ООО «КБ Пожарной Автоматики»

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ Rubezh-STRAZH

Руководство по эксплуатации

ПАСН.425728.007 РЭ

Редакция 6

https://products.rubezh.ru/

Настоящее руководство по эксплуатации предназначено для изучения и правильной эксплуатации системы контроля и управления доступом **Rubezh-STRAZH**.

Настоящий документ устанавливает порядок и правила, необходимые для успешной эксплуатации СКУД.

Документ содержит сведения о назначении, технических характеристиках, описании и общих принципах функционирования СКУД, а также сведения о подготовке к использованию, использовании при работе, контроле работоспособности, техническом обслуживании, хранении, транспортировании и утилизации.

Настоящий документ распространяется на СКУД, построенный на следующих компонентах:

- контроллеры:
  STR20-IP,
  STR20-IP-Ent,
  STR20-1AP-IP-M,
  STR20-2AP-IP-M,
  КД-Pro;
- модули доступа:
  STR-1AP,
  STR-1AP-M,
  STR-2AP-M,
  STR-3AP-M.

К работе и обслуживанию допускаются лица, изучившие настоящее руководство по эксплуатации.

Содержание

Перечень сокращений

АПБ	– Антипассбэк (antipassback). Функция зонального контроля, запрет повторного прохода через точку доступа
БП	– блок питания – встроенный источник вторичного электропитания резервированный.
КАПС R-PLATFORMA	– комплекс аппаратно-программных средств системы сбора и обработки информации и ситуационного управления R-PLATFORMA.
ПО	– программное обеспечение.
СКУД	– система контроля и управления доступом Rubezh-STRAZH.
СМК	– Сигнализатор магнитоконтактный.
ТД	– точка доступа.
ТУ	– технические условия ПАСН.42725.007 ТУ.
OSDP	– Стандартизованный ассоциацией SIA протокол взаимодействия контроллера и периферийных устройств для применения в СКУД.

Перечень терминов

Пользователь	– лицо или организация, использующее Rubezh-STRAZH для решения стоящих перед ним задач (администратор, оператор и т.д.).
Права доступа	– определяют набор действий с объектами системы (например, просмотр, редактирование, управление), разрешенных для выполнения пользователю.
Профиль доступа	– совокупность точек доступа и графика доступа.
Регламент	– определяет порядок и способ выполнения задач, ответственность владельца и исполнителей, процедуры управления.
Учетная запись	– хранимая совокупность данных о пользователе, необходимая для его проверки и предоставления ему прав доступа.

1 Описание и работа

1.1 Назначение СКУД

1.1.1 СКУД предназначена для управления преграждающими устройствами в соответствии с настроенными для субъектов доступа правилами, ведения журнала перемещений и формирования отчетов. Основной способ идентификации субъектов – это RFID-карты, считывание которых осуществляется на подключенных к контроллерам Rubezh-STRAZH считывателях.

1.1.2 Основными компонентами СКУД являются контроллеры доступа, управляемые ими модули доступа и считыватели RFID-карт.

1.1.3 Контроллер Rubezh-STRAZH является ведущим устройством и поддерживает управление точками доступа:

- односторонней;
- двусторонней;
- турникетом;
- турникетом с картоприемником;
- шлагбаумом или воротами;
- шлюзовыми кабинами и т. д.

1.1.4 Контроллер Rubezh-STRAZH может использоваться как автономно (под управлением встроенного в контроллер ПО), так и управляться с помощью ПО верхнего уровня R-Платформа через API любого контроллера. Работа контроллера под управлением ПО R-платформа описано в руководстве по эксплуатации этого ПО.

1.1.5 Контроллеры Rubezh-STRAZH могут быть объединены в единую виртуальную сеть (далее – кластер). В этом режиме контроллеры взаимодействуют друг с другом и формируют распределенную многоконтроллерную СКУД. Поддерживаемый размер кластера зависит от типа контроллеров: 8 для базовых, 32 для Enterprise (программное ограничение для версии Enterprise отсутствует, указанное значение в 32 контроллера является протестированным и гарантированным производителем). При использовании только встроенного ПО появляется возможность построения достаточно крупной СКУД (большое количество точек) без внешнего выделенного сервера используя только контроллеры. В этом случае каждый контроллер является сервером СКУД, он хранит все данные системы, предоставляет доступ к консоли управления и администрирования и предоставляет внешний API. Все контроллеры синхронизируют свои данные друг с другом и любой из них может использоваться для работы со всей СКУД.

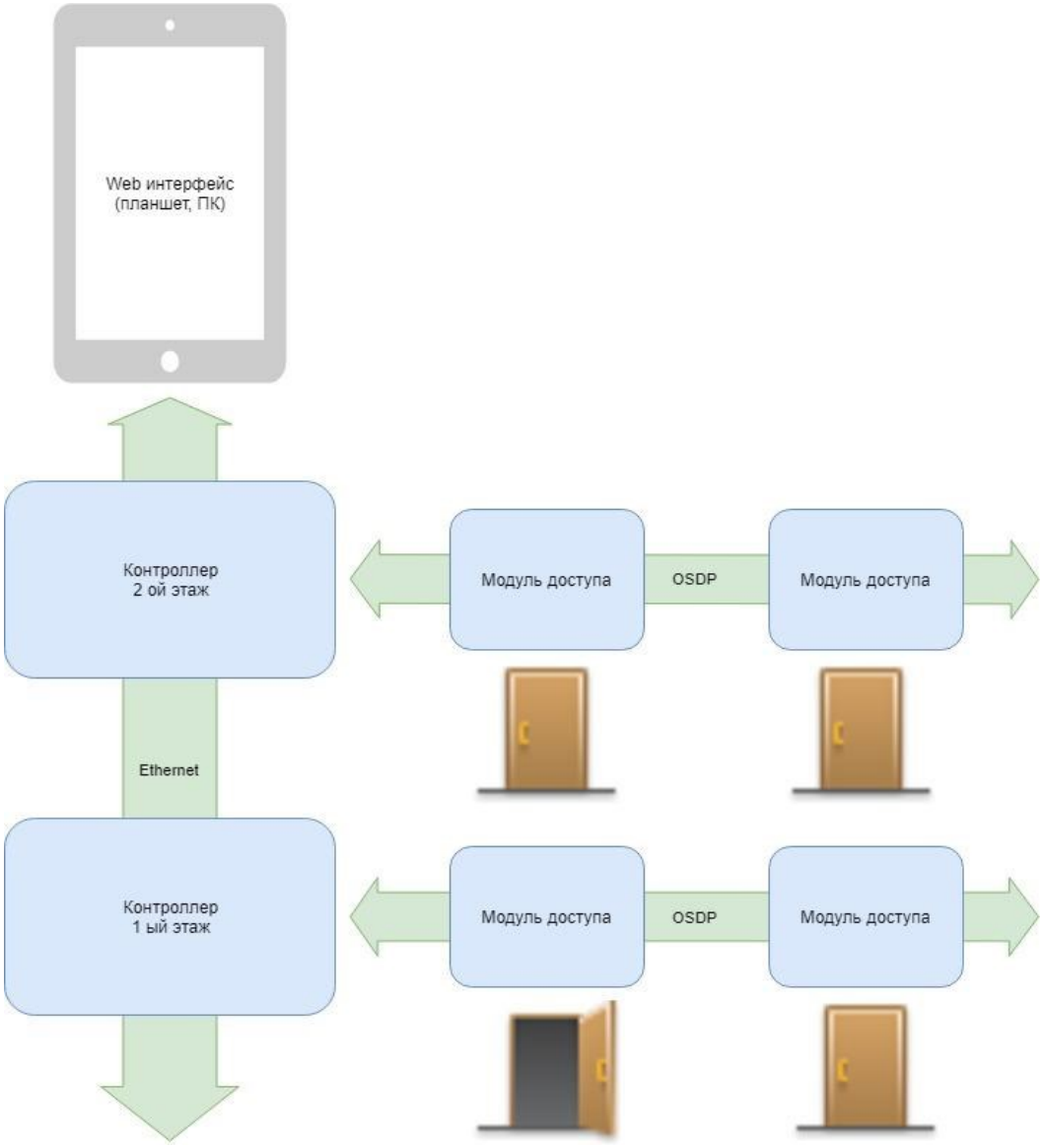
1.1.6 Встроенная распределенная СКУД обеспечивает:

- возможность настройки и администрирования всей системы через единый Web-интерфейс;
- учет и редактирование информации, необходимой для управления доступом (данные о режимах доступа, временных зонах, пропусках и их владельцах и т. д.);
- автоматизированное управление режимом прохода в контролируемую зону через ТД;
- управление режимами работы точки прохода (разблокировка, блокировка);

- возможность использования функции глобального зонального контроля (а также режима запрета повторного прохода через ТД), с настраиваемым временем контроля. Поддерживается для всех типов ТД, за исключением однопроходных;
- возможность работы без подключения исполнительных механизмов для учёта рабочего времени;
- автоматическое ведение журнала доступа и изменений данных системы, журнала перемещений персонала, оповещений о событиях оборудования;
- настройку оповещений о срабатывании датчиков;
- выгрузку событий по перемещениям для построения отчетов учета рабочего времени;
- сохранение общей работоспособности при выходе из строя отдельных контроллеров;
- автоматическую синхронизацию данных при добавлении контроллеров;
- обновление программного обеспечения.

1.2 Общие характеристики

1.2.1 СКУД состоит из сетевых контроллеров Rubezh-STRAZH, объединенных в кластер. К каждому контроллеру подключены наборы модулей доступа, обслуживающих точки прохода. Контроллеры управляют поведением точек прохода, получая и посылая информацию устройствам, подключенным к модулям доступа. Таким образом, ключевыми компонентами системы являются контроллеры и модули доступа.



1.2.2 Каждое устройство может содержать одну или несколько плат двух типов: плату контроллера и плату внешних подключений.

1.2.3 Функционально плата контроллера представляет собой устройство управления платами модулей внешних подключений, подключенными к ней посредством стандартного интерфейса OSDP либо OSDP-устройствами, подключенными непосредственно к контроллеру.

1.2.4 Плата контроллера содержит разъем для установки вычислительного модуля Raspberry PI CM3 (CM3+). На плате расположены:

- клеммная колодка питания;
- разъем Ethernet для подключения к сети;
- микропереключатель вскрытия корпуса и контакты внешнего датчика вскрытия корпуса;
- два входа типа «сухой контакт» SENS1, SENS2 с контролем целостности линии. Входы могут быть использованы для подключения кнопки аварийной разблокировки точек прохода, датчика отрыва от стены, датчика контроля внешнего питания и прочих датчиков;
- два разъема интерфейса RS-485 (OSPD) для подключения плат периферии и OSDP-считывателей (интерфейсы независимые и могут использоваться для подключения);
- гнездо с батарейкой часов реального времени;
- USB-разъем для подключения дополнительных устройств при наличии соответствующей поддержки в прошивке устройства;
- USB-разъем для внутреннего использования (не предназначен для пользователей);
- светодиодные индикаторы, отображающие текущее состояние контроллера и Ethernet связи.

1.2.5 Характеристики контроллера Rubezh-STRAZH:

Характеристика	Значение
Напряжение питания, В	9-28
Максимальный ток, А	0,8

Характеристика	Значение
Режим работы	круглосуточный
Скорость обмена в сети Ethernet, Мбит/с	10/100
Количество OSDP-каналов (RS-485)	2
Максимальное количество OSDP адресов	30
Количество подключаемых OSDP-считывателей	20
Тип подключения считывателей	OSDP
Максимальная длина кабеля RS-485 (линия OSDP), м	не более 1000
Максимальная длина кабеля для подключения датчиков, м	не более 100
Максимальная длина кабеля Ethernet, м	не более 100
Количество карт доступа	не менее 10 000 (не менее 100 000*)
Количество временных расписаний	не менее 2 000
Количество событий в журнале	не менее 400 000
Количество контроллеров в автономном кластере	8 (не менее 32*)
Зональный контроль (АПБ)	Да
** Для контроллеров с лицензией Enterprise*	

1.2.6 Плата модуля внешних подключений предназначена для подключения периферийных устройств точек прохода и двусторонней трансляции данных от устройств и к устройствам через шину OSDP к плате и от платы контроллера. Модуль, взаимодействуя со считывателями по шине данных интерфейса Wiegand, принимает, преобразовывает и передает коды карт по шине OSDP. Максимальная длина идентификатора ограничена 80 битами. Модуль внешних подключений осуществляет трансляцию состояния входных датчиков в шину OSDP и получает команды управления релейными выходами. На плате расположены:

- клеммная колодка питания;
- микропереключатель вскрытия корпуса и контакты внешнего датчика вскрытия корпуса;
- два входа типа «сухой контакт» SENS1, SENS2 с контролем целостности линии. Входы могут быть использованы для подключения охранных шлейфов и прочих датчиков;
- два семи контактных разъема типа Wiegand для подключения считывателей;
- два разъема интерфейса RS-485 (OSDP) для подключения к шине платы контроллера (второй интерфейс является резервным);
- четыре входа для подключения датчиков точки прохода (датчик двери/турникета, кнопка запроса на выход);
- две клеммные колодки для подключения к двум реле с нормально замкнутыми и нормально разомкнутыми контактами;
- колодка установки адреса на шине OSDP;
- перемычки терминатора шины;
- перемычки, управляющие сигналом световой и звуковой индикации считывателей;
- светодиодные индикаторы, отображающие текущее состояние модуля.

1.2.7 Характеристики модуля внешних подключений:

Характеристика	Значение
Напряжение питания, В	9-28
Максимальный ток, А	0,15
Режим работы	круглосуточный
Количество OSDP (485) каналов	2
Тип подключения считывателей	Wiegand 24; 26; 32; 33, 34; 35; 37; 40; 42; 48; 50; 56; 58; 64; 66; 72; 74; 80
Максимальная длина кабеля RS-485 (линия OSDP), м	не более 1000
Максимальная длина кабеля Wiegand, м	не более 100
Максимальная длина кабеля для подключения кнопок и датчиков, м	не более 100
Максимальная длина кабеля от реле до замков	Рассчитывается с учетом падения напряжения
Напряжение питания считывателей	Соответствует питанию устройства
Количество входов Wiegand для подключения внешних считывателей	2
Количество входов с контролем линии типа «сухой контакт»	6
Количество выходов линий управления индикацией считывателей	6
Количество релейных выходов типа «сухой контакт» (NC/NO)	2
Максимальное напряжение постоянного тока, коммутируемое контактами реле, В	30
Максимальный постоянный ток, коммутируемый контактами реле, А	3

1.2.8 Конечные изделия состоят из плат контроллеров и модулей внешних подключений. В зависимости от типа и количества установленных плат, материала корпуса и наличия встроенного источника вторичного питания существуют следующие модели:

STR20-IP – контроллер с базовой лицензией. Объединение в кластер до 8 контроллеров. Без поддержки ПО верхнего уровня. База пользователей – не менее 10000 идентификаторов. Поддерживает до 20 считывателей. Пластиковый корпус, крепление на DIN-рейку, без встроенного источника питания;

STR20-IP-Ent – контроллер с лицензией Enterprise. Объединение в кластер до 32 контроллеров. Возможность работы с ПО верхнего уровня. База пользователей – не менее 100 000 идентификаторов. Поддерживает до 20 считывателей. Пластиковый корпус, крепление на DIN-рейку, без встроенного источника питания;

STR20-1AP-IP-M – контроллер плюс модуль с лицензией Enterprise. Объединение в кластер до 32 контроллеров. Возможность работы с ПО верхнего уровня. База пользователей – не менее 100000 идентификаторов. Управление одной точкой доступа типа считыватель/считыватель или до двух – по алгоритму считыватель/кнопка выхода. Поддерживает до 18 дополнительных считывателей. Металлический корпус со встроенным источником питания;

STR20-2AP-IP-M – контроллер плюс 2 модуля с лицензией Enterprise. Объединение в кластер до 32 контроллеров. Возможность работы с ПО верхнего уровня. База пользователей – не менее 100000 идентификаторов. Управление двумя точками доступа типа считыватель/считыватель или до четырех – по алгоритму считыватель/кнопка

выхода. Поддерживает до 16 дополнительных считывателей. Металлический корпус со встроенным источником питания;

КД-Pro – контроллер плюс 2 модуля с лицензией Enterprise. Объединение в кластер до 32 контроллеров. Возможность работы с ПО верхнего уровня. База пользователей – не менее 100000 идентификаторов. Управление двумя точками доступа типа считыватель/считыватель или до четырех – по алгоритму считыватель/кнопка выхода. Поддерживает до 16 дополнительных считывателей. Металлический корпус со встроенным источником питания;

STR-1AP – модуль (OSDP – Wiegand). Подключение оборудования одной точки доступа типа считыватель/считыватель или до двух – по алгоритму считыватель/кнопка выхода. Пластиковый корпус, крепление на DIN-рейку, без встроенного источника питания;

STR-1AP-M – модуль (OSDP – Wiegand). Подключение оборудования одной точки доступа типа считыватель/считыватель или до двух – по алгоритму считыватель/кнопка выхода. Металлический корпус. Встроенный источник питания;

STR-2AP-M – два модуля (OSDP – Wiegand). Подключение оборудования двух точек доступа типа считыватель/считыватель или до четырех – по алгоритму считыватель/кнопка выхода. Металлический корпус. Встроенный источник питания;

STR-3AP-M – три модуля (OSDP – Wiegand). Подключение оборудования трёх точек доступа типа считыватель/считыватель или до шести – по

алгоритму считыватель/кнопка выхода. Металлический корпус. Встроенный источник питания.

1.3 Модификации встроенного программного обеспечения

1.3.1 Программное обеспечение контроллеров Rubezh-STRAZH выпускается в двух модификациях: обычная (базовая) и Enterprise (Ent.). Контроллеры в пластиковом корпусе могут нести на борту как обычную модификацию, так и Enterprise, а контроллеры в металлическом корпусе – только Enterprise.

1.3.2 Различия между двумя модификациями следующие:

- обычная модификация поддерживает до 8 контроллеров в кластере, а Enterprise – до 32 контроллеров;
- в обычном режиме недоступна API-интеграция, Enterprise поддерживает использование ПО верхнего уровня;
- для пользования контроллером в базовом исполнении требуется ввод логина, пароля и проверочного кода, для версии Enterprise ввод проверочного кода не нужен.

1.3.3 В кластер могут быть объединены контроллеры с разными модификациями, однако при наличии в кластере контроллеров в модификации базовая, параметры кластера будут соответствовать базовой версии.

1.3.4 Базовое программное обеспечение может быть заменено на Enterprise. Для этого необходимо предоставить компании-производителю информацию обо всех контроллерах кластера.

1.4 Питание контроллера

1.4.1 Контроллеры и модули в одноплатном пластиковом исполнении (STR20-IP, STR20-IP-Ent, STR-1AP) должны подключаться к источнику постоянного тока с напряжением (9 – 28) В. Важно, питание считывателей соответствует подаваемому напряжению.

1.4.2 Контроллеры и модули в металлическом исполнении (STR20-1AP-IP-M, STR20-2AP-IP-M, КД-Pro, STR-1AP-M, STR-2AP-M, STR-3AP-M) подключаются к стандартной сети переменного тока напряжением 230 В частотой 50 Гц. В комплект входит импульсный стабилизированный (блок питания) БП с отдельным выходом для зарядки аккумулятора. БП преобразует переменный ток в постоянный с напряжением 12 В, который используется для питания плат, а также для подзарядки резервного аккумулятора.

1.4.3 БП имеет защиту от длительного превышения тока нагрузки и короткого замыкания. Защита обеспечивает отключение нагрузки с последующими периодическими попытками восстановления вторичного питания (до устранения причины отключения).

1.4.4 БП обеспечивает формирование сигнала «Авария», передаваемого на плату контроллера по сигналу, формируемому контактами реле:

- при отключении питания по основному вводу;
- при пропадании вторичного напряжения;
- при разряде в аварийном режиме или отсутствии АКБ.

