PERCo®

Единая система безопасности и повышения эффективности предприятия

PERCo-S-20

Подсистема СКУД

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Контроллеры:
PERCo-CT/L04.2
PERCo-CT03.2
PERCo-CR01.2
PERCo-CL05.2
PERCo-CT/L04
PERCo-CT03
PERCo-CR01
PERCo-CL05.1
PERCo-CL201.1

Единая система безопасности и повышения эффективности предприятия *PERCo-S-20.* Подсистема СКУД

Руководство по эксплуатации

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящее Руководство по эксплуатации (далее – *руководство*) предназначено для ознакомления с функциональными возможностями, принципом работы и особенностями настройки **Подсистемы СКУД, входящей в состав Единой системы безопасности и повышения эффективности предприятия *PERCo-S-20*** (далее - *Подсистема СКУД PERCo-S-20*), с целью обеспечения правильной эксплуатации и наиболее полного использования всех ее возможностей.

Данное руководство должно использоваться совместно с *«Техническим описанием Единой системы безопасности и повышения эффективности PERCo-S-20»* и руководствами по эксплуатации на входящие в систему контроллеры и электронные проходные. Описание программного обеспечения приводится в руководствах пользователя на соответствующие модули.

Примечание:

Эксплуатационная документация доступна в электронном виде на сайте компании ***PERCo***, по адресу: www.perco.ru, в разделе **Поддержка> Документация**.

Принятые в руководстве сокращения:

АТП – автотранспортная проходная;
ВВУ – внешнее верифицирующее устройство;
ИУ – исполнительное устройство;
ОЗ – охранная зона;
ОПС – охранно-пожарная сигнализация;
ПДУ – пульт дистанционного управления;
ПК – персональный компьютер, ноутбук;
ПО – программное обеспечение;
ПЦН – пульт централизованного наблюдения;
СКУД – система контроля и управления доступом;
ТС – транспортное средство;
ШС – шлейф сигнализации;
ЭП – электронная проходная.

1 НАЗНАЧЕНИЕ

Подсистема СКУД *PERCo-S-20* с элементами охранной сигнализации предназначена для организации контроля и управления доступом сотрудников, посетителей и ТС на территорию и в помещения предприятия.

Доступ может осуществляться по пропускам на основе бесконтактных карт через специально оборудованные точки прохода. Каждая карта обладает уникальной информацией – *идентификатором*. В БД системы идентификатор связан с данными сотрудника, посетителя или ТС, которому она выдана.

В качестве идентификатора в системе также могут выступать и биометрические признаки человека, в частности, в системе ***PERCo-S-20*** предусмотрена интеграция с биометрическими контроллерами ***Suprema***, которые осуществляют биоидентификацию по отпечаткам пальцев.

Контроллеры ***Suprema*** поддерживают несколько режимов доступа, которые обеспечивают доступ по карте, пальцу, карте и пальцу, карте или пальцу, что позволяет гибко настраивать параметры верификации для сотрудников с разным уровнем прав доступа/режимом работы.

Контроллеры всех точек прохода связаны по сети *Ethernet* между собой и с единой БД системы. Каждое событие предъявления идентификатора фиксируется в БД с указанием места и времени предъявления. Это позволяет отслеживать время пребывания и перемещения пользователей по территории и в помещениях предприятия.

Для каждого контролируемого направления через исполнительные устройства точек прохода может быть установлен один из режимов контроля доступа (РКД): *«Открыто»*,

«Закрыто», *«Контроль»*. Это позволяет при необходимости обеспечить свободный проход в данном направлении или полностью его перекрыть. РКД *«Контроль»* используется для прохода по идентификаторам.

Для точек прохода типа «дверь» доступна возможность конфигурирования ОЗ. В зависимости от модели контроллера в ОЗ может входить ИУ и ШС. Эту ОЗ можно перевести в режим *«ОХРАНА»* и снять с охраны при помощи идентификатора - бесконтактной карты доступа, которой выдан соответствующий тип прав, или оператором через ПО. При постановке на охрану для считывателей точки прохода устанавливается РКД *«Охрана»*. Поддержка ШС позволяет контролировать не только вход в помещение, но также и весь его объем.

2 ПРИНЦИП РАБОТЫ ПОДСИСТЕМЫ

Пространственные зоны

При установке системы территория предприятия разделяется на пространственные зоны контроля. Переход пользователей из одной пространственной зоны в другую осуществляется только через специально оборудованные точки прохода, с предъявлением карт доступа или иных идентификаторов. Пространственные зоны могут быть вложенными одна в другую.

Точки прохода

Каждая точка прохода оборудуется исполнительным устройством (турникетом, замком, электронной проходной, шлагбаумом и т.п.), которое управляется контроллером СКУД – функциональной единицей подсистемы СКУД. К контроллеру подключается различное дополнительное оборудование (считыватели, ПДУ, датчики, оповещатели и др.). Для поддержки всех функций системы каждый контроллер точки прохода должен быть подключен по сети *Ethernet* к серверу системы. Полный перечень оборудования и ПО подсистемы СКУД приведен в *«Техническом описании»* системы.

В зависимости от подключенного к контроллеру ИУ может отличаться алгоритм работы контроллера с идентификаторами, смены РКД и др. Поэтому при описании функционирования подсистемы выделяются следующие типы контроллеров:

- *«Контроллер управления односторонней дверью»*
- *«Контроллер управления двухсторонней дверью»*
- *«Контроллер управления турникетом»*
- *«Контроллер АТП»*
- *«Контроллер регистрации»*

Действия контроллера

При предъявлении идентификатора считывателю на точке прохода его идентификационная информация передается в контроллер. Если данный идентификатор находится в списке контроллера, то контроллер проверяет его *права доступа*, статус и срок действия. После этого в зависимости от установленных параметров ресурсов контроллер выполняет одно из следующих действий:

- разрешает доступ;
- запрещает доступ;
- формирует запрос на комиссионирование;
- формирует запрос на верифицирующее устройство;
- формирует сообщения индикации для АРМ.

Проход по идентификатору – карте доступа

Проход по идентификатору возможен только в том случае, если ему выданы соответствующие права доступа. При проходе по идентификатору регистрируется событие прохода с указанием даты и времени прохода. В ПО передается событие мониторинга о проходе. Также фиксируется смена номера пространственной зоны, в которой находится пользователь.

Регистрируемые данные о проходах передаются по сети *Ethernet* в БД системы и ПО (см. разд. 4). На основе этих данных в дальнейшем могут формироваться отчеты для учета рабочего времени, о нарушениях трудовой дисциплины, местоположении и т.д.

Проход по идентификатору – отпечатку пальца

Проход по отпечатку пальца возможен только в случае, если ему выданы соответствующие права доступа. При проходе по отпечатку пальца регистрируется событие прохода с указанием даты и времени прохода. В ПО передается событие мониторинга о проходе. Также фиксируется смена номера пространственной зоны, в которой находится пользователь.

Регистрируемые данные о проходах передаются по сети *Ethernet* в БД системы и ПО (см. разд. 4). На основе этих данных в дальнейшем могут формироваться отчеты для учета рабочего времени, о нарушениях трудовой дисциплины, местоположении и т.д.

В системе реализована возможность зарегистрировать до 5 отпечатков пальцев на одного сотрудника / посетителя, а также назначить тревожные отпечатки, в результате сканирования которых контроллером будет автоматически сгенерирован сигнал тревоги.

В системе **не хранятся** изображения отпечатков пальцев. При регистрации отпечатков получаемое изображение папиллярных узоров подушечки пальца преобразуется контроллером по сложному алгоритму в специальный цифровой код, который называется *сверткой*. Свертка хранится в системе и используется для сравнения со сверткой, которая получается в результате сканирования отпечатков пальцев во время верификации пользователя.

Контроллеры ***Suprema*** поддерживают следующие режимы доступа:

- **Палец** – для верификации требуется пройти процедуру сканирования отпечатка пальца;
- **Карта** – для верификации требуется предъявить считывателю карту доступа;
- **Карта и палец** – для верификации требуется предъявить считывателю карту доступа, после чего пройти процедуру сканирования отпечатка пальца;
- **Карта или палец** – для верификации требуется предъявить считывателю карту доступа или пройти процедуру сканирования отпечатка пальца.

Для работы в режиме доступа **Карта и палец** и **Карта или палец** необходимо, чтобы пользователю была выдана карта доступа для работы с контроллерами ***Suprema*** и проведена процедура сканирования отпечатков пальцев.

Система позволяет выбрать желаемый **Уровень безопасности** при использовании верификации по отпечатку пальца:

- Нормальный,
- Безопасный,
- Наиболее безопасный.

Чем выше установленный уровень безопасности, тем больше характерных точек будет считываться с отсканированного изображения папиллярных узоров отпечатка пальца, а значит – снизится вероятность ложного срабатывания (прохода по чужому / поддельному отпечатку). Однако, чем выше установленный уровень безопасности, тем выше вероятность отказа при сканировании отпечатков. Отказы могут возникать вследствие возникновения ошибок сканирования, связанных с более высоким влиянием на процедуру сканирования влажности и температуры воздуха, загрязнённости сканируемой поверхности пальцев и т.д. В этом случае для успешной верификации потребуется повторно пройти процедуру сканирования отпечатков.

3 ПРАВА ДОСТУПА ИДЕНТИФИКАТОРА

Права доступа идентификатора в системе могут быть связаны с данными сотрудника, посетителя или транспортного средства.

Права доступа идентификатора условно подразделяются на единые, которые задаются для всей системы, и персональные, которые задаются независимо для каждого направления

каждой точки прохода. Для обеспечения доступа по идентификатору его идентификационная информация и права доступа должны быть переданы в контроллер.

Контроль тех или иных персональных прав доступа зависит от индивидуальных настроек параметров ресурсов контроллера (см. разд. 5.5) и установленного РКД.

3.1 Единые права на систему

Статус идентификатора:

- **Заблокирован** – доступ по идентификатору временно запрещен (рекомендуется устанавливать, если пользователь находится в отпуске, командировке и т.п.).
- **Разблокирован** – доступ по идентификатору разрешен при условии соблюдения всех установленных прав доступа.
- **СТОП-лист** – доступ по идентификатору запрещен, идентификатор занесен в СТОП-лист (например, если карта доступа была утеряна или повреждена).
- **Карта ТС** – идентификатор транспортного средства (используется в конфигурации *«Контроллер АТП»*).

Категории идентификаторов по их владельцам:

- **Карта сотрудника** – для постоянных идентификаторов (срок действия от нескольких дней до нескольких лет);
- **Карта посетителя** – для разовых или временных идентификаторов (срок действия от 15 минут до нескольких месяцев).

3.2 Персональные права

Персональные права доступа выдаются идентификатору независимо на каждое направление каждой точки прохода.

3.2.1 Тип права доступа

Для сотрудников можно выдать один из следующих типов прав доступа:

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

Для посетителей можно выдать один из следующих типов прав:

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

Постановка на охрану

Для контроллеров типа *«Контроллер управления дверью»* доступна возможность конфигурирования ОЗ, включающей ИУ. Эту ОЗ можно перевести в режим *«ОХРАНА»* при помощи бесконтактной карты доступа, или оператором через ПО. При этом для считывателей устанавливается РКД *«Охрана»*.

Для этого карте доступа необходимо выдать соответствующий тип права на контроллер: …**с постановкой на охрану**…/ …**со снятием с охраны**…, и указать номер ОЗ (**Группы ресурсов**), которые будут ставиться на охрану / сниматься с охраны при помощи карты.

Комиссионирование

Комиссионирование – процедура подтверждения прав предъявленного идентификатора посредством предъявления второго, комиссионирующего идентификатора.

Примечание:

Если одновременно установлены функции комиссионирования и верификации, первой выполняется процедура комиссионирования, а затем верификации.

Если необходимо проводить процедуру комиссионирования при предъявлении идентификатора, то ему выдается тип права доступа на данный контроллер **… с комиссионированием**.

Примечание:

Для *«Контроллера АТП»* процедура комиссионирования ТС называется *досмотр*. Для ТС сотрудников и посетителей возможны следующие типы прав на контроллер:

- **Доступ без досмотра**
- **Доступ с досмотром**

Для служебных ТС доступно назначение процедуры проезда через АТП с дополнительным комиссионированием картой водителя (сотрудника).

Комиссионирующим идентификатором для конкретного ИУ контроллера может служить, например, бесконтактная карта доступа, выданная сотруднику-комиссионеру и внесенная для ресурса контроллера **Контроллер ИУ** в **Список карт сотрудников, имеющих право на комиссионирование (досмотр)**.

3.2.2 Функция Antipass

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

Для локального контроля зональности необходимо установить в правах доступа идентификатора параметр **Защита от передачи карт (Antipass)**. По умолчанию все идентификаторы подвержены контролю зональности.

Для включения функции локального контроля зональности на точке прохода необходимо установить:

- Для ресурса контроллера **ИУ** установить параметр **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 РКД контроллера выбрать один из способов защиты.

Функция Global Antipass

Примечание:

Для работы функции *Global Antipass* должно быть указано расположение точки прохода и должна поддерживаться связь с другими контроллерами сети.

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 во внутреннее помещение, не войдя в само здание). Для работы функции при конфигурации системы из ПО необходимо указать пространственные зоны и расположение точек прохода.

Для реализации этой функции информация о каждом проходе по данному идентификатору (то есть смены пространственной зоны) передается другим контроллерам системы. В результате каждый контроллер системы безопасности, подключенный к сети, имеет информацию о том, в какой пространственной зоне должен находиться пользователь предъявленного идентификатора.

3.2.3 Контроль доступа по времени

Контроллеры системы могут осуществлять управление доступом с учетом текущего времени (дня недели), то есть запретить проход через ИУ, разрешить, либо разрешить с предупреждением в зависимости от выданных идентификатору прав доступа и установленных параметров ресурсов контроллера. Детальное описание типов критериев доступа по времени приводится в руководстве пользователя ПО.

В системе предусмотрены следующие типы критериев доступа по времени (можно настроить до 255 критериев каждого типа) :

- **Временные зоны**;
- **Недельные графики**;
- **Скользящий посуточный график**;
- **Скользящий понедельный график**.

В правах доступа идентификатора необходимо включить подверженность контролю по времени, выбрав тип критерия и указав какой-либо критерий контроля по времени. Для отключения контроля по времени необходимо выбрать временную зону *«Всегда»* (для *«Контроллера регистрации»* – временную зону *«Никогда»*).

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 включения функции контроля по времени в одном из направлений точки прохода необходимо для ресурса контроллера **Считыватель** (обеспечивающего доступ в выбранном направлении) у параметра **Контроль времени для идентификаторов СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ** выбрать один из режимов контроля.

3.2.4 Верификация и индикация

Примечание:

Если одновременно установлены функции комиссионирования и верификации, первой выполняется процедура комиссионирования, а затем верификации.

Верификация – процедура подтверждения прав предъявленного идентификатора оператором с помощью верифицирующего устройства (ПДУ, ПО) на основе сравнения изображения, получаемого с видеокамер, и данных (в том числе графических), хранящихся в базе данных программы и выводимых при предъявлении идентификатора. Также в качестве **внешнего верифицирующего устройства** (*ВВУ*) может выступать и другое дополнительное оборудование, автоматически подтверждающее право прохода при выполнении определенных условий или действий[1]. Например, картоприемник (подтверждением является факт изъятия временной карты доступа), алкостестер (подтверждением является факт трезвости сотрудника) и т.п.

Внимание!

Если при предъявлении идентификатора необходимо подтверждение его прав от верифицирующего устройства, то в его правах доступа необходимо установить параметр **Подверженность верификации**.

Для проведения процедуры верификации с помощью ПДУ при предъявлении идентификатора в одном из направлений точки прохода необходимо для ресурса контроллера **Считыватель** (обеспечивающего доступ в выбранном направлении) установить у параметра **Подтверждение разрешения прохода** значение **"Да"**. После этого отдельно для сотрудников и посетителей необходимо указать типы нарушений, которые будут отслеживаться.

[1] Для контроллеров ***CT/L04*** возможность верификации от ВВУ доступна с версий прошивки x.x.x.20. Обратите внимание, что при обновлении прошивки изменяется конфигурация контроллера. Потребуется повторно добавить контроллер в конфигурацию системы

Для проведения верификации из ПО – должен быть запущен соответствующий модуль ПО и настроена точка верификации для выбранного направления точки прохода (см. Руководство пользователя на соответствующее ПО).

Для проведения автоматической верификации от ВВУ необходимо в ПО настроить соответствующий тип входа контроллера, к которому подключено ВВУ (**Подтверждение от ВВУ**) и установить соответствующую реакцию контроллера на результат верификации. Подробнее порядок настройки ВВУ – см. в руководстве по эксплуатации контроллера и используемого оборудования.

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

4 СОБЫТИЯ РЕГИСТРАЦИИ И МОНИТОРИНГА

Все события регистрируются с учетом календарной даты и времени с точностью до секунды.

События регистрации – все события, регистрируемые контроллером системы в процессе функционирования. Все регистрируемые события сохраняются в энергонезависимой памяти контроллера. Максимальное количество хранимых событий зависит от размера энергонезависимой памяти контроллера и указано в его эксплуатационной документации. В случае переполнения памяти новые события заменяют наиболее старые. При подключении к контроллеру с помощью ПО все события из памяти контроллера переносятся в журнал событий ПО. Перечень событий, регистрируемых контроллерами, а также причины их формирования приведены в Приложении 2.

События мониторинга – события, передаваемые контроллером системы в ПО для оперативного принятия решения оператором системы. При нарушении связи контроллера с ПО события мониторинга не передаются.

5 РЕСУРСЫ КОНТРОЛЛЕРОВ *PERCO* И ПАРАМЕТРЫ ИХ ФУНКЦИОНИРОВАНИЯ

5.1 Ресурсы контроллеров

Используя параметры ресурсов контроллера можно настроить:

- Нормализованные состояния для входов и выходов контроллера (в том числе для входов и выходов ИУ).
- Действия контроллера и его ресурсов при предъявлении считывателю идентификатора, в зависимости от установленного РКД и прав доступа.
- Реакцию контроллера и его ресурсов на регистрируемые события.

