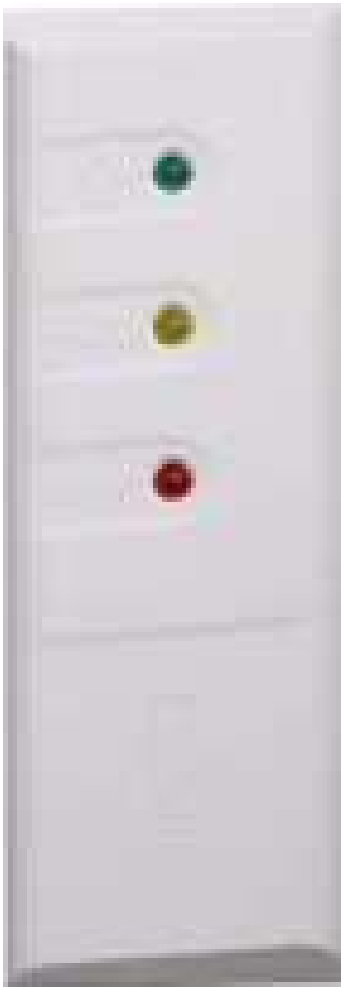
PERCo®

Контроллер замка

PERCo-CL05

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ



ЕДИНАЯ СИСТЕМА PERCo-S-20

Контроллер замка *PERCo-CL05*

Руководство по эксплуатации

СОДЕРЖАНИЕ

Уважаемые покупатели!

PERCo благодарит Вас за выбор контроллера замка нашего производства. Сделав этот выбор, Вы приобрели качественное изделие, которое при соблюдении правил монтажа и эксплуатации прослужит Вам долгие годы.

Настоящее «*Руководство по эксплуатации*» (далее – *Руководство*) предназначено для ознакомления с техническими характеристиками, составом и принципом работы контроллера замка ***PERCo-CL05,*** содержит сведения по транспортированию, хранению, монтажу и эксплуатации указанного изделия.

Данное «*Руководство по эксплуатации*» действует совместно с паспортами на подключаемые устройства.

Принятые сокращения:

ДУ – дистанционное управление;
ИУ – исполнительное устройство;
ПДУ – пульт дистанционного управления
СКУД – система контроля и управления доступом.

1 НАЗНАЧЕНИЕ

Контроллер ***PERCo-CL05*** (далее по тексту – контроллер) входит в единую систему безопасности и повышения эффективности предприятия *PERCo-S-20.*

Контроллер при подключении к нему замка электромагнитного или электромеханического типа позволяет организовать одностороннюю точку прохода, по картам формата *HID* или *EM-Marine.*

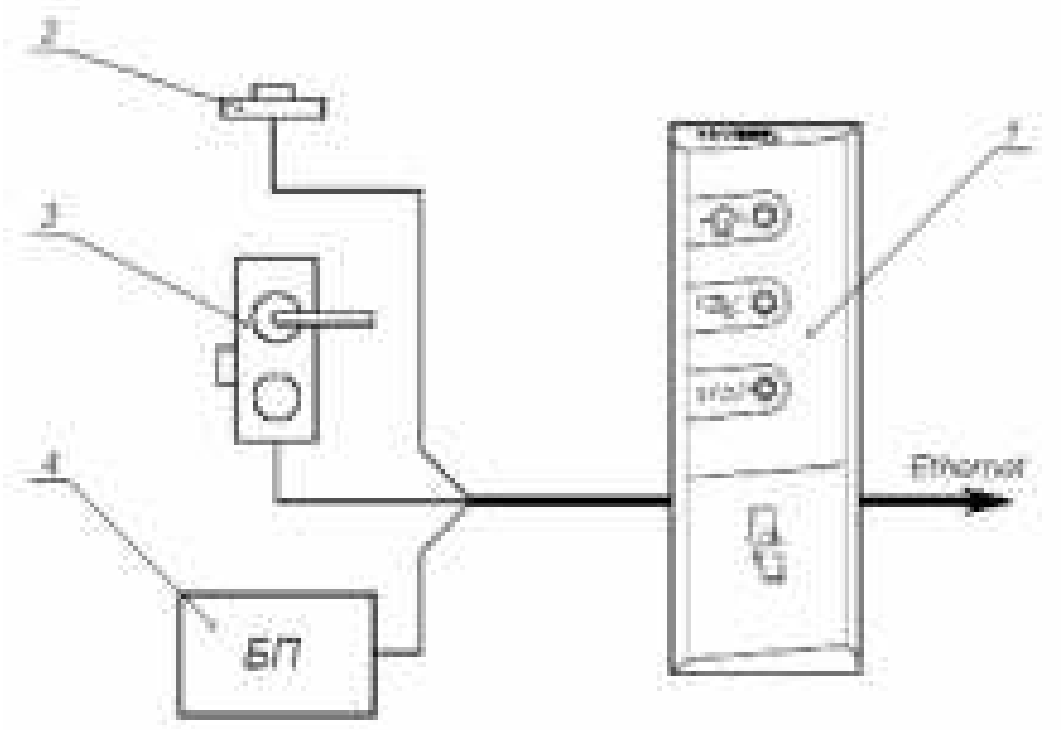


Рисунок 1 Функциональная схема подключений

1 – контроллер; 2 – кнопка ДУ; 3 –замок; 4 – блок питания

2 УСЛОВИЯ ЭКСПЛУАТАЦИИ

Контроллер замка по устойчивости к воздействию климатических факторов соответствует условиям УХЛ4.2 по ГОСТ 15150-69 (для эксплуатации в помещениях с искусственно регулируемыми климатическими условиями).

Эксплуатация контроллера замка разрешается при температуре окружающего воздуха от +1°С до +40°С и относительной влажности воздуха до 80% при +25°С.

3 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Номинальное значение напряжения питания постоянного тока, *В* ..... 12±1,2
Ток потребления, А ..... не более 0,15
Потребляемая мощность, *Вт* ..... не более 2
Типы карт доступа (брелоков) ..... HID, EM-Marine
Дальности считывания кода при номинальном значении напряжения питания:
- Для карт HID, *см* ..... не менее 5
- Для карт EM-Marine, *см* ..... не менее 8

Дальности считывания кода при установке на металлическом основании:
- Для карт HID, *см* ..... не менее 4
- Для карт EM-Marine, *см* ..... не менее 7

Число пользователей (карт доступа) ..... до 50000
Число событий журнала регистрации ..... до 135000
Количество контролируемых дверей 1
Количество входов дистанционного управления 1
Количество выходов (выход типа «открытый коллектор») 1
Стандарт интерфейса связи ..... Ethernet (IEEE 802.3)
Длина кабеля подключения Ethernet, *м* 3
Длина кабеля подключения периферии, *м* 0,9
Масса контроллера, *кг* ..... не более 0,3
Габаритные размеры контроллера (без учета кабеля), *мм* ..... 145×50×20
Средний срок службы, *лет* 8
Класс защиты от поражения электрическим током ..... III по ГОСТ Р МЭК730-1-94

4 КОМПЛЕКТ ПОСТАВКИ

Контроллер, *шт.* 1
Металлическое основание, *шт.* 1
Джампер (перемычка), *шт.* 1
Супрессор на 15 – 18 В, *шт.* 1
Монтажный комплект:
- переходная розетка RJ45, *шт.* 1
- дюбели пластмассовые, *шт.* 4
- шурупы, *шт.* 4

Упаковка, *шт.* 1
Паспорт, *экз.* 1
Руководство по эксплуатации, *экз.* 1

Дополнительное оборудование, поставляемое по отдельному заказу:

PoE-сплиттер PA1212[1], *шт*. 1

5 ОПИСАНИЕ

5.1 Устройство и работа

Контроллер представляет собой блок электроники в пластмассовом корпусе, на передней панели которого расположены три светодиодных индикатора.

Для крепления контроллера к поверхности в комплект поставки входит металлическое основание.

Защита электроники от негативных воздействий окружающей среды обеспечивается за счет заливки компаундом.

Кабель связи для подключения к сети *Ethernet* и кабель для остальных подключений к контроллеру замка выведены с его тыльной стороны.

Контроллер имеет встроенный бесконтактный считыватель карт доступа форматов *HID* и *EM-Marine*;

Контроллер работает с картами, размер кода которых не более 64 бит.

В контроллере установлены:
- энергонезависимая память;
- энергонезависимый RTC-таймер (часы реального времени);
- пьезоизлучатель (звуковой индикатор).

Контроллер способен хранить в энергонезависимой памяти
- до 50 000 идентификаторов карт;
- до 135 000 событий журнала регистрации с указанием даты и времени события[2].

Контроллер обеспечивает:
- связь по интерфейсу *Ethernet* (*IEEE 802.3*);
- поддержку стека протоколов *TCP/IP (ARP, IP, ICMP, TCP, UDP, DHCP)*;
- поддержку прикладного уровня протокола обмена системы *PERCo-S-20*;
- возможность обновления встроенного ПО через *Ethernet*.

На этапе производства контроллеру заданы:
- уникальный физический MAC-адрес (указан в паспорте и на тыльной стороне корпуса);
- IP-адрес (указан в паспорте и на тыльной стороне корпуса);
- маска подсети (255.0.0.0);
- IP-адрес шлюза (0.0.0.0).

Предусмотрены следующие способы задания IP-адреса, шлюза, маски подсети контроллера на этапе конфигурации системы:
- работа с заводскими настройками;

[1] ***PoE-сплиттер PA1212*** позволяет подавать питание на контроллер по сети *Ethernet*. Сплиттер может использоваться с сетевыми коммутаторами, поддерживающими технологию передачи электроэнергии по витой паре PoE и совместимыми со стандартом *IEEE 802.3af*

[2] В случае переполнения журнала регистрации новые события заменяют наиболее старые (Удаление происходит блоками по 256 событий).

- ручной ввод;
- получение от DHCP сервера.

Контроллер позволяет осуществлять управление замком с помощью следующих устройств:

- кнопка ДУ;
- карта доступа, при поднесении ее к контроллеру;
- компьютер (при подключении по сети Ethernet и установке ПО).

Возможно подключение следующего дополнительного оборудования:

- датчик двери (геркон);
- кнопка ДУ;
- внешний звуковой оповещатель (сирена).

Контроллер как элемент СКУД обеспечивает:

- работу в режимах: *«Открыто»*, *«Контроль»*, *«Совещание»*, *«Охрана»*, *«Закрыто»*;
- сохранение установленного режима в энергонезависимой памяти, для предотвращения снятия режима при выключении питания;
- поддержку функции глобального контроля зональности;
- поддержку функции комиссионирования;
- поддержку функции верификации.

Контроллер как элемент охранной сигнализации обеспечивает:

- подключение светового или звукового оповещателя;
- возможность постановки и снятия ИУ с охраны;
- передачу тревожных извещений на пульт централизованного наблюдения.

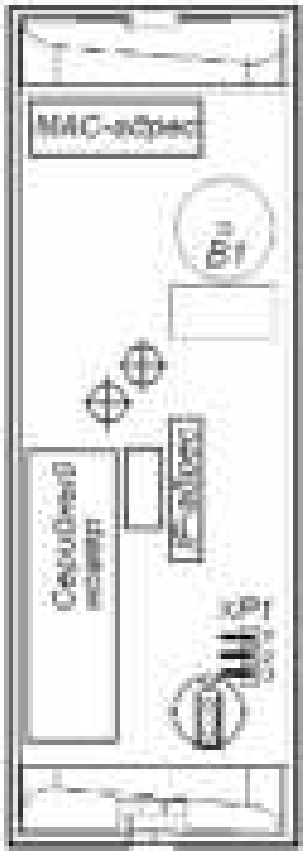


Рисунок 2 Внешний вид тыльной стороны контроллера

5.2 Параметры сигналов релейного выхода управления ИУ

Контроллер имеет один релейный выход управления *И*У: *Lock.*

Схема подключения к выходу указана на рисунке 4.

Релейный выход *Lock* имеет полную группу контактов (нормально разомкнутый NO, нормально замкнутый NC и общий выводной C контакты), используется для управления *И*У и имеет следующие параметры:

максимальное коммутируемое напряжение постоянного тока, *В*.....не более 30
максимальное коммутируемое напряжение переменного тока, *В*.....не более 42
постоянный/переменный ток, *А*.....не более 2

Выход управления может поддерживать потенциальный и импульсный режимы работы замка. Выбор режима осуществляется с помощью параметра *И*У **Режим работы выхода управления.**

При **потенциальном** режиме работы *И*У:

- При реализации однократного прохода релейный выход активизируется на время, определяемое в ПО параметром **Время удержания в разблокированном состоянии**, или до момента совершения прохода**.**
- При установке *И*У в режим *«Открыто»* релейный выход активизируется до изменения режима.

При **импульсном** режиме работы *И*У:

- При реализации однократного прохода выход активизируется на время, определяемое параметром **Длительность импульса управления ИУ.** При этом *И*У разблокируется до момента совершения прохода.
- При установке *И*У в режим *«Открыто»* выход активизируется на время, определяемое параметром **Длительность импульса управления ИУ**, после чего будет активизироваться каждый раз на это же время через одну секунду после нормализации *И*У.

Фактом совершения прохода в заданном направлении является передний или задний фронт сигнала на входе *Door*, в зависимости от конфигурации *И*У.

5.3 Параметры сигналов дополнительного релейного выхода

Контроллер имеет один релейный выход: *Out.*

Схема подключения к выходу указана на рисунке 4.

Выход *Out* типа «открытый коллектор» может использоваться для управления дополнительным оборудованием и имеет следующие параметры:

максимальное напряжение постоянного тока, *В*.....не более 30
максимальный ток, *А*.....не более 0,15

5.4 Параметры сигналов входов Door и DU

Контроллер обеспечивает контроль состояния двух входов под управлением выходами типа «сухой контакт» или «открытый коллектор» (ОК), выполняющих следующие функции:

- *Door* – подключение датчика двери (геркон);
- *DU* – подключение кнопки ДУ («Выход»).

Схема подключения к входам указана на рисунке 4.

Примечание

Все неподключенные входы подтянуты к питанию. Для создания сигнала высокого уровня на всех входных контактах (*Door* и *DU*) используются резисторы с сопротивлением 2 кОм, подключенные к шине питания +3,3 В.

Факт активизации для сигнала *Door* зависит от описания его исходного состояния в параметре **Нормальное состояние контакта** в ПО S-20:

- если вход описан как **Разомкнут**, то его активизация осуществляется подачей на него сигнала низкого уровня относительно контакта *GND*. При этом управляющим элементом могут быть нормально разомкнутый контакт реле или схема с открытым коллекторным выходом.
- если вход описан как **Замкнут**, то его активизация осуществляется снятием с него сигнала низкого уровня относительно контакта *GND*. При этом управляющим элементом могут быть нормально замкнутый контакт реле или схема с открытым коллекторным выходом.

Исходное состояние сигнала *DU* не описывается в ПО PERCo-S-20, оно считается как **Нормально разомкнут**, поэтому активизация для данного входа осуществляется подачей на него сигнала низкого уровня относительно контакта *GND*. При этом управляющим элементом могут быть нормально разомкнутый контакт реле или схема с открытым коллекторным выходом.

Управляющий элемент должен обеспечивать следующие характеристики сигналов:

Управляющий элемент – контакт реле:

минимальный коммутируемый ток, *мА* .....не более 1
сопротивление замкнутого контакта
(с учетом сопротивления кабеля подключения), *Ом* .....не более 300

Управляющий элемент – схема с открытым коллекторным выходом:

напряжение на замкнутом контакте
(сигнал низкого уровня, на входе контроллера), *В* .....не более 0,8

5.5 Выбор способа задания IP-адреса

Внимание

Установка и снятие перемычек должны производиться только при выключенном оборудовании.

Выбор способа задания IP-адреса контроллера осуществляется установкой или снятием перемычки (джампера) на разъем *XP1* на тыльной стороне контроллера. Расположение перемычки указано на рисунке 2. Возможны следующие способы задания IP-адреса:

1. Перемычка снята.
   - Если IP-адрес (шлюз, маска подсети) не был изменен пользователем, контроллер работает с заводскими установками.
   - При изменении IP-адреса (шлюза, маски подсети) в «ручном» режиме (UDP1), контроллер сразу начинает работать с параметрами, заданными пользователем (без переключения питания).

Примечания

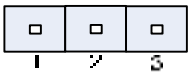
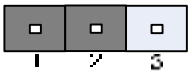
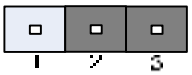
1. Заводские установки контроллера: IP-адрес и MAC-адрес указаны в паспорте и на тыльной стороне контроллера; маска подсети 255.0.0.0; IP-адрес шлюза 0.0.0.0.
2. Конфигурация в «ручном» режиме должна происходить в подсети, в которой расположен сервер системы.

2. *«IP MODE»* Перемычка в положение 1–2. Вариант предназначен для работы в сетях с динамическим распределением IP-адресов.
   - Контроллер получает IP-адрес (шлюз, маску подсети) от DHCP-сервера.
3. *«IP DEFAULT»* Перемычка в положение 2–3.
   - Контроллер работает с заводскими установками IP-адреса (шлюза, маски подсети).
   - Пароль для доступа к контроллеру сбрасывается.

Примечание

Пользовательские установки IP-адреса (шлюза, маски подсети), если они были заданы, при переходе в режим *«IP DEFAULT»* сохраняются. При следующем включении, если перемычка будет снята, контроллер начнет работать с ними.

Таблица 1 Варианты установки перемычки на разъем XP1

№	Расположение перемычки на XP1	Режим
1		Перемычка снята
2		IP MODE
3		IP DEFAULT

6 МАРКИРОВКА И УПАКОВКА

Контроллер имеет маркировку в виде этикетки, расположенной на тыльной стороне корпуса. На этикетке нанесены следующие сведения о контроллере:

- товарный знак и контактные данные предприятия-изготовителя;
- наименование и номер модели;
- серийный номер;
- год и месяц изготовления;
- допустимый диапазон напряжения питания и потребляемый ток.

Кроме этого на тыльной стороне корпуса контроллера находятся этикетки, на которых указаны установленные при производстве: MAC – адрес и IP – адрес.

Расположение этикеток показано на рисунке 2. Контроллер упакован в картонную коробку, предохраняющую его от повреждений во время транспортировки и хранения.

7 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

7.1 Безопасность при монтаже

Внимание!

Все подключения и установка перемычек должны производиться только при выключенном оборудовании, отключенных источниках питания.

