

**СИСТЕМА КОНТРОЛЯ
И УПРАВЛЕНИЯ ДОСТУПОМ
PERCo-SYSTEM-12000**

**Техническое
описание**

СОДЕРЖАНИЕ:

1. ВВЕДЕНИЕ	4
1.1. Основные термины и обозначения.....	4
2. НАЗНАЧЕНИЕ И СОСТАВ СИСТЕМЫ	8
2.1. Устройство контроллеров	10
2.1.1. Устройство концентратора и контроллера-концентратора.....	10
2.1.1.1. Контроллер управления доступом	10
2.1.1.2. Кронштейн с индикаторами.....	10
2.1.1.3. Плата менеджера питания	11
2.1.2. Устройство замкового контроллера.....	11
2.1.3. Подключения к концентратору и контроллеру-концентратору	13
2.2. Состав программного обеспечения	13
2.3. Состав ТКД.....	15
3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ СИСТЕМЫ.....	15
3.1. Основные технические характеристики концентратора и контроллера-концентратора	15
3.2. Основные технические характеристики замкового контроллера	16
4. ОПИСАНИЕ РАБОТЫ СИСТЕМЫ	16
4.1. Конфигурация системы.....	16
4.1.1. Ресурсы терминала контроля доступа и параметры их функционирования..	17
4.1.1.1. Релейный выход.....	17
4.1.1.2. Тестовый вход.....	17
4.1.1.3. Исполнительный механизм	18
4.1.1.4. Считыватель	19
4.1.1.5. Служебный выход	19
4.1.1.6. Генератор тревоги.....	20
4.2. Функционирование системы	20
4.2.1 Принципы функционирования аппаратуры	21
4.2.1.1 Принципы функционирования концентратора (контроллера- концентратора)	21
4.2.1.2 Принципы функционирования замкового контроллера	22
4.2.2 Права доступа и режим контроля доступа.....	23
4.2.3. Временные критерии доступа	25
4.2.4. Мониторинг и регистрация.....	26
4.2.4.1. Перечень возможных событий мониторинга и причины их формирования.....	26
4.2.4.2. Перечень возможных событий регистрации и причины их формирования.....	28
4.2.5. Перемещения персонала. Интерфейс пользователя	29
4.2.6. Диагностика состояния системы и ее элементов. Диагностические индикаторы	30
Приложение 1	31
Приложение 2.....	33

1. ВВЕДЕНИЕ

Настоящее Техническое описание предназначено для ознакомления с техническими характеристиками, составом и принципом работы системы контроля и управления доступом PERCo-SYSTEM-12000 (в дальнейшем — "система") с целью обеспечения правильной эксплуатации и наиболее полного использования всех ее технических возможностей. Техническое описание действует совместно с Инструкцией по монтажу на систему контроля и управления доступом PERCo-SYSTEM-12000, Инструкцией по монтажу на подсистему замковых контроллеров системы контроля и управления доступом PERCo-SYSTEM-12000, а также с паспортами на устройства, входящие и подключаемые к системе.

1.1. ОСНОВНЫЕ ТЕРМИНЫ И ОБОЗНАЧЕНИЯ

- **Сервер системы** — IBM-совместимый персональный компьютер с установленным на нем модулем ПО "Сервер системы", предназначенный для осуществления физической и логической связи между остальными модулями ПО и системными контроллерами.

- **Считыватель** — устройство, предназначенное для считывания и расшифровки кода, содержащегося в карте доступа, с целью идентификации пользователей в системе.

- **Контрольный считыватель (CR-12001)** — устройство, предназначенное для считывания и расшифровки кода, содержащегося в карте доступа, с целью автоматической регистрации пропусков в системе и контроля их работоспособности. Контрольный считыватель подключается к компьютеру с установленным ПО "Отдел кадров".

- **Концентратор (PERCo-SC-12200P)** — унифицированный системный контроллер, предназначенный для управления доступом посредством управления замковыми контроллерами подсистемы второго уровня PERCo-CL-12200 (до 15-ти на один концентратор) через драйвер связи PERCo-DN-12201, регистрации проходов и поддержки функций охранно-пожарной сигнализации. Входящий в состав концентратора менеджер питания управляет питанием периферии и зарядом встроенного резервного аккумулятора.

- **Базовый контроллер-концентратор (PERCo-SC-12300P)** — унифицированный системный контроллер, предназначенный для управления доступом, регистрации проходов, управления драйверами исполнительных устройств, управления замковыми контроллерами подсистемы второго уровня (PERCo-CL-12200, через драйвер связи PERCo-DN-12201) и поддержки функций охранно-пожарной сигнализации. Он поддерживает все функции концентратора PERCo-SC-12200P и дополнительно позволяет управлять драйверами исполнительных механизмов. Входящий в состав базового контроллера-концентратора менеджер питания управляет питанием периферии и зарядом встроенного резервного аккумулятора.

- **Замковый контроллер (PERCo-CL-12200)** — контроллер, подключаемый к концентратору или контроллеру-концентратору через драйвер связи PERCo-DN-12201 и предназначенный для организации доступа через двери и поддержки функций охранно-пожарной сигнализации, а так же для управления доступом и регистрации проходов в аварийном режиме работы. Для считывания кода бесконтактных карт доступа (далее по тексту карт) могут использоваться выносные антенны или стандартные считыватели с выходным форматом Wiegand 26 или ABA Track 2. Для считывания кода магнитных карт используются стандартные считыватели с выходным форматом ABA Track 2.

- **Терминал контроля доступа (ТКД)** — комплекс технических средств, предназначенный для решения задач контроля доступа в пределах одной структурно-логической составляющей системы. Обязательно включает в себя базовый контроллер-концентратор как минимум с одним драйвером исполнительного механизма или замковый контроллер PERCo-CL-12200.

- **Драйвер связи** (PERCo-DN-12201) — аппаратный модуль системы, предназначенный для организации линии связи между концентратором/контроллером-концентратором и замковыми контроллерами PERCo-CL-12200.

- **Драйвер турникета** (PERCo-DT-12301) — аппаратный модуль системы, предназначенный для:

- управления одной стойкой турникета-трипода типа PERCo-T-04W;
- контроля направления вращения преграждающих планок;
- обслуживания одного пульта управления PERCo-H-05/2;
- контроля состояния двух тестовых входов (управляются выходами типа “сухой контакт” или “открытый коллектор”);
- управления одним дополнительным релейным выходом (параметры см. ниже);
- управления одним дополнительным выходом типа “открытый коллектор” (параметры см. ниже);
- управления четырьмя служебными выходами индикации состояний (параметры см. ниже);
- приема данных от двух считывателей по протоколу Wiegand 26 или ABA Track 2;

- **Драйвер роторного турникета** (PERCo-DRT-12301) — аппаратный модуль системы, предназначенный для:

- взаимодействия с блоком управления электромеханической калиткой PERCo (типа WHD) в виде выдачи трех сигналов управления (Left, Stop и Right) и обработки двух сигналов о факте совершения прохода (PASS L и PASS R);
- обслуживания одного пульта управления PERCo-H-05/2;
- контроля состояния двух тестовых входов (управляются выходами типа “сухой контакт” или “открытый коллектор”);
- управления одним дополнительным релейным выходом (параметры см. ниже);
- управления одним дополнительным выходом типа “открытый коллектор” (параметры см. ниже);
- управления четырьмя служебными выходами индикации состояний (параметры см. ниже);
- приема данных от двух считывателей по протоколу Wiegand 26 или ABA Track 2;

- **Драйвер замка/турникета** (PERCo-DL/DT-12310) — аппаратный модуль системы, предназначенный для:

- контроля состояния четырех тестовых входов типа “сухой контакт” или “открытый коллектор”;
- управления двумя дополнительными релейными выходами (параметры см. ниже);
- управления двумя дополнительными выходами типа “открытый коллектор” (параметры см. ниже);
- управления четырьмя служебными выходами индикации состояний (параметры см. ниже);
- приема данных от двух считывателей по протоколу Wiegand 26 или ABA Track 2;
- при работе в варианте «Замок»:

- управления двумя электромеханическими (электромагнитными) замками со следующими параметрами:

- а) при запитывании замка непосредственно от базового контроллера-концентратора:

- $U = 12$ В постоянного тока;
- $I = 1$ А (max) для постоянного уровня;
- $I = 2$ А (max) для импульсного режима на время не более 0,25 секунды.

В этом режиме следует учитывать возможности источника питания базового контроллера-концентратора по максимальному выходному току.

б) при запитывании замка от внешнего источника:

- $U = 30$ В постоянного тока (max);
- $U = 42$ В переменного тока (max);
- $I = 1$ А (max) для постоянного уровня;
- $I = 5$ А (max) для импульсного режима на время не более 0,25 секунды;

- контроля состояния двух датчиков двери (управляются выходами типа "сухой контакт" или "открытый коллектор");

- контроля состояния двух входов дистанционного управления (управляются выходами типа "сухой контакт" или "открытый коллектор");

- при работе в варианте «Турникет»:

- управления турникетом/калиткой со встроенной электроникой производства фирмы PERCo, поддерживающими потенциальный режим управления;

- управление турникетом сторонних производителей (для получения схем подключения к турникетам сторонних производителей обращайтесь к специалистам компании PERCo);

- обслуживания пульта управления PERCo-H-05/04, в том числе:

- контроля состояния трех входов дистанционного управления (управляются выходами типа "сухой контакт" или "открытый коллектор");

- управления четырьмя линиями индикации пульта управления PERCo-H-05/04 (3 светодиодных индикатора и зуммер).

- **Тестовый вход** — контакт драйвера, предназначенный для подключения внешних датчиков охранно-пожарной сигнализации с выходами типа "сухой контакт" или "открытый коллектор" (детекторы движения, дымовые датчики и т.п.). Для более полной информации см. "Инструкцию по монтажу".

- **Релейный выход и выход типа "открытый коллектор"** — контакт драйвера, предназначенный для подключения внешних управляемых устройств, методы активизации которых формулируются на этапе конфигурирования системы (выход тревоги, освещение и т.п.).

Параметры релейного выхода:

- $U = 30$ В постоянного тока (max);
- $U = 42$ В переменного тока (max);
- $I = 2$ А (max) для постоянного уровня;
- $I = 5$ А (max) для импульсного режима на время не более 1 секунды.

Параметры выхода типа "открытый коллектор":

- $U = 30$ В постоянного тока (max);
- $I = 0,25$ А (max) для постоянного уровня;
- $I = 0,5$ А (max) для импульсного режима на время не более 1 секунды.

Релейный выход и выход типа "открытый коллектор" в дальнейшем имеют одинаковое название релейный выход.

- **Служебный выход** — контакт драйвера, предназначенный для подключения внешних устройств (светодиодный индикатор, пьезоизлучатель и т.п.). Используется для индикации состояний контроля доступа в зоне ТКД (имеет стандартные CMOS выходные уровни с выходным током $I_{max} = 20$ мА). Стандартно к нему подключаются входы управления индикацией считывателей.

- **Удлинитель линии (PERCo-SE-12001)** — устройство, предназначенное для удлинения линии связи между сервером системы и первичным контроллером с 15 метров до 1200 метров.

- **Репитер** — устройство, предназначенное для увеличения предельной длины магистрали (1200 метров), связывающей контроллеры системы, на дополнительные 1200 метров.

