**Министерство транспорта и коммуникаций Республики Беларусь**

**Учреждение образования**

**Белорусский государственный университет транспорта**

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К**

**разработке автоматизированной системы авторизации**

**Гомель, 2025**

**Оглавление**

[1 Общие сведения 3](#_Toc194401680)

[2 термины, определения и сокращения 3](#_Toc194401681)

[3 характеристика объекта 3](#_Toc194401682)

[3.1 Назначение 3](#_Toc194401683)

[3.2 Цели создания 3](#_Toc194401684)

[4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ 4](#_Toc194401685)

[5 ТРЕБОВАНИЯ К СИСТЕМЕ 4](#_Toc194401686)

[5.1 Требования к структуре 4](#_Toc194401687)

[5.2 Требования к процедурам доступа к системе 4](#_Toc194401688)

[5.3 Требования к функциональной безопасности 5](#_Toc194401689)

[5.4 Требования к информационной безопасности 5](#_Toc194401690)

[5.5 Требования к патентной чистоте 5](#_Toc194401691)

[6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ 5](#_Toc194401692)

[6.1 Требования к информационному обеспечению 5](#_Toc194401693)

[6.2 Требования к математическому обеспечению 6](#_Toc194401694)

[6.3 Требования к программному обеспечению 6](#_Toc194401695)

[6.4 Требования к техническому обеспечению 6](#_Toc194401696)

[6.5 Требования к организационному обеспечению 7](#_Toc194401697)

[7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ 7](#_Toc194401698)

[7.1 Анализ и исследование требований 7](#_Toc194401699)

[7.2 Проектирование системы 7](#_Toc194401700)

[7.3 Разработка программного обеспечения 7](#_Toc194401701)

[7.4 Тестирование системы 7](#_Toc194401702)

[7.6 Поддержка и развитие 7](#_Toc194401703)

[7.7 Содержание работ 8](#_Toc194401704)

[8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ 8](#_Toc194401705)

[8.1 Подготовительные мероприятия 8](#_Toc194401706)

[8.2 Проведение приемочных испытаний 8](#_Toc194401707)

[8.3 Документирование результатов 9](#_Toc194401708)

[8.4 Исправление выявленных недостатков 9](#_Toc194401709)

[8.5 Финальная приемка в эксплуатацию 9](#_Toc194401710)

[8.6 Постпроектное сопровождение 9](#_Toc194401711)

[9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ 9](#_Toc194401712)

[9.1 Общие требования 9](#_Toc194401713)

[9.2 Требования к проектной документации 9](#_Toc194401714)

[9.3 Требования к эксплуатационной документации 10](#_Toc194401715)

[9.4 Требования к технической документации 10](#_Toc194401716)

[9.5 Требования к документации безопасности 10](#_Toc194401717)

[9.6 Требования к документации сопровождения 10](#_Toc194401718)

[9.7 Требования к патентной документации 11](#_Toc194401719)

# 1 Общие сведения

* 1. Наименование работы: разработка технических требований на разработку автоматизированной системы.
  2. Заказчик – заведующий кафедрой «УЭРиОТ», Козлов В. Г. Ответственный по проекту: студентка группы СИ-31, Мухина А. Г.
  3. Наименование Организации-пользователя: Белорусский государственный университет транспорта.
  4. Наименование объекта внедрения: Белорусский государственный университет транспорта.

# термины, определения и сокращения

* 1. Авторизация – процесс предоставления пользователю или группе пользователей определенных разрешений, прав доступа и привилегий в компьютерной системе.
  2. Идентифика́ция в информационных системах — процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе.
  3. Аутентификация – проверка принадлежности пользователя к учетной записи и аккаунту.

# 3 характеристика объекта

## 3.1 Назначение

Назначение автоматизированной системы авторизации заключается в обеспечении безопасного, быстрого и эффективного процесса идентификации и проверки прав доступа пользователей к ресурсам, системам и данным организации. Она предназначена для минимизации рисков несанкционированного доступа и повышения уровня информационной безопасности.

## 3.2 Цели создания

- Автоматизация процессов управления доступом для сокращения времени и человеческих ошибок.

- Повышение надежности и безопасности авторизации за счет применения современных технологий защиты данных.

