**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 проекта**: разработка технический требований на создание автоматизированной системы аутентификации и авторизации в соответствии с СТП 09150.11.118-2009.

**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;

Управление Белорусской железной дороги

3

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ**

На 15 листах

**ОГЛАВЛЕНИЕ**  
[1. ОБЩИЕ СВЕДЕНИЯ 3](#_Toc193714740)

[2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ 4](#_Toc193714741)

[3. ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ 5](#_Toc193714742)

[3.1 Перечень и краткая характеристика бизнес-процессов 5](#_Toc193714743)

[3.2 Требования к входным и выходным данным, формам их представления 6](#_Toc193714744)

[3.3 Выполняемые технологические операции 8](#_Toc193714745)

[4. ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС 8](#_Toc193714746)

[4.1 Формулировка цели разработки 8](#_Toc193714747)

[4.2 Область и условия применения АС 9](#_Toc193714748)

[4.3 Ограничения применения 9](#_Toc193714749)

[5. ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС 9](#_Toc193714750)

[5.1 Требования к АС в целом 9](#_Toc193714751)

[5.1.1 Требования к структуре и функционированию АС 9](#_Toc193714752)

5.1.2 Требования к защите информации от несанкционированного доступа. 10

[5.1.3 Требования по сохранности информации при авариях 11](#_Toc193714754)

[5.1.4 Требования к информационному обеспечению 11](#_Toc193714755)

[5.1.5 Требования к математическому обеспечению 12](#_Toc193714756)

[5.1.6 Требования к программному обеспечению 12](#_Toc193714757)

[5.1.7 Требования к организационному обеспечению 13](#_Toc193714758)

[5.1.8 Требования к патентной чистоте 13](#_Toc193714759)

[5.1.9 Требования к документированию 13](#_Toc193714760)

[5.2 Требования к функциям (задачам), выполняемым подсистемами 13](#_Toc193714761)

[6. СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА 14](#_Toc193714762)

1. ОБЩИЕ СВЕДЕНИЯ

1.1 Название работы: создание технических требований для автоматизированной системы авторизации, предназначенной для Белорусской железной дороги (АС Авторизация).

1.2 Заказчик и ответственные лица: Заказчиком системы выступает Государственное объединение «Белорусская железная дорога». Руководство проектом осуществляет служба технической политики и инвестиций данного объединения.

1.3 Организация - пользователь системы: Государственное объединение «Белорусская железная дорога».

1.4 Объект внедрения системы: Главное управление Белорусской железной дороги.

2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

2.1 В данных технических требованиях используются термины и определения со следующим смыслом:

2.1.1 Система авторизации: автоматизированный инструмент, предназначенный для безопасного управления доступом пользователей к ресурсам и функциям информационных систем Белорусской железной дороги, основанный на идентификации и проверке их полномочий.

2.1.2 Пользователь: человек, обладающий уникальной учетной записью для работы с информационными системами Белорусской железной дороги.

2.1.3 Аутентификация: процесс подтверждения личности пользователя при входе в систему на основании предоставленных учетных данных (логина, пароля, а также методов двухфакторной аутентификации).

2.1.4 Авторизация: предоставление пользователю доступа к системным ресурсам в соответствии с его установленными полномочиями.

2.1.5 Учетная запись: уникальная совокупность данных, ассоциированная с пользователем для его идентификации и доступа к системе.

2.1.6 Роль: набор полномочий и уровней доступа, назначенных пользователю в системе.

2.1.7 Прочие термины и определения используются в значениях, установленных правовыми и нормативно-техническими документами Белорусской железной дороги.

