**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 Объектом автоматизации является система авторизации пользователей, обеспечивающая безопасный доступ к ресурсам автоматизированной системы на основе проверки учетных данных.

3.1.2 Процесс авторизации пользователей в автоматизированной системе осуществляется на трех уровнях:

- административном: управление доступом и правами пользователей;

- функциональном: определение ролей и привилегий для различных категорий пользователей;

- техническом: реализация механизмов аутентификации и защиты данных.

Процесс авторизации включает в себя:

- первичную авторизацию, устанавливающую учетные данные пользователя и его права доступа к системе;

- периодическую переавторизацию, направленную на подтверждение прав доступа пользователей через заданные интервалы времени;

- текущую авторизацию, обеспечивающую доступ к ресурсам системы в зависимости от состояния сессии пользователя и его активности.

3.1.3 Предметом автоматизации является методика проверки учетных данных пользователей, основанная на использовании различных методов аутентификации, таких как пароли, одноразовые коды и биометрические данные.

3.1.4 Процесс авторизации описывается алгоритмом, устанавливающим зависимость между предоставленными учетными данными и правами доступа пользователя к ресурсам системы. Аутентификация, основанная на проверке учетных данных, позволяет определить уровень доступа пользователя и его возможности взаимодействия с системой. На основе указанного алгоритма устанавливаются права доступа пользователя и его роль в системе.

3.1.5 Реализация процесса авторизации включает автоматизацию трех взаимосвязанных бизнес-процессов:

- сбор и обработка учетных данных пользователей;

- проверка и верификация учетных данных;

- управление правами доступа пользователей.

3.1.6 Сбор и обработка учетных данных пользователей осуществляется за счет реализации задач:

- создание и корректировка базы данных пользователей;

- получение и верификация (проверка на соответствие требованиям безопасности) учетных данных из других информационных систем.

3.1.7 Проверка и верификация учетных данных осуществляется за счет реализации задач:

- аутентификация пользователей на основе предоставленных учетных данных;

- определение уровня доступа пользователя в зависимости от его роли и прав.

3.1.8 Процесс управления правами доступа пользователей включает:

- назначение прав доступа для пользователей в зависимости от их ролей;

- формирование выходного решения с полученными результатами проверки прав доступа.

3.1.9 Обязательным условием функционирования процесса авторизации является предоставление пользователю доступа к системе до начала его работы. Минимальное время, в течение которого система должна определить и предоставить права доступа пользователю, составляет 1 минута относительно момента запроса авторизации.

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

3.2.1 Входными данными для процесса авторизации являются:

- учетные данные пользователя (логин и пароль);

- дополнительные элементы аутентификации (одноразовые коды, биометрические данные);

- информация о ролях и правах доступа пользователя;

- данные о состоянии сессии пользователя (например, время последней активности);

- параметры безопасности (например, IP-адрес, с которого осуществляется доступ).

3.2.2 Выходными данными процесса авторизации являются:

- результат проверки учетных данных (успешная или неуспешная аутентификация);

- информация о правах доступа пользователя в системе;

- данные о текущем состоянии сессии (время начала сессии, время последней активности);

- сообщения об ошибках (например, неверный логин или пароль).

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

- их идентифицировать;

- получать их численные значения или текстовые сообщения.

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

*Таблица 3.1* – Формат представления выходных данных

|  |  |
| --- | --- |
| **Наименование параметра** | **Формат представления** |
| Логин пользователя | Текст (до 50 знаков) |
| Результат аутентификации | Текст (успешно/неуспешно) |
| Роль пользователя | Текст (до 20 знаков) |
| Время начала сессии | Дата и время (формат: ГГГГ-ММ-ДД ЧЧ:ММ:СС) |
| Время последней активности | Дата и время (формат: ГГГГ-ММ-ДД ЧЧ:ММ:СС) |

3.2.5 Формой представления промежуточных результатов процесса авторизации является изображение, содержащее график активности пользователя (например, количество попыток входа в систему за определенный период времени).

3.2.6 Источниками получения входных данных (параметров) для процесса авторизации являются:

ИАС УД: в части получения сведений о пользователях и нормативно-справочной информации;

АС АП: в части получения данных о текущих сессиях пользователей;

АС УПД: в части получения информации о ролях и правах доступа пользователей;

АС ИБ: о действующих ограничениях доступа и предупреждениях для пользователей.

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

| **Наименование параметра** | **Наименование информационной системы** |
| --- | --- |
| Учетные данные пользователя | ИАС УД (база данных пользователей) |
| Роли и права доступа | АС УПД (информация о ролях и правах доступа) |
| Данные о текущих сессиях | АС АП (информация о сессиях пользователей) |
| Ограничения доступа | АС ИБ (информация о действующих ограничениях доступа) |

## 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**

* разработка интегрированной информационной системы для автоматизации процесса авторизации пользователей в автоматизированной системе;
* повышение уровня цифровизации процессов управления доступом и правами пользователей;
* автоматизация процесса проверки учетных данных и управления сессиями пользователей;
* повышение точности и надежности аутентификации пользователей;
* снижение нагрузки на работников в части обработки запросов на авторизацию и управление доступом.

4.2 Область и условия применения АС  
АС АП предназначена для автоматизации процесса авторизации пользователей в различных автоматизированных системах, обеспечивая безопасный доступ к ресурсам и данным.

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 должна разрабатываться на платформе Web-технологий по принципу «сервер – тонкий клиент» с учетом адаптации под локальное программное обеспечение организации.

Клиентский доступ к АС АП обеспечивается посредством интернет-браузера.

