**МИНИСТЕРСТВО ТРАНСПОРТА И КОММУНИКАЦИЙ**

**РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКАЯ ЖЕЛЕЗНАЯ ДОРОГА**

**Автоматизированная система  
аутентификации и авторизации**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**2023**

# СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ 2](#_Toc133956785)

[1 ВВЕДЕНИЕ 3](#_Toc133956786)

[2 ОБЩИЕ СВЕДЕНИЯ 3](#_Toc133956787)

[3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ 3](#_Toc133956788)

[3.1 Назначение 3](#_Toc133956789)

[3.2 Цели создания 3](#_Toc133956790)

[4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ 3](#_Toc133956791)

[5 ТРЕБОВАНИЯ К СИСТЕМЕ 4](#_Toc133956792)

[5.1 Требования к структуре 4](#_Toc133956793)

[5.2 Требования к процедурам доступа к системе 4](#_Toc133956794)

[5.3 Требования к функциональной безопасности 5](#_Toc133956795)

[5.4 Требования к информационной безопасности 5](#_Toc133956796)

[5.5 Требования к патентной чистоте 6](#_Toc133956797)

[6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ 6](#_Toc133956798)

[6.1 Требования к информационному обеспечению 6](#_Toc133956799)

[6.2 Требования к математическому обеспечению 6](#_Toc133956800)

[6.3 Требования к программному обеспечению 6](#_Toc133956801)

[6.7 Требования к организационному обеспечению 7](#_Toc133956802)

[6.9 Требования к техническому обеспечению 7](#_Toc133956803)

[7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ 8](#_Toc133956804)

[8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ 8](#_Toc133956805)

[9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ 8](#_Toc133956806)

# 1 **ВВЕДЕНИЕ**

Настоящее техническое задание разработано на автоматизированную систему аутентификации и авторизации Белорусской железной дороги.

# 2 ОБЩИЕ СВЕДЕНИЯ

2.1 Полное наименование: Автоматизированная система аутентификации и авторизации Белорусской железной дороги.

2.2 Заказчик: Государственное объединение «Белорусская железная дорога», 220030, г. Минск, ул. Ленина, 17;

2.3 Выполнение работ по этапам и стадиям работ, оформление и предъявление Заказчику их результатов осуществляется Исполнителем согласно требованиям данного технического задания.

# 3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ

## 3.1 Назначение

3.1.1 Назначение автоматизированной системы аутентификации и авторизации

– обеспечить безопасность доступа к информационной системе путем проверки подлинности пользователей и контроля их прав на доступ к ресурсам системы.

## 3.2 Цели создания

3.2.1 Цели создания автоматизированной системы аутентификации и авторизации:

* Защита от несанкционированного доступа к данным и ресурсам системы;
* Контроль доступа к разным уровням информации в зависимости от роли и прав пользователя в системе;
* Уменьшение рисков нарушения безопасности информации за счет снижения ошибок ввода паролей;
* Увеличение удобства работы пользователей посредством сокращения времени на вход в систему и упрощения процесса проверки подлинности;
* Обеспечение соответствия системы требованиям законодательства и международным стандартам по защите информации.

Конечная цель – обеспечение высокого уровня защиты информации и уверенности в том, что доступ к системе имеют только авторизованные пользователи.

# 4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ

4.1 Объекты системы разработки автоматизированной системы аутентификации и авторизации могут включать в себя:

4.2 Аутентификационный сервер – это сервер, который проводит аутентификацию пользователей. Он должен иметь высокую производительность, надежность и безопасность. Должна быть возможность настройки механизма аутентификации, используемых протоколов и методов.

4.3 База данных пользователей – хранит информацию о пользователях (логины, пароли, права доступа), а также информацию об устройствах, с которых осуществляется доступ. Должна быть надежной, защищенной и иметь высокую производительность.

4.4 Клиентское приложение – это программное обеспечение, которое позволяет пользователям осуществлять доступ к системе. Оно должно быть легко доступным и удобным в использовании.

4.5 Интерфейс администратора – это веб–интерфейс или приложение для управления системой. Он должен быть интуитивно понятным и обладать всеми необходимыми функциями для управления доступом пользователей.

4.6 База данных журнала – это база данных, которая хранит информацию о попытках доступа к системе и действиях пользователей. Должна быть надежной, защищенной и иметь высокую производительность.

