**ЛАБОРАТОРНАЯ РАБОТА №4**

**РАЗРАБОТКА ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ НА СОЗДАНИЕ**

**АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ДЛЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ ФИНАНСОВ**

**Цель:** Ознакомление с процессом разработки технического задания на создание автоматизированной системы аутентификации и авторизации для мобильного приложения финансов.

**Тема проект:** Разработка технических требований на создание автоматизированной системы аутентификации и авторизации в мобильном приложении для поддержки здорового образа жизни.

**Технические требования:**

1. Система аутентификации и авторизации должна обеспечивать доступ к мобильному приложению "Здоровый Образ Жизни" с использованием логина и пароля.
2. Пароли пользователей должны соответствовать определенным критериям безопасности, включая длину (не менее 8 символов) и использование различных типов символов (буквы верхнего и нижнего регистра, цифры, специальные символы).
3. Пароли пользователей должны храниться в базе данных в зашифрованном виде с использованием надежных алгоритмов хеширования.
4. Запрещено хранить пароли в открытом тексте или в невоспроизводимом формате.
5. После успешной аутентификации пользователю должен быть предоставлен доступ к функционалу приложения, соответствующему его правам.
6. Авторизация должна быть выполнена перед каждым запросом на доступ к защищенным данным или операциям.
7. Система должна отслеживать активность пользователя и завершать сеанс автоматически при отсутствии активности в течение определенного времени (например, 10 минут).
8. Пользователи должны иметь возможность вручную завершить сеанс или выйти из системы.
9. Система должна предоставлять механизм сброса пароля для пользователей, забывших свой пароль.
10. После запроса на сброс пароля, пользователю должна быть отправлена инструкция для восстановления доступа к учетной записи.
11. Система должна предусматривать обработку ошибок при аутентификации и авторизации с предоставлением информативных сообщений пользователю.
12. Должны быть реализованы меры безопасности, такие как защита от атак перебора паролей, защита от подмены данных и предотвращение CSRF (межсайтовой подделки запроса).
13. Разработать UML-диаграмму, отображающую процесс аутентификации и авторизации пользователя в мобильном приложении "Здоровый Образ Жизни", включая взаимодействие между клиентской и серверной частями системы.

**СОДЕРЖАНИЕ**

**1 ОБЩИЕ СВЕДЕНИЯ**

**2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ**

**2.1 Назначение**

**2.2 Цели создания**

**3 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ**

**4 ТРЕБОВАНИЯ К СИСТЕМЕ**

**4.1 Требования к структуре**

**4.2 Требования к процедурам доступа к системе**

**4.3 Требования к функциональной безопасности**

**4.4 Требования к информационной безопасности**

**4.5 Требования к патентной чистоте**

**5 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ**

**5.1 Требования к информационному обеспечению**

**5.2 Требования к математическому обеспечению**

**5.3 Требования к программному обеспечению**

**5.4 Требования к техническому обеспечению**

**5.5 Требования к организационному обеспечению**

**6 СОСТАВ И СОДЕРЖАНИЕ РАБОТ**

**7 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ**

**8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ**

**1 ОБЩИЕ СВЕДЕНИЯ:**

Мобильное приложение "Здоровый Образ Жизни" разработано для помощи пользователю в поддержании здорового образа жизни, включая учет физической активности, питания, сна и других аспектов здоровья. Для обеспечения безопасности данных пользователей необходима надежная система аутентификации и авторизации.

Технические требования на разработку автоматизированной системы (ТТ) – документ, оформленный в установленном порядке и определяющий цели создания автоматизированной системы, детальные требования к разработке/модернизации автоматизированной системы, исходные данные, необходимые для ее разработки, а также план-график создания автоматизированной системы.

ТТ является основным документом, устанавливающим требования и порядок создания автоматизированной системы, в соответствии с которым осуществляется разработка и внедрение автоматизированной системы на объекте.

**2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ**

**2.1 Назначение:**

Разработка технических требований на создание автоматизированной системы аутентификации и авторизации для мобильного приложения "Здоровый Образ Жизни" направлена на определение функциональных и безопасностных характеристик системы, обеспечивающих защиту данных пользователей и удобство использования приложения.

