Управление транспортной системы авторизации и управления доступом

(наименование объекта автоматизации)

3

(класс автоматизированной системы)

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ**

**К РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АВТОРИЗАЦИИ И УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ ТРАНСПОРТНЫЪХ УСЛУГ**

**(АС АУДТ)**

На 13 листах

**ОГЛАВЛЕНИЕ**

[1 ОБЩИЕ СВЕДЕНИЯ 3](#_Toc3598)

[2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ 3](#_Toc11397)

[3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ 4](#_Toc11749)

[3.1 Перечень и краткая характеристика бизнес-процессов 4](#_Toc7081)

[3.2 Требования к входным и выходным данным, формам их представления 6](#_Toc9250)

[3.3 Выполняемые технологические операции 8](#_Toc24339)

[4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС 9](#_Toc5149)

[4.1 Формулировка цели разработки 9](#_Toc23196)

[4.2 Область и условия применения АС 9](#_Toc20667)

[4.3 Ограничения применения АС 9](#_Toc25144)

[5 ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС 10](#_Toc8226)

[5.1 Требования к АС в целом 10](#_Toc25973)

[5.1.1 Требования к структуре и функционированию АС 10](#_Toc21947)

[5.1.2 Требования к защите информации от несанкционированного доступа 10](#_Toc19422)

[5.1.3 Требования по сохранности информации при авариях 11](#_Toc15747)

[5.1.4 Требования к информационному обеспечению 11](#_Toc12695)

[5.1.5 Требования к математическому обеспечению 11](#_Toc27333)

[5.1.6 Требования к программному обеспечению 11](#_Toc28072)

[5.1.7 Требования к организационному обеспечению 12](#_Toc19883)

[5.1.8 Требования к патентной чистоте 12](#_Toc22480)

[5.1.9 Требования к документированию 12](#_Toc20039)

[5.2 Требования к функциям (задачам), выполняемым подсистемами 12](#_Toc12768)

[6 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА 13](#_Toc24840)

**1 ОБЩИЕ СВЕДЕНИЯ**

* 1. Наименование работы: разработка технических требований на автоматизированную систему авторизации и управления доступом для транспортных услуг (АС АУДТ).

1.2 Заказчик - Министерство транспорта Республики Беларусь. Ответственный - Департамент информационных технологий Министерства транспорта.

1.3 Организации-пользователи АС: Государственные и коммерческие транспортные компании (автоперевозчики, логистические операторы, авиа- и ж/д перевозчики).

1.4 Объект внедрения: Централизованная система управления доступом к транспортным услугам и ресурсам.

**2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ**

2.1 В настоящих технических требованиях применены термины и

определения в следующем значении:

* + 1. Автоматизированная система (АС)  - комплекс программно-аппаратных средств, предназначенный для автоматизации процессов управления транспортными услугами, включая авторизацию пользователей, контроль доступа к транспортным средствам (ТС), маршрутизацию и мониторинг выполнения перевозок.
    2. Авторизация -процесс проверки прав пользователя (водителя, диспетчера, клиента) на выполнение определенных действий в системе, таких как доступ к управлению ТС, просмотр маршрутов или внесение изменений в заказы.
    3. Аутентификация  - процедура подтверждения личности пользователя при входе в систему посредством:
    4. Транспортная услуга -услуга, связанная с перевозкой пассажиров или грузов, включая:
    5. Пользователь системы -физическое или юридическое лицо, взаимодействующее с АС:
    6. Администратор  - настраивает систему, управляет правами доступа.
    7. Транспортное средство (ТС) -автомобиль, автобус, грузовик, спецтехника или иной вид транспорта, подключенный к системе для мониторинга и управления.
    8. Маршрутизация  - автоматическое построение оптимальных маршрутов с учетом:
    9. Телематика ТС - сбор и передача данных о местоположении, скорости, расходе топлива и технических параметрах ТС через GPS/ГЛОНАСС и датчики.
    10. Безопасность данных - защита информации от утечек, включая:

2.2 В настоящих технических требованиях использованы сокращения:

АС - автоматизированная система.

АС АУДТ - автоматизированная система авторизации и управления доступом для транспортных услуг.

API - программный интерфейс приложения; средство взаимодействия между компонентами системы, например, между клиентским приложением и серверной частью.

БД - база данных; структурированное хранилище данных, используемое системой для сохранения информации о пользователях, заказах и услугах.

