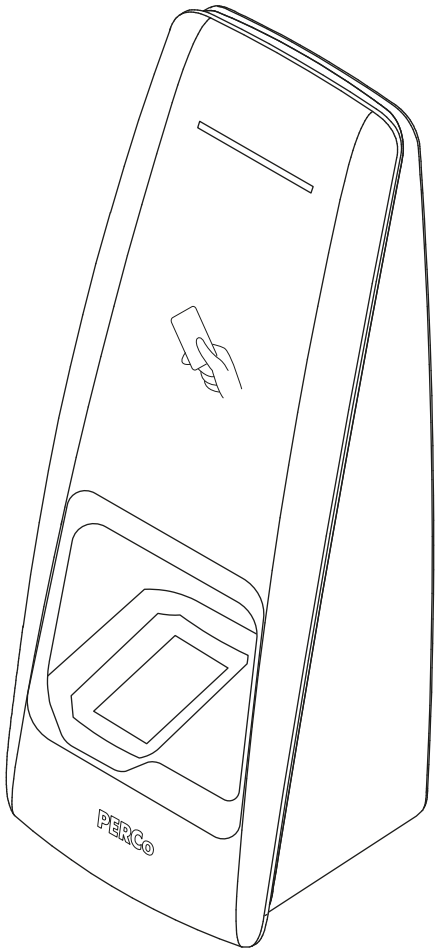
PERCo®

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ



CL15.1

Биометрический контроллер

SEC.RU | Короткий путь к информации
Скачано с sec.ru

СОДЕРЖАНИЕ

1 Назначение ... 2
2 Условия эксплуатации ... 3
3 Основные технические характеристики ... 3
4 Комплект поставки ... 4
4.1 Стандартный комплект поставки ... 4
4.2 Дополнительное оборудование, поставляемое по отдельному заказу ... 4
5 Описание ... 4
5.1 Устройство и работа ... 4
5.3 Параметры сигналов выхода управления ИУ ... 6
5.4 Параметры сигналов входов Door, DU и In ... 6
5.5 Параметры сигналов дополнительного выхода ... 7
5.6 Выбор способа задания IP-адреса ... 7
6 Маркировка и упаковка ... 8
7 Требования безопасности ... 8
7.1 Безопасность при монтаже ... 8
7.2 Безопасность при эксплуатации ... 9
8 Монтаж ... 9
8.1 Общие указания ... 9
8.2 Кабели ... 9
8.3 Последовательность монтажа ... 10
8.3.1 Монтаж контроллера ... 10
8.3.2 Подключение замка ... 11
8.3.3 Подключение турникетов и электромеханических калиток ... 16
8.3.4 Подключение ПДУ ... 17
8.3.5 Подключение дополнительного оборудования ... 18
9 Эксплуатация ... 19
9.1 Включение ... 19
9.2 Подключение по сети Ethernet ... 20
9.3 Конфигурация контроллера ... 20
9.4 Схемы идентификации ... 20
9.5 Принцип работы считывателя *EMM / HID* ... 21
9.6 Принцип работы считывателя *Mifare* ... 21
9.6.1 Особенности работы со смартфонами с функцией *NFC*: ... 22
9.6.2 Конфигурация считывателя *Mifare* ... 23
9.7 Порядок работы со сканером отпечатков пальцев ... 23
9.7.1 Принцип действия сканера отпечатка пальца ... 23
9.7.2 Порядок записи отпечатка пальца на карту Mifare ... 23
9.8 Обновление встроенного ПО ... 24
9.9 РКД при работе в СКУД ... 24
9.10 Индикация ... 24
10 Транспортирование и хранение ... 26
11 Техническое обслуживание ... 26
12 Диагностика и устранение неисправностей ... 27
12.1 Контроллер не работает ... 27
12.2 Нарушение связи с компьютером ... 27
Приложение 1. Инструкция по подключению контроллера через *PoE*-сплиттер ... 29
Приложение 2. Инструкция по подключению пирометра *PERCo-AT01* ... 30
Приложение 3. Настройка контроллера *CL15.1* для работы с картоприемником *IC05* ... 38
Приложение 4. *Web*-интерфейс контроллера *PERCo-CL15.1*. Руководство пользователя ... 40

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Уважаемые покупатели!

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

Руководство по эксплуатации биометрического контроллера со встроенным модулем сканера отпечатков пальцев и RFID-считывателем карт доступа *PERCo-CL15.1* (далее – *руководство*) содержит сведения по транспортированию, хранению, монтажу, эксплуатации и техническому обслуживанию указанного изделия. Монтаж и эксплуатация изделия должны проводиться лицами, полностью изучившими данное руководство, а также эксплуатационную документацию на используемую систему контроля и управления доступом (***PERCo-Web***, ***PERCo-S-20***, ***PERCo-S-20 «Школа»***) и на подключаемые к контроллеру устройства и оборудование.

Принятые сокращения:

ВВУ – внешнее верифицирующее устройство;
ИП – источник питания;
ИУ – исполнительное устройство;
РКД – режим контроля доступа;
СКУД – система контроля и управления доступом.

1 НАЗНАЧЕНИЕ

Биометрический контроллер со встроенным модулем сканера отпечатков пальцев и RFID-считывателем карт доступа *PERCo-CL15.1* (далее – *контроллер*) предназначен для организации одной односторонней точки прохода, одного направления двухсторонней точки прохода (при использовании двух контроллеров данной модели) или одного направления прохода для шлюза (при использовании четырех контроллеров данной модели). Контроллер позволяет управлять:

- одним односторонним электромеханическим или электромагнитным замком;
- одним направлением двухстороннего электромеханического (электромагнитного) замка;
- одним направлением турникета или калитки;
- одним направлением ИУ шлюза[1].

Примечание:

При использовании двух контроллеров ***PERCo-CL15.1*** для управления одним двухсторонним замком рекомендуется в качестве ИУ применять нормально закрытый (открывающийся при подаче напряжения) электромеханический замок. Электромагнитный или нормально открытый электромеханический замок в данной конфигурации возможно использовать только при дополнительной установке промежуточного реле.

Контроллер имеет встроенный сканер отпечатков пальцев и встроенный считыватель карт доступа форматов:

1. ***HID*** / ***EM-Marine***, обеспечивает считывание кода с идентификаторов Proximity с рабочей частотой 125 кГц производства HID Corporation типа ProxCard II, ISOProx II, брелоков ProxKey II (стандартных форматов HID: 26 бит (H10301), 37 бит (H10302, H10304)), а также производства *EM-Microelectronic-Marin SA* (далее - EMM);
2. ***MIFARE***, обеспечивает считывание:
   - при работе с картами MIFARE[2]:
     - либо уникального идентификатора (UID) с карты или транспондера MIFARE (заводская установка)[3];
     - либо данных из внутренней памяти карты или транспондера (применяется в случае, если требуется повышенный уровень безопасности, при этом требуется дополнительное программирование считывателя из ПО).

[1] Шлюз м.б. организован из различных ИУ – замков или турникетов.
[2] Поддерживаемые стандарты карт доступа MIFARE указаны в разделе 3.
[3] В том числе UID с платежных карт с технологией **PayPass**.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- при работе со смартфоном на ОС *Android* с функцией *NFC*:
  - уникального идентификатора, генерируемого приложением «**PERCo. Доступ**» на смартфоне (требуется установка и запуск приложения).
- при работе со смартфоном *Apple* с функцией *NFC*:
  - уникального идентификатора (Token), привязанного к банковской карте (при привязке нескольких банковских карт осуществляется считывание Token той карты, которая активна в данный момент).

Контроллер может использоваться как автономно, так и в качестве элемента системы контроля и управления доступом ***PERCo-Web***, а также в единой системе безопасности и повышения эффективности предприятия ***PERCo-S-20*** (***PERCo-S-20 «Школа»***). Управление контроллером и его конфигурация осуществляется посредством встроенного Web-интерфейса или сетевого ПО ***PERCo-Web, PERCo-S-20*** (***PERCo-S-20 «Школа»***).

2 УСЛОВИЯ ЭКСПЛУАТАЦИИ

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

Эксплуатация контроллера замка разрешается при температуре окружающего воздуха от -10°С до +40°С и относительной влажности воздуха до 80% при +25°С.

3 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Номинальное значение напряжения ИП постоянного тока, *В* ..... 12±1,2
Ток потребления, *А* ..... не более 0,4
Потребляемая мощность, *Вт* ..... не более 5
Типы используемых бесконтактных карт ..... *HID*, *EMM, MIFARE, PayPass,* смартфон с *NFC*
Возможность использования смартфонов с функцией *NFC* ..... да
Поддерживаемые стандарты карт доступа для карт MIFARE:
MIFARE Ultralight (48 byte), *MIFARE Ultralight EV1* (48 byte, 128 byte),
MIFARE Ultralight C (144 byte), *MIFARE ID* (64 byte), *MIFARE Classic 1K*,
MIFARE Classic 4K, *MIFARE Plus* (*X*, *S*, *SE*), *MIFARE DESFire Ev1*
Дальности считывания кода при номинальном значении напряжения ИП:
для карт *HID*, *мм* ..... не менее 25
для карт *EM-Marin*, *мм* ..... не менее 50
для карт *MIFARE*, *мм* ..... не менее 20
для смартфонов с *NFC* ..... от 2 до 6[1]
Число отпечатков для каждого пользователя ..... до 10
Количество карт для каждого пользователя ..... до 5
Максимальное количество пользователей:
со схемой идентификации «отпечаток» ..... не менее 5 000[2]
с другими схемами идентификации [3] ..... не менее 50 000
Количество отпечатков пальцев, которое возможно записать на карту[4] ..... не более 5
Максимальное число событий журнала регистрации ..... не менее 150 000
Количество контролируемых точек прохода 1
Количество входов ДУ 1
Количество дополнительных входов 1
Количество дополнительных выходов 1

[1] Зависит от производителя и модели смартфона.
[2] При условии назначения каждому пользователю в правах доступа не более одного или двух отпечатков.
[3] Со схемами идентификации «карта», «карта и (или) отпечаток» или «карта и отпечаток на карте». **Схема идентификации** – это один из параметров прав доступа сотрудника (посетителя), характеризующий вид идентификатора (комплекта идентификаторов), которым он должен воспользоваться для получения права на проход через точку доступа. Выбор схемы идентификации для конкретного пользователя производится в Web-интерфейсе контроллера.
[4] Зависит от наличия свободного места в памяти карты. Возможностью записи отпечатков пальцев обладают карты стандартов *MIFARE Classic 1K*, *MIFARE Classic 4K*, *MIFARE Plus* (*X*, *S*, *SE*), *MIFARE DESFire Ev1.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

Web-интерфейс ..... да
Стандарт интерфейса связи ..... *Ethernet* (IEEE 802.3)
Средний срок службы, *лет* 8
Класс защиты от поражения электрическим током ..... III по ГОСТ Р МЭК730-1-94
Степень защиты оболочки ..... IP50 по EN 60529
Габаритные размеры контроллера (без учета кабеля), *мм* ..... 170×70×51
Масса контроллера, *кг* ..... не более 0,3

Примечание:

При производстве контроллеру заданы: IP-адрес и MAC-адрес, которые указаны в паспорте и на тыльной стороне корпуса контроллера; маска подсети: 255.0.0.0; IP-адрес шлюза: 0.0.0.0.

4 КОМПЛЕКТ ПОСТАВКИ

4.1 Стандартный комплект поставки

Контроллер с металлическим основанием в сборе, *шт.* 1
Джампер-перемычка, *шт.* 1
Супрессор на 15 – 18 В, *шт.* 1
Дюбели пластмассовые, *шт.* 4
Шурупы, *шт.* 4
Паспорт, *экз.* 1
Руководство по эксплуатации, *экз.* 1

4.2 Дополнительное оборудование, поставляемое по отдельному заказу

Источник питания контроллера, *шт.* 1
PoE-сплиттер[1], *шт.* 1

5 ОПИСАНИЕ

5.1 Устройство и работа

Контроллер представляет собой блок электроники в пластмассовом корпусе, на передней панели которого расположены динамический цветной светодиодный индикатор, сканер отпечатков пальцев и обозначена область для предъявления карт доступа (см. рис. 1). Защита электроники от негативных воздействий окружающей среды обеспечивается за счет герметизирующей прокладки между элементами корпуса. Кабель связи для подключения к сети *Ethernet* и кабель для остальных подключений к контроллеру замка выведены с его тыльной стороны.

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

Контроллер имеет встроенный сканер отпечатков пальцев и один встроенный бесконтактный считыватель карт доступа: форматов *HID* / *EM-Marine* и *MIFARE*.

Контроллер обеспечивает связь по интерфейсу *Ethernet* (*IEEE 802.3*) с поддержкой стека протоколов *TCP/IP (ARP, IP, ICMP, TCP, UDP, DHCP)*, а также поддержку прикладного уровня протокола обмена систем ***PERCo-Web, PERCo-S-20*** (***PERCo-S-20 «Школа»***).

Контроллер обеспечивает управление любыми ИУ:

- при использовании одного контроллера - одним односторонним замком;
- при совместной работе двух контроллеров (с поддержкой смены зональности):
  - одним двухсторонним замком;
  - одним турникетом или калиткой;
- при совместной работе четырех контроллеров (с поддержкой смены зональности):
  - одним шлюзом, организованным из ИУ различного типа[2].

[1] *PoE*-сплиттер 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] Шлюз м.б. организован из любых двух двусторонних ИУ – замков или турникетов и настраивается при конфигурировании ИУ в Web-интерфейсе.

SEC.RU | Короткий путь к информации Скачано с sec.ru

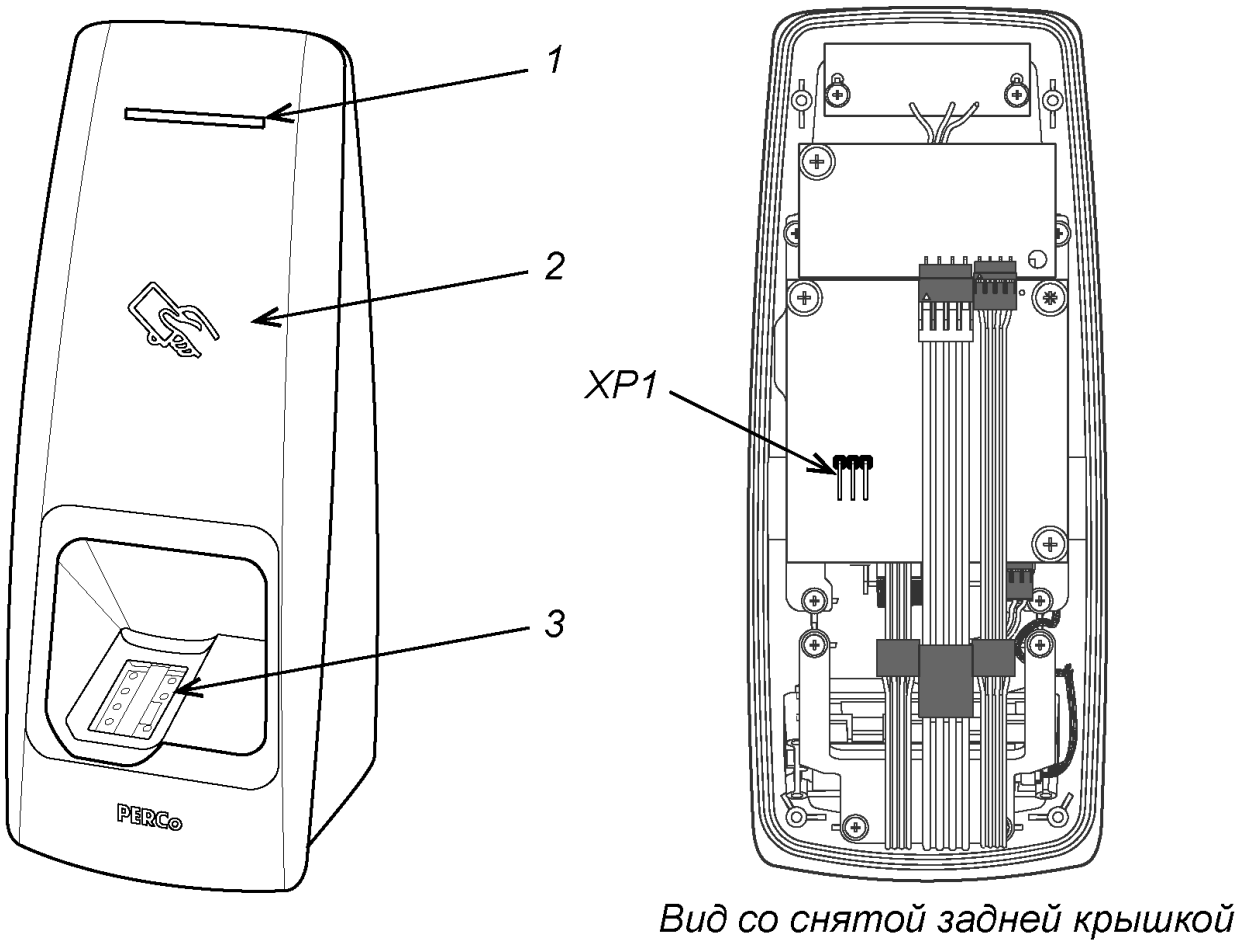


Рисунок 1. Внешний вид контроллера

1 – динамический цветной индикатор, 2 – область предъявления карт доступа, 3 – сканер отпечатков пальцев, ***XP1*** – перемычка выбора способа задания IP-адреса

При использовании электромеханических замков с контактной группой серии ***PERCo-LB*** (***PERCo-LBP***) контроллер отслеживает состояние цепи замка, что позволяет не использовать датчик двери (геркон), в его роли выступает контактная группа замка.

Контроллер позволяет осуществлять управление ИУ с помощью следующих устройств:

- кнопка ДУ (*«Выход»*);
- компьютер (при подключении по сети *Ethernet*);
- устройство аварийной разблокировки («*Fire Alarm*»);
- идентификатор, в роли идентификатора могут выступать:
  - карта доступа, при поднесении ее к считывателю контроллера;
  - палец, при прикладывании его к сканеру отпечатка пальцев;
  - комбинация карты доступа и пальца.

Кроме этого, возможно подключение следующего дополнительного оборудования:

- датчик двери (геркон) / вход PASS;
- дополнительный датчик (извещатель, ВВУ или устройство *FireAlarm*);
- внешний световой или звуковой (сирена) тревожный оповещатель.

Контроллер, как элемент СКУД обеспечивает:

- работу в РКД: *«Открыто»*, *«Контроль»*, *«Закрыто»*, *«Охрана»*;
- сохранение установленного РКД в энергонезависимой памяти, для предотвращения его смены при пропадании - восстановлении питания;
- поддержку функции глобального контроля зональности;
- поддержку функции комиссионирования;
- поддержку функции верификации;
- возможность постановки и снятия ИУ с охраны;
- передачу тревожных извещений на пульт централизованного наблюдения.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.2 Шаблоны конфигурации

Внимание!

- Смена шаблона конфигурации контроллера производится **только через *Web*-интерфейс контроллера** (см. Приложение 4, п. 4.1).
- При смене шаблона происходит удаление всей конфигурации и внутренних реакций всех ресурсов контроллера. Для ресурсов выбранного шаблона устанавливается конфигурация “по умолчанию”. При этом сохраняются загруженные идентификаторы карт доступа, связанные с ними данные пользователей, права и параметры доступа.

Для контроллера доступны следующие шаблоны конфигурации:

1. Замок, биометрический считыватель + считыватель *HID/EMM/Mifare* (по умолчанию).
2. Турникет, биометрический считыватель + считыватель *HID/EMM/Mifare*.

5.3 Параметры сигналов выхода управления ИУ

Контроллер имеет один выход управления ИУ: *Lock* (оранжевый провод). Тип выхода – открытый коллектор.

Выход используется для управления ИУ и имеет следующие параметры:

максимальное напряжение постоянного тока, *В* ..... не более 30
максимальный ток на время не более 30 секунд, *А* ..... не более 1[1]
максимальный ток на время более 30 секунд, *А* ..... не более 0,65

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

При **потенциальном** режиме работы ИУ:

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

При **импульсном** режиме работы ИУ:

- При реализации однократного прохода выход активизируется на время, определяемое параметром **Длительность импульса управления ИУ.** При этом ИУ разблокируется до момента совершения прохода.
- При установке ИУ в РКД *«Открыто»* выход активизируется на время, определяемое параметром **Длительность импульса управления ИУ**, после чего будет активизироваться каждый раз на это же время через 1 секунду после нормализации ИУ.

Фактом совершения прохода служит активизация входа *Door* при использовании датчика двери (геркона). При использовании замков с контактной группой серии ***PERCo-LB*** (***LBP***) фактом совершения прохода служит разрыв цепи через контактную группу замка.

5.4 Параметры сигналов входов Door, DU и In

Контроллер обеспечивает контроль состояния трех входов: *Door* (белый провод), *DU* (зеленый провод) и *In* (синий провод). Схема подключения представлена на рис. 3. Входы могут использоваться:

- *Door* – для подключения датчика двери (геркона) / выхода PASS турникета, калитки;
- *DU* – для подключения кнопки ДУ (*«Выход»*).
- *In* – для подключения дополнительного датчика (например: извещателя, устройства *Fire Alarm* или ВВУ).

Управляющим элементом могут быть нормально разомкнутый контакт реле или схема с открытым коллекторным выходом. Управляющий элемент должен обеспечивать следующие характеристики сигналов:

[1] Если максимальный ток выхода будет составлять более 1 А (или 0,65-1 А в течение более 30 секунд), то необходимо использование промежуточного реле, Пример подключения замка через промежуточное реле представлен на рис. 6 (промежуточное реле на схеме обозначено, как Р1).

SEC.RU | Короткий путь к информации Скачано с sec.ru

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.

Примечание:

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

Факт активизации для сигналов *Door* и *In* зависит от описания их исходного состояния в параметре **Нормальное состояние контакта** в ПО:

- 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.

При использовании замков с контактной группой серии ***PERCo-LB (PERCo-LBP)*** установка геркона и подключение входа *Door* не требуется. В роли датчика двери выступает контактная группа замка. Факт активизации осуществляется разрывом цепи через контактную группу, поэтому для параметра **Нормальное состояние контакта** в ПО должно быть установлено значение **Замкнут**.

Вход *DU* является «нормально разомкнутым» (его исходное состояние не описывается в ПО), поэтому его активизация осуществляется подачей на него сигнала низкого уровня относительно контакта *GND*.

5.5 Параметры сигналов дополнительного выхода

Контроллер имеет один дополнительный выход (коричневый провод), который может использоваться для:

- подключения внешнего светового или звукового (сирены) тревожного оповещателя,
- передачи тревожных извещений на пульт центрального наблюдения,
- подключения другого дополнительного оборудования.

Тип выхода – «открытый коллектор». Параметры сигналов выхода:
максимальное напряжение постоянного тока, *В* ..... не более 12
максимальный ток, *А* ..... не более 0,25

5.6 Выбор способа задания IP-адреса

Внимание!

Задание способа изменения IP-адреса контроллера осуществляется при установленной перемычке без выключения питания.

Выбор способа задания IP-адреса контроллера осуществляется установкой или снятием перемычки (джампера) на разъем ***XP1*** на печатной плате, расположенной под задней крышкой корпуса контроллера. Для снятия крышки необходимо тонкой длинной отверткой PH1-50 мм открутить четыре шурупа. Расположение разъема ***XP1*** указано на рис. 1. 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, контроллер сразу начинает работать с параметрами, заданными пользователем (без переключения питания).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Примечание:

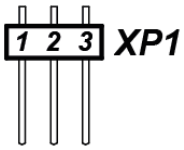
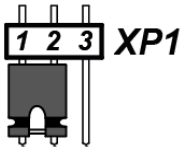
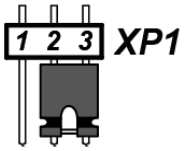
Заводские установки контроллера: IP-адрес и MAC-адрес указаны в паспорте и на задней крышке контроллера; маска подсети 255.0.0.0; IP-адрес шлюза 0.0.0.0. Конфигурация в «ручном» режиме должна производиться в подсети, в которой расположен сервер системы.

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).
   - Доступ к контроллеру осуществляется без пароля. При установке перемычки в режим *«IP DEFAULT»* появляется возможность изменить пароль.

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	Способ задания IP-адреса
1		«Ручной» режим
2		«IP MODE»
3		«IP DEFAULT»

6 МАРКИРОВКА И УПАКОВКА

Контроллер имеет маркировку в виде этикетки, расположенной на тыльной стороне корпуса. На этикетке нанесены наименование, серийный номер и дата изготовления изделия.

Кроме того, на тыльной стороне корпуса контроллера находятся наклейки, на которых указаны установленные при производстве MAC – адрес и IP – адрес контроллера.

Контроллер упакован в картонную коробку, предохраняющую его от повреждений во время транспортировки и хранения.

7 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

7.1 Безопасность при монтаже

Монтаж и техническое обслуживание контроллера должны проводиться лицами, полностью изучившими настоящее руководство. Монтаж контроллера должен производиться специалистом-электромонтажником.

Внимание!

- Все подключения и установка перемычек должны производиться только при выключенном оборудовании, отключенных ИП.
- При монтаже контроллера пользуйтесь только исправным инструментом.

Требования безопасности при монтаже ИП указаны в эксплуатационной документации ИП.

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.2 Безопасность при эксплуатации

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

Запрещается!

- Эксплуатировать контроллер при напряжении ИП, не соответствующем указанному в разд. 3 *«Основные технические характеристики»*.
- Эксплуатировать контроллер в условиях, не соответствующих требованиям разд. 2 *«Условия эксплуатации»*.

Требования безопасности при эксплуатации ИП указаны в его эксплуатационной документации.

8 МОНТАЖ

При монтаже соблюдайте меры безопасности, указанные в разд. 7.1.

8.1 Общие указания

Контроллер рекомендуется монтировать в непосредственной близости от ИУ. Точная высота для монтажа контроллера должна выбираться, исходя из соображения удобства для прикладывания пальцев к сканеру и предъявления карт доступа.

Установка контроллера на металлическую поверхность и за нее **не допускается!**

Взаимное удаление контроллеров друг от друга и от считывателей должно составлять не менее 50 см.

8.2 Кабели

При монтаже контроллера используйте кабели, указанные в табл. 2.

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;
- 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.**

Таблица 2. Типы кабелей, используемые при монтаже

№.	Подключаемое оборудование	Макс. длина, м	Тип	Мин. сечение провода, мм^2	Пример
1	Ethernet (IEEE 802.3)	100	Четыре витые пары не ниже пятой категории	0,22	
2	ИП	10	Двужильный кабель	0,75	ШВВП (2×0,75 двухцветный)
3	ИУ – Замок	10			
	ИУ – Турникет	30	Шестижильный кабель	0,22	CQR CABS6 6x0,22c
4, 5, 6, 7	Кнопка ДУ, датчик двери, дополнительное оборудование (к входу и к выходу контроллера)	10	Двужильный кабель	0,22	RAMCRO SS22AF-T (2×0,22) или CQR-2

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.3 Последовательность монтажа

Подключение к контроллеру осуществляется согласно схемам, представленным на рис. 3 - 10. Используемые типы кабелей указаны в табл. 3.

Монтаж подключаемых к контроллеру устройств (турникетов, замков, блоков питания и т.п.) производится согласно инструкциям, приводимым в технической документации соответствующих изделий.

