**ЛАБОРАТОРНАЯ РАБОТА №4**

РАЗРАБОТКА ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ НА СОЗДАНИЕ

АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ДЛЯ ВЕБ-ПРИЛОЖЕНИЯ

**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 для веб-приложения

**Технические требования:**

- 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;

- предусмотреть UML-диаграмму процесса аутентификации и авторизации

пользователя в системе.

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ**

**К РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ДЛЯ ВЕБ-ПРИЛОЖЕНИЯ**

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 4](#_Toc162100439)

[2. ОБЩИЕ СВЕДЕНИЯ 4](#_Toc162100440)

[3. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ 4](#_Toc162100441)

[3.1 Назначение 4](#_Toc162100442)

[3.2 Цели создания 4](#_Toc162100443)

[4. ХАРАКТЕРИСТИКА ОБЬЕКТОВ СИСТЕМЫ РАЗРАБОТКИ 5](#_Toc162100444)

[5 ТРЕБОВАНИЯ К СИСТЕМЕ 5](#_Toc162100445)

[5.1 Требования к структуре 5](#_Toc162100446)

[5.2 Требования к процедурам доступа к системе 6](#_Toc162100447)

[5.3 Требования к функциональной безопасности 6](#_Toc162100448)

[5.4 Требования к информационной безопасности 7](#_Toc162100449)

[5.5 Требования к патентной чистоте 7](#_Toc162100450)

[6. Требования к видам обеспечения 7](#_Toc162100451)

[6.1 Требования к информационному обеспечению 7](#_Toc162100452)

[6.2 Требования к программному обеспечению 7](#_Toc162100453)

[6.3 Требования к техническому обеспечению 7](#_Toc162100454)

[6.4 Требования к организационному обеспечению 8](#_Toc162100455)

[7. Состав и содержание работ 8](#_Toc162100456)

[8. Порядок приемки в эксплуатацию 9](#_Toc162100457)

[9. Требования к документированию 9](#_Toc162100458)

[Приложение А 10](#_Toc162100459)

## ВВЕДЕНИЕ

Эта система автоматизированной аутентификации и авторизации предназначена для обеспечения безопасного доступа пользователей к веб-приложению. Она является важной частью защиты информации и контроля доступа к ресурсам приложения.

## 2. ОБЩИЕ СВЕДЕНИЯ

Автоматизированная система аутентификации и авторизации представляет собой центральный элемент безопасности веб-приложения, обеспечивая контроль доступа к ресурсам и защиту информации от несанкционированного доступа. Система предоставляет следующие основные функции:

Аутентификация: Проверка подлинности пользователей по их учетным данным (логин и пароль).

Авторизация: Управление правами доступа пользователей к различным функциям и данным приложения.

Управление сеансами: Отслеживание активных сеансов пользователей и управление их состоянием.

Журналирование и мониторинг: Запись действий пользователей и мониторинг системы для обнаружения и реагирования на подозрительную активность.

Восстановление пароля: Предоставление возможности пользователям восстановить доступ к своей учетной записи в случае утери пароля.

## 3. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ

### 3.1 Назначение

Назначение системы автоматизированной аутентификации и авторизации заключается в обеспечении безопасного и удобного доступа пользователей к функционалу веб-приложения. Это важный компонент, который гарантирует контроль доступа к ресурсам приложения и защиту конфиденциальной информации от несанкционированного доступа.

### 3.2 Цели создания

Основной целью является обеспечение высокого уровня безопасности веб-приложения путем надежной аутентификации и авторизации пользователей.

Система должна защищать конфиденциальные данные пользователей, такие как личная информация и учетные данные, от утечек или несанкционированного доступа.

Обеспечение удобства для пользователей при входе в приложение. Процесс аутентификации и авторизации должен быть интуитивно понятным и эффективным.

Система должна соответствовать современным стандартам безопасности и рекомендациям по защите данных, таким как GDPR (Общий регламент по защите данных) или PCI DSS (Стандарт безопасности данных индустрии платежных карт).

Гарантировать совместимость с другими компонентами приложения: Система должна быть легко интегрируема с другими компонентами приложения, такими как управление сеансами и база данных, для обеспечения целостности и функциональности приложения в целом.

