**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 технический требований на создание

автоматизированной системы аутентификации и авторизации в соответствии с СТП 09150.11.118-2009

**Технические требования:**

- Система должна предоставлять пользователю возможность ввода логина и пароля для аутентификации.

- Логин и пароль должны быть переданы серверу для проверки подлинности.

- Пароль должен соответствовать определенным критериям безопасности, включая длину (не менее 8 символов) и наличие различных типов символов (буквы верхнего и нижнего регистра, цифры, специальные символы).

- Пароли пользователей должны храниться в базе данных в зашифрованном виде с использованием сильных алгоритмов хеширования.

- Запрещено хранить пароли в открытом тексте или в невоспроизводимом формате.

- После успешной аутентификации пользователю должен быть предоставлен доступ к функционалу приложения, соответствующему его правам.

- Авторизация должна быть выполнена перед каждым запросом на доступ к защищенным данным или операциям.

- Система должна отслеживать активность пользователя и завершать сеанс автоматически при отсутствии активности в течение определенного времени (например, 10 минут).

- Пользователи должны иметь возможность вручную завершить сеанс или выйти из системы.

- Система должна предоставлять механизм сброса пароля для пользователей, забывших свой пароль.

- После запроса на сброс пароля, пользователю должна быть отправлена инструкция для восстановления доступа к учетной записи.

- Система должна предусматривать обработку ошибок при аутентификации и авторизации с предоставлением информативных сообщений пользователю.

- Должны быть реализованы меры безопасности, такие как защита от атак перебора паролей, защита от подмены данных и предотвращение CSRF (межсайтовой подделки запроса).

- Разработать UML-диаграмму, отображающую процесс аутентификации и авторизации пользователя в мобильном приложении финансов, 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 финансов предназначено для управления финансовыми операциями пользователей, включая переводы, платежи, управление счетами и прочее. Для обеспечения безопасности и конфиденциальности 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:**

Назначением разработки технических требований на создание автоматизированной системы аутентификации и авторизации для мобильного приложения финансов является определение необходимых функциональных и безопасностных характеристик системы, обеспечивающих защиту пользовательских данных и удобство использования приложения.

**2.2 Цели создания:**

Обеспечение безопасного и надежного доступа пользователей к мобильному приложению финансов. Создание системы аутентификации, которая будет соответствовать 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 системы разработки мобильного приложения финансов необходимо определить следующие объекты: Клиентское приложение: мобильное приложение, через которое пользователи будут взаимодействовать с системой. Серверная часть: веб-сервер, обеспечивающий работу приложения, обработку запросов и взаимодействие с базой данных. База данных: хранилище информации о пользователях, их учетных данных, транзакциях и других сведениях, необходимых для функционирования приложения.

**4 ТРЕБОВАНИЯ К СИСТЕМЕ:**

**4.1 Требования к структуре:**

- Разработка клиент-серверной архитектуры приложения.

- Использование протоколов безопасной передачи данных для обмена информацией между клиентом и сервером.

- Хранение пользовательских данных в зашифрованном виде в базе данных.

- Система должна предоставлять пользователю возможность ввода логина и пароля для аутентификации.

- Логин и пароль должны быть переданы серверу для проверки подлинности.

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

- Реализация процедуры аутентификации с использованием логина и пароля.

- Обеспечение возможности восстановления пароля через механизм сброса.

- Проведение сессионного управления для контроля доступа пользователей к приложению.

- Запрещено хранить пароли в открытом тексте или в невоспроизводимом формате.

- После успешной аутентификации пользователю должен быть предоставлен доступ к функционалу приложения, соответствующему его правам.

- Авторизация должна быть выполнена перед каждым запросом на доступ к защищенным данным или операциям.

- Система должна отслеживать активность пользователя и завершать сеанс автоматически при отсутствии активности в течение определенного времени (например, 10 минут).

- Пользователи должны иметь возможность вручную завершить сеанс или выйти из системы.

