СИСТЕМА КОНТРОЛЯ
И УПРАВЛЕНИЯ ДОСТУПОМ
PERCo-SYS-15000

Техническое описание при эксплуатации с контроллерами серии 12000

CE

Содержание

ВВЕДЕНИЕ

Настоящее **Техническое описание** (в дальнейшем — «**ТО**») предназначено для ознакомления с техническими характеристиками, составом, принципом работы системы контроля и управления доступом PERCo-SYS-15000 при ее эксплуатации с контроллерами серии 12000 (в дальнейшем — «система»). Целью данного ТО является обеспечение правильной эксплуатации системы и наиболее полное использование её технических возможностей при всех режимах работы и в различных условиях эксплуатации. ТО действует совместно с Инструкцией по монтажу контроллеров для системы контроля и управления доступом PERCo-SYS-15000, Инструкцией по монтажу на подсистему замковых контроллеров второго уровня, а так же с паспортами на устройства, входящие и подключаемые к системе.

1. ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ

1.1. Основные возможности

Система обеспечивает эффективное решение следующих задач.

1.1.1. Контроль и управление доступом

Система позволяет организовать пропуск сотрудников на предприятие, в цеха и отдельные помещения, осуществляя идентификацию по бесконтактным картам доступа (далее картам)по принципу «свой-чужой» и регистрируя время прохода. Сотрудникам и посетителям могут задаваться индивидуальные права доступа на объекты. Доступ может разграничиваться:

По времени, т.е. каждому сотруднику задается индивидуальный временной график доступа на объект, при этом система поддерживает многосменные и скользящие графики работы для контроллеров 12000 серии и недельные графики для контроллеров 600 серии. В случае попытки прохода сотрудника вне установленных временных рамок доступа, система не пропустит его, фиксируя при этом время попытки прохода;

По статусу, т.е. для каждого сотрудника можно определить объекты, на которые он имеет право доступа и право постановки/снятия на охрану.

Система позволяет запретить двойной проход в одну сторону через турникет, что решает проблему с передачей пропуска другому человеку. Если речь идет о разграничении доступа на особо важные объекты, в системе предусмотрена (в случае 12000 контроллеров) многоуровневая идентификация сотрудника: организация доступа при условии «карта + набор кода», по принципу «только вдвоем» (комиссионное вскрытие помещения), с дополнительным выборочным контролем охраной (по времени или случайным образом).

На любом из объектов может быть организован режим видеоидентификации, когда право доступа реализуется только с подтверждения охранника после сравнения им полученного от видеокамеры изображения лица, предъявившего карточку, с эталонным изображением владельца карточки, хранящимся в системе (для контроллеров 12000 серии).

В системе, в зависимости от типа используемого оборудования, могут быть доступны дополнительные режимы доступа.

Постановка объектов на внутреннюю системную охрану

В системе предусмотрен специальный режим «Охрана». В режиме «Охрана» попасть на объект могут лишь сотрудники, обладающие правом снятия/постановки объекта на охрану, что позволяет разделить сотрудников на иерархические группы в зависимости от прав доступа. Кроме традиционного режима охраны в ночное время, эта функция ПО может обеспечивать дополнительную безопасность объектов в течение рабочего дня.

Например, уходящий последним из кабинета сотрудник бухгалтерии, может перевести контроллер двери в режим охраны, при котором сотрудники других отделов, обычно имеющие право доступа в бухгалтерию, не будут допущены в этот кабинет. При этом любой сотрудник бухгалтерии, вернувшись, сможет открыть дверь.

В случае возникновения нештатных ситуаций находящаяся в режиме «Охрана» система выдает сигнал тревоги. Все события — тревога, факты постановки / снятия объекта с охраны — запоминаются системой и впоследствии могут быть просмотрены в журнале событий.

1.1.2. Учет рабочего времени и контроль за дисциплиной труда

Система дает возможность получить информацию о времени присутствия любого сотрудника на любой части подконтрольной территории, в частности, на рабочем месте. Она автоматически сопоставляет эти сведения с индивидуальным графиком работы конкретного сотрудника и получает информацию о реально отработанном данным сотрудником времени. Системой также обеспечивается возможность задания и обслуживания недельных, сменных и месячных графиков работы со скользящими интервалами работ, календаря праздничных и выходных дней.

Система регистрирует все происходящие в ней события, как по факту, так и по времени. На основе регистрируемых событий система позволяет получать следующие отчеты:

Время присутствия на рабочем месте
Контроль прихода на работу ранее установленного времени
Контроль задержки на работе
Контроль отсутствия выхода;
Опоздания на работу
Уход с работы раньше времени
Отсутствующие
Общий отчет по всем нарушениям

Отчеты можно создавать как для каждого сотрудника отдельно, так и для группы сотрудников. Система позволяет создавать отчеты за четыре фиксированных периода времени (текущий день, предыдущий день, текущая неделя, текущий месяц) и за произвольный период времени.

1.1.3. Автоматизированный кадровый учет, оформление и выдача пропусков

Система обеспечивает ведение базы данных сотрудников (ФИО, подразделение, должность, табельный номер, график работы, фотография, паспортные данные, номер пропуска, права доступа, дополнительные сведения), а также оформление бесконтактных карт в качестве пропусков. Пользователь ПО может создавать и печатать наклейки на пропуска нужного ему вида: с фотографией, информацией о владельце пропуска, логотипом фирмы.

1.2. Программное обеспечение системы

Программное обеспечение предназначено для управления подсистемами контроллеров, цифрового видеонаблюдения и охранно-пожарной сигнализации, а также сбора и обработки информации, поступающей от них. ПО системы построено на клиент-серверной технологии, которая позволяет поднять быстродействие и надежность системы в целом. В качестве сервера БД используется SQL-сервер FireBird.

Базовый комплект поставки системы состоит из ПО сервера аппаратуры серии XXX, соответствующего типу приобретенных контроллеров, и базового пакета, в который входят следующие модули:

- Консоль администратора БД

- Консоль управления со следующими разделами:
  - Конфигуратор
  - Справочники доступа
  - Персонал (с модулем «Оформление пропусков»)
  - Отчеты
  - Доступ на объекты
  - Мониторинг
- Сервер системы
- Сервер управления данными
- Сервер БД

Можно организовать работу системы, установив все ПО на один компьютер или распределив модули по разным хостам, например,определив два выделенных сервера и две рабочие станции. На один выделенный сервер можно установить сервер системы, на другой — сервер управления данными и сервер БД. А на рабочие станции установить консоль управления и консоль администратора.

Кроме базового комплекта ПО, обеспечивающего работу системы в целом, существуют или разрабатываются дополнительные компоненты, расширяющие основные функции системы. Они включают в себя следующие модули:

«Учет рабочего времени»

«Видеоидентификация»

«Мониторинг с мнемосхемами»

«Интеграция с системой видеонаблюдения»

«Интеграция с охранно-пожарной сигнализацией»

«Планировщик задач»

«Мастер отчетов»

ПО поддерживает следующие функции:

Управление подсистемами контроллеров 600 серии (до 64 на один сервер аппаратуры) и 12000 серии (до 128 на один сервер аппаратуры), а также сбор информации с них. Количество подключаемых серверов аппаратуры не ограничено в пределах сети. Количество подключаемых серверов аппаратуры на одном компьютере равно количеству уникальных серий оборудования (на одном компьютере не может быть двух серверов аппаратуры одинаковой серии);

Проведение автоконфигурации системы;

Задание различных прав доступа пользователям ПО системы с помощью паролей;

Ведение базы данных персонала (создание и ведение списков должностей, подразделений, графиков работы, помещений; автоматизированный учет персонала, оформление учетных карточек сотрудников);

Оформление пропусков (разработка шаблонов, автоматизированное оформление и печать пропусков, ввод карт доступа вручную или автоматически с помощью контрольного считывателя);

Задание индивидуальных графиков доступа сотрудников в помещения;

Подключение системы видеонаблюдения;

Подключение системы охранно-пожарной сигнализации;

Формирование отчетов: о рабочем времени сотрудников, о нарушениях (опозданиях, преждевременных уходах, прогулах), как по отдельным сотрудникам, так и по подразделениям;

Мониторинг (слежение за тревожными событиями в системе) и управление аппаратурой с рабочего места оператора (блокировка и разблокировка турникетов, замков, перевод помещений в режим «Охрана», поднятие сигнала тревоги, оперативное запрещение доступа по пропуску в критических ситуациях);

Защита от передачи карт при проходе через турникет;

Управление базами данных и контроль за их сохранностью;

Работать с программным обеспечением рекомендуется под управлением операционных систем MS Windows 2000 (SP4 или выше) / NT (SP6 или выше), Windows XP, Windows Server 2003, хотя возможен вариант работы и под управлением операционной системы Windows 98 SE.