Монтаж и техническое обслуживание контроллера должны проводиться лицами, полностью изучившими настоящее *Руководство*.
Монтаж контроллера должен производиться специалистом-электромонтажником.
При монтаже контроллера пользуйтесь только исправным инструментом.
Монтаж должен соответствовать СНиП 3.05.07-85 Системы автоматизации и СНиП 3.05.06-85 Электротехнические устройства.

7.2 Безопасность при эксплуатации

При эксплуатации контроллера соблюдайте общие правила при работе с электрическими приборами.

Запрещается!

- Эксплуатировать контроллер при напряжении питания, не соответствующем техническим характеристикам контроллера.
- Эксплуатировать контроллер в условиях, не соответствующих требованиям раздела 2 «Условия эксплуатации».
- Использовать абразивные и химически активные вещества для чистки загрязненных наружных поверхностей корпуса контроллера.
- Допускать рывки и удары по корпусу контроллера, замку, датчику двери, кнопке ДУ и соединительным кабелям, которые могут вызвать их механические повреждения и деформацию.

Требования безопасности при эксплуатации источника питания указаны в *Паспорте* на источник питания.

8 МОНТАЖ

8.1 Общие указания

Контроллеры рекомендуется монтировать в непосредственной близости от ИУ. Точная высота для монтажа контроллера должна выбираться исходя из соображения удобства для предъявления карт доступа. Также при выборке места установки контроллера необходимо учитывать, что:

- при установке контроллера на металлическую поверхность, дальность считывания кода с карты уменьшается на 15 - 25 %;
- взаимное удаление контроллеров замка PERCo-CL05 друг от друга и от считывателей должно составлять не менее 50 см.

При прокладке всех сигнальных кабелей (Ethernet, кнопки ДУ, датчика двери и к замку) и кабелей низковольтного питания необходимо учитывать, что:

- близко расположенные источники электрических помех могут вызывать сбои в работе системы, поэтому нельзя устанавливать оборудование на расстоянии менее 1 м от электрогенераторов, электродвигателей, реле переменного тока,

тиристорных регуляторов света и других мощных источников электрических помех;

- при прокладке все сигнальные кабели, датчики, ИУ и кабели низковольтного питания должны быть размещены на расстоянии не менее 50 см от силовых кабелей переменного тока, кабелей управления мощными моторами, насосами, приводами и т. д;
- пересечение всех сигнальных кабелей с силовыми кабелями допускается только под прямым углом;
- любые удлинения кабелей (кроме кабеля Ethernet) производить ***только методом пайки.***

8.2 Кабели

При монтаже контроллера используйте кабели, указанные в таблице 2.

Таблица 2 Кабели, применяемые при монтаже

№	Кабельное соединение	Макс. длина, м	Тип	Мин. сечение провода, мм^2	Пример
1	Ethernet (IEEE 802.3) – контроллер	100	Четыре витые пары не ниже пятой категории	0.2	
2	Контроллер – ИУ	30	Двужильный кабель	0.75	ШВВП (2x0.75 двухцветный)
3	Контроллер – кнопка ДУ	30	Двужильный кабель	0.2	RAMCRO SS22AF-T (2×0.22) или CQR-2
4	Контроллер – датчик двери				
5	Контроллер (выход) – дополнительное оборудование	30	Двужильный кабель	0.2	RAMCRO SS22AF-T (2×0.22) или CQR-2
6	Контроллер – источник питания	2	Двужильный кабель	0.75	ШВВП (2×0.75 двухцветный)

8.3 Порядок монтажа

Придерживайтесь следующей последовательности действий при монтаже контроллера:

1. Распакуйте коробку и проверьте комплектность контроллера, подключаемых устройств и ЗИП согласно сведениям разделов «Комплект поставки» соответствующих руководств по эксплуатации. Убедитесь в отсутствии на оборудовании механических повреждений.
2. Определите место установки контроллера. При выборе места установки следуйте указаниям п. 8.1.
3. Произведите разметку и разделку отверстий на установочной поверхности для крепления металлического основания и проводки кабелей согласно схеме, представленной на рисунке 3.
4. Ослабьте винт, расположенный в нижней части корпуса контроллера и крепящий его к металлическому основанию. Снимите металлическое основание.

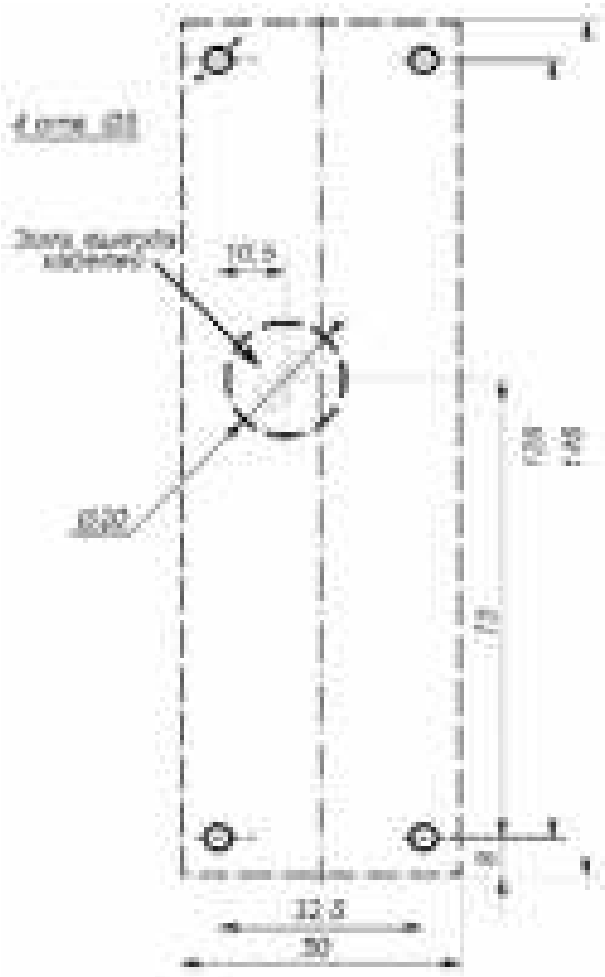


Рисунок 3 Разметка отверстий для установки контроллера (пунктиром показаны габариты корпуса контроллера)

5. Закрепите металлическое основание на установочной поверхности с помощью четырех шурупов из комплекта поставки.
6. Выберите способ задания IP-адреса контроллера (см. п. 5.5) и при необходимости установите перемычку (джампер) на разъем *XP1* согласно таблице 1. Расположение перемычки указано на рисунке 2.
7. Пропустите кабели контроллера через предназначенное для них отверстие на установочной поверхности. При креплении контроллера необходимо обеспечить радиус изгиба кабелей у основания контроллера не менее 10 мм. При эксплуатации контроллера может потребоваться изменить состояние его перемычек, поэтому рекомендуется оставлять запас длины кабелей, выходящих из контроллера, достаточный для отведения его от стены и обеспечения доступа к перемычкам.
8. Установите контроллер на металлическое основание и закрепите на нем с помощью винта, расположенного в нижней части корпуса контроллера.
9. Произведите разделку двери и монтаж замка (защелки) в соответствии с паспортом на замок (защелку). Подключите кабель №2 к замку (защелке).
10. Для снятия статического электричества заземлите корпус или запорную планку замка. В случае установки замка на металлическую дверь, заземлите полотно двери. Заземление выполнять проводом с сечением не менее 0,75 мм^2.
11. Установите кнопку ДУ. Место для монтажа кнопки ДУ должно выбираться, исходя из соображения удобства ее (например, рядом с дверью). Подключите кабель №3 к кнопке ДУ.

12. Смонтируйте магнитный датчик двери. Магнитный датчик двери (геркон) должен быть закреплен на раме двери, а магнит – на двери таким образом, чтобы при закрытой двери обеспечивалось устойчивое замыкание контакта датчика. Подключите кабель №4 к датчику.
13. Смонтируйте при необходимости дополнительное оборудование (например, сирену). Подключите кабель №5 к дополнительному оборудованию.
14. Установите источник питания на место его постоянной эксплуатации. Подключите кабель №6 к источнику питания.

Примечание

Порядок подключения контроллера через PoE-сплиттер ***PA1212*** – см. Приложение В.

15. Подключите кабель Ethernet, выходящий из контроллера к локальной сети. При необходимости используйте переходную розетку RJ45 из комплекта поставки. Для удлинения используйте кабель №1.
16. Подключите кабели устройств к штатному кабелю контроллера согласно схеме на рисунке 4.

Внимание!

- Если подключаемый *замок не имеет встроенной цепи искрозащиты,* то необходимо использовать диод искрозащиты (***VD1*** на рисунке 4). Например, диод Шоттки рассчитанный на рабочий ток не менее 1*А*, типа 1N5819.
- Если подключаемый электромагнитный *замок не имеет размагничивающей цепи*, то необходимо установить двунаправленный супрессор из комплекта поставки. Супрессор устанавливается в непосредственной близости от замка (***VD1*** на рисунке 4).
- При подключении контроллера через PoE-сплиттер ***PA1212*** (см. рис. В.2 в приложении В) рекомендуется использовать только электромеханические замки, поэтому необходимо использовать именно диоды искрозащиты (***VD4*** и ***VD1*** на рис. 4) типа 1N5819. Использование супрессора в этом случае **ЗАПРЕЩЕНО!**

17. Произведите укладку и закрепление кабелей, используя при необходимости пластиковые скобы (например, SC4-6, SC5-7, SC7-10). При монтаже и прокладке кабелей необходимо учитывать требования п. 8.1.
18. Проверьте отсутствие обрывов и коротких замыканий во всех линиях.

8.4 Включение

При включении источника питания все световые индикаторы на корпусе контроллера замка будут мигать в течение 3 секунд. После окончания этого времени на индикаторах контроллера отобразится индикация последнего установленного режима работы.

При первом включении контроллера после завершения монтажа или после форматирования памяти на корпусе контроллера начнется синхронное мигание всех трех индикаторов 2 раза в секунду, что означает отсутствие настроек контроллера. В этом случае необходимо передать конфигурацию контроллеру и подключенным к нему устройствам. Это можно сделать через Web-интерфейс или с помощью ПО.

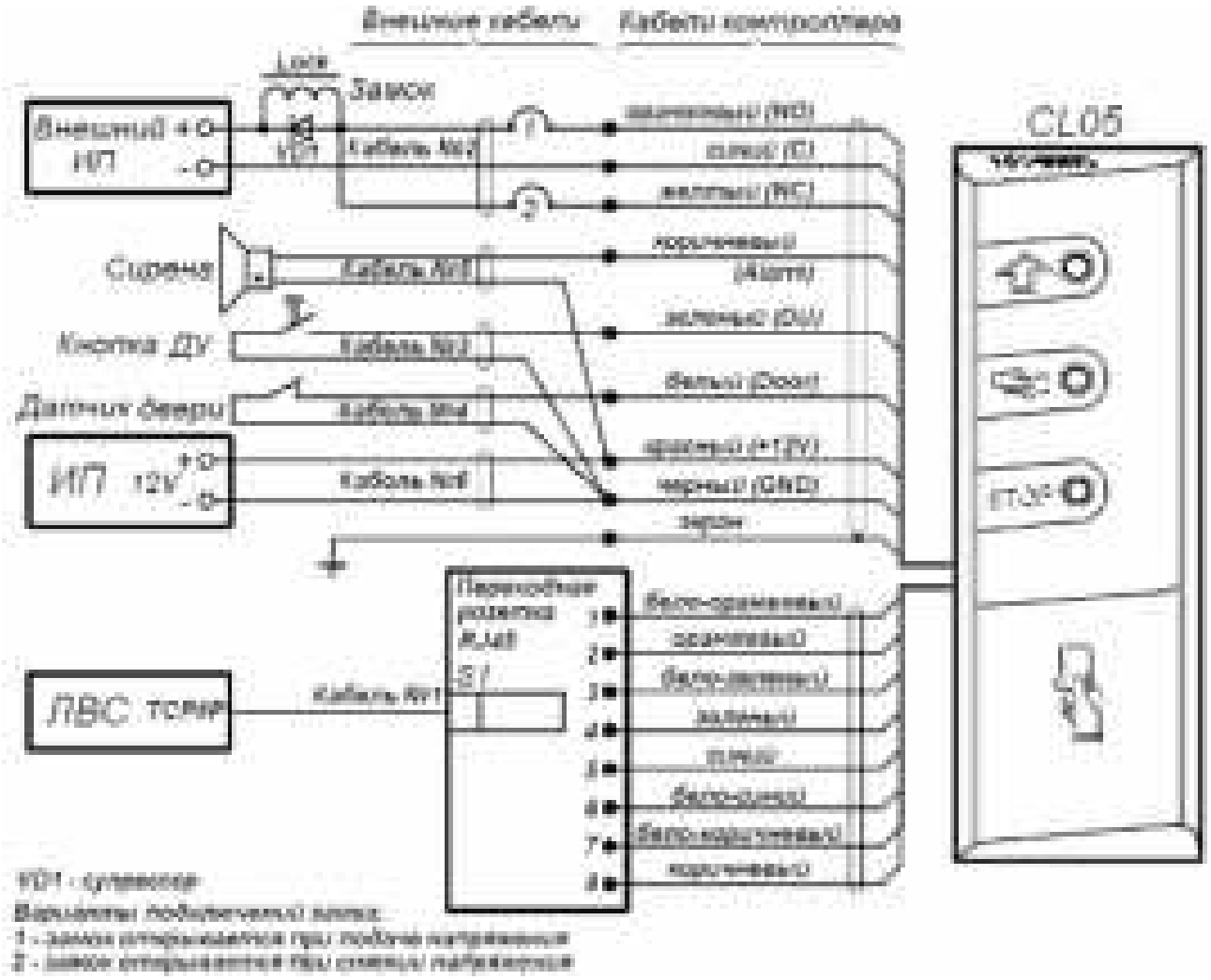


Рисунок 4 Схема подключений контроллера

8.5 Подключение по сети Ethernet

Для подключения к контроллеру по сети *Ethernet* необходимо, чтобы компьютер находился в одной подсети с контроллером. Для этого при первом подключении может потребоваться изменить сетевые настройки компьютера. При производстве контроллерам *PERCo* выдаются IP-адреса из 10-й подсети, поэтому необходимо добавить в дополнительные параметры TCP/IP компьютера IP-адрес: 10.x.x.x (x-произвольные числа) и маску подсети 255.0.0.0. Наличие таких серверов или служб, как DNS и WINS, не требуется. Контроллер при этом должен быть подключен в тот же сегмент сети или непосредственно к разъему сетевой карты компьютера. После подключения сетевые настройки контроллера можно изменить на рекомендованные системным администратором из ПО или через Web-интерфейс.

9 КОНФИГУРАЦИЯ

Конфигурацию контроллера и подключенных к нему устройств можно производить либо через Web-интерфейс, либо установив на компьютер дополнительное ПО:

- ***«Локальное ПО» PERCo-SL01***;
- ***«Локальное ПО с верификацией» PERCo-SL02***;
- Сетевое «***Базовое ПО S-20» PERCo-SN01***;
- Сетевое «***Расширенное ПО S-20» PERCo-SS02***.

9.1 Выбор формата хранения идентификаторов

Внимание

Изменение формата хранения идентификаторов при наличии в памяти контроллера карт приведет к тому, что проход по занесенным ранее в другом формате картам станет невозможен.

В системе доступны следующие форматы хранения идентификаторов:

- *Сокращенный (4 байт)* Используются только 4 младшие байта номера карты. (Данный формат не доступен при работе через Web-интерфейс.)
- *Wiegand-26* (Установлен по умолчанию.) При выборе формата Wiegand-26 будут использоваться только 3 младших байта номера карты. При этом номер карты делится на два числа - серия (1 байт, максимальное значение 255) и номер (2 байта, максимальное значение 65535). В таблицах ПО идентификатору отведено два столбца: **Код семейства** и **Номер**.
- *Универсальный (8 байт)* При выборе данного формата используются все 8 байт номера карты. Значение идентификатора – единое число. Во всех таблицах ПО идентификатору выделен один столбец **Идентификатор** (или **Одним числом**).

Порядок установки выбранного формата описан отдельно для ПО и Web-интерфейса (см. 9.2.8, 9.3.2, 9.4.2).

9.2 Настройка через Web-интерфейс

Использование Web-интерфейса позволяет без инсталляции какого-либо дополнительного ПО производить следующие действия как для самого контроллера, так и для подключенных к нему устройств:

- Задавать параметры конфигурации ИУ и считывателя;
- Устанавливать режимы работы для считывателя;
- Заносить в память контроллера номера карт доступа и выдавать им права постановки и снятия с охраны;
- Просматривать события журнала регистрации контроллера и сохранять их в файл;
- Контролировать состояние контроллера и подключенных к нему устройств;
- Проводить диагностику контроллера, форматирование памяти и обновление встроенного ПО.

9.2.1 Подключение к контроллеру

Для работы с Web-интерфейсом:

1. Откройте Web-браузер, (например, Internet Explorer).
2. Введите в адресную строку IP-адрес контроллера и нажмите кнопку **Enter** на клавиатуре.

Примечания

IP-адрес контроллера указан в паспорте и на плате контроллера.

Для подключения к контроллеру по сети *Ethernet* необходимо, чтобы компьютер находился в одной подсети с контроллером.

В настройках используемого браузера необходимо отключить прокси-сервер.

3. При необходимости введите пароль доступа к контроллеру. По умолчанию пароль отсутствует. При вводе пароля поле **Имя пользователя** оставьте пустым.
4. Откроется главная страница Web-интерфейса контроллера.

Внимание

При работе контроллера под управлением сетевого или локального ПО *PERCo-S-20* подключение к Web-интерфейсу контроллеру невозможно. После прекращения работы ПО и остановки сервера системы подключение к Web-интерфейсу возможно, если в ПО был установлен параметр **Разрешить Web-интерфейс**.

На странице можно выделить следующие элементы:

1. Выбор языка Web-интерфейса:
   - **ru** – русский;
   - **en** – английский.
2. Меню Web-интерфейса. Меню имеет следующую структуру:

«Главная»	*«Изменить настройки»*
«Смена пароля»	
«Конфигурация»	*«Исполнительное устройство»* *«Считыватель»* *«Формат для ввода и хранения карт доступа»*
«Управление»	*«Управление считывателем»* *«Управление исполнительным устройством»*
«Карты доступа»	*«Ввод номера карты вручную / поиск карты»* *«Ввод номера карты через считыватель»* *«Список загруженных карт»* *«Загрузка карт из файла»*
«События»	
«Состояние»	
«Диагностика»	

3. Рабочая область страницы.