8.3.1 Монтаж контроллера

1. Распакуйте коробку и проверьте комплектность контроллера, согласно разд. 4. Убедитесь в отсутствии на изделии механических повреждений.
2. Определите место установки контроллера. При выборе места установки следуйте указаниям разд. 8.1.
3. Произведите разметку и разделку отверстий на установочной поверхности для крепления металлического основания и прокладки кабелей (см. рис. 2).

Примечание:

Отверстие для вывода соединительных кабелей должно иметь диаметр не меньше 27 мм для свободного прохода через него разъема контроллера *Ethernet*. При необходимости разъем можно обрезать и осуществить соединение кабелей *Ethernet* при помощи пайки, в этом случае не забудьте отметить цвета проводов кабеля контроллера (как правило, желтый Tx+, зеленый Tx-, красный Rx+ и черный Rx-, но возможно использование и других цветов жил кабеля).

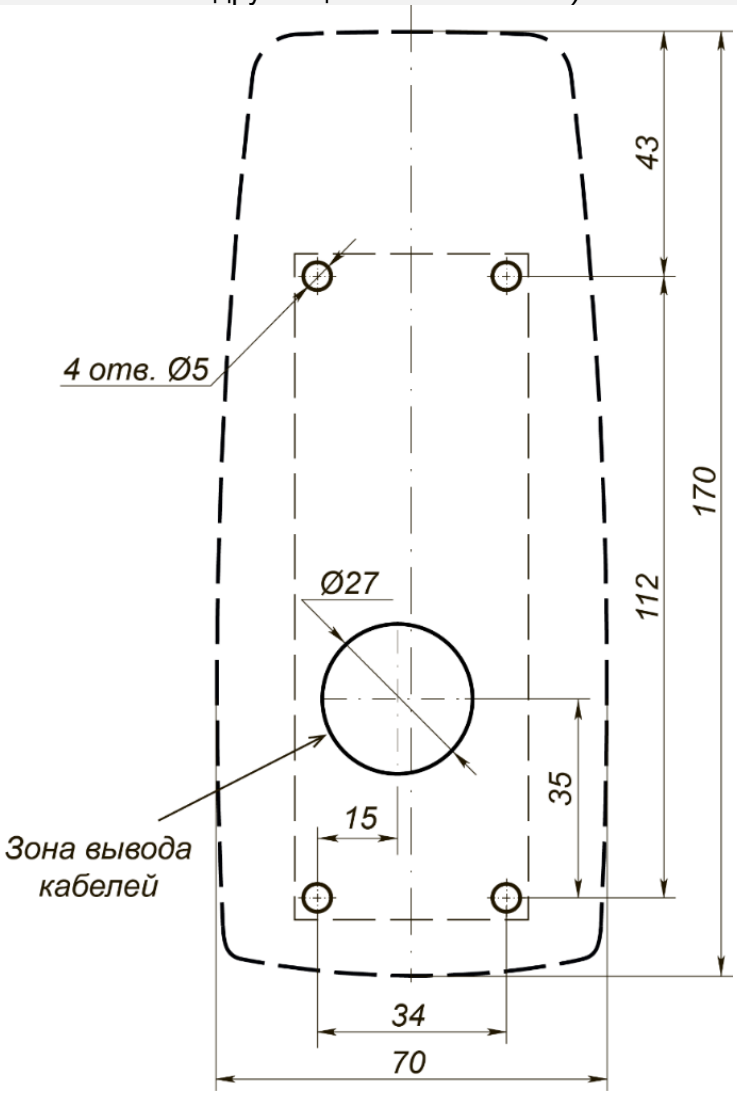


Рисунок 2. Разметка отверстий для установки контроллера (пунктиром показаны габариты корпуса контроллера)

SEC.RU | Короткий путь к информации Скачано с sec.ru

4. Ослабьте винт, расположенный в нижней части корпуса контроллера и крепящий его к металлическому основанию. Снимите основание.
5. Закрепите металлическое основание на установочной поверхности с помощью четырех шурупов из комплекта поставки.
6. При необходимости изменения способа задания IP-адреса контроллера (см. разд. 5.6) открутите четыре винта, крепящие заднюю крышку к корпусу контроллера, аккуратно отодвиньте ее и установите перемычку (джампер) на разъем ***XP1*** согласно табл. 1. Расположение перемычки указано на рис. 1. После чего прикрутите винтами заднюю крышку к корпусу контроллера.
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 перемычки, поэтому рекомендуется оставлять запас длины кабелей, выходящих из контроллера, достаточный для отведения его от стены и обеспечения доступа к перемычке.
8. Установите контроллер на металлическое основание и закрепите на нем с помощью винта, расположенного в нижней части корпуса контроллера.
9. Подключите остальное необходимое оборудование. Следуйте рекомендациям по подключению:
   - электромеханических (электромагнитных) замков (защелок), см. разд. 8.3.2;
   - при совместной работе двух контроллеров подключение[1]:
     - турникета или калитки (см. разд. 8.3.3);
     - ПДУ (устройства РУ) (см. разд. 8.3.4);
   - другого дополнительного оборудования, в том числе устройства аварийной разблокировки (аварийного открытия прохода) *Fire Alarm* (см. разд. 8.3.5).

Примечание:

Порядок подключения внешних верифицирующих устройств к контроллеру на примере подключения алкотестера описан в Приложении 1.

8.3.2 Подключение замка

При подключении к контроллеру замка (защелки) придерживайтесь следующих рекомендаций:

1. Для снятия статического электричества рекомендуется заземлить корпус или запорную планку замка. В случае установки замка на металлическую дверь, рекомендуется заземлять полотно двери. Заземление выполняется проводом с сечением не менее 0,75 мм^2.

Внимание!

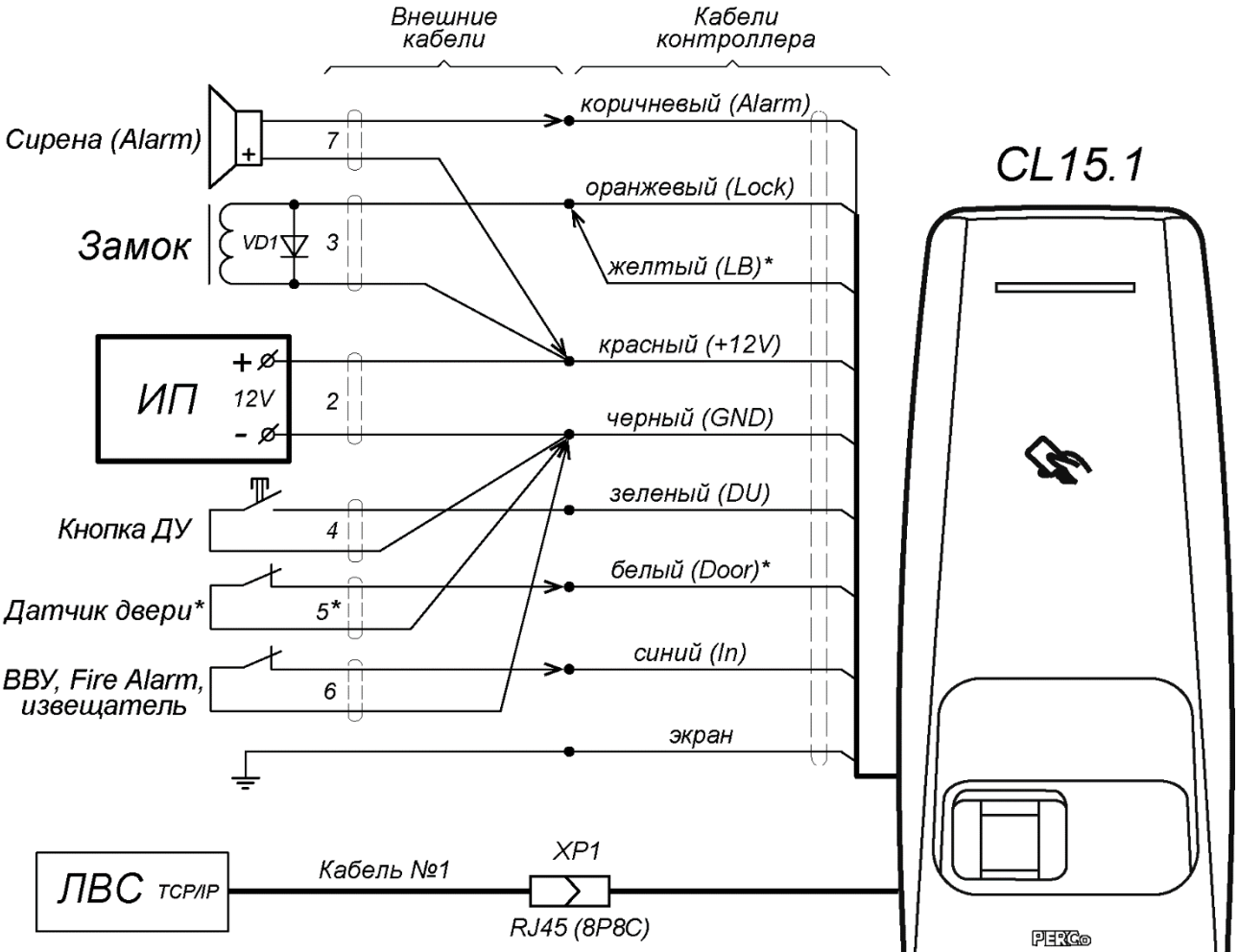
- Если подключаемый *замок не имеет встроенной цепи искрозащиты,* то необходимо использовать диод искрозащиты (***VD1*** на рис. 3-5). Например, диод Шоттки, рассчитанный на рабочий ток не менее 1*А*, типа 1N5819, вместо диода можно поставить двунаправленный супрессор из комплекта поставки.
- Если подключаемый электромагнитный *замок не имеет размагничивающей цепи*, то необходимо установить двунаправленный супрессор из комплекта поставки. Супрессор устанавливается в непосредственной близости от замка (***VD1*** на рис. 6).
- При подключении контроллера через *PoE*-сплиттер (см. рис. 15 в Приложении 1) рекомендуется использовать только электромеханические замки, поэтому необходимо использовать именно диод искрозащиты типа 1N5819. Во избежание выхода из строя PoE-сплиттера использование супрессора в этом случае **не рекомендуется!**

2. Произведите разделку двери и монтаж замка (защелки) в соответствии с их эксплуатационной документацией. Подключите кабель №3 (см. рис. 3, табл. 2) к замку (защелке).

[1] Шлюз организуется из двух независимых двусторонних ИУ.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Установите кнопку ДУ (*«Выход»*). Место для монтажа кнопки ДУ должно выбираться, исходя из соображения удобства ее (например, рядом с дверью). Подключите кабелем №6 (см. рис.3, табл. 2) к кнопке ДУ.
4. При необходимости произведите монтаж магнитного датчика двери (геркона). При установке магнитный датчик должен быть закреплен на дверной коробке, а магнит – на двери таким образом, чтобы при закрытой двери обеспечивалось устойчивое замыкание контакта датчика. Подключение производится кабелем №7 (см. рис.3, табл. 2). В случае использования замка с контактной группой серии ***PERCo-LB*** (***LBP***) установка геркона не требуется, в этом случае в роли датчика двери выступает контактная группа замка. Вход *Door* контроллера в этом случае должен оставаться не подключенным.



* - *при использовании замков с контактной группой серии PERCo-LB (LBP):*
1) датчик двери не устанавливать, белый провод не подключать,
2) подключить желтый провод к оранжевому

Рисунок 3. Схема подключений *PERCo-CL15.1* для управления односторонним замком

5. При необходимости совместной работы двух контроллеров для обслуживания двухсторонней двери, произведите монтаж и подключение второго контроллера. Схема подключения представлена на рис. 4-6. Подключение производится параллельно по цветам проводов (не показано подключение кнопки ДУ, она в этом случае, как правило, не используется), а также сирены и устройства к входу *In* – при необходимости они могут подключаться по отдельности к любому из контроллеров по схеме на рис. 3. Синхронизация работы двух контроллеров производится по *Ethernet.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

Примечание:

При использовании двух контроллеров ***PERCo-CL15.1*** для управления одним двухсторонним замком рекомендуется в качестве ИУ применять нормально закрытый (открывающийся при подаче напряжения) электромеханический замок. Электромагнитный или нормально открытый электромеханический замок в данной конфигурации возможно использовать только при дополнительной установке промежуточного реле. Пример подключения замка через промежуточное реле представлен на рис. 6 (промежуточное реле на схеме обозначено, как Р1).

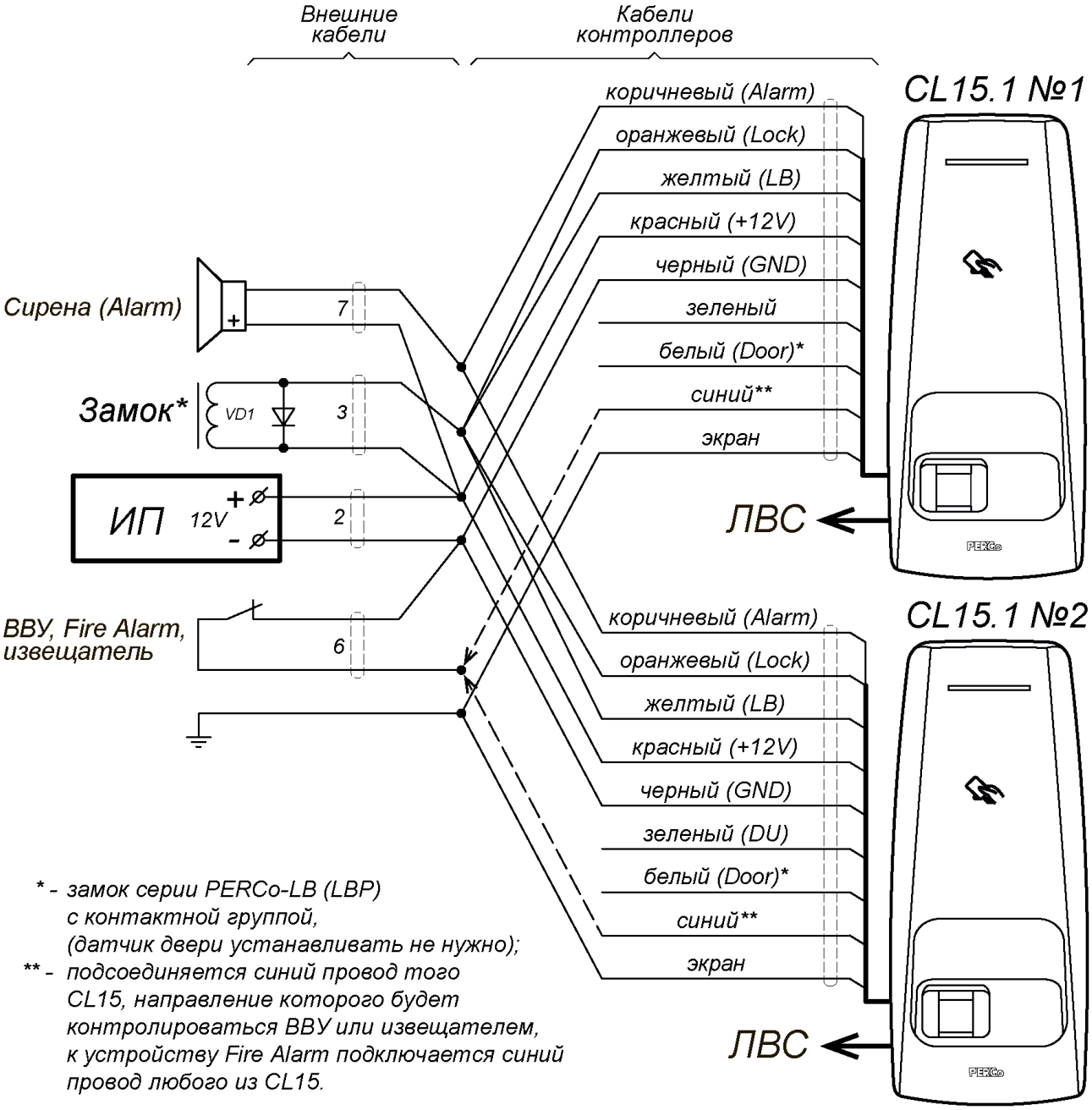


Рисунок 4. Схема параллельного подключения двух контроллеров *PERCo-CL15.1* для управления двусторонней дверью, оборудованной замком с контактной группой типа *PERCo-LB (LBP)* [1]

[1] Электромагнитный или нормально открытый электромеханический замок в данной конфигурации возможно использовать только при дополнительной установке промежуточного реле. Пример подключения замка через промежуточное реле представлен на рис. 6 (промежуточное реле на схеме обозначено, как Р1).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

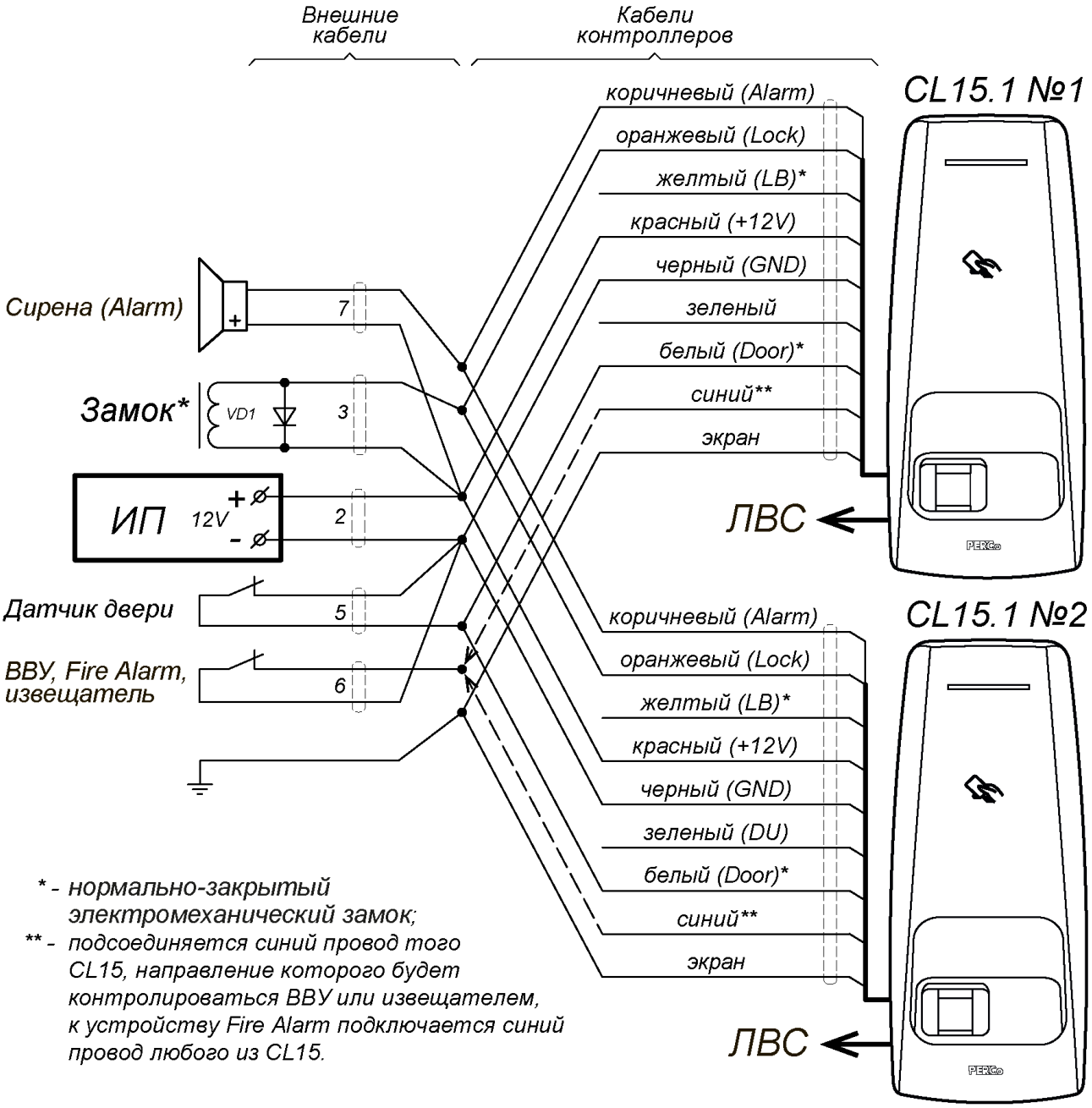


Рисунок 5. Схема параллельного подключения двух контроллеров *PERCo-CL15.1* для управления двусторонней дверью, оборудованной нормально закрытым электромеханическим замком

SEC.RU | Короткий путь к информации
Скачано с sec.ru

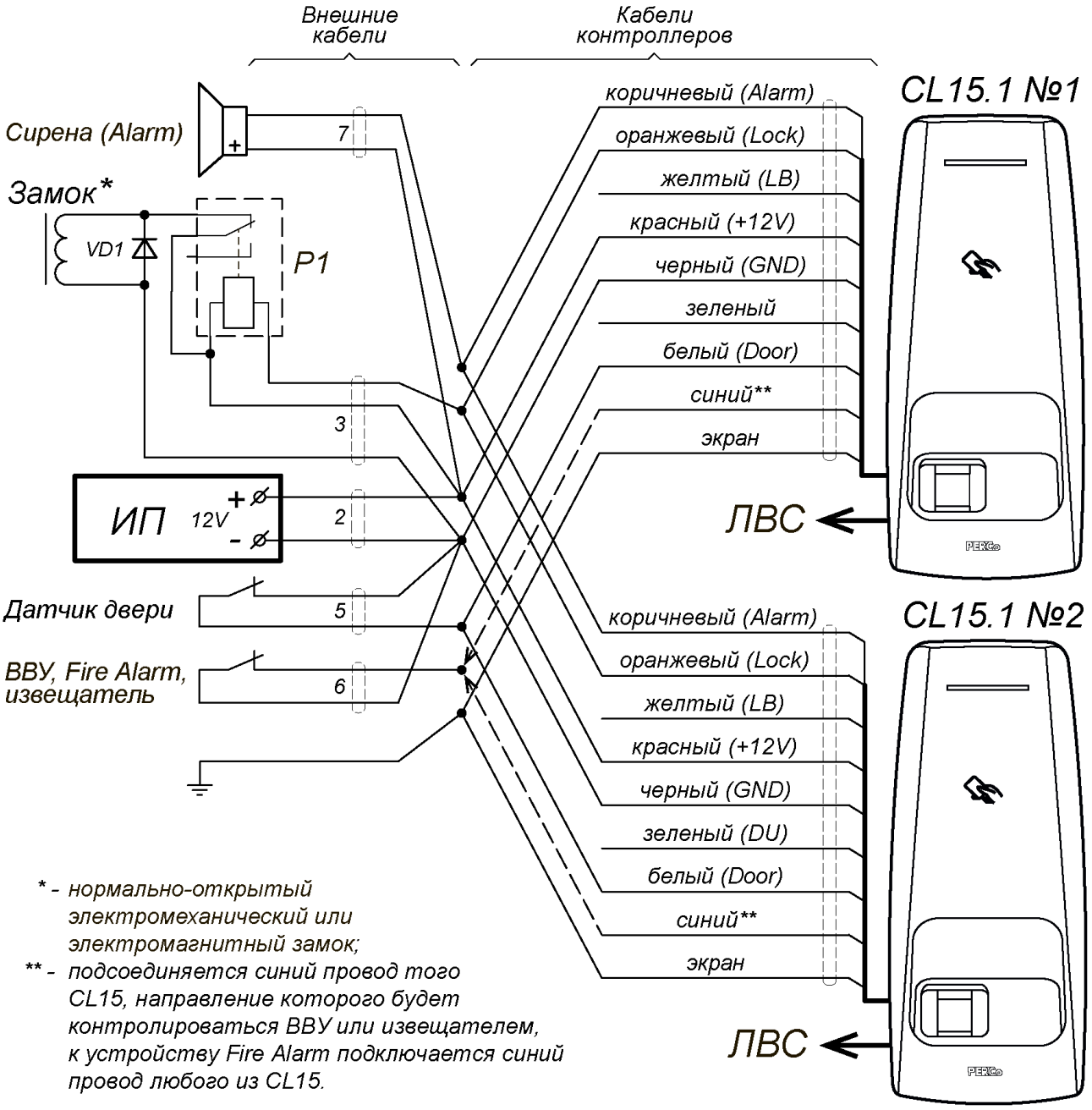


Рисунок 6. Схема параллельного подключения двух контроллеров для управления двусторонней дверью, оборудованной нормально открытым электромеханическим или электромагнитным замком[1]

[1] Промежуточное реле P1 в комплект поставки контроллера не входит, подбирается инсталлятором.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8.3.3 Подключение турникетов и электромеханических калиток

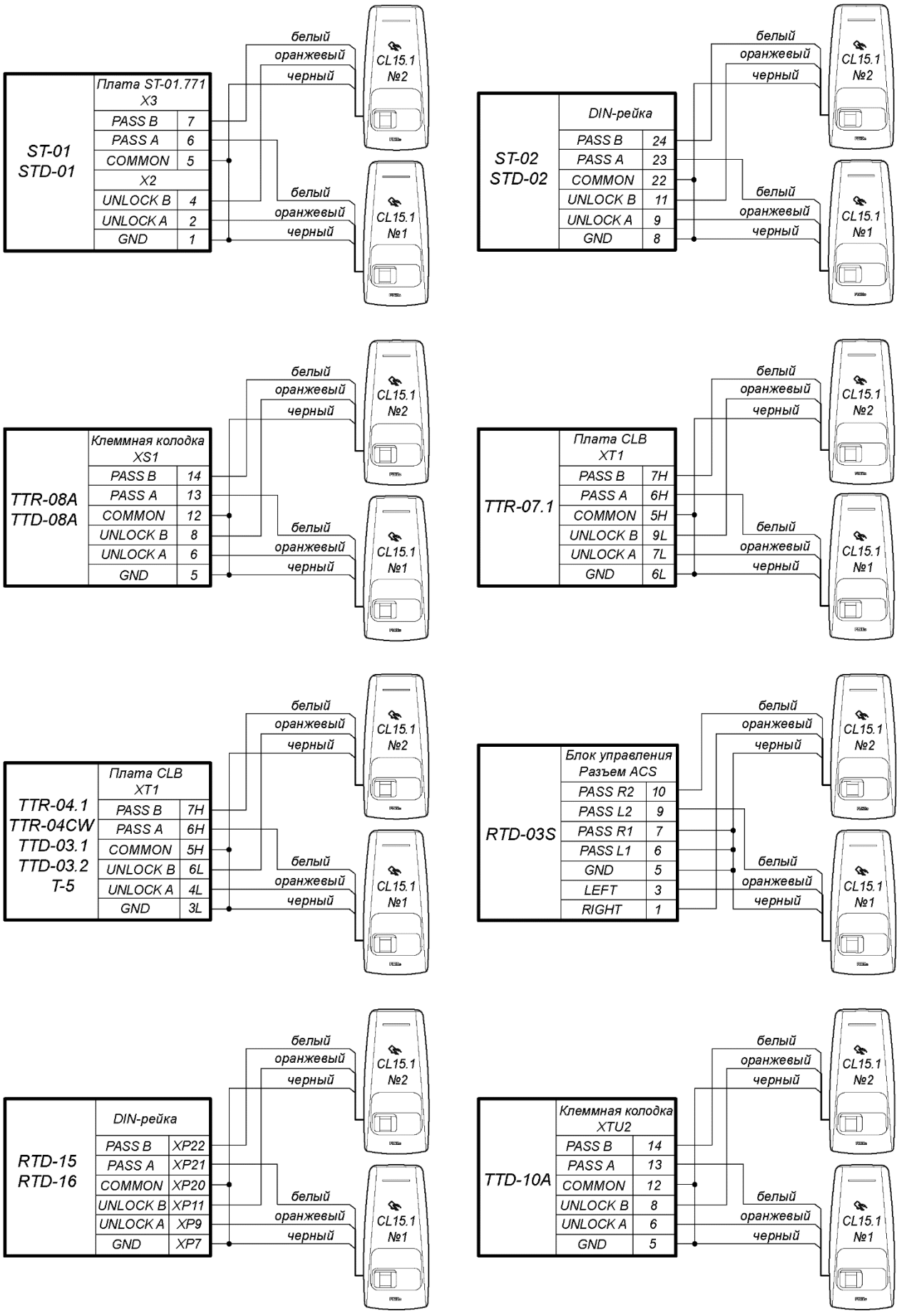


Рисунок 7. Схемы подключений турникетов

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Примечание:

В ПО систем ***PERCo-Web, PERCo-S-20*** (***PERCo-S-20 «Школа»***) для ресурса ИУ:

- Для турникетов производства ***PERCo*** параметр ИУ **Режим работы выхода управления** должен быть установлен в значение **Потенциальный**.
- Для калиток ***PERCo-WMD-05Sx*** и ***PERCo-WMD-06*** установите флажок параметра ИУ **Регистрация прохода по предъявлению идентификатора**.

