



Контроллер
PERCo-CT/L04

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ





ЕДИНАЯ СИСТЕМА PERCo-S-20

Контроллер
PERCo-CT/L04

Руководство по эксплуатации

СОДЕРЖАНИЕ

1	Назначение.....	4
2	Условия эксплуатации.....	4
3	Основные технические характеристики.....	5
4	Комплект поставки.....	6
4.1	Стандартный комплект поставки.....	6
4.2	Дополнительное оборудование, поставляемое под заказ:.....	6
5	Описание.....	7
5.1	Устройство и работа.....	7
5.2	Печатная плата контроллера.....	9
5.3	Параметры сигналов релейных выходов управления ИУ.....	11
5.4	Параметры сигналов дополнительных релейных выходов.....	11
5.5	Параметры сигналов выходов с контролем линии.....	12
5.6	Параметры сигналов входов DS1, DS2, In1, In2.....	12
5.7	Параметры входных сигналов ШС.....	13
5.8	Подключение ПДУ.....	14
5.9	Подключение устройства автоматической разблокировки ИУ.....	14
6	Маркировка и упаковка.....	15
7	Меры безопасности.....	15
8	Монтаж.....	15
8.1	Выбор конфигурации контроллера.....	15
8.2	Выбор способа задания IP-адреса.....	16
8.3	Монтаж внешних связей.....	17
8.4	Подключение к интерфейсу RS-485.....	19
8.5	Последовательность монтажа контроллера.....	19
8.6	Монтаж конфигурации «Контроллер управления дверьми».....	22
8.7	Монтаж конфигурации «Контроллер управления турникетом».....	23
8.8	Монтаж в варианте конфигурации «Контроллер АТП».....	25
8.9	Включение.....	29
8.10	Подключение по сети Ethernet.....	30
9	Конфигурация.....	31
9.1	Выбор формата хранения идентификаторов.....	31
9.2	Настройка через Web-интерфейс.....	31
9.2.1	Подключение к контроллеру.....	31
9.2.2	Установка параметров конфигурации.....	33
9.2.3	Изменение сетевых настроек контроллера.....	33
9.2.4	Изменение пароля контроллера.....	34
9.2.5	Настройка параметров исполнительных устройств.....	34
9.2.6	Настройка параметров считывателей.....	35
9.2.7	Выбор формата хранения идентификаторов.....	36
9.2.8	Управление считывателями.....	36
9.2.9	Сброс тревоги исполнительных устройств.....	37
9.2.10	Добавление карт доступа.....	37
9.2.11	Список сохраненных карт.....	40
9.2.12	Журнал событий.....	40
9.2.13	Обслуживание контроллера.....	41
9.3	Локальное ПО.....	42
9.3.1	Подключение к контроллеру.....	42
9.3.2	Выбор формата хранения идентификаторов.....	43
9.3.3	Разрешение Web-интерфейса.....	43
9.3.4	Параметры исполнительного устройства.....	43
9.3.5	Конфигурация охранных зон сигнализации.....	44

9.4	Сетевое ПО S-20	48
9.4.1	Подключение к контроллеру	48
9.4.2	Параметры системы безопасности	49
9.4.3	Ресурсы контроллера	49
9.4.4	Контроллер	51
9.4.5	Дополнительный вход	51
9.4.6	Дополнительный выход	53
9.4.7	Шлейф сигнализации	56
9.4.8	Охранная зона	57
9.4.9	Контроллер ИУ	58
9.4.10	Считыватель	59
9.4.11	ИУ (Замок/ Турникет/ Шлагбаум)	63
9.4.12	Генератор тревоги	65
9.4.13	Порядок конфигурации охранных зон сигнализации	66
9.5	Функциональные возможности	66
9.5.1	Функция Antipass	66
9.5.2	Функция Global Antipass	67
9.5.3	Контроль по времени	67
9.5.4	Комиссионирование	68
9.5.5	Верификация и индикация	69
9.5.6	Назначение прав доступа карты	70
10	Обновление встроенного ПО	71
11	Эксплуатация	72
11.1	Режимы работы СКУД	72
11.2	Режим работы «Открыто»	73
11.3	Режим работы «Контроль»	74
11.3.1	Процедура верификации	76
11.3.2	Процедура комиссионирования	77
11.4	Режим работы «Закрыто»	78
11.5	Режим работы «Охрана»	79
11.5.1	Постановка ОЗ на охрану	79
11.5.2	Снятие ОЗ с охраны	81
11.5.3	Переход ОЗ в режим «Тревога»	81
11.5.4	Сброс режима «Тревога»	82
11.6	Режимы ШС	82
11.7	Функционирование дополнительных выходов	84
11.7.1	Тип «Обычный»	84
11.7.2	Тип «Генератора тревоги»	84
11.7.3	Тип «ОПС»	85
11.7.4	Выход оповещения	85
11.8	Индикация контроллера	85
12	Транспортирование и хранение	88
13	Техническое обслуживание	88
14	Устранение неисправностей	91
14.1	Контроллер не работает	91
14.2	Нарушение связи с компьютером	91
15	Термины и определения	93
16	Предметный указатель	95
Приложения		99
Приложение А.	Программы управления выходами	99
Приложение Б.	События, регистрируемые контроллером	101
Приложение В.	Инструкция по подключению через PoE-сплиттер PA1212	113

Уважаемые покупатели!

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

Настоящее «Руководство по эксплуатации» (далее – *Руководство*) предназначено для ознакомления с техническими характеристиками и принципом работы контроллера **PERCo-CT/L04**. Целью *Руководства* является обеспечение правильной эксплуатации контроллера и наиболее полное использование всех его технических возможностей. *Руководство* содержит разделы по монтажу и диагностике, а также справочные разделы.

Данное *Руководство* действует совместно с «*Техническим описанием PERCo-S-20*», а также с паспортами подключаемых к контроллеру устройств.

Используемые сокращения:

ПДУ – пульт дистанционного управления;	ШС – шлейф сигнализации;
ПО – программное обеспечение;	ИУ – исполнительное устройство;
СКУД – система контроля и управления доступом;	ТС – транспортное средство;
устройство РУ – устройство радиуправления;	КЗ – короткое замыкание;
АТП – автотранспортная проходная;	ОЗ – охранная зона.

1 НАЗНАЧЕНИЕ

Контроллер **PERCo-CT/L04** (далее по тексту – контроллер) входит в единую систему безопасности и повышения эффективности предприятия **PERCo-S-20**.

Контроллер поддерживает подключение двух считывателей серии **PERCo-IR0x**, что позволяет организовать одну двухстороннюю или две односторонние точки прохода.

В зависимости от выбора конфигурации контроллер позволяет управлять следующими ИУ:

- одним замком электромагнитного или электромеханического типа с возможностью контроля двухстороннего прохода;
- двумя замками электромагнитного или электромеханического типа с возможностью контроля одностороннего прохода;
- одним турникетом или калиткой;
- шлагбаумом или приводом автоматических ворот автотранспортной проходной.

Кроме этого предусмотрена возможность подключения к контроллеру до 8 замковых контроллеров **PERCo-CL201**, обеспечивающих контроль одностороннего прохода.

2 УСЛОВИЯ ЭКСПЛУАТАЦИИ

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

Эксплуатация контроллера допускается при температуре окружающего воздуха от +1°C до +40°C и относительной влажности воздуха до 80% при +25°C.

3 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Варианты конфигурации контроллера:

1. Контроллер для управления одной двухсторонней дверью.
2. Контроллер для управления одной двухсторонней дверью с подключением до 8 контроллеров замка **PERCo-CL201**.
3. Контроллер для управления двумя односторонними дверьми с подключением до 8 контроллеров замка **PERCo-CL201**.
4. Контроллер для управления турникетом.
5. Контроллер для управления турникетом с подключением до 8 контроллеров замка **PERCo-CL201**.
6. Контроллер автотранспортной проходной.
7. Контроллер автотранспортной проходной с подключением до 8 контроллеров замка **PERCo-CL201**.

Вариант конфигурации контроллера задается установкой перемычек на печатной плате контроллера (см. таблицу 5).

Номинальное значение напряжения питания постоянного тока, <i>V</i>	12±1,2
Потребляемый ток (@ 12В), <i>A</i> :	
в вариантах конфигурации №1-3	не более 0,4
в вариантах конфигурации №4-7	не более 0,12
Потребляемая мощность, <i>Wm</i> :	
в вариантах конфигурации №1-3	не более 4,8
в вариантах конфигурации №4-7	не более 1,5
Стандарт интерфейса связи	<i>Ethernet</i> (IEEE 802.3)
Скорости передачи данных <i>Ethernet</i> , <i>Mbit/c</i>	10/100/1000
Количество контролируемых ИУ.....	1 ¹
Количество считывающих устройств.....	2 ²
Интерфейс считывающих устройств	RS-485
Число карт доступа (пользователей).....	до 50 000 ³
Число коммиссионированных карт.....	192 ⁴
Число коммиссионированных карт для каждого подключенного PERCo-CL201	64
Число событий журнала регистрации.....	до 135 000 ⁵
Количество релейных выходов управления ИУ	2
Количество выходов с контролем линии на КЗ и обрыв	2 ⁶
Количество дополнительных релейных выходов	2
Количество дополнительных входов, управляемых выходами типа «сухой контакт»	2
Количество ШС	2 ⁷
Количество входов ДУ	2-3
Количество выходов индикации ДУ	4

¹ В варианте конфигурации №3 можно подключить два ИУ типа замок.

² Два считывателя серии **PERCo-IR0x**.

³ Зависит от варианта конфигурации, см. таблицу 1.

⁴ В варианте конфигурации №3 для второго ИУ типа замок количество карт 64.

⁵ События подключенных контроллеров **PERCo-CL201** хранятся в памяти контроллера **PERCo-CT/L04**

⁶ В вариантах конфигурации №1-3.

⁷ Подключение ШС предусмотрено в вариантах конфигурации №1-3.

Габаритные размеры, мм	205×235×58
Масса, кг.....	не более 1,75
Средний срок службы, лет	8
Класс защиты от поражения электрическим током	III по ГОСТ Р МЭК730-1-94

Таблица 1 Варианты конфигурации контроллера

Вариант конфигурации №	1	2	3	4	5	6	7
Количество подключаемых контроллеров PERCo-CL201	-	8	8	-	8	-	8
Число карт доступа	50 000	10 000	1000	50 000	10 000	50 000	10 000
Число карт в каждом контроллере PERCo-CL201	-	1 000	1 000	-	1 000	-	1 000
Количество ШС	2	2	2	0	0	0	0
Кол-во выходов с контролем линии на КЗ и обрыв	2	2	2	0	0	0	0

4 КОМПЛЕКТ ПОСТАВКИ

4.1 Стандартный комплект поставки

Контроллер PERCo-CT/L04 , шт.	1
Переключатель (джампер), шт.	4
Резистор С2-33Н-0,25-4,7кОм±5%, шт.	4
Супрессор на 15 – 18 В, шт.	2
Монтажный комплект:	
дюбели пластмассовые, шт.	3
шурупы, шт.	3
площадка самоклеящаяся, шт.	3
стяжка неоткрывающаяся 100 мм, шт.	5
Упаковка, шт.	1
Паспорт, экз.	1
Руководство по эксплуатации, экз.	1

4.2 Дополнительное оборудование, поставляемое под заказ:

Источник питания контроллера, шт.	1
РоЕ-сплиттер PA1212 ⁸ , шт.	1



Внимание!

Получение питания от РоЕ-сплиттера возможно только для контроллеров **PERCo-CT/L04**, выпущенных на базе печатной платы с пониженным энергопотреблением **CT/L04.720.00** (внешнее отличие от других вариантов исполнения – отсутствие на плате радиатора).

⁸ **РоЕ-сплиттер PA1212** – позволяет подавать питание контроллера по сети *Ethernet*. Сплиттер может использоваться с сетевыми коммутаторами, поддерживающими технологию передачи электроэнергии по витой паре *PoE* и совместимыми со стандартом *IEEE 802.3af*.

5 ОПИСАНИЕ

5.1 Устройство и работа

Контроллер выполнен в виде блока электроники в металлическом корпусе со съёмной крышкой. На крышку корпуса выведены:

- светодиодная индикация наличия питания;
- светодиодная индикация состояния ШС.

В контроллере установлены:

- энергонезависимая память;
- энергонезависимый RTC-таймер (часы реального времени);
- разъем *8P8C (RJ45)* для подключения к локальной сети *Ethernet*;
- датчик вскрытия корпуса.

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

Контроллер обеспечивает:

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

На этапе производства контроллеру заданы:

- уникальный физический MAC-адрес (указан в паспорте и на плате устройства);
- IP-адрес (указан в паспорте и на плате устройства);
- маска подсети (255.0.0.0);
- IP-адрес шлюза (0.0.0.0).

Предусмотрены следующие способы задания IP-адреса, шлюза, маски подсети контроллера на этапе конфигурации системы:

- работа с заводскими настройками;
- ручной ввод;
- получение от DHCP сервера.

Считыватели подключаются к интерфейсу *RS-485*. Возможны следующие варианты подключения:

- два считывателя серии **PERCo-IR0x**;
- два считывателя с интерфейсом *Wiegand-26* (для их подключения необходимо дополнительно приобрести конвертер интерфейса **PERCo-AC01**);
- до 8 считывателей серии PERCo-IR10.

Возможно подключение следующего дополнительного оборудования:

- до двух блоков индикации с ИК-приемником **PERCo-AI01**;
- до двух датчиков двери (герконов) или двух датчиков прохода, подключаемых к выходам PASS турникета;
- одного табло системного времени **PERCo-AU05**;
- до двух кнопок ДУ для замка или одного ПДУ турникета (калитки);
- до двух устройств, подающих команды на дополнительные входы.

Контроллер способен хранить в энергонезависимой памяти:

- до 50 000 идентификаторов карт;

- до 135 000 событий журнала регистрации с указанием даты и времени события⁹.

Контроллер как элемент СКУД обеспечивает:

- работу в режимах: «Открыто», «Контроль», «Совещание»¹⁰, «Охрана»¹¹, «Закрыто»;
- сохранение установленного режима в энергонезависимой памяти, для предотвращения снятия режима при выключении питания;
- поддержку функций локального и глобального контроля зональности, комиссионирования и верификации.

Контроллер как элемент охранной сигнализации обеспечивает:

- подключение и контроль двух ШС¹²;
- подключение световых и звуковых оповещателей;
- возможность постановки и снятия с охраны ОЗ;
- передачу тревожных извещений на пульт централизованного наблюдения.

⁹ В случае переполнения журнала регистрации новые события заменяют наиболее старые (удаление происходит блоками по 256 событий).

¹⁰ Режим доступен только для варианта конфигурации №3 «Управление двумя односторонними дверьми» и для подключенных контроллеров замка **PERCo-CL201**.

¹¹ Режим доступен только для вариантов конфигураций №1-3 «Управление дверьми» (см. таблицу 5) и для подключенных контроллеров замка **PERCo-CL201**.

¹² В вариантах конфигурации №1-3.

5.2 Печатная плата контроллера

Внешний вид печатной платы контроллера представлен на рисунке 1. Описание назначения клеммных колодок приведено в таблице 2.

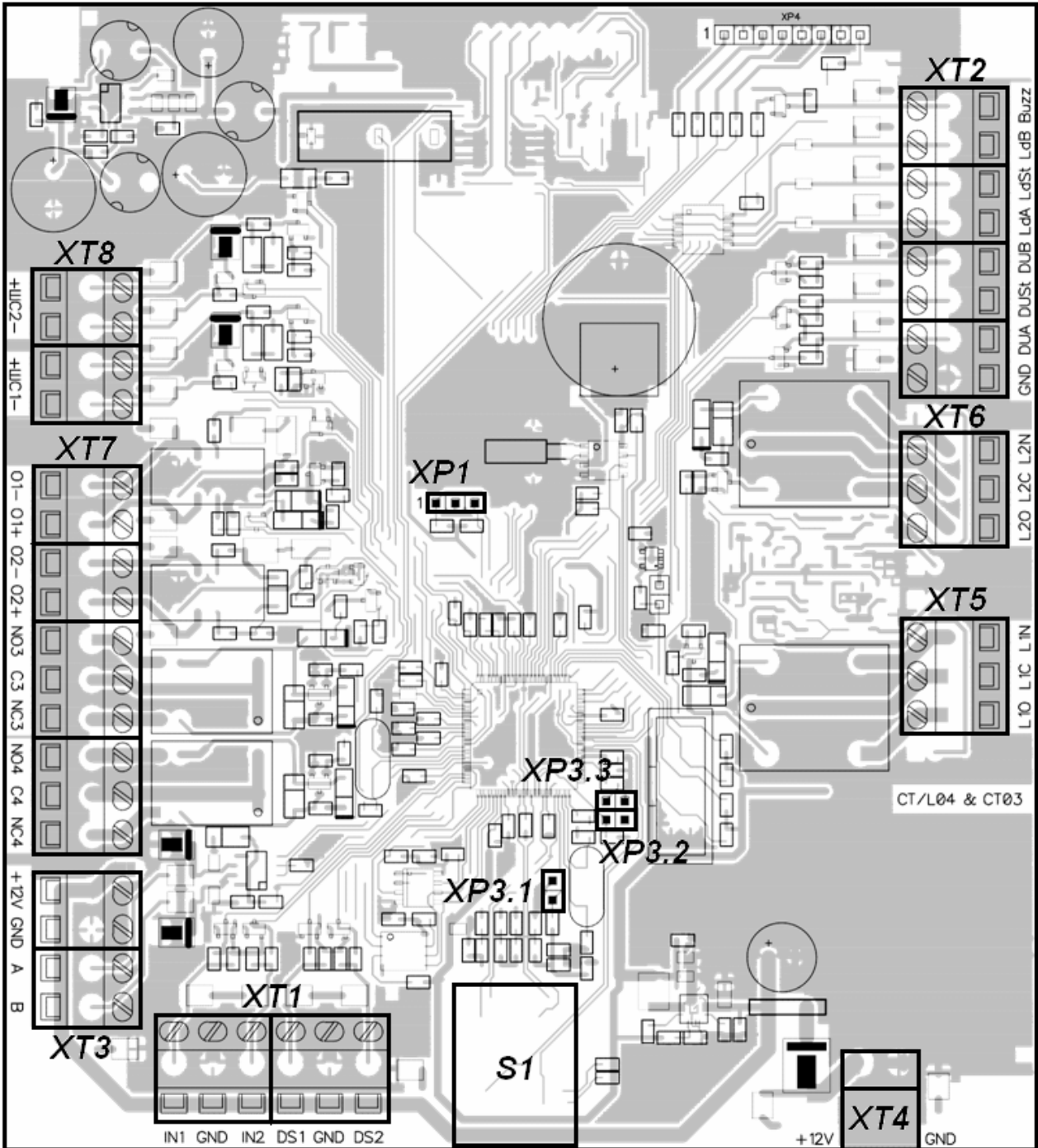


Рисунок 1. Внешний вид печатной платы контроллера

Таблица 2. Назначение клеммных колодок

Контакт	Цепь	Назначение
Разъем XT1		
1	In1	Дополнительный вход 1
2	GND	Общий
3	In2	Дополнительный вход 2
4	DS1	Вход сигнала DS1 (датчик двери или сигнал PASS A)
5	GND	Общий
6	DS2	Вход сигнала DS2 (датчик двери или сигнал PASS B)
Разъем XT2		
1	GND	Общий
2	DUA	Вход ДУ А
3	DUS _t	Вход ДУ СТОП
4	DUB	Вход ДУ В
5	Ld A	Выход индикации ДУ А
6	Ld St	Выход индикации ДУ СТОП
7	Ld B	Выход индикации ДУ В
8	Buzz	Выход звуковой индикации ПДУ
Разъем XT3		
1	+12V	Подключение +12В питания считывателя
2	GND	Общий
3	A	Подключение линии А по RS-485
4	B	Подключение линии В по RS-485
Разъем XT4		
1	+12V	Подключение +12В внешнего источника питания
2	GND	Общий (Минус внешнего источника питания)
Разъем XT5		
1	L1O	Релейный выход Lock 1, нормально разомкнутый контакт
2	L1C	Релейный выход Lock 1, центральный контакт
3	L1N	Релейный выход Lock 1, нормально замкнутый контакт
Разъем XT6		
1	L2O	Релейный выход Lock 2, нормально разомкнутый контакт
2	L2C	Релейный выход Lock 2, центральный контакт
3	L2N	Релейный выход Lock 2, нормально замкнутый контакт
Разъем XT7		
1	O1 -	(-) выхода <i>Out 1</i> с контролем состояния линии связи
2	O1 +	(+) выхода <i>Out 1</i> с контролем состояния линии связи
3	O2 -	(-) выхода <i>Out 2</i> с контролем состояния линии связи
4	O2 +	(+) выхода <i>Out 2</i> с контролем состояния линии связи
5	NO3	Релейный выход <i>Out 3</i> , нормально разомкнутый контакт
6	C3	Релейный выход <i>Out 3</i> , центральный контакт
7	NC3	Релейный выход <i>Out 3</i> , нормально замкнутый контакт
8	NO4	Релейный выход <i>Out 4</i> , нормально разомкнутый контакт
9	C4	Релейный выход <i>Out 4</i> , центральный контакт
10	NC4	Релейный выход <i>Out 4</i> , нормально замкнутый контакт
Разъем XT8		
1	ШС2+	Подключение ШС2+
2	ШС2-	Подключение ШС2-
3	ШС1+	Подключение ШС1+
4	ШС1-	Подключение ШС1-

5.3 Параметры сигналов релейных выходов управления ИУ

Контроллер имеет два релейных выхода управления ИУ: *Lock 1*, *Lock 2*. Подключение к выходам осуществляется через клеммные колодки *XT5* или *XT6* печатной платы контроллера.

Каждый из выходов имеет полную группу контактов: нормально разомкнутый NO, нормально замкнутый NC и общий выводной C.

Параметры выходных сигналов релейных выходов управления ИУ:

- Максимальное коммутируемое напряжение постоянного тока, *V* не более 30
- Максимальное коммутируемое напряжение переменного тока, *V* не более 42
- Максимальный коммутируемый постоянный/переменный ток для выходов *Lock 1* и *Lock 2*, *A*..... не более 5
- Сопrotивление замкнутого контакта, *Om* не более 0,15

Выходы управления могут поддерживать потенциальный и импульсный режимы работы ИУ. Выбор между режимами осуществляется с помощью параметра ИУ **Режим работы выхода управления**.

В **потенциальном** режиме работы ИУ:

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

В **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 режим «Открыто» выход активизируется на время, определяемое параметром **Длительность импульса управления ИУ**, после чего будет активизироваться каждый раз на это же время через одну секунду после нормализации ИУ.

Фактом совершения прохода в заданном направлении является передний или задний фронт сигнала на входах DS1 или DS2.

5.4 Параметры сигналов дополнительных релейных выходов

Контроллер имеет два релейных выхода: *Out3* и *Out4*. Подключение к выходам осуществляется через клеммную колодку *XT7* печатной платы контроллера.

Выходы имеют полную группу контактов: нормально разомкнутый NO, нормально замкнутый NC и общий выводной C.

Выходы могут использоваться для:

- подключения световых и звуковых оповещателей,
- передачи тревожных извещений на пульт централизованного наблюдения,
- подключения другого дополнительного оборудования.

Параметры выходных сигналов релейных выходов:

- Максимальное коммутируемое напряжение постоянного тока, *V* не более 30
- Максимальное коммутируемое напряжение переменного тока, *V* не более 42
- Максимальный коммутируемый постоянный/переменный ток для выходов *Out*, *A*..... не более 2
- Сопrotивление замкнутого контакта, *Om* не более 0,15

5.5 Параметры сигналов выходов с контролем линии

Контроллер имеет два выхода с контролем линии на КЗ и обрыв: *Out1*, *Out2*. Подключение к выходам осуществляется через клеммную колодку *XT7* печатной платы контроллера.

Выходы могут использоваться для:

- подключения световых и звуковых оповещателей,
- передачи тревожных извещений на пульт централизованного наблюдения,
- подключения другого дополнительного оборудования.

Параметры выходных сигналов выходов с контролем линии на КЗ и обрыв:

Напряжение на выходе (напряжение питания прибора), *V* 12
 Максимальный ток выхода, *A* не более 0,15

5.6 Параметры сигналов входов DS1, DS2, In1, In2

Контроллер обеспечивает контроль состояния четырех входов под управлением выходами типа «сухой контакт» или «открытый коллектор» (ОК): *DS1*, *DS2*, *In1*, *In2*. Подключение к входам осуществляется через клеммную колодку *XT1* печатной платы контроллера.

Входы могут использоваться для следующих функций:

- DS1, DS2
 - для подключения датчиков двери (герконов),
 - для подключения датчиков прохода (проезда),
 - для соединения с выходами PASS турникета;
- In1, In2 – для подключения дополнительного оборудования.

Факт активизации для сигналов DS1, DS 2, In1, In2 зависит от описания их исходного состояния в параметре **Нормальное состояние контакта** в ПО S-20:

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



Примечание

Все неподключенные входы подтянуты к питанию. Для создания сигнала высокого уровня на всех входных контактах (DS1, DS 2, In1, In2) используются резисторы с сопротивлением 2 кОм, подключенные к шине питания +3,3 В.

Управляющий элемент «контакт реле» должен обеспечивать следующие характеристики сигналов:

Минимальный коммутируемый ток, *mA* не более 1
 Сопротивление замкнутого контакта
 (с учетом сопротивления кабеля подключения), *Ом* не более 300

Управляющий элемент схема с открытым коллекторным выходом должен обеспечивать следующие характеристики сигналов:

Напряжение на замкнутом контакте
 (сигнал низкого уровня, на входе контроллера), *V* не более 0,8

5.7 Параметры входных сигналов ШС

Контроллер обеспечивает контроль состояния двух ШС, которые подключаются к клеммной колодке ХТ1¹³.

