Управление Белорусской железной дороги

(наименование объекта автоматизации)

3

(класс автоматизированной системы)

**ТЕХНИЧЕСКИЙ ТРЕБОВАНИЙ НА СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ В СООТВЕТСТВИИ С СТП 09150.11.118-2009**

На 7 листах

Оглавление

[1 ОБЩИЕ СВЕДЕНИЯ 3](#_Toc193812245)

[2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ 3](#_Toc193812246)

[3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ 3](#_Toc193812247)

[3.1. Перечень и краткая характеристика бизнес-процессов 3](#_Toc193812248)

[3.2. Требования к входным и выходным данным, формам их представления 4](#_Toc193812249)

[3.3. Выполняемые технологические операции 4](#_Toc193812250)

[4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС 4](#_Toc193812251)

[4.1 Формулировка цели разработки 4](#_Toc193812252)

[4.2. Область и условия применения АС 4](#_Toc193812253)

[4.3. Ограничения применения АС 5](#_Toc193812254)

[5. ФУНКЦИИ И ЗАДАЧИ, СОЗДАВАЕМОЙ АС 5](#_Toc193812255)

[5.1. Требования к АС в целом 5](#_Toc193812256)

[5.2. Требования к функциям, выполняемым подсистемами 6](#_Toc193812257)

[6 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА 6](#_Toc193812258)

[Приложение А 7](#_Toc193812259)

# 1 ОБЩИЕ СВЕДЕНИЯ

1.1 Наименование работы: разработка технический требований на создание автоматизированной системы аутентификации и авторизации в соответствии с СТП 09150.11.118-2009.

1.2 Заказчик АС и Ответственный по проекту: заказчик АС – Государственное объединение «Белорусская железная дорога; Ответственный по проекту – служба технической политики и инвестиций Государственного объединения «Белорусская железная дорога».

1.3 Наименование Организации-пользователя АС: Государственное объединение Белорусская железная дорога.

1.4 Наименование объекта внедрения: Системы аутентификации и авторизации.

# 2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

**2.1 В настоящих технических требованиях применены термины и определения в следующем значении:**

**2.1.1 Аутентификация** – процесс проверки подлинности пользователя на основании предоставленных учетных данных.  
 2.1.2 **Авторизация** – процесс предоставления пользователю прав доступа к ресурсам системы после успешной аутентификации.  
 2.1.3 **Сессия** – период времени, в течение которого пользователь может взаимодействовать с системой после успешной аутентификации.  
 2.1.4 **Пароль** – секретная строка, используемая для подтверждения личности пользователя.

# 3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ

## **3.1. Перечень и краткая характеристика бизнес-процессов**

3.1.1 Регистрацияпользователей**:** Процесс создания учетной записи, включающий ввод логина, пароля и других необходимых данных.

3.1.2 Аутентификацияпользователей**:** Проверка введенных учетных данных на соответствие данным в базе данных.

3.1.3 Авторизацияпользователей**:** Определение прав доступа пользователя к различным ресурсам системы на основе его роли.

3.1.4 Сброспароля**:** Процесс восстановления доступа к учетной записи в случае потери пароля, включающий отправку ссылки на восстановление на электронную почту.

## 3.2. Требования к входным и выходным данным, формам их представления

3.2.1 Входными данными являются: логин, пароль и дополнительные данные при регистрации: имя, фамилия, адрес электронной почты.

Логин должен содержать не менее 8 символов. И не должен содержать пробелов и специальных символов, кроме разрешенных.

Пароль должен содержать не менее 8 символов, и включать как минимум одну заглавную букву, одну строчную букву, одну цифру и один специальный символ.

Имя и фамилия должны содержать не менее 1 символа, а адрес электронной почты должен соответствовать формату электронной почты.

3.2.2 Выходными данными являются: статус аутентификации, токен доступа в случае успешной аутентификации, сообщения об ошибках.

Статус аутентификации должен выдавать значения "успех" или "неудача".

Токен доступа должен быть временным и иметь срок действия.

Сообщения об ошибках должно выводить при ошибке сообщение "Неверный логин или пароль".

## 3.3. Выполняемые технологические операции

Автоматизации подлежат технологические операции:

• Проверка соответствия пароля требованиям безопасности.

• Шифрование паролей перед хранением в базе данных с использованием современных алгоритмов.

• Управление сессиями пользователей, включая создание, обновление и завершение сессий.

# 4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС

## 4.1 Формулировка цели разработки

Создание безопасной и удобной системы аутентификации и авторизации, которая обеспечивает защиту данных пользователей и предотвращает несанкционированный доступ.

## 4.2. Область и условия применения АС

Система будет применяться на железной дороге для приложений, требующих надежной защиты данных пользователей.

## 4.3. Ограничения применения АС

Система не должна использоваться для обработки конфиденциальной информации без надлежащих мер безопасности.

# 5. ФУНКЦИИ И ЗАДАЧИ, СОЗДАВАЕМОЙ АС

## 5.1. Требования к АС в целом

5.1.1. Требования к структуре и функционированию АС. Система должна быть построена по принципу клиент-сервер с использованием API для взаимодействия между клиентом и сервером, и поддерживать различные платформы.

5.1.2. Требования к защите информации от несанкционированного доступа. Пароли пользователей должны храниться в зашифрованном виде. И доступ к данным должен быть ограничен правами пользователей на основе ролей.

5.1.3. Требования по сохранности информации при авариях. Необходимо реализовать резервное копирование данных с возможностью восстановления. Так же проводить регулярное тестирование восстановления данных из резервных копий.

5.1.4. Требования к информационному обеспечению. Должны использоваться защищенные протоколы передачи данных.

5.1.5. Требования к математическому обеспечению. Применение современных алгоритмов шифрования для хранения паролей и токенов доступа с ограниченным временем действия для повышения безопасности.

5.1.6. Требования к программному обеспечению. Совместимость с основными операционными системами и браузерами.

5.1.7. Требования к организационному обеспечению. Разработка регламентов по использованию системы и обучению пользователей.

5.1.8. Требования к патентной чистоте. Все используемые технологии должны быть проверены на предмет патентных прав и лицензий.

5.1.9. Требования к документированию.

Документация должна содержать:

• Инструкции по использованию системы;

• Описание архитектуры и функциональности;

• Руководство по интеграции с другими системами.

5.2. Требования к функциям, выполняемым подсистемами.

Подсистема аутентификации должна выполнять проверку логина и пароля пользователя и генерацию токена доступа при успешной аутентификации.

Подсистема авторизации должна управлять правами доступа на основе ролей и проверять права доступа перед выполнением операций над ресурсами.

Подсистема восстановления пароля должна отправлять ссылки на восстановление пароля на электронную почту пользователя и проверять действительность токена для сброса пароля.

# 6 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА

6.1 Сроки выполнения проекта определяются согласно календарному плану к договору на разработку АС ЭПР.

6.2 Основные этапы разработки выполняются в соответствии с нормативными документами.

6.3 Приемо-сдаточные испытания разработанного программного продукта и документации по каждому этапу разработки АС ЭПР осуществляются комиссией в соответствии с календарным планом к договору.

6.5 Результаты этапов работ по их завершению оформляются двухсторонним актом Заказчика и Исполнителя.

6.6 По завершению разработки Исполнитель представляет документацию на АС ЭПР и проводит обучение администраторов и пользователей

# Приложение А

**UML-диаграмма процесса аутентификации и авторизации**

**пользователя в системе**