Для получения сигнала «авария» в журнале событий контроллера необходимо настроить оповещение (подробнее – в разделе «Оповещения и тревоги»).

1.4.5 От БП допускается питание дополнительных устройств. При подключении замка и дополнительных устройств (например, датчиков сигнализации, сирены и пр.) необходимо контролировать, чтобы суммарная нагрузка на блок питания не превышала предельно допустимую.

1.4.6 Характеристики БП:

Характеристика	Значение
Входное напряжение питания, В	140 – 265
Частота входного напряжение питания, Гц	50 ± 3
Выходное напряжение вторичного электропитания тока, В	10,3 – 13,8
Максимальный выходной постоянный ток, А	2,0
Режим работы	круглосуточный
Емкость аккумуляторной батареи питания (далее – АКБ), А·ч	4,5
Размер АКБ (мм)	90x70x105
Время автоматического заряда АКБ, не более, ч	14
Аккумуляторная батарея не входит в комплект поставки контроллера и приобретается отдельно	

1.5 Часы

1.5.1 Контроллер имеет автономные часы реального времени, используемые, в частности, при формировании событий проходов. Для работы часов необходимо наличие литиевой батарейки типоразмера CR2032 в держателе на плате. Заряда батарейки хватает на 3 года при хранении контроллера, и до 5 лет при работе контроллера от сети. По истечении срока, необходима самостоятельная замена батареи. После замены, необходимо проверить правильность установки времени в веб-интерфейсе контроллера. Синхронизация часов может осуществляться с помощью любого публичного NTP-сервера.

1.6 Перемычки

1.6.1 На плате контроллера расположены:

- перемычки для включения терминаторов RS-485 (линий OSDP):

а) J1, J2 – для первого интерфейса,

б) J3, J4 – для второго.

Нормальное состояние – перемычки отсутствуют. Для последнего устройства на длинной линии необходимо установить соответствующие перемычки. Сигналом установки перемычки может служить низкое качество OSDP-связи (качество связи можно проверить в меню «Контроль связи OSDP»);

- USB BOOT – трехпиновая колодка, предназначена для перевода контроллера в режим прошивки с помощью специальной утилиты по USB-соединению (микроUSB-разъем). Не предназначена для использования конечным пользователем. Нормальное состояние – перемычки отсутствуют. Режим прошивки – замкнуты контакты 1 и 2. Режим загрузки с внешней SD-карты – замкнуты контакты 2 и 3;
- TAMPER – контакты внешнего датчика открытия корпуса.

1.6.2 На плате модуля внешних подключений расположены:

- перемычки для включения терминаторов RS-485 (линий OSDP):

а) J1, J2 – для первого интерфейса,

б) J3, J4 – для второго.

Нормальное состояние – перемычки отсутствуют. Для последнего устройства на длинной линии необходимо установить соответствующие перемычки;

- перемычки ACT-LED, ACT-BEEP задают уровень сигнала по линиям световой и звуковой индикации Wiegand-считывателей соответствующий отсутствию индикации. Нормальное состояние – перемычки отсутствуют. Что соответствует нулевому уровню. При установленных перемычках уровень соответствует напряжению питания;
- TAMPER – контакты внешнего датчика открытия корпуса.

1.7 Индикация контроллера

1.7.1 На контроллерах и модулях расположены светодиоды, отражающие следующие состояния:

- наличие питания;
- наличие связи по первому каналу OSDP;
- наличие связи по второму каналу OSDP;
- наличие ошибки или уведомления о специальном режиме работы контроллера.

1.7.2 Рядом с Ethernet-разъемом на плате контроллера находятся светодиоды, отражающие состояние связи (SPD, LINK, FDX), а также светодиод ACT, показывающий активность процессоров платы.

1.7.3 Контроллер использует индикатор ошибки для отображения специальных состояний:

Тип индикации	Режим работы контроллера
Нет индикации	Запуск контроллера
Однократное мигание с интервалом 5 с	Нормальная работа контроллера
Однократное мигание с интервалом 1 с	Реакция на кнопку RESET на плате

Тип индикации	Режим работы контроллера
Двукратное мигание с интервалом 2 с	Первый запуск контроллера после сброса к заводским настройкам
Трехкратное мигание с интервалом 2 с	Обновление встроенного ПО
Частое мигание в течение 30 с	Реакция на кнопку включения тестовой индикации в WEB-интерфейсе.

1.7.4 На плате модуля присутствует дополнительная индикация активности реле с помощью красных светодиодов.

1.7.5 На плате модуля доступа предусмотрена индикация ошибок связи: частота мигания индикатора зависит от количества ошибок, чем их больше, тем чаще происходит короткое мигание светодиода, вплоть до постоянной его индикации.

2 Монтаж

2.1 Меры безопасности

2.1.1 При установке и эксплуатации устройств необходимо руководствоваться «Правилами технической эксплуатации электроустановок потребителей» и «Правилами техники безопасности при эксплуатации электроустановок потребителей». К работе с контроллером допускаются лица, изучившие настоящее руководство, имеющие аттестацию по технике безопасности при эксплуатации электроустановок не ниже 3 группы и прошедшие инструктаж по технике безопасности на рабочем месте. Проведение всех работ по подключению и монтажу контроллера и модулей не требует применения специальных средств защиты. Для изделий со встроенными блоками питания в рабочем состоянии подводятся опасные для жизни напряжения от электросети, поэтому необходимо:

подключать контроллер или модуль только к электросети, выполненной по трехпроводной схеме (т.е. имеющей провод защитного заземления);

− регламентные и ремонтные работы производить только при отключенных сетевом питании и линиях связи с компьютером и другими устройствами системы. Не допускается использовать при чистке загрязненных поверхностей абразивные и химически активные вещества.

2.1.2 Запрещается устанавливать контроллер или модуль на токоведущих поверхностях и в помещениях с относительной влажностью выше 85%.

2.2 Общие рекомендации

2.2.1 Выбор проводов и кабелей, способов их прокладки должен производиться в соответствии с требованиями СНиП 3.05.06-85, ВСН 116-87, НПБ 88-2001. При подключении оборудования необходимо строго соблюдать полярность соединения устройств. Монтаж изделий осуществляется в любом удобном месте, обеспечивающем соблюдение условий эксплуатации, приведенных в паспорте устройства. Для крепления корпуса изделий снабжены монтажными отверстиями. Изделия в пластиковых корпусах могут также крепиться на DIN-рейку.

2.2.2 Рекомендуемые типы кабелей, используемые при монтаже:

№	Подключаемое к контроллеру оборудование	Макс. длина кабеля, м	Тип кабеля	Сечение, мм², не менее	Пример кабеля
1	**Ethernet (IEEE 802.3)**	100	2 витые пары не ниже пятой категории	0,2	КВПЭф-5е 2х2х0,52F/ UTP2-Cat5e
2	**Wiegand считыватели**	100	4 витые пары не ниже пятой категории		КВПЭф-5е 4х2х0,52F/ UTP2-Cat5e
3	**RS-485 (Модули доступа, OSDP устройства)**	До 200	Витая пара не ниже пятой категории	0,2	КВПЭф-5е / UTP2-Cat5e
		От 200 до 1000	Витая пара, двухжильный	0,2 – 0,5	КПСВЭПс / КПСВВм
4	**Питание**	По падению напряжения	Двужильный	0,75 или по падению напряжения	ШВВП 2х0,75 двухцветный

№	Подключаемое к контроллеру оборудование	Макс. длина кабеля, м	Тип кабеля	Сечение, мм^2, не менее	Пример кабеля
5	**Входы типа «Сухой контакт» - SENS 1 и 2** **Входы для подключения датчиков точки прохода** **DOOR 1 и 2** **EXIT 1 и 2**	100	Двужильный	0,2 – 0,5	КВПЭф-5е / UTP2-Cat5e
6	**Реле К1 и К2** **(Запорное устройство)**	10	Двужильный	0,75 или по падению напряжения	ШВВП 2х0,75с двухцветный

2.2.3 Все клеммные колодки на плате контроллера сделаны съемными. Колодки снимаются в направлении от платы. Максимальное сечение кабеля, который можно подключить в клеммы устройств – 1,5 мм^2.

2.3 Отключение питания

2.3.1 Изделия со встроенным источником питания снабжены отверстием для ввода кабеля сети 230 В, а также клеммными колодками, расположенными справа от блока питания. Блок питания имеет выключатель, позволяющий отключать подачу высокого напряжения. Для полного отключения питания платы, необходимо дополнительно отключить аккумулятор. Плата контроллера содержит в своем составе суперконденсатор. Для проведения работ с контроллером, необходимо подождать 20 секунд после снятия питания (выключения блока питания и отключения аккумулятора).

2.4 Подключение оборудования

2.4.1 Оборудование доступа (замки, датчики, кнопки, и т. д.) подключается к модулям (за исключением дополнительных датчиков на контроллере SENS1 и SENS2). Все подключения необходимо выполнять при выключенном питании модуля. Не все элементы являются обязательными. Например, можно не использовать в системе датчики закрытия двери, второй (внутренний) считыватель и даже кнопку запроса на выход. В соответствии с установленным оборудованием дверной канал будет обеспечивать выполнение тех или иных функций.

2.4.2 Следует иметь в виду, что все входы поддерживают контроль линии на короткое замыкание и обрыв. При подключении кнопок и датчиков следует устанавливать входящие в комплект резисторы в непосредственной близости к датчикам и кнопкам.

2.4.3 В случае, когда контроль линии того или иного датчика не требуется, его можно отключить через интерфейс настройки оборудования. В этом случае нет необходимости устанавливать резисторы.

2.5 Подключение считывателей

2.5.1 Модули предназначены для работы со считывателями с интерфейсом Wiegand, однако непосредственно на шину RS-485 контроллера могут быть подключены считыватели с интерфейсом OSDP.

2.5.2 Следует учитывать особенности считывания карт (формат кода) считывателями разных производителей и разной длины кода карты (26, 32 и т. д.). Предпочтительно использовать на всем объекте один тип считывателей. В случае, если оказалось, что установленные считыватели выдают разный формат карты, рекомендуется их или настроить программным обеспечением производителя, или заменить. Если это невозможно, то можно добавить персоне в качестве разных карт все виды кодов, выдаваемых разными считывателями. Это обеспечит правильную работу системы с несовместимыми считывателями.

2.5.3 При монтаже любого типа считывателя следует выполнять следующие рекомендации:

- считыватель монтируется на удобной высоте, обычно на высоте дверной ручки, со стороны, противоположной дверным петлям;
- proximity-считыватели малого радиуса действия следует монтировать на расстоянии не менее 0,5 метра один от другого с целью предотвращения их взаимного влияния;
- при необходимости установки считывателей с двух сторон одной двери следует разнести их как минимум на (20-25) см по вертикали или горизонтали. Для считывателей увеличенной дальности следует руководствоваться инструкциям по установке;
- необходимо предусмотреть возможность доступа к кабелям в будущем для обслуживания.

2.5.4 Для подключения считывателей используется неэкранированный кабель с сечением каждой жилы не менее 0,22 мм^2. Считыватели малочувствительны к электрическим помехам и наводкам, однако, провода к считывателям должны прокладываться отдельно от силовых и сигнальных (телефонных, компьютерных и т. п.) линий, чтобы избежать возможных сбоев в работе считывателя.

2.5.5 В случае подключения считывателей с клавиатурой, в зависимости от типа возвращаемых кодов, может потребоваться калибровка. Калибровка возможна в течение 10 минут после подачи питания на модуль. Для калибровки необходимо набрать на клавиатуре последовательность 123456789*0#, набирая каждый символ дважды. Калибровку при необходимости нужно проводить для обоих считывателей.

2.5.6 Если считыватель имеет инвертированное управление световой или/и звуковой индикацией, то есть выключенное состояние соответствует высокому уровню, а включенное – низкому, то необходимо установить перемычки ACT-LED или/и ACT-BEEP.

2.6 Подключение дверных замков

2.6.1 Модуль обеспечивает управление практически любыми исполнительными устройствами за счет использования реле с нормально замкнутыми (NC) и нормально разомкнутыми (NO) контактами, а также за счет возможности программирования времени срабатывания реле в широких пределах.

2.6.2 Замки можно подключить к отдельным источникам питания соответствующей мощности. Для удобства подключения замка оба реле на плате модуля снабжены дополнительными колодками, что позволяет встраивать реле в разрыв обоих проводов питания замка.

2.7 Замки, отпираемые и запираемые напряжением

2.7.1 К замкам, отпираемым напряжением, относятся практически все представленные на рынке электромагнитные защелки, большинство накладных и врезных электромеханических замков. Отпирание такого замка осуществляется подачей на него напряжения, причем электромагнитные защелки, как правило, остаются открытыми на все время подачи напряжения, а многие электромеханические замки открываются подачей короткого (порядка 1 секунды) импульса напряжения, после чего для перевода в закрытое состояние требуют открывания и последующего закрывания двери (механический перевзвод).

2.7.2 К замкам, запираемым напряжением, в первую очередь относятся электромагнитные замки, а также некоторые электромагнитные защелки. До подключения замка и программирования его параметров следует внимательно ознакомиться с прилагаемой к нему инструкцией.

2.7.3 Кабель между контроллером и замком должен быть такого сечения, чтобы падение напряжения на кабеле не приводило к падению напряжения на замке ниже минимально допустимого.

2.8 Подавление выбросов на замках

2.8.1 Все замки, управление которыми осуществляется коммутацией силовой обмотки электромагнита, для подавления выбросов напряжения должны быть зашунтированы диодами, включенными в обратном направлении, или варисторами. Такая защита предотвращает сбои или выход оборудования из строя при бросках напряжения на обмотках замков. По возможности, диод должен устанавливаться непосредственно на клеммах замка. Только при невозможности выполнения данного условия допускается установка диода на клеммах контроллера. Однако в этом случае при использовании длинных линий возможны сбои в работе оборудования.

2.9 Подключение турникетов

2.9.1 При использовании контроллера для управления турникетом схема подключения модуля будет отличаться от схемы подключения замка. Это связано, в первую очередь, с тем, что для управления турникетом необходимо формировать два независимых управляющих сигнала для открывания турникета на вход и для открывания на выход. Естественно, при этом модуль используется в режиме двустороннего прохода, то есть с двумя считывателями. Релейный выход 1 (К1) работает на вход, а выход 2 (К2) работает на выход.

2.9.2 Поскольку режим турникета предназначен для обслуживания двусторонней точки прохода, оборудованной быстродействующим турникетом типа «трипод», то при большом потоке людей некоторые функции контроллера в этом режиме недоступны, поскольку лишены физического смысла, например:

- отсутствует понятие «взлом» (поворот турникета без подачи открывающего сигнала) и не выдается соответствующее событие;

– восстановление питания замка происходит в начале (а не в конце, как для двери) импульса поворота для обеспечения надежного запирания турникета после прохода. В некоторых случаях, такое поведение может приводить к проблемам, если датчик срабатывает ранее чем запорный механизм выходит из зацепления (конструктивные особенности турникета). В таком случае можно добавить задержку возврата состояния замка от момента срабатывания датчика.

2.9.3 Чтобы через турникет по одной карте не могли пройти два и более человек, необходимо к входам DOOR1 и DOOR2 клеммной колодки на плате модуля подключить датчик поворота турникета. А в веб-интерфейсе указать датчики прохода. В этом случае время замка будет сбрасываться после фактического поворота турникета.

2.9.4 Схема подключения зависит от количества датчиков поворота турникета (1 или 2), а также порядка их срабатывания. В случае, если турникет имеет два датчика, каждый из которых срабатывает при повороте только в одном направлении (один датчик только на вход, другой только на выход), следует подключать турникет к DOOR1 и DOOR2.

2.9.5 Если же турникет снабжен только одним датчиком поворота, или двумя датчиками, каждый из которых срабатывает при повороте в обоих направлениях, следует использовать схему с подключением одного датчика к обоим входам на плате. В противном случае возможно двойное срабатывание дверного контакта за один поворот турникета.

Примечание – В турникетах разных производителей логика работы датчиков поворота может быть различной. Поэтому, при подключении турникета к контроллеру может потребоваться специальный модуль сопряжения от производителя турникета. Помимо этого, у турникетов различных марок также отличается длина импульса, а для нормальной работы модуля она должна составлять не менее 50 миллисекунд. Модуль сопряжения должен приводить длину импульса к необходимой величине. Для уточнения необходимости установки такого модуля следует обратиться к своему поставщику системы.

2.9.6 К модулю со считывателями, подключенному в турникетном режиме, для открывания турникета на вход и на выход могут подключаться кнопки EXIT1 (открывание турникета на вход) и EXIT2 (открывание турникета на выход).

2.9.7 В турникетном режиме входы датчиков проворота настраиваются в зависимости от уровня сигнала срабатывания датчика(-ов) поворота. Если при фиксации поворотного механизма турникета на выходе датчиков наблюдается разомкнутый контакт, а при повороте состояние меняется на замкнутый, ничего не нужно настраивать. Если при фиксации поворотного механизма турникета на выходе датчиков наблюдается замкнутый контакт, а при повороте состояние меняется на разомкнутый, необходимо включить инверсию датчиков проворота для точки прохода в интерфейсе контроллера (через **«Дополнительные параметры»**).

2.10 Кнопка запроса на выход

2.10.1 Кнопка запроса на выход (EXIT) позволяет человеку, находящемуся внутри помещения, открыть дверь, не вызвав тревоги из-за срабатывания дверного контакта. Если состояния двери не отслеживаются, то изнутри ее можно открывать механически. Кнопка EXIT не является обязательным элементом системы, однако, если система не поддерживает механического открывания изнутри, то ее наличие необходимо.

2.10.2 Поскольку замыкание выводов EXIT приводит к открыванию замка, необходимо обеспечить, чтобы провода кнопки запроса на выход были недоступны с внешней стороны двери (например, при снятии считывателя со стены). Наряду со считывателем, EXIT в турникетном режиме может использоваться для открытия на выход турникета, защищенного контроллером.

2.10.3 Обычно кнопка запроса на выход не подключается при установке двух считывателей (на вход и на выход), а также, если дверь изнутри должна открываться механически (например, с помощью штатной ручки механического врезного замка, работающего в паре с электромагнитной защелкой). Если кнопка EXIT устанавливается, то ее контакты должны быть нормально разомкнутыми и замыкаться при нажатии. Кнопку не обязательно размещать рядом с дверью. Ею может управлять, например, секретарь со своего места. Параллельно можно включить более одной кнопки.

2.11 Дверные контакты

2.11.1 Дверные контакты (DOOR) необходимы для контроля состояния двери. С их помощью определяется, закрыта или открыта дверь. При использовании дверного контакта система может выдавать предупреждение о том, что дверь слишком долго остается открытой, определять несанкционированное открытие двери (взлом), своевременно отключать замок.

2.12 Схема подключения дверного контакта

2.12.1 Дверной контакт всегда подключается с контролем линии. Линия с контролем состояния позволяет определять не только замкнутое или разомкнутое состоянием контактов, но и короткое замыкание или обрыв линии, как это делается в системах сигнализации. Система обеспечивает более высокий уровень безопасности.

2.12.2 Для использования схемы с контролем линии (подводящих проводов) необходимо использовать два резистора. Резисторы могут быть на минимальную мощность рассеивания (например, 0,125 Вт). Номинал резисторов 4,7 кОм.

2.12.3 При использовании дверного контакта в системе могут генерироваться следующие сообщения:

- **«Взлом двери»** – для привлечения внимания при вскрытии двери;
- **«Дверь оставлена открытой»** – генерируется по истечении заданного времени, позволяет определить незакрытые двери;
- **«Обрыв линии»** – повреждены (обрыв) провода шлейфа дверного контакта;
- **«Короткое замыкание»** – повреждены (короткое замыкание) провода шлейфа дверного контакта.