- **Пульт дистанционного управления или дистанционное управление** — класс устройств, предназначенных для управления доступом через исполнительные механизмы в интерактивном режиме.
- **Исполнительный механизм** — устройство, преграждающее доступ куда-либо (турникет, калитка, замок и т.п.).
- **Комиссионирование доступа** — усиление контроля доступа посредством последовательного предъявления двух карт или одной карты и набора кодовой комбинации на клавиатуре для открытия исполнительного механизма.
- **Шунтирование входа** — фиксация логического состояния входа на определенном уровне, без учета внешних воздействий.
- **Пространственная зона контроля** — часть территории объекта, пересечение границ которой осуществляется под контролем системы, т.е. с предъявлением карт (пространственная зона характеризуется стоящим на ее границе как минимум одним исполнительным механизмом с двумя считывателями — один на вход и второй на выход, т.е. по разные границы этой зоны).
- **Временная зона контроля** — совокупность временных интервалов (до 4 для каждого считывателя и до 8-и для исполнительных механизмов, тестовых входов и релейных выходов) в пределах календарных суток, в течение которых возможно:
 - разрешение доступа по пользовательской карте;
 - автоматическое открытие исполнительного механизма;
 - запрещение дистанционного управления исполнительным механизмом;
 - автоматическая активизация релейных выходов;
 - разрешение мониторинга тестовых входов, а также генерация тревоги при их активизации.
- **Режим контроля доступа (РКД)** — режим функционирования системы или отдельной ее части (терминала контроля доступа, считывателя), например, режим "Охрана", режим "Закрето" и т.д.
- **Мнемосхема** — графическое представление территории, контролируемой системой, или ее части, с расположенными на ней пространственными зонами контроля. В качестве подложки может быть использован файл формата *.bmp, с изображенной схемой предприятия. Размер и цветовая палитра файла любые. Система может иметь неограниченное число мнемосхем (более подробно см. "Руководство пользователя по программе "Конфигуратор системы").
- **Мониторинг** — сбор и отображение наиболее важных событий контроля доступа и текущего состояния элементов системы в реальном времени на мониторе оператора системы (компьютере с загруженным программным обеспечением "Управление системой"); собранная информация хранится в специальном файле — журнале мониторинга.
- **Регистрация** — протоколирование всех событий, связанных с перемещениями пользователей, изменениями состояний тестовых входов и релейных выходов и функционированием оборудования. Регистрация осуществляется посредством периодического сбора накопленной контроллерами информации с сохранением в базе данных (журнале регистрации, формат "Paradox7") на жестком диске сервера системы. Эта информация собирается и обрабатывается с помощью ПО "Генератор отчетов".

2. НАЗНАЧЕНИЕ И СОСТАВ СИСТЕМЫ

Система контроля доступа PERCo-SYSTEM-12000 — это мультипрограммная сетевая система контроля доступа, предназначенная для:

- предотвращения несанкционированного доступа на территорию и во внутреннее помещения предприятия;
- мониторинга происходящих в системе событий (см. п. 4.2.4), контроля состояния датчиков охранно-пожарной сигнализации в режиме реального времени;
- автоматизированного учета и оформления пропусков;
- регистрации времени прохода и учета рабочего времени.

Структурная схема системы представлена на рисунке 1.

В аппаратный состав системы входят следующие структурные единицы:

- Компьютер с установленным ПО (может быть несколько)
- Концентратор PERCo-SC-12200P (варианты на 12000 и 32000 пропусков)
- Базовый контроллер-концентратор PERCo-SC-12300P (варианты на 12000 и 32000 пропусков)
- Драйвер турникета PERCo-DT-12301
- Драйвер роторного турникета PERCo-DRT-12301
- Драйвер замка/турникета PERCo-DL/DT-12310
- Драйвер связи PERCo-DN-12201
- Контроллер замка PERCo-CL-12200 (варианты Е и Н)
- Контрольный считыватель PERCo-CR-12001 (варианты Е, Н, ЕН и М)
- Репитер
- Удлинитель линии PERCo-SE-12001
- Считыватель
- Карта
- Электромеханический исполнительный механизм (турникет, замок и т.п.)
- Блок питания

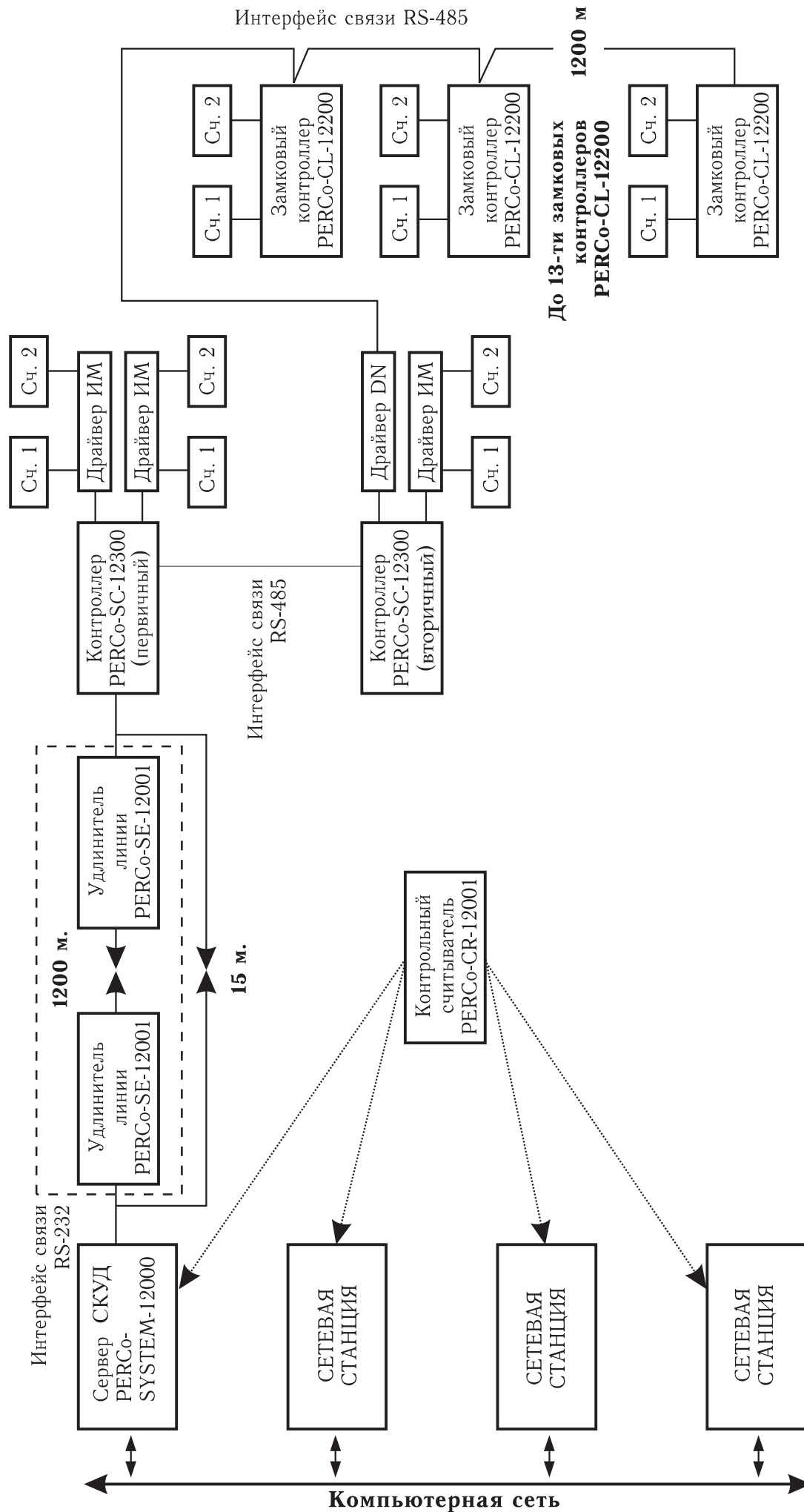


Рис. 1 Структурная схема СКУД PERCo-SYSTEM-12000

2.1. УСТРОЙСТВО КОНТРОЛЛЕРОВ

2.1.1. Устройство концентратора и контроллера-концентратора

Концентратор и контроллер-концентратор — это унифицированный системный контроллер на базе микропроцессорного устройства. Они различаются только внутренним программным обеспечением.

В состав унифицированного системного контроллера входят:

- контроллер управления доступом (Плата Main-12002K);
- менеджер питания (Плата PWR-12002).
- кронштейн с индикаторами;

Блок-схема представлена на рис. 2.

Контроллер размещён в металлическом корпусе. Для защиты от несанкционированного доступа к его узлам передняя крышка закрывается с помощью механического замка.

2.1.1.1. Контроллер управления доступом

Контроллер содержит энергонезависимую память объемом 1 Мбайт, которая предназначена для хранения конфигурации подсистемы, списков карт, временных критериев доступа и журнала регистрации событий. Журнал регистрации событий имеет кольцевую структуру, то есть после его переполнения старые события заменяются новыми.

Контроллер также содержит энергонезависимый таймер, предназначенный для фиксации времени произошедшего события.

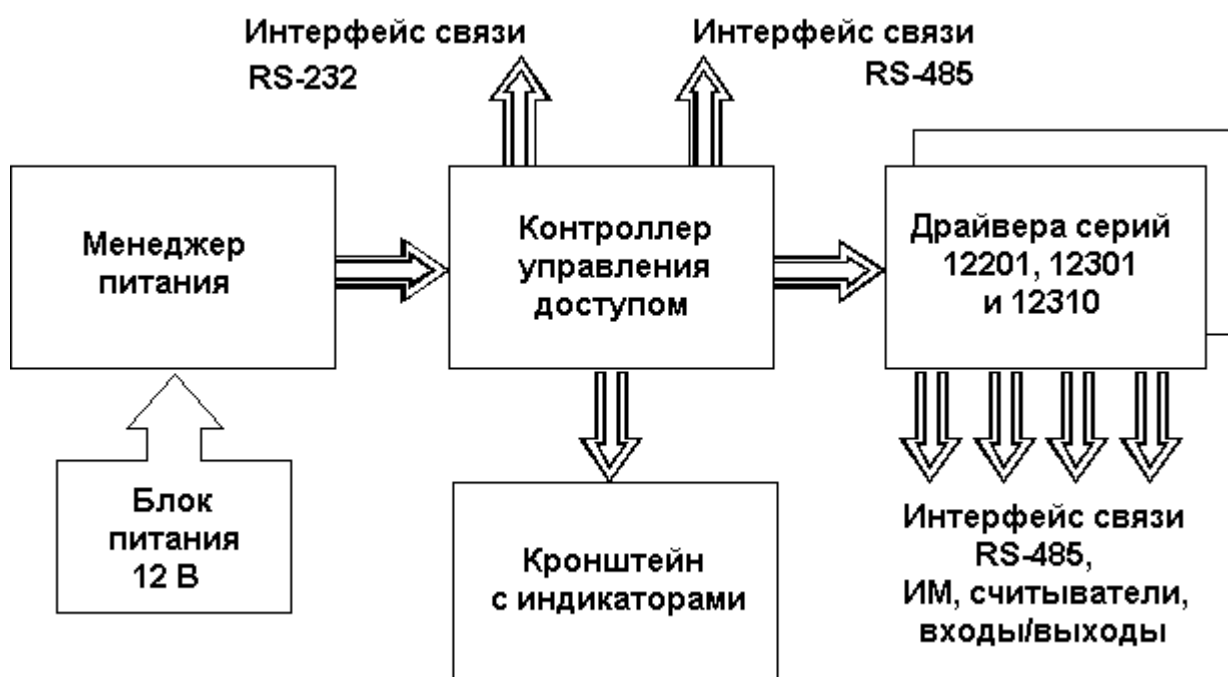


Рис. 2 Блок-схема унифицированного системного контроллера

2.1.1.2. Кронштейн с индикаторами

На лицевой панели блока расположена линейка диагностических индикаторов следующего функционального назначения:

DRIVER — индикатор связи с драйвером/замковым контроллером, подключенным к данному контроллеру;

SYNC CH — индикатор связи в магистрали, связывающей контроллеры системы;

ASYNC CH — индикатор связи между сервером системы и первичным контроллером;

CONFIGURATION — индикатор целостности системных установок, необходимых для нормального функционирования;

PRIMARY — индикатор текущей установки переключки Primary/Slave, определяющей иерархическое положение контроллера;

BATTERY — индикатор работоспособности цепи заряда аккумулятора и непосредственно самого аккумулятора;

POWER — индикатор наличия сетевого питания.

