**1 ОБЩИЕ СВЕДЕНИЯ**

1.1 Наименование работы: разработка технических требований на автоматизированную систему аутентификации и авторизации пользователей спорткомплекса (АС ААП).

1.2 Заказчик АС и Ответственный по проекту

Заказчик АС – Администрация спортивного комплекса «Олимп»;

Ответственный по проекту – отдел информационных технологий Администрации спортивного комплекса «Олимп».

1.3 Наименование Организации-пользователя АС: Администрация спортивного комплекса «Олимп».

1.4 Наименование объекта внедрения: спортивный комплекс «Олимп».

**2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ**

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

2.1.1 **Автоматизированная система аутентификации и авторизации (АС ААП)** – программно-аппаратный комплекс, предназначенный для идентификации, аутентификации и управления правами доступа пользователей к ресурсам спорткомплекса.

2.1.2 **Аутентификация** - процедура проверки подлинности пользователя на основании предоставленных учетных данных (логин, пароль, электронный ключ, биометрические данные).

2.1.3 **Авторизация** - процесс определения прав доступа пользователя к ресурсам спорткомплекса (тренажерные залы, бассейны, зоны отдыха) в соответствии с его ролью.

2.1.4 **Пользователь** - физическое лицо (посетитель, сотрудник, администратор), имеющее учетную запись в системе АС ААП.  
2.1.5 **Роль пользователя** - набор привилегий, определяющих уровень доступа к функционалу и данным спорткомплекса (например: «гость», «тренер», «администратор»).

2.1.6 **Электронный пропуск** – уникальный идентификатор (карта, браслет, мобильное приложение), используемый для аутентификации и доступа на территорию спорткомплекса.

2.1.7 Остальные термины и определения применены в значениях, указанных в нормативной документации спортивного комплекса «Олимп».

2.2 В настоящих технических требованиях использованы сокращения:

АС – автоматизированная система;  
АС ААП – автоматизированная система аутентификации и авторизации пользователей;

ИС – информационная система;

СУБД – система управления базами данных;

API – интерфейс программирования приложений;

ПО – программное обеспечение;

БД – база данных;

OTP – одноразовый пароль (One-Time Password).

СКУД - Система контроля и управления доступом.

**3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ**

**3.1 Перечень и краткая характеристика бизнес-процессов**

3.1.1 **Объект автоматизации** - система управления доступом пользователей к ресурсам спортивного комплекса «Олимп» на основе автоматизированной аутентификации и авторизации.

3.1.2 **Уровни управления доступом**:

* **Административный уровень**:
  + Управление ролями и правами доступа (настройка ролей: «гость», «тренер», «администратор», «технический персонал»).
  + Контроль безопасности: блокировка учетных записей, настройка политик паролей.
* **Функциональный уровень**:
  + Интеграция с зональными системами (бассейн, тренажерные залы, раздевалки).
  + Управление расписанием занятий и бронированием зон.
* **Операционный уровень**:
  + Обработка запросов на доступ в режиме реального времени через турникеты, электронные замки, мобильные приложения.

3.1.3 **Предмет автоматизации** включает:

* Механизмы аутентификации:
  + Многофакторная проверка (пароль + SMS-код, биометрия + электронный пропуск).
  + Интеграция с внешними системами (например, банковские приложения для оплаты абонементов).
* Динамическую авторизацию:
  + Автоматическое назначение временных прав (например, доступ в VIP-зону на 1 час).
  + Ограничение доступа при нарушении правил (просроченный абонемент, попытка несанкционированного входа).

3.1.4 **Алгоритм работы АС ААП** базируется на модели **RBAC (Role-Based Access Control) (управление доступом на основе ролей)** и включает:

* Проверку актуальности абонемента через интеграцию с CRM-системой.
* Сопоставление роли пользователя с расписанием занятий (например, доступ тренера только в зал №3 с 08:00 до 20:00).

3.1.5 **Автоматизируемые бизнес-процессы**:

1. **Регистрация и верификация пользователей**:
   * Сбор персональных данных (ФИО, контакты, фото).
   * Верификация через SMS или email.
   * Синхронизация с базой данных абонементов.
2. **Аутентификация**:
   * Распознавание электронных пропусков (NFC-карты, браслеты).
   * Сканирование QR-кодов в мобильном приложении.
   * Биометрическая идентификация (отпечатки пальцев, распознавание лица).
3. **Авторизация**:
   * Проверка прав доступа к запрашиваемой зоне.
   * Динамическое изменение прав (например, продление абонемента через мобильное приложение).
4. **Формирование отчетности**:
   * Ежедневные отчеты о посещаемости.
   * Анализ попыток несанкционированного доступа.

