Интегрированная
система безопасности
ParsecNET 2

Автономные контроллеры SC-TP16

Паспорт и инструкция по установке

Версия 1.2

www.parsec.ru

Терминология

Далее в тексте данного документа будут использоваться слова и термины, знание которых важно для понимания принципов работы и программирования системы доступа.

Администратор	Выделенный пользователь, имеющий право изменять права других пользователей.
База данных	Специальная энергонезависимая память в контроллере, в которой хранится информация о ключах и кодах пользователей, а также их дополнительных правах.
Дверной контакт	Датчик положения двери, показывающий контроллеру, закрыта ли в настоящее время дверь в помещение. Чаще всего выполняется в виде скрыто установленного геркона.
Инженер	В данном документе человек, осуществляющий установку и настройку системы.
Ключ	Устройство для идентификации пользователя в системе. Может быть выполнен в виде пластиковой бесконтактной (proximity) карточки или брелка.
Код	Полностью называется - Персональный Идентификационный Номер, или сокращенно ПИН - код. Набирается на клавиатуре и также служит для идентификации пользователя в системе.
Охрана	Состояние системы, при котором контроллер следит за состоянием датчика двери (дверного контакта) и, если таковой подключен – дополнительного охранного датчика. Вход простым пользователям при этом запрещен, а любое срабатывание дверного контакта или охранного датчика вызывает сигнал тревоги.

Введение

SC-TP16 – это не просто контроллер совмещенный со считывателем, а автономная система управления доступом с достаточно большими возможностями. На базе SC-TP16 можно организовать доступ в помещение по proximity ключам, по ПИН-коду, а также осуществлять охрану помещения и специальные режимы доступа (режим блокировки, двухстороннего прохода, режим повышенной секретности со входом по ключу плюс коду).

Для обеспечения высокой защищенности контроллер имеет функцию цифрового управления электрозамком, что делает невозможным открывание двери даже в случае, если злоумышленник добрался до проводов управления замком (при наружной установке контроллера).

Вместе с тем, разумное сочетание заводских установок позволяет получить простую систему доступа практически без программирования контроллера, что делает запуск контроллера очень простой и быстрой процедурой.

Совмещение в одном корпусе контроллера, считывателя и схем управления делает конструкцию системы удобной и экономичной, а современный изящный дизайн позволяет устанавливать систему в любом офисе или частном доме.

С использованием контроллера SC-TP16 вы сможете не только обеспечить управление доступом в помещение в различных режимах, но и организовать охрану помещения практически без дополнительных затрат.

Основные возможности

– Полностью законченная автономная система управления доступом, требующая минимального количества внешних компонентов.
– База данных на 512 пользователей, с возможностью назначения каждому пользователю одной из четырех категорий.
– Три варианта режима доступа: только по ключу, по ключу или коду, либо по ключу и коду.
– Возможность подключения второго выносного считывателя для организации двухстороннего прохода либо для повышения стойкости к вандализму.
– Полная поддержка всех функций контроля прохода – подключение дверного контакта, кнопки запроса на выход. Контроль состояния двери.
– Использование любых типов электрически управляемых замков.
– Наличие функции охранной сигнализации с возможностью использования дополнительного охранного датчика.
– Функция блокировки для ограничения доступа в помещение.
– Возможность цифрового управления замком для повышения стойкости системы к взлому при несанкционированном доступе.

Применение

Автономная система управления доступом на базе контроллера SC-TP16 может применяться для ограничения доступа в производственные и бытовые помещения, например:

– В офисах небольших компаний с персоналом до нескольких сотен сотрудников.
– В квартирах, частных домах.
– Для ограничения доступа и охраны отдельных помещений на предприятии.

Что еще потребуется

Для того, чтобы установить у себя в офисе или доме систему доступа, кроме самого контроллера потребуется некоторое дополнительное оборудование, а именно:

– Стабилизированный источник питания с выходным напряжением 12 вольт.
– Электрически управляемый замок или защелка.
– Желательно, чтобы дверь была оборудована дверным контактом и кнопкой запроса на выход. В этом случае появляется возможность следить за состоянием двери, а также контролировать несанкционированное открывание двери.
– При использовании функций охранной сигнализации необходимо обзавестись датчиком – инфракрасным, акустическим или любым другим, имеющим выход в виде нормально замкнутых контактов.

Режимы работы

Контроллер SC-TP16 может гибко перепрограммироваться для максимальной адаптации к требованиям пользователей. Ниже рассмотрены основные особенности, обеспечивающие простоту адаптации контроллера.

Доступ в помещение

Контроллер может быть запрограммирован для доступа в помещение одним из трех способов:

– Только по ключу (карте).
– По ключу или коду. Если коды пользователям не назначены, то мы имеем дело с первым режимом. Если коды пользователям назначены, то контроллер может использоваться вообще без карт, то есть работать в качестве только клавиатурного контроллера.

– По карте и коду. Этот режим требует для доступа в помещение предъявления ключа и обязательно следующего за этим набора кода. Режим полезен тогда, когда необходимо обеспечить повышенный уровень защищенности. При этом коды для пользователей могут быть групповыми (один код для определенной категории пользователей), либо персональными, то есть, когда у каждого пользователя имеется собственный код, отличный от кодов других пользователей.

Управление замком

Контроллер поддерживает два режима управления замком:

– Стандартный режим. В этом режиме замок управляется непосредственно выходом контроллера. Недостаток режима – при наружной установке контроллера возможно снять его со стены, замкнуть выходы L+ и L-, открыв тем самым дверь.

– Режим повышенной секретности (защищенности). В этом режиме управление замком производится цифровым кодом. Для подключения замка требуется специальный дешифратор кода с выходным реле, который может поставляться в виде отдельной платы или входить в состав специализированного источника питания. Поскольку источник питания монтируется внутри защищаемого помещения, открывание двери замыканием проводов невозможно.

Кроме того, контроллер может программироваться для работы с замком отпираемым напряжением или запираемым напряжением, а также для работы с импульсным замком (с механическим перевзводом ригеля).

При использовании дверного контакта контроллер автоматически определяет, когда дверь была открыта, а затем закрыта, и, при необходимости, сокращает время работы замка, если проход был совершен достаточно быстро.

Для импульсных замков установка дверного контакта дополнительно дает возможность определять состояние, когда замок был открыт, но не сброшен в закрытое состояние ввиду того, что дверь реально не открывалась.

Контроллер с входом блокировки или охраны

Один из входов контроллера (желтый провод) может менять свое назначение в соответствии с тем, как это запрограммировал инженер при монтаже системы. По умолчанию (заводская установка) этот вход предназначен для подключения выключателя блокировки. Замыкание желтого провода на общий провод переводит контроллер в режим блокировки, когда проход пользователей без соответствующей привилегии невозможен.

В этом режиме при постановке на охрану обрабатывается в качестве источника тревоги только вход дверного контакта.

Если перепрограммировать функцию рассматриваемого входа, то мы получаем возможность подключения к контроллеру дополнительного охранного датчика (например, инфракрасного детектора движения, акустического датчика разбития стекла и так далее). В этом режиме при постановке на охрану контроллер следит за двумя входами:

– Вход дверного контакта.

– Вход датчика охраны.

Выход тревоги активируется при нарушении на любом из входов. В режиме охраны пользователи, не имеющие привилегии снятия с охраны, войти в помещение не могут.

Примечание: *В конфигурации с дополнительным охранным датчиком контроллер реализует режим блокировки, управляемый с клавиатуры.*

Контроллер с RTE или с выносным считывателем

Открывание двери изнутри возможно либо с помощью кнопки запроса на выход (RTE), либо с помощью карты (или кода) в случае установки выносного считывателя.

По умолчанию контроллер запрограммирован на работу с кнопкой запроса на выход, которая подключается между зеленым и черным (общим) проводом.

