ЛАБОРАТОРНАЯ РАБОТА №4

РАЗРАБОТКА ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ НА СОЗДАНИЕ

АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ

**Цель:** ознакомление с процессом разработки технического задания на создание автоматизированной системы (программного продукта).

**Тема проект:** разработка технический требований на создание Автоматизированной системы аутентификации и авторизации в банке

**1 ОБЩИЕ СВЕДЕНИЯ**

1.1 Наименование работы: разработка технических требований на автоматизированную систему аутентификации и авторизации банка

1.2 Заказчик АС и Ответственный по проекту: заказчик АБС – Сбербанк

1.3 Наименование Организации-пользователя АС: Сбербанк

1.4 Наименование объекта внедрения: Управление банковскими переводами

**3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ**

**3.1 Назначение**

**Аутентификация** — это процесс, когда пользователь вводит ключ, например пароль или пин-код, подтверждая своё право на доступ к той или иной учётной записи и хранящейся в ней информации. Аутентификация бывает одно-, двух- и трёхфакторной.

**Авторизация** — это процесс присвоения учётной записи положенных ей привилегий. Если авторизация прошла успешно, человек попадает в личный кабинет. Он может читать уведомления, видеть список доступных курсов, просматривать их и учиться. Права доступа к этим действиям называются привилегиями.

**3.2 Цели создания**

* Повышение защиты данных
* Разграничение ролей для пользователей, администрации и т.д.
* При обязательной регистрации устраняется большое количество ботов, распространяющих спам и, соответственно, снижается угроза хакерских атак;

**4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ**

* Пользователи: система авторизации должна поддерживать различные типы пользователей и их роли (администратор, пользователь, гость и т. д.), а также обеспечивать управление доступом к различным функциям и данным.
* Учетные записи: каждому пользователю должна быть назначена уникальная учетная запись, которая содержит информацию о его логине, пароле и других идентификационных данных.
* Механизм аутентификации: система должна обеспечивать безопасный и надежный способ проверки подлинности пользователей, например, с помощью пароля, биометрических данных или двухфакторной аутентификации.
* Сессии: для каждой успешно аутентифицированной учетной записи должна создаваться сессия, чтобы отслеживать действия пользователя в системе и автоматически завершать его, если он остается неактивным в течение определенного времени.
* Журналирование: система должна вести логи всех действий пользователей, связанных с процессом аутентификации, чтобы обеспечить отслеживаемость и аудит доступа к системе.
* Защита от атак: система должна иметь механизмы защиты от различных видов атак, таких как подбор пароля, SQL инъекции, CSRF и других уязвимостей.
* Интеграция с другими системами: система авторизации должна быть легко интегрируема с другими приложениями и сервисами для обеспечения единообразного управления доступом к различным ресурсам.

**5 ТРЕБОВАНИЯ К СИСТЕМЕ**

**5.1 Требования к структуре**

Структура приложения: клиент-сервер(Приложение А)

**5.2 Требования к процедурам доступа к системе**

**Аутентификация по паролю**

* При регистрации и при последующей авторизации маскируйте введенный пароль. Это позволит скрыть пароль от злоумышленников, но все же он не удобен для пользовательского ввода.
* Логин и пароль — на одной странице
* При использовании двухфакторной или двухэтапной аутентификации форма для ввода сгенерированного пароля или QR-код должны появляться после ввода логина, пароля и нажатия кнопки «Вход».
* На форме аутентификации необходимо обеспечить переход на форму восстановлени
* Важно обеспечить проверку заполнения логина и пароля и не допустить отправку запроса с незаполненным полем я доступа.