Программное обеспечение организовано по модульному принципу и имеет удобный русскоязычный интерфейс, доступ к управлению которым защищается системой паролей.

Работа ПО в локальных компьютерных сетях предоставляет возможность создания автоматизированных распределенных рабочих мест (АРМов) для различных служб.

АРМ «Администратор»

Обеспечивает удобное и быстрое управление системой:

Управление правами доступа пользователей к разделам ПО

Создание и работа с базами данных

Подключение и изменение настроек аппаратуры

АРМ «Служба безопасности»

Обеспечивает задание прав доступа сотрудников на объекты, позволяет проводить мониторинг системы, обеспечивает удобное и быстрое управление всеми исполнительными устройствами (реакция на тревожные события, оперативный запрет пропуска).

АРМ «Отдел кадров»

Значительно сокращает объем рутинной работы, позволяя автоматизировать кадровый учет, оперативно вносить изменения в кадровое расписание, получать отчеты по сотрудникам, осуществлять контроль за дисциплиной труда.

АРМ «Бюро пропусков»

Значительно облегчает работу по выдаче и учету постоянных и разовых пропусков, ускоряет процесс оформления карт в виде пропуска с фотографией. Фотоизображение может вводиться в компьютер с помощью сканера, цифрового фотоаппарата или видеокамеры. Нанесение изображения на карту может производиться двумя способами: непосредственно на карту с помощью специального принтера или на наклейки с помощью обычного принтера.

1.3. Основные термины и понятия

1.3.1. Общие термины и понятия

Контроллеры доступа — аппаратные модули системы, ее интеллектуальная часть. Они обеспечивают управление исполнительными устройствами и хранение информации о картах доступа и событиях. В системе **PERCo-SYS-15000** могут использоваться контроллеры двух видов — 600 и 12000 серии — образующие две подсистемы контроллеров. Подсистема контроллеров 600 серии имеет в своем составе контроллеры замка и контроллеры турникета. В составе аппаратных модулей 12000 серии, кроме контроллеров замка, имеются концентраторы, объединяющие в сеть замковые контроллеры, а также непосредственно работающие с разными исполнительными устройствами (контроллеры-концентраторы). Контроллеры 600 и 12000 серий имеют различные возможности в плане поддержания графиков доступа. Это обеспечивает гибкую конфигурацию в соответствии с запросами пользователей. Например, на проходной предприятия для организации учета рабочего времени можно применить контроллеры 12000 серии, которые поддерживают большое количество многосменных и скользящих графиков работы и обеспечивают корректный учет, а для оборудования входных дверей использовать более экономичные контроллеры 600 серии.

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

Контрольный считыватель — устройство, предназначенное для считывания и расшифровки кода, содержащегося в карте доступа, с целью автоматической регистрации нового пропуска в системе.

Карта доступа, ее код и серия — пластиковая бесконтактная карта (электронный ключ). Карта доступа содержит чип с уникальным числовым кодом. Общее количество комбинаций чисел кода составляет более 16,5 миллионов, что обеспечивает уникальность каждой карты. Карта не содержит встроенного источника питания, что делает срок службы карты практически неограниченным.

Исполнительные устройства (ИУ) — устройства, преграждающие доступ куда-либо. В качестве исполнительных устройств используются электромеханические и электромагнитные замки, защелки различных типов, турникеты, тумбовые турникеты, роторные турникеты, электромеханические калитки.

Пульт дистанционного управления или **дистанционное управление** — класс устройств, предназначенных для управления доступом через ИУ в интерактивном режиме.

Объекты доступа — охраняемые помещения.

Группа доступа — совокупность прав доступа по всем объектам доступа. Группа доступа присваивается карте доступа и определяет ее возможности в системе.

Точки доступа — места расположения ИУ.

Устройства — аппаратная часть, подключаемая к ИУ.

Защита от передачи карт (Antipassback) — функция, обеспечивающая защиту от передачи пропуска другому лицу. Контроллеры 12000 серии поддерживают глобальную защиту от передачи карт, т. е. в данном случае система не позволит дважды войти на предприятие по одному пропуску не только через тот же турникет, но и через любой другой, в том числе через другую проходную. Более того, если работник все же попал на территорию (например, через забор), система не пропустит его на внутренний объект (в цех или другое помещение).

Права доступа — ограничения, регулирующие возможность посещения сотрудником того или иного объекта.

Временная зона — интервал времени, в течение которого сотрудник имеет право посещения объекта.

Недельный график — схема, задающая время посещения сотрудником объекта в течение семи дней.

Сменный график — схема, задающая время посещения сотрудником объекта в течение заданного периода (до 30 дней).

Мониторинг — автоматический контроль состояния объектов и устройств и предоставление данных о событиях системы в режиме реального времени.

Журнал событий — список событий, произошедших в процессе работы системы за определенный период времени.

Режим доступа — параметры функционирования контроллеров системы: «Открыто», «Закрыто», «Системный контроль», «Автономный контроль», «Охрана».

Регистрация событий в системе — сохранение в энергонезависимой памяти контроллера времени и типа события.

Сервер системы — модуль ПО «Сервер системы», предназначенный для осуществления связи между другими модулями ПО, такими, как модуль ПО “Сервер управления данными” и модулями ПО “Сервер аппаратуры серии 12000 и/или «Сервер аппаратуры серии 600».

Сервер управления данными — модуль, отвечающий за сохранение и обработку всех данных системы.

Сервер БД – FireBird SQL Server - модуль, отвечающий за физическое представление и обработку данных.

Узел аутентификации — программно-аппаратная единица системы, включающая в себя сервер аппаратуры, запускаемый на конкретном ПК, и все аппаратные модули, подключенные к этому ПК через COM-порт.

Драйвер ИУ — плата, встраиваемая в контроллер-концентратор и непосредственно управляющая ИУ (замком, турникетом, калиткой).

Концентратор — аппаратный модуль, представляющий вместе с подключаемыми к нему контроллерами замка (до 7) единую подсистему замковых контроллеров 12000 серии в составе системы PERCo-SYS-15000.

Контроллер-концентратор — аппаратный модуль подсистемы контроллеров 12000 серии, соединяющий в себе функции контроллера (при работе с драйверами ИУ) и концентратора (при работе с контроллерами замка) и предназначенный для управления доступом, регистрации проходов, управления ИУ и поддержки функции охранной сигнализации. Может управлять 2 турникетами или 4 замками. Каждый контроллер-концентратор поддерживает список из 32 000 карт (т.е. в системе может быть до 32 000 пользователей) и имеет энергонезависимый буфер на 16 000 событий.

Контроллер замка — аппаратный модуль системы, входящий в состав сети контроллеров. Замковые контроллеры 600 серии имеют три модификации: со встроенной антенной считывателя (PERCo-SC-600LH, PERCo-SC-600LE), с выносной антенной считывателя (PERCo-SC-601LH, PERCo-SC-601LE), с переговорным устройством (PERCo-SC-600PDP, PERCo-SC-600PDPV с видеокамерой). Контроллеры замка 12000 серии — PERCo-CL-12200H, PERCo-CL-12200E — работают как с выносными антеннами, так и со стандартными считывателями. Контроллеры замка предназначены для:

- Обслуживания одного (для контроллеров 600 серии) или двух (для контроллеров 12000 серии) считывателей (антенн) для бесконтактных карт;
- Управления одним (для контроллеров 600 серии) или двумя (для контроллеров 12000 серии) замками электромагнитного или электромеханического типа по командам от компьютера, пульта дистанционного управления или по сигналу от считывателя бесконтактных карт;
- Управления внешней тревожной сигнализацией;
- Хранения списка из 1000 (контроллеры замка 600 серии) и из 32000 (контроллеры замка 12000 серии) бесконтактных карт;
- Регистрации, хранения и передачи в компьютер до 3000 (контроллеры замка 12000) или 3500 (контроллеры замка 600 серии) событий;
- Ведение аудиопереговоров по двухпроводной линии связи (контроллеры PERCo-SC-600PDP, PERCo-SC-600PDPV);
- Видеонаблюдения за посетителями (контроллер PERCo-SC-600PDPV).

Контроллер турникета (калитки) – аппаратный модуль системы, входящий в состав сети контроллеров. Контроллер турникета (калитки) имеет несколько модификаций: контроллер PERCo-SC-601T, контроллер PERCo-SC-600TH под выносную антенну (оба для турникета-трипода PERCo-T-04(W)), контроллер PERCo-SC-601TR (для роторных турникетов PERCo, тумбового турникета PERCo-TTD-01M, электромеханических калиток PERCo-WHD-03M и PERCo-WHD-04 без привода) и контроллер PERCo-SC-601WM (для электромеханической калитки PERCo-WMD-03M с приводом).