Примечание: *Без выносного считывателя дверь изнутри можно открывать также механически, но в этом случае теряется возможность следить за несанкционированным открыванием двери в рабочем режиме (когда контроллер не поставлен на охрану).*

Можно перепрограммировать контроллер с помощью кода инженера таким образом, что к зеленому проводу будет подключаться выносной считыватель. В этом случае контроллер работает в режиме, который мы будем называть режимом двухстороннего прохода.

В режиме двухстороннего прохода (при установке выносного считывателя) встроенный считыватель контроллера также работает, что позволяет открывать дверь и изнутри, например, при установке электромагнитного замка.

Если наружный считыватель (устанавливаемый с внешней стороны двери) должен работать на улице, а тем более если важна его защищенность от вандализма, то следует использовать, например, автономный контроллер SC-TP15.

Инженер и администратор

Код инженера

Новый контроллер требуется установить и запрограммировать для работы в соответствующем режиме с конкретным подключенным оборудованием. Например, установить время замка, режим внешнего считывателя, режим доступа по ключу или коду.

Программирование таких функций должен осуществлять инженер из компании-установщика или собственный технически подготовленный специалист. Для доступа к функциям конфигурирования требуется специальный код, который мы далее будем называть кодом инженера.

Примечание: *В новом контроллере код инженера отсутствует, поэтому после первого включения для продолжения работы сначала необходимо ввести код инженера. Подробнее об этом смотрите в разделе «Программирование контроллера».*

Инженер может перепрограммировать следующие параметры контроллера:

– Добавлять или изменять ключ инженера.
– Программировать конфигурацию контроллера – режимы работы, состав оборудования системы, тип замка и так далее.
– Программировать параметры контроллера – время двери, время выхода и так далее.

Код администратора

После установки и программирования режимов работы контроллера на протяжении всего срока его эксплуатации потребуется заносить и удалять пользователей в базу данных контроллера (их ключи или коды) и выполнять ряд других операций, связанных с текущим администрированием. Для доступа к функциям администрирования необходим код администратора.

Администратор может перепрограммировать следующие параметры контроллера:

– Изменять код администратора, добавлять и изменять ключ (карту) администратора.
– Переключать режимы работы контроллера – «только карта», «карта или код», «карта и код».
– Добавлять, удалять и изменять права пользователей системы.

Еще раз напомним, что в новом контроллере коды инженера и администратора отсутствуют, поэтому первое, что надо сделать после первого включения контроллера или его возврата к заводским установкам – это занести коды инженера и администратора. Эти коды должны быть уникальными.

Пользователи и их права

База данных пользователей

База данных контроллера может содержать до 512 пользователей. При этом каждому пользователю могут быть присвоены карта, PIN-код и набор привилегий.

В соответствии с наличием кода карты, PIN-кода и привилегий, а также в зависимости от запрограммированного режима работы вход в помещение может осуществляться по карте, по коду или по карте и коду (режим повышенной секретности). Набор привилегий определяет для каждого пользователя возможность ставить на охрану, снимать с охраны, а также проходить при блокировке (в зависимости от режима работы контроллера).

Любой из пользователей может быть отнесен к одной из 4-х категорий (см. таблицу ниже).

Категории пользователей

Пользователь	Проход	Проход при блокировке	Управление охраной	Управление блокировкой
Простой	+	–	–	–
Сторож	+	–	+	–
Привилегированный	+	+	–	–
Хозяин	+	+	+	+

Если контроллер запрограммирован для работы в режиме «только PIN», то пользователи по умолчанию становятся обезличенными, и пользуются при этом общими для конкретной категории PIN-кодами.

Мастер ключи

Помимо данных о пользователях, контролер может содержать в памяти коды мастер ключей, которые позволяют входить в режим программирования без набора кода.

Мастер ключи доступа в помещение не дают. В памяти контроллера может храниться один мастер ключ инженера и один мастер ключ администратора. Занесение в память контроллера мастер ключей не отменяет возможности пользования кодами инженера и администратора (см. предыдущий раздел).

Заводские установки контроллера

При производстве контроллера, а также после аппаратного сброса к заводским установкам, контроллер имеет следующую конфигурацию:

Режим замка ..... Управляемый по времени
Время замка..... 3 сек
Тип замка ..... Отпираемый напряжением, без перевзвода
Управление замком..... Прямое (без декодера)
Время открытой двери..... 30 сек
Время выхода ..... 0 секунд
Время тревоги ..... 0 секунд (по событию)
Режим входа RTE/Внешний считыватель..... По RTE (без внешнего считывателя)
Режим входа Блокировка/Охрана..... Вход блокировки
Блокировка при подборе кода (карты) ..... Включена
Режим выхода тревоги..... Нормально открытый (разомкнутый)
Контроль взлома двери не на охране ..... Включен
Тревога незакрытой двери ..... Выключена
Тревога при подборе кода..... Выключена
Мастер ключи..... Отсутствуют
Пользователи ..... Отсутствуют
Код инженера..... Отсутствует
Код администратора ..... Отсутствует
PIN простого пользователя ..... Отсутствует
PIN сторожа ..... Отсутствует
PIN привилегированного пользователя ..... Отсутствует
PIN хозяина..... Отсутствует

Установка и подключение

Общие рекомендации

– Используйте для питания контроллера только стабилизированный источник питания. Настоятельно рекомендуется использовать источник питания с резервным аккумулятором, что позволит обеспечить работоспособность системы (и возможность открывать дверь по коду или ключу) при пропаданиях сетевого питания.

– Длина всех соединений должна быть минимальной. Особенно это касается цепи управления электрозамком. При значительной длине этой цепи падение напряжения на проводах может оказаться столь большим, что замок не будет стабильно открываться.

– Если дверь выходит на улицу, предпочтительно контроллер и блок питания разместить внутри помещения, а с наружной стороны установить считыватель в антивандальном исполнении.

– Храните коды инженера и администратора в надежном месте, поскольку с их помощью можно обеспечить доступ в помещение путем перепрограммирования контроллера.

– Не теряйте коды администратора и инженера, в противном случае вам придется сбрасывать контроллер в заводские установки и полностью перепрограммировать.

– Для монтажа всех цепей, кроме питания и управления электрозамком, достаточно провода с сечением 0,22 мм^2. Для цепи питания и управления замком желательно использовать провод с сечением не менее 0,5 мм^2 (например, ШВВП 2×0,5).

– Общий провод цепи управления замком подключайте не со стороны контроллера, а со стороны блока питания.

– Обязательно шунтируйте замок варистором (входит в стандартный комплект поставки), либо обратно включенным диодом. Это снизит помехи от коммутации обмотки замка, мешающие нормальной работе контроллера.

Конструкция

Контроллер выполнен в пластиковом корпусе размером 150×46×22 мм с мембранной клавиатурой 2×6 (12 клавиш). Конструкция клавиатуры обеспечивает не менее 1 000 000 нажатий на каждую клавишу.

С обратной стороны корпуса имеется 8-жильный кабель для подключения к контроллеру оборудования системы доступа.

Внешний вид контроллера показан на обложке данного руководства.

Установка контроллера

Место размещения контроллера выбирается из соображений удобства монтажа и использования. Общепринятым является расположение контроллера на стене примерно на уровне ручки отпирания двери со стороны, противоположной дверным петлям. Схема установки контроллера приведена на рисунке 1.