9.2.2 Установка параметров конфигурации

Внимание

При первом включении контроллера после изменения конфигурации с помощью перемычек или форматирования памяти необходимо передать в контроллер конфигурацию подключенных к нему устройств. Индикацией отсутствия настроек параметров служит синхронное мигание всех трех индикаторов на передней панели 2 раза в секунду.

Для установки конфигурации:

1. В меню Web-интерфейса нажмите **Конфигурация.**
2. На странице **Исполнительное устройство** установите необходимые параметры ИУ и нажмите кнопку **Сохранить**.
3. На странице **Считыватель** выберите значение параметра **Управление от ДУ** и нажмите кнопку **Сохранить**.
4. На странице **Формат для ввода и хранения карт доступа** выберите формат и нажмите кнопку **Сохранить**.
5. На странице **Управление считывателем** выберите режим работы для считывателя.
6. Состояние ИУ и индикация на передней панели контроллера должны измениться в соответствии с установленным режимом работы.

9.2.3 Изменение сетевых настроек контроллера

Для изменения сетевых настроек контроллера:

1. Нажмите последовательно в меню Web-интерфейса: **Главная → Изменить настройки.** Откроется страница с рабочей областью следующего вида:

2. В поля ввода **Новый IP-адрес**, **Новый адрес шлюза**, **Новая маска подсети** введите новые значения сетевых параметров контроллера. Нажмите кнопку **Сохранить**. Новые сетевые настройки будут сохранены в контроллере.

Примечание

На этой же странице можно установить системные дату и время и контроллера. Для синхронизации времени и даты контроллера с установленными на компьютере переведите переключатель **Текущее дата и время** в положение **Синхронизация с ПК** и нажмите кнопку **Сохранить**. Для ручного ввода времени и даты переведите переключатель в положение **Ручная настройка**, введите в поля ввода **DD.MM.YYYY** и **HH:MI:SS** новые дату и время. Нажмите кнопку **Сохранить**.

9.2.4 Изменение пароля контроллера

Для смены или задания пароля контроллера:

1. Нажмите в меню Web-интерфейса: **Смена пароля.** Откроется страница с рабочей областью следующего вида:

2. В поле **Новый пароль** введите новый пароль контроллера, в поле **Подтвердите пароль** введите пароль повторно для подтверждения правильности ввода.
3. Нажмите кнопку **Сохранить**.

9.2.5 Настройка параметров исполнительного устройства

Для настройки через Web-интерфейс доступны следующие параметры ИУ:

Предельное время разблокировки. Если до истечения этого времени ИУ не будет заблокировано после прохода по карте доступа, то контроллер сформирует сообщение *«ИУ не закрыто после прохода по идентификатору»*.

Время удержания в разблокированном состоянии. Время, на которое открывается ИУ, а также время, в течение которого необходимо повторно предъявить карту, имеющую право постановки на охрану, для постановки ИУ на охрану (время анализа карты).

Длительность импульса (для импульсного режима). Параметр доступен при выборе импульсного режима работы выхода ИУ. Определяет длительность управляющего импульса и зависит от характеристик ИУ.

Нормальное состояние датчика (геркон) (*Нормально замкнут / Нормально разомкнут*). Состояние датчика двери / выхода PASS турникета при заблокированном состоянии данного ИУ.

Нормальное состояние выхода управления (*Запитан / Не запитан*). Параметр описывает состояние выхода управления ИУ для приведения ИУ в заблокированное состояние.

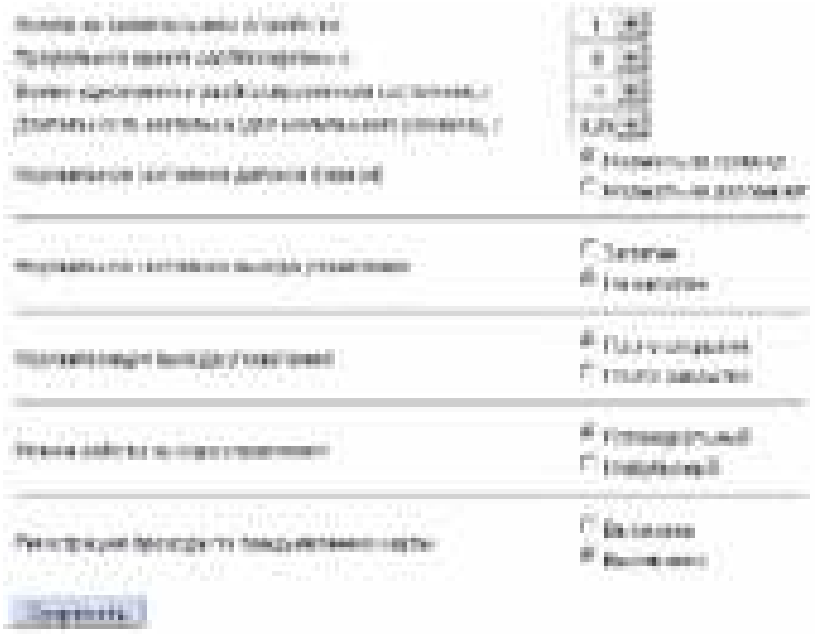
Нормализация выхода управления (*После открытия / После закрытия*). Параметр определяет, в какой момент нормализуется состояние выхода управления ИУ.

Режим работы выхода управления (*Потенциальный / Импульсный*). Импульсный режим управления применяется только для замков, поддерживающих этот режим. Рекомендуется использовать для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки «CISA»).

Регистрация прохода по предъявлению карты. Если выбрано значение параметра **Включена**, то для разрешенной карты событие *«Проход»* формируется сразу в момент ее предъявления, независимо от того, будет ли затем реально совершен проход через это ИУ.

9.2.6 Для настройки параметров ИУ:

1. Нажмите последовательно в меню Web-интерфейса: **Конфигурация** → **Исполнительное устройство.** Откроется страница с рабочей областью следующего вида:



2. Произведите необходимые изменения настроек параметров.
3. Нажмите кнопку **Сохранить**.

9.2.7 Настройка параметров считывателей

Для настройки параметров считывателя:

1. Нажмите последовательно в меню Web-интерфейса: **Конфигурация** → **Считыватель.** Откроется страница с рабочей областью следующего вида:

2. Установите переключатель **Управление от ДУ** в положение **Запрещено**, либо **Разрешено**.
3. Нажмите кнопку **Сохранить**.

9.2.8 Выбор формата хранения идентификаторов

Внимание

Изменение формата хранения идентификаторов может привести к тому, что загруженные ранее в другом формате карты не смогут быть считаны.

Для выбора формата идентификаторов карт:

1. Нажмите последовательно в меню Web-интерфейса: **Конфигурация** → **Формат для ввода и хранения карт доступа.** Откроется страница с рабочей областью следующего вида:

2. С помощью переключателя **Выбор формата** выберите один из предложенных форматов.
3. Нажмите кнопку **Сохранить**.

9.2.9 Управление считывателем

Для управления режимом контроля доступа через ИУ произведите следующие действия:

1. Нажмите последовательно в меню Web-интерфейса: **Управление** → **Управление считывателем.** Откроется страница с рабочей областью следующего вида:

1. В строке **Текущий режим работы** отображается установленный в настоящий момент режим контроля доступа.
2. С помощью кнопок **Контроль**, **Открыто**, **Закрыто**, **Охрана** установите режим работы через выбранный считыватель.

9.2.10 Сброс тревоги исполнительного устройства

Для сброса тревоги исполнительного устройства:

1. Нажмите последовательно в меню Web-интерфейса: **Управление** → **Управление исполнительным устройством.** Откроется страница с рабочей областью следующего вида:

2. Нажмите кнопку **Сбросить тревогу**. Состояние тревоги для выбранного ИУ будет сброшено.

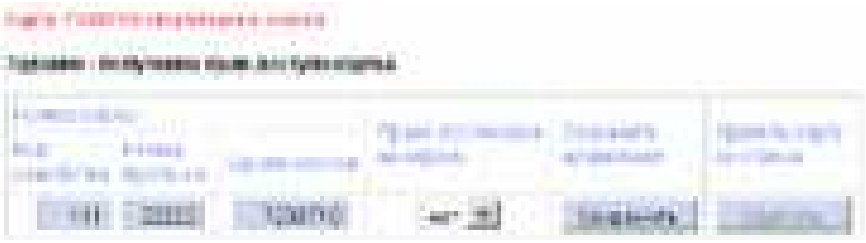
9.2.11 Добавление карт доступа

Ввод идентификатора вручную

Для ввода идентификатора карты вручную:

1. Нажмите последовательно в меню Web-интерфейса: **Карты доступа** → **Ввод номера карты вручную / поиск карты.** Откроется страница с рабочей областью следующего вида:

2. В поля ввода **Код семейства** и **Номер пропуска** введите номер карты. Нажмите кнопку **Ввод**.
3. На странице появится таблица с номером карты:



4. С помощью раскрывающегося списка **Право постановки на охрану** выдайте, если необходимо, право постановки данного помещения на охрану.
5. Нажмите кнопку **Сохранить** в строке с номером карты.
6. Если номер карты был ранее сохранен в контроллере, то будет доступна кнопка **Удалить**. Она позволяет удалить номер карты из памяти контроллера.

Примечание

Данную страницу можно использовать также для поиска и удаления идентификатора из памяти контроллера. Кнопка **Удалить** становится активна, если идентификатор был ранее сохранен в памяти.

Ввод идентификатора через считыватель

Для ввода номеров карт с использованием считывателя:

1. Нажмите последовательно в меню Web-интерфейса: **Карты доступа** → **Ввод номера карты через считыватель.** Откроется страница с рабочей областью следующего вида:

2. Нажмите кнопку **Старт,** строчка **Поднесите карту к считывателю** изменит цвет (потемнеет).

3. Поднесите к считывателю последовательно карты, номера которых необходимо ввести в контроллер. По окончании ввода нажмите кнопку **Стоп**.

Примечание

За один раз через считыватель можно ввести данные не более четырех карт.

4. На странице появится таблица с номерами карт, поднесенными к считывателю:

5. С помощью раскрывающегося списка **Право постановки на охрану** определите для каждой карты право постановки данного помещения на охрану.
6. Нажмите кнопки **Сохранить** в строках с номерами карт, которые необходимо сохранить в памяти контроллера.
7. Если номер карты был ранее сохранен в контроллере, доступна кнопка **Удалить**. Она позволяет удалить номер карты из памяти контроллера

Загрузка идентификатора из файла

Внимание

При загрузке в контроллер списка карт из файла автоматически из памяти контроллера стираются все ранее загруженные карты.

Создайте (например, с помощью программы *«Блокнот»*) текстовый файл следующего содержания:

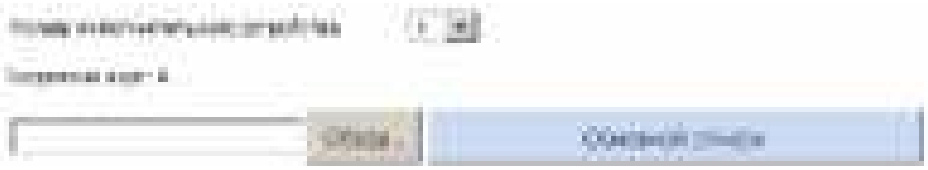
В файле должны находиться два столбца. В первом столбце – номера вводимых карт, во втором – единицы, если идентификатору выдается право постановки данного помещения на охрану, или нули, если такое право не выдается. В качестве разделителя используйте **Пробел** или клавишу **Tab**.

Примечание

При выборе сокращенного формата идентификаторов необходимо вводить в первый столбец идентификаторы карт **Одним числом**.

Для загрузки номеров карт из текстового файла:

1. Нажмите последовательно в меню Web-интерфейса: **Карты доступа** → **Загрузка карт из файла.** Откроется страница с рабочей областью следующего вида:



2. Нажмите кнопку **Обзор**. В открывшемся окне укажите расположение и название текстового файла с номерами карт и нажмите кнопку **Открыть**. Окно будет закрыто, в поле рядом с кнопкой **Обзор** будет указан путь к файлу.
3. Нажмите кнопку **Основной список**. В появившейся странице **Загрузка выполнена** нажмите кнопку **Закрыть окно**.
4. Количество загруженных в память контроллера карт изменится.

9.2.12 Список сохраненных карт

Для работы со списком сохраненных в памяти контроллера карт нажмите последовательно в меню Web-интерфейса: **Карты доступа** → **Список загруженных карт.** Откроется страница с рабочей областью следующего вида:

- Для удаления карты из памяти контроллера нажмите кнопку **Удалить** в строке с номером выбранной карты.
- Для удаления всех карт из памяти контроллера нажмите кнопку **Очистить список карт**.
- Для экспорта списка карт в текстовый файл нажмите кнопку **Сохранить весь список карт в файл**.

9.2.13 Журнал событий

Для просмотра журнала событий нажмите в меню Web-интерфейса: **События.** Откроется страница с рабочей областью следующего вида:

- Установите переключатель **Вариант отображения журнала событий** в положение **Полный** или **Краткий**.

Примечание

События, входящие в краткий и полный списки событий - см. Приложение Б

- Для просмотра журнала событий установите **Интервал просмотра событий** и нажмите кнопку **Ввод**. В таблице будут выведены зарегистрированные контроллером события в обратном хронологическом порядке.

Примечание

При установке **Интервала просмотра событий.** Если поле ввода начальной даты оставить пустым, то в таблице отобразятся события с момента начала регистрации событий до даты, указанной в поле конечной даты. Если оставить пустым поле ввода конечной даты, то с указанной начальной даты по настоящее время. Если оба поля оставить пустыми, то в таблице будут выведены все сохраненные в памяти контроллера события.

- Для удаления всех событий из памяти контроллера нажмите кнопку **Очистить журнал событий**.
- Для экспорта списка событий в текстовый файл нажмите кнопку **Сохранить журнал событий в файл**.

9.2.14 Обслуживание контроллера

Для проведения диагностики и обслуживания контроллера нажмите в меню Web-интерфейса: **Диагностика**. Откроется страница с рабочей областью следующего вида:

- Для тестирования состояния контроллера нажмите кнопку **Тестировать контроллер**. В окне подтверждения нажмите **ОК**. Время тестирования 6–10 минут.

Внимание

При тестировании контроллера журнал регистрации событий автоматически очищается.

- Для форматирования памяти контроллера нажмите кнопку **Форматировать память контроллера**. В окне подтверждения нажмите **ОК**. Время форматирования памяти около минуты.

Внимание

При форматировании памяти контроллера все сведения о конфигурации, картах доступа, временных и пространственных зонах, пароле контроллера и событиях журнала регистрации событий автоматически стираются.

- Для обновления встроенного ПО контроллера (прошивки) укажите с помощью кнопки **Обзор** место расположения файла прошивки и нажмите кнопку **Обновление встроенного ПО**.
- Для просмотра состояния контроллера нажмите в меню Web-интерфейса: **Состояние.** Откроется страница с описанием состояния контроллера.

9.3 Локальное ПО

Рассматривается настройка контроллера в следующем ПО:

- ***«Локальное ПО» PERCo-SL01*;**
- ***«Локальное ПО с верификацией» PERCo-SL02***;

Локальное ПО позволяет производить следующие действия:

- формировать список сотрудников;
- выдавать карты доступа сотрудникам с указанием ФИО сотрудников;
- управлять режимами контроля доступа через подключенное к контроллеру ИУ;
- просматривать журнал событий сотрудников и устройств;
- задавать параметры конфигурации ИУ и считывателя;
- контролировать состояние контроллера и подключенных к нему устройств;
- «Локальное ПО с верификацией», кроме этого, поддерживает работу с функциями верификации и индикации; позволяет выдавать идентификаторам права постановки и снятия с охраны; выдавать идентификаторы посетителям.

9.3.1 Подключение к контроллеру

Для подключения к контроллеру перейдите на вкладку **Конфигурация**.

1. Нажмите кнопку **Выбрать контроллер** в окне **Контроллер** рабочей области окна программы.
2. Откроется окно **Выбор контроллера**. После открытия окна автоматически начнется поиск контроллеров в сети, ход которого будет отображаться в строке состояния. В рабочей области появится список найденных контроллеров. При большом количестве подключенных контроллеров процесс поиска может занять длительное время. Если необходимый контроллер уже найден, можно остановить поиск кнопкой **Завершить поиск**.
3. Выделите строку с нужным контроллером и нажмите кнопку **Выбрать**. Окно **Выбор контроллера** закроется.

Внимание

Если искомый контроллер и компьютер с установленным «Локальным ПО» находятся в разных подсетях, то контроллер не будет найден.