2.12.4 Дверной контакт должен находиться в замкнутом состоянии всегда, когда дверь закрыта, и в разомкнутом состоянии всегда, когда дверь открыта.

2.12.5 Для предотвращения ложных тревог следует выполнить следующие действия:

- убедиться, что дверной контакт не срабатывает при люфтах двери, отрегулировать положение двери и дверного контакта;
- для обеспечения закрывания двери оборудовать ее доводчиком.

2.12.6 При использовании системы управления турникетами контакты DOOR подключаются к датчикам поворота турникета. Это позволяет закрывать турникет после его поворота для исключения множественного прохода.

2.13 Охранный датчик

2.13.1 Модуль позволяет подключить до двух шлейфов безадресных датчиков.

2.13.2 Питание датчиков можно осуществлять от встроенного источника питания модуля (для модулей со встроенным источником), при этом ток потребления датчиков вычитается из максимального тока, обеспечиваемого модулем. Напряжение питания можно взять с соответствующих разъемов клеммных колодок.

2.14 Реле

2.14.1 Модуль снабжен двумя реле, причем на клеммные колодки выведены все три контакта каждого реле – общий (COM), нормально замкнутый (NC) и нормально разомкнутый (NO).

2.14.2 Контактные группы каждого реле позволяют коммутировать постоянный ток до 3 А при напряжении 30 В.

2.15 Контроль вскрытия корпуса устройства

2.15.1 На плате контроллера, помимо микропереключателя вскрытия корпуса, имеется разъем контактов для подключения внешнего датчика вскрытия корпуса контроллера (обозначен на плате контроллера как TAMPER). Он используется для изделий в металлическом корпусе. Корпус считается открытым, если микропереключатель и контакты внешнего датчика разомкнуты. Для предотвращения сигнала о вскрытии корпуса при проведении работ необходимо установить на разъем перемычку.

2.16 Аварийный выход

2.16.1 Любая дверь, используемая для эвакуации (например, при пожаре), должна быть оборудована средствами, открывающими замок в аварийной ситуации. Обычно на такой двери устанавливается замок, запираемый напряжением, снабженный также аварийной кнопкой, включенной в цепь питания замка. При нажатии кнопки замок открывается независимо от состояния системы управления доступом.

2.16.2 В некоторых случаях можно использовать возможности контроллера (например, вход SENS1) для аварийной разблокировки дверей, подключенных к контроллеру. В таком случае к контактам подключается система пожарной сигнализации либо кнопка аварийного открывания двери.

2.16.3 Следует учитывать данные особенности при использовании этих контактов контроллера и при проектировании подводки проводов данной цепи, поскольку можно легко нарушить защищенность помещения.

2.16.4 Повреждение контроллера или коммуникаций может привести к тому, что аварийный выход не будет функционировать, поэтому данную цепь нельзя использовать как главный механизм противопожарной безопасности.

2.17 Средства индикации

2.17.1 Изделия в пластиковом корпусе снабжены видимой индикацией:

- питание подключено;
- обмен по первому каналу;
- обмен по второму каналу;
- ошибки или особые режимы работы.

2.17.2 В случае с металлическим корпусом индикация недоступна. Все параметры могут контролироваться через веб-интерфейс или при открытой крышке.

2.18 Подключение к Ethernet

2.18.1 Подключение устройства к сети Ethernet производится стандартным сетевым кабелем. Для подключения данного кабеля плата контроллера снабжена Ethernet-разъемом (RJ-45). В сети Ethernet каждый контроллер занимает один IP-адрес.

2.18.2 Контроллер поддерживает USB Wi-Fi-модуль TP-LINK TL-WN725N (не входит в комплект с устройством) для локальной настройки. Если нет возможности соединения контроллера с проводной сетью, то при подключении к нему USB Wi-Fi-модуля контроллер создаст Wi-Fi-точку доступа с именем SKD_AP_XXXXXXXX, где XXXXXXXX – серийный номер контроллера. Пароль: abc12345. С помощью этой точки доступа контроллером можно управлять удаленно.

3 Начало работы

3.1 Первый запуск контроллера

3.1.1 По окончании монтажа необходимо подключить кабель сетевого соединения Ethernet и подать питание на контроллер и модули.

3.1.2 Следует иметь в виду, что первый запуск контроллера может занять до 7 минут (идет процесс распаковки и установки встроенного программного обеспечения). В течение этого времени индикатор ошибки будет моргать двойными импульсами раз в две секунды.

3.2 Обнаружение контроллера

3.2.1 Контроллер настроен заводом-изготовителем для работы в режиме DHCP. То есть при подключении к сети он получит автоматически IP-адрес от сервера DHCP. Если в системе отсутствует DHCP или точка подключения находится за маршрутизатором с фильтрацией трафика, возможно подключение контроллера непосредственно к компьютеру. В этом случае контроллер получит так называемый link-local-адрес.

3.2.2 Для поиска контроллера в сети используется протокол обнаружения UPNP. При любом из вышеперечисленных подключений, контроллер появится в сетевом окружении под названием **«RUBEZH STR20-IP»** или **«RUBEZH КД-PRO»** с указанием серийного номера устройства. При выборе этого устройства будет автоматически запущен веб-интерфейс управления. Заводом-изготовителем предустановлены следующие логин и пароль: **«admin»**, **«abc12345»**.

3.2.3 Для обнаружения контроллера убедитесь, что в сетевых настройках вашего ПК параметры «IP версии 4» и «IP версии 6» выставлены на автоматическое получение адресов. Сетевые настройки контроллера могут быть любые (статический или динамически IP адрес) они не влияют на подключение к ПК на прямую. По умолчанию в контроллере установлен динамический IP адрес.

Важно! Если подключение контроллера напрямую к ПК проводное, WiFi модуль на плате контроллера должен быть ***отключен****.*

3.2.4 После подачи питания контроллер отобразиться в сетевом окружении примерно через одну минуту.

3.3 Начальная настройка контроллера

3.3.1 Сразу после активизации контроллера необходимо провести ряд настроек для его корректной работы в дальнейшем. Все настройки устройства находятся в пункте меню **«Настройки контроллера»**. Данные настройки являются уникальными для каждого устройства и должны быть установлены через его веб-интерфейс сразу после включения устройства.

3.4 Установка сетевых параметров

3.4.1 Прежде чем продолжать работу с контроллером, необходимо установить правильный режим работы сети.

3.4.2 Контроллер поддерживает два режима работы в сетях Ethernet:

3.4.3 **«Динамический IP»**. В этом случае все параметры будут установлены автоматически с помощью DHCP-сервера согласно настроенной политике;

3.4.4 **«Статический IP»**. В этом случае необходимо установить фиксированный IP-адрес и прочие параметры сети вручную согласно параметрам сети.

3.4.5 После применения настроек, в случае динамического IP, связь с контроллером может пропасть. В таком случае необходимо осуществить его поиск в сетевом окружении заново (см. раздел Обнаружение контроллера).

3.5 Установка времени

3.5.1 Для корректной работы системы, в частности для правильного ведения журнала событий, необходимо установить часы контроллера. Для задания времени вручную, сначала необходимо установить дату и часовой пояс. Потом задать время.

3.5.2 В качестве более простого и быстрого способа можно использовать кнопку **"Синхронизировать с ПК"**. В этом случае, на контроллере будут установлены параметры даты и времени (включая часовой пояс) с компьютера. Если контроллер при этом находится в другом часовом поясе (удаленное подключение), то необходимо просто изменить часовой пояс после этого.

3.5.3 Дополнительно, контроллер поддерживает синхронизацию времени через NTP-сервер. В этом случае следует указать доступный сервер и часовой пояс контроллера. Остальные параметры будут установлены автоматически.

3.6 Поиск устройств на линии

3.6.1 Так как контроллер взаимодействует с оборудованием точки доступа через модули, то необходимо активизировать их в системе. OSDP-устройства

3.6.2 Адрес модуля доступа устанавливается с помощью колодки DIP переключателей. У всех устройств на линии адреса должны быть разными. Адрес по колодке определяется в двоичном виде и равен сумме чисел, соответствующих включенным переключателям 1-5 (от младшего к старшему). Максимальным значением адреса является 031 (001+002+004+008+016). При изменении адреса модуль необходимо перезагрузить по питанию.

3.6.3 По результатам поиска будет выдана таблица найденных устройств с указанием их скорости обмена. В случае, если устройство поддерживает OSDP-команду смены скорости, то имеется возможность переключить найденные устройства на нужную скорость обмена (модули поддерживают эту команду).

3.6.4 В результатах поиска всегда присутствует сама плата контроллера для возможности использования датчиков SENS1 и SENS2. Под контроллер на линии OSDP зарезервирован адрес 126. Однако, для удобства пользователя, плата контроллера показывается под адресом 0. OSDP-устройства также будут представлены в этой таблице с указанием модели и производителя.

3.6.5 Для использования найденного устройства в системе необходимо нажать кнопку **«Добавить»** в интерфейсе поиска устройств.

3.7 Настройки OSDP

3.7.1 Контроллер осуществляет взаимодействие с модулями по шинам OSDP (интерфейс RS-485). Заводом-изготовителем контроллер настроен на оптимальное взаимодействие. Однако, при использовании сторонних OSDP-устройств, может понадобиться изменение параметров линий.

3.7.2 Некоторые устройства требуют дополнительной задержки в процессе опроса, в таком случае следует увеличить **«Интервал опроса»**. Он задается в миллисекундах.

3.7.3 Параметр **«Таймаут ответа»** задает максимальное время ожидания ответа устройства в миллисекундах. Контроллер использует интеллектуальный опрос устройств и опрашивает не отвечающие устройства по одному за цикл опроса. Однако наличие таких устройств добавляет задержку на весь цикл. Данный параметр может быть уменьшен, но необходимо убедиться, что все используемые устройства достаточно быстрые.

3.7.4 Скорость линии необходимо установить по самому медленному устройству на линии. Все модули поддерживают работу на максимальной скорости (заводская настройка).

3.8 Контроль связи OSDP

3.8.1 Контроллер использует данную функцию для анализа состояния запросов и ответов от контроллера к модулям доступа. Индикация состояния качества связи контроллера и модуля доступа представлена в интерфейсе в виде строки состояния, цвет которой зависит от количества неудачных ответов на запросы контроллера:

- неудачных ответов менее 5% – зеленый цвет;
- неудачных ответов более 5%, но менее 40% – желтый цвет;
- неудачных ответов более 40 % – красный цвет.

3.9 Обновление

3.9.1 Контроллер поддерживает обновление встроенного ПО через веб-интерфейс. Текущую версию можно посмотреть в заголовке панели. При нажатии на информацию о версии ПО открывается таблица версий всех программных компонент.

3.9.2 Для обновления необходимо выбрать файл обновления (на данный момент файлы располагаются на сайте продукта и могут быть скачаны оттуда) и установить его. В контроллере присутствует защита от неправильного файла обновления. Если файл обновления не подходит, то будет выдано сообщение о соответствующей ошибке. Обновление проводится в режиме отката по ошибке. Если в процессе обновления возникнет какая-нибудь ошибка, то система будет автоматически восстановлена на состояние до начала обновления.

3.9.3 Обновление идет без полной остановки работы контроллера. В процессе обновления возможны короткие периоды неактивности контроллера. На некоторых фазах перезапускаются компоненты, в этом случае в интерфейсе могут показываться ошибки связи. Данное поведение считается нормальным.

3.9.4 В процессе обновления присутствует индикация в виде трехкратного мигания красным светодиодом с интервалом 2 секунды.

3.9.5 Обновление прошивки сохраняет все настройки контроллера (включая зарегистрированные карты, пользователей и журналы). Таким образом, контроллер может продолжать использоваться со всеми своими настройками сразу после обновления ПО.

3.9.6 Через веб-интерфейс контроллера можно обновить программное обеспечение модулей. Действия аналогичные обновлению контроллера.

3.9.7 Пакеты обновления могут быть полные (слово FULL в названии файла) и инкрементальные. В некоторых случаях может потребоваться поставить специальную прошивку для отладки (слово DEVELOP в названии файла). В такой прошивке присутствует инструмент удаленного мониторинга журналов и удаленного доступа.

3.10 Мониторинг состояния (ONVIF)

3.10.1 Контроллеры поддерживают несколько способов передачи информации о своем состоянии во внешние средства мониторинга.

3.10.2 Контроллеры поддерживают передачу информации о сетевой активности, состоянии системы хранения данных и загрузке процессора по протоколу SNMP.

3.10.3 Для работы на объектах транспортной безопасности, контроллеры поддерживают ONVIF протокол систем мониторинга оборудования объектов транспортной инфраструктуры. Для его активизации необходимо установить параметры авторизации.

3.11 Перезагрузка контроллера

3.11.1 Веб-интерфейс поддерживает функцию перезагрузки контроллера в случае необходимости.

3.11.2 Если контроллер перестал отвечать на API-запросы, можно перезапустить REST-сервер.

3.12 Возврат заводских параметров

3.12.1 Если в процессе настройки сетевых параметров контроллера возникли нерешаемые трудности, или забыт пароль доступа в систему, есть возможность вернуть его к заводским настройкам. Для этого следует открыть крышку и удерживать кнопку RESET в течение 10 секунд. Удерживать кнопку необходимо до появления однократного мигания красного светодиода с интервалом 1 секунда. После отпускания кнопки все пользовательские данные будут стерты, однако все обновления ПО сохранятся.

3.12.2 В случае, если необходимо вернуть контроллер к заводской прошивке и полностью стереть все данные и настройки, удерживайте кнопку RESET в течение 20 секунд до начала второго однократного мигания красного светодиода с интервалом 1 секунда. После отпускания кнопки контроллер перезагрузится и начнет процесс восстановления. О чем будет свидетельствовать индикация красного светодиода (двойные импульсы раз в 2 секунды). Процесс восстановления занимает порядка 7 минут.

3.13 Системный журнал и диагностика

3.13.1 В некоторых случаях может понадобиться диагностика работы системы для поиска проблемы или программной ошибки. Панель **«Системный журнал»** позволяет включить вывод внутренней отладочной информации и сохранить ее в файл. После этого, файл может быть отослан в службу технической поддержки для анализа поведения. Важно, в файл не записывается секретная информация: пароли, пин-коды и так далее. Записи с этими данными маскируются значками ****.

3.14 О системе

3.14.1 Вкладка веб-интерфейса **«О системе»** позволяет посмотреть текущую информацию о контроллере. На вкладке представлена кнопка-маячок (справа в виде лампочки). При нажатии на нее включается 30-секундная индикация красным светодиодом на соответствующем контроллере.

4 Встроенная СКУД

4.1 Общие сведения о встроенной СКУД

4.1.1 Помимо интерфейса настройки, контроллер Rubezh-STRAZH имеет на борту программное обеспечение, реализующее СКУД, использующее стандартные понятия, такие как картотека, пользователи, точки прохода и т.д., для настройки и управления доступом на объекте, анализа событий и мониторинга.

4.1.2 Важное замечание, СКУД является распределенной и может управляться с любого контроллера кластера. Все данные, модифицируемые или создаваемые через веб-интерфейс контроллера, автоматически передаются на все контроллеры кластера.

4.2 Структура веб-интерфейса системы

4.2.1 Веб-интерфейс состоит из навигационной панели наверху страницы и набора окон для просмотра и модификации данных. В некоторых окнах предусмотрена дополнительная категоризация с помощью меню в левой части страницы**.**

4.2.2 Первая страница (активизируется при выборе значка RUBEZH в левом углу навигационной панели) представляет собой панель, где собрана общая статистика по отказам оборудования, проходам, панель важных оповещений, в ней также находится меню часто используемых действий. В меню быстрого доступа в левой части страницы находится ссылка на руководство пользователя, которое размещено в памяти контроллера**.**

4.3 Настройки СКУД

4.3.1 После монтажа и настройки контроллеров и модулей необходимо произвести настройку встроенной СКУД для дальнейшего администрирования системы. Данную **настройку лучше производить с одного контроллера** (через его веб-интерфейс) для исключения путаницы с источниками данных.

4.4 Управление кластером

4.4.1 Если в системе предполагается использование более одного контроллера Rubezh-STRAZH, то, прежде всего, необходимо объединить все контроллеры в единый кластер. После этого, все данные заносимые на одном контроллере автоматически будут синхронизироваться со всеми контроллерами кластера**.**

4.4.2 Начальная синхронизация данных может оказаться достаточно длительной, однако контроллеры могут быть добавлены все сразу, так как поддерживается внутренняя очередь синхронизации**.**

4.4.3 Контроллеры кластера взаимодействуют друг с другом с помощью, децентрализованной распределенной VPN-сети, автоматически устанавливаемой при объединении контроллеров. Сеть построена на протоколе UDP, поэтому необходимо обеспечить передачу UDP-пакетов между маршрутизаторами до всех контроллеров кластера**.**

4.4.4 Обмен данными идет посредством прямого взаимодействия с помощью зашифрованных пакетов. Таким образом, сеть является нечувствительной к отключению от нее отдельных контроллеров**.**

4.4.5 Для добавления контроллеров в кластер следует перейти в панель **«Настройки СКД/Управление кластером»** и начать поиск. Текущий контроллер всегда отмечен символом домика. В процессе поиска контроллер опрашивает сеть по протоколу UPNP в поисках других контроллеров. Если сеть не во всех сегментах поддерживает UPNP, то можно добавить контроллер вручную, указав его IP-адрес.

4.4.6 После того, как список сформирован, следует добавить контроллеры в кластер (нажимая кнопки добавить в веб-интерфейсе для выбранных контроллеров). При добавлении контроллера формируется секретный ключ доступа к внутренней VPN-сети. Поэтому необходимо войти на подключаемый контроллер и подтвердить его включение. Сразу после добавления, контроллер начинает процедуру синхронизации своих данных с данными кластера. Важно, при включении контроллера в кластер, его данные стираются и заменяются данными кластера.

4.4.7 Процедура поиска находит все контроллеры, вне зависимости от того включен он уже в какой-то кластер или нет. При попытке добавления контроллера, принадлежащего другому кластеру, выдается предупреждение.

4.4.8 Контроллер может быть удален из кластера. Однако если вы удаляете из кластера контроллер, выключенный в данный момент, то, очевидно, удаляемому контроллеру не передается информация о его удалении из кластера. Если планируется в дальнейшем использовать этот контроллер, то его будет необходимо или добавить в другой кластер, или сбросить его данные после включения.

4.4.9 Панель управления кластером содержит информацию о состоянии связи и текущих IP-адресах контроллеров. Информация автоматически не обновляется. Для обновления следует нажать специальный значок в правом верхнем углу панели.

4.5 Карта устройств

4.5.1 Можно посмотреть состояние всех устройств кластера в панели **«Настройка СКД/Карта устройств»**. Карта состоит из карточек сегментов контроллер + модули. Для каждого сегмента указывается состояние связи с ним, общее состояние устройств и кнопка удаления устройства из сегмента. Если ранее удалено какое-то устройство, то его можно добавить позже через поиск устройств с того контроллера, к которому устройство подключено. Важно, если компоненты устройств привязаны к точкам прохода, то после удаления устройства нужно будет отредактировать точки прохода.

4.5.2 При раскрытии карточки становится доступным подробное состояние датчиков каждого устройства. Если датчик не используется в системе, то его аварийное состояние (обрыв или короткое замыкание) не является тревожным и индицируется серым цветом.

4.5.3 Из меню «Карта устройств» можно осуществить привязку датчика к оповещению.

4.5.4 В карте устройств можно дать другое (кроме автоматически созданного) описание устройства. Это позволит в дальнейшем работать с устройствами, используя пользовательские имена.

4.6 Резервирование OSDP-линий и адресация оборудования

4.6.1 Для подключенных контроллеров Rubezh-STRAZH можно настроить резервирование OSDP-линий. Резервирование позволит сохранить соединение с подключенными устройствами или их частью в случае обрыва на одной из линий OSDP.