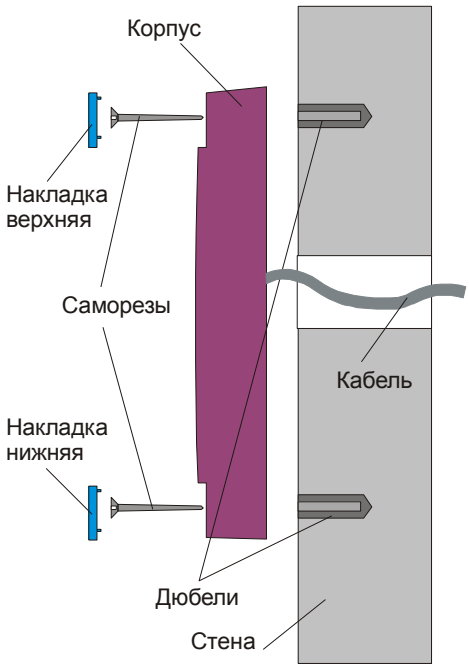


Рисунок 1. Крепление контроллера.

Для установки контроллера SC-TP16 необходимо выполнить следующее:

1. Если установлены декоративные накладки в верхней и в нижней частях корпуса контроллера, то снимите их, поддев сбоку тонкой отверткой или другим тонким плоским предметом. Нижней считается накладка с логотипом, верхней – с линзой для светодиода.
2. Просверлите в стене два крепежных отверстия под прилагаемые дюбели с расстоянием между центрами отверстий 132 мм.
3. Просверлите отверстие под кабель в стене под средней частью корпуса контроллера.
4. Подключите к контроллеру остальное оборудование (источник питания, дверной контакт, замок, кнопка запроса на выход). Подробнее о подключении оборудования к контроллеру рассказано в следующем подразделе.
5. Закрепите корпус контроллера двумя прилагаемыми саморезами.
6. Защелкните верхнюю и нижнюю накладки. При необходимости накладки можно дополнительно зафиксировать каплей нитроклея, но в этом случае демонтаж контроллера станет проблематичным.

Подключение контроллера

Внешнее оборудование подключается к контроллеру с помощью 8-жильного кабеля. Назначение выводов кабеля приведено в таблице 1.

Таблица 1

Цвет провода	Вывод	Назначение
Красный	+12	Питание контроллера +12...14 В постоянного тока
Черный	GND	Общий провод источника питания, дверного контакта и кнопки запроса на выход.
Белый	DC	Подключение нормально замкнутого дверного контакта.
Зеленый	RTE/ER	Подключение нормально разомкнутой кнопки запроса на выход или внешнего считывателя.
Коричневый	L+	Управление замком, выход ключа.
Синий	L-	Общий провод ключа управления замком
Оранжевый	ALARM	Выход тревоги.
Желтый	HLD/SNS	Вход аппаратной блокировки, либо вход внешнего охранного датчика.

Выводы RTE/ER и HLD/SNS являются многофункциональными, их назначение определяется при программировании контроллера инженером.

Заводская конфигурация

Схема подключения будет варьироваться в зависимости от конфигурации контроллера. На рисунке 2 представлена схема подключения контроллера в заводской конфигурации (см. раздел «Заводские установки контроллера»). Использование заводской конфигурации не требует программирования, за исключением занесения кодов инженера, администратора и непосредственно пользователей

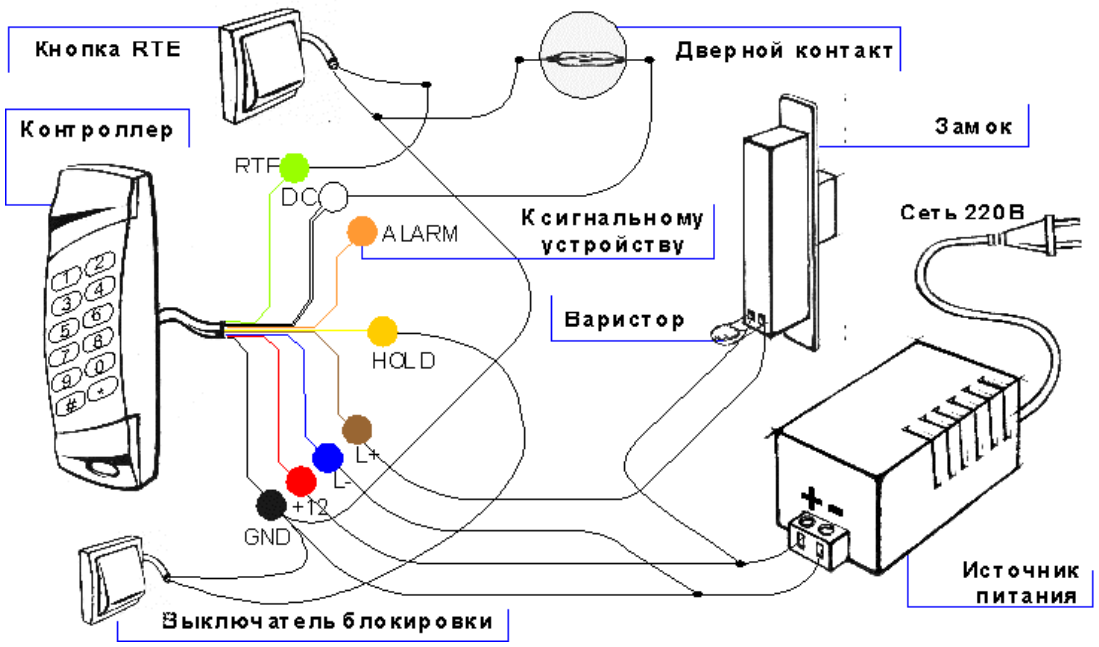


Рисунок 2. Подключение контроллера в заводской конфигурации.

В заводской конфигурации контроллер поддерживает следующее оборудование:

– Электрозамок или электрозащелка, отпираемые напряжением. Подключаются в соответствии со схемой (рисунок 2).
– Кнопка запроса на выход. Нормально разомкнутая, подключается между выводами RTE/ER и GND (соответственно зеленый и черный провода).
– Дверной контакт. Нормально замкнутый, подключается между выводами DC и GND (белый и черный провода соответственно). Если DC не используется, то выводы DC и GND необходимо замкнуть (соединить между собой).
– Выключатель блокировки. Нормально разомкнутый, подключается между выводами HLD/SNS и GND (желтый и черный провода соответственно).
– Сигнальное устройство. Подключается в соответствии со схемой (рисунок 2).

Режим с охранным датчиком

Для использования дополнительного охранного датчика, его необходимо подключить в соответствии со схемой, приведенной на рисунке 3. Если необходимо, на датчик следует подать питание от того же источника, от которого питается контроллер. Если питание датчика осуществляется от отдельного источника, то необходимо объединить земли (общий провод) обоих источников питания. Остальные элементы системы подключаются в соответствии с приведенными выше указаниями (рисунок 2).

Режим работы с дополнительным охранным датчиком необходимо включить, используя команды инженера (см. раздел «Программирование контроллера»).

При использовании охранного датчика режим аппаратной блокировки (с помощью выключателя) использовать уже нельзя, поскольку вместо него к желтому проводу кабеля подключается охранный датчик.

