**1. Введение**

Разработка автоматизированной системы аутентификации и авторизации (АС АА) обусловлена необходимостью повышения уровня безопасности и эффективности управления доступом к ресурсам организации. В современных условиях, когда объем данных и требования к их защите стремительно растут, традиционные методы аутентификации и авторизации уже не способны справляться с новыми вызовами. АС АА позволит оптимизировать процессы идентификации пользователей, свести к минимуму риск несанкционированного доступа и обеспечить надежную защиту информационных ресурсов.

Актуальность создания такой системы также продиктована требованиями к повышению производительности и уменьшению временных затрат на авторизацию пользователей. Интеграция современных методов безопасности, таких как двухфакторная аутентификация и шифрование данных, позволяет не только улучшить пользовательский опыт, но и гарантировать соответствие системы установленным международным и национальным стандартам информационной безопасности.

При реализации проекта используются современные подходы к разработке программного обеспечения, включая модульную архитектуру и возможность масштабирования. Это позволит не только решить текущие задачи, но и предусмотреть возможность расширения функционала системы в будущем. Данный подход соответствует положениям нормативной документации, включая СТП 09150.11.118-2009, что обеспечивает правовую и техническую основу для успешного внедрения системы.

Таким образом, АС АА станет неотъемлемой частью информационной инфраструктуры предприятия, способствуя достижению стратегических целей в области цифровизации и обеспечения безопасности. Ее создание направлено на долгосрочное развитие и укрепление устойчивости информационных систем в условиях быстро меняющегося технологического ландшафта.

**2. ОБЩИЕ СВЕДЕНИЯ**

**2.1 Наименование работы**

Разработка технических требований на автоматизированную систему аутентификации и авторизации (АС АА).

**2.2 Заказчик АС и Ответственный по проекту**

Заказчик АС — Государственное объединение «Белорусская железная дорога». Ответственный по проекту — служба технической политики и инвестиций Государственного объединения «Белорусская железная дорога».

**2.3 Наименование Организации-пользователя АС**

Государственное объединение «Белорусская железная дорога».

**2.4 Наименование объекта внедрения**

Управление Белорусской железной дороги.

**2.5 Термины определения и сокращения**

* *АС (Автоматизированная система*) – совокупность программно-аппаратных средств и алгоритмов, предназначенных для выполнения определённых задач без постоянного вмешательства человека.
* *АС АА (Автоматизированная система аутентификации и авторизации)* система, разработанная для управления процессами идентификации пользователей и предоставления им прав доступа к определённым ресурсам.
* *ИАС (Информационно-аналитическая система)* – система, предназначенная для сбора, анализа и визуализации данных, используемых для принятия управленческих решений.
* *ПО (Программное обеспечение)* – набор программ, выполняющих вычисления и управляющих техническими устройствами или процессами.
* *ИБ (Информационная безопасность)* – комплекс мер и технологий, направленных на защиту информации от несанкционированного доступа, уничтожения, изменения и других угроз.
* *ДФА (Двухфакторная аутентификация)* – метод идентификации пользователя, использующий два независимых элемента подтверждения личности, таких как пароль и одноразовый код.
* *НСИ (Нормативно-справочная информация)* – структурированная информация, которая используется для унификации процессов и данных в системах управления.

**3. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ**

**3.1 Назначение**

Автоматизированная система аутентификации и авторизации (АС АА) предназначена для решения ключевых задач, связанных с управлением доступом к информационным ресурсам Белорусской железной дороги. Система оптимизирует процессы идентификации пользователей, упрощая взаимодействие сотрудников с корпоративными и техническими платформами. Это особенно актуально для обеспечения бесперебойной работы бизнес-проектов, таких как управление расписанием движения поездов, мониторинг состояния объектов инфраструктуры и системы контроля энергетических затрат.

АС АА создаёт централизованное и защищённое цифровое пространство, где права доступа распределяются в соответствии с должностными обязанностями сотрудников. Это не только ускоряет выполнение задач, но и минимизирует риски утечек данных, что важно для проектов стратегического значения на железнодорожном транспорте, таких как внедрение новых технологий анализа перевозок и оптимизация топливно-энергетических ресурсов.

Кроме того, система поддерживает интеграцию с существующими автоматизированными решениями, такими как АС «Паспорт ОЖИ» и АС ПРЕД, что обеспечивает единую инфраструктуру для выполнения управленческих и технических задач. Это позволит достичь согласованности работы различных подразделений организации.

**3.2 Цели создания**

Повышение уровня информационной безопасности: Актуальные угрозы кибератак требуют усиленных мер защиты. АС АА гарантирует безопасность ключевых данных, таких как коммерческая информация, расписания движения поездов, энергетические показатели и оперативные сведения. Защита осуществляется через реализацию двухфакторной аутентификации, мониторинг действий пользователей и регулярное обновление алгоритмов безопасности.

Ускорение процесса идентификации пользователей: Одной из ключевых проблем железнодорожной отрасли является снижение времени на выполнение административных и технических процедур. АС АА автоматизирует процесс авторизации, позволяя сотрудникам быстрее получать доступ к необходимым данным и системам, таким как ИАС ПУРГП. Это особенно важно для повышения скорости принятия решений в экстренных ситуациях.

