**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ**

**К РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АВТОРИЗАЦИИ**

**ОГЛАВЛЕНИЕ**

[1 ОБЩИЕ СВЕДЕНИЯ 3](#_Toc193958465)

[2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ 3](#_Toc193958466)

[3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ 4](#_Toc193958467)

[3.1 Перечень и краткая характеристика бизнес-процессов 4](#_Toc193958468)

[3.2 Требования к входным и выходным данным, формам их представления 5](#_Toc193958469)

[3.3 Выполняемые технологические операции 6](#_Toc193958470)

[4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС 7](#_Toc193958471)

[4.1 Формулировка цели работы 7](#_Toc193958472)

[4.2 Область и условия применения АС 7](#_Toc193958473)

[4.3 Ограничения применения АС 7](#_Toc193958474)

[5 ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС 7](#_Toc193958475)

[5.1 Требования к АС в целом 7](#_Toc193958476)

[5.1.1 Требования к структуре и функционированию АС 7](#_Toc193958477)

[5.1.2 Требования к защите информации от несанкционированного доступа 8](#_Toc193958478)

[5.1.3 Требования по сохранности информации при авария 8](#_Toc193958479)

[5.1.4 Требования к информационному обеспечению 8](#_Toc193958480)

[5.1.5 Требования к математическому обеспечению 9](#_Toc193958481)

[5.1.6 Требования к программному обеспечению 9](#_Toc193958482)

[5.1.7 Требования к организационному обеспечению 10](#_Toc193958483)

[5.1.8 Требования к патентной чистоте 10](#_Toc193958484)

[5.1.9 Требования к документированию 10](#_Toc193958485)

[5.2 Требования к функциям (задачам), выполняемым подсистемами 10](#_Toc193958486)

[6 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА 11](#_Toc193958487)

# 1 ОБЩИЕ СВЕДЕНИЯ

1.1 Наименование работы: разработка технических требований на процесс авторизации пользователей в автоматизированной системе (АС АП).

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

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

1.4 Наименование объекта внедрения: Управление информационных систем и технологий Белорусской железной дороги.

# 2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

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

2.1.1 Автоматизированная система (АС) – комплекс программных и аппаратных средств, предназначенных для автоматизации процессов, связанных с управлением, обработкой и хранением данных, а также взаимодействием пользователей с системой.

2.1.2 Пользователь – физическое или юридическое лицо, имеющее доступ к автоматизированной системе и использующее ее функционал для выполнения своих задач.

2.1.3 Авторизация – процесс проверки и подтверждения прав доступа пользователя к ресурсам автоматизированной системы на основании предоставленных учетных данных.

2.1.4 Учетные данные – информация, необходимая для идентификации пользователя в системе, включая логин и пароль, а также дополнительные элементы, такие как одноразовые коды или биометрические данные.

2.1.5 Роль пользователя – набор прав и привилегий, определяющий уровень доступа и функциональные возможности пользователя в автоматизированной системе.

2.1.6 Сессия – период времени, в течение которого пользователь находится в системе после успешной авторизации, в течение которого он может выполнять операции и взаимодействовать с ресурсами системы.

2.1.7 Безопасность данных – совокупность мер и процедур, направленных на защиту информации от несанкционированного доступа, утраты или повреждения в процессе авторизации и использования автоматизированной системы.

2.1.8 Аудит доступа – процесс мониторинга и анализа действий пользователей в системе с целью обеспечения безопасности и соблюдения установленных политик доступа.

2.1.9 Остальные термины и определения применены в значениях, указанных в действующей правовой и нормативно-технической документации, относящейся к информационным системам и безопасности данных.

2.2 В настоящих технических требованиях использованы сокращения:

АС – автоматизированная система;

АС АП – автоматизированная система авторизации пользователей;

АС УПД – автоматизированная система управления персональными данными;

АС БД – автоматизированная система баз данных;

АС ИБ – автоматизированная система информационной безопасности;

ИАС УД – информационно-аналитическая система управления данными.

ИАС – информационная аналитическая система;

ПД – персональные данные;

ПО – программное обеспечение;

РП – роль пользователя;

СУ – система управления доступом;

ТД – техническая документация.