4.6.2 Контроллеру доступны для резервирования две OSDP-линии, он может резервировать как сам себя, так и другие устройства. При настройке резервирования указывается резервный контроллер и до двух резервируемых.

4.6.3 Для начала настройки резервирования нужно выбрать резервный контроллер. Линия резервного контроллера переносится в поле линии, которую она будет резервировать. Так OSDP Line 1 может резервировать OSDP Line 2 самого резервного контроллера или быть перенесена в OSDP Line 1 или 2 резервируемого контроллера, то же относится и к OSDP Line 2 резервного контроллера. Для фиксации полученных настроек и добавления новых резервирований нужно нажать кнопку добавления в правом верхнем углу формы.

4.6.4 Для сохранения полученной конфигурации резервирования после добавления всех резервных контроллеров и их настройки необходимо нажать кнопку “Сохранить”, иначе вся конфигурация будет потеряна после обновления страницы.

4.6.5 В событиях системы в случае работы без обрыва адреса контактов и устройств приходят в соответствии с изначальной адресацией, полученной при добавлении. Когда на одной из линий происходит разрыв в событиях первая цифра адреса – номер линии, меняется на ту, по которой в данной момент доступна связь. Например, если устройство изначально имело адрес /1/4, т. е. добавлено по первой линии, то при настроенном кольцевом резервировании в случае обрыва на первой линии, адрес устройства в событиях изменится на /2/4, в соответствии с номером линии, по которой в данный момент осуществляется связь.

4.7 Оповещения и тревоги

4.7.1 Программное обеспечение позволяет регистрировать в журнале срабатывания и отслеживать статус датчиков, подключенных к входам

контроллеров и модулей. Для этого необходимо указать нормальное состояние датчика (например, если датчик нормально замкнутый, то срабатывание будет происходить при размыкании контактов, если нормально разомкнутый, то при замыкании), присвоить срабатыванию код ошибки (код передается через API во внешние системы) и описание.

4.7.2 Система поддерживает два типа оповещений при срабатывании датчика: **«Предупреждение»** и **«Тревога».** Эти статусы датчика будут отслеживаться как аварийные.

4.7.3 Для исключения лишних оповещений в журнале срабатывания система позволяет настроить дополнительное условие сработки. При выборе режима **«Точка прохода на охране»** датчики будут отправлять оповещения, только если точки прохода находятся в статусе охраны.

4.7.4 В процессе формирования описаний событий имеется возможность указать список входов, к которым подключаются соответствующие устройства. Для указания входов, генерирующих события, можно использовать и карту устройств. В карточке контроллера или модуля будет доступна настройка оповещения о срабатывании входов.

4.7.5 В контроллерах Rubezh-STRAZH со встроенным блоком питания (в металлическом корпусе) реле сигнала «авария» блока питания подключено к датчику контроллера SENS2. Используется нормально замкнутое состояние датчика. Для получения соответствующего события в журнале оповещений, необходимо настроить оповещение по сработке датчика SENS2 контроллера.

4.8 Тревожные события

4.8.1 В системе существует два типа **Тревожного состояния** точки прохода – удержание и взлом. При возникновении одного из них, в системе инициируется **Тревожное событие.**

4.8.2 Тревожное состояние точки прохода можно наблюдать на графплане в виде красного маркера у ТП, и в разделе «Точки прохода» в виде красного восклицательного знака.

Важно! Тревожное состояние ТП отображается на графплане только в том случае, если настроена конфигурация точек прохода, и расставлены маркеры на графическом представлении плана вашего объекта.

4.8.3 Тревожные события будут отображаться в правой верхней части экрана в виде красного виджета «Тревоги», и на главной странице – карточка «Тревоги».

4.8.4 Тревожное состояние отображается в реальном времени, т. е. если положение ТП вернется в исходное состояние, то на графплане красный маркер поменяет цвет, а в разделе «Точки прохода» красный восклицательный знак пропадет.

4.8.5 Тревожное событие будет отображаться пока оператор его не примет. Для этого нужно выбрать виджет «Тревоги», что бы открылась карточка Тревоги, либо перейти на главную страницу. В карточке «Тревоги» отображаются ТП с тревожными событиями. Можно принять как по одному событию на ТП, так и все сразу. На каждое событие можно оставить комментарий, который будет виден в Журнале событий.

4.8.6 После сработки Тревожного состояния в «Журнале событий» во вкладке «Оповещение» появиться запись, а после принятия Тревожного события

во вкладке «Аудит» появиться запись о принятии события.

4.8.7 Для тревожных событий существуют следующие уровни доступа к ним, в зависимости от профиля входа:

- Администратор – видит события и может их принимать
- Оператор – видит события и может их принимать
- Менеджер – видит события, но не может их принимать
- Инсталлятор – не видит события и не может их принимать

4.9 Точки прохода

4.9.1 Точки прохода являются основным понятием системы при описании правил прохода. Они являются программным объектом, описывающим реальные двери, турникеты и прочие устройства ограничения доступа.

4.9.2 В системе поддерживаются несколько типов точек прохода:

- односторонняя;
- двусторонняя;
- турникет;
- турникет с картоприемником;
- шлагбаум;
- шлюз и т. д.

4.9.3 Описание точки прохода содержит информацию о ее режиме работы, типе, названии, свойствах и устройствах, которые осуществляют получение данных карт, сигналы состояния точки, управляют замками и т. д. Для разных типов точек реализована различная логика поведения и требуется привязка разного оборудования. Элементы оборудования, прикрепляемые к

точке прохода, необязательно должны находиться на одном модуле. При необходимости, можно подключать элементы разных модулей. Однако в целях повышения надежности работы, все используемые для конкретной точки модули должны быть подключены к одному контроллеру. Интерфейс настройки точки прохода не позволяет использовать элементы модулей с разных контроллеров.

4.9.4 Элементы модулей можно выбирать в конкретных пунктах, при настройке точки прохода (вкладка «Настройки СКД», раздел «Точки прохода»).

4.9.5 Не все элементы являются обязательными. В зависимости от оборудования конкретной точки, часть элементов может отсутствовать. Например, точка может не иметь кнопки дистанционного открытия или датчика положения двери. В случае, если какой-либо элемент не используется, то соответствующее поле в настройке не заполняется.

4.9.6 В системе существует набор дополнительных параметров точек прохода. Установленные заводом изготовителем значения применяются для всех точек. При необходимости, для каждой точки можно установить свои значения параметров с помощью выпадающего списка **«Дополнительные параметры»**:

- **«Время закрытия замка двери после локального открытия»** – время от момента поднесения карты к считывателю до момента закрытия замка. Изменение этого параметра в большую сторону может потребоваться для автоматизированных дверей шлюзов. В противном случае могут появляться события несовершенных проходов;
- **«Время закрытия замка двери после удаленного открытия»** – время от момента нажатия кнопки дистанционного открывания до момента закрытия замка. Использование аналогично предыдущему параметру;
- **«Максимальное время удержания двери»** – время, в течении которого контроллер ожидает срабатывание датчика закрытия двери;
- **«Время действия ограничений зонального контроля»** – время, через которое будет сброшена защита от попытки прохода с нарушением зоны, после последней такой попытки на точке;

- **«Звуковая индикация срабатывания считывателя»** – подача звукового сигнала на считывателе при поднесении карты к считывателю. Имеется ввиду управление звуком со стороны контроллера. Большинство считывателей имеет свой собственный звуковой сигнал при считывании карты, выключение которого осуществляется утилитами производителя или аппаратно;
- **«Световая индикация срабатывания считывателя»** – наблюдается мигание светового индикатора при поднесении карты к считывателю. Имеется ввиду управление световой индикацией со стороны контроллера. Большинство считывателей имеет свою собственную индикацию, отключение которой осуществляется утилитами производителя или аппаратно;
- **«Пин-код точки прохода»** – при его указании точку можно будет разблокировать с помощью единого кода. Точка должна в этом случае иметь считыватель с клавиатурой. Данная настройка не связана с методом идентификации и позволяет независимо от него совершить неавторизованный проход по указанному пин-коду;
- **«Датчик прохода/проезда/положения двери нормально замкнутый»** – данный режим позволяет изменить тип датчика с нормально замкнутого на нормально разомкнутый;
- **«Импульсное реле подъема шлагбаума»** – управление происходит в импульсном режиме, то есть подаются кратковременные импульсы на открытие/закрытие, а далее блок управления шлагбаумом отрабатывает команды по заданному алгоритму;
- **«Длительность импульса на реле шлагбаума, мс»** – длина импульса срабатывания реле открывания шлагбаума в миллисекундах;
- **«Шлагбаум закрывается самостоятельно»** – при выборе данного режима закрытие шлагбаума осуществляется контроллером шлагбаума;
- **«Количество неудачных попыток входа подряд до блокировки»** – сторона точки прохода блокируется на заданное время после указанного количества подряд попыток поднесений к считывателю несоответствующих карт или введений неверного ПИН-кода; Событие блокировки наступает на следующее после указанного количества попыток событие вне зависимости от правильности карты или пина;

- **«Время блокировки двери после превышения лимита неудачных попыток доступа»** – период, на который дверь будет заблокирована для нового доступа;
- **«Проход по разовым картам со стороны А запрещен»** – проход по разовым картам заблокирован со стороны А;
- **«Проход по разовым картам со стороны В запрещен»** – проход по разовым картам заблокирован со стороны В. Данная настройка не влияет на картоприемник со стороны В;
- **«Разрешить аварийный выход при потере связи»** – при выборе этого режима, в случае аварийной ситуации (повреждение кабеля питания, отключение электричества и т.д.), контроллер будет разрешать проход с одной из сторон при поднесении любой карты или при нажатии кнопки;
- **«Аварийный выход со стороны А»** – при выборе этого режима стороной аварийного выхода будет считаться сторона А, в противном случае – это сторона В;
- **«Проход под принуждением запрещен»** – запрет режима прохода под принуждением. В случае, если он разрешен, то при принуждении ко входу через точку с клавиатурным считывателем, персона должна ввести последнюю цифру пин кода на единицу меньше, чем реальное значение или 9 вместо 0 (например, для кода 1234 – это будет 1233, для кода 1230 – это будет 1239). В этом случае, точка прохода разблокируется, но на пост охраны и в журнал пойдет событие прохода под принуждением. Если проход под принуждением запрещен, то точка прохода не будет разблокирована, однако событий прохода под принуждением в журнал пойдет;
- **«Задержка при постановке на охрану через код на считывателе, в секундах»** – время на выход персоны перед постановкой на охрану в случае, если считыватель стоит внутри зоны;
- **«Количество человек, необходимое для прохода»** – указание необходимого количества человек для открывания точки прохода. Необходимо поднести указанное количество разных карт с правами доступа на точку;
- **«Максимальное время ожидания множественного прохода, в секундах»** – время, в течение которого система ожидает прикладывания карт при множественном проходе;

- **«Подтверждение прохода внешней системой»** – используется при взаимодействии с мобильным приложением или внешним ПО (например, R-платформой). При разрешенном доступе на точку прохода система будет ожидать подтверждения от внешней системы;
- **«Максимальное время ожидания подтверждения прохода внешней системой, в секундах»** – время, после которого проход будет разрешен или запрещен автоматически;
- **«Время ожидания перед блокировкой турникета»** - время от момента разблокировки до срабатывания запорного механизма турникета;
- **«Разрешить проход с подтверждением при недостаточном уровне привилегий» -** при выборе этого режима, при проходе с недостаточным уровнем привилегий не придет сразу запрет на проход, а запустится ожидание подтверждения от внешней системы, для работы данного режима также нужно включить параметр «Подтверждение прохода внешней системой»;
- **«Разрешать доступ после истечения времени ожидания внешнего подтверждения» -** при выборе этого режима, в случае если от внешней системы не пришел ответ проход будет разрешен, а не запрещен, данный режим используется при взаимодействии с параметром «Подтверждение прохода внешней системой»;
- **«Величина добавочного уровня привилегий пин-кода»** - уровень привилегий, добавляемый при введении пин-кода. Точка должна в этом случае иметь считыватель с клавиатурой;
- **«Точка прохода используется для автопостановки на охрану личной точки сотрудника» -** при проходе через данную точку запускается автопостановка на охрану личной точки, если в ее помещении не осталось ни одного посетителя, при данном режиме контроллер, к которому подключена точка хранит карту личных точек и отслеживает присутствие владельцев точек на объекте, для корректного подсчета на нескольких точках, нужно чтобы все они были подключены к одному контроллеру;
- **«Сторона В используется как вход для определения автопостановки на охрану» -** при проходе через данную точку при подсчете контроллером присутствующих владельцев точек для автопостановки на охрану будет учитываться обратное направление прохода.

4.9.7 Если в системе есть точка прохода со всеми требующимися характеристиками, то по ее подобию можно создать новую точку прохода.

4.9.8 Типовую точку прохода можно создавать из раздела устройств с модуля доступа, в таком случае будет использоваться типовая схема подключения оборудования точки.

4.9.9 Точки прохода односторонняя, двусторонняя, турникет, турникет с картоприемником, шлюз, поддерживают идентификацию по карте, карте и пин-коду, карте или пин-коду, по биометрическим параметрам и многофакторную авторизацию. Точка прохода типа шлагбаум, поддерживает те же методы идентификации что и остальные, плюс по номеру (Госномер), номеру и карте, номеру или карте.

4.9.10 Для точек прохода, в случае карты или пин-кода можно получить доступ вводя персональный код, не используя карту, персональный код указан в карточке сотрудника. Важная особенность, система не запрещает вводить одинаковые пин-коды. Проверка кода на уникальность осуществляется в момент его предъявления. В случае, если введенный пин-код указан у нескольких сотрудников, доступ не предоставляется, а в журнал заносится соответствующее событие. Пин-код самой точки прохода можно использовать в любом режиме, в этом случае в журнал не заносится информация о том, кто именно получил доступ.

4.9.11 Для точки типа шлагбаум, в настройках данной точки, предусмотрен пункт датчик проезда (создан для регистрации факта проезда), с ним можно связать датчик безопасности/проезда. Если данного датчика нет, то факт проезда будет регистрироваться при подаче команды на реле подъема.

4.9.12 Персональный код и пин-код точки прохода требуют подтверждения ввода кнопками «ENT» или «#». Для удаления неверного ввода можно использовать – «ESC» или «*» - данная кнопка удаляет последний

введенный символ, несколько нажатий удаляет несколько введенных символов равное количеству нажатий.

4.9.13 К каждой точке прохода может быть привязана одна или две метки территории или зоны, которые она разделяет. Односторонняя точка не поддерживает контроля перемещений и поэтому всегда находится в одной зоне. Двусторонняя точка разделяет две зоны. Метка зоны – текстовая строка, однако для удобства навигации, она разделена на три части: здание, этаж, зона. Внутренний формат метки – **«зона:этаж:здание»**. Метка, как и любые ее части не являются обязательными. Однако если метка не задана, то некоторые функции будут недоступны, например, зональный контроль.

4.9.14 При каждом успешном пересечении точки прохода система запоминает зону, на которой оказался посетитель. Зона привязывается к человеку, поэтому неважно, какой картой он идентифицировался. Таким образом, внутреннее ПО постоянно отслеживает местонахождение всех посетителей. Эта информация синхронизируется между всеми контроллерами кластера, то есть является глобальной. Если на какой-либо точке включен контроль зоны в направлении перемещения посетителя, то идет проверка является ли эта зона соседней и не находится ли посетитель в ней уже (частный случай АПБ). Если это не так, то точка прохода не разблокируется и порождается событие нарушения зонного контроля. Чтобы такие нарушения не накапливались, в настройках можно задать интервал времени, в течение которого будет действовать запрет повторного прохода этой точки доступа для данного посетителя.

4.9.15 Еще один важный параметр точки прохода – уровень привилегий: ее «важность» или требуемый уровень доверия к идентификатору. Таким образом ограничивается доступ при использовании карт с низким уровнем, даже если у персоны есть доступ через эту точку.

4.9.16 Есть несколько способов повысить уровень привилегий сотрудника в момент авторизации. Для этих целей на точке прохода можно указать метод идентификации по карте и пин-коду или многофакторную авторизацию.

4.9.17 В случае карты и пин-кода, пин-код добавляет к карте то количество привилегий, которое указано для точки доступа в дополнительном параметре «Величина добавочного уровня привилегий пин-кода».

> *Важно! В случае использования метода идентификации «карта и пин-код», ввод пин-кода обязателен, даже если уровень привилегий карты достаточен.*

4.9.18 Для отдельных категорий многоразовых карт, можно организовать проход без ввода пин-кода, при методе идентификации «карта и пин-код». Для этого в доп. привилегиях карты необходимо указать пункт «Упрощенный проход».

4.9.19 В случае многофакторной авторизации каждый следующий идентификатор добавляет относящееся к нему количество привилегий, т.е. допустимо поднести разные типы идентификаторов в любом порядке с задержкой не более семи секунд между ними. После каждого поднесения идентификатора происходит проверка достаточности суммы полученных привилегий, если величина достаточна точка прохода открывается, если нет запускается ожидание следующего идентификатора, в случае если в течении семи секунд нового идентификатора не было предъявлено доступ будет запрещен по причине низкого уровня привилегий предъявленных идентификаторов.

4.9.20 Точка прохода поддерживает настройку нескольких режимов работы, которые можно выбрать в выпадающем списке «Режим работы»:

- **«Дежурный»** – при поднесении карты к считывателю проход разрешается;
- **«Заблокирована»** – при поднесении карты к считывателю проход запрещается. Режим сопровождается морганием красного индикатора (раз в секунду) на считывателях;
- **«Заблокирована со стороны А»** (для односторонней точки прохода – Считыватель заблокирован) – при поднесении карты к считывателю на стороне А проход запрещается. Режим сопровождается морганием красного индикатора (раз в секунду) на считывателе А. При поднесении карты к считывателю на стороне В модуля доступа проход разрешается;
- **«Заблокирована со стороны В»** (для односторонней точки прохода – Кнопка заблокирована) – при поднесении карты к считывателю на стороне В проход запрещается. Режим сопровождается миганием красного индикатора (раз в секунду) на считывателе В. При поднесении карты к считывателю на стороне А модуля доступа проход разрешается;
- **«Разблокирована»** – точка прохода разблокирована и проход разрешается с обеих сторон без использования карт. Режим сопровождается миганием зеленым (раз в две секунды) обоих считывателей;
- **«На охране»** – при поднесении карты к любому из считывателей проход запрещается по причине охраны. Режим сопровождается миганием красным (раз в две секунды) обоих считывателей.

Следует иметь ввиду, что не все считыватели имеют управляемую двухцветную индикацию. Более того, ряд считывателей еще имеет собственную индикацию при считывании карт.

4.9.21 Режим работы точки прохода можно сменить не только с помощью соответствующего веб-интерфейса, но и с помощью клавиатурного считывателя. Для этого необходимо ввести одно символьный код, # и приложить карту с достаточными привилегиями. В системе используются следующие коды:

1# - дежурный;
2# - заблокирована;
3# - заблокирована со стороны А;

4# - заблокирована со стороны В;

5# - разблокирована;

6# - на охране.

4.9.22 Шлюз

Данная точка прохода предназначена для предотвращения несанкционированного прохода, сквозного прохода, разделяет потоки людей или автомобилей и реализована в двух исполнениях:

- автоматическая шлюзовая кабина;
- тамбурный двери.

Автоматизированная шлюзованная кабина:

- оснащена собственным контроллером;
- может иметь двухфакторную авторизацию при проходе: посредством карты доступа и pin-кода;
- может иметь весовую платформу для определения нахождения человека в кабине.

Тамбурные двери:

- работают по шлюзовому алгоритму на базе двух взаимозависимых точек прохода, оснащенных замками и датчиками дверей/шлагбаумов;
- предназначены для предотвращения сквозного прохода, разграничения потоков людей или автомобилей и т. д.