В зависимости от типа и конфигурации контроллера наличие тех или иных ресурсов и их количество может отличаться. В таблице 1 представлен перечень ресурсов контроллеров системы. Ресурсы контроллера сгруппированы по типам:

- **Дополнительные входы**;
- **Дополнительные выходы**;
- **Шлейфы сигнализации**;
- **Зоны** (охранные);
- **Контроллер ИУ** (замка, турникета, шлагбаума);

Если к контроллеру подключены несколько ИУ или контроллеры второго уровня, 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 доступных для настройки параметров каждого ресурса приведен ниже. Порядок настройки зависит от используемого ПО.

Таблица 1. Ресурсы контроллеров и ЭП PERCo

Модель	Доп. вход	Доп. выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считы-ватель	ИУ	Ген. тревоги	ОЗ
Контроллеры доступа									
CT/L04 (1) [1]	2	4[2]	2	2	0	2	2L	1	1
CT/L04 (2)	2	4[2]	2	2	8	2	2L	1	1
CT/L04 (3)	2	4[2]	2	2	8	2	L+ L	2	2
CT/L04 (4)	2	2	0	0	0	2	T	1	0
CT/L04 (5)	2	2	0	0	8	2	T	1	0
CT/L04 (6)	2	2	0	0	0	2	G	1	0
CT/L04 (7)	2	2	0	0	8	2	G	1	0
CT/L04.2 (1) [3]	4	4	0	0	до 8	2	T	1	0
CT/L04.2 (2)	2	3	0	0	до 8	3	T+L	2	1
CT/L04.2 (3)	0	2	0	0	до 8	4	T+L+L	3	2
CT/L04.2 (4)	2	3	0	0	до 8	4	T+2L	2	1
CT/L04.2 (5)	5	4	0	0	до 8	2	G	1	0
CT/L04.2 (6)	3	3	0	0	до 8	3	G+L	2	1
CT/L04.2 (7)	1	2	0	0	до 8	4	G+L+L	3	2
CT/L04.2 (8)	3	3	0	0	до 8	4	G+2L	2	1
CT/L04.2 (9)	5	8	2	2	до 8	1	L	1	1
CT/L04.2 (10)	6	8	1	1	до 8	1	L	1	1
CT/L04.2 (11)	7	8	0	0	до 8	1	L	1	1
CT/L04.2 (12)	3	7	2	2	до 8	2	L+L	2	2
CT/L04.2 (13)	4	7	1	1	до 8	2	L+L	2	2
CT/L04.2 (14)	5	7	0	0	до 8	2	L+L	2	2
CT/L04.2 (15)	2	6	1	1	до 8	3	L+L+L	3	3
CT/L04.2 (16)	3	6	0	0	до 8	3	L+L+L	3	3
CT/L04.2 (17)	0	4	0	0	до 8	4	L+L+L+L	4	4
CT/L04.2 (18)	5	8	2	2	до 8	2	2L	1	1
CT/L04.2 (19)	6	8	1	1	до 8	2	2L	1	1
CT/L04.2 (20)	7	8	0	0	до 8	2	2L	1	1
CT/L04.2 (21)	4	7	1	1	до 8	3	2L+L	2	2
CT/L04.2 (22)	5	7	0	0	до 8	3	2L+L	2	2
CT/L04.2 (23)	3	6	0	0	до 8	4	2L+L+L	3	3
CT/L04.2 (24)	4	7	1	1	до 8	4	2L+2L	2	2
CT/L04.2 (25)	5	7	0	0	до 8	4	2L+2L	2	2

[1] В скобках указан номер конфигурации контроллера.
[2] Два выхода снабжены контролем линии на КЗ и обрыв (см. разд. 8.4).
[3] В скобках указан номер конфигурации (шаблона конфигурации) контроллера.

Модель	Доп. вход	Доп. выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считы-ватель	ИУ	Ген. тревоги	ОЗ
CL05.1, CL05.2	1/1[1]		0	0	-	1	L	1	1
CL201.1	0	0	0	0	-	1	L	1	1
Контроллеры регистрации									
CR01, CR01.2	-	-	-	-	-	2	-	-	-
Встроенные контроллеры электронных проходных									
CT03 (1)	2	2	0	0	0	2	T	1	0
CT03 (2)	2	2	0	0	8	2	T	1	0
CT03.2 (1)	4	4	0	0	до 8	2	IP-Stile	1	0
CT03.2 (2)	2	3	0	0	до 8	2	IP-Stile+IC	1	0
CT03.2 (3)	4	3	0	0	до 8	2	IP-Stile+AP	1	0
CT03.2 (4)	2	2	0	0	до 8	2	IP-Stile+IC+AP	1	0

Принятые в таблице сокращения:

L – односторонний замок;
2L – двусторонний замок;
T – турникет;
G – шлагбаум;
IP-Stile – электронная проходная;
IC – встроенный картоприемник;
AP – встроенное устройство «Антипаника".

Варианты конфигурации контроллера ***PERCo-CT/L04***:

1. Контроллер для управления одной двухсторонней дверью.
2. Контроллер для управления одной двухсторонней дверью с возможностью подключения до восьми контроллеров замка ***PERCo-CL201***.
3. Контроллер для управления двумя односторонними дверьми с возможностью подключения до восьми контроллеров замка ***PERCo-CL201***.
4. Контроллер для управления турникетом.
5. Контроллер для управления турникетом с возможностью подключения до восьми контроллеров замка ***PERCo-CL201***.
6. Контроллер АТП.
7. Контроллер АТП с возможностью подключения до восьми контроллеров ***PERCo-CL201***.

Варианты шаблонов конфигурации контроллера ***PERCo-CT/L04*** (к любой конфигурации возможно подключить до восьми контроллеров замка ***PERCo-CL201***):

1. Контроллер для управления турникетом.
2. Контроллер для управления турникетом и одним односторонним замком.
3. Контроллер для управления турникетом и двумя односторонними замками.
4. Контроллер для управления турникетом и одним двусторонним замком.
5. Контроллер для управления автотранспортной проходной (АТП).
6. Контроллер для управления АТП и одним односторонним замком.
7. Контроллер для управления АТП и двумя односторонними замками.
8. Контроллер для управления АТП и одним двусторонним замком.
9. Контроллер для управления одним односторонним замком с двумя ШС.
10. Контроллер для управления одним односторонним замком с одним ШС.

[1] Имеющийся вывод м.б. сконфигурирован либо как вход, либо как выход, либо как вход/выход для синхронизации с другим контроллером ***PERCo-CL05.2*** (используется при совместной работе двух контроллеров для организации одной двухсторонней точки прохода с поддержкой смены зональности).

11. Контроллер для управления одним односторонним замком.
12. Контроллер для управления двумя односторонними замками с двумя ШС.
13. Контроллер для управления двумя односторонними замками с одним ШС.
14. Контроллер для управления двумя односторонними замками.
15. Контроллер для управления тремя односторонними замками с одним ШС.
16. Контроллер для управления тремя односторонними замками.
17. Контроллер для управления четырьмя односторонними замками.
18. Контроллер для управления одним двусторонним замком с двумя ШС.
19. Контроллер для управления одним двусторонним замком с одним ШС.
20. Контроллер для управления одним двусторонним замком.
21. Контроллер для управления одним двусторонним и одним односторонним замками с одним ШС.
22. Контроллер для управления одним двусторонним и одним односторонним замками.
23. Контроллер для управления одним двусторонним и двумя односторонними замками.
24. Контроллер для управления двумя двусторонними замками с одним ШС.
25. Контроллер для управления двумя двусторонними замками.

Варианты конфигурации ЭП ***PERCo-CT03***:

1. Электронная проходная.
2. Электронная проходная с возможностью подключения до восьми контроллеров замка ***PERCo-CL201***.

Варианты шаблонов конфигурации ЭП ***PERCo-CT03.2*** (к любой конфигурации возможно подключить до восьми контроллеров замка ***PERCo-CL201***):

1. Электронная проходная.
2. Электронная проходная со встроенным картоприемником.
3. Электронная проходная со встроенным устройством «Антипаника».
4. Электронная проходная со встроенными картоприемником и устройством «Антипаника».

5.2 Общие параметры контроллеров

Разрешить Web-интерфейс. По умолчанию у контроллеров доступ к Web-интерфейсу разрешен, но при подключении к контроллеру через ПО систем ***PERCo*** доступ к Web-интерфейсу запрещается или ограничивается с целью предотвращения коллизий. После этого полный доступ к Web-интерфейсу будет возможен при условии установленного и переданного в контроллер параметра **Разрешить Web-интерфейс** только после остановки сервера системы или исключения контроллера из конфигурации системы в ПО.

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

5.3 Параметры контроллера регистрации (LICON)

Прямое направление прохода параметр позволяет указать, в направлении какого из считывателей проход считается входом. При установленном параметре правый считыватель считается входным, левый – выходным. При снятом параметре – наоборот.

Примечание:

При изменении прямого направления прохода подписи указателей *«Вход»* и *«Выход»* на ЖКИ не меняются. Изменить текст надписей указателей можно в раскрывающемся меню **Локализация отображаемых строк.**

Защита от передачи идентификаторов (Antipass). Раскрывающийся список позволяет определить реакцию системы в случае повторного предъявления одной и той же карты доступа к считывателю, то есть при работе функции системы *Antipass*. Возможен выбор одного из следующих вариантов:

- **Нет** – реакция не задана.
- **Мягкая** – регистрируется событие *«Проход с нарушением зональности»*.

- **Жесткая** – при нарушении локальной зональности (*Antipass*) – проход по карте разрешается, при этом регистрируется событие *«Проход с нарушением зональности»*; при нарушении глобальной зональности (*Global Antipass*) регистрируется событие *«Запрет прохода по причине нарушения зональности».*

Время ожидания персонализации. Поле ввода позволяет задать время, в течение которого контроллер ожидает получения от сервера системы персональной информации (ФИО), связанной с предъявленной картой доступа. В случае невозможности получения информации на ЖКИ отображается идентификатор карты.

Время отображения персонализации. Поле ввода позволяет задать время, в течение которого на ЖКИ контроллера отображается персональная информация, связанная с предъявленной картой доступа.

Локализация отображаемых строк. Раскрывающийся список позволяет изменить содержание сообщений, отображаемых на ЖКИ контроллера.

Контроллер регистрации имеет два встроенных считывателя. Для считывателей доступно поле ввода **Текущее наименование**, позволяющее изменить описательное название считывателей. По умолчанию: *«Считыватель №…».*

5.4 Параметры ресурса «Исполнительное устройство» (ИУ)

Прямое направление прохода. Параметр позволяет указать, в направлении какого из считывателей для двустороннего ИУ проход считается входом.

- По умолчанию параметр установлен, и нумерация считывателей соответствует положению перемычки *«номер считывателя» (XP2)* на плате считывателя.
- Если параметр отключен, то тот считыватель, который в соответствии с его перемычкой должен иметь номер 1, в контроллере будет опознан как считыватель номер 2, и наоборот.

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

Нормальное состояние «Закрыто» выхода ИУ (*Не запитан* / *Запитан*) (Не доступен в конфигурации *«Контроллер АТП»*). Параметр указывает, активизирован ли выход управления ИУ (подано управляющее напряжение на реле или транзистор) при заблокированном ИУ.

Нормализация выхода ИУ (*После «Открытия»* / *После «Закрытия»*). Параметр определяет, в какой момент нормализуется состояние выхода управления ИУ.

Режим работы выхода управления ИУ (Доступен только в конфигурации *«Контроллер управления дверьми»*) Описывает логику управления подключенным ИУ.

- **Потенциальный**
- **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 ИУ и определяет длительность импульса управления ИУ.

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 разблокируемом состоянии (**Время анализа идентификатора**). Время, на которое разблокируется ИУ при разрешении доступа.

Время ожидания комиссионирования / **Время досмотра** / **Время ожидания подтверждения проезда картой водителя (сотрудника)**. Параметр позволяет ограничить интервал времени между предъявлением идентификатора пользователя (сотрудника / посетителя / служебного ТС) и комиссионирующей карты (сотрудника / охранника /

водителя), в случае если в правах идентификатора пользователя установлен доступ с комиссионированием / доступ с досмотром / подтверждение проезда картой водителя.

Регистрация прохода по предъявлению идентификатора (Не доступен в конфигурации *«Контроллер АТП»*). При установке параметра контроллер будет считать проход совершившимся сразу после предъявления идентификатора, независимо от того, будет ли реально совершен проход через ИУ или нет.

Внимание!

При установке параметра **Регистрация прохода по предъявлению идентификатора** недопустимо у ресурсов **Считыватель** для обоих направлений прохода:

- Устанавливать для параметра **Подтверждение разрешения** значение отличное от **Нет**. То есть запрещено проведение процедуры верификации от ПДУ или ВВУ.
- Проводить процедуру верификации из ПО.

Обратное может привести к некорректной работе функции контроля зональности (Antipass). Также при установке этого параметра не рекомендуется устанавливать для параметра **Защита от передачи идентификаторов** значение **Жесткая**.

Отсутствие датчиков проезда (Доступен только в конфигурации *«Контроллер АТП»*). При установке параметра контроллер будет считать проезд совершившимся сразу после предъявления идентификатора, независимо от того, будет ли реально совершен проход через ИУ или нет. ИУ будет открыто на **Время удержания в разблокированном состоянии**.

Задержка восстановления датчиков проезда (Доступен только в конфигурации *«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 установленном параметра контроллер отслеживает случаи повторного предъявления одного и того же идентификатора к тому же считывателю.

Fire Alarm в РЕЖИМЕ РАБОТЫ «ОХРАНА» – При установленном параметре аварийная разблокировка (открытие прохода ИУ) в случае поступления управляющего сигнала от устройства *Fire Alarm* произойдет также при взятой на охрану ОЗ, включающей данное ИУ. При снятом параметре (по умолчанию) в РКД *«Охрана»* сигналы на входах **Тип: Fire Alarm** игнорируются.

5.5 Параметры ресурса «Считыватель»

Запрещение ДУ. При установке параметра для РКД *«Контроль»* нажатие на кнопку ПДУ в направлении данного считывателя будет игнорироваться.

Подтверждение разрешения прохода. Параметр позволяет указать, будет ли при предъявлении идентификатора считывателю в РКД *«Контроль»* формироваться запрос на верифицирующее устройство. В качестве верифицирующих устройств могут использоваться: ПДУ, картоприемник, алкотестер (алкометр) или другое оборудование. В случае прохода с верификацией от ПО и отсутствия связи с верифицирующим устройством доступ может быть подтвержден кнопкой ПДУ.

- **От ДУ.** Для настройки картоприемника и верификации от ПДУ или ПО. Имеется возможность гибко настроить условия запуска процедуры верификации независимо для карт доступа сотрудников и посетителей в следующих случаях:
  - **при проходе СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ** – верификация проводится при каждой попытке прохода;
  - **при проходе с НАРУШЕНИЕМ ВРЕМЕНИ СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ** – верификация проводится при попытке прохода в случае нарушения времени (параметр **Контроль времени для идентификаторов** должен быть установлен на значение **Жесткий**).

  - **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ** – верификация проводится в случае попытке повторного входа без предварительного выхода (параметр **Защита от передачи идентификаторов** должен быть установлен на значение **Жесткая**).
- **От ВВУ**. Для верификации от алкотестера (алкометра) или другого оборудования. Имеется возможность настроить запуск процедуры верификации независимо для карт доступа сотрудников и посетителей.

Подтверждение прохода для ПОСЕТИТЕЛЕЙ. Параметр позволяет выбрать дополнительное условие проведения процедуры верификации для посетителей.
- **Постоянно.** Верификация проводится независимо от срока действия карты.
- **В последний день действия идентификатора.** Верификация проводится в случае, если дата предъявления совпадает с датой окончания срока действия карты

Время ожидания подтверждения. Параметр позволяет установить время, в течение которого контроллер ожидает подтверждение запроса от верифицирующего устройства.

По истечении времени ожидания подтверждения генерировать событие. Параметр позволяет выбрать событие, регистрируемое, в случае отсутствия подтверждения прохода от ВВУ:
- **Запрет прохода от ВВУ**. Рекомендуется в случае подключения ВВУ имеющего только один выход разрешения прохода.
- **Отказ от прохода, нет ответа от ВВУ**. Рекомендуется в случае подключения ВВУ имеющего выходы, как для разрешения прохода, так и для запрета прохода.

Защита от передачи идентификаторов СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ (Antipass). Параметр позволяет для выбранных РКД определить реакцию контроллера на предъявление карты доступа сотрудника / посетителя к считывателю в случае нарушения им функции контроля зональности (Antipass). Для каждого из указанных РКД контроллера можно выбрать один из видов контроля:
- **Нет** – Контроллер не учитывает зональность идентификатора карты для разрешения доступа.
- **Мягкая.** Контроллер разрешит доступ по карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение зональности»* и после совершения прохода регистрируется событие «*Проход по карте с несоответствием текущему местоположению»*.
- **Жесткая.** Контроллер запретит доступ по карте, при этом передается событие мониторинга *«Предъявление карты с нарушением зональности»* и регистрируется событие *«Запрет прохода по причине нарушения зональности».* Если для считывателя установлен параметр **Подтверждение разрешения прохода** (или верификация от ПО), то будет запущена процедура верификации.

Контроль времени для идентификаторов СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ. Параметр позволяет для выбранных РКД определить реакцию контроллера на предъявление карты доступа сотрудника / посетителя к считывателю в случае нарушения установленного критерия доступа по времени. Для каждого из указанных РКД контроллера можно выбрать один из видов контроля:
- **Нет.** Контроллер не отслеживает временные критерии прав доступа карты.
- **Мягкий.** Контроллер разрешит доступ по предъявленной карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение времени»*, а после прохода регистрируется событие «*Проход по карте с несоответствием временным критериям доступа»*.
- **Жесткий.** Контроллер запретит доступ по карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение времени»* и регистрируется событие «*Запрет прохода, несоответствие временным критериям доступа»*. Если для считывателя установлен параметр **Подтверждение разрешения прохода** (или верификация от ПО), то 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 те дополнительные входы, 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 время.