- Упрощение процедур аутентификации для пользователей при сохранении высокого уровня защиты.

- Централизованное управление доступом для удобства администрирования и анализа.

- Обеспечение гибкости системы для интеграции с другими приложениями и платформами.

# ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ

Пользователи системы:

- Физические лица, имеющие доступ к защищенным ресурсам, таким как сотрудники организации, партнеры или клиенты.

- Категории пользователей с различными уровнями прав доступа, включая администраторов, технический персонал и конечных пользователей.

Ресурсысистемы:

- Программные и аппаратные компоненты, включая серверы, базы данных, рабочие станции и мобильные устройства.

- Сетевые ресурсы и приложения, требующие контроля доступа.

Данные:

- Информация о пользователях: учетные записи, идентификаторы, персональные данные.

- Логирование действий пользователей: записи о доступе, временные метки, анализ поведения.

Интеграция:

- Взаимодействие системы с другими внутренними и внешними приложениями, такими как ERP, CRM, облачные сервисы.

- Адаптация для использования API сторонних сервисов.

Инфраструктурабезопасности:

- Средства шифрования данных и аутентификации пользователей.

- Механизмы защиты от атак, таких как попытки взлома или утечек данных.

# 5 ТРЕБОВАНИЯ К СИСТЕМЕ

## 5.1 Требования к структуре

- Система должна включать модуль аутентификации, модуль авторизации, модуль управления доступом и журнал действий пользователей.

- Архитектура системы должна быть модульной и обеспечивать возможность масштабирования.

- Поддержка многопользовательского режима и интеграция с внешними информационными системами (например, ERP, CRM).

## 5.2 Требования к процедурам доступа к системе

- Процедуры доступа должны предусматривать многофакторную аутентификацию (пароль + одноразовый код или биометрические данные).

- Предусмотрено разграничение прав пользователей в зависимости от их ролей.

- Необходима поддержка процессов восстановления доступа в случае утраты данных для аутентификации.

## 5.3 Требования к функциональной безопасности

- Система должна обеспечивать надежное выполнение всех функций без сбоев и потери данных.

- Предусмотрены механизмы самодиагностики и уведомлений об ошибках.

- В случае сбоя или отказа работа должна быть восстановлена с минимальными потерями информации.

## 5.4 Требования к информационной безопасности

- Система должна реализовывать современные методы шифрования данных как при передаче, так и при хранении.

- Предусмотрены защита от атак (например, «человек посередине», подбор паролей) и защита конфиденциальной информации.

- Наличие механизма блокировки учетных записей при подозрительной активности.

## 5.5 Требования к патентной чистоте

- Решение должно быть разработано с учетом исключения нарушений интеллектуальной собственности третьих лиц.

- Используемые компоненты и алгоритмы не должны нарушать действующие патенты и лицензии.

- Разработчики обязаны провести проверку патентной чистоты до завершения проекта.

# 6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

## 6.1 Требования к информационному обеспечению

-База данных пользователей должна включать полную и актуальную информацию о каждом пользователе: идентификатор, учетные данные, роль, историю доступа.

- Должны быть предусмотрены методы обновления и синхронизации данных с учетом реального времени для минимизации ошибок.

- Необходимо обеспечить возможность ведения журнала событий (логирования), включая фиксацию всех действий пользователей в системе (вход, изменение данных, попытки доступа).

- Используемые форматы данных должны поддерживать совместимость с другими системами (например, XML, JSON).

- Должна быть реализована защита информации от несанкционированного доступа с использованием современных стандартов шифрования.

## 6.2 Требования к математическому обеспечению

- Математическая модель авторизации должна обеспечивать поддержку ролевого управления доступом (RBAC) с возможностью гибкой настройки ролей.

- Применение алгоритмов шифрования данных, таких как AES или RSA, для обеспечения конфиденциальности информации.

- Необходимы алгоритмы анализа поведения пользователей для выявления аномальной активности (например, машинное обучение или правила анализа).

- Математическое обеспечение должно включать расчет показателей производительности системы, таких как время отклика при увеличении количества пользователей.

- Обеспечение корректности и точности вычислений в процессе проверки прав доступа.