Нормальный цвет свечения всех диагностических индикаторов "зеленый". Переход индикаторов (кроме "PRIMARY") в режим "красного" свечения свидетельствует о неисправности данной функции. Индикатор "PRIMARY" непосредственно связан с переключкой Primary/Slave и светится только в случае, если эта переключка установлена, т.е. контроллер является первичным в данной ветви контроллеров (смотри п.2.2.).

2.1.1.3. Плата менеджера питания

Предназначена для формирования всех питающих напряжений и обслуживания аккумулятора.

2.1.2. Устройство замкового контроллера

Блок-схема замкового контроллера представлена на рис. 3.

Конструктивно замковый контроллер состоит из платы считывателей и платы контроллера замков, которые размещены в металлическом корпусе и соединены между собой с помощью разъема. Для защиты от несанкционированного доступа к узлам замкового контроллера передняя крышка закрывается с помощью механического замка.

Индикация состояния замкового контроллера обеспечивается диагностическими индикаторами, расположенными на его платах.

На плате контроллера замков установлены два индикатора (см рис.1 Инструкции по монтажу на подсистему замковых контроллеров системы контроля и управления доступом PERCo-SYSTEM-12000). Первый индикатор (VD27) индицирует наличие питания на плате. Второй индикатор (VD26) индицирует наличие связи с концентратором (контроллером-концентратором). До проведения конфигурации системы второй индикатор мигает зеленым светом. Когда контроллер сконфигурирован и работает в составе системы, второй индикатор постоянно горит зеленым светом. Второй индикатор также начинает мигать зеленым светом при переходе контроллера в аварийный режим работы, т.е. при пропадании связи с концентратором (контроллером-концентратором).

На плате считывателей установлен индикатор, который индицирует наличие питания: горит оранжевым — норма, горит зеленым — нет питания аналоговой части, горит красным — нет питания цифровой части, не горит — питание на плату не подано.

Плата контроллера замков содержит энергонезависимую память, которая предназначена для сохранения программной конфигурации подсистемы и списка карт, имеющих право открывать замок в аварийном режиме работы, а также для сохранения журнала регистрации событий. Журнал регистрации событий имеет кольцевую структуру, то есть после его переполнения старые события заменяются новыми. На ней также установлен энергонезависимый таймер, предназначенный для фиксации времени произошедшего события.

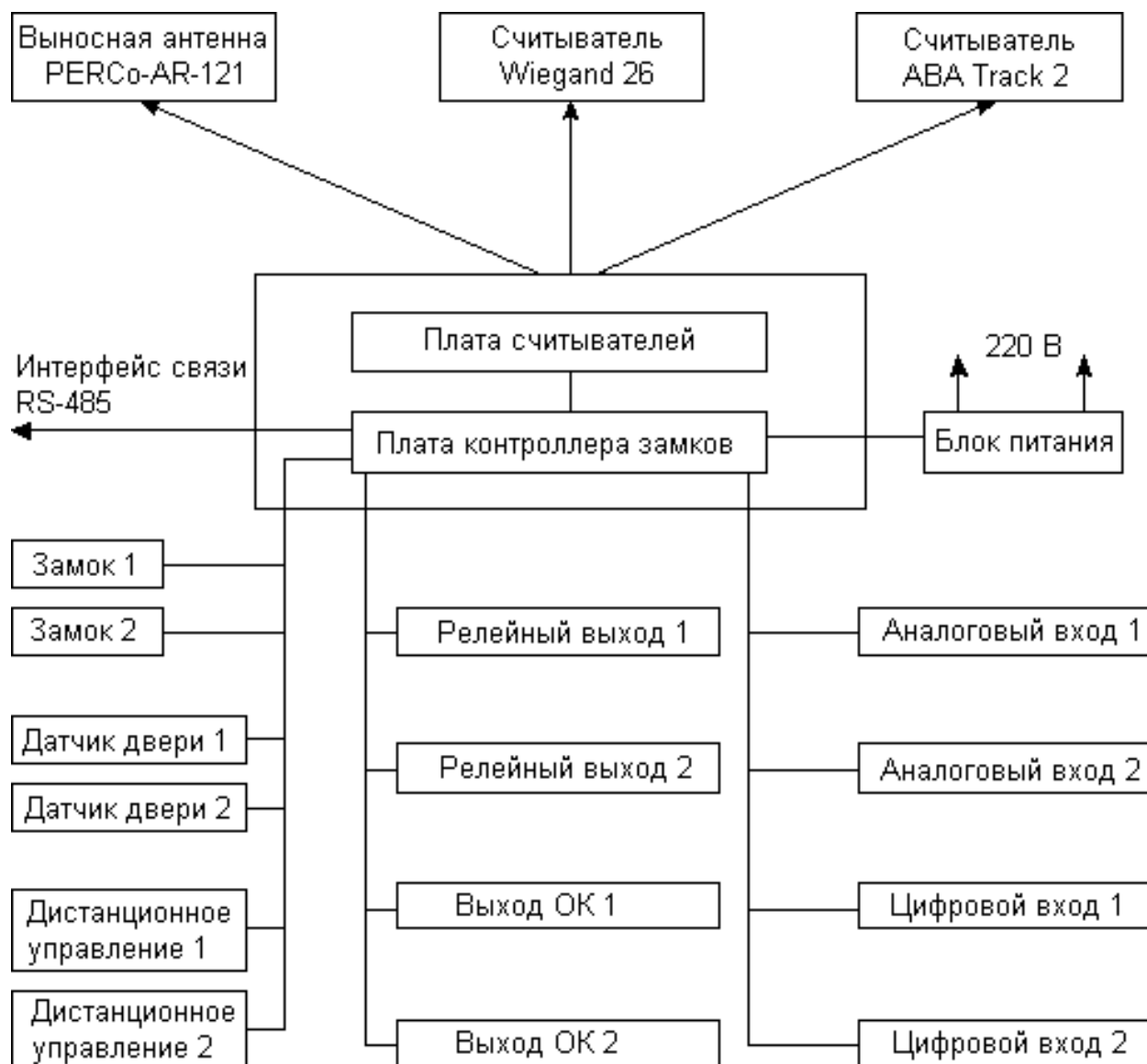


Рис. 3 Блок-схема контроллера PERCo-CL-12200

Аналоговые тестовые входы — это контакты на плате контроллера замка, предназначенные для подключения шлейфов пожарной или охранной сигнализации (аналоговые входы 1-2 на рис. 3.).

Параметры шлейфов:

Максимально допустимое сопротивление

проводов шлейфа.....не более 50 Ом

Сопротивление изоляции проводов шлейфане менее 30 кОм

Напряжение в шлейфе..... 12±1,5 В

Максимальный ток в шлейфе (охранном) 22 мА

Сопротивление концевого резистора 4,3±5% кОм

Максимальное количество пассивных извещателей, включенных в один шлейф (рекомендуемое) не более 10 шт.

Максимально возможный суммарный ток потребления активных пожарных извещателей, включенных в один шлейф..... не более 1 мА

Цифровые тестовые входы — это контакты на плате контроллера замка, предназначенные для подключения внешних датчиков с выходами типа "сухой контакт" или "открытый коллектор" (детекторы движения, дымовые датчики и т.д.) (цифровые входы 1÷2 на рис. 3.).

Релейные выходы и выходы типа "открытый коллектор" — это контакты на плате контроллера замка, предназначенные для подключения внешних управляемых устройств (выход тревоги, освещение и т.д.) (релейные выходы 1-2 и выходы ОК 1-2 на рис. 3.).

Параметры релейных выходов и выходов типа "открытый коллектор" аналогичны параметрам драйверов серий 12301 и 12310.

Служебные выходы — это контакты на плате считывателей, предназначенные для подключения внешних устройств индикации (индикатор, пьезоизлучатель и т.д.). Используются для индикации состояний контроля доступа.

Параметры служебных выходов аналогичны параметрам драйверов серий 12301 и 12310.

Управление замками (до 2-х замков).

Контроллер может работать с различными типами электромеханических и магнитных замков и защёлоч. Могут применяться замки с управлением как постоянным, так и переменным током, открывающиеся как при подаче, так и при снятии с них управляющего напряжения. Управление замками осуществляется с помощью контактов реле. Параметры выходов управления замками аналогичны параметрам драйверов серий 12301 и 12310.

Аппаратная конфигурация замкового контроллера.

При поставке замковый контроллер имеет следующую аппаратную конфигурацию:

Питание замков от штатного блока питания контроллера

Сетевой номер контроллера 0000

Для того чтобы изменить начальную конфигурацию, необходимо изменить установки переключателей и переключателей на плате контроллера замков и плате считывателей (см. Инструкцию по монтажу соответствующего замкового контроллера).

2.1.3. Подключения к концентратору и контроллеру-концентратору

К концентратору PERCo-SC-12200P могут подключаться через один (два) драйвер(а) связи PERCo-DN-12201 до 15 (до 7 при варианте на 32000 пропусков) замковых контроллеров PERCo-CL-12200.

К контроллеру-концентратору PERCo-SC-12300P могут подключаться:

1. До двух драйверов серий 12301 и 12310;
2. Один драйвер серий 12301 или 12310 и через драйвер связи PERCo-DN-12201 до 13 (до 5 при варианте на 32000 пропусков) замковых контроллеров PERCo-CL-12200.

Внимание!!! В этом случае у замковых контроллеров PERCo-CL-12200 сетевой номер контроллера должен быть установлен в диапазоне от 2 до 14 (от 2 до 6 при варианте на 32000 пропусков).

3. Через один (два) драйвер(а) связи PERCo-DN-12201 до 15 (до 7 при варианте на 32000 пропусков) замковых контроллеров PERCo-CL-12200.

2.2. СОСТАВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Программное обеспечение системы выпускается в трех вариантах:

PERCO-SS-12100.01 — однопользовательский комплект с модулем оформления пропусков;

PERCO-SL-12100.01 — сетевой комплект на неограниченное число рабочих мест операторов с модулем оформления пропусков;

PERCO-SN-12100.01 — сетевой комплект для многосегментных систем на неограниченное число рабочих мест операторов с модулем оформления пропусков.

Принципиальным различием между этими вариантами, кроме неограниченного количества рабочих мест операторов, является то, что ПО PERCO-SN-12100.01 может иметь в своем составе до 16 серверов системы. Это свойство позволяет подключить

в систему до 16 "ветвей" аппаратуры, т.е. увеличить максимальный аппаратный состав системы в 16 раз.