В качестве извещателей, включаемых в ШС, могут использоваться только охранные извещатели:

- электроконтактного и магнитоконтактного типов (герконы, предохранители);
- имеющие на выходе реле (4-х проводная схема);
- активные, с питанием по ШС.

Параметры входных сигналов ШС:

Величина напряжения в ШС, В не более 16±2

Ток короткого замыкания в ШС, мА не более 20

Сопротивление выносного элемента, кОм 4,7±5%

Сопротивление проводов ШС

(без учета сопротивления выносного элемента), кОм не более 1

Сопротивление проводов ШС при контроле вскрытия корпуса

извещателей (без учета сопротивления выносного элемента), кОм не более 0,5

Сопротивление утечки между проводами ШС

или каждым проводом и «землей», кОм не менее 20



Примечание

Параметры ШС контролируются по их сопротивлению.

Таблица 3 Состояния и пороги ШС

Сопротивление ШС, Ом	Действительное состояние ШС	Определенное прибором состояние ШС
Вариант конфигурации: «Охранный»		
Меньше 2 кОм	КЗ	Нарушение – КЗ
2,4 кОм - 7 кОм	Норма	Норма
Больше 9 кОм	Обрыв	Нарушение – Обрыв
Вариант конфигурации: «Охранный с контролем вскрытия корпуса извещателей»		
Меньше 1,3 кОм	КЗ	Нарушение – КЗ
1,5 кОм - 2,3 кОм	Норма	Норма
2,5 кОм - 3,6 кОм	Корпус извещателя вскрыт	Нарушение – корпус извещателя вскрыт
4 кОм - 6 кОм	Срабатывание извещателя с контролем вскрытия корпуса	Нарушение – срабатывание извещателя с контролем вскрытия корпуса
Больше 7 кОм	Срабатывание извещателя с контролем вскрытия корпуса и корпус извещателя вскрыт или обрыв	Нарушение – срабатывание извещателя с контролем вскрытия корпуса и корпус извещателя вскрыт или обрыв

Время интегрирования ШС – максимальное время, в течение которого изменение сопротивления ШС не рассматривается как его нарушение и не приводит к переходу ШС в тревожное состояние.

¹³ В вариантах конфигурации №1-3.

Когда ШС взят на охрану, непрерывно производится измерение значения его сопротивления с необходимым усреднением. Время интегрирования для ШС задается параметром конфигурации **Длительность нарушения** и равно 70 мс или 300 мс. При этом требования к обнаружению состояния ШС следующие:

Таблица 4. Время интегрирования ШС

Время интегрирования (Длительность нарушения), мс.	70	300
Нарушения ШС не должны приводить к определению прибором состояния ШС «нарушение», если они имели место в течение времени, не более , мс.	50	250
Нарушения ШС должны приводить к определению прибором состояния ШС «нарушение», если они имели место в течение времени, более , мс.	70	300

5.8 Подключение ПДУ

Контроллер обеспечивает возможность подключения кнопки ДУ для замка и ПДУ для турникета или калитки. Для этого предназначены:

- 3 входа управления проходом: DUA, DUS_t, DUB;
- 4 выхода управления индикацией ПДУ: LdA, LdS_t, LdB, Buzz.

Подключение осуществляется к контактам клеммной колодки XT2.

Активизация для данных входов DUA, DUB и DUS_t осуществляется подачей на них сигналов низкого уровня (нормально разомкнутый контакт) относительно контакта GND. При этом управляющим элементом могут быть нормально разомкнутый контакт реле или схема с открытым коллекторным выходом.



Примечание

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

5.9 Подключение устройства автоматической разблокировки ИУ

В случае возникновения пожара или других нештатных ситуаций предусмотрена возможность автоматической разблокировки по команде устройства аварийной разблокировки всех ИУ, подключенных к контроллеру первого и к контроллерам второго уровня, за исключением тех ИУ, которые находятся в режиме «Охрана». Настройка функции автоматической разблокировки возможна при работе в составе системы **PERCo-S-20** для вариантов конфигурации контроллера №1-5 (см. табл. 5).

Устройства автоматической разблокировки ИУ подключаются к дополнительным входам контроллера *In1* или *In2* клеммной колодки XT1 (см. рис. 1).

При подаче управляющего сигнала на дополнительный вход, контроллер переводится в режим **Fire Alarm**. В этом режиме все подключенные ИУ разблокируются для прохода в обоих направлениях. Другие команды управления при этом игнорируются.

Порядок конфигурирования дополнительного входа контроллера в сетевом ПО **PERCo-S-20** подробно описан в разделе 9.4.5.

6 МАРКИРОВКА И УПАКОВКА

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

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

На плате контроллера находятся этикетки, 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 МЕРЫ БЕЗОПАСНОСТИ



Внимание!

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

- Монтаж и техобслуживание контроллера должны производиться только квалифицированными специалистами, ознакомленные с настоящим «Руководством по эксплуатации» и «Техническим описанием системы PERCo S-20».
- Монтаж должен соответствовать СНиП 3.05.07-85 «Системы автоматизации» и СНиП 3.05.06-85 «Электротехнические устройства».
- По способу защиты от поражения электрическим током контроллер соответствует классу III по ГОСТ Р МЭК 730-1-94.
- Запрещается эксплуатировать контроллер при напряжении питания, не соответствующем допустимыми техническими характеристиками.
- Запрещается эксплуатировать контроллер в условиях, не соответствующих требованиям условий эксплуатации.
- Запрещается использование устройства в агрессивных средах с содержанием в атмосфере кислот, щелочей, масел и т. п.
- Монтаж линий связи должен соответствовать рекомендациям стандартов EIA/TIA RS-422A/485.
- Прокладку кабелей необходимо производить с соблюдением правил эксплуатации электроустановок.

8 МОНТАЖ

8.1 Выбор конфигурации контроллера



Внимание!

Установка и снятие перемычек должны производиться только при выключенном оборудовании.

После изменения конфигурации контроллера с помощью перемычек XР3.1 – XР3.3 автоматически производится форматирование внутренней памяти контроллера.

Установите конфигурацию контроллера, с помощью перемычек *XP3.1 – XP3.3* на печатной плате согласно таблице 5. Расположение перемычек указано на рисунке 1.



Примечание

При поставке установлена конфигурация №4 «Контроллер для управления турникетом».

Таблица 5. Выбор конфигурации

№	Вариант конфигурации	Установлена перемычка		
		XP3.1	XP3.2	XP3.3
1	Контроллер для управления одной двухсторонней дверью.	нет	нет	нет
2	Контроллер для управления одной двухсторонней дверью с подключением к интерфейсу <i>RS-485</i> до 8 контроллеров замка PERCo-CL201 .	да	нет	нет
3	Контроллер для управления двумя односторонними дверьми с подключением к интерфейсу <i>RS-485</i> до 8 контроллеров замка PERCo-CL201 .	да	да	нет
4	Контроллер для управления турникетом.	нет	нет	да
5	Контроллер для управления турникетом с подключением к интерфейсу <i>RS-485</i> до 8 контроллеров замка PERCo-CL201 .	да	нет	да
6	Контроллер автотранспортной проходной.	нет	да	да
7	Контроллер автотранспортной проходной с подключением к интерфейсу <i>RS-485</i> до 8 контроллеров замка PERCo-CL201 .	да	да	да

8.2 Выбор способа задания IP-адреса



Внимание!

Установка и снятие перемычек должны производиться только при выключенном оборудовании.

Выбор способа задания IP-адреса контроллера осуществляется установкой или снятием перемычки (джампера) на разъем *XP1* на плате контроллера. Возможны следующие способы задания IP-адреса:

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



Примечания

- Заводские установки контроллера: IP-адрес и MAC-адрес указаны в паспорте и на плате контроллера; маска подсети 255.0.0.0; IP-адрес шлюза 0.0.0.0.
 - Конфигурация в «ручном» режиме должна происходить в подсети, в которой расположен сервер системы.
2. «*IP MODE*» Перемычка в положение 1–2. Вариант предназначен для работы в сетях с динамическим распределением IP-адресов.
 - Контроллер получает IP-адрес (шлюз, маску подсети) от DHCP-сервера.
 3. «*IP DEFAULT*» Перемычка в положение 2–3.

- Контроллер работает с заводскими установками IP-адреса (шлюза, маски подсети).
- Пароль для доступа к контроллеру сбрасывается.



Примечание

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

Таблица 6. Варианты установки переключателя на разъем XP1

№	Расположение переключателя на XP1	Режим
1		Переключатель снят
2		IP MODE
3		IP DEFAULT

8.3 Монтаж внешних связей

Кабели, применяемые при монтаже, указаны в таблице 7.

- Монтаж линий связи должен соответствовать рекомендациям стандартов *EIA/TIA RS-422A/485*.
- Не прокладывайте кабели на расстоянии менее 50 см от источников электромагнитных помех.
- Пересечение всех кабелей с силовыми кабелями допускается только под прямым углом.
- Любые удлинения кабелей производить только методом пайки.
- Все кабели, входящие в контроллеры, должны быть закреплены пластиковыми стяжками к самоклеющимся площадкам из комплекта поставки, устанавливаемым по месту внутри корпуса.
- Произведите укладку и закрепление кабелей, используя при необходимости пластиковые крепежные скобы.
- После прокладки кабелей проверьте отсутствие обрывов и коротких замыканий во всех линиях.
- Не допускается совместная прокладка с проводами заземления проводов питания замка, кабелей от датчиков, кнопок дистанционного управления и от считывателей на участке более чем 1 м.

Таблица 7. Кабели, применяемые при монтаже системы PERCo-S-20

№	Подключаемое к контроллеру оборудование	Макс. длина кабеля	Тип кабеля	Пример кабеля
1	Ethernet (IEEE 802.3)	100 м	Четыре витые пары не ниже пятой категории с сечением проводов не менее 0.2 мм ²	
2	Считыватель или блок индикации с ИК-приемником PERCo-AI01	50 м (суммарная)		
3	ИУ	30 м	Двужильный кабель с сечением проводов не менее 0.75 мм ²	ШВВП 2×0,75 двухцветный
4	Кнопка ДУ	30 м	Двужильный кабель с сечением проводов не менее 0.2 мм ²	RAMCRO SS22AF-T 2×0,22 или CQR-2
5	Датчик двери (геркон)	30 м		
6	ШС		Двужильный кабель с сечением проводов не менее 0,5 мм ²	КСПВ 2×0,5
7	Дополнительный датчик (ко входу контроллера)	30 м	Двужильный кабель с сечением проводов не менее 0.2 мм ²	RAMCRO SS22AF-T 2×0,22 или CQR-2
8	Дополнительное оборудование (к выходу контроллера)	30 м		
9	Турникет PERCo	30 м	Шестижильный кабель с сечением проводов не менее 0,2 мм ²	CQR CABS6 6×0,22с
10	Турникет сторонних производителей	30 м	Шестижильный кабель с сечением проводов не менее 0,2 мм ²	CQR CABS6 6×0,22с
11	ПДУ	50 м	Восьмижильный кабель с сечением проводов не менее 0,2 мм ²	CQR CABS8 8×0,22с
12	Стойка турникета (для встроенного контроллера турникета)	1 м	Кабель турникета TTD-03.1.930.00	
13	Источник питания	2 м	Двужильный кабель с сечением проводов не менее 0.75 мм ²	ШВВП 2×0,75 двухцветный
14	Устройство РУ	50 м	Шестижильный кабель с сечением проводов не менее 0,2 мм ²	CQR CABS6 6×0,22с
15	Контроллер замка PERCo-CL201	1200 м (суммарная)	Витая пара не ниже пятой категории с сечением проводов не менее 0.2 мм ²	
16	Табло системного времени PERCo-AU05	1200 м (суммарная)		
17	ИУ АТП	30 м	Четырехжильный кабель с сечением проводов не менее 0,2 мм ²	CQR CABS4 4×0,22с

8.4 Подключение к интерфейсу RS-485



Внимание!

При подключении нескольких устройств по интерфейсу RS-485 линия связи последовательно подводится ко всем устройствам. Концевые резисторы должны быть подключены только по концам линии связи. Поэтому на всех изделиях, которые не являются конечными устройствами на данной линии связи необходимо отключить концевой резистор, для чего перекусите у них кусачками перемычку «отключение концевого резистора».

Монтаж устройств производится согласно инструкциям, приводимым в технической документации соответствующих изделий. Подключение осуществляется к клеммной колодке ХТЗ печатной платы контроллера согласно схеме, представленной на рисунке 3. Для подключения считывателей и блоков индикации **PERCo-AI01** применяется кабель №2. Для подключения контроллеров замка **PERCo-CL201** и табло системного времени **PERCo-AU05** применяются кабели №15 и №16 соответственно. Используемые при монтаже кабели указаны в таблице 7

Возможны следующие варианты подключения считывателей:

- Два считывателя серии **PERCo-IR0x**.
- Два считывателя с интерфейсом *Wiegand-26*. Для подключения требуется конвертер интерфейса **PERCo-AC01**. Схема подключения и описание индикации считывателей в этом случае приведены в «Руководстве пользователя» на конвертер интерфейса **PERCo-AC01**.
- Один считыватель серии **PERCo-IR0x**.



Примечание

При установке считывателей (блоков индикации) им необходимо установить разные номера. Номер определяется состоянием перемычки «номер считывателя», находящейся под металлическим основанием считывателя (блока индикации). Перемычка целая – №1, перемычка перекушена – №2).

8.5 Последовательность монтажа контроллера

Придерживайтесь следующей последовательности действий при монтаже контроллера:

1. Распакуйте коробку и проверьте комплектность контроллера. Убедитесь в отсутствии на оборудовании механических повреждений.
2. Определите место установки контроллера. Контроллер рекомендуется монтировать на расстоянии не более 30 метров от ИУ. Расположение контроллера должно соответствовать условиям эксплуатации и выбираться исходя из соображения удобства проведения работ по его обслуживанию.



Внимание!

Не располагайте контроллер на расстоянии менее 1 м от источников электромагнитных помех.

3. Произведите разметку и разделку отверстий на установочной поверхности для крепления контроллера и подводки кабелей согласно рисунку 2.
4. Осуществите прокладку и крепеж кабелей связи, питания и *Ethernet* к месту установки контроллера.
5. Отвинтите винты, расположенные в правой части корпуса контроллера и крепящие его крышку к корпусу. Снимите крышку с контроллера.

6. Закрепите контроллер с помощью трех шурупов, установив их через отверстия в корпусе контроллера (при необходимости используйте дюбели из комплекта поставки).
7. Установите переключки на разъемы *XP3.1* – *XP3.3* печатной платы контроллера согласно выбранной конфигурации. Расположение разъемов приведено на рисунке 1. Варианты конфигурации и положение переключек указаны в таблице 5.
8. Выберите способ задания IP-адреса контроллера и при необходимости установите переключку (джампер) на разъем *XP1* согласно таблице 6.
9. Подключите кабель *Ethernet* №1 к разьему *S1* печатной платы контроллера.
10. Подключите кабель источника питания к клеммной колодке *XT4* печатной платы контроллера согласно схеме, представленной на рисунке 3. Для подключения используйте кабель №13.
11. Далее следуйте порядку монтажа для выбранной конфигурации контроллера.

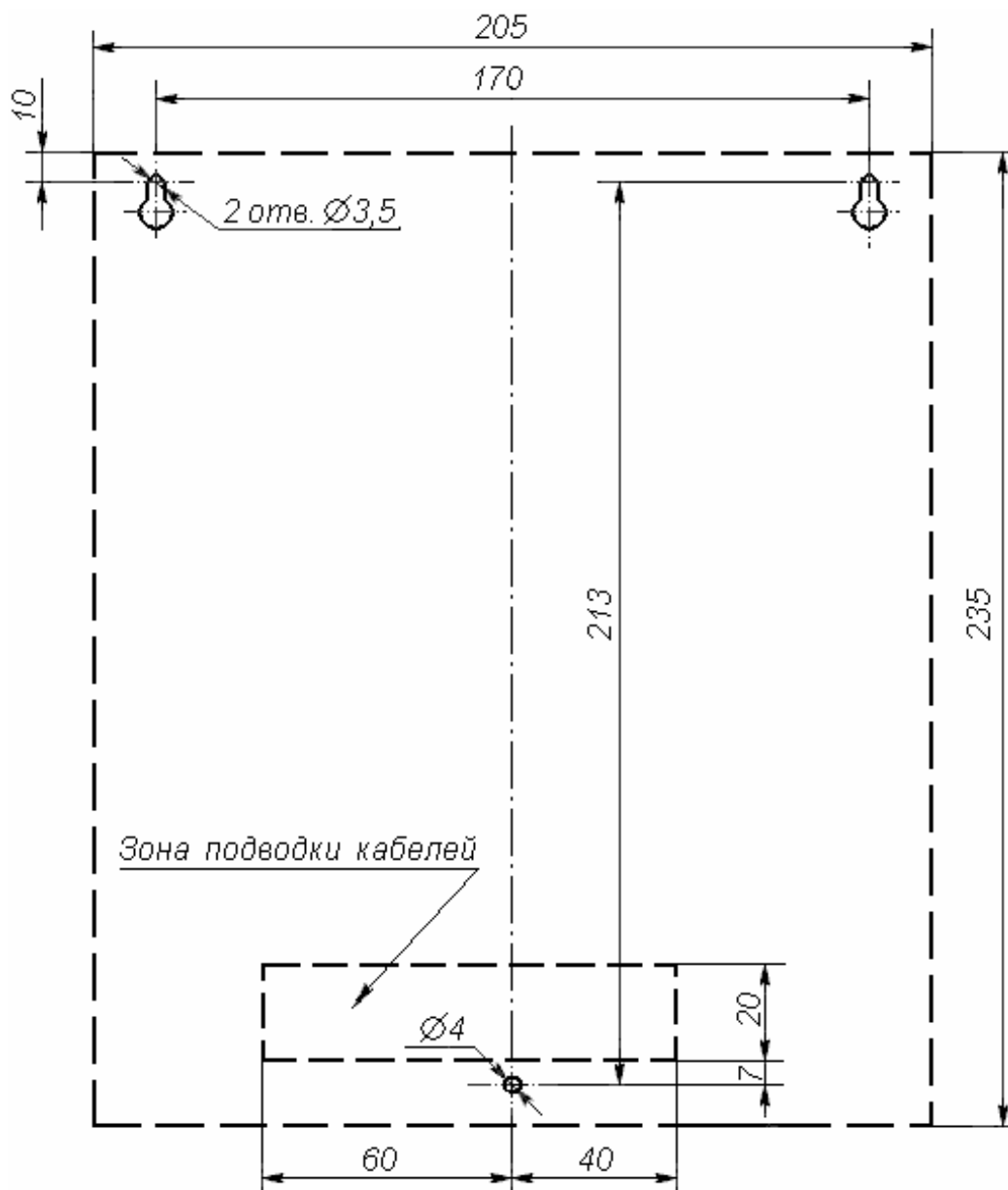


Рисунок 2. Разметка отверстий для установки контроллера PERCo-CT/L04 (пунктиром показаны размеры корпуса контроллера)

8.6 Монтаж конфигурации «Контроллер управления дверьми»

Описано подключение устройств для вариантов конфигурации контроллера №1-3 (см. таблицу 5).

Монтаж устройств производится согласно инструкциям, приводимым в технической документации соответствующих изделий.

Подключение к контроллеру осуществляется согласно схеме, представленной на рисунке 3, с использованием кабелей из таблицы 7. Расположение клеммных колодок на плате контроллера указано на рисунке 1.

1. Произведите монтаж контроллера.
2. Произведите монтаж и подключение устройств к интерфейсу *RS-485* контроллера.
3. Произведите монтаж замка (защелки).



Внимание!

- Если подключаемый замок не имеет встроенной цепи искрозащиты, то необходимо использовать диод искрозащиты (**VD4** и **VD5** на рис. 3). Например, диод Шоттки, рассчитанный на рабочий ток не менее 1А (1N5819).
 - Если подключаемый электромагнитный замок не имеет размагничивающей цепи, то необходимо установить двунаправленный супрессор из комплекта поставки. Супрессор устанавливается в непосредственной близости от замка (**VD4** и **VD5** на рис. 3).
 - При подключении контроллера через PoE-сплиттер **PA1212** (см. рис. В.2 Приложения В к *Руководству*) рекомендуется использовать только электромеханические замки, поэтому необходимо использовать именно диоды искрозащиты (**VD4** и **VD5** на рис. 3) типа 1N5819. Использование супрессора в этом случае **ЗАПРЕЩЕНО!**
 - Также при подключении к релейным выходам *дополнительного оборудования* с индуктивной нагрузкой (*Rn1*) необходимо использовать диод искрозащиты (**VD3** на рис. 3). Например, диод Шоттки, рассчитанный на рабочий ток не менее 1А (1N5819).
4. Подключите замок (защелку) к клеммной колодке *XT5* или *XT6* печатной платы контроллера, используя кабель №3.
 5. Для снятия статического электричества рекомендуется заземлить корпус или запорную планку замка. В случае установки замка на металлическую дверь, рекомендуется заземлять полотно двери. Заземление выполнять проводом с сечением не менее 0,75 мм².
 6. Произведите монтаж кнопки ДУ замка (защелки).
 7. Подключите кнопку ДУ к клеммной колодке *XT2* печатной платы контроллера, используя кабель №4.
 8. Произведите монтаж магнитного датчика двери (геркона). Магнитный датчик двери должен быть закреплен на раме двери, а магнит – на двери таким образом, чтобы при закрытой двери обеспечивалось устойчивое замыкание контакта датчика.
 9. Подключите магнитный датчик двери (геркон) к клеммной колодке *XT1* печатной платы контроллера, используя кабель №5.
 10. Произведите при необходимости монтаж охранных извещателей и прокладку ШС.
 11. Подключите ШС к клеммной колодке *XT8* печатной платы контроллера, используя кабель №6.

12. Установите при необходимости дополнительное оборудование. Для подключения используйте кабели №7 и №8.
12. Закрепите кабели пластиковыми стяжками к самоклеящимся площадкам из комплекта поставки, установив их по месту внутри корпуса контроллера.
13. Установите крышку контроллера и закрепите ее с помощью винтов.

8.7 Монтаж конфигурации «Контроллер управления турникетом»

Описано подключение устройств для вариантов конфигурации контроллера №4, 5.

Монтаж устройств производится согласно инструкциям, приводимым в технической документации соответствующих изделий.

Для подключения используются кабели, перечисленные в таблице 7. Расположение клеммных колодок на плате контроллера указано на рисунке 1.

1. Произведите монтаж контроллера.
2. Произведите монтаж и подключение устройств к интерфейсу RS-485 контроллера.
3. Произведите монтаж турникета производства фирмы PERCo¹⁴.



Примечание

Схема подключения цепи питания контроллера и турникета при подключении через PoE-сплиттера приведена на рисунке В.3 Приложения В к *Руководству*.

4. Для снятия статического электричества рекомендуется заземлить корпус турникета. Заземление выполнять проводом с сечением не менее 0,75 мм².
5. Подключите турникет (блок управления турникетом) к клеммным колодкам XT1, XT5, XT6 печатной платы контроллера согласно схеме, представленной на рисунке 4, для используемого типа турникета. Для подключения используйте кабель №9.



Примечание

Для турникетов производства PERCo параметр ИУ **Режим работы выхода управления** должен быть установлен в **Потенциальный**.
Для калитки **PERCo-WMD-05S** в ПО **PERCo-S-20** установите флажок параметра ИУ **Регистрация прохода по предъявлению идентификатора**.

6. Подключите ПДУ (или устройство РУ) к клеммной колодке XT2 печатной платы контроллера согласно схеме, представленной на рисунке 5. Для подключения используйте кабель №11 (№14).
7. Установите, при необходимости, дополнительное оборудование. Для подключения используйте кабели №7 и №8.
8. Закрепите кабели пластиковыми стяжками к самоклеящимся площадкам из комплекта поставки, установив их по месту внутри корпуса контроллера.
9. Установите крышку контроллера и закрепите ее с помощью винтов.

¹⁴ Для получения схем подключения турникетов сторонних производителей обращайтесь к специалистам **PERCo**.