## 6.3 Требования к программному обеспечению

- Программное обеспечение должно быть совместимо с основными операционными системами (Windows, Linux, macOS).

- Должна поддерживаться интеграция через API для взаимодействия с внешними системами.

- Интерфейс пользователя должен быть интуитивно понятным, с возможностью адаптации под нужды разных категорий пользователей.

- Обновления программного обеспечения должны быть автоматизированы и не нарушать текущую работу системы.

- Программное обеспечение должно включать инструменты мониторинга и администрирования для управления доступом.

## 6.4 Требования к техническому обеспечению

-Система должна поддерживаться на серверных платформах с высокой производительностью, достаточной для обработки запросов в режиме реального времени.

- Наличие резервного копирования и отказоустойчивой архитектуры для предотвращения потери данных.

- Поддержка облачных и локальных инфраструктур в зависимости от потребностей пользователя.

- Используемое оборудование должно обеспечивать физическую защиту данных (например, защиту от несанкционированного доступа).

- Оборудование должно соответствовать требованиям энергоэффективности и быть сертифицированным в соответствии с международными стандартами.

## 6.5 Требования к организационному обеспечению

- Должна быть разработана четкая политика доступа, определяющая роли и права пользователей.

- Необходимо организовать регулярное обучение сотрудников по вопросам информационной безопасности и работы с системой.

- Назначение ответственных лиц за администрирование системы и контроль прав доступа.

- Разработка процедур управления инцидентами, включая протоколы действий при попытке несанкционированного доступа.

- Проведение регулярных аудитов системы для оценки её соответствия заданным требованиям.

# 7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ

## 7.1 Анализ и исследование требований

- Изучение бизнес-процессов, связанных с авторизацией.

- Выявление потребностей пользователей и заинтересованных сторон.

- Сбор и формализация требований к системе.

## 7.2 Проектирование системы

- Разработка архитектуры системы авторизации, включая модульную структуру.

- Создание схем данных, процессов аутентификации и авторизации.

- Подготовка технического задания для реализации системы.

## 7.3 Разработка программного обеспечения

-Программирование основных функциональных модулей системы.

- Реализация пользовательского интерфейса, поддерживающего удобное взаимодействие.

- Интеграция системы с другими приложениями и платформами.

## 7.4 Тестирование системы

- Проведение функционального тестирования для проверки работы системы.

- Стресс-тестирование для оценки устойчивости к высокой нагрузке.

- Испытания безопасности для проверки защиты данных.

7.5 Внедрение системы

- Установка системы на серверы и рабочие устройства.

- Проведение настройки параметров системы согласно требованиям организации.

- Обучение пользователей и технического персонала.

## 7.6 Поддержка и развитие

- Обеспечение технической поддержки пользователей системы.

- Проведение регулярного обновления и улучшения функциональности.

- Аудит системы для выявления слабых мест и возможности улучшений.

## 7.7 Содержание работ

- Подробное изучение существующих процессов авторизации и их недостатков для разработки системы, отвечающей текущим потребностям.

- Формирование модели угроз для определения и минимизации рисков информационной безопасности.

- Выбор и интеграция инструментов, обеспечивающих многофакторную аутентификацию и современные методы шифрования.

- Создание гибких механизмов управления доступом, включая настройку ролей и прав пользователей.

- Обеспечение совместимости системы с инфраструктурой компании, включая аппаратное и программное обеспечение.

- Тестирование на всех этапах разработки для обеспечения качества и надежности системы.

- Проведение обучения сотрудников и документирование всех этапов внедрения.

- Предоставление рекомендаций по дальнейшему развитию системы и её возможной модернизации.

# 8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ

## 8.1 Подготовительные мероприятия

- Проведение предварительного тестирования системы с привлечением специалистов по информационной безопасности, а также представителей разработчика.

- Составление плана приемочных испытаний, включающего перечень проверяемых функций, сценарии тестирования и критерии приемки.

- Определение ответственных лиц за процесс приемки со стороны заказчика и разработчика.

- Обеспечение готовности инфраструктуры для проведения испытаний, включая серверы, рабочие станции и сетевое оборудование.