# 3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ

## 3.1 Перечень и краткая характеристика бизнес-процессов

3.1.1. Объект автоматизации

Объектом автоматизации является система управления доступом пользователей к ресурсам информационных систем на основе процедур аутентификации и авторизации. Система обеспечивает безопасный и контролируемый доступ пользователей к данным и функциональным модулям в зависимости от их роли и прав доступа.

3.1.2. Уровни управления доступом

Управление доступом в системе авторизации осуществляется на трех уровнях:

* **административный уровень:** управление учетными записями, ролями и правами доступа. На этом уровне администраторы системы создают, редактируют и удаляют пользователей, а также назначают им роли и права доступа.
* **пользовательский уровень**: доступ пользователей к ресурсам системы в соответствии с их ролью и правами. Пользователи могут выполнять действия, разрешенные их ролью (например, просмотр данных, редактирование, удаление).
* **аудиторский уровень:** мониторинг и аудит действий пользователей. На этом уровне ведется журнал событий, фиксирующий все действия пользователей (например, вход в систему, изменение данных, попытки несанкционированного доступа).

3.1.3. Основные бизнес-процессы

Автоматизации подлежат следующие бизнес-процессы:

* регистрация пользователей: создание учетных записей новых пользователей с назначением ролей и прав доступа.
* аутентификация: проверка подлинности пользователя на основе логина и пароля.
* авторизация: предоставление доступа к ресурсам системы в зависимости от роли пользователя.
* управление учетными записями: редактирование и удаление учетных записей, сброс паролей, блокировка и разблокировка пользователей.
* восстановление доступа: сброс и восстановление пароля пользователя через email или sms.
* управление сессиями: контроль активности пользователей, автоматическое завершение сессии при отсутствии активности.
* аудит и мониторинг: ведение журнала событий для отслеживания действий пользователей и выявления подозрительной активности.

3.1.4. Предмет автоматизации

Предметом автоматизации является процесс управления доступом пользователей к ресурсам системы, включая:

* проверку подлинности пользователей (аутентификация).
* управление правами доступа (авторизация).
* ведение журнала событий для обеспечения безопасности и аудита.

3.1.5. Реализация системы авторизации

Реализация системы авторизации включает автоматизацию следующих взаимосвязанных бизнес-процессов:

* формирование учетных данных\*\*: создание и хранение учетных записей пользователей.
* проверка подлинности\*\*: аутентификация пользователей на основе логина и пароля.
* управление доступом\*\*: авторизация пользователей в зависимости от их роли и прав доступа.
* восстановление доступа\*\*: сброс и восстановление пароля пользователя.
* аудит и мониторинг\*\*: ведение журнала событий для отслеживания действий пользователей.

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

3.2.1. Входные данные

Входными данными для системы авторизации являются:

* учетные данные пользователя: логин и пароль для аутентификации.
* роли и права доступа: набор прав, назначенных пользователю в зависимости от его роли.
* данные для восстановления доступа: email или номер телефона для сброса пароля.
* журнал событий: данные о действиях пользователей (например, вход в систему, изменение данных).

3.2.2. Выходные данные

Выходными данными системы авторизации являются:

* результат аутентификации: успешный или неуспешный вход в систему.
* доступ к ресурсам: предоставление доступа к функциональным модулям и данным в зависимости от роли пользователя.
* журнал событий: записи о действиях пользователей (например, вход в систему, попытки несанкционированного доступа).

3.2.3. Формы представления данных

* учетные данные пользователя\*\*: логин и пароль в текстовом формате.
* роли и права доступа\*\*: табличный формат с указанием роли и списка прав доступа.
* журнал событий\*\*: табличный формат с указанием времени, пользователя и выполненного действия.

3.2.4. Формы представления выходных данных

Формой представления выходных данных с результатами работы системы авторизации являются:

* текстовый формат: данные о пользователях, их ролях и правах доступа представляются в виде таблицы.
* графический формат: визуализация данных о действиях пользователей (например, график активности пользователей за определенный период).