Предназначен для:

- Управления турникетами и калитками по командам от компьютера, кнопочного пульта ДУ или по сигналу от считывателя бесконтактных карт;
- Хранения списка из 2000 бесконтактных карт;
- Регистрации, хранения и передачи в компьютер до 2000 событий (с дополнительной энергонезависимой памятью М-600 - до 6000 событий);

1.3.2. Специализированные термины и понятия, относящиеся к работе системы с контроллерами 12000 серии

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.

Концентратор (PERCo-SC-12200P) — унифицированный системный контроллер, предназначенный для управления доступом посредством управления замковыми контроллерами подсистемы второго уровня PERCo-CL-12200 (до 7 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 ИУ, 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 добавочно позволяет управлять драйверами ИУ. 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 работе. Для считывания кода бесконтактных 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 ИУ 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 запитке 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 с.

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

  б) при запитке 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 с;
  - 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.).

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 с.

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 с.

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 Imax = 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.

Комиссионирование доступа — усиление контроля доступа посредством последовательного предъявления двух карт или одной карты и набора кодовой комбинации на клавиатуре для открытия ИУ.

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 ИУ с двумя считывателями — один на вход и второй на выход, т.е. по разные границы этой зоны).

Временная зона контроля — совокупность 4 временных интервалов в пределах календарных суток, в течение которых возможно:

- разрешение доступа по пользовательской карте;
- автоматическое открытие ИУ;
- запрещение дистанционного управления ИУ;
- автоматическая активизация релейных выходов;
- разрешение мониторинга тестовых входов, а также генерация тревоги при их активизации.

2. СОСТАВ СИСТЕМЫ PERCO-SYS-15000 ПРИ ЕЕ ЭКСПЛУАТАЦИИ С КОНТРОЛЛЕРАМИ 12000 СЕРИИ

В аппаратный состав системы входят следующие структурные единицы:
Компьютеры с установленным ПО;
Концентратор PERCo-SC-12200;
Базовый контроллер-концентратор PERCo-SC-12300;
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 E и H);
Контрольный считыватель PERCo-CR-12001 (варианты E, H, EH и M);
Репитер;
Удлинитель линии PERCo-SE-12001;
Считыватель;
Карта доступа (далее - карта);
Электромеханическое ИУ (турникет, замок и т.п.)
Блок питания.

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. 1.

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

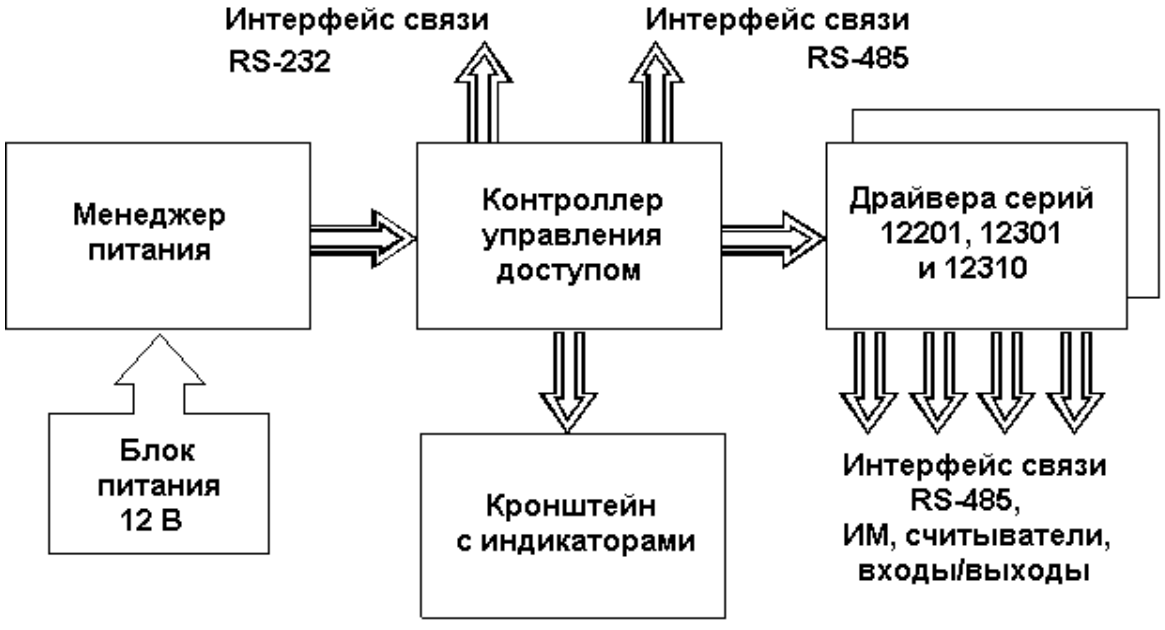

Рис. 1 Блок-схема унифицированного системного контроллера

2.1.1.1. Плата контроллера управления доступом

Контроллер содержит энергонезависимую память объемом 1 Мбайт, которая предназначена для хранения конфигурации подсистемы, списков карт доступа, 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.

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 модулем ПО «Сервер аппаратуры» 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.).

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. 2.

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). 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 зелёным светом. Когда контроллер сконфигурирован и работает в составе системы, второй индикатор постоянно горит зелёным светом. Второй индикатор также начинает мигать зелёным 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.

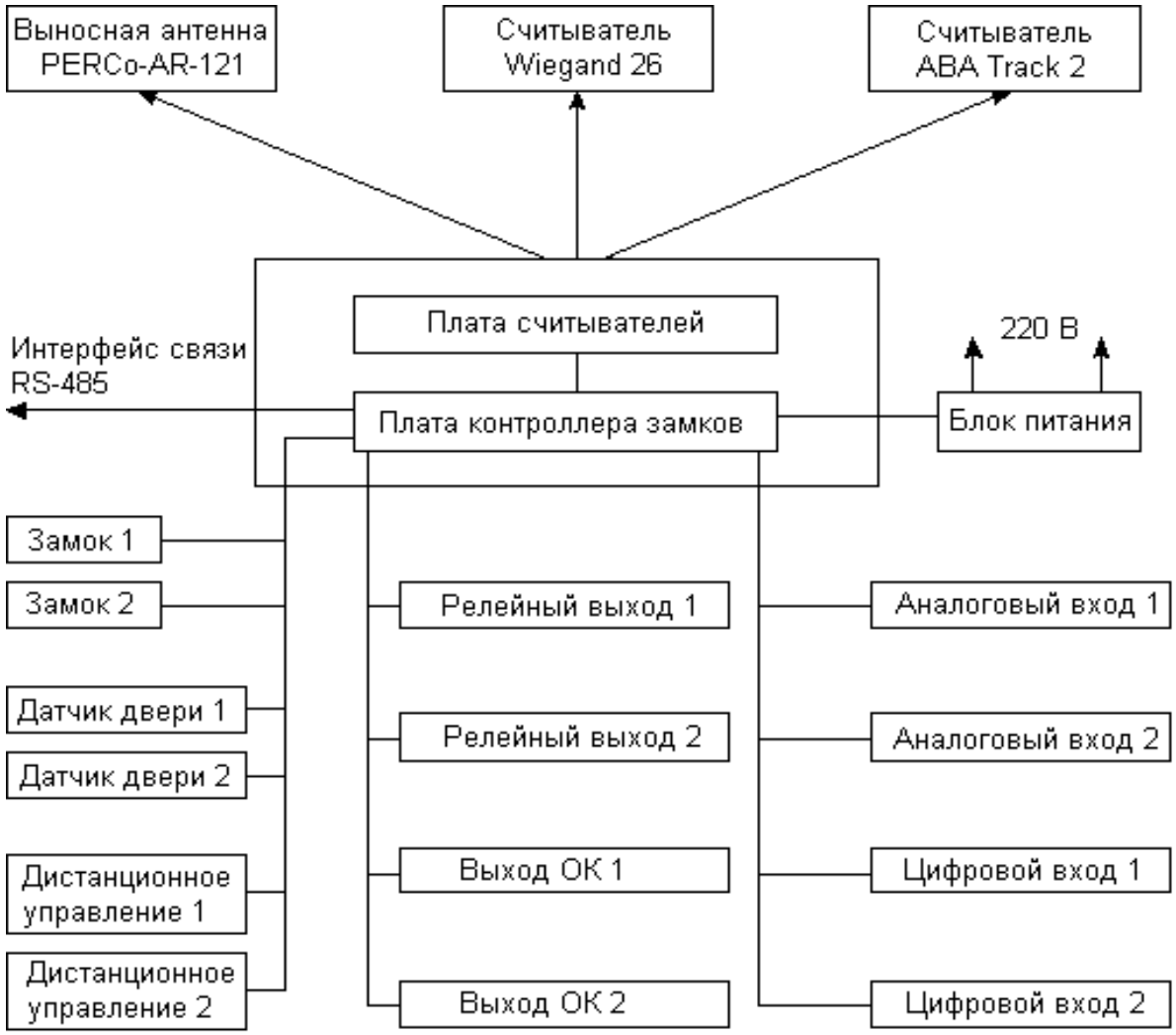

Рис. 2 Блок-схема контроллера PERCo-CL-12200

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

Параметры шлейфов:

Максимально допустимое сопротивление проводов шлейфа ..... не более 50 Ом
Сопротивление изоляции проводов шлейфа ..... не 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

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. 2.). Параметры релейных выходов и выходов типа «открытый коллектор» аналогичны параметрам драйверов серий 12301 и 12310.