В состав программного обеспечения входят следующие модули:

- **"Сервер системы" (входит в базовый комплект)**

Предназначен для обеспечения связи между остальными модулями ПО и аппаратурой, проведения мониторинга системы и автоматического приема журнала регистрации контроллеров в случае их предельного переполнения.

- **"Администратор системы" (входит в базовый комплект)**

Предназначен для создания и восстановления баз данных системы, установки паролей и формирования прав доступа к программным ресурсам системы.

- **"Конфигуратор системы" (входит в базовый комплект)**

Предназначен для первичной конфигурации системы, задания параметров работы системы, создания мнемосхемы контролируемой территории с привязкой к ней ресурсов системы, разбиения территории на пространственные зоны контроля и создания сегментированного набора системных карт.

- **"Управление системой" (входит в базовый комплект)**

Предназначен для оперативного управления системой на любом уровне — от единичного датчика до системы в целом и слежения за текущим состоянием системы в реальном времени с отображением информации как на мнемосхеме, так и в журнале мониторинга.

- **"Отдел кадров" (входит в базовый комплект)**

Предназначен для выдачи пропусков, создания базы данных персонала с сопоставлением пропуска конкретному лицу, определения прав доступа этих пропусков в системе, ведение списка временных пропусков, ведение стоп-листа.

- **"Генератор отчетов" (входит в базовый комплект)**

Предназначен для просмотра зарегистрированных событий по любым терминалам контроля доступа за определенный интервал времени и получения отчетов различной формы.

- **Утилита "Планировщик задач" (входит в базовый комплект)**

Предназначена для однократного либо периодического выполнения различных действий (периодичность для каждого действия задается пользователем): удаление карт, срок действия которых истек, получение журнала регистрации с одного из ТКД, получение журнала регистрации со всей системы и запуск внешних программ.

- **Утилита "Снятие локировок" (входит в базовый комплект)**

Предназначена для разрешения конфликтных ситуаций при коллективной обработке баз данных различными модулями ПО системы.

- **"Оформление пропусков" (входит в базовый комплект)**

Предназначен для оформления карт путем создания наклеек с персональными атрибутами владельца, в том числе с фотографиями.

- **"Учет рабочего времени"**

Предназначен для получения отчетов, связанных с рабочим временем (отчеты по форме: кто опоздал, кто задержался, кто сколько отработал). Отчеты выдаются по любой группе пользователей системы за выбранный период.

- **"Маршрут обхода"**

Предназначен для создания маршрутов и графиков обхода охраной контролируемой территории и контроля за их соблюдением.

- **"Удаленное управление"**

Предназначен для организации видеонаблюдения за объектами системы и разрешения доступа только с подтверждения оператора системы после сравнения им изображения, полученного с видеокамеры, с эталонным изображением владельца предъявленной карты, хранящимся в памяти компьютера.

2.3. СОСТАВ ТКД

Каждый ТКД системы состоит из:

Вариант 1.

- базового контроллера-концентратора и необходимой периферии, которая может включать в себя следующие элементы:

- до двух драйверов серий 12301, 12310 и DN-12201 в любой произвольной комбинации (минимум один драйвер серий 12301 или 12310);
- количество считывателей определяется количеством установленных драйверов и не превышает четырёх;
- количество исполнительных механизмов определяется количеством установленных драйверов и не превышает четырёх.

Вариант 2.

- замкового контроллера PERCo-CL-12200 и необходимой периферии, которая может включать в себя следующие элементы:

- до двух считывателей;
- до двух исполнительных механизмов.

3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ СИСТЕМЫ

Количество контроллеров.....	до 255
Количество исполнительных устройств	до 1020
Количество считывателей	до 510
Количество карт	до 12000
Расширенное количество карт	до 32000
Количество наборов карт	до 32
Количество пространственных зон контроля	до 128
Количество временных зон контроля	до 256
Количество недельных графиков	до 128
Количество сменных графиков	до 32
Максимальный размер буфера событий на один драйвер/контроллер:	
- для драйверов серий 12301 и 12310, шт.....	до 16384
- для замкового контроллера PERCo-CL-12200, шт.....	до 3000

3.1. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ КОНЦЕНТРАТОРА И КОНТРОЛЛЕРА-КОНЦЕНТРАТОРА

Напряжение питания	12±1.2 В
Ток потребления (без учета тока заряда аккумулятора)	не более 0.15 А
Ток потребления (с учетом тока заряда аккумулятора).....	не более 0.5 А
Потребляемая мощность	не более 6 Вт
Максимальное количество драйверов серии 12201, 12301 и 12310 (драйверов серий 12301 и 12310 — только для контроллера-концентратора), шт... 2	
Скорость обмена в канале связи подсистемы.....	9600 бод
Время опроса всех замковых контроллеров подсистемы	не более 1 сек
Масса (без аккумулятора и блока питания)	не более 5,5 кг
Габаритные размеры	384x360x108 мм

Условия эксплуатации:

Температура окружающего воздуха	от +1 до +40°C
Относительная влажность.....	не более 80% при t = 25°C

3.2. ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ЗАМКОВОГО КОНТРОЛЛЕРА

Номинальное значение напряжения питания	
постоянного тока	12±1.2 В
Ток потребления	не более 0,25 А
Потребляемая мощность	не более 3 Вт
Масса контроллера	не более 1,5 кг
Габаритные размеры контроллера	205x185x45 мм
Количество контролируемых дверей	2
Количество считывающих устройств	2
Тип карт	бесконтактные, магнитные, Wiegand, PIN-код
Количество входов дистанционного управления	2
Количество аналоговых тестовых входов	2
Количество цифровых тестовых входов	2
Количество релейных выходов	2
Количество выходов с открытым коллектором	2
Количество служебных выходов	4
Стандарт интерфейса связи	RS-485
Максимальная дальность связи без повторителя, м	1200
Характеристики контроллера в аварийном режиме:	
Максимальное количество пользователей	1000
Максимальное количество событий журнала регистраций	1000
Условия эксплуатации:	
Температура окружающего воздуха	от +1 до +40°C
Относительная влажность	не более 80% при t = 25°C

4. ОПИСАНИЕ РАБОТЫ СИСТЕМЫ

4.1. КОНФИГУРАЦИЯ СИСТЕМЫ

• После полного завершения монтажа системы и установки входящего в комплект поставки программного обеспечения (с учетом требуемой сетевой топологии), систему необходимо сконфигурировать, см. ПО "Конфигуратор системы".

• Перед этим необходимо еще раз проверить правильность установки перемычки Primary/Slave в каждом контроллере системы (см. инструкцию по монтажу системы).

После завершения конфигурации необходимо задать все параметры функционирования каждого используемого ресурса системы. Для корректной работы системы рекомендуется задавать параметры в порядке, приведенном ниже:

- **для карт** — сегментированный набор системных карт (каждый сегмент описывается следующими атрибутами: код семейства (1÷255), диапазон (1÷65535));
- **для релейных выходов** — параметры функционирования и условия для автоактивизации/автонормализации ресурсов;
- **для тестовых входов** — параметры функционирования и условия для мониторинга;
- **для исполнительных механизмов** — параметры управления и условия для автоактивизации/автонормализации ресурсов;
- **для считывателей** — тип, привязка к исполнительным механизмам, алгоритм принятия решения по предъявленной карте, время анализа предъявленной карты и привязка к пространственной зоне контроля;
- **для служебных выходов** — параметры функционирования и типы реакций на состояния;

- **для генератора тревоги** — "громкая" тревога (сирена) или "тихая" тревога (оповещение только оператора системы) и причины генерации тревоги, связанные:
 - а) с предъявлением карт,
 - б) с состоянием исполнительных механизмов,
 - в) с состоянием тестовых входов;
- **для аварийного режима работы** — конфигурация режима автономной работы, список пропусков для работы в аварийном режиме (из модулей ПО "Управление системой" и "Отдел кадров").

После передачи параметров каждого ресурса в систему он вступает в действие и получает управление как на уровне контроллера, так и на уровне программы "Управление системой".

Для перевода системы в режим работы от карт необходимо, используя ПО "Отдел кадров", сформировать группы допуска и их права, временные критерии (временные зоны, недельные графики, сменные графики и календарь праздничных дней) и передать их в систему. Затем, используя ПО "Управление системой", необходимо установить режим "Системный контроль" с соответствующими атрибутами.

В результате этих действий система переходит в режим нормальной работы с полной реализацией всех ее возможностей.

4.1.1. Ресурсы терминала контроля доступа и параметры их функционирования

4.1.1.1. Релейный выход

Для управления релейным выходом необходимо определить следующие параметры:

1. Нормальное состояние выхода (запитан или не запитан). Этот параметр определяет состояние выхода при отсутствии на нем активизирующих управляющих воздействий.

2. Период активизации (00:00÷08:28 мин:с). Этот параметр определяет промежуток времени, в течение которого при наличии активизирующего управляющего воздействия релейный выход меняет свое состояние из нормального в противоположное.

3. Критерий для автоактивизации:

- связан с режимом контроля доступа 1-го считывателя, т.е. активизируется (без учета периода активизации), если 1-й считыватель установлен в режим "Охрана" и нормализуется во всех остальных режимах;
- связан с режимом контроля доступа 2-го считывателя, т.е. активизируется (без учета периода активизации), если 2-ой считыватель установлен в режим "Охрана" и нормализуется во всех остальных режимах;
- связан с режимом контроля доступа 1-го и 2-го считывателей, т.е. активизируется (без учета периода активизации), если 1-й и 2-ой считыватели установлены в режим "Охрана" и нормализуется, если режим одного из считывателей не "Охрана";
- связан с временем суток (временная зона или недельный график). Одна из системных временных зон (или недельных графиков) в установленные интервалы времени которой релейный выход переходит в активное состояние и остается в нем до его истечения (без учета периода активизации).

4.1.1.2. Тестовый вход

Для реализации функций контроля состояния тестового входа необходимо обязательно определить следующие параметры:

1. Нормальное состояние контакта (нормально замкнут или нормально разомкнут). Этот параметр определяет тот уровень сигнала на входе, который система должна воспринимать как норма. В драйвере входов/выходов с аналоговыми входами этот параметр имеет несколько другое значение:

- установка опции нормально замкнут приводит к 20 мс задержке на изменение уровня сигнала на входе;

- установка опции нормально разомкнут приводит к 500 мс задержке на изменение уровня сигнала на входе.

2. Период шунтирования (00:00÷07:56 мин:с). Этот параметр определяет тот промежуток времени в течение которого состояние входа считается нормальным независимо от уровня входного сигнала. Причиной шунтирования может быть активизация других тестовых входов или открытие исполнительного механизма.

3. Номера тестовых входов, шунтируемых при активизации данного входа.

4. Номера релейных выходов, активизируемых при активизации данного входа.

Следует заметить, что активизация релейного выхода привязанная к активизации тестового входа не учитывает возможного шунтирования этого входа. Это очень важно для случаев применения в системе детекторов движения, расположенных в зоне прохода через исполнительные механизмы.

5. Критерий для мониторинга:

- связан с режимом контроля доступа 1-го считывателя, т.е. мониторинг активизируется, если 1-ый считыватель установлен в режим "Охрана" и прекращается во всех остальных режимах;

- связан с режимом контроля доступа 2-го считывателя, т.е. мониторинг активизируется, если 1-ый считыватель установлен в режим "Охрана" и прекращается во всех остальных режимах;

- связан с режимом контроля доступа 1-го и 2-го считывателей, т.е. мониторинг активизируется, если 1-ый и 2-ой считыватели установлены в режим "Охрана" и прекращается, если режим одного из считывателей не "Охрана";

- связан с временем суток (временная зона или недельный график). Одна из системных временных зон (или недельных графиков) в установленные интервалы времени которой осуществляется мониторинг состояния данного входа, а в остальное время состояние входа считается нормальным независимо от уровня входного сигнала.