*таблица 3.1 – формат представления выходных данных*

|  |  |
| --- | --- |
| наименование параметра | формат представления |
| логин пользователя | текст (до 50 знаков) |
| роль пользователя | текст (до 20 знаков) |
| права доступа | список (до 100 знаков) |
| дата и время последнего входа | дата и время (формат: гггг-мм-дд чч:мм:сс) |
| статус учетной записи | текст (активна/заблокирована)| |
|  |  |

3.2.5. Формы представления промежуточных результатов

Промежуточные результаты работы системы авторизации могут быть представлены в виде:

* графиков активности пользователей: визуализация данных о количестве входов в систему, попытках несанкционированного доступа и других событиях.
* диаграмм распределения ролей\*\*: графическое представление распределения пользователей по ролям и правам доступа.

3.2.6. Источники получения входных данных

Источниками получения входных данных для системы авторизации являются:

* база данных пользователей: хранилище учетных записей пользователей, их ролей и прав доступа.
* система регистрации: данные о новых пользователях, зарегистрированных в системе.
* система аудита: журнал событий, фиксирующий действия пользователей (например, вход в систему, изменение данных).

3.2.7. Источники получения входных данных (параметров)

Источники получения входных данных для системы авторизации приведены в таблице 3.2.

*таблица 3.2 – источники получения входных данных (параметров)*

|  |  |
| --- | --- |
| наименование параметра | наименование информационной системы |
| учетные данные пользователя | база данных пользователей |
| роли и права доступа | система управления ролями |
| данные для восстановления доступа | система регистрации пользователей |
| журнал событий | система аудита и мониторинга |

## 3.3 Выполняемые технологические операции

Автоматизации подлежат технологические операции:

* сбор и обработка учетных данных пользователей, включая идентификацию пользователя и проверку его учетных данных;
* проверка и верификация учетных данных, включая аутентификацию пользователя и определение его прав доступа;
* управление сессиями пользователей, включая создание, обновление и завершение сессий;
* формирование выходного решения с результатами авторизации, включая информацию о статусе аутентификации и правах доступа пользователя.

4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС

## **4.1 Формулировка цели работы**

* Создание единой информационной системы для автоматизации процедур авторизации в автоматизированных процессах.
* Увеличение уровня цифровизации в управлении доступом и распределении пользовательских прав.
* Автоматизация проверки учетных данных и управления пользовательскими сессиями.
* Улучшение точности и надежности процесса аутентификации пользователей.
* Оптимизация нагрузки на сотрудников при обработке запросов на авторизацию и управлении доступом.

4.2 Область и условия применения АС  
АС АП создана для автоматизации авторизации пользователей в разнообразных автоматизированных системах, гарантируя безопасный доступ к данным и ресурсам.

4.3 Ограничения применения АС  
Для АС АП должно обеспечиваться функционирование:

* серверной части: в центре обработки данных на имеющихся технических средствах с учетом установленных операционных систем и действующих информационных систем;
* клиентской части: на рабочих местах пользователей с учетом установленных операционных систем, клиентского программного обеспечения (в том числе вариантов интернет-браузеров).

# 5 ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС

## 5.1 Требования к АС в целом

### АС АП необходимо разрабатывать на основе Web-технологий с использованием архитектуры «сервер – тонкий клиент», учитывая возможность адаптации к локальному программному обеспечению организации. Доступ пользователей к системе осуществляется через интернет-браузер, а взаимодействие с другими информационными системами обеспечивается через программный интерфейс API.

### 5.1.1 Требования к структуре и функционированию АС

5.1.1.1 Реализация функций АС АП обеспечивается функционированием подсистем:

* доступа и авторизации;
* информационного обеспечения и взаимодействия;
* управления сессиями и правами доступа;
* формирования выходных решений.

5.1.1.2 Обмен информацией между подсистемами АС АП и другими информационно-управляющими системами должен происходить через Единую сеть передачи данных организации.

5.1.1.3 Функционирование и обслуживание АС АП должно соответствовать нормам законодательства Республики Беларусь, а также внутренним нормативным актам организации в сфере информационной безопасности и информационных технологий.