Доступ к АС АП 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 АП обеспечивается функционированием подсистем:

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

5.1.1.2 Информационный обмен между подсистемами АС АП, а также с другими информационно-управляющими системами должен осуществляться по Единой сети передачи данных организации.

5.1.1.3 Режимы функционирования и обслуживания АС АП должны соответствовать требованиям законодательства Республики Беларусь, а также локальным правовым актам организации 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 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 При разработке АС АП должны учитываться следующие требования к информационной безопасности:

* доступ к информации АС АП должен осуществляться через систему авторизации и аутентификации пользователей;
* хранение учетных данных на сервере АС АП должно осуществляться в зашифрованном виде согласно государственному стандарту симметричного шифрования и контроля целостности;
* передача информации по сети, в том числе по беспроводному каналу, должна осуществляться по протоколу с поддержкой шифрования данных;
* должна быть предусмотрена функция учета доступа к АС АП;
* должна быть разработана функция периодического резервного копирования (сохранения) базы данных АС АП.

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 совокупность массивов информации, составляющих базу данных о пользователях, ролях и правах доступа, используемых в системе. Информационное обеспечение должно быть достаточным для реализации заданных техническими требованиями функций и быть масштабируемым для внесения дополнительных функций.

5.1.4.2 Идентификация пользователей и событий в АС АП должна состоять в их однозначном формализованном обозначении. Формализация данных должна соответствовать требованиям эффективной цифровой обработки и обеспечивать уникальность каждого пользователя и его действий.

5.1.4.3 АС АП должна обеспечивать ввод и корректировку информации администратором, а также последующее многократное использование данных с защитой от несанкционированных изменений пользователями.

5.1.4.4 Поиск, извлечение, изменение и внесение необходимых данных в АС АП должны обеспечиваться наиболее быстрым способом, при этом не должны возникать трудности при их декодировании и восприятии.

5.1.4.5 Ввод нормативно-справочной информации и формирование базы исходных данных должны производиться на стадии разработки программного обеспечения. Корректировку и ввод дополнительных исходных данных должен осуществлять администратор с использованием предусмотренной подсистемы автоматического обновления (синхронизации) данных из базы данных пользователей.

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 Заказчик организует поставку необходимого лицензионного программного обеспечения для обеспечения функционирования АС АП.

5.1.6.2 Программное обеспечение АС АП не должно препятствовать бесперебойному функционированию технических средств и других интегрированных систем.

5.1.6.3 ПО должно быть достаточным для выполнения всех функций АС АП, включая аутентификацию пользователей, управление сессиями и защиту данных.

5.1.6.4 В состав АС АП должны входить серверная и клиентская части ПО с учетом настоящих технических требований на разработку.

5.1.6.5 В процессе разработки ПО АС АП должна соблюдаться методическая преемственность и опыт разработки смежных систем, что обеспечит высокое качество и надежность системы.

5.1.6.6 Качественные значения параметров ПО АС АП определяются в процессе разработки и уточняются по результатам опытной эксплуатации или независимой экспертизы.

5.1.6.7 Кроме вышеназванных требований для АС АП необходимо предусмотреть:

* процедуры оценки эффективности в части времени реакции и ответов, времени на подготовку и обработку входных и выходных данных;
* возможность освоения работы с АС АП без использования документации (с использованием функций подсказок и интуитивно понятного интерфейса).

### 5.1.7 Требования к организационному обеспечению

5.1.7.1 Функционирование АС АП не должно предусматривать дополнительного эксплуатационного персонала (кроме затрат человеко-часов, связанных с технической и иной поддержкой непрерывного функционирования программного обеспечения).

5.1.7.2 Сопровождение АС АП должно осуществляться инженерами и специалистами, причастными к поддержке информационных систем организации, обеспечивая необходимую техническую поддержку и обновления системы.

### 5.1.8 Требования к патентной чистоте

5.1.8.1 При выполнении работ Исполнителем обеспечивается патентная чистота результатов работ. Данная работа не должна содержать патентов, зарегистрированных в Республике Беларусь и других странах, что гарантирует отсутствие правовых конфликтов.

5.1.8.2 По требованию Заказчика Исполнитель представляет сведения о рыночной стоимости созданных при выполнении работ объектов интеллектуальной собственности, связанных с разработкой и внедрением 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» предназначена:**

* для аутентификации и авторизации пользователей в системе (уникальное имя пользователя, пароль, учет доступа);
* для доступа к информации на трех уровнях: администратор (полный доступ с правами администрирования базы данных и учетных данных пользователей); пользователь (без права внесения изменений); API (доступ для других информационных систем).

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

* сбор и проверка информации из взаимодействующих информационных систем на соответствие требованиям безопасности и актуальности;
* обеспечение локального ввода информации пользователем (с обязательной верификацией данных и возможностью корректировки информации, полученной из взаимодействующих информационных систем).

5.2.3 Подсистема «Исполнительские процессы и математическое обеспечение» предназначена для решения задач:

* валидация информации (приведение в соответствие требованиям безопасности и стандартам обработки данных);
* обработка и хранение учетных данных пользователей с учетом требований к защите информации.

5.2.4 Подсистема «Формирование выходных решений» предназначена для решения задач:

* представление результатов авторизации пользователю в текстовом и графическом формате (например, статус аутентификации, права доступа и информация о текущей сессии);
* сохранение результатов авторизации (в базе данных АС АП и экспорт в форматы xlsx, pdf).

# 6 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА

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

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 АП осуществляются комиссией в соответствии с календарным планом к договору.

6.4 На технических ресурсах организации проводится опытная эксплуатация АС АП. Затем Заказчиком должен быть решен вопрос о порядке и сроках внедрения и ввода АС АП в промышленную эксплуатацию.

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

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

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