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

Служебные выходы — это контакты на плате считывателей, предназначенные для подключения внешних устройств индикации (светодиодный 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 защёлок. 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 перемычек 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-12200 могут подключаться через один (два) драйвер (а) связи PERCo-DN-12201 до 7 замковых контроллеров PERCo-CL-12200.

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

- до двух драйверов ИУ серии 12301 в любой произвольной комбинации;
- один (любой) драйвер ИУ серии 12301 и через драйвер связи PERCo-DN-12201 до 5 замковых контроллеров PERCo-CL-122004

Внимание!!! В этом случае у замковых контроллеров PERCo-CL-12200 сетевой номер контроллера должен быть установлен в диапазоне от 2 до 6.

- через один (два) драйвер(а) связи PERCo-DN-12201 до 7 замковых контроллеров PERCo-CL-12200.

2.2. 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 ИУ 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 ИУ.

Структурная схема системы представлена на рис. 3.

3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ СИСТЕМЫ

Количество контроллеров на один сервер аппаратуры..... до 128
Количество ИУ на один сервер аппаратуры ..... до 224
Количество считывателей на один сервер аппаратуры..... до 224
Количество карт доступа .....до 32000
Количество диапазонов карт доступа ..... 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 драйвера серии 12301, шт**.** .....до 16384
для замкового контроллера PERCo-CL-12200, шт**.**.....до 3000

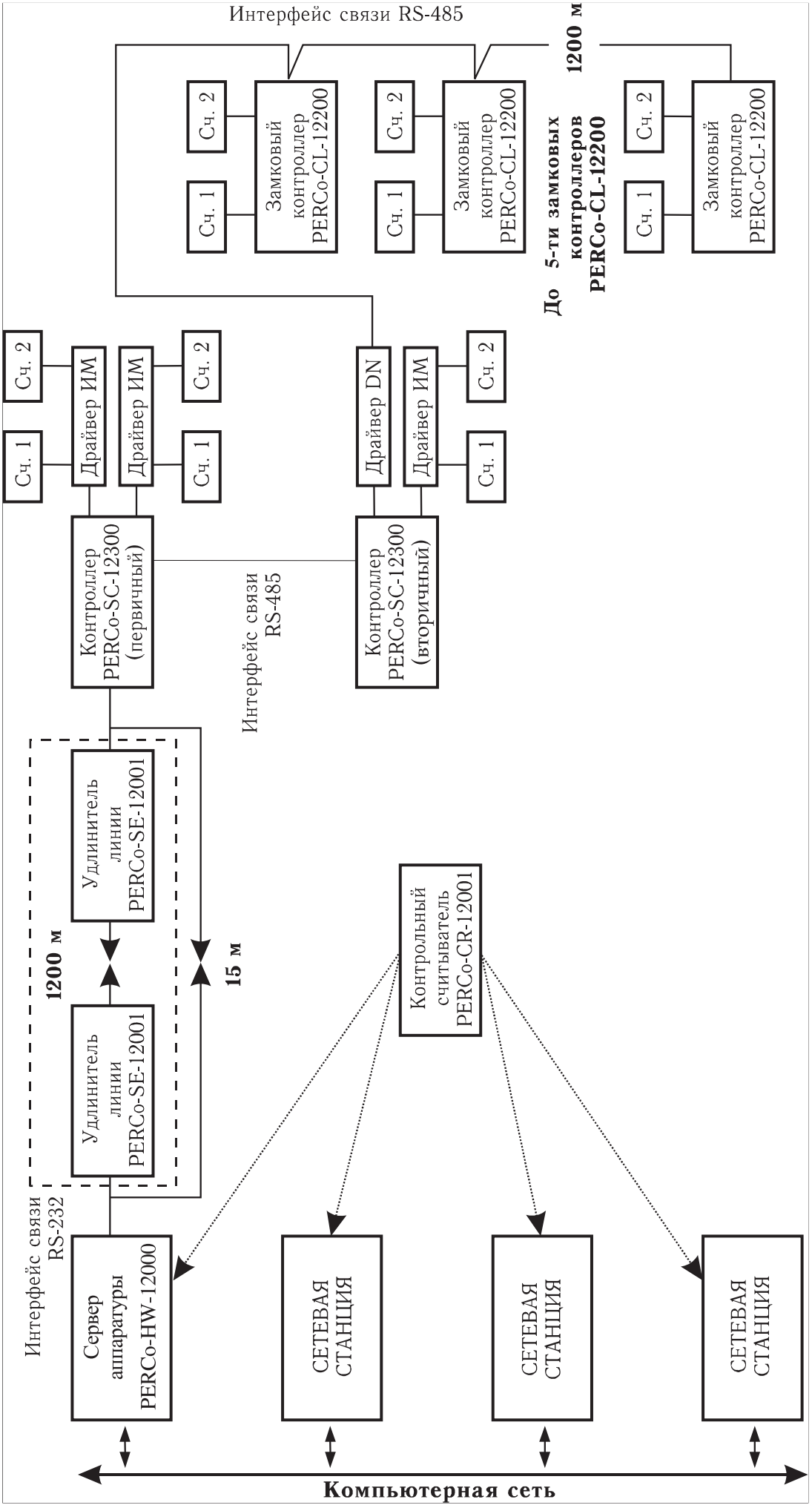

Рис. 3 Структурная схема СКД PERCo-SYSTEM-15000

3.1. Основные технические характеристики концентратора и контроллера-концентратора

Напряжение питания ..... 12±1.2 В
Ток потребления (без учета тока заряда аккумулятора)..... не более 0.15А
Ток потребления (с учетом тока заряда аккумулятора)..... не более 0.5А
Потребляемая мощность ..... не более 6Вт
Максимальное количество драйверов серии 12201 и 12301
(12301 — только для контроллера-концентратора), шт. 2
Скорость обмена в канале связи подсистемы ..... 9600 бод
Время опроса всех замковых контроллеров подсистемы ..... не более 1 с
Масса (без аккумулятора и блока питания) ..... не более 5,5 кг
Габаритные размеры ..... 384x360x108 мм
Условия эксплуатации:
Температура окружающего воздуха ..... от +1 до +40°С
Относительная влажность ..... не более 80% при t = 25°С

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

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

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. «Руководство администратора СКУД PERCo- SYS-15000»).

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 доступа — 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 ресурсов;

Для тестовых входов — параметры функционирования и условия для мониторинга;

Для ИУ — параметры управления и условия для автоактивизации ресурсов;

Для считывателей — параметры функционирования, параметры для режима доступа «Автономный контроль» и режима доступа «Системный контроль»;

Для служебных выходов — параметры функционирования и типы реакций на состояния;

Для генератора тревоги — тип и причины генерации тревоги, связанные:

С предъявлением карт доступа;

С состоянием ИУ;

С состоянием тестовых входов;

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

Одновременно с задачей параметров функционирования в закладке «События» раздела «Конфигуратор» можно устанавливать виды реагирования ПО системы на все происходящие с этим ресурсом события. На каждое событие можно задать до 8 различных реакций.

Для перевода системы в режим работы от карт доступа необходимо, используя соответствующие разделы ПО, сформировать группы допуска и их права, временные критерии (временные зоны, недельные графики, сменные графики и календарь праздничных дней) и передать их в систему (см. «Руководство пользователя СКУД PERCo- SYS-15000»). Затем 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 ТКД и параметры их функционирования

Релейный выход

Для управления релейным выходом необходимо определить следующие параметры:

1. Нормальное состояние выхода (запитан: «да» или «нет»). Этот параметр определяет состояние выхода при отсутствии на нем активизирующих управляющих воздействий.

2. Период активизации (00:00 - 07:56 мин:сек). Это — период времени, в течение которого при наличии активизирующего управляющего воздействия релейный выход изменит свое состояние из нормального в противоположное и остается в нем до его истечения.