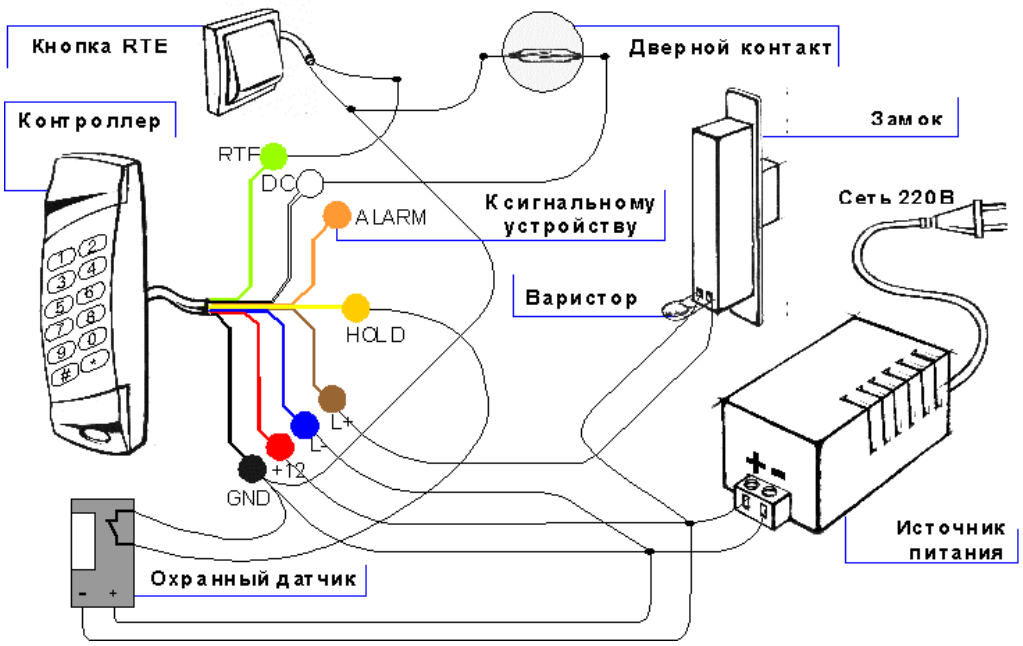


Рисунок 3. Подключение охранного датчика.

Режим с дополнительным считывателем

Допустим, вам необходимо установить с наружной стороны помещения считыватель в антивандальном исполнении, либо вы хотите осуществлять по ключу как вход в помещение, так и выход. В этом случае следует при установке системы с наружной стороны установить внешний считыватель (подключается вместо кнопки запроса на выход), а контроллер установить с внутренней стороны помещения. Схема подключения внешнего считывателя приведена на рисунке 4.

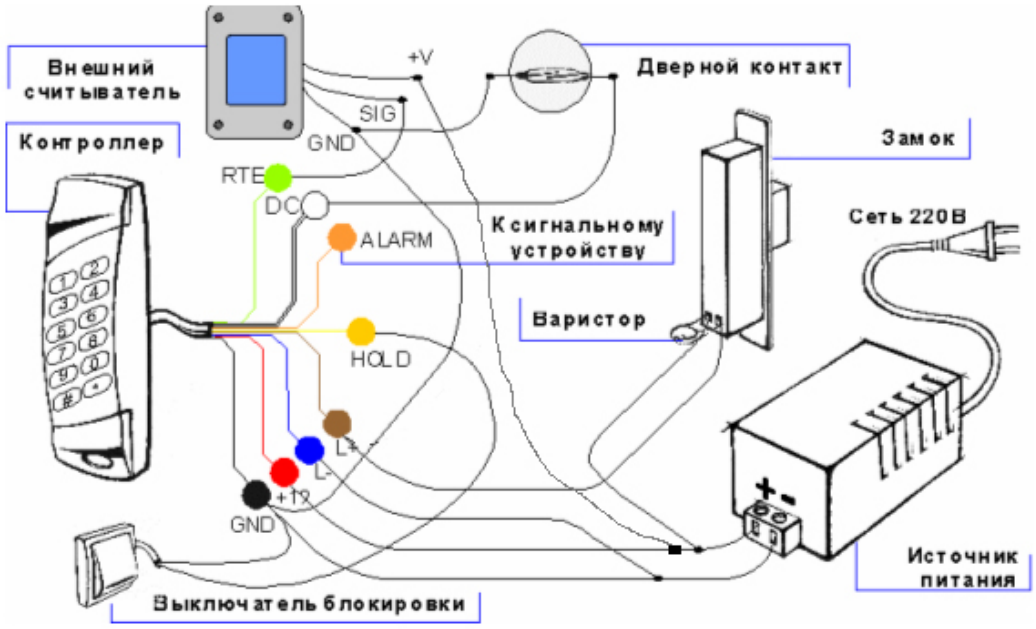


Рисунок 4. Подключение внешнего считывателя.

Режим работы с внешним считывателем необходимо включить, используя команды инженера (см. раздел «Программирование контроллера»).

В качестве внешних считывателей для организации двусторонней точки прохода могут использоваться автономные контроллеры SC-TP15, SC-TP16, SC-TP19, подключенные в режиме считывателя. Для перевода контроллеров SC-TP15 и SC-TP19 в режим считывателя соедините на них между собой Зеленый (RTE) и Коричневый (L+) выводы.

Процедуру перевода в режим считывателя контроллера SC-TP16 смотрите далее в таблицах программирования.

Цифровое управление замком и сигнальным устройством

Если необходимо обеспечить надежную защиту помещения при внешней установке контроллера, то можно использовать цифровое управление замком и сигнальным устройством. В этом случае, даже если оторвать контроллер от стены и подать питание на провода управления замком, дверь не откроется, потому что для открывания замка необходим специальный код, формируемый контроллером.

Замок и сигнальное устройство при такой конфигурации подключаются через специальный дешифратор (LD-01), расположенный в защищенном месте. Смысл всего сказанного выше поясняется рисунком 5.

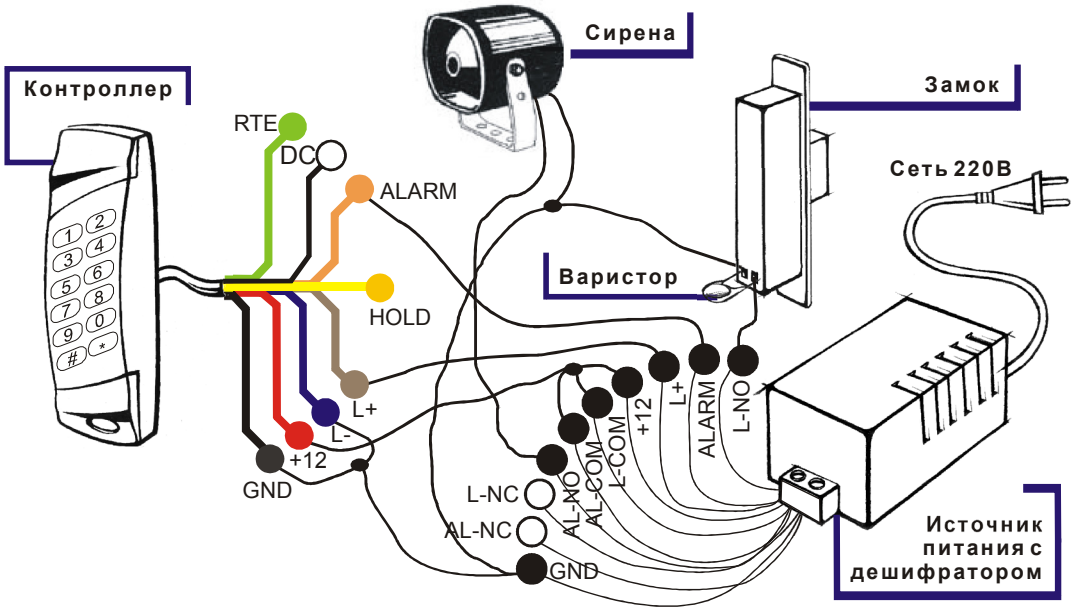


Рисунок 5. Управление замком и сиреной через дешифратор.

Если вам даже необходимо управлять только замком (не требуется управление сигнальным устройством), все равно необходимо соединить с дешифратором оба выхода контроллера – и коричневый, и оранжевый провода.

При использовании дешифратора контроллер необходимо включить в режим цифрового управления замком и сигнальным устройством, используя команды инженера (см. раздел «Программирование контроллера»).

Еще раз обратите внимание на точки подключения проводов замка к линиям питания, а также на необходимость шунтирования замка варистором.

Программирование контроллера

Общие положения

С помощью кода инженера можно менять конфигурацию контроллера и режимы его работы, например, время замка, наличие дополнительного охранного датчика и так далее.