4.1.1.3. Исполнительный механизм

Для управления и контроля состояния исполнительного механизма необходимо определить следующие параметры:

1. Состояние "Закрыто" (подано или нет напряжение) — определяет уровень управляющего сигнала, поданного на исполнительный механизм, который необходим для его перевода в закрытое состояние.

2. Нормальное состояние контакта — устанавливает состояние контакта исполнительного механизма в состоянии "Закрыто".

3. Время удержания в открытом состоянии (0÷120 с) — время, в течение которого исполнительный механизм должен находиться в открытом состоянии после разблокировки; по истечении этого времени он будет автоматически закрыт.

4. Восстановление состояния "Закрыто" — определяет момент перевода исполнительного механизма в состояние "Закрыто", т.е. исполнительный механизм перейдет в состояние "Закрыто" либо после начала прохода (открытия двери), либо после завершения прохода (закрытия двери).

5. Триггерный режим управления — только для исполнительных механизмов, поддерживающих этот режим работы: устанавливает длительность управляющего импульса.

Триггерный режим рекомендуется использовать для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки "CISA").

6. Предельное время разблокировки исполнительного механизма (00:00÷04:15 мин:с) — максимальное время, в течение которого исполнительный механизм может быть открыт. По истечении этого времени в событиях мониторинга формируется сообщение о недопустимо долгой разблокировке, возможна генерация тревоги.

7. Время предтревоги — интервал времени, равный половине предельного времени разблокировки. По его истечении первичному контроллеру будет отправлено сообщение о появлении предтревожной ситуации на данном исполнительном механизме.

8. Номера релейных выходов, автоматически активизируемых при открытии исполнительного механизма.

9. Номера тестовых входов, автоматически шунтируемых при открытии исполнительного механизма.

10. Номера тестовых входов, активизация которых должна аварийно разблокировать исполнительный механизм. Аварийная разблокировка сопровождается запрещением дистанционного управления и может быть снята только с помощью ПО "Управление системой" через установку режима контроля доступа или сброс тревоги.

11. Номера тестовых входов, активизация которых должна аварийно блокировать исполнительный механизм. Аварийная блокировка сопровождается запрещением дистанционного управления, запрещением управления от карт и может быть снята только с помощью ПО "Управление системой" через установку режима контроля доступа или сброс тревоги.

12. Временной критерий для автооткрытия исполнительного механизма — одна из системных временных зон (или недельных графиков), в установленные интервалы времени которой исполнительный механизм автоматически переходит в открытое состояние.

13. Временной критерий для запрещения дистанционного управления — одна из системных временных зон (или недельных графиков), в установленные интервалы времени которой автоматически запрещается дистанционное управление исполнительным механизмом.

4.1.1.4. Считыватель

Для управления доступом и контроля перемещения пользователей с помощью карт необходимо определить следующие параметры:

1. Тип используемых карт (магнитные или бесконтактные). Этот параметр соответственно определяет и тип интерфейса между считывателем и контроллером. Тип используемых карт для обоих считывателей одного контроллера должен быть одинаковым.

2. Наличие клавиатуры.

3. Номера исполнительных механизмов, с которыми связан считыватель. Этот параметр определяет, какие исполнительные механизмы должны открываться под управлением данного считывателя.

4. Время принятия решения ($0 \div 126$ с) — время, в течение которого данный считыватель будет занят обработкой предъявленной ему карты.

Кроме этого, при установке считывателя на мнемосхему ему присваивается пространственная зона контроля.

4.1.1.5. Служебный выход

Для индикации текущих событий и состояний в зоне терминала контроля доступа необходимо определить следующие параметры:

□ Глобальные параметры

1. Нормальное состояние выхода (подано напряжение или нет) — определяет состояние выхода при отсутствии на нем активизирующих управляющих воздействий.

2. Номера считывателей, с которыми связан выход ("Нет"/№1/№2) — определяет, состояния каких считывателей должен отображать данный служебный выход.

3. Период непрерывной индикации ($1 \div 15$ с) — единичный временной интервал непрерывной активизации, от которого рассчитываются все остальные значения.

4. Период вспышки ($0 \div 3,75$ с) — единичный временной интервал пульсирующей активизации, от которого рассчитываются все остальные значения.

□ Индикация режима контроля доступа

Описывает способ уникальной индикации для каждого из существующих режимов контроля доступа.

□ Индикация состояний исполнительного механизма

Описывает способ уникальной индикации предтревоги по разблокировке каждого из существующих исполнительных механизмов. Время старта индикации предтревоги устанавливается в параметрах исполнительного механизма. Индикация предтревоги прекращается после восстановления заблокированного состояния исполнительного механизма.

□ Индикация событий

Описывает способ уникальной индикации следующих событий, связанных с доступом:

- Доступ разрешен;
- Доступ запрещен;
- Запрос на подтверждение (от дистанционного управления);
- Запрос на подтверждение (от компьютера);
- Ожидание смены режима (автономной смены РКД);
- Ожидание комиссионирования;
- Смена РКД.

4.1.1.6. Генератор тревоги

Для выделения событий, которые должны приводить к генерации тревоги в системе, и соответствующего управления выделенным выходом тревоги (один из релейных выходов) необходимо определить следующие параметры:

1. Причины генерации тревоги по предъявлению карты.

Этот параметр охватывает все возможные нарушения контроля доступа, связанные с предъявлением карт, и позволяет указать, в случае каких нарушений необходима генерация тревоги.

2. Причины генерации тревоги по состоянию исполнительного механизма.

- Несанкционированное системой открытие — разблокировка исполнительного механизма, произошедшая без предшествующей санкции системы на его открытие. Устанавливается отдельно для каждого РКД.

- Недопустимо долгое открытие исполнительного механизма — разблокировка исполнительного механизма дольше описанного в его параметрах предельного времени разблокировки.

3. Тестовые входы, активизация которых приводит к генерации тревоги.

Необходимо перечислить номера тестовых входов, активизация которых должна сопровождаться генерацией тревоги.

4. Тестовый вход для автономного сброса тревоги.

Необходимо указать номер тестового входа, активизация которого приведет к сбросу тревоги.

4.2 ФУНКЦИОНИРОВАНИЕ СИСТЕМЫ

Функционирование системы складывается из работы всех ее частей и в целом происходит следующим образом:

Каждый пользователь получает карту, зарегистрированную через контрольный считыватель (или с помощью клавиатуры ПК) в базе пользователей, см. ПО "Отдел кадров".

Регистрация карты подразумевает присвоение ей атрибутов владельца, прав доступа соответствующей группы допуска и передачу в систему.

4.2.1 Принципы функционирования аппаратуры

В системе PERCo-SYSTEM-12000 концентратор (контроллер-концентратор) может быть как первичным, т.е. подключенным непосредственно к серверу, так и вторичным, т.е. подключенным к первичному контроллеру. Его конфигурация зависит от состояния переключки Primary/Slave.

Функции управления в подсистеме замковых контроллеров осуществляет концентратор (контроллер-концентратор). Обмен информацией между ним и замковыми контроллерами осуществляется через драйвер связи DN-12201 по интерфейсу RS-485. Скорость обмена информацией составляет 9600 бод.

При нарушении связи с концентратором замковые контроллеры через 5 с переходят в аварийный режим работы и берут на себя функции управления доступом и регистрации событий. Доступ в этом случае зависит от установленного варианта функционирования замковых контроллеров в аварийном режиме работы подсистемы и списка аварийных карт (до 1000 шт.).

В аварийном режиме возможны следующие варианты функционирования замковых контроллеров:

- Замкнуто, доступ запрещен — проход возможен только с использованием механического ключа.
- Открыто, доступ разрешен — исполнительные устройства находятся в разблокированном состоянии, доступ неограничен.
- Доступ по картам из аварийного списка — доступ через исполнительные устройства разрешен только с использованием карт внесенных в аварийный список доступа, или кнопки дистанционного управления.

4.2.1.1 Принципы функционирования концентратора (контроллера-концентратора)

В процессе функционирования системы PERCo-SYSTEM-12000 связь сервера со всеми замковыми контроллерами, входящими в данную подсистему, осуществляется через ее концентратор (контроллер-концентратор). Таким образом, при нарушении связи сервера с этим концентратором (контроллером-концентратором) одновременно прерывается связь со всеми замковыми контроллерами PERCo-CL-12200 данной подсистемы.

Осуществляя мониторинг драйверов/контроллеров подсистемы, концентратор (для драйверов — только контроллер-концентратор):

- принимает коды предъявленных карт и, после анализа их прав, разрешает или запрещает доступ, фиксируя событие в журнале регистрации;
- следит за состоянием исполнительных механизмов, тестовых входов и релейных выходов, реагируя на их изменение и фиксируя их в журнале регистрации;
- в зависимости от параметров конфигурации ресурсов подсистемы и времени суток выдает команды активизации ресурсов;
- управляет генерацией сигналов тревоги в подсистеме в случае нештатных ситуаций.

В случае нарушения связи с замковым(и) контроллером(ми) подсистемы концентратор (контроллер-концентратор) продолжает мониторинг этого(их) замкового(ых) контроллера(ов) и сразу же после восстановления связи передает в него (в них) все изменения, произошедшие за время аварии.

Одновременно с восстановлением связи концентратор (контроллер-концентратор) осуществляет повторную инициализацию текущего режима контроля доступа для данного замкового контроллера и считывает все события, произошедшие за время отсутствия связи.

Индикация состояния связи с драйверами/замковыми контроллерами подсистемы осуществляется с помощью индикатора "DRIVER" (см п. 4.2.6.).

4.2.1.2 Принципы функционирования замкового контроллера

При первом включении замковый контроллер не имеет параметров функционирования исполнительных механизмов, тестовых входов, релейных выходов, служебных выходов и считывателей. Все эти ресурсы не могут быть использованы до тех пор, пока не будут переданы параметры функционирования каждого из ресурсов.

Установки замкового контроллера по умолчанию следующие:

- Служебные выходы установлены в нормальное состояние;
- Дистанционное управление разрешено;
- Тестовые входы не маскируются;
- Список пропусков пуст;
- Журнал регистрации событий пуст;
- Текущее время не установлено;
- В аварийном режиме замковый контроллер закрывает исполнительные механизмы и запрещает доступ.

Аварийный режим работы контроллера

Если в процессе работы контроллера происходит прекращение его связи с концентратором, то через 5 с после этого он переходит в аварийный режим работы. Индикатор на плате контроллера замков начинает мигать зелёным светом.

Контроллер для работы в аварийном режиме может быть сконфигурирован следующим образом:

- контроллер закрывает замки и по предъявлению считывателю карт фиксирует событие **“Отказ в доступе”**;
- контроллер поддерживает замки в открытом состоянии, и по предъявлению считывателю карт из списка доступа фиксирует события **“Проход”** или **“Попытка доступа”**. По предъявлению считывателю карт, которые отсутствуют в списке доступа, происходит фиксация события **“Отказ в доступе”**;
- контроллер закрывает замки и производит допуск только по картам из аварийного списка доступа или по сигналу от кнопки дистанционного управления. После предъявления считывателю карты из аварийного списка доступа и совершения прохода фиксируется событие **“Проход”**. Если проход не был совершён в течение времени анализа карты, фиксируется событие **“Попытка доступа”**. По предъявлению считывателю карт, которые отсутствуют в списке аварийного доступа, происходит фиксация события **“Отказ в доступе”**.