ПО - программное обеспечение; включает все приложения и программы, обеспечивающие работу системы.

СУБД - система управления базами данных; программный инструмент для работы с базами данных, их создания, управления и обработки запросов.

ТЗ - техническое задание; документ, описывающий требования к системе, её функциональность и технические характеристики.

ТС - Транспортное средство.

**3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ**

## Перечень и краткая характеристика бизнес-процессов

* + 1. Объектом автоматизации является система авторизации и управления доступом для транспортных услуг, обеспечивающая: Контроль доступа водителей и диспетчеров к транспортным средствам (ТС). Управление правами пользователей в системах мониторинга транспорта (GPS/ГЛОНАСС). Интеграцию с платформами бронирования и логистическими сервисами.
    2. Процесс авторизации осуществляется на трех основных уровнях:

3.1.2.1 Административный уровень: Управление учетными записями водителей, диспетчеров, клиентов. Настройка прав доступа к ТС (например, ограничение запуска двигателя без авторизации).

3.1.2.2 Функциональный уровень: Распределение ролей (водитель, диспетчер, клиент, техник). Назначение прав для каждой роли (просмотр маршрутов, управление ТС, доступ к телематике).

3.1.2.3 Технический уровень:

Механизмы аутентификации: логин/пароль, OTP-коды, RFID-карты, биометрия. Шифрование данных GPS и параметров ТС.

3.1.3 Предметом автоматизации является методика проверки и обработки учетных данных пользователей. Для этого применяются такие методы, как стандартные пароли, одноразовые коды и биометрические данные.

3.1.4 Методы аутентификации

3.1.4.1 Для водителей: RFID-карты или брелоки для разблокировки ТС. Мобильное приложение с QR-кодами.

3.1.4.2 Для диспетчеров: Двухфакторная аутентификация (SMS + пароль).

3.1.4.3 Аварийный доступ: Временные коды для сервисных бригад.

3.1.5 Алгоритм авторизации:

Водитель вставляет RFID-карту в считыватель или вводит код в мобильном приложении.

Система проверяет:

* + Соответствие карты/кода базе данных.
  + Наличие прав на управление данным ТС.
  + Актуальность страховки/техосмотра.

При успешной проверке:

* + Разблокируется зажигание.
  + Загружается персональный профиль (настройки сиденья, маршруты).
    1. Ключевые бизнес-процессы

Управление доступом к ТС:

* + Авторизация водителей перед запуском двигателя.
  + Дистанционная блокировка ТС при утере ключа.

Мониторинг активности:

* + Фиксация времени работы водителя (согласно трудовому законодательству).
  + Контроль соблюдения маршрутов.

Интеграция с логистическими системами:

* + Автоматическая выгрузка данных о рейсах в 1С/TMS.

3.1.7 Требования к скорости и безопасности

* Время авторизации: не более 15 секунд (критично для коммерческого транспорта).
* Защита данных:
  + Шифрование GPS-треков (AES-256).
  + Регулярный аудит прав доступа.

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

3.2.1 Входными данными, которые используются для процесса авторизации в системе транспортных услуг, являются:

- Учетные данные пользователя: Логин и пароль (для диспетчеров и администраторов). Идентификатор RFID-карты или мобильного устройства (для водителей). Биометрические данные (отпечаток пальца, сканирование лица - опционально)

- Данные транспортного средства: VIN-номер или гос. номер ТС. Текущее местоположение (GPS/ГЛОНАСС координаты). Техническое состояние (данные с бортовых датчиков)

- Дополнительные параметры доступа: Временные одноразовые коды (для аварийного доступа). Цифровая подпись (для юридически значимых операций). IP-адрес терминала доступ;

- Контекстные данные: График работы водителя. Назначенные маршруты. Текущие заказы

3.2.2 Выходными данными, генерируемыми в процессе авторизации, являются:

- Статус авторизации: Успешная/неуспешная аутентификация. Код ошибки (при неудачной попытке);

- Права доступа: Разрешенные операции (управление ТС, просмотр маршрутов и т.д.). Ограничения (зональные, временные);

- Сессионные данные: Время начала сессии. Предполагаемое время окончания (с учетом графика). Таймер неактивности (для автоматического завершения);

- Технические параметры: Уровень доступа к телематике. Настройки бортового оборудования.