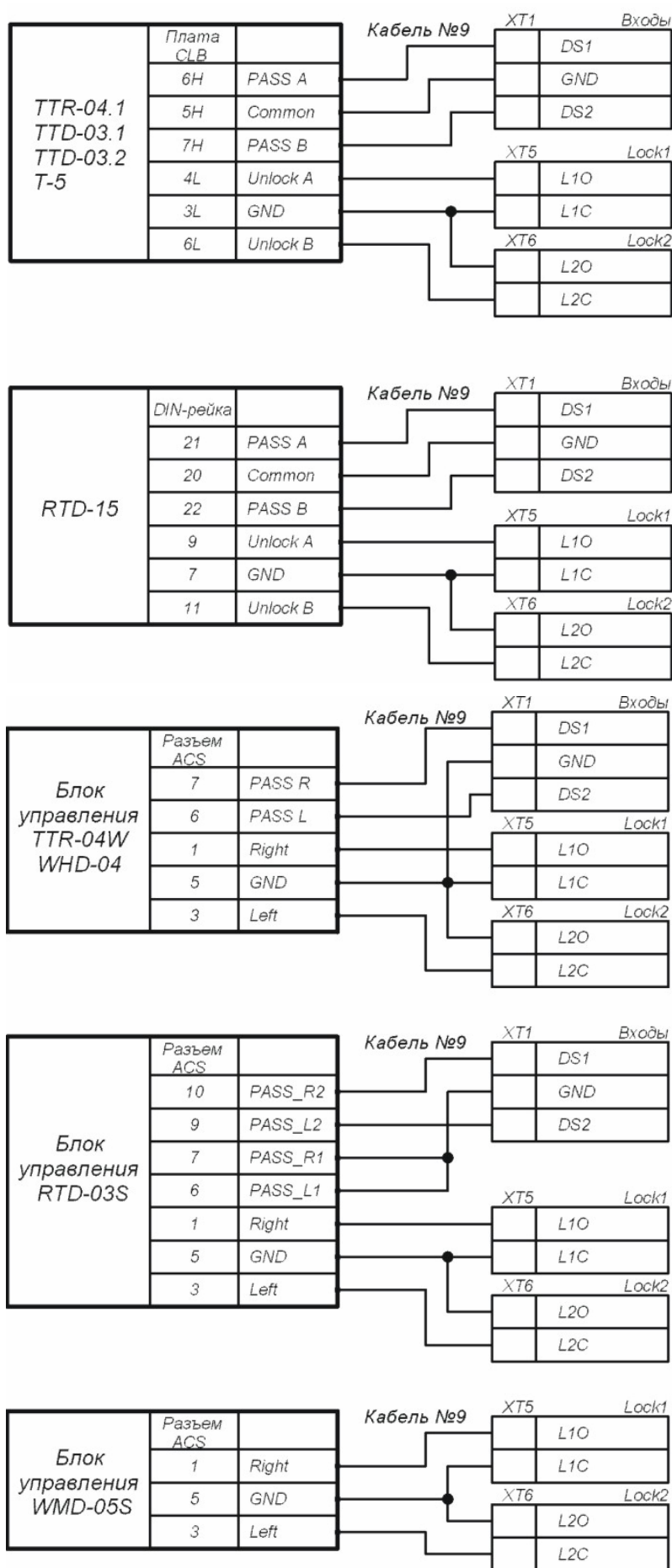


Рисунок 4. Схемы подключений ИУ в варианте «Управление турникетом»

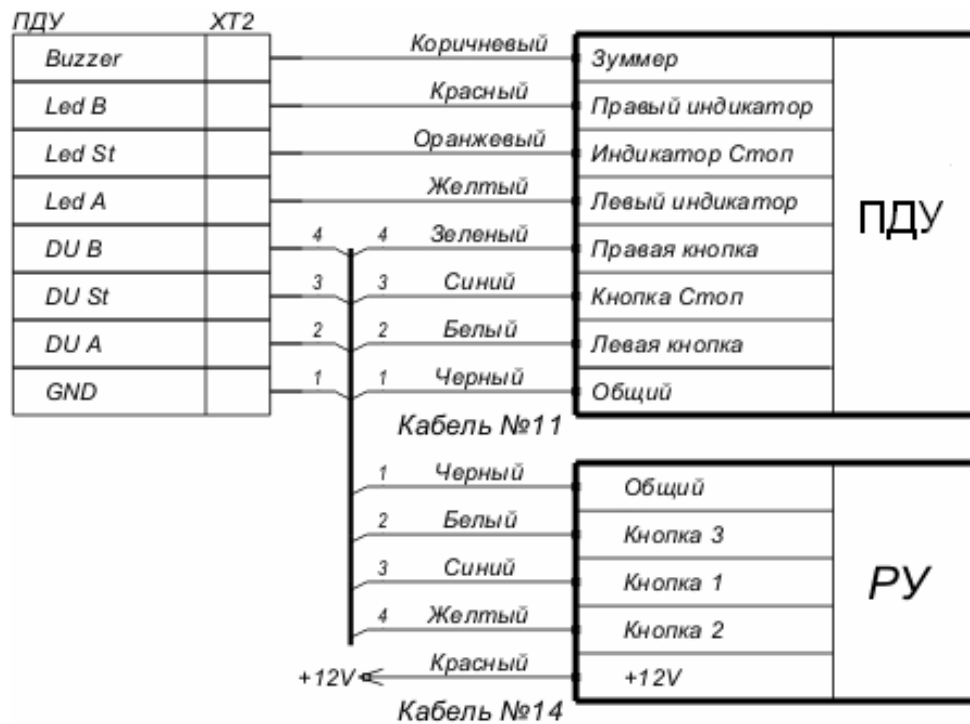


Рисунок 5. Схема подключений ПДУ или устройства РУ в варианте конфигурации «Управление турникетом» и «Контроллер АТП»

8.8 Монтаж в варианте конфигурации «Контроллер АТП»

Описано подключение устройств для вариантов конфигурации контроллера №6, 7.

При монтаже контроллера необходимо учесть логику работы с блоком управления ИУ автотранспортной проходной:

- Управление блоком управления ИУ автотранспортной проходной от контроллера АТП осуществляется от двух реле – при разрешении проезда активизируется и удерживается реле *Lock1*, подавая команду «Открыть». После проезда ТС (определяется по датчику проезда), либо по истечении времени ожидания прохода, реле *Lock1* нормализуется, после чего на 1 сек. активизируется реле *Lock2*, подавая команду «Закрыть». Так же реле *Lock2* активизируется на 1 сек. по нажатию кнопки ДУ **Закрыть**.
- При включенной в блоке управления ИУ автотранспортной проходной функции **Автоматического закрывания** управление от контроллера АТП осуществляется от одного реле. При разрешении проезда активизируется и удерживается реле *Lock1*, подавая команду «Открыть». После проезда ТС (определяется по датчику проезда), либо по истечении времени ожидания прохода реле *Lock1* нормализуется, после чего шлагбаум автоматически закрывается (время ожидания для автозакрывания рекомендуется устанавливать минимально возможное). Реле *Lock2* при этом работает согласно вышеописанному алгоритму, но не используется.

Монтаж устройств производится согласно инструкциям, приводимым в технической документации соответствующих изделий. Для подключения используются кабели, перечисленные в таблице 7. Расположение клеммных колодок на плате контроллера указано на рисунке 1.

1. Произведите монтаж контроллера.
2. Произведите монтаж и подключение устройств к интерфейсу *RS-485* контроллера.
3. Произведите монтаж ИУ автотранспортной проходной.



Примечание

Для снятия статического электричества рекомендуется заземлить корпус ИУ. Заземление выполнять проводом с сечением не менее 0,75 мм².

4. Подключите блок управления ИУ автотранспортной проходной.¹⁵ Для подключения используйте кабель №17.
 - Схема подключения шлагбаума CAME с блоками управления ZL37/ZL38 представлена на рисунке 6.
 - Схема подключения шлагбаума CAME с блоком управления C5 представлена на рисунке 7.
 - Схема подключения шлагбаума GENIYS SPIN с блоком управления LYNX 06 представлена на рисунке 8.
 - Пример схемы подключения шлагбаума NICE WIL4/WIL6 представлен на рисунке 9.
 - Пример схемы подключения шлагбаума FAAC с блоками управления 596/615 BPR представлен на рисунке 10.
 - Пример схемы подключения шлагбаума FAAC с блоком управления 624BLD представлен на рисунке 11.



Примечание

Параметр ИУ **Нормализация выхода ИУ** должен быть установлен в режим **После закрытия**.

При управлении от одного реле в блоке управления ИУ автотранспортной проходной должна быть включена функция **Автоматическое закрывание**, при этом время паузы для автоматического закрывания должно быть установлено на минимум - **Регулировка Т.С.А** (для CAME) и **PAUSE TIME** (для NICE).

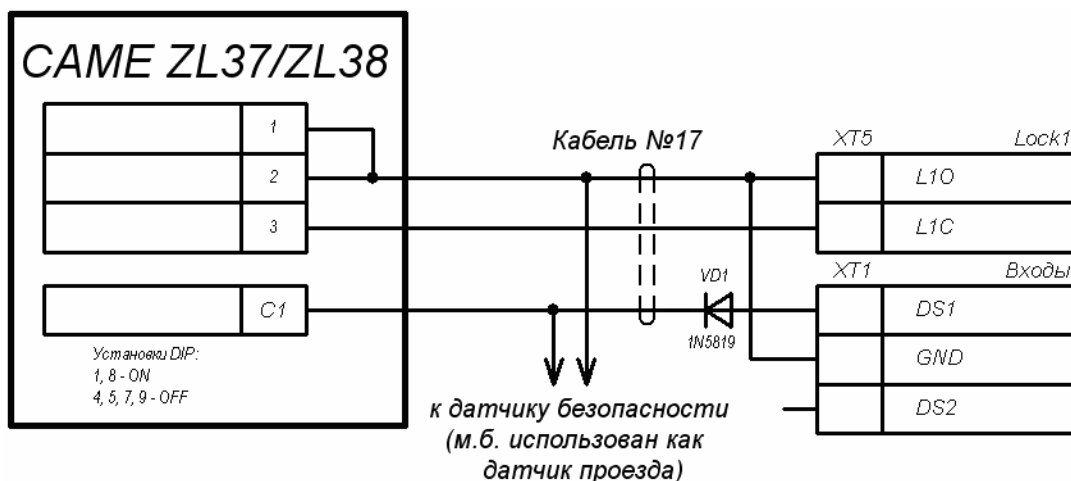


Рисунок 6. Схема подключения шлагбаума CAME с блоками управления ZL37/ZL38 к контроллеру автотранспортной проходной

¹⁵ Для получения схемы подключения блока управления ИУ автотранспортной проходной другого типа обращайтесь к специалистам **PERCo**.

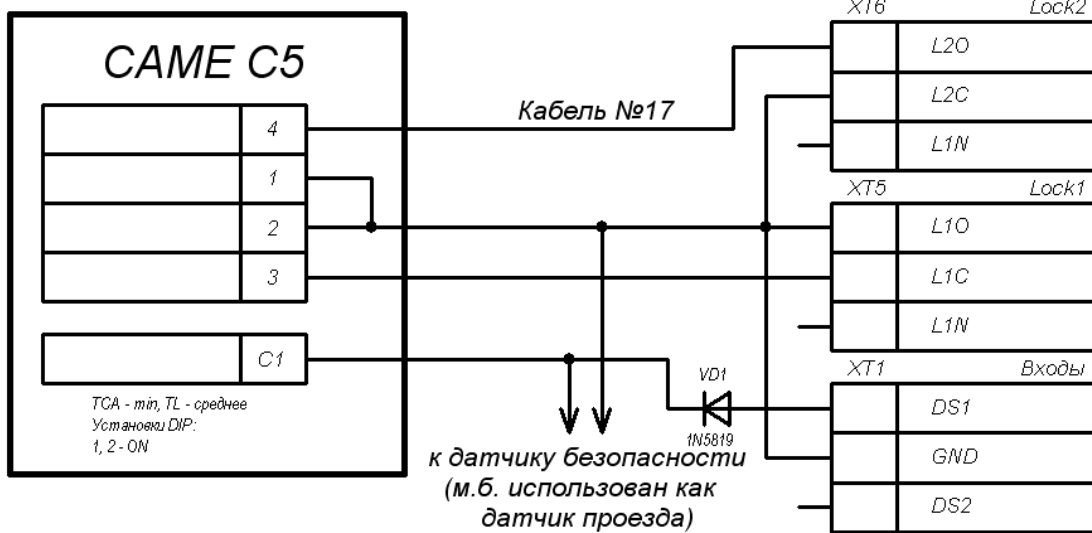


Рисунок 7. Схема подключения шлагбаума CAME с блоком управления C5 к контроллеру автотранспортной проходной

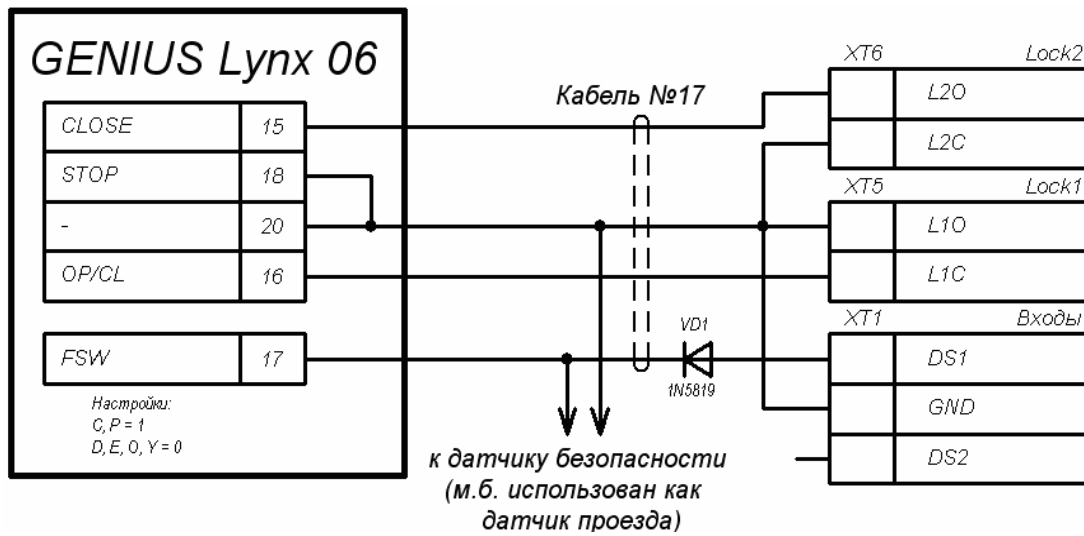


Рисунок 8. Схема подключения шлагбаума GENIUS SPIN с блоком управления LYNX 06 к контроллеру автотранспортной проходной

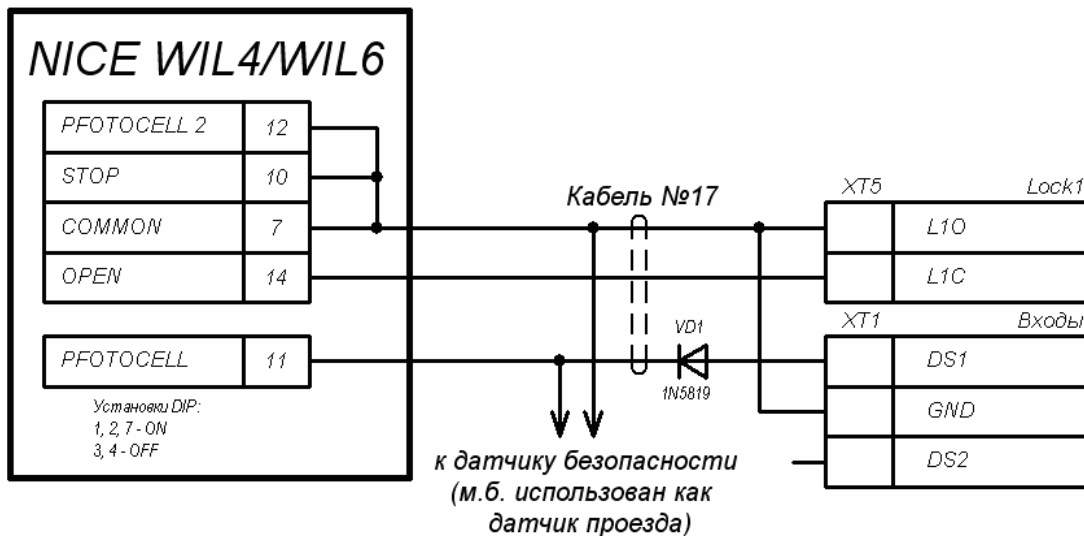


Рисунок 9. Пример схемы подключения шлагбаума NICE WIL4/WIL6 к контроллеру автотранспортной проходной

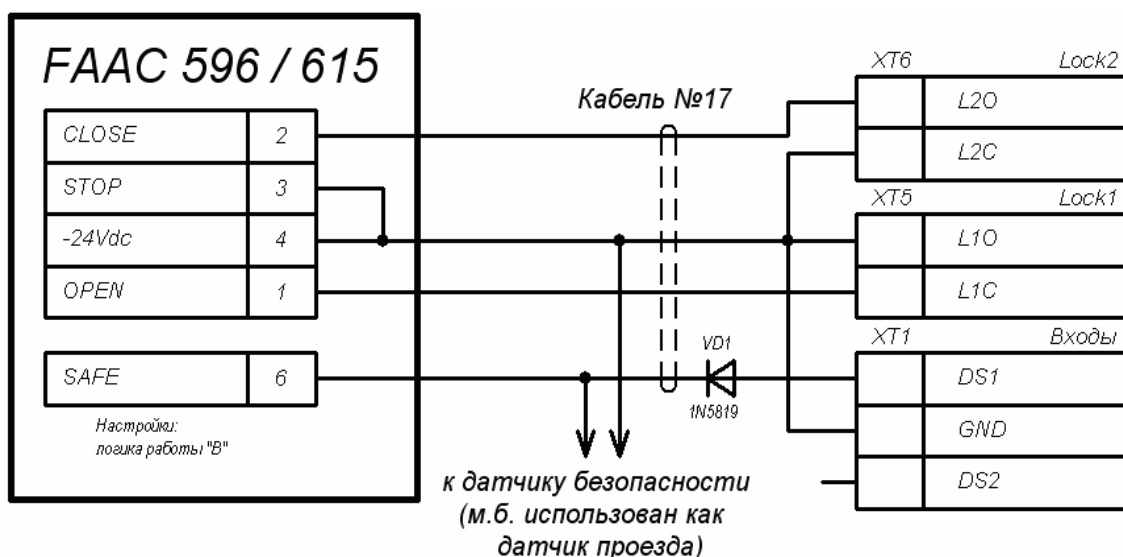


Рисунок 10. Пример схемы подключения шлагбаума FAAC с блоками управления FAAC 596/615 к контроллеру автотранспортной проходной

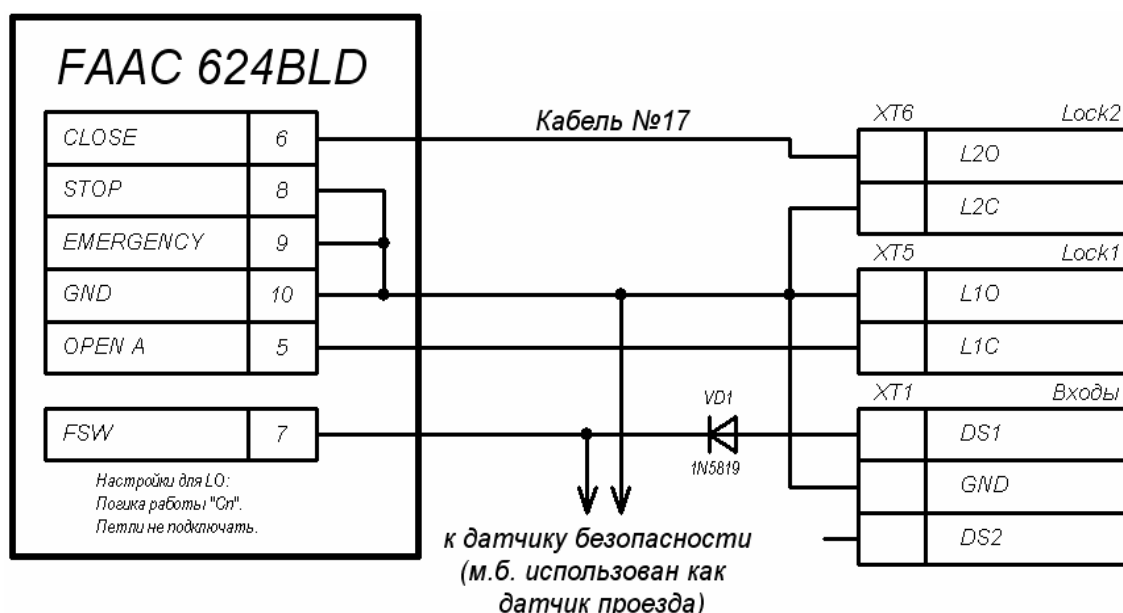


Рисунок 11. Пример схемы подключения шлагбаума FAAC с блоком управления FAAC 624BLD к контроллеру автотранспортной проходной

5. Подключите датчик проезда к клеммной колодке XT1 печатной платы контроллера согласно схеме представленной на рисунке 12. Для подключения используйте кабель №5. При подключении нескольких датчиков их выходы включаются последовательно.

Для моделей шлагбаумов CAME и GENIUS в качестве датчиков проезда используются ИК-датчики безопасности, штатно подключаемые к блоку управления ИУ автотранспортной проходной. В этом случае они параллельно подключаются к контроллеру АТП.

Для моделей шлагбаумов NICE и FAAC общий принцип подключения ИК-датчика к контроллеру АТП показан на примерах схем подключений блока управления для соответствующей модели. Вместо диода VD1 может потребоваться другая развязывающая цепь.

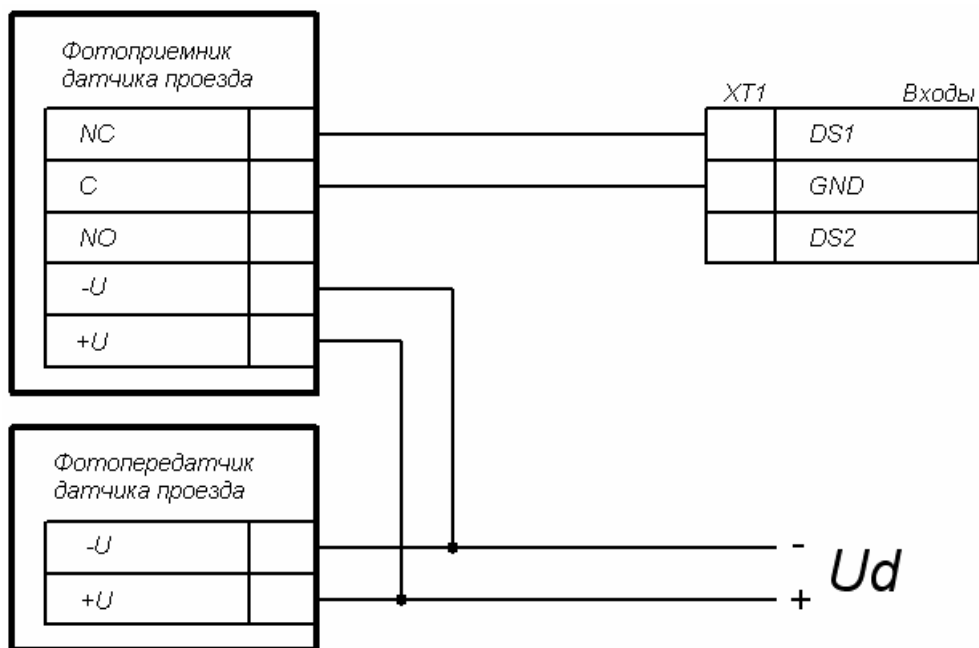


Рисунок 12. Схема подключения датчиков проезда

**Внимание!**

Для корректного проезда через ИУ транспортного средства с прицепом или имеющего другие прозрачные для датчика проезда места, рекомендуется устанавливать несколько разнесенных датчиков либо задать достаточное для прохождения мимо датчика прозрачного участка ТС значение параметра **Задержка восстановления датчиков проезда**.

При отсутствии датчика проезда необходимо установить флажок у параметра ИУ **Отсутствие датчика проезда** в ПО, при этом возможна некорректная работа ИУ автотранспортной проходной, связанная с невозможностью выбора оптимального времени проезда.

6. Установите при необходимости дополнительное оборудование. Для подключения используйте кабели №7 и №8.
7. Закрепите кабели пластиковыми стяжками к самоклеящимся площадкам из комплекта поставки, установив их по месту внутри корпуса контроллера.
8. Установите крышку контроллера и закрепите ее с помощью винтов.

8.9 Включение

При включении источника питания контроллера на крышке корпуса должна засветиться светодиодная индикация наличия питания.

При первом включении контроллера после завершения монтажа на передних панелях выносных считывателей и выносных блоков индикации, подключенных к контроллеру, начнется синхронное мигание всех трех индикаторов 2 раза в секунду, что означает отсутствие настроек контроллера.

Необходимо передать конфигурацию контроллеру и подключенным к нему устройствам. Это можно сделать через Web-интерфейс или с помощью ПО.



Примечание

Если было произведено изменение конфигурации контроллера с помощью переключателя, то при включении питания в течение примерно 1 минуты производится автоматическое форматирование памяти контроллера. В это время доступ к контроллеру из ПО или через Web-интерфейс невозможен. После форматирования в контроллер необходимо передать конфигурацию.

8.10 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.х.х.х (х-произвольные числа) и маску подсети 255.0.0.0. Наличие таких серверов или служб, как DNS и WINS, не требуется. Контроллер при этом должен быть подключен в тот же сегмент сети или непосредственно к разъему сетевой карты компьютера. После подключения сетевые настройки контроллера можно изменить на рекомендованные системным администратором из ПО или через Web-интерфейс.

9 КОНФИГУРАЦИЯ

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

- **«Локальное ПО» PERCo-SL01;**
- **«Локальное ПО с верификацией» PERCo-SL02;**
- Сетевое **«Базовое ПО S-20» PERCo-SN01 (PERCo-SS01 «Школа»);**
- Сетевое **«Расширенное ПО S-20» PERCo-SN02 (PERCo-SS02 «Школа»).**

9.1 Выбор формата хранения идентификаторов



Внимание!

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

В системе доступны следующие форматы хранения идентификаторов:

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

Порядок установки выбранного формата описан отдельно для ПО и Web-интерфейса. (См. 9.2.7, 9.3.2, 9.4.2.)

9.2 Настройка через Web-интерфейс

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

- задавать параметры конфигурации ИУ и считывателей;
- устанавливать режимы работы для считывателей;
- 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.

9.2.1 Подключение к контроллеру

Для работы с Web-интерфейсом:

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



Примечания

IP-адрес контроллера указан в паспорте и на плате контроллера. Для подключения к контроллеру по сети *Ethernet* необходимо, чтобы компьютер находился в одной подсети с контроллером (см. 8.10).

В настройках используемого браузера необходимо отключить прокси-сервер.

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



Внимание!

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

На странице можно выделить следующие элементы:

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

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

3. Рабочая область страницы.

9.2.2 Установка параметров конфигурации



Внимание!

