



ООО «КБ Пожарной Автоматики»

**СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ
Rubezh-STRAZH**

Руководство по эксплуатации

ПАСН.425728.007 РЭ

Редакция 2

<http://www.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, в составе которых содержатся компоненты:

– 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	6
Перечень терминов	7
1 Описание и работа	8
1.1 Назначение СКУД	8
1.2 Общие характеристики	10
1.3 Модификации встроенного программного обеспечения	15
1.4 Питание контроллера	16
1.5 Часы	17
1.6 Перемычки	17
1.7 Индикация контроллера	18
2 Монтаж	20
2.1 Меры безопасности	20
2.2 Общие рекомендации	20
2.3 Отключение питания	24
2.4 Подключение оборудования	24
2.5 Подключение считывателей	24
2.6 Дверной замок	26
2.7 Замки, отпираемые и запираемые напряжением	26
2.8 Подавление выбросов на замках	27
2.9 Безопасность	27
2.10 Подключение турникетов	27

2.11	Кнопка запроса на выход	29
2.12	Дверные контакты	29
2.13	Схема подключения дверного контакта	30
2.14	Охранный датчик	30
2.15	Реле	31
2.16	Контроль вскрытия корпуса устройства	31
2.17	Аварийный выход	31
2.18	Средства индикации	31
2.19	Подключение к Ethernet	32
3	Начало работы	32
3.1	Первый запуск контроллера	32
3.2	Обнаружение контроллера	33
3.3	Начальная настройка контроллера	33
3.4	Установка сетевых параметров	33
3.5	Установка времени	34
3.6	Настройки OSDP	34
3.7	Контроль связи OSDP	35
3.8	Поиск устройств на линии	35
3.9	Обновление	36
3.10	Мониторинг состояния (ONVIF)	37
3.11	Перезагрузка контроллера	37
3.12	Возврат заводских параметров	37

3.13	Системный журнал и диагностика	38
3.14	О системе	38
4	Встроенная СКУД	39
5	Проблемы и их решения	63
6	Хранение	69
7	Транспортирование	69
8	Утилизация	70

Перечень сокращений

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.
ТД	– точка доступа.
ТУ	– технические условия ПАСН.42725.007 ТУ.

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.
Регламент	– определяет порядок и способ выполнения задач, ответственность владельца и исполнителей, процедуры управления.
Профиль доступа	– совокупность точек доступа и графика доступа.
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 правилами доступа, ведения журнала перемещений и формирования отчетов. Субъекты доступа идентифицируются с помощью RFID-карт, считываемых с подключенных считывателей.

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

1.1.3 Контроллер 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 Модуль доступа предназначен для подключения периферийного оборудования и трансляции команд управления и событий между устройствами и контроллером посредством шины OSDP. Один контроллер может управлять 10 модулями, что соответствует 20 односторонним точкам доступа или 10 двусторонним.

1.1.5 Контроллер 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.

1.1.6 Контроллеры 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.