Уменьшение риска несанкционированного доступа: Система снижает вероятность проникновения злоумышленников, внедряя современные алгоритмы шифрования и управление доступом на основе ролей. Такие меры обеспечивают защиту как внутренних, так и внешних данных, что важно для проектов с большими объемами информации, таких как тяговые расчёты и анализ энергозатрат.

Обеспечение простоты использования системы для сотрудников организации: Удобство интерфейса и простота эксплуатации позволяют внедрить систему без необходимости длительного обучения персонала. Это особенно актуально в условиях высокой занятости сотрудников Белорусской железной дороги, работающих с проектами, такими как АС ПРЕД или ИРЦ, где требуется оперативное выполнение задач.

**4. ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ**

**4.1 Объекты, участвующие в системе**

* Серверы обработки данных;
* Клиентские устройства;
* Базы данных пользователей.

**4.2 Основные характеристики:**

* Серверы высокой производительности, поддерживающие шифрование данных.
* Клиентские устройства с функцией двухфакторной аутентификации.
* Базы данных с защищенными каналами передачи информации.

**5. ТРЕБОВАНИЯ К СИСТЕМЕ**

**5.1 Требования к структуре**

Описание общей архитектуры системы, включая серверную часть, клиентские приложения и интерфейсы.

**5.2 Требования к процедурам доступа к системе**

Особенности авторизации, включая двухфакторную аутентификацию и управление ролями.

**5.3 Требования к функциональной безопасности**

Меры, предотвращающие сбои системы и обеспечивающие её бесперебойную работу.

**5.4 Требования к информационной безопасности**

Описание криптографических методов защиты, управление паролями и защита данных.

**5.5 Требования к патентной чистоте**

Подтверждение отсутствия нарушений прав интеллектуальной собственности.

**6. ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ**

**6.1 Требования к информационному обеспечению АС АА должна включать:**

* Данные о пользователях (персональная информация, роли, доступы).
* Лог-файлы, фиксирующие операции системы, включая данные о входах и выходах пользователей.
* Нормативно-справочную информацию для унификации процессов и данных.

Для защиты данных должны применяться резервное копирование и системы восстановления после сбоев. Должен быть обеспечен доступ к данным только авторизованным пользователям через криптографические методы.

**6.2 Требования к математическому обеспечению Алгоритмы, используемые в АС АА, должны включать:**

* Метод двухфакторной аутентификации, использующий независимые элементы проверки (пароль и одноразовый код).
* Алгоритмы управления доступом на основе ролей (RBAC).
* Криптографические методы шифрования данных (AES, RSA).

Обновление математических моделей должно происходить регулярно, чтобы соответствовать современным требованиям информационной безопасности.

6.3 Требования к программному обеспечению АС АА должна поддерживать:

* Серверные приложения для обработки данных аутентификации и авторизации.
* Клиентские приложения, совместимые с основными операционными системами (Windows, Linux, Android).
* Облачные технологии для масштабируемости и обеспечения быстродействия.
* Мониторинг действий пользователей и генерацию отчетов о доступе.

ПО должно быть сертифицировано и соответствовать стандартам международной и национальной информационной безопасности.

**6.4 Требования к техническому обеспечению АС АА должна быть внедрена на:**

* Высокопроизводительных серверах, поддерживающих функции резервного копирования и шифрования.
* Клиентских устройствах, поддерживающих двухфакторную аутентификацию.
* Надежных сетевых компонентах, обеспечивающих защищенную передачу данных.

Все оборудование должно быть протестировано на совместимость и устойчивость к внешним воздействиям.

**6.5 Требования к организационному обеспечению**

* Регламент работы АС АА должен быть разработан в соответствии с национальными и международными стандартами безопасности.
* Потребуется обучение сотрудников для использования системы и предотвращения потенциальных нарушений.
* Разработаны инструкции для штатного и аварийного использования системы.

**7. СОСТАВ И СОДЕРЖАНИЕ РАБОТ**

АС АА должна быть разработана в несколько этапов:

1. *Планирование:*

* Определение объема работы, требований заказчика, подготовка технического задания.

1. *Проектирование:*

* Разработка архитектуры системы, включая серверную часть, клиентские приложения и интерфейсы.
* Моделирование алгоритмов безопасности.

1. *Тестирование:*

* Проверка системы на уязвимости.
* Тестирование на совместимость с существующими системами (например, АС «Паспорт ОЖИ»).

1. *Внедрение:*

* Установка оборудования и ПО.
* Проведение обучающих семинаров для сотрудников.
* Постановка системы на эксплуатацию.

**8. ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ**

Процедура приемки должна включать:

1. Проведение функционального тестирования, проверка соответствия системы техническим требованиям.
2. Тестирование безопасности (включая двухфакторную аутентификацию и управление ролями).
3. Создание отчетов о тестировании, указание выявленных проблем и способов их устранения.
4. Финальное утверждение системы заказчиком после демонстрации её работы.
5. Подписание акта приемки оборудования и ПО в эксплуатацию.

**9. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ**

Документация должна включать:

1. *Техническое описание:*

* Спецификация архитектуры системы.
* Детализация алгоритмов аутентификации и шифрования.

1. *Руководство пользователя:*

* Инструкции по работе с интерфейсом.
* Описание процедур авторизации и восстановления доступа.

1. *Инструкции для администратора:*

* Регламент обновлений и резервного копирования.
* Процедуры настройки системы.

1. *Отчеты о тестировании:*

* Результаты тестов на функциональность и безопасность.
* Планы устранения выявленных проблем.