При первом включении контроллера после изменения конфигурации или форматирования памяти необходимо передать в контроллер конфигурацию подключенных к нему устройств. Индикацией отсутствия настройки параметров служит синхронное мигание с частотой 2 Гц всех трех индикаторов на передней панели контроллера. ПО автоматически задает параметры подключенных устройств. Для передачи параметров в контроллер необходимо нажать кнопку **Передать конфигурацию** на вкладке **Конфигурация** в окне **Контроллер** или в главном меню программы последовательно выбрать **Редактирование** → **Передать конфигурацию.**

9.3.2 Выбор формата хранения идентификаторов

Формат хранения идентификаторов можно выбрать с помощью пункта основного меню программы **Настройки → Протокол считывателей.**

Доступны следующие форматы:

- **Сокращенный (4 байта);**
- **Wiegand-26** (Установлен по умолчанию.);
- **Универсальный (8 байт).**

9.3.3 Разрешение Web-интерфейса

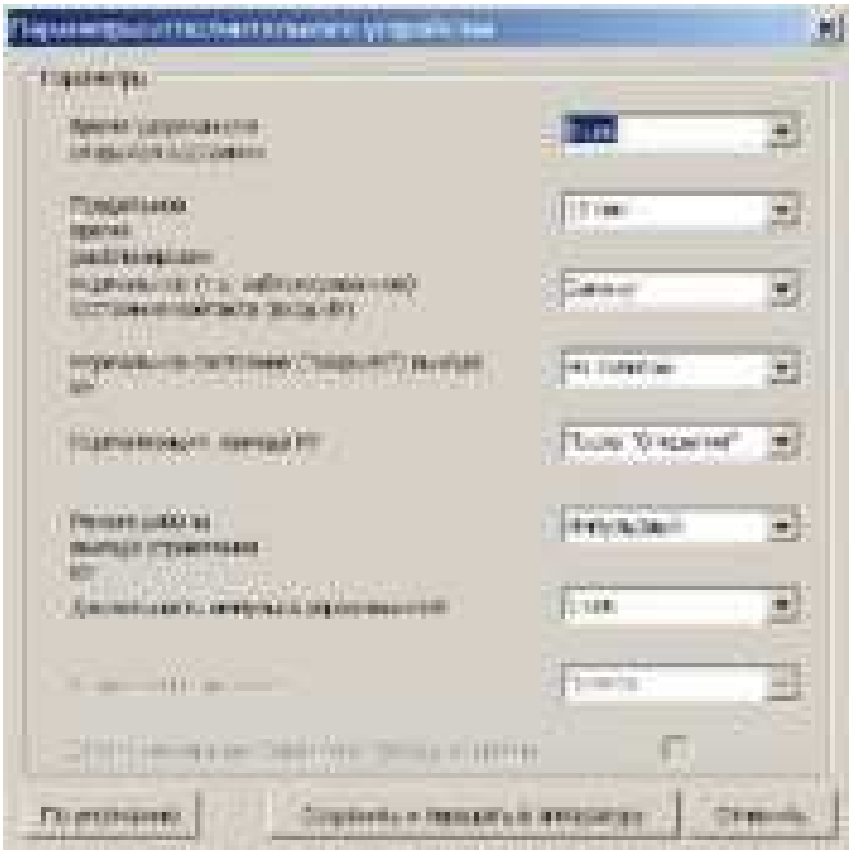
С помощью пункта основного меню **Настройки → Web-интерфейс** можно разрешить или запретить использование Web-интерфейса для контроллера.

Примечание

По умолчанию каждый раз при подключении контроллера к ПО доступ к Web-интерфейсу запрещается.

9.3.4 Параметры исполнительного устройства

Для настройки параметров исполнительного устройства нажмите кнопку **Параметры** в окне **Исполнительное устройство** рабочей области раздела **Конфигурация**. Откроется окно **Параметры исполнительного устройства**:



Область **Параметры**. Программа автоматически определяет тип исполнительного устройства и задает его параметры по умолчанию. Доступны следующие параметры:

Время удержания в открытом состоянии. Параметр устанавливает время, в течение которого ИУ после предъявления идентификатора будет разблокировано.

Предельное время разблокировки. По истечении этого времени контроллер формирует сообщение о недопустимо долгой разблокировке ИУ, при соответствующей настройке контроллера возможна генерация тревоги.

Нормальное (т.е. заблокированное) состояние контакта (вход ИУ) (*Замкнут / Разомкнут*). Этот параметр зависит от типа подключенного оборудования и указывает контроллеру на то, какое значение уровня сигнала (низкий при *Замкнут* и высокий при *Разомкнут*) на данном дополнительном входе он должен воспринимать как нормальное (т.е. при заблокированном ИУ).

Нормальное состояние («закрыто») выхода ИУ (*Не запитан / Запитан*). Параметр описывает, должен ли контроллер подавать напряжение на ИУ в состоянии *«Закрыто»*.

Нормализация выхода ИУ (*После «Открытия» / После «Закрытия»*) Параметр указывает, в какой момент контроллер должен блокировать ИУ. Факт открытия / закрытия ИУ контроллер определяет по датчику открытия / закрытия двери (геркону).

Режим работы выхода управления ИУ :

- **Потенциальный** режим. Используется для большинства ИУ, установлен по умолчанию.
- **Импульсный** режим. Рекомендуется использовать для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки «CISA»).

Длительность импульса управления ИУ. Параметр доступен при выборе импульсного режима работы выхода исполнительного устройства. Определяет длительность управляющего импульса и зависит от характеристик ИУ.

По умолчанию. Кнопка возвращает параметры, автоматически установленные программой.

Сохранить и передать в аппаратуру. Кнопка закрывает окно и передает измененные параметры в контроллер.

Отменить. Кнопка закрывает окно, не изменяя параметры.

9.4 Сетевое ПО S-20

Программное обеспечение системы *PERCO-S-20* выполнено по модульному принципу. Каждый сетевой модуль предназначен для выполнения определенных функций.

Настройка и подключение контроллера осуществляется в разделе **Конфигуратор** модуля ***«Базовое ПО» PERCo-SN01***.

9.4.1 Подключение к контроллеру

Для подключения контроллера:

1. Нажмите кнопку  в панели инструментов. Откроется панель **Поиск нового устройства**.

2. В раскрывающемся списке **Категория** выберите **Контроллеры доступа и регистрации, КБО, ППКОП**.
3. В поле ввода **IP-адрес** введите IP-адрес подключаемого контроллера.

Примечание

IP-адрес контроллера указан в паспорте и на тыльной стороне корпуса устройства.

Для подключения к контроллеру по сети *Ethernet* необходимо, чтобы компьютер находился в одной подсети с контроллером.

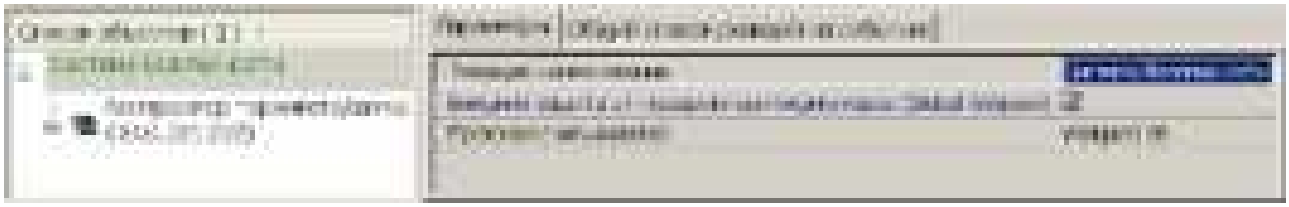
4. Нажмите Кнопку **Найти** на панели **Поиск нового устройства**. Начнется поиск устройства.
5. В случае удачного завершения контроллер появится в окне **Список объектов**.

Внимание

При первом включении контроллера после изменения конфигурации или форматирования памяти необходимо передать в контроллер конфигурацию подключенных к нему устройств. Индикацией отсутствия настройки параметров служит синхронное мигание с частотой 2 Гц всех трех индикаторов на передней панелях контроллера. ПО автоматически задает параметры подключенных устройств. Для передачи параметров в контроллер необходимо нажать кнопку в панели инструментов раздела **Конфигуратор.**

9.4.2 Параметры системы безопасности

Для настройки параметров системы безопасности в области **Список объектов** выберите корневой элемент. На вкладке **Параметры** будут доступны следующие параметры:



Поле ввода **Текущее наименование** позволяет ввести название системы безопасности.

Внешняя защита от передачи идентификаторов (Global Antipass). При установке флажка система безопасности будет контролировать последовательность прохождения (регистрации) сотрудников (посетителей) через точки прохода с учетом направления прохода. Последовательность прохождения точек прохода определяется взаимным расположением пространственных зон с учетом их вложенности. (То есть, к примеру, нельзя войти в помещение, не войдя в здание.)

Протокол считывателей. Раскрывающийся список позволяет выбрать формат хранения идентификаторов в системе. Доступны следующие форматы:

- **Сокращенный (4 байта);**
- **Wiegand 26** (установлен по умолчанию);
- **Универсальный (8 байт).**

9.4.3 Ресурсы контроллера

Для доступа к списку ресурсов контроллера нажмите на рядом с названием контроллера в области **Список объектов** раздела **Конфигуратор**. Откроется список доступных ресурсов контроллера, сгруппированных по типам:

- Считыватель;
- Замок;
- Генератор тревоги;
- Дополнительные выходы;
- Охранные зоны.

Для настройки параметров выделите в списке необходимый ресурс и перейдите на вкладку **Параметры** в правой части экрана.

В процессе работы контроллер записывает в журнал регистрации события, связанные с каждым из ресурсов. Список возможных событий каждого ресурса приведен на вкладке **События**. (Описание событий – см. Приложение Б) Существует возможность задать реакцию системы, то есть выбранного ресурса или контроллера на каждое событие.

Для задания реакций на события ресурса необходимо выбрать этот ресурс в **Списке объектов** и выделить необходимое событие на вкладке **События**. С помощью кнопок , в панели инструментов вкладки можно задавать и удалять реакции на события. С помощью кнопок и устанавливается порядок реакций.

9.4.4 Контроллер

Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название контроллера.

Разрешить Web-интерфейс. Флажок определяет, будет ли поддерживаться возможность конфигурации контроллера через Web-интерфейс.

- Флажок снят. Доступ к контроллеру через Web-интерфейс запрещен.
- Флажок установлен. Доступ к контроллеру через Web-интерфейс разрешен.

Примечание

По умолчанию при подключении к контроллеру Web-интерфейс отключен.

Доступ через Web-интерфейс будет возможен после остановки сервера системы PERCo-S-20 или удаления контроллера из списка объектов. Для остановки сервера: выйдите из «Консоли управления PERCo-S-20»; запустите «Центр управления PERCo-S-20»; перейдите на вкладку **Настройка серверов**; в области **Сервер системы PERCo-S-20** нажмите кнопку **Остановить**; индикатор справа от кнопки станет красным, сервер будет остановлен.

Коррекция времени относительно сервера. Параметр позволяет согласовать работу, если контроллер и сервер системы находятся в разных часовых поясах.

На вкладке **События** можно установить следующие реакции данного ресурса на события системы:

Установить режим работы «Открыто». При включении режима ИУ разблокируется и остается разблокированным в течение всего времени, пока режим включен. Нажатие на кнопки ДУ игнорируются. При предъявлении карт доступа к считывателю контроллера регистрируются события о проходе или нарушении доступа, при этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.

Установить режим работы «Контроль». Приводит к блокировке ИУ. При нажатии кнопки ДУ или при поднесении карты, удовлетворяющей всем критериям разрешения доступа ИУ разблокируется на время, определяемое параметром **Время удержания ИУ в разблокированном состоянии (время анализа карты).** Последующая блокировка ИУ происходит либо после прохода либо по истечении **Время удержания ИУ в разблокированном состоянии** в зависимости от параметров ИУ.

Установить режим работы «Совещание». Аналогично режиму работы «Контроль», за исключением индикации на корпусе контроллера.

Установить режим работы «Закрыто». При включении режима ИУ блокируется и остается заблокированным в течение всего времени, пока режим включен. Нажатие кнопки ДУ игнорируется. Предъявление любой карты вызывает регистрацию события о нарушении прав доступа. Проход через ИУ (открытое механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.

Открыть (разблокировать) ИУ. Приводит к разблокированию ИУ.

Закрыть (заблокировать) ИУ. Приводит к блокированию ИУ.

Поднять тревогу. Приводит к включению механизма реакции контроллера на возникновение тревожной ситуации. Параметры обработки тревожной ситуации для выбранного контроллера описываются в «*Генераторе тревоги*».

Сбросить тревогу. Приводит к прекращению выполнения контроллером механизма обработки тревожной ситуации.

Активизировать дополнительные выходы. Приводит к активизации дополнительного выхода контроллера, если для него указан **Тип** выхода, отличный от **Нет**.

Нормализовать дополнительные выходы. Приводит к нормализации дополнительного выхода контроллера, если для него указан **Тип** выхода, отличный от **Нет**.

Сбросить зональность идентификаторов. После получения данной команды контроллер будет игнорировать нарушение зональности при первом предъявлении для каждого из зарегистрированных в контроллере идентификаторов.

9.4.5 Считыватель

Ресурс позволяет настроить с помощью ПО параметры функции верификации, контроля времени, защиты от передачи идентификаторов (Antipass):

Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название считывателя.

Запрещение ДУ. При установке флажка для выбранного режима блокируется возможность управления ИУ с помощью кнопки ДУ.

Подтверждение от ДУ (Верификация). При помощи этого параметра можно указать, будет ли в выбранных режимах доступа при поднесении идентификатора к данному считывателю формироваться запрос на подтверждение от ДУ.

- **Нет.** Подтверждение не требуется.
- **Да.** Имеется возможность гибко настроить условия верификации идентификаторов отдельно для сотрудников и посетителей в следующих случаях:
  - **при проходе** – верификация будет осуществляться при попытке прохода без каких-либо нарушений
  - **при проходе с НАРУШЕНИЕМ ВРЕМЕНИ** – верификация будет осуществляться при попытке прохода с нарушением времени (параметр **Контроль времени** должен быть установлен на значение **Жесткий**).
  - **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ** – верификация будет осуществляться при попытке повторного прохода без предварительного прохода в обратную сторону (параметр **Защита от передачи идентификаторов** должен быть установлен на значение **Жесткая**).

Время ожидания подтверждения при верификации. Параметр позволяет установить время, в течение которого контроллер будет ожидать подтверждение от верифицирующего устройства. В качестве верифицирующего устройства может быть использована кнопка ДУ контроллера или ПО PERCo-S-20.

Защита от передачи идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ (Antipass). Параметр позволяет для выбранных режимов определить реакцию контроллера в случае попытки повторного прохода сотрудника/посетителя без предварительного прохода в обратную сторону. Для каждого из указанных режимов работы контроллера можно выбрать один из вариантов защиты:

- **Нет.** Контроллер не осуществляет проверку факта повторного прохода по идентификатору, предъявленному к выбранному считывателю.
- **Мягкая.** Контроллер разрешит повторный проход по идентификатору, предъявленному к считывателю, и при этом в журнале мониторинга записывается факт предъявления карты с нарушением местоположения, а после прохода в журнал регистрации записывается событие о проходе с нарушением зональности.
- **Жесткая.** Контроллер либо запретит попытку повторного прохода при предъявлении идентификатора к считывателю и при этом в журнал мониторинга записывается факт предъявления карты с нарушением местоположения, а в журнал регистрации записывается событие о запрете прохода по причине нарушения зональности, либо будет запущена процедура верификации.

Контроль времени для идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ. Параметр позволяет для выбранных режимов определить реакцию контроллера на предъявление карты сотрудника/посетителя с учетом временного критерия. Для каждого из указанных режимов работы контроллера можно выбрать один из видов контроля:

- **Нет.** Контроллер не учитывает временные параметры доступа карты для разрешения прохода.
- **Мягкий.** Контроллер разрешит доступ по предъявленной карте, но проведет сравнение текущего времени и даты с временными параметрами доступа предъявленной карты. В случае их нарушения в журнал мониторинга

записывается факт предъявления карты с нарушением местоположения, а после прохода в журнал регистрации записывается событие о проходе с нарушением времени.

- **Жесткий.** При выборе этого параметра контроллер проведет сравнение текущего времени и даты с временными параметрами доступа предъявленной карты. В случае их совпадения (то есть владелец карты не нарушает режим доступа) контроллер разрешит проход через ИУ. В случае их нарушения контроллер либо запретит проход и запишет в журнал мониторинга факт предъявления карты с нарушением местоположения, а в журнал регистрации событие о запрете прохода в связи с нарушением времени, либо будет запущена процедура верификации.

Дополнительные выходы, активизируемые при разблокировке ИУ. Параметр позволяет указать, что выход контроллера должен быть активизирован при разблокировке ИУ. Для выбора установите флажок у дополнительного выхода. Укажите временной критерий активизации.

Дополнительные выходы, нормализируемые при разблокировке ИУ. Параметр позволяет указать, что выход контроллера должен быть нормализован при разблокировке ИУ. Для выбора установите флажок у дополнительного выхода. Укажите временной критерий нормализации.

Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ. Параметр позволяет указать что выход будет активизирован на указанное время в случае предъявления незаблокированного и с не истекшим сроком действия идентификатора сотрудника/посетителя. Этот параметр может быть использован в случае, если к дополнительному выходу подключена индикация, информирующая работников охраны о статусе предъявленной карты. Для выбора установите флажок у дополнительного выхода. Укажите временной критерий активизации.

Временной **Критерий активизации/нормализации**:

- **На указанное время.** Дополнительный выход будет активизирован / нормализирован на указанное время, начиная с момента предъявления идентификатора, независимо от того, будет или нет разрешен проход.
- **На время срабатывания.** Дополнительный выход будет активизирован / нормализирован на указанное время, начиная с момента разблокирования ИУ и до момента его блокирования, либо, если проход не был совершен, то до истечения времени анализа идентификатора.
- **На время срабатывания и после срабатывания.** Выбор этого параметра является комбинацией двух предыдущих. Дополнительный выход будет активизирован / нормализирован на указанное время, начиная с момента разблокирования ИУ и до момента его блокирования, плюс указанное вами время, либо, если проход не был совершен, до истечения времени анализа идентификатора.

Изымать в СТОП-ЛИСТ идентификаторы ПОСЕТИТЕЛЕЙ после прохода. При установке флажка идентификаторы посетителей после совершения прохода будут помещаться в список идентификаторов, запрещенных к проходу.

На вкладке **События** можно установить следующие реакции данного ресурса на события системы:

- **Установить режим работы «Открыто».** Приводит к установке для ИУ режима *«Открыто»*.

- **Установить режим работы «Контроль».** Приводит к установке для ИУ режима *«Контроль»*.
- **Установить режим работы «Совещание».** Приводит к установке для ИУ режима *«Совещание»*.
- **Установить режим работы «Закрыто».** Приводит к установке для ИУ режима *«Закрыто»*.
- **Открыть (разблокировать) ИУ.** Приводит к разблокировке ИУ на время, установленное параметром **Время удержания в разблокированном состоянии**.
- **Закрыть (заблокировать) ИУ.** Приводит к блокировке ИУ.

9.4.6 Замок

Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название ИУ.

Нормальное (т.е. заблокированное) состояние контакта (вход ИУ) (*Нормально разомкнут / Нормально замкнут*). Состояние датчика двери / выхода PASS турникета при заблокированном состоянии данного ИУ.

Нормальное состояние «Закрыто» выхода ИУ (*Не запитан / Запитан*) (Не доступен в конфигурациях 6, 7 «Контроллер АТП»). Параметр описывает, активизировано ли реле управления ИУ в состоянии *«Закрыто»*.

Нормализация выхода ИУ (*После «Открытия» / После «Закрытия»*). В какой момент нормализуется состояние выхода управления исполнительным устройством.