3. Критерий для автоактивизации:

3.1. Критерий для автоактивизации «Временной»:

Связан со 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).

По умолчанию в ПО установлены две временные зоны (№1 — «Никогда» и №2 — «Всегда») и два недельных графика (№1 «Доступ запрещен» и №2 — «Доступ разрешен»). При необходимости автоактивизации релейного выхода для конкретных временных зон или недельных графиков требуется сначала их создать в «Справочниках доступа», а затем изменить параметры релейного выхода, передав измененные параметры в аппаратуру.

3.2. Критерий для автоактивизации «При постановке на охрану»:

Связан с режимом контроля доступа 1-го считывателя, т.е. активизируется (без учета периода активизации), если 1-ый считыватель устанавливается в режим «Охрана», и нормализуется во всех остальных режимах;

Связан с режимом доступа 2-го считывателя, т.е. активизируется (без учета периода активизации), если 2-ой считыватель устанавливается в режим «Охрана» и нормализуется во всех остальных режимах;

Связан с режимом доступа всего контроллера (т.е. обоих его считывателей): активизируется (без учета периода активизации), если контроллер (т.е. оба его считывателя) устанавливается в режим «Охрана», и нормализуется, если режим одного из считывателей не «Охрана»;

Тестовый вход

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

1. Нормальное состояние контакта (нормально замкнут «да» или «нет»). Этот параметр определяет тот уровень сигнала на входе, который система должна воспринимать как норма.

2. Период шунтирования (00:00 - 07:56 мин:сек). Этот параметр определяет тот период времени, в течение которого состояние входа считается нормальным независимо от уровня входного сигнала. Причиной шунтирования может быть активизация других тестовых входов или открытие ИУ. Шунтирование тестовых входов при открытии ИУ устанавливается при задании параметров ИУ.

3. Номера тестовых входов, шунтируемых при активизации данного входа (для каждого входа – «да» или «нет»).

4. Номера релейных выходов, активизируемых при активизации данного входа (для каждого выхода – «да» или «нет»). Следует заметить, что активизация релейного выхода привязанная к активизации тестового входа не учитывает возможного шунтирования этого входа (т.е. факт шунтирования игнорируется). Это очень важно учитывать для случаев применения в системе детекторов движения, расположенных в зоне прохода через ИУ, т.е., если тестовый вход зашунтирован, то все равно будет активизация релейного выхода, привязанная к активизации этого тестового входа.

5. Критерий для мониторинга:

5.1. Критерий для мониторинга «Временной»:

Связан со 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 (по умолчанию в ПО установлены две временные зоны и два недельных графика).

5.2. Критерий для мониторинга «При постановке на охрану»:

Связан с режимом доступа 1-го считывателя, т.е. мониторинг активизируется, если 1-ый считыватель устанавливается в режим «Охрана» и прекращается во всех остальных режимах;

Связан с режимом доступа 2-го считывателя, т.е. мониторинг активизируется, если 2-ой считыватель устанавливается в режим «Охрана» и прекращается во всех остальных режимах;

Связан с режимом доступа всего контроллера (т.е. обоих его считывателей). Мониторинг активизируется, если контроллер (т.е. оба его считывателя) устанавливается в режим «Охрана» и прекращается, если режим одного из считывателей не «Охрана»;

Исполнительное устройство

Для управления и контроля состояния ИУ необходимо определить следующие параметры:

1.Наличие и номер входного считывателя.

2.Наличие и номер выходного считывателя.

3.Ориентация считывателей (стандартная, не стандартная) – связь считывателя с ИУ (**только для турникетов и калиток**). Если при поднесении карты доступа ИУ открывается в обратную сторону, то необходимо изменить значение данного параметра на противоположное.

4. Время удержания в открытом состоянии от ДУ (00:00 – 02:00 мин:сек) — время, в течение которого ИУ должно находиться в открытом состоянии после разблокировки; по истечении этого времени оно будет автоматически закрыто.

5. Предельное время разблокировки ИУ (сек) — максимальное время, в течение которого ИУ может быть открыто. По истечении этого времени в событиях мониторинга формируется сообщение о недопустимо долгой разблокировке, возможна генерация тревоги.

6. Время предтревоги (с) — интервал времени, равный половине предельного времени разблокировки. По его истечении первичному контроллеру будет отправлено сообщение о появлении предтревожной ситуации на данном ИУ.

7. Режим управления:

7.1. Статический: длительность управляющего импульса равна длительности времени удержания в открытом состоянии.

7.2. Импульсный: длительность управляющего импульса устанавливается отдельно. Этот режим используется для ИУ с импульсным управлением. Импульсный режим устанавливается, в частности, для замков типа «CISA».

8. Состояние «Закрыто» (запитан: «да» или «нет») — определяет уровень управляющего сигнала, поданного на ИУ, который необходим для его перевода в закрытое состояние.

9. Нормальное (т.е. заблокированное) состояние контакта (нормально замкнут «да» или «нет») — устанавливает состояние контакта ИУ в состоянии «Закрыто».

10. Восстановление состояния «Закрыто» («после открытия» или «после закрытия») — определяет момент перевода ИУ в состояние «Закрыто», т.е. ИУ перейдет в состояние «Закрыто» либо после начала прохода (открытия двери), либо после завершения прохода (закрытия двери).

11. Номера релейных выходов, автоматически активизируемых при открытии ИУ (для каждого выхода — «да» или «нет»).

12. Номера тестовых входов, автоматически шунтируемых при открытии ИУ (для каждого входа – «да» или «нет»).

13. Время шунтирования после блокировки — (00:00 - 04:15 мин:сек). Этот параметр определяет тот промежуток времени, в течение которого состояние входа считается нормальным независимо от уровня входного сигнала.

14. Номера тестовых входов, активизация которых должна аварийно блокировать ИУ (для каждого входа — «да» или «нет»). Аварийная блокировка сопровождается запрещением дистанционного управления, запрещением управления от карт доступа и может быть снята только с помощью раздела ПО «Мониторинг» через установку режима доступа или сброс тревоги.

15. Номера тестовых входов, активизация которых должна аварийно разблокировать ИУ (для каждого входа – «да» или «нет»). Аварийная разблокировка сопровождается запрещением дистанционного управления и может быть снята только с помощью раздела ПО «Мониторинг» через установку режима доступа или сброс тревоги.

16. Временной критерий для автооткрытия ИУ — одна из системных временных зон (или недельных графиков), в установленные интервалы времени которой ИУ автоматически переходит в открытое состояние.

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

Считыватель

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

1. Тип используемых карт доступа (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 («да» или «нет»).

3. Регистрация прохода по предъявлению карты («да» или «нет»).

4. Время удержания в открытом состоянии (00:04 – 02:04 мин:сек) — время, в течение которого соответствующее ИУ будет разблокировано.

5. Параметры режима доступа «Автономный контроль» — 4 цифры Пинкода.

6. Параметры режима доступа «Системный контроль». Режим «Системный контроль» имеет набор следующих атрибутов, которые позволяют плавно ужесточать или смягчать режим контроля (устанавливаемый режим «Охрана» всегда наследует все текущие атрибуты режима «Системный контроль»):

6.1. Контроль времени.

Может быть установлен один из следующих атрибутов:

Контроль времени отсутствует;

Мягкий контроль времени (доступ разрешен, нарушение фиксируется в журнале мониторинга и может вызвать генерацию тревоги);

Жесткий контроль времени (доступ запрещен, нарушение фиксируется в журнале мониторинга и журнале регистрации и может вызвать генерацию тревоги);

Жесткий контроль времени с подтверждением от ДУ (доступ запрещен, на пульт ДУ охранника генерируется запрос на проход, моргание индикатора турникета и пульта ДУ, звуковой сигнал пульта).

6.2. Контроль зональности.

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);

Жесткий зональный контроль с подтверждением от ДУ (доступ запрещен, на пульт ДУ охранника генерируется запрос на проход, моргание индикатора турникета и пульта ДУ, звуковой сигнал).

6.3. Снятие с охраны.

Может быть установлен один из следующих атрибутов:

Только ПО (снятие с охраны производится только под управлением ПО — подраздел «Управление устройствами» раздела «Мониторинг»);

ПО или пропуском — снятие с охраны производится:

- ✓ Под управлением ПО (раздел «Мониторинг», подраздел «Управление устройствами»);
- ✓ Двойным предъявлением карты, обладающей правом автономной смены режима доступа и удовлетворяющей остальным критериям допуска (если карта комиссионируется другой картой, то под двойным предъявлением следует понимать предъявление основной и комиссионирующей карты).