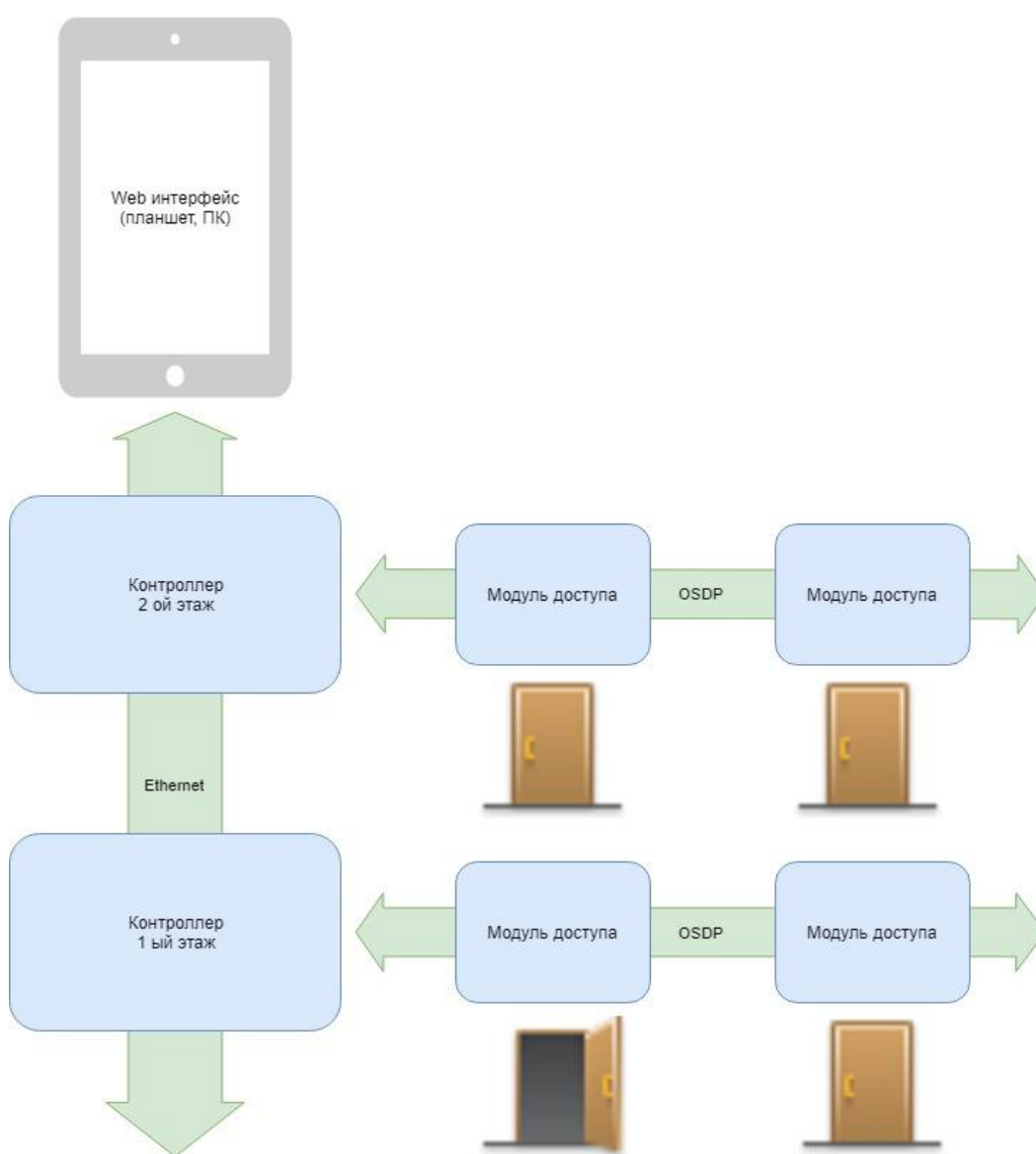
1.1.7 Встроенная распределенная СКУД обеспечивает:

- 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, 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 батареей 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:

Характеристика	Значение
Напряжение питания, В	9-28
Максимальный ток, А	0,8
Режим работы	круглосуточный
Скорость обмена в сети Ethernet, Мбит/с	10/100
Количество OSDP-каналов (RS-485)	2
Максимальное количество OSDP адресов	30

Характеристика	Значение
Количество подключаемых OSDP-считывателей	20
Тип подключения считывателей	OSDP
Количество входов с контролем линии типа «сухой контакт»	2
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

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
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 10 000 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 100 000 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 (он же 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 100 000 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 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 CAPTCHA, для версии Enterprise ввод CAPTCHA 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 (см. раздел «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
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 линий OSDP (RS-485). J1, J2 – для первого интерфейса. 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 (микро USB-разъем). Не предназначена для использования конечным пользователем. Нормальное состояние – переключки 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 переключки:

- для включения терминаторов линий OSDP (RS-485). J1, J2 – для первого интерфейса. J3, J4 – для второго. Нормальное состояние – переключки отсутствуют. Для последнего устройства на длинной линии необходимо установить соответствующие переключки;

- переключки ACT-LED, ACT-BEEP задают уровень сигнала по линиям световой и звуковой индикации Wiegand-считывателей соответствующий отсутствию индикации. Нормальное состояние – переключки отсутствуют. Что соответствует нулевому уровню. При установленных переключках 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
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 Рекомендуемая максимальная длина кабеля при подключении оборудования:

- линия OSDP до считывателей – не более 1000 м;

- для интерфейса Wiegand – не более 100 м;
- для подключения кнопок и концевиков – не более 100 м;
- для Ethernet – не более 100 м;
- от реле до замков – длина кабеля зависит от типа устройства и сечения провода.