## 4. ХАРАКТЕРИСТИКА ОБЬЕКТОВ СИСТЕМЫ РАЗРАБОТКИ

Серверная часть

База данных пользователей: представляет собой хранилище информации о пользователях, включая их учетные данные (логины, хэши паролей), роли и права доступа. Для обеспечения безопасности важно хранить учетные данные в зашифрованном виде и регулярно проводить аудит базы данных.

Алгоритмы аутентификации и авторизации: объекты реализуют логику аутентификации и авторизации пользователей. Включают в себя проверку учетных данных, сопоставление с данными в базе данных, управление сеансами пользователей и управление правами доступа.

Клиентская часть

Интерфейс аутентификации и авторизации: пользовательский интерфейс, через который пользователи вводят свои учетные данные для аутентификации. Включает в себя формы ввода логина и пароля, а также элементы управления для восстановления пароля или регистрации нового пользователя.

Средства разработки и тестирования

Языки программирования и фреймворки: Для разработки серверной части могут использоваться языки программирования, такие как Python, Java или JavaScript, а также фреймворки, такие как Django, Spring или Express.

## 5 ТРЕБОВАНИЯ К СИСТЕМЕ

## 5.1 Требования к структуре

Серверная часть клиент-серверного приложения включает следующие основные элементы:

Web-сервер: Этот компонент отвечает за обработку запросов от клиентов и возврат соответствующих ответов. Он обеспечивает связь между клиентами и серверной логикой приложения.

Бизнес-логика: Это ядро приложения, которое реализует функциональные возможности системы. Она включает в себя алгоритмы аутентификации, авторизации, управление пользователями и другие бизнес-процессы.

База данных: Серверная часть взаимодействует с базой данных для хранения пользовательских данных, таких как учетные записи, роли, сеансы и журналы событий.

Клиентская часть

Клиентская часть клиент-серверного приложения включает следующие элементы:

Пользовательский интерфейс: Это компонент, который взаимодействует с пользователем и предоставляет ему возможность взаимодействия с приложением. Он включает в себя формы для ввода учетных данных, кнопки для отправки запросов и другие элементы управления.

Механизмы безопасности на стороне клиента: Клиентская часть содержит механизмы безопасности, такие как защита от XSS и CSRF атак, которые обеспечивают безопасность при взаимодействии с пользовательскими данными.

Взаимодействие между клиентом и сервером

Для обеспечения функциональности системы клиент и сервер взаимодействуют между собой посредством HTTPS протокола. Клиент отправляет запросы на сервер, содержащие необходимые данные для аутентификации или авторизации, а сервер обрабатывает эти запросы, выполняет необходимые операции и отправляет обратно соответствующие ответы.

### 5.2 Требования к процедурам доступа к системе

В системе должны быть определены различные роли пользователей с соответствующими правами доступа:

Администратор: Пользователь с полными правами доступа к системе, включая управление пользователями, ролями и настройками безопасности.

Пользователь: Основной тип пользователей, который имеет доступ к основному функционалу приложения, но ограничен в правах администрирования.

Гость: Пользователь, который имеет ограниченный доступ к системе, обычно только для просмотра информации без возможности внесения изменений.

Для усиления безопасности входа в систему может быть включена двухфакторная проверка. Этот метод требует предоставления двух видов подтверждения личности пользователя:

Что знает пользователь: Пароль.

Что пользователь имеет: Временный код, отправленный на заранее зарегистрированное устройство пользователя (мобильный телефон) или использование приложения аутентификации Google Authenticator или Authy.

### 5.3 Требования к функциональной безопасности

Длина пароля: Пароль должен состоять как минимум из 8 символов.

Комплексность пароля: Пароль должен содержать символы как верхнего, так и нижнего регистра, а также цифры и специальные символы.

Шифрование пароля: Пароль должен храниться в зашифрованном виде в базе данных

Хэширование пароля: Пароль должен быть хэширован перед сохранением в базе данных с использованием криптографической функции хэширования, такой как SHA-256.

Ограничение попыток ввода пароля: Система должна ограничивать количество попыток ввода пароля, до трех неудачных попыток, после чего аккаунт пользователя блокируется на некоторое время или требуется сброс пароля для восстановления доступа.