При совместной работе двух контроллеров при подключении турникета (калитки) придерживайтесь следующих рекомендаций:

1. Для снятия статического электричества рекомендуется заземлить корпус турникета (калитки). Заземление выполнять проводом с сечением не менее 0,75 мм^2.
2. ПДУ (или устройство РУ) подключается согласно схеме, представленной на рис. 9.
3. Подключаемые ИУ д.б. переведены в потенциальный режим управления (см. инструкции на соответствующие ИУ).
4. Калитки ***PERCo-WHD-15*** и ***PERCo-WHD-16*** должны подключаться только через промежуточное реле (см. рис. 6).

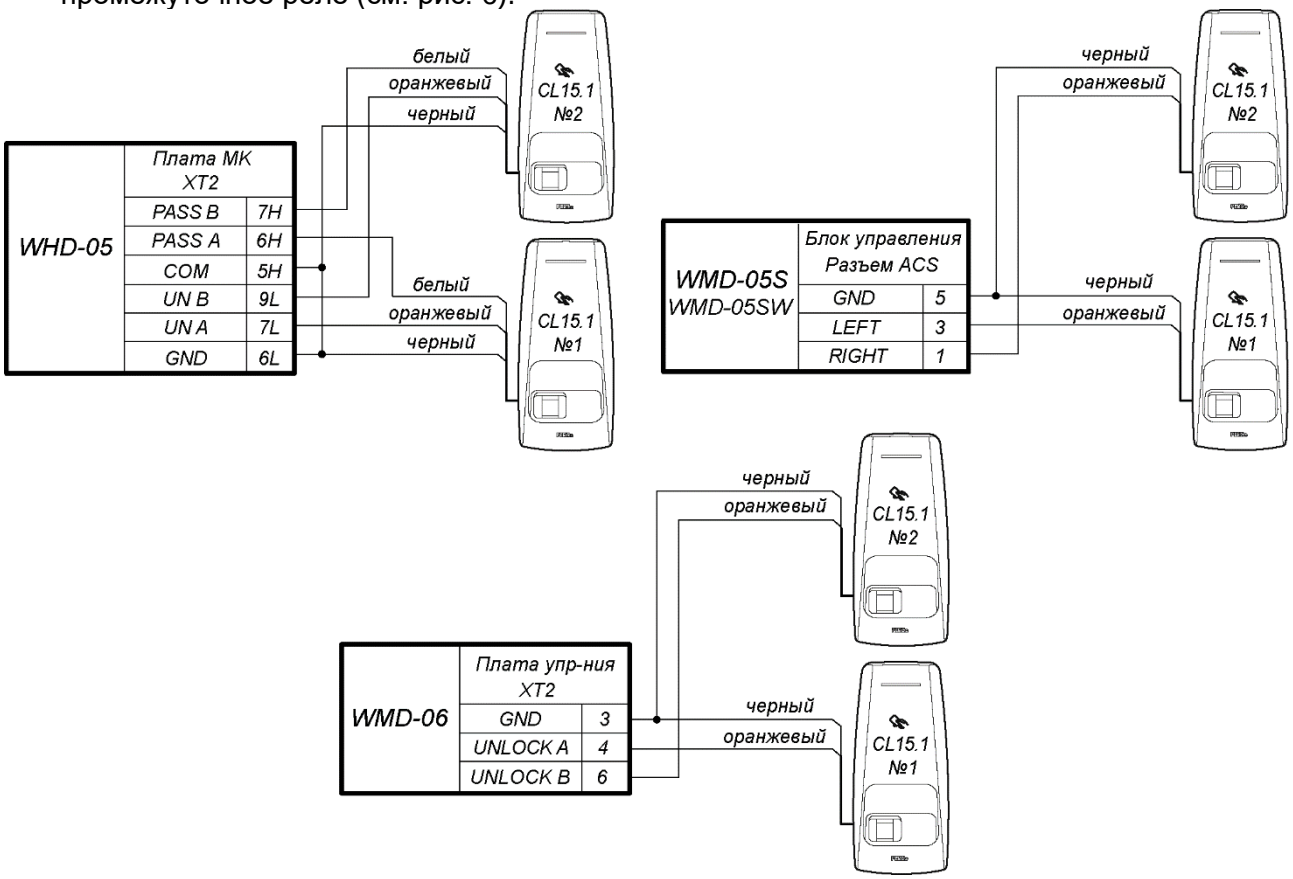


Рисунок 8. Схемы подключений калиток

8.3.4 Подключение ПДУ

При совместной работе двух контроллеров обеспечивается возможность подключения ПДУ для управления турникетом или калиткой. Для подключения ПДУ используются по 2 входа на каждом контроллере: *DU* и *In* (подключение осуществляется согласно схеме на рис. 9, при этом входы *In* обоих контроллеров д.б. сконфигурированы в *Web*-интерфейсе контроллера как *Кнопка ПДУ, направление 3*). Управление индикацией ПДУ (*Индикаторы Левый/Стоп/Правый и Зуммер)* возможно только для ИУ производства PERCo, при этом подключение осуществляется к соответствующим выходам платы CLB – см. схемы подключения ПДУ для соответствующих ИУ.

Входы ПДУ в данных конфигурациях контроллера активизируются подачей на них сигналов низкого уровня (нормально разомкнутый контакт) относительно контакта *GND*. Параметры сигналов, которые могут использоваться для подключения ПДУ, указаны в разд. 5.4.

SEC.RU | Короткий путь к информации Скачано с sec.ru

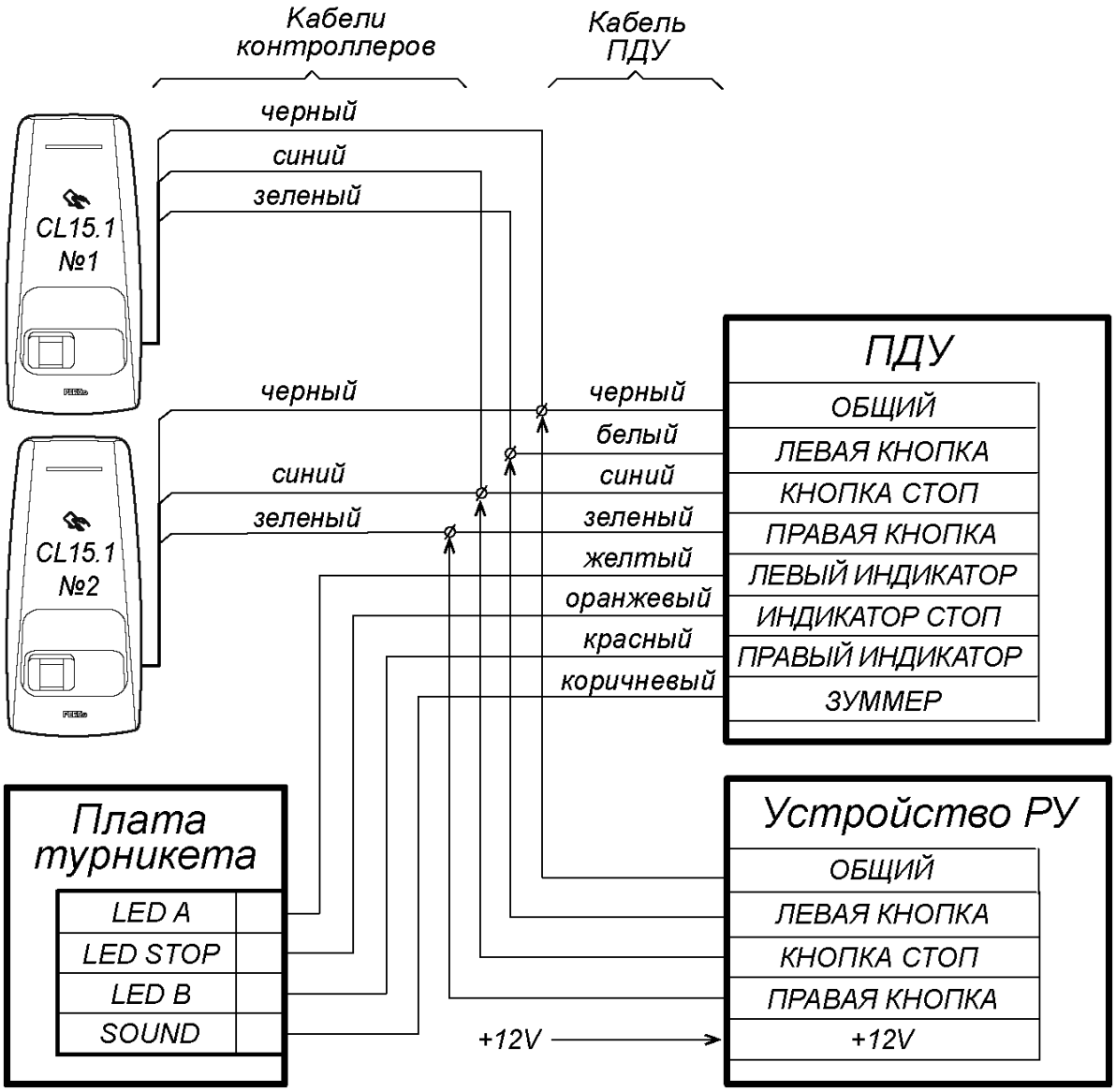


Рисунок 9. Схема подключения ПДУ и устройства РУ

8.3.5 Подключение дополнительного оборудования

1. Подключите кабели от устройств к штатному кабелю контроллера согласно схемам, на рис. 3 - 9.
2. Смонтируйте при необходимости дополнительное оборудование (например, датчик *FireAlarm,* ВВУ, сирену и т.д.). Подключите кабели №6 и №7 (см. рис. 3 и 10, табл. 2) к дополнительному оборудованию.
3. Подключите кабель *Ethernet*, выходящий из контроллера к локальной сети.
4. Установите ИП на место его постоянной эксплуатации. Подключите кабель №2 (см. рис. 3, табл. 2) к ИП и контроллеру.
5. 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 разд. 8.2.
6. Проверьте отсутствие обрывов и коротких замыканий во всех линиях.

Пример подключения алкотестера, как верифицирующего устройства, представлен на рис. 10. Вход контроллера *In* должен быть сконфигурирован как «Вход подтверждения от ВВУ». Тип выхода *Alarm* – «Обычный», и для него необходимо будет сконфигурировать внутреннюю реакцию контроллера – «Запрос на верификацию → Активизация выхода».

SEC.RU | Короткий путь к информации Скачано с sec.ru

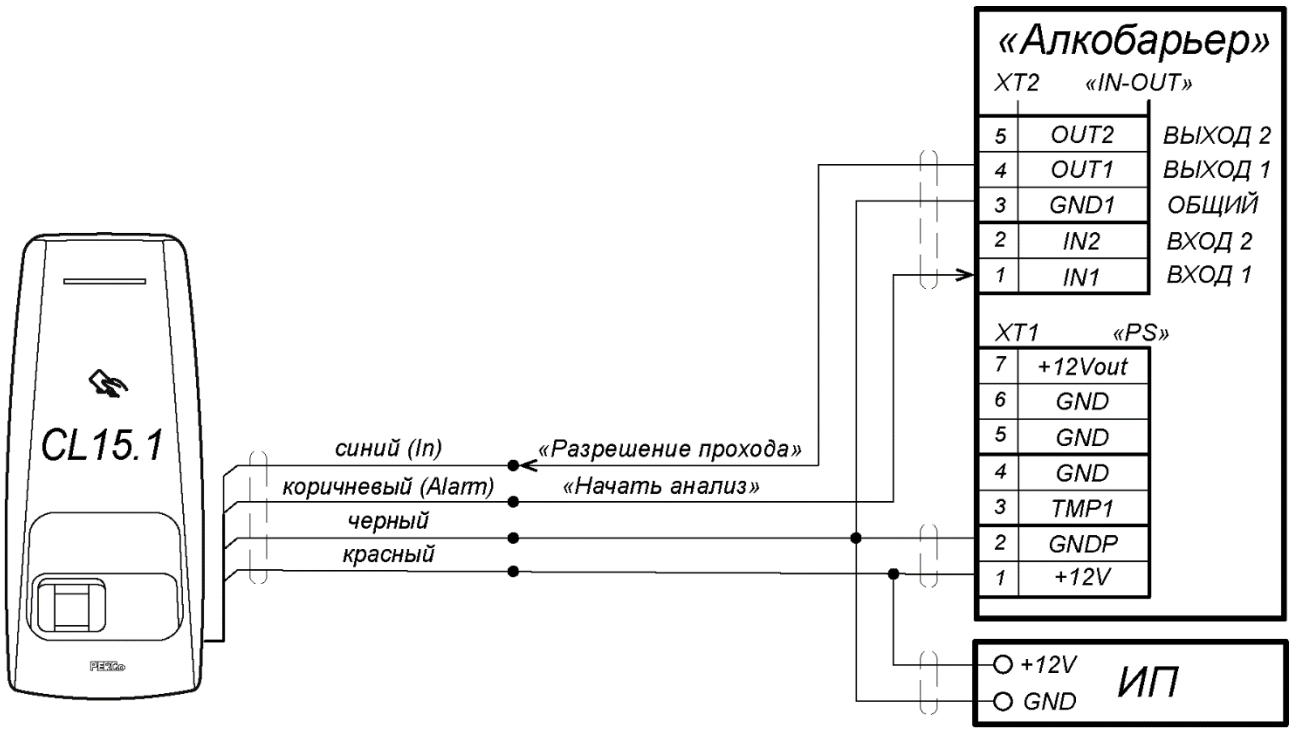


Рисунок 10. Схема подключения ВВУ на примере алкотестера

Примечания:

Подключение контроллера через *PoE*-сплиттер см. в Приложении 1.

Подключение к контроллеру пирометра ***PERCo-AT01*** см. в Приложении 2.

Подключение к контроллеру картоприемника ***PERCo-IC05*** см. в Приложении 3.

С помощью ПО ***PERCo-Web*** возможно подключение алкотестера «Алкобарьер» по интерфейсу *Ethernet* (при наличии Ethernet-модуля в алкотестере).

В случае возникновения пожара или других нештатных ситуаций предусмотрена возможность автоматической разблокировки (открытия прохода) ИУ, подключенного к контроллеру, за исключением ИУ, которое находится в РКД *«Охрана»* (возможность аварийной разблокировки настраивается при конфигурации).

Аварийная разблокировка (аварийное открытие прохода) исполнительного устройства производится по команде устройства аварийной разблокировки (аварийного открытия прохода) *Fire Alarm.* Устройство *Fire Alarm* подключается к входу контроллера *In – GND*, сконфигурированному, как вход *FireAlarm*. Параметры для сигнала *FA* указаны в разд. 5.4. При подаче управляющего сигнала на вход *In* контроллер переводится в режим *Fire Alarm*. В этом режиме подключенный ИУ разблокируется (открывается) для прохода. Другие команды управления при этом игнорируются.

9 ЭКСПЛУАТАЦИЯ

При эксплуатации ЭП соблюдайте меры безопасности, указанные в разд. 7.2.

Запрещается!

- 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.

9.1 Включение

При включении ИП световой индикатор на корпусе контроллера замка не будет гореть в течение примерно 15 секунд. После окончания этого времени на индикаторе контроллера отобразится индикация последнего установленного РКД.

SEC.RU | Короткий путь к информации Скачано с sec.ru

9.2 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.

9.3 Конфигурация контроллера

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

- Сетевое **ПО *PERCo-Web***;
- Сетевое ***«Базовое ПО S-20» PERCo-SN01*** (***PERCo-SS01 «Школа»***);
- Сетевое ***«Расширенное ПО S-20» PERCo-SN02*** (***PERCo-SS02 «Школа»***).

Дополнительное ПО Вы можете приобрести у официальных дилеров компании PERCo. Также указанное ПО, порядок его лицензирования и электронные версии руководств пользователя на ПО доступны на сайте компании PERCo http://www.perco.ru в разделе **Поддержка > Программное обеспечение**.

После проведения конфигурации контроллер может работать в следующих режимах:

1. **Без подключения к серверу СКУД (системы безопасности)**

Без подключения к сети *Ethernet* и к ПК контроллер выполняет следующие функции:

- Принимает идентификаторы: от одного из встроенных считывателей номера предъявленных карт и от встроенного сканера отпечатков свертки отпечатков приложенных пальцев и в зависимости от наличия их в списке, хранящемся в памяти контроллера, разрешает или запрещает доступ.
- Управляет подключенным ИУ.
- Ставит и снимает ИУ типа «замок» с охраны; контролирует ИУ в РКД *«Охрана»*.
- Активизирует перекрестные ссылки.
- Фиксирует события в журнале регистрации событий в памяти контроллера.
- Поддерживает функции контроля прохода по времени и комиссионирования.
- Поддерживает верификацию от кнопки ДУ и от ВВУ.

При подключении к сети и обеспечении связи с другими контроллерами системы становится доступной функция глобального контроля зональности и синхронизация двух контроллеров при работе на одно ИУ.

2. **С подключением к серверу СКУД (системы безопасности)**

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

- Данные из журнала событий автоматически переносятся в базу данных на сервере системы безопасности.
- Данные владельцев (ФИО) идентификаторов хранятся в базе данных программы.
- Функция верификации от ПО доступна в зависимости от установленных модулей сетевого ПО.

9.4 Схемы идентификации

Схема идентификации – это основной параметр прав доступа сотрудника (посетителя), характеризующий вид идентификатора (комплекта идентификаторов), которым он должен воспользоваться для получения права на проход через точку доступа. Выбор схемы

SEC.RU | Короткий путь к информации Скачано с sec.ru

идентификации для каждого конкретного пользователя производится в *Web*-интерфейсе контроллера в разделе ***Доступ*** → ***Пользователи***.(Приложение 4).

Данный параметр в контроллере ***PERCo-CL15.1*** может иметь следующие значения:

- схема идентификации **"карта"** – проход осуществляется по предъявлению только карты или смартфона;
- схема идентификации **"карта и отпечаток"** – проход осуществляется по предъявлению сначала карты или смартфона, затем отпечатка пальца;
- схема идентификации **"карта или отпечаток"** – проход осуществляется по предъявлению либо карты (смартфона), либо отпечатка пальца;
- схема идентификации **"карта и отпечаток на карте"** – проход осуществляется по предъявлению сначала карты с предварительно записанными на нее (см. разд. 9.7.2) отпечатками пальцев, а затем отпечатка пальца из списка записанных на карте.

9.5 Принцип работы считывателя *EMM / HID*

Считыватели *EMM/HID* обеспечивают считывание кода с идентификаторов Proximity с рабочей частотой 125 кГц производства HID Corporation типа ProxCard II, ISOProx II, брелоков ProxKey II (стандартных форматов HID: 26 бит (H10301), 37 бит (H10302, H10304)), а также производства *EM-Microelectronic-Marin SA*.

Считывание кода происходит при поднесении идентификатора к считывателю. При этом идентификатор может находиться в кармане, в бумажнике или в любом другом радиопрозрачном контейнере (футляре).

Предельное расстояние, на котором считывателем обеспечивается считывание идентификаторов, зависит от типа идентификатора (см. разд. 3).

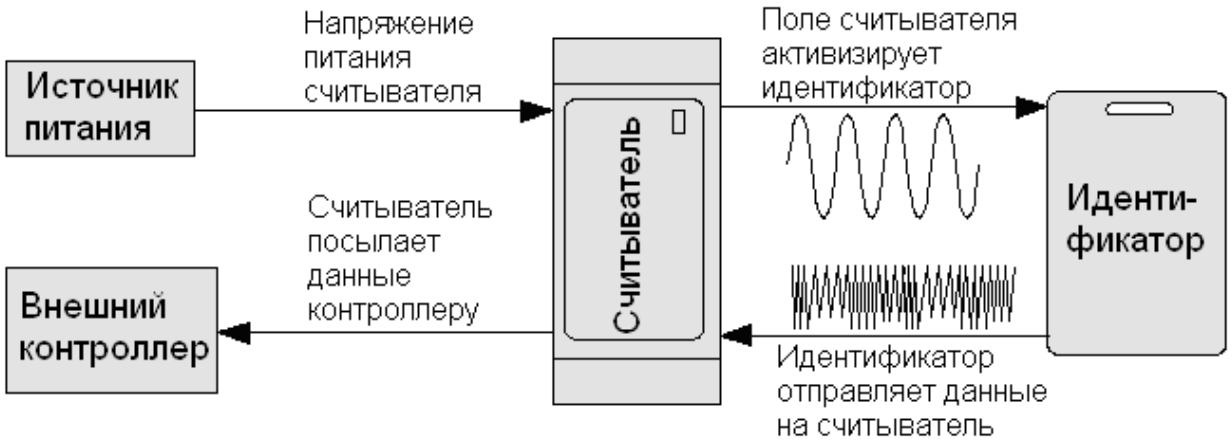


Рисунок 11. Функциональная схема, поясняющая работу считывателя

Во включенном состоянии считыватель излучает вблизи себя низкочастотное (125 кГц) электромагнитное поле. Идентификатор, оказываясь в этом поле, активизируется и начинает передавать индивидуальный кодированный сигнал, принимаемый считывателем.

Считыватель преобразует принятый сигнал в соответствии с требованиями используемого для связи с внешним устройством протокола и передает полученный код идентификатора в контроллер исполнительного устройства по интерфейсу RS-485.

9.6 Принцип работы считывателя *Mifare*

Считыватели *Mifare* обеспечивают (заводская установка) чтение уникального идентификатора *UID* с карты или транспондера *ISO/IEC 14443 A/MIFARE*; а также чтение уникальных идентификаторов со смартфонов с функцией *NFC*. Физический принцип считывания идентификационной информации с карты *Mifare* аналогичен указанному в разд. 9.4 (рабочая частота – 13,56 МГц).

Кроме того, с целью повышения уровня безопасности системы доступа предусмотрена возможность использования дополнительной идентификационной информации *ID* из внутренней памяти карты или транспондера *ISO/IEC 14443 A/MIFARE*, при этом требуется

SEC.RU | Короткий путь к информации Скачано с sec.ru

дополнительное программирование (далее – *конфигурация*) считывателя в ПО ***PERCo-Web*** или ***PERCo-S-20***.

Считывание кода происходит при поднесении идентификатора к считывателю. При этом идентификатор может находиться в кармане, в бумажнике или в любом другом радиопрозрачном контейнере (футляре).

Внимание!

Для работы с идентификационной информацией из защищенной области карт (в том числе и для записи отпечатков пальцев на карту, см. разд. 9.7.2) все используемые в системе карты пользователей необходимо персонифицировать, т.е. записать в них конфигурацию для считывателей и карт *Mifare*, заданную на данный момент в системе СКУД. Сделать это можно посредством ПО ***PERCo-Web*** или ***PERCo-S-20*** с использованием контрольного считывателя ***PERCo-IR18***, ***IR15.9***, персонификация карт через считыватель контроллера ***PERCo-CL15.1*** не предусмотрена!

9.6.1 Особенности работы со смартфонами с функцией *NFC*:

Чтобы смартфон использовать в качестве карты доступа, необходимо, чтобы на нем была включена функция использования *NFC* (в настройках самого смартфона).

В смартфоне с ОС *“Android”* в качестве идентификатора доступа используется уникальный идентификатор, генерируемый приложением «**PERCo. Доступ**» (бесплатное, имеется на ресурсе «Google Play»). двумя способами:

- либо случайным образом (вероятность совпадения идентификаторов ничтожно мала);
- либо по желанию пользователя можно использовать *IMSI* – индивидуальный номер абонента, ассоциированный с SIM-картой смартфона, в этом случае приложение может запрашивать доступ к контактам телефона.

Для корректной работы приложения «**PERCo. Доступ**» необходима версия ОС *“Android” 5.0* и выше.

В смартфонах *“Apple”* (ОС *“iOS”*) в качестве идентификатора используется уникальный *Token*, привязанный к одной из банковских карт, эмулированных на смартфоне, (т.е. перед использованием в СКУД необходимо будет на смартфоне активировать именно эту банковскую карту), установка дополнительного приложения не требуется.

Для использования смартфона с функцией *NFC* в качестве идентификатора доступа необходимо:

1. В программном обеспечении СКУД ***PERCo*** в разделах, касающихся настройки работы с картами *MIFARE*, включить функцию использования смартфона (по умолчанию на считывателях и в программном обеспечении ***PERCo*** – включена).
2. Занести идентификатор со смартфона в базу данных, как обычную карту доступа:
   - вручную, получив номер идентификатора в смартфоне через приложение «**PERCo. Доступ**» (только для смартфонов на ОС “*Android”*);
   - автоматически при помощи контрольного считывателя ***PERCo-IR18***, ***PERCo-IR15.9,*** подключенного к ПК с установленным ПО ***PERCo-Web***, ***PERCo-S-20*** или ***PERCo-S-20 «Школа»***.

Далее смартфон можно использовать в качестве идентификатора при проходах через считыватели:

- Для большинства современных смартфонов с ОС *“Android”* после загрузки приложения «**PERCo. Доступ**» для использования его в качестве идентификатора достаточно разблокировать смартфон и поднести его к считывателю (в настройках телефона обязательно должен быть разрешен обмен данными по *NFC*). Однако для некоторых моделей смартфонов может понадобиться каждый раз перед поднесением открывать приложение «**PERCo. Доступ**».
- Для смартфонов *“Apple”* (ОС “*iOS*”) достаточно приложить смартфон к считывателю, при этом смартфон должен автоматически перейти в режим *“Apple Pay”* (режим оплаты), и пройти аутентификацию (*“Face ID”* или *“Touch ID”*). При этом, если к идентификатору в СКУД ***PERCo*** привязана банковская карта, не установленная в смартфоне по умолчанию, то дополнительно еще ее придется выбрать из списка банковских карт, привязанных к смартфону.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Примечание:

В СКУД ***PERCo*** для идентификации с помощью смартфона используются только такие данные, которые никаким образом не могут повлиять на уровень безопасности персональных данных владельца, в том числе и на безопасность данных о банковских картах.

9.6.2 Конфигурация считывателя *Mifare*

По умолчанию считыватель *Mifare* сконфигурирован для работы с UID (без защиты от копирования) и со смартфонами с функцией *NFC*. Конфигурирование считывателя *Mifare* для работы с дополнительной идентификационной информацией ID (с защитой от копирования) производится при помощи ПО систем ***PERCo-Web*** или ***PERCo-S-20*** (порядок конфигурации – см. в Руководствах пользователя данного ПО).

