ООО «РУВЕНТС»

ИНН 7703806326 / КПП 770301001
123100, г. Москва, Студенецкий переулок,

дом 3, помещение 1/2
email: info@ruvents.com

Программное обеспечение

РУВЕНТС.Комплекс

Модуль «РУВЕНТС.ИС»

Описание функциональных характеристик

Содержание

Серверная часть «Единой информационной системы управления мероприятиями и контроля доступа» (Модуль «РУВЕНТС.ИС») реализует единый реестр посетителей с категориями, квотами и статусами, ролевую аутентификацию с MFA и хешированием паролей по ГОСТ «Стрибог», REST API с токенной аутентификацией и Swagger-документацией, неизменяемый журнал аудита (ClickHouse), а также фоновые задачи – архивацию, плановую очистку персональных данных и фотографий, восстановление блокировок учётных записей.

В ее состав входят:

- **Веб-АРМ администратора**

Рабочее место для управления мероприятием и его инфраструктурой: создание мероприятий, категорий посетителей, квот и клиентских групп; управление учётными записями и ролями операторов; ведение реестра посетителей с поиском, фильтрацией и редактированием профилей и ПДн; настройка шаблонов бейджей и правил модерации; доступ к журналу аудита, отчётам и выгрузкам.

- **Партнёрский АРМ**

Инструмент для организаций-партнёров, ведущих собственные списки посетителей в рамках выделенной квоты: ведение и модерация списков, редактирование данных посетителей, выгрузка/загрузка списков, ПДн и фотографий, распределение квот на ответственных за группы посетителей.

- **Интерфейс ответственного за группы посетителей и форма самостоятельной регистрации**

Обеспечивает приём заявок от посетителей: распределение квот, создание ссылок для самостоятельной регистрации, предварительную модерацию поступивших заявок, настраиваемые анкеты под конкретное мероприятие, валидацию вводимых данных и фотографий, передачу заявок на итоговую модерацию.

Функциональные блоки серверного ядра

Серверное ядро реализует прикладную логику системы и предоставляет общие сервисы всем интерфейсам и подсистемам.

Его основные функциональные блоки:

- **Единый реестр посетителей** – профили, категории (клиентские группы), квоты, статусы. Изменение профиля в любом интерфейсе отражается во всех остальных через общую модель данных.
- **Аутентификация и авторизация** – учётные записи, ролевая модель (права закрепляются за учётной записью один раз и применяются во всех подсистемах), MFA по TOTP, пароли хранятся только в виде хешей по ГОСТ «Стрибог».
- **REST API** – точка интеграции для внешних систем и подсистем (аккредитация, контроль доступа): токенная аутентификация, версионирование, Swagger-документация.
- **Журнал аудита** – ClickHouse, режим только добавления (удаление и изменение записей средствами системы не предусмотрены). Оперативный доступ – 12 месяцев, архив – без ограничения срока.
- **Файловое хранилище** – работа с фотографиями, сканами документов и медиафайлами через S3-совместимый протокол.
- **Фоновые задачи** – архивация событий, плановая очистка персональных данных и фотографий по истечении сроков хранения, восстановление заблокированных учётных записей, рассылки.
- **Мониторинг** – сбор метрик, структурированных логов, отчётов об ошибках (интеграция с Sentry).

Ролевая модель

Роль и набор прав хранятся в учётной записи и применяются во всех подсистемах, включая операторские терминалы.

В модуле предусмотрены следующие роли:

- **Администратор** – доступ ко всем интерфейсам и разделам, включая административный: создание мероприятий, глобальная настройка справочников, просмотр глобального журнала, списка устройств и источников данных.
- **Оператор** – доступ только к ПО аккредитации.
- **Партнёр** – доступ к назначенным мероприятиям: статистика, модерация списков, редактирование данных посетителей, выгрузка/загрузка списков, распределение квот на ответственных за группы посетителей.
- **Ответственный за группы посетителей** – распределение квот, создание ссылок для самостоятельной регистрации, предварительная модерация заявок, выгрузка/загрузка списков.
- **Модератор/Безопасность** – просмотр заявок посетителей, решение о допуске или недопуске.
- **Транспортная безопасность** – просмотр заявок на автотранспорт, решение о допуске или недопуске.
- **КПП** – доступ только к ПО контроля доступа на назначенных точках прохода.