**5.3 Требования к функциональной безопасности**

* Регулярное выражение

^(?=.\*[a-z])(?=.\*[A-Z])(?=.\*\d)(?=.\*[@$!%\*?&])[A-Za-z\d@$!%\*?&]{8,}$

* процесс аутентификации и авторизации должен осуществляться через
* запрос данных учетной записи (логин и пароль) пользователя.
* пароль пользователя должен быть не менее 8 символов и обязательно содержать цифры и символы разного регистра.
* Проверка пароля на соответствие требованиям должно осуществляться на стороне клиента;
* хранение пароля пользователя в системе должно осуществляться в зашифрованном виде;
* при отсутствии активности пользователя в системе более 10 минут уничтожается сессия;
* предусмотреть подсистему сброса и восстановления данных учетной записи пользователя;

**5.4 Требования к информационной безопасности**

* Ограничение на количество попыток ввода пароля
* В базе данных необходимо хранить хэш пароля. Избежать подбора пароля с помощью радужных таблиц поможет динамически генерируемая соль.
* Разграничение доступа
* Передача пароля методом POST

**5.5 Требования к патентной чистоте**

Чисто

**6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ**

**6.1 Требования к информационному обеспечению**

* Некоторые из основных требований к информационному обеспечению включают:
* Надежность: информация должна быть точной, достоверной и актуальной, чтобы избежать ошибочных решений.
* Конфиденциальность: информация должна быть защищена от несанкционированного доступа, чтобы предотвратить утечку конфиденциальных данных.
* Доступность: информация должна быть доступна в нужное время и в нужном месте для того, чтобы пользователи могли быстро получить к ней доступ.
* Понятность: информация должна быть представлена в понятной форме, чтобы пользователи могли легко интерпретировать ее и принимать обоснованные решения.
* Расширяемость: информационное обеспечение должно быть гибким и способным масштабироваться в соответствии с изменяющимися потребностями бизнеса.
* Интегрируемость: информационные системы должны быть способны взаимодействовать между собой и с другими внешними системами для обеспечения эффективного обмена данными.
* Совместимость: информационное обеспечение должно быть совместимо с существующими бизнес-процессами и технологиями для минимизации затрат на внедрение и обучение персонала.

**6.2 Требования к математическому обеспечению**

Нет

**6.3 Требования к программному обеспечению**

Функциональные требования: программное обеспечение должно выполнять определенные функции, которые были описаны в спецификации требований. Например, веб-браузер должен позволять пользователю открывать веб-страницы, отправлять формы и т.д.

* Надежность и безопасность: программное обеспечение должно обеспечивать защиту данных пользователей и быть надежным в работе. Это может включать в себя защиту от хакерских атак, обеспечение резервного копирования данных и предотвращение сбоев в работе.
* Производительность: программное обеспечение должно обладать оптимальной производительностью, чтобы обеспечить быструю обработку данных и минимальное время отклика на действия пользователя.
* Удобство использования: программа должна быть легко понятной для пользователя и иметь удобный интерфейс, который позволит пользователю легко осуществлять необходимые действия.
* Совместимость: программное обеспечение должно работать на различных устройствах и операционных системах, чтобы обеспечить максимальную доступность для пользователей.
* Масштабируемость: программа должна быть готова к масштабированию и обеспечивать возможность добавления новой функциональности и расширения возможностей без значительных изменений в коде.
* Легкость обновления: программное обеспечение должно быть легко обновляться и иметь механизмы автоматического обновления для обеспечения безопасности и исправления ошибок.

**6.9 Требования к техническому обеспечению**

Наличие необходимого оборудования и программного обеспечения для выполнения поставленных задач.

* Соответствие технических характеристик компьютеров, серверов, сетевого оборудования и других устройств с требованиями системы.
* Надежность и стабильность работы оборудования и программного обеспечения.
* Обеспечение безопасности данных и защита от внешних угроз.
* Поддержка и обновление технического оборудования и программного обеспечения.
* Соблюдение всех законодательных норм и правил в области информационной безопасности.

**6.5 Требования к организационному обеспечению**

Наличие четкой иерархической структуры организации, определение ролей и обязанностей сотрудников.

* Разработка и внедрение эффективных систем коммуникации и обратной связи между сотрудниками.
* Обеспечение достаточного количества квалифицированных сотрудников для выполнения поставленных задач.
* Создание и поддержание благоприятной рабочей атмосферы, способствующей мотивации и профессиональному развитию сотрудников.
* Разработка и внедрение эффективных процессов управления ресурсами организации, включая финансовые, материальные и информационные ресурсы.
* Проведение регулярного мониторинга и анализа работы организации с целью выявления проблем и разработки мероприятий по их устранению.
* Соблюдение законодательства и нормативных требований, касающихся организационного обеспечения.