2.2.3 Рекомендуемые типы кабелей, используемые при монтаже:

№	Подключаемое к контроллеру оборудование	Макс. длина кабеля, м	Тип кабеля	Сечение, мм ² , не менее	Пример кабеля
1	Ethernet (IEEE 802.3)	100	Четыре витые пары не ниже пятой категории	0,2	КВПЭф-5е 4х2х0,52F/ UTP2-Cat5e
2	Считыватель, картоприемник	50 (суммарная)	Витая пара не ниже пятой категории		КВПЭф-5е 2х2х0,52F/ UTP2-Cat5e
3	ИП	10	Двужильный	0,75	ШВВП 2х0,75 двухцветный
4	Кнопка ДУ («выход») Датчик двери (геркон) Дополнительное оборудование	30	Двужильный	0,2	RAMCRO SS22AF-T 2х0,22 CQR-2
5	ПДУ	40	Восьмижильный	0,2	CQR CABS8 8х0,22с

6	ИУ – замок	30	Двужильный	0,75	ШВВП 2x0,75с двухцветны й
7	ИУ – Турникет	30	Шестижильный	0,2	CQR CABS6 6x0,22с
8	ИУ АТП	30	Четырехжильный	0,2	CQR CABS4 4x0,22с

2.2.4 Краткие рекомендации по выбору кабелей:

Назначение кабеля	Рекомендации
Линия питания контроллера (от БП до контроллера)	Для внутренней проводки выполняется проводом типа ВВГ (ВВГнг), ШВВП, ПВС. Для внешней проводки возможно использование кабеля ВВГ (ВВГнг). Сечение кабеля зависит от длины линии питания. Как правило, для линий длиной до 50 метров достаточно использовать кабель сечением не менее 0,75 мм ² . Для линий большей длины рекомендуется сечение 1,5-2,5 мм ² .
Линия питания замковых механизмов	Для внутренней проводки выполняется проводом типа ВВГ (ВВГнг), ШВВП, ПВС. Для внешней проводки возможно использование кабеля ВВГ (ВВГнг). Сечение кабеля зависит от длины линии питания и потребляемого нагрузкой тока. Как правило, для линий длиной до 50

	метров достаточно использовать кабель сечением не менее 1,0 мм ² . Для линий большей длины рекомендуется сечение 1,5-2,5 мм ² .
Подключение считывателей к контроллеру	На небольшом удалении считывателей от контроллера (до 50м) рекомендуется выполнять кабелем сечением 0,22-0,5 мм². Допустимо использование любых типов сигнальных кабелей, например, КСПВ 8х0,5. При большей удаленности (50-100м) необходим кабель большего сечения (0,75-1,0 мм²), как минимум на линиях питания считывателей. Так же при подключении ознакомьтесь с рекомендациями от производителя считывателя.
Сигнальные линии от датчика до контроллеров, а также управляющие линии от контроллера до исполнительных устройств.	Выполняются кабелем сечением 0,22-0,5 мм², допустимо использование любых типов кабелей, например, КСПВ 8х0,5. Не рекомендуется использовать для соединения кабель типа «витая пара». Он обладает повышенной распределенной емкостью между перевитыми проводниками, что может привести к ощутимым задержкам передачи сигнала, например, от фотодатчиков до контроллера.

2.2.5 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 мм².

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.

2.5 Подключение считывателей

2.5.1 Модули предназначены для работы со считывателями с интерфейсом Wiegand, однако непосредственно на шину 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 мм². 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 переключки АСТ-LED или/и АСТ-БЕЕР.

2.6 Дверной замок

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 следует подключать 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 Безопасность

2.9.1 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.

2.10 Подключение турникетов

2.10.1 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 (K1) работает на вход, а выход 2 (K2) работает на выход.

2.10.2 Поскольку турникетный режим 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:

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

– отключение замка происходит в начале (а не в конце, как для двери) импульса поворота для обеспечения надежного запираания турникета после прохода.

2.10.3 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.

2.10.4 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.

2.10.5 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.

2.10.6 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).

2.10.7 В турникетном режиме входы датчиков поворота 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**»).

2.11 Кнопка запроса на выход

2.11.1 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.

2.11.2 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.

2.11.3 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.

2.12 Дверные контакты

2.12.1 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.

2.13 Схема подключения дверного контакта

2.13.1 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.

2.13.2 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.

2.13.3 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.

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

2.13.5 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.

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

2.14 Охранный датчик

2.14.1 Модуль позволяет подключить до двух шлейфов безадресных датчиков.