2.2 В настоящих технических требованиях использованы сокращения:

АС – автоматизированная система;

АС АВТ – автоматизированная система авторизации;

АС АРДП – автоматизированная система актуального расписания движения поездов;

АС «Паспорт ОЖИ» – автоматизированная система паспортов объектов железнодорожной инфраструктуры;

АС ПРЕД – автоматизированная система подготовки и выдачи предупреждений;

АС ЭПР – автоматизированная система по определению энергозатрат для поездной работы на Белорусской железной дороге;

ИАС ПУРГП – информационная аналитическая система поддержки управленческих решений для грузовых перевозок;

ИРЦ – РУП «Главный расчетный информационный центр» Белорусской железной дороги;

НСИ – нормативно-справочная информация;

ПО – программное обеспечение;

ТЭР – топливно-энергетические ресурсы.

3. ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ

# 3.1 Перечень и краткая характеристика бизнес-процессов

3.1.1 Объектом автоматизации является система управления доступом к информационным системам Белорусской железной дороги с целью обеспечения безопасной авторизации пользователей.

3.1.2 Управление доступом и авторизацией в рамках решаемой задачи автоматизации осуществляется на трех уровнях:

дорожном: служба информационных технологий и службы обеспечения безопасности;

отделенческом: отделы отделений Белорусской железной дороги, отвечающие за локальные информационные системы;

линейном: железнодорожные станции, локомотивные депо и другие подразделения.

Процессы управления авторизацией включают:

разработку политик и процедур безопасности, регулирующих управление учетными записями пользователей;

регистрацию и управление учетными записями для сотрудников;

текущее управление доступом, включая предоставление, отзыв или изменение полномочий пользователей в зависимости от их ролей и обязанностей.

3.1.3 Предметом автоматизации является методика безопасного управления доступом на основе современных технологий аутентификации и авторизации, включая использование многофакторной аутентификации (MFA), методов шифрования и ролевого управления доступом (RBAC).

3.1.4 Процесс авторизации описывается последовательностью действий, направленных на идентификацию пользователя, проверку полномочий и предоставление разрешенного уровня доступа к системе. Используемые методы включают проверку учетных данных, привязку к определенным ролям и применение политик безопасности, установленных для соответствующего пользователя.

3.1.5 Реализация АС Авторизации включает автоматизацию трех взаимосвязанных бизнес-процессов:

формирование и управление базой данных учетных записей;

проверка и подтверждение учетных данных пользователей (аутентификация);

распределение и контроль доступа пользователей к различным ресурсам системы (авторизация).

3.1.6 Формирование и управление базой данных учетных записей осуществляется за счет реализации следующих задач:

создание, изменение и удаление учетных записей в системе;

управление ролевым доступом;

интеграция данных о пользователях из внешних систем (например, HR-системы).

3.1.7 Проверка и подтверждение учетных данных пользователей осуществляется за счет реализации следующих задач:

проверка корректности предоставленных учетных данных (логин, пароль, код подтверждения);

использование методов двухфакторной аутентификации (пароль + SMS/приложение);

ведение журнала аутентификаций для мониторинга и предотвращения подозрительной активности.

3.1.8 Процесс авторизации включает:

проверку полномочий пользователя для доступа к запрашиваемым ресурсам;

динамическое назначение уровней доступа в зависимости от контекста (например, IP-адрес, местоположение);

формирование отчета о действиях пользователя и уровне предоставленного доступа.

3.1.9 Обязательным условием функционирования АС Авторизации является выполнение проверки и авторизации пользователя за минимально возможное время. Максимально допустимое время на выполнение процесса авторизации составляет 1 секунда с момента отправки запроса.

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

3.2.1 Входными данными для выполнения авторизации пользователей являются:

учетные данные пользователя (логин и пароль);

данные двухфакторной аутентификации (например, SMS-код или код приложения);

информация о роли пользователя в системе;

IP-адрес и местоположение (при необходимости динамического распределения доступа);

метаданные сеанса (дата и время, используемое устройство).

3.2.2 Выходными данными системы авторизации являются:

результат авторизации (успех или отказ);

данные о предоставленных полномочиях и доступе к ресурсам;

информация о блокировке учетной записи или необходимости смены пароля;

журнал событий авторизации, включающий дату, время, IP-адрес и результат.