Режим работы выхода управления ИУ (*Потенциальный / Импульсный*). (Доступен только в конфигурациях 1-3 «Контроллер управления дверьми») Описывает логику управления подключенным исполнительным устройством. Импульсный режим управления применяется только для замков, поддерживающих этот режим. Рекомендуется использовать для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки «CISA»).

Время управляющего импульса. Параметр доступен при выборе импульсного режима работы выхода исполнительного устройства. Определяет время управляющего импульса.

Предельное время разблокировки. Параметр позволяет указать время, по истечении которого контроллер сформирует сообщение *«ИУ не закрыто после прохода по идентификатору»* по причине того, что ИУ не заблокировано.

Время удержания в разблокированном состоянии (время анализа идентификатора). Время, на которое открывается ИУ, а также время, в течение которого необходимо повторно предъявить карту, имеющую право постановки на охрану, для постановки ИУ на охрану.

Время ожидания комиссионирования. Параметр позволяет ограничить интервал времени между предъявлением карт пользователя (сотрудника/ посетителя) и комиссионирующей карты (сотрудника), в случае если в правах карты пользователя установлен доступ с комиссионированием.

Регистрация прохода по предъявлению идентификатора При установке флажка контроллер будет считать проход совершившимся сразу после поднесения идентификатора, независимо от того, будет ли реально совершен проход через ИУ.

Внутренняя защита от передачи идентификаторов (Local Antipass). При установке флажка контроллер будет отслеживать случаи повторного предъявления идентификатора.

9.4.7 Генератор тревоги

Ресурс связан с контроллером ИУ и позволяет установить с помощью параметров события, приводящие к переходу системы в состояние *«Тревога СКУД»*. Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название генератора тревоги.

Генерация тревоги при предъявлении идентификатора. Параметр позволяет указать события, при которых контроллер переходит в состояние *«Тревога»* при предъявлении идентификатора.

Типы тревоги:

- **Нет.** Контроллер не переходит в состояние *«Тревога»* при выбранном событии.

- **Тихая.** Контроллер переходит в состояние *«Тревога»,* но при этом выходы, **Тип** которых выбран, как **Генератор тревоги** (см. п. 9.4.8)**,** не активизируются.
- **Громкая.** Контроллер переходит в состояние *«Тревога».*

Генерация тревоги при несанкционированной разблокировке ИУ. Параметр позволяет для выбранных режимов доступа указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние *«Тревога»* в случае механической разблокировки ИУ при помощи ключа, то есть без команды от контроллера.

Генерация тревоги по недопустимо долгому открытию ИУ. Параметр позволяет для выбранных режимов доступа указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние *«Тревога»* в случае, если после открытия ИУ не было нормализировано в течение **Предельного времени разблокировки**, заданного в параметрах этого ИУ.

9.4.8 Дополнительный выход

Дополнительные выходы могут быть использованы для управления любым дополнительным оборудованием в рамках системы *PERCo-S-20*.

Для настройки ресурса доступны следующие параметры:

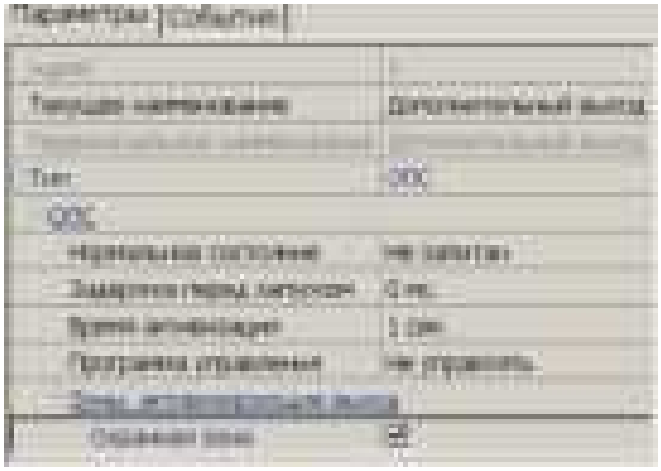
Текущее наименование. Поле ввода позволяет ввести описательное название выхода.

Тип. Раскрывающийся список позволяет выбрать следующие типы выхода:

- **Нет.** К данному выходу не подключено никакое внешнее оборудование.
- **Обычный.** К выходу подключено дополнительное оборудование, логика управления которым описывается через описание других устройств системы (за исключением генератора тревоги).

- **Генератор тревоги.** Решение об активизации дополнительного выхода принимается в соответствии с параметрами, указанными в генераторе тревоги. Этот дополнительный выход будет использоваться для индикации перехода в состояние *«Тревога».*

- **ОПС.** Выход предназначен для управления световым оповещением, звуковым оповещением, а также для передачи тревожных извещений на пульт центрального наблюдения при изменении режимов и состояний охранной зоны. Программа управления задает логику работы контроллера по управлению этим дополнительным выходом. Инициатором активизации выхода являются изменения режимов и состояний охранных зон, отмеченных как **Зоны, активизирующие выход**. После возникновения события, инициирующего активизацию выхода (в соответствии с заданной программой), начинается отсчет задержки, указанной в параметре **Задержка перед запуском**, после чего выход активизируется. В зависимости от параметра **Программа управления** выход может быть запитан (не запитан) постоянно (пока ресурс панели находится в текущем режиме), либо изменять свое физическое состояние (мигать) из нормализированного на противоположное. Нормализация выхода происходит либо по истечению времени, указанному в параметре **Время активизации** (если оно не бесконечное), либо по сбросу панели, либо после выключения ее питания.



Нормальное состояние (*Не запитан / Запитан*). Параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий.

Задержка перед запуском. Промежуток времени между изменением состояния ОЗ и запуском программы управления выходом.

Время активизации. Время, в течение которого при наличии активизирующего управляющего воздействия выход меняет свое состояние из нормализированного на противоположное. Как правило, в этом случае к такому дополнительному выходу подключают тревожный оповещатель (сирена, проблесковая лампа).

Программа управления. Режим работы выхода после активизации. Доступны следующие программы (описание программ – см Приложение А):

1. **Не управлять.**
2. **Включить при тревоге.** В случае перехода одной из зон в режим *«Тревога»* произойдет замыкание контакта дополнительного выхода.
3. **Мигать при тревоге.** В случае перехода одной из зон в режим *«Тревога»* произойдет попеременное замыкание/размыкание контактов дополнительного выхода.
4. **Лампа 1.** Программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы **все зоны** изменили свой режим.
5. **Лампа 2.** Программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для

активизации программы требуется, чтобы **хотя бы одна из зон** изменила свой режим.

6. **ПЦН 1.** Программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы **все зоны** изменили свой режим.
7. **ПЦН 2.** Программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы **хотя бы одна из зон** изменила свой режим.
8. **Сирена.** Программа управления, указывающая на то, что к дополнительному выходу подключен звуковой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы **хотя бы одна из зон** изменила свой режим.
9. **Включить перед взятием.** Перед переходом одной из зон в режим *«Взятие»* произойдет замыкание контакта дополнительного выхода.
10. **Включить при взятии.** При переходе одной из зон в режим *«Взятие»* произойдет замыкание контакта дополнительного выхода.
11. **Включить при снятии.** Перед переходом одной из зон в режим *«Снята»* произойдет замыкание контакта дополнительного выхода.
12. **Включить при автоперевзятии.** При переходе одной из охранных зон в режим *«Автоперевзятие»* произойдет замыкание контакта дополнительного выхода.

Зоны, активизирующие выход. Параметр позволяет выбрать охранные зоны, нарушение которых приведет к активизации выхода.

Примечание

После включения питания все выходы нормализуются.

На вкладке **События** можно установить следующие реакции данного ресурса на события системы:

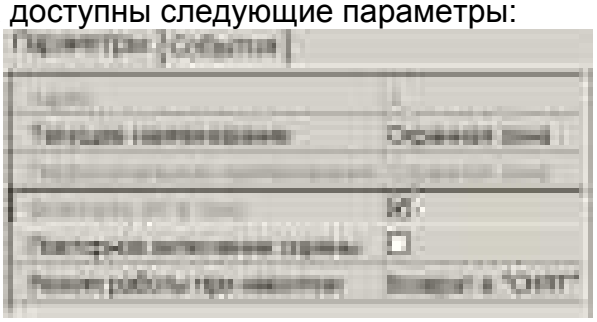
Активизировать. Приводит к переводу выбранного релейного выхода в активное состояние на время, установленное параметром **Время активизации** для данного выхода.

Нормализовать. Приводит к переводу выбранного релейного выхода в нормальное (исходное) состояние.

9.4.9 Охранная зона

Охранная зона – это логическая структура, которая позволяет создать комбинации ресурсов контроллера, которые одновременно будут ставиться на охрану.

Для настройки ресурса доступны следующие параметры:



Текущее наименование. Поле ввода позволяет ввести описательное название охранной зоны.

Включить ИУ в зону. В ОЗ контроллера входит только ИУ, поэтому изменение этого параметра недоступно.

Повторное включение сирены. При установке флажка активизация дополнительного выхода, управляемого по программе *«Сирена»,* происходит при каждом нарушении зоны, даже если она уже находится в режиме «Тревога».

Режим работы при невзятии. Для параметра доступно значение **Возврат в «Снята»**. При невозможности взятия ОЗ на охрану зона перейдет в режим *«Снята».*

На вкладке **События** можно установить следующие реакции данного ресурса на события системы:

Поставить на охрану/контроль. Приводит к постановке ОЗ на охрану. ИУ блокируется и остается заблокированным в течение всего времени, пока режим включен. Нажатие кнопки ДУ игнорируется. Открывание двери в режиме постановки на охрану вызывает регистрацию события о несанкционированном проходе (взломе) через ИУ и, при задании соответствующих опций, включение сигнала тревоги. Если по истечении времени выдачи сигнала тревоги дверь будет закрыта (вход *Door* нормализуется), сигнал тревоги выключается. Иначе выдача сигнала тревоги продолжается до закрытия двери.

Снять с охраны/контроля. Происходит снятие охранной зоны с охраны.

Сбросить тревогу. Приводит к сбросу тревоги и прекращению выполнения алгоритма обработки тревожной ситуации.

9.5 Функциональные возможности

9.5.1 Функция Global Antipass

Функция Global Antipass доступна при использовании программного модуля: ***«Базовое ПО» PERCo-S-20***.

Global Antipass (функция глобального контроля зональности) – Функция системы безопасности, заключающаяся в контроле нарушений последовательности прохождения (регистрации) сотрудников через точки прохода, с учетом направления прохода. Последовательность прохождения точек прохода определяется взаимным расположением пространственных зон с учетом их вложенности (то есть нельзя войти в помещение, не войдя в здание).

Для реализации этой функции информация о каждом проходе по данной карте передается другим контроллерам сети с помощью широковещательной рассылки. В результате каждый контроллер системы безопасности, подключенный к сети, имеет информацию о том, в какой пространственной зоне должен находиться владелец предъявленной карты.

Внимание

Для работы функции **Внешняя защита от передачи идентификаторов (Global Antipass)** необходимо указать расположение контроллера на схеме помещений в разделе ПО **Помещения и мнемосхема**.

Для включения функции глобального контроля зональности (Global Antipass) произведите следующие действия:

1. Включите функцию локальной зональности (Antipass).
2. Для включения функции контроля зональности в разделе **Конфигуратор** на вкладке **Параметры** необходимо:
   2.1. Для ресурсов контроллера **Считыватель** в параметрах **Защита от передачи идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ (Antipass)** для различных режимов работы контроллера с помощью раскрывающихся списков указать один из способов защиты, отличный от **Нет**.
   2.2. Для ресурса контроллера **ИУ** установить флажок **Внутренняя защита от передачи идентификаторов (Local Antipass**);
3. В параметрах доступа карт необходимо установить подверженность контролю локальной зональности, поставив флажок у параметра **Защита от передачи карт (Antipass)**. По умолчанию все идентификаторы, зарегистрированные в ПО, подвержены контролю локальной зональности.
4. Установите флажок **Внешняя защита от передачи идентификаторов (Global Antipass)** в разделе ПО **Конфигуратор** на вкладке **Параметры** системы безопасности.

9.5.2 Контроль по времени

Задание критерия контроля прохода по времени доступно при использовании расширенной версии ПО. Должны быть установлены программные модули ***PERCo-SM03 «Бюро пропусков»*** и ***PERCo-SM04 «Управление доступом»*.**

Контроллер может осуществлять управление доступом с учетом текущего времени (дня недели), то есть запретить проход через ИУ, разрешить, либо разрешить с предупреждением в зависимости от настроек системы.

Временная зона – это совокупность временных интервалов (до 4-х) в пределах календарных суток, в течение которых пользователю разрешен доступ в соответствии с выданными правами доступа. Временные интервалы представляют собой отрезки времени с точностью до минуты.

Для задания критериев контроля по времени в разделе ПО **Временные зоны** создайте временную зону контроля и укажите временные интервалы, в течение которых сотруднику/посетителю будет разрешен доступ.

Если необходимо, то в соответствующих разделах ПО на основе установленных временных зон создайте **Недельные графики**, **Скользящие посуточные графики**, **Скользящие понедельные графики** контроля для различных категорий сотрудников.

Для включения функции контроля по времени в разделе **Конфигуратор**, на вкладке **Параметры** необходимо для ресурсов контроллера **Считыватель** в параметрах **Контроль времени для идентификаторов СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ** для различных режимов работы контроллера с помощью раскрывающихся списков указать один из способов защиты:

- **Мягкий.** Контроллер разрешит доступ по предъявленной карте, но проведет сравнение текущего времени и даты с временными параметрами доступа предъявленной карты. В случае их нарушения в журнал мониторинга записывается факт предъявления карты с нарушением местоположения, а после прохода в журнал регистрации записывается событие о проходе с нарушением времени.

- **Жесткий.** При выборе этого параметра контроллер проведет сравнение текущего времени и даты с временными параметрами доступа предъявленной карты. В случае их совпадения (владелец карты не нарушает режим доступа) контроллер разрешит проход через ИУ. В случае их нарушения контроллер запретит проход и запишет в журнал мониторинга факт предъявления карты с нарушением местоположения, а в журнал регистрации – событие о запрете прохода в связи с нарушением времени.

В параметрах доступа карт необходимо включить подверженность карты контролю по времени, указав какой-либо критерий контроля по времени.

Примечание

Для отключения контроля по времени используйте временную зону *«Никогда»*.

9.5.3 Комиссионирование

Процедура комиссионирования доступна при использовании программного модуля: ***«Базовое ПО» PERCo-S-20***.

Комиссионирование. Процедура подтверждения прав предъявленной карты посредством предъявления второй, комиссионирующей карты.

Комиссионирующей картой может служить любая карта, выданная сотруднику и внесенная в **Список карт сотрудников, имеющих право на комиссионирование (досмотр)**.

Для внесения карты в список имеющих право комиссионирования необходимо в разделе **Конфигуратор** в области **Список объектов** выбрать ресурс контроллера **Контроллер ИУ** и нажать правую кнопку мыши. В открывшемся контекстном меню выбрать пункт **Показать дополнительную информацию**. Откроется панель **Список карт сотрудников, имеющих право на комиссионирование (досмотр)**. С помощью кнопок  и  можно добавить и удалить идентификатор сотрудника из списка комиссионирующих карт. Есть возможность добавить до 192 комиссионирующих карт.

В параметрах доступа карт требуется указать необходимость подтверждения прав данной карты с помощью комиссионирования (комиссионирующей карты). Для этого в раскрывающемся списке **Тип права** выберите пункт **…с комиссионированием**, например **Доступ с комиссионированием**.

9.5.4 Верификация и индикация

Процедуры верификации и индикации доступны при использовании программных модулей: ***PERCo-SM09 «Видеоидентификация»***, ***PERCo-SM10 «Прием посетителей»***, ***PERCo-SM13 «Центральный пост»***, а также, в ***PERCo-SL02 «Локальное ПО с верификацией»***.

Верификация – процедура подтверждения прав предъявленной карты оператором с помощью комиссионирующего устройства (пульта ДУ, кнопки ДУ, команды ПО) на основе сравнения изображения, получаемого с видеокамер, и данных (в том числе графических), хранящихся в базе данных программы и выводимых при предъявлении идентификатора.

Примечание

В случае, если одновременно установлены функции комиссионирования и верификации, первой выполняется процедура комиссионирования, а затем верификации.

Для включения функции верификации в разделе **Конфигуратор** на вкладке **Параметры** необходимо для ресурсов контроллера **Считыватель** в параметрах **Подтверждение от ДУ** для необходимых режимов работы контроллера с помощью раскрывающихся списков выбрать значение **Да** и указать отдельно для сотрудников и посетителей в каких случаях требуется верификация:

- **При проходе**. Верификация будет осуществляться при попытке прохода без каких-либо нарушений
- **При проходе с НАРУШЕНИЕМ ВРЕМЕНИ.** Верификация будет осуществляться при попытке прохода с нарушением времени (параметр **Контроль времени** должен быть установлен на значение **Жесткий**.)
- **При проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ.** Верификация будет осуществляться при попытке прохода с нарушением зональности (параметр **Защита от передачи идентификаторов** должен быть установлен на значение **Жесткая**.)

В параметрах доступа карт необходимо установить подверженность карты верификации, поставив флажок у параметра **Подверженность верификации**.

Индикация – это процедура, при которой в режиме реального времени оператору предоставляется информация о событиях системы, связанных с предъявлением идентификаторов, соответствующие этим событиями кадры с видеокамер и информация из базы данных программы о предъявленных идентификаторах.

9.5.5 Назначение прав доступа карты

Назначение прав доступа карты доступно при использовании расширенной версии ПО. Должен быть установлен программный модуль ***PERCo-SM03 «Бюро пропусков»***.

При выдаче карт сотрудникам (посетителям) в разделе **Доступ сотрудников (посетителей)** необходимо задать для каждого контроллера, входящего в систему безопасности права доступа выдаваемой карте.

Примечание

Для выдачи карт необходимо указать расположение контроллера в разделе **Помещения и мнемосхема**.

Окно настройки параметров доступа карты:

Защита от передачи карт (Antipass). При установке флажка контроллер будет отслеживать нарушения локальной зональности.