## 8.2 Проведение приемочных испытаний

- Проверка функциональности системы, включая корректность работы модулей авторизации, аутентификации и управления доступом.

- Тестирование системы на соответствие техническим требованиям, заявленным в проектной документации.

- Проверка интеграции с другими приложениями и платформами, которые являются частью инфраструктуры заказчика.

- Оценка производительности системы, включая скорость обработки запросов и устойчивость к нагрузкам.

- Тестирование механизмов безопасности: защита данных, отказоустойчивость, противодействие угрозам.

## 8.3 Документирование результатов

- Составление акта приемочных испытаний с указанием обнаруженных несоответствий и их устранения.

- Подготовка отчета о проверке всех параметров системы, включая выполнение требований функциональной и информационной безопасности.

- Регистрация всех замечаний, которые необходимо устранить до окончательной приемки системы.

## 8.4 Исправление выявленных недостатков

- Проведение разработчиком доработок системы на основании замечаний, выявленных в ходе приемочных испытаний.

- Повторное тестирование тех компонентов системы, которые подверглись изменениям.

## 8.5 Финальная приемка в эксплуатацию

- Проведение итоговой проверки всех функций и параметров системы на предмет соответствия техническому заданию.

- Подписание акта приемки-передачи системы в эксплуатацию обеими сторонами.

- Формальное утверждение системы для использования в рабочей среде заказчика.

## 8.6 Постпроектное сопровождение

- Предоставление технической поддержки в первые месяцы эксплуатации.

- Проведение обучения пользователей системы и администратора.

- Утверждение плана дальнейшего развития и улучшения системы, если требуется.

# 9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

## 9.1 Общие требования

- Документирование всех этапов разработки системы должно быть четким, последовательным и соответствовать установленным стандартам.

- Все документы должны быть структурированы и легко доступны для заинтересованных сторон.

- Форматы документации должны быть совместимы с основными офисными программами (например, PDF, DOCX).

## 9.2 Требования к проектной документации

- Техническое задание должно содержать подробное описание целей, задач и требований к системе.

- Архитектурные схемы должны быть представлены в виде диаграмм, отражающих структуру системы и взаимодействие её компонентов.

- Документы должны включать спецификации используемых программных и аппаратных компонентов.

- Проектная документация должна быть утверждена и подписана соответствующими ответственными лицами.

## 9.3 Требования к эксплуатационной документации

- Руководство пользователя должно содержать подробные инструкции по использованию системы, включая пошаговое описание основных функций.

- Административная документация должна включать руководство для технических специалистов, описывающее процессы установки, настройки и поддержки системы.

- Все инструкции должны быть снабжены визуальными элементами (например, схемами и скриншотами) для облегчения восприятия.

- Эксплуатационная документация должна быть регулярно обновляемой в случае внесения изменений в систему.

## 9.4 Требования к технической документации

- Описание алгоритмов системы должно быть представлено в виде структурированных блоков с комментариями к каждому этапу работы.

- Программный код должен быть снабжен комментариями для облегчения понимания разработчиками и дальнейшего сопровождения.

- Технические требования должны включать описание архитектуры, сетевых протоколов и методов шифрования, используемых в системе.

- Документация должна содержать данные о тестировании: планы, сценарии, результаты.

## 9.5 Требования к документации безопасности

- Информация о методах защиты данных должна быть представлена в подробных отчетах, включая описание используемых алгоритмов шифрования и мер противодействия угрозам.

- Политика безопасности должна быть документирована, включая права доступа, процедуры аутентификации и действия в случае инцидентов.

- Отчетность по аудиту безопасности должна быть частью документации для оценки соответствия системы требованиям.

## 9.6 Требования к документации сопровождения

- Система должна иметь подробную документацию по обновлению, включая описание процесса внедрения новых версий и резервного копирования данных.

- Документы сопровождения должны содержать список контактов службы технической поддержки.

- Должны быть предоставлены инструкции для быстрого устранения распространённых проблем.

## 9.7 Требования к патентной документации

- Документация должна подтверждать патентную чистоту используемых решений, включая анализ на отсутствие нарушений интеллектуальной собственности.

- Все используемые лицензии и сертификаты должны быть задокументированы и приложены к проекту.