При первом включении контроллера после изменения конфигурации с помощью переключателей или форматирования памяти необходимо передать в контроллер конфигурацию подключенных к нему устройств. Индикацией отсутствия настройки параметров служит синхронное мигание всех трех индикаторов на передних панелях выносных считывателей и выносных блоков индикации, подключенных к контроллеру 2 раза в секунду.

Для установки конфигурации:

1. В меню Web-интерфейса нажмите **Конфигурация**.
2. На странице **Исполнительное устройство** с помощью раскрывающегося списка **Номер исполнительного устройства** выберите последовательно номера подключенных ИУ. Для каждого ИУ установите необходимые параметры и нажмите кнопку **Сохранить**.
3. На странице **Считыватель** с помощью раскрывающегося списка **Номер считывателя** последовательно выберите номера подключенных считывателей. Для каждого считывателя установите параметры и нажмите кнопку **Сохранить**.
4. На странице **Формат для ввода и хранения карт доступа** выберите формат и нажмите кнопку **Сохранить**.
5. На странице **Управление считывателем** выберите режим работы для каждого считывателя.
6. Состояние ИУ и индикация на передних панелях выносных считывателей и выносных блоков индикации, подключенных к контроллеру, должны измениться в соответствии с установленным режимом работы.

9.2.3 Изменение сетевых настроек контроллера

Для изменения сетевых настроек контроллера:

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

Текущий IP-адрес	10.0.103.253
Новый IP-адрес	<input type="text"/>
Текущий адрес шлюза	0.0.0.0
Новый адрес шлюза	<input type="text"/>
Текущая маска подсети	255.0.0.0
Новая маска подсети	<input type="text"/>
<input checked="" type="radio"/> Текущая дата и время	14.08.2012 16:27:37
<input type="radio"/> Синхронизация с ПК	14.08.2012 16:26:57
<input type="radio"/> Ручная настройка	14.08.2012 DD.MM.YYYY 16:27:37 HH:MI:SS

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

**Примечание**

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

9.2.4 Изменение пароля контроллера

Для смены или задания пароля контроллера:

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

Новый пароль*

Подтвердите пароль*

* Пароль должен содержать не более 10 символов

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

9.2.5 Настройка параметров исполнительных устройств

Для настройки через Web-интерфейс доступны следующие параметры ИУ:

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

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

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

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

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

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

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

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

Направление прохода Если выбрано значение параметра **Прямое**, то нумерация считывателей соответствует состоянию переключателей «номер считывателя» на считывателях. Если выбрано **Обратное**, то тот считыватель, который в соответствии с его переключателем должен иметь номер 1, в контроллере будет опознаваться, как считыватель номер 2, и соответственно наоборот, считыватель номер 2 в контроллере будет опознаваться как считыватель номер 1.

Для настройки параметров ИУ:

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

Номер исполнительного устройства	<input type="text" value="1"/>
Предельное время разблокировки, с	<input type="text" value="8"/>
Время удержания в разблокированном состоянии, с	<input type="text" value="4"/>
Длительность импульса (для импульсного режима), с	<input type="text" value="0,25"/>
Нормальное состояние датчика (геркон)	<input checked="" type="radio"/> Нормально замкнут <input type="radio"/> Нормально разомкнут
Нормальное состояние выхода управления	<input type="radio"/> Запитан <input checked="" type="radio"/> Не запитан
Нормализация выхода управления	<input checked="" type="radio"/> После открытия <input type="radio"/> После закрытия
Режим работы выхода управления	<input checked="" type="radio"/> Потенциальный <input type="radio"/> Импульсный
Регистрация прохода по предъявлению карты	<input type="radio"/> Включена <input checked="" type="radio"/> Выключена
Направление прохода	<input checked="" type="radio"/> Прямое <input type="radio"/> Обратное

2. Из раскрывающегося списка **Номер исполнительного устройства** выберите ИУ, параметры которого необходимо настроить.
3. Произведите необходимые изменения настроек параметров.
4. Нажмите кнопку **Сохранить**.

9.2.6 Настройка параметров считывателей

Для настройки параметров считывателя:

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

Номер считывателя	<input type="text" value="1"/>
Управление от ДУ	<input type="radio"/> Запрещено <input checked="" type="radio"/> Разрешено

2. Из раскрывающегося списка **Номер считывателя** выберите необходимый считыватель.

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

9.2.7 Выбор формата хранения идентификаторов



Внимание!

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

Для выбора формата идентификаторов карт:

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

Выбор формата

Универсальный (8 байт)
 Сокращённый (3 байта, Wiegand 26)

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

9.2.8 Управление считывателями

Для управления режимом контроля доступа через ИУ в направлении, связанном с подключенным к нему считывателем произведите следующие действия:

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

Номер считывателя

Текущий режим работы

Установить:

1. Из раскрывающегося списка **Номер считывателя** выберите необходимый считыватель.
2. В строке **Текущий режим работы** отображается установленный в настоящий момент режим контроля доступа через ИУ при проходе в направлении выбранного считывателя.
3. С помощью кнопок **Контроль**, **Открыто**, **Закрыто**, **Охрана** установите режим работы через выбранный считыватель.



Примечания

При установке режима работы «**Охрана**» на охрану ставится направление ИУ, связанное со считывателем, выбранном в раскрывающемся списке **Номер считывателя**.

Режим работы «**Охрана**» возможен только для вариантов конфигураций № 1 – 3 (см. таблицу 5).

9.2.9 Сброс тревоги исполнительных устройств

Для сброса тревоги исполнительного устройства:

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

Номер исполнительного устройства

2. Из раскрывающегося списка **Номер исполнительного устройства** выберите ИУ, для которого необходимо сбросить тревогу.
3. Нажмите кнопку **Сбросить тревогу**. Состояние тревоги для выбранного ИУ будет сброшено.

9.2.10 Добавление карт доступа

Ввод идентификатора вручную

Для ввода идентификатора карты вручную:

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

Номер исполнительного устройства

Загружено карт: 4

Ввод номера карты / поиск карты:

Код семейства	Номер пропуска	Одним числом	
<input type="text" value="111"/>	<input type="text" value="22222"/>	<input type="text" value="33333333"/>	<input type="button" value="Ввод"/>

2. Из раскрывающегося списка **Номер исполнительного устройства** выберите ИУ, для которого необходимо ввести номера карт.
3. В поля ввода **Код семейства** и **Номер пропуска** введите номер карты. Нажмите кнопку **Ввод**.
4. На странице появится таблица с номером карты:

Карта 7296718 отсутствует в списке

Задание / получение прав доступа карты:

Номер карты			Право постановки на охрану	Сохранить изменения	Удалить карту из списка
Код семейства	Номер пропуска	Одним числом			
<input type="text" value="111"/>	<input type="text" value="22222"/>	<input type="text" value="7296718"/>	<input type="text" value="нет"/>	<input type="button" value="Сохранить"/>	<input type="button" value="Удалить"/>

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



Примечание

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

Ввод идентификатора через считыватель

Для ввода номеров карт с использованием считывателя:

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

Номер исполнительного устройства

Загружено карт: 4

Получение номера карты от контроллера доступа:

Поднесите карту к считывателю

2. Из раскрывающегося списка **Номер исполнительного устройства** выберите ИУ, для которого необходимо ввести номера карт.
3. Нажмите кнопку **Старт**, строчка **Поднесите карту к считывателю** изменит цвет (потемнеет).
4. Поднесите к считывателю последовательно карты, номера которых необходимо ввести в контроллер. По окончании ввода нажмите кнопку **Стоп**.



Примечание

За один раз через считыватель возможно ввести не более четырех карт.

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

Задание / получение прав доступа карты:

Номер карты			Право постановки на охрану	Сохранить изменения	Удалить карту из списка
Код семейства	Номер пропуска	Одним числом			
12	41897	828329	нет	<input type="button" value="Сохранить"/>	<input type="button" value="Удалить"/>
10	30915	686275	да	<input type="button" value="Сохранить"/>	<input type="button" value="Удалить"/>
12	45460	831892	нет	<input type="button" value="Сохранить"/>	<input type="button" value="Удалить"/>
85	8222	5578782	да	<input type="button" value="Сохранить"/>	<input type="button" value="Удалить"/>

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

Загрузка идентификатора из файла



Внимание!

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

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

9716931	1
11027887 0	
12979604	1
645634 1	
1236879	0

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



Примечание

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

Для загрузки номеров карт из текстового файла:

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

Номер исполнительного устройства

Загружено карт: 4

2. Из раскрывающегося списка **Номер исполнительного устройства** выберите ИУ, для которого необходимо загрузить номера карт.
3. Нажмите кнопку **Обзор**. В открывшемся окне укажите расположение и название текстового файла с номерами карт и нажмите кнопку **Открыть**. Окно будет закрыто, в поле рядом с кнопкой **Обзор** будет указан путь к файлу.
4. Нажмите кнопку **Основной список**. В появившейся странице **Загрузка выполнена** нажмите кнопку **Закрыть окно**.
5. Количество загруженных в память контроллера карт изменится.



Примечание

Если в качестве ИУ выбран контроллер второго уровня **PERCo-CL201**, то кроме кнопки **Основной список** в рабочей области страницы будет присутствовать кнопка **Аварийный список**.

Аварийный список карт это дополнительный список номеров карт, по которому при пропадании связи с контроллером **PERCo-CL201** осуществляется доступ в контролируемое им помещение.

Для загрузки аварийного списка карт: создайте текстовый файл, наберите в нем одним столбцом список карт, входящих в аварийный список и загрузите в контроллер, используя кнопку **Аварийный список**.

9.2.11 Список сохраненных карт

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

Номер исполнительного устройства

Загружено карт: 4

Список карт для исполнительного устройства № 1

Номер карты			Право постановки на охрану	Сохранить изменения	Удалить карту из списка
Код семейства	Номер пропуска	Одним числом			
<input type="text" value="9"/>	<input type="text" value="64999"/>	<input type="text" value="654823"/>	<input type="text" value="нет"/>	<input type="button" value="Сохранить"/>	<input type="button" value="Удалить"/>
<input type="text" value="11"/>	<input type="text" value="44860"/>	<input type="text" value="765756"/>	<input type="text" value="да"/>	<input type="button" value="Сохранить"/>	<input type="button" value="Удалить"/>
<input type="text" value="52"/>	<input type="text" value="45586"/>	<input type="text" value="3453458"/>	<input type="text" value="нет"/>	<input type="button" value="Сохранить"/>	<input type="button" value="Удалить"/>
<input type="text" value="69"/>	<input type="text" value="32373"/>	<input type="text" value="4554357"/>	<input type="text" value="нет"/>	<input type="button" value="Сохранить"/>	<input type="button" value="Удалить"/>

[Предыдущие 20 карт](#) | [Следующие 20 карт](#)

Из раскрывающегося списка **Номер исполнительного устройства** выберите ИУ для просмотра используемого при проходе через него списка карт:

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



Примечание

Максимальное число хранимых в памяти контроллера номеров карт доступа зависит от его конфигурации (см. таблицу 5).

9.2.12 Журнал событий

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

Событий в памяти контроллера: 194

Вариант отображения журнала событий Полный Краткий

Интервал просмотра событий: с по

№	Дата	Время	Событие	Ресурс	Номер карты
1	14.08.2012	08:37:46	Проход по карте с нарушением времени	Считыватель № 1	3542652 (54. 3708)
2	14.08.2012	08:37:46	Проход по карте с нарушением времени	Считыватель № 1	7935550 (121. 5694)
3	14.08.2012	08:36:44	Восстановление связи		

<< [Следующие 20 событий](#) | [Предыдущие 20 событий](#) >>

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



Примечание

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

- Для просмотра журнала событий установите **Интервал просмотра событий** и нажмите кнопку **Ввод**. В таблице будут выведены

зарегистрированные контроллером события в обратном хронологическом порядке.



Примечание

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

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



Примечание

Максимальное число хранимых в памяти контроллера событий 135 000.

9.2.13 Обслуживание контроллера

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



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



Внимание!

При тестировании контроллера журнал регистрации событий автоматически очищается.

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



Внимание!

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

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

9.3 Локальное ПО

Рассматривается настройка контроллера в следующем ПО:

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

«Локальное ПО» позволяет производить следующие действия:

- формировать список сотрудников;
- выдавать карты доступа сотрудникам с указанием ФИО сотрудников;
- управлять режимами контроля доступа через подключенные к контроллеру ИУ;
- просматривать журнал событий сотрудников и устройств;
- задавать параметры конфигурации ИУ и считывателей;
- контролировать состояние контроллера и подключенных к нему устройств;

«Локальное ПО с верификацией», кроме этого:

- позволяет формировать и контролировать режимы работы охранных зон;
- поддерживает работу с функциями верификации и индикации;
- позволяет выдавать права постановки и снятия с охраны ИУ с помощью идентификатора;
- выдавать карты доступа посетителям.



Внимание!

В «Локальном ПО» и «Локальное ПО с верификацией» не предусмотрена возможность использования контроллера в вариантах конфигурации №6 и №7 «Контроллер автотранспортной проходной».

9.3.1 Подключение к контроллеру

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

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



Внимание!

Если искомый контроллер и компьютер с установленным «Локальным ПО» находятся в разных подсетях, то контроллер не будет найден (см. 8.10). При первом включении контроллера после изменения конфигурации или форматирования памяти необходимо передать в контроллер конфигурацию подключенных к нему устройств. Индикацией отсутствия настройки параметров служит синхронное мигание с частотой 2 Гц всех трех индикаторов на передних панелях выносных считывателей и выносных блоков индикации, подключенных к контроллеру. ПО автоматически задает параметры подключенных устройств. Для передачи параметров в контроллер необходимо нажать кнопку **Передать конфигурацию** на вкладке **Конфигурация** в окне **Контроллер** или в главном меню программы последовательно выбрать **Редактирование** → **Передать конфигурацию**.

9.3.2 Выбор формата хранения идентификаторов

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

Доступны следующие форматы:

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

9.3.3 Разрешение Web-интерфейса

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



Примечание

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

9.3.4 Параметры исполнительного устройства

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

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

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

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

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

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

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

Режим работы выхода управления ИУ :

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

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

Направление прохода. Параметр доступен при наличии двух считывателей для одного исполнительного устройства (двухсторонняя дверь, турникет). Значение:

- **Прямое** означает регистрацию входа по считывателю, указанному в окне «Исполнительное устройство» в строке «Входной считыватель», и регистрацию выхода по другому считывателю.
- **Обратное** означает регистрацию входа и выхода в обратном направлении.

Датчик несанкционированного прохода и сирены. При установке флажка активизирует датчик контроля зоны прохода и сирены, доступный для некоторых моделей турникетов.

По умолчанию. Кнопка возвращает параметры, автоматически установленные программой.

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

Отменить. Кнопка закрывает окно, не изменяя параметры.

9.3.5 Конфигурация охранных зон сигнализации



Внимание!

Конфигурация зон сигнализации доступна только в «**Локальное ПО с верификацией**» **PERCo-SL02**.

Подключение двух ШС и настройка двух ОЗ предусматривается в вариантах конфигурации контроллера №1-3 (см. таблицу 5).

Для настройки охранных и пожарных зон сигнализации на вкладке **Конфигурация** в окне **Контроллер** нажмите кнопку **Выходы, шлейфы, зоны**.

Окно **Выходы, шлейфы, зоны** предназначено для создания охранных и пожарных зон сигнализации, конфигурирования шлейфов сигнализации, настройки программ поведения устройств (оповещателей), подключенных к выходам контроллера.

Выходы, шлейфы, зоны

Выходы

Выход 1
Выход 2
Выход 3
Выход 4

Тип: Охранный

Нормализованное состояние: Не запитан

Параметры:

Выполняемая программа: Включить при тревоге

Время работы программы: 1 сек

Задержка перед запуском: 1 сек

Зоны

Зона 1
Зона 2

Шлейфы

Шлейф 1
Шлейф 2

Тип: ОШС

Параметры:

Перезапрос

Задержка взятия на охрану: 1 сек

Длительность нарушения: 70 миллисекунд

Задержка нарушенного ШС в режиме "СНЯТ": 1 сек

Зоны

Зона 1
Зона 2

Тип: Охранная

Шлейфы:

Шлейф 1
 Шлейф 2

Параметры:

Работа при невзятии: Тревога

ИУ, входящий в зону: Замок

Повторное включение сирены

Не менять при тревоге на ОШС

выходы, работающие по программам «Сирена» и «Лампа»

Сохранить и передать в аппаратуру Закрыть

Параметры настройки ОЗ

- Список доступных ШС **Шлейфы**.
- Раскрывающийся список **Тип** для выбора типа подключенного ШС:
 - Не используется**. Шлейф не подключен.
 - ОШС**. Подключен охранный ШС.
 - ОШС с контролем вскрытия корпуса**. Подключен охранный ШС с контролем вскрытия корпусов извещателей.
- Область **Параметры**, для настройки доступны следующие параметры ШС:
 - Перезапрос** (Поддержка перезапроса). При установке флажка контроллер после срабатывания извещателей снимает питание со шлейфа и перепроверяет его состояние.
 - Задержка взятия на охрану**. Параметр определяет время, через которое панель предпринимает попытку взять шлейф на охрану после поступления соответствующей команды.
 - Длительность нарушения**. Параметр определяет время интегрирования для шлейфа (то есть максимальное время нарушения, не приводящее к переходу в состояние «Тревога»).
 - Задержка нарушенного ШС в режиме «Снят»** (Задержка восстановления нарушенного шлейфа в снятом состоянии):
 - Если в данном параметре установлено значение «0», то шлейф в состоянии «Снят» не контролируется.

В противном случае продолжается отслеживание шлейфа в режиме «Снят»:

- Если при этом шлейф перейдет в состояние «Нарушение», то в журнал также записывается событие «Неисправность снятого ОШС», состояние выходов и встроенная звуковая индикация панели не изменяются.
 - Если после этого нормальное состояние шлейфа восстановится и продержится период времени, указанный в этом параметре, то шлейф выйдет из состояния «Нарушение» и при этом в журнал также будет записано сообщение «Нормализация снятого ОШС». Состояние выходов и встроенная звуковая индикация панели не изменяются.
4. Список доступных ОЗ **Зоны**, с включенными в них ИУ.
 5. Раскрывающийся список **Тип** для создания ОЗ:
 - **Не используется.** ОЗ не используется.
 - **Охранная.** Создана ОЗ.
 6. Список **Шлейфы** для указания ШС, входящих в выбранную ОЗ.
 7. Область **Параметры** для настройки доступны следующие параметры ОЗ:
 - **Работа при невзятии** (Режим работы при невзятии). Параметр указывает действие, которое будет происходить при невозможности взятия данной зоны на охрану. Имеются следующие значения:
 - **Тревога.** Зона будет переведена в режим «Тревога».
 - **Автоматическое перевзятие.** Зона будет переведена в режим «Взятие», а затем будет производиться повторная попытка взятия до тех пор, пока взятие не произойдет.
 - **Возврат в «Снят».** Зона перейдет в режим «Снята».
 - **ИУ, входящий в зону.** В строке отображается ИУ, входящее в выбранную ОЗ.
 - **Повторное включение сирены.** При установке флажка активизация дополнительного выхода, управляемого по программе «Сирена», происходит при каждом нарушении зоны, даже если она уже находится в режиме «Тревога».
 - **Не менять при тревоге на ОШС выходы, работающие по программам «Сирена» и «Лампа».** При установке флажка при переходе ОЗ в состояние «Тревога» не будут активизироваться выходы, работающие по программам «Сирена» и «Лампа», что соответствует тихой тревоге.
 8. Список доступных выходов **Выходы**.
 9. Раскрывающийся список **Тип выхода**:
 - **Не используется.**
 - **Охранный.**
 10. **Нормализованное состояние** (*Не запитан / Запитан*). Параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий.
 11. **Зоны.** Зоны, активизирующие выход. Параметр позволяет выбрать зоны, нарушения в которых приведет к активизации выхода.
 12. Область **Параметры**. Для настройки доступны следующие параметры дополнительных выходов контроллера:
 - **Выполняемая программа** (Программа управления). Режим работы выхода после активизации. Доступны следующие программы:
 - **Включить при тревоге.** В случае перехода одной из зон в режим «ТРЕВОГА» произойдет замыкание контакта дополнительного выхода.

- **Мигать при тревоге.** В случае перехода **одной из зон** в режим «ТРЕВОГА» произойдет попеременное замыкание/размыкание контактов дополнительного выхода.
 - **Лампа 1.** Программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы **все зоны** изменили свой режим.
 - **Время работы программы** (Время активизации). Время, в течение которого при наличии активизирующего управляющего воздействия выход меняет свое состояние из нормализованного на противоположное. Как правило, в этом случае к такому дополнительному выходу подключают тревожный оповещатель (сирена, проблесковая лампа).
 - **Задержка перед запуском.** Промежуток времени между изменением состояния ОЗ и запуском программы управлением выходом.
13. **Сохранить и передать в аппаратуру.** При нажатии кнопки измененные параметры передаются в контроллер, окно закрывается.
14. **Закреть.** При нажатии кнопки окно закрывается без сохранения внесенных изменений.

Порядок настройки ОЗ

В окне настройки элементов **Выходы, шлейфы, зоны**:

1. В списке **Шлейфы** (1) укажите подключенные к контроллеру шлейфы и с помощью раскрывающегося списка **Тип** (2) укажите их типы.
2. Настройте **Параметры** (3) каждого шлейфа.
3. В списке **Зоны** (4) укажите создаваемые зоны и с помощью раскрывающегося списка **Тип** (5) укажите их типы.
4. С помощью переключателей **Шлейфы** (6) отметьте для каждой из зон входящие в нее шлейфы.
5. Настройте **Параметры** (7) каждой зоны.
6. В списке **Выходы** (8) укажите выходы контроллера, к которым подключены устройства, и с помощью раскрывающегося списка **Тип** (9) укажите их типы.
7. Установите с помощью раскрывающегося списка **Нормализованное состояние** (10) подключенного устройств.
8. Используя переключатели **Зоны** (11), укажите для каждого из устройств зоны, нарушения в которых приведут к его срабатыванию.
9. В области настройки **Параметры** выхода (12) выберите программу срабатывания каждого устройства и ее временные характеристики.
10. Закройте окно **Выходы, шлейфы, зоны**, нажав кнопку **Сохранить и передать в аппаратуру** (13).
11. Для закрытия окна без сохранения измененных параметров нажмите кнопку **Закреть** (14).



Примечание

Прежде чем передавать новые параметры в контроллер, убедитесь, что система снята с охраны.


9.4 Сетевое ПО S-20

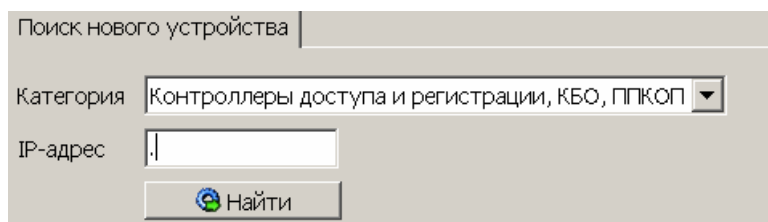
Программное обеспечение системы **PERCO-S-20** выполнено по модульному принципу. Каждый сетевой модуль предназначен для выполнения определенных функций.

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

9.4.1 Подключение к контроллеру

Для подключения контроллера:

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



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



Примечание


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

Для подключения к контроллеру по сети *Ethernet* необходимо, чтобы компьютер находился в одной подсети с контроллером (см. 8.10).

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



Внимание!

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

9.4.2 Параметры системы безопасности

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

Список объектов (1) ▲	Параметры Общий список реакций на события						
<ul style="list-style-type: none"> [-] Система безопасности <ul style="list-style-type: none"> [-] Контроллер турникета/замка (10.0.201.232) 	<table border="1"> <tr> <td>Текущее наименование</td> <td>Система безопасности</td> </tr> <tr> <td>Внешняя защита от передачи идентификаторов (Global Antipass)</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Протокол считывателей</td> <td>Wiegand 26</td> </tr> </table>	Текущее наименование	Система безопасности	Внешняя защита от передачи идентификаторов (Global Antipass)	<input checked="" type="checkbox"/>	Протокол считывателей	Wiegand 26
Текущее наименование	Система безопасности						
Внешняя защита от передачи идентификаторов (Global Antipass)	<input checked="" type="checkbox"/>						
Протокол считывателей	Wiegand 26						


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

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

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

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

9.4.3 Ресурсы контроллера

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

- Дополнительные входы;
- Дополнительные выходы;
- Шлейфы сигнализации;
- Охранные зоны;
- Контроллер ИУ (замка, турникета, шлагбаума);

Если к контроллеру подключены несколько исполнительных устройств или замковые контроллеры **PERCo-CL201**, то в списке ресурсов будет отображаться несколько контроллеров ИУ. Каждый контроллер ИУ также обладает своим списком ресурсов:

- Считыватель;
- ИУ (замок, турникет, шлагбаум);
- Генератор тревоги;
- ОЗ.

Список объектов (1) ▲

- Система безопасности
 - Контроллер турникета/замка (10.0.201.232)
 - Дополнительные входы
 - Дополнительный вход №1
 - Дополнительный вход №2
 - Дополнительные выходы
 - Дополнительный выход №1
 - Дополнительный выход №2
 - Дополнительный выход №3
 - Дополнительный выход №4
 - Шлейфы сигнализации
 - Шлейф сигнализации №1
 - Шлейф сигнализации №2
 - Охранные зоны
 - Охранная зона №11
 - Охранная зона №12
 - Контроллер замка (10.0.201.232)
 - Считыватель №1
 - Считыватель №2
 - Замок №1
 - Генератор тревоги №1
 - Охранная зона №1

Параметры		События	
MAC-адрес	00:25:0B:00:C9:E8		
IP-адрес	10.0.201.232		
Маска подсети	255.0.0.0		
Шлюз	0.0.0.0		
Порт конфигурации	18900		
Порт управления	18902		
Порт журнала регистрации	18903		
Порт журнала мониторинга	18906		
Порт индикации	18904		
Порт верификации	18905		
Текущее наименование	Контроллер турникета/замка		
Первоначальное наименование	Контроллер турникета/замка		
Модель	PERCo-CT/L04		
Разрешить WEB-интерфейс	<input checked="" type="checkbox"/>		
Коррекция времени относительно времени сервера системы	0 час.		