2.14.2 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.

2.15 Реле

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

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

2.16 Контроль вскрытия корпуса устройства

2.16.1 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.

2.17 Аварийный выход

2.17.1 Вход SENS1 контроллера может использоваться для аварийной разблокировки дверей, например, в случае пожара, подключенных к контроллеру. К контактам аварийного выхода может быть подключена система пожарной сигнализации либо кнопка аварийного открывания двери.

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

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

2.18 Средства индикации

2.18.1 Изделия в пластиковом корпусе снабжены видимой индикацией:

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

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

2.19 Подключение к Ethernet

2.19.1 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.

2.19.2 Контроллер поддерживает USB Wi-Fi-модуль TP-LINK TL-WN725N 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_XXXXXXXXX, где XXXXXXXXXX – 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 По умолчанию, контроллер настроен 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. Логин и пароль по умолчанию: «**admin**», «**abc12345**».

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 Настройки OSDP

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

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

3.6.3 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.

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

3.6.5 На модуле доступа располагается колодка выставления адреса. 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. Максимальным значением адреса является 031 (001+002+004+008+016).

3.7 Контроль связи OSDP

3.7.1 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.

3.8 Поиск устройств на линии

3.8.1 Так как контроллер взаимодействует с оборудованием точки доступа через модули, то необходимо активизировать их в системе. OSDP-устройства поддерживают протокол обнаружения. Так как сканирование линии идет по адресам и таймаут отсутствия ответа достаточно большой, то сканирование занимает достаточно большое время. Для уменьшения этого времени в панели поиска устройств можно выбрать диапазон адресов и диапазон скоростей, на которых будет произведена попытка найти устройства. По умолчанию, поиск осуществляется на всем диапазоне адресов при максимальной скорости канала только.

3.8.2 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).

3.8.3 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.

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

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 скачены 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 моргания 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 моргания 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 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) во избежание путаницы с источниками данных.

4.4 Управление кластером

4.4.1 Если в системе предполагается использование более одного контроллера, 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 выпадению из 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 Оповещения и тревоги

4.6.1 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.

4.6.2 Система поддерживает три уровня важности срабатывания датчика. В случае установки уровня **«Информационное сообщение»**, информация о срабатывании будет попадать в журнал, как информационное сообщение. Данный статус не будет отражаться в списке неисправностей на стартовой странице (а также не будет индизироваться как аварийный статус в карте устройств). При использовании уровней **«Предупреждение»** или **«Тревога»**, статус датчика будет отслеживаться как аварийный.

4.6.3 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.

4.6.4 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.

4.6.5 В контроллерах 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.

4.7 Точки прохода

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

4.7.2 В системе поддерживаются несколько типов точек прохода:

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

4.7.3 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 не позволяет использовать элементы модулей с разных контроллеров.

4.7.4 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.

4.7.5 Каждая точка прохода имеет набор дополнительных настроек, значения которых заданы одинаковыми для всех точек. По умолчанию, у каждой двусторонней точки прохода есть сторона А – вход и сторона В – выход, а при использовании разовых карт блокируется сторона В (выход). При необходимости данные параметры можно поменять в настройках. При формировании точки можно изменить значения этих параметров для конкретной точки с помощью выпадающего списка **«Дополнительные параметры»**:

- **«Время закрытия замка двери после локального открытия»** – время от момента поднесения карты к считывателю до момента закрытия замка;

- **«Время закрытия замка двери после удаленного открытия»** – время от момента нажатия кнопки дистанционного открывания до момента закрытия замка;

- **«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;

- **«Световая индикация срабатывания считывателя»** – наблюдается моргание светового индикатора при поднесении карты к считывателю;

– **«Пин-код точки прохода»** – при его указании точку можно будет разблокировать с помощью единого кода. Точка должна в этом случае иметь считыватель с кодонаборником;

– **«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 (по умолчанию вход);

– **«Проход по разовым картам со стороны В запрещен»** – проход по разовым картам заблокирован со стороны В (по умолчанию выход);

– **«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 Б.

– **«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.

– **«Задержка при постановке на охрану через код на считывателе, сек»** – 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.

– **«Максимальное время ожидания множественного прохода, сек»** – 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, сек»** – время, после которого проход будет разрешен или запрещен автоматически, согласно настройкам по-умолчанию.