4.7 Средства обработки антиспама и защиты от атак – это компоненты системы, которые обеспечивают безопасность и защиту системы от хакерских атак, DDoS–атак, вирусов и спама. Они должны быть интегрированы в систему и обладать надежностью и эффективностью.

4.8 Интеграция с другими системами – это возможность интеграции с другими системами, которые используются в организации. Обеспечивает удобство использования и минимизирует затраты на обслуживание системы.

4.9 Разработка и поддержка документации – это важный компонент системы, который позволяет обеспечить ее устойчивость и надежность в долгосрочной перспективе.

# 5 ТРЕБОВАНИЯ К СИСТЕМЕ

## 5.1 Требования к структуре

Данная система должна следующие основные компоненты:

* База данных пользователей. Для хранения информации о всех пользователях системы, включая их учетные записи, пароли, роли и разрешения.
* Сервер аутентификации. Предпочтительно использование протокола OpenID.
* Сервер авторизации. С помощью протокола OAuth 2
* Интерфейс пользователя. Для взаимодействия пользователя с системой аутентификации и авторизации, обычно через веб-интерфейс или мобильное приложение.
* Журнал аудита. Для записи всех действия пользователей в системе, включая их аутентификацию, авторизацию и доступ к ресурсам, чтобы обеспечить безопасность и отслеживаемость.

Кроме того, система должна включать такие компоненты, как шифрование данных, механизмы многофакторной аутентификации, а также механизмы обнаружения и предотвращения взлома и атак.

## 5.2 Требования к процедурам доступа к системе

5.2.1 Функции доступа к автоматизированной системе авторизации и аутентификации реализуются с различными уровнями доступа к информации.

5.2.2 Пользователи (все уровни) могут:

–Подтверждать свою личность, чтобы получить доступ к системе.

–Получать доступ к определенным ресурсам и функциям системы на основе своих прав доступа.

–Управлять своей учетной записью. Изменять свои учетные данные, например, пароль или адрес электронной почты.

–Создавать новые учетные записи для других пользователей системы.

–Управлять правами доступа. Устанавливать, изменять или отменять права доступа для других пользователей системы.

5.2.3 Разработчики:

Конкретные уровни доступа к информации зависят от роли разработчика и должны определяться на основе принципа наименьших привилегий (least privilege). Этот принцип предполагает, что каждый пользователь должен иметь только необходимый для выполнения своей работы уровень доступа к информации и ресурсам системы.

* Исходный код программного обеспечения, обеспечивающее функциональность системы аутентификации и авторизации.
* Документацию, которая описывает концептуальную модель системы, ее архитектуру, спецификации и детали реализации.
* Конфигурационные файлы и настройки системы, позволяющие настраивать и управлять ее работой.
* Журналы системных событий, которые отслеживают действия пользователей и другие события, происходящие в системе.
* Сведения об аутентификационных данных, таких как хэши паролей или сертификаты, используемые для проверки подлинности пользователей.
* Информацию о пользователях, их правах доступа и других параметрах, используемых для управления доступом.

В целом, доступ к информации должен быть ограничен и контролируемый, и разработчики должны следовать принципу необходимости минимального уровня доступа, чтобы обеспечить безопасность системы и ее пользователей.

## 5.3 Требования к функциональной безопасности

5.3.1 Программное обеспечение должно соотвествовать следующим требованиям к функциональной системе:

* Надежность аутентификации: Для этого система может использовать механизмы многофакторной аутентификации, такие как SMS-коды, временные пароли, биометрические данные и т.д. Предпочтительно использование Google Authenticator.
* Контроль доступа: Система должна обеспечивать строгий контроль доступа к ресурсам и функциям системы, в зависимости от роли пользователя. Для этого система может использовать различные методы, такие как разрешения на основе ролей, привилегированный доступ, политики контроля доступа и т.д. Примеры сервисов: AWS IAM, Okta, Azure AD, Keycloak.
* Защита паролей: Система должна защищать пароли пользователей от несанкционированного доступа и использовать надежные методы шифрования данных. Для этого система может использовать такие методы, как хеширование паролей, соление паролей, ограничение количества попыток входа и т.д. Сервис: HashiCorp Vault.
* Аудит и мониторинг: Система должна записывать все действия пользователей, чтобы обеспечить безопасность и отслеживаемость. Для этого система может использовать логирование и анализ журналов, мониторинг событий, оповещение о нарушениях с помощью сервиса Splunk.
* Антивирусная защита: Система должна быть защищена от вредоносных программ и вирусов. Для этого система может использовать антивирусные программы, механизмы защиты от DDoS-атак, фильтрацию сетевых трафиков. Для этого предпочтительно использование сервиса Kaspersky.