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

Дополнительные выходы, нормализируемые при разблокировке ИУ. Параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализированы при разблокировке ИУ. Для выбора отметьте те дополнительные выходы, которые должны быть нормализированы. Укажите временной критерий нормализации.

Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ. Параметр позволяет указать выходы, активизируемые при предъявлении карты доступа сотрудника / посетителя, которой выданы права доступа на контроллер (карта не заблокирована и ее сроком действия не истек). Этот параметр может быть использован в случае, если к дополнительным выходам подключена индикация, информирующая оператора о статусе предъявленной карты. Для выбора отметьте те дополнительные выходы, которые должны быть активизированы. Укажите временной критерий активизации.

Временной **Критерий активизации / нормализации**:

- **На указанное время**. Выход активизируется / нормализуется на указанное время. Отсчет времени начинается с момента предъявления карты доступа, независимо от того, будет разрешен проход или нет.
- **На время срабатывания.** Выход активизируется / нормализуется на указанное время. Отсчет времени начинается с момента разблокирования ИУ. Выход возвращается в исходное состояние при блокировании ИУ, либо по истечении **Времени удержания в разблокированном состоянии**.
- **На время срабатывания и после срабатывания.** Выбор этого параметра является комбинацией двух предыдущих. Выход активизируется / нормализуется на указанное время, начиная с момента разблокирования ИУ и до момента его блокирования, плюс указанное время, либо, если проход не был совершен, до истечения **Времени удержания в разблокированном состоянии**.

Изымать в СТОП-ЛИСТ идентификаторы ПОСЕТИТЕЛЕЙ. Функция доступна только при наличии связи контроллера с сервером системы. Параметр позволяет выбрать условие, при котором предъявленный идентификатор посетителя автоматически заносится в СТОП-лист, то есть в список идентификаторов, запрещенных к использованию:

- **Нет**. Идентификатор не заносится в СТОП-лист.
- **После любого прохода**. Идентификатор заносится в СТОП-лист при первом предъявлении.
- **После прохода в последний день действия идентификатора**. Идентификатор заносится в СТОП-лист, если дата предъявления совпадает с датой окончания срока его действия.

5.6 Параметры ресурса «Генератор тревоги»

Ресурс связан с контроллером ИУ и позволяет выделить события, которые должны приводить к генерации тревоги в контроллере, и соответствующему управлению выделенным выходом тревоги (один из релейных выходов контроллера для которого выбран **Тип: Генератор тревоги**). Для настройки ресурса доступны следующие параметры:

Генерация тревоги при предъявлении идентификатора. Параметр позволяет указать события, связанные с предъявлением идентификаторов, при регистрации которых произойдет генерация тревоги. Для каждого события есть возможность выбрать тип тревоги:

- **Нет**
- **Тихая.** Тревога генерируется, но при этом не активизируются выходы, для которых, выбран **Тип: Генератор тревоги**.
- **Громкая.** Генерируется тревога.

Генерация тревоги при несанкционированной разблокировке ИУ. Параметр позволяет для РКД *«Контроль»* и *«Закрыто»* указать, будет ли генерироваться 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 РКД *«Контроль»* указать, будет ли генерироваться 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, позволяет указать, будет ли генерироваться тревога в случае вскрытия корпуса контроллера.

5.7 Параметры ресурса «Шлейф сигнализации» (ШС)

Тип. Раскрывающийся список позволяет выбрать тип ШС:

- **Охранный** – Подключен охранный ШС.

Контроль вскрытия корпуса извещателей. При установке параметра контроллер отслеживает вскрытие корпуса извещателя ШС.

Длительность нарушения. Параметр определяет время интегрирования для ШС (70 / 300 мс), то есть максимальное время нарушения, не приводящее к переходу в режим *«ТРЕВОГА»*.

Задержка взятия на охрану. Параметр определяет время, по истечение которого контроллер предпринимает попытку взять ШС на охрану после поступления соответствующей команды. Время, определяемое значением этого параметра, может быть использовано как «задержка на выход» для ШС входных зон.

Внимание!

В версиях прошивки x.0.0.19 и старше установленное в ПО ***PERCo-S-20*** значение параметра **Задержка взятия на охрану** игнорируется и всегда считается равным **0**.

Задержка восстановления нарушенного шлейфа в снятом состоянии:

- Если для параметра установлено значение: **0**, то ШС в режиме *«СНЯТ»* не контролируется.
- В противном случае в режиме *«СНЯТ»* продолжается отслеживание состояния ШС.
  - Если ШС перейдет в состояние *«нарушение»*, то регистрируется событие *«Неисправность снятого ОШС»*. Состояние выходов ОПС не изменяется.
  - Если после этого ШС возвращается в состояние *«норма»* и продержится этом состоянии время, указанное в этом параметре, то регистрируется событие *«Нормализация снятого ОШС»*. Состояние выходов ОПС не изменяется.

5.8 Параметры ресурса «Охранная зона» (ОЗ)

Включить ИУ в зону. При установке параметра ИУ, подключенное к контроллеру будет включено в ОЗ. В РКД *«Охрана»* при регистрации события *«Взлом ИУ»* ОЗ перейдет в режим *«ТРЕВОГА»*.

Повторное включение сирены. При установке параметра активизация дополнительного выхода, для которого установлен **Тип: ОПС** и выбрана программа управления *«Сирена»,* происходит при каждом переходе ИУ или одного из ШС в состояние *«нарушение»*, даже если ОЗ уже находится в режиме *«ТРЕВОГА»*.

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

- **Тревога.** ОЗ будет переведена в режим *«ТРЕВОГА»*.
- **Автоматическое перевзятие**. Производится повторная попытка взятия на охрану до тех пор, пока постановка на охрану не произойдет.
- **Возврат в «Снята»**. ОЗ перейдет в режим *«СНЯТА»*.

Внимание!

В версиях прошивки x.x.x.19 и старше установленное в ПО ***PERCo-S-20*** значение параметра **Режим работы при невзятии** игнорируется и всегда считается равным **Возврат в «Снята»**.

Тихая тревога: При установке параметра в случае перехода ОЗ в режим *«ТРЕВОГА»* запрещена активизация дополнительных выходов, для которого установлен **Тип: ОПС** и выбрана программа управления *«Включить при тревоге»*.

Шлейфы, активизирующие зону. Параметр позволяет отметить ШС, которые будут входить в ОЗ и состояние которых будет отслеживаться контроллером в режиме ОЗ *«ОХРАНА».* В ОЗ могут входить ШС для которых выбран **Тип: Охранный**. При этом каждый ШС может входить только в одну ОЗ.

5.9 Параметры ресурса «Дополнительный вход»

Дополнительные входы контроллеров могут быть использованы для наблюдения за состоянием внешнего оборудования, подключенного к ним, и для подключения кнопки сброса тревоги, ВВУ, устройства подачи сигнала аварийной разблокировки *FireAlarm*.

Внимание!

Возможность верификации от ВВУ доступна для контроллеров с версий прошивки x.x.x.20 и старше. Обратите внимание, что при обновлении прошивки изменяется конфигурация контроллера. Потребуется повторно добавить контроллер в конфигурацию системы.

Для настройки ресурса доступны следующие параметры:

Тип. Раскрывающийся список позволяет выбрать один из следующих типов:

- **Нет.** К данному входу не подключено никакое внешнее оборудование.
- **Обычный.** К данному входу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
- **Специальный**. Предназначен для автономного сброса тревоги, выключения сирены.
- **Подтверждение от ВВУ.** Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае разрешения прохода.
- **Запрет от ВВУ.** Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае запрета прохода.

Нормальное состояние контакта (*Разомкнут / Замкнут*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

Тип: Обычный

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 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 те дополнительные выходы, которые должны быть активизированы. Укажите временной критерий активизации. Следует заметить, что активизация релейного выхода, привязанная к активизации дополнительного входа, не учитывает возможного шунтирования этого входа. Это очень важно для случаев применения в системе датчиков контроля зоны прохода.

Дополнительные выходы, нормализируемые при активизации. Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть нормализированы. 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 время.

Тип: Специальный

Сброс тревоги. Параметр определяет реакцию на получение управляющего сигнала:

- **Генератор тревоги.** При установке параметра получение управляющего сигнала на данном дополнительном входе приведет к сбросу тревоги.
- **Выход «С» ОПС.** При установке параметра получение управляющего сигнала на данном дополнительном входе приведет к выключению сирены, подключенной к выходу, работающему по программе *«Сирена»*.
- **Генератор тревоги и выход «С» ОПС.**

Тип: Подтверждение от ВВУ

Номер ИУ. Параметр задаёт номер ИУ, к которому привязывается считыватель.

Направление. Параметр задаёт направление ИУ, к которому привязывается считыватель.

5.10 Параметры ресурса «Вход FireAlarm»

Дополнительный вход **FireAlarm** предназначен для подключения устройства подачи сигнала аварийной разблокировки *FireAlarm*.

Для настройки ресурса доступны следующие параметры:

Тип. Зафиксировано значение **FireAlarm**.

Нормальное состояние контакта (*Разомкнут / Замкнут*). Параметр не доступен для редактирования для входа **FireAlarm**. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

5.11 Параметры ресурса «Дополнительный выход»

Дополнительные выходы могут быть использованы для управления любым дополнительным оборудованием в рамках системы. Для настройки ресурса доступны следующие параметры:

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 ресурса **Генератор тревоги**).
- **Генератора тревоги.** Решение об активизации дополнительного выхода принимается в соответствии с параметрами, заданными для ресурса **Генератор тревоги**.
- **ОПС.** Выход предназначен для управления световым или звуковым оповещателем, а также для передачи тревожных извещений на ПЦН при изменении режима ОЗ.

Примечание:

После включения питания все выходы нормализуются.

Нормальное состояние (*Не запитан / Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода. Для выходов №1 и № 2 нормальное состояние: **Не запитан**.

Тип: Генератор тревоги

Время активизации. Время, на которое, при наличии активизирующего управляющего воздействия, выход меняет свое состояние из нормализированного на противоположное.

Тип: ОПС

Программа управления задает логику работы контроллера по управлению этим дополнительным выходом. Инициатором активизации выхода является изменение режима ОЗ, отмеченных как **Зоны, активизирующие выход**. После возникновения события, инициирующего активизацию выхода, он активизируется. В зависимости от параметра **Программа управления** выход может быть запитан / не запитан постоянно (пока ресурс панели находится в текущем режиме), либо изменять свое физическое состояние (мигать) из нормализированного на противоположное. Нормализация выхода происходит либо по истечению времени, указанному в параметре **Время активизации** (если оно не бесконечное), либо по сбросу панели, либо после выключения ее питания.

Время активизации. Время, на которое, при наличии активизирующего управляющего воздействия, выход меняет свое состояние из нормализированного на противоположное.

Примечание:

Для программ *«ПЦН 1»* рекомендуется устанавливать **Время активизации: Бесконечно**.

Программа управления. Раскрывающийся список позволяет выбрать режим работы выхода после его активизации. Описание доступных программ управления выходом приведено в разд. 5.10.

Зоны, активизирующие выход. Параметр позволяет выбрать ОЗ, нарушение которых приведет к активизации выхода (запуску выбранной для него программы управления). Для программы *«ПЦН 1»* активизация выхода произойдет только при переходе в данный режим всех ОЗ, указанных в параметре **Зоны, активизирующие выход** (логическое «И»). Во всех остальных случаях для активизации выхода достаточно поступления сигнала об изменении режима любой из ОЗ, указанных в параметре (логическое «ИЛИ»).

Программы управления выходами

При управлении выходом отслеживается режим работы ОЗ, отмеченных в списке **Зоны, активирующие выход**. Доступны следующие программы управления выходом (см. табл. 2):

- **Включить при тревоге.** В случае перехода хотя бы одной из ОЗ в режим *«ТРЕВОГА»* выход будет активизирован на **Время активизации**.
- **ПЦН 1.** Программа для передачи тревожных извещений на ПЦН. В случае перехода всех ОЗ в режим *«ОХРАНА»* выход будет активизирован.
- **Включить при снятии.** В случае перехода хотя бы одной из ОЗ в режим *«СНЯТА»* выход будет активизирован на **Время активизации**.

Таблица 2. Режимы работы выхода «ОПС»

Название программы	ОЗ	Режим ОЗ		
		«СНЯТА»	«ОХРАНА»	«ТРЕВОГА»
«Включить при тревоге»	OR	0	0	$t_{акт}$
«ПЦН 1»	AND	0	∞	0
«Вкл. при снятии»	OR	$t_{акт}$	0	0

В столбце «ОЗ» указано условие смены режима работы выхода:

OR – для смены режима необходимо, чтобы хотя бы одна из ОЗ, отмеченных в списке **Зоны, активирующие выход,** изменила свое состояние.

AND – для смены режима необходимо, чтобы все ОЗ, отмеченные в списке **Зоны, активирующие выход**, перешли в одно и то же состояние.

В таблице указаны следующие режимы работы выхода:

0 – выход нормализован.

∞ – выход активизирован постоянно.

$t_{акт}$ – выход активизирован в течение времени, определенного параметром **Время активизации**.

6 ВОЗМОЖНОСТИ ИНТЕГРАЦИИ БИОМЕТРИЧЕСКОЙ СИСТЕМЫ *SUPREMA* С *PERCO-S-20*

В системе имеется возможность проведения интеграции с биометрическими контроллерами производства ***Suprema (BioEntry Plus*** и ***BioEntry W2)***. Предусмотрено два варианта подключения данных контроллеров к системе:

1. В качестве контроллера одностороннего замка. В этом случае ИУ подключается непосредственно к управляющему выходу контроллера ***Suprema***, связь с контроллером ***Suprema*** в системе осуществляется по интерфейсу Ethernet, соответственно, контроль зональности для данного ИУ в системе поддерживаться не будет.
2. В качестве считывателя отпечатков пальцев при управлении одним из направлений двухстороннего замка (турникета). В этом случае поддерживается контроль зональности, ИУ управляется выходами контроллера ***PERCo-CT/L04***, контроллер ***Suprema*** подключается к контроллеру ***PERCo-CT/L04*** по интерфейсу *Wiegand* через конвертер интерфейса ***PERCo-AC02*** (порядок подключения контроллеров представлен в руководствах по эксплуатации контроллера ***PERCo-CT/L04*** и конвертера интерфейса ***PERCo-AC02***).

6.1 Параметры индикации контроллеров *Suprema*

Реализована возможность настроить цветовую индикацию и звуковые сигналы контроллера ***Suprema*** для представленного списка событий:

- **Нормальное** – событие возникает в случае нормальной работы контроллера (режим работы "Контроль");
- **Считыватель заблокирован** – событие возникает в случае блокировки контроллера (режим работы "Закрыто");
- **Ошибка часов RTC (Real Time Clock)** – событие возникает в случае несовпадения внутреннего времени контроллера со временем сети;
- **Ожидание поднесения пальца** – событие возникает в случае, если был выбран тип прав доступа «Доступ по карте и пальцу» после предъявления карты;
- **Ожидание DHCP (Dynamic Host Configuration Protocol)** – событие возникает в случае ожидания получения IP-адреса от DHCP-сервера;
- **Сканирование пальца** – событие возникает в случае добавления отпечатков пальцев как идентификатора сотруднику или посетителю (если контроллер выбран как устройство для получения идентификатора);

- **Сканирование карты** – событие возникает в случае добавления карты доступа как идентификатора сотруднику или посетителю (если контроллер выбран как устройство для получения идентификатора);
- **Успешная аутентификация** – событие возникает в случае успешной идентификации;
- **Неудачная аутентификация** – событие возникает в случае ошибки идентификации.

Область **Настройка световой индикации** – отображает параметры настройки цветовой индикации контроллера для выбранного события из списка событий:

- **Подсветка** – при установке флажка для индикации выбранного события будет использоваться подсветка;
- **Бесконечно** – при установке флажка подсветка буде производиться бесконечно;
- **Количество повторов** – позволяет задать количество повторений подсветки;

Примечание:

Параметры **Бесконечно / Количество повторов** являются взаимоиcклю-чающими.

- **Цвет** – параметр позволяет выбрать цвета индикации (не более трёх);
- **Длительность** – параметр позволяет задать длительность свечения индикации тем или иным цветом;
- **Задержка** – параметр позволяет задать задержку перед началом свечения тем или иным цветом от начала цикла индикации.

Область **Настройка звуковой индикации** – отображает параметры настройки звуковых сигналов контроллера для выбранного события из списка событий:

- **Звук** – при установке флажка для индикации выбранного события будет использоваться звук;
- **Бесконечно** – при установке флажка звук будет воспроизводиться бесконечно;
- **Количество повторов** – позволяет задать количество повторений звучания;

Примечание:

Параметры **Бесконечно / Количество повторов** являются взаимо-исключающими.

- **Тон** – параметр позволяет выбрать тон звучания;
- **Длительность** – параметр позволяет задать длительность звучания индикации тем или иным тоном;
- **Задержка** – параметр позволяет задать задержку перед началом звучания индикации тем или иным тоном от начала цикла индикации.

6.2 Параметры контроллеров *Suprema*

Для контроллеров ***Suprema BioEntry Plus*** и ***BioEntry W2*** доступны для редактирования следующие параметры:

Уровень безопасности – уровень безопасности, устанавливаемый при использовании верификации по отпечатку пальца:

- Нормальный,
- Безопасный,
- Наиболее безопасный.