3.2.3 Форматы представления данных

Данные должны быть представлены в структурированных форматах:

* + - Для автоматизированной обработки: JSON/XML для интеграции с другими системами. Protobuf для обмена данными с бортовыми устройствами
    - Для визуализации: HTML-панели для диспетчерских центров. Упрощенные интерфейсы для мобильных устройств данных, необходимую для дальнейшего анализа и принятия решений.

3.2.4 Выходные данные представляются в текстовом формате, содержащем параметры проверки и результаты авторизации. Пример формата данных приведён в таблице 3.1.

Таблица 3.1 -Формат представления выходных данных

| **Параметр** | **Формат** | **Пример** |
| --- | --- | --- |
| ID сессии | UUID | 550e8400-e29b-41d4-a716-446655440000 |
| Статус | Текст (success/error) | success |
| ID водителя | Число (int) | 142857 |
| Привязанное ТС | Текст (VIN) | XTA210990Y2765432 |
| Уровень доступа | Перечисление (driver/dispatcher/admin) | driver |
| Время начала | ISO 8601 | 2024-03-15T08:30:45+03:00 |
| Время окончания | ISO 8601 | 2024-03-15T17:45:00+03:00 |
| Ограничения | JSON-массив | {"zones": ["M1", "K5"], "speed\_limit": 90} |

* + 1. Визуализация данных

- Для мониторинга используются: Heat-карты активности водителей. Графики попыток несанкционированного доступа. Диаграммы загрузки транспортных средств

3.2.6 Источники входных данных

Основные системы-источники:

* + - Транспортный реестр (АС ТР): База данных зарегистрированных ТС. История технического обслуживания
    - Система управления автопарком (FMS): Распределение ТС по водителям. Графики работы
    - Навигационная платформа (АС МТ): Текущие координаты. Данные датчиков
    - Система безопасности (АС БДТ): Журнал инцидентов. Черные списки

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

Таблица 3.2 -Источники получения входных данных (параметров)

| **Параметр** | **Источник данных** |
| --- | --- |
| Учетные данные водителя | HR-система (АС "Кадры") |
| Данные ТС | Транспортный реестр (АС ТР) |
| Текущее местоположение | Навигационная система (АС МТ) |
| График работы | Система планирования (АС "График") |
| Права доступа | Система безопасности (АС БДТ) |
| Технические параметры | Система диагностики (АС "Техсостояние") |

## 3.3 Выполняемые технологические операции

Процесс автоматизации включает выполнение следующих технологических операций:

- сбор и обработка учетных данных пользователей: идентификация пользователя и проверка предоставленных данных на соответствие требованиям безопасности;

- проверка и верификация учетных данных: аутентификация пользователя, включая использование паролей, биометрических данных или одноразовых кодов;

- управление сессиями пользователей: создание новых сессий, обновление данных по активности и завершение сессий при отсутствии активности или по запросу пользователя;

- формирование выходного решения: предоставление данных о статусе аутентификации, правах доступа и состоянии сессии пользователя.

**4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС**

## 4.1 Формулировка цели разработки

Основными целями создания автоматизированной системы авторизации и управления доступом для туристических услуг (АС АУДТ) являются:

- Разработка интегрированной платформы для: Управления доступом водителей, диспетчеров и клиентов к транспортным средствам и логистическим сервисам. Автоматизации процессов авторизации с учетом отраслевых требований (например, контроль техосмотра, страховки, графика работы);

- Повышение безопасности и прозрачности транспортных операций за счет: Многофакторной аутентификации (RFID, биометрия, OTP-коды). Контроля несанкционированного доступа к ТС (блокировка двигателя при попытке угона). Шифрования данных телематики и персональных данных пользователей;

- Оптимизация логистических процессов через: Интеграцию с системами мониторинга транспорта (GPS/ГЛОНАСС). Автоматическое распределение прав доступа в зависимости от маршрута и графика. Снижение времени простоя ТС за счет ускоренной авторизации (≤15 секунд);

- Снижение операционных издержек за счет: Уменьшения manual-процессов (ручная проверка документов водителей). Автоматического формирования отчетов для контролирующих органов. Минимизации рисков, связанных с человеческим фактором;

- Обеспечение масштабируемости системы для: Поддержки растущего парка ТС. Интеграции с внешними сервисами (платежные системы, государственные реестры).