9.7 Порядок работы со сканером отпечатков пальцев

9.7.1 Принцип действия сканера отпечатка пальца

В контроллере в качестве сканера отпечатка пальца используется модуль производства *Morpho*. Для сканирования отпечатка пальца пользователь должен приложить кончик пальца по всей длине окна модуля сканера параллельно его оси и немного прижать. После сканирования отпечатка пальца модуль по особому алгоритму создает уникальный шаблон-паттерн или так называемую «свертку» отпечатка, которая и используется в системе СКУД в качестве идентификатора пользователя. В Web-интерфейсе контроллера и в СКУД под термином «отпечаток пальца» подразумевается именно его свертка. После получения свертки контроллер в зависимости от режима и результата работы с отпечатком сгенерирует соответствующие управляющие сигналы и световую и звуковую индикацию (см. разд. 9.10).

Внимание!

При определенных условиях (например, повышенная сухость или влажность кожи, повреждения пальца и т.д.) сканер может не распознавать ваш отпечаток пальца. В таких случаях подуйте на палец или высушите кожу и попробуйте еще раз, отсканируйте отпечаток другого пальца. Если отпечаток пальца отсканировать не получается, используйте другие способы аутентификации.

Перед использованием в качестве идентификатора отпечаток пальца пользователя необходимо зарегистрировать в системе (занести в базу данных аналогично карте доступа) или же записать его на карту доступа *Mifare* (только для схемы идентификации **"карта и отпечаток на карте"**, разд. 9.4), зарегистрированную в системе за данным пользователем (разд. 9.7.2). Это можно произвести в разделе ***Доступ*** → ***Пользователи*** *Web*-интерфейса контроллера (см. Приложение 4) или в ПО систем ***PERCo-Web*** и ***PERCo-S-20***.

Примечание:

Если в память контроллера не было занесено ни одного отпечатка пальца (например, при первом включении контроллера), модуль может не подсвечиваться постоянной индикацией (красного цвета), что не говорит о его неисправности.

9.7.2 Порядок записи отпечатка пальца на карту Mifare

Контроллер поддерживает функцию записи отпечатка пальца на карту доступа *Mifare* (данной возможностью обладают карты стандартов *MIFARE Classic 1K*, *MIFARE Classic 4K*, *MIFARE Plus* (*X*, *S*, *SE*) и *MIFARE DESFire Ev1)*. Данная функция позволяет ускорить процесс авторизации пользователя в системе, так как при этом системой не тратится время на поиск нужного отпечатка в базе данных пользователей, а сравнение предъявленного отпечатка производится сразу с отпечатком, записанным на карте. Для ее реализации в правах доступа пользователя необходимо установить схему идентификации **"карта и отпечаток на карте"**, см. разд. 9.4.

Запись отпечатка пальца на карту осуществляется в разделе ***Доступ*** → ***Пользователи*** *Web*-интерфейса контроллера (Приложение 4, п. 5.2) или в ПО ***PERCo-Web*** и ***PERCo S-20***. При этом в *Web*-интерфейсе контроллера перед нажатием на кнопку **«Записать на Mifare»** необходимо заранее отсканировать и закрепить записываемые на карту отпечатки за пользователем.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Количество отпечатков, записываемых на карту *Mifare*, зависит от наличия свободного места в ее памяти и ограничено производителем – не более 5 штук. Записываются отпечатки на карту в порядке очередности по списку в *Web*-интерфейсе, после записи рекомендуется проверить попытками прохода, какие отпечатки записались, а какие – нет.

Внимание!

Запись отпечатка пальца производится в защищенную область карты, поэтому заранее необходимо будет персонифицировать карты пользователей, т.е. записать в них конфигурацию для считывателей и карт *Mifare*, заданную на данный момент в системе СКУД (см. разд. 9.6). Записать отпечаток пальца в не персонифицированную карту нельзя!

9.8 Обновление встроенного ПО

Обновление встроенного ПО и форматирование памяти возможно при помощи *Web*-интерфейса контроллера в разделе **Сервис** (см. Приложение 4, п 9).

При эксплуатации соблюдайте меры безопасности, указанные в разд. 7.2.

9.9 РКД при работе в СКУД

Смена РКД осуществляется автономно или по команде ПО, при этом для ИУ типа «замок» она производится одновременно для обоих направлений прохода.

РКД *«Открыто»* – режим свободного прохода.

- ИУ разблокируется до смены РКД.
- Нажатие кнопки ДУ (*«Выход»*) игнорируется.

РКД *«Контроль»* – основной режим работы как элемента СКУД.

- ИУ блокируется.
- При предъявлении идентификатора, удовлетворяющего всем критериям разрешения прохода ИУ разблокируется на **Время удержания в разблокированном состоянии**.

РКД *«Закрыто»* – режим запрета прохода.

- ИУ блокируется до смены РКД.
- Нажатие кнопки ДУ (*«Выход»*) игнорируется.
- При предъявлении любой карты регистрируется событие о нарушении РКД.

РКД *«Охрана» (только для ИУ типа замок)*

- ИУ блокируется до смены РКД.
- Нажатие кнопки ДУ (*«Выход»*) игнорируется.
- Взят на охрану ИУ.
- Постановка на охрану / снятие с охраны осуществляется двойным поднесением идентификатора, имеющего соответствующие права, в соответствии со схемой идентификации[1].
- Проход через ИУ (взлом ИУ) переводит ИУ в режим «*Тревога»*.

9.10 Индикация

Возможные варианты индикации РКД, состояний и реакций контроллера на предъявление идентификаторов представлены в табл. 3. Индикация осуществляется на блоке индикации, расположенном на лицевой панели корпуса контроллера.

Примечание:

При разрешении доступа по карте световая индикация включается на **Время удержания в разблокированном состоянии**, либо до факта совершения прохода. При запрете прохода индикация включается на 1 с.

[1] Если для пользователя установлена схема идентификации «карта+палец», то постановка на охрану / снятие с охраны осуществляется двойным поднесением идентификаторов по данной схеме, т.е. карта-палец-карта-палец.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Таблица 3. Индикация контроллера

Событие индикации	Световая индикация	Звуковая индикация
Нет конфигурации контроллера	Попеременное мигание красной и зеленой строки (2 Гц)	Нет
РКД "КОНТРОЛЬ"	Горит красная строка	Нет
• Ожидание окончания идентификации доступа	Бегут справа-налево синие огни	Нет
• Предъявление идентификатора, доступ разрешен, ожидание прохода	Бегут слева-направо зеленые огни	Мелодия разрешения
• Предъявление идентификатора, доступ запрещён	Мигает красная строка (два раза)	Сигнал запрета
РКД "ОТКРЫТО"	Горит зеленая строка	Нет
• Предъявление любого идентификатора	Бегут слева-направо зеленые огни	Мелодия разрешения
РКД "ЗАКРЫТО"	Мигает красная строка (2 Гц)	Нет
• Предъявление любого идентификатора	Мигает красная строка (два раза)	Сигнал запрета
РКД "ОХРАНА"	Бегут слева-направо красные огни	Нет
• Ожидание взятия на охрану	Бегут слева-направо синие огни	Нет
• Невзятие на охрану	Горит красная строка 1 секунду, переход в предыдущий режим	Сигнал запрета
• Предъявление любого идентификатора	Мигает красная строка (два раза)	Сигнал запрета
РКД «FIRE ALARM»	Мигает зеленая строка (1 Гц)	Нет
Режим ввода отпечатков	Горит белая строка	Нет
• Успешное промежуточное предъявление пальца	Горит зеленая строка (0,25 сек)	Высокий звук на 0,25 сек
• Неудачное промежуточное предъявление пальца	Горит красная строка (0,25 сек)	Низкий звук на 0,25 сек
• Отпечаток зарегистрирован	Мигает зеленая строка (3 Гц, 1 сек)	Мелодия разрешения
• Отпечаток не зарегистрирован	Мигает красная строка (3 Гц, 1 сек)	Сигнал запрета
Индикация режима записи отпечатков на карту	Горит белая строка	Нет
• Успешная очистка / запись отпечатков на карте	Горит зеленая строка (0,5 сек)	Нет
• Неудачная очистка / запись отпечатков на карте	Горит красная строка (0,5 сек)	Нет
Ожидание комиссионирования	Бегут слева-направо синие огни	Нет
Успешное комиссионирование (после предъявления 1-й комиссионирующей карты для 2-го комиссионирования)	Горит зеленая строка (0,25 сек)	Высокий звук на 0,25 сек
Ожидание верификации	Бегут справа-налево синие огни	Нет
Успешная верификация очередного уровня (для разделения между последовательными уровнями верификации)	Горит зеленая строка (0,25 сек)	Высокий звук на 0,25 сек

SEC.RU | Короткий путь к информации Скачано с sec.ru

10 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.

11 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 3 разряда.

При производстве работ по техническому обслуживанию следует руководствоваться указаниями разд. 7 «*Требования безопасности*» данного руководства.

Внимание!

- Перед началом работ отключить контроллер от ИП.
- Используемая КИА должна быть поверена.

Один раз в три месяца предусматриваются плановые работы в объеме регламента №1. Перечень работ приведен в табл. 4. Сведения о проведении регламентных работ заносятся в журнал учета регламентных работ. Соблюдение периодичности, технологической последовательности и методики выполнения регламентных работ являются обязательными.

Таблица 4. Перечень работ по регламенту №1 (технологическая карта №1)

Содержание работ	Порядок выполнения	Приборы, инструмент, материалы	Нормы и наблюдаемые явления
1 Внешний осмотр, чистка контроллера	1.1 Отключить ИП от сети переменного тока и удалить с поверхностей контроллера и ИП пыль, грязь и влагу.	Ветошь, кисть флейц.	Не должно быть следов грязи и влаги.
	1.2 Снять крышки с ИП, при наличии резервного ИП (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).
	1.3 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 разд. 9.		Индикация на контроллере согласно разд. 9.10. Формирование сигналов на выходе согласно его конфигурации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

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

12 ДИАГНОСТИКА И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Возможные варианты неисправностей:

12.1 Контроллер не работает

Причинами неисправности контроллера могут быть:

1. **Неисправность ИП** контроллера – проверьте ИП.
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.

12.2 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 (см. рис. 14).

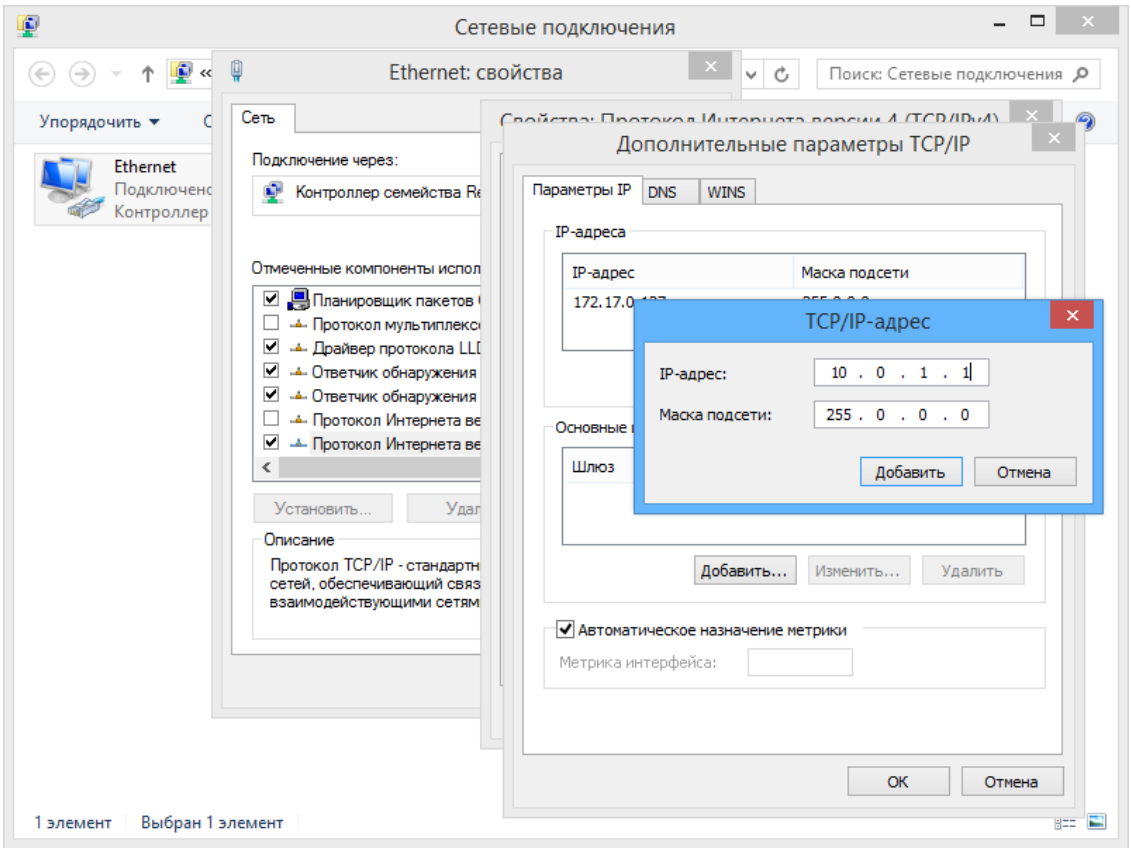


Рисунок 12. Добавление IP-адреса ПК

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`

SEC.RU | Короткий путь к информации Скачано с sec.ru

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.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Приложение 1. Инструкция по подключению контроллера через *PoE*-сплиттер

Внимание!

- Инструкция дана для сплиттеров, входящих в комплект поставки дополнительного оборудования.
- 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 %.

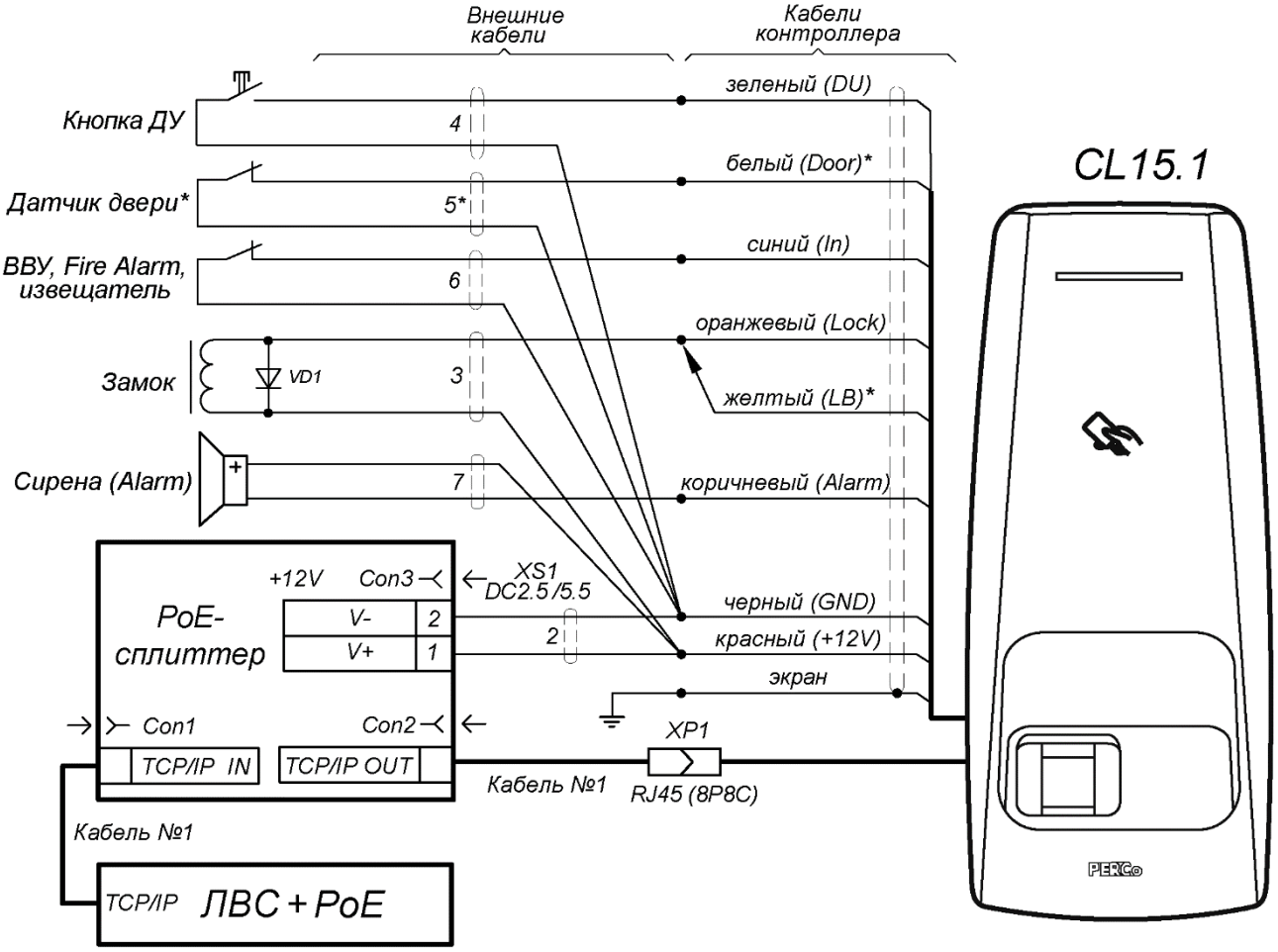
PoE-сплиттер (далее – *сплиттер*) предназначен для подачи питания на устройства, подключаемые по сети *Ethernet*. Сплиттер работает с любыми сетевыми коммутаторами (далее – *Switch)*, поддерживающими технологию передачи электроэнергии по витой паре *PoE* и совместимыми со стандартом *IEEE 802.3af*.

Сплиттер представляет собой блок электроники в пластиковом корпусе и снабжен следующими разъемами:

Con 1 – разъем для подключения кабеля *Ethernet* от *Switch*.
Con 2 – разъем подключения кабеля *Ethernet* контроллера;
Con 3 – разъем выхода питания для подключения кабеля питания контроллера.

Примечание:

Для некоторых моделей сплиттера выбор выходного напряжения осуществляется с помощью переключателя. При работе с оборудованием компании PERCo необходимо перевести переключатель в положение «12В».



* - *при использовании замков с контактной группой серии PERCo-LB (LBP):*
1) датчик двери не устанавливать, белый провод не подключать,
2) подключить желтый провод к оранжевому

Рисунок 13. Схема подключения контроллера через *PoE*-сплиттер

SEC.RU | Короткий путь к информации Скачано с sec.ru

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.
3. Подключите цепи питания контроллера к разъему ***Con3*** сплиттера. Схема подключения приведена на рис. 13 (остальные подключения – см. схему на рис. 3 - 10, штекер для подключения к разъему входит в комплект поставки сплиттера).



Внимание!

При подключении замка установка диода искрозащиты ***VD1*** (см. рис. 3-4), типа 1N5819 – **ОБЯЗАТЕЛЬНА!** Использование супрессоров вместо диодов искрозащиты – **ЗАПРЕЩЕНО!** Рекомендуется использовать только электромеханические замки.

4. Подключите кабель *Ethernet* от *Switch* к разъему ***Con1*** сплиттера.
5. После верификации между *Switch* и сплиттером на контроллер будет подано питание.

Для отключения питания контроллера отсоедините кабель *Ethernet* (идущий от *Switch*) от разъема ***Con1*** сплиттера.

Приложение 2. Инструкция по подключению пирометра *PERCo-AT01*

Пирометр ***PERCo-AT01*** предназначен для предварительного определения людей с возможно повышенной температурой тела и ограничения для них доступа через ИУ, управляемые контроллером. Может как встраиваться непосредственно в исполнительные устройства (например, на крышках турникетов и электронных проходных), так и устанавливаться отдельно от них, например, на стене, на стойке ограждения и т.д. Порядок монтажа пирометра описан в его эксплуатационной документации.

Работа контроллера с пирометром возможна после конфигурирования его в *Web*-интерфейсе контроллера или в сетевом ПО ***PERCo-Web, PERCo-S-20 (PERCo-S-20 «Школа»)***.

В совместной работе с контроллером ***PERCo-CL15.1*** применяется конфигурация пирометра "ВВУ с тактированием" (на пирометре установлена по умолчанию). Для этого пирометр подключается к контроллеру по схеме на рис. 16, а контроллер конфигурируется для работы с ВВУ по предъявлению разрешенного идентификатора (см. пример конфигурации контроллера ниже по тексту).

В этом случае алгоритм работы контроллера с пирометром следующий:

1. Пользователь подносит карту к считывателю контроллера, контроллер анализирует код карты, при разрешенном доступе контроллер переводит данное направление прохода в режим верификации и на вход пирометра контроллером подается команда на проведение измерения.
2. Пользователь после считывания карты и перехода в режим ожидания верификации (на считывателе мигает желтый индикатор) подносит запястье руки к датчику пирометра. Пирометр проводит измерение температуры поверхности запястья и если ее значение не превышает порог, установленный на пирометре, выдает на вход контроллера сигнал разрешения прохода.
3. Контроллер при получении команды разрешает проход пользователю. Пирометр переходит в режим ожидания новой команды на измерение. Если команда не поступила, то по истечению времени ожидания верификации контроллер переходит в дежурный режим.

SEC.RU | Короткий путь к информации Скачано с sec.ru

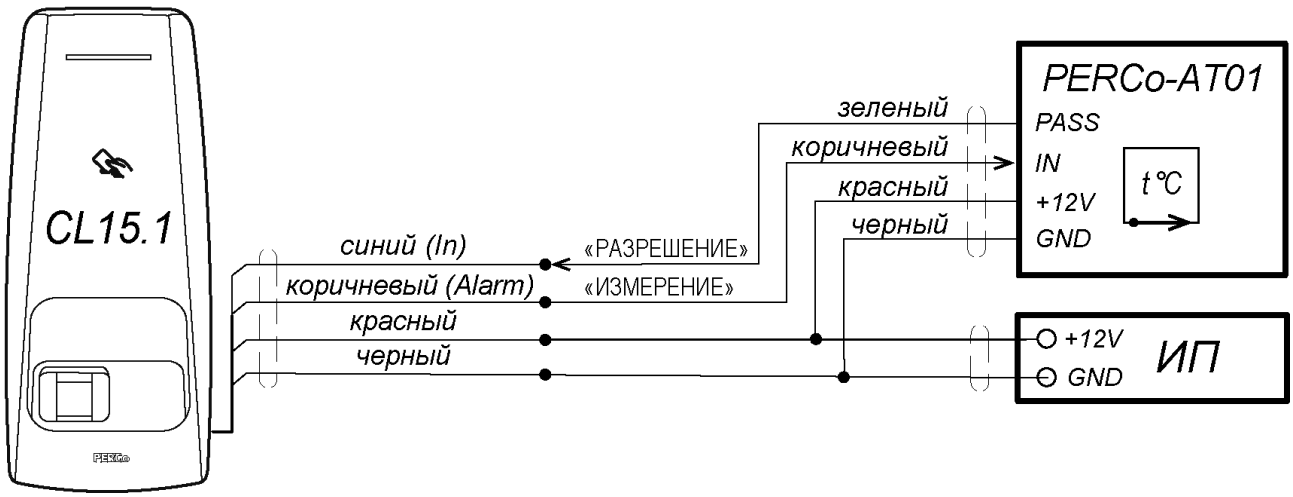


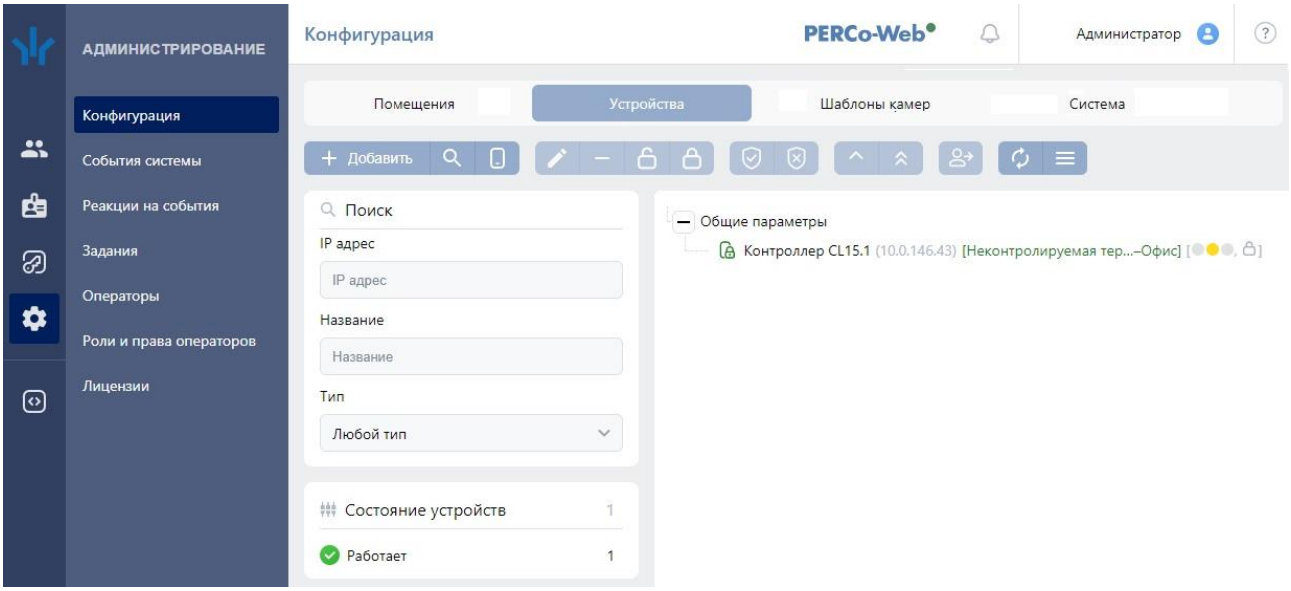
Рисунок 14. Схема подключения к контроллеру *PERCo-CL15.1* пирометра *PERCo-AT01*

Примечание:

Если выход контроллера занят под другое оборудование и нет возможности подавать сигнал ИЗМЕРЕНИЕ, то возможна работа с пирометром в режиме **"ВВУ без тактирования"**: для этого на пирометре при помощи джамперов установите данный режим и соедините коричневый (IN) и оранжевый (GND) провода пирометра между собой. В этом случае измерение температуры пирометром будет проводиться непрерывно и, соответственно, в ПО не нужно конфигурировать выход контроллера под сигнал ИЗМЕРЕНИЕ и задавать внутреннюю реакцию на запрос верификации (см. ниже по тексту).