Код администратора дает возможность добавления, удаления и редактирования прав доступа и PIN-кодов пользователей.

Ряд команд может вводить пользователь, имеющий соответствующие привилегии. Это команды постановки на охрану, включения и выключения режима блокировки.

Вход в режим программирования возможен только из дежурного режима. При включенном режиме блокировки или охраны перепрограммирование контроллера или изменение базы данных пользователей невозможно.

Индикация при программировании

Процесс программирования сопровождается звуковой и световой индикацией.

Нажатие каждой клавиши сопровождается коротким звуковым сигналом (бипом).

После набора каждого элемента (кода установщика, кода функции, значения) необходимо нажать «**#**». После анализа введенного значения, корректно введенная команда подтверждается длинным звуковым сигналом (бипом). При вводе некорректной команды контроллер подает три коротких «бипа».

После поднесения мастер карты, заменяющей код инженера или администратора, нажимать «**#**» не нужно.

Три коротких звуковых сигнала (три коротких «бипа») – признак ошибки. Другие варианты индикации рассмотрены в соответствующих разделах. Для проверки корректности своих действий следите также за светодиодным индикатором.

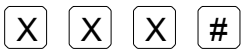
Условные обозначения

При описании процедур программирования для большей наглядности используются следующие обозначения:

Обозначение	Смысл обозначения
	Непрерывно горящий светодиод соответствующего цвета.
	Мигающий светодиод соответствующего цвета.

Нажатие клавиши обозначается квадратом с наименованием клавиши внутри, например, нажатие клавиши «**5**» будет выглядеть так:

а набор произвольной комбинации из трех цифр и «**#**» обозначается следующим образом:



«Бипы» обозначаются следующим образом:

Обозначение	Смысл обозначения
	Короткий «бип» длительностью 50мс.
	Длинный «бип» длительностью 500мс.

Если в процессе программирования необходимо поднести карту (ключ), то это обозначается следующим образом:

Обозначение	Смысл обозначения
	Предъявление карты инженера.
	Предъявление карты администратора.
	Предъявление карты пользователя.

«Бипы», сопровождающие нажатие клавиш, для наглядности мнемоники команд не показываются.

Начальная авторизация

Новый контроллер не содержит в памяти кодов инженера и администратора, поэтому до того, как производить программирование нового контроллера, следует ввести код инженера.

Затем следует занести код администратора для обеспечения возможности работы с базой данных пользователей (добавление, удаление и изменение прав пользователей).

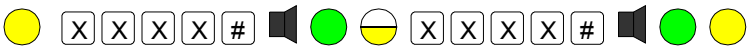
Первоначально код администратора вводит инженер. После того, как код администратора введен, он может быть изменен только с использованием кода администратора. Это сделано для того, чтобы можно было разделить функции конфигурирования системы и управления правами персонала между установщиком (он может быть из другой компании) и человеком, отвечающим за права доступа в помещение – это, как правило, сотрудник компании, которая эксплуатирует контроллер.

Создание кода инженера

При первом включении, когда в контроллере нет кода инженера, индикатор светится желтым цветом и контроллер с интервалом в три секунды издает длинные «бип»-ы. Контроллер будет находиться в этом состоянии до тех пор, пока не будет введен код инженера. В такое же состояние контроллер переходит после принудительного возврата к заводским установкам.

Коды инженера и администратора при вводе повторяются по два разу с целью исключить ошибку ввода, поскольку при ошибочном вводе будет потерян доступ к контроллеру и придется сбрасывать его снова в заводские установки.

Начальное занесение кода инженера производится следующим образом:



новый код новый код

Длина кода инженера может быть от 4-х до 8 цифр. Если код введен неправильно, контроллер издаст три коротких «бип»-а и вернется в начало процедуры.

Если код инженера введен корректно, то контроллер переходит в режим инженера, в котором можно сразу перейти к занесению кода администратора.

Если заносить код администратора планируется позже, то для выхода в дежурный режим необходимо нажать три раза на клавишу «**0**», после чего «**#**», либо подождать 15 секунд. Дежурный режим индицируется горящим красным светодиодом.

В качестве кода инженера нельзя использовать сочетание «9999», поскольку это является зарезервированной комбинацией.

Создание кода администратора

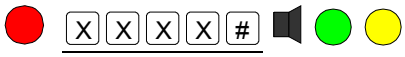
Код администратора можно заносить сразу после занесения кода инженера (см. предыдущий подраздел), либо из дежурного режима.

Примечание: *Первый раз код администратора заносится с использованием кода инженера. В дальнейшем для получения доступа к изменению кода администратора необходим только старый код администратора - код инженера для данной процедуры будет уже недействительным.*

Из режима инженера код администратора заносится следующим образом:

команда новый код новый код

Из дежурного режима занесение кода администратора производится следующим образом. Необходимо ввести код инженера, нажать «**#**»:



код инженера

а затем ввести описанную выше последовательность:

команда новый код новый код

Контроллер после этого находится в режиме инженера, из которого выйдет автоматически через 15 секунд либо после набора комбинации:

Примечание: *Приведенная выше комбинация является универсальным способом выхода в дежурный режим из любого места любой процедуры программирования.*

Код администратора не может совпадать с кодом инженера. Контроллер не позволит ввести совпадающие коды.

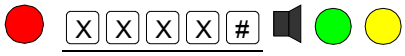
Изменение кодов доступа

В некоторых случаях бывает необходимо поменять коды инженера или администратора. Ниже описаны соответствующие процедуры.

Кроме того, код инженера и администратора может быть дополнен картой (ключом), что упрощает вход в режим программирования. Если у вас есть ключ инженера, то для перехода в режим программирования нет необходимости вводить код и «решетку» – простое поднесение карты к считывателю контроллера заменяет эту последовательность действий.

Изменение кода инженера

Для изменения кода инженера необходимо знать старый код. Изменение производится следующим образом. Сначала переходим в режим инженера:



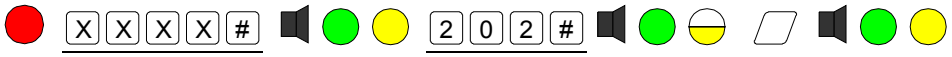
старый код инженера

либо поднесением карты инженера (если она ранее была занесена в память контроллера), а затем вводим команду смены кода инженера:

команда новый код новый код

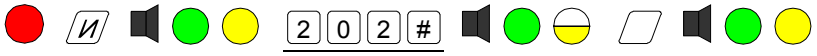
Добавление/изменение карты инженера

Добавление или изменение карты (ключа) инженера производится одинаково. Для входа в режим может использоваться как код инженера, так и его карта (только при изменении, если есть уже занесенная карта). С использованием кода процедура добавления/изменения выглядит следующим образом:



код инженера команда карта

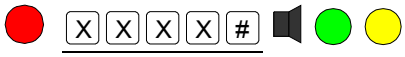
Или с использованием ранее занесенной карты инженера:



старая карта команда новая карта

Изменение кода администратора

Для изменения кода администратора необходимо знать его старый код. Изменение производится следующим образом. Сначала переходим в режим администратора:



старый код администратора

либо поднесением карты администратора (если она ранее была занесена в память контроллера), а затем вводим команду смены кода администратора:

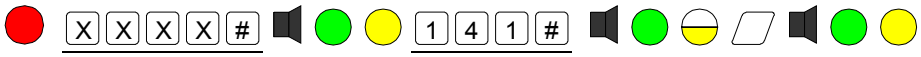
команда — новый код — новый код

Добавление/изменение карты администратора

Добавление или изменение карты (ключа) администратора производится одинаково. Для входа в режим может использоваться как код администратора, так и его карта (только при изменении, если есть уже занесенная карта).