Права ролей разграничены. Совмещение ролей допускается только по решению администратора с фиксацией в журнале аудита.

Веб-АРМ в составе модуля

Веб-АРМ – браузерное рабочее место, реализующее пользовательские функции системы. Каждое рабочее место работает с общей моделью данных серверного ядра, а объём доступных функций и видимость данных определяются ролью учётной записи.

Ниже перечислены рабочие места и интерфейсы модуля, и доступные в них функции:

АРМ администратора	• **Создание и настройка мероприятий, категорий посетителей, квот, клиентских групп.** • **Управление учётными записями и ролями операторов.** • **Ведение реестра посетителей: поиск, фильтрация, просмотр и редактирование профилей и персональных данных.** • **Управление фотографиями и сканами документов (загрузка, замена, редактирование).** • **Настройка шаблонов бейджей, правил выдачи, параметров модерации.** • **Глобальные справочники (атрибуты, контакты, статусы, группы), просмотр глобального журнала, списка подключённых устройств и источников данных.** • **Доступ к журналу аудита, отчётам и выгрузкам.**
Партнёрский АРМ	• Ведение списков посетителей по назначенным администратором мероприятиям в рамках выделенной квоты и категорий. • Просмотр статистики, модерация списков, редактирование данных посетителей. • Выгрузка и загрузка списков посетителей, персональных данных и фотографий. • Распределение квот на ответственных за группы посетителей. • Видимость данных ограничена посетителями партнёра.

Интерфейс ответственного за группы посетителей	• Распределение квот, полученных от администраторов и партнёров. • Создание ссылок для самостоятельной регистрации посетителей. • Предварительная модерация заявок, поступивших от посетителей. • Выгрузка и загрузка списков посетителей.
Форма самостоятельной регистрации	• Регистрация посетителя по ссылке: ввод персональных данных, загрузка фотографии. • Настраиваемые поля анкеты, включая кастомные анкеты под конкретное мероприятие. • Валидация вводимых данных и форматов фотографий. • Передача заявки на модерацию. • Защита канала передачи данных по TLS, обработка персональных данных в соответствии с 152-ФЗ.

Описание отдельных функциональностей

Управление посетителями, персональными данными и фотографиями

Модуль ведёт единый реестр посетителей мероприятия: профиль посетителя создаётся один раз и в дальнейшем используется всеми интерфейсами и подсистемами, включая аккредитацию и контроль доступа.

Персональные данные и фотографии обрабатываются с учётом требований 152-ФЗ: доступ к ним определяется ролью учётной записи, все операции просмотра и изменения фиксируются в журнале аудита, а по истечении установленных сроков хранения данные удаляются автоматически.

В профиле посетителя обрабатываются следующие данные:

- ФИО;
- дата, место и страна рождения;
- пол;
- гражданство и страна проживания;

- паспортные данные (серия, номер, скан); ИНН; СНИЛС;
- телефон;
- адрес электронной почты;
- фотография; место работы и должность.

Модуль обеспечивает следующие функции работы с данными посетителей:

- импорт списков посетителей, паспортных данных и фотографий из файлов, в том числе пакетная загрузка по шаблону с валидацией форматов и контролем дублей;
- выгрузка списков посетителей, персональных данных и фотографий для передачи в смежные системы и подсистемы;
- загрузка, замена и удаление фотографий и сканов документов с проверкой формата, размера и качества изображения;
- хранение фотографий и сканов в S3-совместимом объектном хранилище отдельно от базы данных профилей;
- поиск, фильтрация и редактирование профилей посетителей по категориям, статусам и клиентским группам;
- плановая очистка персональных данных и фотографий фоновыми задачами по истечении установленных сроков хранения;
- контроль целостности файлов обмена и защита аутентификационных данных средствами ГОСТ «Стрибог»;
- фиксация всех операций с персональными данными и фотографиями в журнале аудита.