5.3.2 Программное обеспечение должно обеспечивать во всех регламентированных условиях и режимах его эксплуатации требуемый уровень качества функционирования и требуемые уровни безопасности и надежности. Указанные требования должны достигаться выполнением модели качества соответственно ГОСТ 27.003–90.

## 5.4 Требования к информационной безопасности

5.4.1 При разработке программного обеспечения должны быть учтены следующие требования к информационной безопасности:

* Высокий уровень безопасности системы: поддержка криптографических протоколов шифрования, механизм проверки подлинности сертификатов, защита от атак DoS и DDoS;
* Высокая производительность системы: возможность обработки большого числа запросов в единицу времени;
* Возможность интеграции с другими системами;
* Надежная защита от несанкционированного доступа: контроль прав доступа, система журналирования действий пользователей, защита от вредоносного ПО, от перебора паролей и т. д.;
* Удобные интерфейсы для пользователей и администраторов системы: понятные и интуитивно понятные формы аутентификации и авторизации, удобная настройка параметров, доступ к контролирующей информации.

## 5.5 Требования к патентной чистоте

5.5.1 При выполнении работ исполнителем обеспечивается патентная чистота результатов работ. Данная работа не должна содержать патентов, зарегистрированных в Республике Беларусь и других странах.

5.5.2 По требованию Заказчика Исполнитель представляет сведения о рыночной стоимости созданных при выполнении работ объектов интеллектуальной собственности.

# 6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

## 6.1 Требования к информационному обеспечению

6.1.1 Информационное обеспечение аутентификации и авторизации должно соответствовать следующим требованиям.

* Система должна хранить информацию о пользователях, включая их идентификаторы, пароли, атрибуты аутентификации (например, биометрические данные) и права доступа.
* Журнал событий: система должна сохранять записи о всех событиях, связанных с аутентификацией и авторизацией пользователей, таких как попытки входа в систему, изменения прав доступа и т.д. Эти записи могут быть использованы для отслеживания несанкционированного доступа или для анализа поведения пользователей.
* Для обеспечения безопасности системы, администраторы должны иметь инструменты мониторинга для отслеживания активности пользователей и обнаружения необычного поведения.
* Инструменты анализа: система должна включать инструменты анализа для обработки данных о пользователях и их активности, чтобы выявить тенденции и повысить эффективность системы.
* Правила и политики безопасности: система должна быть настроена в соответствии с установленными правилами и политиками безопасности, которые определяют, какие пользователи имеют доступ к каким ресурсам, какой уровень безопасности должен быть установлен для каждого ресурса и т.д.
* Обучающие материалы: для того чтобы пользователи могли эффективно использовать систему, им должны быть предоставлены обучающие материалы, включая инструкции по регистрации, аутентификации и использованию различных функций системы.
* Инструменты управления: для управления системой, в том числе добавления или удаления пользователей, изменения их прав доступа и т.д., администраторам должны быть предоставлены соответствующие инструменты.

## 6.2 Требования к математическому обеспечению

6.2.1 Специальных требований к применению в подсистеме математических моделей, методов или типовых алгоритмов не предъявляется.

## 6.3 Требования к программному обеспечению

 В требованиях к проекту в области аутентификации и авторизации должны быть учтены следующие моменты:

6.3.1 Безопасность: система должна быть разработана с учетом высоких стандартов безопасности и соответствовать требованиям соответствующих стандартов безопасности, таких как ISO 27001. Для обеспечения безопасности могут использоваться различные методы, включая шифрование данных, многоуровневую аутентификацию, контроль доступа и т.д.

6.3.2 Масштабируемость: система должна быть способна масштабироваться для обработки большого количества запросов на аутентификацию и автоматизацию. Для этого может использоваться распределенная архитектура с выделенными серверами для обработки запросов.

6.3.3 Надежность: система должна быть надежной и работать без простоев. Для обеспечения надежности могут использоваться механизмы резервирования и восстановления после сбоев.

6.3.4 Гибкость: система должна быть гибкой и адаптироваться к различным требованиям клиентов. Для этого может использоваться модульная архитектура, позволяющая добавлять и удалять модули по мере необходимости.