6.4. Доступ

Может быть установлен один из следующих атрибутов:

Без подтверждения (при предъявлении карты, удовлетворяющей всем текущим критериям доступа, ИУ сразу разблокируется);

С подтверждением от ДУ (при предъявлении карты, удовлетворяющей всем текущим критериям доступа, ИУ разблокируется после нажатия кнопки дистанционного управления).

6.5. Автоблокировка при запрете доступа («да» или «нет»).

Установка этого атрибута позволяет автоматически блокировать ИУ в случае предъявления карты, доступ по которой запрещен.

6.6. Выборочный контроль

Установка данной опции позволяет автоматически (по определенному закону) переводить режим прохода из свободного доступа по всем картам, в доступ с подтверждением от ДУ 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 ДУ, или каждые 5-30 минут (кратно 5 минутам), или случайным образом, но не реже, чем каждый 30-й проход.

Служебный выход

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

1. Глобальные параметры

1.1. Нормальное состояние выхода (запитан: «да» или «нет») — определяет состояние выхода при отсутствии на нем активизирующих управляющих воздействий.

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

1.3. Период непрерывной индикации (1 – 15 сек) — единичный временной интервал непрерывной активизации, от которого рассчитываются все остальные значения.

1.4. Период вспышки (00:000 – 03:750 сек:мс) — единичный временной интервал пульсирующей активизации, от которого рассчитываются все остальные значения.

2. Индикация режима доступа (описывает способ уникальной индикации для каждого из существующих режимов доступа):

Нормальная — исходное состояние индикации соответствует «нормальному» из глобальных параметров;

Активная — состояние индикации противоположно «нормальному» из глобальных параметров;

Вспышкой — индикация прерывистая с периодом равным «периоду вспышки» из глобальных параметров.

3. Индикация состояний «ПРЕДТРЕВОГА» ИУ (описывает способ уникальной индикации предтревоги по разблокировке каждого из существующих ИУ. Время старта индикации предтревоги устанавливается в параметрах ИУ. Индикация предтревоги прекращается после восстановления заблокированного состояния ИУ).

Нет — текущая индикация не изменяется

Непрерывная — состояние индикации противоположна «нормальному» из глобальных параметров

Вспышкой — индикация прерывистая с периодом равным «периоду вспышки» из глобальных параметров

4. Индикация событий (Описывает способ уникальной индикации следующих событий, связанных с доступом):

Пропуск разрешен;

Пропуск запрещен;

Запрос на подтверждение от ДУ;

Запрос на подтверждение от подраздела “Управление видеоидентификацией”;

Ожидание смены режима доступа;

Ожидание комиссионирования;

Смена режима доступа;

Возможны следующие типы индикации:

Нет — текущая индикация не изменяется;

Непрерывная — состояние индикации противоположна «нормальному» из глобальных параметров, длительность индикации 1 – 5 с;

Вспышкой — индикация прерывистая с периодом равным «периоду вспышки» из глобальных параметров. Количество вспышек 1 – 7 шт.

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. Вид тревоги («тихая» или «сирена»). Этот параметр определяет, сопровождается ли генерация тревоги активизацией релейного выхода.

2. Сирена. Этот параметр определяет, на каком из драйверов будет активизироваться по тревоге релейный выход.

3. Драйвер XXXX. Этот параметр определяет, какой именно релейный выход будет активизироваться по тревоге.

4. Причины генерации тревоги по предъявлению карты.

Этот параметр охватывает все возможные нарушения режима доступа, связанные с предъявлением карт, и позволяет указать, в случае каких нарушений необходима генерация тревоги. Необходимо установить «да» или «нет» напротив соответствующих причин.

5. Причины генерации тревоги по состоянию ИУ. Необходимо установить «да» или «нет» напротив соответствующих причин.

Несанкционированное системой открытие ИУ — разблокировка ИУ, произошедшая без предшествующей санкции системы на его открытие. Устанавливается отдельно для каждого режима доступа.

Недопустимо долгое открытие ИУ — разблокировка ИУ дольше описанного в его параметрах предельного времени разблокировки.

6. Тестовые входы, активизация которых приводит к генерации тревоги («да» или «нет»).

Необходимо установить «да» или «нет» напротив тестовых входов, активизация которых должна сопровождаться генерацией тревоги.

7.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 доступа, зарегистрированную через контрольный считыватель (или с помощью клавиатуры ПК) в базе пользователей (см. «Руководство пользователя СКУД PERCo-SYS-15000»);

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-15000 концентратор (контроллер-концентратор) может быть как первичным, т.е. подключенным непосредственно к серверу аппаратуры, так и вторичным, т.е. подключенным к первичному контроллеру. Его конфигурация зависит от состояния перемычки 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 секунд переходят в аварийный режим работы и доступ, при этом, возможен только с использованием механического ключа.

Принципы функционирования концентратора (контроллера - концентратора)

В процессе функционирования системы PERCo-SYSTEM-15000 связь ПО «Сервер аппаратуры серии 12000» со всеми замковыми контроллерами, входящими в данную подсистему, осуществляется через ее концентратор (контроллер-концентратор).

Таким образом, при нарушении связи ПО «Сервер аппаратуры серии 12000» с этим концентратором (контроллером-концентратором) одновременно прерывается связь и со всеми замковыми контроллерами PERCo-CL-12200 данной подсистемы.

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

Принимает коды предъявленных карт доступа и, после анализа их прав, разрешает или запрещает доступ, фиксируя событие в журнале регистрации;

Следит за состоянием ИУ, 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 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 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 светодиодного индикатора «DRIVER» (см п. 4.2.6. данного описания).

Принципы функционирования замкового контроллера

При первом включении замковый контроллер не имеет параметров функционирования ИУ, 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 ИУ и запрещает доступ.

Аварийный режим работы контроллера

Если в процессе работы контроллера происходит прекращение его связи с концентратором, то через 5 секунд после этого он переходит в аварийный режим работы. Индикатор на плате контроллера замков начинает мигать зелёным светом, контроллер закрывает замки и по предъявлению считывателю карточек фиксирует событие «Отказ в доступе».

4.2.2. Права доступа и режим доступа

Под правом доступа карты понимают следующее:

Разрешена ли карта в данной системе;

Через какие считыватели, каких ТКД 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 доступа;

К группе специальных карт относятся следующие карты:

«Генеральная» — карта, доступ которой ничем не ограничен;

«Временный пропуск» — карта, доступ которой может быть ограничен периодом времени;

«Стоп-лист» — карта, 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 доступа:

1.«Открыто» (аварийный режим);

2.«Автономный контроль» с параметрами;

3.«Системный контроль» с параметрами;

4.«Охрана» (наследует параметры режима «Системный контроль»);

5.«Закрыто» (аварийный режим);

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

При присвоении считывателю режима «Открыто» ИУ, связанные с этим считывателем, переводятся в разблокированное состояние, а их дистанционное управление блокируется (рекомендуется для быстрого перевода ИУ в открытое состояние в случае чрезвычайных ситуаций).

При присвоении считывателю режима «Автономный контроль» ИУ, связанные с этим считывателем, переводятся в заблокированное состояние, и доступ через ИУ возможен в следующих случаях:

При нажатии кнопки дистанционного управления;

При выборе соответствующей команды в подразделе ПО«Управление устройствами»;

При наборе на клавиатуре 4-значной кодовой комбинации, задаваемой в параметрах режима доступа;

При присвоении считывателю режима «Системный контроль» ИУ, связанные с этим считывателем, переводятся в заблокированное состояние, и доступ через ИУ возможен в следующих случаях:

При нажатии кнопки дистанционного управления;

При выборе соответствующей команды в подразделе ПО«Управление устройствами»;

При предъявлении карты с соответствующими правами доступа.

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

При нажатии кнопки дистанционного управления;

При выборе соответствующей команды в подразделе ПО«Управление устройствами»;

При предъявлении карты с правом автономной смены режима или спецкарты «генеральная»;

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

Доступ через ИУ в режиме «Закрыто» возможен:

При выборе соответствующей команды в подразделе ПО «Управление устройствами»;

При предъявлении «генеральной» спецкарты.

К базовым режимам системы относятся «Системный контроль» и «Охрана».

Режим «Системный контроль» считывателя имеет набор следующих параметров, которые позволяют плавно ужесточать или смягчать режим контроля (параметры устанавливаются в подразделе «Устройства» консоли управления):

Контроль РЕЖИМА ДОСТУПА;

Контроль РЕЖИМА ВРЕМЕНИ;

Контроль РЕЖИМА ЗОНАЛЬНОСТИ;

Снятие режима доступа “ОХРАНА”;

Автоблокировка при запрете доступа;

Выборочный контроль.

4.2.3. Временные критерии доступа

К временным критериям доступа относятся:

временные зоны;

недельные графики;

сменные графики;

календарь праздничных дней.

