

РУКОВОДСТВО АДМИНИСТРАТОРА

Единая система **S-20**

Базовый комплект ПО PERCo-SN01



ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	5
СОСТАВ СИСТЕМЫ PERCO-S-20	6
ПОРЯДОК ПОДГОТОВКИ СИСТЕМЫ К РАБОТЕ.....	6
ИНСТАЛЛЯЦИЯ ПО	8
Инсталляция PERCo-SN01 «Базовое ПО».....	8
Удаление PERCo-SN01 «Базовое ПО»	9
ЛИЦЕНЗИИ.....	10
ОБЩИЕ СВЕДЕНИЯ	14
Настройка контроллера	17
Режимы получения адреса	17
Настройка без DHCP	18
Настройка с DHCP	20
ОС Windows.....	20
ОС Linux.....	23
Особенности работы стека протокола TCP/IP в Windows XP.....	24
КОНФИГУРАЦИЯ КОНТРОЛЛЕРОВ	25
Конфигурация устройств системы безопасности	25
Задание пароля связи с контроллерами	27
Изменение сетевых настроек	28
Описание параметров функционирования контроллеров	
доступа	29
Дополнительный вход.....	29
Дополнительный выход	32
Исполнительное устройство	36
Считыватель.....	38
Генератор тревоги	43
Шлейф сигнализации.....	45
Группы ресурсов	46
Защита от передачи идентификаторов	47
Протокол работы со считывателями	49
Описание параметров функционирования контроллеров ППКОП	
(КБО).....	49
Контроллер	50
Дополнительный выход	50
Шлейф сигнализации.....	54
Зоны сигнализации	56
Интеграция ППКОП с ПЦН «АИР»	58
ПОМЕЩЕНИЯ	59

Помещения	59
Мнемосхема	60
ПЕРСОНАЛ	62
Учётные данные	62
Справочник Подразделения	63
Справочник Должности.....	64
Сотрудники	65
ПАРАМЕТРЫ ДОСТУПА.....	65
НАЗНАЧЕНИЕ ПРАВ ДОСТУПА ОПЕРАТОРОВ	65
Рабочее окно.....	65
Основные функции.....	67
Добавление пользователя.....	67
Редактирование данных пользователя	68
Удаление пользователя	69
Предоставление прав доступа оператору	70
1. Права доступа на разделы	70
2. Права доступа на подразделения.....	71
3. Права доступа на помещения	71
4. Права доступа на управление устройствами.....	72
5. Запрет доступа пользователя	72
Копирование прав	72
УПРАВЛЕНИЕ УСТРОЙСТВАМИ.....	73
Управление устройствами	73
УПРАВЛЕНИЕ СЕРВЕРАМИ	74
База данных	75
Создание базы данных.....	76
Сохранение настроек базы данных	78
Сохранение базы данных	78
Восстановление базы данных из резервной копии	79
Удаление данных мониторинга.....	79
Удаление данных о событиях	80
Настройки сервера баз данных	80
Оптимизация индексов базы данных.....	81
Обновление версии базы данных.....	81
Восстановление предыдущего пароля устройств	82
Настройка работы с 1С	83
Резервное копирование БД	84
Настройка USB – Модема.....	87
ТРЕБОВАНИЯ К АППАРАТУРЕ.....	88
ПРИЛОЖЕНИЕ 1. СОБЫТИЯ.....	89

События, записываемые в журнал регистрации.....	89
1. События, связанные с перемещением через ИУ.....	89
2. События, связанные с изменением текущего состояния дополнительных входов.....	92
3. События, связанные с изменением текущего состояния дополнительных выходов.....	92
4. События, связанные с изменением текущего состояния корпуса контроллера.....	92
5. События, связанные с работоспособностью сетевых каналов контроллера.....	92
6. События, связанные с изменением текущего состояния контроллеров или системы.....	94
7. События, связанные с изменениями состояний группы ресурсов.....	96
8. События, связанные с изменением текущего состояния ресурсов, входящих в группу ресурсов.....	99
События КБО и ППКОП.....	100
1. События, связанные с перемещением через ИУ (только КБО)....	100
2. События, связанные с изменением текущего состояния дополнительных выходов.....	104
3. События, связанные с изменением текущего состояния корпуса контроллера.....	104
4. События, связанные с работоспособностью сетевых каналов контроллера.....	104
5. События, связанные с изменением текущего состояния контроллеров или системы.....	106
6. События, связанные с изменениями состояний зон.....	109
7. События, связанные с изменением текущего состояния ШС, входящих в ОЗ, КТС и ПЗ.....	114
8. События, связанные с Устройствами охранными объектовыми (УОО) (только ППКОП).....	116
9. События, связанные с изменением текущего состояния ИУ, входящих в ОЗ (только КБО).....	116
Команды управления.....	116
Контроллер управления доступом.....	117
Считыватель.....	118
Дополнительный выход.....	119
Группа ресурсов.....	121
Контроллер ППКОП.....	122
Контроллер КБО.....	122
Зона контроллера ППКОП (КБО).....	124
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ.....	126

ВВЕДЕНИЕ

PERCo-S-20 - это многофункциональная система для обеспечения безопасности и повышения эффективности работы промышленных предприятий, банков, бизнес - центров, медицинских, образовательных, государственных учреждений и организаций других сфер деятельности.

PERCo-S-20 предназначена для эффективной и экономически оправданной защиты предприятия от основных видов внешних и внутренних угроз (пожар, хищения и вандализм, нарушения трудовой дисциплины).

Широкие возможности и надежность функционирования PERCo-S-20 обеспечены рядом новых технических решений:

- Задачи обеспечения безопасности и повышения эффективности деятельности предприятия решаются с использованием одного и того же оборудования, линий связи, баз данных и программного обеспечения.
- PERCo-S-20 совмещает функции систем охранной и пожарной сигнализации, контроля и управления доступом, видеонаблюдения.
- Возможна настройка сценариев реагирования на основе сигналов от систем контроля доступа, видеонаблюдения, охранной и пожарной сигнализации.
- Все технические средства системы работают в единой информационной среде Ethernet, которая значительно упрощает и расширяет выбор IT-решений при монтаже.
- Эффективная защита предприятия от пожара за счет применения адресно-аналоговой системы пожарной сигнализации.
- Система позволяет организовать Центральный пост охраны, обеспечивающий взаимодействие технических и программных средств, в том числе в автоматическом режиме (включение видеокамеры в зоне сработавшего охранного датчика и т.д.), снижая негативное влияние человеческого фактора.
- Организация автоматизированных рабочих мест (АРМ), объединенных в единую локальную сеть по технологии «клиент-сервер», и подсистема «электронный кабинет» для автоматизации приема посетителей – дают возможность повысить производительность труда сотрудников.
- Включение в конфигурацию PERCo-S-20 подсистемы «прозрачное здание» позволяет руководителю предприятия лучше контролировать работу сотрудников, добиваясь снижения финансовых потерь от падения объема выпускаемой продукции, оказанных услуг, или иного ущерба для бизнеса в результате нарушений работниками трудовой дисциплины.
- Система дает возможность наращивания функций базового варианта и интеграции в существующие сети.

Программное обеспечение PERCo-S-20 состоит из разделов, что позволяет формировать ПО под задачи конкретного заказчика.

Данное руководство предназначено для администраторов системы, а также для системных администраторов компьютерных сетей и сотрудников служб (подразделений) по поддержке программного и аппаратного обеспечения. В него включены следующие описания:

- инсталляция программного обеспечения;
- требования к сети Ethernet;
- особенности работы с программным обеспечением;
- порядок подготовки системы к работе;
- задание первоначальных установок функционирования системы;
- задание прав доступа пользователей к программному обеспечению системы;
- настройка сервера системы;
- работа с сервером системы.

СОСТАВ СИСТЕМЫ PERCo-S-20

Структурный состав системы PERCo-S-20 показан на рис.1. Все технические средства и ПО системы PERCo-S-20 работают в единой информационной среде передачи данных, реализованной на основе сети Ethernet. Структурно систему можно разделить на две составляющие:

1. Подсистема безопасности.
2. Подсистема повышения эффективности.

К первой части можно отнести оборудование, АРМы безопасности. Ко второй - административные АРМы, не требующие оперативного контроля. Исходя из специфичности решаемых системой PERCo-S-20 задач, рекомендуется разделение существующей или создание отдельной сети Ethernet для подсистемы безопасности. При этом административные АРМы могут находиться в сети предприятия.

ПОРЯДОК ПОДГОТОВКИ СИСТЕМЫ К РАБОТЕ

Для осуществления подготовки системы к работе необходимо выполнить следующие действия:

1. Разработать структурную схему системы.
2. Выбрать компьютеры, где будет установлен сервер системы и сервер БД, и будут работать модули ПО PERCo-S-20.
3. Провести инсталляцию ПО в соответствии с разработанной схемой.
4. Запустить «Центр управления PERCo-S-20». На данном этапе осуществить подключение к серверу БД и создание базы данных.
5. Запустить модуль «Консоль управления» (для регистрации разделов программы).
6. Задать права доступа пользователей к программному обеспечению системы.

На данном этапе определить пользователей системы, задать их права доступа к разделам программного обеспечения и присвоить им индивидуальные пароли.

Структурная схема PERCo-S-20

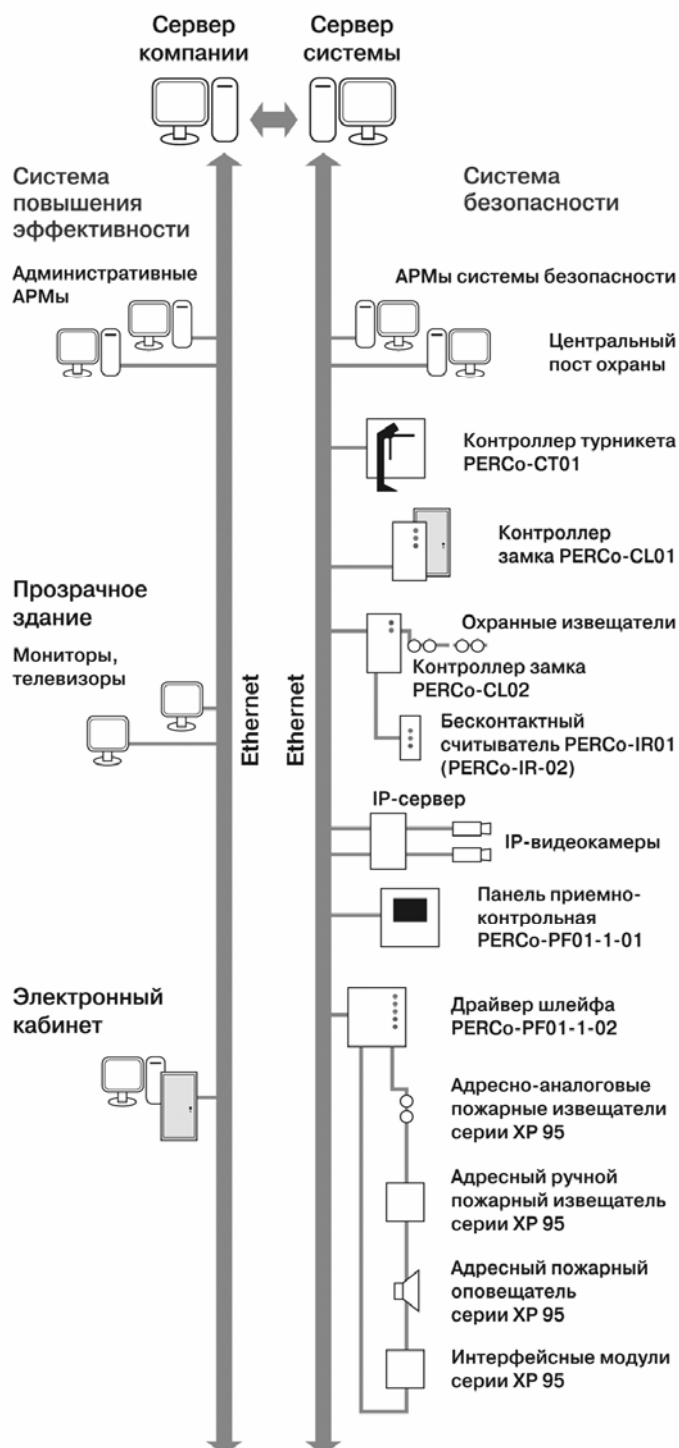


Рис.1. Структурный состав системы PERCo-S-20

7. Настроить контроллеры в соответствии с топологией Вашей сети Ethernet. При необходимости настроить DHCP сервер.
8. Провести автоконфигурацию системы, т.е. операцию по автоматическому

определению состава подключенной аппаратуры с дальнейшим заданием параметров работы подключенных устройств и привязкой этих устройств к объектам доступа. Если автоконфигурация осуществляется не администратором системы, то данный пункт выполняется после задания прав доступа пользователей к программному обеспечению.

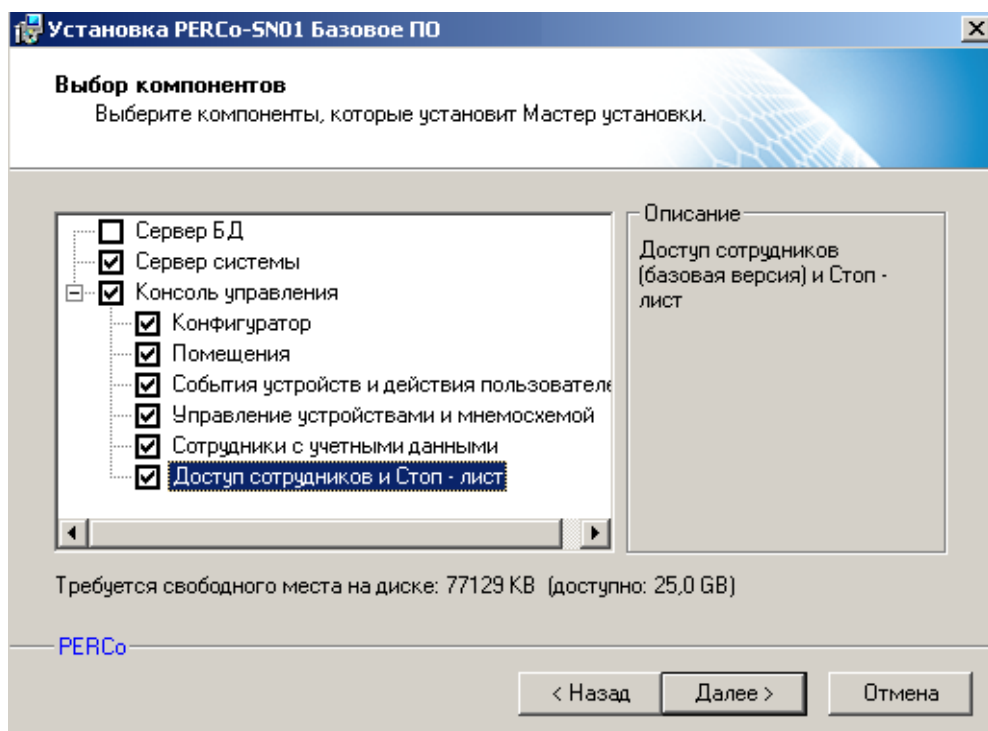
После проведения всех необходимых операций по настройке системы администратору рекомендуется задать себе пароль для входа в нее. Данная процедура необходима для установки эксклюзивного права администратора изменять настройки системы.

ИНСТАЛЛЯЦИЯ ПО

Перед началом инсталляции программного обеспечения ознакомьтесь с разработанной структурной схемой системы безопасности. Определите какие модули программного обеспечения на какие компьютеры будут установлены.

ИНСТАЛЛЯЦИЯ PERCO-SN01 «БАЗОВОЕ ПО»

Вставьте компакт диск с дистрибутивом в привод CD-ROM. Должен автоматически завестись инсталляционный модуль SetupBase.exe. Если этого не происходит — запустите данный модуль вручную. Следуйте указаниям мастера установки. Внимательно ознакомьтесь с предлагаемой информацией и лицензионным соглашением. После принятия лицензионного соглашения будет предложено выбрать устанавливаемые компоненты программного обеспечения:

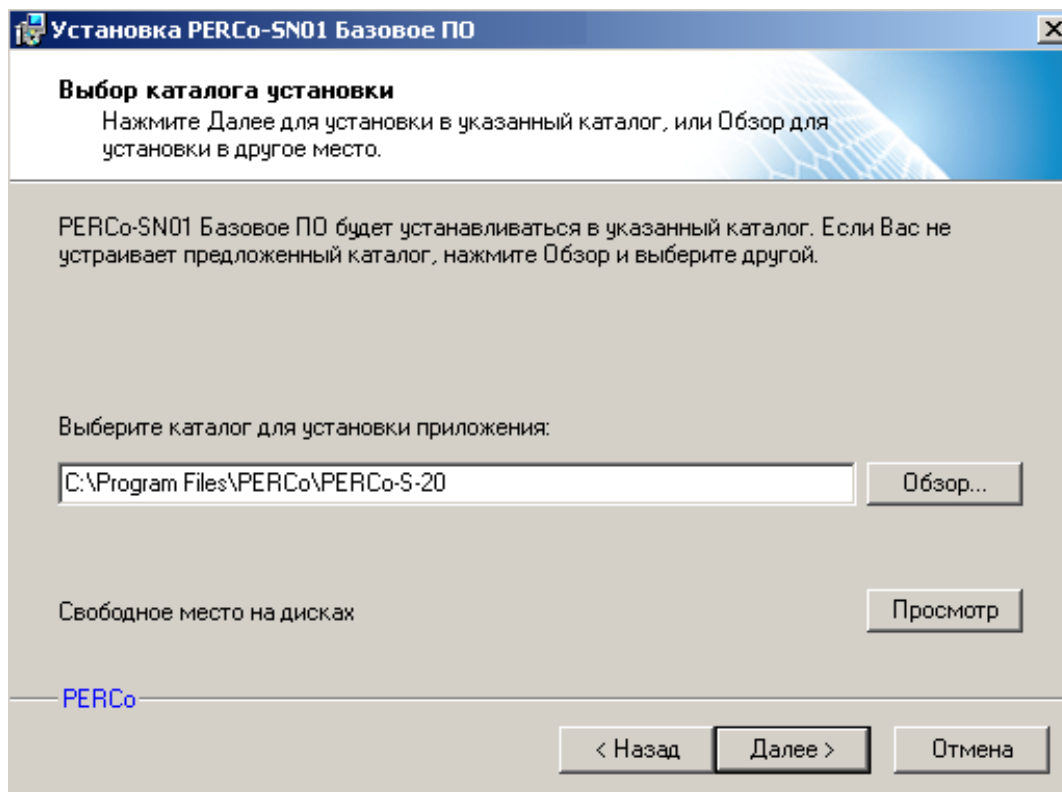


В соответствии с разработанной схемой системы безопасности выберите именно те компоненты программного обеспечения, которые должны быть проинсталлированы на данном компьютере. Щелкните на кнопке Далее.



ПРИМЕЧАНИЕ

Сервер системы может быть установлен только в единственном экземпляре в составе системы безопасности. Установка сервера системы автоматически приводит к установке сервера управления базой данных Firebird 2.5.



В открывшемся диалоговом окне укажите каталог, в который будет произведена установка программного обеспечения, и щелкните на кнопке **Далее**.

Следуйте указаниям мастера установки. После завершения установки программное обеспечение готово к работе.

Создайте или обновите Базу Данных. Инструкция по управлению Базами Данных приведена в **п. Управление серверами** данного Руководства Администратора.

УДАЛЕНИЕ PERCO-SN01 «БАЗОВОЕ ПО»

Вставьте компакт диск с дистрибутивом в привод CD-ROM. Должен автоматически запуститься инсталляционный модуль SetupBase.exe. Если этого не происходит — запустите данный модуль вручную. Следуйте указаниям мастера установки.

Возможен другой способ удаления ПО: запустите Панель управления Windows (**Пуск → Программы → PERCo → PERCo-S-20 → Удалить PERCo-SN01 «Базовое ПО»**). (Приведенный путь предопределен при инсталляции. Если в момент инсталляции был выбран другой каталог, приложение **Удалить PERCo-SN01 «Базовое ПО»** будет открываться, соответственно, из выбранного при инсталляции каталога.) Далее следуйте указаниям мастера установки, который автоматически выбирает программу удаления.

ЛИЦЕНЗИИ

Все программное обеспечение, входящее в состав Единой системы безопасности и повышения эффективности предприятия, требует после проведения инсталляции дополнительного ввода ключей активации.

В качестве аппаратного средства защиты программного обеспечения от несанкционированного использования применяются контроллеры, входящие в состав приобретенной вами системы безопасности. Выполнение функции аппаратного контроля лицензий одним из контроллеров не влияет на его остальные функциональные возможности.

Для упрощения процедуры регистрации программного обеспечения, а так же для ознакомления с его возможностями, в течение 30 дней с момента первого запуска программное обеспечение работает в ознакомительном режиме.

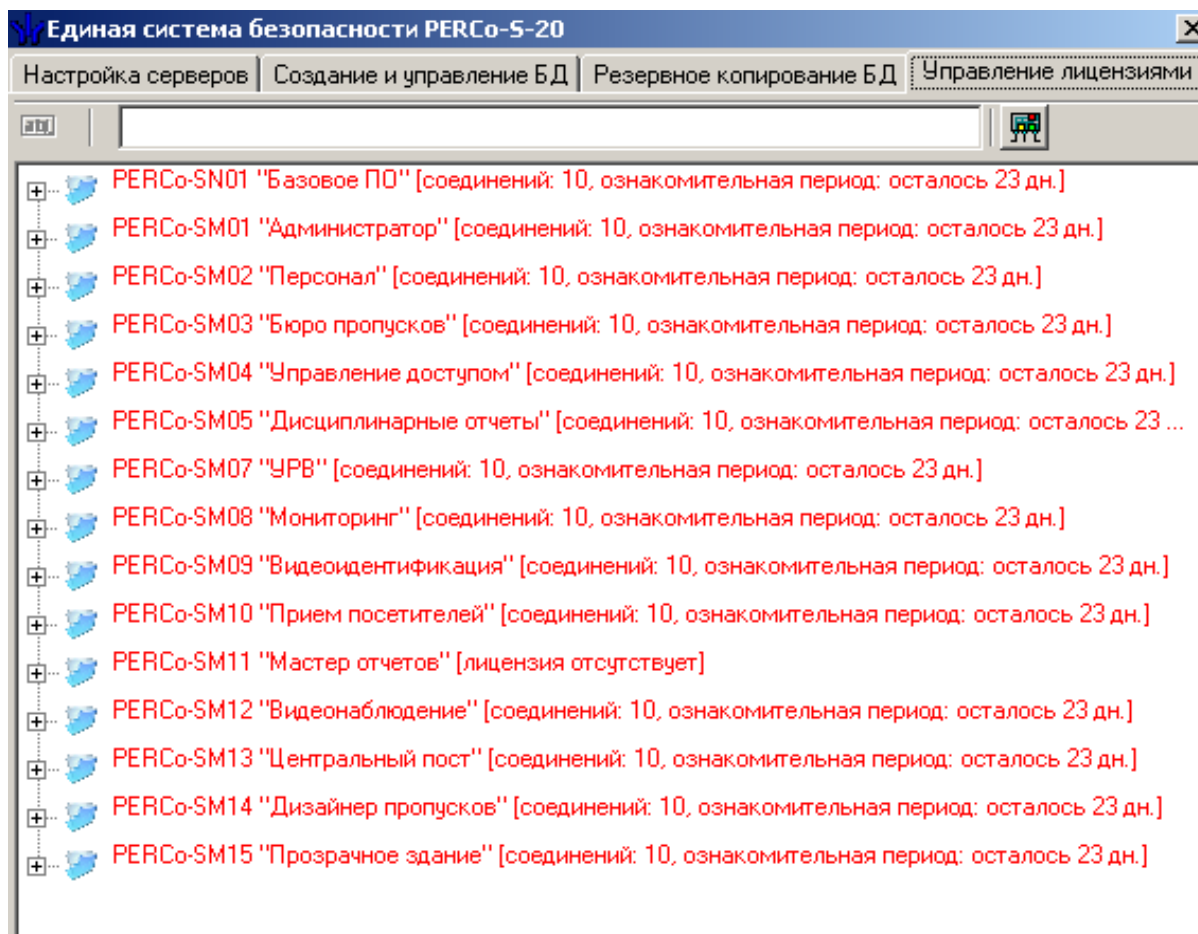
Под ознакомительным режимом понимается режим работы ПО с сохранением всех функциональных возможностей, но с выводом предупреждающего напоминания и указанием времени оставшегося до окончания ознакомительного периода. По прошествии 30 дней доступ к не активированным сетевым модулям будет запрещен.

Для получения ключей активации приобретенного вами программного обеспечения вам необходимо выбрать один из контроллеров, входящих в систему безопасности, который будет выполнять функцию аппаратного контроля лицензий на программное обеспечение; заполнить соответствующим образом заявку на приобретение лицензии, и отправить его в компанию PERCo.

После получения лицензионного соглашения содержащего ключи активации вам необходимо ввести их в программное обеспечение. Ввод ключей активации производится в модуле Центр управления PERCo-S-20, входящем в состав **PERCo-SN01 «Базовое ПО»**. Более подробная информация о работе с этим модулем приведена в разделе **«Управление серверами»** данного руководства.

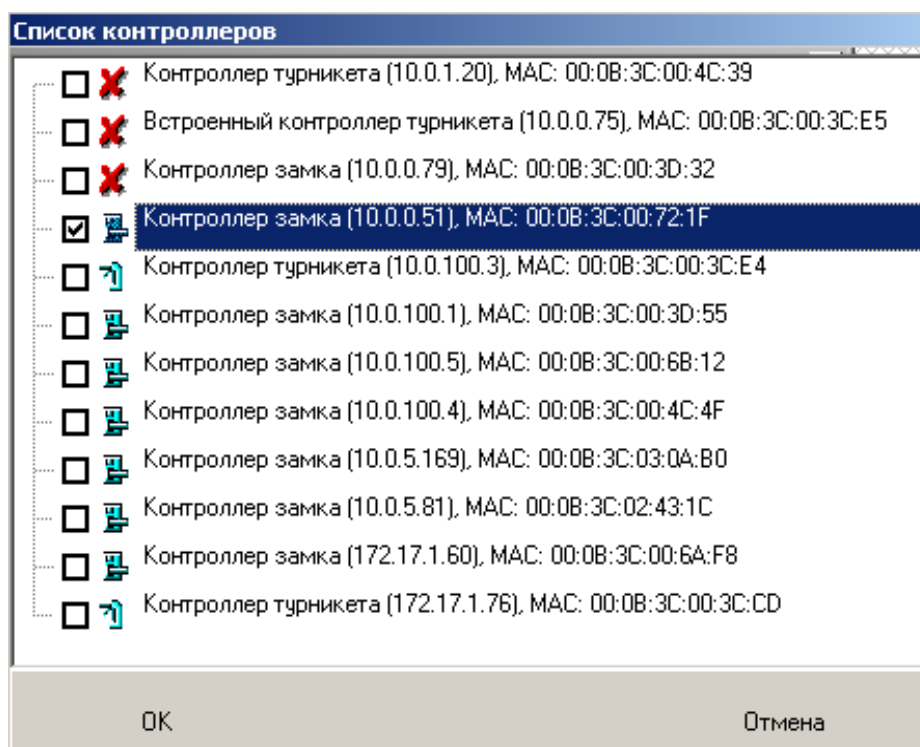
Для запуска центра управления PERCo-S-20 запустите Панель управления Windows

(**Пуск → Настройка → Панель управления →  Центр управления PERCo-S-20**). Убедитесь, что в данный момент сервер управления Firebird 2.5 и сервер системы запущены и работают. Перейдите на вкладку **Управление лицензиями**:

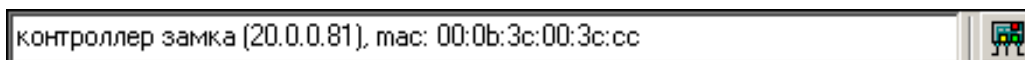


Для ввода лицензии укажите контроллер, MAC адрес которого был внесен вами в лицензионное соглашение. Для этого воспользуйтесь кнопкой, расположенной в верхней части программного окна.

