документации**

* Должно быть предоставлено руководство пользователя, описывающее основные функции системы.
* Должна быть разработана базовая техническая документация по архитектуре и развертыванию.

**6.2. Требования к тестированию**

* Все функциональные требования должны быть покрыты тестами.
* Должно быть проведено тестирование производительности на целевых платформах.
* Должна быть проведена проверка на устойчивость к некорректным входным данным.

**6.3. Требования к развертыванию**

* Должна быть предоставлена инструкция по развертыванию серверной и клиентской частей в целевых окружениях.
* Процесс развертывания должен быть по возможности автоматизирован (с использованием скриптов).

**7. Приложения**

**7.1. Глоссарий**

Шифр Виженера - метод полиалфавитного шифрования текста.

SHA-512 - криптографическая хеш-функция, генерирующая 512-битный хеш.

Метод деления пополам - численный метод нахождения корня уравнения.

Граф - математическая структура, состоящая из вершин и рёбер.

Кратчайший путь - путь между двумя вершинами графа с минимальной суммой весов рёбер.

GUI - графический пользовательский интерфейс.

БД - база данных.

ПО - программное обеспечение.

СУБД - система управления базами данных.

TCP/IP - стек сетевых протоколов для передачи данных.

SQL - язык структурированных запросов для работы с базами данных.