Для работы в аварийном режиме контроллеру необходимо заранее передать список карт, дающих право доступа в данном режиме. Фиксация событий, связанных с предъявлением считывателю карт из списка, осуществляется только после того, как будет установлено текущее время.

Фиксируемые события:

- Попытка доступа (проход не был совершён до истечения времени анализа карты).
- Проход (проход был совершён).
- Отказ в доступе (проход был запрещён).

После восстановления связи контроллера с концентратором, индикатор на плате контроллера замков загорается постоянно зелёным светом, индицируя переход в системный режим работы. Журнал регистрации событий, которые происходили во время аварийного режима работы, считывается и обрабатывается системными ресурсами.

4.2.2 Права доступа и режим контроля доступа

Под правом доступа карты понимают следующее:

- разрешена ли карта в данной системе;
- через какие считыватели каких терминалов контроля доступа разрешен доступ;
- временной критерий допуска (временная зона, недельный график, сменный график);
- контроль местоположения (невозможности пройти во внутреннюю зону, если не пересек границу внешней);
- подверженность комиссионированию (предъявление карты и набор кодовой комбинации на клавиатуре или предъявление двух карт);
- право автономной смены режима контроля доступа.

К группе специальных карт относятся следующие карты:

- **"генеральная"** — доступ которой ничем не ограничен;
- **"охранник"** — предъявление которой сопровождается внутрисистемным сообщением для ПО "Маршрут охраны", а доступ может быть ограничен временем;
- **"разовый пропуск"** — доступ которой может быть ограничен количеством предъявлений карты одному и тому же считывателю, временным критерием допуска (только по временной зоне) и контролем местоположения;
- **"стоп-лист"** — доступ которой запрещен, а ее предъявление приводит к появлению специального системного сообщения и возможной генерации тревоги (рекомендуется внесение в "стоп-лист" утерянных или украденных карт).

Система поддерживает следующие режимы контроля доступа:

1. "Открыто" (аварийный режим);
2. "Автономный контроль" с параметрами;
3. "Системный контроль" с параметрами;
4. "Охрана" (наследует параметры режима "Системный контроль");
5. "Закрето" (аварийный режим).

Режим контроля доступа может быть установлен для любого считывателя, контроллера, пространственной зоны и всей системы.

При присвоении считывателю режима "Открыто" исполнительные механизмы, связанные с этим считывателем, переводятся в разблокированное состояние, а их дистанционное управление блокируется (рекомендуется для быстрого перевода исполнительных механизмов в открытое состояние в случае чрезвычайных ситуаций).

При присвоении считывателю режима "Автономный контроль" исполнительные механизмы, связанные с этим считывателем, переводятся в заблокированное состояние, и доступ через исполнительный механизм возможен в следующих случаях:

- при нажатии кнопки дистанционного управления;
- при наборе на клавиатуре 4-значной кодовой комбинации, задаваемой в параметрах режима контроля доступа;
- под управлением ПО "Управление системой".

При присвоении считывателю режима "Системный контроль" исполнительные механизмы, связанные с этим считывателем, переводятся в заблокированное состояние, и доступ через исполнительный механизм возможен в следующих случаях:

- при предъявлении карты с соответствующими правами доступа;
- при нажатии кнопки дистанционного управления;
- под управлением ПО "Управление системой".

При присвоении считывателю режима "Охрана" исполнительные механизмы, связанные с этим считывателем, переводятся в заблокированное состояние, и доступ через исполнительный механизм возможен в следующих случаях:

- при предъявлении карты с правом автономной смены режима или спецкарты ("охранник" или "генеральный");

- при нажатии кнопки дистанционного управления;
- под управлением ПО "Управление системой".

При присвоении считывателю режима "Закрыто" исполнительные механизмы, связанные с этим считывателем, переводятся в заблокированное состояние, их дистанционное управление запрещается (рекомендуется для быстрого перевода исполнительных механизмов в заблокированное состояние в случае необходимости экстренно ограничить перемещение по контролируемой территории).

Доступ через исполнительный механизм в режиме "Закрыто" возможен:

- при предъявлении спецкарт ("охранник" или "генеральный");
- под управлением ПО "Управление системой".

К базовым режимам системы относятся "Системный контроль" и "Охрана"

Режим "Системный контроль" имеет набор следующих атрибутов, которые позволяют плавно ужесточать или смягчать режим контроля:

1. Контроль времени доступа.

Может быть установлен один из следующих атрибутов:

- контроль времени отсутствует;
- мягкий контроль времени (доступ разрешен, нарушение фиксируется в мониторинге и может вызвать генерацию тревоги);
- жесткий контроль времени (доступ запрещен, нарушение фиксируется в мониторинге и журнале регистрации и может вызвать генерацию тревоги).

При установке соответствующих атрибутов при жестком контроле времени возможна организация доступа нарушителя через процедуру запроса на подтверждение на пульт дистанционного управления или на монитор компьютера с загруженным ПО "Удаленное управление".

2. Контроль зональности (местоположения).

Может быть установлен один из следующих атрибутов:

- зональный контроль отсутствует;
- мягкий зональный контроль (доступ разрешен, нарушение фиксируется в мониторинге и может вызвать генерацию тревоги);
- жесткий зональный контроль (доступ запрещен, нарушение фиксируется в мониторинге, журнале регистрации и может вызвать генерацию тревоги).

При установке соответствующих атрибутов при жестком контроле местоположения возможна организация доступа нарушителя через процедуру запроса на подтверждение на пульт дистанционного управления или на монитор компьютера с загруженным ПО "Удаленное управление".

3. Автономная смена режима контроля доступа (только снятие с охраны).

Может быть установлен один из следующих атрибутов:

- управление только системой (снятие с охраны производится только под управлением ПО "Управление системой");
- управление системой и пропуском - снятие с охраны производится:
 - двойным предъявлением карты, обладающей правом автономной смены режима контроля доступа и удовлетворяющей остальным критериям допуска (если карта коммиссионирована другой картой, то под двойным предъявлением следует понимать предъявление основной и коммиссионированной карт);
 - под управлением ПО "Управление системой".
- системой и пропуском с подтверждением от компьютера — снятие с охраны производится:
 - двойным предъявлением карты, обладающей правом автономной смены режима контроля доступа, удовлетворяющей остальным критериям допуска и подтверждаемой от управляющего модуля ПО "Удаленное управление";
 - под управлением ПО "Управление системой".

4. Все проходы с подтверждением.

Может быть установлен один из следующих атрибутов:

- без подтверждения (при предъявлении карты, удовлетворяющей всем текущим критериям доступа, исполнительный механизм сразу разблокируется);
- с подтверждением от дистанционного управления (при предъявлении карты, удовлетворяющей всем текущим критериям доступа, исполнительный механизм разблокируется после нажатия кнопки дистанционного управления);
- с подтверждением от компьютера (при предъявлении карты, удовлетворяющей всем текущим критериям доступа, исполнительный механизм разблокируется после выдачи подтверждения от управляющего модуля ПО "Удаленное управление").

5. Автоблокировка при запрещении доступа.

Установка этого атрибута позволяет автоматически блокировать исполнительный механизм в случае предъявления карты, доступ которой запрещен.

Устанавливаемый режим "Охрана" всегда наследует все текущие атрибуты режима "Системный контроль".

6. Выборочный контроль.

Установка данной опции позволяет автоматически (по определенному закону) переводить режим прохода из свободного доступа по всем картам, в доступ с подтверждением от дистанционного управления и обратно.

В качестве закона для переключения режима доступа может выбран:

- по временному критерию;
- случайным образом.

Выбор одного из этих законов позволяет автоматически (на один проход) переходить в режим доступа с подтверждением от дистанционного управления, или каждые 5÷30 минут, или случайным образом, но не реже, чем каждый 30 проход.

4.2.3. Временные критерии доступа

К временным критериям доступа относятся:

- временные зоны контроля;
- недельные графики;
- сменные графики;
- календарь праздничных дней.

Каждая временная зона состоит из восьми интервалов времени суток и имеет свой фиксированный уникальный номер.

При присвоении карте временной зоны первые четыре интервала времени ограничивают доступ со стороны первого считывателя, а другие четыре со стороны второго.

Недельный график состоит из десяти временных зон, каждая из которых связана с одним из семи дней недели и одним из трех типов праздничных дней (см. ниже календарь праздничных дней).

Присвоение карте недельного графика позволяет автоматически изменять временные ограничения этой карты в зависимости от дней недели, праздничных и предпраздничных дней.

Каждый сменный график может быть длиной от одного до тридцати дней и представляет собой список временных зон, по одной для каждого дня графика.

Присвоение карте сменного графика позволяет автоматически изменять временные ограничения этой карты в зависимости от текущего дня смены.

Календарь праздничных дней позволяет любому из дней года присвоить атрибуты праздничного дня одного из трех типов.

Доступ карт, связанных с недельным графиком, в праздничные дни ограничивается по времени временной зоной, присвоенной празднику соответствующего типа и не зависит от текущего дня недели.

Временные зоны и недельные графики, кроме временных ограничений доступа, используются также в качестве критериев автоматизации управления следующими ресурсами системы:

- исполнительный механизм (открытие/закрытие);
- дистанционное управление исполнительным механизмом (запрещение/разрешение использования);
- тестовый вход (разрешение/запрещение мониторинга);
- релейный выход (активизация/нормализация).

При этом все восемь интервалов времени суток, входящие в состав временной зоны, будут использованы для автоматизации управления соответствующим ресурсом.

Комбинация атрибутов режима контроля доступа, временных критериев автоактивизации и параметров генератора тревоги позволяет реализовать практически любой метод обеспечения безопасности контролируемой территории.

4.2.4. Мониторинг и регистрация

В процессе работы система осуществляет сбор и регистрацию практически всех событий и состояний каждого терминала контроля доступа. Сбор информации осуществляется двумя независимыми потоками: мониторингом и регистрацией.

Все события протоколируются с учетом календарной даты и времени суток (с точностью до секунды).

Максимальный ресурс хранения событий мониторинга при выключенном сервере системы определяется буфером мониторинга и равен 512 событиям. В случае переполнения новые события заменяют наиболее старые.

Максимальный ресурс хранения событий регистрации определяется буфером каждого контроллера и равен 16384 события (для каждого контроллера). В случае переполнения новые события заменяют наиболее старые.

4.2.4.1. Перечень возможных событий мониторинга и причины их формирования

4.2.4.1.1. События, связанные с предъявлениями карт

1. Нарушение режима контроля доступа (вызвавшее или нет генерацию тревоги, в зависимости от параметров генератора тревоги) по следующим причинам:

- карта запрещена;
- карта включена в стоп-лист;
- карта не относится к системным, т.е. карта не входит в сегментированный набор системных карт;
- нарушение коммиссионирования, т.е. было зафиксировано несоответствие с коммиссионирующей картой или кодовой комбинацией, или коммиссионирование не было выполнено вообще;
- несоответствие временным критериям доступа;
- несоответствие текущему местоположению, т.е. предъявленная карта нарушила зональность данной системы;
- предъявленная карта не имеет права доступа через исполнительный механизм, считыватель которого находится в режимах "Охрана" или "Закрето".