Настройка контроллера для работы с пирометром в ПО *PERCo-Web*

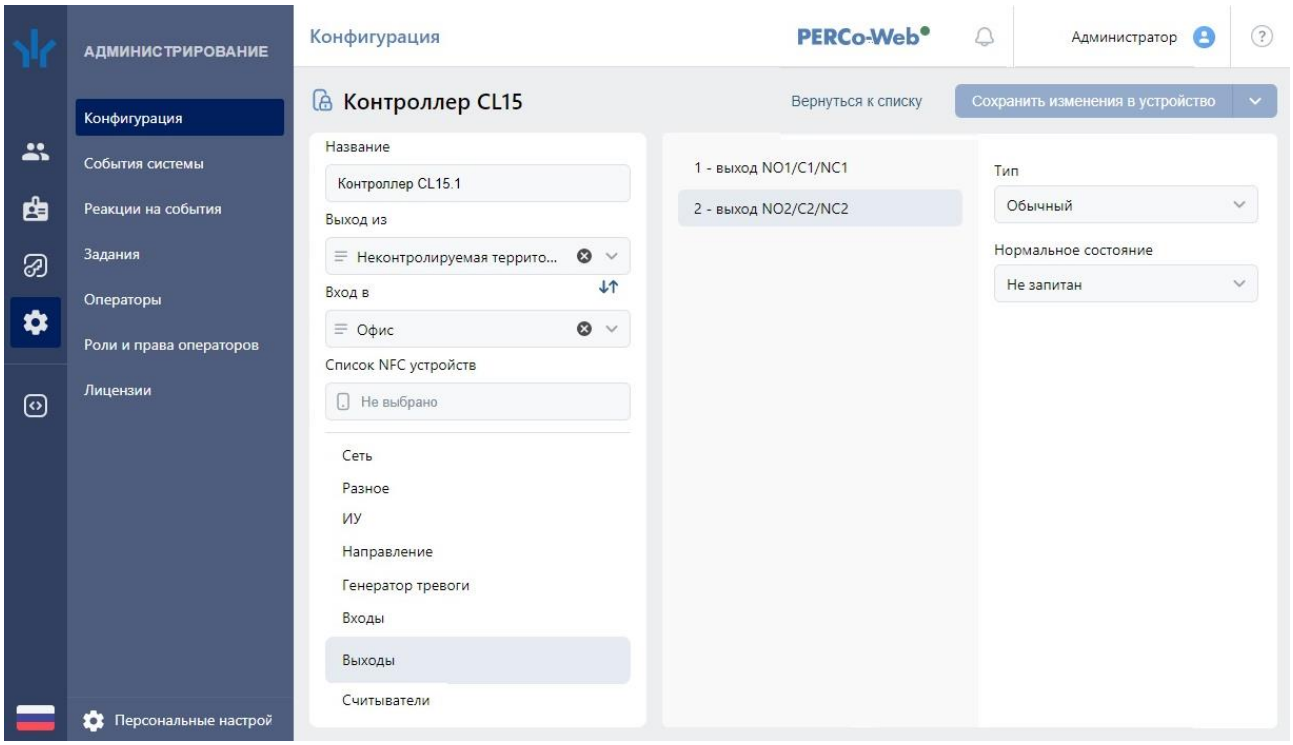
1. Осуществите вход в систему, используя *Web*-браузер (см. *Руководство администратора PERCo-Web*).
2. Используя панель навигации, перейдите в раздел ***«Администрирование»*** → ***«Конфигурация»***.
3. В рабочей области страницы выделите контроллер (**Контроллер CL15.1**):



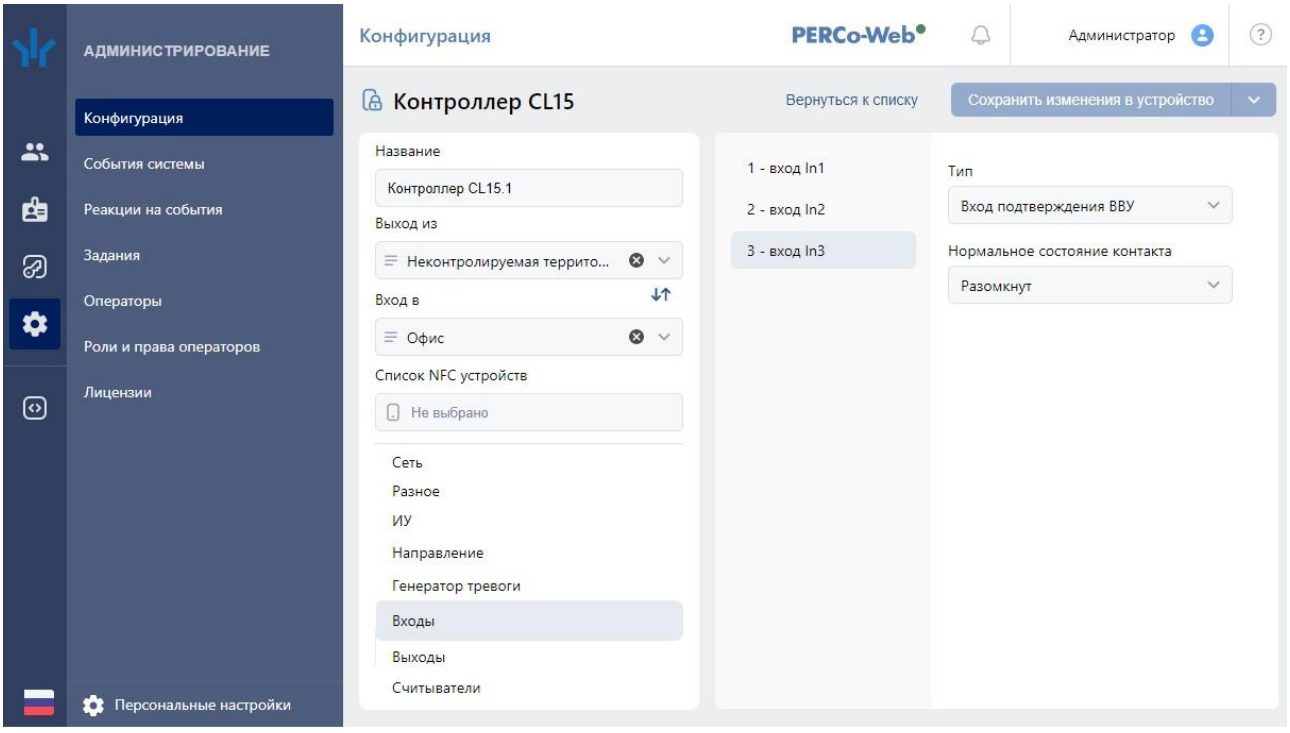
4. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется окно **Контроллер CL15**.
5. В открывшемся окне перейдите на вкладку **Выходы**.
6. В рабочей области окна выберите выход OUT2 (**NO2/C2/NC2**) (к нему физически подключен вход *«ИЗМЕРЕНИЕ»* пирометра).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7. Установите с помощью раскрывающегося списка в рабочей области окна:
   - для параметра **Тип** – значение **Обычный**;
   - для параметра **Нормальное состояние** – значение **Не запитан**:

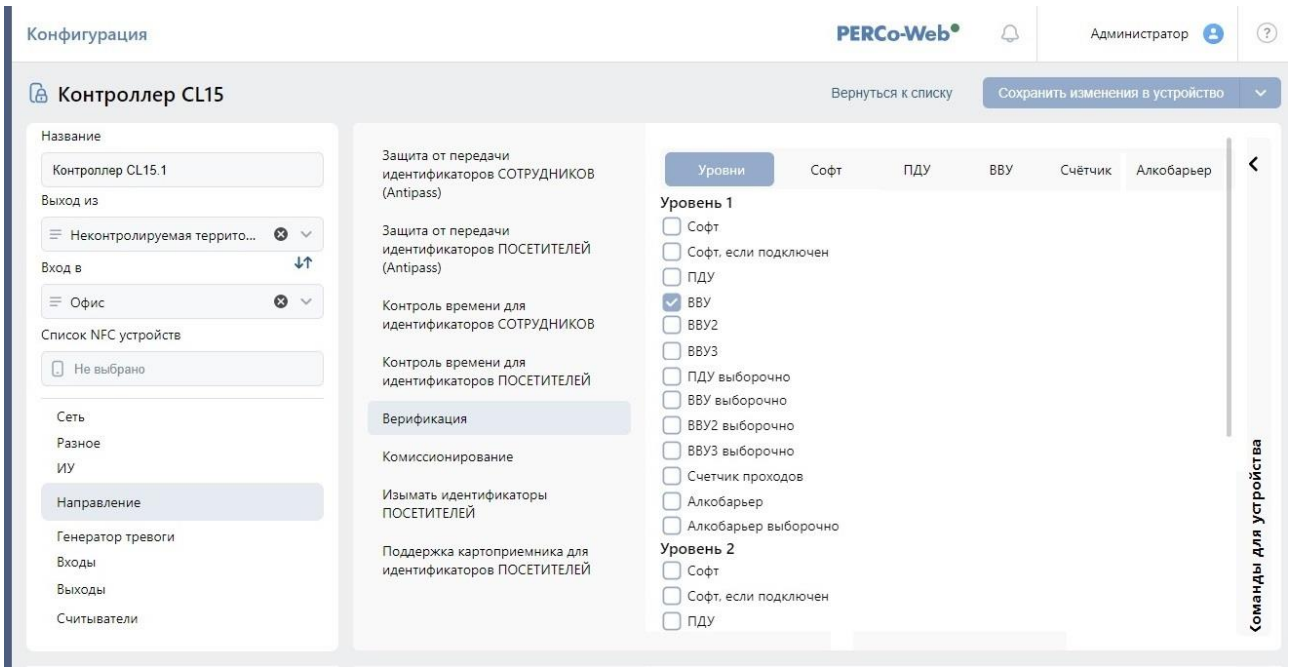


8. Перейдите на вкладку **Входы**.
9. В рабочей области окна выберите вход контроллера **3 - вход In3 (**к нему физически подключен выход *«РАЗРЕШЕНИЕ»* пирометра) и установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
   - для параметра **Тип** – значение **Вход подтверждения ВВУ**;
   - для параметра **Нормальное состояние контакта** – значение **Разомкнут**;



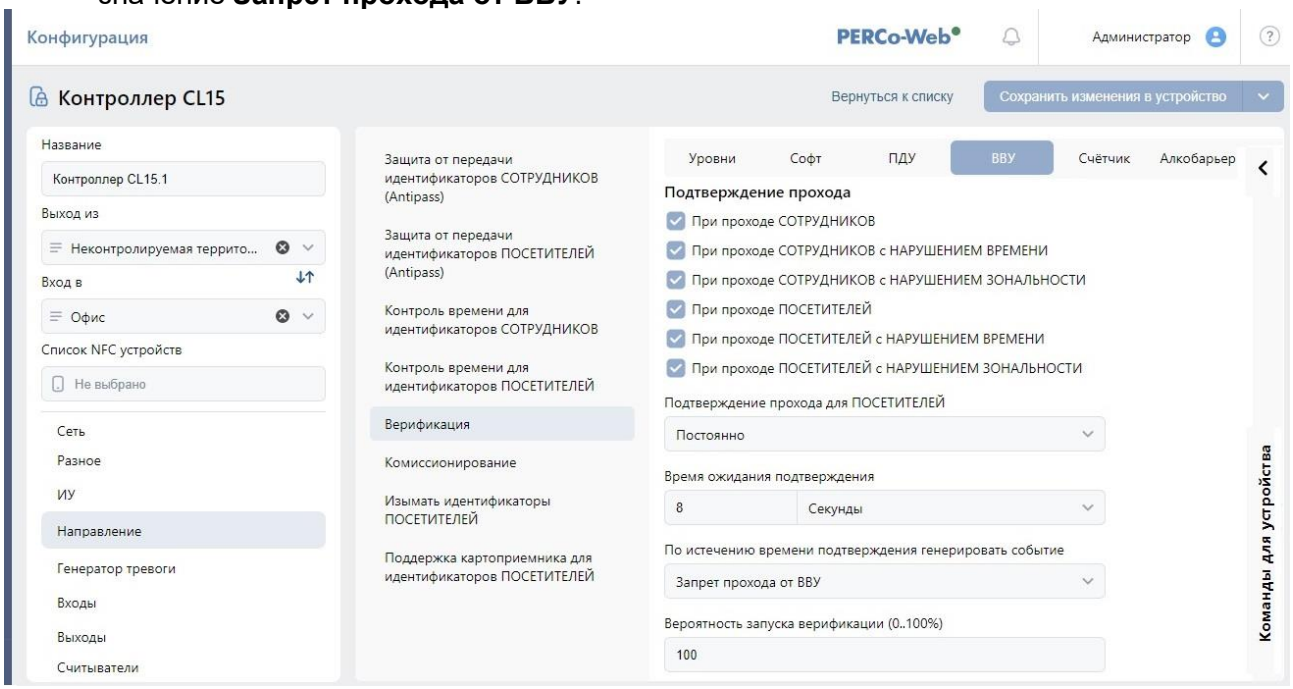
10. Перейдите на вкладку **Направление**. В левой части рабочей области вкладки выберите группу параметров **Верификация**, в правой части – колонку **Уровни** и для **Уровня №1** поставьте галочку **ВВУ**:

SEC.RU | Короткий путь к информации Скачано с sec.ru



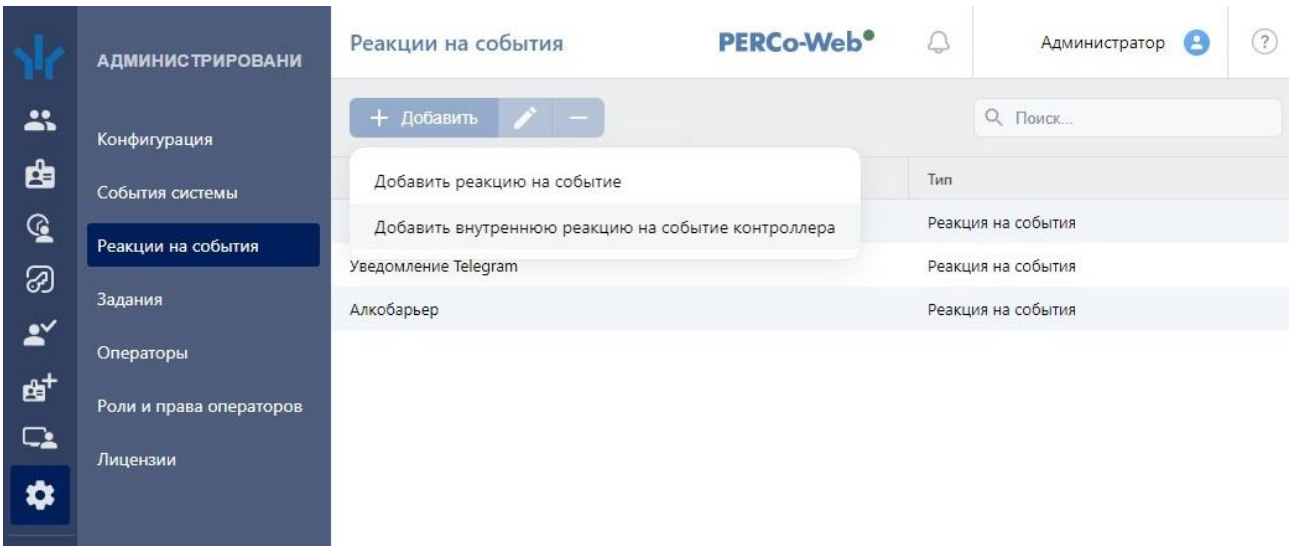
Затем в правой части выберите колонку **ВВУ** (в этом случае подтверждением для разрешения или запрета прохода будет являться сигнал от ВВУ – пирометра) и установите:

- для параметра **Подтверждение прохода** – флажки для значений **при проходе СОТРУДНИКОВ (ПОСЕТИТЕЛЕЙ)**;
- для параметра **Подтверждение прохода для ПОСЕТИТЕЛЕЙ** – значение **Постоянно**;
- для параметра **Время ожидания подтверждения** – необходимое значение, в течение которого контроллер должен ожидать сигнал *«РАЗРЕШЕНИЕ»* от пирометра;
- для параметра **По истечению времени подтверждения генерировать событие –** значение **Запрет прохода от ВВУ**.



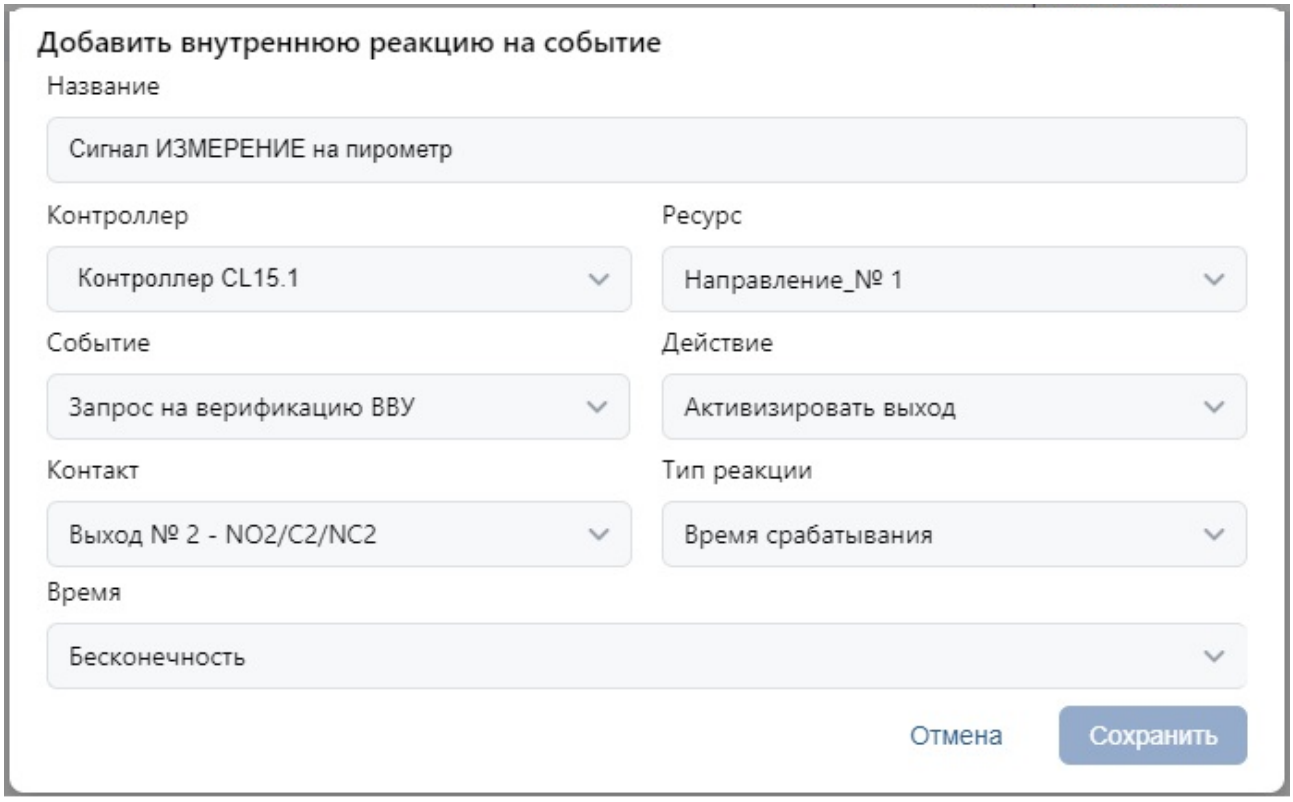
11. Нажмите кнопку **Сохранить и закрыть**. Окно **Контроллер CL15** будет закрыто, настройки точки верификации будут сохранены.
12. Перейдите в раздел ***«Администрирование»*** → ***«Реакции на события»***. Нажмите кнопку , в выпадающем списке выберите **Добавить внутреннюю реакцию на событие контроллера**:

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Откроется окно **Добавить внутреннюю реакцию на событие**. Задайте название новой реакции и установите для параметров реакции следующие значения:

- **Контроллер** – в появившемся списке устройств выберите данный **Контроллер CL15.1** и ресурс **НАПРАВЛЕНИЕ №1**;
- **Событие** – с помощью раскрывающегося списка выберите тип события – **Запрос на верификацию ВВУ**;
- **Действие** – с помощью раскрывающегося списка выберите тип реакции **Активизировать выход**;
- **Контакт** – с помощью раскрывающегося списка выберите **Выход №2** (выход контроллера, к которому физически подключен вход *«ИЗМЕРЕНИЕ»*);
- **Тип реакции** – с помощью раскрывающегося списка установите значение **Время срабатывания**;
- **Время** – с помощью раскрывающегося списка выберите значение **Бесконечность**:

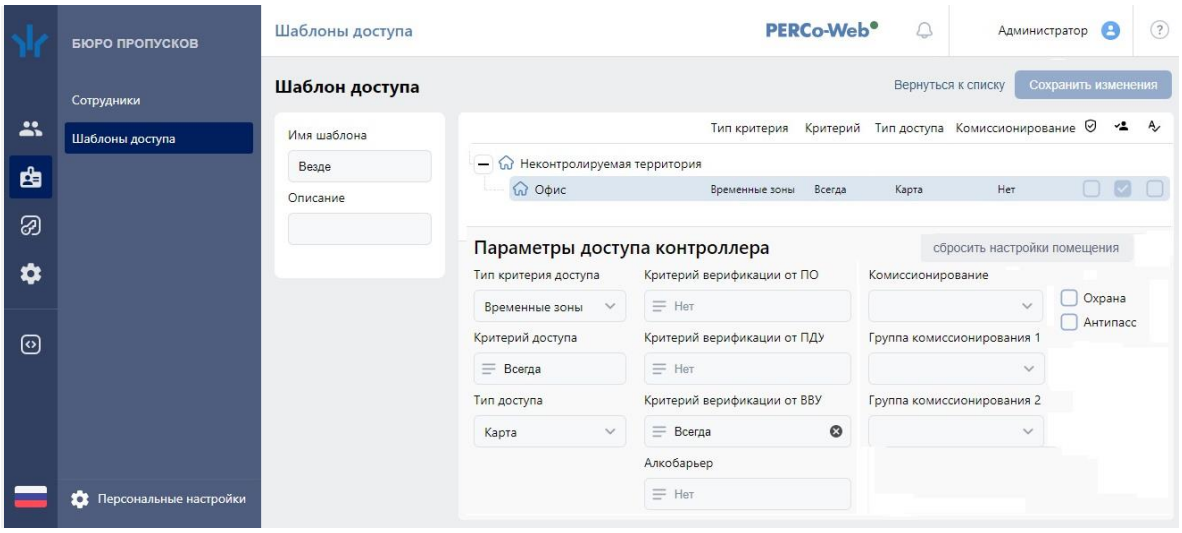


13. Нажмите кнопку **Сохранить**. Окно **Добавить внутреннюю реакцию на событие** будет закрыто, в списке реакций будет добавлена реакция, генерирующая сигнал ИЗМЕРЕНИЕ на пирометр при запросе на верификацию.

SEC.RU | Короткий путь к информации Скачано с sec.ru

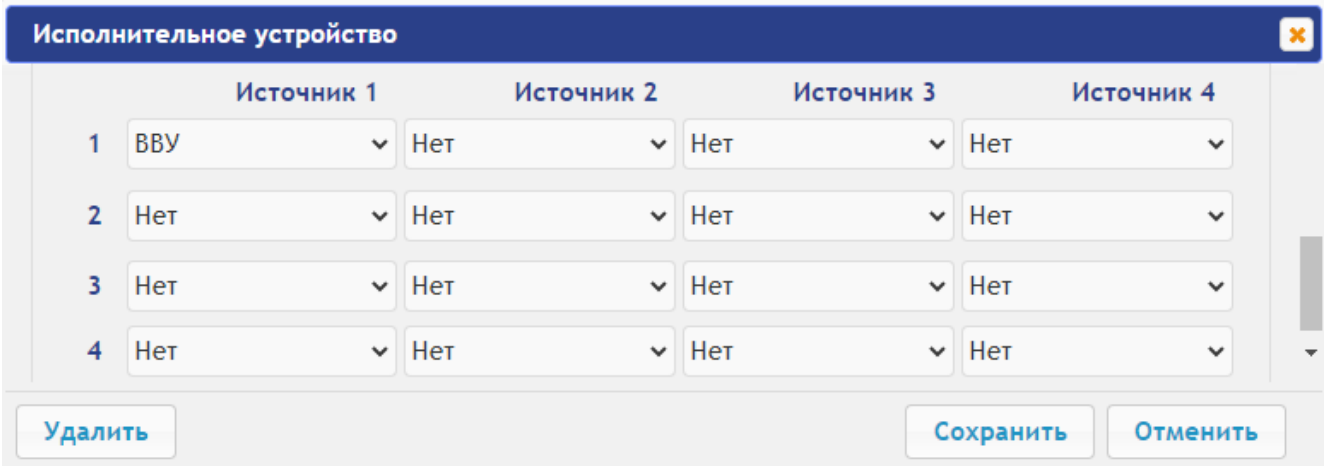
Внимание!