Примечание:

Чем выше установленный уровень безопасности – тем больше характерных точек будет считываться с отсканированного изображения папиллярных узоров при прикладывании пальца, а значит – снизится вероятность ложного срабатывания (прохода по чужому / поддельному отпечатку). Однако, чем выше установленный уровень безопасности, тем выше вероятность отказа при сканировании отпечатков. Отказы могут возникать вследствие возникновения ошибок сканирования, связанных с более высоким влиянием на процедуру сканирования влажности и температуры воздуха, загрязнённости сканируемой поверхности пальцев и т.д. В этом случае для успешной верификации потребуется повторно пройти процедуру сканирования отпечатков.

Таймаут сканирования пальца – время, которое выделяется системой на поднесение одного пальца при вводе отпечатков. Параметр может быть задан в интервале от 3 до 20 сек.

Таймаут верификации пальцем (используется в режиме доступа ***«карта и палец»***) – интервал времени, в течении которого ожидается поднесение пальца для сканирования отпечатков, при этом отсчёт времени интервала начинается после того, как была предъявлена считывателю карта доступа**.** Параметр может быть задан в интервале от 1 до 20 сек.

Таймаут поиска отпечатков – время поиска отпечатка в памяти контроллера. Если за отведенное время отпечаток не будет найден, то аутентификация будет отклонена. Параметр может быть задан в интервале от 1 до 20 сек.

Чувствительность сканера – определяет чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности – обеспечивается высокое качество и скорость сканирования, при низком заданном уровне чувствительности – уменьшается влияние факторов внешней среды (температуры и влажности воздуха, освещённости помещения, чистоты сканируемой поверхности подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию. Понижение заданного уровня чувствительности сканера осуществляется при необходимости в зависимости от условий эксплуатации. Параметр может быть задан в интервале от 1 до 7, где значение 1 – соответствует самой низкой чувствительности, а значение 7 – самой высокой.

Алгоритм поиска отпечатков – позволяет выбрать алгоритм поиска отпечатков пальца. Выбор алгоритма влияет на скорость верификации по отпечатку пальца:

- Автоматический (рекомендован производителем),
- Нормальный,
- Быстрый,
- Очень быстрый.

Выбор **алгоритма поиска отпечатков** определяет тот объём памяти контроллера, который будет выделяться для поиска совпадения отсканированного отпечатка с отпечатком в базе данных. Если в базе данных контроллера большое количество разных отпечатков, то для быстрого поиска совпадений потребуется больший объём памяти контроллера. Однако, выделение большего объёма памяти контроллера для поиска совпадений может замедлить остальные параллельно происходящие процессы поиска совпадений, например, если к контроллеру подключены несколько считывателей, на которых в этот же момент времени происходит верификация по отпечаткам пальцев.

Режим авторизации – позволяет выбрать между использованием:

- частного режима доступа (в этом случае параметры доступа устанавливаются для отдельного сотрудника / посетителя в рамках СКУД);
- общего режима доступа (в этом случае параметры доступа устанавливаются в рамках устройства и будут применяться для всех пользователей, взаимодействующих с этим устройством).

Режим доступа – определяет режим доступа при общем режиме авторизации (отображается, только если режим авторизации выставлен как «Общий»):

- **«Палец»** – для верификации требуется пройти процедуру сканирования отпечатка пальца;
- **«Карта»** – для верификации требуется предъявить считывателю карту доступа;
- **«Карта и палец»** – для верификации требуется предъявить считывателю карту доступа, после чего пройти процедуру сканирования отпечатка пальца;
- ***«*Карта или палец»** – для верификации требуется предъявить считывателю карту доступа после или пройти процедуру сканирования отпечатка пальца.

Примечание:

Параметр **Режим доступа** доступен для редактирования в случае, если выбран **Общий** режим авторизации.

Схема входных портов – позволяет назначить на входные порты «Кнопку выхода» и «Датчик прохода» («Датчик открытия \ закрытия двери»):

- Нет;
- Кнопка выхода – порт 0;
- Кнопка выхода – порт 1;
- Датчик прохода – порт 0;
- Датчик прохода – порт 1;
- Кнопка выхода – порт 0; Датчик прохода – порт 1;
- Кнопка выхода – порт 1; Датчик прохода – порт 0.

Примечание:

Категорически не рекомендуется подключать датчик прохода и кнопку выхода на один и тот же вход контроллера.

Параметры кнопки выхода (Нормальное состояние) – нормальное состояние входного порта, на который назначена «Кнопка выхода»:

- «Нормально открыто»,
- «Нормально закрыто».

Примечание:

Нормальным состоянием кнопки выхода считается то состояние, в котором находится кнопка при заблокированной двери. Соответственно, если конструктивно предусмотрено, что при нажатии кнопки выхода размыкается контакт реле и дверь разблокируется (т.е. – переходит из нормального состояния в состояние разблокировки), то необходимо из раскрывающегося списка выбрать «**Нормально закрыто**».

Параметры датчика прохода (Нормальное состояние) – нормальное состояние входного порта, на который назначен «Датчик прохода»:

- «Нормально открыто»,
- «Нормально закрыто».

Порядок байтов идентификатора карты – определяет порядок следования байтов идентификатора карты:

- От старшего байта к младшему,
- От младшего байта к старшему.

Примечание:

Нормальным состоянием датчика прохода (геркона) считается то состояние, в котором находится датчик при закрытой двери. Соответственно, если датчик прохода конструктивно расположен так, что при закрытой двери датчик нормально замкнут, то необходимо из раскрывающегося списка для датчика прохода выбрать «**Нормально закрыто**».

Настройки Wiegand (Режим) – позволяет задать режим работы контроллера ***Suprema*** по интерфейсу *Wiegand*:

- **Вход** – контроллер ***Suprema*** работает как обычный контроллер доступа;
- **Выход** – контроллер ***Suprema*** работает совместно с контроллером ***PERCo*** (может производить аутентификацию и управление замком).

Использовать аутентификацию – при установке флажка процедура аутентификации будет производится контроллером ***Suprema***. В случае успешной аутентификации данные будут переданы в контроллер ***PERCo*** (загорится зелёная индикация), в случае ошибки аутентификации данные передаваться не будут - необходимо провести успешную аутентификацию. Если флажок не выставлен, то процедура аутентификации будет производится контроллером ***PERCo***.

Управление замком – если флажок не установлен (по умолчанию), то управление замком осуществляется контроллером компании ***PERCo*** (для обычных дверей с

электромеханическим замком). Если флажок установлен, то контроллер ***Suprema*** получает возможность управлять замком (для автоматических дверей). (Обязательным условием передачи функций управления замком контроллеру ***Suprema*** является установка флажка **Использовать аутентификацию**).

Коррекция времени относительно времени сервера системы – позволяет задать коррекцию времени. Параметр может быть задан в интервале от минус 12 до плюс 14 часов.

6.3 Ресурсы ИУ (Замок)

Для ресурсов контроллера ***Suprema*** **(Замок)** доступны для редактирования следующие параметры:

Блокировать замок при закрытии двери – при установке флажка дверь будет заблокирована сразу после закрытия;

Блокировать замок по таймауту, только если дверь закрыта – при установке флажка замок будет заблокирован по истечении времени удержания в разблокированном состоянии только после закрытия двери. Если флажок не установлен – замок будет заблокирован, даже если дверь открыта.

Время удержания в разблокированном состоянии – устанавливает время, которое должно пройти от разблокировки замка до его блокировки после успешной аутентификации. За это время необходимо открыть дверь – иначе замок заблокируется. Параметр может быть задан в интервале от 1 до 30 секунд или от 1 до 15 минут;

Предельное время разблокировки – максимальное разрешенное время для нахождения двери в открытом состоянии. Если дверь не закрыть за отведенное время – будет сгенерирован сигнал тревоги. Параметр может быть задан в интервале от 1 до 30 секунд или от 1 до 15 минут;

Генерация тревоги по взлому двери – при установке флажка сигнал тревоги будет автоматически сгенерирован в случае, если был зафиксирован факт открытия двери без команды на открытие от контроллера;

Генерация тревоги по удержанию двери – при установке флажка сигнал тревоги будет автоматически сгенерирован в случае, если истекло **Предельное время разблокировки** и дверь не была закрыта;

Регистрация прохода по предъявлению идентификатора / пальца –если флажок выставлен, то считается, что проход совершен сразу после поднесения карты доступа / сканирования пальца без ожидания сигнала от датчика прохода. Если флажок не выставлен, то считается, что проход совершен после поднесения карты доступа / сканирования пальца и срабатывания датчика прохода.

7 ФУНКЦИОНИРОВАНИЕ ШС И ОЗ

При переводе ОЗ в режим «*ОХРАНА»* контроллер следит за состояниями ИУ и ШС, входящих в ОЗ. Реагируя на их изменения, контроллер может перевести ОЗ в режим *«ТРЕВОГА»* и, в зависимости от параметров конфигурации, подать команды активизации или нормализации соответствующих ресурсов.

7.1 Состояния и режимы ШС

ШС может находиться в следующих физических состояниях:

- *«нормализован»*;
- *«не нормализован» - «КЗ»* (короткое замыкание);
- *«не нормализован» - «вскрытие корпуса извещателя»*;
- *«не нормализован» - «сработал извещатель с контролем вскрытия корпуса»*;
- *«не нормализован» - «обрыв».*

ШС может находиться в следующих логических состояниях (см. табл. 3):

- *«норма»*;
- *«нарушение»*.

Поддерживаются следующие режимы ШС (см. табл. 3):
- *«ОТКЛЮЧЕН»* – мониторинг ШС не производится;
- *«СНЯТ»*;
- *«ОХРАНА»*;
- *«ТРЕВОГА»*.

Различие между логическим и физическим состояниями ШС зависят от конфигурации ШС и режима ШС:
- для режимов ШС «*ОХРАНА*» и «*ТРЕВОГА*» логические и физические состояния ШС совпадают («*нормализован*» = «*норма*» и «не *нормализован*» = «*нарушение*»);
- для режима ШС «*СНЯТ*» логическое состояние зависит от параметра конфигурации **Задержка восстановления нарушенного ШС в режиме «Снят»**:
  - если данный параметр равен 0, то логическое состояние всегда «*норма*»;
  - если данный параметр отличен от 0, то логическое состояние зависит от физического состояния:
    - если при переходе в режим ШС «*СНЯТ*» его физическое состояние «*нормализован*», то логическое состояние будет «*норма*»;
    - если при переходе в режим ШС «*СНЯТ*» его физическое состояние «не *нормализован*», то логическое состояние будет «*нарушение*»;
    - если при нахождении в режиме ШС «*СНЯТ*» его физическое состояние изменится из состояния «не *нормализован*» в состояние «*нормализован*» и продержится в таком состоянии дольше, чем установлено в параметре **Задержка восстановления нарушенного ШС в режиме «Снят»**, то логическое состояние перейдет в состояние «*норма*».

7.2 Изменение состояний и режимов ШС

Изменение состояний

Возможны следующие переходы между состояниями ШС:

1. Из состояния *«норма»* ШС, изменив свое физическое состояние, может перейти в состояние *«нарушение»* (физическое состояние – *«КЗ», «вскрытие корпуса извещателя», «сработал извещатель с контролем вскрытия корпуса», «обрыв»*).
2. При обнаружении нарушения ШС регистрируется событие *«Обнаружено нарушение ШС»*. Если при этом физическое состояние определено как *«корпус извещателя вскрыт»*, дополнительно регистрируется событие *«Корпус извещателя вскрыт»*.
3. В состоянии *«нарушение»* при изменении физического состояния с *«обрыв»* на *«сработал извещатель с контролем вскрытия корпуса»* и обратно регистрируются соответственно события *«Корпус извещателя вскрыт»* и *«Корпус извещателя закрыт»*.
4. Из состояния *«нарушение»* ШС, изменив свое физическое состояние, может перейти в состояние *«норма»*.

Изменения режимов

Возможны следующие переходы между режимами работы ШС в зависимости от его состояния и установленных параметров конфигурации. Индикация режимов работы ШС указана в разд. 10.2.

Из режима *«ОТКЛЮЧЕН»* ШС можно конфигурированием перевести в режим:
- *«СНЯТ»* с состоянием *«норма»*.
- *«СНЯТ»* с состоянием *«нарушение»*.

Примечание:

ШС находится в режиме *«ОТКЛЮЧЕН»*, если при конфигурировании в ПО:
- Для ШС установлен **Тип: Не используется**;
- ШС отмечен как **Шлейфы, активизирующие зону**, но для ОЗ установлен **Тип: Не используется**;
- ШС не отмечен как **Шлейфы, активизирующие зону** ни для одной ОЗ.

Из режима *«СНЯТ»* с состоянием *«норма»* ШС можно перевести в режимы:
- *«ОТКЛЮЧЕН»* – конфигурированием.
- *«ОХРАНА»* с состоянием *«норма»,* при постановке на охрану, если ШС нормализован
- *«СНЯТ»* с состоянием *«норма»* при попытке постановки ШС на охрану, если ШС не нормализован.

Из режима *«СНЯТ»* с состоянием *«нарушение»* ШС можно перевести в режимы:
- *«ОТКЛЮЧЕН»* – конфигурированием.
- *«СНЯТ»* с состоянием *«нарушение»* при попытке постановки ШС на охрану.

Из режима *«ОХРАНА»* с состоянием *«норма»* ШС может перейти в режимы:
- *«СНЯТ»* с состоянием *«норма»,* снятием ШС.
- *«ТРЕВОГА»* с состоянием *«нарушение»* по нарушению ШС.

Из режима *«ОХРАНА»* с состоянием *«нарушение»* ШС может перейти в режимы:
- *«ОХРАНА»* с состоянием *«норма»,* по нормализации ШС.
- *«ТРЕВОГА»* с состоянием *«нарушение»* по нарушению ШС.
- *«СНЯТ»* с состоянием *«норма»,* при снятии ШС с охраны.
- *«СНЯТ»* с состоянием *«нарушение»* при снятии ШС с охраны.

Из режима *«ТРЕВОГА»* с состоянием *«норма»* ШС может перейти в режимы:
- *«ТРЕВОГА»* с состоянием *«нарушение»* по нарушению ШС.
- *«ОХРАНА»* с состоянием *«норма»* по сбросу тревоги.
- *«СНЯТ»* с состоянием *«норма»* снятием ШС.

Из режима *«ТРЕВОГА»* с состоянием *«нарушение»* ШС может перейти в режимы:
- *«СНЯТ»* с состоянием *«норма»* при снятии ШС с охраны.
- *«СНЯТ»* с состоянием *«нарушение»* при снятии ШС с охраны.
- *«ОХРАНА»* с состоянием *«нарушение»* по сбросу тревоги.
- *«ТРЕВОГА»* с состоянием *«норма»* по восстановлению ШС (до сброса тревоги).

7.3 Режимы ОЗ

Режимы ОЗ (см. табл. 3):
- *«СНЯТА»*;
- *«ОХРАНА»*;
- *«ТРЕВОГА»*.

Режим «СНЯТА»

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

При поступлении команды взятия ОЗ на охрану поднесением карты с соответствующими правами к считывателю или от ПО начинается взятие ее на охрану. Если ИУ и все ШС данной ОЗ нормализованы, то ОЗ переходит в режим *«ОХРАНА»*. Если ИУ или хотя бы один ШС данной ОЗ нарушен, то ОЗ перейдет в режим *«СНЯТА»* и будет сформировано событие «*Попытка взятия ОЗ (невозможно взять)»* с указанием источника команды и причины невзятия.

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 ОЗ. В этом режиме ОЗ остается до получения команды снятия с охраны или до первого нарушения ИУ или ШС, входящих в ОЗ.

Режим «ТРЕВОГА»

При нарушении любого ИУ или ШС ОЗ, которой принадлежит данный ресурс, переходит в режим *«ТРЕВОГА»*, при этом формируется одно из событий, в зависимости от конфигурации параметра ОЗ: **Тихая тревога.**

- Если параметр установлен, то сформируется событие *«Тихая тревога по ОЗ»*, при этом выходы **Тип: ОПС**, работающие по программам «Включить при тревоге» активироваться не будут.
- Если параметр не установлен, то регистрируется событие *«Тревога по ОЗ»* и активизируются выходы **Тип: ОПС**, работающие по программам *«Включить при тревоге»*.

При нормализации ИУ и всех ШС режим ОЗ не меняет. Повторное нарушение ИУ или какого-либо ШС ОЗ, приведет к повторной активизации (с учетом параметра конфигурации **Тихая тревога** выходов, работающего по программе *«Сирена»*, если установлен параметр конфигурации ОЗ **Повторное включение сирены** и выход нормализован (т.е. время предыдущей активизации выхода истекло).

При поступлении команды от ПО **Сброс тревоги** ОЗ режим не меняет.

При поступлении команды снятия ОЗ с охраны поднесением карты с соответствующими правами к считывателю или от ПО, ОЗ переходит в режим *«СНЯТА»* с формированием события *«ОЗ снята с охраны»* с указанием источника команды.

Таблица 3. Режимы ОЗ

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 с охраны ОЗ, находящейся в режиме «*ОХРАНА*», ИУ и все ШС этой ОЗ снимаются, и она переходит в режим «*СНЯТА*».
	«нарушение»	При снятии с охраны ОЗ, находящейся в режимах «*ОХРАНА*» или «*ТРЕВОГА*», ИУ и все ШС этой ОЗ снимаются, и она переходит в режим «*СНЯТА*».
		Если при постановке на охрану ОЗ, находящейся в режиме «*СНЯТА*», ИУ или как минимум один из ШС этой ОЗ в состоянии «*нарушение*», то она останется в режиме «*СНЯТА*».
«ОХРАНА»	*«норма»*	Если при постановке на охрану ОЗ, находящейся в режиме «*СНЯТА*», ИУ и все ШС этой ОЗ в состоянии «*норма*», то она переходит в режим «*ОХРАНА*».
		При сбросе тревоги по ОЗ, находящейся в режиме *«ТРЕВОГА»* ИУ и все ШС которой находятся в состоянии *«норма»*, эта ОЗ переходит в режим *«ОХРАНА»* с состоянием *«норма»*.
		При нормализации ИУ и всех ШС у ОЗ, находящейся в режиме *«ОХРАНА»* с состоянием *«нарушение»*, эта ОЗ переходит в режим *«ОХРАНА»* с состоянием *«норма»*.
	«нарушение»	При сбросе тревоги по ОЗ, находящейся в режиме *«ТРЕВОГА»* с как минимум одним ИУ или 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 режиме *«ТРЕВОГА»*. При этом изменяется индикация на индикаторах ШС и регистрируется событие *«ШС нормализован»*.