3.2.3 Входные и выходные данные должны представляться в форме, позволяющей средствами автоматизации:

их идентифицировать;

получать их численные значения (где это применимо).

3.2.4 Формой представления выходных данных с результатами авторизации является текст, содержащий параметры авторизации и результат выполнения (таблица 3.1).

*Таблица 3.1* – Формат представления выходных данных

| Наименование параметра | Формат представления |
| --- | --- |
| Имя пользователя | Текст (до 50 знаков) |
| Дата и время авторизации | Дата и время (формат: ISO 8601) |
| IP-адрес | Текст (IPv4/IPv6) |
| Результат авторизации | Текст ("успех" или "отказ") |
| Роль пользователя | Текст (до 30 знаков) |

3.2.5 Формой представления промежуточных результатов авторизации является журнал событий, содержащий записи о процессе авторизации, включая успешные и неуспешные попытки входа.

3.2.6 Источниками получения входных данных (параметров) являются:

Информационные системы Белорусской железной дороги: в части получения данных о пользователях, их ролях и правах доступа.

Система управления учетными записями (IAM): в части управления учетными данными (логин, пароль) и параметрами двухфакторной аутентификации.

Система мониторинга и безопасности: для получения информации о подозрительных действиях и предотвращения угроз.

Внешние сервисы аутентификации: при использовании сторонних решений для двухфакторной аутентификации (например, Google Authenticator, SMS-шлюзы).

3.2.7 Источники получения входных данных (параметров) для выполнения авторизации приведены в таблице 3.2.

*Таблица 3.2* – **Источники получения входных данных (параметров)**

| Наименование параметра | Наименование информационной системы |
| --- | --- |
| Учетные данные (логин, пароль) | IAM (Система управления учетными записями) |
| Роль пользователя | Информационные системы Белорусской железной дороги |
| Двухфакторная аутентификация | Сторонние сервисы (SMS/приложение) |
| Метаданные сеанса (IP, устройство) | Система мониторинга и безопасности |
| История входов | Журнал событий авторизации |
| Политики безопасности | Система мониторинга и управления безопасностью |

# 3.3 Выполняемые технологические операции

Автоматизации подлежат технологические операции:

Формирование исходных данных: сбор информации о пользователях, включая идентификацию их учетных записей, назначение ролей и определение уровней доступа в соответствии с требованиями безопасности.

Проведение процесса аутентификации: проверка учетных данных (логин, пароль) пользователя, выполнение двухфакторной аутентификации (если применимо).

Определение полномочий пользователя: проверка роли пользователя, определение перечня доступных функций и ресурсов в зависимости от его полномочий.

Формирование выходного решения: предоставление или отказ в доступе с регистрацией всех действий в журнале событий для последующего анализа и обеспечения безопасности.

4. ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС

4.1 Цель разработки Создание АС Авторизации направлено на достижение следующих целей:

разработка интегрированной автоматизированной системы, обеспечивающей управление доступом к информационным системам Белорусской железной дороги;

повышение уровня безопасности и усиление контроля над доступом к данным и ресурсам;

автоматизация процедур аутентификации и авторизации пользователей;

снижение влияния человеческого фактора и связанных с ним рисков при управлении учетными записями;

уменьшение нагрузки на сотрудников, ответственных за контроль и управление доступом.

4.2 Область применения и условия эксплуатации АС Авторизации предназначена для автоматизации процессов аутентификации и авторизации работников Белорусской железной дороги, обеспечивая доступ к ресурсам в соответствии с назначенными ролями.

4.3 Ограничения использования Работа АС Авторизации должна обеспечиваться при выполнении следующих условий:

серверная часть функционирование на технических средствах ИРЦ с учетом требований по операционным системам и их совместимости с действующими информационными системами;

клиентская часть работа на автоматизированных рабочих местах сотрудников, использующих систему, с учетом установленных операционных систем и клиентского программного обеспечения, включая веб-браузеры.

5. ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС

# 5.1 Требования к АС в целом

АС Авторизации должна разрабатываться на платформе Web-технологий по принципу «сервер – тонкий клиент» с учетом адаптации под локальное программное обеспечение Белорусской железной дороги. Клиентский доступ к АС Авторизации обеспечивается посредством интернет-браузера. Доступ к АС Авторизации из других информационных систем обеспечивается через программный интерфейс API.

## 5.1.1 Требования к структуре и функционированию АС

5.1.1.1 Реализация функций АС Авторизации обеспечивается функционированием подсистем:

Доступа и авторизации: управление учетными записями, аутентификация пользователей, проверка полномочий и управление ролями.

Информационного обеспечения и взаимодействия: интеграция с другими системами Белорусской железной дороги, централизованное управление учетными данными.

Исполнительских процессов: выполнение операций аутентификации и авторизации в режиме реального времени.

Формирования выходных решений: генерация отчетов и ведение журнала событий для анализа безопасности и контроля доступа.

5.1.1.2 Информационный обмен между подсистемами

Информационный обмен между подсистемами АС Авторизации, а также с другими информационно-управляющими системами, должен осуществляться по Единой сети передачи данных Белорусской железной дороги для обеспечения безопасности и целостности данных.

5.1.1.3 Режимы функционирования и обслуживания

Режимы функционирования и обслуживания АС Авторизации должны соответствовать требованиям законодательства Республики Беларусь, а также локальным правовым актам Белорусской железной дороги в области информационной безопасности и информационных технологий.

## 5.1.2 Требования к защите информации от несанкционированного доступа

5.1.2.1 Процедура доступа к АС Авторизации должна учитывать многоуровневую реализацию защиты информации.

Доступ к системе осуществляется на основании ввода учетных данных (логина и пароля), назначаемых администраторами системы.

Пароль пользователя должен соответствовать требованиям безопасности: не менее 8 символов, включающих цифры и символы разного регистра. Проверка пароля должна выполняться на стороне клиента.

Все пароли хранятся в системе исключительно в зашифрованном виде для предотвращения утечек данных.

5.1.2.2 Программный интерфейс

В АС Авторизации должен быть предусмотрен программный интерфейс (API) для автоматизации обмена данными с другими информационно-управляющими системами Белорусской железной дороги. API должен поддерживать:

интеграцию с внешними системами для проверки учетных данных и полномочий;

возможность передачи данных об учетных записях, ролях и статусах пользователей;

безопасный протокол взаимодействия с системами.

5.1.2.3 Требования к информационной безопасности

При разработке АС Авторизации должны учитываться следующие требования к информационной безопасности:

Авторизация и аутентификация: доступ к информации должен осуществляться только через систему авторизации и аутентификации пользователей.

Шифрование учетных данных: хранение учетных данных на сервере должно выполняться в зашифрованном виде с использованием государственного стандарта симметричного шифрования и контроля целостности Республики Беларусь.

Передача данных: вся передача информации, включая через беспроводные каналы, должна быть защищена протоколом, поддерживающим шифрование данных (например, HTTPS).

Учет доступа: должна быть предусмотрена функция учета всех попыток и фактического доступа пользователей к системе.

Резервное копирование: необходимо разработать механизм периодического резервного копирования базы данных АС Авторизации для предотвращения потери данных.

## 5.1.3 Требования по сохранности информации при авариях

Для АС Авторизации должны быть предусмотрены процедуры обеспечения сохранности данных:

Копирование и восстановление: регулярное резервное копирование базы данных и создание плана восстановления данных.

Защита от несанкционированного доступа: реализация механизмов, предотвращающих доступ к данным при сбоях и отказах.

Устойчивость к катастрофическим событиям: создание резервных копий на удалённых серверах, которые защищены от физических повреждений и кибератак.