Карты инженера и администратора должны быть разными – контроллер не позволит занести дважды одну и ту же карту с разными функциями. По этой же причине карты пользователя не могут быть картами инженера или администратора.

С использованием кода процедура добавления/изменения выглядит следующим образом:



код администратора — команда — карта

или с использованием ранее занесенной карты администратора:

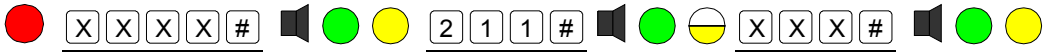
старая карта — команда — новая карта

Конфигурирование контроллера (команды инженера)

Конфигурирование контроллера производится с помощью кода или карты инженера и позволяет задать конфигурацию подключенного оборудования и временные параметры.

Установка времени замка

Время замка может быть установлено в диапазоне от 0 до 255 секунд, при этом «0» соответствует 256 секундам. Установка времени замка производится следующим образом:



код инженера — команда — время замка

или при помощи карты инженера:

карта инженера — команда — время замка

Примечание: *При вводе малых значений ведущие нули не требуются. Контроллер не позволит ввести значение больше 255 секунд. Значение по умолчанию (заводская конфигурация) составляет 3 секунды.*

Назначение типа замка

Контроллер может управлять различными типами замков: отпираемых напряжением или запираемых напряжением. Кроме того, можно настроить контроллер на работу с замком с механическим перевзводом ригеля.

Примечание: *По умолчанию контроллер настроен на работу с замком, отпираемым напряжением без перевзвода ригеля.*

Назначение типа замка производится командами инженера. Вход в режим инженера производится набором на клавиатуре кода инженера, завершаемого нажатием клавиши «**#**»:

код инженера

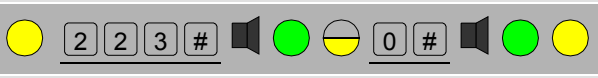
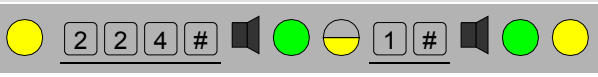
либо поднесением карты инженера (если она была предварительно занесена):

карта инженера

После перехода в инженерный режим светодиод светится желтым цветом. Вы можете последовательно выполнять требуемые команды для программирования параметров контроллера. Для возврата в дежурный режим необходимо набрать на клавиатуре

или подождать 15 секунд, по истечении которых контроллер автоматически перейдет в дежурный режим.

Команды назначения типа замка приведены в таблице ниже. Еще раз напомним, что они вводятся из инженерного режима.

Тип замка	Команда
Замок, отпираемый напряжением	
Замок, запираемый напряжением	
Замок с перевзводом ригеля	
Замок без перевзвода ригеля	

Триггерный режим замка

Выход управления замком можно переключить для работы в триггерном режиме, при котором каждое предъявление карты пользователя (или набор PIN-кода) переключает замок в противоположное состояние. Такой режим можно использовать, например, для управления охранной панелью. По умолчанию триггерный режим выключен. В таблице ниже приведены команды для включения и выключения триггерного режима.

Триггерный режим	Команда
Включить	
Выключить	

Цифровое управление замком

В контроллере предусмотрены два режима управления замком: обычный и цифровой. При обычном режиме (заводская установка) замок подключается непосредственно к выходам контроллера.

Примечание: *При использовании цифрового управления замок подключается через специальную плату дешифратора, которая может быть размещена, например, в корпусе источника питания.*

Схема подключения замка через плату дешифратора приведена выше, на рисунке 5. Режим управления замком переключается следующими командами инженера:

Цифровое управление замком	Команда
Включить	
Выключить	

Режим цифрового управления замком повышает стойкость системы против взлома, поскольку, даже если снять контроллер со стены для доступа к проводам управления замком, открыть его все равно будет невозможно.

Одновременно с переключением режима управления замком переключается и режим работы выхода тревоги. При цифровом управлении замком сигнальное устройство для индикации тревоги также необходимо будет подключать к выходу платы дешифратора.

Программирование функции входа RTE/ER

Ко входу RTE можно подключить нормально разомкнутую кнопу запроса на выход (RTE) для открывания двери изнутри, либо второй считыватель. В последнем случае контроллер можно разместить с внутренней стороны двери, в более защищенном месте, а снаружи смонтировать антивандальный считыватель. Соответствующие схемы включения контроллера приведены на рисунках 2 и 4.

Программирование функции входа из инженерного режима производится следующими командами:

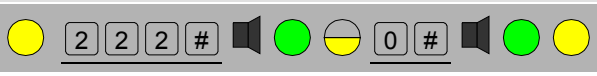
Функция входа RTE/ER	Команда
Кнопка RTE	
Внешний считыватель	

Примечание: *Внешний считыватель позволяет только открывать дверь, ставить систему на охрану и снимать с охраны. Программирование контроллера с внешнего считывателя невозможно.*

Программирование входа HLD/SNS

Вход HLD/SNS может использоваться либо для подключения нормально разомкнутого выключателя блокировки (рисунок 2), либо для подключения дополнительного охранного датчика (рисунок 3).

Переключение функции входа HLD/SNS производится из инженерного режима следующими командами:

Функция входа HLD/SNS	Команда
Вход выключателя блокировки	
Вход охранного датчика	

Защита от подбора кода

Контроллер имеет функцию защиты от подбора кода или карты. Работает она следующим образом: после ввода на одном считывателе 8 различных неправильных PIN-кодов или предъявления 8-ми разных незанесенных в базу данных карт контроллер на 1 минуту блокирует работу этого считывателя.

Тем самым процесс подбора кода или карты замедляется в десятки раз, делая подбор практически невозможным.

Примечание: *Дополнительно можно включить сигнал тревоги на подбор кода, о чем будет сказано в следующем подразделе.*

Включение и выключение режима защиты от подбора кода производится в режиме инженера следующими командами:

Защита от подбора кода	Команда
Включить	
Выключить	

Конфигурация выхода тревоги

Выход тревоги может работать в режиме нормально разомкнутого или нормально замкнутого контакта. В первом случае при возникновении сигнала тревоги выход замыкается на общий провод. Во втором случае в нормальном состоянии выход замкнут на общий провод, а при возникновении тревоги размыкается.

Тревога может подаваться в различных ситуациях. Так, при активировании охранного датчика в режиме охраны сигнал тревоги включается всегда. По другим событиям тревога может либо включаться, либо не включаться.

Команды конфигурирования выхода тревоги из инженерного режима приведены ниже:

Выход тревоги	Команда
Нормально разомкнутый	2 3 1 # 1 #
Нормально замкнутый	2 3 1 # 0 #
Не включать тревогу при взломе не на охране	2 3 2 # 1 #
Включать тревогу при взломе не на охране	2 3 2 # 0 #
Не включать тревогу при незакрытой двери	2 3 3 # 1 #
Выключать тревогу при незакрытой двери	2 3 3 # 0 #
Не включать тревогу при подборе кода	2 3 4 # 1 #
Включать тревогу при подборе кода	2 3 4 # 0 #

Установка времени открытой двери

Время открытой двери – это время, начинающееся после окончания времени замка. Если по истечении времени открытой двери она останется открытой, то контроллер начнет издавать звуковой сигнал. Это сигнал можно выключить двумя способами:

– Закрыв дверь.

– Поднесением ключа, имеющегося в базе данных.

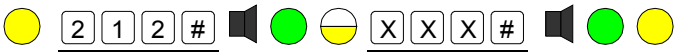
Примечание: *Контроль состояния двери возможен только в случае, если установлен нормально замкнутый дверной контакт.*

Если установить время открытой двери, равное нулю, то контроль состояния двери отключается (значение по умолчанию 30 секунд).

Можно запрограммировать контроллер на подачу сигнала тревоги в случае, если дверь оставлена открытой дольше установленного времени (см. предыдущий подраздел).