ШС		Режимы ОЗ, причины переходов в данные режимы
Режим	**Состояние**	
	«нарушение»	При срабатывании ИУ или как минимум одного из ШС в ОЗ, находящейся в режиме *«ОХРАНА»*, данная ОЗ переходит в режим *«ТРЕВОГА»*

8 ФУНКЦИОНИРОВАНИЕ ДОПОЛНИТЕЛЬНЫХ ВЫХОДОВ

8.1 Выход «Обычный»

Если выход сконфигурирован как обычный, то, в зависимости от конфигурации ресурсов контроллера, к его активизации могут привести следующие управляющие воздействия:

- команда ПО (имеет бóльший приоритет относительно остальных управляющих воздействий);
- разблокировка ИУ;
- предъявление идентификаторов, имеющих статус временных (посетителей);
- предъявление идентификаторов, имеющих статус постоянных (сотрудников).

При активизации выхода регистрируется событие *«Активизация выхода»*. Время активизации выхода определяется либо при получении команды ПО, либо в соответствии с временной характеристикой соответствующего управляющего воздействия (см. конфигурацию ресурсов **ИУ** и **Считыватель**).

Если выход сконфигурирован как обычный, то, в зависимости от конфигурации ресурсов контроллера, к его нормализации могут привести следующие управляющие воздействия:

- команда ПО (имеет больший приоритет относительно остальных управляющих воздействий);
- разблокировка ИУ;
- окончание времени активизации.

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

После включения питания все выходы нормализуются не зависимо от их логического состояния на момент выключения питания. При этом, если выход на момент выключения питания был активизирован, то будет зарегистрировано событие «*Нормализация выхода*».

8.2 Выход «Генератор тревоги»

Выход типа генератора тревоги активизируется, как только возникает одно из управляющих воздействий (генерация тревоги), описанных в конфигурации, либо по команде ПО. При активизации выхода регистрируется событие «*Активизация выхода*». Нормализация выхода происходит либо по окончанию времени активизации, либо по команде ПО, либо при выключении питания. При нормализации выхода регистрируется событие «*Нормализация выхода*».

8.3 Выход «ОПС»

Любой выход, которому присвоен тип – ОПС, может быть сконфигурирован для работы под управлением определенной программы (см. конфигурацию выходов). Конфигурация выхода может быть произведена только, когда он нормализован. После конфигурации выход «готов к работе». Программа управления представляет собой набор правил для изменения физического состояния выхода в зависимости от различных событий и режимов ресурсов прибора (см. разд. 5.10).

В зависимости от программы управления выход может быть запитан / не запитан постоянно (пока ресурс контроллера находится в текущем режиме. Нормализация выхода происходит либо по истечению времени, указанному в конфигурации (если оно не бесконечное), либо по сбросу прибора, либо после выключения питания. После включения питания все выходы нормализуются не зависимо от их логического состояния на момент выключения питания. При этом, если выход на момент выключения питания был активизирован, то будет зарегистрировано событие *«Нормализация выхода»*.

При работе выхода регистрируются следующие события:

- *«Активизация выхода»* - в момент активизации выхода (окончание отсчета задержки);
- *«Нормализация выхода»* - в момент окончания работы выхода по программе управления.

Пример: Выход № 3 имеет следующую конфигурацию: **Нормальное состояние** – не запитан; **Программа управления** – *«Мигать при тревоге»;* **Маска зон** – все зоны.

После сброса либо после включения питания все выходы будут нормализованы. При переходе одной из ОЗ контроллера в режим *«ТРЕВОГА»* выход № 3 начнет работать по программе *«Включить при тревоге»*. Если во время работы выхода № 3 по программе будут переходы других ОЗ в режим *«ТРЕВОГА»*, то данные события на работу выхода № 3 влияния не окажут. Работа выхода № 3 по программе будет прекращена в следующих случаях:

- произведен сброс тревоги с ПК или с контроллера;
- выключено и затем снова включено питания контроллера;
- произведен сброс по Watchdog;
- если после выполнения указанных действий все ОЗ будут в режиме *«ОХРАНА»*.

8.4 Выход с контролем линии

Два выхода с контролем линии на КЗ и обрыв доступны для контроллера ***PERCo-CT/L04*** (*Out1* и *Out2*) в вариантах конфигурации *«Контроллер управления дверью»*.

Для этих выходов в дополнение к вышеописанной логике работы дополнительно осуществляется проверка на КЗ и обрыв. При обнаружении КЗ или обрыва на данном выходе регистрируется соответствующее событие «*КЗ на выходе»* или «*Обрыв на выходе»*. При этом выход с обнаруженным КЗ при подаче управляющего воздействия активизирован не будет. В этом случае регистрируется событие «*Активизация выхода невозможна, причина – КЗ»*. После устранения неисправности регистрируется событие «*Восстановление выхода»*.

Выходы могут использоваться для:

- подключения световых или звуковых оповещателей,
- передачи тревожных извещений на ПЦН,
- подключения другого дополнительного оборудования.

Для выходов при конфигурировании в ПО может быть выбран **Тип: ОПС**, **Генератор тревоги** или **Обычный**.

9 РКД СИСТЕМЫ

В системе предусмотрены следующие РКД:

- *«Открыто»*;
- *«Контроль»*;
- *«Охрана»*;
- *«Закрыто»*.

Примечание:

Для *«Контроллера управление двухсторонней дверью»* и *«Контроллера АТП»* смена РКД производится одновременно для обоих направлений. Для *«Контроллера управление турникетом»* РКД устанавливаются независимо для каждого направления.

9.1 РКД «Контроль»

При переходе в РКД *«Контроль»*:

- контроллер переводит ИУ в заблокированное состояние (нормализует выход управления ИУ) и удерживает его в этом состоянии до предъявления разрешенных идентификаторов или до подачи команды от ПДУ или ПО.

Переход в РКД *«Контроль»* возможен:

- По команде от ПО или Web-интерфейса из любого РКД.
- По команде от ИК-пульта из любого РКД, кроме *«Охрана»*.
- По идентификатору, имеющему право снятия с охраны из РКД *«Охрана»*.

Выход из РКД *«Контроль»* возможен:

- По команде от ПО или Web-интерфейса в любой РКД.
- По команде от ИК-пульта в любой РКД, кроме *«Охрана»*.
- По идентификатору, имеющему право постановки на охрану в РКД *«Охрана»*.

9.1.1 Алгоритм прохода по идентификатору через ИУ

При предъявлении идентификатора считывателю, он анализирует его и передает идентификационную информацию в контроллер. Действия контроллера зависят от типа подключенного ИУ и варианта конфигурации контроллера. Рассмотрим предъявление идентификатора, удовлетворяющего всем правам доступа:

Контроллер управления дверьми

1. Если датчик двери нормализован (дверь закрыта) и команды на открытие замка в направлении данного считывателя не поступало (выход управления замка нормализован), то контроллер открывает замок на **Время удержания ИУ в открытом состоянии** и передает событие мониторинга «*ИУ разблокирован»*.
2. Если до истечения **Времени удержания ИУ в открытом состоянии**:
   - не будет совершен проход (активизация датчика двери), то контроллер закроет замок. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Отказ от прохода»*.
   - будет совершен проход, то контроллер закроет замок. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Проход по идентификатору».*
   - оператор с ПДУ подаст команду на закрытие замка, то контроллер закроет замок. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Запрет прохода по команде от ПДУ».*
   - оператор от ПК подаст команду на закрытие замка, то контроллер закроет замок. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Запрет прохода по команде оператора».*
3. Если датчик двери нормализован (дверь закрыта), но ранее поступила команда на открытие в направлении данного считывателя (выход управления замка активирован), то контроллер игнорирует предъявление любого идентификатора.
4. Если датчик двери не нормализован (дверь открыта), то контроллер перезапускает **Время удержания ИУ в открытом состоянии**. Регистрируется событие «*Проход по идентификатору»*.

Контроллер управления турникетом

1. Если турникет в исходном положении и команды на открытие его в направлении данного считывателя не поступало, то контроллер открывает турникет в этом направлении на **Время удержания ИУ в открытом состоянии** и передает событие мониторинга «*ИУ разблокирован»*.
2. Если до истечения **Времени удержания ИУ в открытом состоянии**:
   - не будет совершен проход, то контроллер закроет турникет в этом направлении. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Отказ от прохода*».
   - будет совершен проход в данном направлении, то контроллер закроет турникет в этом направлении. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Проход по идентификатору».*

- оператор с ПДУ подаст команду на закрытие турникета, то контроллер закроет турникет. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Запрет прохода по команде от ДУ».*
- оператор от ПК подаст команду на закрытие турникета в данном направлении, то контроллер закроет турникет в этом направлении. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Запрет прохода по команде оператора».*

3. Если турникет в исходном положении, но ранее поступила команда на открытие в направлении данного считывателя (турникет в направлении данного считывателя открыт), то контроллер игнорирует предъявление любого идентификатора в направлении данного считывателя.
4. Если через турникет начат проход в направлении данного считывателя, то контроллер поставит данный идентификатор в очередь и приступит к выполнению действий по нему после завершения этого прохода.
5. Если до завершения прохода предъявлен другой идентификатор, то идентификатор, находящийся в очереди, меняется на предъявленный.

Контроллер АТП

Внимание!

При отсутствии датчиков проезда могут возникнуть проблемы со временем проезда (либо кто-то не успеет, либо после кого-то долго не закроется).

1. Если датчик проезда нормализован и команды на открытие ИУ не поступало (выход управления ИУ нормализован), то контроллер открывает ИУ на **Время удержания ИУ в открытом состоянии** и передает событие мониторинга «*ИУ разблокирован»*.
2. Если до истечения **Времени удержания ИУ в открытом состоянии**:
   - Не будет совершен проезд (активизация датчика проезда), то контроллер закроет ИУ. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Отказ от прохода»*.
   - Будет совершен проезд, то контроллер закроет ИУ. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Проход по идентификатору».*
   - Оператор с ПДУ даст команду на закрытие ИУ, то контроллер закроет ИУ. Передает события мониторинга «*ИУ заблокирован»* и регистрирует событие «*Запрет прохода по команде от ДУ».*
   - Оператор от ПК даст команду на закрытие ИУ, то контроллер закроет ИУ. Передает событие мониторинга «*ИУ заблокирован»* и регистрирует событие «*Запрет прохода по команде оператора».*
3. Если поступила команда на открытие в любом направлении, то контроллер игнорирует предъявление любого идентификатора к любому считывателю.
4. При отсутствии датчика проезда и при установке параметра **Отсутствие датчика проезда** факт проезда фиксируется при разрешении проезда (активизации выхода управления ИУ), при этом ИУ закрывается по истечении **Времени удержания ИУ в открытом состоянии** или по соответствующей команде оператора с ПДУ или ПК.

9.1.2 Предъявление идентификатора с нарушением прав доступа

Предъявление идентификатора с нарушением единых права доступа

При предъявлении в РКД *«Контроль»* идентификатора с нарушением единых прав доступа регистрируются следующие события мониторинга и регистрации (в зависимости от параметров ресурса **Генератор тревоги** событие может вызывать генерацию тревоги):

- Если предъявленного идентификатора нет в списке данного контроллера, то *«Предъявление невалидной карты, Идентификатор не зарегистрирован»*,
- Если у предъявленного идентификатора установлен статус «заблокирован», то *«Предъявление невалидной карты, Идентификатор запрещен»*,

- Если предъявленный идентификатор помещен в «СТОП-лист», то *«Предъявление невалидной карты, Идентификатор из СТОП-листа»*,
- Если у предъявленного идентификатора истек срок действия, то *«Предъявление невалидной карты, Идентификатор просрочен»*.

Предъявление идентификатора с нарушением персональных прав доступа

При предъявлении в РКД *«Контроль»* идентификатора с нарушением персональных прав доступа регистрируются следующие события мониторинга и регистрации (в зависимости от параметров ресурса **Генератор тревоги** событие может вызывать генерацию тревоги):

- Если предъявлен идентификатор с нарушением критерия доступа по времени, то «Н*есоответствие временным критериям доступа»,*
- Если предъявлен идентификатор с нарушением функции контроля зональности (Antipass), то «*Несоответствие текущему местоположению»,*
- Если предъявлен идентификатор с нарушением времени и зональности, то «*Несоответствие временным критериям доступа и текущему местоположению».*

Действия контроллера зависят от параметров ресурса контроллера **Считыватель** соответственно **Контроль времени для идентификаторов** и **Защита от передачи идентификаторов** в РКД *«Контроль»:*

- Если установлено значение **Мягкий контроль**, то контроллер производит действия в соответствии с разд. 9.1.1, и регистрируется событие «*Проход по идентификатору с несоответствием временным критериям доступа / текущему местоположению».*

- Если установлено значение **Жесткий контроль**, то действия контроллера зависят от параметра **Подтверждение разрешения прохода** (или верификации от ПО) для данного считывателя:

– Если параметр не установлен, то регистрируется событие «*Запрет прохода, несоответствие временным критериям доступа / текущему местоположению»*.
– Если параметр установлен, то контроллер в зависимости от типа и состояния ИУ:
  - *«Контроллер управления дверью»*, датчик двери не нормализован (дверь открыта). Контроллер регистрирует событие «*Проход по идентификатору с несоответствием временным критериям / текущему местоположению доступа и при отказе в подтверждении прохода от верификации»;*
  - Все остальные по разд. 9.1.1 – контроллер передает запрос разрешения прохода с нарушением времени и ждет ответа от верифицирующего устройства. Если до истечения **Времени ожидания подтверждения при верификации** устройства для данного считывателя:
    - не придет подтверждения на разрешение прохода от верифицирующего устройства либо придет запрет прохода, либо будет нажата кнопка **Stop**, то регистрируется событие «*Запрет прохода, отказ в подтверждении прохода от верификации»*;
    - придет подтверждение на разрешение прохода от верифицирующего устройства, то контроллер производит действия в соответствии с разд. 9.1.1, и регистрируется событие «*Проход с подтверждением от верификации с несоответствием временным критериям доступа / текущему местоположению»*;
    - произойдет открывание двери до прихода подтверждения от верифицирующего устройства (например, при проходе по другому считывателю), то контроллер регистрирует событие «*Проход по идентификатору с несоответствием временным критериям доступа / текущему местоположению и при отказе в подтверждении прохода от верификации».*

9.1.3 Доступ при установленных дополнительных параметрах

При задании прав доступа идентификатору можно установить дополнительные параметры: комиссионирование, верификация или одновременное выполнение обоих действий. Если дополнительные параметры доступа не установлены, то проход по идентификатору происходит согласно разд. 9.1.1.

Для описания отличий от вышеописанных вариантов прохода из-за наличия дополнительных параметров введем два понятия:

- карта №1 – идентификатор, удовлетворяющий всем критериям доступа;
- карта №2 – идентификатор, входящий в список комиссионирующих карт данного контроллера;

Доступ с комиссионированием

Поднести карту №1, контроллер в зависимости от типа и состояния ИУ:

1. *«Контроллер управления дверью»:* ИУ – замок, датчик двери не нормализован (дверь открыта). Контроллер регистрирует событие «*Проход по идентификатору, нарушение комиссионирования»*;
2. Все остальные типы: контроллер: перейдет в состояние «*Ожидание комиссионирования»*, если до истечения времени удержания ИУ в открытом состоянии:
   - карта №2 поднесена не будет, то контроллер снимет данное состояние и регистрирует событие «*Запрет прохода, нарушение комиссионирования»*;
   - будет поднесена карта отличная от карты №2, то передается событие мониторинга «*Предъявление карты*, *нарушение комиссионирования»*, снимет данное состояние и регистрирует событие «*Запрет прохода, нарушение комиссионирования»*;
   - произойдет открывание двери (например, при проходе по другому считывателю), то контроллер снимет данное состояние и регистрирует событие «*Проход по идентификатору, нарушение комиссионирования»*;
   - будет поднесена карта №2, то контроллер производит действия в соответствии с разд. 9.1.1;

Доступ с верификацией

Поднести карту №1, контроллер в зависимости от типа и состояния ИУ:

1. *«Контроллер управления дверью»:* ИУ – замок, датчик двери не нормализован (дверь открыта). Контроллер регистрирует событие «*Проход по идентификатору, при отказе в подтверждении прохода от верификации»*;
2. Все остальные типы: контроллер перейдет в состояние «*Ожидание верификации»*, если до истечения времени ожидания подтверждения от верифицирующего устройства для данного считывателя;
   - Не придет подтверждения на разрешение прохода от верифицирующего устройства либо придет запрет прохода, либо будет нажата кнопка **Stop**, то контроллер регистрирует событие *«Запрет прохода, отказ в подтверждении прохода от верификации»*;
   - Будет поднесена любая карта, то она будет игнорирована;
   - Произойдет открывание двери (например, при проходе по другому считывателю), то контроллер регистрирует событие «*Проход по карте при отказе в подтверждении прохода от верификации»*.
   - Придет подтверждение на разрешение прохода от верифицирующего устройства, то контроллер производит действия в соответствии с разд. 9.1.1, но вместо события «*Проход по карте»* будет зафиксировано событие «*Проход с подтверждением от верификации»*;

Доступ с комиссионированием и верификацией

В случае если одновременно установлены параметры доступа с комиссионированием и верификацией, то первым должно выполняться комиссионирование, а затем верификация.