3.1.6 **Регистрация пользователей** включает:

* Заполнение анкеты в мобильном приложении или на терминалах в холле спорткомплекса.
* Автоматическую генерацию электронного пропуска (виртуального или физического).
* Интеграцию с платежными системами для активации абонемента.

3.1.7 **Аутентификация** поддерживает:

* **Одноразовые пароли** для гостей.
* **Биометрию** для постоянных клиентов (снижение риска передачи пропусков третьим лицам).
* **Экстренную блокировку** пропусков через административную панель.

3.1.8 **Управление ролями** предусматривает:

* Гибкое назначение прав (например, доступ тренера к служебным помещениям).
* Автоматическую деактивацию временных пропусков (гостевые визиты, разовые мероприятия).

3.1.9 **Ключевое требование**: время обработки запроса на доступ не должно превышать **2 секунды** с момента предъявления пропуска.

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

3.2.1 **Входные данные**:

* **Учетные данные пользователя**:
  + Логин, пароль, одноразовый пароль.
  + Уникальный идентификатор электронного пропуска (NFC-метка, QR-код).
* **Контекстные данные**:
  + Расписание занятий (интеграция с системой бронирования).
  + Статус абонемента (активен/заблокирован/просрочен).
* **Биометрические шаблоны**:
  + Цифровые отпечатки пальцев.
  + Фотографии для распознавания лиц (разрешение не менее 720p).

3.2.2 **Выходные данные**:

* **Результат аутентификации**:
  + «Доступ разрешен» + информация о зоне доступа.
  + «Доступ запрещен» + причина (просроченный абонемент, неверный код).
* **Журнал событий**:
  + Логи с деталями: время, место, метод аутентификации, ID пользователя.
* **Аналитические отчеты**:
  + Графики посещаемости по часам/дням.
  + Список подозрительных активностей (частые ошибки аутентификации).

3.2.3 **Форматы данных**:

* Входные данные принимаются в форматах: JSON (для мобильного приложения), XML (интеграция с биометрическими сканерами).
* Выходные данные сохраняются в СУБД (MySQL/PostgreSQL) с возможностью экспорта в PDF/Excel.

3.2.4 **Пример выходных данных** (таблица 3.1):  
**Таблица 3.1 – Формат выходных данных**

| **Параметр** | **Формат** | **Пример значения** |
| --- | --- | --- |
| ID пользователя | Число (10 знаков) | 0000000123 |
| Роль | Текст (20 символов) | «Тренер зала №5» |
| Время запроса | Дата/Время (ISO 8601) | 2024-05-20T14:30:00+03:00 |
| Статус доступа | Текст | «Разрешен: тренажерный зал» |

3.2.5 **Визуализация данных** (рис. 3.1):  
**Рисунок 3.1 – Диаграмма посещаемости по зонам**

* Столбчатая диаграмма, отображающая количество посещений тренажерного зала, бассейна и групповых занятий за неделю.

3.2.6 **Источники входных данных**:

* **CRM-система**: данные о пользователях и абонементах.
* **Мобильное приложение**: QR-коды для входа, история посещений.
* **Биометрические устройства**: шаблоны отпечатков пальцев, фотографии.

3.2.7 **Связь с внешними системами** (таблица 3.2):  
**Таблица 3.2 – Источники данных**

| **Параметр** | **Источник** |
| --- | --- |
| Номер абонемента | CRM «Олимп-Менеджмент» |
| Расписание занятий | Система бронирования «SportTime» |
| Биометрические шаблоны | Сканеры «BioScan» |

**3.3 Выполняемые технологические операции**

Автоматизации подлежат:

1. **Регистрация пользователя**:
   * Ввод данных → верификация через SMS → создание учетной записи → привязка абонемента.
2. **Аутентификация**:
   * Сканирование пропуска → проверка в БД → подтверждение доступа → открытие турникета.
3. **Авторизация**:
   * Сверка роли пользователя с расписанием → проверка зоны доступа → передача сигнала на СКУД.
4. **Формирование отчетов**:
   * Ежедневный сбор логов → анализ данных → генерация PDF-отчетов для администрации.

**Критичные требования**:

* Интеграция с существующими СКУД (турникеты, камеры).
* Резервное копирование данных каждые 24 часа.
* Защита персональных данных.

**4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС**

**4.1 Формулировка цели разработки**

Целями создания АС ААП являются:

1. Разработка интегрированной системы управления доступом пользователей к ресурсам спорткомплекса на основе автоматизированной аутентификации и авторизации.
2. Повышение уровня безопасности и контроля доступа в зоны спорткомплекса (тренажерные залы, бассейны, служебные помещения).
3. Автоматизация процессов регистрации пользователей, верификации абонементов и управления правами доступа.
4. Снижение нагрузки на персонал за счет исключения ручной проверки пропусков и документов.
5. Обеспечение интеграции с существующими системами (CRM, СКУД, мобильное приложение) для оперативного обмена данными.
6. Повышение удобства пользователей через внедрение современных методов аутентификации (биометрия, электронные пропуска, одноразовые пароли).