Временная зона состоит из 4-х интервалов времени суток и имеет свой фиксированный уникальный номер.

Присвоение временной зоны карте доступа позволяет автоматически изменять временные ограничения для такой карты в пределах одних суток.

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 недельного графика карте доступа позволяет автоматически изменять временные ограничения для такой 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 сменного графика карте доступа позволяет автоматически изменять временные ограничения такой 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:

ИУ (открытие/закрытие);

Дистанционное управление ИУ (запрещение/разрешение использования);

Тестовый вход (разрешение/запрещение мониторинга);

Релейный выход (активизация/нормализация).

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

4.2.4. Мониторинг и регистрация событий

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 аппаратуры серии 12000» определяется буфером мониторинга контроллера 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.

Описание событий мониторинга и регистрации представлено в приложении 2.

4.2.5. Перемещения персонала. Интерфейс пользователя

Пользователь системы, обладающий картой доступа с соответствующими правами (с которыми он должен быть ознакомлен, во избежание недоразумений) имеет возможность пройти через любую точку доступа, доступ через которую 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 ИУ, сопровождающееся индикацией события «Пропуск разрешен» через служебные выходы;

Блокирование ИУ (если установлена автоблокировка), сопровождающееся индикацией «Пропуск запрещен» через служебные выходы;

Блокирование ИУ (если установлена автоблокировка), сопровождающееся индикацией «Запрос на подтверждение от ДУ» через служебные выходы;

Блокирование ИУ (если установлена автоблокировка), сопровождающееся индикацией «Запрос на подтверждение из подраздела “Управление видеоидентификацией”» через служебные выходы;

Блокирование ИУ (если установлена автоблокировка), сопровождающееся индикацией «Ожидание комиссионирования» через служебные выходы;

Открытие ИУ, сопровождающееся индикацией события «Ожидание смены режима доступа» через служебные выходы (режим «Системный контроль»*);*

Блокирование ИУ (если установлена автоблокировка), сопровождающееся индикацией события «Ожидание смены режима доступа» через служебные выходы (режим «Охрана»);

Открытие ИУ с помощью дистанционного управления не сопровождается индикацией через служебные выходы, за исключением случаев подтверждения прохода по карте, хотя в состав системы входят электромеханические ИУ с расширенными средствами индикации и дистанционного управления (электромеханические турникеты серии PERCo-T-04).

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 через тумблер «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 (ИУ, 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;

ASYNC CH — 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

Инструкция по автономной постановке и снятию с охраны помещений, контролируемых СКУД PERCo-SYSTEM-15000 при ее работе с контроллерами 12000 серии.

Для постановки на охрану необходимо определить группу доступа, обладающую правами на постановку/снятие с охраны, для чего в разделе «Справочники доступа», в подразделе «Группы доступа» для выбранной группы установить параметр «Постановка/снятие с охраны» - «Да» для выделенной точки доступа. Затем в разделе «Конфигуратор», в подразделе «Устройства» для считывателя замкового контроллера установить параметр «Снятие режима доступа “ОХРАНА”» в значение “ПО или пропуском”, и при системном контроле двойным поднесением карты, обладающей правом постановки/снятия с охраны, считыватель будет переведен в режим “ОХРАНА”.

Постановка в режим «ОХРАНА»

В разделе «Конфигуратор» подраздела «Устройства» для считывателя замкового контроллера установить параметр «Снятие режима доступа “ОХРАНА”» в значение «ПО или пропуском», а в разделе «Мониторинг» подраздела «Управление устройствами» – установить режим доступа «Системный контроль». Покинуть помещение, плотно закрыв за собой дверь. Убедиться в том, что индикатор считывателя соответствует нормальному состоянию. Поднести карточку доступа, обладающую правом автономной смены режима доступа, к считывателю. После этого, считыватель перейдет к индикации «Ожидание смены режима». Пока считыватель индицирует «Ожидание смены режима», повторно поднести к считывателю ту же карту доступа. Считыватель перейдет к индикации «Смена режима доступа», замок двери заблокируется, и считыватель перейдет к индикации «Охрана». С этого момента помещение будет поставлено в режим «Охрана».

Снятие с режима «ОХРАНА»

Убедиться в том, что считыватель индицирует состояние «Охрана» т.е. помещение находится в режиме «Охрана». Поднести карточку доступа, обладающую правом автономной смены режима доступа, к считывателю. После этого, считыватель перейдет к индикации «Ожидание смены режима». Пока считыватель индицирует «Ожидание смены режима», повторно поднести к считывателю ту же карту доступа. Считыватель перейдет к индикации «Смена режима доступа», замок двери разблокируется, а считыватель перейдет к индикации «Доступ разрешен». По истечении времени данной индикации считыватель перейдет к индикации «Системный контроль», что означает снятие помещения с «Охраны» и перевод в режим «Системный контроль».

Возможные причины отказа в автономной смене режима доступа. Постановка в режим «Охрана» осуществляется при недостаточно хорошо закрытой двери или неисправном датчике двери. Параметры режима доступа «Системный контроль» запрещают автономную смену режима 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.).

ПРИЛОЖЕНИЕ 2

Событие	Категория		Причины возникновения события
	Мониторинг	Журнал регистрации	
Системные события узла Аутентификации			
Запрет разового пропуска	*		Запрет разового пропуска
Системные события контроллера			
Очистка журнала регистрации	*	*	Событие происходит после чтения переполненного журнала регистрации
Переполнение журнала регистрации	*	*	Событие возникает после заполнения в памяти контроллера предпоследней свободной страницы журнала (размер одной страницы равен 32 событиям)
Авария питания от электросети	*	*	Событие возникает в случае отсутствия внешнего сетевого питания, т.е. при переходе контроллера на питание от встроенного резервного аккумулятора
Восстановление питания от эл.сети	*	*	Событие возникает в случае возобновления внешнего сетевого питания
Авария питания от аккумулятора	*	*	Событие возникает при разряде встроенного резервного аккумулятора до напряжения 10±0.5 В. Это событие сопровождается автоматическим выключением контроллера
Восстановление питания от аккумулятора	*	*	Событие 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
Тревога	*		Событие связано с возникновением тревожной ситуации в системе (см. параметры генератора тревоги)
Сброс тревоги	*		Событие связано со сбросом сигнала тревоги оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Нарушение связи	*	*	Событие относится к разряду диагностических и отражает возможное нарушение работоспособности контроллера
Восстановление связи	*	*	Событие относится к разряду диагностических и отражает возможное восстановление работоспособности контроллера
Нарушение системной конфигурации	*		Событие связано с нарушением энергонезависимости оперативной памяти контроллера и, как следствие, с потерей системных установок, необходимых для нормального функционирования. Для восстановления системной конфигурации необходимо выполнить переконфигурацию системы
Восстановление системной конфигурации	*		События связаны с восстановлением энергонезависимости оперативной памяти контроллера и, как следствие, с восстановлением системных установок, необходимых для нормального функционирования
Включение питания		*	Событие связано с включением питания контроллера
Выключение питания		*	Событие связано с выключением питания контроллера

Системные события считывателя			
Запрос на подтверждение, пропуск РАЗРЕШЕН	*		Специальное событие для видеоидентификации
Запрос на подтверждение, нарушение РЕЖИМА ВРЕМЕНИ	*		Специальное событие для видеоидентификации
Запрос на подтверждение, нарушение РЕЖИМА ЗОНАЛЬНОСТИ	*		Специальное событие для видеоидентификации
Запрос на подтверждение, пропуском снят режим доступа “ОХРАНА”	*		Специальное событие для видеоидентификации
Тревога, пропуск ЗАПРЕЩЕН или НЕ ЗАРЕГИСТРИРОВАН	*		Предъявленная карта запрещена или никому не выдана (если установлен параметр генератора тревоги «Причины генерации тревоги» - «Пропуск ЗАПРЕЩЕН или НЕ ЗАРЕГИСТРИРОВАН», и в параметре считывателя «Контроль РЕЖИМА ДОСТУПА установлен вариант «Жесткий без подтверждения»)
Тревога, пропуск из СТОП-листа	*		Предъявленная карта включена в СТОП-лист (если установлен параметр генератора тревоги «Причины генерации тревоги» — «Пропуск из СТОП-листа»)
Тревога, нарушение КОМИССИОНИРО-ВАНИЯ	*		Нарушение комиссионирования, т.е. было зафиксировано несоответствие с комиссионирующей картой или кодовой комбинацией, или комиссионирование не было выполнено вообще (если установлен параметр генератора тревоги «Причины генерации тревоги» — «Нарушение комиссионирования»)
Тревога, пропуск вне ДИАПАЗОНОВ КАРТ ДОСТУПА	*		Предъявленная карта не относится к системным, т.е. карта не входит в сегментированный набор системных карт (если установлен параметр генератора тревоги «Причины генерации тревоги» — «Пропуск вне ДИАПАЗОНОВ КАРТ ДОСТУПА»)
Тревога, нарушение РЕЖИМА ВРЕМЕНИ	*		Несоответствие предъявленного пропуска временным критериям доступа (если установлен параметр генератора тревоги «Причины генерации тревоги» — «Нарушение РЕЖИМА ВРЕМЕНИ» и в параметре считывателя «Контроль РЕЖИМА ВРЕМЕНИ» выбран вариант “Мягкий” или “ Жесткий без подтверждения ”)
Тревога, нарушение РЕЖИМА ДОСТУПА	*		Несоответствие режима доступа предъявленного пропуска текущему режиму доступа контроллера (если установлен параметр генератора тревоги «Причины генерации тревоги» — «Несоответствие РЕЖИМА ДОСТУПА»)