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

4.7.7 Типовую точку прохода можно создавать и заполнять с устройства, чтобы не делать это вручную.

4.7.8 Точки прохода поддерживают идентификацию по карте, карте и пин-коду, карте или пин-коду. В последнем случае можно разблокировать точку прохода персональным пин-кодом, не используя карту. 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, точка прохода остается заблокированной, а в журнал заносится соответствующее событие. В этом

режиме возможно разблокирование пин-кодом самой точки. В этом случае в журнал не заносится информация о том, кто именно разблокировал точку.

4.7.9 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.

4.7.10 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.

4.7.11 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.

4.7.12 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 морганием 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 морганием зеленым (раз в две секунды) обоих считывателей;

– **«На охране»** – при поднесении карты к любому из считывателей проход запрещается по причине охраны. Режим сопровождается морганием красным (раз в две секунды) обоих считывателей.

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

4.7.13 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;

4.8 Автоматизация

4.8.1 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.

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

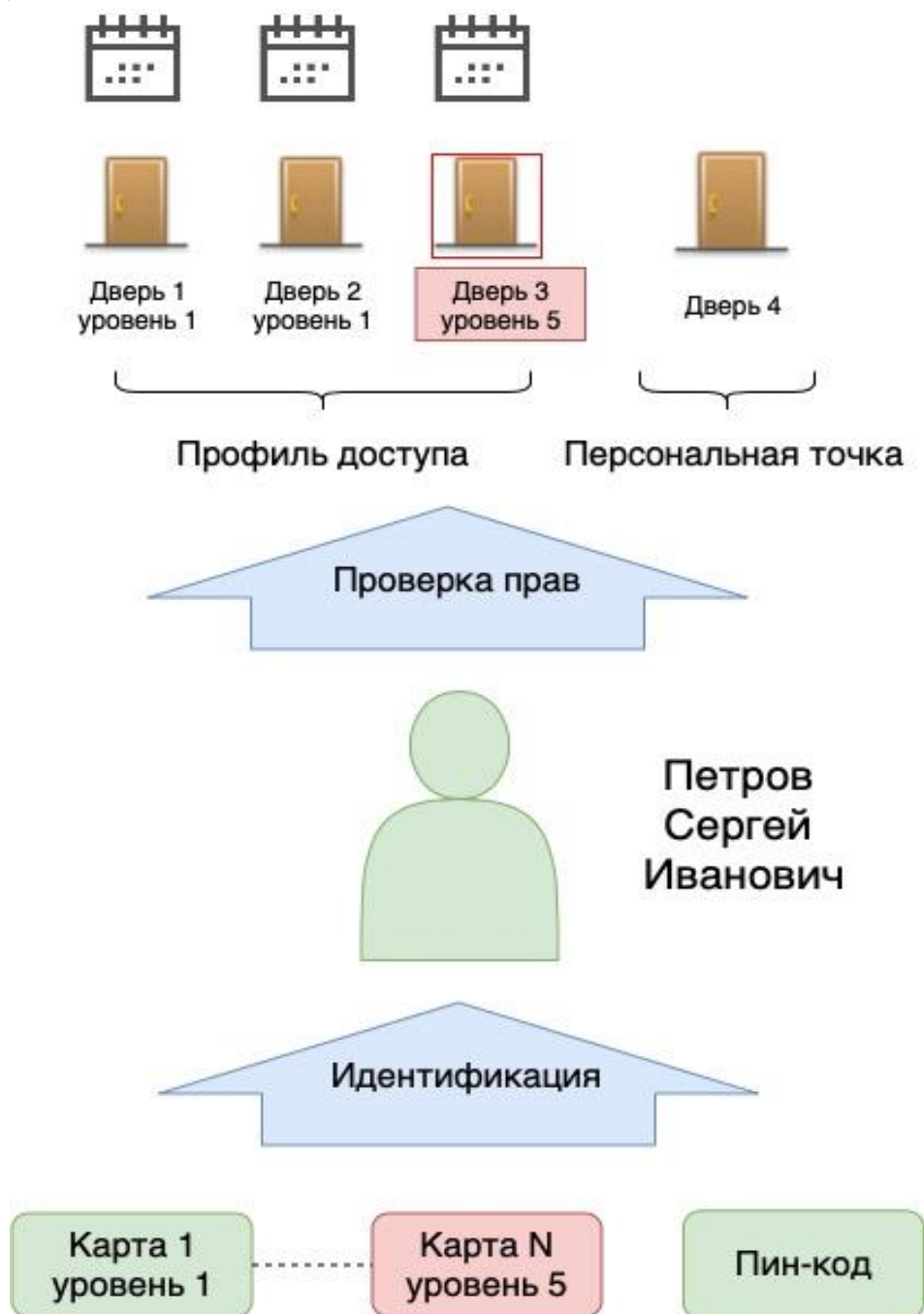
4.8.3 Если состояние точки было изменено вручную или по другому событию после сработки датчика, то возврат в предыдущее состояние не произойдет.