Для всех шаблонов доступа в подразделе **Шаблоны доступа** раздела **Бюро пропусков** необходимо установить обязательный процесс верификации при предъявлении их к считывателю направления, контролируемого пирометром:



Настройка контроллера для работы с пирометром в *Web*-интерфейсе

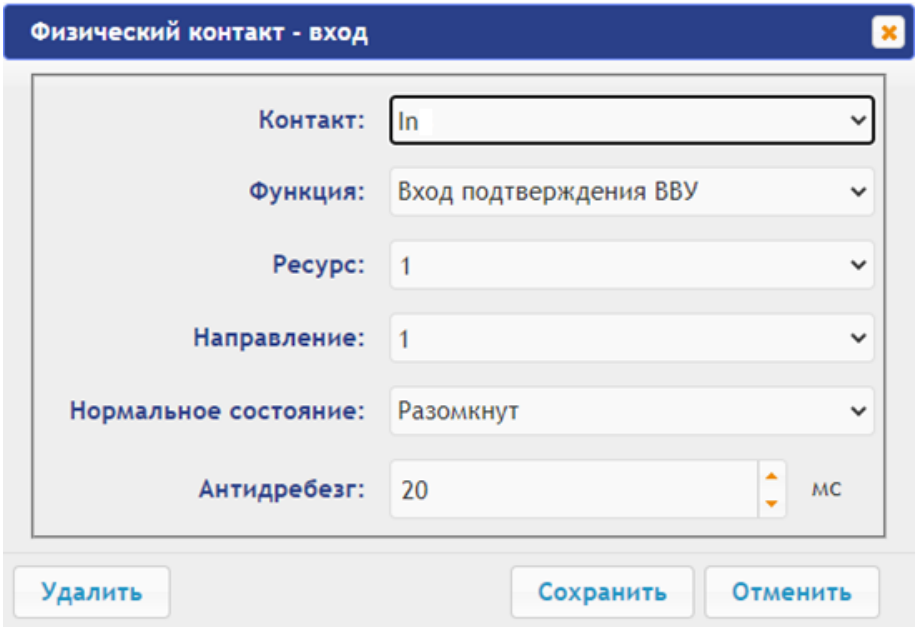
1. В разделе **Конфигурация → Редактировать → Исполнительные устройства** выберите исполнительное устройство, контролируемое пирометром, затем в открывшемся окне на вкладке **Доступ по направлению** выберите **Направление 1** (направление прохода, контролируемое пирометром). В группе параметров **Верификация** для направления ИУ установите:
   - задайте **Время ожидания от ВВУ** (не менее 3 секунд).
   - для параметров **от ВВУ при запросе на проход сотрудника** (**посетителя**) **–** значения **Да**,
   - для параметра **Запуск верификации ВВУ для посетителей** – значение **Ежедневно**,
   - для параметра **Работа при отсутствии ответа от ВВУ – действие** – значение **Запрет**,
   - в таблице уровней источников – для **Источника 1** первому уровню задайте значение **ВВУ**:



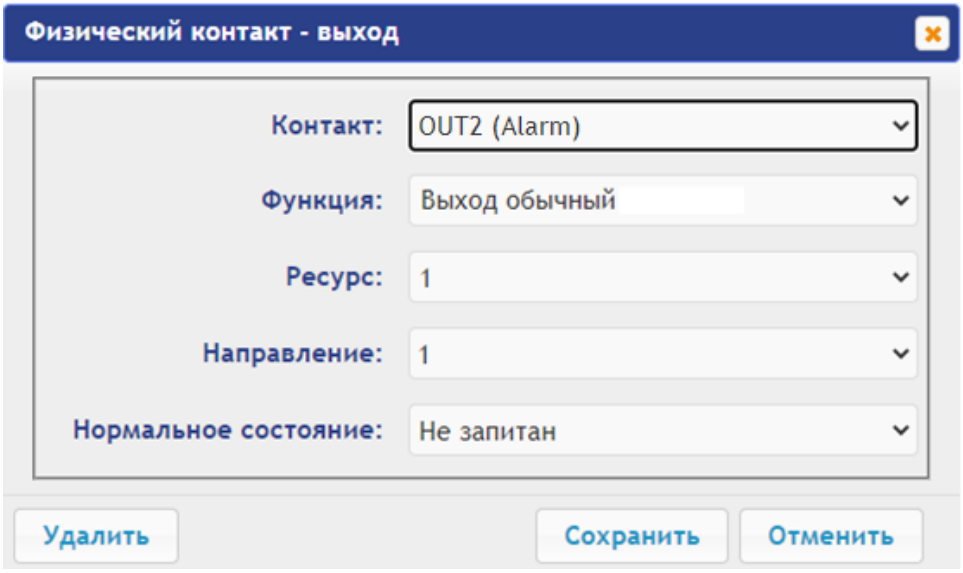
2. В разделе **Конфигурация → Редактировать → Физические контакты**:
   - для входа **In** (к нему физически подключен выход пирометра «РАЗРЕШЕНИЕ»), установите следующие значения параметров:
     - **Функция:** – **Вход подтверждения от ВВУ**,
     - **Ресурс:** – **1** (номер ИУ, к которому физически подключен пирометр),
     - **Направление:** – **1** (направление прохода, контролируемое пирометром),

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Нормальное состояние:** – **Разомкнут**:

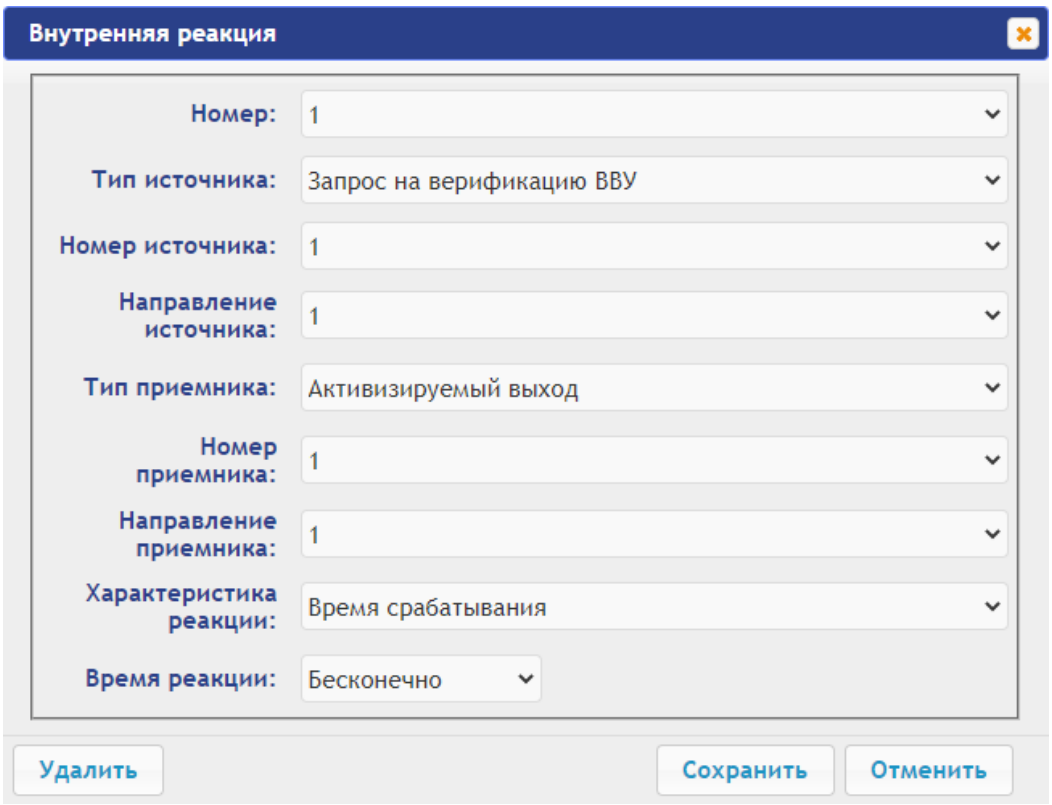


- для выхода **OUT2 (Alarm)** (к нему физически подключен вход пирометра «ИЗМЕРЕНИЕ») установите следующие значения параметров:
  - **Функция:** – **Выход обычный**,
  - **Ресурс:** – **1** (номер источника для внутренней реакции контроллера для сигнала «ИЗМЕРЕНИЕ»),
  - **Нормальное состояние:** – **Не запитан**:

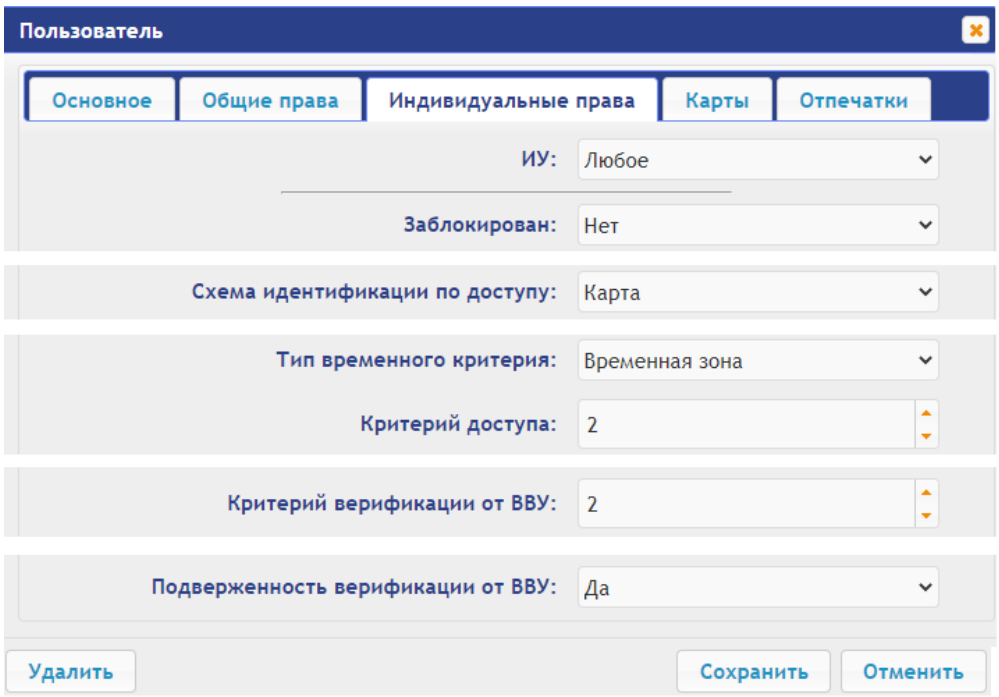


3. В разделе **Конфигурация** → **Редактировать** → **Внутренние реакции** добавьте внутреннюю реакцию:
   - **Тип источника** – **Запрос на верификацию ВВУ**,
   - **Номер источника** – **1** (номер ИУ, к которому физически подключен пирометр),
   - **Номер направления** – **1** (направление прохода, контролируемое пирометром),
   - **Тип приемника** – **Активизируемый выход**,
   - **Номер приемника** – **1** (номер ресурса, указанный в разделе **Физические контакты** для выхода контроллера, к которому физически подключен вход пирометра «ИЗМЕРЕНИЕ»),
   - **Характеристика реакции** – **Время срабатывания**:

SEC.RU | Короткий путь к информации Скачано с sec.ru



4. В разделе *Web*-интерфейса **Доступ** в подразделе **Пользователи** задайте всем картам обязательную верификацию. Для этого для каждой карты на вкладке **Индивидуальные права** для ИУ и направления прохода, контролируемого пирометром, для параметра **Подверженность верификации от ВВУ** установите значение **Да** и установите необходимый **Тип временного критерия** и **Критерий верификации от ВВУ** (по умолчанию – критерий **2**: временная зона "Всегда"):



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Приложение 3. Подключение и настройка контроллера *PERCo-CL15.1* для работы с картоприемником *PERCo-IC05*

Имеется возможность подключения двух контроллеров ***PERCo-CL15.1*** для управления турникетом и картоприемником ***PERCo-IC05***. При этом следует иметь в виду, что в данной конфигурации не предусмотрен считыватель, встраиваемый в картоприемник, т.е. изъятие карты картоприемником будет производиться после ее поднесения к считывателю ***PERCo-CL15.1***, контролируемого направление прохода, к которому привязан картоприемник.

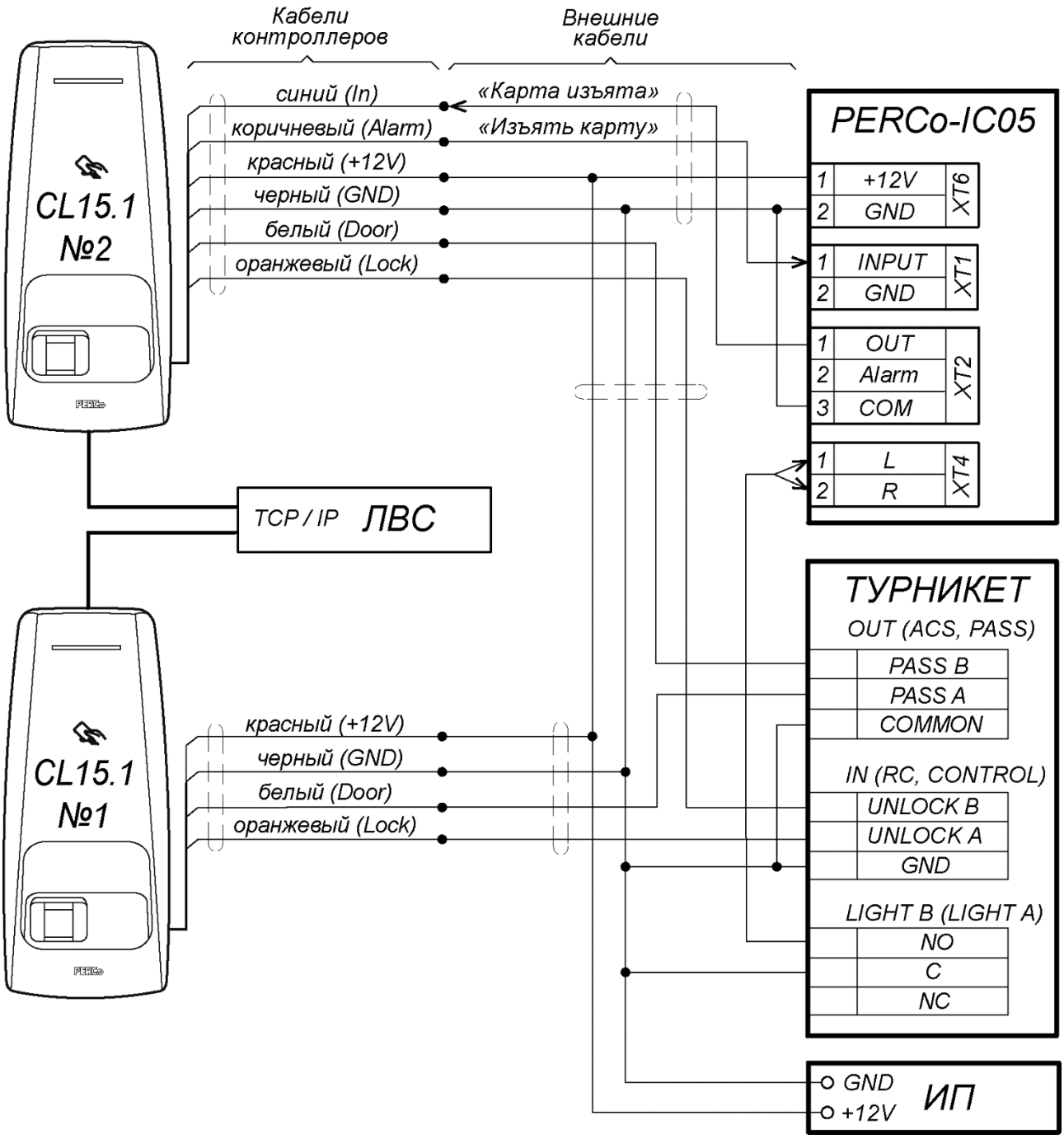


Рисунок 15. Схема подключения *PERCo-CL15.1* к турникету с картоприемником *PERCo-IC05*

SEC.RU | Короткий путь к информации
Скачано с sec.ru

В *Web*-интерфейсе контроллера, к которому физически подключен картоприемник, настройте следующие параметры:

1. В разделе **Конфигурация → Редактировать → Исполнительные устройства** выберите исполнительное устройство (**Односторонний замок**), в открывшемся окне выберите вкладку **Доступ по направлению** и для **Направления 1** установите:
   - в группе параметров **Верификация** для параметра **От ВВУ при запросе на проход сотрудника** – значение **Да**, для параметра **Работа при отсутствии ответа от ВВУ** – значение **Запрет**, а также необходимые значения для параметров **Время ожидания от ВВУ**, **Запуск верификации ВВУ для посетителей**;
   - В таблице источников для **Источника 1** в первой строке установите значение **ВВУ**.
2. В разделе **Конфигурация → Редактировать → Физические контакты**:
   - для входа **In**, к которому физически подключен выход картоприемника «Карта Изъята» (синий провод), установите следующие значения параметров:
     - **Функция:** – **Вход подтверждения от ВВУ**,
     - **Ресурс:** – **1** (номер ИУ, к которому физически подключен картоприемник),
     - **Направление:** – **1**,
     - **Нормальное состояние:** – **Разомкнут**;
   - для выхода **OUT2**, к которому физически подключен вход картоприемника «Изъять карту» (коричневый провод), установите следующие значения параметров:
     - **Функция:** – **Выход обычный**,
     - **Ресурс:** – **1**,
     - **Направление:** – **1**,
     - **Нормальное состояние:** – **Не запитан**.
3. В разделе **Конфигурация → Редактировать → Внутренние реакции** добавьте следующую внутреннюю реакцию:
   - **Тип источника** – **Запрос на верификацию ВВУ**,
   - **Номер источника** – **1**,
   - **Номер направления** – **1**,
   - **Тип приемника** – **Активизируемый выход**,
   - **Номер приемника** – **1** (номер выхода, к которому физически подключен вход картоприемника «Изъять карту»),
   - **Характеристика реакции** – **Время срабатывания**.
4. Временные карты для посетителей можно выдавать в разделе **Допуск → Пользователи**. При добавлении нового пользователя:
   - на вкладке **Карты** выдайте ему карту доступа,
   - на вкладке **Общие права** выберите **Тип:** – **Посетитель**,
   - на вкладке **Индивидуальные права** для **ИУ 1** и **Направления 1** задайте соответствующие права доступа и критерии верификации, например:
     - для параметра **Заблокирован** – значение **Нет**,
     - **Схема идентификации по доступу** –**Карта**,
     - **Тип временного критерия** – **Временная зона**,
     - **Критерий доступа** – **2** (по умолчанию это временная зона **Всегда**),
     - **Критерий верификации от ВВУ** – **2**,
     - для параметра **Подверженность верификации от ВВУ:** установите значение **Да**.

Внимание!

После данной настройки контроллера в *Web*-интерфейсе можно осуществлять дальнейшее конфигурирование точки прохода через турникет с картоприемником в ПО ***PERCo-Web***.

Картам посетителей, подлежащим изъятию, необходимо установить в ПО обязательный процесс верификации при предъявлении их к считывателю направления, контролируемого картоприемником.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Приложение 4. *Web*-интерфейс контроллера *PERCo-CL15.1*. Руководство пользователя

СОДЕРЖАНИЕ

1. ВОЗМОЖНОСТИ *WEB*-ИНТЕРФЕЙСА 40
2. ПОДКЛЮЧЕНИЕ К *WEB*-ИНТЕРФЕЙСУ КОНТРОЛЛЕРА 41
3. НАСТРОЙКА 42
   - 3.1 Изменение системного времени контроллера 42
   - 3.2 Изменение сетевых настроек контроллера 43
   - 3.3 Изменение настроек сервера 43
   - 3.4 Задание пароля доступа к контроллеру 43
   - 3.5 Формат считывания идентификаторов карт 44
4. КОНФИГУРАЦИЯ 44
   - 4.1 Выбор шаблона конфигурации контроллера 44
   - 4.2 Настройка параметров ресурсов контроллера 45
     - 4.2.1 Исполнительные устройства 45
     - 4.2.2 Физические контакты (входы и выходы) 45
     - 4.2.3 Считыватель 46
     - 4.2.4 Внутренние реакции 48
     - 4.2.5 Фильтры событий 49
5. ОФОРМЛЕНИЕ ДОСТУПА 50
   - 5.1 Временные критерии 50
     - 5.1.1 Временные зоны 50
     - 5.1.2 Праздничные дни 51
     - 5.1.3 Недельные графики 52
     - 5.1.4 Скользящий подневной график 53
     - 5.1.5 Скользящий понедельный график 54
   - 5.2 Пользователи 55
6. УПРАВЛЕНИЕ ИУ 56
7. СОБЫТИЯ 57
8. СОСТОЯНИЕ 58
9. СЕРВИС 58

1. ВОЗМОЖНОСТИ *WEB*-ИНТЕРФЕЙСА

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

- Изменять сетевые настройки, пароль доступа и время встроенных часов контроллера.
- Задавать параметры конфигурации ИУ и других ресурсов контроллера.
- Устанавливать РКД для ИУ.
- 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, просматривать журнал событий.
- Проводить диагностику контроллера, форматирование его памяти и обновление его встроенного ПО.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. ПОДКЛЮЧЕНИЕ К *WEB*-ИНТЕРФЕЙСУ КОНТРОЛЛЕРА

Связь между контроллером и компьютером осуществляется по интерфейсу *Ethernet* (IEEE 802.3). Убедитесь, что компьютер, с которого осуществляется подключение и контроллер, находятся в одной подсети *Ethernet.* Может потребоваться изменить сетевые настройки компьютера, настройки используемого браузера и проверить работу сети. IP-адрес контроллера указан в паспорте и на плате контроллера.

Для подключения к *Web*-интерфейсу контроллера:

1. Откройте *Web*-браузер (например, *Internet Explorer*).

Примечание:

Web-интерфейс тестировался в совместной работе с *Web*-браузерами: *Microsoft IE* версии 10 или выше, *Google Chrome* версии 32 или выше, *Mozilla Firefox* версии 32 или выше, *Opera* версии 30 или выше, *Microsoft Edge* и для *MacOS Apple Safari 9* или выше. При использовании других браузеров и устаревших версий возможна некорректная работа *Web*-интерфейса.

Внимание!

Для подключения к *Web*-интерфейсу контроллера с помощью браузера *MacOS Safari необходимо* в текстовом редакторе *TextEdit* настроить кодировку для файла простого текста – **Кириллическая (Windows)**.

2. Введите в адресную строку IP-адрес контроллера и нажмите кнопку **Enter** на клавиатуре. При необходимости введите пароль доступа к контроллеру. По умолчанию пароль отсутствует.
3. Откроется главная страница *Web*-интерфейса контроллера. На главной странице отображается модель, конфигурация, сетевые настройки контроллера и версия встроенного ПО. При каждой загрузке главной страницы на ней отображаются текущие данные, считанные с контроллера. Страница имеет следующий вид:



На странице можно выделить следующие элементы:

1. Панель заголовка страницы содержит логотип компании ***PERCo*** и кнопки выбора языка *Web*-интерфейса. Нажатием на логотип компании ***PERCo*** осуществляется переход на главную страницу из других разделов *Web*-интерфейса.
2. Боковая панель навигации *Web*-интерфейса.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Панель имеет следующую структуру:

«Настройки»	*«Время»*	
	«Сеть»	
	«Сервер»	
	«Пароль доступа»	
	«Формат карты»	
«Конфигурация»	*«Шаблон»*	
	«Редактировать»	*«Исполнительные устройства»*
		«Физические контакты»
		«Считыватели»
		«Внутренние реакции»
		«Фильтры событий»
«Доступ»	*«Временные критерии»*	*«Временные зоны»*
		«Праздничные дни»
		«Недельные графики»
		«Скользящий подневной»
		«Скользящий понедельный»
	«Пользователи»	
«Управление ИУ»		
«События»		
«Состояние»		
«Сервис»		

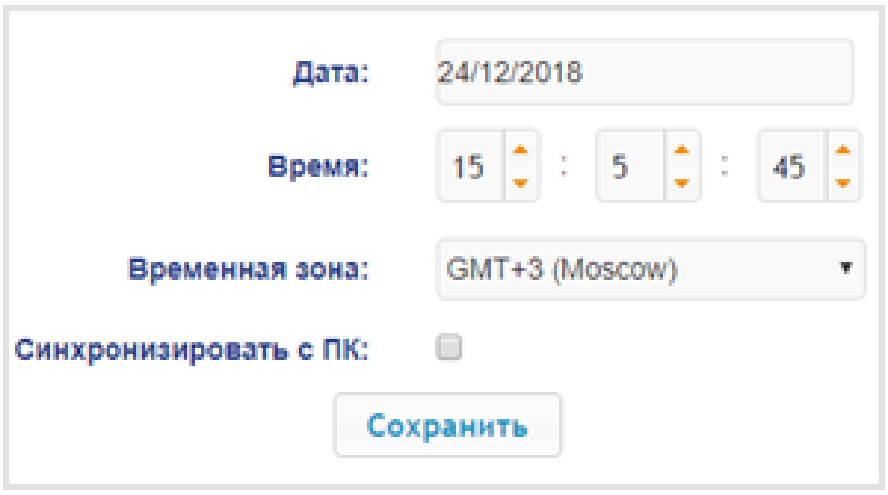
3. Рабочая область страницы.

3. НАСТРОЙКА

3.1 Изменение системного времени контроллера

Для изменения времени выполните следующие действия:

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



2. В полях ввода **Дата** и **Время** измените установленные значения.
3. Выберите необходимое значение для параметра **Временная зона.**
4. Для синхронизации времени и даты контроллера с установленными параметрами на подключенном к *Web*-интерфейсу компьютере установите флажок у параметра **Синхронизировать с ПК:**.
5. Нажмите кнопку **Сохранить**. Внесенные изменения будут сохранены.

SEC.RU | Короткий путь к информации Скачано с sec.ru

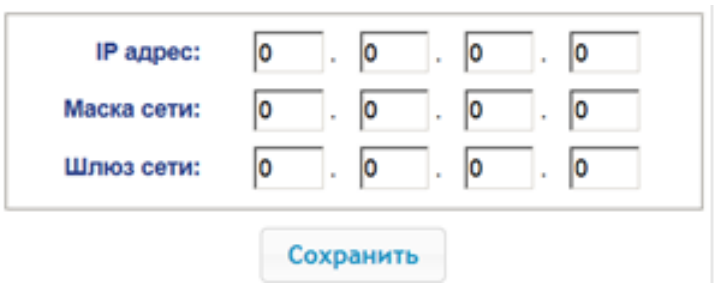
3.2 Изменение сетевых настроек контроллера

При поставке контроллер имеет следующие заводские установки (указаны в паспорте изделия и на наклейках на самом контроллере):

- уникальный MAC-адрес `00-25-0B-xx-xx-xx`, где `xx` – число от `00` до `FE`;
- уникальный IP-адрес `10.x.x.x`, где `x` – число от 0 до 254;
- маска подсети `255.0.0.0`.

Для изменения сетевых настроек контроллера:

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

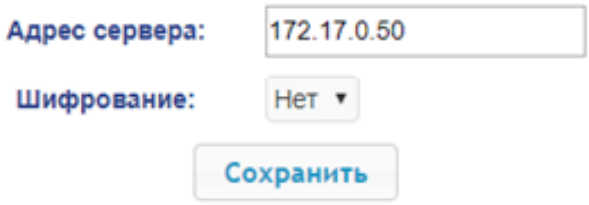


2. В поля ввода **IP-адрес**, **Маска подсети** и **Шлюз сети** введите новые значения сетевых параметров контроллера.
3. Нажмите кнопку **Сохранить**. Новые сетевые настройки будут сохранены в контроллере.

3.3 Изменение настроек сервера

Для изменения настроек севера выполните следующие действия:

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

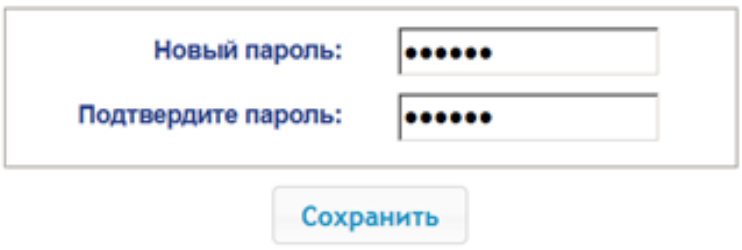


2. В открывшемся окне произведите необходимые изменения для параметров:
   - в параметре **Адрес сервера** задается адрес сервера.
   - в параметре **Шифрование** задается способ шифрования: **Нет** или **SSL**.
3. Нажмите кнопку **Сохранить**. Внесенные изменения будут сохранены.

3.4 Задание пароля доступа к контроллеру

По умолчанию пароль доступа к контроллеру не задан. Для смены или задания нового пароля:

1. Нажмите последовательно в меню *Web*-интерфейса: **Настройки → Пароль доступа**. 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**. Новый пароль будет сохранен в контроллере.

SEC.RU | Короткий путь к информации Скачано с sec.ru

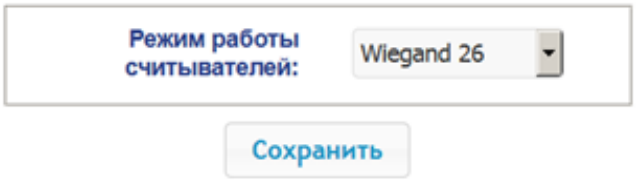
3.5 Формат считывания идентификаторов карт

Внимание!

- Изменение данного параметра при уже введенных картах доступа приведет к тому, что проход по этим картам будет невозможен.
- При подключении к контроллеру, работавшему под управлением ПО систем ***PERCo***, текущий формат может быть не показан (не будет выбран ни один из форматов). В этом случае формат считывания идентификаторов карт менять **ЗАПРЕЩАЕТСЯ**.

Для выбора формата считывания идентификаторов карт доступа:

1. Нажмите последовательно в меню *Web*-интерфейса: **Настройки→ Формат карт**. Откроется страница с рабочей областью следующего вида:



2. С помощью выпадающего списка **Режим работы считывателей** выберите один из предложенных режимов и нажмите кнопку **Сохранить**. Внесенные изменения будут сохранены.

4. КОНФИГУРАЦИЯ

4.1 Выбор шаблона конфигурации контроллера

Внимание!