Временной критерий. С помощью раскрывающегося списка можно выбрать один из временных критериев доступа:

- **Временные зоны**
- **Недельные графики**
- **Скользящие посуточные графики**
- **Скользящие понедельные графики**

Тип права. С помощью раскрывающегося списка можно выбрать один из вариантов задания прав доступа по карте:

Для сотрудников:

- **Только доступ**
- **Доступ с постановкой на охрану**
- **Доступ со снятием с охраны**
- **Доступ с постановкой на охрану и снятием с охраны**
- **Доступ с комиссионированием**
- **Доступ и постановка на охрану с комиссионированием**
- **Доступ и снятие с охраны с комиссионированием**
- **Доступ и постановка/снятие на/с охран(у,ы) с комиссионированием**
- **Доступ с комиссионированием и снятие с охраны с комиссионированием**
- **Доступ с комиссионированием и постановка/снятие на/с охран(у,ы) с комиссионированием**

Для посетителей:

- **Только доступ**
- **Доступ с комиссионированием**

Подверженность верификации. При установке флажка контроллер будет ожидать для данной карты подтверждение от верифицирующего устройства.

10 ОБНОВЛЕНИЕ ВСТРОЕННОГО ПО

Для обновления встроенного ПО и форматирования памяти контроллеров системы *PERCo-S-20* используется программа *«Прошиватель»,* входящая вместе с файлами прошивок в состав *«Программного обеспечения для смены прошивок в контроллерах системы S-20»*. Актуальную версию программы можно скачать на сайте www.perco.ru в разделе **Поддержка → Программное обеспечение.**

11 ЭКСПЛУАТАЦИЯ

После проведения конфигурации контроллер может работать в следующих режимах:

Без подключения к серверу системы безопасности PERCo-S-20.

Если подключение к сети *Ethernet* и ПК также недоступно, контроллер выполняет следующие функции:

- Принимает от считывателей идентификаторы предъявленных карт и в зависимости от наличия их в списке, хранящемся в памяти контроллера, разрешает или запрещает доступ.
- Управляет подключенными ИУ.
- Ставит и снимает ОЗ с охраны; контролирует ШС и ИУ в режиме *«Охрана»*; активизирует дополнительные выходы в режиме *«Тревога»*.

- Фиксирует события в журнале регистрации событий в памяти контроллера.
- Поддерживает функции контроля прохода по времени и комиссионирования.

При подключении к сети и обеспечении связи с другими контроллерами системы становится доступной функция глобального контроля зональности.

При подключении к ПК с установленным ***«Локальным ПО»***:

- Данные из журнала событий автоматически переносятся в базу данных программы каждый раз при запуске программы. Также данные можно перенести по нажатию в программе соответствующей кнопки.
- Данные владельцев (ФИО) идентификаторов хранятся в базе данных программы.
- Функция верификации доступна при установке *«Локального ПО с верификацией»*.

При подключении к серверу системы PERCo-S-20.

Кроме функций, поддерживаемых при автономной работе, становятся доступными также следующие:

- Данные из журнала событий автоматически переносятся в базу данных на сервере системы безопасности.
- Функция верификации доступна в зависимости от установленных модулей сетевого ПО.

11.1 Режимы работы как элемента СКУД

Изменение режимов работы контроллера как элемента системы безопасности возможно только из ПО, за исключением постановки/снятия с охраны, которое возможно двойным поднесением карты доступа к считывателю. Контроллер, как элемент СКУД, обеспечивает следующие режимы работы ИУ:

Режим работы *«Открыто»*

- ИУ разблокируется и остается разблокированным в течение всего времени, пока режим включен.
- Нажатие кнопки ДУ игнорируется.
- Горит зеленый световой индикатор.

Режим работы *«Контроль»*

- ИУ блокируется.
- При предъявлении к считывателю карты, удовлетворяющей всем критериям разрешения доступа, ИУ разблокируется на **Время удержания в разблокированном состоянии**.
- Горит желтый индикатор.

Режим работы *«Закрыто»*

- ИУ блокируется и остается заблокированным в течение всего времени, пока режим включен.
- Нажатие кнопки ДУ игнорируется.
- При предъявлении любой карты регистрируется событие о нарушении прав доступа.
- Горит красный индикатор.
- Проход через ИУ (взлом ИУ) может переводить систему в состояние «*Тревога»,* при соответствующих настройках системы.

Режим работы *«Совещание»*

- ИУ блокируется.
- При предъявлении карты, удовлетворяющей всем критериям разрешения доступа, к считывателю (при нажатии на кнопку ДУ) ИУ разблокируется на **Время удержания в разблокированном состоянии**.
- Горят желтый и зеленый индикаторы.

Примечание

Данный режим не поддерживается в Web-интерфейсе, однако он может быть установлен по команде от ПО.

Режим работы *«Охрана»*

- ИУ блокируется и остается заблокированным в течение всего времени, пока режим включен.
- Нажатие кнопки ДУ игнорируется.
- При предъявлении карты, не имеющей права снятия с охраны, регистрируется событие о нарушении прав доступа.
- Установлена на охрану ОЗ, включающая ИУ.
- Проход через ИУ (взлом ИУ) переводит систему в состояние «*Тревога»,* при соответствующей настройки через ПО.
- Мигают желтый и красный индикаторы.

11.2 Режим «Открыто»

Переход в режим работы *«Открыто»* возможен:

- По команде от Web-интерфейса из любого режима работы.
- По карте, имеющей право снятия с охраны, если режим предшествовал режиму работы *«Охрана»*.

Выход из режима работы *«Открыто»* возможен:

- По команде от Web-интерфейса в любой режим работы.
- По карте, имеющей право постановки на охрану в режим работы «Охрана».

Таблица 3 Реакция контроллера на предъявление идентификатора в режиме «Открыто»

Дверь открыта (вход Door – активизирован)	**Дверь закрыта, ИУ разблокировано (вход Door – нормализован)**
Предъявление карты, имеющей право прохода	
Регистрируется событие *«Проход по карте*	Регистрируется событие *«Проход по карте»* если дверь была открыта в течение **Времени удержания в разблокированном состоянии** после предъявления.
	Регистрируется событие *«Отказ от прохода»,* если в течение **Времени удержания в разблокированном состоянии** проход не произошел.
Предъявление карты, не имеющей права прохода	
Регистрируется событие *«Запрет прохода» («Идентификатор не зарегистрирован», «Карта запрещена»* и т.п.).	

11.3 Режим «Контроль»

Переход в режим работы «Контроль» возможен:

- По команде от ПО из любого режима работы.
- По команде от Web-интерфейса из любого режима работы.

Выход из режима работы «Контроль» возможен:

- По команде от ПО в любой режима работы.
- По команде от Web-интерфейса в любой режим работы.

Таблица 4 Реакция контроллера на предъявление идентификатора в режиме «Контроль»

Дверь открыта (вход Door – активизирован)	**Дверь закрыта ИУ заблокировано (вход Door – нормализован)**
Предъявление карты, имеющей право прохода или нажатие кнопки ДУ	
Перезапускается отсчет **Времени удержания в разблокированном состоянии**.	ИУ разблокируется на **Время удержания в разблокированном состоянии**.
Регистрируется событие *«Проход по карте».*	Регистрируется событие *«Проход по карте»,* если дверь была открыта в течение **Времени удержания в разблокированном состоянии** после предъявления карты.
	Регистрируется событие *«Отказ от прохода»,* если в течение **Времени удержания в разблокированном состоянии** проход не произошел. ИУ блокируется.
ИУ блокируется после нормализации датчика двери.	
Предъявление карты, не имеющей права прохода	
Регистрируется событие *«Запрет прохода» («Идентификатор не зарегистрирован», «Карта запрещена»* и т.п.).	ИУ остается в заблокированном состоянии. Регистрируется событие *«Запрет прохода» («Идентификатор не зарегистрирован», «Карта запрещена»* и т.п.).

Примечание

Если ИУ нормализовано, но ранее поступила команда на открытие (выход управления активирован), то контроллер игнорирует поднесение любой разрешенной карты.

В таблице 5 рассматриваются случаи поднесения карты в течение **Времени удержания в разблокированном состоянии** после поднесения карты, имеющей право на проход.

Таблица 5 Реакция контроллера на повторное предъявление идентификатора в режиме «Контроль»

Предъявление карты, имеющей право прохода
Контроллер игнорирует предъявление данной карты
Предъявление карты, не имеющей права прохода
Регистрируется событие о предъявлении карты с нарушениями каких-либо критериев доступа.

11.3.1 Процедура верификации

При поднесении к считывателю карты, не имеющей нарушений, в правах которой установлена подверженность верификации, контроллер переходит в режим *«Ожидание верификации».* Контроллер игнорирует нажатие кнопки ДУ и предъявление любой карты.

При подтверждении прав карты оператор нажимает кнопку **Разрешить** верифицирующего устройства:

- ИУ разблокируется (открывается).
- Индикация на считывателе: режим *«Открыто»*.
- Регистрируется событие *«Проход с подтверждением от верификации (с возможными причинами)»*

При запрете прав карты оператор нажимает кнопку **Запретить** верифицирующего устройства:

- Индикация на считывателе: режим *«Контроль»*.
- Регистрируется событие *«Запрет прохода (отказ в подтверждении от верификации)»*

11.3.2 Процедура комиссионирования

При поднесении к считывателю карты, не имеющей нарушений, в правах которой установлен **Тип права** *«с комиссионированием»*, контроллер переходит в режим *«Ожидание комиссионирования».* Время ожидания комиссионирования определяется параметром ИУ **Время ожидания комиссионирования**. По истечении этого времени если не была предъявлена комиссионирующая карта контроллер возвращается в предыдущий режим и регистрируется событие *«Нарушение комиссионирования»*.

Таблица 6 Реакция контроллера на предъявление идентификаторов в режиме «Ожидание комиссионирования»

Предъявление комиссионирующей карты
ИУ разблокируется. Режим *«Ожидание комиссионирования»* снимается. Регистрируется событие *«Проход по идентификатору (с возможными причинами)»*. По факту прохода добавляется событие *«Была предъявлена комиссионирующая карта №…»*.
Предъявление любой некомиссионирующей карты
Регистрируется событие *«Предъявление карты №…, нарушение комиссионирования»*. Режим *«Ожидание комиссионирования»* снимается. Регистрируется событие *«Запрет прохода №…, нарушение комиссионирования»*.

11.4 Режим «Охрана»

В режиме *«Охрана»* контроллер отслеживает состояние охранных зон. В ОЗ входит ИУ. ОЗ может находиться в следующих состояниях: *«Снята»*, *«Взятие»*, *«Охрана»*, *«Тревога»*. Права постановки и снятия с охраны выдаются картам в ПО или через Web-интерфейс.

Таблица 7 Реакция контроллера на предъявление идентификаторов в режиме «Охрана»

Дверь закрыта ИУ заблокировано (вход Door – нормализован)
Предъявление карты, не имеющей прав снятия с охраны
Регистрируется событие *«Запрет прохода – нарушение режима контроля доступа»* (*«Запрет прохода, нарушение РЕЖИМОВ РАБОТЫ»*) Регистрируется событие *«Запрет прохода»* (*«Идентификатор не зарегистрирован»*, *«Карта запрещена»* и т.п.).
Предъявление карты, имеющей право снятия с охраны
Регистрируется событие *«ОЗ снята с охраны»* с указанием источника команды. ИУ переходит в режим работы, который предшествовал установке режима *«Охрана»,* если это был режим *«Закрыто»*, то в режим работы *«Контроль».*
Механическое открытие ИУ
Регистрируется событие *«Несанкционированный проход (взлом)»* (*«Несанкционированное открытие (взлом) ИУ»*)

11.4.1 Постановка ОЗ на охрану

Постановка ОЗ на охрану возможна следующими способами:

- По карте, имеющей право постановки на охрану, из любого режима работы кроме *«Закрыто»*.
- По команде от ПО из любого режима работы.
- По команде от Web-интерфейса может быть взято на охрану направление прохода через ИУ, связанное с выбранным считывателем.

Примечание

При постановке на охрану ОЗ контроллер переходит в режим *«Охрана»*, если ИУ входит в ОЗ и остается в текущем режиме, если ИУ не входит ОЗ.

Для постановки на охрану с помощью карты, обладающей правом постановки на охрану, следует дважды предъявить ее считывателю, не совершая при этом прохода (В случае использования функции комиссионирования и/или верификации дополнительно требуется поднесение комиссионирующей карты и/или подтверждение прав от оператора.):

- После однократного поднесения карты к считывателю контроллер разблокирует ИУ и перейдет в режим *«Ожидание постановки на охрану плюс разрешение прохода»*. При этом горит зеленый и мигают красный и желтый индикаторы.
- После этого в течение времени, определенном параметром **Время удержания в разблокированном состоянии** (**Время анализа идентификатора)**, необходимо повторно предъявить ту же карту. В этом случае контроллер закроет ИУ и начнет постановку отдельных ресурсов ОЗ на охрану.
- Если повторного предъявления карты не произойдет, то контроллер вернется в исходный режим работы.

Примечание

Двери, снабженные замками с механическим автовзводом, при постановке на охрану, необходимо открыть и снова закрыть. После первого поднесения карты замок будет разблокирован. После второго поднесения на считывателе начнет мигать красный индикатор, показывая, что для сброса автовзвода дверь необходимо открыть и снова закрыть.

Режим работы выхода управления ИУ при работе с замком с механическим автовзводом должен быть установлен **Импульсный**.

При поступлении команды взятия на охрану, ОЗ переходит в режим *«Взятие»*. Формируется соответствующее событие *«Взятие ОЗ на охрану»* с указанием источника команды. Если ИУ данной ОЗ нормализировано, то ОЗ переходит в режим *«Охрана»*. Если ИУ не нормализировано, то в зависимости от значения параметра **Режим работы при невзятии**, ОЗ либо останется в режиме *«Взятие»*, либо перейдет в один из режимов *«Снята»* или *«Тревога»*. Если ОЗ переходит в режим *«Снята»*, будет сформировано событие *«Попытка взятия ОЗ (невозможно взять)»* с указанием источника команды и причины невзятия. Если ОЗ остается в режиме *«Взятие»*, то ОЗ переходят в режим *«Автоперевзятие»*. Будет постоянно осуществляться попытка взятия ИУ на охрану до тех пор, пока либо данная ОЗ не будет снята, либо ИУ не будут нормализировано, в этом случае ОЗ перейдет в режим *«Охрана»*.

При переходе ОЗ в режим *«Охрана»* формируется событие *«ОЗ взята на охрану»* с указанием источника команды. В этом режиме постоянно осуществляется мониторинг ИУ. Контроль ИУ осуществляется по состоянию датчика (нормализован/не нормализован). В этом режиме ОЗ остается до получения команды снятия с охраны или до первого нарушения ШС, входящего в ОЗ.

11.4.2 Снятие ОЗ с охраны

Снятие ОЗ с охраны возможно следующими способами:

- По карте, имеющей право снятия с охраны, в предыдущий режим работы (если это был режим *«Закрыто»*, то в режим работы *«Контроль»*).
- По команде от ПО в любой режим работы.
- По команде от Web-интерфейса в любой режим работы.

Для снятия с охраны необходимо **дважды** предъявить одну и ту же карту с правом снятия с охраны (в случае использования функции комиссионирования и/или верификации дополнительно требуется поднесение комиссионирующей карты и/или подтверждение прав от оператора):

- После первого поднесения карты к считывателю контроллер переходит в состояние *«Ожидание снятия с охраны».* При этом мигают зеленый и желтый индикаторы.
- После этого в течение времени, определенном параметром **Время удержания в разблокированном состоянии** (**Время анализа идентификатора)**, необходимо повторно предъявить ту же карту. Контроллер сменит режим работы с «Охрана» на режим, установленный до постановки на охрану (если это был режим *«Закрыто»*, то в режим работы *«Контроль»*).
- Если повторного предъявления карты не произойдет, то контроллер останется в режиме работы «Охрана».

При поступлении команды снятия ОЗ с охраны ОЗ переходит в режим *«Снята»,* записывается событие *«ОЗ снята с охраны»* с указанием источника команды. ИУ переходит в режим работы, который предшествовал установке режима *«Охрана»*.

11.4.3 Режим «Тревога»

ОЗ переводится в режим *«Тревога»* при взломе ИУ. При переходе в режим *«Тревога»* формируется событие *«Тревога по ОЗ»* и активизируются выходы, для которых выбран **Тип: ОПС**.

При нормализации ИУ режим *«Тревога»* не снимается. Повторное взлом ИУ приведет к повторной активизации выходов, работающих по программе *«Сирена»*, если установлен параметр конфигурации ОЗ **Повторное включение сирены** и выход нормализован (т.е. время предыдущей активизации выхода истекло).

Сброс режима *«Тревога»* производится из ПО сбросом тревоги по ОЗ или снятием ОЗ с охраны. Поступлении команды от ПО *«Сброс тревоги»* ОЗ режим не меняет.

11.5 Режим «Закрыто»

Переход в режим работы *«Закрыто»* возможен:

- По команде от ПО из любого режима работы.
- По команде от Web-интерфейса из любого режима работы.

Примечание

При установке режима работы *«Закрыто»* с ИК-пульта: управление с ДУ не блокируется; управление с ИК-пульта по кнопке *«Посетитель»* не блокируется; при открывании ИУ происходит возврат к предыдущему режиму работы.

Выход из режима работы *«Закрыто»* возможен:

- По команде от ПО в любой режима работы.
- По команде от Web-интерфейса в любой режим работы.

Таблица 8 Реакция контроллера на предъявление идентификатора в режиме «Закрыто»

ИУ заблокировано
Предъявление карты
Регистрируется событие *«Запрет прохода – нарушение режима контроля доступа»* (*«Запрет прохода, нарушение РЕЖИМОВ РАБОТЫ»*) Регистрируется событие *«Запрет прохода» («Идентификатор не зарегистрирован», «Карта запрещена»* и т.п.).
Механическое открытие ИУ
Регистрируется событие *«Несанкционированный проход (взлом)»* (*«Несанкционированное открытие (взлом) ИУ»*)

11.6 Индикация

Индикация режимов работы, состояний и реакций контроллера на предъявление идентификаторов осуществляется на корпусе контроллера. Возможные варианты индикации представлены в таблицах 9 и 10.

Примечание

При разрешении прохода по карте световая индикация включается на **Время удержания в разблокированном состоянии**, либо до факта совершения прохода. При запрете прохода индикация включается на 2 секунды.