После щелчка на ней откроется диалоговое окно выбора:



В этом окне отметьте выбранный вами раньше контроллер и щелкните на кнопке «ОК», что приведет к закрытию диалогового окна и отображению имени выбранного контроллера в поле в верхней части рабочего окна:

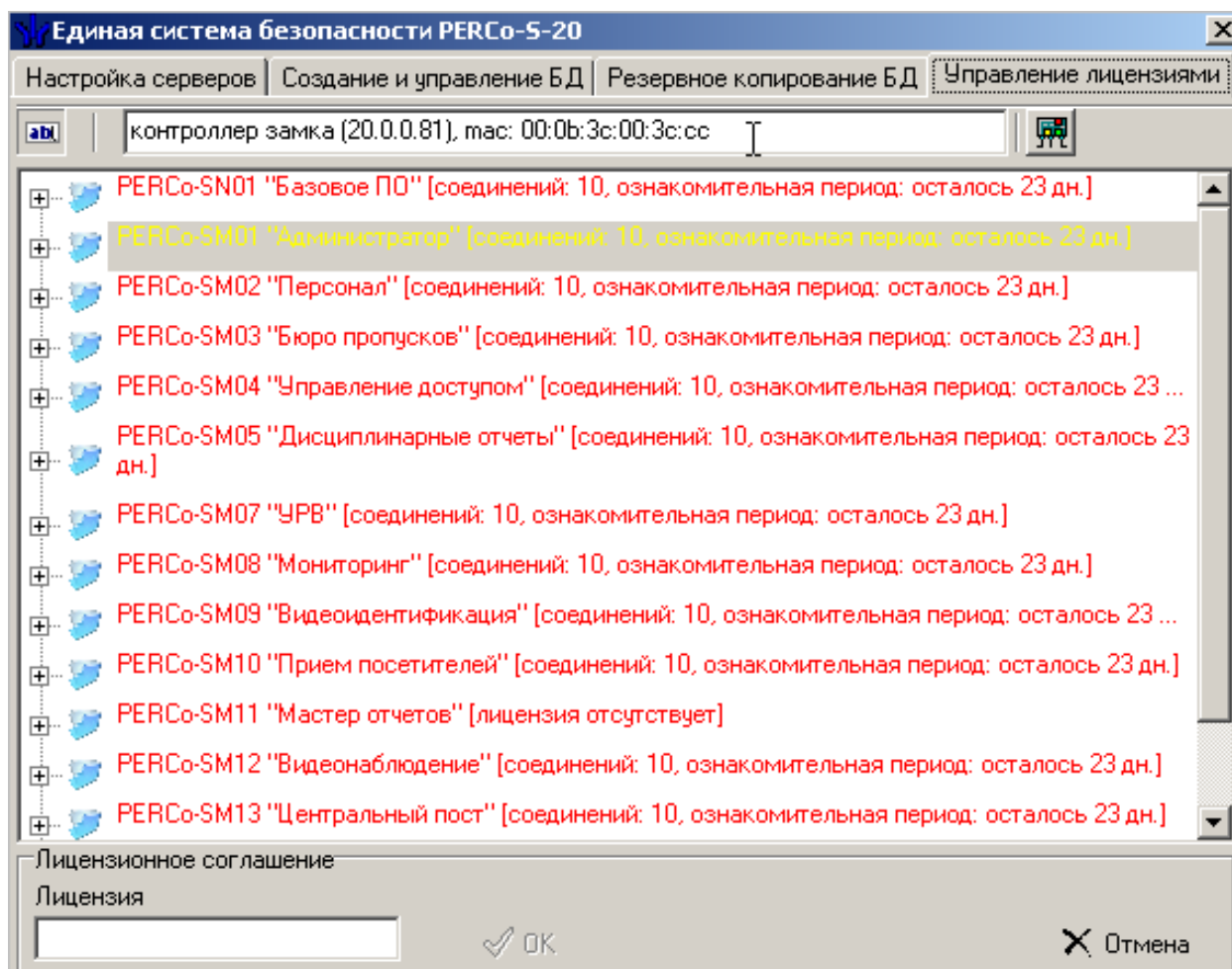


После выбора контроллера выделите в списке тот программный модуль, лицензию на который вы собираетесь ввести, и щелкните на кнопке Изменить лицензию — . При этом становится доступным строка ввода ключа активации:



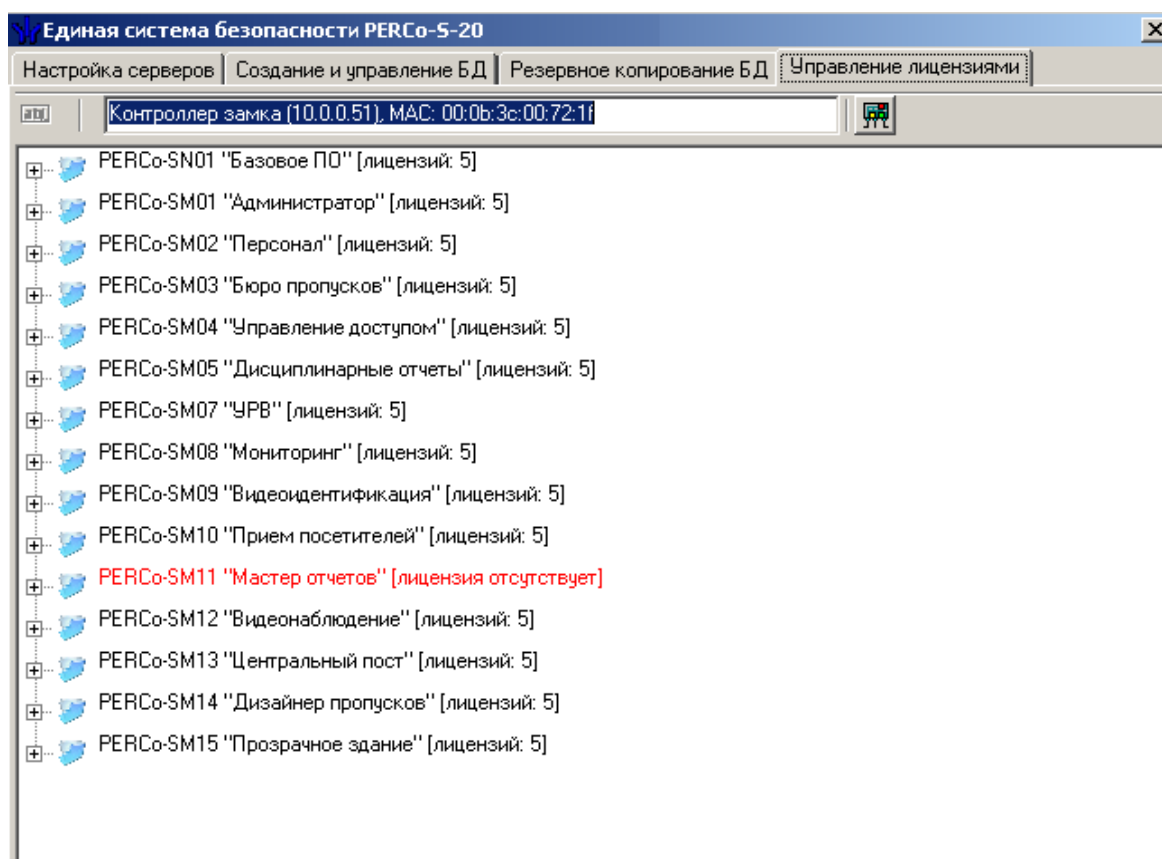
ПРИМЕЧАНИЕ

Код активации вводится без разделителей. Выбранный вами контроллер должен находиться во включенном состоянии, и быть подключенным к программному обеспечению. Для проверки наличия связи между программным обеспечением и выбранным контроллером можно воспользоваться разделом «Управление устройствами».

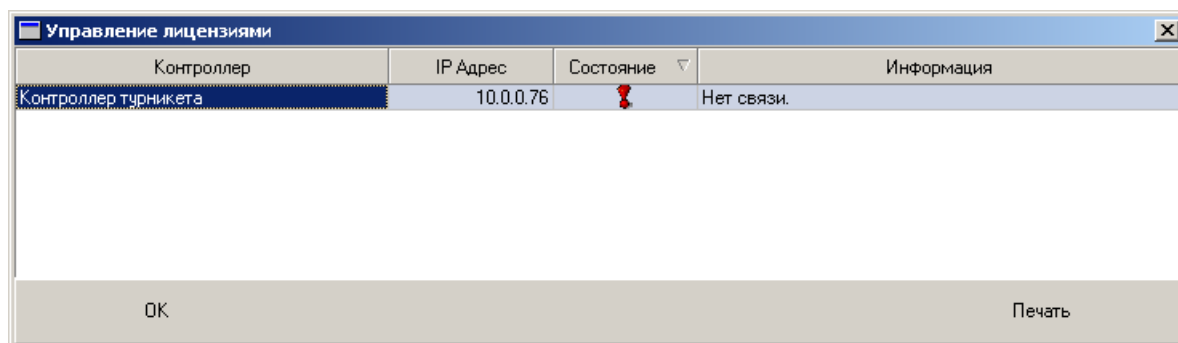


Введите код активации и нажмите кнопку . После этого программное обеспечение автоматически осуществит проверку введенного вами кода активации. При

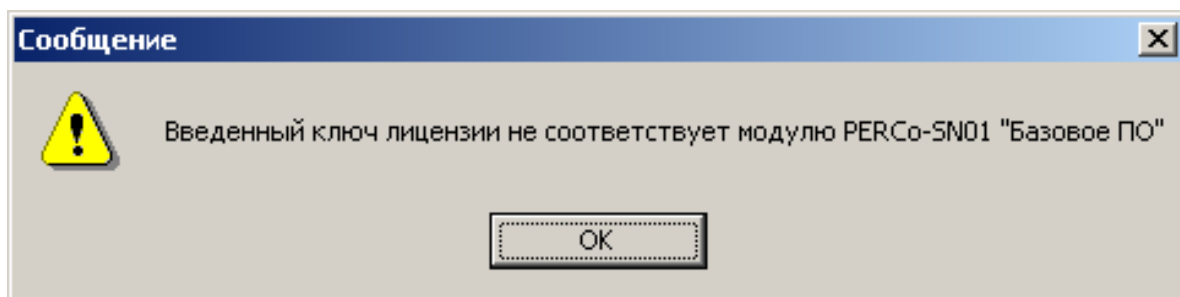
положительном ответе рядом с названием выбранного модуля отображается информации о количестве активированных рабочих мест.



В случае невозможности связаться с выбранным контроллером программное обеспечение выдаст сообщение о невозможности подключения и проверки правильности введенного ключа активации:



В случае если вы ошиблись при вводе ключа активации, и система не может правильно декодировать его, то есть он не соответствует выбранному модулю и/или контроллеру, программное обеспечение выдаст сообщение об ошибке регистрации ключа активации:



В случае выдачи ошибки проверьте, что контроллер в данный момент находится на связи с программным обеспечением, что вы не ошиблись при вводе ключа активации. И повторите попытку.



ПРИМЕЧАНИЕ

Выбранный вами контроллер всегда будет использоваться для проверки введенных ключей активации! В случае отсутствия связи с контроллером система автоматически перейдет в 30-ти дневный режим ознакомления.

ОБЩИЕ СВЕДЕНИЯ

Для функционирования сетевых контроллеров необходима сеть Ethernet 10-BaseT, 100-BaseTX или 1000-BaseTX. Для передачи данных используются непосредственно IP-адреса контроллеров, а также UDP протокол. Наличие таких серверов или служб, как DNS и WINS, не требуется.

С точки зрения правильной настройки системы передачи данных в существующей топологии сети организации, эксплуатирующей систему PERCo-S-20, необходимо понимание реализованного механизма передачи данных. Ниже представлена информация необходимая системным администраторам, при наличии в организации нескольких подсетей, межсетевых экранов, маршрутизаторов и т.п.

Для обмена данными в системе используется следующий стек протоколов Рис.2. Также для передачи данных используются следующие порты:

Табл. 1

Протокол	Порт	Назначение
UDP	18900	конфигурация сетевых параметров контроллера
	18901	широковещательные кадры (только между контроллерами) внутри подсети
TCP	18902	порт контроллера для конфигурации, управления и диагностики
	18903	порт контроллера для приема журнала регистрации
	18904	порт контроллера для регистрации индицирующего устройства

Протокол	Порт	Назначение
	18905	порт контроллера для регистрации верифицирующего устройства
	18906	порт контроллера для приема и анализа мониторинга

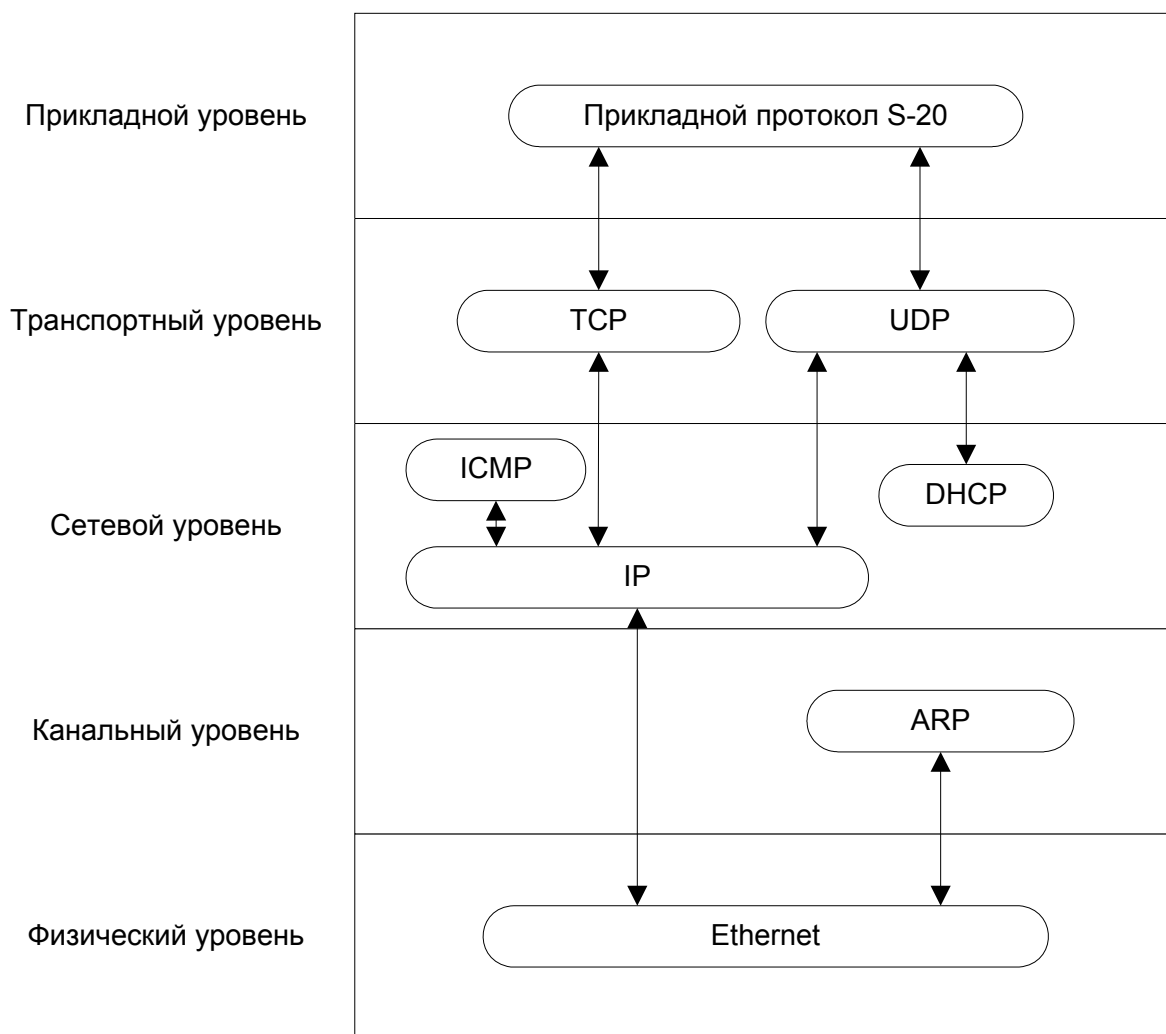


Рис.2. Стек протоколов, используемых для обмена в системе

С точки зрения конфигурирования сетевых коммутаторов и подобного оборудования, следует иметь в виду, что контроллерами и сервером системы PERCo-S-20 помимо адресной передачи пакетов используется и широковещательная передача. Однако, «достаточным» условием будет возможность прохождения широковещательных пакетов в пределах своей подсети, трансляции в другие подсети не требуется. При установке контроллеров в другие подсети для обеспечения связи с ПО PERCo-S-20 их адреса в других подсетях придется заносить в ПО PERCo-S-20 вручную.

Сетевые контроллеры не поддерживают фрагментацию IP-пакетов. Поэтому, если у Вас на предприятии довольно разветвленная сеть, использующая роутеры, концентраторы

и сетевые модемы, то удостоверьтесь, что IP-пакеты на всем протяжении от сервера системы PERCo-S-20 до контроллера не фрагментируются:

1. Убедитесь на примере компьютера с сетевыми настройками аналогичными настройкам контроллера, который предполагается установить, что между точками подключения сервера системы PERCo-S-20 и контроллера существует связь (маршрутизация настроена правильно, нет обрывов кабеля и т.п.).

Для проверки связи (на примере ОС Windows):

а) щелкните на панели инструментов **Пуск** → **Выполнить** → в открывшемся окошке введите *cmd.exe*;

б) в появившейся консоли введите

ping XX.XX.XX.XX,

где (XX.XX.XX.XX – адрес вашего компьютера, т.е. тот адрес, который планируется установить контроллеру).

Если связь есть, то вы увидите строки вида:

Ответ от 193.124.71.56: число байт=32 время<10мс TTL=128.

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

2. Подключите настроенный (см. ниже) контроллер.

3. «Пропингуйте» контроллер с порта, к которому планируется подключать сервер PERCo-S-20.

Для этого в этой же консоли введите:

ping XX.XX.XX.XX -l 576.

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

Ответ от 193.124.71.56: число байт=576 время<10мс TTL=128.

В данном случае можно утверждать, что IP-пакеты размером меньшим 576 байт не фрагментируются, и выбранное Вами подключение должно работать.

Если положительный ответ получить не удастся, то вероятнее всего на пути следования IP-пакетов находится сетевое коммутирующее оборудование, фрагментирующее IP-пакеты, которые размером меньше 576 байт. Проверьте настройки этого оборудования, при возможности увеличьте размер MTU (Maximum Transmission Unit). Обычно этот параметр обозначается как *MaxMTU* или *IPMTU*.

Если у Вас возможны несколько вариантов коммутации, то воспользуйтесь командой:

ping XX.XX.XX.XX -l 576 -t.

Коммутируя разными способами, смотрите на время ответа, выбирая соединение, дающее максимально быстрый ответ.

НАСТРОЙКА КОНТРОЛЛЕРА

Помимо определения местоположения контроллера как физически, так и в сети, настройте сам контроллер.

Для этого:

1. Задайте IP-адрес и выберите режим получения адреса, согласовав его с работой Вашей сети.
2. Сконфигурируйте контроллер с помощью раздела Конфигуратор (см. Руководство оператора по разделу Конфигуратор), определив его целевые параметры.

Каждый контроллер имеет следующие предопределенные (заводские) сетевые настройки:

IP-адрес : 10.x.x.x

Шлюз : 10.0.0.1

Маска сети : 255.0.0.0

MAC-адрес : xx xx xx xx xx xx (уникальный, неизменяемый при настройках).

Конкретные для каждого контроллера значения (вместо символа «х») указываются в паспорте на изделие и на наклейке на корпусе контроллера.

После задания настроек (*IP-адрес, шлюз, маска сети*) при конфигурировании контроллера в силу вступают заданные *пользовательские настройки*.

Настройка контроллера производится в зависимости от наличия в сети организации DHCP сервера. Главное, что нужно учитывать при задании сетевых настроек и последующей конфигурации самой системы PERCo-S-20 это необходимость обеспечения:

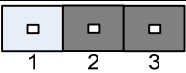
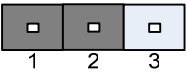
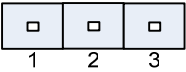
- уникальности сетевых адресов контроллеров в своей сети;
- предотвращения смены контроллерами своих IP-адресов после конфигурации системы PERCo-S-20, т.е. резервирование IP-адресов в сервере DHCP.

Режимы получения адреса

Режим работы по получению контроллером адреса задается с помощью устанавливаемых на плате контроллера перемычек на разъеме XP1. Расположение разъема на плате указывается в Руководстве по эксплуатации на конкретное изделие.

Результаты изменений положения перемычек вступают в силу только при перезапуске контроллера.

Табл. 2. Варианты перемычек на контроллерах

№	Расположение перемычек на XP1	Режим
1.		Работа с заводскими настройками
2.		Работа с DHCP
3.		Работа с пользовательскими настройками. Если их нет, то работа с заводскими настройками

Настройка без DHCP

Настройка производится с помощью персонального компьютера с установленным ПО PERCo-S-20. Обеспечьте связь по сети Ethernet контроллера и компьютера с установленным ПО PERCo-S-20. Для обеспечения данной связи контроллер с установленными сетевыми настройками подключается в тот же сегмент сети или непосредственно к сетевому разъему сетевой карты компьютера.

Для обеспечения этого условия:

1. Добавьте (см. Рис.4) новый IP-адрес на сетевой интерфейс Вашего персонального компьютера с установленным ПО PERCo-S-20. Или измените существующие IP-адрес (например, 10.0.0.1) и маску сети на те, которые указаны в паспорте на контроллер. Сделайте это соответствующим для операционной системы образом.

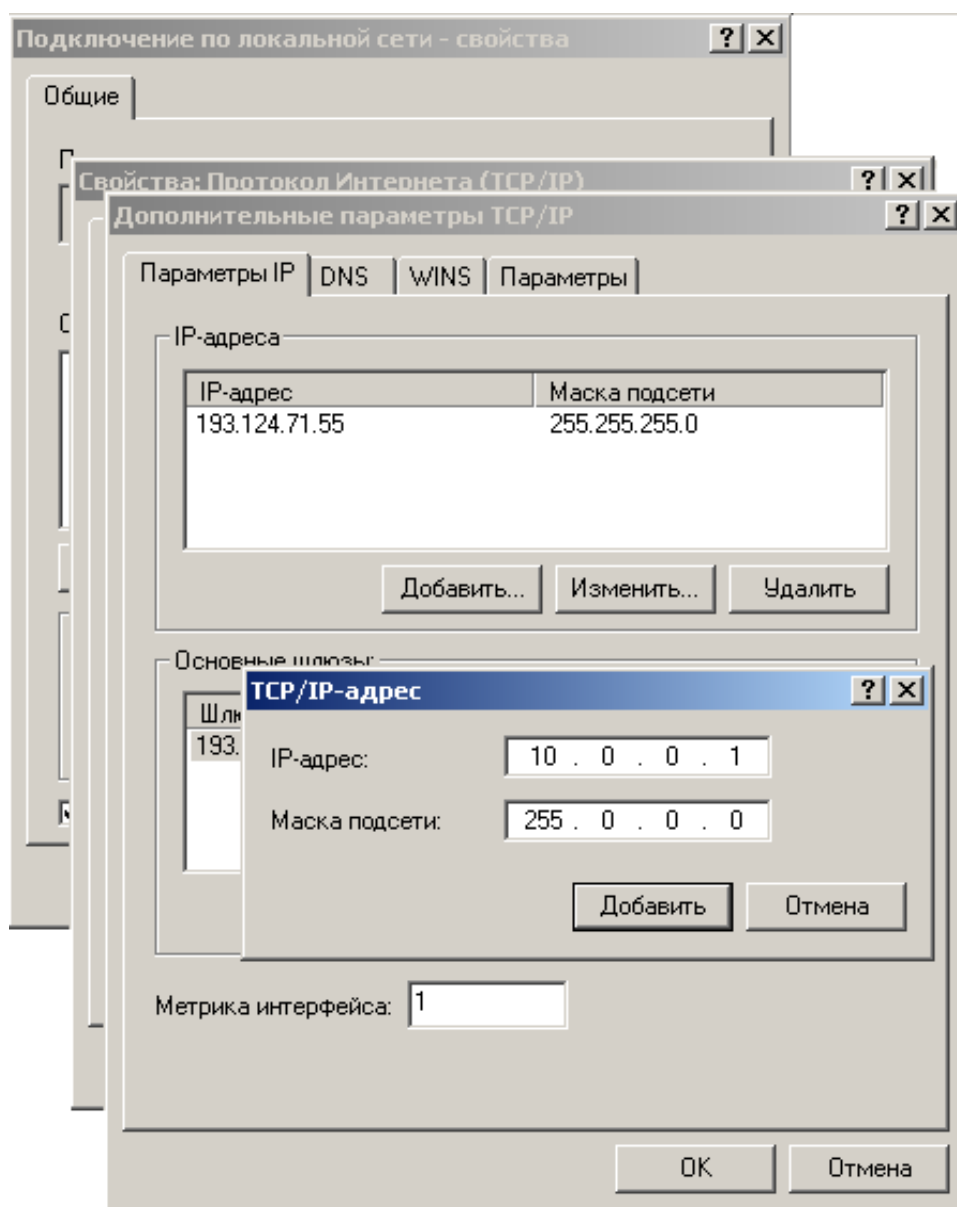


Рис. 4. Добавление нового IP-адреса

2. Установите переключки по 4-му варианту (см. Табл. 2).
3. Подключите контроллер к сети (в тот же сегмент) или непосредственно к сетевому разъему сетевой карты компьютера.

Если при подключении контроллера непосредственно к разъему RJ-45 (порт MDI-X) связь с контроллером не удалось установить, то используйте сетевой кабель с перекрестным соединением пар. Такой кабель, например, применяют при соединении концентраторов через стандартный порт MDI-X.

4. Включите контроллер. Произведите настройку согласно п. «[Конфигурация контроллеров](#)».

У контроллера достаточно сконфигурировать только сетевые настройки.

5. Установите контроллер на выбранное место работы.

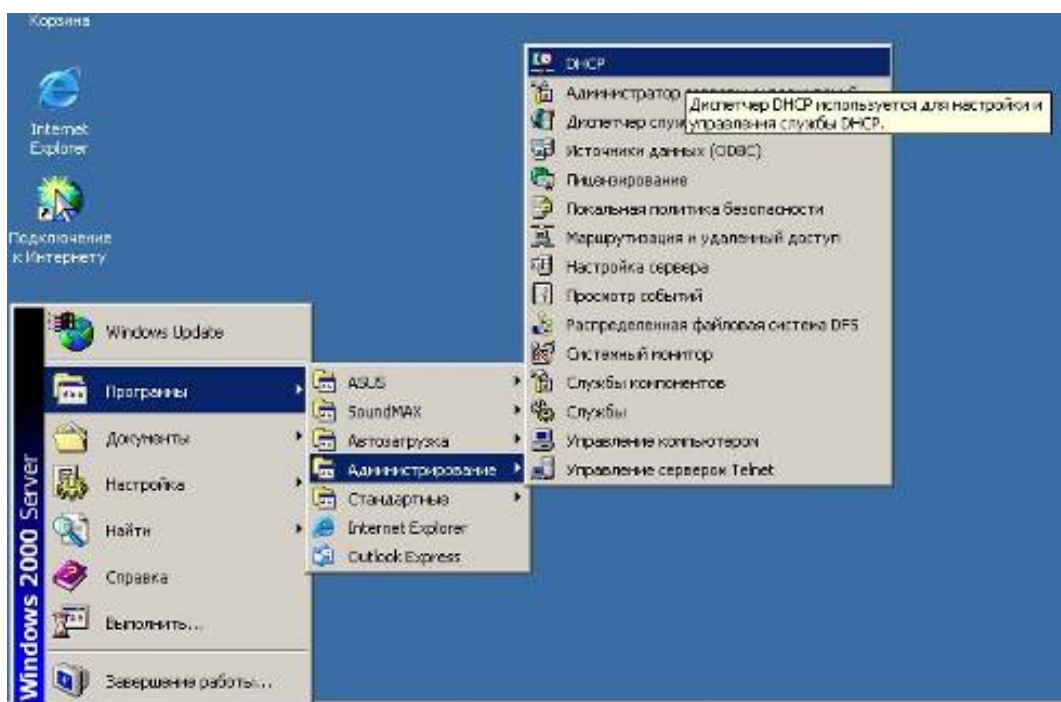
Настройка с DHCP

Настройка DHCP сервера, установленного в сети предприятия, сводится к резервированию диапазона IP-адресов, выделяемых под контроллеры, и к привязке MAC-адреса контроллера к зарезервированному IP-адресу. Следует обратить внимание, что при настройке (перемычками на плате) контроллера на режим работы с DHCP изменения настроек, сделанные через Конфигуратор, не будут иметь силы.