9.1.4 Реакции на предъявление карты, если контроллер находится в процессе обработки предъявленного ранее идентификатора

1. Ожидание прохода по разрешенному идентификатору и предъявление другого идентификатора к этому же считывателю:
   - если по данному идентификатору может быть разблокировано ИУ. Контроллер игнорирует предъявление данного идентификатора;

- если по данному идентификатору не может быть разблокировано ИУ. Регистрируются события мониторинга и регистрации о предъявлении идентификатора, с указанием нарушения.

2. Ожидание прохода по разрешенному идентификатору и предъявление другого идентификатора к другому считывателю:
   - если по данному идентификатору не может быть разблокировано ИУ. Регистрируются события мониторинга и регистрации о предъявлении идентификатора, с указанием нарушения;
   - если по данному идентификатору может быть разблокировано ИУ – контроллер разблокирует ИУ:
     - для *«Контроллера управления дверьми»* – перезапуская **Время удержания в разблокированном состоянии**;
     - для *«Контроллера управления турникетом»* – разблокируется второе направление прохода;
     - для *«Контроллера АТП»* – контроллер игнорирует предъявление данного идентификатора;
3. Ожидание комиссионирования и предъявление карты, не являющейся комиссионирующей, к этому же считывателю. Передается событие мониторинга «*Предъявление карты (№ карты)*, *нарушение комиссионирования».* Снимется ожидание комиссионирования и регистрируется событие «*Запрет прохода (№ карты), нарушение комиссионирования»*.
4. Ожидание комиссионирования и предъявление другого идентификатора к другому считывателю:
   - если по данному идентификатору не может быть разблокировано ИУ – регистрируется событие мониторинга и регистрации о предъявлении идентификатора, с указанием нарушения;
   - если по данному идентификатору может быть разблокировано ИУ – контроллер разблокирует ИУ:
     - для *«Контроллера управления дверьми»* – при открытии двери контроллер снимет ожидание комиссионирования и регистрирует событие «*Проход по идентификатору (№), нарушение комиссионирования»* и событие прохода по второму идентификатору;
     - для *«Контроллера управления турникетом»* – разблокируется второе направление прохода;
     - для *«Контроллера АТП»* – контроллер игнорирует предъявление идентификатора;
5. Ожидание верификации и предъявление другого идентификатора к этому же считывателю – контроллер игнорирует предъявление данного идентификатора.
6. Ожидание верификации и поднесении другого идентификатора к другому считывателю:
   - если по данному идентификатору не может быть разблокировано ИУ, регистрируется событие мониторинга и регистрации о предъявлении идентификатора с указанием нарушения;
   - если по данному идентификатору может быть разблокировано ИУ – контроллер разблокирует ИУ:
     - для замка – при открытии двери контроллер снимет ожидание верификации и регистрирует событие «*Проход по идентификатору при отказе в подтверждении прохода от верификации (с № ожидавшей верификации)»* плюс проход по второй карте (для *«Контроллера управления дверьми»*);
     - для турникета – разблокируется второе направление прохода (для *«Контроллера управления турникетом»*);
     - АТП – контроллер игнорирует предъявление данного идентификатора (для *«Контроллера АТП»*).

9.2 РКД «Охрана»

РКД *«Охрана»* доступен для *«Контроллеров управления дверьми».* РКД устанавливается и снимается контроллером автоматически соответственно при успешной постановке и снятии с охрану ОЗ, в которую входит ИУ.

При переходе в РКД *«Охрана»:*

- контроллер переводит ИУ в закрытое состояние (нормализирует выход управления ИУ) и удерживает его в этом состоянии до смены РКД;
- нажатие кнопки ДУ *«Выход»* игнорируется;
- при открывании двери контроллер регистрирует событие «*Несанкционированный проход через ИУ (взлом ИУ)»* и, при задании соответствующих параметров, включает сигнал тревоги.

Переход в РКД *«Охрана»* возможен:

- по команде от ПО или Web-интерфейса из любого РКД;
- по карте доступа, имеющей право постановки на охрану из РКД *«Контроль»* или *«Открыто»*.

Выход из РКД *«Охрана»* возможен:

- по карте доступа, имеющей право снятия с охраны в предыдущий РКД, если это были РКД *«Контроль»* или *«Открыто»*, либо в РКД *«Контроль»*, если предыдущий РКД был *«Закрыто»* (т.е. РКД *«Охрана»* был установлен из ПО);
- по команде от ПО или Web-интерфейса в любой РКД.

9.2.1 Постановка на охрану

При постановке на охрану ОЗ, ее ресурсы ставятся в определенной последовательности: первым на охрану ставится ресурс ИУ, затем ШС.

Индикация факта постановки на охрану ОЗ без ИУ возможна только через назначение соответствующей программы для релейных выходов.

Постановка на охрану картой доступа

Постановка на охрану ОЗ с помощью карты доступа возможна только при закрытой двери из РКД *«Открыто»* и РКД *«Контроль»*.

Для постановки на охрану ОЗ надо дважды предъявить одну и ту же карту доступа, не совершая при этом прохода. При этом карте должно быть выдано право постановки на охрану данной ОЗ, и она должна удовлетворять всем критериям доступа (временным и пространственным).

Внимание!

При постановке на охрану картой доступа ИУ с механическим автовзводом (режим работы выхода управления ИУ установлен **Импульсный**) после первого поднесения карты ИУ будет разблокирован, поэтому для сброса автовзвода данное ИУ, в течение не более 4 секунд после второго поднесения карты, необходимо открыть и снова закрыть.

При первом предъявлении карты ИУ будет разблокировано. Если до истечения **Времени удержания ИУ в разблокированном состоянии**:

- не будет ни прохода, ни повторного предъявления этой же карты, то контроллер закроет ИУ (только для РКД работы *«Контроль»*) и снимет данное состояние (с регистрацией события «*Отказ от прохода»*).
- будет совершен проход через ИУ, то контроллер закроет ИУ (только для РКД *«Контроль»*) и снимет данное состояние (с регистрацией события *«Проход по карте»).*
- будет повторное поднесение этой же карты, то контроллер закроет ИУ и начнет постановку отдельных ресурсов ОЗ на охрану в нижеприведенной последовательности:
  - ресурс ИУ:

- если ИУ нормализовано, или будет нормализовано не позже, чем через 4 секунды (дверь, оборудованную замком с механическим автовзводом, для этого необходимо будет открыть и снова закрыть), то оно перейдет в режим *«ОХРАНА»*, с регистрацией события *«Взят на охрану»*; далее контроллер перейдет к постановке ресурса ШС;
- если по истечении 4 секунд ИУ не будет нормализовано, то оно перейдет в режим *«СНЯТ»*, с регистрацией события *«Снят»* – контроллер вернется в исходный РКД (с индикацией на 1 секунду состояния *«Невзятие»* и регистрацией события «*Попытка взятия ОЗ (невозможно взять) по идентификатору, нарушение состояния ресурса ИУ»*);

- ресурс ШС (если ни один ШС не входит в ОЗ, то после постановки на охрану ресурса ИУ, ОЗ перейдет в режим *«ОХРАНА»* с регистрацией события «*ОЗ взята на охрану по идентификатору»*):
  - если все ШС входящие в ОЗ нормализованы (в состоянии *«норма»*), то каждый из них перейдет в режим *«ОХРАНА»*, с регистрацией события *«Взят на охрану»*. ОЗ перейдет в режим *«ОХРАНА»* с регистрацией события «*ОЗ взята на охрану по идентификатору»*;
  - если хотя бы один ШС не нормализован (в состоянии *«нарушение»*), то ИУ перейдет в режим *«СНЯТ»*, с регистрацией события *«Снят с охраны»*, контроллер вернется в исходный РКД (с индикацией на 1 секунды состояния *«Невзятие»* и регистрацией события «*Попытка взятия ОЗ (невозможно взять) по идентификатору, нарушение состояния ресурса ШС»*).

Примечание:

Алгоритм постановки на охрану ОЗ по команде ПО аналогичен постановке на охрану ОЗ с помощью карты доступа с момента повторного поднесения карты.

9.2.2 Снятие с охраны

Снятие с охраны картой доступа

Для снятия с охраны ОЗ надо предъявить карту, имеющую право снятия с охраны данной ОЗ. После этого каждый ресурс ОЗ перейдет в режим *«СНЯТ»* (с регистрацией события *«Снят»*), ОЗ перейдет в режим *«СНЯТА»* (с регистрацией события *«ОЗ снята с охраны по идентификатору»)*, а ИУ будет разблокировано.

Контроллер сменит РКД *«Охрана»* на РКД, который был установлен до постановки на охрану (*«Контроль»* или *«Открыто»*), за исключение РКД *«Закрыто»*, в этом случае контролер перейдет в РКД *«Контроль»*.

После этого в случае прохода регистрируется событие «*Проход по карте»*, в случае отказа от прохода событие «*Отказ от прохода»*.

Снятие с охраны по команде от ПО

При получении команды от ПО **Снять с охраны**, каждый ресурс ОЗ перейдет в режим *«СНЯТ»* (с регистрацией события *«Снят с охраны»*), ОЗ перейдет в режим *«СНЯТА»* (с регистрацией события «*ОЗ снята с охраны по команде оператора»*).

При снятии с охраны ОЗ с ИУ контроллер сменит РКД *«Охрана»* на РКД, который был установлен до постановки на охрану, за исключением РКД *«Закрыто»*, в этом случае контроллер перейдет в РКД *«Контроль»*.

ОЗ с ИУ можно также снять с охраны, передав одну из команд изменения РКД. В этом случае контролер перейдет в указанный РКД, а каждый ресурс ОЗ и сама ОЗ будут сняты с охраны так же, как и по команде **Снять с охраны**.

9.2.3 Постановка и снятие с охраны при установленных дополнительных параметрах

При задании прав доступа карты для постановки на охрану и снятия с охраны можно также установить дополнительные параметры: комиссионирование, верификация или одновременно обе эти параметра.

При заданном параметре доступа *«комиссионирование»* после повторного поднесения карты контроллер перейдет в состояние *«Ожидание комиссионирования»* с соответствующей индикацией. Для завершения процедуры постановки на охрану или снятия с охраны, необходимо до истечения **Времени удержания ИУ в разблокированном состоянии** предъявить комиссионирующую карту (карта, входящая в список комиссионирующих карт данного контроллера). Если такая карта предъявлена не будет, то процедура постановки / снятия будет прервана, с регистрацией соответствующего события: либо «*Попытка взятия ОЗ на охрану (невозможно взять) по идентификатору, нарушение комиссионирования»,* либо «*Попытка снятия ОЗ с охраны (невозможно снять) по идентификатору, нарушение комиссионирования».*

При заданном параметре доступа *«верификация»* после повторного поднесения карты контроллер перейдет в состояние *«Ожидание верификации»* с соответствующей индикацией. Для завершения процедуры постановки на охрану или снятия с охраны, контроллер должен до истечения **Времени ожидания подтверждения при верификации** получить такое подтверждение от верифицирующего устройства.

Если подтверждение получено не будет, то процедура постановки / снятия будет прервана, с регистрацией соответствующего события: либо «*Попытка взятия ОЗ на охрану (невозможно взять) по идентификатору, отказ в подтверждении взятия»,* либо «*Попытка снятия ОЗ с охраны (невозможно снять) по идентификатору, отказ в подтверждении снятия».*

В случае если одновременно установлены параметры доступа комиссионирование и верификация, первым должно выполняться условие комиссионирования и затем верификации.

В случае если контроллер находится в РКД *«Контроль»*, а дополнительные параметры доступа (комиссионирование, верификация) заданы не только для постановки на охрану или снятия с охраны ОЗ, но и для доступа, то сначала выполняются действия необходимые для получения доступа (предъявление комиссионирующей карты, получение подтверждения от верифицирующего устройства).

9.3 РКД «Открыто»

При переходе в РКД *«Открыто»:*

- контроллер переводит ИУ в открытое состояние (активизирует выход управления ИУ) и удерживает его в этом состоянии до смены РКД.
- нажатие кнопок ПДУ (кнопки ДУ *«Выход»*) игнорируется.

Переход в РКД *«Открыто»* возможен:

- по команде от ПО или Web-интерфейса из любого режима работы;
- по команде от ИК-пульта из любого РКД, кроме *«Охрана»;*
- по карте, имеющей право снятия с охраны, если режим предшествовал РКД *«Охрана»*.

Выход из РКД *«Открыто»* возможен:

- по команде от ПО или Web-интерфейса в любой РКД;
- по команде от ИК-пульта в любой РКД, кроме *«Охрана»*;
- по карте, имеющей право постановки на охрану, в РКД *«Охрана»*;

Предъявление идентификатора с нарушением единых прав доступа

При предъявлении в РКД *«Открыто»* идентификатора с нарушением единых прав доступа регистрируются следующие события мониторинга и регистрации (в зависимости от параметров ресурса **Генератор тревоги** событие может вызывать генерацию тревоги):

- если предъявленного идентификатора нет в списке данного контроллера, то *«Предъявление невалидной карты, Идентификатор не зарегистрирован»*;
- если у предъявленного идентификатора установлен статус «заблокирован», то *«Предъявление невалидной карты, Идентификатор запрещен»*;
- если предъявленный идентификатор помещен в «СТОП-лист», то *«Предъявление невалидной карты, Идентификатор из СТОП-листа»*;

- если у предъявленного идентификатора истек срок действия, то *«Предъявление невалидной карты, Идентификатор просрочен»*.

Предъявление идентификатора с нарушением персональных прав доступа

При предъявлении в РКД *«Открыто»* идентификатора с нарушением персональных прав доступа регистрируются следующие события мониторинга и регистрации (в зависимости от параметров ресурса **Генератор тревоги** событие может вызывать генерацию тревоги):

- если предъявлен идентификатор с нарушением критерия доступа по времени, то «*Предъявление идентификатора, несоответствие временным критериям доступа»*;
- если предъявлен идентификатор с нарушением функции контроля зональности (Antipass), то «*Несоответствие текущему местоположению»*;
- если предъявлен идентификатор с нарушением времени и зональности, то «*Несоответствие временным критериям доступа и текущему местоположению».*

Предъявление идентификатора при установленном дополнительном параметре «комиссионирование»

При предъявлении в РКД *«Открыто»* идентификатора с установленным дополнительным параметром доступа «*комиссионирование*»:

- то регистрируется событие «*Проход по идентификатору с нарушением комиссионирования»*;
- если при этом идентификатор предъявлен с нарушением временного критерия доступа, то регистрируется событие «*Проход по идентификатору с несоответствием временным критериям доступа и с нарушением комиссионирования»*;
- если при этом идентификатор предъявлен с нарушением зональности, то регистрируется событие «*Проход по идентификатору с несоответствием текущему местоположению и с нарушением комиссионирования»*;
- если при этом идентификатор предъявлен с нарушением временного критерия доступа и зональности, то регистрируется событие «*Проход по идентификатору с несоответствием временным критериям доступа и текущему местоположению и с нарушением комиссионирования»*.

9.4 РКД «Закрыто»

При установке в РКД *«Закрыто»*:

- контроллер переводит ИУ в заблокированное состояние (нормализирует выход управления ИУ) и удерживает его в этом состоянии до смены РКД;
- нажатие кнопок ПДУ (кнопки ДУ *«Выход»*) игнорируется;
- по предъявлению любого идентификатора регистрируется событие «*Предъявление запрещенного идентификатора, нарушение РКД»*;
- при механическом открытии ИУ регистрируется событие «*Несанкционированный проход через ИУ (взлом ИУ)»* (при задании соответствующих параметров может генерироваться тревога).

Переход в РКД *«Закрыто»* возможен:

- по команде от ПО или Web-интерфейса из любого РКД;
- по команде ИК-пульта из любого РКД, кроме *«Охрана»*.

Выход из РКД *«Закрыто»* возможен:

- по команде от ПО или Web-интерфейса в любой РКД;
- по команде ИК-пульта в любой РКД, кроме *«Охрана»*;
- если РКД *«Закрыто»* был установлен от ИК-пульта, то при открывании ИУ происходит возврат в предыдущий РКД.

Примечание:

Особенности РКД *«Закрыто»* в случае установки с ИК-пульта:

- управление от ПДУ не блокируется;
- управление с ИК-пульта по кнопке *«Посетитель»* не блокируется;
- при открытии ИУ происходит возврат к предыдущему РКД.

10 ИНДИКАЦИЯ

10.1 Индикация РКД, событий и состояний контроллера

Индикация РКД, состояний и реакций контроллера на предъявление идентификатора осуществляется на блоках индикации. Наличие и расположение блока индикации зависит от типа и модели контроллера и ИУ. Возможные варианты индикации представлены в табл. 4.