4.8.4 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:
 - **«По датчику»** – при возвращении датчика в исходное состояние точки прохода также переходят в исходное состояние.
 - **«По таймеру»** – заданный режим работы сохраняется, пока не истечет время на таймере.
 - **«Нет»**.

4.9 Схема установки и проверки правил доступа

4.9.1 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:



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

4.9.3 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.

4.9.4 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.

4.9.5 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.

4.10 Поля персонала

4.10.1 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: «**строка**», «**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.

4.11 Справочники

4.11.1 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.

4.12 Профили входа

4.12.1 Внутреннее программное обеспечение имеет защиту от несанкционированного доступа, основанную на логинах и паролях. Заводские настройки предусматривают наличие в системе оператора 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 административными правами. 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;
- «**Установщик**» – доступны только настройки оборудования.

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

4.12.3 При входе в систему оператор начинает сессию, которая будет автоматически закрыта по истечении времени сеанса. Такое поведение позволяет решить проблему оставленных окон в браузере. Длительность сессии по умолчанию – 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.

4.13 Интеграция с ОПС Рубеж R3

4.13.1 В целях более удобной эксплуатации СКУД на объектах, где установлена ОПС Рубеж R3, контроллеры могут взаимодействовать с приборами управления ОПС.

4.13.2 Интеграция осуществляется на аппаратном уровне и не требует для работы сервера FireSec.

4.13.3 В результате взаимодействия подсистем пользователь получает возможность управлять некоторыми охранными функциями через любую из них, а именно:

- при постановке/снятии с охраны охранных зон в ОПС Рубеж R3 будут ставиться/сниматься с охраны, связанные с этими зонами точки доступа СКУД Rubezh-Strazh;

- при постановке/снятии с охраны точек доступа в СКУД Rubezh-Strazh будут ставиться/сниматься с охраны, связанные с этими точками охранные зоны ОПС Рубеж R3.

4.13.4 Интеграция осуществляется через модуль MC-1, который подключается к RS-485 линии приборов управления ОПС и к USB-порту любого контроллера кластера. После подключения, необходимо произвести настройку внутреннего программного обеспечения. Предварительно нужно выгрузить файл описания охранной системы из ПО FireSec «Администратор».

4.13.5 Для настройки интеграции необходимо в Web-интерфейсе указать контроллер с подключенным к нему модулем MC-1, адрес модуля на RS-485 шине и скорость обмена.

4.13.6 Для связывания номеров охранных зон с точками доступа необходимо загрузить в систему файл синхронизации. После этого добавить требуемый список охранных зон и произвести ассоциацию с ними точек доступа путем перетаскивания точек на требуемые зоны. К каждой зоне могут быть привязаны несколько точек доступа.

4.13.7 После добавления настроек необходимо включить интеграцию и сохранить данные.

4.14 Администрирование доступа

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

4.15 Расписания доступа

4.15.1 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.

4.16 Профили доступа

4.16.1 Профиль доступа – это набор точек прохода, разрешенных для какой-либо персоны или группы персон. По умолчанию, точки добавляются 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, VIP-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.

4.16.2 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.

4.16.3 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.

4.16.4 Панель позволяет отфильтровать профили по содержащимся в них точкам. Что может быть удобно для анализа того, куда входит каждая конкретная точка.

4.17 Персонал

4.17.1 Весь персонал, который перемещается по территории, регистрируется в общей базе данных. Эта база синхронизируется между контроллерами кластера и является единой на весь кластер. Персона, по умолчанию, описывается ФИО, однако, 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 Raspberri (от 4 до 32 Гб) система способна хранить до миллиона фотографий.

4.17.2 Панель персонала позволяет фильтровать (искать) людей по фамилии и имени. Первая буква каждого слова в поле ввода вносится заглавной по умолчанию. 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.