В зависимости от выбранного варианта конфигурации (см. таблицу 5) наличие и количество ресурсов может различаться. В таблице 8 представлен перечень ресурсов контроллера в разных вариантах конфигурации.

Таблица 8. Ресурсы контроллера для различных конфигураций

№	Доп. вход	Доп. выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считыватель	ИУ	Ген. тревоги	ОЗ
1	2	4	2	2	0	2	замок	1	1
2	2	4	2	2	8	2	замок	1	1
3	2	4	2	2	8	2	2 замка	2	2
4	2	2	0	0	0	2	турникет	1	0
5	2	2	0	0	8	2	турникет	1	0
6	2	2	0	0	0	2	шлагбаум	1	0
7	2	2	0	0	8	2	шлагбаум	1	0

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

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

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

9.4.4 Контроллер

Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название контроллера.

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

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



Примечание

По умолчанию при подключении к контроллеру Web-интерфейс отключен.

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

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

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

Активизировать дополнительные выходы. Приводит к активизации всех релейных выходов выбранного контроллера, для которых выбран **Тип: Обычный**.

Нормализовать дополнительные выходы. Приводит к нормализации всех релейных выходов данного контроллера, для которых выбран **Тип: Обычный**.

9.4.5 Дополнительный вход

Дополнительные входы контроллеров могут быть использованы для наблюдения за состоянием внешнего оборудования, подключенного к ним, и для подключения кнопок сброса тревоги и активизации режима **Fire Alarm**. Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название входа.

Тип. Раскрывающийся список позволяет выбрать следующие типы входа:

- **Нет.** К данному входу не подключено никакое внешнее оборудование.
- **Обычный.** К данному входу подключено внешнее оборудование, состояние которого должно контролироваться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.

Параметры	События
Адрес	1
Текущее наименование	Дополнительный вход №1
Первоначальное наименование	Дополнительный вход №1
Тип	Обычный
<input type="checkbox"/> Обычный	
Нормальное состояние контакт.	Разомкнут
<input type="checkbox"/> Дополнительные входы, маскируемые при активизации	
<input type="checkbox"/> Критерий маскирования	На указанное время
<input type="checkbox"/> На указанное время	
Время	0 мс.
<input type="checkbox"/> Дополнительные выходы, активизируемые при активизации	
<input type="checkbox"/> Критерий активизации	На указанное время
<input type="checkbox"/> На указанное время	
Время	0 мс.
Дополнительный выход №3	<input type="checkbox"/>
<input type="checkbox"/> Дополнительные выходы, нормализируемые при активизации	
<input type="checkbox"/> Критерий нормализации	На указанное время
<input type="checkbox"/> На указанное время	
Дополнительный выход №3	<input checked="" type="checkbox"/>

- **Специальный.** Предназначен для автономного сброса тревоги, выключения sireны либо перевода контроллера в режим **Fire Alarm** при поступлении управляющего сигнала на этот дополнительный вход.

Параметры	События
Адрес	1
Текущее наименование	Дополнительный вход №1
Первоначальное наименование	Дополнительный вход №1
Тип	Специальный
<input type="checkbox"/> Специальный	
Нормальное состояние контакта	Разомкнут
Сброс тревоги (Генератор тревоги)	<input type="checkbox"/>
Сброс sireны (Выход "С" ОПС)	<input type="checkbox"/>

Нормальное состояние контакта (*Разомкнут / Замкнут*). Этот параметр зависит от типа подключенного оборудования и указывает контроллеру на то, какое значение уровня сигнала на данном дополнительном входе он должен воспринимать как нормальное.

Дополнительные входы, маскируемые при активизации. Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы (т.е. не воспринимать управляющий сигнал от внешнего оборудования) при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажками те дополнительные входы, которые должны быть маскированы. Укажите временной критерий маскирования.

Дополнительные выходы, активизируемые при активизации. Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Укажите временной критерий активизации.

Дополнительные выходы, нормализуемые при активизации. Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализованы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажками те дополнительные выходы, которые должны быть нормализованы. Укажите временной критерий нормализации.

Временной Критерий маскирования/активизации/нормализации:

- **На указанное время.** Выбранные дополнительные входы будут маскированы на указанное время.
- **На время срабатывания.** Выбранные дополнительные входы будут маскированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
- **На время срабатывания и после срабатывания.** Выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал, плюс указанное вами время.

Сброс тревоги (Генератор тревоги). При установке флажка получение управляющего сигнала на данном дополнительном входе приведет к сбросу тревоги.

Сброс сирены (Выход «С» ОПС). При установке флажка получение управляющего сигнала на данном дополнительном входе приведет к выключению сирены, подключенной к выходу, работающему по программе «Сирена».

Fire Alarm. Режим работы турникета в случае возникновения пожара. Турникет в этом режиме разблокирован для прохода в обоих направлениях. Для активизации режима необходимо подать управляющий сигнал на **Дополнительный вход**, сконфигурированный как **Специальный**. При этом ни один из флажков **Сброс тревоги (Генератор тревоги)**, **Сброс сирены (Выход «С» ОПС)**, не должен быть установлен.

9.4.6 Дополнительный выход

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

Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название выхода.

Тип. Раскрывающийся список позволяет выбрать следующие типы выхода:

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

Параметры	События
Адрес	3
Текущее наименование	Дополнительный выход №3
Первоначальное наименование	Дополнительный выход №3
Тип	Обычный
<input type="checkbox"/> Обычный	
Нормальное состояние	Не запитан

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

Параметры	События
Адрес	3
Текущее наименование	Дополнительный выход №3
Первоначальное наименование	Дополнительный выход №3
Тип	Генератора тревоги
Генератора тревоги	
Нормальное состояние	Не запитан
Время активизации	1 сек.

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

Параметры	События
Адрес	1
Текущее наименование	Дополнительный выход №1
Первоначальное наименование	Дополнительный выход №1
Тип	ОПС
ОПС	
Нормальное состояние	Не запитан
Задержка перед запуском	0 мс.
Время активизации	1 сек.
Программа управления	Не управлять
Зоны, активизирующие выход	
Охранная зона №11	<input type="checkbox"/>
Охранная зона №12	<input type="checkbox"/>
Охранная зона №1	<input type="checkbox"/>

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

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

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

Программа управления. Режим работы выхода после активизации. Доступны следующие программы:

- **Не управлять.**
- **Включить при тревоге.** В случае перехода одной из зон в режим «Тревога» произойдет замыкание контакта дополнительного выхода.
- **Мигать при тревоге.** В случае перехода одной из зон в режим «Тревога» произойдет попеременное замыкание/размыкание контактов дополнительного выхода.
- **Лампа 1.** Программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы **все зоны** изменили свой режим.
- **Лампа 2.** Программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы **хотя бы одна из зон** изменила свой режим.
- **ПЦН 1.** Программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы **все зоны** изменили свой режим.
- **ПЦН 2.** Программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы **хотя бы одна из зон** изменила свой режим.
- **Сирена.** Программа управления, указывающая на то, что к дополнительному выходу подключен звуковой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы **хотя бы одна из зон** изменила свой режим.
- **Включить перед взятием.** Перед переходом одной из зон в режим «Взятие» произойдет замыкание контакта дополнительного выхода.
- **Включить при взятии.** При переходе одной из зон в режим «Взятие» произойдет замыкание контакта дополнительного выхода.
- **Включить при снятии.** Перед переходом одной из зон в режим «Снята» произойдет замыкание контакта дополнительного выхода.
- **Включить при автоперевзятии.** При переходе одной из охранных зон в режим «Автоперевзятие» произойдет замыкание контакта дополнительного выхода.

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



Примечание

После включения питания все выходы нормализуются.

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

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

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

9.4.7 Шлейф сигнализации

Контроллер в вариантах конфигурации №1–3 (см. таблицу 5) имеет возможность подключения стандартных шлейфов охранной сигнализации. Использование охранных шлейфов позволяет системе безопасности контролировать не только вход в помещение, но и внутренний объем помещения, открывание окон и так далее за счет подключения дополнительных охранных датчиков. Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название шлейфа сигнализации.

Тип. Раскрывающийся список позволяет выбрать тип ШС:

- **Нет.** ШС не подключен.
- **Охранный.** Подключен охранный ШС.

Параметры		События	
Адрес		1	
Текущее наименование		Шлейф сигнализации №1	
Первоначальное наименование		Шлейф сигнализации №1	
Тип		Охранный	▼
<input type="checkbox"/> Охранный			
Контроль вскрытия корпуса извещателей		<input type="checkbox"/>	
Поддержка перезапроса		<input type="checkbox"/>	
Длительность нарушения		70 мс.	
Задержка взятия на охрану		0 мс.	
Задержка восстановления нарушенного шлейфа в снятом состоянии		0 мс.	

Контроль вскрытия корпуса извещателей. При установке флажка шлейф контролирует вскрытие корпусов извещателей.

Поддержка перезапроса. При установке флажка контроллер после срабатывания извещателей снимает питание со шлейфа и перепроверяет его состояние.

Длительность нарушения. Параметр определяет время интегрирования для шлейфа, то есть максимальное время нарушения, не приводящее к переходу в режим «Тревога».

Задержка взятия на охрану. Параметр определяет время, через которое панель предпринимает попытку взять шлейф на охрану после поступления соответствующей команды. Время, определяемое значением этого параметра, может быть использовано как «задержка на выход» для шлейфов входных зон.

Задержка восстановления нарушенного шлейфа в снятом состоянии:

- Если данный параметр установлен в **0**, то шлейф в состоянии «Снят» не контролируется.
- В противном случае продолжается отслеживание шлейфа в режиме «Снят». Если при этом шлейф перейдет в состояние «Нарушение», то в журнал также записывается событие «Неисправность снятого ОШС», состояние выходов и встроенная звуковая индикация панели не изменяются. Если после этого нормальное состояние шлейфа восстановится и **продержится время, указанное в этом параметре**, то шлейф выйдет из состояния «Нарушение» и при этом в журнал также будет записано сообщение «Нормализация снятого ОШС». Состояние выходов и встроенная звуковая индикация панели не изменяются.

9.4.8 Охранная зона

Охранная зона – это логическая структура, которая позволяет создать комбинации ресурсов контроллера, которые одновременно будут ставиться на охрану. Для настройки ресурса доступны следующие параметры:

Параметры	События
Адрес	1
Текущее наименование	Охранная зона №1
Первоначальное наименование	Охранная зона №1
Включить ИУ в зону	<input checked="" type="checkbox"/>
Повторное включение сирены	<input type="checkbox"/>
Режим работы при невзятии	Тревога
[-] Не активизировать при тревоге по Охранным шлейфам сигнализации	
Выходы, работающие по программе "Сирена" или "Лампа"	<input type="checkbox"/>
[-] Шлейфы, активизирующие зону	
Шлейф сигнализации №1	<input type="checkbox"/>

Включить ИУ в зону. При установке флажка ИУ будет включено в охранную зону. Если ИУ добавлено в зону, то при постановке на охрану контроллер будет контролировать его состояние.

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

Режим работы при невзятии. Параметр указывает действие, которое будет происходить при невозможности взятия данной зоны на охрану. Имеются следующие значения:

- **Тревога.** Зона будет переведена в режим «Тревога».
- **Автоматическое перевзятие.** Зона будет переведена в режим «Взятие», а затем будет производиться повторная попытка взятия на охрану до тех пор, пока постановка на охрану не произойдет.
- **Возврат в «Снята».** Зона перейдет в режим «Снята».

Не активизировать при тревоге по охранным шлейфам сигнализации:

- **Выходы, работающие по программе Сирена или Лампа.** При установке флажка в случае тревоги в данной зоне будет запрещена активизация дополнительных выходов, работающие по программе управления **Сирена** или **Лампа**.

Шлейфы, активизирующие зону. Параметр позволяет указать флажками шлейфы сигнализации, которые будут входить в ОЗ и состояние которых будет отслеживаться контроллером при постановке зоны на охрану.

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

Поставить на охрану/контроль. Приводит к постановке выбранной ОЗ на охрану. Если в состав выбранной охранной зоны входит ИУ, то ИУ блокируется и остается заблокированным в течение всего времени, пока режим включен. Нажатие на кнопку ДУ игнорируется. Открывание двери в режиме постановки на охрану вызывает регистрацию события о несанкционированном проходе (взломе) через ИУ и, при задании соответствующих опций, включение сигнала тревоги. Если по истечении времени выдачи сигнала тревоги дверь будет закрыта (вход PASS нормализуется), сигнал тревоги выключается. Иначе выдача сигнала тревоги продолжается до закрытия двери. Если в выбранную группу ресурсов входит шлейф охранной сигнализации, то ШС переходит в состояние «на охране». Если сопротивление ШС, устанавливаемого на охрану, не в норме, ШС переходит в состояние «невзятие» через время задержки, задаваемое при конфигурации. Для взятого на охрану ШС контроллер отслеживает сопротивление в его линии и принимает решение о его состоянии.

Снять с охраны/контроля. Происходит снятие охранной зоны с охраны. Если в состав охранной зоны входит ИУ, то контроллер переходит в режим доступа «Контроль». Если в состав ОЗ входит ШС, контроллер перестает отслеживать сопротивление в его линии.

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

9.4.9 Контроллер ИУ

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

Установить режим работы «Открыто». Приводит к разблокировке всех исполнительных устройств выбранного контроллера. Исполнительные устройства остаются разблокированными в течение всего времени, пока данный режим не будет сменен. Нажатие на кнопки ДУ исполнительных устройств игнорируются. При предъявлении карт доступа к считывателям данного контроллера регистрируются события о проходе или нарушении доступа, при этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.

Установить режим работы «Контроль». Приводит к блокировке всех исполнительных устройств выбранного контроллера. При нажатии на кнопку ПДУ для данного направления или при поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ разблокируется на время, определяемое параметром **Время удержания в разблокированном состоянии (время анализа карты)**. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии в зависимости от значения параметра, устанавливаемого в конфигурации ИУ.

Установить режим работы «Совещание». Аналогично режиму работы «Контроль», за исключением индикации на считывателях и блоке внутренней индикации. Более подробно об индикации режимов доступа изложено в техническом описании системы безопасности.

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

Открыть (разблокировать) ИУ. Приводит к разблокированию ИУ.

Закреть (заблокировать) ИУ. Приводит к блокированию ИУ.

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

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

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

9.4.10 Считыватель

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

Для настройки ресурса доступны следующие параметры:

Параметры События	
Адрес	1
Текущее наименование	Считыватель №1
Первоначальное наименование	Считыватель №1
Модель	PERCo-IRxx
<input type="checkbox"/> <u>Запрещение ДУ</u>	
в РЕЖИМЕ РАБОТЫ "Контроль"	<input type="checkbox"/>
в РЕЖИМЕ РАБОТЫ "Совещание"	<input type="checkbox"/>
<input type="checkbox"/> <u>Подтверждение от ДУ</u>	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
Время ожидания подтверждения при верификации	5 сек.
<input type="checkbox"/> <u>Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)</u>	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Охрана"	Нет
<input type="checkbox"/> <u>Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)</u>	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
<input checked="" type="checkbox"/> <u>Контроль времени для идентификаторов СОТРУДНИКОВ</u>	
<input checked="" type="checkbox"/> <u>Контроль времени для идентификаторов ПОСЕТИТЕЛЕЙ</u>	
<input type="checkbox"/> <u>Дополнительные входы, маскируемые при разблокировке ИУ</u>	
<input type="checkbox"/> Критерий маскирования	На указанное время
<input type="checkbox"/> На указанное время	
Время	0 мс.
<input type="checkbox"/> <u>Дополнительные выходы, активизируемые при разблокировке ИУ</u>	
<input type="checkbox"/> Критерий активизации	На указанное время
<input type="checkbox"/> На указанное время	
Время	0 мс.
<input type="checkbox"/> <u>Дополнительные выходы, нормализируемые при разблокировке ИУ</u>	
<input type="checkbox"/> Критерий нормализации	На указанное время
<input type="checkbox"/> На указанное время	
Время	0 мс.
<input checked="" type="checkbox"/> <u>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ</u>	
<input checked="" type="checkbox"/> <u>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ</u>	
Изымать в СТОП-ЛИСТ идентификаторы ПОСЕТИТЕЛЕЙ после прохода	<input type="checkbox"/>

Текущее наименование. Поле ввода позволяет ввести описательное название считывателя.

Запрещение ДУ. При установке флажка для выбранного режима блокируется возможность управления ИУ с помощью ПДУ контроллера в направлении данного считывателя.

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

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

предварительного прохода в обратную сторону (параметр **Защита от передачи идентификаторов** должен быть установлен на значение **Жесткая**).

Время ожидания подтверждения при верификации. Параметр позволяет установить время, в течение которого контроллер будет ожидать подтверждение от верифицирующего устройства. В качестве верифицирующего устройства может быть использовано ПДУ контроллера или картоприемник.

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

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

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

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

Дополнительные входы, маскируемые при разблокировке ИУ. Параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы (т.е. не воспринимать управляющий сигнал от внешнего оборудования) при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных входов, которые должны быть маскированы. Укажите временной критерий маскирования.

Временной Критерий маскирования:

- **На указанное время.** Выбранные дополнительные входы будут маскированы на указанное время.
- **На время срабатывания.** Выбранные дополнительные входы будут маскированы на протяжении всего времени, пока ИУ будет разблокировано.
- **На время срабатывания и после срабатывания.** Выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого ИУ будет разблокировано, плюс указанное вами время.

Дополнительные выходы, активизируемые при разблокировке ИУ. Параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Укажите временной критерий активизации.

Дополнительные выходы, нормализуемые при разблокировке ИУ. Параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализованы при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть нормализованы. Укажите временной критерий нормализации.

Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ. Параметр позволяет указать те дополнительные выходы, которые будут активизированы на указанное время в случае предъявления незаблокированного и с неистекшим сроком действия идентификатора сотрудника/посетителя. Этот параметр может быть использован в случае, если к дополнительным выходам подключена индикация, информирующая работников охраны о статусе предъявленной карты. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Укажите временной критерий активизации.

Временной Критерий активизации/нормализации:

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

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

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

Установить режим работы «Открыто». Приводит к установлению режима работы «Открыто» для ИУ, связанного с данным считывателем.

Установить режим работы «Контроль». Приводит к установлению режима работы «Контроль» для ИУ, связанного с данным считывателем.

Установить режим работы «Совещание». Приводит к установлению режима работы «Совещание» для ИУ, связанного с данным считывателем.

Установить режим работы «Закрыто». Приводит к установлению режима работы «Закрыто» для ИУ, связанного с данным считывателем.

Открыть (разблокировать) ИУ. Приводит к разблокировке ИУ, связанного с этим считывателем, на время, установленное параметром **Время разблокировки** для данного считывателя.

Закрыть (заблокировать) ИУ. Приводит к закрытию ИУ, связанного с данным считывателем.

9.4.11 ИУ (Замок/ Турникет/ Шлагбаум)

Для настройки ресурса доступны следующие параметры:

Параметры	События
Текущее наименование	Замок №1
Первоначальное наименование	Замок №1
Прямое направление прохода	<input checked="" type="checkbox"/>
Нормальное (т.е. заблокированное) состояние контакта (вход ИУ)	Нормально замкнут
Нормальное состояние "Закрыто" выхода ИУ	Не запитан
Нормализация выхода ИУ	После "Открытия"
Режим работы выхода управления ИУ	Потенциальный
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа идентификатора)	4 сек.
Время ожидания комиссионирования	15 сек.
Регистрация прохода по предъявлению идентификатора	<input type="checkbox"/>
Внутренняя защита от передачи идентификаторов (Local Antipass)	<input type="checkbox"/>

Текущее наименование. Поле ввода позволяет ввести описательное название ИУ.

Прямое направление прохода. Параметр определяет, какой из считывателей считается входным, а какой выходным.

- Если флажок установлен, то нумерация считывателей соответствует состоянию переключки «номер считывателя».
- Если флажок не установлен, то тот считыватель, который в соответствии с состоянием его переключки должен иметь номер 1, в контроллере будет опознан как считыватель номер 2, и соответственно наоборот, считыватель номер 2, в контроллере будет опознан как считыватель номер 1.

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

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

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

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

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

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

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

Время ожидания коммиссионирования/Время досмотра/Время ожидания подтверждения проезда картой водителя (сотрудника). Параметр позволяет ограничить интервал времени между предъявлением карт пользователя (сотрудника/ посетителя/ служебного ТС) и коммиссионировающей карты (сотрудника/ охранника/ водителя), в случае если в правах карты пользователя установлен доступ с коммиссионированием/ доступ с досмотром/ подтверждение проезда картой водителя.

Регистрация прохода по предъявлению идентификатора (Не доступен в конфигурациях 6, 7 «Контроллер АТП»). При установке флажка контроллер будет считать проход совершившимся сразу после поднесения идентификатора, независимо от того, будет ли реально совершен проход через ИУ.

Отсутствие датчиков проезда (Доступен только в конфигурациях 6, 7 «Контроллер АТП»). При установке флажка контроллер будет считать проезд совершившимся сразу после поднесения идентификатора, ИУ будет открыто на **Время удержания в разблокированном состоянии**.

Задержка восстановления датчиков проезда (Доступен только в конфигурациях 6, 7 «Контроллер АТП») Параметр определяет промежуток времени между моментом нормализации датчика проезда и подачей команды на закрытие ИУ. Рекомендуемое время 0,5-3 сек.

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

9.4.12 Генератор тревоги

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

Параметры	События
Текущее наименование	Генератор тревоги №1
Первоначальное наименование	Генератор тревоги №1
<input type="checkbox"/> Генерация тревоги при предъявлении идентификатора	
если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН	Нет
если ИДЕНТИФИКАТОР ЗАПРЕЩЕН	Нет
если ИДЕНТИФИКАТОР ИЗ СТОП-ЛИСТА	Нет
если ИСТЕК СРОК ДЕЙСТВИЯ	Нет
если НАРУШЕНО ВРЕМЯ	Нет
если НАРУШЕНА ЗОНАЛЬНОСТЬ	Нет
если НАРУШЕН РЕЖИМ РАБОТЫ	Нет
если НАРУШЕНО КОМИССИОНИРОВАНИЕ	Нет
<input type="checkbox"/> Генерация тревоги при несанкционированной разблокировке ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Закрыто"	Нет
<input type="checkbox"/> Генерация тревоги по недопустимо долгому открытию ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
Генерация тревоги по датчику вскрытия корпуса контроллера	Нет

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

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

Тип тревоги:

- **Нет.** Контроллер не переходит в состояние «Тревога» при выбранном событии.
- **Тихая.** Контроллер переходит в состояние «Тревога», но при этом не активизируются выходы для которого, **Тип** выбран как **Генератор тревоги**.
- **Громкая.** Контроллер переходит в состояние «Тревога».

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

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

Генерация тревоги по датчику вскрытия корпуса контроллера. Параметр, который позволяет указать, будет ли контроллер автоматически генерировать тревожное событие, если его корпус был вскрыт.

9.4.13 Порядок конфигурации охранных зон сигнализации

Подключение к контроллеру охранных ШС предусмотрено только в конфигурациях №1-3 (см. Таблицу 5).

1. Контроллер имеет два входа для подключения ШС, им соответствуют два ресурса **Шлейф сигнализации № 1** и **№ 2**. Для каждого ШС с помощью параметра **Тип** установите значение **Охранный**, если он физически подключен к входу контроллера и **Нет**, если шлейф не подключен.
2. При выборе типа **Охранный** становятся доступны параметры настройки ШС. Установите параметры для каждого подключенного ШС.
3. Для создания ОЗ с входящим в нее ИУ выберите ресурс контроллера ИУ **Охранный зона №1** или **№2** и поставьте флажок у параметра **Включить ИУ в зону**. С помощью параметра ОЗ **Шлейфы активирующие зону** отметьте флажками ШС, входящие в зону. Для создания ОЗ, включающих только ШС, используйте ресурсы контроллера **Охранный зона №11** или **№12**.
4. Настройте параметры каждой охранной зоны, в которую включены ШС или ИУ.
5. Контроллер имеет четыре выхода для подключения дополнительного оборудования, им соответствуют ресурсы контроллера **Дополнительный выход №1–4**. Для каждого ресурса с помощью параметра **Тип** укажите физически подключенные к выходам контроллера устройства, выбрав для них пункт **ОПС**. С помощью параметра **Зоны, активизирующие выход** отметьте флажками ОЗ, нарушения в которых должны активизировать выход.
6. Выберите **Программу управления** и другие параметры каждого выхода с подключенным оборудованием.



Примечание

Прежде чем передавать новые параметры в контроллер убедитесь, что все ОЗ сняты с охраны.

9.5 Функциональные возможности

9.5.1 Функция Antipass

Antipass (функция локального контроля зональности) – функция системы безопасности, заключающаяся в контроле повторного прохождения (регистрации) через одну точку прохода в том же направлении с использованием одного и того же идентификатора.

Для включения функции локального контроля зональности в разделе **«Конфигуратор»** на вкладке **Параметры** необходимо:

- Для ресурса контроллера **ИУ** установить флажок **Внутренняя защита от передачи идентификаторов (Local Antipass)**;
- Для ресурсов контроллера **Считыватель №1** и **№2** в параметрах **Защита от передачи идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ (Antipass)** для различных режимов работы контроллера с помощью раскрывающихся списков указать один из способов защиты:
 - **Мягкая**. Контроллер разрешит повторный проход по идентификатору, предъявленному к выбранному считывателю, и при этом в журнале мониторинга в ПО запишется факт предъявления карты с нарушением местоположения, а в журнале регистрации после прохода запишется событие о проходе с нарушением зональности.