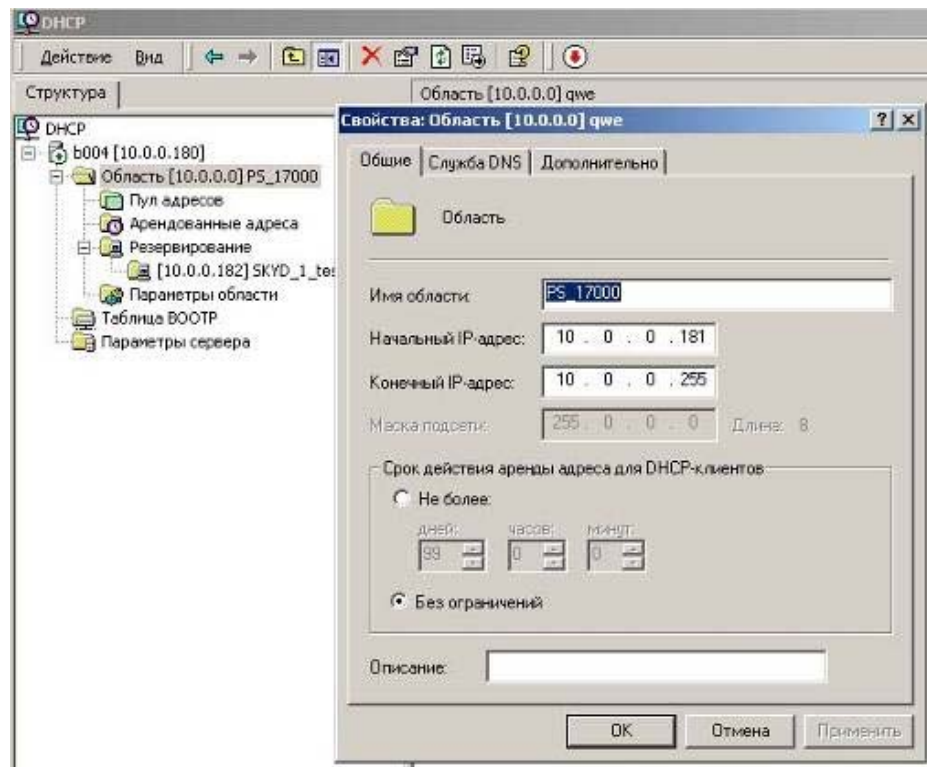
ОС Windows

Описание настройки приведено на примере Windows 2000. Для других операционных систем смысл остается таким же.

1. Запустите DHCP сервер:



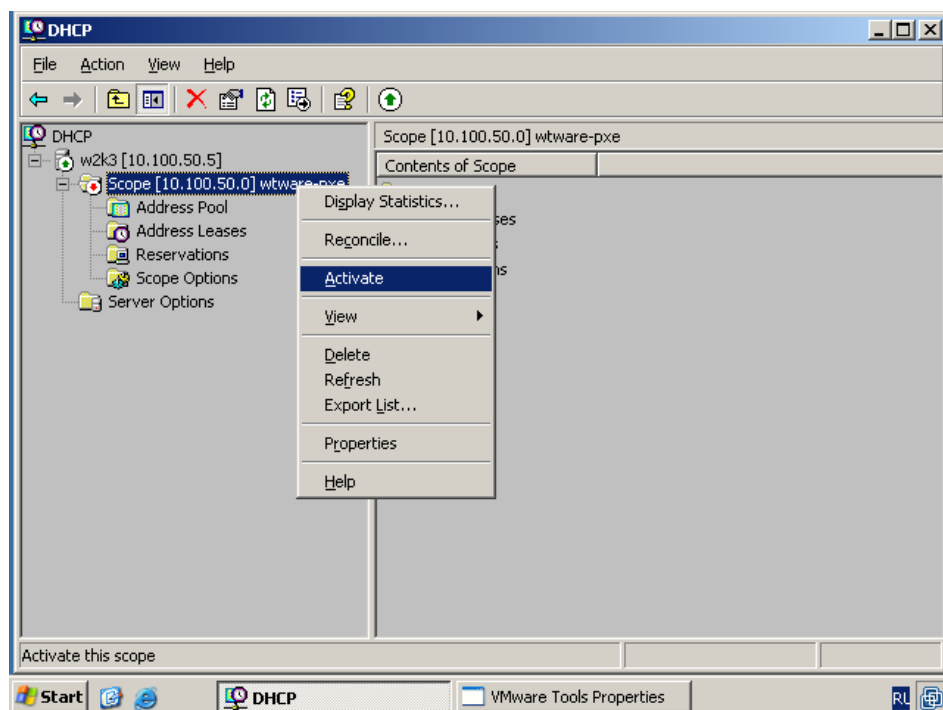
2. Создайте область адресов для контроллеров системы PERCo-S-20:



Название области и описание могут быть любыми. Это информация не для системы, а для системного администратора. Лучше, если название достаточно информативно, чтоб не вспоминать потом, что настраивается в этой области.

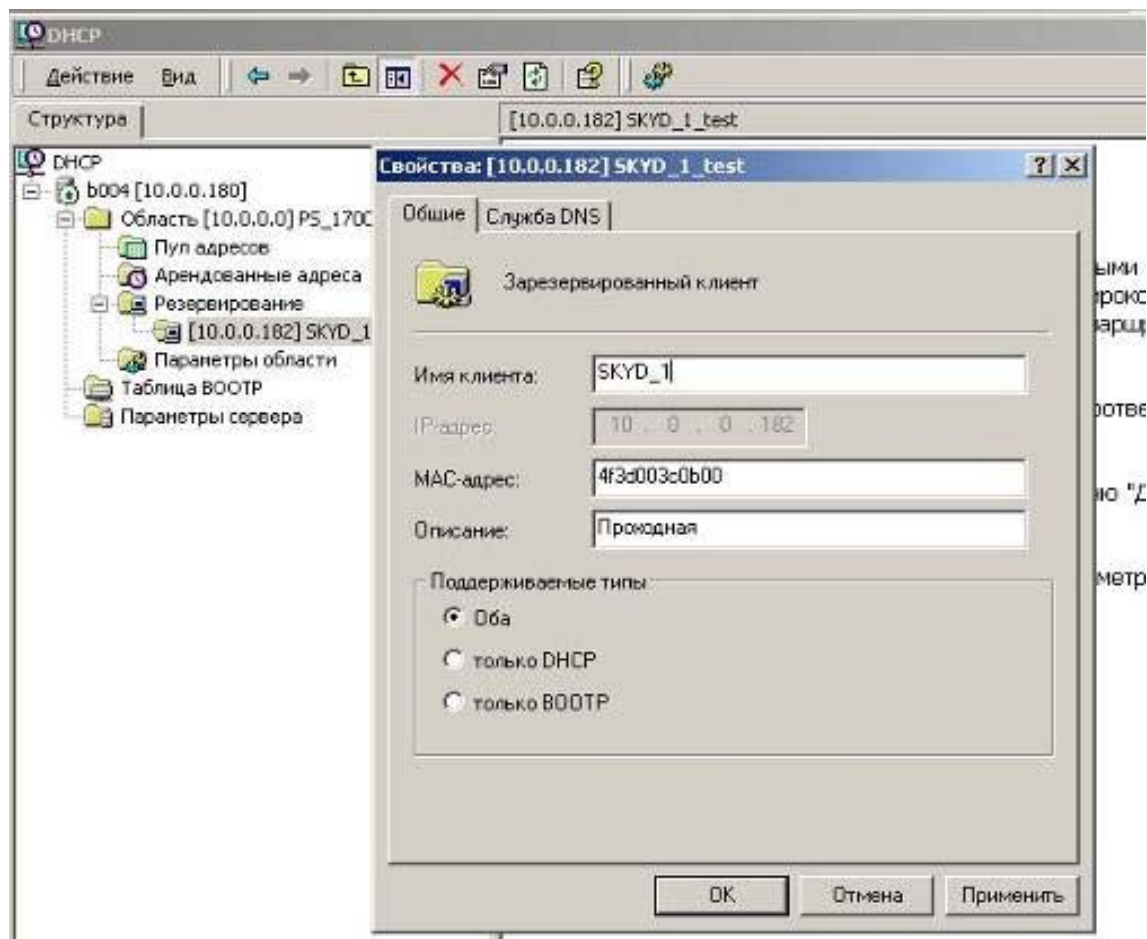
Рекомендуется делать область несколько больше, чем число контроллеров, которое планируется использовать. Также задавайте такую область адресов, которая не будет включать в себя уже существующие машины с фиксированными адресами.

3. Последний и обязательный шаг - активация области:



После этого Ваш DHCP сервер сможет предоставить информацию, необходимую контроллеру для получения IP-адреса.

4. Проведите резервирование адресов своих контроллеров. Для этого задайте IP-адрес из выбранной Вами области и поставьте его в соответствии с MAC-адресом контроллера, указанном в паспорте.
5. Для удобства добавьте описание.



Данную операцию повторите для всех контроллеров, которые планируется установить в Вашей сети.

6. Установите перемычки по 2-му варианту (см. Табл. 2).
7. Подключите контроллеры к сети и включите их.

Если вы не ошиблись при вводе, то все контроллеры будут отображаться в списке арендованных адресов.

8. Обязательно проверьте, чтобы в столбце о времени аренды адреса находилась информация об активном резервировании.

ОС Linux

Если у Вас сервер DHCP установлен на ОС Linux, то настройка сведется к редакции файла конфигурации «демона» сервера DHCP (dhcpd). Конфигурационным файлом для dhcpd является */etc/dhcp.conf*. Не забудьте, что, чтобы внесенные Вами в файл */etc/dhcp.conf* изменения вступили в силу, «демон» (dhcpd) необходимо остановить и запустить снова.

При этом можно использовать команду */etc/rc.d/init.d/dhcpd stop* для остановки «демона», и команду */etc/rc.d/init.d/dhcpd start* для его запуска.

Примерный вариант файла конфигурации показан ниже:

```
# Подсеть 10.100.0.0, маска сети 255.255.255.0
subnet 10.100.0.0 netmask 255.255.255.0 {
# маска подсети 255.255.255.0
option subnet-mask 255.255.255.0;
...
# диапазон адресов для контроллеров
# 10.100.0.10-10.100.0.254
range 10.100.0.10- 10.100.0.254;
...
# описание контроллеров (proxod_1, ..., office_room_101)
# обратите внимание на то, что вы должны использовать
# IP-адрес из указанного Вами диапазона

host proxod_1 {
hardware ethernet XX:XX:XX:XX:XX:XX;
fixed-address 10.100.0.50;
}
...
host office_room_101 {
hardware ethernet XX:XX:XX:XX:XX:XX;
fixed-address 10.100.0.37;
}
...
}
```

Опции настроек маршрутизатора, домена, широковещательного адреса, DNS и т.д. прописываются при необходимости (для более полной информации о вариантах конфигурации воспользуйтесь командой *man dhcpd.conf*).

Особенности работы стека протокола TCP/IP в Windows XP

В операционной системе Windows XP существует ограничение на количество попыток одновременных TCP-подключений. Количество таких попыток по умолчанию равно 10 и введено для защиты от вирусов и DoS-атак. Если Сервер системы установлен на компьютер с Windows XP, то следует пропатчить драйвер TCPIP.SYS на количество таких попыток равное 100. Один из возможных патчей находится по адресу http://half-open.com/download_ru.htm. О наличии ограничения на количество попыток одновременных TCP-подключений можно судить по записям в журнале событий системы. Запустите Event Viewer (например через Control Panel — Administrative Tools; или Пуск — Выполнить — EventVwr.msc). Каждое сообщение вида «EventID 4226: Достигнут предел безопасности для TCP/IP, налагаемый на количество попыток одновременных TCP-подключений.» говорит о том, что такое ограничение сработало.

КОНФИГУРАЦИЯ КОНТРОЛЛЕРОВ

КОНФИГУРАЦИЯ УСТРОЙСТВ СИСТЕМЫ БЕЗОПАСНОСТИ

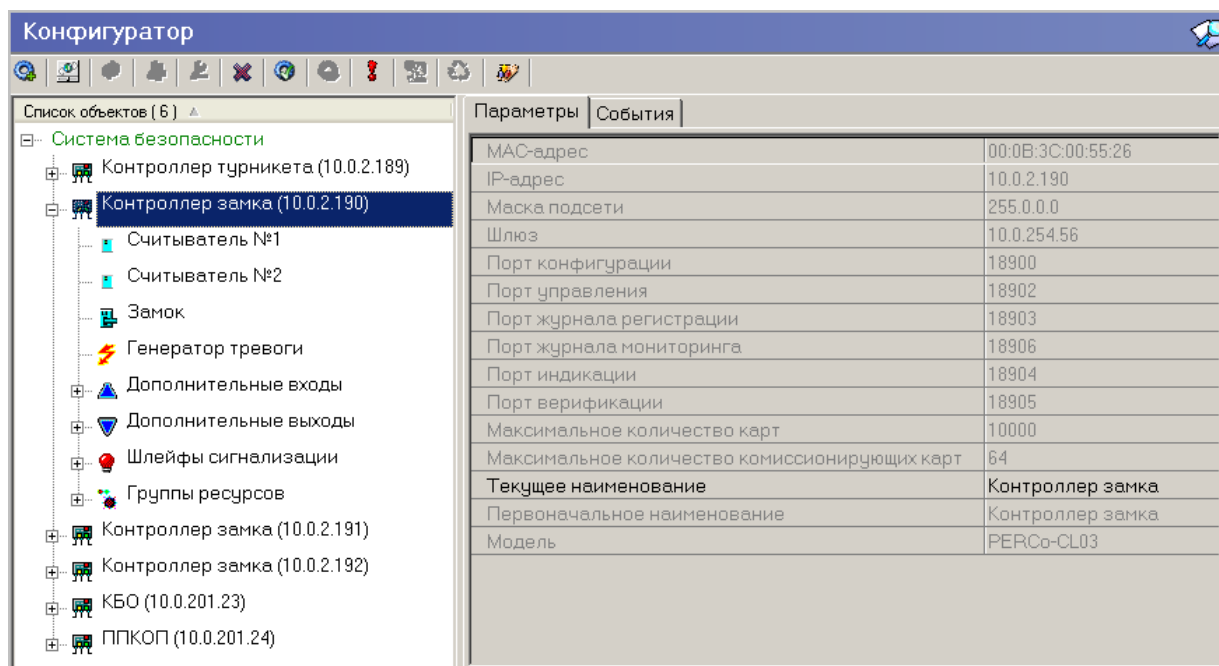
Конфигурация контроллеров системы безопасности может происходить в автоматическом и ручном режиме.

Для автоматической конфигурации контроллеров системы безопасности необходимо, чтобы все IP-адреса контроллеров системы безопасности PERCo-S-20 находились в одной подсети. В той же подсети должны находиться компьютеры, на которых установлено программное обеспечение системы.

Самым простым вариантом работы по данному сценарию является использование заданных при производстве контроллеров IP-адресов и задание IP-адресов из той же подсети в стеки IP-адресов персональных компьютеров, на которых установлено программное обеспечение системы безопасности.

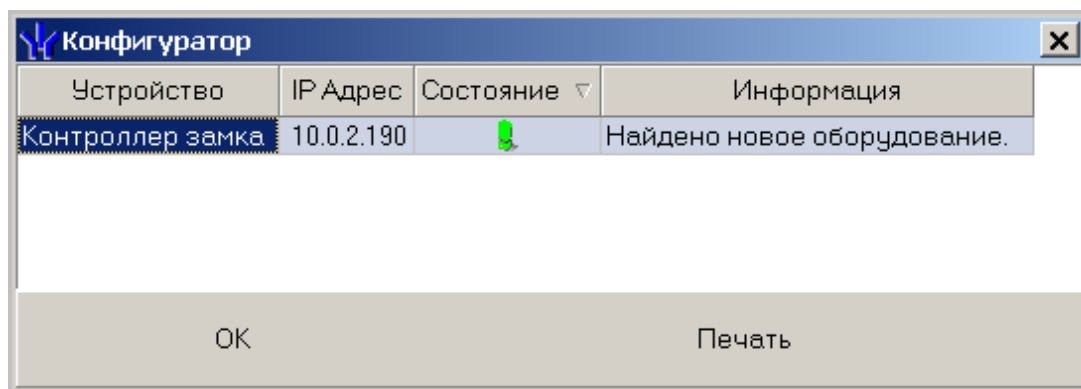
Если все вышесказанное выполнено, произведен монтаж контроллеров системы, при помощи команды “ping” проверено прохождение IP-пакетов с компьютера с установленным сервером системы, можно приступить к проведению конфигурации системы безопасности:

Запустите «Консоль управления» на компьютере, на котором был проинсталлирован раздел Конфигуратор.



Подробная информация о назначении элементов меню раздела Конфигуратор приведена в Руководстве оператора раздела Конфигуратор.

Проведите конфигурацию. После окончания сканирования локальной сети откроется диалоговое окно со списком найденного оборудования:



Проанализируйте полученную информацию, а именно проверьте, все ли контроллеры были найдены в результате проведения конфигурации.

Если какой либо из контроллеров не был найден, проверьте правильность его монтажа, прохождение IP-пакетов к этому контроллеру от компьютера с установленным сервером системы и повторите конфигурацию.

Если контроллер так и остался найденным, попробуйте добавить его в конфигурацию вручную. Более подробная информация о способе ручного добавления контроллеров в конфигурацию приведена в Руководстве оператора в разделе Конфигуратор.

Перед началом добавления убедитесь, что оборудование смонтировано в соответствии с инструкцией по монтажу и включено.

Для этого необходимо войти в раздел Конфигуратор и нажать на кнопку **Добавить новое устройство** — . При этом в нижней части рабочего окна откроется дополнительная панель поиска:

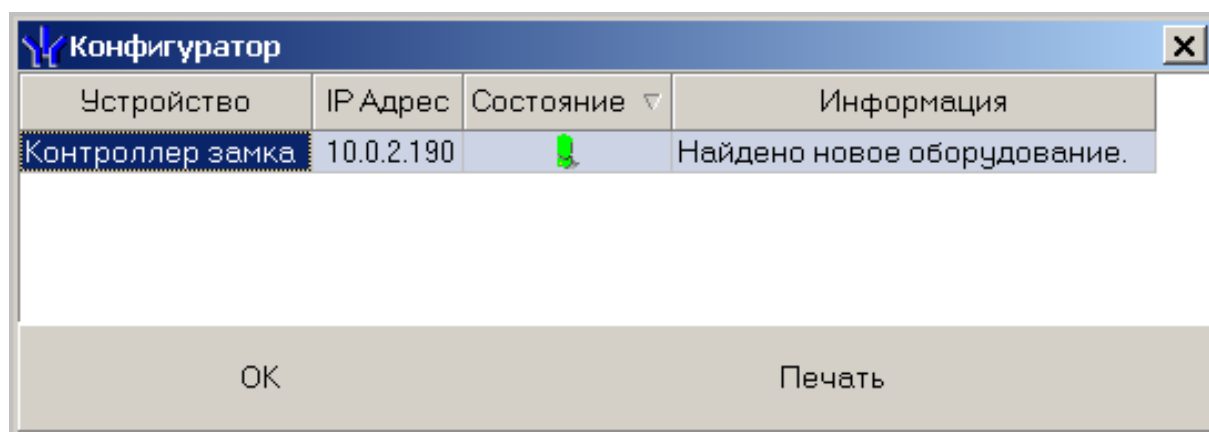
В списке **Категория** выберите одно из предлагаемых значений:

- ✓ **Контроллер доступа и регистрации, КБО, ППКОП** – в случае, если вы хотите добавить контроллер управления доступом или регистрации, контроллер безопасности объекта (КБО) или прибор приемно-контрольный охранно-пожарный (ППКОП).

В поле **IP адрес** необходимо указать IP адрес устройства в формате XXX.XXX.XXX.XXX.

После задания этих параметров, автоматически становится доступной кнопка **Найти**. Нажмите на нее, программное обеспечение проведет проверку возможности

подключения к заданному вами устройству. Итоги этой проверки будут отображены в диалоговом окне:



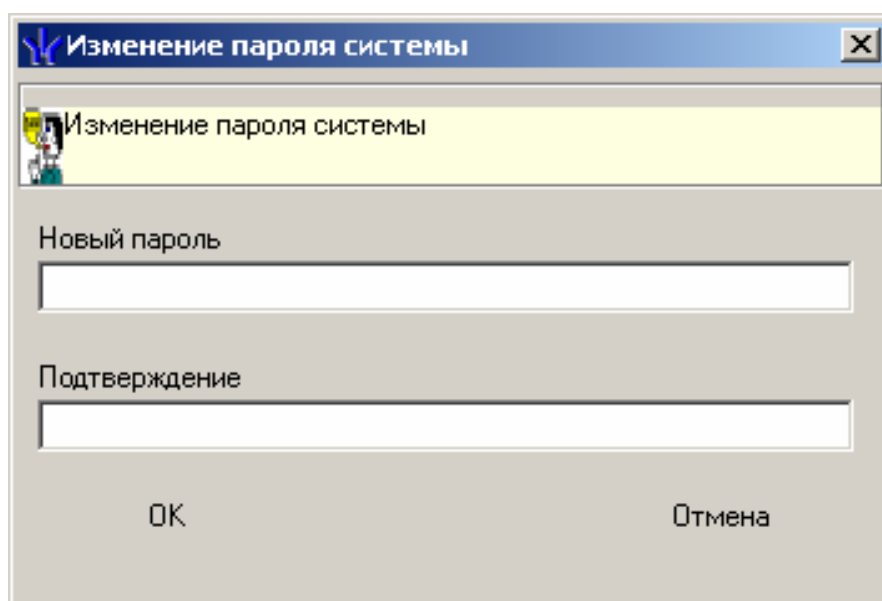
Нажмите на кнопку «**ОК**». Найденное оборудование будет добавлено в конфигурацию системы.

После того, как все контроллеры будут добавлены, необходимо перейти к описанию параметров их функционирования.

ЗАДАНИЕ ПАРОЛЯ СВЯЗИ С КОНТРОЛЛЕРАМИ

Для защиты контроллеров, входящих в состав системы безопасности, от несанкционированного доступа по сети Ethernet необходимо задать пароль. Этот пароль используется при установлении связи между контроллерами системы и программным обеспечением.

Для задания пароля необходимо воспользоваться кнопкой **Изменение пароля** — , расположенной в верхней части окна раздела Конфигуратор. Нажатие на нее приводит к появлению диалогового окна, в котором вы должны ввести пароль, и продублировать его в окне **Подтверждение**:





ПРИМЕЧАНИЕ

В качестве символов пароля допустимо использовать только английские буквы и цифры. Максимальная длина пароля 10 символов.

После ввода пароля необходимо передать измененные параметры.

ИЗМЕНЕНИЕ СЕТЕВЫХ НАСТРОЕК

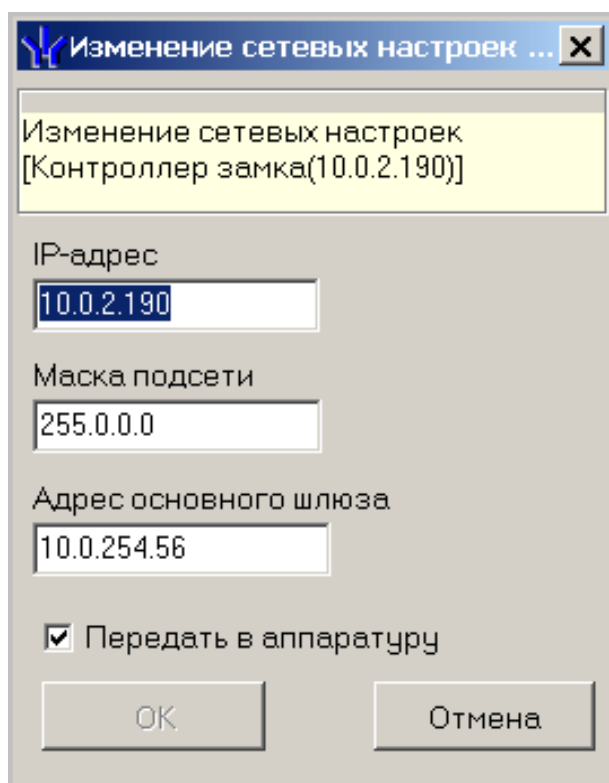
Каждый контроллер имеет свои собственные настройки в сети, что упрощает их поиск, подключение друг к другу, обеспечивает связь между ними.

Для изменения сетевых настроек:

1. Выделите контроллер, чьи сетевые настройки подлежат изменению.

2. Исклучите контроллер из конфигурации, нажав на .

3. Щелкните на кнопке **Изменение сетевых настроек** — . Откроется окно:



4. Произведите изменения.

5. Щелкните на кнопке «ОК», а затем передайте измененные параметры в аппаратуру с помощью кнопки **Передать измененные параметры** — . Сетевые настройки изменятся.

ОПИСАНИЕ ПАРАМЕТРОВ ФУНКЦИОНИРОВАНИЯ КОНТРОЛЛЕРОВ ДОСТУПА

Подробная информация о параметрах функционирования контроллеров системы безопасности PERCo-S-20 приведена в техническом описании системы безопасности.

Ниже будут приведены общие рекомендации, проиллюстрированные примерами задания тех или иных параметров контроллеров.

Дополнительный вход

Каждый контроллер доступа, входящий в систему безопасности PERCo-S-20, в зависимости от своего типа имеет до четырех дополнительных входов.

Дополнительные входы контроллеров могут быть использованы для наблюдения за состоянием внешнего оборудования, подключенного к ним, и для подключения кнопок сброса тревоги.

В зависимости от того, какое внешнее оборудование подключено к дополнительному входу, существуют следующие варианты описания параметров его работы:

1. При условии, что к данному дополнительному входу не подключено никакое внешнее оборудование, менять параметры работы входа не нужно.
2. **Нормальное состояние контакта** (нормально замкнут или нормально разомкнут). Этот параметр зависит от типа подключенного оборудования и указывает системе на то, какое значение уровня сигнала на входе она должна воспринимать как нормальное.
3. Тип входа – **Обычный**. Означает что к данному тестовому входу подключено дополнительное оборудование, состояние которого должно контролироваться контроллером. При выборе этого типа можно так же указать алгоритм действий контроллера при получении управляющего воздействия от подключенного оборудования, а именно:

Текущее наименование	Дополнительный вход №1
Адрес	1
Первоначальное наименование	Дополнительный вход №1
Нормальное состояние контакта	Разомкнут
Тип	Обычный
☐ Обычный	
☐ <u>Дополнительные входы, маскируемые при активизации</u>	
☐ Критерий маскирования	На указанное время
☐ <u>На указанное время</u>	
Время	3 сек.
Дополнительный вход №2	☒
☐ <u>Дополнительные выходы, активизируемые при активизации</u>	
Критерий активизации	На время срабатывания
Дополнительный выход №1	☒
Дополнительный выход №2	☐
☐ <u>Дополнительные выходы, нормализируемые при активизации</u>	
☐ Критерий нормализации	На время срабатывания и после срабатывания
☐ <u>На время срабатывания и после срабатывания</u>	
Время	250 мс.
Дополнительный выход №1	☒
Дополнительный выход №2	☐
☐ <u>Дополнительные выходы, реагирующие через группу ресурсов</u>	
Дополнительный выход №4	☒
Дополнительный выход №5	☐

- **Дополнительные входы, маскируемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы, т.е. не воспринимать управляющий сигнал от внешнего оборудования, при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных входов, которые должны быть маскированы. Кроме этого, укажите временной критерий маскирования, который может быть одним из трех видов:

☐ Критерий маскирования	На указанное время
☐ <u>На указанное время</u>	На указанное время
Время	На время срабатывания
Дополнительный вход №2	На время срабатывания и после срабатывания
	☒

- ✓ **На указанное время** – выбранные дополнительные входы будут маскированы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные входы будут маскированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал плюс указанное вами время.
- **Дополнительные выходы активизируемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Кроме этого, укажите временной

☐ Критерий активизации	На указанное время
☐ На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания

✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время.

✓ **На время срабатывания** – выбранные дополнительные выходы будут активизированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.

✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал плюс указанное вами время.

- **Дополнительные выходы, нормализуемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализованы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть нормализованы. Кроме этого, укажите временной критерий нормализации, который может быть одним из трех видов:

☐ Критерий нормализации	На указанное время
☐ На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания

✓ **На указанное время** – выбранные дополнительные выходы будут нормализованы на указанное время.

✓ **На время срабатывания** – выбранные дополнительные выходы будут нормализованы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.

✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут нормализованы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал плюс указанное вами время.

- **Дополнительные выходы, реагирующие через группу ресурсов.** Этот параметр указывает те дополнительные выходы, которые будут активизированы, при условии, что данный дополнительный вход входит в группу ресурсов.

4. Тип входа – **Специальный**. Предназначен для автономного сброса тревоги в состоянии «Тревога как СКУД» либо выключения sireны в состоянии «Тревога как ОПС».

Текущее наименование	Дополнительный вход №2
Адрес	2
Первоначальное наименование	Дополнительный вход №2
Нормальное состояние контакта	Разомкнут
Тип	Специальный ▼
☐ <u>Специальный</u>	
Сброс тревоги (Генератор тревоги)	☐
Сброс сирены (Выход "С" ОПС)	☐

Если выбранный вход используется как вход автономного сброса тревоги, необходимо указать какой тип тревоги будет сбрасываться при поступлении управляющего сигнала на дополнительный вход.