Таблица 9 Индикация режимов работы контроллера

Установленный режим	Предъявление карты	Индикаторы			
		Зеленый	Желтый	Красный	Звук
Отсутствие конфигурации	Нет	2 Гц	2 Гц	2 Гц	выкл.
	Считывание идентификатора	выкл.	меняет состояние	выкл.	0,5 сек.
Контроль Совещание Охрана	Ожидание комиссионирования	выкл.	2 Гц	выкл.	выкл.
Контроль Совещание Охрана	Ожидание верификации	2 Гц	выкл.	2 Гц	выкл.
Открыто	Нет	вкл.	выкл.	выкл.	выкл.
Контроль		выкл.	вкл.	выкл.	выкл.
Совещание		вкл.	вкл.	выкл.	выкл.
Охрана		выкл.	1 Гц	1 Гц	выкл.
Закрыто		выкл.	выкл.	вкл.	выкл.
Открыто Контроль Совещание	Карта имеет право прохода	вкл.	выкл.	выкл.	1 сек.
Открыто	Карта не имеет права прохода	вкл.	выкл.	вкл.	2 сек.
Контроль		выкл.	выкл.	вкл.	2 сек.
Совещание		выкл.	выкл.	вкл.	2 сек.
Охрана		выкл.	выкл.	вкл.	2 сек.
Открыто	Карта имеет права прохода и постановки/снятия с охраны	вкл.	2 Гц	2 Гц	1 сек.
Контроль		вкл.	2 Гц	2 Гц	1 сек.
Совещание		вкл.	2 Гц	2 Гц	1 сек.
Охрана		2 Гц	2 Гц	выкл.	выкл.
Закрыто	Любая карта	выкл.	выкл.	1 Гц	2 сек.

Таблица 10 Предъявление карты, имеющей право прохода и постановки/снятия ОЗ с охраны

Установленный режим	Состояние ОЗ	Индикаторы			
		Зеленый	Желтый	Красный	Звук
Контроль Совещание Охрана	*«Взятие»* (ОЗ нормализована)	выкл.	выкл.	2 Гц	выкл.
Контроль Совещание Охрана	*«Невзятие»* (ОЗ не нормализована)	выкл.	выкл.	2 Гц	2 Гц
Открыто Контроль Совещание	*«Ожидание постановки на охрану плюс разрешение прохода»*	вкл.	2 Гц	2 Гц	1 сек.
Охрана	*«Ожидание постановки на охрану ОЗ без ИУ*	выкл.	2 Гц	2 Гц	выкл.
Открыто Контроль Совещание	*«Ожидание снятия с охраны ОЗ без ИУ плюс разрешение прохода»*	вкл.	2 Гц	выкл.	1 сек.
Охрана	*«Ожидание снятия с охраны»*	2 Гц	2 Гц	выкл.	выкл.
Охрана	*«Ожидание снятия с охраны ОЗ без ИУ»*	2 Гц	2 Гц	2 Гц	выкл.

12 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ

Контроллер в оригинальной упаковке предприятия-изготовителя допускается транспортировать только в закрытом транспорте (самолетах, железнодорожных вагонах, контейнерах, закрытых автомашинах, трюмах и т.д.).

Хранение контроллера допускается в закрытых помещениях при температуре окружающего воздуха от –20˚С до +40˚С и относительной влажности воздуха до 98% при +25˚С. Условия транспортирования являются такими же, как условия хранения.

13 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

Эксплуатационно-технический персонал, в обязанности которого входит техническое обслуживание контроллера, должен знать конструкцию и правила эксплуатации контроллера.

Работы должен производить электромонтер с квалификацией не ниже 5 разряда.

При производстве работ по техническому обслуживанию следует руководствоваться разделом 7 *«Требования безопасности»* данного *«Руководства по эксплуатации»*.

Внимание!

- Перед началом работ отключить контроллер от сети переменного тока и резервного питания.
- Вся контрольно-измерительная аппаратура должна быть поверена.

Один раз в три месяца предусматриваются плановые работы в объеме регламента №1. Перечень работ приведен в таблице 11.

Сведения о проведении регламентных работ заносятся в журнал учета регламентных.

Соблюдение периодичности, технологической последовательности и методики выполнения регламентных работ являются обязательными.

Техническое обслуживание других устройств, подключенных к контроллеру, указано в эксплуатационной документации на данные устройства.

Таблица 11 Перечень работ по регламенту №1 (технологическая карта №1)

Содержание работ	Порядок выполнения	Приборы, инструмент, оборудование, материалы	Нормы и наблюдаемые явления
1 Внешний осмотр, чистка контроллера	1.1 Отключить источник питания от сети переменного тока и удалить с поверхностей контроллера и источника питания пыль, грязь и влагу.	Ветошь, кисть флейц.	Не должно быть следов грязи и влаги.
	1.2 Снять крышки с источника питания, при наличии резервного источника питания (аккумулятора) удалить с его поверхности пыль, грязь, влагу, окислы с клемм. Измерить напряжение резервного источника. В случае необходимости зарядить или заменить батарею.	Отвертка, ветошь, кисть флейц, прибор Ц4352.	Напряжение должно соответствовать паспортным данным на батарею (не менее 12,6 В).
1 Внешний осмотр, чистка контроллера	1.3 Удалить с поверхности контактов перемычек, предохранителей пыль, грязь, следы коррозии.	Ветошь, кисть флейц, бензин Б-70.	Не должно быть следов коррозии, грязи.
	1.4 Проверить соответствие номиналу и исправность предохранителей.		
	1.5 Проверить соответствие подключения внешних цепей.		Должно быть соответствие схеме внешних соединений.
	1.6 Восстановить соединение, если провод оборван. Заменить провод, если нарушена изоляция.		Не должно быть повреждений изоляции и обрывов проводов.
2 Проверка работоспособности	2.1 Проверить работоспособность контроллера по разделу 11.		Включение соответствующей индикации на контроллере согласно разделу 11.6. Формирование сигналов на релейном выходе согласно его конфигурации.

14 ДИАГНОСТИКА И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Возможные варианты неисправностей:

14.1 Контроллер не работает

Причинами неисправности контроллера могут быть:

1. **Неисправность источника питания** контроллера – проверьте источник питания.
2. **Выход из строя подключенных к контроллеру устройств** (замка, датчика двери, кнопки ДУ.). Проверьте исправность устройств.
3. **Неисправность линий подключения** к контроллеру устройств. Проверьте исправность линий подключения этих устройств.
4. **Выход из строя электро-радио-элементов**, установленных на плате контроллера, – данный контроллер необходимо прислать в ремонт.

14.2 Нарушение связи с компьютером

Причинами данной неисправности могут быть:

1. **Отсутствуют сетевые настройки в компьютере** – установите IP-адрес и маску подсети компьютера. Контроллер при этом должен быть подключен либо непосредственно к сетевому разъему сетевой карты компьютера, либо к тому же Hub/Switch, в который включен компьютер.
2. **Неправильно введен пароль к данному контроллеру**. Проверьте правильность введенного в ПО пароля.
3. **Неисправности, связанные с компьютером** (с ПО, с базами данных и т.п.).
   Диагностика данной неисправности заключается в запуске команды:
   ```
   ping x.x.x.x
   ```
   где `x.x.x.x` – IP-адрес данного контроллера.
   Если связь есть, то вы увидите строки вида:
   ```
   Ответ от x.x.x.x: число байт=32 время<10мс TTL=128
   ```
   Если связи (ответа) нет, то проверьте правильность настройки маршрутизации в вашей сети.
4. **Неисправности, связанные с оборудованием сети Ethernet**, находящимся между компьютером и контроллером: концентратор (HUB), коммутатор (SWITCH) и прочее сетевое оборудование, включая кабели связи.
   Диагностика данной неисправности заключается в запуске команды:
   ```
   ping x.x.x.x -l 576
   ```
   где `x.x.x.x` – IP-адрес данного контроллера.
   Если связь есть и стандартные минимальные пакеты (576 байт) не фрагментируются, то вы увидите строки вида:
   ```
   Ответ от x.x.x.x: число байт=576 время<10мс TTL=128
   ```
   В данном случае можно утверждать, что IP-пакеты не фрагментируются до размера меньше 576 байт, и выбранное вами подключение должно работать.
   Если положительный ответ получить не удается, то вероятнее всего на пути следования IP-пакетов находится сетевое коммутирующее оборудование, фрагментирующее IP-пакеты до размера меньше 576 байт. Проверьте настройки этого оборудования, при возможности увеличьте размер *MTU*. Обычно этот параметр обозначается как *MaxMTU* или *IPMTU*.
5. **Если у вас возможны несколько вариантов коммутации**, то воспользуйтесь командой:
   ```
   ping x.x.x.x -l 576 -t
   ```

Коммутируя разными способами, смотрите на время ответа, выбирая соединение, дающее максимально быстрый ответ.

6. **Неисправности, связанные с контроллером.** Выход из строя элементов, обеспечивающих связь по интерфейсу *Ethernet (IEEE 802.3)*.
   Если контроллер «не видит» подключения к сети *Ethernet*, подключите его к кабелю, на котором работает другой контроллер. Если контроллер «не увидит» подключение к сети *Ethernet*, либо связь с ним не восстанавливается, то этот контроллер необходимо прислать в ремонт.

15 ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ПРИЛОЖЕНИЯ

Приложение А Программы управления выходами

В заголовках строк таблицы перечислены названия программ управления и времена активации и нормализации выхода. В заголовках столбцов перечислены возможные режимы зон.

Реакция выхода на наступление режима определяется временем активации (такт.) и временем нормализации (tнорм.).

- Значение «0» для обоих времен означает, что при наступлении соответствующего режима, выход свое состояние не изменяет.
- Значение «время» означает, что выход активируется (такт.) до истечения времени, заданного в конфигурации либо до наступления другого режима, либо до сброса (добавление * означает, что активизация будет только при переходе в данный режим из режима *«Снята»*).
- Значение «беск.» для времени активации (такт.) означает, что выход активируется до наступления другого режима, либо до сброса.
- Значение «беск.» для временем нормализации (tнорм.) означает, что выход нормализуется до наступления другого режима.
- Прочие значения определяют параметры мигания в секундах.

Параметр **Зоны, активирующие выход**, по которым срабатывает данный выход, группирует зоны, изменение режима которых приведут к запуску программы управления.

Для программ *«Лампа 1»*, *«ПЦН 1»* и *«ПЦН 2»* активация выхода на время «беск.» произойдет только при переходе в данный режим **всех зон**, указанных в маске (маска по «И»). Во всех остальных случаях для активации выхода достаточно поступления сигнала об изменении режима **любой из зон**, указанных в маске (маска по «ИЛИ»).

Таблица А.1 Программы управления выходами

№	Название программы		Режим ОЗ				ШС в режиме «Автоперевзятие»	Неисправность контроллера
			«Снята»	«Охрана»	«Взятие»	«Тревога»		
1	Включить при тревоге	такт., с	0	0	0	время	0	0
		тнорм.,с	беск.	беск.	0	0	0	0
2	Мигать при тревоге	такт., с	0	0	0	0,5	0	0
		тнорм.,с	беск.	беск.	0	0,5	0	0
3	Лампа 1	такт., с	0	беск.	1	0,5	0	0
		тнорм.,с	беск.	0	1	0,5	0	0
4	Лампа 2	такт., с	0	беск.	1	0,5	0	0
		тнорм.,с	беск.	0	1	0,5	0	0
5	ПЦН 1	такт., с	0	беск.	0	0	0	0
		тнорм.,с	беск.	0	беск.	беск.	0	0
6	ПЦН 2	такт., с	беск.	беск.	0	0	0	0
		тнорм.,с	0	0	беск.	беск.	0	0
7	Сирена	такт., с	0	0	0	время	0	0
		тнорм.,с	беск.	беск.	0	0	0	0
8	Вкл. перед взятием	такт., с	0	0	время	0	0	0
		тнорм.,с	беск.	беск.	0	беск.	0	0
9	Вкл. при взятии	такт., с	0	время	0	время*	0	0
		тнорм.,с	беск.	0	0	0	0	0
10	Вкл. при снятии	такт., с	время	0	0	0	0	0
		тнорм.,с	0	беск.	беск.	беск.	0	0
11	Вкл. при автоперевзятии	такт., с	0	0	0	0	время	0
		тнорм.,с	беск.	беск.	0	беск.	0	0

Приложение Б События, регистрируемые контроллером

В процессе работы система осуществляет сбор и регистрацию всех событий и состояний контроллера. Сбор информации осуществляется двумя независимыми потоками: мониторингом и регистрацией. Все события протоколируются с учетом календарной даты и времени суток (с точностью до секунды).

При выключенном сервере системы события мониторинга не передаются, а события регистрации хранятся в энергонезависимой памяти контроллера. Максимальное количество событий регистрации определяются размерами энергонезависимой памяти контроллера. В случае переполнения новые события заменяют наиболее старые.

1. События мониторинга.
2. Событие регистрации и Web – интерфейса.
3. Событие отображается в кратком списке событий Web – интерфейса.

1. События, связанные с доступом по коду идентификатора

№	Тип события	Причина	1	2	3	Примечание
1	Предъявление невалидной карты	Идентификатор не зарегистрирован (Карта не зарегистрирована)	+	+	+	Может вызывать или нет генерацию тревоги (в зависимости от параметров генератора тревоги).
2		Идентификатор запрещен (Карта запрещена)	+	+	+	
3		Идентификатор из «СТОП-листа» (Карта из «СТОП-листа»)	+	+	+	
4		Идентификатор просрочен (Истек срок действия карты)	+	+	+	
5	Предъявление карты	несоответствие временным критериям доступа	+	-	-	
6		несоответствие текущему местоположению	+	-	-	
7		несоответствие временным критериям доступа и текущему местоположению	+	-	-	
8	Запрет прохода		-	+	+	Предъявление карты либо при не заданном значении параметра **Время удержания в разблокированном состоянии**, либо при неисправности одного из датчиков (герконов).

№	Тип события	Причина	1	2	3	Примечание
9		несоответствие временным критериям доступа (нарушение времени)	-	+	+	Предъявленная карта является нарушителем по времени (событие, вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги).
10		несоответствие текущему местоположению (нарушение зональности)	-	+	+	Предъявленная карта является нарушителем и по времени и по зональности (событие, вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги).
11		несоответствие временным критериям доступа и текущему местоположению (нарушение времени и зональности)	-	+	+	Предъявленная карта является нарушителем и по времени и зональности (событие, вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги).
12		нарушение комиссионирования	+	+	+	Несоответствие с комиссионирующей картой или комиссионирование не было выполнено вообще (событие, вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги).
13		отказ в подтверждении прохода от верификации	-	+	+	Не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет.
14	Предъявление запрещенной карты (Запрет прохода)	нарушение РКД (нарушение режима контроля доступа)	+	+	+	Предъявление любой карты в режиме работы *«Закрыто»* или предъявление в режиме работы *«Охрана»* карты, которая не имеет права автономного снятия с охраны ОЗ с ИУ либо права автономной постановки / снятия с охраны ОЗ без ИУ, (вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги).
15	Запрет прохода по команде оператора		-	+	-	

№	Тип события	Причина	1	2	3	Примечание
16	Запрет прохода по команде от ДУ		-	+	+	После того, как контроллер разрешил проход, охранник пультом ДУ подал команду на запрет прохода.
17	Отказ от прохода		-	+	+	Отказ от предоставленного системой права пройти через ИУ по карте.
18	Проход по идентификатору (Проход по карте)		-	+	+	Проход через ИУ, произошедший после предоставления контроллером права пройти через него и до истечения **Времени удержания в разблокированном состоянии**.
19		с несоответствием временным критериям доступа (с нарушением времени)	-	+	+	Событие возникает при проходе по карте с каким-либо нарушением при установленном **мягком** контроле данного нарушения. Также событие возникает у контроллеров замка при предъявлении карты с каким-либо нарушением, либо карты, требующей комиссионирования / верификации в двух случаях: - либо при предъявлении при открытом замке, - либо если замок будет открыт по какой-либо внешней причине до окончания **Времени анализа карты** по данному предъявлению
20		с несоответствием текущему местоположению (с нарушением зональности)	-	+	+	
21		несоответствие временным критериям доступа и текущему местоположению (с нарушением времени и зональности)	-	+	+	
22		с нарушением комиссионирования	-	+	+	
23		с несоответствием временным критериям доступа и с нарушением комиссионирования (с нарушением времени, зональности и комиссионирования)	-	+	+	
24		с несоответствием текущему местоположению и с нарушением комиссионирования	-	+	+	

№	Тип события	Причина	1	2	3	Примечание
25		несоответствие временным критериям доступа и текущему местоположению и с нарушением комиссионирования (с нарушением времени, зональности и комиссионирования)	-	+	+	
26		при отказе в подтверждении прохода от верификации (без учета верификации)	-	+	+	
27		с несоответствием временным критериям доступа и при отказе в подтверждении прохода от верификации (с нарушением времени и без учета верификации)	-	+	+	
28		с несоответствием текущему местоположению и при отказе в подтверждении прохода от верификации (с нарушением зональности и без учета верификации)	-	+	+	
29		несоответствие временным критериям доступа и текущему местоположению и при отказе в подтверждении прохода от верификации (с нарушением времени, зональности и без учета верификации)	-	+	+	

№	Тип события	Причина	1	2	3	Примечание
30	Проход с подтверждением от ДУ (Проход по карте с подтверждением от пульта ДУ)		-	+	+	Проход через ИУ, произошедший после предоставления контроллером с подтверждением от ДУ права пройти через него и до истечения **Времени удержания в разблокированном состоянии**. Подтверждение от ДУ осуществляется при условии, что верифицирующее устройство не определено и стоят соответствующие опции верификации
31		с несоответствием временным критериям доступа (с нарушением времени)	-	+	+	
32		с несоответствием текущему местоположению (с нарушением зональности)	-	+	+	
33		несоответствие временным критериям доступа и текущему местоположению (с нарушением времени и зональности)	-	+	+	
34	Проход с подтверждением от верификации (Проход по карте с верификацией)		-	+	+	Проход через ИУ, произошедший после предоставления контроллером с подтверждением от верифицирующего устройства права пройти через него и до истечения **Времени удержания в разблокированном состоянии**. Подтверждение от верифицирующего устройства осуществляется при условии, что верифицирующее устройство определено и стоят соответствующие опции верификации.
35		с несоответствием временным критериям доступа (с нарушением времени)	-	+	+	
36		с несоответствием текущему местоположению (с нарушением зональности)	-	+	+	
37		несоответствие временным критериям доступа и текущему местоположению (с нарушением времени и зональности)	-	+	+	
38	ИУ не закрыто после прохода по идентификатору (карте)		+	+	+	После прохода по карте время активизации состояния контакта ИУ превысило установленное **Предельное время разблокировки**
39	Предъявлена комиссионирующая карта		-	+	-	

2. События, связанные с изменениями состояний ОЗ

№	Тип события	Причина	1	2	3	Примечание
1	ОЗ взята на охрану по идентификатору (карте)		+	+	-	ОЗ перешла в режим «Охрана» по карте с соответствующими правами. Если ОЗ включает в себя ИУ, то данное событие будет сопровождаться событием «Изменение режима работы на режим «Охрана» по идентификатору».
2	ОЗ снята с охраны по идентификатору (карте)		+	+	-	ОЗ перешла в режим «Снята», по предъявлению карты с соответствующими правами. Если ОЗ включает в себя ИУ, то данное событие будет сопровождаться событием «Изменение режима работы на режим «…» по идентификатору», где «…» – тот режим работы, в который будет осуществлен переход.
3	Попытка взятия ОЗ (невозможно взять) по идентификатору (ОЗ не взята на охрану по карте е)	нарушение состояния ресурса ИУ	+	+	-	ИУ в состоянии «Нарушение» при взятии ОЗ.
4		нарушение комиссионирования	+	+	-	В процессе постановки ОЗ на охрану было зафиксировано несоответствие с комиссионирующей картой или комиссионирование не было выполнено.
5		отказ в подтверждении взятия от верификации	+	+	-	В процессе постановки ОЗ на охрану не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет.
6		несоответствие временных критериев доступа (нарушение времени)	+	+	-	Предъявленная карта с правами постановки ОЗ на охрану является нарушителем по времени.
7		несоответствие текущему местоположению (нарушение зональности)	+	+	-	Предъявленная карта с правами постановки ОЗ на охрану является нарушителем по зональности.