Общие характеристики шлюза:

- система не позволяет открыть внутреннюю дверь, пока не закрыта внешняя;
- проход через шлюз может контролироваться оператором, при этом доступ к внутренней двери может быть предоставлен как оператором (с помощью пульта ручного управления шлюзом), так и посредством кодонаборника (при наличии внутри шлюза);
- если оператор подтверждает проход кнопкой, то в журнале событий отображается событие: «Доступ разрешён ФИО (сотрудник, подтвердивший проход картой доступа)»;
- для точек прохода и карт доступа предусмотрены настраиваемые уровни доступа. В логике шлюза проход предоставляется только в случае, если уровень доступа карты не ниже уровня доступа точки прохода. В ином случае в

настройках интерфейса есть функция, подтверждающая доступ охранником только тогда, когда уровень доступа карты ниже необходимого. Так же для разных посетителей можно настроить разные режимы работы прохода (например, для сотрудников – кнопки на пульте оператора, для остальных – карты доступа);

- на вход и выход предусмотрена несимметричная работа шлюза: на вход требуется подтверждение прохода картой или оператором, на выход – проход свободный;
- двери шлюза оборудованы электромагнитными замками, доводчиком, датчиком прохода, световыми индикаторами состояния занятости шлюза.

4.9.23 Для определения текущего состояния шлюза используется реле индикации занятости. У шлюза есть два состояния: «Свободен» шлюз находится в режиме ожидания и доступен для совершения прохода, индикация реле выключена и «Занят» - шлюз находится в режиме исполнения и не доступен для других проходов, реле индикации включено.

Шлюз переходит в состояние «Занят», при поднесении карты или нажатии кнопки удаленного открытия.

Шлюз выходит из состояния «Занят» и переходит в состояние «Свободен»:

- после завершения алгоритма прохода, пользователь покинул шлюз в прямом направлении, или в обратном в случае запрета прохода от оператора
- после истечения времени ожидания прохода через внешнюю дверь, к которой была поднесена карта или нажата кнопка удаленного открытия двери без совершения прохода
- при бездействии в течении 180 секунд

4.9.24 Алгоритмы прохода через шлюз

Для точки прохода «Шлюз» реализованы три алгоритма прохода: «Стандартный», «3 кнопки», «Устаревший».

Авторизованный проход:

- **Проход без подтверждения** (достаточен уровень привилегий, все алгоритмы шлюза)

Проход A -> B:

– Авторизация на стороне А, дверь открыта и доступен проход в шлюз, шлюз переходит в состояние «занят», сторона В заблокирована внешний считыватель не реагирует на поднесение,

– После прохода в шлюз обе стороны заблокированы, ожидается авторизация на внутреннем считывателе,

– Авторизация на внутреннем считывателе, сторона В разблокирована для выхода, сторона А заблокирована внешний считыватель не реагирует на поднесение,

– После выхода из шлюза, шлюз переходит в состояние «свободен» и вновь доступен для осуществления прохода в одном из направлений;

Проход В -> А:

– Авторизация на стороне В (доступно использование картоприемника с забором карты), дверь открыта и доступен проход в шлюз, шлюз переходит в состояние «занят»,

– После прохода в шлюз сторона А разблокируется автоматически, сторона В заблокирована внешний и внутренний считыватели не реагируют на поднесение,

– После выхода из шлюза, шлюз переходит в состояние «свободен» и вновь доступен для осуществления прохода в одном из направлений.

- **Проход с подтверждением** (недостаточен уровень привилегий)

Алгоритм шлюза – «Стандартный»:

Проход А -> В:

– Авторизация на стороне А, дверь открыта и доступен проход в шлюз, шлюз переходит в состояние «занят», сторона В заблокирована внешний считыватель не реагирует на поднесение,

– После прохода в шлюз обе стороны заблокированы, ожидается подтверждение прохода от оператора или использование пин-кода на внутреннем считывателе, если установлена кодонаборная панель,

– Оператор подтвердил проход ***по кнопке удаленного открытия стороны В*** – проход разрешен, сторона В разблокирована для выхода, сторона А заблокирована внешний считыватель не реагирует на поднесение. В событиях системы будет отметка о подтверждении прохода оператором,

– Оператор запретил проход ***по кнопке удаленного открытия стороны А*** – проход запрещен, разблокирована сторона А для обратного выхода, сторона В заблокирована внешний считыватель не реагирует на поднесение. В событиях системы будет отметка о запрете прохода оператором,

– Введен пин-код добавляющий достаточно привилегий, сторона В разблокирована для выхода, сторона А заблокирована внешний считыватель не реагирует на поднесение,

– Введен пин-код не добавляющий достаточно привилегий, двери заблокированы, ожидание решения оператора,

– После выхода из шлюза, шлюз переходит в состояние «свободен» и вновь доступен для осуществления прохода в одном из направлений;

Проход В -> А

– Авторизация на стороне В (доступно использование картоприемника с забором карты), дверь открыта и доступен проход в шлюз, шлюз переходит в состояние «занят»,

– После прохода в шлюз обе стороны заблокированы, ожидается подтверждение прохода от оператора,

– Оператор подтвердил проход ***по кнопке удаленного открытия стороны А*** – проход разрешен, сторона А разблокирована для выхода, сторона В заблокирована внешний считыватель не реагирует на поднесение. В событиях системы будет отметка о подтверждении прохода оператором,

– Оператор запретил проход ***по кнопке удаленного открытия стороны В*** – проход запрещен, разблокирована сторона В для обратного выхода, сторона А заблокирована внешний считыватель не реагирует на поднесение. В событиях системы будет отметка о запрете прохода оператором,

– После выхода из шлюза, шлюз переходит в состояние «свободен» и вновь доступен для осуществления прохода в одном из направлений;

Алгоритм шлюза - «3 кнопки»:

Проход А -> В:

– Авторизация на стороне А, дверь открыта и доступен проход в шлюз, шлюз переходит в состояние «занят», сторона В заблокирована внешний считыватель не реагирует на поднесение,

– После прохода в шлюз обе стороны заблокированы, ожидается подтверждение прохода от оператора или использование пин-кода на внутреннем считывателе, если установлена кодонаборная панель,

– Оператор подтвердил проход ***по кнопке подтверждения внутри кабинки*** – проход разрешен, сторона В разблокирована для выхода, сторона А заблокирована внешний считыватель не реагирует на поднесение. В событиях системы будет отметка о подтверждении прохода оператором,

– Оператор запретил проход ***по кнопке удаленного открытия стороны А*** – проход запрещен, разблокирована сторона А для обратного выхода, сторона В заблокирована внешний считыватель не реагирует на поднесение. В событиях системы будет отметка о запрете прохода оператором,

– Введен пин-код добавляющий достаточно привилегий, сторона В разблокирована для выхода, сторона А заблокирована внешний считыватель не реагирует на поднесение,

– Введен пин-код не добавляющий достаточно привилегий, двери заблокированы, ожидание решения оператора,

– После выхода из шлюза, шлюз переходит в состояние «свободен» и вновь доступен для осуществления прохода в одном из направлений;

Проход В -> А:

– Авторизация на стороне В (доступно использование картоприемника с забором карты), дверь открыта и доступен проход в шлюз, шлюз переходит в состояние «занят»,

– После прохода в шлюз обе стороны заблокированы, ожидается подтверждение прохода от оператора,

– Оператор подтвердил проход ***по кнопке подтверждения внутри кабинки*** – проход разрешен, сторона А разблокирована для выхода, сторона В заблокирована внешний считыватель не реагирует на поднесение. В событиях системы будет отметка о подтверждении прохода оператором,

– Оператор запретил проход ***по кнопке удаленного открытия стороны В*** – проход запрещен, разблокирована сторона В для обратного выхода, сторона А заблокирована внешний считыватель не реагирует на поднесение. В событиях системы будет отметка о запрете прохода оператором,

– После выхода из шлюза, шлюз переходит в состояние «свободен» и вновь доступен для осуществления прохода в одном из направлений.

Алгоритм шлюза – «Устаревший»

– При недостаточном уровне привилегий проход по данному алгоритму доступен только при вводе пин-кода добавляющего привилегий на входе, после чего работа шлюза повторяет обычный проход без подтверждения. В случае если пин-код не добавляет достаточно привилегий или на входе нет кодонаборной панели, то проход будет запрещен сразу.

Неавторизованный проход:

- Проход по кнопкам удаленного открытия (алгоритмы «3 кнопки» и «Устаревший»)

Проход А -> В:

– Сторона А разблокирована по кнопке, сторона В заблокирована, считыватель не реагирует, кнопка удаленного открытия стороны В так же не работает,

– После прохода в шлюз доступна разблокировка стороны В по кнопке удаленного открытия;

Проход В -> А:

– Сторона В разблокирована по кнопке, сторона А заблокирована, считыватель не реагирует, кнопка удаленного открытия стороны А так же не работает,

– После прохода в шлюз доступна разблокировка стороны А по кнопке удаленного открытия.

- Проход по кнопкам удаленного открытия (алгоритм «Стандартный»)

– Неавторизованный проход по данному алгоритму не доступен, кнопки используются только как кнопки подтверждения авторизованного прохода.

4.10 Графплан

4.10.1 Графплан позволяет настроить графическое представление конфигурации созданных точек прохода в соответствии с планами объекта.

> *Важно! Точки прохода без этажа и/или здания не доступны для использования в графплане.*

4.10.2 Для каждого этажа каждого здания доступна загрузка изображения плана и расположения точек этажа на загруженном плане. ПО СКУД Rubezh-Strazh поддерживает любой популярный формат файлов растровых изображений размером до 20 Мб. Удаление точек и самого плана доступно по правой кнопке мыши. При удалении плана все расположенные на нем точки будут также удалены.

4.10.3 Область этажей можно свернуть и развернуть, переход между этажами и отображение точек происходит по клику на нужном этаже. Для перехода между зданиями нужно нажать на иконку в правом углу в поле с названием здания.

4.10.4 Для каждой точки, расположенной на графплане доступно изменение режима работы в меню этажа.

4.11 План

4.11.1 План дает возможность удобного просмотра карты точек прохода и управления их режимами работы. Управление режимом работы доступно как на самом плане по правой кнопке мыши, так и в меню этажа. Доступно массовое изменение режима работы для всех точек на этаже.

4.11.2 Каждому режиму работы соответствует свой цвет и своя иконка: желтый – на дежурстве, зеленый – разблокирован, синий – на охране, красный – заблокирован (целиком или на одной из сторон). В поле этажа отображаются иконки всех установленных на этаже режимов работы.

4.11.3 Область этажей можно свернуть и развернуть, переход между этажами и отображение точек происходит по клику на нужном этаже. Для перехода между зданиями нужно нажать на иконку в правом углу в поле с названием здания.

4.12 Пост охраны

4.12.1 Пост охраны дает возможность оператору осуществлять мониторинг точек прохода и управлять ими вручную или по заданному алгоритму. Параметры поста охраны можно задать в настройках:

- **«Точка прохода»** – выбор одной или нескольких точек прохода для мониторинга;
- **«Движение из А в В», «Движение из В в А»** – замена посредством мнемоники заданные системой названия вектора движения персоны через точки прохода на более удобные и запоминаемые для пользователя;
- **«Дополнительные поля»** – фильтр, позволяющий задать дополнительные параметры для отображения персон (должность, подразделение, номер импорта).

4.12.2 Функции “заблокировать”, “разблокировать” и “дежурный”: точку прохода можно заблокировать (запретить проход) или полностью разблокировать (например, при перемещении грузов и т. д.), после чего можно вернуться в “дежурный” режим работы.

4.12.3 По центру отображается только карточка последней прошедшей персоны, карточки предыдущих персон распределяются по зонам, в которых они были зафиксированы.

4.13 Автоматизация

4.13.1 Программное обеспечение позволяет изменять режим работы точек прохода по изменению состояния датчика. Данный функционал может быть использован для массового аварийного разблокирования точек прохода по датчику или кнопке либо для блокировки точек по тревожной кнопке.

4.13.2 При сработке выбранного датчика происходит переход в указанный режим. Можно указать автоматический возврат в предыдущее состояние по восстановлению состояния датчика или по времени.

4.13.3 Если состояние точки было изменено вручную или по другому событию после сработки датчика, то возврат в предыдущее состояние не произойдет.

4.13.4 Программное обеспечение поддерживает следующие параметры для настройки каждого датчика:

- **«Имя»** – можно задать любое имя для датчика;
- **«Датчик»** – в выпадающем списке следует выбрать нужный контроллер;
- «**Тип датчика**» – состояние датчика в дежурном режиме. Датчику можно задать один из двух типов: нормально замкнутый или нормально разомкнутый;

- **«Контроль линии»** – можно включить или отключить контроль исправности всех линий связи в системе;
- **«Код активации»** – альтернативный способ запуска автоматизации по двух символьному коду с клавиатурного считывателя. Если код указан, то автоматизация может быть запущена с любого клавиатурного считывателя в системе с помощью следующей последовательности: <код активации> # <карта с достаточными привилегиями>;
- **«Сменить режим работы на»** – это тот режим, в который перейдут точки прохода при получении сигнала от датчика. Варианты режимов работы, следующие: **«Дежурный»**, **«Заблокирована»**, **«Заблокирована сторона А»**, **«Заблокирована сторона В»**, **«Разблокирована»**, **«На охране»**;
- **«Возвращать в исходный режим»** – данный параметр представлен тремя вариантами:

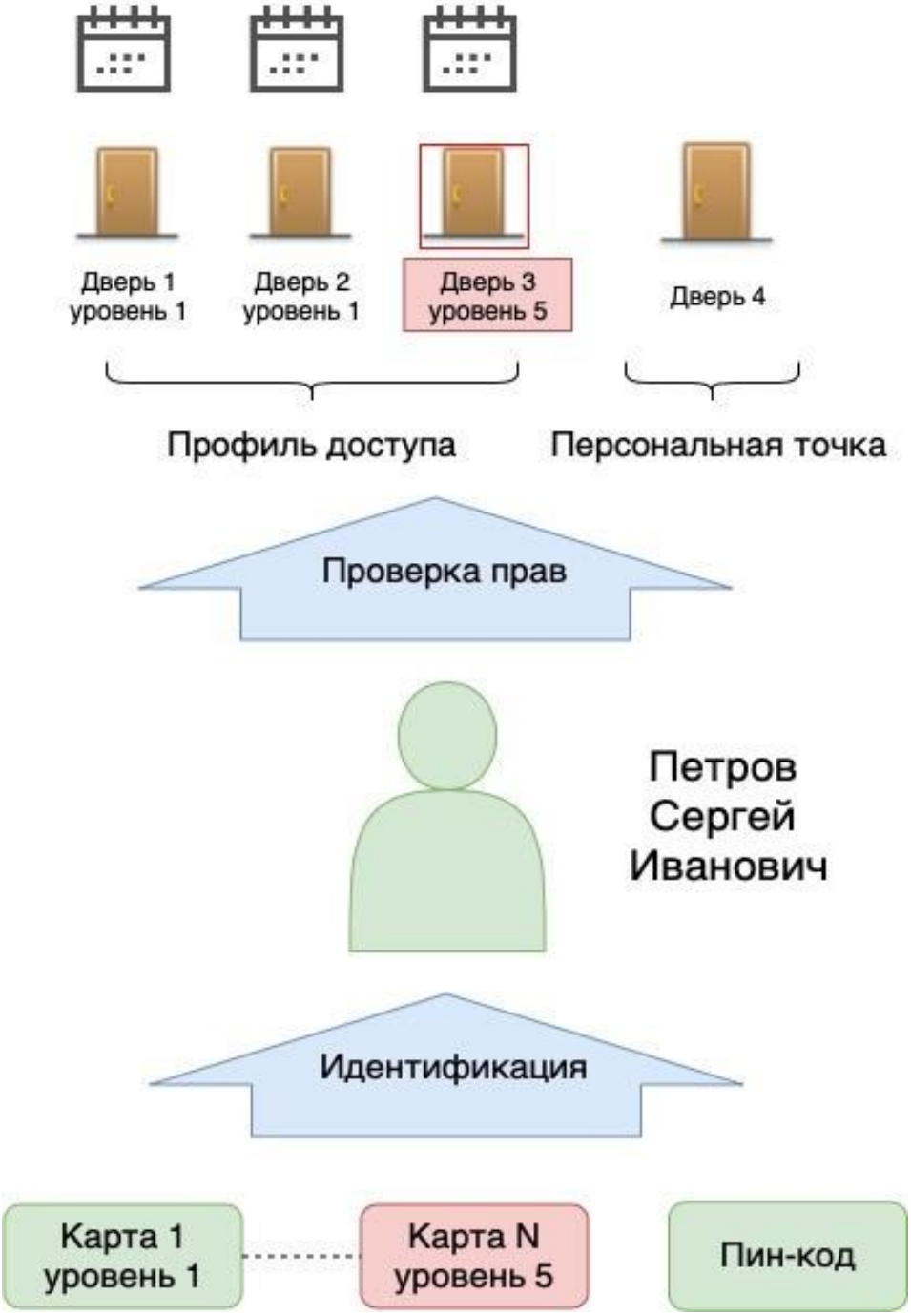
а) **«По датчику»** – при возвращении датчика в исходное состояние точки прохода также переходят в исходное состояние;

б) **«По таймеру»** – заданный режим работы сохраняется, пока не истечет время на таймере;

в) **«Нет»**.

4.14 Схема установки и проверки правил доступа

4.14.1 Основной задачей СКУД является построение набора правил доступа и предоставления соответствующих прав персоналу, который перемещается по территории объекта. Встроенная СКУД использует следующую схему настройки доступа:



4.14.2 RFID-карты и прочие способы идентификации (пин-код, например) определяют персону, которая пытается осуществить доступ через некоторую точку прохода.

4.14.3 Непосредственно к самой карте не привязаны никакие правила доступа. Карта предназначена только для идентификации персоны. У человека может быть зарегистрировано несколько карт (например, разных типов), может быть задан пин-код, в будущих версиях могут присутствовать биометрические данные и т. д. В любом случае, после предъявления карты и/или пин-кода идентифицируется персона.

4.14.4 Каждая персона имеет набор информационных свойств для понимания того, кто этот человек: ФИО, фотография, и прочее. Помимо этого, у каждой персоны может быть указан один профиль доступа (именованный набор точек прохода с расписаниями доступа) и его персональная точка доступа, куда он имеет доступ всегда.

4.14.5 После идентификации персоны идет проверка входит ли точка доступа, где была произведена попытка доступа, в профиль приписанный персоне (совокупность точек прохода и расписаний доступа для них) или является ли она его персональной точкой. Если нет, то доступ не предоставляется. Если да, то дополнительно проверяется, соответствует ли уровень доверия идентификатора минимальному уровню точки. Если да, то доступ предоставляется. Данная дополнительная проверка позволяет модифицировать доступ для внешних (низкий уровень доверия) и внутренних (высокий уровень доверия) идентификаторов в рамках одного набора разрешенных точек доступа.

4.15 Поля персонала

4.15.1 Минимальный набор данных для описания персонала объекта – ФИО. При необходимости, в этот набор можно добавить дополнительные свойства, облегчающие идентификацию и ускоряющие поиск нужного лица в системе. Можно задать свойства трех типов: **«текст»**, **«целое число»** и **«справочник»**. Дополнительно можно потребовать обязательного ввода. Для работы со свойствами через внешнее API имеется возможность задать его идентификатор. Свойства типа “справочник” – это, готовый набор вариантов из которого оператор системы может выбирать значения, например, список должностей.

4.16 Справочники

4.16.1 Для свойств персонала справочного типа имеется возможность создавать справочники значений. Справочники могут быть как строками, так и целыми числами. Каждый справочник имеет свое уникальное название и может быть наполнен как путем ввода значений, так и путем импорта из текстового файла, где каждое значение представлено одной строкой. Справочники ограничены 2000 значений.