Тревога, нарушение РЕЖИМА ЗОНАЛЬНОСТИ	*		Несоответствие текущему местоположению, т.е. предъявленная карта нарушила зональность данной системы (если установлен параметр генератора тревоги «Причины генерации тревоги» - «Нарушение РЕЖИМА ЗОНАЛЬНОСТИ» и в параметрах считывателя «Контроль РЕЖИМА ВРЕМЕНИ» и «Контроль РЕЖИМА ЗОНАЛЬНОСТИ» установлены варианты «Жесткий…»)
Пропуск ЗАПРЕЩЕН или НЕ ЗАРЕГИСТРИРОВАН	*		Карта запрещена или никому не выдана
Пропуск из СТОП-ЛИСТА	*		Предъявленная карта включена в СТОП-лист
Пропуск вне ДИАПАЗОНОВ КАРТ ДОСТУПА	*		Предъявленная карта не относится к системным, т.е. карта не входит в сегментированный набор системных карт
Нарушение КОМИССИОНИРО-ВАНИЯ	*		Нарушение комиссионирования, т.е. было зафиксировано несоответствие с комиссионирующей картой или кодовой комбинацией, или комиссионирование не было выполнено вообще
Нарушение РЕЖИМА ВРЕМЕНИ	*		Несоответствие предъявленного пропуска временным критериям доступа
Нарушение РЕЖИМА ДОСТУПА	*		Несоответствие режима доступа предъявленного пропуска текущему режиму доступа контроллера
Нарушение РЕЖИМА ЗОНАЛЬНОСТИ	*		Несоответствие текущему местоположению, т.е. предъявленная карта нарушила зональность данной системы
Пропуском снят режим доступа ОХРАНА	*	*	Установлен режим доступа СИСТЕМНЫЙ КОНТРОЛЬ поднесением карты, обладающей правом автономной смены режима доступа
Пропуском установлен режим доступа ОХРАНА	*	*	Установлен режим доступа ОХРАНА поднесением карты, обладающей правом автономной смены режима доступа
Системой установлен режим доступа ОТКРЫТО	*	*	Установлен режим доступа ОТКРЫТО оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Системой установлен режим доступа АВТОНОМНЫЙ КОНТРОЛЬ	*	*	Установлен режим доступа АВТОНОМНЫЙ КОНТРОЛЬ оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Системой установлен режим доступа СИСТЕМНЫЙ КОНТРОЛЬ	*	*	Установлен режим доступа СИСТЕМНЫЙ КОНТРОЛЬ оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”

Системой установлен режим доступа ОХРАНА	*	*	Установлен режим доступа ОХРАНА оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Системой установлен режим доступа ЗАКРЫТО	*	*	Установлен режим доступа ЗАКРЫТО оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”.
Попытка доступа без совершения прохода		*	После поднесения карты, обладающей правом доступа, к считывателю, проход не был совершен
Проход		*	Проход по карте
Вход		*	Вход на объект по карте
Выход		*	Выход с объекта по карте
Проход с подтверждением от ДУ, нарушение РЕЖИМА ВРЕМЕНИ		*	Проход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ВРЕМЕНИ» - «Жесткий с подтверждением от ДУ»
Вход с подтверждением от ДУ, нарушение РЕЖИМА ВРЕМЕНИ		*	Вход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ВРЕМЕНИ» - «Жесткий с подтверждением от ДУ»
Выход с подтверждением от ДУ, нарушение РЕЖИМА ВРЕМЕНИ		*	Выход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ВРЕМЕНИ» - «Жесткий с подтверждением от ДУ»
Проход с подтверждением от ДУ, нарушение РЕЖИМА ЗОНАЛЬНОСТИ		*	Проход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ЗОНАЛЬНОСТИ» - «Жесткий с подтверждением от ДУ»
Вход с подтверждением от ДУ, нарушение РЕЖИМА ЗОНАЛЬНОСТИ		*	Вход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ЗОНАЛЬНОСТИ» - «Жесткий с подтверждением от ДУ»
Выход с подтверждением от ДУ, нарушение РЕЖИМА ЗОНАЛЬНОСТИ		*	Выход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ЗОНАЛЬНОСТИ» - «Жесткий с подтверждением от ДУ»
Отказ в доступе, пропуск ЗАПРЕЩЕН или НЕ ЗАРЕГИСТРИРОВАН		*	Предъявленная карта запрещена или никому не выдана
Отказ в доступе, пропуск из СТОП-листа		*	Предъявленная карта включена в СТОП-лист

Отказ в доступе, пропуск вне ДИАПАЗОНОВ КАРТ ДОСТУПА		*	Предъявленная карта не относится к системным, т.е. карта не входит в сегментированный набор системных карт
Отказ в доступе, нарушение РЕЖИМА КОМИССИОНИРО-ВАНИЯ		*	Нарушение комиссионирования, т.е. было зафиксировано несоответствие с комиссионирующей картой или кодовой комбинацией, или комиссионирование не было выполнено вообще
Отказ в доступе, нарушение РЕЖИМА ВРЕМЕНИ		*	Несоответствие предъявленного пропуска временным критериям доступа
Отказ в доступе, нарушение РЕЖИМА ДОСТУПА		*	Событие связано с предъявлением карты, не имеющей права доступа через ИУ, считыватель которого находится в режимах "Охрана" или "Закрыто"
Отказ в доступе, нарушение РЕЖИМА ЗОНАЛЬНОСТИ		*	Несоответствие текущему местоположению, т.е. предъявленная карта нарушила зональность системы
Отказ в доступе по ДУ		*	Отказ в доступе охранником с помощью ДУ при установленном параметре считывателя ”Контроль РЕЖИМА ДОСТУПА” – “Жесткий с подтверждением от ДУ”
Пропуск РАЗРЕШЕН	*		Предъявленная карта удовлетворяет всем критериям доступа, произошла разблокировка ИУ, возможен проход.

Системные события драйвера			
Нарушение связи	*	*	Это событие относится к разряду диагностических и отражает возможное нарушение работоспособности структурных элементов системы. Нарушение связи с драйвером влечет за собой полное прекращение управления следующими ресурсами: ИУ, мониторинг тестовых входов, релейные выходы (соответственно, невозможна громкая тревога) и служебные выходы
Восстановление связи	*	*	Это событие относится к разряду диагностических и отражает возможное восстановление работоспособности структурных элементов системы
Системные события ИУ			
Заблокирован	*		Событие отражает изменение текущего состояния блокирующего контакта.
Разблокирован	*		Событие отражает изменение текущего состояния блокирующего контакта
Тревога по разблокировке ИУ – ВЗЛОМ	*		Несанкционированное открытие ИУ

Тревога по разблокировке ИУ - Слишком долгое ОТКРЫТИЕ	*		Время активизации состояния блокирующего контакта превысило установленное предельное время разблокировки и для генератора тревоги установлен параметр «недопустимо долгое открытие. Если ИУ было разблокировано картой доступа, то дополнительно фиксируется и номер этой карты (или последней прошедшей карты)
Заблокирован Вход	*		Событие отражает изменение текущего состояния блокирующего контакта.
Разблокирован Вход	*		Событие отражает изменение текущего состояния блокирующего контакта.
Заблокирован Выход	*		Событие отражает изменение текущего состояния блокирующего контакта.
Разблокирован Выход	*		Событие отражает изменение текущего состояния блокирующего контакта.
Системные события Тестового входа			
Активизация	*	*	Изменение текущего уровня сигнала тестового входа
Сброс	*	*	Сброс входа
Тревога по АКТИВИЗАЦИИ входа	*	*	Если в генераторе тревоги установлен параметр «Тестовые входы, активизирующие генерацию тревоги»
Системные события Релейного выхода			
Активизация	*	*	Изменение текущего уровня сигнала релейного выхода
Сброс	*	*	Сброс выхода