№	Тип события	Причина	1	2	3	Примечание
8		несоответствие временным критериям доступа и текущему местоположению (нарушение времени и зональности)	+	+	-	Предъявленная карта с правами постановки ОЗ на охрану является нарушителем и по времени и зональности.
9		отказ от постановки	+	+	-	В процессе постановки ОЗ на охрану карта не была поднесена повторно до истечения Времени удержания в разблокированном состоянии
10	Попытка снятия ОЗ (невозможно снять) по идентификатору (ОЗ не снята с охраны по карте)	нарушение комиссионирования	+	+		В процессе снятия ОЗ с охраны было зафиксировано несоответствие с комиссионирующей картой или комиссионирование не было выполнено вообще.
11		отказ в подтверждении снятия от верификации	+	+	-	В процессе снятия ОЗ с охраны не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет.
12		несоответствие временных критериев доступа (нарушение времени)	+	+	-	Предъявленная карта с правами снятия ОЗ с охраны является нарушителем по времени.
13		несоответствие текущему местоположению (нарушение зональности)	+	+	-	Предъявленная карта с правами снятия ОЗ с охраны является нарушителем по зональности.
14		несоответствие временным критериям доступа и текущему местоположению (нарушение времени и зональности)	+	+	-	Предъявленная карта с правами снятия ОЗ с охраны является нарушителем и по времени и зональности.
15		отказ от снятия	+	+	-	В процессе снятия ОЗ с охраны карта не была поднесена повторно до истечения времени удержания в разблокированном состоянии.
16	ОЗ взята на охрану по идентификатору с подтверждением	ОЗ перешла в режим ОХРАНА	+	+	-	

№	Тип события	Причина	1	2	3	Примечание
17	ОЗ снята с охраны по идентификатору с подтверждением	ОЗ перешла в режим СНЯТА	+	+	-	
18	ОЗ взята на охрану по команде оператора		+	+	-	ОЗ перешла в режим *«Охрана»* по команде оператора. Если ОЗ включает в себя ИУ, то данное событие будет сопровождаться событием *«Изменение режима работы на режим «Охрана» по команде оператора»*.
19	ОЗ снята с охраны по команде оператора		+	+	-	ОЗ перешла в режим *«Снята»* по команде оператора. Если ОЗ включает в себя ИУ, то данное событие будет сопровождаться событием *«Изменение режима работы на режим «…» по команде оператора»*, где «х» – тот режим работы, в который будет осуществлен переход.
20	Попытка взятия ОЗ (невозможно взять) по команде оператора (ОЗ не взята на охрану по команде оператора)	нарушение состояния ресурса ИУ	+	+	-	ИУ в состоянии *«Нарушение»* при взятии ОЗ.
21	Тихая тревога по ОЗ		+	+	-	ОЗ перешла в режим *«Тревога»*, в том числе и если параметр конфигурации ОЗ **Работа при невзятии ОЗ** установлен в значение – **«Тревога»**
22	Тревога по ОЗ		+	+	-	ОЗ перешла в режим *«Тревога»*, в том числе и если параметр конфигурации ОЗ **Работа при невзятии ОЗ** установлен в значение – **«Тревога»**
23	Сброс тревоги по ОЗ		+	+	-	
24	Взятие ОЗ на охрану по идентификатору (Переход охранной зоны в режим Взятие на охрану по карте)		+	+	-	Запущена процедура взятия на охрану всех ресурсов ОЗ по карте с соответствующими правами (идет задержка взятия). ОЗ перешла в режим *«Взятие»*.

№	Тип события	Причина	1	2	3	Примечание
25	Взятие ОЗ на охрану по команде оператора (Переход охранной зоны в режим Взятие на охрану по команде оператора)		+	+	-	Запущена процедура взятия на охрану всех ресурсов ОЗ по команде оператора (идет задержка взятия). ОЗ перешла в режим *«Взятие»*.

3. События, связанные с состояниями входов и выходов

№	Тип события	1	2	3	Примечание
1	Активизация входа	+	+	-	
2	Нормализация входа	+	+	-	
3	Активизация выхода	+	+	-	
4	Нормализация выхода	+	+	-	
5	Запуск задержки активизации выхода	+	+	-	Начат отсчет задержки перед запуском программы управления выходом.

4. События, связанные с проходами через ИУ без идентификаторов

№	Тип события	1	2	3	Примечание
1	Проход по команде от ДУ	-	+	+	Проход через ИУ, произошедший после предоставления контроллером по команде от ДУ права пройти через него и до истечения **Времени удержания в разблокированном состоянии.**
2	Проход по команде от ПК (оператора)	-	+	+	Проход через ИУ, произошедший после предоставления контроллером по команде от ПК права пройти через него и до истечения **Времени удержания в разблокированном состоянии** (в случае, если между подачей разрешения на проход и самим проходом произойдет пропадание связи с ПК).
3	Несанкционированный проход через ИУ (взлом ИУ)	+	+	+	Активизация состояния контакта заблокированного ИУ.
4	ИУ не закрыто после прохода от ДУ	+	-	-	Время активизации состояния контакта ИУ по команде от ДУ превысило установленное **Предельное время разблокировки**.
5	ИУ не закрыто после прохода от ПК	+	-	-	Время активизации состояния контакта ИУ по команде от ПК превысило установленное **Предельное время разблокировки**.
6.	ИУ разблокирован	+	-	-	Изменение текущего состояния контакта ИУ.
7	ИУ заблокирован	+	-	-	

5. События связанные с функционированием

№	Тип события	Причина	1	2	3	Примечание
1	Включение питания контроллера		-	+	+	

№	Тип события	Причина	1	2	3	Примечание
2	Выключение питания контроллера		-	+	+	
3	Нарушение связи		-/+	+	+	Отключение от локальной сети.
4	Восстановление связи		-/+	+	+	Подключение к локальной сети.
5	Переполнение журнала регистрации		+	+	+	Переполнение журнала возникает после заполнения в памяти контроллера предпоследней свободной страницы журнала (размер 1-й страницы равен 32 событиям).
6	Переполнение буфера журнала мониторинга		+	-	-	Если в единицу времени регистрируется больше событий чем передается, то буфер мониторинга (на 16 событий) переполняется и более старые события затираются более новыми.
7	Сбой физического уровня Ethernet		-	+	-	
8	Очистка журнала регистрации		+	+	+	Очистка журнала происходит всегда после чтения переполненного журнала регистрации.
9	Перезапуск контроллера	WatchDog	-	+	+	Программный сброс контроллера (после обновления встроенного ПО или форматирования памяти, либо после первого обнаружения фатальной неисправности).
11	Переполнение списка идентификаторов		+	+	-	Событие появляется в случае, если из-за внутренней ошибки программного обеспечения в контроллер передано количество карт доступа, превышающее его ресурсы.
12	Неисправность контроллера	память FRAM	+	+	+	Фатальная неисправность – отказ электронных элементов платы контроллера.
13		память DataFlash	+	+	+	
14		часы RTC	+	+	+	
15		шина I2C	+	+	+	
16	Форматирование памяти	журнал событий	-	+	+	Форматирование памяти контроллера – очистка журнала регистрации, списка карт, области конфигурации и режимов работы.
17		список карт	-	+		
18		конфигурация	-	+		
19		прошивка	-	+		
20		текущие установки (режимы работы и т.д.)	-	+		

№	Тип события	Причина	1	2	3	Примечание
21	Корпус контроллера открыт		+	+	-	
22	Корпус контроллера закрыт		+	+	-	
23	Изменение режима работы по команде оператора (Установка режима «…» по команде оператора)	режим «Открыто»	+	+	+	Изменение любого режима работы на любой другой режим работы по команде ПО или Web-интерфейса.
24		режим «Контроль»	+	+	+	
25		режим «Совещание»	+	+	-	
26		режим «Закрыто»	+	+	+	
27		режим «Охрана»	+	+	+	
28	Изменение режима работы на режим «Охрана» по идентификатору (Установка режима Охрана по карте)		+	+	+	Постановка на охрану по идентификатору.
29	Изменение режима работы «Охрана» на режим «…» по идентификатору	режим «Открыто»	+	+	+	Снятие с охраны по идентификатору, с возвратом к режиму, предшествовавшему постановке на охрану по идентификатору.
30		режим «Контроль»	+	+	+	
31		режим «Совещание»	+	+	+	
32	Тревога		+	+	-	От Генератора тревоги
33	Сброс тревоги		+	+	+	По команде от ПО или Web-интерфейса
34	Тестирование прибора (контроллера) начато		+	+	+	Переход прибора в режим «Тестирование прибора» по команде от ПО или Web-интерфейса
35	Тестирование прибора завершено успешно (Тестирование контроллера завершено, неисправностей не выявлено)		+	+	+	Переход прибора в дежурный режим по завершению самодиагностики. Фатальных неисправностей не выявлено.
36	Тестирование прибора выявило неисправности (Тестирование контроллера завершено, выявлены неисправности)		+	+	+	Завершение самодиагностики. Выявлены фатальные неисправности.

Приложение В Инструкция по подключению через PoE-сплиттер PA1212

В.1 Описание сплиттера

PoE-сплиттер PA1212 (далее – *сплиттер*) предназначен для подачи питания на устройства, подключаемые по сети *Ethernet*. Сплиттер работает с любыми сетевыми коммутаторами (далее – *Switch)*, поддерживающими технологию передачи электроэнергии по витой паре *PoE* и совместимыми со стандартом *IEEE 802.3af*.

Сплиттер представляет собой блок электроники в пластиковом корпусе и снабжен следующими разъемами и индикаторами, обозначенными на рисунке В.1:

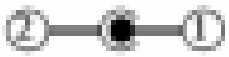
На стороне *«IN»:*

Con 1 – разъем для подключения кабеля *Ethernet* от *Switch*.

На стороне *«OUT»*:

Con 2 – разъем подключения кабеля *Ethernet* контроллера;

Con 3 – разъем DC Jack 5,5×2,5 мм выхода питания ***«12В»***, для подключения кабеля питания контроллера;



1 – V+
2 – V-

LED – световой индикатор зеленого цвета.

Рисунок В.1 Внешний вид сплиттера

В.2 Порядок подключения

Внимание!

Суммарная потребляемая мощность контроллера и всех получающих от него питание устройств не должна превышать 12 Вт. При этом рекомендуется оставлять запас мощности не менее 10 %.

При подключении контроллера через сплиттер придерживайтесь следующей последовательности действий:

1. Определите место установки сплиттера. Не устанавливайте сплиттер на расстоянии более 2 м от контроллера.
2. Подключите кабель *Ethernet* от контроллера к разъему ***Con2*** сплиттера, расположенному на стороне, обозначенной как *«OUT»*.
3. Подключите цепи питания контроллера и управляемого им замка к разъему ***Con3*** сплиттера, расположенному на стороне, обозначенной как *«OUT»*. Схема подключения приведена на рисунке В.2. (Штекер для подключения к разъему входит в комплект поставки сплиттера).

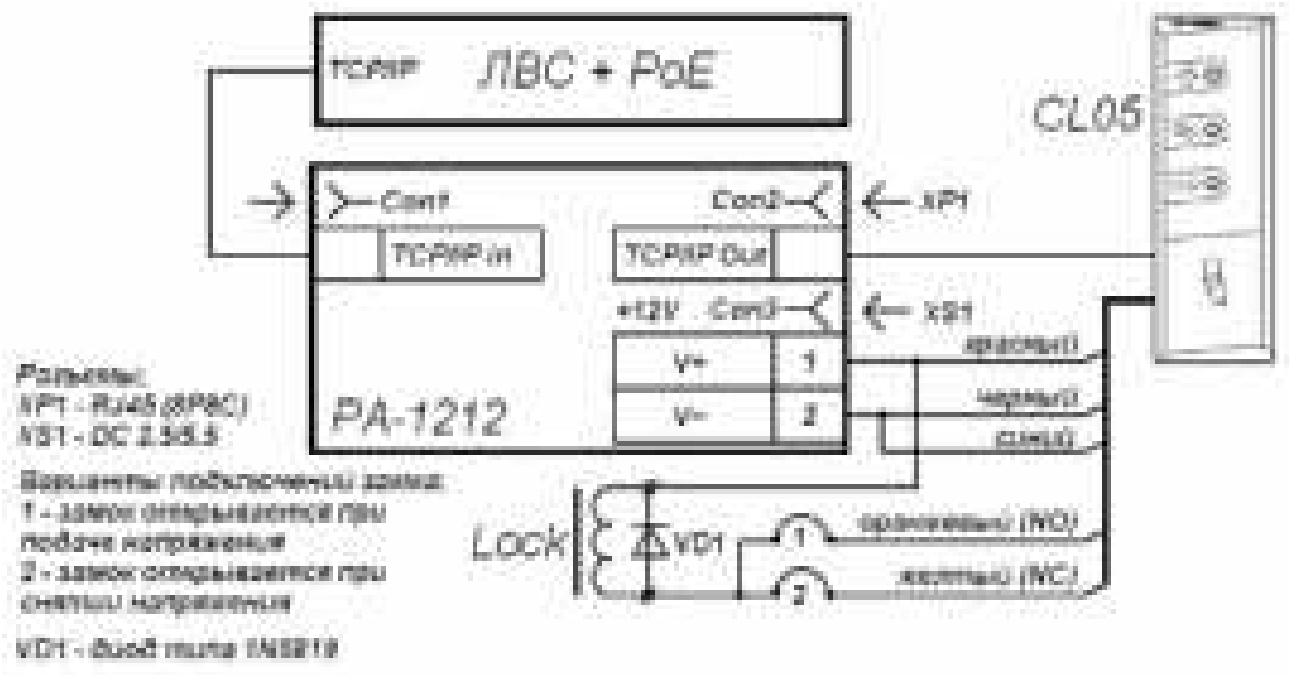


Рисунок В.2 Схема подключения контроллера через PoE-сплиттер PA1212 (Lock – замок, управляемый контроллером)

Внимание!

При подключении замка установка диода искрозащиты ***VD1*** (см. рис. **Ошибка! Источник ссылки не найден.**), типа 1N5819 – **ОБЯЗАТЕЛЬНА!** Использование супрессоров вместо диодов искрозащиты – **ЗАПРЕЩЕНО!** Рекомендуется использовать только электромеханические замки.

4. Подключите кабель *Ethernet* от *Switch* к разъему ***Con1*** сплиттера, расположенному на стороне обозначенной как *«IN»*.
5. После верификации между *Switch* и сплиттером на контроллер будет подано питание. Световой индикатор ***LED*** должен при этом гореть зеленым. Возможные неисправности и методы их устранения указаны в таблице В.1.

Примечание

Для отключения питания контроллера отсоедините кабель *Ethernet,* идущий от *Switch,* от разъема ***Con1*** сплиттера. Разъем расположен на стороне обозначенной как *«IN»*.

B.3 Индикация сплиттера и устранение неисправностей

Индикатор ***LED*** сплиттера находится возле разъема подключения питания ***«12В»*** на стороне, обозначенной как *«OUT»,* и служит для индикации состояния сплиттера.

Таблица B.1 Индикация сплиттера и устранение неисправностей

Индикация LED	Состояние питания контроллера	Возможные неисправности и порядок их устранение
Индикатор горит	Питание подается.	
Индикатор не горит	Питание **НЕ** подается.	Проверьте кабель *Ethernet* от *Switch* и убедитесь, что *Switch* работает нормально.
Индикатор горит	Питание **НЕ** подается.	Проверьте кабель питания, подключенный к контроллеру.
Индикатор гаснет при подключении устройства	Питание **НЕ** подается.	Убедитесь, что суммарная потребляемая мощность всех подключенных устройств не превышает указанного выше значения. Проверьте кабель питания, подключенный к контроллеру.
Индикатор мигает и выключается	Питание **НЕ** подается.	Кабель питания контроллера не подключен. Проверьте кабель питания, подключенный к контроллеру.

ООО «Завод ПЭРКо»

Тел.: (812) 329-89-24, 329-89-25
Факс: (812) 292-36-08

Юридический адрес:
180600, г. Псков, ул. Леона Поземского, 123 В

Техническая поддержка:

Тел./факс: (812) 321-61-55, 292-36-05

system@perco.ru – по вопросам обслуживания электроники систем безопасности

turnstile@perco.ru – по вопросам обслуживания турникетов, ограждений

locks@perco.ru – по вопросам обслуживания замков

soft@perco.ru – по вопросам технической поддержки программного обеспечения

www.perco.ru

Утв. 06.09.2011
Кор. 18.09.2013
Отп. 18.09.2013

www.perco.ru

тел: 8 (800) 333-52-53