**7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ**

Перечень стадий и этапов работ по созданию системы в соответствии с ГОСТ 24.601

**8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ**

* Тестирование программного продукта: перед передачей программного продукта на эксплуатацию необходимо провести тестирование для выявления возможных ошибок и недочетов. Обычно проводятся функциональное тестирование, интеграционное тестирование, нагрузочное тестирование и др.
* Составление документации: необходимо подготовить все необходимые документы, включая руководство пользователя, инструкции по установке и настройке, техническую документацию и т.д.
* Подготовка обучения пользователей: перед внедрением программного продукта необходимо обучить пользователей его использованию. Обычно проводятся обучающие семинары, тренинги либо составляется обучающий материал.
* Внедрение программного продукта: после завершения всех предыдущих этапов происходит непосредственное внедрение программного продукта на рабочие места пользователей.
* Мониторинг и поддержка: после внедрения необходимо проводить мониторинг работы программного продукта, решать возникающие проблемы и обеспечивать его поддержку.
* Оценка результатов: по прошествии определенного периода времени необходимо провести оценку результатов внедрения программного продукта, выявить его эффективность и принять решение о необходимости доработки или изменения.

**ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ**

Согласованный Разработчиком и Заказчиком перечень подлежащих разработке комплектов и видов документов, соответствующих требованиям ГОСТ 34.201-89 и НТД отрасли Заказчика;

Требования по документированию комплектующих элементов межотраслевого применения в соответствии с требованиями ЕСКД и ЕСПД;

Приложение А

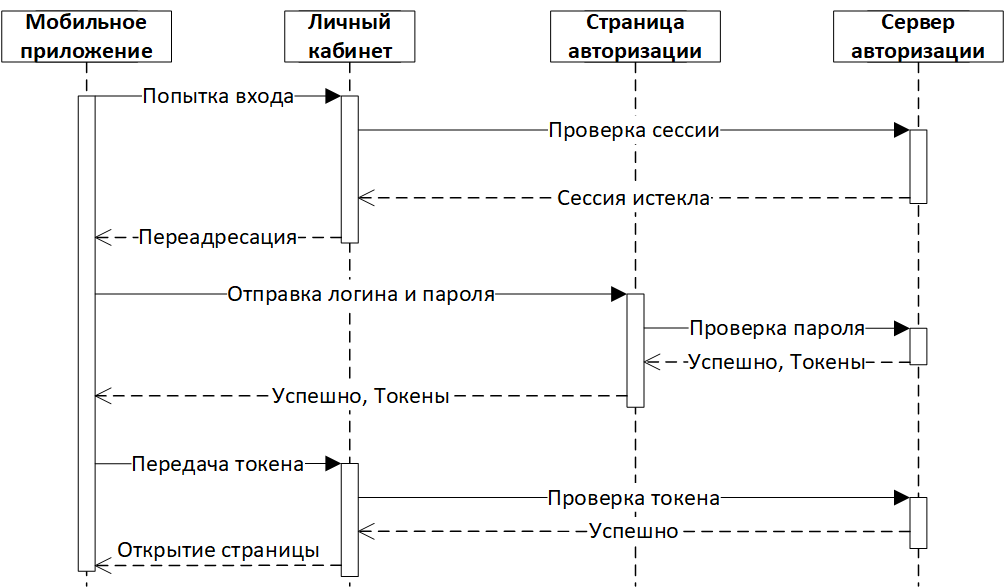


Рисунок 1- UML диаграмма последовательности

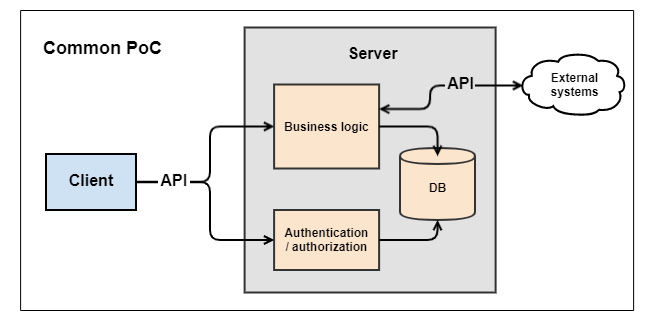


Рисунок 2 – Структура приложения