**4.2 Область и условия применения АС**

АС ААП предназначена для:

* Управления доступом пользователей на территорию и в зоны спорткомплекса «Олимп».
* Интеграции с турникетами, электронными замками и биометрическими сканерами.
* Автоматизации процессов:
  + Регистрации новых пользователей.
  + Проверки статуса абонементов в режиме реального времени.
  + Формирования отчетности о посещаемости.
* Применения в условиях:
  + Работы 24/7 с учетом графика работы спорткомплекса.
  + Одновременного обслуживания до 5000 пользователей в день.

**4.3 Ограничения применения АС**

Для АС ААП должно быть обеспечено функционирование:

1. **Серверная часть**:
   * Развертывание на облачной платформе (например, AWS, Azure) или локальном сервере спорткомплекса с ОС Linux (Ubuntu 22.04 LTS) или Windows.
   * Совместимость с СУБД: PostgreSQL или MySQL.
2. **Клиентская часть**:
   * Работа на АРМ администраторов: ОС Windows, macOS, с предустановленными браузерами Chrome (последняя версия), Firefox.
   * Поддержка мобильного приложения: iOS 15+, Android 12+.
3. **Аппаратные ограничения**:
   * Турникеты и сканеры: совместимость с протоколами NFC, Bluetooth 5.0.
   * Биометрические устройства: поддержка стандартов ISO/IEC 19794-2 (отпечатки пальцев), ISO/IEC 30107-1 (распознавание лиц).
4. **Сетевые требования**:
   * Минимальная скорость интернета: 50 Мбит/с.
   * Резервирование каналов связи для бесперебойной работы.

**5 ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС**

**5.1 Требования к АС в целом**

АС ААП должна разрабатываться на основе **веб-технологий** по архитектуре «клиент-сервер» с поддержкой интеграции с локальными системами спортивного комплекса «Олимп».

* **Клиентский доступ**: через веб-браузер (Chrome, Firefox, Safari) или мобильное приложение (iOS/Android).
* **Интеграция с внешними системами**: через REST API с поддержкой JSON/XML.

**5.1.1 Требования к структуре и функционированию АС**

5.1.1.1 Функционирование АС ААП обеспечивается следующими подсистемами:

* **Подсистема доступа и авторизации**: управление ролями, многофакторная аутентификация.
* **Подсистема информационного обеспечения**: сбор данных из CRM, биометрических устройств, мобильных приложений.
* **Подсистема обработки данных**: алгоритмы RBAC, генерация отчетов.
* **Подсистема формирования решений**: передача сигналов на СКУД (турникеты, замки).

**Рисунок 5.1 – Структура подсистем АС ААП**  
(Схема взаимодействия подсистем с указанием потоков данных.)

5.1.1.2 Обмен данными между подсистемами и внешними системами (CRM, СКУД) осуществляется через **защищенные каналы связи** (HTTPS, VPN).

5.1.1.3 Режимы работы АС ААП должны соответствовать:

* Законодательству РБ в области защиты персональных данных.
* Внутренним регламентам спортивного комплекса «Олимп».

**5.1.2 Требования к защите информации от НСД**

5.1.2.1 Доступ к АС ААП предоставляется после:

* Аутентификации по логину/паролю + одноразовому паролю или биометрии.
* Проверки роли пользователя (администратор, тренер, посетитель).

5.1.2.2 Для интеграции с внешними системами (CRM, СКУД) используется **API с авторизацией**.

5.1.2.3 Требования к безопасности:

* Хранение паролей в БД - только в хешированном виде.
* Шифрование данных при передаче.
* Ведение журнала аудита (логирование всех попыток доступа).
* Ежедневное резервное копирование БД на облачное хранилище.

**5.1.3 Требования по сохранности информации при авариях**

* Автоматическое восстановление данных из резервных копий при сбоях (максимальное время простоя - 15 минут).
* Защита от DDoS-атак.

**5.1.4 Требования к информационному обеспечению**

5.1.4.1 Информационное обеспечение включает:

* Базу данных пользователей (ФИО, роли, биометрические шаблоны).
* Расписание занятий и бронирование зон.
* Журналы событий доступа.

5.1.4.2 Идентификация пользователей: уникальный ID (10 цифр) + RFID-метка.

5.1.4.3 Ввод и корректировка данных доступны только администраторам через защищенный веб-интерфейс.