-Для проверки формата ввода пароля 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 @$!%\*?&.

**4.3 Требования к функциональной безопасности:**

- Защита от атак перебора паролей и подбора сеансов.

- Пароль должен соответствовать определенным критериям безопасности, включая длину (не менее 8 символов) и наличие различных типов символов (буквы верхнего и нижнего регистра, цифры, специальные символы).

- Обеспечение контроля доступа к различным функциональным возможностям приложения в зависимости от роли пользователя.

- Пароли пользователей должны храниться в базе данных в зашифрованном виде с использованием сильных алгоритмов хеширования.

- Система должна предоставлять механизм сброса пароля для пользователей, забывших свой пароль.

- После запроса на сброс пароля, пользователю должна быть отправлена инструкция для восстановления доступа к учетной записи.

- Система должна предусматривать обработку ошибок при аутентификации и авторизации с предоставлением информативных сообщений пользователю.

- Должны быть реализованы меры безопасности, такие как защита от атак перебора паролей, защита от подмены данных и предотвращение CSRF (межсайтовой подделки запроса).

**4.4 Требования к информационной безопасности:**

- Шифрование данных, передаваемых между клиентом и сервером.

- Резервное копирование и обеспечение целостности данных в базе данных.

- Разработать UML-диаграмму, отображающую процесс аутентификации и авторизации пользователя в мобильном приложении финансов, включая взаимодействие между клиентской и серверной частями системы

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

- Использование только технологий и решений, не нарушающих интеллектуальную собственность и патентные права других компаний.

**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:**

Разработка автоматизированной системы аутентификации и авторизации для мобильного приложения финансов включает следующие этапы и задачи:

**Анализ требований и сбор информации:**

- Проведение анализа требований заказчика к системе аутентификации и авторизации.

- Сбор информации о функциональности и безопасности мобильного приложения финансов.

**Проектирование системы:**

- Разработка архитектуры системы аутентификации и авторизации.

- Проектирование интерфейсов пользовательского взаимодействия.

- Создание схемы базы данных для хранения пользовательских данных и сессий.

**Разработка и тестирование:**

- Написание кода клиентской и серверной частей системы.

- Реализация алгоритмов аутентификации и авторизации.

- Проведение тестирования разработанных модулей на соответствие требованиям.

**Интеграция и оптимизация:**

- Интеграция системы аутентификации и авторизации с мобильным приложением финансов.

- Оптимизация производительности и безопасности системы.

**Документация и поддержка:**

- Подготовка технической документации по системе аутентификации и авторизации.

- Предоставление инструкций по развертыванию и использованию системы.

- Поддержка и обновление системы в дальнейшем.

**7 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ**

Порядок приемки в эксплуатацию разработанной системы автоматизированной аутентификации и авторизации для мобильного приложения финансов начинается с тщательного тестирования всех ее компонентов и функций. После завершения тестирования составляется подробная документация, включающая техническую документацию и инструкции по использованию системы. Затем производится оценка соответствия системы требованиям и оценка ее качества. После успешного завершения всех проверок система предоставляется заказчику для процедуры приемки. На этом этапе проводится демонстрация функциональности системы и обсуждение ее работы. После утверждения заказчиком системы и получения обратной связи производится ее развертывание на рабочих серверах и мобильных устройствах, а также настройка доступа пользователей. После успешного внедрения системы в эксплуатацию она подвергается мониторингу и технической поддержке, при необходимости вносятся изменения и обновления для обеспечения бесперебойной работы.

**8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ**

Требования к документированию для системы автоматизированной аутентификации и авторизации мобильного приложения финансов включают:

**Техническая документация:** Подробное описание архитектуры системы, ее компонентов и интерфейсов. Включает в себя описание алгоритмов аутентификации и авторизации, схему базы данных, используемые технологии и интеграционные точки.