## 5.1.4 Требования к информационному обеспечению

5.1.4.1 Информационное обеспечение АС Авторизации представляет собой совокупность массивов информации, составляющих базу данных об учетных записях пользователей, их ролях, полномочиях и параметрах безопасности. Информационное обеспечение должно быть достаточным для выполнения функций, заданных техническими требованиями, а также масштабируемым для добавления новых функций.

5.1.4.2 Идентификация пользователей или событий в АС Авторизации должна быть реализована через однозначное формализованное обозначение, например уникальные идентификаторы пользователей или записи журнала событий. Формализация данных должна соответствовать требованиям эффективной цифровой обработки и безопасности.

5.1.4.3 АС Авторизации должна обеспечивать ввод и корректировку данных администратором с возможностью многократного использования данных. При этом должна быть предусмотрена защита данных от изменений со стороны обычных пользователей.

5.1.4.4 Поиск, извлечение, изменение и внесение данных в АС Авторизации должны обеспечиваться наиболее эффективным способом, исключающим затруднения в обработке данных и их восприятии администраторами или системой.

5.1.4.5 Ввод нормативно-справочной информации и формирование базы данных учетных записей должны быть выполнены на стадии разработки программного обеспечения. Администратор должен иметь возможность вводить дополнительные данные или корректировать существующие, используя автоматизированную подсистему обновления (синхронизации) данных, например, из внешних систем управления.

## 5.1.5 Требования к математическому обеспечению

5.1.5.1 Математическое обеспечение должно поддерживать все необходимые функции системы, включая:

* аутентификацию и авторизацию пользователей через запрос учетных данных (логин и пароль);
* проверку пароля на соответствие требованиям (не менее 8 символов, наличие цифр и символов разного регистра), выполняемую на стороне клиента;
* уничтожение сессии пользователя при отсутствии активности более 10 минут;
* сброс и восстановление данных учетной записи пользователя.

5.1.5.2 Алгоритмы должны быть гибкими, поддерживать переконфигурирование и реализовываться через библиотечные блочные структуры для обеспечения модульности.

## 5.1.6 Требования к программному обеспечению

5.1.6.1 Заказчик организует поставку необходимого лицензионного программного обеспечения для обеспечения работы серверной и клиентской частей системы.

5.1.6.2 Программное обеспечение АС Авторизации не должно препятствовать бесперебойному функционированию технических средств Белорусской железной дороги.

5.1.6.3 Программное обеспечение должно включать:

* подсистему проверки пароля на стороне клиента;
* подсистему хранения паролей в зашифрованном виде;
* подсистему уничтожения сессии пользователя при отсутствии активности более 10 минут;
* подсистему сброса и восстановления учетных данных.

5.1.6.4 В состав АС Авторизации должны входить серверная часть (централизованное управление и хранение данных) и клиентская часть (интерфейс для пользователей), разработанные согласно настоящим техническим требованиям.

5.1.6.5 В процессе разработки программного обеспечения должна соблюдаться методическая преемственность и использоваться накопленный опыт создания аналогичных систем для обеспечения совместимости и эффективности.

5.1.6.6 Качественные параметры программного обеспечения определяются на стадии разработки и уточняются на основании результатов опытной эксплуатации или независимой экспертизы.

5.1.6.7 Кроме указанных выше требований, программное обеспечение должно предусматривать:

процедуры оценки эффективности, включая время реакции системы, время обработки входных и выходных данных;

интуитивно понятный интерфейс, который позволяет освоить работу с системой без использования дополнительной документации, благодаря встроенным функциям подсказок.

## 5.1.7 Требования к организационному обеспечению

5.1.7.1 Функционирование АС

Организация работы не должна предусматривать дополнительного эксплуатационного персонала для контроля выполнения процессов уничтожения сессий или сброса учетных данных, так как они автоматизированы.