## Область и условия применения АС

## Система предназначена для: Коммерческого транспорта: грузоперевозки, пассажирские перевозки (такси, автобусы). Логистических компаний: управление автопарком, контроль доступа к грузам. Сервисных центров: аварийный доступ к ТС для ремонта.

## Ограничения применения АС

Технические: Требуется совместимое бортовое оборудование (RFID-считыватели, датчики). Обязательная интеграция с системами навигации.

Организационные: Обучение персонала (водителей, диспетчеров). Юридическая поддержка (соответствие законам о персональных данных).

Экономические: Затраты на внедрение для малых автопарков.

**5 ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС**

## Требования к АС в целом

АС АУДТ разрабатывается на основе **микросервисной архитектуры** с использованием современных Web-технологий, что обеспечивает:

* + - Масштабируемость – возможность увеличения нагрузки при росте парка ТС
    - Кросс-платформенность – доступ с любых устройств (ПК, планшеты, бортовые терминалы)
    - Гибкость интеграции – поддержка API для подключения внешних систем (логистические платформы, ГЛОНАСС-трекеры)

Клиентский доступ:

* + - Веб-интерфейс для диспетчеров и администраторов
    - Мобильное приложение для водителей (Android/iOS)

- Light-версия для бортовых терминалов с ограниченным функционалом.

### 5.1.1 Требования к структуре и функционированию АС

5.1.1.1 Реализация функций АС АУДТ обеспечивается функционированием подсистем:

- Подсистема доступа и авторизации: Многофакторная аутентификация (RFID + PIN-код). Биометрическая верификация (по требованию). Контроль доступа к ТС по расписанию

- Подсистема информационного обмена: Интеграция с ГАИ (проверка водительских прав). Подключение к системам телематики (GPS/ГЛОНАСС). Обмен данными с логистическими платформами

- Подсистема управления сессиями: Автоматическое завершение сессии при простое. Контроль рабочего времени водителей. Удаленная блокировка ТС при утере ключа.

- Подсистема отчетности: Формирование журналов доступа. Анализ нарушений режима работы. Интеграция с бухгалтерскими системами

* + - 1. Безопасность передачи данных: Обязательное использование TLS 1.3+ для всех соединений. Двухуровневое шифрование для телематических данных. Резервный канал связи через SMS-команды
      2. Соответствие стандартам: Требованиям СТБ 34.101.45 (Беларусь). Директивам GDPR (для международных перевозок). Отраслевым стандартам ISO 39001 (безопасность дорожного движения)
    1. Требования к защите информации от несанкционированного доступа  
       5.1.2.1 Многоуровневая аутентификация: Для водителей: RFID-карта + PIN-код (4-6 цифр). Для диспетчеров: Логин/пароль + SMS-код. Для администраторов: Биометрия (отпечаток пальца/распознавание лица) + аппаратный токен. Критичные операции (изменение маршрутов, блокировка ТС) требуют подтверждения двумя сотрудниками
       1. Хранение учетных данных: Пароли хранятся в виде хешей (алгоритм Argon2id). Биометрические шаблоны - в изолированном secure enclave. Ключи шифрования: AES-256 для данных, ECC-384 для TLS. Сертифицированные аппаратные модули безопасности (HSM) для хранения мастер-ключей
       2. Защита передачи данных: Обязательное использование TLS 1.3 с PFS (Perfect Forward Secrecy). Дополнительное шифрование GPS-треков (протокол SIGFOX). Квантово-устойчивые алгоритмы для долгосрочной защиты данных
       3. Система мониторинга: Журналирование всех событий в immutable-хранилище. AI-анализ аномалий (необычные маршруты, множественные попытки доступа). Автоматические алерты при подозрительной активности. Интеграция с SIEM-системами (например, IBM QRadar)

5.1.3 Требования по сохранности информации при авариях  
 - Геораспределенный кластер БД (минимально 3 ноды в разных ЦОД)

- Режимы восстановления: Hot-standby для критичных компонентов (переключение <1 мин). Ежечасные инкрементные бэкапы + ежедневные полные

- Аварийные сценарии: Автоматическое переключение на резервный ЦОД. Локальное кэширование данных в бортовых терминалах (до 72 часов)

- Тестирование - ежеквартальные учения по восстановлению

5.1.4 Требования к информационному обеспечению  
5.1.4.1 Должна быть создана масштабируемая база данных, содержащая информацию о пользователях, ролях и правах доступа.