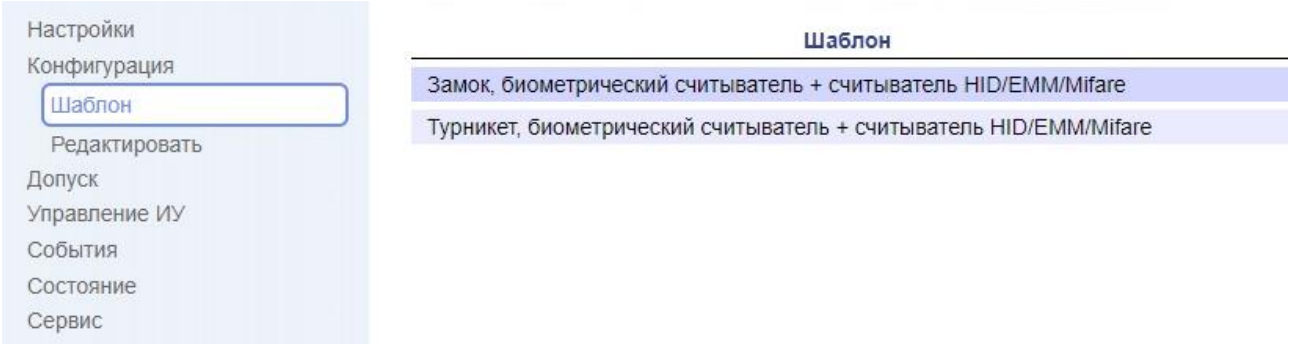
При смене шаблона происходит удаление предыдущей конфигурации и ранее установленных внутренних реакций всех ресурсов контроллера. В новом шаблоне для ресурсов контроллера устанавливается предусмотренная для данного шаблона конфигурация “по умолчанию”. При этом список загруженных идентификаторов карт доступа, а также связанные с ними данные пользователей, права и параметры доступа сохраняются.

Для контроллера ***PERCo-CL15.1*** доступно два шаблона конфигурации:

- **Замок, биометрический считыватель + считыватель HID / EMM / Mifare;**
- **Турникет, биометрический считыватель + считыватель HID / EMM / Mifare;**

Для изменения конфигурации контроллера:

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



2. В рабочей области страницы выберите необходимый вариант конфигурации. Смена шаблона конфигурации может занимать до 30 секунд.

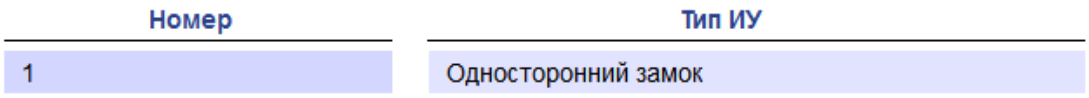
SEC.RU | Короткий путь к информации Скачано с sec.ru

4.2 Настройка параметров ресурсов контроллера

4.2.1 Исполнительные устройства

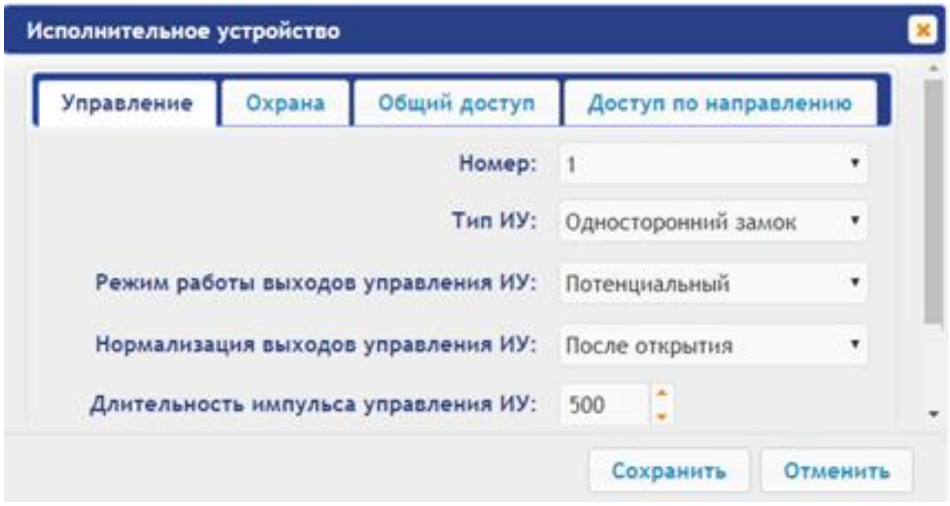
Для настройки параметров ресурсов контроллера для управления ИУ:

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



Номер	Тип ИУ
1	Односторонний замок

2. Для изменения параметров ИУ нажмите на строку с его наименованием (**Односторонний замок**). Откроется новое окно:

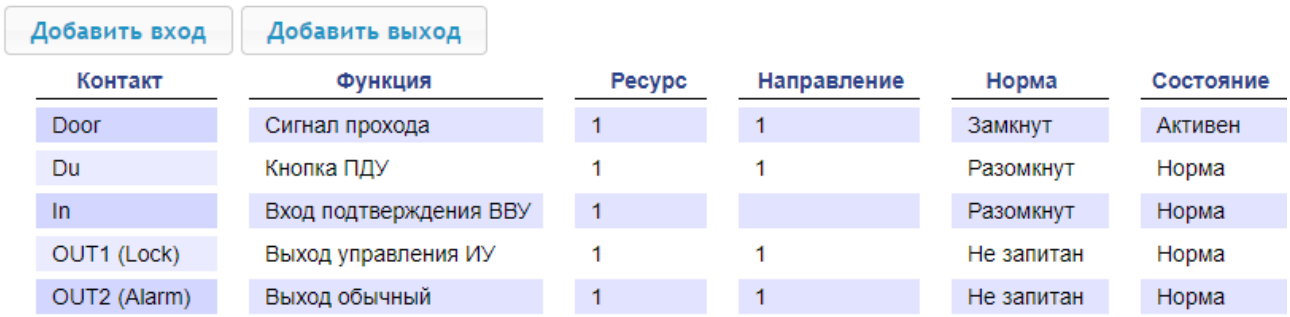


3. В открывшемся окне на вкладках **Управление**, **Охрана**, **Общий доступ**, **Доступ по направлению** произведите необходимые изменения параметров.
4. Нажмите кнопку **Сохранить**. Окно будет закрыто, измененные параметры будут переданы в контроллер.
5. Для выхода без сохранения внесенных изменений нажмите кнопку **Отменить** или кнопку **Close** .

4.2.2 Физические контакты (входы и выходы)

Для настройки параметров входов и выходов контроллера:

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



Контакт	Функция	Ресурс	Направление	Норма	Состояние
Door	Сигнал прохода	1	1	Замкнут	Активен
Du	Кнопка ПДУ	1	1	Разомкнут	Норма
In	Вход подтверждения ВВУ	1		Разомкнут	Норма
OUT1 (Lock)	Выход управления ИУ	1	1	Не запитан	Норма
OUT2 (Alarm)	Выход обычный	1	1	Не запитан	Норма

На странице перечислены все входы и выходы контроллера.

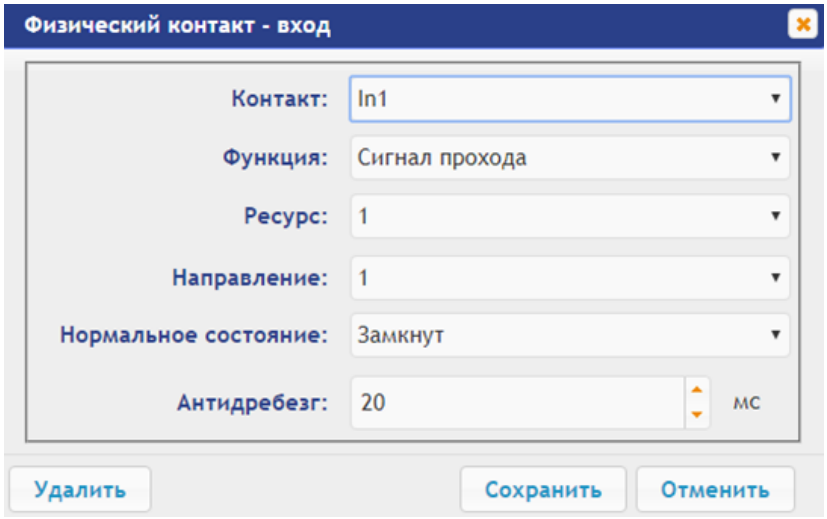
SEC.RU | Короткий путь к информации Скачано с sec.ru

По умолчанию входам и выходам, которые задействованы в управлении ИУ (замком), установлены соответствующие функции (для входов – Кнопка ПДУ/ Сигнал прохода, для выходов – управления ИУ / индикации ПДУ) и задаются номер и направление ИУ, к которому привязан данный физический контакт. Входам и выходам, которые не задействованы в выбранном шаблоне, устанавливается значение **Вход/Выход обычный**. Эти выходы и входы доступны для задания (и изменения в дальнейшем) своих функций.

Примечание:

Возвратиться к заводским установкам по умолчанию можно, перезагрузив шаблон конфигурации (см. п. 4.1 данного Приложения).

2. Для изменения параметров входа или выхода нажмите в рабочей области страницы на строку с его наименованием. Откроется окно **Физический контакт**:



3. В открывшемся окне произведите необходимые изменения для параметров:
   - в параметре **Контакт** задается контакт, к которому подключается внешнее оборудование;
   - в параметре **Функция** задается функция контакта для возможности работы с подключаемым оборудованием;
   - в параметре **Ресурс** задается ресурс контакта;
   - в параметре **Направление** задается направление ИУ, к которому привязывается считыватель контроллера**;**
   - в параметре **Нормальное состояние** задаётся нормальное состояние контакта – **разомкнут** или **замкнут** для входов и **запитан** или **не запитан** для выходов;
   - в параметре **Антидребезг** задаётся время антидребезга контакта (для входов).
4. Нажмите кнопку **Сохранить**. Окно с наименованием физического контакта будет закрыто, измененные параметры входа (выхода) будут переданы в контроллер.
5. Для выхода из окна физического контакта без сохранения изменений нажмите кнопку **Отменить**. Также закрыть окно можно при помощи кнопки **Close** .

4.2.3 Считыватель

В обоих шаблонах конфигурации контроллера определены один встроенный мультиформатный считыватель *HID* / *EMM* / *Mifare* и один сканер отпечатков пальцев *Morpho*.

Внимание!

Во избежание некорректной работы изделия не изменяйте параметры встроенного считывателя №1, задействованного в управлении ИУ!

При необходимости, возвратиться к заводским установкам по умолчанию можно, перезагрузив шаблон конфигурации (см. п. 4.1 данного Приложения).

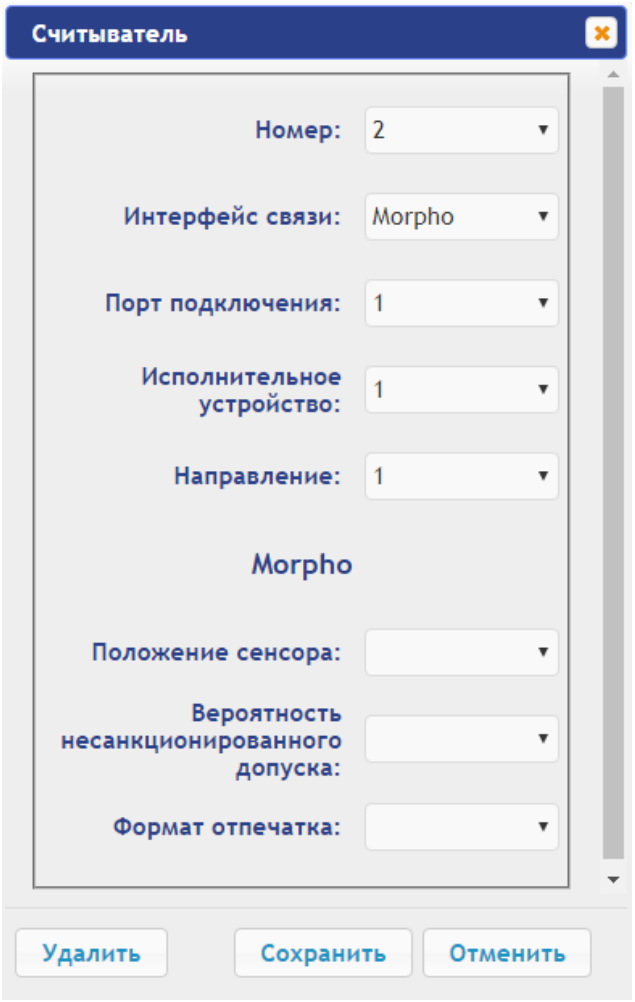
SEC.RU | Короткий путь к информации Скачано с sec.ru

Для изменения параметров сканера отпечатков пальцев выполните следующие действия:

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



2. Нажмите в рабочей области страницы на строку сканера с наименованием **morpho**. Откроется окно **Считыватель**:



3. В открывшемся окне произведите необходимые изменения для параметров сканера *Morpho*:
   - в параметре **Положение сенсора** задается положение, в котором сканер будет производить идентификацию и верификацию для пальца с учётом его возможного разворота;
   - в параметре **Вероятность несанкционированного допуска** задается вероятность несанкционированного допуска (ошибка первого рода), выраженное в процентах число допусков системой неавторизованных лиц;
   - в параметре **Формат отпечатка** задается формат отпечатков.
4. Для передачи измененных параметров в контроллер нажмите кнопку **Сохранить**. Окно **Считыватель** будет закрыто.
5. Для выхода из окна **Считыватель** без сохранения изменений нажмите кнопку **Отменить**. Также закрыть окно можно при помощи кнопки **Close** .

SEC.RU | Короткий путь к информации Скачано с sec.ru

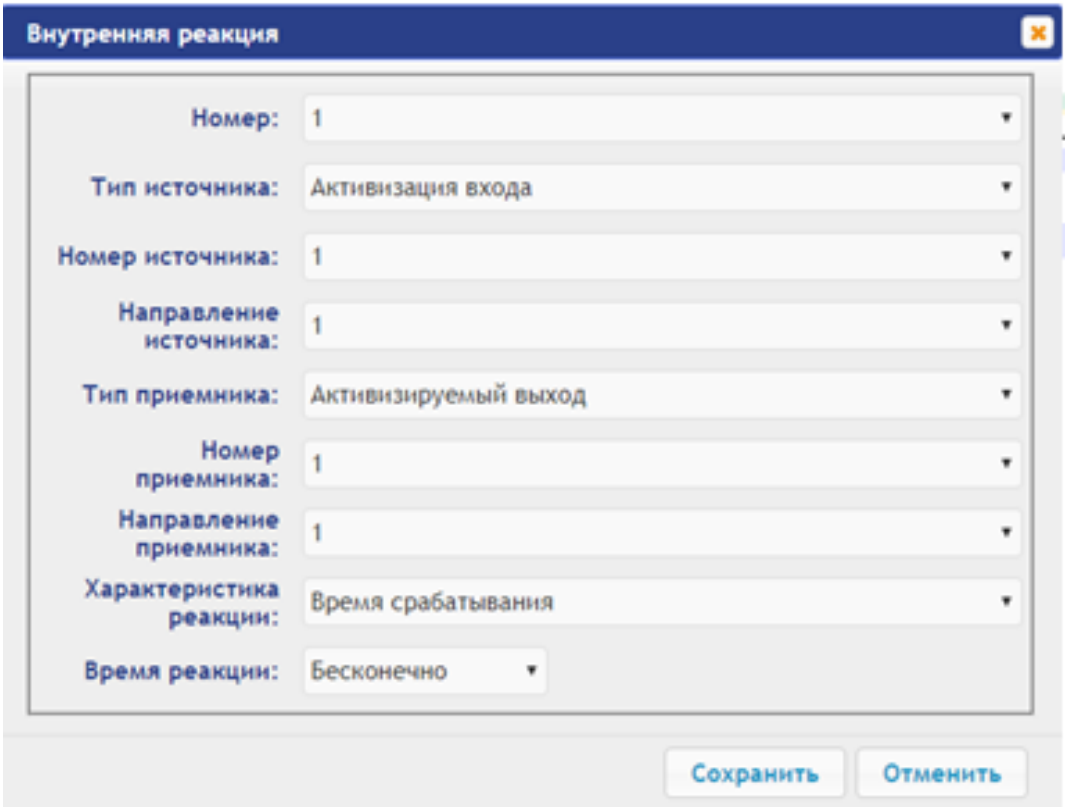
4.2.4 Внутренние реакции

Для настройки внутренних реакций контроллера:

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



2. Для добавления новой внутренней реакции нажмите кнопку **Добавить**, для изменения параметров внутренней реакции или ее удаления нажмите в рабочей области страницы на строку с ее наименованием. Откроется окно **Внутренняя реакция**:



3. В открывшемся окне произведите необходимые изменения параметров:
   - в параметре **Номер** задается номер реакции в БД контроллера (от 1 до 40);
   - в параметре **Тип источника** задается условие запуска реакции контроллера;
   - в параметре **Номер источника** (**приемника**) и **Направление источника** (**приемника**) задаются номера и направления соответствующих ресурсов контроллера, которые являются источниками (приемниками) данной реакции;
   - в параметре **Тип приемника** задается реакция контроллера при возникновении условия запуска реакции;
   - в параметре **Характеристика реакции** и **Время реакции** задаются соответствующие параметры реакции.
4. Для сохранения и передачи измененных параметров в контроллер нажмите кнопку **Сохранить**. Окно **Внутренняя реакция** будет закрыто.
5. Для выхода из окна **Внутренняя реакция** без сохранения изменений нажмите кнопку **Отменить**. Также закрыть окно можно при помощи кнопки **Close** .

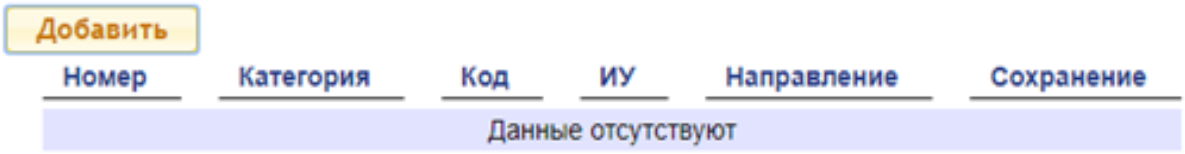
SEC.RU | Короткий путь к информации Скачано с sec.ru

6. Для удаления внутренней реакции из списка нажмите в рабочей области страницы на строку с ее наименованием, откроется окно **Внутренняя реакция.** Нажмите кнопку **Удалить**. Окно **Внутренняя реакция** будет закрыто, выбранная внутренняя реакция будет удалена.

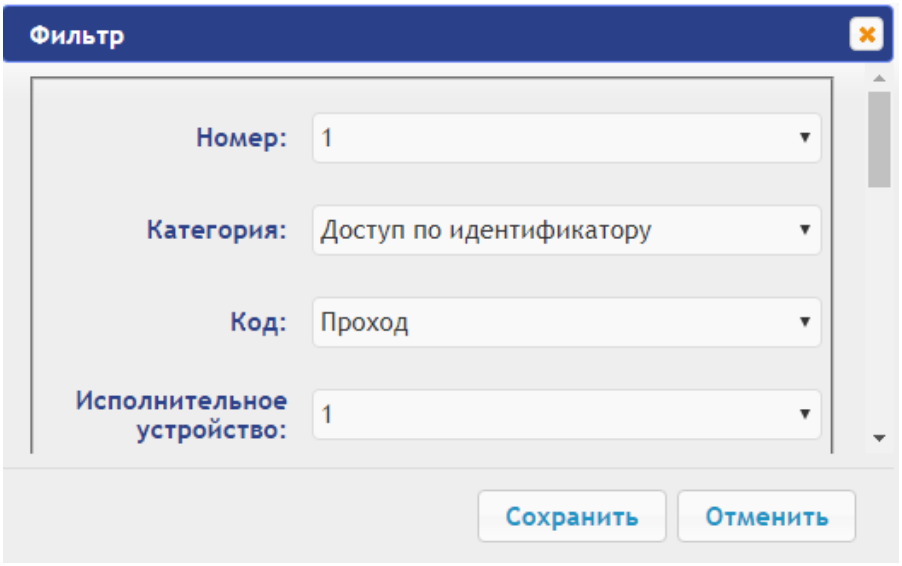
4.2.5 Фильтры событий

Для настройки фильтров событий выполните следующие действия:

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



2. Для добавления нового фильтра нажмите кнопку **Добавить**, для изменения параметров или удаления фильтра нажмите в рабочей области страницы на строку с его наименованием. Откроется окно **Фильтр**:



3. В открывшемся окне произведите необходимые изменения для параметров:
   - в параметре **Номер** задается номер фильтра (от 1 до 20);
   - в параметре **Категория** задается категорию события;
   - в параметре **Код** задается код события;
   - в параметре **Исполнительное устройство** задается номер ИУ, к которому привязан считыватель;
   - в параметре **Направление** задается направление ИУ, к которому привязывается считыватель;
   - в параметре **Доступ** задается валидность пользователя: запрещен или просрочен;
   - в параметре **Пользователь** задается тип пользователя: посетитель / сотрудник / ТС;
   - в параметре **Тревожность** задается тревожность: да или нет;
   - в параметре **Нарушение времени** и **Нарушение местоположения** задается возможность нарушения времени или местоположения: да или нет;
   - в параметре **Нарушение идентификации** задается причина нарушения идентификации: нет карты / нет пальца / не та карта / неизвестный палец / нет отпечатков пользователя в БД;
   - в параметре **Подтверждение** задается способ подтверждения: одинарное / двойное / нарушение-нет UID / нарушение-неправильный UID / двойное с нарушением — нет UID / двойное с нарушением — неправильный UID / нарушение — взлом / запрет командой ПДУ;

SEC.RU | Короткий путь к информации Скачано с sec.ru

- в параметре **Верификация** задается верификация: подтверждение / отказ счетчик проходов / отказ ПДУ / отказ ВВУ / отказ ПО / таймаут верификации / нет ответа счётчик прохода / нет ответа ПДУ / нет ответа ВВУ / нет ответа ПО / нарушение — взлом;
- в параметре **Сохранять** задается возможность сохранения в БД события, если оно проходит через фильтр (совпадение всех установленных полей фильтра с соответствующими полями в событии (если какое-либо поле в фильтре не установлено, то сравнения по нему не производится)). Если в поле "Сохранять" установить "да", то такое событие будет сохранено в БД, в противном случае не будет.

4. Для сохранения фильтра нажмите кнопку **Сохранить**. Окно **Фильтр** будет закрыто.
5. Для выхода из окна **Фильтр** без сохранения изменений нажмите кнопку **Отменить**. Также закрыть окно можно при помощи кнопки **Close** .
6. Для удаления фильтра из списка нажмите в рабочей области страницы на строку с его наименованием, откроется окно **Фильтр.** Нажмите кнопку **Удалить**. Окно **Фильтр** будет закрыто, выбранная фильтр будет удален.

5. ОФОРМЛЕНИЕ ДОСТУПА

5.1 Временные критерии

5.1.1 Временные зоны

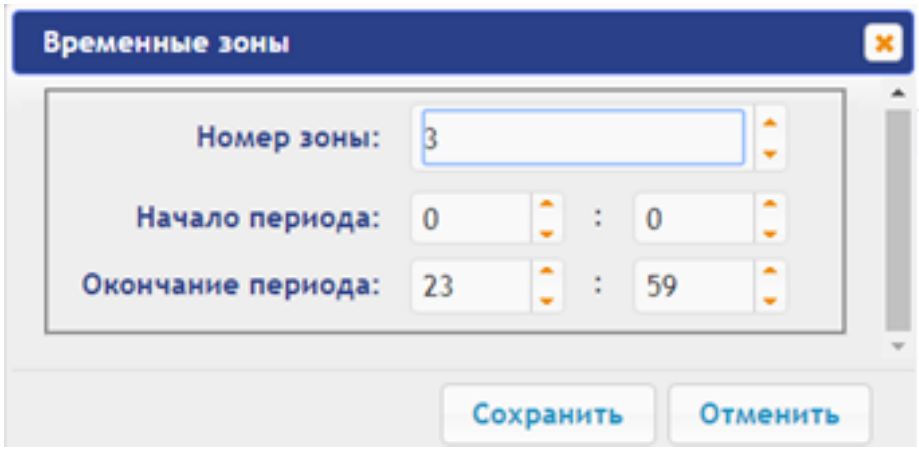
Есть две предопределённые временные зоны - №1 - «Никогда» и №2 - «Всегда».

Для настройки временных зон выполните следующие действия:

1. Нажмите последовательно в меню *Web*-интерфейса: **Доступ → Временные критерии → Временные зоны.** Откроется страница с рабочей областью следующего вида:



2. Для добавления новой временной зоны нажмите кнопку **Добавить**, для изменения параметров временной зоны или ее удаления нажмите в рабочей области страницы на строку с ее наименованием. Откроется окно **Временные зоны:**



3. В открывшемся окне произведите необходимые изменения для параметров:
   - в параметре **Номер зоны** задается порядковый номер временной зоны;
   - в параметре **Начало периода** задается начало периода;
   - в параметре **Окончание периода** задается конец периода.
4. Для сохранения временной зоны и передачи параметров в контроллер нажмите кнопку **Сохранить**. Окно **Временные зоны** будет закрыто.

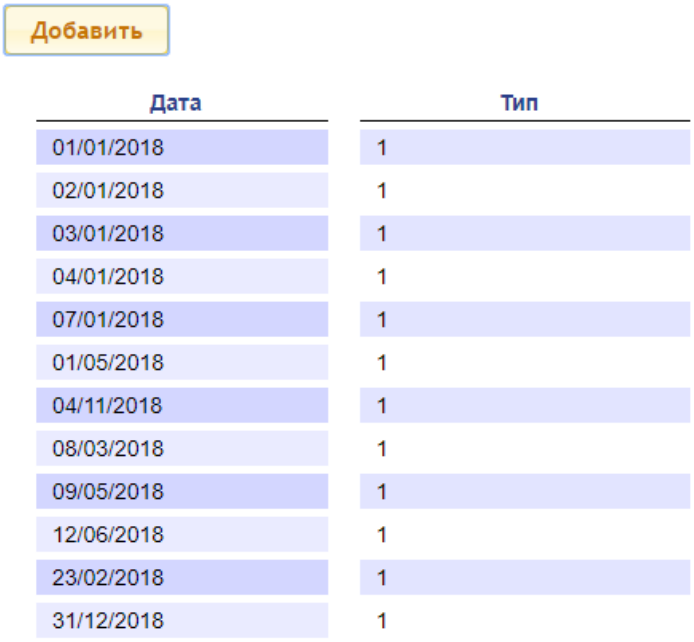
SEC.RU | Короткий путь к информации
Скачано с sec.ru

5. Для выхода из окна **Временные зоны** без сохранения изменений нажмите кнопку **Отменить**. Также закрыть окно можно при помощи кнопки **Close** .
6. Для удаления временной зоны из списка нажмите в рабочей области страницы на строку с ее наименованием, откроется окно **Временные зоны.** Нажмите кнопку **Удалить**. Окно **Временные зоны** будет закрыто, выбранная временная зона будет удалена.