- **Жесткая.** Контроллер запретит попытку повторного прохода при предъявлении идентификатора к выбранному считывателю и при этом в журнал мониторинга запишется факт предъявления карты с нарушением местоположения, а в журнал регистрации запишется событие о запрете прохода по причине нарушения зональности.

В параметрах доступа карт необходимо установить подверженность контролю локальной зональности, поставив флажок у параметра **Защита от передачи карт (Antipass)**. По умолчанию все идентификаторы, зарегистрированные в ПО, подвержены контролю локальной зональности.

9.5.2 Функция Global Antipass

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

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



Внимание!

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

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

1. Включите функцию локальной зональности (Antipass).
2. Установите флажок **Внешняя защита от передачи идентификаторов (Global Antipass)** в разделе ПО **«Конфигуратор»** на вкладке **Параметры** системы безопасности.

9.5.3 Контроль по времени

Задание критерия контроля прохода по времени доступно в расширенной версии ПО. Должен быть установлен программный модуль **PERCo-SM03 «Бюро пропусков»** и **PERCo-SM04 «Управление доступом»** с разделами ПО: **«Доступ сотрудников»**, **«Доступ посетителей»**, **«Временные зоны»**, **«Недельные графики»**, **«Скользящие посуточные графики»**, **«Скользящие понедельные графики»**.

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

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

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

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

Для включения функции контроля по времени в разделе **«Конфигуратор»**, на вкладке **Параметры** необходимо для ресурсов контроллера **Считыватель №1 и №2** в параметрах **Контроль времени для идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ** для различных режимов работы контроллера с помощью раскрывающихся списков указать один из способов защиты:

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

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



Примечание

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

9.5.4 Комиссионирование





Примечание

В вариантах конфигурации № 6, 7 «Контроллер АТП» (см. Таблицу 5) процедура комиссионирования называется **«Досмотр»**.

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

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

Для внесения карты в список имеющих право комиссионирования необходимо в разделе **«Конфигуратор»** в области **Список объектов** выбрать ресурс контроллера **Контроллер ИУ** и нажать правую кнопку мыши. В открывшемся контекстном меню выбрать пункт **Показать дополнительную информацию**. Откроется панель **Список карт сотрудников, имеющих право на комиссионирование (досмотр)**. С помощью кнопок  и  можно добавить и удалить идентификатор сотрудника из списка комиссионированных карт. Есть возможность добавить до 192 комиссионированных карт для ИУ №1 и до 64 карт для остальных ИУ.

В параметрах доступа карт требуется указать необходимость подтверждения прав данной карты с помощью комиссионирования (комиссионированной карты). Для этого в раскрываемом списке **Тип права** выберите пункт **...с комиссионированием**, например **Доступ с комиссионированием** (для АТП только – **Доступ с досмотром**).

9.5.5 Верификация и индикация

Процедуры верификации и индикации доступны в программных модулях: **PERCo-SM09 «Верификация»**, **PERCo-SM10 «Прием посетителей»**, **PERCo-SM13 «Центральный пост»**, **PERCo-SM17 «АТП»**, в разделе **«АТП: Верификация»**, а также, в **PERCo-SL02 «Локальное ПО с верификацией»**.

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



Примечание

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

Для включения функции верификации в разделе **«Конфигуратор»** на вкладке **Параметры** необходимо для ресурсов контроллера **Считыватель №1** и **№2** в параметрах **Подтверждение от ДУ** для необходимых режимов работы контроллера с помощью раскрываемых списков выбрать значение **Да** и указать отдельно для сотрудников и посетителей в каких случаях требуется верификация:

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

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

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

9.5.6 Назначение прав доступа карты

При выдаче карт сотрудникам (посетителям) в разделе **«Доступ сотрудников (посетителей)»** или служебным ТС в разделе **«АТП: Автотранспортные средства»** необходимо задать для каждого контроллера, входящего в систему безопасности права доступа выдаваемой карте.



Примечание

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

Окно настройки параметров доступа карты:

Параметры доступа	
Защита от передачи карт (Antipass)	<input checked="" type="checkbox"/>
[-] Доступ из "Неконтролируемая территория" в "КПП" (Считыватель №1)	
[-] Временной критерий	Временные зоны
Временные зоны	Всегда
[-] Тип права	Доступ с постановкой на охрану
[-] Доступ с постановкой на охрану	
Группа ресурсов	Охранная зона №1
Подверженность верификации	<input checked="" type="checkbox"/>
[-] Доступ из "КПП" в "Неконтролируемая территория" (Считыватель №2)	
[-] Временной критерий	Временные зоны
Временные зоны	Всегда
[-] Тип права	Доступ с постановкой на охрану и снятием с охраны
[-] Доступ с постановкой на охрану и снятием с охраны	
Группа ресурсов	Охранная зона №1
Подверженность верификации	<input checked="" type="checkbox"/>

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

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

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

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

Для сотрудников:

- **Только доступ**
- **Доступ с постановкой на охрану**
- **Доступ со снятием с охраны**
- **Доступ с постановкой на охрану и снятием с охраны**
- **Доступ с коммиссионированием**
- **Доступ и постановка на охрану с коммиссионированием**
- **Доступ и снятие с охраны с коммиссионированием**
- **Доступ и постановка/снятие на/с охран(у,ы) с коммиссионированием**
- **Доступ без досмотра** (доступен только для вариантов конфигурации «Контроллер АТП», см. Таблицу 5)
- **Доступ с досмотром** (доступен только для вариантов конфигурации «Контроллер АТП»)

Для посетителей:

- **Только доступ**
- **Доступ с комиссионированием**
- **Доступ без досмотра** (доступен только для вариантов конфигурации «Контроллер АТП»)
- **Доступ с досмотром** (доступен только для вариантов конфигурации «Контроллер АТП»)

Группа ресурсов (ОЗ). Раскрывающийся список появляется, если в списке **Тип права** указаны права постановки и/или снятия с охраны. С его помощью можно выбрать ОЗ, которая будет ставиться и/или сниматься с охраны по выдаваемому идентификатору.

Подверженность верификации. При установке флажка контроллер будет ожидать для данной карты подтверждение от верифицирующего устройства на считывателях, у которых включен режим верификации.

Подтверждение проезда картой водителя (сотрудника) (доступно только для вариантов конфигурации «Контроллер АТП»). При установке флажка контроллер будет ожидать предъявления идентификатора водителя ТС.

10 ОБНОВЛЕНИЕ ВСТРОЕННОГО ПО

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

Также обновление встроенного ПО и форматирование памяти возможно из Web-интерфейса контроллера (см. п. 9.2.13).

11 ЭКСПЛУАТАЦИЯ

После проведения конфигурации контроллер может работать в следующих режимах:

Без подключения к серверу системы безопасности **PERCo-S-20**. Если подключение к сети *Ethernet* и ПК также недоступно, контроллер выполняет следующие функции:

- Принимает от считывателей идентификаторы предъявленных карт и в зависимости от наличия их в списке, хранящемся в памяти контроллера, разрешает или запрещает доступ.
- Управляет подключенными ИУ.
- Ставит и снимает ОЗ с охраны; контролирует ШС и ИУ в режиме «Охрана»; активизирует дополнительные выходы в режиме «Тревога».
- Фиксирует события в журнале регистрации событий в памяти контроллера.
- Поддерживает функции локального контроля зональности, контроля прохода по времени, комиссионирования.

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

При подключении к ПК с установленным «Локальным ПО»:

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

При подключении к серверу системы **PERCo-S-20**. Кроме функций, поддерживаемых при автономной работе доступны следующие:

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

11.1 Режимы работы СКУД



Примечание

В вариантах конфигурации №1, 2 «Управление одной двухсторонней дверью» и № 6, 7 «Контроллер АТП» (см. Таблицу 5) смена режима работы производится одновременно для обоих направлений.

В вариантах конфигурации №4, 5 «Управление турникетом» режим работы задается независимо для каждого направления.

Контроллер, как элемент СКУД, обеспечивает следующие режимы работы ИУ:

Режим работы «Открыто»

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

Режим работы «Контроль»

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

Режим работы «Закрото»

- ИУ блокируется и остается заблокированным в течение всего времени, пока режим включен;
- Нажатие на кнопку пульта ДУ игнорируется.
- При предъявлении любой карты регистрируется событие о нарушении прав доступа.
- Горит красный индикатор.

Режим работы «Совещание»

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

**Примечание**

Режим доступен только для варианта конфигурации №3 «Управление двумя односторонними дверьми» и для подключенных контроллеров замка **PERCo-CL201** (см. таблицу 5).

Данный режим не поддерживается в Web-интерфейсе, однако он может быть установлен с ИК-пульта или от ПО.

Режим работы «Охрана»

- ИУ блокируется и остается заблокированным в течение всего времени, пока режим включен.
- Нажатие на кнопку пульта ДУ игнорируется.
- Установлена на охрану ОЗ, включающая выбранное ИУ.
- Проход через ИУ (взлом ИУ) переводит систему в состояние «Тревога».
- Мигают желтый и красный индикаторы.

**Примечание**

Режим доступен только для вариантов конфигураций №1-3 «Управление дверьми» и для подключенных контроллеров замка **PERCo-CL201** (см. таблицу 5).

11.2 Режим работы «Открыто»

Переход в режим работы «Открыто» возможен:

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

Выход из режима работы «Открыто» возможен:

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

Таблица 9. Реакция контроллера на предъявление идентификатора в режиме «Открыто»

Вариант конфигурации контроллера		
№ 1-3 «Контроллер управления дверьми»	№ 4, 5 «Контроллер управления турникетом»	№ 6, 7 «Контроллер АТП»
ИУ разблокировано		
Предъявление карты, имеющей право прохода		
Регистрируется событие «Проход по карте» если дверь была открыта (датчик двери активизирован) в момент предъявления карты, либо в течение Времени удержания в разблокированном состоянии после предъявления.	Регистрируется событие «Проход по карте» по факту прохода в данном направлении, в течение Времени удержания в разблокированном состоянии .	При отсутствии датчиков проезда - событие «Проход по карте» регистрируется по факту предъявления карты. При наличии датчиков проезда - событие «Проход по карте» регистрируется по факту проезда, если проезд произошел в течение Времени удержания в разблокированном состоянии с момента поднесения карты.
Регистрируется событие «Отказ от прохода», если в течение Времени удержания в разблокированном состоянии проход не произошел.		
Предъявление карты, не имеющей права прохода		
Регистрируется событие «Запрет прохода» («Идентификатор не зарегистрирован», «Карта запрещена» и т.п.).		

11.3 Режим работы «Контроль»

Переход в режим работы «Контроль» возможен:

- По команде от ПО из любого режима работы.
- По команде от Web-интерфейса из любого режима работы.
- По команде от ИК-пульта из любого режима работы, кроме режима «Охрана».

Выход из режима работы «Контроль» возможен:

- По команде от ПО в любой режим работы.
- По команде от Web-интерфейса в любой режим работы.
- По команде от ИК-пульта в любой режим работы, кроме режима «Охрана».

Таблица 10. Реакция контроллера на предъявление идентификатора в режиме «Контроль»

Вариант конфигурации контроллера		
№ 1-3 «Контроллер управления дверьми»	№ 4, 5 «Контроллер управления турникетом»	№ 6, 7 «Контроллер АТП»
Предъявление карты, имеющей право прохода или команда от ДУ		
ИУ разблокируется на Время удержания в разблокированном состоянии.		
Регистрируется событие « <i>Проход по карте</i> » если дверь была открыта (датчик двери активизирован) в момент предъявления карты. Регистрируется событие « <i>Проход по карте</i> » если дверь была открыта и поступила команда на открытие от ДУ. (При этом перезапускается отсчет Времени удержания в разблокированном состоянии.) Регистрируется событие « <i>Проход по карте</i> » если закрытая дверь была открыта в течение Времени удержания в разблокированном состоянии после предъявления карты.	Регистрируется событие « <i>Проход по карте</i> » если совершен прохода в данном направлении, в течение Времени удержания в разблокированном состоянии.	При отсутствии датчиков проезда - событие « <i>Проход по карте</i> » регистрируется по факту предъявления карты; При наличии датчиков проезда - событие « <i>Проход по карте</i> » регистрируется по факту проезда, если проезд произошел в течение Времени удержания в разблокированном состоянии с момента поднесения карты.
ИУ блокируется после нормализации датчика двери.	ИУ блокируется после совершения прохода и нормализации.	ИУ блокируется после нормализации датчика проезда, либо по истечению Времени удержания в разблокированном состоянии.
Регистрируется событие « <i>Отказ от прохода</i> », если в течение Времени удержания в разблокированном состоянии проход не произошел. ИУ блокируется.		
Предъявление карты, не имеющей права прохода		
ИУ остается в заблокированном состоянии. Регистрируется событие « <i>Запрет прохода</i> » (« <i>Идентификатор не зарегистрирован</i> », « <i>Карта запрещена</i> » и т.п.).		

**Примечание**

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

Если через турникет начат проход (ИУ не нормализовано) в направлении данного считывателя и поступила команда на открытие, то контроллер поставит данную карту в очередь и приступит к выполнению действий по ней после завершения этого прохода. Если до завершения прохода будет поднесена другая карта, то карта, находящаяся в очереди, меняется на вновь поднесенную.

В таблице 11 рассматривается реакция контроллера в случае поднесения карты в течение **Времени удержания в разблокированном состоянии** после поднесения карты, имеющей право на проход.

Таблица 11. Реакция контроллера на повторное предъявление идентификатора в режиме «Контроль»

Вариант конфигурации контроллера		
№ 1-3 «Контроллер управления дверьми»	№ 4, 5 «Контроллер управления турникетом»	№ 6, 7 «Контроллер АТП»
Предъявление имеющей право прохода карты к тому же считывателю		
Контроллер игнорирует предъявление данной карты;		
Предъявление не имеющей права карты к тому же считывателю		
Регистрируется событие о предъявлении карты с нарушениями каких-либо критериев доступа.		
Предъявление карты, имеющей право прохода к другому считывателю		
Перезапускается отсчет Времени удержания в разблокированном состоянии.	Для прохода будет открыто второе направление.	Контроллер игнорирует предъявление карты.
Предъявление карты, не имеющей права прохода к другому считывателю		
Регистрируется событие о предъявлении карты с нарушениями каких-либо критериев доступа.		

11.3.1 Процедура верификации

При поднесении к считывателю карты, не имеющей нарушений, в правах которой установлена подверженность верификации, контроллер переходит в режим *«Ожидание верификации»*. Кнопки ПДУ игнорируются.

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

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

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

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

Таблица 12. Реакция контроллера на предъявление идентификатора в режиме «Ожидание верификации»

Вариант конфигурации контроллера		
№ 1-3 «Контроллер управления дверьми»	№ 4, 5 «Контроллер управления турникетом»	№ 6, 7 «Контроллер АТП»
Предъявление любой карты к тому же считывателю		
Контроллер игнорирует предъявление карты.		
Предъявление карты, имеющей право прохода к другому считывателю		
ИУ разблокируется. Режим <i>«Ожидание верификации»</i> снимается при открытии двери. Регистрируются события <i>«Проход по карте при отказе в подтверждении прохода от верификации (с № карты ожидавшей верификации)»</i> плюс <i>«Проход»</i> по второй карте.	Для прохода будет открыто второе направление.	Контроллер игнорирует предъявление карты.
Предъявление карты, не имеющей права прохода к другому считывателю		
Регистрируется событие о предъявлении карты с нарушениями каких-либо критериев доступа.		

11.3.2 Процедура комиссионирования

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

Таблица 13. Реакция контроллера на предъявление идентификаторов в режиме «Ожидание комиссионирования»

Вариант конфигурации контроллера		
№ 1-3 «Контроллер управления дверьми»	№ 4, 5 «Контроллер управления турникетом»	№ 6, 7 «Контроллер АТП»
Предъявление любой некомиссионирующей карты к тому же считывателю		
Регистрируется событие «Предъявление карты №..., нарушение комиссионирования». Режим «Ожидание комиссионирования» снимается. Регистрируется событие «Запрет прохода №..., нарушение комиссионирования».		
Предъявление комиссионирующей карты к тому же считывателю		
ИУ разблокируется. Режим «Ожидание комиссионирования» снимается. Регистрируется событие «Проход по идентификатору (с возможными причинами)». По факту прохода добавляется событие «Была предъявлена комиссионирующая карта №...».		
Предъявление карты, имеющей право прохода к другому считывателю		
ИУ разблокируется. Режим «Ожидание комиссионирования» снимается при открытии двери. Регистрируются события: «Проход по идентификатору №..., нарушение комиссионирования» плюс «Проход» по второй карте.	Для прохода будет открыто второе направление.	Контроллер игнорирует предъявление карты.
Предъявление карты, не имеющей права прохода к другому считывателю		
Регистрируется событие о предъявлении карты с нарушениями каких-либо критериев доступа.		

11.4 Режим работы «Закрыто»

Переход в режим работы «Закрыто» возможен:

- По команде от ПО из любого режима работы.
- По команде от Web-интерфейса из любого режима работы.
- По команде ИК-пульта из любого режима работы, кроме режима «Охрана».



Примечание

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

Выход из режима работы «Закрыто» возможен:

- По команде от ПО в любой режим работы.
- По команде от Web-интерфейса в любой режим работы.
- По команде ИК-пульта в любой режим работы, кроме режима «Охрана».

Таблица 14. Реакция контроллера на предъявление идентификатора в режиме «Закрото»

Вариант конфигурации контроллера			
№ 1-3 «Контроллер управления дверьми»	№ 4, 5 «Контроллер управления турникетом»	№ 6, 7 «Контроллер АТП»	
ИУ заблокировано			
Предъявление карты			
Регистрируется событие «Запрет прохода – нарушение режима контроля доступа» («Запрет прохода, нарушение РЕЖИМОВ РАБОТЫ») Регистрируется событие «Запрет прохода» («Идентификатор не зарегистрирован», «Карта запрещена» и т.п.).			
Механическое открытие ИУ			
Регистрируется событие «Несанкционированный проход (взлом)» («Несанкционированное открытие (взлом) ИУ»)			

11.5 Режим работы «Охрана»

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

Таблица 15. Реакция контроллера на предъявление идентификаторов в режиме «Охрана»

Вариант конфигурации контроллера			
№ 1-3 «Контроллер управления дверьми»	№ 4, 5 «Контроллер управления турникетом»	№ 6, 7 «Контроллер АТП»	
ИУ заблокировано			
Предъявление карты, не имеющей прав снятия с охраны			
Регистрируется событие «Запрет прохода – нарушение режима контроля доступа» («Запрет прохода, нарушение РЕЖИМОВ РАБОТЫ») Регистрируется событие «Запрет прохода» («Идентификатор не зарегистрирован», «Карта запрещена» и т.п.).			
Предъявление карты, имеющей право снятия с охраны			
Регистрируется событие «ОЗ снята с охраны» с указанием источника команды. ИУ переходит в режим работы, который предшествовал установке режима «Охрана», если это был режим «Закрото», то в режим работы «Контроль».			
Механическое открытие ИУ			
Регистрируется событие «Несанкционированный проход (взлом)» («Несанкционированное открытие (взлом) ИУ»)			

11.5.1 Постановка ОЗ на охрану

Постановка ОЗ на охрану возможна следующими способами:

- По карте, имеющей право постановки на охрану, из любого режима работы кроме «Закрото».
- По команде от ПО из любого режима работы.

- По команде от Web-интерфейса может быть взято на охрану направление прохода через ИУ, связанное с выбранным считывателем.



Примечание

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

Для постановки на охрану с помощью карты, обладающей правом постановки на охрану, следует дважды предъявить ее считывателю, не совершая при этом прохода:

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



Примечание

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

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

При поступлении команды взятия на охрану, ОЗ переходит в режим «Взятие». Формируется соответствующее событие «Взятие ОЗ на охрану» с указанием источника команды. В этом режиме ИУ ставится на охрану, далее отсчитываются **Задержки взятия ОШС на охрану** для каждого охранного ШС, входящего в ОЗ, после чего начинается взятие ШС на охрану. Если все ИУ и ШС данной ОЗ нормализованы, то ОЗ переходит в режим «Охрана».

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

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

11.5.2 Снятие ОЗ с охраны

Снятие ОЗ с охраны возможно следующими способами:

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

Для снятия с охраны необходимо дважды предъявить одну и ту же карту с правом снятия с охраны:

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

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

В режиме ОЗ «*Снята*» осуществляется мониторинг тех ШС, входящих в ОЗ, параметр **Задержка восстановления нарушенного ОШС в режиме «Снят»** которых отличен от нуля. При нарушении такого снятого ОШС будет формироваться событие «*Неисправность снятого ОШС*». При восстановлении такого ОШС, если нормализованное состояние ОШС продержится дольше, чем установлено в параметре **Задержка восстановления нарушенного ОШС в режиме «Снят»**, будет формироваться событие «*Нормализация снятого ОШС*».

11.5.3 Переход ОЗ в режим «Тревога»

Когда ШС взят, непрерывно производится измерение значения его сопротивления с необходимым усреднением. Время интегрирования для ШС задается параметром конфигурации **Длительность нарушения** и равно 70 мс или 300 мс.

ОЗ переводится в режим «*Тревога*»:

- При нарушении любого ресурса ОЗ, находящейся на охране (ИУ либо ШС).
- При невзятии ОЗ на охрану, если для параметра ОЗ **Режим работы при невзятии** выбран вариант **Тревога**.



Примечание

Невзятие ОЗ на охрану возможно, если ИУ не нормализовано или сопротивление ШС отлично от нормы. При невзятии ОЗ на охрану через время, определенное параметром **Задержка взятия на охрану** система будет выполнять действия, определенные параметром **Режим работы при невзятии** для данной ОЗ.

При переходе в режим «*Тревога*» формируется событие «*Тревога по ОЗ*» или «*Тихая тревога по ОЗ*» (в зависимости от конфигурации ОЗ).

Реакция релейных выходов зависит от параметра конфигурации **Отключить при тревоге по ОШС выходы, работающие по программам «Сирена» и «Лампа»**.

Если этот параметр не установлен, то сформируется событие «Тревога по ОЗ» и активизируются выходы, работающие по программам «Сирена» и «Лампа».

Если этот параметр установлен, то сформируется событие «Тихая тревога по ОЗ», при этом выходы, работающие по программам «Сирена» и «Лампа» активизироваться не будут.

При нормализации всех ОШС ОЗ режим не меняет. Повторное нарушение какого-либо ОШС ОЗ приведет к повторной активизации выходов, работающих по программе «Сирена», если установлен параметр конфигурации ОЗ **Повторное включение сирены** и выход нормализован (т.е. время предыдущей активизации выхода истекло).

11.5.4 Сброс режима «Тревога»

Сброс режима «Тревога» производится из ПО сбросом тревоги по ОЗ или снятием ОЗ с охраны. По поступлении команды от ПО «Сброс тревоги» ОЗ режим не меняет, при этом индикация на лицевой панели контроллера для нарушенных ШС этой ОЗ будет отличаться от нормализованных.

11.6 Режимы ШС

Из состояния «норма» ШС может перейти в состояние «нарушение» изменив свое физическое состояние:

- КЗ.
- Вскрытие корпуса извещателя.
- Срабатывание извещателя с контролем вскрытия корпуса.
- Обрыв.

При обнаружении нарушения ШС регистрируется событие «Обнаружено нарушение ШС», если при этом физическое состояние определено как вскрытие корпуса извещателя, то дополнительно регистрируется событие «Корпус извещателя вскрыт». В состоянии «нарушение» при изменении физического состояния со «вскрытие корпуса извещателя» на «сработал извещатель с контролем вскрытия корпуса» и обратно на ПК будут регистрироваться события «Корпус извещателя вскрыт» и «Корпус извещателя закрыт».

Из состояния «нарушение» ШС может перейти в состояние «норма», нормализовав свое физическое состояние.

Таблица 16. Режимы и состояния ШС

ШС		Режимы ОЗ, причины переходов в данные режимы
Режим	Состояние	
Отключен		Если хотя бы один ШС в ОЗ отключен, то вся ОЗ не сконфигурирована.
Снят	норма	При снятии любого ШС, входящего в ОЗ, находящуюся в режимах «Взятие» или «Охрана», все остальные ШС этой ОЗ снимаются и она переходит в режим «Снята».
	нарушение	При снятии любого ШС, входящего в ОЗ, находящуюся в режимах «Взятие», «Охрана» или «Тревога», все остальные ШС этой ОЗ снимаются и ОЗ переходит в режим «Снята»

ШС		Режимы ОЗ, причины переходов в данные режимы
Режим	Состояние	
		Если при взятии любого ШС, входящего в ОЗ, находящуюся в режиме «Снята», и истечении времени Задержки взятия на охрану при как минимум одном ШС в состоянии «нарушение», опция Режим работы при невзятии установлена в Возврат в «Снята» , то ОЗ переходит в режим «Снята».
Взятие	норма	При взятии любого ШС, входящего в ОЗ, находящуюся в режиме «Снята», если значение параметра конфигурации Задержки взятия на охрану не равно нулю, то взятие ШС начинается только после истечения задержки, заданной данным параметром. На время этой задержки ОЗ находится в режиме «Взятие».
	нарушение	
Авто-перевзятие	норма	При взятии любого ШС, входящего в ОЗ, находящуюся в режиме «Снята», и истечении времени Задержки взятия на охрану при всех ШС в состоянии «норма» ОЗ переходит в режим «Охрана».
	нарушение	Если при взятии любого ШС, входящего в ОЗ, находящуюся в режиме «Снята», и истечении времени Задержки взятия на охрану при как минимум одном ШС в состоянии «нарушение», опция Режим работы при невзятии установлена в Автоматическое перевзятие , ОЗ остается в режиме «Взятие».
Охрана	норма	При взятии любого ШС, входящего в ОЗ, находящуюся в режиме «Снята», производится взятие всех остальных ШС этой ОЗ и, если они все в состоянии «норма», то эта ОЗ переходит в режим «Охрана».
		При сбросе тревоги от ПО по ОЗ, находящейся в режиме «Тревога», все ШС которой в состоянии «норма», эта ОЗ переходит в режим «Охрана» с состоянием «норма».
	При нормализации всех ШС у ОЗ, находящейся в режиме «Охрана», с состоянием «нарушение» эта ОЗ переходит в режим «Охрана» с состоянием «норма».	
	нарушение	При сбросе тревоги от ПО по ОЗ, находящейся в режиме «Тревога», с как минимум одним ШС в состоянии «нарушение» эта ОЗ переходит в режим «Охрана» с состоянием «нарушение».
Тревога	норма	При нормализации всех ШС в ОЗ, находящейся в режиме «Тревога», данная ОЗ остается в этом режиме, при этом изменяется индикация на индикаторах ШС и регистрируется событие «ШС нормализован».
	нарушение	Если при взятии любого ШС, входящего в ОЗ, находящуюся в режиме «Снята», и истечении времени Задержки взятия на охрану при как минимум одном ШС в состоянии «нарушение» опция Режим работы при невзятии установлена в «Тревога», то ОЗ переходит в режим «Тревога».
		При срабатывании как минимум одного ШС в ОЗ, находящейся в режиме «Охрана», данная ОЗ переходит в режим «Тревога».