4.17 Профили входа

4.17.1 Внутреннее программное обеспечение имеет защиту от несанкционированного доступа, основанную на логинах и паролях. Заводские настройки предусматривают наличие в системе профиля входа с административными правами с логином: **«admin»** и паролем: **«abc12345»**. Удалить или изменить пароль данного оператора нельзя. Однако система позволяет создавать дополнительных операторов. Встроенный в систему admin становится недоступным при создании любого оператора с правами «Администратор». Для того что бы профиль входа admin стал доступен, нужно удалить все созданные профили с правами «Администратор». В текущей версии используется ролевая безопасность. При создании оператора, ему можно предоставить права:

- **«Администратор»** – полный доступ в систему;
- **«Менеджер»** – недоступны настройки оборудования;
- **«Оператор»** – доступны только журналы событий, управление режимом работы точек прохода;
- **«Инсталлятор»** – доступны только настройки оборудования.

4.17.2 Оператор системы может быть ассоциирован с персоной, зарегистрированной с СКУД. В этом случае события в журнал идут от лица этой персоны.

4.17.3 При входе в систему оператор начинает сессию, которая будет автоматически закрыта по истечении времени сеанса. Такое поведение позволяет решить проблему оставленных окон в браузере. Предустановленная в программном обеспечении длительность сессии составляет 10 часов. Для каждого оператора можно задать свою длительность сессии. В правом верхнем углу Web-интерфейса постоянно показывается текущий оператор и оставшееся

время сессии. Если по какой-то причине необходимо продлить сессию, то это можно сделать из меню на индикаторе оператора.

4.18 Администрирование доступа

4.18.1 В данной части интерфейса осуществляется настройка типовых профилей доступа – наборов точек прохода с расписаниями доступа на них.

4.19 Расписания доступа

4.19.1 Расписания доступа определяют время, когда доступ разрешен. Внутренне, каждое расписание – это набор дней на три года с указанием времени доступа в каждом дне. Благодаря такой структуре, внешнее программное обеспечение может строить графики любой сложности. Однако надо помнить, что расписание не имеет автоматически повторяющихся циклов и требует редактирования, по крайней мере, раз в три года. Встроенный редактор позволяет формировать список дней путем применения к ним шаблонов. Для этого надо выбрать интервал дней, шаблон, и применить его. Каждый шаблон оперирует набором дней. Всего в редакторе можно задать 4 разных дня для расписания. Однако для API этого ограничения нет. Помимо группового шаблона можно выбрать тип дня на каждое отдельное число.

4.20 Профили доступа

4.20.1 Профиль доступа – это набор точек прохода, разрешенных для какой-либо персоны или группы персон. В программном обеспечении предустановлен режим добавления точек с круглосуточным доступом. Имеется возможность для каждой точки доступа установить свое расписание. Профили

предполагают одинаковые правила доступа для группы лиц. Почти всегда можно разделить всех людей на группы с одинаковым доступом. Например, сотрудники, гости, вип-персоны, клиенты и т.д. В этом случае можно создать соответствующие профили доступа и выдавать их разным посетителям в зависимости от группы. Удобно называть профили по категории пользователей. Например, гостевой доступ, сотрудники круглосуточно, сотрудники по рабочим дням и т. д.

4.20.2 Из этого сценария выделяется случай, когда у сотрудника есть свой кабинет (врачи, адвокаты и т. д.). В таком случае у посетителя есть некоторый общий профиль доступа плюс свой кабинет. Для таких целей система предусматривает помимо профиля доступа еще указание личного кабинета с полным доступом.

4.20.3 Панель настройки профилей позволяет выводить их в виде карточек или в виде списка. В списочном виде показывается количество точек прохода в профиле и основное (примененное к большему числу точек) расписание. Если в профиле больше одного расписания, то к названию основного расписания добавлено многоточие.

4.20.4 Панель позволяет фильтровать профили по содержащимся в них точкам. Это удобно для анализа того, куда входит каждая конкретная точка.

4.21 Личная точка прохода

4.21.1 Указание личной точки прохода можно использовать для предоставления персонального доступа в личный кабинет, например. Это позволяет указывать только общие точки в профилях доступа и не создавать большого количества личных профилей.

4.21.2 Изменять режим работы личной точки прохода можно картой без соответствующих дополнительных привилегий.

4.21.3 Проход под принуждением через личную точку прохода всегда разрешён.

4.22 Разовый доступ

4.22.1 Дополнительно к схеме с профилями доступа, основанными на расписании, система имеет возможность назначать доступ на выбранные точки в указанное время в один конкретный день для любой персоны в системе.

4.22.2 Как было указано выше, выдача разового доступа используется дополнительно к стандартной схеме. Разовый доступ выше по приоритету и позволяет предоставлять доступ на территорию или в дни, которые не разрешены по профилю доступа. Более того, разовый доступ можно предоставить сотруднику без указания ему профиля доступа.

4.22.3 Для работы с разовым доступом выделена отдельная страница в меню «Администрирование доступа». На этой странице доступна информация о всех выданных разовых доступах. Можно выдать или удалить разовый доступ любому сотруднику. Страница содержит фильтры по ФИО и по дате доступа.

4.22.4 Доступ на каждый конкретный день автоматически удаляется в конце дня. Это позволяет контролировать размер хранимых данных.

4.23 Персонал

4.23.1 Весь персонал, который перемещается по территории, регистрируется в общей базе данных. Эта база синхронизируется между контроллерами кластера и является единой на весь кластер. Основными данными персоны является ФИО, но как было упомянуто выше, в каждом конкретном кластере можно расширить набор описательных полей. Помимо данных, к каждой персоне можно прикрепить фотографию. При загрузке фотографии уменьшаются по размеру и сжимаются, пока не достигнут размера порядка 30 кб. Таким образом, с учетом размера флеш-памяти на каждой планке Raspberry (от 4 до 32 Гб) система способна хранить до миллиона фотографий.

4.23.2 Панель персонала позволяет фильтровать (искать) людей по фамилии и имени. Первая буква каждого слова в поле ввода вносится автоматически делается заглавной. Поле ввода устроено таким образом, что при вводе одного слова оно трактуется как часть фамилии или имени. Если в поле введено два слова, то первое трактуется как часть фамилии, а второе как часть имени. Поиск по отчеству не осуществляется.

4.23.3 Так же можно дополнительно фильтровать персонал по двум признакам (полям) «Должность» и «Отдел». Поля фильтра работают по логическому «И», т.е. фильтровать можно как по одному признаку, так и по двум сразу. Сбросить все фильтры (ФИО, Должность и Отдел) можно нажав на кнопку «Сбросить все фильтры» (красный крестик). При выборе ФИО персоны в списке, происходит переход в карточку персоны. Если оставить курсор мыши на ФИО не нажимая, то через секунду всплывет фотография персоны под курсором.

4.23.4 Список данных персоны, видимый в панели, определяется настройками полей персонала в меню **«Настройки СКД»**.

4.23.5 При удалении персон из системы выдается предупреждение. После удаления, в целях повышения производительности не производится обновление всего списка персонала. Вместо этого удаленные персоны маркируются другим цветом.

4.23.6 При добавлении или изменении персоны, обязательные для заполнения полей обозначены звездочками. Поля ФИО автоматически сохраняются с первой заглавной буквой в каждом элементе.

4.23.7 Фотография может быть загружена из файла, а может быть сделана с веб-камеры устройства, на котором запущен интерфейс контроллера. Для корректной работы камеры, необходимо разрешить браузеру доступ к камере. Если видеокамер больше одной, пользователь может переключаться между ними.

4.23.8 Одновременно с созданием персоны или после ее создания можно добавить идентификационные карты. Карты добавляются из картотеки. В списке карт всегда показывается не более 10 карт. При наборе цифр, список меняется и показывает первые несколько карт, содержащие введенный номер. Если карта уже выдана, то она показывается как недоступная.

4.23.9 Вместо ручного ввода можно использовать считыватели с точек прохода. Достаточно включить получение карт и при поднесении не выданной карты к любому считывателю карта появится в поле выбора. Для организации нескольких рабочих мест выдачи и для уменьшения вероятности считывания не той карты в поле ожидания точек прохода можно выбрать конкретную точку. В этом случае в веб-интерфейс будут приходить события только с этой точки прохода.

4.23.10 Параметры персоны и профилей доступа можно изменить как для одной конкретной персоны или профиля доступа, так и для нескольких одновременно посредством групповых операций.

4.23.11 Данные по персоналу можно экспортировать в текстовый файл для целей переноса между кластерами, переноса в другие системы или хранения копии. Экспортировать можно как всю базу, так и только выделенные персоны. Формат JSON более удобен для программной обработки или же для переноса данных между кластерами. Формат CSV является стандартом переноса данных между системами и может использоваться для переноса данных во внешние системы, такие как Microsoft Excel, 1С и т. д.

4.24 Импорт персонала

4.24.1 Данные персонала можно не только экспортировать, но и импортировать в СКУД. При переносе данных из других систем или из других кластеров состав полей персонала может не совпадать. Для таких случаев используется настройка – “Параметры по умолчанию”. Если импортируемые данные не содержат значения для поля (а поле при этом является обязательным) или содержат неправильное значение, то значение заменяется на указанное. Для значений типа справочники есть возможность сразу пополнять их новыми значениями. Аналогично с профилями доступа. Если нет профиля с таким именем, то можно потребовать его создание. В этом случае будет создан пустой профиль с указанным именем. В случае с картами, имеется возможность сразу добавить недостающие карты в картотеку и приписать пользователю. Стоит иметь ввиду, что в этом случае у карт будет установлен только код карты. Остальные параметры будут установлены в следующие значения: тип - многоразовая, уровень привилегий – 1, время действия – 5 лет, описание – «Создана при импорте персонала». Для полного переноса картотеки (карт со всеми свойствами) необходимо импортировать картотеку отдельно (см. ниже).

4.24.2 В случае с форматом файла JSON, все остальные данные находятся в файле импорта. Более того, в файле содержится уникальный идентификатор персоны, это позволяет обновлять данные или, наоборот, не трогать объекты, которые уже существуют.

4.24.3 Для формата CSV необходимо настроить соответствие параметров. При выборе файла импорта/Проанализировать данные, считывается первая строка данных. На ее основе необходимо расставить соответствие параметров. Для идентификатора персоны имеется возможность генерировать его автоматически (в большинстве случаев, это правильная настройка, так как нет никакой гарантии, что номер из внешней системы будет уникален). Так как в случае с CSV файлом, как правило, нет идентификатора персоны, то имеется возможность добавить проверку на уникальность по ФИО и/или еще какому-либо полю данных. Например, в организации может быть табельный номер или какой-то другой внутренний способ отличить персонал. Аналогично формату JSON, имеется возможность обновлять существующие объекты (найденные по указанным критериям) либо отбрасывать данные, если объект уже создан.

4.24.4 Для указания пути к файлу с фото нужно обозначить поле (из файла CSV), в котором прописаны наименования фотографий сотрудников с указанием графического формата изображения (например, xxxxx.jpg) и выбрать все фотографии в этом поле. Сами фотографии под соответствующими именами должны быть сохранены на жестком диске компьютера. Программа автоматически сопоставит выбранные фотографии с выделенными в списке и предложит нужные фото для импорта.

4.24.5 Если при импорте персоны оказывается, что ее данные внесены в систему ранее, но эти данные содержат иные идентификационные карты, то они дополняются данными новых идентификационных карт из импортируемого файла.

4.24.6 Программа способна при импорте распознавать ФИО в файлах разных форматов, в том числе использовать ФИО из одного поля файла.

4.25 Карты

4.25.1 Картотека представляет собой реестр всех карт, используемых в системе для идентификации пользователей. Так как карта является элементом идентификации, и ее потеря может повлиять на безопасность объекта, необходимо вести учет всех карт объекта вне зависимости выдана она в данный момент кому-либо или нет. Таким образом, прежде чем использовать карты для идентификации, карты должны быть добавлены в картотеку.

4.26 Карты добавление

4.26.1 Карта идентифицирует пользователя, однако помимо кода у нее есть ряд важных характеристик. В первую очередь уровень привилегий или уровень доверия идентификатору. Поведение этого параметра было рассмотрено выше. Во-вторых, карты бывают разовые и многоразовые. Данный параметр влияет на работу картоприемника. Разовые карты забираются картоприемниками (и автоматически отвязываются от персоны становясь опять свободными в картотеке), в то время как многоразовые – нет. У каждой карты есть время ее действия. Даже карты, считающиеся постоянными, имеют время действия (хоть и достаточно большое – несколько лет). Главная цель такого поведения – борьба с естественной утерей карт. Даже если карта утеряна и не была обработана по факту утери, то со временем она все равно перестает идентифицировать персону.

4.26.2 Если при добавлении карты параметры не заданы, то они берутся из настроек автоматизации ввода. Это позволяет ускорить занесение новых карт.

4.26.3 В системе поддерживается набор действий, выполняемых путем ввода специальных кодов на клавиатурном считывателе. Для защиты от несанкционированного выполнения эти действия сопровождаются авторизацией картой доступа. Для этой цели карта может иметь набор привилегий, разрешающих то или иное действие:

- **Установка режима точек прохода (кроме постановки/снятия режима охраны)** – разрешает менять режим точки прохода односимвольной командой;
- **Постановка точки прохода на охрану** – разрешает ставить точку прохода на охрану односимвольной командой;
- **Снятие точки прохода с охраны** – разрешает снимать точку прохода с охраны односимвольной командой;
- **Запуск автоматизации** – разрешает запускать автоматизацию двухсимвольной командой.

4.26.4 Аналогично карточке персоны поддерживается регистрация карт путем считывания их на точках прохода. Механизм работает точно так же, за исключением того, что система сообщает только об отсутствующих в картотеке картах и не дает повторно вводить уже зарегистрированные.

4.26.5 Параметры карты можно изменить как для одной конкретной карты, так и для нескольких одновременно посредством групповых операций.

4.27 Карты экспорт и импорт

4.27.1 Экспорт карт в файл и импорт карт из файла работают и настраиваются полностью аналогично экспорту/импорту персонала.

4.28 Журнал событий

4.28.1 Все происходящие в системе события записываются в журнал. Журнал событий каждого контроллера Rubezh-STRAZH синхронизируется друг с другом. То есть, СКУД любого контроллера содержит события всего кластера. Однако есть несколько специальных случаев. События потери связи с контроллерами кластера не реплицируются, так как они парные (каждый контроллер имеет свое событие потери связи с другим контроллером). Очистка событий по переполнению выполняется каждым контроллером самостоятельно (поддерживается порядка 400 000 событий). Таким образом, точный состав событий может отличаться на разных контроллерах. Однако это не является существенным.

4.28.2 Все события в журнале разделены на три категории:

- **«Доступ»** – логические события о перемещении персонала через точки прохода. Данные события описываются параметрами: время, тип, место, персона.
- **«Аудит»** – события доступа в СКУД и изменения данных в ней. Данные события описываются параметрами: время, тип, что изменено, оператор, который изменил.
- **«Оповещения»** – важные события от оборудования и системы. Основное назначение – привлечение внимания для диагностики проблем или срабатывания датчиков. Данные события описываются параметрами: время, тип, контроллер, где произошло, название системы.

4.28.3 События доступа построены по накопительной схеме. По факту успешного или неуспешного прохода через точку порождается всегда одно событие, которое содержит дополнительную информацию, например, о причине отказа в доступе или о типе успешного прохода. Однако в процессе прохода состав события может быть другой, каждая фаза прохода меняет состав начального события. Таким образом, если проход прервется, то событие будет

соответствовать точке прерывания. Такая модель позволяет с одной стороны не терять промежуточную информацию, а с другой – не порождать избыточные события.

4.28.4 При наличии датчика положения двери на точке прохода статус события в журнале может фиксироваться в зависимости от срабатывания этого датчика. Если карта поднесена к считывателю, проход разрешается и дверь открывается, то в журнале отмечается событие о фактическом (совершившемся) проходе. Если датчик не зафиксировал открытия двери после разрешения прохода, то фиксируется событие о несостоявшемся проходе.

4.28.5 Если на точке прохода установлен датчик положения двери и после поднесения карты к считывателю проход был запрещён, но на дверь или турникет было осуществлено внешнее воздействие в целях прохода, то в журнале появляется событие о взломе.

4.28.6 Также, если после совершенного прохода датчик зафиксировал, что дверь остается открытой (отсутствует доводчик или дверь зафиксирована, например), то после заданного промежутка времени считыватели подают звуковой сигнал, а в журнал заносится событие об оставлении двери открытой.

4.28.7 Если считывание карт неустойчивое (длинная линия связи или большие помехи), то в журнале могут появляться события с кодом карты вида: #[<код>] x <число бит>. В поле код будет содержаться прочитанный код, а число бит скажет о том сколько бит было прочитано.

4.28.8 При потере питания контроллер благодаря суперконденсатору способен некоторое время до отключения сохранить рабочее состояние. За это время контроллером помещается в журнал событие об аварийном отключении при потере питания.

4.28.9 В зависимости от важности или критичности события они подкрашиваются цветом. При просмотре события можно переходить на элементы системы, которые упоминаются в событии (в случае если они еще не удалены).

4.28.10 Журнал событий поддерживает два режима работы: онлайн и работа с архивом. При включении режима онлайн в окно дополнительно подгружаются события ТЕКУЩЕГО дня.

4.28.11 В журнале событий для каждой категории можно настроить параметры данных с помощью фильтров:

- категория **«Доступ»** – фильтр по времени, фильтр по типу события, фильтр по точке прохода, фильтр по персоналу;
- категория **«Аудит»** – фильтр по времени, фильтр по типу события, фильтр по лицам, совершившим событие;
- категория **«Оповещения»** – фильтр по времени, фильтр по типу события, фильтр по объекту.

4.28.12 В целях анализа работы точек прохода журнал событий поддерживает интерактивный (с участием оператора) экспорт событий в файл. Выгрузка файла выполняется непосредственно браузером, поэтому нельзя закрывать окно до окончания выгрузки данных. Поддерживаемый формат файла – CSV.

4.28.13 Для удобства ориентирования во временных рамках журнала событий предусмотрена функция смещения тайм-зоны в событиях. Если точки прохода и журнал событий находятся в разных часовых поясах, то в списке событий отображается время, соответствующее часовому поясу журнала событий, а при выборе конкретного события в его карточке указывается уже время, соответствующее местонахождению точек прохода.

4.28.14 События можно экспортировать в текстовый файл для целей переноса между кластерами, переноса в другие системы или хранения копии. Экспортировать можно как всю базу, так и отдельные события.

4.29 Онлайн мониторинг

4.29.1 В онлайн режиме события всех категорий (Доступ, Аудит, Оповещение) показываются в журнале по факту их возникновения. В этом режиме нельзя выбрать тип события. Максимальное количество событий на странице для каждой категории – 300. При достижении этого количества, в конкретной категории, старые события удаляются с экрана, новые добавляются. Верхнее – текущее событие сразу показывается в виде карточки с деталями (разворачивается).

4.30 Поиски в архиве

4.30.1 В режиме поиска необходимо выбрать категорию события и временной интервал. Диалог выбора временного интервала подставляет значения по факту выбора. Это позволяет, выбрав время, сразу начать поиск (сокращается количество кликов мыши). При выборе временного интервала осуществляется проверка, что временной интервал возможный. При попытке выбрать начало позже конца или события из будущего интерфейс подставляет разрешенные значения и сбрасывает время начала интервала поиска на 0:00, а время конца интервала поиска 23:59. Выдача результатов происходит в списке, подгружаемом по мере прокрутки, нумерация событий идет с конца. Таким образом, первое событие имеет номер, соответствующий общему количеству найденных событий. Важно: так как вывод событий осуществляется по времени, то при неправильном времени контроллера возможны пробелы в выдаче данных (либо данные могут не выдаваться).

4.31 Выгрузка событий доступа во вне

4.31.1 Для целей более подробного анализа событий доступа, а также для построения внешних отчетов учета рабочего времени СКУД поддерживает выгрузку событий.