Таблица 4. Индикация контроллера *PERCo*

<table>
<tr><th colspan="2" rowspan="2">Предъявление карты</th><th rowspan="2">РКД</th><th colspan="4">Индикаторы</th></tr>
<tr><th>Зеленый</th><th>Желтый</th><th>Красный</th><th>Звук (сек.)</th></tr>
<tr><td colspan="2">Отсутствие конфигурации</td><td>Нет</td><td>5 Гц</td><td>5 Гц</td><td>5 Гц</td><td>выкл.</td></tr>
<tr><td colspan="2" rowspan="4">Нет</td><td>«Открыто»</td><td>вкл.</td><td>выкл.</td><td>выкл.</td><td>выкл.</td></tr>
<tr><td>«Контроль»</td><td>выкл.</td><td>вкл.</td><td>выкл.</td><td>выкл.</td></tr>
<tr><td>«Охрана»[1]</td><td>выкл.</td><td>1 Гц</td><td>1Гц</td><td>выкл.</td></tr>
<tr><td>«Закрыто»</td><td>выкл.</td><td>выкл.</td><td>вкл.</td><td>выкл.</td></tr>
<tr><td colspan="2" rowspan="3">Карта не имеет прав доступа</td><td>«Открыто»</td><td>вкл.</td><td>выкл.</td><td>выкл.</td><td>0,5</td></tr>
<tr><td>«Контроль»</td><td rowspan="3">выкл.</td><td rowspan="3">выкл.</td><td rowspan="3">вкл.</td><td rowspan="3">1</td></tr>
<tr><td>«Охрана»</td></tr>
<tr><td colspan="2">Любая карта</td><td>«Закрыто»</td></tr>
<tr><td colspan="2" rowspan="3">Карта имеет право доступа</td><td>«Открыто»</td><td rowspan="2">вкл.</td><td rowspan="2">выкл.</td><td rowspan="2">выкл.</td><td rowspan="2">0,5</td></tr>
<tr><td>«Контроль»</td></tr>
<tr><td>«Охрана»</td><td>выкл.</td><td>выкл.</td><td>вкл.</td><td>1</td></tr>
<tr><td colspan="2" rowspan="3">Карта имеет права доступа и постановки / снятия с охраны</td><td>«Открыто»</td><td rowspan="3">вкл.</td><td rowspan="3">выкл.</td><td rowspan="3">выкл.</td><td rowspan="3">0,5</td></tr>
<tr><td>«Контроль»</td></tr>
<tr><td>«Охрана» [2]</td></tr>
<tr><td rowspan="3">Повторное поднесение карты с правом постановки на охрану</td><td>При взятии (переход в РКД «Охрана»)</td><td>«Охрана»</td><td>выкл.</td><td>1 Гц</td><td>1Гц</td><td>0,5</td></tr>
<tr><td rowspan="2">При невзятии[3] (до возврата в исходный РКД)</td><td>«Открыто»</td><td rowspan="2">выкл.</td><td rowspan="2">выкл.</td><td rowspan="2">1сек</td><td rowspan="2">1</td></tr>
<tr><td>«Контроль»</td></tr>
<tr><td colspan="2">Ожидание верификации / комиссионирования</td><td>Любой</td><td>выкл.</td><td>2 Гц</td><td>выкл.</td><td>0,5</td></tr>
</table>

Примечания:

При считывании идентификатора в любом РКД подается звуковой сигнал длительностью 0,5 с, желтый световой индикатор меняет свое состояние на 0,5 сек. Состояние других индикаторов не меняется.

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

[1] РКД *«Охрана»* доступен для контроллеров ***PERCo-CL05***, ***PERCo-CL201*** и ***PERCo-CT/L04*** в варианте конфигураций *«Управление дверьми»*.

[2] При предъявлении в РКД *«Охрана»* карты доступа, имеющей право снятия с охраны происходит: снятие ОЗ, включающей ИУ с охраны и разблокировка ИУ на **Время удержания в разблокированном состоянии**. После истечения этого времени ИУ переход в РКД, установленный до взятия ОЗ на охрану (*«Открыто»* или *«Контроль»*, если предыдущий РКД был *«Закрыто»*, то в РКД *«Контроль»)*.

[3] Звуковая и световая индикация включается на 1 сек.

10.2 Индикация режимов и состояний ШС

Индикация состояния ШС осуществляется для имеющего в своем составе ШС контроллера ***PERCo-CT/L04***. Индикация осуществляется на индикаторах *«ШС1»* и *«ШС2»,* расположенные на передней панели корпуса контроллера. Возможны следующие виды индикации:

Таблица 5. Индикация состояния ШС

Режим ШС	Состояние ШС	Состояние светового индикатора
«ОТКЛЮЧЕН»	-	Не горит
«СНЯТ»	*«Норма»*	Горит желтым.
	«Нарушение»	Мигание желтым с частотой 2 Гц.
«ОХРАНА»	*«Норма»*	Горит зеленым.
	«Нарушение»	Горит зеленым цветом, кратковременно прерываясь красным (1,875 с / 0,125 с).
«ТРЕВОГА»	*«Норма»*	Изменение цвета индикатора желтый / красный с частотой 2 Гц.
	«Нарушение»	Мигание красным с частотой 2 Гц.

ПРИЛОЖЕНИЯ

Приложение 1. Методика составления инструкций по постановке ОЗ на охрану

Пошаговая инструкция для персонала по постановке на охрану ОЗ, а также ответная реакция контроллера, индикация считывателей могут различаться в зависимости от состава конкретной ОЗ, параметров конфигурации самих ресурсов, наличия или отсутствия дополнительных параметров доступа (верификации, комиссионирования). Поэтому окончательную, подробную инструкцию для персонала рекомендуется составлять после определения конфигурации контроллера уже с учетом влияния всех выше перечисленных факторов.

Примечание:

Дополнительную индикацию факта постановки на охрану можно организовать с помощью дополнительных устройств оповещения, подключенных к релейным выходам (при задании соответствующих установок для них при конфигурации).

Ниже приводятся примеры инструкции постановки на охрану ОЗ (см. также разд. 9.2.1).

Последовательность действий сотрудника и ответная реакция контроллера при постановке ОЗ на охрану

1. Постановка на охрану ОЗ, в которую входит ИУ

Постановка на охрану возможна только при закрытой двери.

Постановка на охрану возможна, если контроллер находится в РКД *«Контроль»* (горит желтый индикатор) или *«Открыто»* (горит зеленый индикатор).

Для постановки ОЗ на охрану надо дважды предъявить одну и ту же карту, не совершая при этом прохода:

1.1. Предъявите карту:

- в РКД *«Контроль»* – контроллер разблокирует замок, на считывателе появится индикация *«Разрешение прохода»* – непрерывно горящий зеленый индикатор, и прозвучит звуковой сигнал длительностью 0,5 секунды.
- в РКД *«Открыто»* – на считывателе останется индикация *«Разрешение прохода»* – непрерывно горящий зеленый индикатор.

1.2. Не совершая прохода через дверь, в течение времени, пока на считывателе горит указанная индикация (подставьте время из установленного в параметре **Время анализа карты**), повторно предъявите эту же карту – контроллер заблокирует замок, далее:
- для замка с потенциальным управлением – на считывателе появится индикация РКД *«Охрана»* – попеременно мигающие желтый и красный индикаторы.
- для замка с импульсным управлением – на считывателе останется предыдущая индикация:
  - в случае если до истечения 4-х секунд дверь будет открыта и снова закрыта, на считывателе появится индикация РКД *«Охрана»* – попеременно мигающие желтый и красный индикаторы.
  - в случае если до истечения 4-х секунд дверь не будет открыта, контроллер возвратится в исходный режим работы с соответствующей индикацией и состоянием замка.

2. Последовательность действий при постановке ОЗ на охрану с комиссионированием

Постановка на охрану ОЗ с ИУ, установлена функция *комиссионирование* при переводе в РКД *«Охрана»*.

Постановка на охрану возможна только при закрытой двери. Постановка на охрану возможна, если ИУ находится в РКД *«Контроль»* (горит желтый индикатор) или *«Открыто»* (горит зеленый индикатор).

Для постановки ОЗ на охрану надо дважды предъявить одну и ту же карту, не совершая при этом прохода, после второго предъявления карты необходимо предъявить комиссионирующую карту.

2.1. Предъявите карту. Закрытый ранее замок разблокируется и на считывателе появится индикация разрешения прохода – непрерывно горящий зеленый индикатор.
2.2. Не совершая прохода через дверь, в течение времени, пока на считывателе горит указанная индикация (подставьте время из установленного в параметре **Время анализа карты**), повторно предъявите эту же карту, на считывателе появится индикация ожидания комиссионирования – мигающий желтый индикатор.
2.3. Предъявите комиссионирующую карту. Если такая карта предъявлена не будет, то процесс постановки на охрану будет прерван и индикация на считывателе вернется в исходное состояние. После предъявления комиссионирующей карты контроллер заблокирует замок, далее смотри п. 1.2.

3. Последовательность действий при постановке ОЗ на охрану с верификацией

Постановка на охрану ОЗ с ИУ, установлен дополнительном параметр доступа «*верификация»* при постановке на *«Охрану»*.)

Постановка на охрану возможна только при закрытой двери.

Постановка на охрану возможна, если ИУ находится в РКД *«Контроль»* (горит желтый индикатор) или *«Открыто»* (горит зеленый индикатор).

Для постановки ОЗ на охрану надо дважды предъявить одну и ту же карту, не совершая при этом прохода, после второго предъявления карты дождаться подтверждения от компьютера.

3.1. Предъявите карту. Закрытый ранее замок разблокируется и на считывателе появится индикация разрешения прохода – непрерывно горящий зеленый индикатор.
3.2. Не совершая прохода через дверь, в течение времени, пока на считывателе горит указанная индикация (подставьте время из установленного в параметре **Время анализа карты**), повторно предъявите эту же карту, на считывателе появится индикация *«Ожидание верификации»* – мигающий желтый индикатор.
3.3. Если в течение заданного времени подтверждения от компьютера не будет, то процесс постановки на охрану будет прерван и индикация на считывателе вернется в исходное состояние. После получения подтверждения от компьютера контроллер заблокирует замок, далее смотри п.1.2.

Приложение 2. События, регистрируемые контроллерами

События, связанные с функционированием

Тип события		Мн	Рг	Примечания
Включение питания	-	-	+	
Выключение питания	-	-	+	
Нарушение связи	-	-	+	Отключение от локальной сети
Восстановление связи	-	-	+	Подключение к локальной сети
Переполнение журнала регистрации	-	+	+	Переполнение журнала фиксируется после заполнения в памяти контроллера предпоследней свободной страницы журнала (размер 1-й страницы равен 32 событиям).
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.
Сбой физического уровня Ethernet	-	-	+	
Очистка журнала регистрации	-	+	+	Очистка журнала происходит всегда после чтения переполненного журнала регистрации.
Перезапуск контроллера	-	-	+	Программный сброс контроллера (после перепрошивки или форматирования памяти, либо после первого обнаружения фатальной неисправности)
Неисправность контроллера	*(память FRAM)*	+	+/-	Фатальная неисправность – отказ ЭРЭ платы прибора
	(память DataFlash)	+	+/-	
	(часы RTC)	+	+/-	
	(шина I2C)	+	+/-	
Форматирование памяти	-	+	+	Форматирование памяти прибора
Корпус прибора открыт	-	+	+	Может вызывать или нет генерацию тревоги (в зависимости от параметров генератора тревоги)
Корпус прибора закрыт	-	+	+	
Изменение режима работы по команде оператора	*(режим «Открыто»)*	+	+	Изменение любого РКД по команде оператора.
	(режим «Контроль»)	+	+	
	(режим «Совещание»)	+	+	
	(режим «Закрыто»)	+	+	
	(режим «Охрана»)	+	+	
Изменение режима работы по команде ИК-пульта	*(режим «Открыто»)*	+	+	Изменение любого РКД по команде ИК-пульта (только для контроллера ***PERCo-CT/L04***).
	(режим «Контроль»)	+	+	
	(режим «Совещание»)	+	+	
	(режим «Закрыто»)	+	+	
Тревога по команде ИК-пульта	-	+	+	Нажата кнопка «Вызов» на ИК-пульте (только для контроллера ***PERCo-CT/L04***).
Изменение режима работы на режим «Охрана» по идентификатору	-	+	+	Постановка на охрану ОЗ, включающую ИУ, с помощью карты доступа.

Тип события		Мн	Рг	Примечания
Изменение режима работы с режима «Охрана» на режим	*«Открыто» по идентификатору*	+	+	Снятие с охраны ОЗ, в которую входит ИУ, с помощью карты доступа, с переходом в РКД, который был установлен до постановки на охрану с помощью карты доступа.
	«Контроль» по идентификатору	+	+	
	«Совещание» по идентификатору	+	+	
Неисправность ИП	-	+	+	Напряжение питания более 14.7 В, или напряжение питания менее 10.5 В
Восстановление ИП	-	+	+	Напряжение питания находится в диапазоне 10.5 – 14.7 В
Тревога	-	+	+	От генератора тревоги
Сброс тревоги	-	+	+	По команде от ПО
Автономный сброс тревоги	-	+	+	Сброс тревоги ОПС при сбросе прибора кнопкой, определенной для сброса тревоги
Тестирование прибора начато	-	+	+	Переход прибора в режим - *«Тестирование прибора»* по команде ПО
Тестирование прибора завершено успешно	-	+	+	Переход прибора в дежурный режим по завершению самодиагностики. Фатальных неисправностей не выявлено.
Тестирование прибора выявило неисправности	-	+	+	Переход прибора в дежурный режим по завершению самодиагностики. Фатальные неисправности выявлены.
Тестирование ШС начато	-	+	+	Переход прибора в режим - *«Тестирование ШС»* по команде ПО
Тестирование ШС завершено	-	+	+	Переход прибора в дежурный режим по команде ПО
Неисправность ИП +18В	-	+	+	Выход напряжения питания ШС за рабочий диапазон
Восстановление ИП +18В	-	+	+	Напряжения питания ШС в норме
Пропадание связи с контроллером 2-го уровня	-	+	+	Пропадание связи с ***PERCo-CL201*** по RS-485
Восстановление связи с контроллером 2-го уровня	-	+	+	Восстановление связи с ***PERCo-CL201*** по RS-485
Неисправность контроллера 2-го уровня	-	+	+	
Восстановление после неисправности контроллера 2-го уровня	-	+	+	

События, связанные с состояниями входов и выходов

Тип события	Мн	Рг	Примечания
Активизация входа	+	+	
Нормализация входа	+	+	
Активизация выхода	+	+	
Нормализация выхода	+	+	
Запуск задержки активизации выхода	+	+	Начат отчет задержки перед запуском программы управления выходом
КЗ на выходе	+	+	Обнаружено КЗ в шлейфе, подключенном к выходу оповещения

Обрыв на выходе	+	+	Обнаружен обрыв в шлейфе, подключенном к выходу оповещения
Активизация выхода невозможна, причина - КЗ	+	+	При активизации выхода оповещения обнаружено КЗ в подключенном к нему шлейфе
Восстановление выхода	+	+	Обнаружено восстановление шлейфа, подключенного к выходу оповещения после КЗ или обрыва

События, связанные с изменениями состояний ОЗ

Тип события		Мн	Рг	Примечания
ОЗ взята на охрану по идентификатору	-	+	+	ОЗ перешла в режим *«ОХРАНА»*, по карте с соответствующими правами. Данное событие сопровождается событием *«Изменение режима работы на режим «Охрана» по идентификатору*»
ОЗ снята с охраны по идентификатору	-	+	+	ОЗ перешла в режим *«СНЯТА»*, по предъявлению карты с соответствующими правами. Данное событие сопровождается событием *«Изменение режима работы на режим «ххх» по идентификатору*», где «ххх» – тот режим работы, в который будет осуществлен переход
Попытка взятия ОЗ (невозможно взять) по идентификатору	*нарушение состояния ресурса ИУ*	+	+	ИУ в состоянии *«нарушение»* при взятии ОЗ
	нарушение состояния ресурса ШС	+	+	ШС в состоянии *«нарушение»* при взятии ОЗ.
	нарушение комиссионирования	+	+	В процессе постановки ОЗ на охрану было зафиксировано несоответствие с комиссионирующей картой или комиссионирование не было выполнено вообще
	отказ в подтверждении взятия от верификации	+	+	В процессе постановки ОЗ на охрану не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет
	несоответствие временных критериев доступа	+	+	Предъявленная карта с правами постановки ОЗ на охрану является нарушителем по времени
	несоответствие текущему местоположению	+	+	Предъявленная карта с правами постановки ОЗ на охрану является нарушителем по зональности
	несоответствие временным критериям доступа и текущему местоположению	+	+	Предъявленная карта с правами постановки ОЗ на охрану является нарушителем и по времени и зональности
	отказ от постановки	+	+	В процессе постановки ОЗ на охрану карта не была поднесена повторно до истечения времени удержания ИУ в открытом состоянии
Попытка снятия ОЗ (невозможно снять) по идентификатору	*нарушение комиссионирования*	+	+	В процессе снятия ОЗ с охраны было зафиксировано несоответствие с комиссионирующей картой или комиссионирование не было выполнено вообще

Тип события		Мн	Рг	Примечания
	отказ в подтверждении снятия от верификации	+	+	В процессе снятия ОЗ с охраны не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет
	несоответствие временных критериев доступа	+	+	Предъявленная карта с правами снятия ОЗ с охраны является нарушителем по времени
	несоответствие текущему местоположению	+	+	Предъявленная карта с правами снятия ОЗ с охраны является нарушителем по зональности
	несоответствие временным критериям доступа и текущему местоположению	+	+	Предъявленная карта с правами снятия ОЗ с охраны является нарушителем и по времени и зональности
ОЗ взята на охрану по идентификатору с подтверждением	-	+	+	ОЗ перешла в режим *«ОХРАНА»* по карте с соответствующими правами и с подтверждением от верифицирующего устройства. Данное событие будет сопровождаться событием *«Изменение режима работы на режим «Охрана» по идентификатору»*
ОЗ снята с охраны по идентификатору с подтверждением	-	+	+	ОЗ перешла в режим *«СНЯТА»* по карте с соответствующими правами и с подтверждением от верифицирующего устройства. Данное событие будет сопровождаться *событием «Изменение режима работы на режим «ххх» по идентификатору»*, где «ххх» – тот режим работы, в который будет осуществлен переход
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»*
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 «ххх» по команде оператора»*, где «ххх» – тот режим работы, в который будет осуществлен переход
Попытка взятия ОЗ (невозможно взять) по команде оператора	*нарушение состояния ресурса ИУ*	+	+	ИУ в состоянии «нарушение» при взятии ОЗ
	нарушение состояния ресурса ШС	+	+	ШС в состоянии «нарушение» при взятии ОЗ.
Тихая тревога по ОЗ	-	+	+	ОЗ перешла в режим *«ТРЕВОГА»*,
Тревога по ОЗ	-	+	+	ОЗ перешла в режим *«ТРЕВОГА»*,
Сброс тревоги по ОЗ	-	+	+	