**2.2 Цели создания:**

Обеспечение безопасного и надежного доступа пользователей к мобильному приложению "Здоровый Образ Жизни". Создание системы аутентификации, соответствующей современным стандартам безопасности и требованиям компании. Гарантирование удобства и простоты использования системы аутентификации и авторизации для конечных пользователей приложения.

**3 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ:**

В рамках разработки мобильного приложения "Здоровый Образ Жизни" следующие объекты системы определены: Клиентское приложение: Мобильное приложение, через которое пользователи взаимодействуют с системой, вводят данные о своем образе жизни и просматривают рекомендации. Серверная часть: Веб-сервер, обрабатывающий запросы от клиентских приложений, проводящий аутентификацию и авторизацию пользователей, а также обеспечивающий доступ к данным. База данных: Хранилище информации о пользователях, их профилях, активности, рекомендациях и других сведениях, необходимых для функционирования приложения.

**4 ТРЕБОВАНИЯ К СИСТЕМЕ:**

**4.1 Требования к структуре:**

* Разработка клиент-серверной архитектуры приложения, где клиентское приложение будет работать на мобильных устройствах, а серверная часть будет находиться на удаленном сервере.
* Использование протоколов безопасной передачи данных, таких как HTTPS, для обмена информацией между клиентом и сервером, обеспечивая шифрование данных во время передачи.
* Хранение пользовательских данных в зашифрованном виде в базе данных, используя современные алгоритмы шифрования.

**4.2 Требования к процедурам доступа к системе:**

* Реализация процедуры аутентификации с использованием логина и пароля, где пользователи вводят свои учетные данные для доступа к приложению.
* Пароли пользователей должны соответствовать определенным критериям безопасности, включая длину (не менее 8 символов) и использование различных типов символов (буквы верхнего и нижнего регистра, цифры, специальные символы).
* Для проверки формата ввода пароля в ТТ (техническом задании) для авторизации и аутентификации мобильного приложения финансов можно использовать следующее регулярное выражение: ^(?=.\*[A-Za-z])(?=.\*\d)[A-Za-z\d@$!%\*?&]{8,}$

Это регулярное выражение требует, чтобы пароль содержал как минимум одну букву и одну цифру, и имел длину не менее 8 символов. Оно также позволяет использовать специальные символы, такие как @$!%\*?&.

* Обеспечение возможности восстановления пароля через механизм сброса, например, путем отправки ссылки для сброса пароля на зарегистрированный электронный адрес.
* Проведение сессионного управления для контроля доступа пользователей к приложению, где пользовательские сеансы должны быть уникальными и автоматически завершаться после определенного периода неактивности.
* Запрещено хранить пароли в открытом тексте или в невоспроизводимом формате для обеспечения безопасности пользовательских данных.

**4.3 Требования к функциональной безопасности:**

* **Реализация защиты от атак перебора паролей и подбора сеансов, например, с помощью механизмов блокировки учетной записи после нескольких неудачных попыток входа.**
* **Установка критериев безопасности для паролей пользователей, таких как минимальная длина и использование различных типов символов.**
* **Обеспечение контроля доступа к различным функциям приложения в зависимости от роли пользователя, например, администраторы могут иметь доступ к расширенным функциям, чем обычные пользователи.**
* **Пароли пользователей должны храниться в базе данных в зашифрованном виде с использованием сильных алгоритмов хеширования для предотвращения несанкционированного доступа.**

**4.4 Требования к информационной безопасности:**

* Шифрование данных, передаваемых между клиентом и сервером, чтобы предотвратить перехват и подмену данных.
* Резервное копирование и обеспечение целостности данных в базе данных для защиты от потери информации и ее повреждения.

**4.5** **Требования к патентной чистоте:**

При разработке системы необходимо учитывать интеллектуальную собственность и патентные права других компаний, чтобы избежать нарушений патентов и авторских прав.

**5** **ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ:**

**5.1 Требования к информационному обеспечению:**

* Обеспечение надежного хранения и передачи информации между клиентским приложением и сервером.
* Разработка информационных моделей для эффективного управления данными приложения.

**5.2 Требования к математическому обеспечению:**

- Реализация алгоритмов хеширования для защиты паролей пользователей.

- Проектирование алгоритмов сессионного управления для контроля доступа.