5.1.4.2 Все данные о действиях пользователей должны быть уникально идентифицированы и защищены от несанкционированного изменения.

5.1.4.3 Администраторы системы обеспечивают ввод, корректировку и актуализацию данных.

### 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 системы должны быть адаптивными, поддерживать переконфигурирование в условиях изменения требований безопасности и предоставлять гибкость для масштабирования.

5.1.6 Требования к программному обеспечению  
5.1.6.1 Программное обеспечение должно поддерживать все функции АС АУДТ, включая авторизацию, управление сессиями и обработку данных пользователей.

5.1.6.2 Операционная часть системы должна включать серверную и клиентскую составляющие, совместимые с актуальными браузерами и платформами.

5.1.6.3 Интерфейс системы должен быть интуитивно понятным для туристов.

### 5.1.7 Требования к организационному обеспечению

5.1.7.1 Функционирование системы не требует привлечения дополнительного персонала, кроме стандартной технической поддержки.

5.1.7.2 Обновление системы выполняется специалистами в области информационных технологий организации.

### 5.1.8 Требования к патентной чистоте

5.1.8.1 При разработке и внедрении АС АУДТ должна быть обеспечена патентная чистота, исключающая использование чужих объектов интеллектуальной собственности.

5.1.8.2 Исполнитель предоставляет сведения о рыночной стоимости транспортных услуг, оказываемых в рамках выполнения договора.

### 5.1.9 Требования к документированию

5.1.9.1 Состав и перечень документов по завершении этапов оказания транспортных услуг определяются договором с заказчиком.

5.1.9.2 Вся документация оформляется в соответствии с нормативными требованиями организации.

5.1.9.3 Система сопровождается инструкциями для пользователей (клиентов, партнёров и администраторов) и логистических операторов.

## 5.2 Требования к функциям (задачам), выполняемым подсистемами

5.2.1 Подсистема «Доступ и авторизация»:

- обеспечивает аутентификацию и авторизацию клиентов, партнёров и администраторов;

- предоставляет доступ к информации на трёх уровнях: клиенты, партнёры и администраторы.

5.2.2 Подсистема «Информационное обеспечение и взаимодействие»:

- взаимодействие с логистическими платформами для получения данных о заказах и маршутах;

- проверка вводимых данных на корректность и соответствие требованиям безопасности.

5.2.3 Подсистема «Исполнительские процессы и математическое обеспечение»:

- валидация данных пользователей в соответствии со стандартами безопасности;

- надёжное хранение данных о транспортировках с применением шифрования.

5.2.4 Подсистема «Формирование выходных решений»:

- Предоставление результатов обработки данных в текстовом и графическом формате (отчеты, накладные, маршрутные листы);

- сохранение результатов авторизации в базе данных или экспорт данных для логистического анализа.

**6 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА**

6.1 Сроки выполнения проекта устанавливаются в соответствии с календарным планом, который является приложением к договору между Заказчиком и Исполнителем.

6.2 Основные этапы разработки выполняются в строгом соответствии с нормативными документами, регулирующими проектирование, тестирование и внедрение информационных систем в транспортных и логистических услуг.

6.3 Приемо-сдаточные испытания, направленные на проверку работоспособности программного продукта и соответствующей документации, проводятся комиссией на каждом этапе разработки. Испытания осуществляются в соответствии с календарным планом, закреплённым в договоре.

6.4 На технических ресурсах организации проводится опытная эксплуатация АС АУДТ для проверки системы в условиях реальной работы. После завершения испытаний Заказчик принимает решение о порядке и сроках внедрения системы в промышленную эксплуатацию.

6.5 Результаты завершённых этапов разработки оформляются в виде двухстороннего акта, подписываемого Заказчиком и Исполнителем. Это гарантирует прозрачность и согласованность выполнения проекта.

6.6 После завершения разработки Исполнитель передаёт Заказчику полную техническую и пользовательскую документацию на АС АУДТ. Также проводится обучение администраторов и пользователей системы для обеспечения эффективного использования и администрирования платформы.

**НАСТОЯЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ МОГУТ БЫТЬ УТОЧНЕНЫ И КОРРЕКТИРОВАНЫ ПО ВЗАИМНОЙ ДОГОВОРЕННОСТИ МЕЖДУ ЗАКАЗЧИКОМ И ИСПОЛНИТЕЛЕМ В РАБОЧЕМ ПОРЯДКЕ.**