4.31.2 Простейший способ – интерактивная (с участием оператора) выгрузка событий в файл. В данной выгрузке поддерживается фильтр по времени (с возможностью быстро выбрать текущий день, неделю, месяц), фильтр по точкам прохода и фильтр по персоналу. Фильтр по персоналу позволяет отбирать персон по списочным полям (это удобно для выборки, например подразделения). Можно изменить сортировку данных в файле по ФИО или по

времени. Выгрузка файла выполняется непосредственно браузером, поэтому нельзя закрывать окно до окончания выгрузки данных. Поддерживаемый формат файла – CSV

4.31.3 Автоматизированная выгрузка по зонам – вариант выгрузки с использованием вызова API по указанному URL (с авторизацией). Данный способ предназначен для программной интеграции с внешними системами учета рабочего времени. Фактически тут настраиваются параметры выборки, которая будет осуществляться по факту вызова, указанного URL. Так как предполагается периодическая работа внешней системы, то выборка по времени делается относительно момента вызова (сегодня, вчера, текущая неделя, прошлая неделя и т. д.). Основное назначение данного API – выдача информации для внешних систем учета рабочего времени, поэтому необходимой частью обработки данных является определение входов и выходов на территорию. Для этого используются зоны системы. Можно задавать, как только внешние зоны, только внутренние зоны, так и оба списка. В зависимости от конфигурации логика выборки будет разная:

- заданы внешние зоны: все переходы из заданных зон – вход. В заданные – выход;
- заданы внутренние зоны: все переходы из заданных зон – выход. В заданные – вход;
- заданы и те, и другие внутренние зоны: все переходы из внешних зон во внутренние – вход. Из внутренних во внешние – выход.

4.31.4 Настроенные параметры сохраняются системой. Можно сохранить несколько наборов параметров для построения разных отчетов.

4.31.5 Поддерживаемые форматы файлов – CSV и JSON.

4.32 Отчеты

4.32.1 Все совершенные проходы могут быть использованы для оценки времени нахождения персонала на объекте.

4.32.2 Оценить время присутствия и рабочее время можно в разделах отчетов УРВ.

4.32.3 Расчеты УРВ можно посмотреть, как в браузере в табличной форме, так и скачать в форматах CSV, JSON, PDF и XLSX.

4.32.4 Также доступен экспорт событий доступа без расчетов через api метод и через скачивание журнала событий в форматах CSV и JSON.

4.32.5 Экспортируемые данные можно предварительно отфильтровать по дате, точкам прохода и доп. полям персонала на основе справочника (для данных полей также должна быть включена настройка “Учитывать в результатах поиска”).

4.33 Настройки отчетов УРВ

4.33.1 Для построения отчета за период нужно предварительно создать шаблон настроек, по которым будут осуществляться расчеты.

4.33.2 В шаблоне можно указать следующие параметры:

- Имя – название шаблона;
- Период – период, который автоматически выставится при выборе данного шаблона с поправкой на день построения отчета. Доступны для выбора: за вчера и сегодня, текущую и прошлую неделю, текущий и прошлый месяц;
- Начало рабочего дня – время, с которого должен начинаться учет рабочего времени – на основе данного значения также определяется время опоздания;

- Окончание рабочего дня – время, до которого учитывается рабочее время - на основе данного параметра определяется уход раньше;
- Длительность рабочего дня – минимальное время, которое персонал должен присутствовать на рабочем месте – на основе этого параметра определяется недоработка и переработка;
- Внешние и Внутренние зоны – на основе выбранных зон определяется вход и выход в учет рабочего времени/времени присутствия. Вход во внешнюю зону будет считаться “Выходом”, а во внутреннюю “Входом”;
- Учитывать зоны – включение учета внутренних и внешних зон для варианта первый вход – последний выход (добавлена для обратной совместимости с предыдущими версиями) по умолчанию выключена. В этом случае зоны учитываться не будут и при расчетах будет браться первый и последний проход по любым зонам за день.
- Фильтры по персоналу – фильтры по добавленным полям персонала на основе справочников (для данных полей также должна быть включена настройка “Учитывать в результатах поиска”);
- Из созданного шаблона можно сразу перейти к расчетам по команде – «Перейти к оформлению отчета».

4.34 Отчет УРВ за период

4.34.1 В отчете УРВ за период доступен выбор всех ранее созданных шаблонов настроек.

4.34.2 Независимо от того какой период был выбран в шаблоне при необходимости можно указать конкретные даты “с” и “по” перед формированием отчета.

4.34.3 Также можно настроить количество отображаемых сотрудников на странице, поле по которому данные будут сгруппированы и доп. поля, которые будут отображаться в таблице.

4.34.4 И группировка и доп поля используют поля персонала на основе справочника (для данных полей также должна быть включена настройка “Учитывать в результатах поиска”).

4.34.5 После выбора шаблона доступна команда формирования отчета.

4.34.6 После формирования отчета становятся доступны дополнительные фильтры и команда скачивания отчета в файл.

4.34.7 Дополнительные фильтры позволяют применить поиск по ФИО, а также убрать из отображения сотрудников без рабочего времени или наоборот с рабочим временем.

4.34.8 Скачать отчет можно в четырех форматах: CSV, JSON, PDF и XLSX.

4.34.9 Отчет в XLSX доступен в двух представлениях - календарном и табличном.

4.34.10 Календарный вид совпадает по отображению с отчетом в браузере и в PDF, табличный вид включает дополнительные параметры за день как опоздания, уход раньше и количество пропущенных часов рабочего времени.

4.34.11 Отчет в PDF нельзя построить более чем за три месяца или для более 5000 сотрудников, если необходимо выгрузить больше данных следует использовать другие форматы или добавить фильтры.

4.34.12 В случае если сформированный отчет учитывал проходы в течении дня, то при расчетах для каждого дня отчета будут сформированы пары вход-выход. На основе времени сформированных пар определяется общее время присутствия.

4.34.13 В случае если у входа или выхода нет пары, то данный проход не будет учитываться при расчетах.

4.34.14 День, в котором присутствуют проходы без пары будет отмечен.

4.34.15 Так же для любого дня с проходами доступен просмотр всех полученных пар.

4.34.16 Открыть подсказку с проходами можно при помощи клика на иконку проходов в выбранном дне.

> *Примечание. Если по каким-то причинам у прохода нет пары, но время парного прохода известно, можно воспользоваться api методом POST http://[ip_контроллера]/api/v1/access_events /user_defined/, для добавления потерянного прохода, подробнее в Описании REST API: https://[ip_контроллера]/api-docs/ui.*

4.35 Настройка экспорта данных УРВ

4.35.1 Дневной отчет можно построить за любой день указав настройки отчета без предварительной настройки шаблона.

4.35.2 Настройки дневного отчета совпадают с настройками шаблона для УРВ за период.

4.35.3 Кроме основных настроек для дневного отчета доступен выбор событий прохода, которые будут использованы в расчетах: все события проходов или только совершенные.

4.35.4 Сформированный дневной отчет можно фильтровать по имени и группировать по полям персонала на основе справочника (для данных полей также должна быть включена настройка «Учитывать в результатах поиска»).

4.35.5 Также можно добавить отображение доп. поля в таблице отчета.

4.35.6 В отображение можно добавить только одно доп. поле.

4.36 Настройка экспорта данных УРВ

4.36.1 Предварительная настройка справочников. Для настройки фильтров в отчетах экспорта данных УРВ рекомендуется добавить несколько справочников, например, “График работы”, “Подразделение” и т. д. Справочники добавляются в разделе “Настройки СКД” подразделе “Справочники”.

4.36.2 Для того что бы справочники стали доступны в карточке персонала и в фильтрах отчета нужно в подразделе “Поля персонала” добавить созданные справочники, включить для этих полей настройку «Показывать в результатах поиска» и “Применить конфигурацию”.

4.36.3 Для настройки отчета экспорта данных УРВ перейти в раздел “Отчеты” подраздел “Настройка экспорта данных УРВ”. В данном подразделе можно создать несколько отчетов для получения данных о проходах по заданным настройкам. В отчете доступна выборка за следующие периоды:

- За вчера,

- За сегодня,
- За прошлую неделю,
- За текущую неделю,
- За прошлый месяц,
- За текущий месяц.

4.36.4 Форма вывода в формате JSON и CSV. Для CSV в качестве разделителя можно указать точку с запятой, запятую или табуляцию.

4.36.5 Для определения зон учета рабочего времени используется настройка Внешних и Внутренних зон. Вход во внешнюю зону будет считаться “Выходом”, а во внутреннюю “Входом”.

4.36.6 Поля вывода одного прохода, получаемого по «Ссылка API»:

- Время прохода – "Date_Time",
- Направление прохода – "Zone_control" – Вход ENTRANCE Выход EXIT,
- UUID отчета – "UUID",
- ФИО сотрудника – "User_full_name",
- UUID сотрудника – "User_UUID",
- Номер карты – "Card_code" по которой был совершен проход,
- Из какой зоны – "From_zone" совершен проход,
- В какую зону – "To_zone" совершен проход.

4.36.7 На основе этих данных можно определить все пары входов и выходов в зону учета рабочего времени по ним вычислить общее количество часов присутствия, по времени прохода в рамках одних суток можно определить первый вход и последний выход для определения опозданий и уходов раньше и т. д.

5 Интеграция

5.1 Интеграция с ОПС Рубеж R3

5.1.1 В целях более удобной эксплуатации СКУД на объектах, где установлена охранная система Рубеж R3, контроллеры Rubezh-STRAZH могут взаимодействовать с приборами управления ОПС (Рубеж-2ОП порт.R3 и КАУ).

5.1.2 В результате взаимодействия подсистем пользователь получает возможность управлять некоторыми охранными функциями через любую из этих подсистем:

- Постановка/снятие с охраны точек доступа СКУД Rubezh-Strazh, через ОПС Рубеж R3;
- Постановка/снятие с охраны зон ОПС, через точки доступа СКУД Rubezh-Strazh;
- Формирование тревоги, по факту взлома точки прохода (использование СМК СКУД Rubezh-Strazh в качестве охранного датчика для ОС Рубеж R3).

5.1.3 Для одновременного мониторинга приборов ОС R3 и интеграции со СКУД Rubezh-STRAZH, в интерфейсе RS-485 должно быть минимум два модуля сопряжения. Первый модуль МС-1, подключается к любому контроллеру кластера через USB-порт, и к приборам управления ОПС линии RS-485. Второй модуль (МС-1, МС-2, МС-Е), используется для вывода информации из интерфейса R3 на ПК с ПО FireSec.

5.1.4 После подключения необходимо произвести настройку внутреннего программного обеспечения.

5.1.5 Если нужно использовать функционал, при котором происходит взаимный обмен командами постановки/снятия охранных зон/точек прохода, то создайте список охранных зон в ПО FireSec «Администратор» (не ниже 3.1.5.0), в которые будут помещены адресные охранные извещатели. Вид зоны: «обычная», «с задержкой входа/выхода», «без права снятия».

> *Важно! МС-1, связывающий R3 и СКУД, в конфигурации ПО FireSec отображается как «Удаленный сервер», подключаемый на канал модуля сопряжения.*

5.1.6 После создания конфигурации и применения ее на сервере, в папке «External Config» должен находиться файл «Канал 1.1. json». (путь: **C:\Users***\Documents\FireSec3\External Config)**. Данный файл содержит список охранных зон и используется для загрузки в ПО СКУД Rubezh-STRAZH.

5.1.7 Для настройки интеграции необходимо во встроенном ПО, вкладка “Настройки СКД”, раздел “Интеграция с R3”, указать:

- контроллер с подключенным к нему модулем МС-1 (указан в ПО FireSec, вкладка «Планы», таблица «Устройства»),
- адрес канала через который подключен модуль МС-1,
- скорость обмена данных в RS-485 R3 (как правило 57 600),
- в окне «Файл конфигурации МС-1» загрузить файл, полученный из ПО FireSec (Канал 1.1. json).

После обработки файла, появится список охранных зон. Для группировки охранных зон с точками доступа, необходимо указать какие точки доступа входят в требуемые охранные зоны. Сделать это можно, перетащив точку на зону. К каждой зоне может быть привязано несколько точек доступа.

5.1.8 После завершения настроек необходимо нажать “+” для добавления данной интеграции в систему, активировать ее в окне «Состояние» и сохранить настройку.

5.1.9 Если нужно использовать функционал, при котором происходит взаимный обмен командами постановки/снятия охранных зон/точек прохода, плюс в ОС R3 может формироваться тревога, по факту взлома точки прохода, то создайте список охранных зон в ПО FireSec «Администратор» (не ниже 3.1.5.0), в которые будут помещены адресные охранные извещатели. Вид зоны: «обычная», «с задержкой входа/выхода», «без права снятия».

5.1.10 После, создайте виртуальные охранные зоны, в которые не будут добавляться охранные извещатели. В дальнейшем они будут ассоциированы с точками доступа и при формировании тревоги по датчику прохода в СКУД, виртуальная зона будет переходить в тревогу.

> *<u>Важно!</u> Данная охранная зона, должна иметь вид «STRAZH» и привязана к тому прибору, на котором должна будет сформироваться охранная тревога.*

5.1.11 Количество виртуальных охранных зон «STRAZH», должно совпадать с количеством точек прохода в СКУД, от которых нам нужно получить тревожное сообщение.

> *<u>Важно!</u> МС-1, связывающий R3 и СКУД, в конфигурации ПО FireSec отображается как «Удаленный сервер», подключаемый на канал модуля сопряжения.*

5.1.12 После создания конфигурации и применения ее на сервере, в папке «External Config» должен находиться файл «Канал 1.1. json». (путь: C:\Users***\Documents\FireSec3\External Config). Данный файл содержит список охранных зон и используется для загрузки в ПО СКУД Rubezh-STRAZH.

5.1.13 Для настройки интеграции необходимо во встроенном ПО, вкладка “Настройки СКД”, раздел “Интеграция с R3”, указать:

– контроллер с подключенным к нему модулем МС-1 (указан в ПО FireSec, вкладка «Планы», таблица «Устройства»),

– адрес канала через который подключен модуль МС-1,

– скорость обмена данных в RS-485 R3 (как правило 57 600),

– в окне «Файл конфигурации МС-1» загрузить файл, полученный из ПО FireSec (Канал 1.1. json).

После обработки файла, появится список охранных зон. Для группировки охранных зон с точками доступа, необходимо указать какие точки доступа входят в требуемые охранные зоны. Сделать это можно, перетащив точку на зону. К каждой зоне может быть привязано несколько точек доступа.

5.1.14 В отличии от первого варианта реализации, в данном случае, нужно ассоциировать точку прохода с двумя зонами, с обычной и ее клоном, виртуальной. По завершению настройки, нужно нажать «+» для добавления данной интеграции в систему, активировать ее в окне «Состояние» и сохранить настройку.

5.1.15 В результате реализации второго варианта интеграции, пользователь получает возможность осуществлять постановку/снятие зон ОС R3 через кодонаборный считыватель СКУД, управлять режимом работы (постановка/снятие) точки прохода по команде из R3 и получать тревогу в ОС R3 от датчика прохода, используемого в точке прохода СКУД.

5.1.16 Алгоритм управления ОС Рубеж R3 через кодонаборный считыватель СКУД, выглядит следующим образом:

– покидая помещение, пользователь нажимает на кодонаборном считывателе клавишу 6,

– подтверждает ввод команды завершающим символом (# или Ent),

– подтверждает свою манипуляцию картой, у которой есть право управления смены режима точки прохода.

В системе используются следующие коды:

1# - дежурный;
2# - заблокирована;
3# - заблокирована со стороны A;
4# - заблокирована со стороны B;
5# - разблокирована;
6# - на охране.

5.2 Интеграция с приборами биометрической идентификации. Общее описание

5.2.1 В целях обеспечения дополнительной проверки доступа персонала на объектах, контроллеры Rubezh-STRAZH могут взаимодействовать с приборами биометрической идентификации BioSmart, ZKTeco и Hikvision. Контроллеры Rubezh-STRAZH взаимодействуют непосредственно с приборами минуя программное обеспечение верхнего уровня. Программное обеспечение BioSmart studio и интерфейс приборов ZKTeco и Hikvision необходим только для настройки приборов.

5.2.2 Поддержка приборов биометрической идентификации:

- Реализована поддержка приборов BioSmart Quasar, BioSmart 5M. Осуществлена поддержка приборов, в ПО СКУД Rubezh-STRAZH с версией 1.2.210712.613 от 12.07.2021 и выше, предназначенных для идентификации человека по карте, геометрии лица, отпечатку пальцев и их комбинации;
- Реализована поддержка приборов ZKTeco, линейки Visible Light, с прошивкой у которой протокол «AC Push Protocol» с версией не ниже 3.1.2. Данную информацию можно посмотреть в меню прибора «информация о прошивке», а также запросить у вашего менеджера, в организации которой приобретался товар. Осуществлена поддержка приборов в ПО СКУД Rubezh-STRAZH с версией 1.2.220617.660 от 17.06.2022 и выше, предназначенных для идентификации человека по карте, геометрии лица и их комбинации;

- Реализована поддержка приборов Hikvision на базе версии API протокола, а не модели. В текущей реализации ПО, поддержана версия 3.3.1 и выше) Осуществлена поддержка приборов, предназначенных для идентификации человека по карте, геометрии лица и их комбинации.

5.2.3 Для правильной работы, приборы биометрии должны физически находиться в одной общей подсети с контроллером и быть подключены к модулю доступа через Wiegand.

5.2.4 Возможности системы:

- Управление (добавление и удаление) биометрической информации осуществляется непосредственно из карточки персоны (встроенное ПО, вкладка «Персонал»),

- Биометрические данные автоматически не передаются в приборы. Для ее передачи / обновления необходимо нажатие кнопки «обновление биометрической информации» для выбранного типа,

- ПО СКУД Rubezh-Strazh поддерживает любой популярный формат файлов растровых изображений.

> *Важно! При любом типе биометрической идентификации персона должна иметь карту (выданную или виртуальную) для связи ее с биометрической информацией. Это необходимо для авторизации пользователя, так как результат идентификации по биометрическим признакам передается через протокол Wiegand как номер карты.*

5.2.5 Тип проверки (биометрические данные, или комбинация биометрических данных, кода, карты и т д) задается в настройках приборов.

> *Важно! В данной версии ПО не предусмотрена проверка на то, что добавленная (не через биометрический считыватель) фотография сотрудника подходит для его идентификации.*

5.3 Интеграция с приборами биометрической идентификации ZKTeco

5.3.1 Предварительная настройка

Для обеспечения регистрации терминала ZKTeco в системе, необходимо провести его предварительную настройку. В интерфейсе устройства:

- В разделе «настройки сети» указать статический IP адрес,
- В разделе «настройки облачного сервиса» указать IP адрес контроллера Rubezh-STRAZH, к которому терминал ZKTeco подключен по Wiegand, порт 443 и включить работу по HTTPS.

> *Важно! При первом добавлении в систему терминала ZKTeco, пользователи, добавленные в память терминала ZKTeco будут удалены.*
>
> *Также биометрические данные в ПО СКУД Rubezh-STRAZH будут очищены.*

5.3.2 Добавление терминала ZKTeco в ПО СКУД Rubezh-STRAZH. Для добавления терминала ZKTeco в ПО СКУД Rubezh-STRAZH нужно перейти во вкладку “Настройки СКД” раздел “Биометрия”. В карточке биометрического устройства указать:

- Имя – пользовательское название для определения прибора (серийный номер, модель),
- IP адрес – указать статический IP настроенный на терминале ZKTeco,
- Модель – указать ZKTeco 3.x,
- Считыватель – указать контроллер и считыватель, к которому терминал ZKTeco подключено по Wiegand.

После заполнения карточки нажать «+».

5.3.3 Настройка биометрического доступа.