Возможны два варианта:

- ✓ **Сброс тревоги (Генератор тревоги).** В этом случае при возникновении тревоги из-за ситуации, описанной в генераторе тревоги, получение управляющего сигнала на выбранный дополнительный вход приведет к ее сбросу.
- ✓ **Сброс сирены (Выход «С» ОПС).** Аналогично предыдущему, за исключением того, что будет выключена сирена, подключенная к выходу «С» ОПС.

Дополнительный выход

Каждый контроллер доступа, входящий в систему безопасности PERCo-S-20, в зависимости от своего типа имеет до шести дополнительных выходов и один звуковой извещатель.

Дополнительные выходы могут быть использованы для управления любым внешним оборудованием в рамках системы безопасности. Технические параметры дополнительных выходов для каждого типа контроллеров приведены в техническом описании системы безопасности.

В зависимости от того, какое внешнее оборудование подключено к дополнительному выходу, существуют следующие варианты описания параметров его работы:

1. При условии, что к данному дополнительному выходу не подключено никакое дополнительное оборудование, менять параметры работы дополнительного выхода не нужно.
2. Тип дополнительного выхода – **Обычный**.

Текущее наименование	Дополнительный выход №2
Адрес	2
Первоначальное наименование	Дополнительный выход №2
Тип	Обычный
☐ <u>Обычный</u>	
Нормальное состояние	Не запитан

Этот параметр указывает, что к данному дополнительному выходу подключено внешнее оборудование, логика управления которым описывается через описание других устройств системы (за исключением генератора тревоги). Так же необходимо указать нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/не запитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий.

3. Тип дополнительного выхода – Генератор тревоги.

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

В этом случае решение об активизации дополнительного выхода принимается исключительно контроллером в соответствии с параметрами, указанными в его генераторе тревоги. Этот дополнительный выход будет использоваться исключительно для индикации перехода контроллера в состояние «Тревога». Так же задайте нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/не запитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий. Кроме этого, укажите время активизации дополнительного выхода, время, в течение которого при наличии активизирующего управляющего воздействия выход меняет своё состояние из нормализованного на противоположное. Как правило, в этом случае к такому дополнительному выходу подключают тревожный оповещатель (сирена, проблесковая лампа).

4. Тип дополнительного выхода – ОПС.

Текущее наименование	Дополнительный выход №1
Адрес	1
Первоначальное наименование	Дополнительный выход №1
Тип	ОПС
ОПС	
Программа управления	Выключить на время при невзятии
Выключить на время при невзятии	
Время активизации	3 сек.

В этом случае дополнительный выход предназначен для управления световым оповещением (СО), звуковым оповещением (ЗО), а так же для передачи тревожных извещений на пост центрального наблюдения (ПЦН) при активизации шлейфов сигнализации (ШС), дополнительных входов или контакта ИУ, входящих в группу ресурсов.

Программа управления задает логику работы контроллера по управлению данным дополнительным выходом. Вид программы выбирается из выпадающего списка.

Возможны следующие варианты программ управления:

- ✓ **Не управлять.** Дополнительный выход не используется как элемент системы охранной сигнализации.
- ✓ **Включить при тревоге.** В случае возникновения тревоги произойдет замыкание контакта дополнительного выхода.
- ✓ **Выключить при тревоге.** В случае возникновения тревоги произойдет размыкание контакта дополнительного выхода.
- ✓ **Включить на время при тревоге.** В случае возникновения тревоги произойдет замыкание контакта дополнительного выхода на время указанное в параметре время активизации.
- ✓ **Выключить на время при тревоге.** В случае возникновения тревоги произойдет размыкание контакта дополнительного выхода на время указанное в параметре время активизации.
- ✓ **Мигать из состояния выключено при тревоге.** В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода разомкнуты. В случае возникновения тревоги произойдет попеременное замыкание – размыкание контактов дополнительного выхода.
- ✓ **Мигать из состояния включено при тревоге.** В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода замкнуты. В случае возникновения тревоги произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Мигать на время из состояния выключено при тревоге.** В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода разомкнуты. В случае возникновения тревоги произойдет попеременное замыкание – размыкание контактов дополнительного выхода на время, указанное в параметре время активизации.
- ✓ **Мигать на время из состояния включено при тревоге.** В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода замкнуты. В случае возникновения тревоги произойдет попеременное размыкание – замыкание контактов дополнительного выхода на время, указанное в параметре время активизации.
- ✓ **Лампа** – программа управления, указывающая на то, что к данному дополнительному выходу подключен световой оповещатель тревожной ситуации.
- ✓ **ПЦН** – программа управления, указывающая на то, что данный дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН).
- ✓ **ПЦН (старая тактика)** – программа управления, указывающая на то, что данный дополнительный выход используется для передачи тревожного

извещения на пост центрального наблюдения (ПЦН) по старой тактике передачи тревожного оповещения.

- ✓ **Сирена** – программа управления, указывающая на то, что к данному дополнительному выходу подключен звуковой оповещатель тревожной ситуации.
- ✓ **Включить на время перед взятием** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, перед началом взятия шлейфа на охрану.
- ✓ **Выключить на время перед взятием** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, перед началом взятия шлейфа на охрану.
- ✓ **Включить на время при взятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, при взятии шлейфа на охрану.
- ✓ **Выключить на время при взятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, при взятии шлейфа на охрану.
- ✓ **Включить при взятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода при взятии шлейфа на охрану.
- ✓ **Выключить при взятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода при взятии шлейфа на охрану.
- ✓ **Включить на время при снятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, при снятии шлейфа с охраны.
- ✓ **Выключить на время при снятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, при снятии шлейфа с охраны.
- ✓ **Включить при снятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода при снятии шлейфа с охраны.
- ✓ **Выключить при снятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода при снятии шлейфа с охраны.
- ✓ **Включить на время при невзятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода при невозможности взятия шлейфа на охрану.
- ✓ **Выключить на время при невзятии** – программа управления,

указывающая на необходимость разомкнуть контакты дополнительного выхода при невозможности взятия шлейфа на охрану.

Исполнительное устройство

Каждый контроллер управления доступом, входящий в систему безопасности PERCo-S-20, может управлять одним исполнительным устройством. Тип исполнительного устройства определяется типом контроллера. Так как контроллер не может автоматически определить параметры функционирования исполнительного устройства, их необходимо задать. Для этого необходимо выбрать исполнительное устройство у контроллера. В правой части в инспекторе параметров будут отображены все возможные параметры функционирования.

Для контроллера управления замком:

Текущее наименование	Замок
Первоначальное наименование	Замок
Прямое направление прохода	☒
Нормальное (т.е заблокированное) состояние контакта (вход ИЧ)	Нормально замкнут
Нормальное состояние "Закрыто" выхода ИЧ	Не запитан
Нормализация выхода ИЧ	После "Открытия"
Режим работы выхода управления ИЧ	Потенциальный
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа идентификатора)	4 сек.
Регистрация прохода по предъявлению идентификатора	☐
Внутренняя защита от передачи идентификаторов (Local Antipass)	☐
Дополнительные выходы, реагирующие через группу ресурсов	
Дополнительный выход №4	☐
Дополнительный выход №5	☐

Для контроллера управления турникетом:

Текущее наименование	Турникет
Первоначальное наименование	Турникет
Прямое направление прохода	☒
Нормальное (т.е заблокированное) состояние контакта (вход ИЧ)	Нормально замкнут
Нормальное состояние "Закрыто" выхода ИЧ	Не запитан
Нормализация выхода ИЧ	После "Открытия"
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа идентификатора)	4 сек.
Регистрация прохода по предъявлению идентификатора	☐
Внутренняя защита от передачи идентификаторов (Local Antipass)	☐

Большинство параметров идентичны для всех типов контроллеров. Отличительные особенности будут описаны ниже после описания основных параметров. Ниже приведено описание параметров исполнительного устройства:

- 1. Прямое направление прохода.** Данный параметр определяет, в какую сторону будет

разблокирован ИУ при предъявлении карты к первому считывателю контроллера.

2. Нормальное (т.е. заблокированное) состояние контакта (вход ИУ). Параметр описывает состояние датчика двери/турникета. В зависимости от его конструкции он может быть при закрытом ИУ замкнут (как правило, герконы двери) или разомкнут.

3. Нормальное состояние «Закрыто» выхода ИУ. Параметр описывает должен ли контроллер подавать напряжение на ИУ в состоянии «Закрыто». Так, например, для электромагнитных замков в состоянии «Закрыто» необходимо подавать напряжение на ИУ, для электромеханических такой необходимости нет.

4. Нормализация ИУ. Параметр описывает, в какой момент времени контроллер должен начать свои действия по блокировке ИУ (сразу после открытия ИУ или после его закрытия). Факт открытия/закрытия ИУ контроллер определяет по датчику, установленному на вход ИУ.

5. Режим работы выхода управления ИУ описывает логику управления подключенным исполнительным устройством. Его значение определяется исходя из параметров работы подключенного устройства.

6. Предельное время разблокировки описывает время, по истечении которого контроллер управления доступом перейдет в состояние тревога по причине того, что исполнительное устройство не заблокировано.

7. Время удержания в разблокированном состоянии (время анализа карты) описывает время, по истечении которого контроллер управления доступом переведет исполнительное устройство в состояние «Закрыто». Снимет управляющий сигнал с линии управления исполнительным устройством.

8. Регистрация прохода по предъявлению идентификатора указывает на то, что контроллер будет считать проход совершившимся сразу после поднесения идентификатора доступа к его считывателю, игнорируя информацию о сигнале, получаемом с датчика ИУ.

9. Внутренняя защита от передачи идентификаторов задает режим работы контроллера по контролю за повторными входами/выходами. При отмеченной опции, контроллер будет блокировать попытки повторного входа/выхода.

10. Дополнительные выходы, реагирующие через группу ресурсов. Параметр указывает, должны ли активизироваться отмеченные дополнительные выходы, при условии, что исполнительное устройство входит в группу ресурсов.

Считыватель

В зависимости от типа используемого контроллера количество считывателей может быть от одного до двух. Так же считыватель может быть уже интегрирован в корпус контроллера.

Задание параметров функционирования считывателей фактически определяет порядок и условия работы контроллера при предъявлении карты доступа. Часть параметров считывателя определяют параметры разрешения прохода в направлении, контролируемым данным считывателем.

1. Время ожидания подтверждения при верификации - временной параметр, который устанавливает время, в течение которого контроллер будет ожидать поднесения коммиссионированного идентификатора или подтверждения от верифицирующего устройства. В качестве верифицирующего устройства может быть использовано ДУ контроллера или программное обеспечение.

2. Запрещение ДУ - параметр, который дает возможность запретить работу ДУ контроллера по разблокировке ИУ в направлении работы данного считывателя в выбранных режимах доступа. При выборе данного параметра произвести разблокировку ИМ в этом направлении в выбранных режимах доступа будет невозможно.

Текущее наименование	Считыватель №1
Первоначальное наименование	Считыватель №1
Модель	PERCo-IPxx
Время ожидания подтверждения при верификации	5 сек.
[-] <u>Запрещение ДУ</u>	
в РЕЖИМЕ РАБОТЫ "Контроль"	☐
в РЕЖИМЕ РАБОТЫ "Совещание"	☐
[-] <u>Подтверждение от ДУ</u>	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
[-] <u>Защита от передачи идентификаторов (Antipass)</u>	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Охрана"	Нет
[-] <u>Контроль времени</u>	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Охрана"	Нет
+ <u>Дополнительные входы, маскируемые при разблокировке ИУ</u>	
+ <u>Дополнительные выходы, активизируемые при разблокировке ИУ</u>	
+ <u>Дополнительные выходы, нормализируемые при разблокировке ИУ</u>	
+ <u>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов сотрудников</u>	
+ <u>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов гостей</u>	

3. Подтверждение от ДУ. При помощи этого параметра можно указать как в выбранных режимах доступа при поднесении идентификатора к данному считывателю будет формироваться запрос на подтверждение от ДУ.

Подтверждение от ДУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Да
Да	
Верифицировать идентификаторы Сотрудников	
при проходе	☐
при проходе с НАРУШЕНИЕМ ВРЕМЕНИ	☐
при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	☐
Верифицировать идентификаторы Посетителей	
при проходе	☐
при проходе с НАРУШЕНИЕМ ВРЕМЕНИ	☐
при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	☐
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет

Можно гибко настроить условия верификации идентификаторов сотрудников и гостей. Имеются следующие условия верификации:

- ✓ **при проходе** — верификация будет осуществляется при попытке прохода без каких-либо нарушений
- ✓ **при проходе с НАРУШЕНИЕМ ВРЕМЕНИ** — верификация будет осуществляется при попытке прохода с нарушением временных параметров доступа (параметр «Контроль времени» должен быть установлен на значение «Мягкий или жесткий»)
- ✓ **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ** — верификация будет осуществляется случае попытки повторного прохода без предварительного прохода в обратную сторону (параметр «Защита от передачи идентификаторов» должен быть установлен на значение «Мягкая или Жесткая»)

4. Защита от передачи идентификаторов - параметр, который позволяет определить реакцию контроллера в случае попытки повторного прохода без предварительного прохода в обратную сторону. Для каждого из указанных режимов работы контроллера можно выбрать один из вариантов работы:

Нет
Нет
Мягкая
Жесткая

- ✓ **Нет.** Контроллер не осуществляет проверку факта повторного прохода по идентификатору, предъявленному к выбранному считывателю.
- ✓ **Мягкая.** Контроллер разрешит повторный проход по идентификатору, предъявленному к выбранному считывателю и при этом в журнале регистрации записывается событие о проходе с нарушением зональности.
- ✓ **Жесткая.** Контроллер запретит попытку повторного прохода при предъявлении идентификатора к выбранному считывателю и при этом в журнал регистрации записывается событие о запрете прохода по причине нарушения зональности, а в журнале мониторинга — событие о предъявлении такого идентификатора.

5. Контроль времени – параметр, который позволяет задать реакцию контроллера

на предъявление идентификатора с учетом временных критериев доступа (временных зоны, недельных графиков, скользящих посуточных графиков, скользящих понедельных графиков). Контроль времени задается отдельно для указанных режимов доступа и может иметь следующие значения:



- ✓ **Нет.** Контроллер не осуществляет проверку временных параметров доступа предъявленного идентификатора для разрешения прохода .
- ✓ **Мягкий.** Контроллер разрешит проход по предъявленному идентификатору, но проведет сравнение текущего времени и даты с временными параметрами доступа предъявленного идентификатора и в случае их нарушения запишет в журнал регистрации событие о проходе с несоответствием временным критериям доступа.
- ✓ **Жесткий.** Контроллер проведет сравнение текущего времени и даты с временными параметрами доступа предъявленного идентификатора. В случае их совпадения, то есть владелец идентификатора не нарушает режим доступа, контроллер разрешит проход по идентификатору предъявленному к выбранному считывателю. В случае их нарушения - запретит проход и запишет в журналы регистрации событие о запрете прохода в связи с несоответствием временным критериям доступа, а в журнале мониторинга — событие о предъявлении такого идентификатора.

Кроме перечисленных выше параметров можно указать дополнительные параметры, влияющие на действия контроллера при поднесении идентификатора:

Дополнительные входы, маскируемые при разблокировке ИУ	
Критерий маскирования	На указанное время
☐ На указанное время	
Время	3 сек.
Дополнительный вход №1	☐
Дополнительный вход №2	☐
Дополнительные выходы, активизируемые при разблокировке ИУ	
Критерий активизации	На время срабатывания
Дополнительный выход №1	☐
Дополнительный выход №2	☐
Дополнительные выходы, нормализируемые при разблокировке ИУ	
Критерий нормализации	На время срабатывания и после срабатывания
☐ На время срабатывания и после срабатывания	
Время	250 мс.
Дополнительный выход №1	☐
Дополнительный выход №2	☐
Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов сотрудников	
Критерий активизации	На указанное время
☐ На указанное время	
Время	3 сек.
Дополнительный выход №1	☐
Дополнительный выход №2	☐
Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов гостей	
Критерий активизации	На указанное время
☐ На указанное время	
Время	3 сек.
Дополнительный выход №1	☐
Дополнительный выход №2	☐

6. Дополнительные входы, маскируемые при разблокировке ИУ. Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы, т.е. не воспринимать управляющий сигнал от внешнего оборудования, при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных входов, которые должны быть маскированы. Кроме этого, укажите временной критерий маскирования, который может быть одним из трех видов:

Критерий маскирования	На указанное время
☐ На указанное время	На указанное время
Время	На время срабатывания
Дополнительный вход №2	На время срабатывания и после срабатывания
	☒

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

7. Дополнительные выходы, активизируемые при разблокировке ИУ. Этот параметр позволяет указать, какие именно дополнительные выходы контроллера

Критерий активизации	На указанное время
На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания
	☐

- ✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут активизированы на протяжении всего времени, когда ИУ будет разблокировано.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы на время, в течение которого ИУ будет разблокировано плюс указанное вами время.

8. Дополнительные выходы, нормализируемые при разблокировке ИУ. Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализованы при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть нормализованы. Кроме этого, укажите временной критерий нормализации, который может быть одним из трех видов:

Критерий нормализации	На указанное время
На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания
	☐

- ✓ **На указанное время** – выбранные дополнительные выходы будут нормализованы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут нормализованы на протяжении всего времени, когда ИУ будет разблокировано.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут нормализованы на время, в течение которого ИУ будет разблокировано плюс указанное вами время.

9. Дополнительные выходы, активизируемые при предъявлении валидных пропусков сотрудников. Этот параметр позволяет указать те дополнительные выходы, которые будут активизированы на указанное время в случае предъявления не заблокированного и с не истекшим сроком действия идентификатора сотрудника. Этот параметр может быть использован в случае, если к этим дополнительным выходам подключена дополнительная индикация, информирующая работников охраны о статусе предъявленной карты. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Кроме этого,

Критерий активизации	На указанное время
На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время начиная с момента предъявления идентификатора, независимо от того будет или нет разрешён проход.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут активизированы на указанное время начиная с момента разблокирования ИУ и до момента его блокирования, либо, если проход не был совершён, по истечению времени анализа идентификатора.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы на указанное время начиная с момента разблокирования ИУ и до момента его блокирования плюс указанное вами время, либо, если проход не был совершён, по истечению времени анализа идентификатора.

10. Дополнительные выходы, активизируемые при предъявлении валидных пропусков гостей. Этот параметр позволяет указать те дополнительные выходы, которые будут активизированы на указанное время в случае предъявления не заблокированного и с не истёкшим сроком действия идентификатора гостя. Этот параметр может быть использован в случае, если к этим дополнительным выходам подключена дополнительная индикация, информирующая работников охраны о статусе предъявленной карты. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Кроме этого, укажите временной критерий активизации, который аналогичен п.4.

Генератор тревоги

В зависимости от структуры системы безопасности, ее задач, местоположения контроллера управления доступом, текущего режима доступа те или иные действия пользователей системы могут приводить к генерации тревоги.

Для выявления причин генерации тревоги и управления выделенным выходом тревоги (один из дополнительных выходов) определите следующие параметры:

Текущее наименование	Генератор тревоги
Первоначальное наименование	Генератор тревоги
Генерация тревоги при предъявлении идентификатора	
если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН	Нет
если ИДЕНТИФИКАТОР ЗАПРЕЩЕН	Нет
если ИДЕНТИФИКАТОР ИЗ СТОП-ЛИСТА	Нет
если ИСТЕК СРОК ДЕЙСТВИЯ	Нет
если НАРУШЕНО ВРЕМЯ	Нет
если НАРУШЕНА ЗОНАЛЬНОСТЬ	Нет
если НАРУШЕН РЕЖИМ РАБОТЫ	Нет
если НАРУШЕНО КОМИССИОНИРОВАНИЕ	Нет
Генерация тревоги при несанкционированной разблокировке ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Закрето"	Нет
Генерация тревоги по недопустимо долгому открытию ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
Генерация тревоги по датчику вскрытия корпуса контроллера	Нет
Дополнительные входы, активизирующие генерацию тревоги	
Тип тревоги	Тихая
Дополнительный вход №1	☐
Дополнительный вход №2	☐

- 1. Генерация тревоги при предъявлении идентификатора.** Этот параметр позволяет указать причины генерации тревожных событие и перехода контроллера в состояние «Тревога» при предъявлении идентификатора с указанными параметрами доступа.
- 2. Генерация тревоги при несанкционированной разблокировке ИУ.** Этот параметр позволяет указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» в случае разблокировки ИУ при помощи ключа (то есть разблокировке ИУ без команды от контроллера) в выбранных режимах доступа.
- 3. Генерация тревоги по недопустимо долгому открытию ИУ.** Этот параметр позволяет указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» в случае, если после открытия ИУ оно не было приведено в исходное состояние в течение времени большего, чем указано в параметрах этого ИУ. Другими словами, должен ли контроллер перейти в состояние «Тревога», если после прохода через дверь она осталось открытой.
- 4. Дополнительные входы, активизирующие генерацию тревоги** – параметр, позволяющий выбрать те дополнительные входы контроллера, активизация которых будет приводить к переходу контроллера в состояние «Тревога». Это может быть использовано, например, при подключении к этому дополнительному входу кнопки тревожной сигнализации.
- 5. Тип тревоги** – параметр, который позволяет управлять активизацией

Тихая
Тихая
Громкая

- ✓ **Тихая** — в этом случае активизация дополнительного выхода не произойдет, а контроллер запишет в журнал регистрации и в журнал мониторинга событие о тревоге.
- ✓ **Громкая** - в этом случае произойдет активизация дополнительного выхода и контроллер запишет в журнал регистрации и в журнал мониторинга событие о тревоге.

Шлейф сигнализации

Контроллеры имеют возможность подключения стандартных шлейфов охранной сигнализации. Использование охранного шлейфа позволяет системе безопасности контролировать не только вход в помещение, но и внутренний объем помещения, открывание окон и так далее за счет подключения дополнительных охранных датчиков.

Для задания параметров работы шлейфа сигнализации необходимо выбрать в дереве объектов интересующий шлейф сигнализации. В инспекторе объектов отобразятся его параметры функционирования:

Текущее наименование	Шлейф сигнализации №1
Первоначальное наименование	Шлейф сигнализации №1
Тип	Охранный
Автоматическое перевзятие	☒
Тихая тревога	☒
Повторное включение sireны	☐
Длительность нарушения	70 мс.
Задержка взятия на охрану	0 мс.
Задержка управления выходом "С"	0 мс.
Задержка управления выходом "Л"	0 мс.
Задержка восстановления нарушенного шлейфа в снятом состоянии	0 мс.
Дополнительные выходы, реагирующие через группу ресурсов	
Дополнительный выход №4	☐
Дополнительный выход №5	☐

1. **Тип.** Параметр дает возможность указать тип шлейфа охранной сигнализации:

Охранный
Охранный
Охранный с контролем блокировки

- ✓ **Охранный**
- ✓ **Охранный с блокировкой**

2. **Автоматическое перевзятие.** При включенной опции, при постановке на охрану шлейфа охранной сигнализации, в случае невозможности взятия шлейфа на охрану, контроллер автоматически будет пытаться взять шлейф на охрану повторно.
3. **Тихая тревога.** При включении этой опции, если в состав шлейфа включены дополнительные релейные выходы, работающие по программам «Сирена» или «Лампа», то эти программы не будут активизированы.
4. **Повторное включение sireны.** Параметр указывает, должен ли контроллер повторно включить сирену, при условии повторного нарушения шлейфа.
5. **Длительность нарушения.** Параметр указывает временной параметр, в течении которого нарушение шлейфа не будет считаться тревожным.
6. **Задержка взятия на охрану** – интервал времени, по истечению которого контроллер начнет анализировать состояние шлейфа охранной сигнализации для постановки на охрану. Как правило, это время устанавливают отличным от нуля в ситуации, когда место постановки на охрану находится так же под контролем этого шлейфа. И после постановки на охрану необходимо время для того, чтобы покинуть охраняемое помещение.
7. **Задержка управления выходом «С».** Параметр указывает время, в течении которого контроллер не будет активизировать выход с программой управления «Серена» после нарушения шлейфа.
8. **Задержка управления выходом «Л».** Параметр указывает время, в течении которого контроллер не будет активизировать выход с программой управления «Лампа» после нарушения шлейфа.
9. **Задержка восстановления нарушенного шлейфа в снятом состоянии.** Параметр указывает время, по истечении которого контроллер будет пытаться восстановить нарушенный шлейф. Если значение параметра установлено 0 или Бесконечность, а шлейф находится в снятом состоянии - сопротивление шлейфа не отслеживается.
10. **Дополнительные выходы.** Вы можете указать дополнительные выходы этого контроллера, которые будут использованы в соответствии с указанной у них программой.



ПРИМЕЧАНИЕ

Могут быть задействованы только выходы, у которых в качестве типа указан тип «ОПС».

Группы ресурсов

Группа ресурсов – логическая структура, которая позволяет создать комбинации ресурсов контроллера, которые будут ставиться на охрану в зависимости от прав пользователя системы.

Для добавления группы ресурсов необходимо выделить группу ресурсов у интересующего контроллера и нажать на кнопку . В дереве объектов выделенного контроллера появятся дополнительная группа ресурсов. Выбрав ее, можно задать ее параметры:

Текущее наименование	Группа ресурсов №1
Первоначальное наименование	Группа ресурсов №1
Включить ИУ в группу	☒
[-] <u>Дополнительные входы, включённые в группу</u>	
Дополнительный вход №1	☐
Дополнительный вход №2	☐
[-] <u>Шлейфы сигнализации, включённые в группу</u>	
Шлейф сигнализации №1	☐
Шлейф сигнализации №2	☐

1. **Включить ИУ в группу** – параметр, указывающий на то, входит ли исполнительное устройство в эту группу. То есть, если исполнительное устройство добавлено в группу, при постановке на охрану контроллер будет контролировать его состояние. В противном случае открытие двери не будет приводить к возникновению тревоги после постановки группы ресурсов на охрану. Это может быть использовано в том случае, когда ресурсы контроллера используются не только для контроля помещения, доступ в которое он контролирует.
2. **Дополнительные входы, входящие в группу.** Параметр позволяет указать дополнительные входы контроллера, которые будут так же контролироваться контроллером при постановке группы ресурсов на охрану.
3. **Шлейфы сигнализации, входящие в группу.** Параметр позволяет указать, шлейфы сигнализации, которые будут контролироваться контроллером при постановке группы ресурсов на охрану.

Защита от передачи идентификаторов

Контроллеры системы PERCo-S-20 поддерживают режим защиты от передачи идентификаторов, т.е. запрет повторного входа без предварительного выхода.

Для реализации этого режима, факт прохода с данной картой передается другим контроллерам сети. Так как при конфигурации контроллеров (см. «**Конфигурация контроллеров**») каждому контроллеру передаются списки контроллеров других подсетей, то алгоритм передачи следующий:

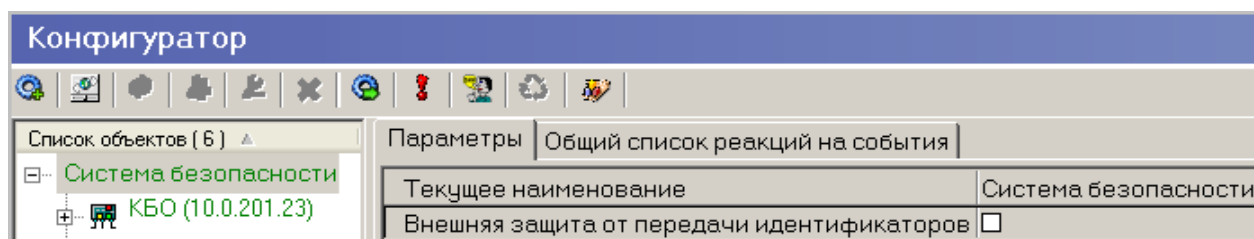
1. Происходит широковещательная рассылка контроллерам своей подсети.
2. Выбирается первый контроллер другой подсети, и ему передаются данные. В случае невозможности передачи ему, выбирается следующий контроллер этой подсети и т.д. Затем эта же процедура проводится и с другими подсетями.
3. Контроллер в другой подсети, получив данные, распространяет их

широковещательно по всем контроллерам своей подсети.