**Инструкции по использованию:** Подробное руководство для администраторов и конечных пользователей, объясняющее процесс установки, настройки и использования системы аутентификации и авторизации.

**Документация по безопасности:** Описание мер безопасности, реализованных в системе, и инструкции по их использованию. Включает в себя политики паролей, механизмы защиты данных и процедуры обработки инцидентов.

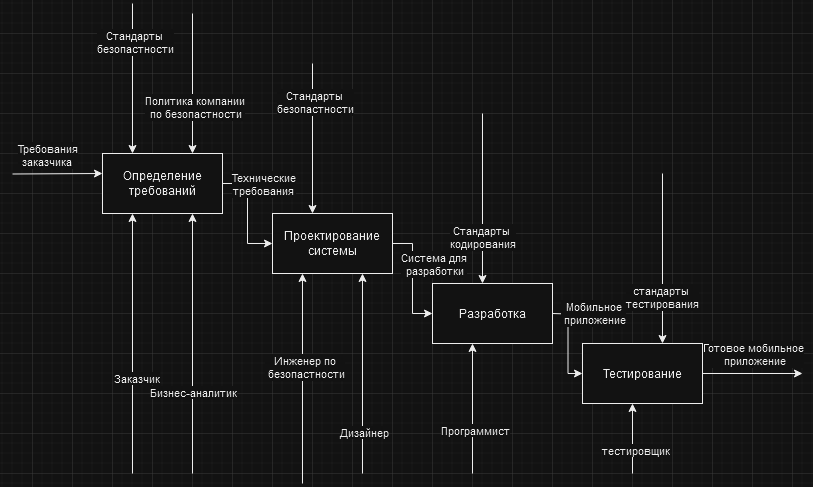
**Руководство по администрированию:** Инструкции для администраторов системы по управлению пользователями, ролями, доступом и другими аспектами администрирования.

**Тестовая документация:** Описание проведенных тестов, их результаты и выявленные ошибки. Включает в себя тест-кейсы, скриншоты и отчеты о выполненных тестах.

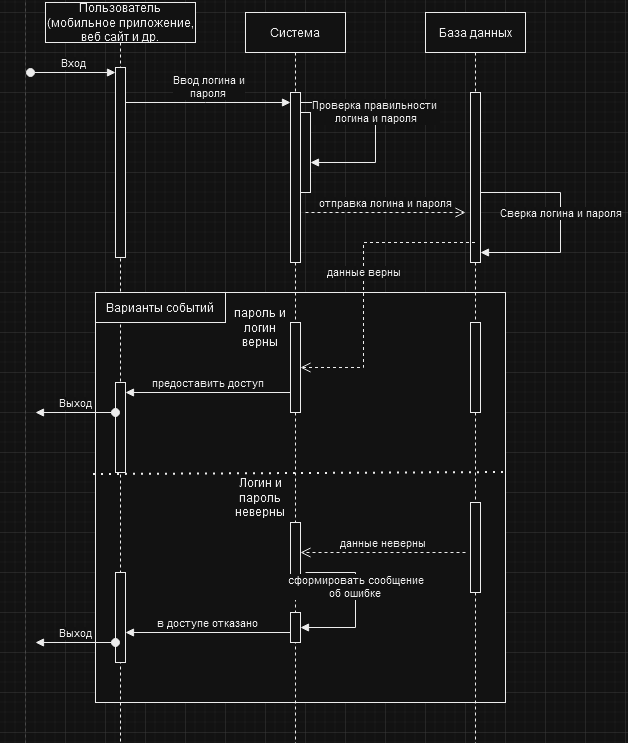
**Документация по обновлениям и изменениям:** Описание всех изменений и обновлений, внесенных в систему после ее внедрения. Включает в себя список исправлений, новые функции и инструкции по их использованию.

**ПРИЛОЖЕНИЕ А**

**(справочное)**

****

**Рисунок 1 – диаграмма процесса**

****

**Рисунок 2 Диаграмма последовательности**