Для настройки биометрического доступа с идентификацией через терминал ZKTeco, нужно настроить точку прохода на основе контроллера и считывателя, к которому подключен терминал ZKTeco. Сформировать профиль доступа на точку прохода. В карточке сотрудника необходимо:

- Добавить фотографию (загрузить файл или сделать снимок с веб-камеры),
- Добавить карту (можно добавить, как реальную, так и сгенерировать виртуальную карту),
- Назначить профиль доступа и сохранить,
- Нажать кнопку “Добавить биометрию” в карточке «Личные данные сотрудника»,
- Заполнить карточку «считывание биометрических данных», выбрать добавленное устройство ZKTeco и карту, по которой будет проходить идентификация сотрудника,
- Нажать кнопку “Включить режим считывания биометрии”. В случае удачной связи появится сообщение о том, что данные приняты.

На терминал ZKTeco данные будут переданы автоматически, и идентификация будет доступна через 10–15 секунд.

В случае замены фотографии у сотрудника нужно или повторно добавить биометрию «карта – биометрический считыватель» или обновить базу данных сотрудников на биометрических считывателях целиком. При удалении биометрии очистка биометрии в приборе ZKTeco произойдет в течении 10 секунд.

> *<u>Важно!</u> Если в системе добавлено несколько терминалов ZKTeco, достаточно для сотрудника указать одну связку «карта-*

биометрический считыватель» (пункт «Добавить биометрию» в карточке Личные данные сотрудника), на остальные терминалы ZKTeco информация о сотруднике передастся автоматически.

5.3.4 Биометрический считыватель реагирует положительно вне зависимости от предоставленных прав доступа, но решение о предоставлении доступа выдает контроллер Rubezh-STRAZH. Так, при недостаточном уровне доступа, считыватель подтвердит идентификацию, но доступ будет заблокирован.

5.4 Интеграция с приборами биометрической идентификации Hikvision

5.4.1 Предварительная настройка

Для обеспечения регистрации терминала Hikvision в системе, необходимо провести его предварительную настройку. В интерфейсе необходимо:

- Добавить пользователя с правами администратора, задать login и password,
- В разделе «настройки» в меню «связи для Wiegand» указать значение «Wiegand 34».

<u>Важно!</u> При первом добавлении терминала Hikvision, все биометрические данные о сотруднике в ПО СКУД Rubezh-STRAZH будут очищены. Пользователей, добавленных через прибор Hikvision, можно удалить только через сам прибор.

5.4.2 Добавление терминала в ПО СКУД Strazh Rubezh

Для добавления терминала Hikvision в ПО СКУД Rubezh-STRAZH, необходимо перейти во вкладку “Настройки СКД” раздел “Биометрия”. В карточке биометрического устройства указать:

- Имя – пользовательское название для определения терминала (серийный номер, модель),
- IP адрес – указать статический IP настроенный в Hikvision,
- Модель – указать Hikvision ISAPI,
- Логин и пароль, указать (от созданного в терминале Hikvision) пользователя с правами администратора,
- Считыватель – указать контроллер и считыватель, к которому терминал подключен по Wiegand.

После заполнения карточки нажать «+».

5.4.3 Настройка биометрического доступа

Для настройки биометрического доступа с идентификацией через терминал Hikvision нужно настроить точку прохода на основе контроллера и считывателя, к которому подключен терминал Hikvision. Сформировать профиль доступа на точку прохода. В карточку сотрудника необходимо:

- Добавить фотографию (загрузить файл или сделать снимок с веб-камеры),
- Добавить карту (можно добавить, как реальную, так и сгенерировать виртуальную карту),
- Назначить профиль доступа и сохранить,
- Нажать кнопку “Добавить биометрию” в карточке «Личные данные сотрудника»,
- Заполнить карточку «считывание биометрических данных», выбрать добавленный терминал Hikvision и карту, по которой будет проходить идентификация сотрудника,
- Нажать кнопку “Включить режим считывания биометрии”. В случае удачной связи появится сообщение о том, что данные приняты.

На терминал Hikvision данные будут переданы автоматически, и идентификация будет доступна через (10 – 15) секунд.

5.4.4 В случае замены фотографии у сотрудника нужно или повторно добавить биометрию «карта – биометрический считыватель» в карточке Личные данные сотрудника, или обновить базу данных сотрудников на биометрических считывателях целиком. При удалении биометрии, очистка биометрии на терминале Hikvision произойдет в течении 10 секунд.

> *Важно! если в системе добавлено несколько терминалов Hikvision, достаточно для сотрудника указать одну связку «карта-биометрический считыватель» (пункт «Добавить биометрию» в карточке Личные данные сотрудника), на остальные терминалы Hikvision информация о сотруднике передастся автоматически.*

5.4.5 При добавлении еще одного терминала Hikvision, либо нового пользователя, необходимо обновить базу данных сотрудников на биометрических считывателях целиком (в карточке сотрудника, либо «Настройки СКД» в разделе «Биометрия»).

5.4.6 В случае добавления нового пользователя у оборудования Hikvision есть ограничение скорости передачи информации. Скорость передачи зависит от количества сотрудников (приблизительно 5 человек в секунду). Передача информации осуществляется одновременно во все считыватели (параллельно).

5.4.7 Биометрический считыватель реагирует положительно вне зависимости от предоставленных прав доступа, но решение о предоставлении доступа выдает контроллер. Так, при недостаточном уровне доступа, считыватель подтвердит идентификацию, но доступ будет заблокирован.

5.5 Интеграция с приборами биометрической идентификации BioSmart

5.5.1 Предварительная настройка

Для обеспечения регистрации терминала BioSmart в системе, необходимо провести предварительную настройку в интерфейсе терминала, Web-интерфейсе либо через ПО BioSmart Studio.

5.5.2 Для BioSmart Quasar:

- В разделе «настройки сети» указать статический адрес, IP адрес, маску и основной шлюз,
- В разделе «Система» настроить параметры в разделах «Wiegand 0» и/или «Wiegand 1». Выберите направление передачи данных – Wiegand Out (передать на внешнее устройство) или Wiegand In (принять от внешнего устройства), режим работы терминала – «Wiegand 26», ширина импульса – 200 мкс (рекомендованное значение), время между посылками – 2000 мкс (рекомендованное значение), тип данных Wiegand – Card ID (код RFID карты) или UID (код сотрудника (ID)).

5.5.3 Для BioSmart 5M настройки лучше производить в ПО BioSmart-STUDIO:

- По умолчанию на терминале установлен IP-адрес 172.25.10.71. сменить адрес можно через web-интерфейс либо ПО BioSmart- STUDIO. Выберите свойства терминала и измените сетевые параметры в соответствии с настройками вашей сети,
- Во вкладке «Системные», раздел «Доп. устройства», для параметра «Режим Wiegand выхода» выбрать значение «Wiegand-26».

Подробнее о настройках терминалов BioSmart указано в руководствах по эксплуатации к конкретным терминалам.

5.5.4 Для добавления терминала BioSmart в ПО СКУД Rubezh-STRAZH, перейти во вкладку «Настройки СКД» раздел «Биометрия». В карточке биометрического считывателя указать:

- Имя – пользовательское название для определения прибора (серийный номер, модель),
- IP адрес – указать статический IP настроенный в приборе BioSmart,
- Модель – выбрать из списка необходимую модель BioSmart,
- Считыватель – указать контроллер и считыватель, к которому прибор BioSmart подключено по Wiegand.

После заполнения карточки нажать «+».

5.5.5 Настройка биометрического доступа

Для настройки биометрического доступа нужно настроить точку прохода на основе контроллера и считывателя, к которому подключен терминал BioSmart. Сформировать профиль доступа на точку прохода. В карточке сотрудника необходимо:

- Добавить фотографию (загрузить файл или сделать снимок с веб-камеры),
- Добавить карту (можно добавить, как реальную, так и сгенерировать виртуальную карту),
- Назначить профиль доступа и сохранить,
- Нажать кнопку “Добавить биометрию” в карточке «Личные данные сотрудника»,
- Заполнить карточку «считывание биометрических данных», выбрать добавленный терминал BioSmart и карту, по которой будет проходить идентификация сотрудника,
- Нажать кнопку “Включить режим считывания биометрии”. В случае удачной связи появится сообщение о том, что данные приняты.

> *<u>Важно!</u> Если в системе добавлено несколько терминалов BioSmart, то для каждого сотрудника нужно указывать связку «карта-биометрический считыватель» (пункт добавить биометрию в карточке Личные данные сотрудника) с каждым прибором BioSmart.*

В случае замены фотографии у сотрудника, нужно или повторно добавить биометрию «карта – биометрический считыватель» в карточке Личные данные сотрудника, или обновить базу данных сотрудников на биометрических считывателях целиком.

5.6 Интеграция с системами распознавания госномеров

5.6.1 Интеграция позволяет организовать контроль и учет проезда транспорта через точку доступа типа Шлагбаум с идентификацией персоны по номеру авто, карте или номеру и карте, управлять доступом и получать отчеты через ПО СКУД Rubezh-Strazh.

5.6.2 В качестве устройств распознавания автомобильных номеров поддерживается сервер RVI-Авто (из состава RVI оператор) или «умные» камеры с поддержкой распознавания номеров на борту и передачей событий по протоколу ONVIF.

5.6.3 Обрабатывать события с устройств распознавания будет контроллер Rubezh-STRAZH, который управляет шлагбаумом, связанным с устройством. Это позволяет обеспечить дополнительную отказоустойчивость системы.

5.6.4 В данной версии ПО СКУД Rubezh-Strazh, поддерживается RVI-Авто с версиями 1.4 и 2.0.

5.6.5 Для настройки функции распознавания номеров необходимо установленное на вашем сервере лицензионное ПО RVI-Авто, а также физически подключенные камеры. Настройки распознавания номеров производятся в ПО RVI-Авто. В разделе «Соединение» установите соединение с физической камерой и укажите пользовательское наименование камеры. Для настройки интеграции вам потребуется RTSP ссылка (находиться в нижней части экрана). **Необходимо скопировать только часть ссылки – IP-адрес сервера.**

Пример ссылки: rtsp://172.16.135.84:19007/h264/1

Часть для копирования: 172.16.135.84

5.6.6 Интеграция с распознаванием номеров настраивается в ПО СКУД Rubezh-Strazh.

5.6.7 Что бы настроить функцию распознавания номеров в ПО СКУД Rubezh-Strazh, во вкладке «Настройка СКД» разделе «Распознавание номеров» заполните карточку:

- Имя – пользовательское название для определения прибора/системы;
- ONVIF URL – путь к ONVIF серверу. Состоит из адреса вашего сервера (часть ссылки скопированной в ПО RVI-Авто), и статическим описанием – порт сервера на котором работает RVI-Авто :19006/onvif/ device_service;

Например: http://192.168.10.01:19006/onvif/device_service

- Тип – тип события. Доступно для выбора стандартные ONVIF (для «умных» камер) и события формата RVI-Авто (для интеграции с RVI-Авто);
- Логин и пароль – вводиться в случае если на физической камере установлены эти параметры.

В разделе «Точки прохода» создайте и/или настройте точку прохода типа шлагбаум, с обязательным указанием пунктов: контроллер, считыватель либо реле и устройство распознавания номеров. В разделе «профили входа» для каждого сотрудника в личной карточке, укажите номер автомобиля. Во вкладке «Администрирование доступа», раздел «Профили доступа», создайте профиль доступа и укажите расписание.

5.6.8 После распознавания номера в журнале событий появится запись о совершенном событии, на основании которого могут быть построены отчеты (вкладка «Отчеты»).

5.7 Интеграция с внешними системами через REST API

5.7.1 Для организации работы контроля и учета доступа можно использовать напрямую REST API ПО Страж.

5.7.2 При помощи интеграции внешнего ПО через API можно осуществлять, как контроль времени присутствия на объекте, так и управление точками прохода, добавление учетных данных пользователей, их профилей доступа и т. д.

5.7.3 API ПО Страж доступно по ссылке https://IP-контроллера/api-docs/ui/ так же данную ссылку можно найти в разделе «Настройки контроллера» на вкладке «О системе».

6 Проблемы и их решения

6.1 Проблемы отображения веб интерфейса контроллера

6.1.1 Убедитесь, что используете совместимый веб-браузер. Поддерживаемые браузеры: Google Chrome, Opera, Mozilla FireFox, Safary, Microsoft Edge (Chromium).

6.2 Предупреждения браузера

6.2.1 Контроллер использует шифрованный протокол взаимодействия с веб-браузером компьютера (TLS). Так как устройство является локальным и его веб-сервер не находится в глобальной сети, то веб-браузер не может проверить подлинность сертификата. В таком случае, в зависимости от типа браузера, могут быть выданы предупреждения о невозможности проверить подлинность сертификата. Для удаления этих сообщений необходимо добавить файлы сертификатов на компьютер, с которого идет управление, поместить их в реестр (обычно это делается путем двойного щелчка мышью на файле). Контроллер предоставляет как корневой сертификат (для работы с любыми контроллерами), так и сертификат конкретного контроллера. Важно: сертификат контроллера привязан к его IP-адресу, поэтому его можно использовать только при статической адресации. В зависимости от политики безопасности необходимо добавить или корневой, или сертификат контроллера в реестр компьютера. И сделать их доверенными (через свойства). Файлы сертификатов доступны в пункте **"Настройки контроллера/ SSL сертификаты"**.

6.3 Кодировка при загрузке справочников из файла

6.3.1 Если при импорте файла в справочник текст представлен нечитаемыми символами, нужно попробовать изменить кодировку файла для устранения проблемы.

6.4 Диагностика неисправностей, причины их возникновения и способы устранения

	Описание проблемы	Причина возникновения	Способ устранения
1	В журнал событий часто поступают события о потере/восстановлении связи, наблюдается моргание индикатора ERROR и RS-485	Закольцована линия RS-485-1 на R-S485-2	Проверить правильность подключения линии связи, устранить закольцованный участок
2	Медленно совершаются проходы, либо не совершаются вовсе. Наблюдается моргание индикаторов ERROR и RS-485	Закольцованы линии RS-485	Проверить правильность подключения линии связи
3	В журнале событий регистрируется событие о потере связи устройства в системе. На данном устройстве не совершаются проходы, сработки концевиков и т. д.	1. Контакт линии RS-485 A или B с земляной клеммой	Проверить правильность подключения
		2. Потеря питания, либо плохой контакт на устройстве	Проверить источник питания, которым питается устройство. Проверить целостность линии питания
		3. Оборвана линия RS-485	Проверить целостность линии RS-485
4	После записи конфигурации в устройство, не совершается проход на точке прохода настраиваемого устройства	Дублирован адрес устройства	Проверить правильность выставления адреса на DIP переключателях, продублированные адреса при наличии устранить

	Описание проблемы	Причина возникновения	Способ устранения
5	Не устанавливается проводная связь напрямую с контроллером (STR20-IP или КД-PRO)	На ПК установлены статические сетевые настройки	Привести сетевые настройки ПК в соответствие с п.3.2.3 настоящего руководства
6	Потеря связи с контроллером (STR20-IP или КД-PRO)	1. Неисправность питания	Проверить мультиметром напряжение на клемме питания сетевого контроллера, в случае отсутствия такового, проверить работоспособность самого источника, от которого производится питание
		2. Установлен IP-адрес не для той сети, в котором предполагается работа	Подключить сетевой контроллер напрямую к ПК и там произвести первоначальную настройку, согласно настоящему Руководству по эксплуатации
		3. Конфликт IP-адресов с другими устройствами в локальной сети	Проверить локальную сеть и исправить конфликт IP-адресов
7	Потеря связи с модулем доступа (STR-1AP)	1. Неисправность питания	Проверить источник питания, с помощью которого запитан модуль доступа
		2. Обрыв линии связи	Проверить целостность линии RS-485 и правильность монтажа

	Описание проблемы	Причина возникновения	Способ устранения
		3. Неисправен модуль доступа	Проверить целостность линии питания
8	Отсутствует модуль доступа в конфигурации	1. Потеря связи с модулем доступа	Проверить линию связи
		2. Модуль доступа не добавлен в конфигурацию	Запустить повторный поиск и добавить в конфигурацию модуль доступа
		3. Проблема с питанием модуля доступа	Мультиметром проверить напряжение на клеммах питания модуля доступа. При его отсутствии устранить причину и произвести поиск устройства снова
9	Не совершается проход при прикладывании карты доступа к считывателю	1. Неверно сконфигурирована точка доступа	Произвести правильную настройку точки доступа согласно актуальному Руководству по эксплуатации, расположенному в веб-интерфейсе СКУД Strazh
		2. Карта доступа не добавлена в конфигурацию	
		3. Карта доступа не привязана к конкретному пользователю	
		4. У пользователя, которому принадлежит карта доступа, не настроен график доступа	
10	Карта доступа не считывается, либо	Неправильное подключение	Проверить и произвести правильное подключение, согласно схеме на считыватель и

	Описание проблемы	Причина возникновения	Способ устранения
	считывается с неверными значениями	считывателя Wiegand	Руководству по эксплуатации на СКУД Strazh
11	Точка доступа турникет / шлагбаум / турникет с картоприемником не работает	1. Неправильное подключение турникета / шлагбаума / турникета с картоприемником к модулю доступа	Проверить и произвести правильное подключение согласно паспорту на турникет / шлагбаум / турникет с картоприемником и Руководству по эксплуатации на СКУД Strazh
		2. Неправильно настроена точка доступа «турникет»	Произвести корректную настройку точки доступа согласно Руководству по эксплуатации на СКУД Strazh
12	Неправильная работа концевиков двери и кнопок, подключаемых к модулю доступа	1. Неисправные концевики или кнопки	Проверить исправность работы концевиков и кнопок, согласно их документации
		2. Неправильное подключение концевика или кнопки	Проверить и произвести правильное подключение согласно схемам, указанным в Руководстве по эксплуатации
		3. Неправильная конфигурация при создании точки доступа	Произвести правильную конфигурацию концевиков и кнопок в настройках точек доступа, согласно режиму их работы

7 Хранение

7.1 Условия хранения

7.1.1 Рекомендуется хранить устройства в транспортной упаковке в отапливаемом складском помещении не более 10 штук в стопке. Допускается хранение при температуре окружающего воздуха от минус 20 °С до плюс 60 °С и относительной влажности до 90 % (условия хранения 1 по ГОСТ 15150-69).

7.1.2 Не следует хранить устройства в местах, подверженных воздействию прямых солнечных лучей, резкому изменению температуры и повышенной влажности. Кроме того, устройства не предназначены для эксплуатации и хранения в условиях воздействия токопроводящей пыли, паров кислот и щелочей, соляного тумана, а также газов, вызывающих коррозию и разрушающих изоляцию.

8 Транспортирование

8.1 Условия транспортирования

8.1.1 Транспортирование упакованных в транспортную упаковку изделий может производиться любым видом транспорта на любые расстояния в соответствии с правилами перевозки грузов, действующими на соответствующем виде транспорта. При этом тара должна быть защищена от прямого воздействия атмосферных осадков. При транспортировании самолетом допускается размещение груза только в отапливаемых герметизированных отсеках. Транспортная упаковка на транспортных средствах должна быть размещена и закреплена таким образом, чтобы были обеспечены ее устойчивое положение и отсутствие перемещения. Условия транспортирования должны соответствовать условиям хранения 5 по ГОСТ 15150-69.

8.1.2 После транспортирования при отрицательных температурах непосредственно перед вводом в эксплуатацию изделия должны быть выдержаны в нормальных климатических условиях в упаковке изготовителя не менее 2 часов в целях исключения конденсации влаги.

9 Утилизация

9.1 Правила утилизации

9.1.1 Поскольку некоторые модификации изделий содержат батарею, по истечении срока службы их необходимо утилизировать в соответствии с законом об обращении с отходами производства и потребления, принятом в регионе применения. Для уточнения правил утилизации, а также для получения информации об организациях, занимающихся утилизацией электронной техники, следует обратиться к представителям местного органа власти.