Примечание: *При вводе малых значений ведущие нули не требуются. Контроллер не позволит ввести значение больше 255 секунд.*

Время открытой двери в диапазоне от 0 до 255 секунд устанавливается из режима инженера следующим образом (0 соответствует 256 секундам):



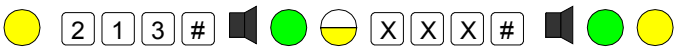
команда время двери

Установка времени выхода

Если при постановке на охрану требуется время на успокоение охранного датчика, то следует установить соответствующее время выхода, которое является задержкой фактической постановки контроллера на охрану после выполнения соответствующей процедуры.

В заводской конфигурации время выхода установлено в 0, то есть постановка на охрану производится без задержки.

Время выхода устанавливается из режима инженера следующей командой:

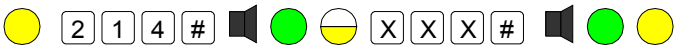


команда время выхода

Установка времени тревоги

Еще один параметр контроллера, программируемый инженером - это время сигнала тревоги, которое может программироваться в диапазоне от 0 до 255 секунд. При этом 0 соответствует активированию выхода тревоги «по событию», то есть на время действия источника тревоги.

Время тревоги устанавливается следующей командой инженера:

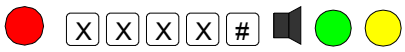


команда время тревоги

Команды администратора

Команды администратора предназначены для управления базой данных пользователей - добавление, удаление, изменение прав, а также для изменения режимов доступа в помещение. Кроме того, в режиме администратора можно изменить код администратора на новый, как это описано ранее.

Переход контроллера в режим администратора производится из дежурного режима с помощью кода администратора:



код администратора

или с помощью карты администратора (если она была перед этим занесена):

После перехода в режим администратора можно выполнить одну или несколько команд. Для возврата в дежурный режим необходимо набрать команду:

или подождать 15 секунд – контроллер автоматически перейдет в дежурный режим.

Управление режимами доступа

Доступ в помещение, защищаемое контроллером SC-TP16, можно осуществлять только по карте, по карте и коду, а также по карте или коду. Переключение режимов доступа производится следующими командами:

Режим доступа	Команда
Только по карте	1 3 2 #
По карте и коду	1 3 1 #
По карте или коду	1 3 0 #

Редактирование пользователей

Администратор может добавлять, удалять отдельных пользователей, а также менять их индивидуальные и групповые характеристики. Ниже описаны все команды редактирования пользователей.

Добавление карт пользователей

Карты пользователей можно добавлять по одной или несколько за один раз («пакетом»), но только в одну группу. Добавление производится следующим образом:

команда №группы добавляемые карты

Номер группы определяет привилегии пользователя следующим образом:

№ группы	Категория пользователя
1	Хозяин
2	Привилегированный пользователь
3	Охранник
4	Простой пользователь

Для завершения процедуры и возврата в режим администратора необходимо набрать команду:

или подождать 15 секунд - контроллер автоматически вернется в дежурный режим.

При занесении новых карт возможна следующая звуковая индикация:


– если карта успешно занесена в базу данных.

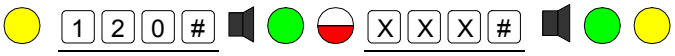

– база данных переполнена, добавление невозможно.


– эта карта уже есть в базе данных.

Примечание: *При занесении новых пользователей они размещаются в базе данных на первое же свободное место последовательно. Например, если существуют пользователи с номерами 1, 2, 3, 5, 6, 7 и 9, то следующие пользователи будут размещены под номерами 4, затем 8, а затем 10, 11 и так далее.*

Удаление пользователя

Занесенного в БД пользователя можно удалить, зная номер удаляемого пользователя в БД. Удаление пользователя производится следующей командой администратора:

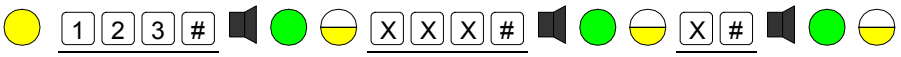


команда № пользователя

Если карты с заданным номером нет, то контроллер издаст три коротких «бип»-а.

Изменение группы пользователя

Права пользователя определяются группой, к которой он приписан. Изменить группу пользователя можно следующей командой в режиме администратора:



команда № пользователя № группы

или с помощью карты пользователя:

команда карта № группы

Желтый мигающий светодиод говорит о том, что можно продолжать редактировать группу следующего пользователя, введя его номер или предъявив карту. Для выхода из режима необходимо ввести команду

Напомним, что права пользователя в соответствии с его группой определяются следующим образом:

№ группы	Категория пользователя
1	Хозяин
2	Привилегированный пользователь
3	Охранник
4	Простой пользователь

Добавление/изменение кода пользователя

По умолчанию каждый пользователь имеет групповой PIN-код (программирование PIN-кода группы описано ниже). Если необходимо присвоить ему индивидуальный код или заменить уже существующий индивидуальный код, необходимо воспользоваться следующей командой администратора:

команда карта новый ПИН - код

Желтый мигающий светодиод говорит о том, что можно продолжать редактировать PIN-код следующего пользователя, предъявив его карту. Для выхода из режима необходимо ввести команду.

Напомним, что ПИН - код может содержать от 4 до 8 цифр.

Примечание: *Индивидуальные коды пользователей не могут совпадать с кодами других пользователей, с кодами инженера, администратора, с групповыми кодами и кодами принуждения.*

Изменение кода группы

Для того, чтобы всегда можно было использовать режимы доступа с кодом, каждая группа имеет свой групповой код, который используется в случае, если пользователю не присваивали индивидуальный код.

Занести или изменить значение PIN-кода группы можно с помощью следующих команд администратора:

Поменять PIN для группы:	Команда (XXXX - PIN группы)
Группа 1 (Хозяин)	1 1 1 # X X X X #
Группа 2 (Привилегированный)	1 1 2 # X X X X #
Группа 3 (Охранник)	1 1 3 # X X X X #
Группа 4 (Простой)	1 1 4 # X X X X #

Примечание: *Контроллер может работать в режиме доступа только по групповым PIN-кодам, без карт, но для этого коды должны быть запрограммированы описанной выше командой.*

Очистка базы данных

Можно удалить сразу всех пользователей и их индивидуальные PIN-коды. Это делается командой администратора:

Поскольку операция является необратимой и потребует заново заносить всю БД пользователей, команда вводится два раза.

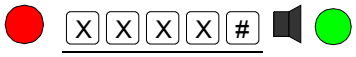
Примечание: *Групповые PIN-коды, коды инженера и администратора при этом не удаляются.*

Команды пользователя

Открывание двери

Все занесенные в базу данных пользователи, независимо от того, к какой группе они приписаны, имеют право прохода через точку, защищаемую данным контроллером. В зависимости от режима прохода (по карте, по коду или по карте и коду) последовательность действий будет следующей.

Проход по коду:

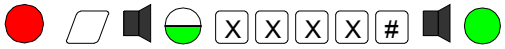


PIN-код

Проход по карте:

карта

Проход по карте и коду:



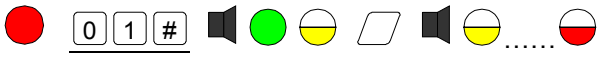
карта PIN-код

Примечание: *В режиме «карта + код» пользователь должен ввести свой PIN-код не позднее 15 секунд после поднесения карты. Если за это время пользователь не ввел свой PIN-код, контроллер переходит обратно в режим ожидания.*

Привилегированные пользователи могут переключать такие режимы работы контроллера, как охрана и блокировка.