4.17.3 Панель содержит возможность дополнительно фильтровать персонал по любому полю типа справочник. Оба фильтра работают одновременно. При выборе ФИО персоны происходит переход в карточку персоны. Если оставить курсор мыши на ФИО не нажимая, то через секунду всплывет фотография персоны под курсором.

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

4.17.5 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.

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

4.17.7 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.

4.17.8 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.

4.17.9 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.

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

4.17.11 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.

4.18 Импорт персонала

4.18.1 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. Поэтому одна из важных настроек – 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 в виду, что карты будут созданы с параметрами по-умолчанию для всех полей карт, кроме кода. Для полного сохранения картотеки (карт со всеми свойствами) необходимо экспортировать картотеку отдельно (см ниже).

4.18.2 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.

4.18.3 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.

4.18.4 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.

4.18.5 Если при импорте персоны оказывается, что в систему данные этого человека уже внесены ранее, но в его файле указаны иные идентификационные карты, то они дополняются данными новых идентификационных карт из импортируемого файла.

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

4.19 Картотека

4.19.1 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, то 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.

4.20 Картотека добавление

4.20.1 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. Все эти параметры могут быть настроены по умолчанию. Это позволяет ускорить занесение новых карт.

4.20.2 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 одно символьной командой;
- **Постановка точки прохода на охрану** – разрешает ставить точку прохода на охрану одно символьной командой;
- **Снятие точки прохода с охраны** – разрешает снимать точку прохода с охраны одно символьной командой;
- **Запуск автоматизации** – разрешает запускать автоматизацию двух символьной командой.

4.20.3 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.

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

4.21 Картотека экспорт и импорт

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

4.22 Журнал событий

4.22.1 Все что происходит в системе, записывается в журнал. Журнал событий каждого контроллера 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.

4.22.2 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.

4.22.3 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 стороны не порождать избыточные события.

4.22.4 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 же датчик не зафиксировал открытия двери после разрешения прохода, то фиксируется событие о несостоявшемся проходе.

4.22.5 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.

4.22.6 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.

4.22.7 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.

4.22.8 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.

4.22.9 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).

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

4.22.11 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.

4.22.12 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.

4.22.13 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.

4.22.14 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.

4.23 Онлайн мониторинг

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

4.24 Поиски в архиве

4.24.1 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 постранично, 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).

4.25 Выгрузка событий доступа во вне

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

4.25.2 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.

4.25.3 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.

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

4.25.5 Поддерживаемые форматы файлов – CSV и JSON.

5 Проблемы и их решения

5.1 Проблемы отображения веб интерфейса контроллера

5.1.1 Убедитесь, что используете совместимый веб браузер.

Поддерживаемые браузеры: Google Chrome, Opera, Mozilla FireFox, Safari, Microsoft Edge (Chromium).

5.2 Предупреждения браузера

5.2.1 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**".

5.3 Кодировка при загрузке справочников из файла

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

5.4 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 А или В 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

	Описание проблемы	Причина возникновения	Способ устранения
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
5	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

	Описание проблемы	Причина возникновения	Способ устранения
6	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
		3. Неисправен модуль доступа	Проверить целостность линии питания
7	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
8	Не совершается проход при прикладывании карты	1. Неверно сконфигурирована точка доступа	Произвести правильную настройку точки

	Описание проблемы	Причина возникновения	Способ устранения
	доступа к считывателю	2. Карта доступа не добавлена в конфигурацию	доступа согласно актуальному Руководству по эксплуатации, расположенному в веб-интерфейсе СКУД Strazh
		3. Карта доступа не привязана к конкретному пользователю	
		4. У пользователя, которому принадлежит карта доступа, не настроен график доступа	
9	Карта доступа не считывается, либо считывается с неверными значениями	Неправильное подключение считывателя Wiegand	Проверить и произвести правильное подключение, согласно схеме на считыватель и Руководству по эксплуатации на СКУД Strazh
10	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

	Описание проблемы	Причина возникновения	Способ устранения
		2. Неправильно настроена точка доступа «турникет»	Произвести корректную настройку точки доступа согласно Руководству по эксплуатации на СКУД Strazh
11	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

6 Хранение

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

6.2 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.

7 Транспортирование

7.1 Транспортирование упакованных в тару 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. Тара 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.

7.2 После транспортирования при отрицательных или повышенных 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.

8 Утилизация

8.1 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.