5.1.2 Требования к защите информации от несанкционированного доступа  
5.1.2.1 Процедура доступа к АС АП должна учитывать многоуровневую реализацию доступа к служебной информации. Доступ к АС АП должен осуществляться на основании ввода учетных данных (имени пользователя и пароля), которые назначаются администраторами системы.

5.1.2.2 В АС АП должен быть предусмотрен программный интерфейс для автоматизации обмена данными с другими информационно-управляющими системами организации.

5.1.2.3 Разработка АС АП должна соответствовать следующим требованиям информационной безопасности:

* Доступ к данным системы осуществляется через механизмы авторизации и аутентификации пользователей.
* Учетные данные на сервере системы должны храниться в зашифрованном виде, соответствующем государственному стандарту симметричного шифрования и контроля целостности.
* Передача информации по сетевым каналам, включая беспроводные, должна происходить с использованием протоколов, поддерживающих шифрование данных.
* В системе необходимо предусмотреть функцию учета доступа пользователей.
* Обязательной является разработка функции регулярного резервного копирования базы данных системы.

5.1.3 Требования по сохранности информации при авариях  
Для АС АП необходимо предусмотреть процедуры копирования и защиты данных от разрушения в результате отказов, несанкционированного доступа и других катастрофических последствий. Эти процедуры должны включать регулярное резервное копирование данных и восстановление системы после сбоев, чтобы обеспечить непрерывность работы и защиту информации.

5.1.4 Требования к информационному обеспечению  
5.1.4.1 Информационное обеспечение АС АП представляет собой набор информационных массивов, образующих базу данных, содержащую сведения о пользователях, их ролях и правах доступа. Оно должно быть достаточным для выполнения функций, заданных техническими требованиями, а также обеспечивать возможность масштабирования для добавления новых функций.

5.1.4.2 Пользователи и события в АС АП должны быть однозначно идентифицированы с помощью формализованного обозначения. Формализация данных должна соответствовать требованиям цифровой обработки, обеспечивая уникальность каждой записи пользователя и его действий.

5.1.4.3 АС АП должна предусматривать ввод и корректировку данных администратором с последующим многократным использованием информации. Система также должна защищать данные от несанкционированного изменения со стороны пользователей.

5.1.4.4 Процесс поиска, извлечения, изменения и добавления данных в АС АП должен быть организован максимально быстро и удобно, исключая трудности в их интерпретации и восприятии.

5.1.4.5 Ввод нормативной и справочной информации, а также создание базы исходных данных должны быть реализованы на этапе разработки системы. Администратор должен иметь возможность корректировать и дополнять исходные данные с использованием встроенной системы автоматического обновления и синхронизации данных из пользовательской базы.

5.1.5 Требования к математическому обеспечению  
5.1.5.1 Математическое обеспечение должно обеспечивать реализацию перечисленных в данных технических требованиях функций, а также выполнение операций конфигурирования, программирования, управления базами данных пользователей и документирования.

5.1.5.2 Алгоритмы аутентификации и авторизации должны иметь возможность переконфигурирования и реализовываться через библиотечные блочные структуры, что позволит адаптировать систему под изменяющиеся требования безопасности.

5.1.6 Требования к программному обеспечению  
5.1.6.1 Организация поставки необходимого лицензионного программного обеспечения для обеспечения работы АС АП осуществляется заказчиком.

5.1.6.2 Программное обеспечение АС АП должно гарантировать беспрепятственное функционирование технических средств и других интегрированных систем.

5.1.6.3 ПО должно обеспечивать выполнение всех функций АС АП, включая процессы аутентификации пользователей, управление сессиями и защиту данных.

5.1.6.4 АС АП включает в себя серверную и клиентскую части программного обеспечения, разработанные в соответствии с настоящими техническими требованиями.

5.1.6.5 В процессе разработки программного обеспечения АС АП необходимо учитывать методологическую преемственность и опыт разработки аналогичных систем, что позволит обеспечить высокую надежность и качество.