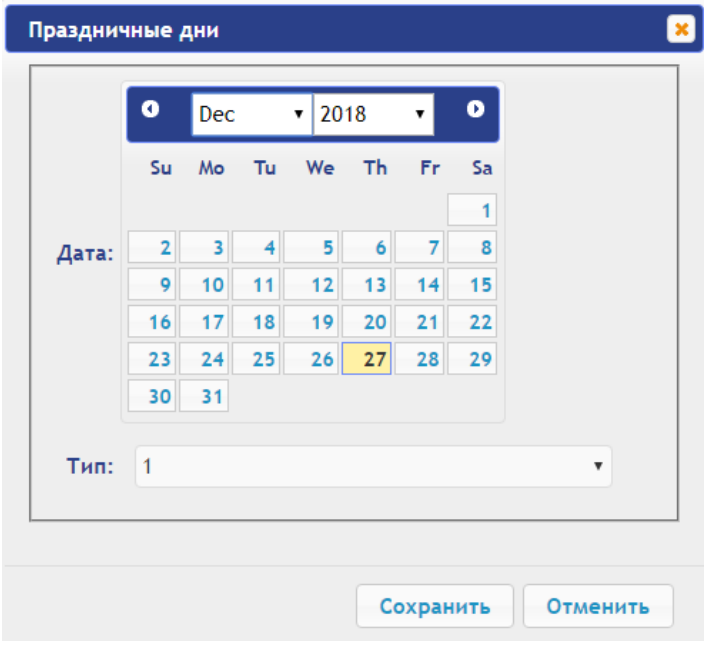
5.1.2 Праздничные дни

Для настройки праздничных дней выполните следующие действия:

1. Нажмите последовательно в меню *Web*-интерфейса: **Доступ → Временные критерии → Праздничные дни.** Откроется страница с рабочей областью следующего вида:



2. Для добавления нового праздничного дня нажмите кнопку **Добавить**, для изменения параметров праздничного дня или его удаления нажмите в рабочей области страницы на строку с его наименованием. Откроется окно **Праздничные дни:**



3. В открывшемся окне выберите дату и **Тип** праздника.
4. Для сохранения изменений и передачи параметров в контроллер нажмите кнопку **Сохранить**. Окно **Праздничные дни** будет закрыто.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5. Для выхода из окна **Праздничные дни** без сохранения изменений нажмите кнопку **Отменить**. Также закрыть окно можно при помощи кнопки **Close** .
6. Для удаления праздничного дня из списка нажмите в рабочей области страницы на строку с его наименованием, откроется окно **Праздничные дни.** Нажмите кнопку **Удалить**. Окно **Праздничные дни** будет закрыто, выбранный праздничный день будет удален.

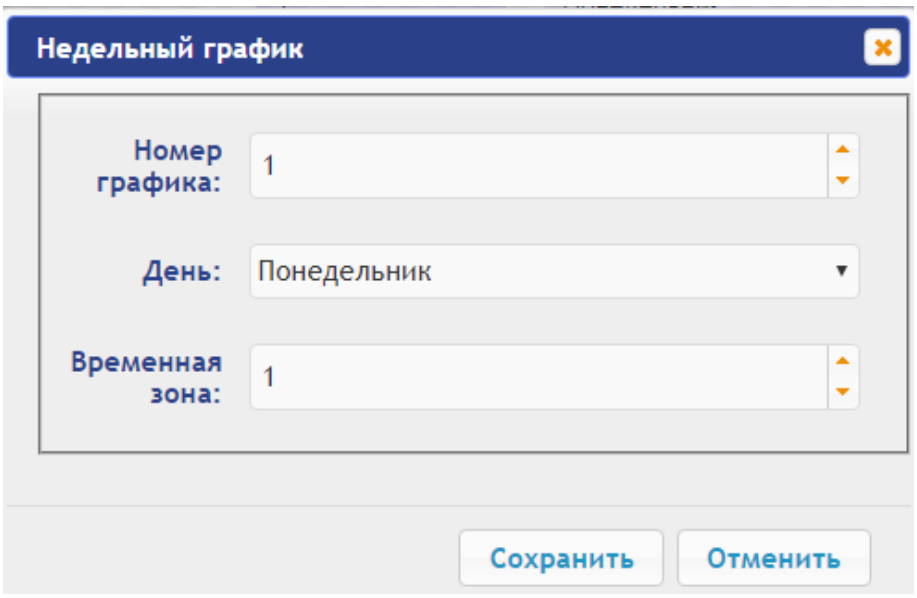
5.1.3 Недельные графики

Для настройки недельных графиков выполните следующие действия:

1. Нажмите последовательно в меню *Web*-интерфейса: **Доступ → Временные критерии → Недельный график.** Откроется страница с рабочей областью следующего вида:



2. Для добавления нового недельного графика нажмите кнопку **Добавить**, для изменения параметров недельного графика или его удаления нажмите в рабочей области страницы на строку с его наименованием. Откроется окно **Недельный график:**



SEC.RU | Короткий путь к информации Скачано с sec.ru

3. В открывшемся окне произведите необходимые изменения для параметров:
   - в параметре **Номер графика** задается номер графика;
   - в параметре **День** задается день недели;
   - в параметре **Временная зона** задается номер временной зоны для выбранного дня графика.
4. Для сохранения изменений и передачи параметров в контроллер нажмите кнопку **Сохранить**. Окно **Недельный график** будет закрыто.
5. Для выхода из окна **Недельный график** без сохранения изменений нажмите кнопку **Отменить**. Также закрыть окно можно при помощи кнопки **Close** .
6. Для удаления недельного графика из списка нажмите в рабочей области страницы на строку с его наименованием, откроется окно **Недельный график.** Нажмите кнопку **Удалить**. Окно **Недельный график** будет закрыто, выбранный график будет удален.

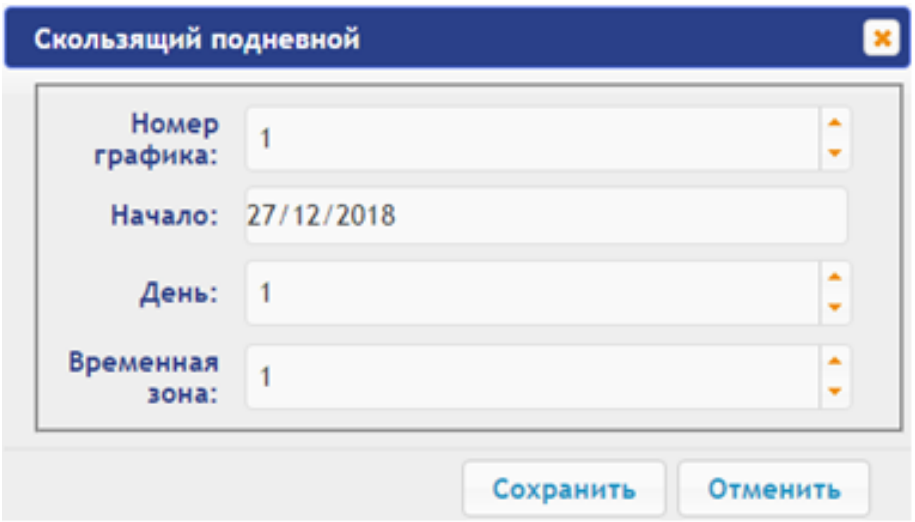
5.1.4 Скользящий подневной график

Для настройки скользящего подневного графика выполните следующие действия:

1. Нажмите последовательно в меню *Web*-интерфейса: **Доступ → Временные критерии → Скользящий подневной.** Откроется страница с рабочей областью следующего вида:



2. Для добавления нового скользящего подневного графика нажмите кнопку **Добавить**, для изменения параметров скользящего подневного графика или его удаления нажмите в рабочей области страницы на строку с его наименованием. Откроется окно **Скользящий подневной:**



3. В открывшемся окне произведите необходимые изменения для параметров:
   - в параметре **Номер графика** задается номер графика;
   - в параметре **Начало** задается дата начала действия графика;
   - в параметре **День** задается количество дней для данного графика;
   - в параметре **Временная зона** задается номер временной зоны для данного графика.
4. Для сохранения изменений и передачи параметров в контроллер нажмите кнопку **Сохранить.** Окно **Скользящий подневной** будет закрыто.
5. Для выхода из окна **Скользящий подневной** без сохранения изменений нажмите кнопку **Отменить**. Также закрыть окно можно при помощи кнопки **Close** .

SEC.RU | Короткий путь к информации Скачано с sec.ru

6. Для удаления графика из списка нажмите в рабочей области страницы на строку с его наименованием, откроется окно **Скользящий подневной**. Нажмите кнопку **Удалить**. Окно **Скользящий подневной** будет закрыто, выбранный график будет удален.

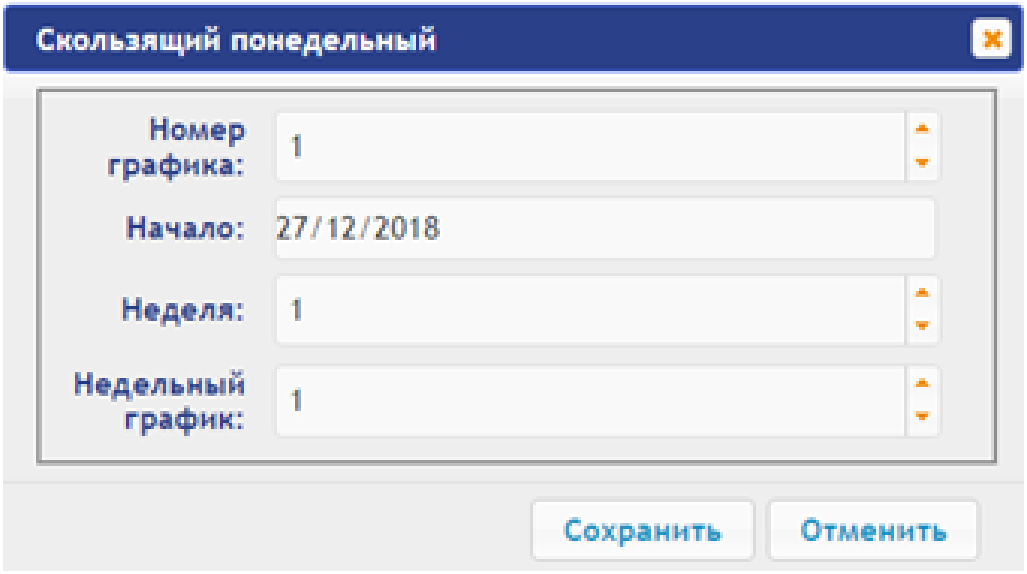
5.1.5 Скользящий понедельный график

Для настройки скользящего понедельного графика выполните следующие действия:

1. Нажмите последовательно в меню *Web*-интерфейса: **Доступ → Временные критерии → Скользящий понедельный.** Откроется страница с рабочей областью следующего вида:



2. Для добавления нового скользящего понедельного графика нажмите кнопку **Добавить**, для изменения параметров скользящего понедельного графика или его удаления нажмите в рабочей области страницы на строку с его наименованием. Откроется окно **Скользящий понедельный:**



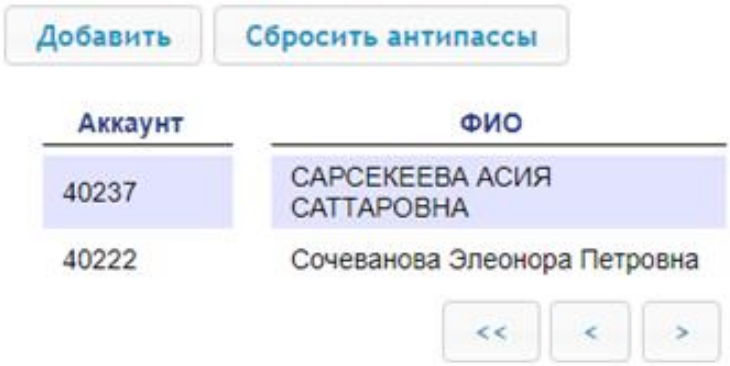
3. В открывшемся окне произведите необходимые изменения параметров:
   - в параметре **Номер графика** задается номер графика;
   - в параметре **Начало** задается дата начала действия графика;
   - в параметре **Неделя** задается количество недель для данного графика;
   - в параметре **Недельный график** задается номер временных критериев недельного графика для выбранной недели.
4. Для сохранения изменений и передачи параметров в контроллер нажмите кнопку **Сохранить**. Окно **Скользящий понедельный** будет закрыто.
5. Для выхода из окна **Скользящий понедельный** без сохранения изменений нажмите кнопку **Отменить**. Также закрыть окно можно при помощи кнопки **Close** .
6. Для удаления скользящего понедельного графика из списка нажмите в рабочей области страницы на строку с его наименованием, откроется окно **Скользящий понедельный.** Нажмите кнопку **Удалить**. Окно **Скользящий понедельный** будет закрыто, выбранный график будет удален.

SEC.RU | Короткий путь к информации Скачано с sec.ru

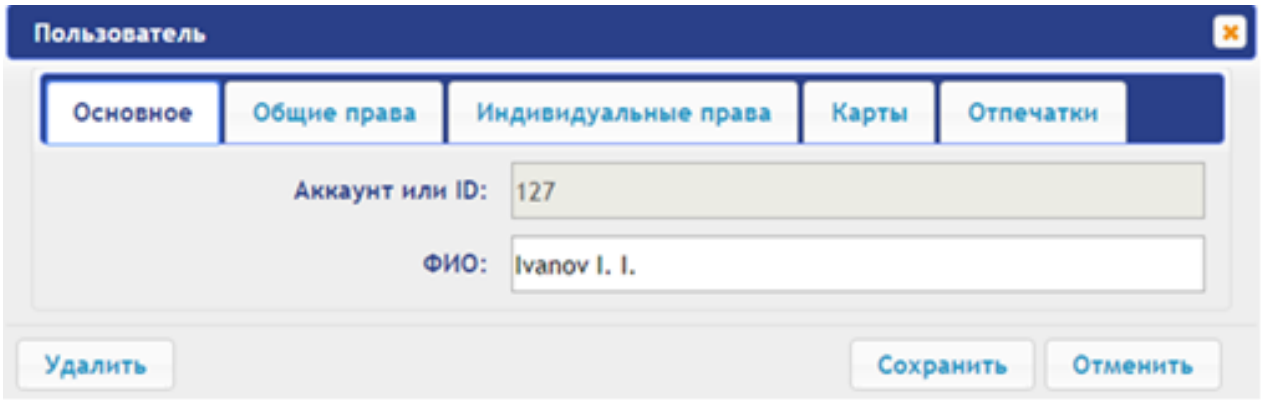
5.2 Пользователи

Для настройки информации о пользователях выполните следующие действия:

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



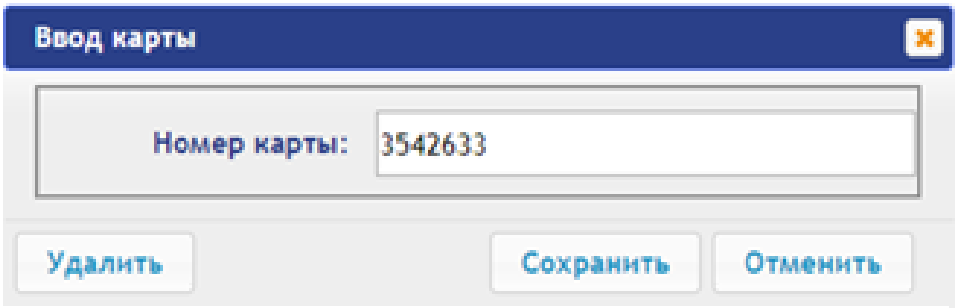
2. Для добавления нового пользователя нажмите кнопку **Добавить**, для изменения информации о пользователе или его удаления выберите необходимого пользователя в рабочей области страницы. Откроется окно **Пользователь:**



3. В открывшемся окне на вкладках **Основное**, **Общие права**, **Индивидуальные права** произведите необходимые изменения параметров.
4. С помощью вкладки **Карты** выдайте пользователю идентификатор. Для этого:

Ввод идентификаторов от считывателя:

- Предъявите карту одному из считывателей, входящих в конфигурацию контроллера. Откроется новое окно **Ввод карты**:



Для сохранения идентификатора нажмите кнопку **Сохранить**. Окно **Ввод карты** будет закрыто, идентификатор карты появится в рабочей области страницы.

Ввод идентификаторов вручную:

- В рабочей области страницы нажмите кнопку **Ввод вручную**. Откроется окно **Ввод карты**:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- В поле **Номер карты** введите идентификатор карты. Нажмите кнопку **Сохранить**. Окно **Ввод карты** будет закрыто, идентификатор карты появится в рабочей области страницы.

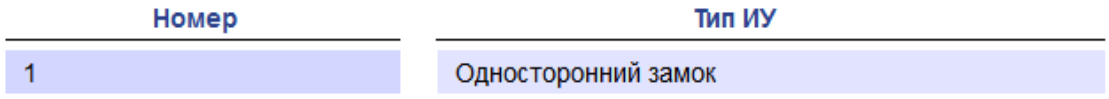
При необходимости аналогично добавьте другие карты.

5. С помощью вкладки **Отпечатки** присвойте пользователю отпечатки. Для этого:
   - Нажмите кнопку **Включить добавление** и поднесите палец к считывающему устройству.
   - Для удаления всех отпечатков нажмите кнопку **Удалить все.** Все отпечатки будут удалены из контроллера.
   - Для удаления отпечатков с карты *Mifare* нажмите **Очистить Mifare** и поднесите карту к считывателю. Отпечатки с карты будут удалены.
   - Для записи отпечатков на карту *Mifare* нажмите **Записать на Mifare** и поднесите карту к считывателю. Отпечатки из базы контроллера будут записаны на карту.
6. Для сохранения изменений и передачи параметров в контроллер нажмите кнопку **Сохранить**.

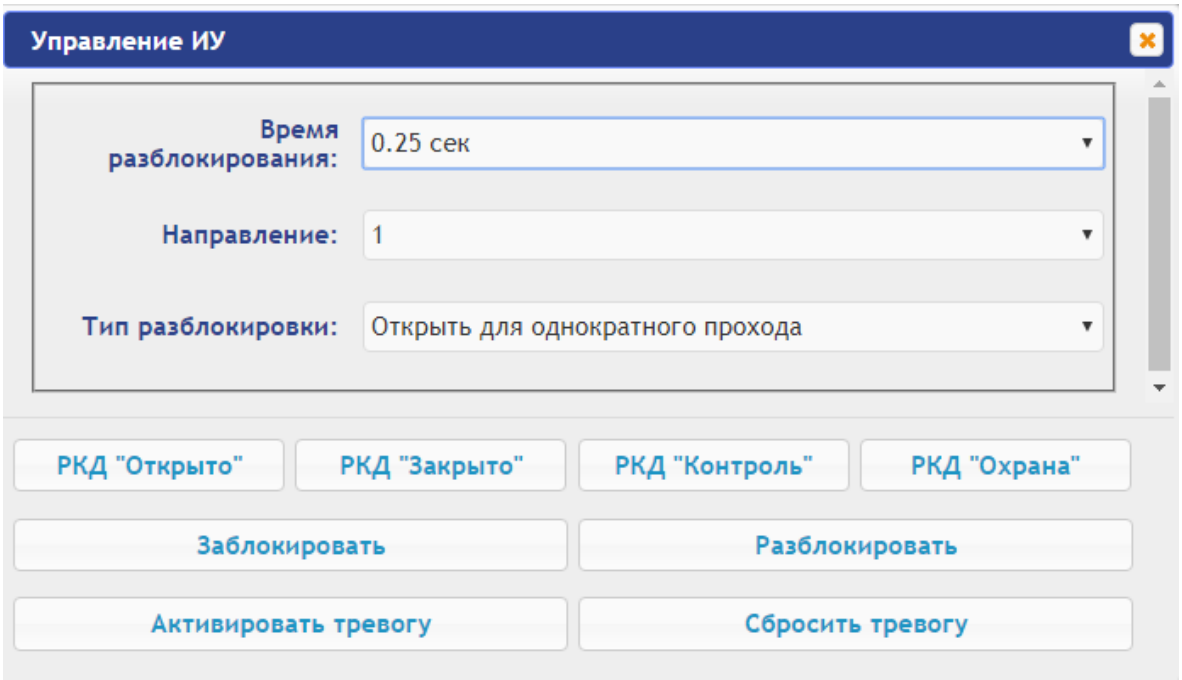
6. УПРАВЛЕНИЕ ИУ

Для управления ИУ и смены РКД в направлении, связанном с подключенным к нему считывателем, произведите следующие действия:

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



2. Нажмите в рабочей области страницы на строку с ИУ. Откроется окно управления ИУ:



3. С помощью кнопок в нижней части окна подайте нужную команду. Окно управления будет закрыто, команда будет передана в контроллер. Также закрыть окно без подачи команды можно при помощи кнопки **Close** .

Примечание:

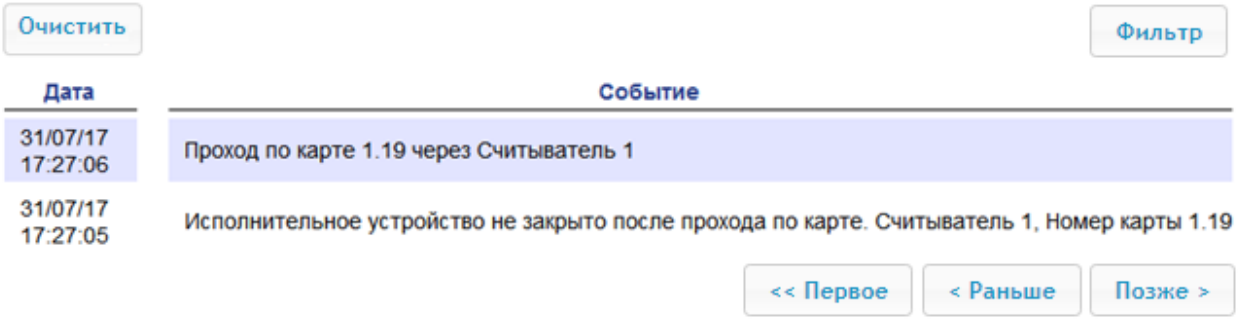
При разблокировке ИУ разблокируется на время, выбранное в раскрывающемся списке **Время разблокирования**.

SEC.RU | Короткий путь к информации Скачано с sec.ru

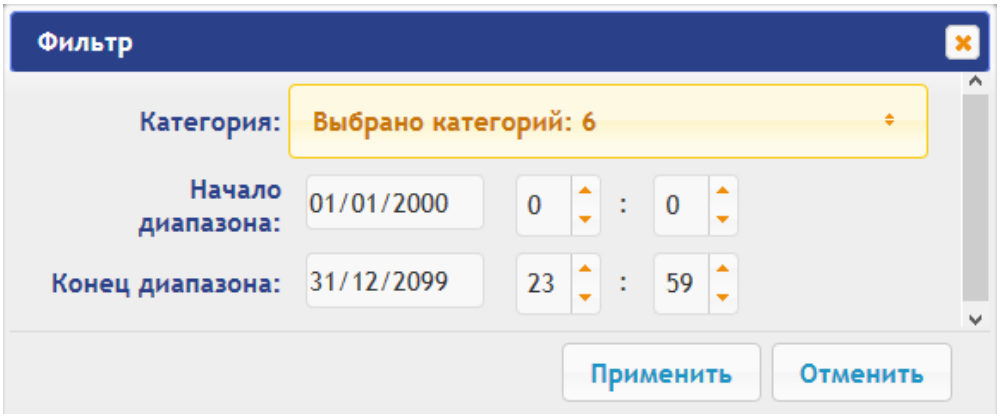
7. СОБЫТИЯ

Для просмотра журнала событий регистрации контроллера:

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



2. По умолчанию отображаются все события, хранящиеся в памяти контроллера, по 20 событий на странице. Для перемещения по страницам списка событий используйте кнопки, расположенные в нижней части рабочей области. События в рабочей области страницы отображаются в обратном хронологическом порядке.
3. Имеется возможность выборки в отчет событий по категориям и по времени. Для этого нажмите кнопку **Фильтр**, откроется окно **Фильтр**:



4. В выпадающем списке **Категория** отметьте флажками категории событий, которые необходимо отображать в отчете. Доступны следующие категории событий:
   - **Доступ по идентификатору;**
   - **Доступ без идентификаторов;**
   - **Изменение состояний ОЗ;**
   - **Изменение состояний входов/ выходов;**
   - **Функционирование;**
   - **Сервис.**
5. С помощью полей **Начало диапазона** и **Конец диапазона** установите период отчета.
6. Нажмите кнопку **Применить** для применения фильтра, кнопку **Отменить** для отмены внесенных в него изменений. Окно **Фильтр** закроется, в отчет будут выведены события в соответствии с установками фильтра.
7. Для удаления всех событий из памяти контроллера нажмите кнопку **Очистить** в рабочей области страницы.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8. СОСТОЯНИЕ

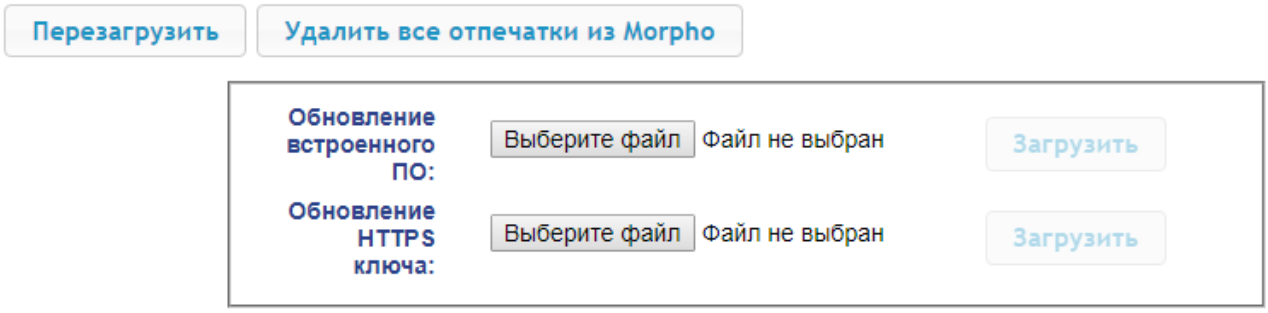
Для просмотра состояния контроллера и состояния всех его ресурсов нажмите в меню *Web*-интерфейса: **Состояние**. Откроется страница с рабочей областью следующего вида:

Объект	Статус
ИУ 1, направление 1	датчик прохода нормализован, ИУ заблокировано, РКД Контроль
Выход 2	норма
Корпус	закрыт
Перемычка IP Mode	снята
Перемычка IP Default	снята
Использование NAND	Да
Свободно на диске	466944кб

9. СЕРВИС

Для обслуживания контроллера:

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



2. Для перезагрузки контроллера нажмите кнопку **Перезагрузить**.
3. Для удаления всех отпечатков из *Morpho* нажмите кнопку **Удалить все отпечатки из *Morpho***.
4. Для обновления встроенного ПО контроллера (прошивки) укажите с помощью кнопки **Выберите файл** место расположения файла прошивки и нажмите кнопку **Загрузить**. Обновление прошивки и ключа вступает в силу после перезагрузки контроллера.
5. Для обновления HTTPS ключа укажите с помощью кнопки **Выберите файл** место расположения файла прошивки и нажмите кнопку **Загрузить**. Начнет отображаться прогресс загрузки файла, перезагрузить контроллер можно будет только после окончания загрузки.

SEC.RU | Короткий путь к информации Скачано с sec.ru

SEC.RU | Короткий путь к информации
Скачано с sec.ru

ООО «ПЭРКо»

Call-центр: 8-800-333-52-53 (бесплатно)
Тел.: (812) 247-04-57

Почтовый адрес:
194021, Россия, Санкт-Петербург,
Политехническая улица, дом 4, корпус 2

Техническая поддержка:

Call-центр: 8-800-775-37-05 (бесплатно)

Тел.: (812) 247-04-55

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

turniket@perco.ru - по вопросам обслуживания турникетов и ограждений

locks@perco.ru - по вопросам обслуживания замков

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

www.perco.ru

Кор. 28.03.2024

SEC.RU | Короткий путь к информации

Скачано с sec.ru

www.perco.ru

SEC.RU
SEC.RU | Короткий путь к информации
Скачано с sec.ru