Модерация и дополнительный учёт

Модерация заявок выполняется в два этапа: предварительную проверку выполняет сторона, сформировавшая заявку, итоговое решение о допуске принимает служба безопасности.

На первом этапе предварительную модерацию выполняет ответственный за группы посетителей или партнёр: проверяются корректность и полнота персональных данных, наличие обязательных документов и соответствие фотографии установленным требованиям. По результатам проверки заявка принимается либо отклоняется с обязательным указанием причины, которая возвращается заявителю для устранения замечаний. На втором этапе итоговое решение о допуске или недопуске посетителя до аккредитации принимает модератор или служба безопасности; отклонённая заявка может быть возвращена на доработку с сохранением истории изменений. Заявки на въезд автотранспорта обрабатываются отдельным потоком: решение по ним принимает транспортная безопасность независимо от модерации заявок посетителей.

Все действия модерации – смена статуса заявки, причина отклонения, автор и время принятия решения – фиксируются в журнале аудита и доступны для последующего разбора.

Дополнительно модуль ведёт учёт сопутствующих прав и событий: настройку права посетителя на питание (за настройку отвечает роль «Администратор», выдача реализуется в подсистеме контроля доступа); сбор данных о времени, проведённом посетителями на площадках мероприятия, на основе событий проходов, регистрируемых точками контроля доступа.

Производительность

Показатели производительности рассчитаны на работу крупного мероприятия с высокой плотностью проходов и одновременной работой множества стоек регистрации и точек контроля доступа:

- время отклика на идентификацию посетителя – не более 1 секунды;
- обновление данных зонирования – не реже раза в 5 секунд;
- устойчивая работа при пиковой нагрузке стойки регистрации;
- масштаб – до 100 000 посетителей и 200 одновременных терминалов на мероприятие.

Информационная безопасность

Меры информационной безопасности реализованы на уровне серверного ядра и распространяются на все интерфейсы и подсистемы модуля:

- аутентификация пользователей по учётной записи и паролю; пароли хранятся исключительно в виде хешей по ГОСТ «Стрибог», восстановление исходного пароля средствами системы не предусмотрено;
- многофакторная аутентификация (TOTP) для привилегированных учётных записей и внешних кабинетов — партнёрского АРМ и интерфейса ответственного за группы посетителей;
- разграничение доступа по ролевой модели: набор операций и объём видимых данных определяются ролью учётной записи и применяются одинаково во всех подсистемах;
- блокировка учётной записи при превышении допустимого числа неудачных попыток входа с последующим автоматическим восстановлением фоновой задачей;
- передача данных между компонентами модуля и с внешними системами — только по защищённым каналам TLS/HTTPS; при передаче персональных данных за пределы контролируемой зоны применяются сертифицированные СКЗИ;
- контроль целостности файлов обмена и выгрузок средствами ГОСТ «Стрибог»;
- ведение журнала аудита в режиме только добавления: записи о входах, изменениях профилей, действиях модерации и операциях с персональными данными не могут быть изменены или удалены средствами системы;
- обработка персональных данных в соответствии с требованиями 152-ФЗ, включая ограничение сроков хранения и плановое удаление данных по их истечении;

- мониторинг событий безопасности, сбор структурированных логов и регистрация ошибок с передачей во внешние системы мониторинга.

Взаимодействие с офлайн-режимом терминалов

Автономная (офлайн) работа реализуется на стороне терминальных модулей – «РУВЕНТС.Клиент» и «РУВЕНТС.Контроль доступа»: при потере связи с сервером они продолжают идентификацию посетителей и регистрацию проходов по локальной копии данных.

Модуль «РУВЕНТС.ИС» отвечает за серверную часть этого сценария: передаёт терминалам актуальные наборы данных для локального кеша, а после восстановления связи автоматически, без участия оператора, принимает накопленные события и синхронизирует их с общей моделью данных. Конфликты, возникшие при одновременном изменении записей, разрешаются по предопределённым правилам, а результат синхронизации фиксируется в журнале.