2. Автономная смена режима контроля доступа, т.е. предъявленная карта осуществила смену режима. Кроме информации о владельце карты, событие содержит наименование установленного режима ("Системный контроль" или "Охрана").

4.2.4.1.2. События, связанные с состоянием исполнительного механизма

1. Несанкционированное открытие исполнительного механизма, вызвавшее генерацию тревоги (в зависимости от параметров генератора тревоги). Оно возникает при активизации состояния блокирующего контакта, не сопровождающегося санкционированным системой открытием исполнительного механизма.

2. Недопустимо долгое открытие исполнительного механизма, вызвавшее генерацию тревоги (это зависит от параметров генератора тревоги). Оно возникает, если время активизации состояния блокирующего контакта превысило установленное предельное время разблокировки. Если исполнительный механизм был разблокирован картой, то дополнительно фиксируется и номер этой карты (или последней прошедшей карты).

3. Исполнительный механизм разблокирован или заблокирован. Событие отражает изменение текущего состояния блокирующего контакта.

4.2.4.1.3. События, связанные с изменением текущего состояния тестовых входов

Активизация (вызвавшая или нет генерацию тревоги, в зависимости от параметров генератора тревоги) или нормализация состояния тестового входа.

4.2.4.1.4. События, связанные с изменением текущего состояния контроллера или системы

1. *Изменение режима контроля доступа по команде оператора системы.* Возникает в случае смены текущего режима под управлением ПО "Управление системой".

2. *Переполнение или очистка журнала регистрации контроллера.* Переполнение журнала возникает после заполнения в памяти контроллера предпоследней свободной страницы журнала (размер одной страницы равен 32 событиям). Очистка журнала происходит всегда после чтения переполненного журнала регистрации.

3. *Авария или восстановление сетевого питания.* Авария сетевого питания возникает в случае отсутствия внешнего сетевого питания, т.е. при переходе контроллера на питание от встроенного резервного аккумулятора.

4. *Авария или восстановление аккумуляторного питания.* Авария аккумуляторного питания возникает при разряде встроенного резервного аккумулятора до напряжения 10 ± 0.5 В. Это событие сопровождается автоматическим выключением контроллера. Восстановление аккумуляторного питания возникает после включения контроллера с восстановленным сетевым питанием и предельно разряженным аккумулятором. Это событие означает восстановление возможности заряда аккумулятора в фоновом режиме. Сам процесс заряда может длиться несколько часов, в зависимости от степени разряда.

5. *Нарушение или восстановление системной конфигурации.* События связаны с нарушением или восстановлением энергонезависимости оперативной памяти контроллера и, как следствие, с потерей или восстановлением системных установок, необходимых для нормального функционирования. Для восстановления системных установок, кроме восстановления энергонезависимости, необходимо произвести конфигурацию системы.

6. *Тревога или сброс тревоги.* События связаны с возникновением тревожной ситуации в системе (см. параметры генератора тревоги) и сбросом сигнала тревоги оператором системы под управлением ПО "Управление системой".

7. *Активизация или нормализация состояния релейного выхода.* События связаны с изменением текущего уровня сигнала релейного выхода. Активизация и нормализация релейного выхода возможна как вследствие конфигурационных установок, так и под управлением ПО "Управление системой".

8. *Нарушение или восстановление связи с драйвером.* Эти события относятся к разряду диагностических и отражают возможное нарушение и восстановление работоспособности структурных элементов системы. Нарушение связи с драйвером влечет за собой полное прекращение управления следующими ресурсами: исполнительные механизмы, мониторинг тестовых входов, релейные выходы (соответственно, невозможна громкая тревога) и служебные выходы.

9. *Нарушение или восстановление связи с контроллером.* Эти события относятся к разряду диагностических и отражают возможное нарушение и восстановление работоспособности структурных элементов системы. Нарушение связи с первичным контроллером системы фактически означает нарушение связи со всей системой в целом.

4.2.4.1.5. События, связанные с протоколированием действий операторов

Все действия операторов, связанные с изменением свойств и параметров системы, управлением ресурсами системы и запуском модуля(ей) ПО или выходом из них, сопровождаются регистрацией в журнале мониторинга с учетом времени и имени оператора вводимого при входе в модуль ПО.

4.2.4.2. Перечень возможных событий регистрации и причины их формирования

4.2.4.2.1. События, связанные с перемещением через исполнительный механизм

1. Отказ карте в доступе по причине:

- карта запрещена;
- карта включена в стоп-лист;
- карта не относится к системным, т.е. карта не входит в сегментированный набор системных карт;
- нарушение коммиссионирования, т.е. было зафиксировано несоответствие с коммиссионирующей картой или кодовой комбинацией, или коммиссионирование не было выполнено вообще;
- несоответствие временным критериям доступа;
- несоответствие текущему местоположению, т.е. предъявленная карта нарушила зональность данной системы;
- нарушение текущего режима, т.е. предъявленная карта не имеет права доступа через исполнительный механизм, считыватель которого находится в режимах "Охрана" или "Закрето";
- запрещающая команда охранника или оператора системы.

2. *Попытка доступа карты,* т.е. отказ от предоставленного системой права пройти через исполнительный механизм.

3. Проход по карте или без карты. Проходы по карте подразделяются на:

- просто проход;
- проход с подтверждением по времени (нарушение времени с допуском через процедуру запроса на подтверждение);
- проход с подтверждением по местоположению (нарушение зональности с допуском через процедуру запроса на подтверждение).

4.2.4.2.2. События, связанные со сменой режима контроля доступа

1. Автономная смена режима контроля доступа. Причина формирования и содержание аналогичны такому же событию мониторинга.

2. Смена режима контроля доступа оператором системы. Причина формирования и содержание аналогичны такому же событию мониторинга.

4.2.4.2.3. События, связанные с изменением текущего состояния тестовых входов

Активизация (вызвавшая или нет генерацию тревоги, в зависимости от параметров генератора тревоги) или нормализация состояния тестового входа.

4.2.4.2.4. События, связанные с изменением текущего состояния контроллера или системы

1. *Включение или выключение питания контроллера.* Выключение питания может возникнуть в двух случаях: или при штатном выключении контроллера (см. "PERCo-SYSTEM-12000. Инструкция по монтажу"), или при аварийном выключении, связанным с аварией сети и разрядом аккумулятора. Включение питания

возникает аналогично выключению в двух случаях: или при штатном включении контроллера, или при восстановлении сетевого питания.

2. *Переполнение или очистка журнала регистрации контроллера.* Причины формирования аналогичны такому же событию мониторинга.

3. Авария или восстановление сетевого питания. Причины формирования аналогичны такому же событию мониторинга.

4. *Авария или восстановление аккумуляторного питания.* Причины формирования аналогичны такому же событию мониторинга.

5. Нарушение или восстановление связи с драйвером. Причины формирования аналогичны такому же событию мониторинга.

6. *Нарушение или восстановление связи с первичным устройством системы.* Событие отражает наличие связи между элементами системы и, в зависимости от иерархического положения, отражает следующее:

- для первичного контроллера — нарушение связи с сервером системы;
- для вторичного контроллера — нарушение связи с первичным контроллером.

4.2.5. Перемещения персонала. Интерфейс пользователя

Пользователь системы, обладающий картой с соответствующими правами (с которыми он должен быть ознакомлен, во избежание недоразумений) имеет возможность пройти через любой терминал, доступ через который ему разрешен. После первого предъявления карты считывателю система определяет её текущее местоположение (пространственная зона контроля), которое в дальнейшем отслеживает после каждого следующего предъявления.

Результатом предъявления карты, в зависимости от её прав доступа, может быть:

- открытие исполнительного механизма, сопровождающееся индикацией события "доступ разрешен" через служебные выходы;
- блокирование исполнительного механизма (если установлена автоблокировка), сопровождающееся индикацией "доступ запрещен" через служебные выходы;
- блокирование исполнительного механизма (если установлена автоблокировка), сопровождающееся индикацией "запрос на подтверждение от дистанционного управления" через служебные выходы;
- блокирование исполнительного механизма (если установлена автоблокировка), сопровождающееся индикацией "запрос на подтверждение от компьютера" через служебные выходы;
- блокирование исполнительного механизма (если установлена автоблокировка), сопровождающееся индикацией "ожидание комиссионирования" через служебные выходы;
- открытие исполнительного механизма, сопровождающееся индикацией события "ожидание автономной смены режима контроля доступа" через служебные выходы (режим "Системный контроль");
- блокирование исполнительного механизма (если установлена автоблокировка), сопровождающееся индикацией события "ожидание автономной смены режима контроля доступа" через служебные выходы (режим "Охрана").

Открытие исполнительного механизма с помощью дистанционного управления не сопровождается индикацией через служебные выходы, за исключением случаев подтверждения прохода по карте, хотя в состав системы входят электромеханические исполнительные механизмы с расширенными средствами индикации и дистанционного управления (электромеханические турникеты типа PERCo-TTR-04X), см. приложение 1.

4.2.6. Диагностика состояния системы и ее элементов.

Диагностические индикаторы

Диагностика состояния системы осуществляется оператором системы на основании данных мониторинга.

К критическим, с точки зрения дальнейшего функционирования, относятся следующие события:

- **Авария сетевого питания.** Это событие связано с возникшим нарушением сетевого питания контроллера и автоматическим переходом на питание от встроенного аккумулятора. Если это событие сопровождается событием "Нарушение связи с контроллером", то вполне возможно, что произошло выключение контроллера тумблером "Сеть".
- **Авария аккумуляторного питания.** Это событие связано с предельным разрядом встроенного аккумулятора и обычно сопровождается событием "Нарушение связи с контроллером", возникающим по причине автоматического выключения контроллера.
- **Нарушение системной конфигурации.** Это событие связано с потерей энергонезависимости памяти первичного контроллера (потеря энергонезависимости вторичного контроллера диагностируется через индикатор, см. ниже) и может означать следующее:
 - разрядилась встроенная литиевая батарейка;
 - нарушился контакт в перемычке "J2-Энергонезависимость" (см. "Инструкцию по монтажу");
 - кратковременный сбой, связанный с мощной электромагнитной наводкой на блок контроллера.

Проведение повторной конфигурации чаще всего позволяет восстановить работоспособность контроллера, но после последующего выключения/включения питания контроллера это событие может повториться. Это является следствием сохранившейся неисправности.

- **Нарушение связи с драйвером/замковым контроллером.** Это событие связано с возникшим нарушением обмена между системой и конкретным драйвером/замковым контроллером и, как следствие, с невозможностью управления ресурсами этого драйвера/замкового контроллера (исполнительные механизмы, тестовые входы, релейные и служебные выходы).

- **Нарушение связи с контроллером.** Это событие связано с возникшим нарушением обмена между системой и конкретным контроллером и, как следствие, с невозможностью управления его ресурсами (драйверы, считыватели и т.д.). Нарушение связи с первичным контроллером означает нарушение обмена со всем аппаратным составом, подключенным через данный первичный контроллер. Чаще всего это событие связано с выключением питания контроллера, но может означать и нарушение линии связи или наличие мощной электромагнитной помехи (см. "Инструкцию по монтажу").