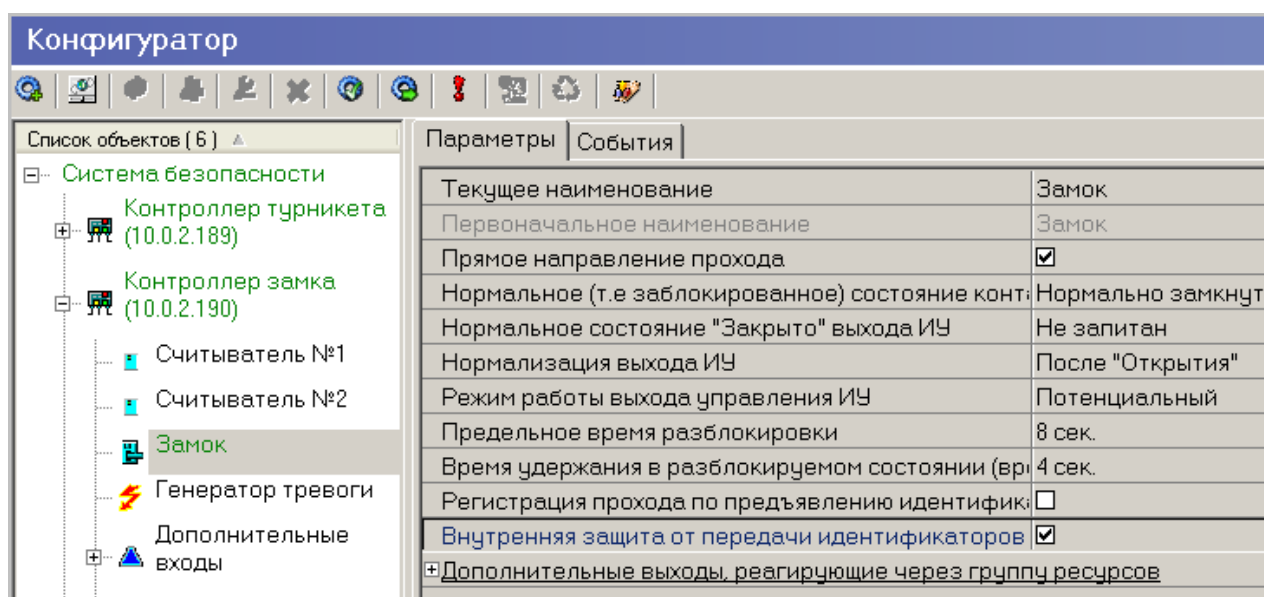
4. В результате этих действий контроллеров каждый контроллер знает, на каком из уровней доступа (безопасности) находится владелец предъявленной карты.

По умолчанию все идентификаторы, зарегистрированные Базовой версией ПО контролируются системой на предмет повторного входа/выхода. Для включения защиты от передачи идентификаторов в разделе Конфигуратор:

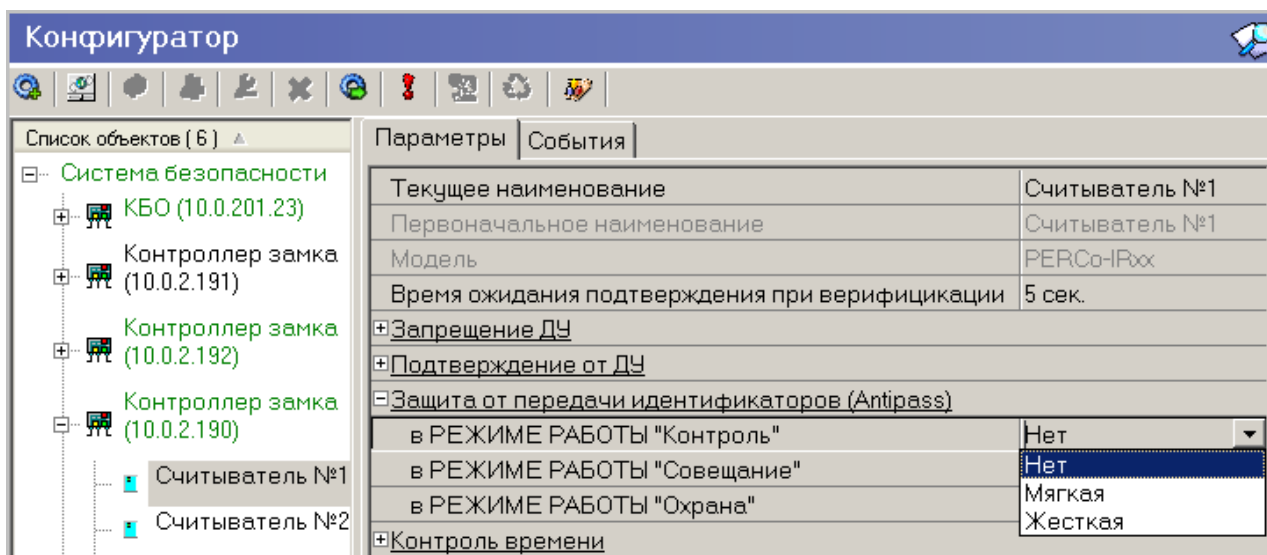
✓ **для системы безопасности в целом:** отметьте флажок Внешняя защита от передачи идентификаторов (Global Antipass) в панели параметров



✓ **для отдельного исполнительного устройства:** отметьте флажок Внутренняя защита от передачи идентификаторов (Local Antipass) в панели параметров

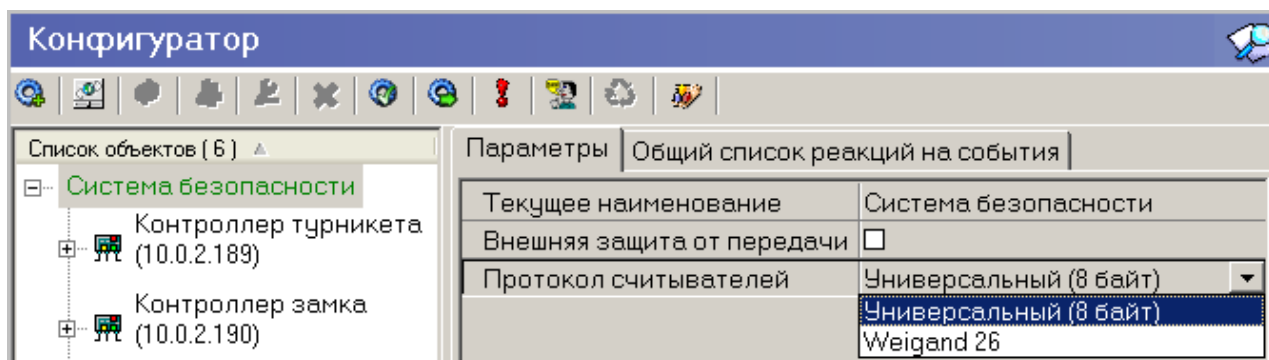


✓ **для отдельного считывателя:** установите у считывателя в параметре Защита от передачи идентификаторов (Antipass) значение Жесткая: для требуемых режимов работы



Протокол работы со считывателями

Контроллеры системы PERCo-S-20 поддерживают два протокола работы со считывателями. Для изменения протокола в разделе Конфигуратор измените параметр «Протокол считывателей».



Имеется два значения этого параметра:

- ✓ **Универсальный (8 байт)** — протокол считывателя, по которому контроллер воспринимает 64 бита кода идентификатора доступа.
- ✓ **Widgand 26** – протокол считывателя, по которому контроллер воспринимает 26 бит кода идентификатора доступа.
- ✓ **Сокращенный (4 байта)** - протокол считывателя, по которому контроллер воспринимает 32 бита кода идентификатора доступа.

ОПИСАНИЕ ПАРАМЕТРОВ ФУНКЦИОНИРОВАНИЯ КОНТРОЛЛЕРОВ ППКОП (КБО)

Подробная информация о параметрах функционирования контроллера ППКОП (КБО) системы безопасности PERCo-S-20 приведена в техническом описании системы безопасности.

Контроллер ППКОП (КБО) — предназначен для контроля состояния шлейфов сигнализации (ШС), пожарных или охранных, выдачи тревожных сообщений на пост

центрального наблюдения (ПЦН), световое оповещение (СО) и звуковое оповещение (ЗО), управления дополнительным оборудованием, сохранению событий, произошедших в системе, в энергонезависимой памяти и передаче их ПО. Дополнительно панель КБО обеспечивает управление одним электромагнитным или электромеханическим замком и имеет энергонезависимую память на 200 карт доступа и 8000 событий.

Ниже будут приведены общие рекомендации, проиллюстрированные примерами задания параметров ресурсов контроллеров, которые отличаются от аналогичных у контроллеров доступа.

Контроллер

Каждый контроллер ППКОП (КБО) входящий в систему безопасности PERCo-S-20 имеет следующие параметры:

Использовать встроенный звуковой извещатель	☐
Режим активизации кнопки "КЛЮЧ"	Одно длинное нажатие ▾
	Одно нажатие
	Одно длинное нажатие
	Два длинных нажатия
	Три коротких нажатия

1. Использовать встроенный звуковой извещатель — параметр, управляющий звуковой индикацией на блоке управления индикацией (БУИ). При сбросе данного параметра встроенный звуковой индикатор у БУИ ППКОП включаться не будет, а у БУИ КБО будет включаться только по части СКУД. На контроллере будет действовать только световая индикация.

2. Режим активизации кнопки "КЛЮЧ" — параметр, задающий способ разблокирования управления на блоке управления индикацией (БУИ). Имеются следующие значения:

- ✓ Одно нажатие
- ✓ Одно длинное нажатие
- ✓ Два длинных нажатия
- ✓ Три коротких нажатия

Дополнительный выход

Каждый контроллер ППКОП (КБО) входящий в систему безопасности PERCo-S-20, имеет шесть дополнительных выходов (для КБО первый выход зарезервирован).

Дополнительные выходы могут быть использованы для управления любым дополнительным оборудованием в рамках системы безопасности. Технические параметры дополнительных выходов для каждого типа контроллера приведены в техническом описании системы безопасности.

В зависимости от алгоритма работы внешних устройств, подключенных к дополнительному выходу существуют следующие варианты описания параметров работы выхода:

1. При условии, что к данному дополнительному выходу не подключено никакое дополнительное оборудование, менять параметры работы выхода не нужно.

2. Тип дополнительного выхода – **Обычный** (только для КБО)

Текущее наименование	Дополнительный выход №2
Адрес	2
Первоначальное наименование	Дополнительный выход №2
▢Тип	Обычный ▾
▢Обычный	
Нормальное состояние	Не запитан

Этот параметр указывает, что к данному дополнительному выходу подключено дополнительное оборудование, логика управления которым описывается через описание других устройств системы (за исключением генератора тревоги). Задайте нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/незапитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий.

3. Тип дополнительного выхода – **генератор тревоги**. (только для КБО)

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

В этом случае решение об активизации дополнительного выхода принимается исключительно панелью в соответствии с параметрами, указанными в ее генераторе тревоги. Этот дополнительный выход будет использоваться для индикации перехода панели в состояние «Тревога». Так же задайте нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/не запитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий. Кроме этого, укажите время активизации дополнительного выхода, время, в течение которого при наличии активизирующего управляющего воздействия выход меняет своё состояние из нормализованного на противоположное. Как правило, в этом случае к такому дополнительному выходу подключают тревожный оповещатель (сирена, проблесковая лампа).

4. Тип дополнительного выхода – **ОПС**.

для ППКОП:

Текущее наименование	Дополнительный выход №2
Адрес	2
Первоначальное наименование	Дополнительный выход №2
Тип	ОПС
ОПС	
Нормальное состояние	Не запитан
Задержка перед запуском	0 мс.
Время активизации	1 сек.
Программа управления	Включить при пожаре
Зоны, активизирующие выход	
Охранная зона	☐
Пожарная зона	☐

для КБО:

Текущее наименование	Дополнительный выход №1
Адрес	1
Первоначальное наименование	Дополнительный выход №1
Тип	ОПС
ОПС	
Нормальное состояние	Не запитан
Задержка перед запуском	0 мс.
Время активизации	1 сек.
Программа управления	Включить при пожаре
Зоны, активизирующие выход	
Зона №1	☐
Зона №2	☐
Зона №3	☐

В этом случае дополнительный выход предназначен для управления световым оповещением (СО), звуковым оповещением (ЗО), а так же для передачи тревожных извещений на пульт центрального наблюдения (ПЦН) при изменении режимов и состояний пожарных зон (ПЗ) и охранных зон (ОЗ).

Программа управления задает логику работы панели по управлению этим дополнительным выходом. Инициатором активизации выхода являются изменения режимов и состояний зон, отмеченных под параметром «Зоны, активизирующие выход». После возникновения события, инициирующего активизацию выхода (в соответствии с заданной программой), начинается отсчёт задержки, указанной в параметре «Задержка перед запуском» (если задержка ненулевая), по окончании которой выход активизируется. В зависимости от программы управления выход может быть запитан (не запитан) постоянно (пока ресурс панели находится в текущем режиме), либо изменять своё физическое состояние (мигать) из нормализованного на противоположное. Нормализация выхода происходит либо по истечению времени, указанному в параметре «Время активизации» (если оно не бесконечное), либо по сбросу панели, либо после выключения ее питания. После включения питания все выходы нормализуются.

Вид программы выбирается из выпадающего списка. Возможны следующие варианты программ управления дополнительным выходом:

- ✓ **Включить при пожаре.** В случае перехода одной из зон в режим «ПОЖАР» произойдет замыкание контакта дополнительного выхода.

- ✓ **Мигать при пожаре.** В случае перехода одной из зон в режим «ПОЖАР» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Включить при внимании и пожаре.** В случае перехода одной из зон в режим «ВНИМАНИЕ» или «ПОЖАР» произойдет замыкание контакта дополнительного выхода.
- ✓ **Мигать при внимании и пожаре.** В случае перехода одной из зон в режим «ВНИМАНИЕ» или «ПОЖАР» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Включить при тревоге.** В случае перехода одной из зон в режим «ТРЕВОГА» произойдет замыкание контакта дополнительного выхода.
- ✓ **Мигать при тревоге.** В случае перехода одной из зон в режим «ТРЕВОГА» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Лампа 1** – программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы все зоны изменили свой режим.
- ✓ **Лампа 2** – программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы хотя бы одна из зон изменила свой режим.
- ✓ **ПЦН 1** – программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы все зоны изменили свой режим.
- ✓ **ПЦН 2** – программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы все зоны изменили свой режим.
- ✓ **Сирена** – программа управления, указывающая на то, что к дополнительному выходу подключен звуковой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы хотя бы одна из зон изменила свой режим.
- ✓ **Включить перед взятием** – Перед переходом одной из зон в режим «ВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.
- ✓ **Включить при взятии** — При переходе одной из зон в режим «ВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.
- ✓ **Включить при снятии** – Перед переходом одной из зон в режим «СНЯТА» произойдет замыкание контакта дополнительного выхода.
- ✓ **Включить при автоперевзятии** – При переходе одной из охранных зон в режим «АВТОПЕРЕВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.

- ✓ **Включить при неисправности.** При переходе одной из зон в режим «НЕИСПРАВНОСТЬ» произойдет замыкание контакта дополнительного выхода.
- ✓ **Мигать при неисправности.** При переходе одной из зон в режим «НЕИСПРАВНОСТЬ» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.

Шлейф сигнализации

Контроллеры имеют возможность подключения стандартных шлейфов охранной и пожарной сигнализации. Использование охранных шлейфов позволяет системе безопасности контролировать не только вход в помещение, но и внутренний объем помещения, открывание окон и так далее за счет подключения дополнительных охранных датчиков. Использование пожарных шлейфов позволяет контролировать пожарную безопасность помещения за счет подключения пожарных извещателей. ППКОП имеет 8 шлейфов сигнализации, а КБО - только 3 шлейфа.

В зависимости от алгоритма работы внешних датчиков и извещателей, подключенных к шлейфу сигнализации существуют следующие варианты описания параметров работы шлейфа:

1. Тип шлейфа сигнализации — Охранный

Текущее наименование	Шлейф сигнализации №1
Адрес	1
Первоначальное наименование	Шлейф сигнализации №1
Тип	Охранный
Охранный	
Контроль вскрытия корпуса извещателей	☐
Длительность нарушения	70 мс.
Задержка взятия на охрану	0 мс.
Задержка восстановления нарушенного шлейфа в снятом состоянии	0 мс.

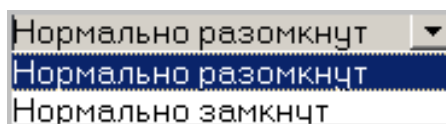
- ✓ **Контроль вскрытия корпуса извещателей** — параметр, указывающий шлейфу контролировать вскрытие корпуса извещателей.
- ✓ **Длительность нарушения** - параметр, определяющий для шлейфа время интегрирования
- ✓ **Задержка взятия на охрану** — параметр, определяющий для шлейфа время, через которое панель предпринимает попытку взять шлейф на охрану после поступления соответствующей команды.
- ✓ **Задержка восстановления нарушенного шлейфа в снятом состоянии** — если данный параметр установлена в 0, то шлейф в состоянии «СНЯТ» не контролируется. В противном случае продолжается отслеживание шлейфа в режиме «Снят». Если при этом шлейф перейдет в состояние «НАРУШЕНИЕ», то в журнал регистраций записывается событие «Неисправность снятого ОПС», состояние выходов и встроенная звуковая индикация панели не изменяются. Если после этого нормальное состояние шлейфа восстановится и продержится время, указанное в этом параметре, то шлейф выйдет из состояния «НАРУШЕНИЕ» и при

этом в журнал регистраций будет записано сообщение «Нормализация снятого ОШС». Состояние выходов и встроенная звуковая индикация панели не изменяются.

2. Тип шлейфа сигнализации — **Пожарный**

Текущее наименование	Шлейф сигнализации №2
Адрес	2
Первоначальное наименование	Шлейф сигнализации №2
Тип	Пожарный
Пожарный	
Нормальное состояние контакта извещателей	Нормально разомкнут ▼
Нормально разомкнут	
Поддержка перезапроса	☐
Задержка при включении	0 мс.
Задержка сброса	0 мс.

✓ **Нормальное состояние контактов извещателей** - параметр, определяющий изначальное состояние контакта извещателей, подключенных к шлейфу. Возможны два значения — нормально разомкнут или нормально замкнут.



✓ **Поддержка перезапроса** - параметр, определяющий, надо или нет после срабатывания извещателей снимать питание с шлейфа и перепроверять его состояние.

✓ **Задержка при включении** — параметр, определяющий время задержки до начала измерений сопротивления шлейфа после подачи на него питания при перезапросе и взятии.

✓ **Задержка сброса** — параметр, определяющий время нахождения шлейфа в состоянии «СБРОС» (без питания).

3. Тип шлейфа сигнализации — **КТС (только для ППКОН)**

Текущее наименование	Шлейф сигнализации №3
Адрес	3
Первоначальное наименование	Шлейф сигнализации №3
Тип	КТС ▼
КТС	
Длительность нарушения	70 мс.

✓ **Длительность нарушения** - параметр, определяющий для шлейфа время интегрирования

Зоны сигнализации

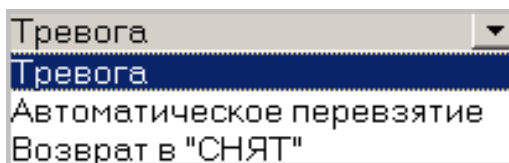
Зона сигнализации — это часть территории объекта, на которой физически расположены один или несколько шлейфов сигнализации. Пересечение границы охранной зоны (ОЗ) приводит к нарушению охранного шлейфа сигнализации (ОШС), входящего в данную зону, а возникновение пожарного фактора в пожарной зоне (ПЗ) (задымление, превышение определённого порога температуры, открытое пламя и т.д.) приводит к изменению состояния входящего в данную пожарную зону (ПЗ) пожарного шлейфа сигнализации (ПШС). ППКОП имеет 8 зон сигнализации, а КБО — только 2 зоны (пожарную и охранную).

В зависимости от алгоритма работы шлейфов сигнализации существуют следующие варианты описания параметров работы зоны:

1. Тип зоны сигнализации — **Охранная**

Текущее наименование	Охранная зона
Адрес	1
Первоначальное наименование	Охранная зона
▢Тип	Охранная
▢Охранная	
Повторное включение sireны	☐
Режим работы при невзятии	Тревога
▢Не активизировать при тревоге по Охранным шлейфам сигнализации	
Выходы, работающие по программе "Сирена" или "Лампа"	☐
▢Шлейфы, включенные в зону	
Шлейф сигнализации №1	☐

- ✓ **Повторное включение sireны** - параметр, позволяющий реализовать тактику активизации дополнительного выхода, управляемого по программе "Сирена" при каждом нарушении охранной зоны, даже если она уже находится в режиме "Тревога".
- ✓ **Режим работы при невзятии** — параметр указывает действие, которое будет происходить при невозможности взятия данной зоны на охрану. Имеются следующие значения:



- **Тревога** — зона будет переведена в режим «ТРЕВОГА».
 - **Автоматическое перевзятие** — зона будет переведена в режим «Взятие», а затем, будет производиться повторная попытка взятия до тех пор, пока взятие не произойдет.
 - **Возврат в режим снят** — зона перейдет в режим «СНЯТА».
- ✓ **Не активизировать при тревоге по охранным шлейфам сигнализации**

дополнительные выходы, работающие по программе «Сирена» или «Лампа» - параметр указывает, должна ли панель в случае тревоги в данной зоне запрещать активизацию дополнительных выходов, работающие по программе управления «Сирена» или «Лампа».

✓ **Шлейфы, включенные в зону** - список охранных шлейфов, контролируемых в данной зоне.

2. Тип зоны сигнализации - Пожарная

Текущее наименование	Пожарная зона
Адрес	2
Первоначальное наименование	Пожарная зона
≡Тип	Пожарная
☐ Пожарная	
Количество сработавших извещателей для перехода в режим "ПОЖАР"	2
Повторное включение сирены	☐
Переводить ИУ в режим "Открыто"	Никогда
☐ Шлейфы, включенные в зону	
Шлейф сигнализации №2	☐

✓ **Количество сработавших извещателей для перехода в режим "ПОЖАР"** - параметр, задающий минимальное количество извещателей, срабатывание которых переводит данную пожарную зону в режим «ПОЖАР».

✓ **Переводить ИУ в режим «Открыто» (только для КБО)** - параметр, задающий условия перевода ИУ в режим «ОТКРЫТО». Можно установить следующие значения:

- **Никогда** — изменения режимов зон не влияют на ИУ.
- При переходе ПЗ в режим "ПОЖАР", но ОЗ не в режиме "Охрана"
- При переходе ПЗ в режим "ПОЖАР", ОЗ в любом режиме
- При переходе ПЗ в режим "ПОЖАР" или "ВНИМАНИЕ", но ОЗ не в режиме "Охрана"
- При переходе ПЗ в режим "ПОЖАР" или "ВНИМАНИЕ", ОЗ в любом режиме
- При переходе ПЗ в режим "ПОЖАР" (ОЗ в любом режиме) или "ВНИМАНИЕ" (ОЗ не в режиме "Охрана")

✓ **Шлейфы, включенные в зону** - список пожарных шлейфов, контролируемых в данной зоне.

3. Тип зоны сигнализации — КТС

Текущее наименование	Зона №3
Адрес	3
Первоначальное наименование	Зона №3
☐ Тип	КТС
☐ КТС	
☐ Шлейфы, активизирующие зону	
Шлейф сигнализации №3	☒

✓ Шлейфы, активизирующие зону - **список шлейфов КТС, контролируемых в данной зоне.**

ИНТЕГРАЦИЯ ППКОП С ПЦН «АИР»

Включение интеграция ППКОП с ПЦН «АИР» дает возможность передавать тревожные сообщения на внешний пульт центрального наблюдения (ПЦН), предназначенный для охраны объектов через широкополосные каналы передачи информации (Internet), в том числе и по каналам GSM.

Для включения интеграции следует задействовать параметр «Включить интеграцию с ПЦН «АИР» на контроллере ППКОП.

Включить интеграцию с ПЦН "АИР"	☒
---------------------------------	-------------------------------------

После включения данного параметра в дереве объектов конфигурации (см. раздел «КОНФИГУРАТОР») под контроллером ППКОП появится «Объект интеграции с ПЦН "АИР"» с шестью УОО (устройство объективное охранное).

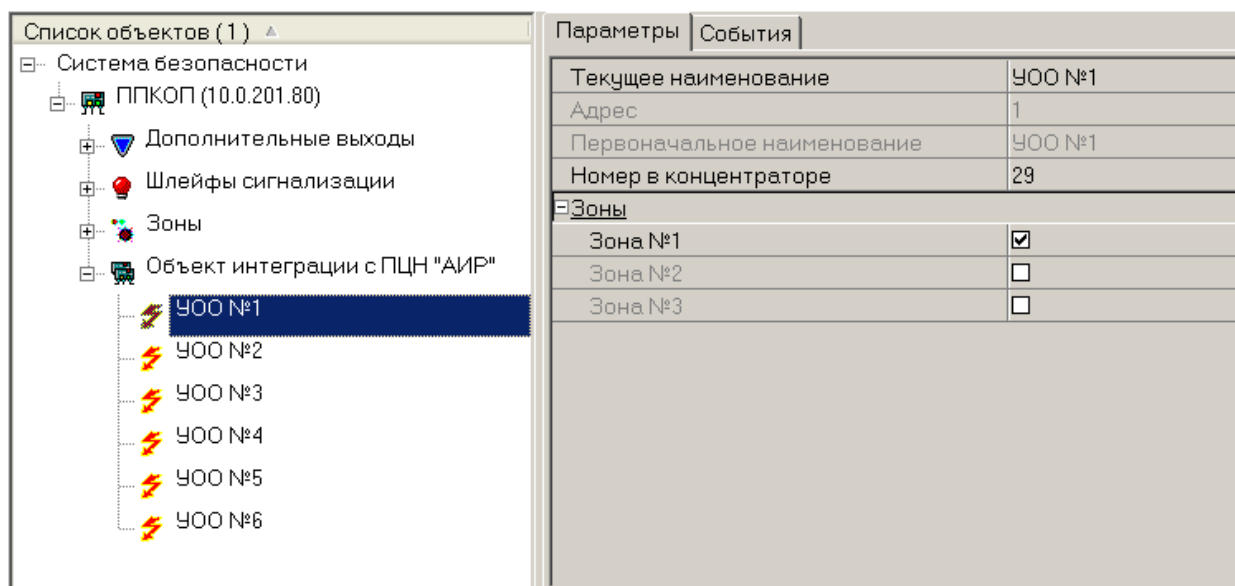
Система безопасности

- ППКОП (10.0.201.80)
 - Дополнительные выходы
 - Шлейфы сигнализации
 - Зоны
 - Объект интеграции с ПЦН "АИР"**
 - УОО №1
 - УОО №2
 - УОО №3
 - УОО №4
 - УОО №5
 - УОО №6

Текущее наименование	Объект интеграции с ПЦН "АИР"
Первоначальное наименование	Объект интеграции с ПЦН "АИР"
☐ Сетевые параметры концентратора	
IP-адрес	10.0.201.254
Маска подсети	255.0.0.0

Для объекта интеграции существуют следующие параметры:

- **Сетевые параметры концентратора** — сетевые параметры концентратора, связанного с ПЦН «АИР»
- **IP-адрес**
- **Маска подсети**



Для каждого УОО существуют следующие параметры:

- **Номер в концентраторе** — номер УОО в адресном пространстве концентратора
- **Зоны** — список охраняемые зоны.

ПОМЕЩЕНИЯ

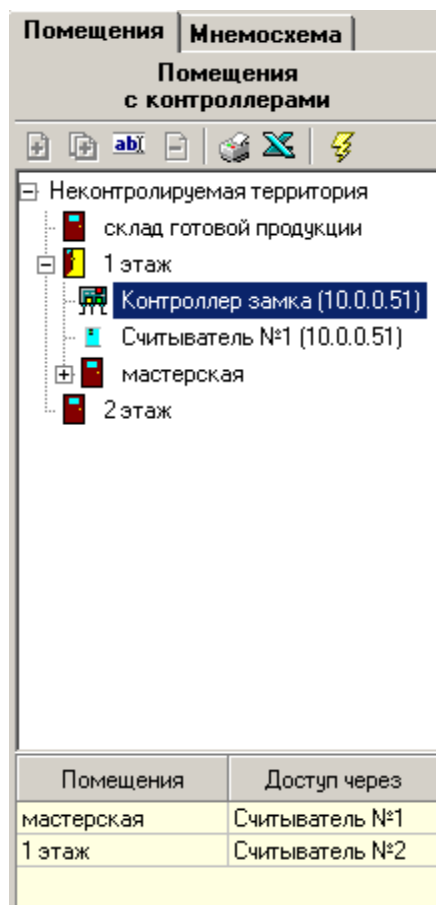
Нормальное функционирование системы безопасности невозможно без привязки объектов системы к помещениям предприятия, его территории. Привязка объектов системы осуществляется в разделе Помещения и мнемосхема. Правила работы с этим разделом описаны в Руководстве оператора в разделе Помещения и мнемосхема.