11.7 Функционирование дополнительных выходов

Контроллер имеет 4 выхода *Out1 – Out4*. Каждый выход может быть индивидуально сконфигурирован для выполнения поставленной ему задачи.

11.7.1 Тип «Обычный»

Если тип выхода сконфигурирован как **Обычный**, то в зависимости от конфигурации ресурсов контроллера к его активизации могут привести следующие управляющие воздействия:

- Команда ПО (имеет больший приоритет относительно остальных управляющих воздействий).
- Разблокировка ИУ.
- Предъявление карт, имеющих статус посетительских.
- Предъявление карт, имеющих статус сотрудников.

Время активизации выхода определяется либо при получении команды ПО, либо в соответствии с временной характеристикой соответствующего управляющего воздействия.

Для настройки событий, приводящих к активизации выхода, необходимо отметить его в параметрах считывателя **Дополнительные выходы, активизируемые при разблокировке ИУ** или **Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ** и указать время его активизации.

При активизации выхода регистрируется событие «*Активизация выхода*».

К нормализации выхода приводят следующие управляющие воздействия:

- Команда ПО (имеет больший приоритет относительно остальных управляющих воздействий).
- Разблокировка ИУ. Для настройки событий необходимо отметить выход в параметрах считывателя **Дополнительные выходы, нормализируемые при разблокировке ИУ**.
- Окончание времени активизации.
- Выключение питания контроллера.

При нормализации выхода регистрируется событие «*Нормализация выхода*».

11.7.2 Тип «Генератора тревоги»

К активизации выхода типа генератора тревоги приводят следующие управляющие воздействия:

- Команда ПО.
- «*Тревога СКУД*». События, приводящие контроллер в состояние «*Тревога СКУД*», указываются в параметрах ресурса **Генератор тревоги**, время активизации указывается в параметрах выхода.

При активизации выхода регистрируется событие «*Активизация выхода*».

К нормализации выхода приводят следующие управляющие воздействия:

- Команда ПО (имеет больший приоритет относительно остальных управляющих воздействий).
- Окончание времени активизации.
- Выключение питания контроллера.

При нормализации выхода регистрируется событие «*Нормализация выхода*».

11.7.3 Тип «ОПС»

Любой выход, которому присвоен тип – **ОПС**, может быть сконфигурирован для работы под управлением определенной заранее заданной программы. Выбор программы определяется параметром выхода **Программа управления**, например, «ПЦН», «Лампа», «Сирена» и др. Программа управления представляет собой набор правил для изменения физического состояния выхода в зависимости от различных событий и режимов ресурсов прибора. В зависимости от программы управления выход может быть запитан (не запитан) постоянно (пока ресурс контроллера находится в текущем режиме), либо изменять свое физическое состояние (мигать) с частотой и скважностью, указанными в программе.

Конфигурация выхода может быть произведена только, когда он нормализован. После конфигурации выход готов к работе.

К активизация выхода приводят события, определяемые заданной программой и происходящие в охранных зонах, указанных в параметре выхода **Зоны, активизирующие выход**. После возникновения события, ведущего к активизации выхода, начинается отсчет задержки, длительность которой определяется параметром выхода **Задержка перед запуском**. Регистрируется событие «*Запуск задержки активизации выхода*».

По окончании отсчета выход активизируется. Время активизации определяется параметром выхода **Время активизации**. Регистрируется событие «*Активизация выхода*».

К нормализации выхода, то есть прекращению работы программы приводят следующие управляющие воздействия:

- Окончание времени активизации.
- Сброс состояния «Тревога» от ПО.
- Сброс прибора по Watchdog (если все ОЗ будут в режиме «Норма»).
- Выключение питания контроллера.

При нормализации выхода регистрируется событие «*Нормализация выхода*».

11.7.4 Выход оповещения

Выходы оповещения (Out1 и Out2) могут быть сконфигурированы как выходы **ОПС**, выходы **Генератора тревоги** или **Обычный**.

Для выходов оповещения в дополнение к вышеописанной логике работы осуществляется проверка на КЗ и обрыв. При обнаружении КЗ или обрыва на данном выходе будет регистрироваться соответствующее событие «*КЗ на выходе*» или «*Обрыв на выходе*». При устранении неисправности будет регистрироваться событие «*Восстановление выхода*». Если при возникновении управляющего воздействия на выходе определяется КЗ, то выход активизирован не будет, в этом случае будет регистрироваться событие «*Активизация выхода невозможна, причина – КЗ*».

11.8 Индикация контроллера

Индикация режимов работы, состояний и реакций контроллера на предъявление идентификаторов осуществляется на подключенных к нему выносных считывателях и блоках индикации. Возможные варианты индикации представлены в таблицах 17 и 18.

**Примечание**

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

Таблица 17. Индикация режимов работы контроллера

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

Таблица 18. Предъявление карты, имеющей право прохода и постановки/снятия ОЗ с охраны

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

Индикация состояния ШС

Индикация состояния ШС осуществляется на индикаторах «ШС1» и «ШС2» расположенные на передней панели корпуса контроллера. Возможны следующие виды индикации (см. таблицу 19).

Таблица 19. Индикация состояния ШС

Режим ШС	Состояние ШС	Цвет и режим работы светового индикатора ШС
Снят	Норма	Горит желтым.
Снят	Нарушение	Мигание желтым с частотой 2 Гц.
Взятие		Изменение цвета индикатора желтый/зеленый с частотой 2 Гц.
Автоперевзятие		Мигание зеленым с частотой 2 Гц.
Взят	Норма	Горит зеленым.
Взят	Нарушение	Горит зеленым цветом, кратковременно прерываясь красным (1,875 с / 0,125 с).
Тревога	Норма	Изменение цвета индикатора желтый/красный с частотой 2 Гц.
Тревога	Нарушение	Мигание красным с частотой 2 Гц.

12 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ

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

Хранение контроллера допускается в закрытых помещениях при температуре окружающего воздуха от -20°C до $+40^{\circ}\text{C}$ и относительной влажности воздуха до 98% при $+25^{\circ}\text{C}$.

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

13 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ

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

Работы должен производить электромонтер с квалификацией не ниже 5 разряда.

Сведения о проведении регламентных работ заносятся в журнал учета регламентных работ и контроля технического состояния средств охранно-пожарной сигнализации.

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

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

Предусматриваются следующие виды и периодичность технического обслуживания:

- плановые работы в объеме регламента №1 - один раз в три месяца;
- плановые работы в объеме регламента №2 - при поступлении с охраняемого объекта двух и более ложных тревог в течение 30 дней.

Перечни работ для регламентов приведены в таблицах 20 и 21.

Перед началом работ необходимо отключить контроллер от сети переменного тока и резервного питания.

Таблица 20. Перечень работ по регламенту №1 (технологическая карта №1)

Содержание работ	Порядок выполнения	Приборы, инструмент, оборудование, материалы	Нормы и наблюдаемые явления
1 Внешний осмотр, чистка контроллера	1.1 Отключить источник питания от сети переменного тока и удалить с поверхностей контроллера и источника питания пыль, грязь и влагу.	Ветошь, кисть флейц.	Не должно быть следов грязи и влаги.
	1.2 Снять крышки с контроллера и источника питания, при наличии резервного источника питания (аккумулятора) удалить с его поверхности пыль, грязь, влагу, окислы с клемм. Измерить напряжение резервного источника. В случае необходимости зарядить или заменить батарею.	Отвертка, ветошь, кисть флейц, прибор Ц4352.	Напряжение должно соответствовать паспортным данным на батарею (не менее 12,6 В).
	1.3 Удалить с поверхности клемм, 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 к клеммам контроллера.	Отвертка.	Должно быть соответствие схеме внешних соединений.
	1.6 Подтянуть винты на клеммах, где крепление ослабло. Восстановить соединение, если провод оборван. Заменить провод, если нарушена изоляция.	Отвертка.	Не должно быть повреждений изоляции и обрывов проводов.
2 Проверка работоспособности	2.1 Провести проверку контроллера имитацией срабатывания извещателей в соответствии с конфигурацией ресурсов.		Включение соответствующей индикации на контроллере. Формирование сигналов на релейных выходах согласно их конфигурации.

Таблица 21. Перечень работ по регламенту №2 (технологическая карта №2)

Содержание работ	Порядок выполнения	Приборы, инструмент, оборудование, материалы	Нормы и наблюдаемые явления
1 Внешний осмотр, чистка контроллера	1.1 Выполнить по 1.1 – 1.6 технологической карты №1.		
2 Измерение сопротивления изоляции	2.1 Отключить источник питания контроллера от сети и резервного источника питания		
	2.2 Соединить между собой все клеммы контроллера.		
	2.3 Измерить сопротивление изоляции между соединенными клеммами и сетевыми клеммами источника питания.	Мегомметр типа М4100/3, Е6-16, Е6-24/1, отвертка	Сопротивление должно быть не менее 20 МОм
3 Проверка работоспособности	3.1 Проверить работоспособность по разделу 11.1 в соответствии с выбранной конфигурацией.		Включение соответствующей индикации на контроллере согласно разделу 11.8. Формирование сигналов на релейных выходах согласно их конфигурации.

Вся контрольно-измерительная аппаратура должна быть поверена.

Не реже одного раза в год необходимо проводить проверку сопротивления изоляции контроллера в соответствии с таблицей 21.

Техническое обслуживание контроллеров замка **PERCo-CL201** заключается в периодической чистке корпуса контроллера и проверке качества всех подключений к кабелю, выходящему из контроллера.

Техническое обслуживание других устройств, входящих в систему, как-то: замков, турникетов, калиток, охранных извещателей, источников питания и т.п. смотри в эксплуатационной документации на данные устройства.

14 УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Перед проведением диагностики необходимо открыть крышку контроллера.

Для удобства проведения диагностики релейных выходов контроллера возле каждого реле установлены диагностические светодиоды. Факт срабатывания/отпускания реле можно определить по загоранию/гашению данных светодиодов.

Возможные варианты неисправностей:

14.1 Контроллер не работает

Причинами неисправности контроллера могут быть:

1. **Ослабление крепления клемм** кабелей в клеммных колодках платы контроллера – подтяните отверткой винты клеммных колодок.
2. **Неисправность источника питания** контроллера – проверьте источник питания.
3. **Неисправность линий подключения** к контроллеру различных устройств (считывателя, блока индикации с ИК-приемником, замка, турникета, датчика двери, кнопки ДУ, сирены и т.п.) – проверьте исправность линий подключения этих устройств.
4. **Установлены одинаковые адреса** у подключенных к контроллеру устройств – установите разные. Проверьте подключение адресных линий.
5. **Выход из строя подключенных к контроллеру устройств** – проверьте исправность устройств.
6. **Выход из строя электро-радио-элементов**, установленных на плате контроллера, – данный контроллер необходимо прислать в ремонт.

14.2 Нарушение связи с компьютером

Причинами данной неисправности могут быть:

1. **Отсутствуют сетевые настройки в компьютере** – установите IP-адрес и маску подсети компьютера. Контроллер при этом должен быть подключен либо непосредственно к сетевому разъему сетевой карты компьютера, либо к тому же Hub/Switch, в который включен компьютер.
2. **Неправильно введен пароль к данному контроллеру.** Проверьте правильность введенного в ПО пароля.
3. **Неисправности, связанные с компьютером** (с ПО, с базами данных и т.п.).

Диагностика данной неисправности заключается в запуске команды:

```
ping x.x.x.x
```

где x.x.x.x – IP-адрес данного контроллера.

Если связь есть, то вы увидите строки вида:

```
Ответ от x.x.x.x: число байт=32 время<10мс TTL=128
```

Если связи (ответа) нет, то проверьте правильность настройки маршрутизации в вашей сети.

4. **Неисправности, связанные с оборудованием сети Ethernet**, находящимся между компьютером и контроллером: концентратор (HUB), коммутатор (SWITCH) и прочее сетевое оборудование, включая кабели связи.

Диагностика данной неисправности заключается в запуске команды:

```
ping x.x.x.x -l 576
```

где x.x.x.x – IP-адрес данного контроллера.

Если связь есть и стандартные минимальные пакеты (576 байт) не фрагментируются, то вы увидите строки вида:

```
Ответ от x.x.x.x: число байт=576 время<10мс TTL=128
```

В данном случае можно утверждать, что IP-пакеты не фрагментируются до размера меньше 576 байт, и выбранное вами подключение должно работать. Если положительный ответ получить не удастся, 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)*.

Для диагностики данной неисправности обратите внимание на два индикатора, установленные в разъеме *8P8C (RJ45)* подключения к сети *Ethernet*:

- *LINK* – факт подключения:
 - зеленый горит – контроллер «видит» подключение к сети *Ethernet*,
 - зеленый не горит – контроллер «не видит» подключение к сети *Ethernet*;
- *ACT* – факт обмена данными
 - желтый мигает – контроллер «видит» обмен данными по сети *Ethernet*,
 - желтый не горит – контроллер «не видит» обмен данными по сети *Ethernet*.

Если контроллер «не видит» подключения к сети *Ethernet*, подключите его к кабелю, на котором работает другой контроллер. Если контроллер «не увидит» подключение к сети *Ethernet*, либо связь с ним не восстанавливается, то этот контроллер необходимо прислать в ремонт.

15 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Antipass	Функция системы безопасности, заключающаяся в контроле повторного прохождения (регистрации) через одну точку прохода в том же направлении с использованием одного и того же идентификатора.
Global Antipass	Функция системы безопасности, запрещающая проход через ИУ при нарушении последовательности прохождения точек прохода, с учетом направления прохода. Последовательность прохождения точек прохода определяется взаимным расположением пространственных зон с учетом их вложенности. (То есть нельзя войти в помещение, не войдя в здание.)
IP-адрес	Уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.
MAC-адрес	Уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей.
PASS	Датчик прохода через турникет. Подключается к дополнительному входу контроллера
Верификация	Процедура подтверждения прав предъявленной карты оператором с помощью комиссионированного устройства (пульта ДУ, кнопки, команды ПО) на основе сравнения изображения, получаемого с видеокамер, и данных (в том числе графических), хранящихся в базе данных программы и выводимых при предъявлении идентификатора.
Временная зона	Совокупность временных интервалов (до 4-х) в пределах календарных суток, в течение которых пользователю разрешен доступ, согласно выданных прав. Временные интервалы представляют собой отрезки времени с точностью до минуты.
Идентификатор	Это некоторое устройство или признак, по которому определяется пользователь. Каждый идентификатор характеризуется определенным уникальным кодом. В качестве идентификатора используются магнитные карты формата <i>EM-Marine</i> и <i>HID</i> .
Исполнительное устройство (ИУ)	Устройство, ограничивающее доступ (турникет, калитка, замок и т.п.).
Комиссионирование	Процедура подтверждения прав предъявленной карты посредством предъявления второй, комиссионированной карты.
Контроллер	Устройство, управляющее системой безопасности или ее элементами.
Нарушение глобальной зональности	Нарушение последовательности прохождения точек прохода, с учетом направления прохода.

Нарушение локальной зональности	Повторный проход через ИУ в том же направлении, используя один идентификатор. Нарушения входа, выхода в пределах одной пространственной зоны контроля.
Охранная зона (ОЗ)	Это логическое объединение ресурсов контроллера (<i>ИУ</i> и <i>ШС</i>), которые ставятся на охрану и снимаются с охраны как одно целое. При этом каждый ресурс может входить только в одну охранную зону.
Пространственная зона	Часть территории объекта, пересечение границ которой осуществляется только через точки прохода с предъявлением идентификатора.
Считыватель	Устройство, предназначенное для считывания кода с идентификатора, и передачи этого кода в контроллер.
Точка прохода	Место, где непосредственно осуществляется контроль (регистрация) прохода в соответствующем направлении. Точка прохода оборудуется двумя считывателями и, возможно, исполнительным устройством (замком, турникетом, калиткой и т.п.).
Форматирование памяти	Очистка журнала регистрации, списка карт, области конфигурации и режимов работы.
Электромагнитная помеха	Нежелательное воздействие электромагнитных полей, которое нарушает нормальную работу технических средств, или вызывает ухудшение технических характеристик и параметров этих средств. Источником электромагнитных помех могут являться: считыватели, линии передач переменного тока, электрогенераторы, электродвигатели реле переменного тока, тиристорные регуляторы света, мониторы компьютеров, линии передач компьютерных и телефонных сигналов.

16 ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Antipass	61, 64, 66, 93
Antipass Back	См. Antipass
FireAlarm	14, 53
Global Antipass	49, 67, 93
IP-адрес	93
Изменение	33
Способ задания	16
Local Antipass	См. Antipass
MAC-адрес	93
PASS	93
Web-интерфейс	31, 43, 51
Варианты конфигурации	6, 15, 16
Верификация	60, 61, 69, 71, 76, 93
Включение	29, 33, 42, 48
Внешняя защита от передачи идентификаторов	См. Global Antipass
Временная зона	67, 93
Время анализа карты	См. ИУ: Время удержания в разблокированном (открытом) состоянии
Выбор формата хранения идентификаторов	31, 36, 43, 49
Генератор тревоги	65
Параметры	
Генерация тревоги по датчику вскрытия корпуса контроллера	65
Генерация тревоги по недопустимо долгому открытию ИУ	65
Генерация тревоги при несанкционированной разблокировке ИУ	65
Генерация тревоги при предъявлении идентификатора	65
Добавление карт доступа	37
Дополнительный вход	51
Параметры	
Дополнительные входы, маскируемые при активизации	52
Дополнительные выходы, активизируемые при активизации	52
Дополнительные выходы, нормализируемые при активизации	53
Нормальное состояние контакта	52
Сброс сирены (Выход С ОПС)	53
Сброс тревоги (Генератор тревоги)	53
Тип Обычный	51
Тип Специальный	52
Параметры сигналов	12
Дополнительный выход	84
Параметры	
Время активизации	47, 54
Задержка перед запуском	47, 54
Нормальное состояние	46, 54
Программа управления	55
Тип Генератор тревоги	54, 84
Тип Обычный	53, 84
Тип ОПС	54, 85
Параметры сигналов	
Реакция на события	
Активизировать	55

Нормализовать	55
Досмотр	См. Комиссионирование
Журнал событий.....	40
Запрет повторного прохода.....	См. Antipass
Защита от передачи идентификаторов	См. Antipass
Идентификатор	93
Назначение прав доступа карты.....	70
Индикация	69
Индикация контроллера	85
Исполнительное устройство	См. ИУ
ИУ.....	93
Импульсный режим работы	11, 34, 44, 64, 80
Параметры	
Внутренняя защита от передачи идентификаторов	64
Время досмотра/Время ожидания подтверждения проезда картой водителя (сотрудника)	64
Время ожидания комиссионирования.....	64, 77
Время удержания в разблокированном (открытом) состоянии.....	34, 43, 64
Датчик несанкционированного прохода и сирены	44
Длительность импульса (управления ИУ)	34, 44, 64
Задержка восстановления датчиков проезда.....	64
Направление прохода	35, 44
Нормализация выхода (управления) ИУ	34, 44, 64
Нормальное состояние выхода (управления) ИУ	34, 44, 64
Нормальное состояние датчика	34
Нормальное состояние контакта	44
Отсутствие датчиков проезда.....	64
Предельное время разблокировки.....	34, 43, 64
Прямое направление прохода.....	63
Регистрация прохода по предъявлению карты/идентификатора	23, 35, 64
Режим работы выхода управления (ИУ).....	34, 44, 64
Потенциальный режим работы.....	11, 34, 44, 64
Кабели	18
Карта доступа.....	См. Идентификатор
Клеммные колодки.....	10
Комиссионирование	68, 69, 70, 77, 93
Комплект поставки	6
Контроллер.....	93
подключение	42
Контроль по времени.....	61, 67, 70
Маркировка контроллера	15
Меры безопасности	15
Монтаж	
Внешние связи	17
Контроллер.....	19
Контроллер АТП	25
Контроллер управления дверьми.....	22
Контроллер управления турникетом	23
Нарушение зональности	
глобальной	93
локальной.....	94
Обновление встроенного ПО	41, 71

ОЗ.....	79, 94
Конфигурация	44, 66
Параметры	
Включить ИУ в зону	57
Не активизировать при тревоге по охранным шлейфам сигнализации выходы, работающие по программе Сирена или Лампа.....	57
Повторное включение сирены	46, 57
Режим работы при невзятии	46, 57
Шлейфы, активизирующие зону	57
Постановка на охрану.....	79
Права постановки на охрану.....	37, 71
Реакция на события	
Поставить на охрану/контроль	58
Сбросить тревогу.....	58
Снять с охраны/контроля	58
Снятие с охраны	81
Параметры сигналов	
Выход управления ИУ	11
Выходов с контролем линии	12
Дополнительный вход	12
Дополнительный релейный выход	11
ПДУ	14
ШС.....	13
Пароль	
Изменение.....	34
Сброс.....	16
ПДУ	
Подключение.....	14, 21, 25
Передача тревожных извещений на пульт центрального наблюдения.....	11, 12, 54
Переключатель	
Установка	9, 16
Перепрограммирование.....	41, 71
Плата контроллера	9
Пространственная зона	94
Протокол считывателей	См. Выбор формата хранения идентификаторов
Режимы работы СКУД	36, 72
Закрывать.....	78
Контроль.....	74
Открыто	73
Охрана	79
Ресурсы контроллера	49
Генератор тревоги	65
Дополнительный вход	51
Дополнительный выход.....	53
ИУ.....	63
Контроллер.....	51
Контроллер ИУ	58
ОЗ	57
Считыватель	59
ШС.....	56
Сброс тревоги	37, 82
Синхронизация.....	34

Список сохраненных карт	40
Считыватель.....	94
Параметры	
Время ожидания подтверждения при верификации	61
Дополнительные входы, маскируемые при разблокировке ИУ	62
Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ.....	62
Дополнительные выходы, активизируемые при разблокировке ИУ	62
Дополнительные выходы, нормализируемые при разблокировке ИУ.....	62
Запрещение ДУ.....	60
Защита от передачи идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ.....	61
Изымать в Стоп-лист идентификаторы посетителей после прохода	63
Контроль времени для идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ.....	61, 68
Подтверждение от ДУ	60, 69
Управление от ДУ.....	36
Подключение.....	19
Реакция на события	
Закрыть (заблокировать) ИУ.....	63
Открыть (разблокировать) ИУ	63
Установить режим работы Закрыто	63
Установить режим работы Контроль.....	63
Установить режим работы Открыто	63
Установить режим работы Совещание	63
Формат идентификаторов	См. Выбор формата хранения идентификаторов
Тестирование	41
Технические характеристики.....	5
Техническое обслуживание.....	88
Точка прохода	94
Транспортирование контроллера	88
Упаковка контроллера	15
Условия эксплуатации	4
Установка времени	34
Устранение неисправностей	91
Устройство автоматической разблокировки ИУ	14
Форматирование памяти	41, 71, 94
Хранение контроллера	88
Часы.....	34
ШС	
Время интегрирования	13
Индикация	87
Параметры	
Длительность нарушения	45, 56
Задержка взятия на охрану.....	45, 56
Задержка восстановления нарушенного шлейфа в снятом состоянии.....	45, 56
Контроль вскрытия корпуса извещателей	56
Поддержка перезапроса	45, 56
Параметры сигналов	13
Режимы и состояния.....	82
Электромагнитная помеха	94

ПРИЛОЖЕНИЯ

Приложение А. Программы управления выходами

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

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

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

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

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

Таблица А.1 Программы управления выходами

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

Приложение Б. События, регистрируемые контроллером

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

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

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

1. События, связанные с доступом по коду идентификатора

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

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

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

Руководство по эксплуатации

№	Тип события	Причина	1	2	3	Примечание
26		при отказе в подтверждении прохода от верификации (без учета верификации)	-	+	+	
27		с несоответствием временным критериям доступа и при отказе в подтверждении прохода от верификации (с нарушением времени и без учета верификации)	-	+	+	
28		с несоответствием текущему местоположению и при отказе в подтверждении прохода от верификации (с нарушением зональности и без учета верификации)	-	+	+	
29		несоответствие временным критериям доступа и текущему местоположению и при отказе в подтверждении прохода от верификации (с нарушением времени, зональности и без учета верификации)	-	+	+	
30			-	+	+	
31	Проход с подтверждением от ДУ (Проход по карте с подтверждением от пульта ДУ)	с несоответствием временным критериям доступа (с нарушением времени)	-	+	+	Проход через ИУ, произошедший после предоставления контроллером с подтверждением от ДУ права пройти через него и до истечения Времени удержания в разблокированном состоянии . Подтверждение от ДУ осуществляется при условии, что верифицирующее устройство не определено и стоят соответствующие опции верификации
32		с несоответствием текущему местоположению (с нарушением зональности)	-	+	+	
33		несоответствие временным критериям доступа и текущему местоположению (с нарушением времени и зональности)	-	+	+	
34	Проход с		-	+	+	Проход через ИУ,

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

2 События, связанные с изменениями состояний ОЗ

№	Тип события	Причина	1	2	3	Примечание
1	ОЗ взята на охрану по идентификатору (карте)		+	+	-	ОЗ перешла в режим «Охрана» по карте с соответствующими правами. Если ОЗ включает в себя ИУ, то данное событие будет сопровождаться событием «Изменение режима работы на режим «Охрана» по идентификатору».
2	ОЗ снята с охраны по идентификатору (карте)		+	+	-	ОЗ перешла в режим «Снята», по предъявлению карты с соответствующими правами. Если ОЗ включает в себя ИУ, то данное событие будет сопровождаться событием «Изменение режима работы на режим «...» по идентификатору», где «...» – тот режим работы, в который будет осуществлен переход.
3	Попытка взятия ОЗ (невозможно взять) по идентификатору (ОЗ не взята на охрану по карте e)	нарушение состояния ресурса ИУ	+	+	-	ИУ в состоянии «Нарушение» при взятии ОЗ.
4		нарушение состояния ресурса ШС	+	+	-	ШС в состоянии «Нарушение» при взятии ОЗ. При этом параметр конфигурации ОЗ Работа при невзятии ОЗ установлен в значение – Возврат в «Снят».