5.1.4.4 Поиск и изменение данных:

* Время отклика при поиске пользователя - не более 1 секунды.
* Экспорт данных в CSV/PDF за 3 клика.

5.1.4.5 НСИ (нормативно-справочная информация) синхронизируется с CRM каждые 24 часа.

**5.1.5 Требования к математическому обеспечению**

5.1.5.1 Алгоритмы:

* Машинное обучение для анализа подозрительной активности.

5.1.5.2 Библиотеки:

* Использование открытых решений (OpenCV для распознавания лиц).
* Модульность для легкого обновления.

**5.1.6 Требования к программному обеспечению**

5.1.6.1 Лицензии:

* Серверная ОС: Linux Ubuntu / Windows.
* СУБД: PostgreSQL.

5.1.6.2 Требования к клиентскому ПО:

* Поддержка браузеров: последние 2 версии Chrome, Firefox, Safari.
* Мобильное приложение: iOS 15+, Android 12+.

5.1.6.3 Критерии качества:

* Время обработки запроса: ≤ 2 сек.
* Интуитивный интерфейс с подсказками.

**5.1.7 Требования к организационному обеспечению**

5.1.7.1 Эксплуатация:

* Не требует дополнительного персонала (кроме техподдержки).
* Обучение администраторов - 8 часов.

5.1.7.2 Сопровождение:

* Силами IT-отдела спорткомплекса или внешнего подрядчика.

**5.1.8 Требования к патентной чистоте**

5.1.8.1 Используемые технологии должны быть свободны от патентных ограничений.

5.1.8.2 Отчет о стоимости разработки предоставляется по запросу заказчика.

**5.1.9 Требования к документированию**

5.1.9.1 Комплект документов:

* Техническое задание.
* Руководство администратора и пользователя.
* API-документация.

5.1.9.2 Оформление: по ГОСТ.

**5.2 Требования к функциям подсистем**

**5.2.1 Подсистема «Доступ и авторизация»**

* Многофакторная аутентификация (пароль + SMS/биометрия).
* Управление ролями:
  + Администратор: полный доступ к настройкам.
  + Тренер: доступ к закрепленным зонам.
  + Посетитель: ограниченный доступ по абонементу.

**5.2.2 Подсистема «Информационное обеспечение»**

* Автоматический импорт данных из CRM (абонементы, расписание).
* Верификация биометрических шаблонов (погрешность ≤ 0,01%).

**5.2.3 Подсистема «Обработка данных»**

* Реализация RBAC.
* Генерация отчетов:
  + Ежедневная посещаемость.
  + Сводка по нарушениям доступа.

**5.2.4 Подсистема «Формирование решений»**

* Передача сигналов на турникеты/замки.
* Уведомления в мобильное приложение (push-сообщения).

**6 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА**

**6.1** Сроки выполнения проекта определяются **календарным планом**, утвержденным договором на разработку АС ААП между Заказчиком и Исполнителем.

**6.2** Основные этапы разработки:

* Анализ требований и проектирование архитектуры - 1 месяц.
* Реализация базового функционала (аутентификация, авторизация) - 2 месяца.
* Интеграция с CRM, СКУД и мобильным приложением - 1 месяц.
* Тестирование и отладка - 1 месяц.
* Подготовка документации - 2 недели.

**6.3** Приемо-сдаточные испытания проводятся комиссией, включающей представителей Заказчика и Исполнителя. Критерии приемки:

* Соответствие функционала техническим требованиям (разделы 1-5).
* Успешная обработка 1000+ одновременных запросов на доступ.
* Отсутствие критических уязвимостей (проверка пентестом).

**6.4** **Опытная эксплуатация АС ААП** осуществляется в пилотных зонах спорткомплекса «Олимп» (тренажерный зал №1, бассейн) в течение 30 дней. По итогам Заказчик принимает решение о вводе системы в промышленную эксплуатацию.

**6.5** Результаты каждого этапа фиксируются **двусторонними актами**. Примеры этапов:

* Подписание ТЗ.
* Успешное тестирование интеграции с биометрическими сканерами.
* Завершение обучения персонала.

**6.6** По завершении проекта Исполнитель предоставляет:

* Рабочую документацию (руководства пользователя, администратора, API).
* Проводит обучение для администраторов (8 часов) и технического персонала (4 часа).

**НАСТОЯЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ МОГУТ БЫТЬ УТОЧНЕНЫ ПО ДОГОВОРЕННОСТИ МЕЖДУ ЗАКАЗЧИКОМ (АДМИНИСТРАЦИЯ СПОРТКОМПЛЕКСА «ОЛИМП») И ИСПОЛНИТЕЛЕМ.**