Под помещениями в системе безопасности подразумевается иерархическая структура помещений предприятий (организации). Эта информация необходима для определения уровней доступа, указания, какие контроллеры контролируют доступ в какие помещения, привязки шлейфов охранно-пожарной сигнализации, видеокамер, дополнительных устройств к помещениям, в которых они установлены.

ПОМЕЩЕНИЯ

На вкладке список помещений строится в виде дерева. Максимальное количество вложенных равно 128. Такое представление структуры помещений наиболее полно отражает реальное расположение помещений на предприятии (организации).

Кроме этого, структуру представления помещений можно рассматривать и как схему уровней безопасности. То есть каждый следующий уровень есть не что иное, как следующий уровень доступа на предприятии. Так, например проходная предприятия находится на первом уровне доступа, переход из проходной в другие помещения - это уже переход на следующий уровень доступа. Соответственно в дереве помещений он отображается, как второй уровень вложенности.



Распределение помещений по уровням в дереве помещений и размещение в них контроллеров управления доступом также определяет правила доступа из помещения в помещение при условии включенного «антипасбэка» (защиты от повторного прохода).

Так, например, на рисунке представлено дерево помещений предприятия, на котором вход на первый этаж из неконтролируемой территории вне предприятия контролируется контроллером замка. В случае задания включения защиты от передачи карт вход на первый этаж без предварительного выхода будет невозможен. Так же справедливо и обратное, нельзя выйти с территории предприятия, не совершив предварительного входа.

Значком  в дереве помещений отмечены помещения, на которые не назначены права для оператора данного рабочего места.

МНЕМОСХЕМА

Мнемосхема - это графическое отображение созданного в подразделе Помещение дерева помещений вместе с размещенными в помещениях устройствами системы безопасности. Создавая мнемосхемы предприятия, вы даете возможность операторам службы безопасности видеть визуальное отображение состояния устройств системы. Это упрощает понимание ситуации на объекте.

Существует два варианта создания мнемосхем:

- ✓ Создание мнемосхемы без использования графических изображений территории предприятия. В этом случае графические изображения располагаются

на автоматически созданном белом квадрате с размером 1600x1600 пикселей. Использование такого подхода оправдано только в том случае, если территория предприятия небольшая или система безопасности состоит только из турникетов установленных на проходной.

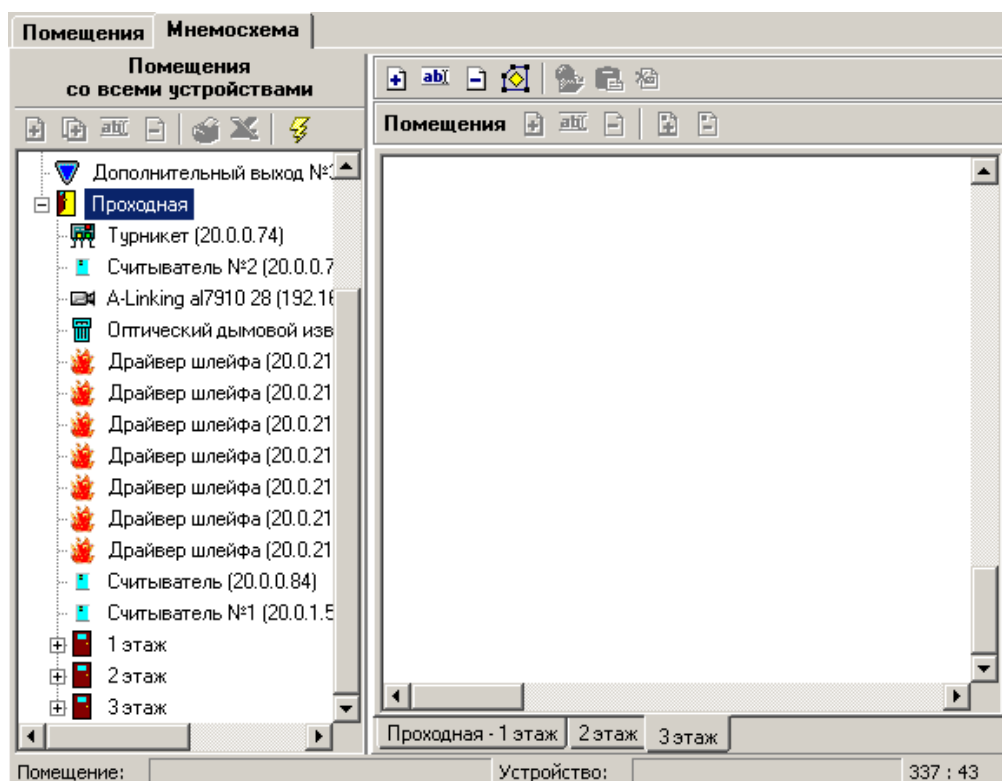
✓ Создание мнемосхем с использованием графических изображений территории предприятия. В этом случае размер каждой мнемосхемы определяется размером загружаемого изображения, который не может превышать 1600x1600 пикселей.

Далее рассмотрим создание мнемосхем с использованием графических планов. Создание без графических планов полностью аналогично.

Для создания мнемосхемы предприятия (поэтажных планов) в первую очередь подготовьте их графические изображения. Для этого могут быть использованы отсканированные поэтажные планы предприятия и/или созданные при помощи других средств графические изображения.

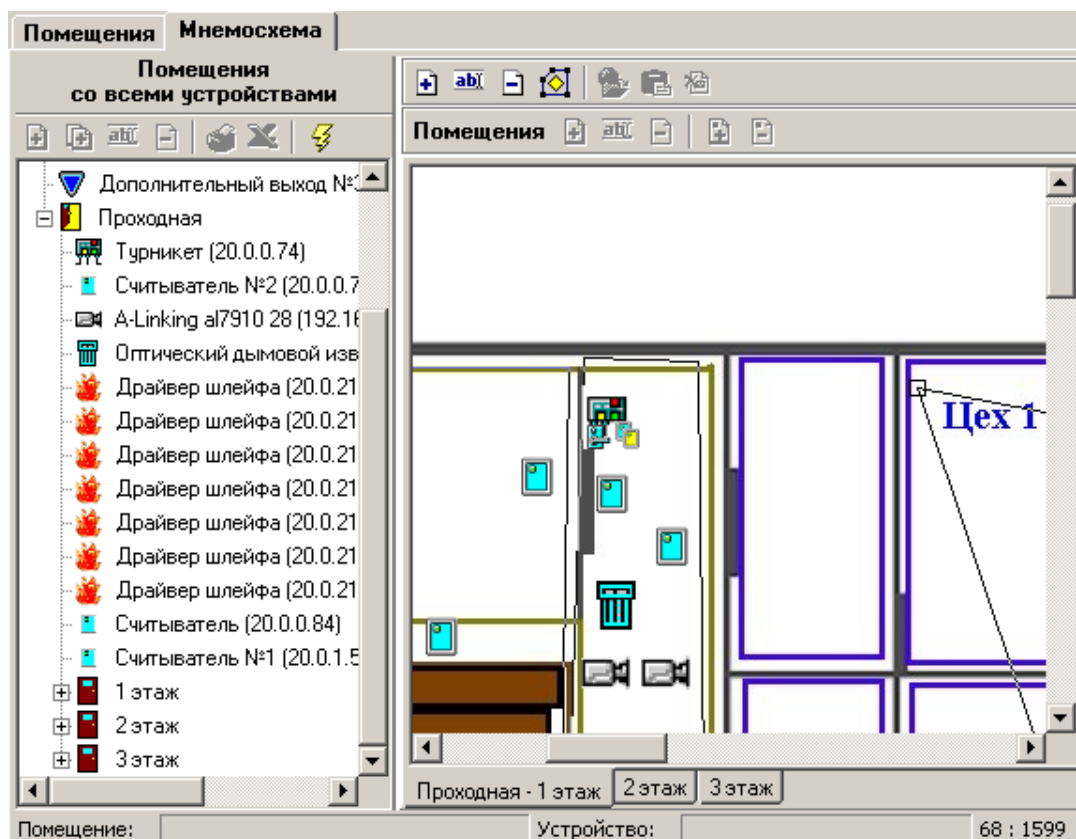
После создания графических изображений и дерева помещений можно переходить непосредственно к созданию мнемосхем предприятия:

1. Создайте необходимое количество мнемосхем с соответствующими названиями. Например, ваше предприятие состоит из 3 этажей, для каждого из которых создано графическое изображение. Создайте 3 мнемосхемы: первую назовите, например, 1 этаж, вторую - 2 этаж и третью - 3 этаж.



2. Выберите поочередно мнемосхемы и загрузите туда созданные ранее графические планы предприятия:

3. Выберите поочередно мнемосхемы каждого этажа и разместите на них созданные в дереве помещений объекты. Добавляя точки к графическим отображениям помещений, измените их конфигурацию так, чтобы они наиболее точно совпадали с контурами помещений на графическом изображении. Расставьте объекты системы внутри помещений в соответствии с их реальным расположением.



4. Сохраните сделанные изменения и передайте измененные параметры конфигурации.

ПЕРСОНАЛ

Одной из важнейших частей системы безопасности являются сотрудники и посетители предприятия. Именно они, как правило, являются источниками большинства событий, происходящих в системе. Единая система безопасности PERCo-S-20 содержит в себе все необходимое как для организации доступа сотрудников и посетителей на территорию предприятия, так и для ведения информационной базы данных сотрудников и построения всего комплекса дисциплинарных отчетов, включая стандартизованные отчеты T-12 и T13.

УЧЁТНЫЕ ДАННЫЕ

Любое предприятие имеет свою собственную структуру подразделений, свое штатное расписание и установленные требования к хранению информации о сотрудниках.

Раздел Учётные данные позволяет создавать и изменять справочные данные о структуре подразделений предприятия, должностях, дополнительных данных о сотрудниках.

Подробная информация о правилах работы с этим разделом приведена в Руководстве пользователя в разделе Учётные данные.

СПРАВОЧНИК ПОДРАЗДЕЛЕНИЯ

Учётные данные

Подразделения Должности

Показывать скрытые

- (не определено)
- КПП - контрольно-пропускной пункт
- Предприятие - административно-заводское здание
- Технопарк - служебные машины предприятия

Название Описание

OK Отмена

Справочник **Подразделения** предназначен для создания и редактирования структуры подразделений предприятия в соответствии с его штатным расписанием. Эта информация в дальнейшем используется при вводе данных о сотрудниках предприятия и при составлении отчетов по сотрудникам.

Необходимо отметить, что данные о структуре подразделений при удалении переходят в раздел «скрытых» подразделений. Это сделано для того, чтобы сохранить историю изменений штатного расписания, перевода сотрудников из одного подразделения в другое для возможности последующего построения отчетов по дисциплине труда.

Для отображения/восстановления скрытых подразделений необходимо отметить

☒ Показывать скрытые

СПРАВОЧНИК ДОЛЖНОСТИ

Учётные данные

Подразделения | Должности

Показывать скрытые

Название	Описание
(не определена)	
Аналитик	
Бухгалтер	
Вице-президент	
Водитель	
Директор	
Кладовщик	
Механик	
Охранник	
Переводчик	
Программист	
Слесарь	
Тестер	
Уборщица	

Название Описание

OK Отмена

Справочник **Должности** по своему назначению аналогичен справочнику подразделений. В отличие от справочника **Подразделения** он представлен не в виде иерархического дерева, а в виде линейного списка.

Данные, вносимые в этот справочник, используются при вводе информации о сотруднике и при построении отчетов по сотрудникам.

Сотрудники

Раздел **Сотрудники** облегчает ведение и оперативное внесение изменений в учетные данные сотрудников, упорядочивает эти данные, что значительно сокращает объем рутинной работы и повышает эффективность работы сотрудников отделов кадров (отделов персонала).

Подробная информация о работе с разделом, ведении единой базы сотрудников приведена в Руководстве пользователя в разделе **Сотрудники**.

ПАРАМЕТРЫ ДОСТУПА

Для нормального функционирования системы безопасности недостаточно провести конфигурацию устройств системы, задать принципы ее работы и ввести данные о сотрудниках. Необходимо выдать карты сотрудникам и указать для каждого из них права доступа, то есть указать, где и в какое время каждый сотрудник имеет право на проход, на постановку/снятие с охраны помещений.

Перед началом работы с разделами программного обеспечения по управлению доступом сотрудников необходимо тщательно подготовить информацию о графиках работы сотрудников предприятия, об их административных правах по постановке помещений на охрану. И следует увязать ее с конфигурацией установленного оборудования, входящего в единую систему безопасности.

После подготовки можно переходить к выдаче карт доступа и назначению прав доступа сотрудников.



ПРИМЕЧАНИЕ

В базовом ПО не поддерживается разграничение доступа по времени и постановка/снятие с охраны.

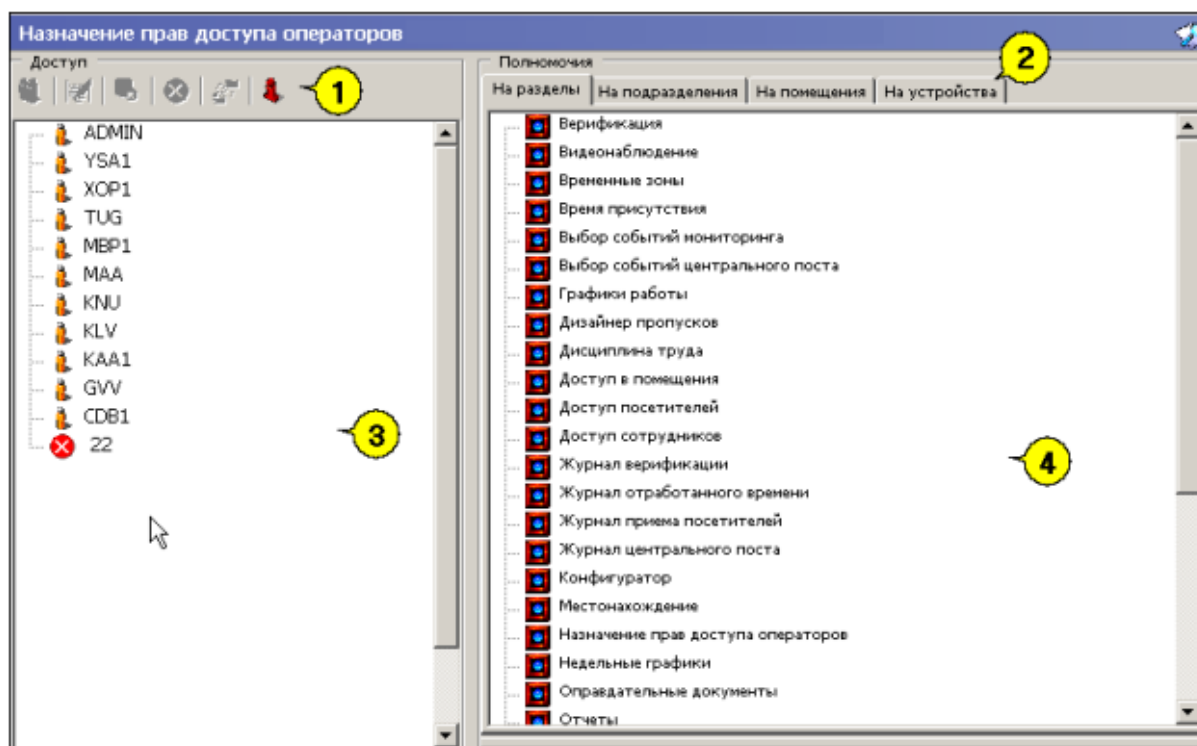
НАЗНАЧЕНИЕ ПРАВ ДОСТУПА ОПЕРАТОРОВ

Раздел Назначение прав доступа операторов предназначен для ведения списка операторов системы, установки для них пароля, оперативного управления их правами, выдачи для каждого из них прав на работу со всеми разделами программного обеспечения.

Для активизации раздела щелкните на кнопке раздела Назначение прав доступа операторов. Рабочее окно раздела отобразится в основной части окна Консоли управления.

РАБОЧЕЕ ОКНО

Рабочее окно раздела Назначение прав доступа операторов состоит из следующих элементов:



1. Функциональные элементы раздела

Функциональные элементы раздела Назначение прав доступа операторов



- 1 — Добавить пользователя
- 2 — Редактирование данных пользователя
- 3 — Удалить пользователя
- 4 — Запретить доступ оператору
- 5 — Копирование прав
- 6 — Показать скрытых пользователей

2. Вкладки рабочей области Полномочия: На разделы, На подразделения, На помещения, На устройства.

3. Список всех зарегистрированных пользователей с указанием прав каждого из них.

4. Рабочая область вкладок представлена в виде многостраничного блокнота с информацией о разделах ПО и объектах системы, на которые могут быть предоставлены права доступа операторам системы.

ОСНОВНЫЕ ФУНКЦИИ

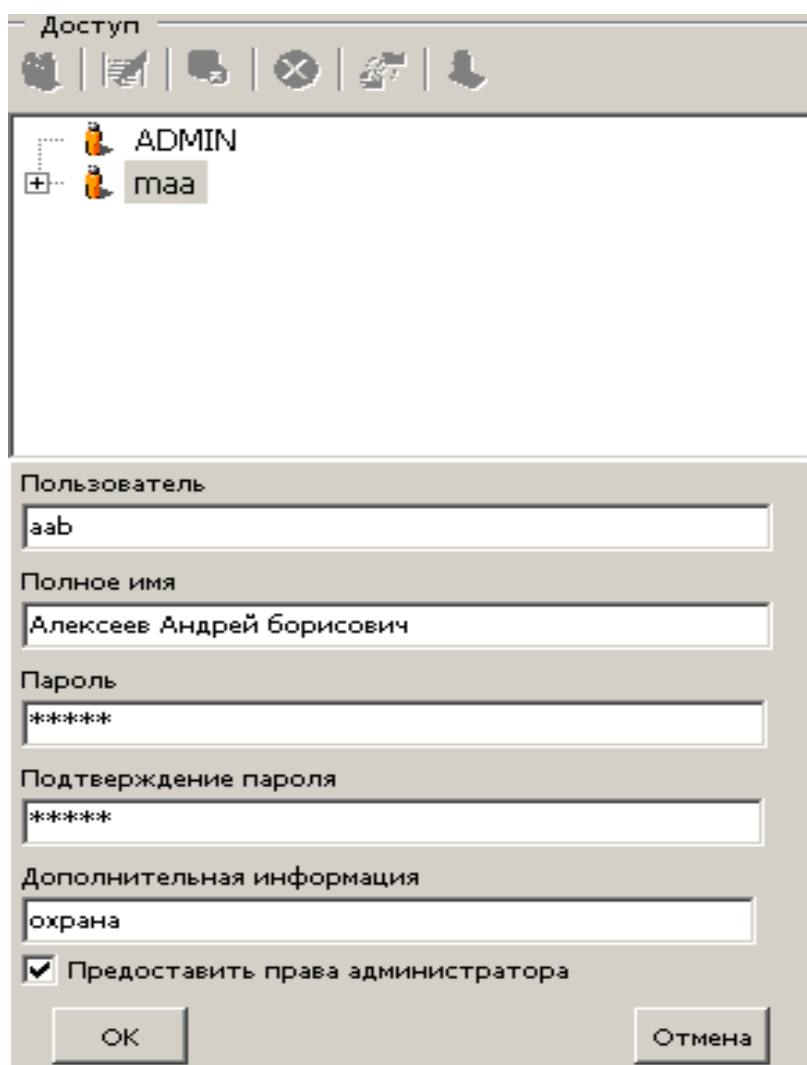
Ниже описываются функциональные возможности, предоставляемые системой пользователю раздела Назначение прав доступа операторов.

Добавление пользователя

Перед добавлением новых операторов необходимо подготовить соответствующий административный документ, который должен определять права каждого оператора по работе с системой безопасности. После составления этого документа можно приступить к вводу данных об операторах программного обеспечения.

Для добавления пользователя:

1. Щелкните на кнопке Добавить пользователя — . В нижней части рабочей области Доступ откроется дополнительная панель для ввода данных:



The screenshot shows a window titled "Доступ" (Access). At the top, there is a toolbar with several icons. Below the toolbar, there is a list of users: "ADMIN" and "таа". To the left of the list is a "+" icon. Below the list, there is a form to add a new user. The form has the following fields:

- Пользователь (User): a text box containing "aab".
- Полное имя (Full name): a text box containing "Алексеев Андрей борисович".
- Пароль (Password): a text box containing "*****".
- Подтверждение пароля (Password confirmation): a text box containing "*****".
- Дополнительная информация (Additional information): a text box containing "охрана".
- Предоставить права администратора (Grant administrator rights): a checkbox that is checked.

At the bottom of the form, there are two buttons: "ОК" (OK) and "Отмена" (Cancel).

Укажите следующие данные на оператора (необходимым является только поле **Пользователь**, остальные – по желанию):

- **Пользователь** – в этой строке указывается имя пользователя, которое он будет вводить при запуске программного обеспечения.

- **Полное имя** – в этой строке указывается ФИО пользователя.
- **Пароль** – указывается пароль пользователя.
- **Подтверждение пароля** - указывается тот же самый пароль для избежания ошибки ввода.
- **Дополнительная информация** – в этой строке ввода можно ввести любую дополнительную информацию об операторе.

Флажок: **Предоставить права администратора** позволяет предоставить вводимому пользователю права администратора системы безопасности. При этом этот пользователь будет иметь право доступа ко всему программному обеспечению, к изменению любых настроек системы и прав, а так же иметь возможность управлять любым устройством, входящим в систему безопасности.



ПРИМЕЧАНИЕ

Предоставить оператору права администратора может только администратор.

2. Для подтверждения введенных данных щелкните на кнопке «ОК».



ПРИМЕЧАНИЕ

В системе всегда присутствует предопределенный пользователь “ADMIN”. После установки системы необходимо задать ему пароль, по умолчанию пароль отсутствует. Этот пользователь или любой другой пользователь с правами администратора имеет доступ ко всем разделам программного обеспечения и возможность управления и изменения параметров всех устройств, входящих в систему безопасности.

Редактирование данных пользователя

Для редактирования данных пользователя:

1. Выделите пользователя, чьи данные необходимо отредактировать.
2. Щелкните на кнопке Редактирование данных пользователя — . В нижней части рабочей области Доступ откроется дополнительная панель для редактирования данных:
3. Для подтверждения измененных данных щелкните на кнопке «ОК».

Удаление пользователя

Для удаления пользователя:

- Выделите пользователя, которого необходимо удалить.
- Щелкните на кнопке **Удалить пользователя** — . Откроется окно подтверждения:

- Щелкните на кнопке «Да». Пользователь будет скрыт.
- Сохраните данные с помощью кнопки  **Сохранить** в основном меню Консоли управления.

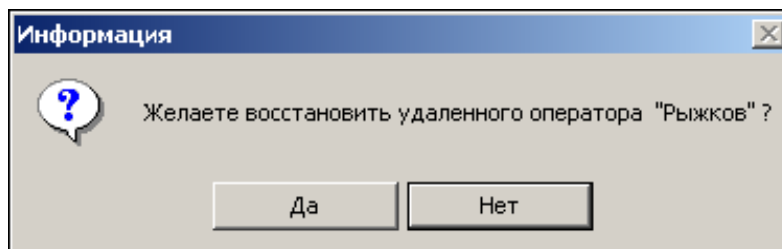
Если пользователю были назначены права доступа, а его удалили по каким-либо

причинам, то пользователь будет скрыт, а его права удалены.

Для отображения скрытых пользователей щелкните на кнопке Показать скрытых пользователей — .

Для восстановления скрытых пользователей:

- Щелкните на кнопке **Восстановить пользователя** — . Откроется окно подтверждения:



- Щелкните на кнопке «Да». Пользователь будет восстановлен.
- Сохраните данные с помощью кнопки  Сохранить в основном меню Консоли управления.

Предоставление прав доступа оператору

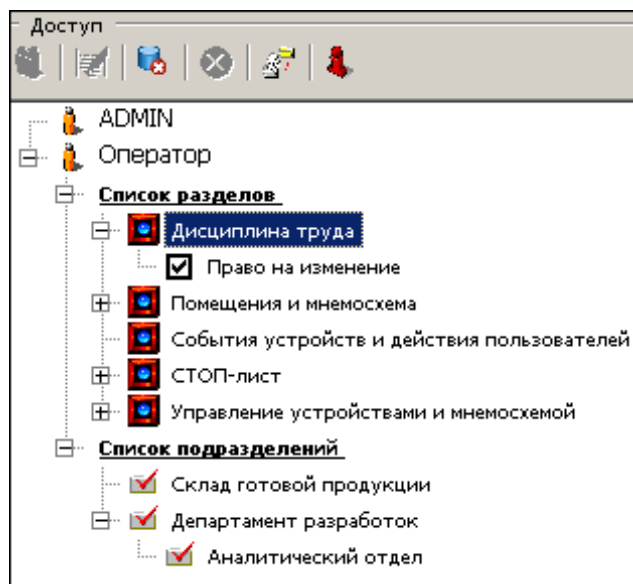
Для предоставления прав доступа оператору выделите его мышью в списке операторов системы и выберите соответствующую вкладку в правой части рабочего окна.

1. Права доступа на разделы

На вкладке: На разделы представлен список всех разделов программного обеспечения, к которым может быть предоставлен доступ выбранному оператору.

Для предоставления доступа выберите необходимый раздел программного обеспечения в списке, и, не отпуская клавиши мыши, перетащите его на имя оператора, которому предоставляется доступ.

После этого название добавленного раздела программного обеспечения отобразится под оператором:



Перетаскивание названия раздела определяет, что данный оператор имеет право на вход в этот раздел и просмотр имеющейся там информации. Кроме этого для раздела могут быть указаны дополнительные права:

- **Право на изменение** – позволяет вносить и сохранять изменения в данные, предоставляемые этим разделом.
- **Право на передачу данных в аппаратуру** – позволяет оператору передавать измененные данные в устройства системы.



ПРИМЕЧАНИЕ

Возможно выделение сразу нескольких разделов: выделите группу разделов, удерживая клавишу Shift и не отпуская левую кнопку мыши, либо щелкайте по отдельным разделам, удерживая клавишу Ctrl.

Для предоставления дополнительных прав необходимо установить метку у соответствующего права.

2. Права доступа на подразделения

Вкладка **На подразделения** позволяет указать список подразделений, информация о сотрудниках которых будет доступна этому оператору.

Порядок действий предоставления права оператору полностью аналогичен описанному выше (см. *Права доступа на разделы выше*). При этом при перетаскивании подразделения, имеющего вложенные подразделения, автоматически будут добавлены все вложенные подразделения.

3. Права доступа на помещения

Вкладка **На помещения** позволяет указать список помещений данного предприятия, в которые данный оператор сможет разрешать/запрещать доступ сотрудникам и посетителям. И также устанавливать параметры этого доступа.

Порядок действий предоставления права оператору полностью аналогичен описанному выше (см. *Права доступа на разделы* выше).

4. Права доступа на управление устройствами

Вкладка **На устройства** дает возможность указать, какими именно устройствами, входящими в систему безопасности, будет разрешено управлять оператору.

Порядок действий предоставления права оператору полностью аналогичен описанному выше (см. *Права доступа на разделы* выше).

5. Запрет доступа пользователя

Для запрета доступа пользователя:

1. Выделите пользователя, которому необходимо запретить доступ.
2. Щелкните на кнопке Запретить доступ оператору — . Слева от пользователя отобразится значок .

Для восстановления доступа пользователя щелкните на этой же кнопке еще раз.



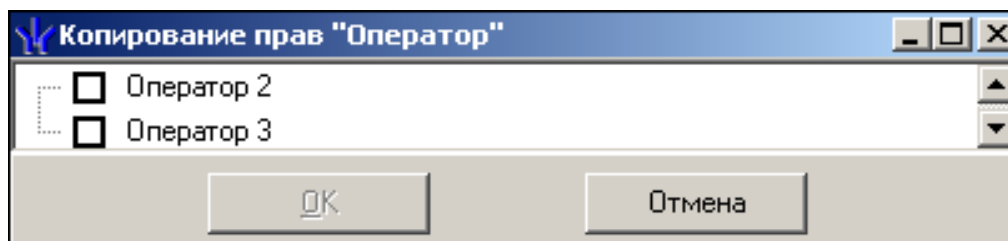
ПРИМЕЧАНИЕ

Запрет доступа, изменения списка доступных устройств, разделов, помещений и подразделений вступит в силу после начала нового сеанса пользователем, которому были внесены изменения.

Копирование прав

Для копирования прав:

1. Выделите пользователя, чьи права будут скопированы (права могут быть скопированы не полностью, а частично, например, права доступа только в один раздел или на один этаж).
2. Щелкните на кнопке Копирование прав — . Откроется окно:



3. Укажите, кому надо скопировать права, отметив флажки, и щелкните на кнопке «ОК». Права будут скопированы.