6.3.5 Совместимость: система должна быть совместима с другими системами и сервисами, с которыми может взаимодействовать. Для этого может использоваться стандартизированные протоколы и интерфейсы взаимодействия.

6.3.6 Простота использования: система должна быть простой в использовании для конечных пользователей и обеспечивать быстрый доступ к необходимым функциям. Для этого может использоваться интуитивно понятный пользовательский интерфейс и удобное управление функциями.

## 6.7 Требования к организационному обеспечению

6.5.1 Функционирование программного обеспечения не требует дополнительного оперативного эксплуатационного персонала.

6.5.2 Сопровождение программного обеспечения осуществляется специалистами ИРЦ Белорусской железной дороги.

## 6.9 Требования к техническому обеспечению

Требования к техническому обеспечению для аутентификации и авторизации должны включать в себя следующее:

* Серверы: серверы, на которых будет установлена система, должны иметь достаточную производительность для обработки большого количества запросов. Также могут использоваться выделенные серверы для обработки запросов на аутентификацию и автоматизацию.
* Сетевое оборудование: для обеспечения быстрого и надежного соединения между серверами и клиентами должны использоваться сетевые коммутаторы, маршрутизаторы и другое сетевое оборудование.
* Хранилище данных: система должна иметь достаточно большое и надежное хранилище данных для сохранения информации о пользователях и их учетных записях. Также может использоваться распределенное хранилище данных для обеспечения отказоустойчивости и масштабируемости.
* Безопасное соединение: для защиты данных, передаваемых между клиентами и серверами, должно использоваться безопасное соединение, например, протокол HTTPS.
* Аппаратное обеспечение: кроме серверов и сетевого оборудования, для работы системы могут потребоваться дополнительные компоненты, такие как датчики биометрической аутентификации, сканеры отпечатков пальцев, камеры для распознавания лиц и т.д.
* Поддержка протоколов безопасности: система должна поддерживать различные протоколы безопасности, такие как SSL/TLS, S/MIME и VPN, для защиты передачи данных.

# 7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ

7.1 Состав, содержание и этапность выполнения работ определяются согласно календарному плану к договору.

7.2 Заказчик организует поставку необходимого оборудования и лицензионного программного обеспечения.

7.3 Состав и перечень документов, предъявляемых по окончании соответствующих стадий и этапов, определяется в соответствии с договором на разработку ПО.

7.4 Основные этапы разработки выполняются в соответствии с нормативными документами.

# 8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ

Порядок приемки в эксплуатацию автоматизированной системы аутентификации и авторизации может включать в себя следующие этапы:

– Подготовительный этап – на этом этапе необходимо определить требования к системе, подготовить технические средства, установить программное обеспечение, обеспечить безопасность и достоверность информации.

– Испытательный этап – на этом этапе проводятся испытания системы на соответствие функциональным требованиям и стандартам безопасности. При этом проверяется правильность работы системы, отображение и передача информации, качество и скорость ее обработки.

– Аттестационный этап – на этом этапе проводится проверка соответствия системы установленным требованиям и стандартам безопасности. После успешного прохождения аттестационных испытаний выдается соответствующий сертификат, подтверждающий ее соответствие стандартам.

– Приёмочный этап – после прохождения всех предыдущих этапов система готова к приемке в эксплуатацию. На этом этапе решается вопрос об официальной передаче системы заказчику, подписывается акт приемки–передачи, и система передается в управление заказчику.

– Эксплуатационный этап – после приемки системы в эксплуатацию необходимо обеспечивать ее надежную работу, проводить ее техническое обслуживание и обновление программного обеспечения, а также регулярно проверять соответствие системы установленным требованиям и стандартам безопасности.

# 9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

9.1 Вся разрабатываемая документация оформляется в соответствии с действующими нормативными документами.

9.2 К ПО должна прилагаться инструкция пользователю. Рабочая документация должна соответствовать действующим стандартам и ГОСТ, ЕСКД и ЕСПД.

**НАСТОЯЩЕЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ МОЖЕТ УТОЧНЯТЬСЯ И КОРРЕКТИРОВАТЬСЯ ПО ВЗАИМНОЙ ДОГОВОРЕННОСТИ МЕЖДУ ИСПОЛНИТЕЛЕМ И ЗАКАЗЧИКОМ В РАБОЧЕМ ПОРЯДКЕ.**