На лицевой панели блока каждого контроллера расположена линейка диагностических индикаторов следующего функционального назначения:

DRIVER — индикатор связи с драйвером/замковым контроллером, подключенным к данному контроллеру;

SYNC CH — индикатор связи в магистрали, связывающей контроллеры системы;

ASYNCH — индикатор связи между сервером системы и первичным контроллером;

CONFIGURATION — индикатор целостности системных установок, необходимых для нормального функционирования;

PRIMARY — индикатор текущей установки перемычки Primary/Slave, определяющей иерархическое положение контроллера;

BATTERY — индикатор работоспособности цепи заряда аккумулятора и непосредственно самого аккумулятора;

POWER — индикатор наличия сетевого питания.

Нормальный цвет свечения всех диагностических индикаторов "зеленый". Переход индикаторов (кроме "PRIMARY") в режим "красного" свечения свидетельствует о неисправности данной функции. Индикатор "PRIMARY" непосредственно связан с перемычкой Primary/Slave и светится только в случае, если эта перемычка установлена, т.е. контроллер является первичным в данной ветви контроллеров (смотри п.2.2.).

ПРИЛОЖЕНИЕ 1

Стойка турникета-трипода PERCo-T-04W. Индикация состояний и дистанционное управление.

Эти электромеханические устройства обладают следующими особенностями:

1. Хотя структурно стойка турникета в системе представляет собой два независимых исполнительных механизма, описание параметров их функционирования должно быть взаимосвязано. Это необходимо, в первую очередь, из-за датчиков блокировки, последовательный анализ которых важен при фиксации завершения прохода через каждый исполнительный механизм.

2. На стойке турникета-трипода PERCo-T-04W расположено табло индикации, которое состоит из трех индикаторов:

- зелёная стрелка направления (исполнительный механизм 1);
- зелёная стрелка направления (исполнительный механизм 2);
- центральный красный крест.

Стрелки предназначены для индикации разблокированного состояния соответствующего исполнительного механизма (непрерывный режим индикации) и, в частном случае, индицируют запрос на подтверждение прохода (пульсирующий режим индикации).

Крест предназначен для индикации состояния механизма блокировки обоих исполнительных механизмов и имеет следующие режимы индикации:

- горит постоянно, если оба исполнительных механизма заблокированы;
- мигает, если через один из исполнительных механизмов совершается проход, или не зафиксирован полный проворот преграждающей планки турникета;
- не горит, если один или оба исполнительных механизма разблокированы, но проход не совершается.

3. Пульт дистанционного управления имеет линейку из трех индикаторов, полностью совпадающую по функциональному назначению и режимам индикации с индикаторным табло стойки турникета-трипода PERCo-T-04W. Кроме того, пульт снабжен линейкой из трех кнопок и пьезоизлучателем.

Пьезоизлучатель предназначен для звукового сопровождения запросов на подтверждение прохода (прерывистый звук) или запрещения дистанционного управления исполнительным механизмом (непрерывный звук в течении 2-3 с).

Левая и правая кнопки предназначены для управления раздельным открытием исполнительного механизма 1 и исполнительного механизма 2, а центральная кнопка является общей и предназначена для блокировки обоих исполнительных механизмов или формирования спецкоманд. Общий перечень команд управления представлен в табл. 1.

СПОСОБ ФОРМИРОВАНИЯ	ОСНОВНАЯ ФУНКЦИЯ	ДОПОЛНИТЕЛЬНАЯ ФУНКЦИЯ
Нажатие крайней кнопки	Открытие соответствующего ИМ в режиме однократного* прохода	Подтверждение прохода при наличии запроса на подтверждение
Нажатие центральной кнопки	Закрытие обоих ИМ	Отказ в подтверждении прохода. Приведение турникета в рабочее положение
Одновременное нажатие крайней и центральной кнопки	Открытие соответствующего ИМ в режиме многократного** прохода	
Одновременное нажатие обоих крайних и центральной кнопки	Открытие обоих ИМ в режиме многократного** прохода	

* Приведение стойки турникета в рабочее положение — необходимо в случае некорректного совершения прохода. Признаком некорректного прохода для стойки турникета-трипода типа PERCo-T-04W является мигание "креста" (см. табло индикации) и центрального (красного) индикатора пульта управления при блокировании обоих исполнительных механизмов.

** Однократный проход — исполнительный механизм открывается на время удержания в открытом состоянии (см. параметры исполнительного механизма) и блокируется после совершения прохода или истечения этого времени.

*** Многократный проход — исполнительный механизм открывается на время удержания в открытом состоянии (см. параметры исполнительного механизма) и блокируется только в случае, если в течение этого времени через исполнительный механизм не совершалось ни одного прохода.

ПРИЛОЖЕНИЕ 2

Инструкция по автономной постановке и снятию с охраны помещений контролируемых СКД PERCo-SYSTEM-12000

1. Постановка в режим "ОХРАНА". Покиньте помещение, плотно закрыв за собой дверь. Убедитесь в том, что индикатор считывателя соответствует нормальному состоянию (см. Конфигуратор — Работа с ТКД — Панель состояния — Функциональные свойства объекта — Индикация РКД — Системный контроль). Поднесите карту, обладающую правом автономной смены режима (АСРКД), к считывателю. После этого, считыватель перейдет к индикации "Ожидание смены режима" (см. Конфигуратор — Работа с ТКД — Панель состояния — Функциональные свойства объекта — Индикация событий — Ожидание смены режима). Пока считыватель индицирует "Ожидание смены режима", повторно поднесите к считывателю ту же карту.

Считыватель перейдет к индикации "Смена РКД" (см. Конфигуратор — Работа с ТКД — Панель состояния — Функциональные свойства объекта — Индикация событий — Смена РКД). Считыватель перейдет к индикации "Охрана" (см. Конфигуратор — Работа с ТКД — Панель состояния — Функциональные свойства объекта — Индикация РКД — Охрана).

Внимание! Для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замков "CISA"), необходимо в течение 10 с открыть и тут же закрыть дверь.

Помещение поставлено в режим "Охрана".

2. Снятие с режима "ОХРАНА". Убедитесь в том, что считыватель индицирует состояние "Охрана" (см. Конфигуратор — Работа с ТКД — Панель состояния — Функциональные свойства объекта — Индикация РКД — Охрана) т.е. помещение находится в режиме "Охрана". Поднесите карту, обладающую правом автономной смены режима (АСРКД), к считывателю. После этого, считыватель перейдет к индикации "Ожидание смены режима" (см. Конфигуратор — Работа с ТКД — Панель состояния — Функциональные свойства объекта — Индикация событий — Ожидание смены режима). Пока считыватель индицирует "Ожидание смены режима", повторно поднесите к считывателю ту же карту. Считыватель перейдет к индикации "Смена РКД" (см. Конфигуратор — Работа с ТКД — Панель состояния — Функциональные свойства объекта — Индикация событий — Смена РКД), замок двери разблокируется, а считыватель перейдет к индикации "Доступ разрешен" (см. Конфигуратор — Работа с ТКД — Панель состояния — Функциональные свойства объекта — Индикация событий — Доступ разрешен). По истечении времени данной индикации считыватель перейдет к индикации "Системный контроль" (см. Конфигуратор — Работа с ТКД — Панель состояния — Функциональные свойства объекта — Индикация РКД — Системный контроль), что означает снятие помещения с "Охраны" и перевод в режим "Системный контроль".

3. Возможные причины отказа в автономной смене режима контроля доступа. Постановка в режим "Охрана" осуществляется при недостаточно хорошо закрытой двери или неисправном датчике двери. Параметры РКД "Системный контроль" запрещают автономную смену режима контроля доступа, т.е. были изменены установки системы. Используемая карта не обладает правом автономной смены режима. Используемая карта нарушила один из установленных в данный момент критериев контроля доступа (время, местоположение и т.п.).

СЕРВИСНЫЕ ЦЕНТРЫ PERCo:

Москва ул. Краснобогатырская, 2 стр.1, офис 411 Тел.: (095) 514-35-84 Факс: (095) 913-30-39 E-mail: naladka@sotops.ru	ООО "СОТОПС"	Минск ул. Кульман, 2, офис 424 Тел.: (10-375-17) 232-35-52 Факс: (10-375-17) 232-70-52 E-mail: pb9160@belsonet.net	ИВО "Просвет"
Москва Ленинградский пр., 80, корп. 5А, офис 203 Тел.: (095) 799-92-80 Факс: (095) 799-92-81 E-mail: mail@megalion.ru	ООО "Компания МЕГАЛИОН"	Нижний Новгород ул. Алексеевская, 26 Тел.: (8312) 78-40-02 Факс: (8312) 78-40-01 E-mail: perco@r-style.nnov.ru	ООО "Эр-Стайл Волга"
Санкт-Петербург Б. Сампсониевский пр., 87 Тел.: (812) 324-17-51 Факс: (812) 324-17-54 E-mail: service@telros.ru	ЗАО "ТЕЛРОС"	Новосибирск ул. Коммунистическая 43 Тел.: (3832) 125-255, 125-235 Факс: (3832) 125-255, 125-235 E-mail: bedarev@ctgroup.ru	ООО "Си-Трэйд Новосибирск"
Барнаул Социалистический пр., 109 Тел.: (3852) 23-10-08, (3852) 23-10-98 Факс: (3852) 66-69-00 E-mail: support@ctrade.ru	ООО "СТ Group"	Ростов-на-Дону ул. 1-й Конной Армии, 15а, офис 405 Тел.: (8632) 90-83-60, 52-48-13 Факс: (8632) 58-71-70 E-mail: perco@r-style.donpac.ru	ООО "R-Style Дон"
Воронеж Московский пр., 4, офис 919 Тел.: (0732) 51-22-25 многоканальный Факс: (0732) 51-22-25 E-mail: perco@radomir.intercon.ru	ООО "Радомир"	Тольятти ул. Юбилейная, 31Е, оф. 705 Тел.: (8482) 70-65-46, 42-02-41 Факс: (8482) 70-65-46, 42-02-41 E-mail: perco@unitcom.ru	ООО "Юнит"
Екатеринбург Виз-бульвар, 13, ТЦ, ком. 524 Тел./Факс: (3433) 727227 E-mail: armo-ural@armo.ru	ООО "АРМО-Урал"	Тюмень ул. Северная, 3 Тел.: (3452) 45-55-13 Факс: (3452) 45-55-13 E-mail: perco@tmk-pilot.ru	ООО ТМК "ПИЛОТ"
Красноярск пр. Мира, 10, офис 550 Тел.: (3912) 522-422, 522-423 Факс: (3912) 522-424 E-mail: stb@stbk.ru	ООО "СТБ"		

Получить свежую информацию о сервисных центрах Вы можете на нашем интернет-сайте **www.perco.ru**, а также по телефону (812) 321-61-55, 517-85-45

Услуги, предоставляемые сервис-центрами PERCo:

- гарантийный и послегарантийный ремонт оборудования
- технические консультации
- обучение пользователей
- продажа запчастей
- монтаж и пусконаладка оборудования, инсталляция и настройка ПО

По вопросам, связанным с работой сервис-центров компании, пожалуйста, обращайтесь в Департамент сервисного обслуживания PERCo

телефон: (812) 321-61-55
517-85-45
e-mail: **service@perco.ru**

Почтовый адрес:
195267, **Санкт-Петербург**, а/я 109

пр. Просвещения, 85
Тел.: (812) 329-89-24,
329-89-25
Тех. поддержка:
(812) 321-61-55
(812) 517-85-45
Факс: (812) 517-68-84
E-mail: system@perco.ru
soft@perco.ru

Почтовый адрес:
123007, **Москва**, 4-я Магистральная ул., 11
Тел./факс (095) 221-60-83, 221-60-84,
221-60-85

E-mail: moscow@perco.ru

www.perco.ru