УПРАВЛЕНИЕ УСТРОЙСТВАМИ

Любая система безопасности имеет в своем составе систему оповещения службы безопасности о тревожных событиях, происходящих на охраняемом объекте. Единая система безопасности PERCo-S-20 предлагает гибкую, легко настраиваемую в зависимости от задач системы безопасности систему оповещения сотрудников предприятия и сотрудников службы безопасности о ситуации на охраняемом объекте.

Организация системы оповещения сотрудников предприятия на основе подключения тревожных оповещателей хорошо всем известна. Принципы подключения и задания параметров функционирования такой системы оповещения описаны выше в разделе Конфигурация контроллеров.

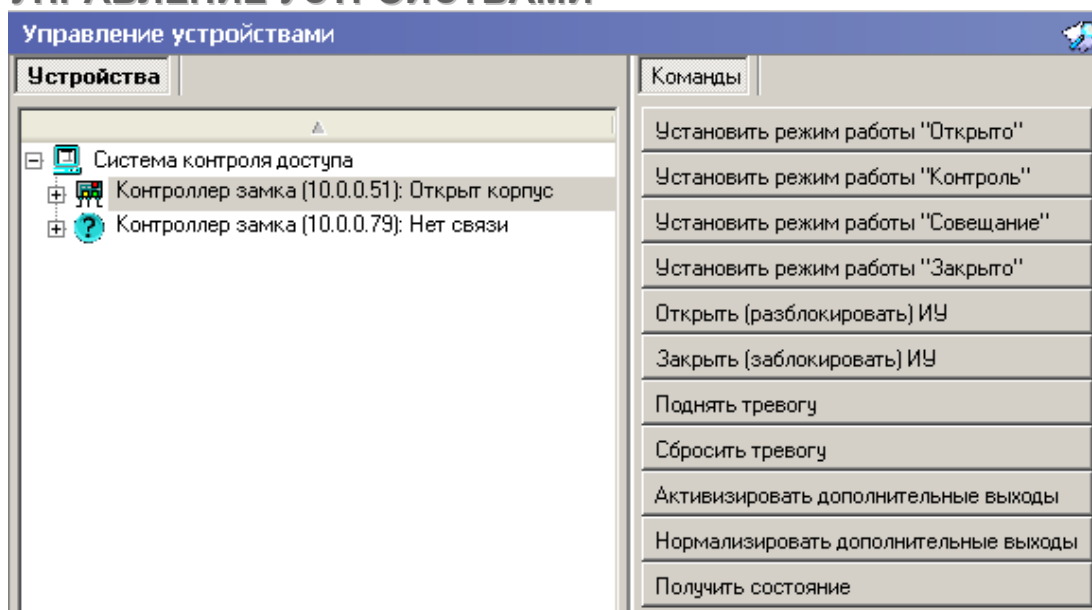
Программное обеспечение единой системы безопасности PERCo-S-20 предоставляет возможность создания рабочих мест сотрудников отдела безопасности для контроля за состоянием охраняемых объектов.

Общей характеристикой разделов мониторинга и управления устройствами является отображение состояния объектов в том или ином виде и отображение в табличном виде событий, происходящих на устройствах системы безопасности.

Отличительной особенностью единой системы безопасности PERCo-S-20 является то, что контроллеры системы самостоятельно сообщают программному обеспечению обо всех событиях, тем самым скорость доставки и отображения информации превосходит аналогичные системы.

Ниже приведена общая информация о возможностях разделов. Информация об интерфейсе пользователя приведена в соответствующих руководствах оператора. В этом документе мы остановимся на ключевых моментах, необходимых при настройке рабочего места.

УПРАВЛЕНИЕ УСТРОЙСТВАМИ



Раздел **Управление устройствами** предоставляет возможность отображения информации о состоянии объектов, произошедших событиях в системе безопасности и управления устройствами системы безопасности.

Состояние устройств отображается в виде изменения пиктограммы устройства в дереве объектов системы.

События, произошедшие на устройствах системы безопасности, отображаются в нижней части окна в виде таблицы. Список событий и причины их формирования приведен в *Приложении 1*.

УПРАВЛЕНИЕ СЕРВЕРАМИ

Для управления сервером PERCo-S-20 запустите Панель управления Windows (**Пуск** → **Настройка** → **Панель управления**), в которой присутствует иконка:

✓ — , для управления сервером системы PERCo-S-20 и сервером баз данных (Рис.4.):

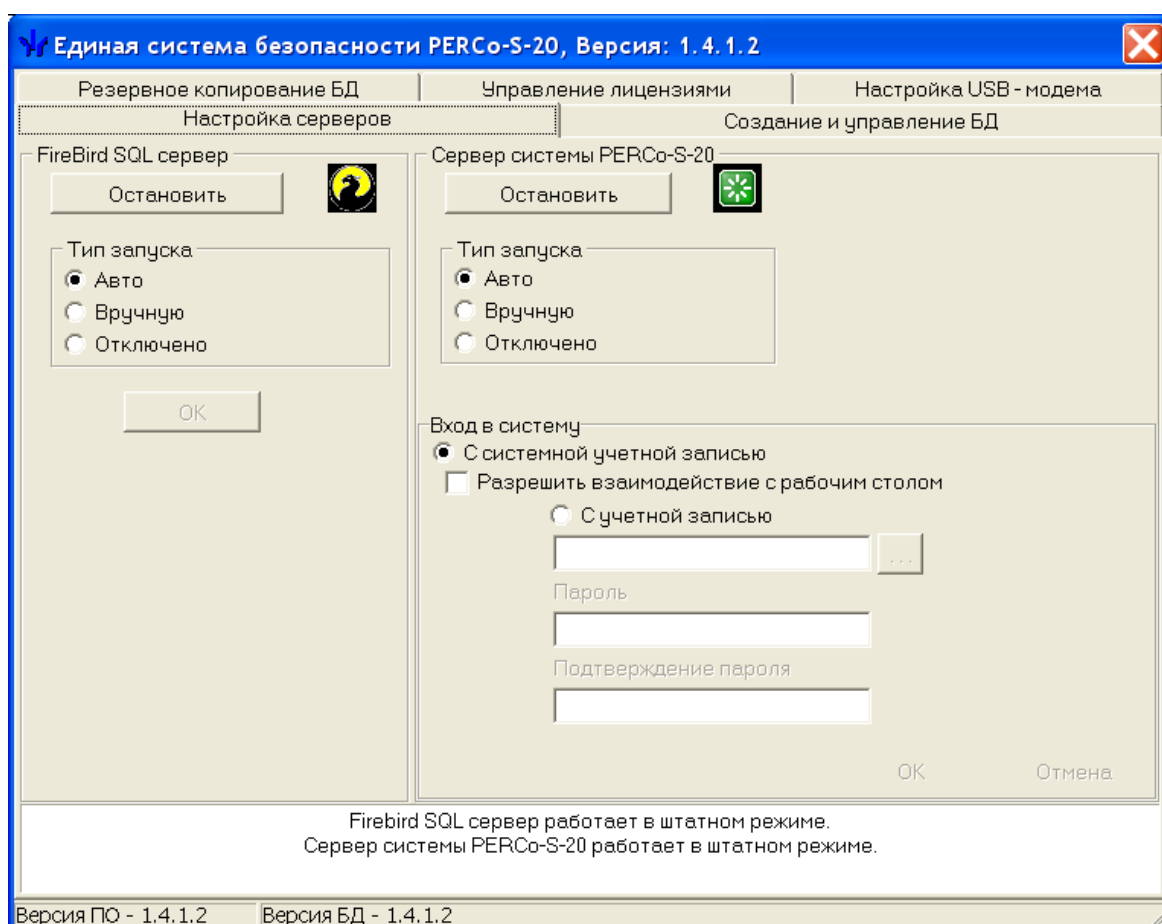


Рис. 4. Центр управления серверами системы PERCo-S-20

Вход в систему в режиме, когда отмечен переключатель **С системной учетной записью**, позволяет настроить почтовую рассылку сообщений о создании резервных копий базы данных (см. п. *Резервное копирование БД*).

БАЗА ДАННЫХ

В качестве СУБД в системе PERCo-S-20 используется SQL-сервер Firebird 2.0. Он устанавливается вместе с ПО системы, тем не менее, создание самой базы данных необходимо проводить вручную.

Для создания и управления настройками базы данных единой системы безопасности PERCo-S-20 предназначена закладка **Создание и управление БД**:

Единая система безопасности PERCo-S-20, Версия: 1.3.1.4

Резервное копирование БД | Управление лицензиями

Настройка серверов | **Создание и управление БД**

Расположение базы данных: D:\BaseScd17K\SCD17K.FDB

Расположение архивов базы данных: D:\BaseScd17K\

Учетная запись пользователя: sysdba

Пароль пользователя: [masked]

Настройка сервера системы и сервера Firebird

Порт данных	Порт FireBird
211	3050
Порт уведомлений	Время восстановления соединения (сек.)
411	30
Время конфигурации по одному сетевому интерфейсу (мин.)	
1	

Режим

☒ Изменение настроек

☐ Создание базы данных

- **Расположение базы данных.** В этой строке указывается путь к файлу БД. Данный путь может быть введен непосредственно в строке ввода или выбран при использовании кнопки, которая расположена справа от строки ввода.
- **Расположение архивов базы данных.** В этой строке указывается путь к каталогу, в котором будут размещаться архивные копии базы данных. Правила ввода пути аналогичны предыдущим.
- **Учетная запись пользователя.** Этот параметр задает имя пользователя, от которого будет осуществляться доступ к файлу базы данных.
- **Пароль пользователя.** Этот параметр задает пароль пользователя, от имени которого будет происходить обращение к файлу базы данных.
- **Настройки сервера системы** – параметры, определяющие значения портов ввода/вывода, которые используются программным обеспечением для связи между программными модулями.
- **Время восстановления (сек)** - время, через которое Сервер системы попытается восстановить связь с любым контроллером системы в случае ее неожиданной потери.
- **Время конфигурации по одному сетевому интерфейсу (мин)** – предельный минимум времени, отведенный на конфигурацию по одному адресу и маске подсети. Пользователь может изменить его по своему усмотрению, но значение не может быть

меньше предопределенного (1 мин).

Создание базы данных

Щелкнув на иконке из Панели управления  , запустите «Центр управления серверами PERCo-S-20»

Убедитесь (см. Рис. 4), что Firebird SQL Server запущен. Информация об этом расположена в нижней части окна.

Для создания базы данных перейдите на вкладку **Создание и управление БД** (Рис.5.):

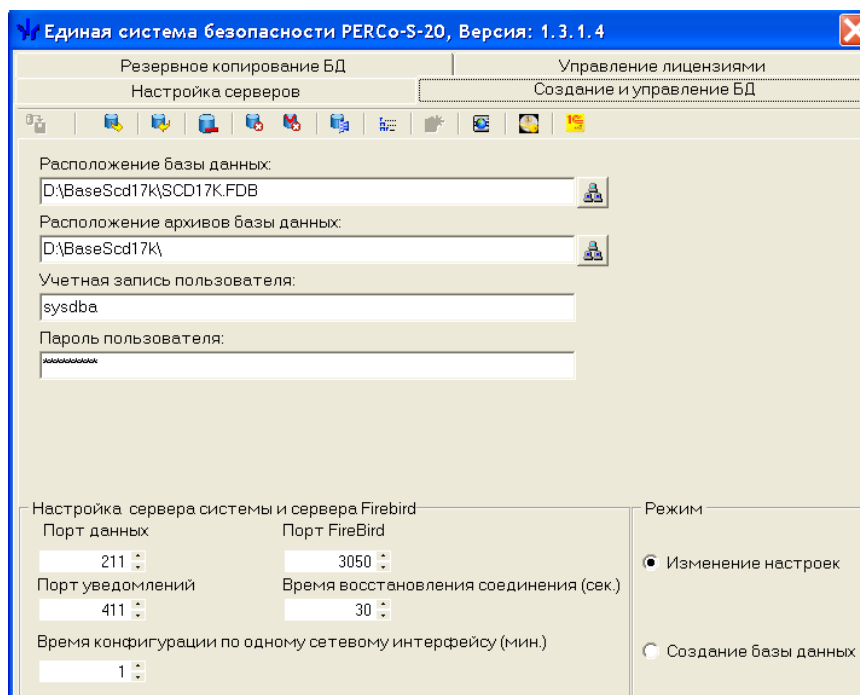


Рис. 5.

Выберите режим работы **Создание базы данных**. Заполните соответствующие поля (Рис.6.):

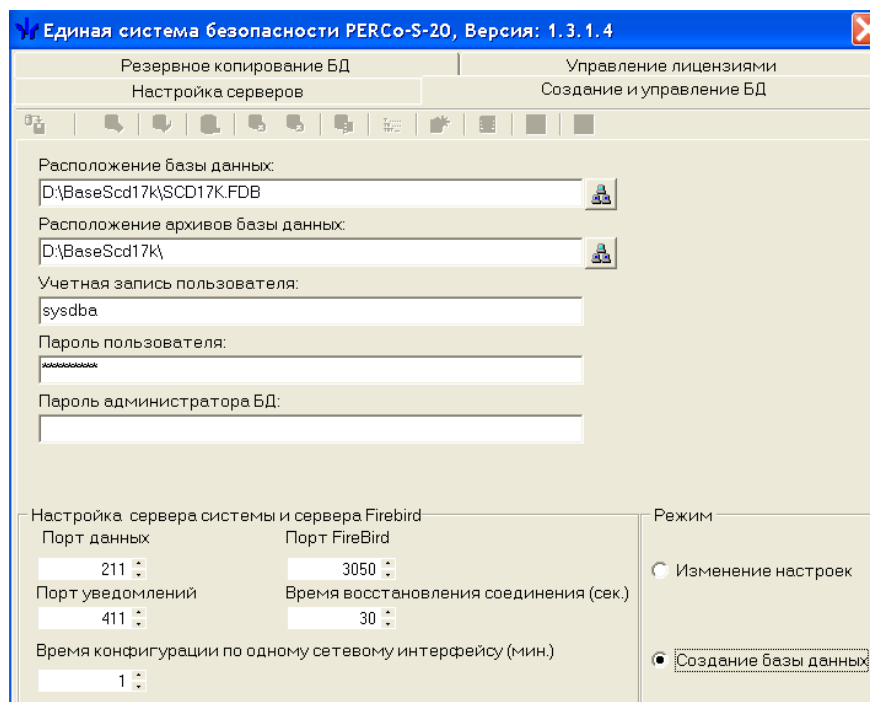


Рис. 6. Создание базы данных

Заполните параметры базы данных:

1. Укажите путь к тому месту, где будет создан файл базы данных. Это путь к компьютеру, где был ранее установлен SQL-сервер Firebird 2.0. Папку, в которой вы создаете файл базы данных, для повышения безопасности не рекомендуется предоставлять в общее пользование. Если база находится на том же компьютере, что и сервер управления, вы можете выбрать путь с помощью кнопки , если нет, то кнопка будет неактивной, и вы должны ввести путь вручную.
2. Укажите путь к архиву базы данных. Это путь к директории, где будут создаваться архивные копии файла базы данных. Имя самого файла базы данных и архива лучше не изменять. Имя директории может вводиться вручную (тогда это директория на компьютере, где находится SQL-сервер) или выбираться нажатием на кнопку . В этом случае можно выбирать директорию, к которой предоставлен общий доступ с любого компьютера сети. Если SQL-сервер запущен как сервис, то данному сервису должен быть предоставлен полный доступ к директории. Если SQL-сервер запущен как приложение, то учетной записи, под которой он запущен, должны быть предоставлены права на директорию.
3. Введите имя пользователя, который будет создателем и владельцем файла базы данных (оставьте предопределенное).
4. Введите пароль пользователя для доступа к БД (оставьте предопределенный).



ПРИМЕЧАНИЕ

Пользовательские имя и пароль указываются один раз при создании базы данных. Они не имеют отношения к реальным пользователям, которые получают доступ к БД из клиентских приложений.

После ввода всех характеристик нового файла баз данных нажмите кнопку **Создать базу данных**.

После создания базы можно работать с любым разделом программного обеспечения системы PERCo-S-20. Поля данных на вкладке заполнятся введенными параметрами. И станут доступными следующие элементы управления (Рис. 7):



Рис. 7. Элементы управления базой данных

- 1 — Сохранение настроек базы данных
- 2 — Сохранение базы данных оптимизация и проверка целостности(см. «Сохранение базы данных»)
- 3 — Восстановление БД
- 4 — Удаление данных мониторинга
- 5 — Удаление данных по событиям
- 6 — Удаление данных по видеоидентификации
- 7 — Настройки сервера БД
- 8 — Оптимизация индексов
- 9 — Создание базы данных
- 10 — Обновление версии базы данных
- 11 — Восстановление предыдущего пароля устройств
- 12 — Настройка работы с 1С

Сохранение настроек базы данных

Этот элемент управления позволяет сохранить изменения, внесенные в параметры базы данных.

Сохранение базы данных

При нажатии на кнопку **Сохранение базы данных** —  происходит создание полной резервной копии базы данных. Выбор места расположения резервной копии БД определяется на этапе создания (см. «Создание базы данных»). Однако резервные копии

БД можно делать и в другом месте. Для внесения изменений необходимо произвести следующие действия:

1. Выбирается имя компьютера, на котором установлен Сервер БД, т.е. указывается имя компьютера, где расположен SQL-сервер Firebird 2.0.
2. Вводится путь к файлу базы данных. Необходимость менять путь к базе может возникнуть при переносе базы. Если “Консоль администратора БД” запущена на том же компьютере, где установлен SQL-сервер Firebird 2.0, то Вы можете выбрать путь с помощью кнопки , если нет, то кнопка будет не активна, и Вы должны ввести путь вручную.
3. Указывается директория, в которой сохраняются архивные файлы. Имя директории может вводиться вручную (тогда это директория на компьютере, где находится SQL-сервер) или выбираться нажатием на кнопку . В этом случае можно выбрать директорию, к которой предоставлен общий доступ с любого компьютера сети (не рекомендуется, т.к. замедляется создание архивов и их восстановление). Рекомендуется иметь второй HDD на компьютере с сервером Firebird и сохранять архивы на диск отличный от диска, где находится БД.
4. Указывается пользователь, от имени которого создается база данных, и его пароль.

Восстановление базы данных из резервной копии

Восстановление данных из архива выполняется при помощи нажатия кнопки **Восстановление базы данных** — .

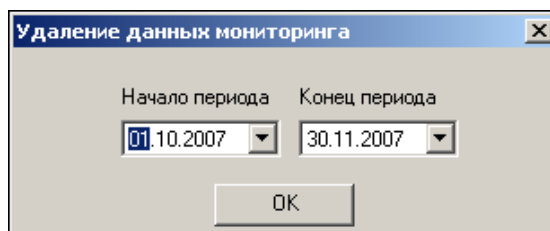
Сохраненная копия базы данных после восстановления имеет то же название, что и рабочая база, но с добавлением символа «#» в конце имени файла. После успешного выполнения команды восстановленная база становится рабочей.

При следующем восстановлении копия будет иметь тоже название, но уже без символа «#» на конце. После выполнения команды она также сразу станет рабочей. В результате, при нормальной работе существуют два файла базы данных (рабочая и предыдущая копия), а также набор архивных копий. Данная особенность создания резервных копий позволяет повысить надежность действий при восстановлении базы данных из архива и обеспечить безусловную работоспособность базы даже при наличии повреждений на диске.

Удаление данных мониторинга

Удаление данных по мониторингу можно выполнить после нажатия кнопки —



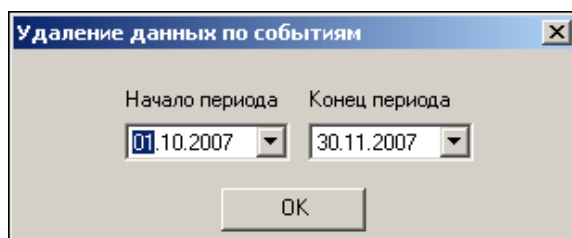


Выберите начало и конец периода мониторинга данных, подлежащих удалению. Подтвердите выбор щелчком на кнопке «**ОК**».

Проводите эти действия периодически. Это позволит уменьшить размер файла базы данных и ускорить работу программных модулей системы безопасности. Рекомендуется проводить эти действия один раз в месяц.

УДАЛЕНИЕ ДАННЫХ О СОБЫТИЯХ

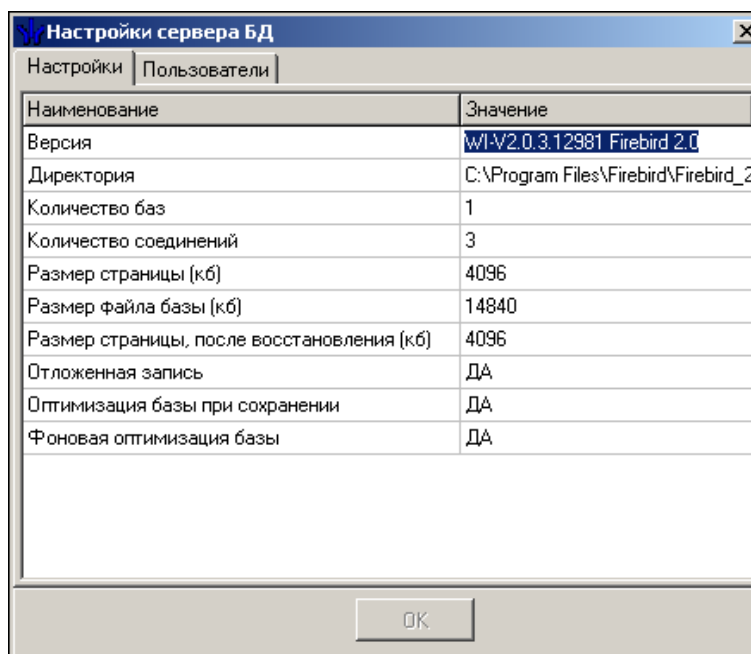
Удаление данных о проходах становится возможным после нажатия кнопки — :



Эти действия аналогичны действиям, описанным выше, за исключением того, что удаляются данные о событиях, зарегистрированных в системе и записанных в журнале регистрации. Рекомендуется проводить эти действия не реже одного раза в квартал после завершения формирования всех необходимых отчетов за удаляемый период.

Настройки сервера баз данных

Окно **Настройки сервера БД** вызывается нажатием кнопки — :



Окно **Настройки сервера БД** включает две закладки **Настройки** и **Пользователи**.

Вкладка **Настройки** включает следующие позиции:

- **Версия SQL-сервера Firebird** для сведения.
- **Директория** - место установки SQL-сервера Firebird.
- **Количество баз** – информационный параметр.
- **Количество соединений** – информационный параметр.
- **Размер страницы**. По умолчанию файл БД создается с размерами страницы 4096 байт.
- **Размер файла базы** - текущий размер файла базы данных системы PERCo-S-20.
- **Размер страницы, после восстановления**. При восстановлении БД, особенно при переносе на другой носитель, размер страницы может быть не кратным размеру кластера жесткого диска. Поэтому для оптимизации производительности рекомендуется устанавливать его кратным размеру кластера.
- **Отложенная запись**. Все изменения, затрагивающие данные на уровне файла базы данных, происходят с участием системного кэша, расположенного в памяти компьютера, что ускоряет файловые операции. Однако при сбоях компьютера, отключении питания и т.п. данные могут пропасть. Для повышения надежности сохранения оперативных данных можно отключить данный параметр, установив «Нет», при этом скорость операций с БД уменьшится.
- **Оптимизация базы при сохранении**. Данный параметр управляет необходимостью оптимизации БД (см. ниже «Фоновая оптимизация») при сохранении резервной копии БД.
- **Фоновая оптимизация базы**. При работе SQL-сервера создаются разные версии записей. При режиме «Да» они чистятся самим сервером, однако это замедляет его основную деятельность. Следует учесть, что сборка «мусора» происходит при сохранении базы данных, которое рекомендуется делать ежедневно. Поэтому рекомендуется выбирать режим «Нет».

В закладке **Пользователи** предоставляется возможность изменить пароль администратора БД. Рекомендуется заменить пароль «masterkey», являющийся общеизвестным, на пароль известный только администратору системы (пароли регистрозависимы).

Оптимизация индексов базы данных

Оптимизация индексов осуществляется нажатием на кнопку  (рекомендуется проводить раз в неделю). Это действие позволяет оптимизировать работы программного обеспечения с базой данных.

Обновление версии базы данных

Обновление версии базы данных производится только в случае получения обновления для программного обеспечения. Подробные инструкции по проведению обновления приводятся в сопроводительной документации на обновленную версию.

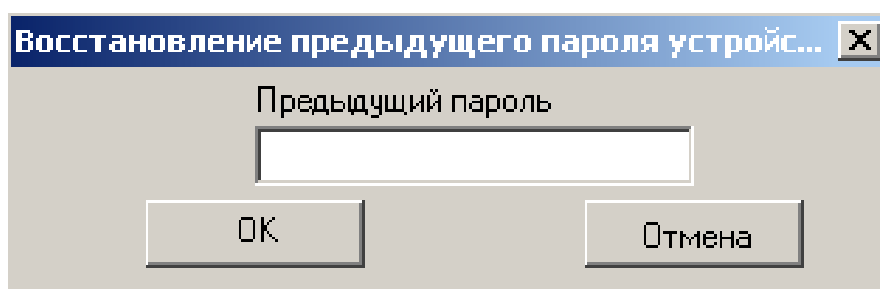
ВОССТАНОВЛЕНИЕ ПРЕДЫДУЩЕГО ПАРОЛЯ УСТРОЙСТВ

Восстановление предыдущего пароля устройств может быть необходимо в следующей ситуации:

После установки пароля и нормального функционирования системы, вы создали резервную копию БД. После этого вы сменили пароль для связи с устройствами системы и передали параметры. После этого вы восстановили БД из резервной копии.

В результате этих действий в программном обеспечении будет использоваться пароль, сохраненный до этого в БД, а в контроллерах системы будет использоваться пароль, установленный ранее. В этой ситуации программное обеспечение не сможет подключиться к контроллерам системы.

Для решения этой проблемы необходимо воспользоваться кнопкой **Восстановление предыдущего пароля устройств** — , расположенной в панели управления. Нажатие на нее приводит к появлению диалогового окна, в котором необходимо указать пароль, введенный ранее (пароль установленный на данный момент в контроллерах системы) и нажать на кнопку «ОК»:

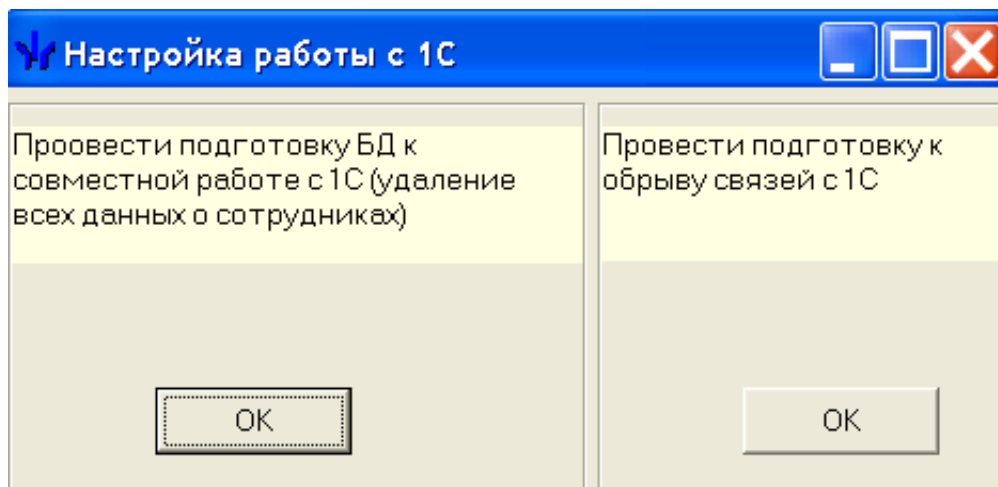


ПРИМЕЧАНИЕ

При восстановлении пароля все «Консоли управления» должны быть закрыты.

После задания нового пароля необходимо завершить работу с «Центром управления серверами». Запустить «Консоль управления» с установленным модулем Конфигуратор и передать измененные параметры в контроллеры системы.

НАСТРОЙКА РАБОТЫ С 1С



- Провести подготовку БД к совместной работе с 1С подразумевает удаление всех данных о сотрудниках и учетных данных включая справочники подразделений, должностей, графиков работы удаление всех данных о картах и правах доступа
- Провести подготовку к обрыву связей с 1С подразумевает удаление связующих элементов в базе между S-20 и 1С сами данные остаются, после выполнения этого действия изменения данных в 1С не будет синхронизироваться с S-20.