**Регулярное выражение для проверки формата пароля**

^(?=.\*[a-z])(?=.\*[A-Z])(?=.\*\d)(?=.\*[@$!%\*?&])[A-Za-z\d@$!%\*?&]{8,20}$

**Разъяснение регулярного выражения:**

* **^** - начало строки.
* **(?=.\*[a-z])** - должна содержать по меньшей мере одну строчную букву.
* **(?=.\*[A-Z])** - должна содержать по меньшей мере одну заглавную букву.
* **(?=.\*\d)** - должна содержать по меньшей мере одну цифру.
* **(?=.\*[@$!%\*?&])** - должна содержать по меньшей мере один из специальных символов.
* **[A-Za-z\d@$!%\*?&]{8,20}** - любые символы, включая строчные и заглавные буквы, цифры и специальные символы, от 8 до 20 раз.
* **$** - конец строки.

### 5.4 Требования к информационной безопасности

Шифрование пользовательских данных в базе данных с использованием современных криптографических алгоритмов.

Резервное копирование базы данных и ее защита от несанкционированного доступа.

Использование безопасного протокола передачи данных: Все коммуникации между клиентом и сервером должны осуществляться через защищенный протокол HTTPS, чтобы обеспечить конфиденциальность передаваемых данных.

Закрытие сеанса после неактивности: Система должна автоматически завершать сеанс работы пользователя после определенного периода неактивности для предотвращения возможных атак похищения сеанса (Session Hijacking).

### 5.5 Требования к патентной чистоте

Использование только лицензионного программного обеспечения и соблюдение авторских прав.

Осуществление работы согласно законодательству Республики Беларусь и внутреннему регламенту компании.

## 6. Требования к видам обеспечения

### 6.1 Требования к информационному обеспечению

Предоставление подробной документации по настройке и использованию системы для администраторов и конечных пользователей.

### 6.2 Требования к программному обеспечению

Использование проверенных библиотек и фреймворков для разработки серверной и клиентской частей системы.

### 6.3 Требования к техническому обеспечению

Система должна быть способна эффективно функционировать на компьютере со следующими характеристиками:

Процессор: Для процессора с тактовой частотой не менее 2 ГГц для обеспечения достаточной производительности при обработке запросов от пользователей.

Оперативная память: Наличие 4 ГБ оперативной памяти.

Система должна быть совместима с следующими операционными системами:

Windows: Поддержка Windows 10 или более новой версии.

Система должна быть совместима с необходимым программным обеспечением, включая:

Web-сервер: Поддержка серверного ПО, такого как Apache, Nginx или Microsoft IIS для развертывания приложения.

База данных: Поддержка установленной базы данных, такой как MySQL, PostgreSQL или MongoDB для хранения данных приложения.

### 6.4 Требования к организационному обеспечению

Роли и права доступа: Система должна иметь механизм управления ролями и правами доступа, позволяющий администраторам назначать роли пользователям и определять, к каким разделам и функциям приложения они имеют доступ.

Администрирование пользователей: Пользователи должны иметь возможность управлять своими учетными записями, в том числе изменять пароли, восстанавливать утерянные пароли и регистрировать новые учетные записи.

Защита данных: Система должна обеспечивать защиту конфиденциальных данных пользователей, включая механизмы шифрования данных при передаче по сети и хранении в базе данных.

Резервное копирование: Регулярное создание резервных копий данных приложения для предотвращения потери информации в случае сбоев или аварий.

Журналирование событий: Система должна вести журнал событий для отслеживания активности пользователей, а также для обнаружения и анализа возможных инцидентов безопасности.

Мониторинг производительности: Проведение мониторинга производительности приложения для выявления узких мест и оптимизации работы системы.

Техническая поддержка: Обеспечение технической поддержки пользователям, включая решение проблем и ответы на вопросы, связанные с работой приложения.

Обновления и патчи: Регулярное выпуск обновлений и патчей для приложения с целью исправления ошибок, улучшения безопасности и добавления нового функционала.

## 7. Состав и содержание работ

* Анализ требований и проектирование системы.
* Разработка серверной и клиентской частей системы.
* Тестирование безопасности и производительности.
* Внедрение и настройка системы на стороне клиента.
* Обучение персонала.

### 8. Порядок приемки в эксплуатацию

* Проведение тестирования системы на соответствие требованиям.
* Аудит безопасности.
* Обучение персонала.
* Подписание акта приемки системы в эксплуатацию.

## 9. Требования к документированию

* Разработка технической документации по системе.
* Создание пользовательской инструкции по использованию системы.
* Составление отчетов о тестировании безопасности и производительности.

## Приложение А

Диаграмма последовательности процесса работы системы аутентификации и авторизации