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

№	Тип события	Причина	1	2	3	Примечание
15		несоответствие временным критериям доступа и текущему местоположению (нарушение времени и зональности)	+	+	-	Предъявленная карта с правами снятия ОЗ с охраны является нарушителем и по времени и зональности.
16		отказ от снятия	+	+	-	В процессе снятия ОЗ с охраны карта не была поднесена повторно до истечения времени удержания в разблокированном состоянии.
18	ОЗ взята на охрану по идентификатору с подтверждением	ОЗ перешла в режим ОХРАНА	+	+	-	
19	ОЗ снята с охраны по идентификатору с подтверждением	ОЗ перешла в режим СНЯТА	+	+	-	
20	ОЗ взята на охрану по команде оператора		+	+	-	ОЗ перешла в режим «Охрана» по команде оператора. Если ОЗ включает в себя ИУ, то данное событие будет сопровождаться событием «Изменение режима работы на режим «Охрана» по команде оператора».
21	ОЗ снята с охраны по команде оператора		+	+	-	ОЗ перешла в режим «Снята» по команде оператора. Если ОЗ включает в себя ИУ, то данное событие будет сопровождаться событием «Изменение режима работы на режим «...» по команде оператора», где «х» – тот режим работы, в который будет осуществлен переход.
22	Попытка взятия ОЗ (невозможно взять) по команде оператора	нарушение состояния ресурса ИУ	+	+	-	ИУ в состоянии «Нарушение» при взятии ОЗ.
23	ОЗ не взята на охрану по команде оператора	нарушение состояния ресурса ШС	+	+	-	ШС в состоянии «Нарушение» при взятии ОЗ. При этом параметр конфигурации ОЗ Работа при невзятии ОЗ установлен в значение – Возврат в «Снят» .
24	Тихая тревога по ОЗ		+	+	-	ОЗ перешла в режим «Тревога», в том числе и если параметр конфигурации ОЗ Работа при невзятии ОЗ установлен в значение – «Тревога»
25	Тревога по ОЗ		+	+	-	ОЗ перешла в режим «Тревога», в том числе и если параметр конфигурации ОЗ Работа при невзятии ОЗ установлен в значение – «Тревога»
26	Сброс тревоги по ОЗ		+	+	-	
27	Взятие ОЗ на охрану по идентификатору (Переход охранной		+	+	-	Запущена процедура взятия на охрану всех ресурсов ОЗ по карте с соответствующими правами (идет

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

3. События, связанные с изменением текущего состояния ШС, входящих в ОЗ

№	Тип события	1	2	3	Примечание
1	ОШС не взят на охрану (Шлейф сигнализации не взят на охрану)	+	+	-	ШС в состоянии «Нарушение» при взятии ОЗ. При этом параметр конфигурации ОЗ Работа при невзятии ОЗ установлен в значение — Автоматическое перевзятие . ШС перешел в режим «Автоперевзятие».
3	ИУ взят на охрану	+	+	-	ИУ перешел в режим «Охрана».
4	ОШС взят на охрану (Шлейф сигнализации взят на охрану)	+	+	-	ШС перешел в режим «Охрана».
5	Взятие ИУ на охрану (Переход ИУ в режим Взятие на охрану)	+	+	-	ИУ перешел в режим «Взятие».
6	Взятие ОШС на охрану (Переход шлейфа сигнализации в режим Взятие на охрану)	+	+	-	ШС перешел в режим «Взятие», если установлено не нулевое значение параметра Задержка взятия на Охрану .
8	ИУ снят с охраны	+	+	-	ИУ перешел в режим «Снят», в том числе и если параметр конфигурации ОЗ Работа при невзятии ОЗ установлен в значение – Возврат в «Снята» .
9	ОШС снят с охраны	+	+	-	ШС перешел в режим «Снят», в том числе и если параметр конфигурации ОЗ Работа при невзятии ОЗ установлен в значение – Возврат в «Снята» .
10	Нарушение снятого ОШС	+	+	-	Нарушение ШС в режиме «Снят», если параметр конфигурации ШС Задержка восстановления нарушенного ШС в режиме «Снят» отличен от нуля.
11	Нормализация снятого ОШС	+	+	-	Восстановление ранее нарушенного ШС в режиме «Снят», если параметр конфигурации ОШС Задержка восстановления нарушенного ШС в режиме «Снят» отличен от нуля.
13	Нарушение ИУ, режим ТРЕВОГА	+	+	-	ИУ перешел в режим «Тревога».
14	Нарушение ОШС, режим ТРЕВОГА	+	+	-	ШС перешел в режим «Тревога», в том числе и если параметр конфигурации ОЗ Работа при невзятии ОЗ установлен в значение – Тревога .
15	Нарушение ОШС, режим ТРЕВОГА с опцией тихая (Переход шлейфа сигнализации в режим Тихая тревога)	+	+	-	ШС перешел в режим ТРЕВОГА, в том числе и если параметр конфигурации ОЗ Работа при невзятии ОЗ установлен в значение – «Тревога».
16	Нарушение ОШС в режиме ТРЕВОГА	+	+	-	Повторное нарушение ШС в режиме «Тревога».

№	Тип события	1	2	3	Примечание
19	Восстановление ОШС в режиме ТРЕВОГА	+	+	-	Восстановление ранее нарушенного ШС в режиме «Тревога».
21	Сброс тревоги ИУ	+	+	-	При снятии ОЗ с охраны или командой «Снять тревогу» от ПО.
22	Сброс тревоги ОШС	+	+	-	При снятии ОЗ с охраны или командой «Снять тревогу» от ПО.
23	ОШС отключен	+	+	-	При удалении конфигурации ШС.
24	Корпус извещателя вскрыт	+	+	-	
25	Корпус извещателя закрыт	+	+	-	

4. События, связанные с состояниями входов и выходов

№	Тип события	1	2	3	Примечание
1	Активизация входа	+	+	-	
2	Нормализация входа	+	+	-	
3	Активизация выхода	+	+	-	
4	Нормализация выхода	+	+	-	
5	Запуск задержки активизации выхода	+	+	-	Начат отсчет задержки перед запуском программы управления выходом.
6	КЗ на выходе (Короткое замыкание на выходе)	+	+	-	Обнаружено КЗ в шлейфе, подключенном к выходу оповещения. (Только для выходов с контролем состояния.)
7	Обрыв на выходе	+	+	-	Обнаружен обрыв в шлейфе, подключенном к выходу оповещения. (Только для выходов с контролем состояния.)
8	Активизация выхода невозможна, причина – КЗ (Активизация выхода невозможна, короткое замыкание)	+	+	-	При активизации выхода оповещения обнаружено КЗ в подключенном к нему шлейфе. (Только для выходов с контролем состояния.)
9	Восстановление выхода (Восстановление работоспособности выхода)	+	+	-	Обнаружено восстановление шлейфа, подключенного к выходу оповещения после КЗ или обрыва. (Только для выходов с контролем состояния.)

5. События, связанные с проходами через ИУ без идентификаторов

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

№	Тип события	1	2	3	Примечание
					разблокировки.
6.	ИУ разблокирован	+	-	-	Изменение текущего состояния контакта ИУ.
7	ИУ заблокирован	+	-	-	
8	Проход по команде ИК-пульта	-	+	+	Проход через ИУ, произошедший после предоставления контроллером по команде от ИК-пульта права пройти через него и до истечения времени удержания в разблокированном состоянии.

6. События связанные с функционированием

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

№	Тип события	Причина	1	2	3	Примечание
14		часы RTC	+	+	+	
15		шина I2C	+	+	+	
16	Форматирование памяти	журнал событий	-	+		Форматирование памяти контроллера – очистка журнала регистрации, списка карт, области конфигурации и режимов работы.
17		список карт	-	+		
18		конфигурация	-	+		
19		прошивка	-	+	+	
20		текущие установки (режимы работы и т.д.)	-	+		
21	Корпус контроллера открыт		+	+	-	
22	Корпус контроллера закрыт		+	+	-	
23	Изменение режима работы по команде оператора (Установка режима «...» по команде оператора)	режим «Открыто»	+	+	+	Изменение любого режима работы на любой другой режим работы по команде ПО или Web-интерфейса.
24		режим «Контроль»	+	+	+	
25		режим «Совещание»	+	+	-	
26		режим «Закрыто»	+	+	+	
27		режим «Охрана»	+	+	+	
28	Изменение режима работы по команде ИК-пульта (Установка режима «...» по команде от ИК-пульта)	режим «Открыто»	+	+	+	Изменение любого режима работы на любой другой режим работы по команде ИК-пульта.
29		режим «Контроль»	+	+	+	
30		режим «Совещание»	+	+	+	
31		режим «Закрыто»	+	+	+	
32	Тревога по команде ИК-пульта		+	+	+	Нажата кнопка «Вызов» на ИК-пульте.
33	Изменение режима работы на режим «Охрана» по идентификатору (Установка режима Охрана по карте)		+	+	+	Постановка на охрану по идентификатору.
34	Изменение режима работы «Охрана» на режим «...» по идентификатору	режим «Открыто»	+	+	+	Снятие с охраны по идентификатору, с возвратом к режиму, предшествовавшему постановке на охрану по идентификатору.
35		режим «Контроль»	+	+	+	
36		режим «Совещание»	+	+	+	
37	Неисправность ИП (Неисправность внешнего источника питания)		+	+	+	Напряжение питания более 14.7 В, или менее 10.5 В. Формируется встроенным АЦП при выходе напряжения питания за рабочий диапазон.

№	Тип события	Причина	1	2	3	Примечание
38	Восстановление ИП (Восстановление внешнего источника питания)		+	+	+	Напряжение питания находится в диапазоне 10.5 – 14.7 В. При условии, что напряжение питания в рабочем диапазоне.
39	Тревога		+	+	-	От Генератора тревоги
40	Сброс тревоги		+	+	+	По команде от ПО или Web-интерфейса
41	Автономный сброс тревоги		+	+	-	Сброс тревоги ОПС при сбросе прибора кнопкой, определенной для сброса тревоги
42	Тестирование прибора (контроллера) начато		+	+	+	Переход прибора в режим «Тестирование прибора» по команде от ПО или Web-интерфейса
43	Тестирование прибора завершено успешно (Тестирование контроллера завершено, неисправностей не выявлено)		+	+	+	Переход прибора в дежурный режим по завершению самодиагностики. Фатальных неисправностей не выявлено.
44	Тестирование прибора выявило неисправности (Тестирование контроллера завершено, выявлены неисправности)		+	+	+	Завершение самодиагностики. Выявлены фатальные неисправности.
45	Тестирование ШС начато		+	+	-	
46	Тестирование ШС завершено		+	+	-	
47	Неисправность ИП +18В (Неисправность внутреннего источника питания +18В)		+	+	+	Выход напряжения питания ШС за рабочий диапазон. Формируется встроенным АЦП при выходе напряжения питания ШС за рабочий диапазон.
48	Восстановление ИП +18В (Восстановление внутреннего источника питания +18В)		+	+	+	Напряжение питания ШС в норме. Формируется встроенным АЦП при возвращении напряжения питания ШС в рабочий диапазон.
49	Пропадание связи с контроллером 2-го уровня		+	+	+	Пропадание связи с CL201 по RS-485.
50	Восстановление связи с контроллером 2-го уровня		+	+	+	Восстановление связи с CL201 по RS-485.
51	Неисправность контроллера 2-го уровня		+	+	+	
52	Восстановление после неисправности контроллера 2-го уровня		+	+	+	

Приложение В. Инструкция по подключению через PoE-сплиттер PA1212

Описание сплиттера

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

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

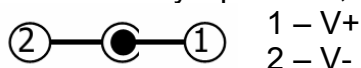
На стороне «IN»:

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

На стороне «OUT»:

Con 2 – разъем подключения кабеля *Ethernet* устройства;

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



LED – световой индикатор зеленого цвета.

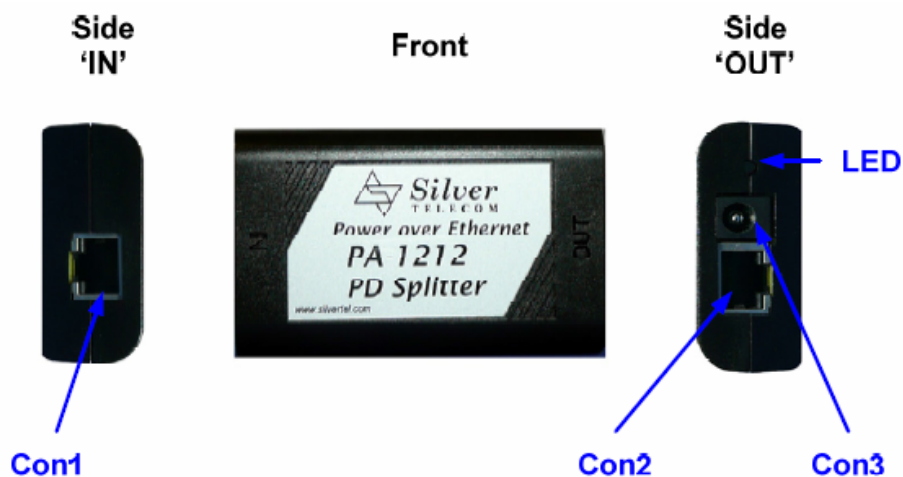


Рисунок В.1 Внешний вид сплиттера

Требования к подключаемым устройствам

Характеристики энергопотребления контроллера при подключении через сплиттер должны удовлетворять следующим требованиям:

Допустимые значения напряжения питания постоянного тока, *В*..... 12±1,2
 Минимальный суммарный ток потребления, *мА*..... не менее 120
 Максимальный суммарный ток потребления (@ 12В), *А* не более 1
 Максимальная суммарная потребляемая мощность, *Вт* не более 12



Внимание!

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

Во избежание превышения суммарной потребляемой мощности не рекомендуется подавать питание от контроллера на подключаемое дополнительное оборудование (сирену, датчики прохода и т. д.) и контроллеры второго уровня. Предусмотрено подключение к контроллеру, питаемому от сплиттера, двух считывателей и ИУ. В качестве ИУ может использоваться электромеханический замок (два, при управлении двумя односторонними дверьми) или один из турникетов указанных в таблице В.1.

Таблица В.1 Подключаемые устройства PERCo-S-20

Контроллер	ИУ	Схема подключения
PERCo-CT/L04 в вариантах конфигурации: «Контроллер управления дверьми»	Замок электромеханический	рисунок В.2
PERCo-CT/L04 в варианте конфигурации «Контроллер управления турникетом»	PERCo-T-5 PERCo-TTR-04.1 PERCo-TTD-03.1 PERCo-TTD-03.2	рисунок В.3

Порядок подключения контроллера

При подключении контроллера через сплиттер придерживайтесь следующей последовательности действий:

1. Определите место установки сплиттера. Рекомендуется устанавливать сплиттер внутри корпуса контроллера. (Не устанавливайте сплиттер на расстоянии более 2 м от контроллера).
2. Подключите кабель *Ethernet* от контроллера к разъему **Con2** сплиттера, расположенному на стороне, обозначенной как «*OUT*».
3. Подключите цепи питания контроллера и управляемого им ИУ к разъему **Con3** сплиттера, расположенному на стороне, обозначенной как «*OUT*» . Схемы подключения приведены на рисунках В.2, В.3 (штекер для подключения к разъему входит в комплект поставки сплиттера).
4. Подключите кабель *Ethernet* от *Switch* к разъему **Con1** сплиттера, расположенному на стороне обозначенной как «*IN*».
5. После верификации между *Switch* и сплиттером на подключенное устройство будет подано питание. Световой индикатор **LED** должен при этом гореть зеленым. Возможные неисправности и методы их устранения указаны в таблице В.2.



Примечание

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

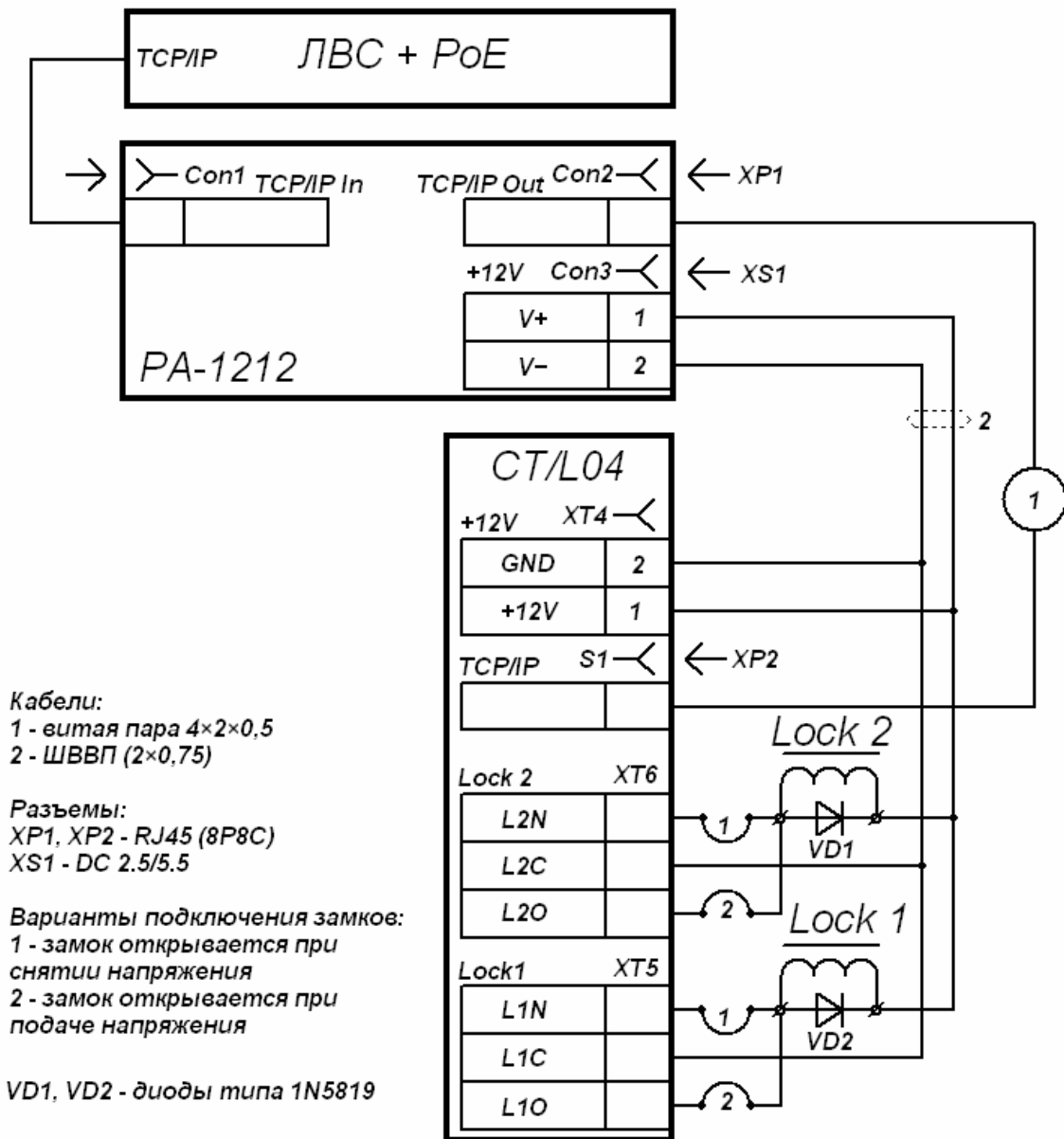


Рисунок В.2 Схема подключения контроллера в вариантах конфигурации «Контроллер управления дверьми» (Lock 1, Lock 2 – замки).



Внимание!

При подключении замков установка диодов искрозащиты **VD1, VD1** (см. рис. В.2), типа 1N5819 – **ОБЯЗАТЕЛЬНА!** Использование супрессоров вместо диодов искрозащиты – **ЗАПРЕЩЕНО!** Рекомендуется использовать только электромеханические замки.

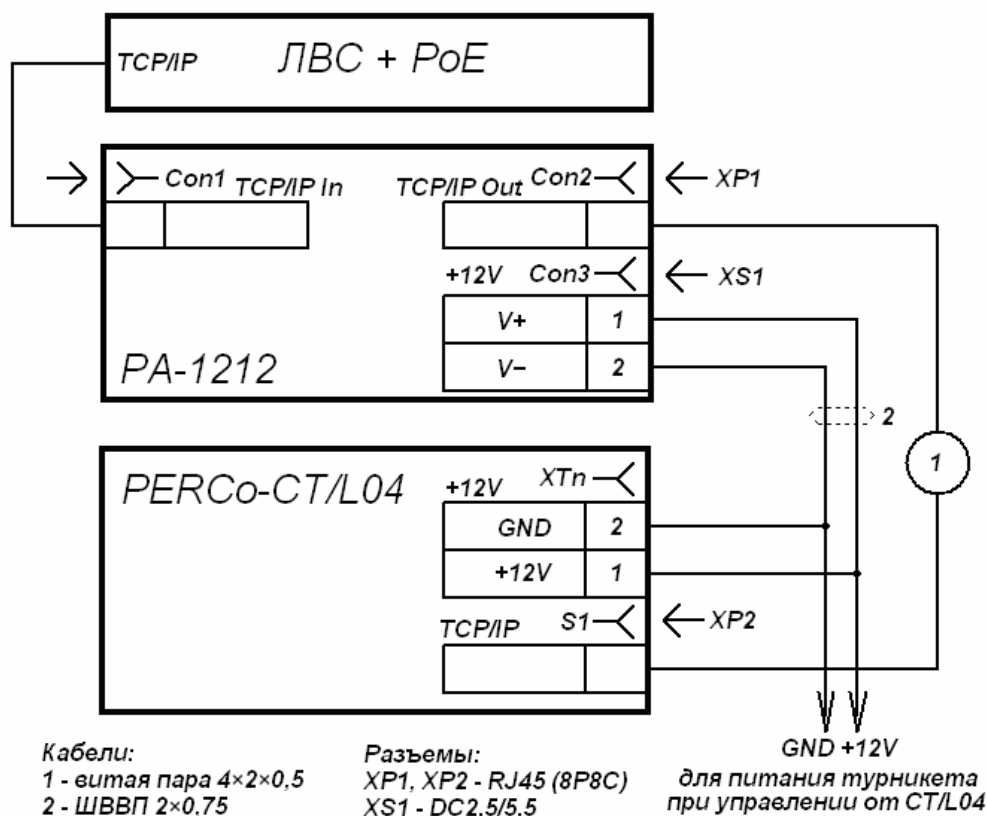


Рисунок В.3 Схема подключения контроллера в варианте конфигурации «Контроллер управление турникетом»



Примечание

Подключение питания турникета от сплиттера на рисунке В.3 производится параллельно питанию контроллера.

Индикация сплиттера и устранение неисправностей

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

Таблица В.2 Индикация сплиттера и устранение неисправностей

Индикация LED	Состояние питания контроллера	Возможная причина и порядок устранения неисправности
Индикатор горит	Питание подается.	
Индикатор не горит	Питание НЕ подается.	Проверьте кабель <i>Ethernet</i> от <i>Switch</i> и убедитесь, что <i>Switch</i> работает нормально.
Индикатор горит	Питание НЕ подается.	Проверьте кабель питания подключенного устройства.
Индикатор гаснет при подключении устройства	Питание НЕ подается.	Убедитесь, что суммарная потребляемая мощность всех подключенных устройств не превышает 12 Вт. Проверьте кабель питания подключенного устройства.
Индикатор мигает и выключается	Питание НЕ подается.	Кабель питания устройств не подключен. Проверьте кабель питания подключенного устройства.

ООО «Завод ПЭРКо»

Тел.: (812) 329-89-24, 329-89-25

Факс: (812) 292-36-08

Юридический адрес:

180600, г. Псков, ул. Леона Поземского, 123В

Техническая поддержка:

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

Тел./факс: (812) 292-36-05

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

turnstile@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

Утв. 07.02.2013

Кор. 29.11.2013

Отп. 02.12.2013



www.perco.ru

тел: 8 (800) 333-52-53