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

Тип события	Мн	Рг	Примечания
ИУ взят на охрану	+	+	ИУ перешел в режим *«ОХРАНА»*
ШС взят на охрану	+	+	ШС перешел в режим *«ОХРАНА»*
ИУ снят с охраны	+	+	ИУ перешел в режим *«СНЯТ»*,
ШС снят с охраны	+	+	ШС перешел в режим *«СНЯТ»*,
Неисправность снятого ШС	+	+	Нарушение ШС в режиме *«СНЯТ»*, если параметр конфигурации ШС **Задержка восстановления нарушенного ШС в режиме «Снят»** отличен от нуля
Нормализация снятого ШС	+	+	Восстановление ранее нарушенного ШС в режиме *«СНЯТ»*, если параметр конфигурации ШС **Задержка восстановления нарушенного ШС в режиме «Снят»** отличен от нуля
Нарушение ИУ, режим ТРЕВОГА	+	+	ИУ перешел в режим *«ТРЕВОГА»*
Нарушение ШС, режим ТРЕВОГА	+	+	ШС перешел в режим *«ТРЕВОГА»*,
Нарушение ШС, режим ТРЕВОГА с опцией тихая	+	+	ШС перешел в режим *«ТРЕВОГА»*,
Нарушение ШС в режиме ТРЕВОГА	+	+	Повторное нарушение ШС в режиме *«ТРЕВОГА»*
Восстановление ШС в режиме ТРЕВОГА	+	+	Восстановление ранее нарушенного ШС в режиме *«ТРЕВОГА»*
Сброс тревоги ИУ	+	+	При снятии ОЗ с охраны или командой **Снять тревогу** от ПО
Сброс тревоги ШС	+	+	При снятии ОЗ с охраны или командой **Снять тревогу** от ПО
ШС отключен	+	+	При удалении конфигурации ШС
Корпус извещателя вскрыт	+	+	
Корпус извещателя закрыт	+	+	

События, связанные с проходами через ИУ по карте доступа

Тип события		Мн	Рг	Примечания
Предъявление невалидной карты	*Идентификатор не зарегистрирован*	+	+	Может вызывать или нет генерацию тревоги (в зависимости от параметров генератора тревоги)
	Идентификатор запрещен	+	+	
	Идентификатор из «стоп-листа»	+	+	
	Идентификатор просрочен	+	+	
Предъявление карты	*несоответствие временным критериям доступа*	+	-	Может вызывать или нет генерацию тревоги (в зависимости от параметров генератора тревоги)
	несоответствие текущему местоположению	+	-	
	несоответствие временным критериям доступа и текущему местоположению	+	-	

Тип события		Мн	Рг	Примечания
Запрет прохода	-	-	+	
	по команде оператора	-	+	После того, как контроллер разрешил проход, оператор с ПК подал команду на запрет прохода
	по команде от ДУ	-	+	После того, как контроллер разрешил проход, оператор с ПДУ подал команду *«Запрет прохода»*
	от ВВУ	+	+	После того, как контроллер разрешил проход, подтверждение от внешнего верифицирующего устройства не было получено.
	несоответствие временным критериям доступа	-	+	Предъявленная карта является нарушителем по времени (вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги)
	несоответствие текущему местоположению	-	+	Предъявленная карта является нарушителем зональности (вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги)
	несоответствие временным критериям доступа и текущему местоположению	-	+	Предъявленная карта является нарушителем и по времени и зональности (вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги)
	нарушение комиссионирования	+	+	Несоответствие с комиссионирующей картой или комиссионирование не было выполнено вообще (вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги)
	отказ в подтверждении прохода от верификации		+	Не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет
Предъявление запрещенной карты - нарушение РКД	-	+	+	Предъявление любой карты в режиме работы *«Закрыто»* или предъявлению в режиме работы *«Охрана»* карты, которая не имеет права автономного снятия с охраны ОЗ с ИУ (вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги)
Отказ от прохода	-	-	+	Отказ от предоставленного системой права пройти через ИУ по карте
	нет ответа от ВВУ	+	+	Истекло время ожидания подтверждения. При этом подтверждение от ВВУ не было получено.

Тип события		Мн	Рг	Примечания
Проход по идентификатору	-	-	+	Проход через ИУ, произошедший после предоставления контроллером права пройти через него и до истечения времени удержания ИУ в открытом состоянии
	с несоответствием временным критериям доступа	-	+	Событие возникает только у контроллеров замка при предъявлении карты с каким-либо нарушением, либо карты, требующей комиссионирования / верификации в двух случаях: либо при предъявлении при открытом замке, либо если замок будет открыт по какой-либо внешней причине до окончания времени анализа карты по данному предъявлению
	с несоответствием текущему местоположению	-	+	
	несоответствие временным критериям доступа и текущему местоположению	-	+	
	с нарушением комиссионирования	-	+	
	с несоответствием временным критериям доступа и с нарушением комиссионирования	-	+	
	с несоответствием текущему местоположению и с нарушением комиссионирования	-	+	
	несоответствие временным критериям доступа и текущему местоположению и с нарушением комиссионирования	-	+	
	при отказе в подтверждении прохода от верификации	-	+	
	с несоответствием временным критериям доступа и при отказе в подтверждении прохода от верификации	-	+	
	с несоответствием текущему местоположению и при отказе в подтверждении прохода от верификации	-	+	
	несоответствие временным критериям доступа и текущему местоположению и при отказе в подтверждении прохода от верификации	-	+	

Тип события		Мн	Рг	Примечания
Проход с подтверждением от ДУ	-	-	+	Проход через ИУ, совершенный после предоставления контроллером с подтверждением от ПДУ права доступа и до истечения времени удержания ИУ в разблокированном состоянии. Подтверждение от ПДУ осуществляется при условии, что верифицирующее устройство не определено и установлен параметр доступа с верификацией
	с несоответствием временным критериям доступа	-	+	
	с несоответствием текущему местоположению	-	+	
	несоответствие временным критериям доступа и текущему местоположению	-	+	
Проход с подтверждением от верификации	-	-	+	Проход через ИУ, произошедший после предоставления контроллером с подтверждением от верифицирующего устройства права пройти через него и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от верифицирующего устройства осуществляется при условии, что верифицирующее устройство определено и установлен параметр доступа с верификацией
	с несоответствием временным критериям доступа	-	+	
	с несоответствием текущему местоположению	-	+	
	несоответствие временным критериям доступа и текущему местоположению	-	+	
Проход, подтверждение от ВВУ	-	-	+	Проход через ИУ, произошедший после подтверждения от внешнего верифицирующего устройства
ИУ не закрыто после прохода по идентификатору	-	+	+	После прохода по карте время активизации состояния контакта ИУ превысило установленное предельное время разблокировки

События, связанные с проходами через ИУ без предъявления карты доступа

Тип события	Мн	Рг	Примечания
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 ИУ в открытом состоянии
Проход по команде от ПК	-	+	Проход через ИУ, произошедший после предоставления контроллером по команде от ПК права пройти через него и до истечения времени удержания ИУ в открытом состоянии
Несанкционированный проход через ИУ (взлом ИУ)	+	+	Активизация состояния контакта заблокированного ИУ
ИУ не закрыто после прохода от ДУ	+	-	Время активизации состояния контакта ИУ по команде от ДУ превысило установленное предельное время разблокировки
ИУ не закрыто после прохода от ПК	+	-	Время активизации состояния контакта ИУ по команде от ПК превысило установленное предельное время разблокировки
ИУ разблокирован	+	-	Изменение текущего состояния контакта ИУ
ИУ заблокирован	+	-	
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 ИУ в открытом состоянии

События, связанные с интеграцией контроллеров *Suprema*

События биометрической системы и контроллеров	
Биометрический считыватель	**Описание**
Успешная верификация по пальцу	Событие происходит при успешной верификации по отпечатку пальца.
Успешная верификация по карте	Событие происходит при поднесении корректной карты.
Успешная верификация по карте и пальцу	Событие приходит при поднесении корректной карты и верификации карты отпечатком пальца.
Неудачная верификация, некорректная карта	Событие приходит при поднесении карты, которой нет в базе контроллера.
Неудачная верификация, некорректный палец	Событие приходит при поднесении пальца, которого нет в базе контроллера, если установлен режим доступа "Карта и палец", и требуется верифицировать поднесенную карту сканированием отпечатка пальца.
Верификация по тревожному пальцу	Событие приходит при успешной верификации по отпечатку пальца, который помечен как тревожный.
Верификация по карте и тревожному пальцу	Событие приходит при поднесении корректной карты и верификации карты тревожным отпечатком пальца.
Успешная идентификация по пальцу	Событие приходит при поднесении корректного пальца.
Неудачная идентификация, некорректный палец	Событие приходит при поднесении пальца, которого нет в базе данных контроллера.
Идентификация по тревожному пальцу	Событие приходит при поднесении тревожного пальца.
Неудачная аутентификация, некорректный режим доступа	Событие приходит при поднесении корректной карты / пальца, но при несоответствии режима доступа. Например, поднесение карты при режиме доступа "Палец".
Неудачная аутентификация, некорректные личные данные	Событие приходит при поднесении корректной карты / пальца, но при несоответствии режима доступа. Например, поднесение карты при режиме доступа "Палец".
Неудачная аутентификация, время вышло	Событие приходит при использовании режима доступа "Палец и карты", если поднести карту и не верифицировать её пальцем за отведенное время.
Доступ запрещен, учетная запись не удовлетворяет критериям доступа	Событие приходит при поднесении карты / пальца учетной записи, доступ которой запрещен в данный момент. Например, график сотрудника не позволяет находиться на территории в данный момент времени.
Доступ запрещен, учетная запись заблокирована	Событие приходит при поднесении карты / пальца заблокированной учетной записи.
Доступ запрещен, истек срок действия учетной записи	Событие приходит при поднесении карты / пальца учетной записи, срок действия которой вышел.
Биометрический считыватель	**Описание**
Перезагрузка устройства	Перезагрузка устройства.
Старт работы устройства	Старт работы устройства.
Установка времени устройства	Установка времени устройства.
Установка временной зоны устройства	Установка временной зоны устройства.
Установлено соединение по LAN	Установка соединения с контроллером.
Разрыв соединения по LAN	Разрыв соединения с контроллером.

IP-адрес выделен DHCP	Выделение IP-адреса устройству, для получения события в сетевых настройках контроллера должна быть установлена автоматическая выдача адресов.
Экран заблокирован	Блокировка сканера пальца для аутентификации.
Экран разблокирован	Разблокировка сканера пальца для аутентификации.
Связь по RS-485 заблокирована	Блокировка связи по RS-485.
Связь по RS-485 разблокирована	Разблокировка связи по RS-485.
Установлено соединение по TCP	Установка соединения с контроллером по TCP.
Разрыв соединения по TCP	Разрыв соединения с контроллером по TCP.
Установлено соединение по RS-485	Установка соединения с контроллером по RS-485.
Разрыв соединения по RS-485	Разрыв соединения с контроллером по RS-485.
Вход устройства активирован	Активизация входа устройства.
Устройство или периферия удалены	Потеря связи с устройством.
Соединение с устройством или периферией восстановлено	Восстановление связи с устройством.
Очистка лога устройства	Очистка лога событий.
Обновление прошивки устройства	Обновление прошивки устройства.
Обновление ресурса	Обновление ресурса.
Системная информация инициализирована	Инициализация системной информации.
База данных инициализирована	Инициализация базы данных.
Заводская конфигурация инициализирована	Инициализация заводской конфигурации.
Вход пожарной сигнализации активирован	Активизация входа пожарной сигнализации. Чтобы получить событие необходимо настроить один из входных портов устройства как "Вход пожарной сигнализации".
Включение пожарной сигнализации	Включение пожарной сигнализации. Чтобы получить событие необходимо настроить один из входных портов устройства как "Вход пожарной сигнализации".
Сброс пожарной сигнализации	Сброс пожарной сигнализации. Чтобы получить событие необходимо настроить один из входных портов устройства как "Вход пожарной сигнализации".
Замок	**Описание**
Замок разблокирован	Замок разблокирован с самым низким приоритетом.
Замок разблокирован в соответствии с графиком	Замок разблокирован с приоритетом "график". В случае, когда замок разблокируется с этим приоритетом приходит событие "Замок разблокирован".
Замок разблокирован оператором	Замок разблокирован с приоритетом "оператор". В случае, когда замок разблокируется с этим приоритетом приходит событие "Замок разблокирован".
Экстренная разблокировка замка	Замок разблокирован с приоритетом "экстренно". В случае, когда замок разблокируется с этим приоритетом приходит событие "Замок разблокирован".
Замок заблокирован	Замок заблокирован с самым низким приоритетом.
Замок заблокирован в соответствии с графиком	Замок заблокирован с приоритетом "график". В случае, когда замок блокируется с этим приоритетом приходит событие "Замок заблокирован".

Замок заблокирован оператором	Замок заблокирован с приоритетом "оператор". В случае, когда замок блокируется с этим приоритетом приходит событие "Замок заблокирован".
Экстренная блокировка замка	Замок заблокирован с приоритетом "экстренно". В случае, когда замок блокируется с этим приоритетом приходит событие "Замок заблокирован".
Дверь открыта	Событие приходит, когда меняется состояние датчика двери на "Открыто". Для этого его необходимо предварительно настроить.
Дверь закрыта	Событие приходит, когда меняется состояние датчика двери на "Закрыто". Для этого его необходимо предварительно настроить.
Взлом двери	Событие приходит при взломе двери.
Удержание двери	Событие приходит при удержании двери в открытом состоянии дольше разрешенного времени.
Тревога, при взломе двери	Событие приходит при подъеме тревоги по взлому двери.
Сброс тревоги, при взломе двери	Событие приходит при сбросе тревоги по взлому двери.
Тревога, при удержании двери	Событие приходит при подъеме тревоги по удержанию двери.
Сброс тревоги, при удержании двери	Событие приходит при сбросе тревоги по удержанию двери.
Команда на сброс состояния замка	Событие приходит, когда дана команда на сброс состояния замка с самым низким приоритетом.
Команда на сброс состояния замка, приоритет - график	Событие приходит, когда дана команда на сброс состояния замка с приоритетом "график".
Команда на сброс состояния замка, приоритет - оператор	Событие приходит, когда дана команда на сброс состояния замка с приоритетом "оператор".
Команда на сброс состояния замка, приоритет - экстренно	Событие приходит, когда дана команда на сброс состояния замка с приоритетом "экстренно".
Команда на блокировку замка	Событие приходит, когда дана команда на блокировку замка с самым низким приоритетом.
Команда на блокировку замка, приоритет - график	Событие приходит, когда дана команда на блокировку замка с приоритетом "график".
Команда на блокировку замка, приоритет - оператор	Событие приходит, когда дана команда на блокировку замка с приоритетом "оператор".
Команда на блокировку замка, приоритет - экстренно	Событие приходит, когда дана команда на блокировку замка с приоритетом "экстренно".
Команда на разблокировку замка	Событие приходит, когда дана команда на разблокировку замка с самым низким приоритетом.
Команда на разблокировку замка, приоритет - график	Событие приходит, когда дана команда на разблокировку замка с приоритетом "график".
Команда на разблокировку замка, приоритет - оператор	Событие приходит, когда дана команда на разблокировку замка с приоритетом "оператор".
Команда на разблокировку замка, приоритет - экстренно	Событие приходит, когда дана команда на разблокировку замка с приоритетом "экстренно".
Биометрическая система	**Описание**
Переполнение журнала регистрации	Переполнение журнала регистрации.
Внутренняя ошибка	Событие об ошибке в работе биометрической системы.
Конфигурация установлена	Конфигурация записана в контроллер.
Временные параметры установлены	Графики и праздники записаны в контроллер.

Служебные события S-20	
Контроллер	**Описание**
Нарушение ресурса	Событие происходит, если контроллер присутствует в системе ***PERCo S-20***, а в биометрической системе отсутствует.
Восстановление ресурса	Событие происходит, если было нарушение ресурса, и он был добавлен в биометрическую систему.
Биометрический считыватель	**Описание**
Проход после успешной верификации по пальцу	Генерируется, если был совершен проход после верификации по пальцу.
Проход после успешной верификации по карте	Генерируется, если был совершен проход после верификации по карте.
Проход после успешной верификации по карте и пальцу	Генерируется, если был совершен проход после верификации по карте и пальцу.
Проход после успешной идентификации пальцу	Генерируется, если был совершен проход после идентификации по пальцу.
Отказ от прохода после успешной верификации по пальцу	Генерируется, если проход не был совершен после верификации по пальцу.
Отказ от прохода после успешной верификации по карте	Генерируется, если проход не был совершен после верификации по карте.
Отказ от прохода после успешной верификации по карте и пальцу	Генерируется, если проход не был совершен после верификации по карте и пальцу.
Отказ от прохода после успешной идентификации пальцу	Генерируется, если проход не был совершен после идентификации по пальцу.
Установлен режим работы "Открыто"	Генерируется, если была успешно выполнена команда "Установить режим работы "Открыто"".
Установлен режим работы "Контроль"	Генерируется, если была успешно выполнена команда "Установить режим работы "Контроль"".
Установлен режим работы "Закрыто"	Генерируется, если была успешно выполнена команда "Установить режим работы "Закрыто"".
Проход после верификации по тревожному пальцу	Генерируется, если был совершен проход после верификации по тревожному пальцу.
Проход после верификации по карте и тревожному пальцу	Генерируется, если был совершен проход после верификации по карте и тревожному пальцу.
Проход после идентификации по тревожному пальцу	Генерируется, если был совершен проход после идентификации по тревожному пальцу.
Отказ от прохода после верификации по тревожному пальцу	Генерируется, если проход не был совершен после верификации по тревожному пальцу.
Отказ от прохода после верификации по карте и тревожному пальцу	Генерируется, если проход не был совершен после верификации по карте и тревожному пальцу.
Отказ от прохода после идентификации по тревожному пальцу	Генерируется, если проход не был совершен после идентификации по тревожному пальцу.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ООО «ПЭРКо»

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

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

Техническая поддержка:

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

Тел.: (812) 247-04-55

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

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

Кор. 01.11.2018

www.perco.ru

тел: 8 (800) 333-52-53