5.1.7.2 Сопровождение АС Авторизации должно осуществляться инженерами соответствующих подразделений Белорусской железной дороги.

## 5.1.8 Требования к патентной чистоте

5.1.8.1 При выполнении работ Исполнителем должно быть обеспечено соблюдение патентной чистоты результатов, исключающее использование патентов, зарегистрированных в Республике Беларусь и других странах.

5.1.8.2 По запросу Заказчика Исполнитель обязан предоставить сведения о рыночной стоимости созданных при выполнении работ объектов интеллектуальной собственности.

## 5.1.9 Требования к документированию

5.1.9.1 Состав и перечень документов, предоставляемых на завершение каждой стадии и этапа разработки, должны быть определены в соответствии с договором на разработку АС Авторизации.

5.1.9.2 Вся документация, разработанная для АС Авторизации, должна оформляться в соответствии с нормативными документами Белорусской железной дороги.

5.1.9.3 К АС Авторизации должны прилагаться инструкции для пользователей и системных администраторов. Рабочая документация должна соответствовать требованиям нормативных документов Белорусской железной дороги.

# 5.2 Требования к функциям (задачам), выполняемым подсистемами

5.2.1 Подсистема «Доступ и авторизация»

Подсистема должна реализовывать:

* процесс аутентификации и авторизации через запрос учетной записи (логин и пароль);
* проверку пароля на стороне клиента (минимум 8 символов, наличие цифр и символов разного регистра);
* уничтожение сессии при отсутствии активности более 10 минут;
* управление сбросом и восстановлением данных учетной записи.

5.2.2 Подсистема «Информационное обеспечение и взаимодействие» Подсистема предназначена для решения следующих задач:

сбор и проверка информации из взаимодействующих информационных систем на соответствие требованиям безопасности и точности данных;

предоставление возможности локального ввода информации пользователем с обязательной верификацией данных и возможностью корректировки (при необходимости) информации, полученной из взаимодействующих информационных систем.

5.2.3 Подсистема «Исполнительские процессы и математическое обеспечение»

Подсистема предназначена для выполнения задач:

валидации вводимой информации, приведения данных к установленным требованиям безопасности и структуре системы;

реализации бизнес-процессов авторизации, включая проверку полномочий пользователя, применение политик безопасности и распределение доступов;

периодического резервного копирования базы данных (не реже одного раза в месяц) для предотвращения потери данных.

5.2.4 Подсистема «Формирование выходных решений»

Подсистема должна включать:

* представление данных пользователя о статусе авторизации в текстовом формате;
* функционал экспортируемого отчета об уничтожении сессий и сбросе учетных записей.

6. СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА

6.1 Сроки выполнения проекта определяются в соответствии с календарным планом, установленным в договоре на разработку АС Авторизации.

6.2 Основные этапы разработки системы выполняются в соответствии с действующими нормативными документами Белорусской железной дороги.

6.3 Приемо-сдаточные испытания разработанного программного продукта и документации по каждому этапу разработки АС Авторизации осуществляются комиссией на основе календарного плана к договору.

6.4 На технических ресурсах Белорусской железной дороги проводится опытная эксплуатация АС Авторизации. После этого Заказчиком принимается решение о порядке и сроках внедрения и ввода системы в промышленную эксплуатацию.

6.5 Результаты выполнения каждого этапа работ оформляются двухсторонним актом между Заказчиком и Исполнителем.

6.6 По завершению разработки, кроме базового обучения администраторов и пользователей, Исполнитель должен обеспечить обучение работе с процессом восстановления учетной записи и уничтожением сессии.

**НАСТОЯЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ МОГУТ УТОЧНЯТЬСЯ И КОРРЕКТИРОВАТЬСЯ ПО ВЗАИМНОЙ ДОГОВОРЕННОСТИ МЕЖДУ ЗАКАЗЧИКОМ И ИСПОЛНИТЕЛЕМ В РАБОЧЕМ ПОРЯДКЕ.**