**5.3 Требования к программному обеспечению:**

* Использование современных технологий разработки мобильных приложений, таких как Kotlin для Android или Swift для iOS.
* Реализация механизмов для управления сеансами пользователей и обработки запросов.

**5.4 Требования к техническому обеспечению:**

* Оптимизация производительности приложения для работы на различных устройствах и операционных системах.
* Обеспечение масштабируемости и отказоустойчивости серверной инфраструктуры.

**5.5 Требования к организационному обеспечению:**

- Организация процесса разработки с использованием современных методологий, таких как Agile или Scrum.

- Назначение ответственных лиц за тестирование, развертывание и поддержку приложения.

**6 СОСТАВ И СОДЕРЖАНИЕ РАБОТ:**

Анализ требований и сбор информации:

* Изучение требований к системе аутентификации и авторизации.
* Анализ функциональных и безопасностных характеристик мобильного приложения здорового образа жизни.
* Определение ключевых особенностей приложения и требований к его безопасности.

Проектирование системы аутентификации и авторизации:

* Разработка архитектуры клиент-серверного взаимодействия.
* Проектирование базы данных для хранения пользовательских данных и учетных записей.
* Выбор протоколов безопасной передачи данных и механизмов шифрования.

Разработка и тестирование функциональности:

* Создание механизма аутентификации с использованием логина и пароля.
* Реализация процесса сброса пароля через механизм сброса.
* Разработка сессионного управления для контроля доступа пользователей.
* Тестирование функциональности системы на соответствие требованиям.

Обеспечение безопасности:

* Реализация защиты от атак перебора паролей и подбора сеансов.
* Внедрение механизмов контроля доступа к функционалу приложения.
* Шифрование данных, передаваемых между клиентом и сервером.

Документирование и поддержка:

* Создание технической документации, включая описание системы, инструкции по использованию и тестированию.
* Обеспечение поддержки и дальнейшего сопровождения системы. **7 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ**
* Проведение тестирования системы на соответствие заявленным требованиям.
* Анализ результатов тестирования и исправление выявленных ошибок.
* Подготовка к внедрению и обучение пользователей работе с системой.
* Приемка системы в эксплуатацию после успешного завершения всех этапов разработки и тестирования.

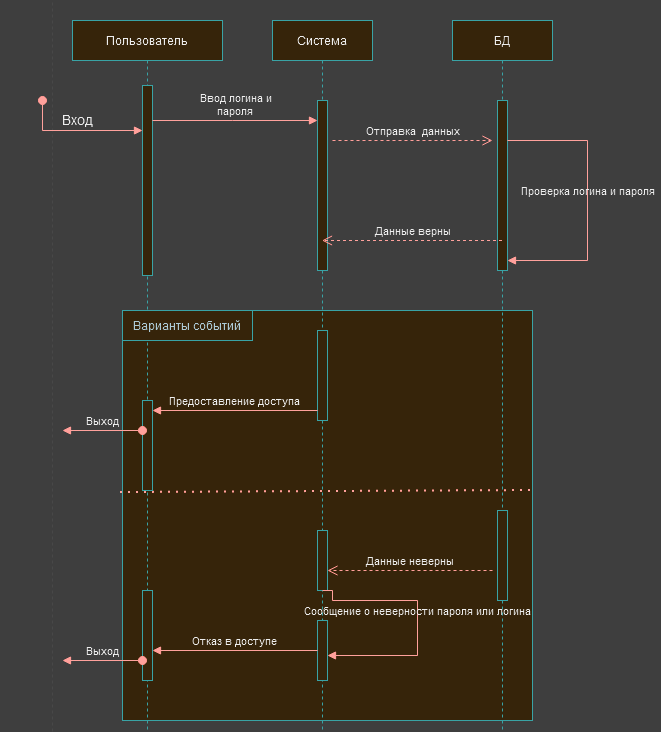
**8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ**

* Техническое задание на создание системы аутентификации и авторизации.
* Описание архитектуры приложения и базы данных.
* Инструкции для пользователей по использованию системы.
* Руководство по администрированию и сопровождению системы.
* Отчеты о результатах тестирования и аудита безопасности.
* Программа обучения пользователей и персонала по работе с системой.

**ПРИЛОЖЕНИЕ А**

**(справочное)**

**Диаграмма процесса**

****