5.1.6.6 Параметры качества программного обеспечения АС АП устанавливаются на этапе разработки и корректируются на основе данных опытной эксплуатации либо независимой экспертизы.

5.1.6.7 Помимо вышеперечисленных требований АС АП должна включать:

* процедуры оценки эффективности, включая время реакции системы, обработки входных и выходных данных;
* возможность освоения работы с системой без необходимости обращения к документации благодаря встроенным подсказкам и интуитивно понятному интерфейсу.

### 5.1.7 Требования к организационному обеспечению:

### 5.1.7.1 Эксплуатация АС АП должна быть организована таким образом, чтобы не требовался дополнительный персонал, за исключением временных затрат на техническое обслуживание и поддержку ее непрерывной работы.

### 5.1.7.2 Поддержка и сопровождение системы осуществляется инженерами и специалистами, ответственными за обеспечение работоспособности информационных систем организации, включая предоставление технической помощи и выполнение обновлений.

### 5.1.8 Требования к патентной чистоте

5.1.8.1 Исполнитель гарантирует патентную чистоту результатов выполнения работ, исключая наличие патентов, зарегистрированных в Республике Беларусь и других государствах, что позволяет избежать правовых споров.

5.1.8.2 По запросу Заказчика Исполнитель предоставляет информацию о рыночной стоимости объектов интеллектуальной собственности, созданных в рамках разработки и внедрения АС АП.

5.1.9 Требования к документированию  
5.1.9.1 Состав и перечень документов, предъявляемых по окончании соответствующих стадий и этапов разработки АС АП, определяется в соответствии с договором на разработку системы.

5.1.9.2 Вся разрабатываемая документация на АС АП оформляется в соответствии с действующими на организации нормативными документами.

5.1.9.3 К АС АП должны прилагаться инструкции для пользователей и системного администратора. Рабочая документация должна соответствовать требованиям нормативных документов организации.

5.2 Требования к функциям (задачам), выполняемым подсистемами  
**5.2.1 Подсистема «Доступ и авторизация» используется для:**

* выполнения аутентификации и авторизации пользователей в системе (уникальный логин, пароль, учет активности доступа);
* предоставления доступа к информации на трех уровнях:
  + **администратор**: полный доступ с возможностью управления базой данных и учетными записями;
  + **пользователь**: доступ без права внесения изменений;
  + **API**: взаимодействие с другими информационными системами.

5.2.2 Подсистема «Информационное обеспечение и взаимодействие» предназначена для:

* сбора и проверки данных, поступающих из других информационных систем, на соответствие актуальности и требованиям безопасности;
* локального ввода данных пользователями с обязательной проверкой и возможностью редактирования информации, полученной из взаимодействующих систем.

5.2.3 Подсистема «Исполнительские процессы и математическое обеспечение» выполняет:

* валидацию данных с приведением их в соответствие установленным стандартам обработки и требованиям безопасности;
* обработку и хранение учетных записей пользователей с учетом правил информационной защиты.

5.2.4 Подсистема «Формирование выходных решений» отвечает за:

* отображение результатов авторизации в текстовом и графическом форматах (например, статус аутентификации, права доступа, информация о текущей сессии);
* сохранение результатов авторизации в базе данных системы и экспорт данных в форматы, такие как xlsx и pdf.

6. СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА

6.1 Сроки реализации проекта устанавливаются в соответствии с календарным планом, который является приложением к договору на разработку АС АП.

6.2 Выполнение основных этапов разработки осуществляется на основании действующих нормативных документов.

6.3 Приемо-сдаточные испытания программного продукта и документации по каждому этапу разработки АС АП проводятся комиссией в соответствии с календарным планом, указанным в договоре.

6.4 Опытная эксплуатация АС АП проводится на технических ресурсах организации. После этого Заказчик определяет порядок и сроки ввода системы в промышленную эксплуатацию.

6.5 По итогам завершения каждого этапа работ результаты оформляются двухсторонним актом между Заказчиком и Исполнителем.

6.6 Завершение разработки сопровождается предоставлением Исполнителем документации на АС АП и проведением обучения администраторов и пользователей.

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