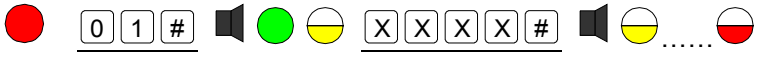
Постановка на охрану

Эта команда разрешена хозяину и охраннику. Постановка на охрану производится следующей командой:



команда карта

или с помощью кода:



команда PIN-код

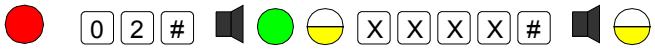
Желтый светодиод после предъявления карты или ввода PIN-кода мигает в течение времени выхода. Красный мигающий светодиод индицирует режим охраны.

Примечание: *Контроллер встанет на охрану по истечении времени выхода только в том случае, если охранные зоны (дверной контакт и охранный датчик) находятся в неактивном состоянии.*

Если постановка на охрану ввиду активности датчика или дверного контакта невозможна, то контроллер издаст три длинных «бип»-а и вернется в дежурный режим. Если пользователь не имеет права ставить на охрану, то контроллер издаст три коротких «бип»-а и будет ждать ввода допустимого PIN-кода или предъявления карты с требуемой привилегией.

Управление блокировкой

Включить или выключить блокировку может только пользователь, имеющий привилегию хозяина. Включение блокировки производится следующей командой пользователя:



команда PIN-код

или с помощью карты:

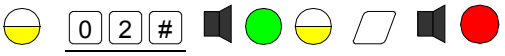
команда карта

Желтый светодиод подтверждает допустимость введенной команды. Редко мигающий желтый светодиод после длинного «бип»-а индицирует состояние блокировки. Если пользователь не имеет необходимой привилегии, то контроллер издаст три коротких «бип»-а и будет ждать ввода допустимого PIN-кода или предъявления карты с требуемой привилегией.

Для снятия блокировки используется следующая команда пользователя:

команда PIN-код

или с помощью карты:



команда карта

Если пользователь не имеет права снимать блокировку, то контроллер издаст три коротких «бип»-а и будет ждать ввода допустимого PIN-кода или предъявления карты с требуемой привилегией. По истечении 15 секунд, если никаких действий не производится, контроллер вернется в режим блокировки (желтый светодиод мигает).

Возврат к заводским установкам

Возврат к заводским установкам может потребоваться в различных ситуациях - если контроллер достался «по наследству» без данных о программировании, если вы запутались в процессе программирования и не можете выйти из этой ситуации и так далее.

При возврате к заводским установкам восстанавливается исходная аппаратная конфигурация контроллера, времена замка и двери, а также время выхода.

Процедура выглядит следующим образом:

1. Выключить питание контроллера.
2. Нажать и удерживать клавишу «**#**».
3. Включить питание контроллера. При этом будет мигать красный светодиод.
4. Через 15 секунд контроллер издаст длинный «бип», сопровождаемый вспышкой зеленого индикатора.
5. Отпустить клавишу «**#**». Контроллер вернется к заводским установкам и перейдет в режим занесения кода инженера.

Примечание: *Коды инженера, администратора и групповые PIN-коды удаляются, восстанавливается заводская конфигурация подключаемого оборудования и временные параметры. База данных пользователей при этом сохраняется.*

Работа контроллера

В зависимости от аппаратной конфигурации, контроллер может работать в различных режимах, как это было описано выше.

Ниже мы еще раз остановимся на некоторых специфических режимах работы контроллера.

Режим блокировки

Этот режим можно включать аппаратно (если вход HLD/SNS сконфигурирован для работы с выключателем блокировки - заводская конфигурация), либо путем ввода с клавиатуры соответствующей команды пользователя, имеющего данную привилегию (ее имеет только хозяин).

В режиме блокировки проход через дверь разрешен только хозяину и привилегированному пользователю. Охранник и простой пользователь в режиме блокировки доступа в помещение иметь не будут.

Режим блокировки, включенный аппаратно (выключателем блокировки) можно выключить набором команды на клавиатуре. Чтобы опять включить режим блокировки аппаратно надо выключить, а затем вновь включить выключатель блокировки.

Охрана помещения

Контроллер поддерживает функции охраны помещения. В зависимости от конфигурации, датчиками являются либо только дверной контакт (заводская установка), либо дверной контакт и внешний датчик, подключенный ко входу HLD/SNS. Для этого надо предварительно сконфигурировать вход HLD/SNS для работы с охранным датчиком соответствующей командой инженера.

Постановку на охрану и снятие с охраны могут производить только хозяин и охранник. При этом для снятия с охраны достаточно предъявить карту, ввести код или предъявить карту и ввести код (в зависимости от режима прохода). Произойдет снятие с охраны и открывание двери.

Если во время состояния охраны произошло нарушение (сработал дверной контакт или охранный датчик), то контроллер начнет подавать сигнал тревоги. Если тревога запрограммирована на определенное время, то по истечении этого времени сигнал тревоги снимется автоматически. При установке работы выхода сигнала тревоги по событию автоматически сигнал тревоги снимется только после пропадания причины (источника) тревоги.

Независимо от режима тревоги (по времени или по событию), сигнал тревоги может быть снят предъявлением любой карты имеющей соответствующую привилегию, занесенной в базу данных контроллера.

Сигналы тревоги

Контроллер может подавать сигнал тревоги в различных случаях. При срабатывании дверного контакта или охранного датчика, а также при проходе под принуждением (см. ниже) сигнал тревоги включается всегда.

В других случаях сигнал тревоги может включаться или не включаться, в соответствии с установками, сделанными инженером. Программируется включение сигнала тревоги на следующие события:

– При взломе не на охране, то есть когда дверь открывается помимо контроллера.
– Если дверь оставлена открытой после истечения времени открытой двери.
– При попытке подбора карты или кода.

Режим входа под принуждением

При проходе по PIN-коду или по карте плюс PIN-коду контроллер реализует режим «duress», или проход под принуждением.

Если вас принуждают открыть дверь с помощью вашего кода, необходимо набрать код, последняя цифра которого отличается от настоящего кода на +1. В этой ситуации контроллер откроет дверь, но при этом активизирует выход тревоги, подавая тем самым сигнал службе безопасности о том, что вас заставляют открыть дверь.

Например, если ваш код равен 12345, то следует набрать 12346. При коде 12349 для подачи сигнала тревоги необходим код 12340.

Поскольку коды принуждения вычисляются контроллером автоматически, они резервируются, и вы не можете одному пользователю назначить PIN-код, равный PIN-коду принуждения другого пользователя. Контроллер просто уведомит вас о том, что данный код в базе данных уже существует.

Технические характеристики

Напряжение питания	12 В постоянного тока, необходим стабилизированный источник питания
Потребляемый ток	Не более 100 мА
Максимальный ток замка	0,7 А для замков, закрываемых напряжением 1,0 А для замков, открываемых напряжением
Максимальный ток выхода на сигнальное устройство	0,7 А
Время замка	От 0 до 255 секунд.
Время двери	От 0 до 255 секунд. 0 секунд соответствует отсутствию контроля состояния двери
Время выхода при постановке на охрану	От 0 до 255 секунд
Максимальное количество пользователей	512 пользователей, произвольно распределенных по 4-м категориям

Комплект поставки и гарантии

Стандартная комплектация

В стандартный комплект поставки входят:

Контроллер SC-TP16	1
Накладка верхняя	1
Накладка нижняя	1
Комплект крепежа в составе: саморезы дюбели	2 2
Паспорт и краткая инструкция по эксплуатации	1
Полное руководство на минидиске	1
Упаковочная коробка	1

Дополнительная информация

Всю дополнительную информацию по работе с контроллерами можно получить по адресу:

support@parsec.ru

Гарантии

Срок гарантии – 24 месяца со дня продажи изделия. Прилагаемым к контроллеру гарантийным талоном производитель подтверждает исправность данного изделия и берет на себя обязательство по бесплатному устранению всех неисправностей, возникших в течение гарантийного срока по вине производителя.