После первичной синхронизации данных между S-20 и 1С, часть действий в консоли управления становятся невозможными: удаление, добавление и изменение данных:

- О сотрудниках
- Учетных данных (подразделения и должности)
- Графики работы, праздничные дни и ночное время
- Оправдательные документы и документы на сверхурочные
- Справочник документов

После обрыва связей все эти действия снова становятся доступными.

Резервное копирование БД

Одной из основных проблем обслуживания информационных систем является своевременное создание резервных копий базы данных. К сожалению, сбои в работе персональных компьютеров, жестких дисков не редкость.

Для обеспечения целостности базы данных и своевременного создания резервных копий программное обеспечение единой системы безопасности PERCo-S-20 предоставляет возможность по автоматизации этого процесса. На вкладке **Резервное копирование БД** модуля управления сервером системы Вы можете создать расписание, по которому будут автоматически создаваться резервные копии БД.

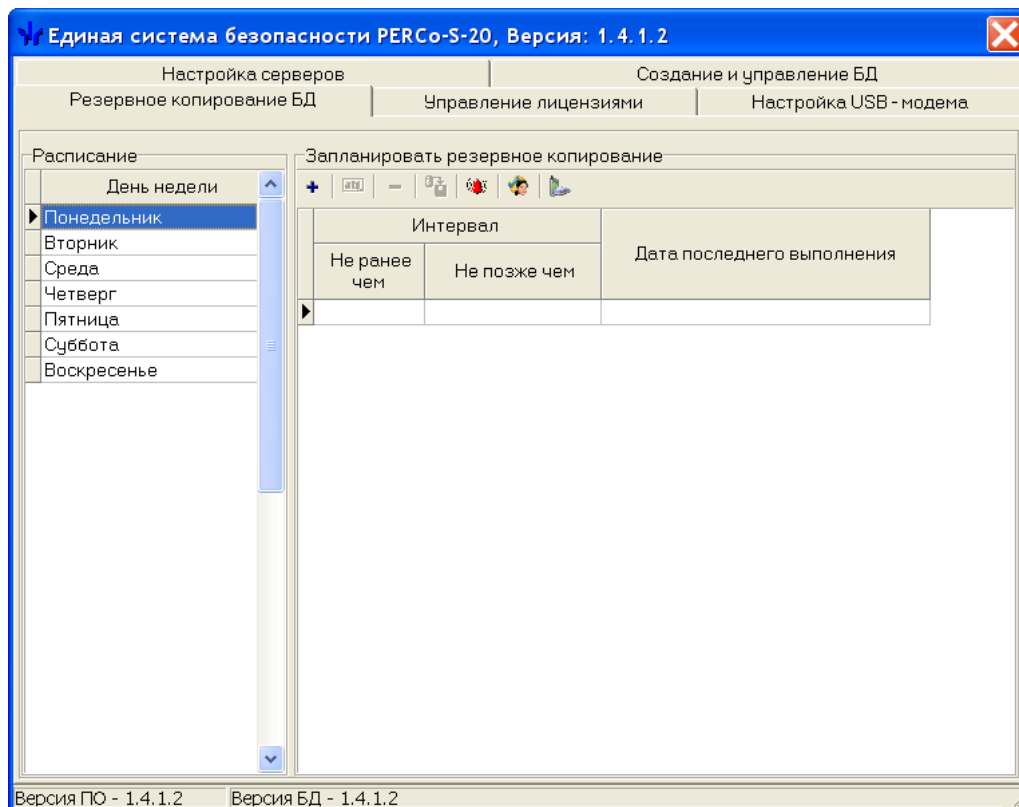
Резервная копия БД будет сохраняться в каталоге, указанном в строке **Расположение резервных копий базы данных** на вкладке **Создание и управление БД** данного модуля.

Для создания расписания выберите день недели и щелкните на кнопке . В нижней части окна откроется панель ввода:

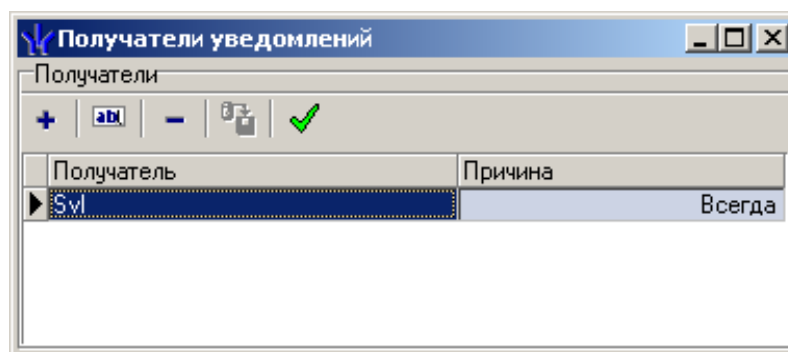
В этой панели укажите интервал времени, в течение которого сервер системы проведет создание резервной копии БД. При условии работы системы в круглосуточном режиме рекомендуется установить этот интервал в ночное время.

После завершения ввода временного интервала щелкните на кнопке «ОК» и сохраните внесенные данные щелчком на кнопке Сохранение расписания — .

Для изменения временного интервала используйте кнопку , для удаления — кнопку .



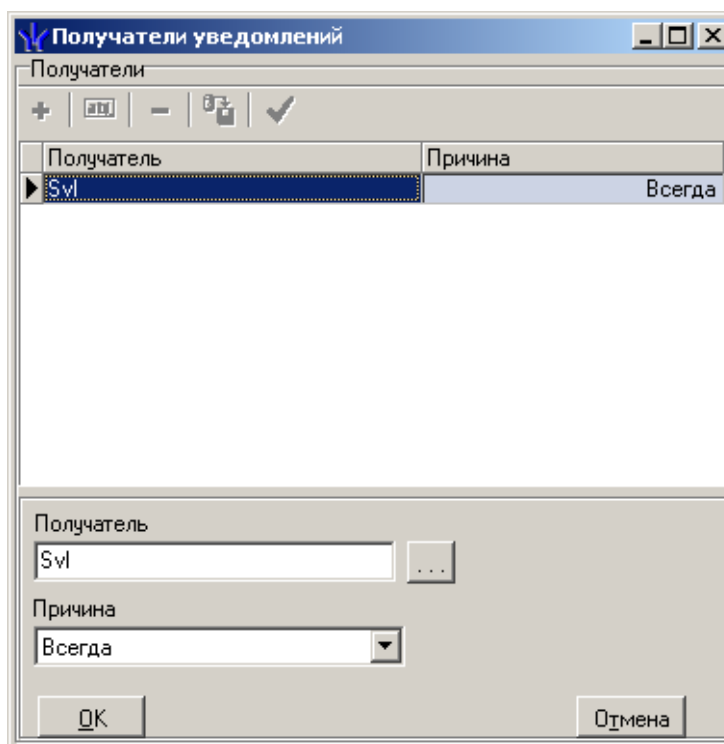
При создании резервной копии базы данных существует возможность рассылки уведомлений о результатах выполнения. Для задания списка рассылки по сети воспользуйтесь кнопкой . Щелчком на ней открывается диалоговое окно, отображающее текущее состояние списка рассылки:



В нем отображается имя получателя уведомления и причина, по которой будет отправляться данное уведомление.

Кнопка  позволяет протестировать работу данной функции. Щелчком на этой кнопке выделенному сотруднику отправляется тестовое сообщение.

Для добавления нового получателя уведомлений используйте кнопку . Щелчком на ней в нижней части окна открывается панель ввода:



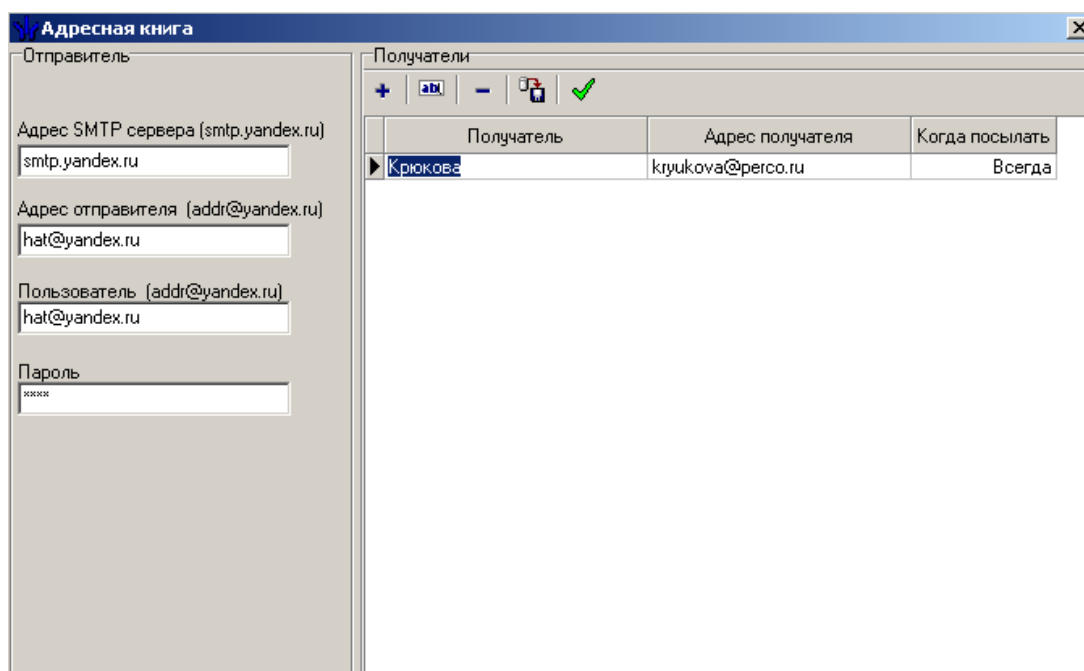
В этой панели введите имя компьютера, на которое будет отправлено сообщение и причину отправки, которая выбирается из списка. Доступны два варианта:

- **Всегда** – данное сообщение будет отправляться всегда, вне зависимости от результатов выполнения действий по созданию архивной копии.

- **В случае ошибки** – сообщение будет отправляться только в случае, если программное обеспечение не может создать резервную копию базы данных.

После завершения ввода щелкните на кнопке «**ОК**» и сохраните внесенные изменения.

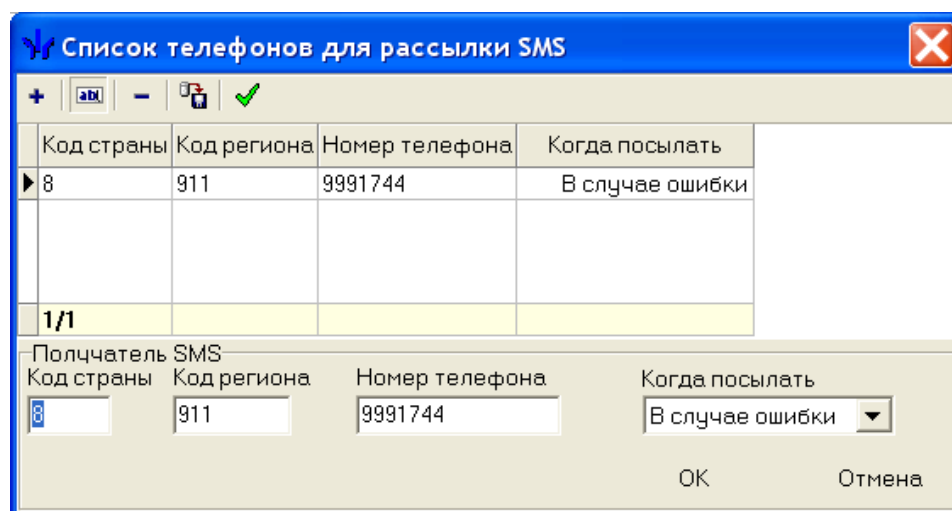
Кнопкой **Настроить почтовую рассылку уведомлений** —  открывается окно настройки рассылки по электронной почте уведомлений о создании резервной копии БД.



Получатель	Адрес получателя	Когда посылать
Крюкова	kryukova@perco.ru	Всегда

Функциональные элементы окна настройки почтовой рассылки уведомлений аналогичны описанным выше функциональным элементам окна настройки рассылки по сети.

Кнопкой **Настройка SMS рассылка**  — открывается окно настройки рассылки SMS уведомлений о создании резервной копии БД.



Код страны	Код региона	Номер телефона	Когда посылать
8	911	9991744	В случае ошибки

1/1

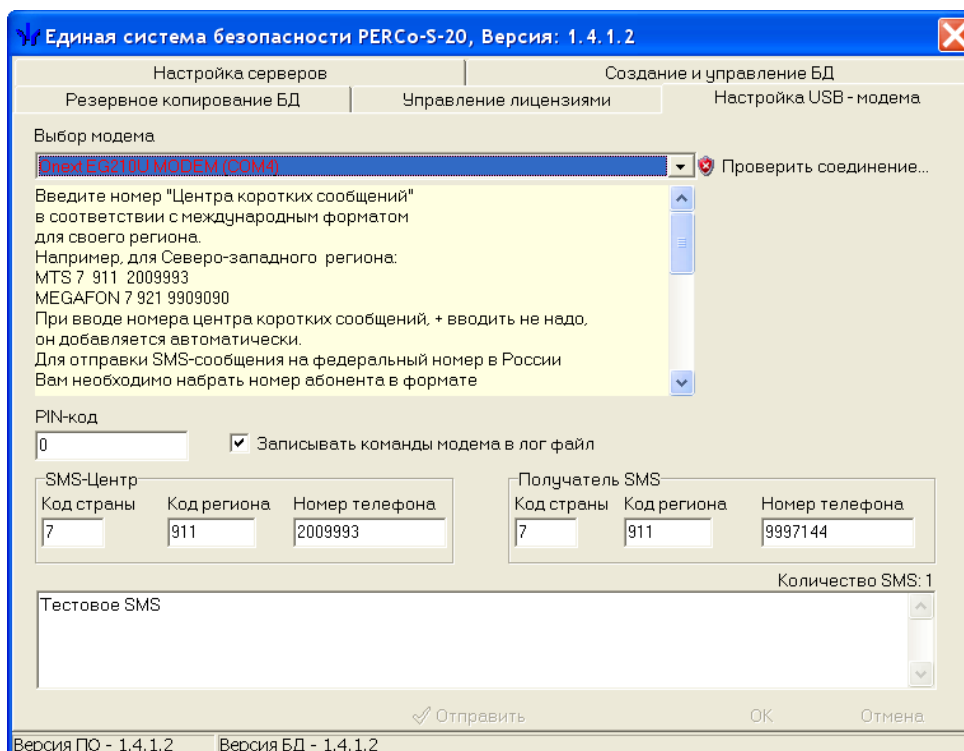
Полчатель SMS

Код страны: 8 Код региона: 911 Номер телефона: 9991744 Когда посылать: В случае ошибки

ОК Отмена

Функциональные элементы окна настройки почтовой рассылки уведомлений аналогичны описанным выше функциональным элементам окна настройки рассылки по сети.

НАСТРОЙКА USB – МОДЕМА



Для использования модема при посылки уведомлений сохранения базы или рассылки СМС сообщений при предъявлении карты доступа или иного события или состояния устройств, необходимо предварительно его настроить. В качестве модема может выступать обычный сотовый телефон с встроенным модемом и возможностью подключением через USB порт компьютера, для рассылки уведомлений о сохранение данных его должно хватить, для массовой рассылки на десятки и сотни номеров необходимо использовать USB-модем.

Порядок настройки:

- Внимательно прочитать документацию по установке модема и установить ПО в соответствии с рекомендациями производителя.(при корректной установке у вас в Панель управления-Телефон и модем должна появится запись о установленном модеме)
- Запустить «Центр управления PERCo S-20» перейти на вкладку «Настройка USB-модема» и заполнить данные
- PIN код вводить нужно только если ваша SIM карта защищена.
- Записывать команды модема в лог файл необходимо при возникновении ошибок при использовании модема, для отсылки лога компании PERCo soft@perco.ru.
- Номер SMS-центра выясняется у оператора поставившего вам модем.
- Номер получателя вводится для проверки правильности настроек модема.

После завершения ввода настроек станет доступна кнопка отправить, нажмите на неё для проверки корректности настроек, при корректном вводе Получатель SMS должен получить SMS с набранным текстом.

ТРЕБОВАНИЯ К АППАРАТУРЕ

Компьютеры:

Объем дискового пространства:

- ✓ Сервер системы: 100 Гб.
- ✓ Сервер видеонаблюдения: Для хранения видеоизображения не менее 300 Гб.
- ✓ Станция: 1 Гб.

Оперативная память:

- ✓ Сервер системы: 3 Гб.
- ✓ Сервер видеонаблюдения: 3 Гб.
- ✓ Станция: 2 Гб.

Процессор:

- ✓ Сервер системы: не ниже Pentium 4
- ✓ Сервер видеонаблюдения: не ниже Pentium 4
- ✓ Станция: не ниже Celeron 2.5 ГГц
- ✓ Операционная система: Windows 2000 Prof., Windows 2003.
- ✓ Для станции Windows XP, Windows 2000 Prof., Windows 2003.
- ✓ Для сервера системы и сервера видеонаблюдения допустимо использование 64 битных версий операционных систем.

Сеть: 100 Mbit,

Рекомендуемые GSM USB-модемы HUAWEI от операторов Мегафон и МТС и ONEXT USB GSM modem,

Камеры и видеосервера.

ПРИЛОЖЕНИЕ 1. События

СОБЫТИЯ, ЗАПИСЫВАЕМЫЕ В ЖУРНАЛ РЕГИСТРАЦИИ.

События контроллера доступа.

1. События, связанные с перемещением через ИУ

1.1. *Запрет прохода* с причиной:

- *идентификатор НЕ ЗАРЕГИСТРИРОВАН* – предъявленный идентификатор никогда не передавался в контроллер, то есть ему не назначались права доступа в этот контроллер;
- *идентификатор ЗАПРЕЩЁН* - доступ предъявленному идентификатора явным образом запрещен в контроллере, то есть данный контроллер включен в список доступа предъявленного идентификатора с явным запрещением проходов;
- *идентификатор из СТОП-ЛИСТА* - предъявленный идентификатор занесен в «СТОП-ЛИСТ»;
- *идентификатор ПРОСРОЧЕН* — у предъявленного идентификатора истек срок действия, указанный в параметрах доступа;
- *нарушение ВРЕМЕНИ* - у данного контроллера установлен «жесткий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* - у данного контроллера установлена «жесткая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* - это комбинация двух причин, описанных выше: нарушение ВРЕМЕНИ и нарушение ЗОНАЛЬНОСТИ;
- *нарушение КОМИССИОНИРОВАНИЯ* - было зафиксировано несоответствие с коммиссионировающим идентификатором или коммиссионирование не было выполнено вообще;
- *запрет по команде от ДУ* - охранник пультом ДУ подал команду на запрет прохода, после того, как контроллер разрешил проход;
- *запрет по команде от ПО* - оператор с ПК подал команду на запрет прохода, после того, как контроллер разрешил проход;
- *отказ в подтверждении от ВЕРИФИКАЦИИ* - не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение РЕЖИМОВ РАБОТЫ* – у данного контроллера установлен такой режим работы, при котором доступ по предъявленному идентификатору запрещен (режимы «ЗАКРЫТО» и «ОХРАНА»);

1.2. *Отказ от прохода* - отказ от предоставленного системой права пройти через ИУ по идентификатору.

1.3. *Проход* — событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером права пройти через него и до истечения времени удержания ИУ в открытом состоянии, без каких-либо выявленных нарушений.

1.4. *Проход с причиной нарушения:*

- *нарушение ВРЕМЕНИ* – у данного контроллера установлен «мягкий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* – у данного контроллера установлена «мягкая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ и нарушение ЗОНАЛЬНОСТИ*;
- *нарушение КОМИССИОНИРОВАНИЯ* – было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВРЕМЕНИ и КОМИССИОНИРОВАНИЯ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ и нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ЗОНАЛЬНОСТИ и КОМИССИОНИРОВАНИЯ* – это комбинация двух причин, описанных выше: *нарушение ЗОНАЛЬНОСТИ и нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ВРЕМЕНИ, ЗОНАЛЬНОСТИ и КОМИССИОНИРОВАНИЯ* – это комбинация трех причин, описанных выше: *нарушение ВРЕМЕНИ, нарушение ЗОНАЛЬНОСТИ и нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ВЕРИФИКАЦИИ* – в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен в другом направлении и по другому считывателю;
- *нарушение ВРЕМЕНИ и ВЕРИФИКАЦИИ* - в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен с *нарушением ВРЕМЕНИ* в другом направлении и по другому считывателю;
- *нарушение ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ* - в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен с *нарушением ЗОНАЛЬНОСТИ* в другом направлении и по другому считывателю;
- *нарушение ВРЕМЕНИ, ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ* - это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ и ВЕРИФИКАЦИИ и*

нарушение ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ;

1.5. *Проход, подтверждение от ДУ* – событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером с подтверждением от ДУ права прохода и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от ДУ осуществляется при условии, что стоят опции «подтверждения от ДУ» для верификации сотрудников либо посетителей на каждый считыватель:

- *при проходе*
- *при проходе с НАРУШЕНИЕМ ВРЕМЕНИ*
- *при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ*

1.6. *Проход с подтверждением от ДУ* и причиной нарушения:

- *нарушение ВРЕМЕНИ* – предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* – предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ и нарушение ЗОНАЛЬНОСТИ*;

1.7. *Проход, подтверждение от ВЕРИФИКАЦИИ* - событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером с подтверждением от верифицирующего устройства права прохода и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от верифицирующего устройства осуществляется в соответствии с параметрами, задаваемыми в модуле «ВЕРИФИКАЦИЯ » для верификации сотрудников либо посетителей на каждый считыватель:

- *при проходе;*
- *при проходе с НАРУШЕНИЕМ ВРЕМЕНИ;*
- *при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ ;*

1.8. *Проход с подтверждением от ВЕРИФИКАЦИИ* и причиной нарушения:

- *нарушение ВРЕМЕНИ* – предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* – предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ и нарушение ЗОНАЛЬНОСТИ*;

1.9. ИУ не закрыто после прохода (с фиксацией номера идентификатора). Событие возникает, если после прохода по идентификатору время активизации состояния контакта ИУ превысило установленное предельное время разблокировки. То есть, например, после открытия дверь остается в открытом состоянии в течение времени большем, чем время удержания в открытом состоянии, установленное для данного контроллера.

1.10. Проход по команде от ДУ. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ДУ права прохода и до истечения времени удержания ИУ в открытом состоянии.

1.11. Проход по команде от ПК. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ПК права прохода и до истечения времени удержания ИУ в открытом состоянии.

1.12. Проход по команде от ИК - пульта. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ИК - пульта права прохода и до истечения времени удержания ИУ в открытом состоянии.

1.13. Несанкционированный проход через ИУ (взлом ИУ). Событие, возникающее при активизации состояния контакта ИУ, не сопровождающегося санкционированным системой открытием ИУ. Механической разблокировки двери, турникета с последующим проходом через него.

2. События, связанные с изменением текущего состояния дополнительных входов

2.1. *Активизация входа* - вызывается срабатыванием устройства, подключенного к данному дополнительному входу.

2.2. *Нормализация входа* – вызывается отключением устройства (переходом в нормальное состояние), подключенного к данному дополнительному входу.

3. События, связанные с изменением текущего состояния дополнительных выходов

3.1. *Активизация выхода*. Событие происходит в случае подачи контроллером управляющего сигнала на дополнительный выход. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

3.2. *Нормализация выхода*. Событие происходит в случае снятия контроллером управляющего сигнала с дополнительного выхода. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

4. События, связанные с изменением текущего состояния корпуса контроллера

4.1. Корпус контроллера открыт. Событие происходит в случае вскрытия корпуса контроллера.

4.2. Корпус контроллера закрыт. Событие происходит при закрытии корпуса контроллера.

5. События, связанные с работоспособностью сетевых каналов контроллера

Система безопасности взаимодействует с любым контроллером по 3 сетевым каналам. Для нормальной работы контроллера требуется, чтобы все 3 сетевых канала были открыты:

- ✓ *канал управления* — служит для передачи команд управления от системы безопасности к контроллеру. С данным каналом связаны следующие события:
- *Канал управления ОТКРЫТ* — событие возникает при открытии канала управления сервером системы;
 - *Канал управления ЗАКРЫТ* — событие возникает при закрытии канала управления сервером системы;
 - *Канал управления НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала управления сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу управления другим программным обеспечением (например, локальным ПО);
 - *Канал управления неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом управления контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
 - *Канал управления НЕ АВТОРИЗИРОВАН* — событие возникает при невозможности сервера системы получить авторизованный доступ к контроллеру. Причиной, вызывающей такое событие, является наличие установленного пароля в контроллере, отличного от передаваемого пароля на этот контроллер системой безопасности;
 - *Ожидание открытия канала управления* - событие возникает при постановке в очередь сервера системы запроса на открытие канала управления;
 - *Отмена ожидания открытия канала управления* - событие возникает при удалении из очереди сервера системы запроса на открытие канала управления;
 - *Попытка открытия канала управления* — событие уведомляет о начале операции по открытию канала управления сервером системы;
 - *Нарушение связи с каналом управления* — событие возникает при отсутствии связи между сервером системы и каналом управления контроллера в течении 2 мин.;
 - *Нет ответа на выполнение команды по каналу управления* — событие возникает в случае отсутствия ответа от контроллера в течении 6 мин. на выполнение команды сервером системы;
- ✓ *канал мониторинга* — служит для получения системой безопасности журнала мониторинга контроллера. С данным каналом связаны следующие события:
- *Канал мониторинга ОТКРЫТ* — событие возникает при открытии канала мониторинга сервером системы;
 - *Канал мониторинга ЗАКРЫТ* — событие возникает при закрытии канала мониторинга сервером системы;
 - *Канал мониторинга НЕ ОТКРЫТ* — событие возникает при невозможности

открытия канала мониторинга сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу мониторинга другим программным обеспечением (например, локальным ПО);

- *Канал мониторинга неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом мониторинга контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
- *Попытка открытия канала мониторинга* — событие уведомляет о начале операции по открытию канала мониторинга сервером системы;
- *Нарушение связи с каналом мониторинга* — событие возникает при отсутствии связи между сервером системы и каналом мониторинга контроллера в течении 2 мин.;

✓ *канал регистрации* - служит для получения системой безопасности журнала регистрации контроллера. С данным каналом связаны следующие события:

- *Канал регистрации ОТКРЫТ* — событие возникает при открытии канала регистрации сервером системы;
- *Канал регистрации ЗАКРЫТ* — событие возникает при закрытии канала регистрации сервером системы;
- *Канал регистрации НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала регистрации сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу регистрации другим программным обеспечением (например, локальным ПО);
- *Канал регистрации неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом регистрации контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
- *Попытка открытия канала регистрации* — событие уведомляет о начале операции по открытию канала регистрации сервером системы;
- *Нарушение связи с каналом регистрации* — событие возникает при отсутствии связи между сервером системы и каналом регистрации контроллера в течении 2 мин.

6. События, связанные с изменением текущего состояния контроллеров или системы

6.1. *Включение или выключение питания контроллера.* Выключение питания может возникнуть в двух случаях: или при штатном выключении блока питания контроллера, или при аварийном выключении, связанным с аварией сети и разрядом аккумулятора. Включение питания возникает аналогично выключению в двух случаях:

или при штатном включении блока питания контроллера, или при восстановлении сетевого питания.

6.2. *Нарушение или восстановление связи с контроллером.* Эти события относятся к разряду диагностических и отражают возможное нарушение и восстановление работоспособности структурных элементов системы. Такие события возникают при нарушении связи между программным обеспечением системы безопасности и контроллером. Через 2 минуты отсутствия связи по одному из каналов контроллера, соединение по всем каналам будет закрыто. События генерируется при нарушении связи с

- каналом управления;
- каналом мониторинга;
- каналом регистрации;

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

6.4. *Переполнение списка идентификаторов.* Событие появляется в случае, если из-за внутренней ошибки программного обеспечения в контроллер передано количество карт доступа, превышающее его ресурсы.

6.5. *Ошибка принятого сообщения.* Событие возникает в случае невозможности контроллера правильно декодировать принятые от программного обеспечения сообщения. Может быть вызвано ошибками сети Ethernet.

6.6. *Перезапуск контроллера.* Событие возникает в случае решения контроллера о поведении аппаратного сброса. Данные события носят диагностический характер:

- внешний сброс;
- сброс по WatchDog.

6.7. *Неисправность контроллера.* Приведенные ниже события носят диагностический характер и содержат информацию о выходе из строя составляющих контроллера:

- памяти FRAM;
- памяти DataFlash;
- памяти SRAM;
- часов RTC;
- шины I2C.

6.8. *Форматирование памяти событий.* Приведенные ниже события содержат информацию об изменении состояния внутренней памяти контроллера и носят диагностический характер:

- область журнала событий;

- *область списка карт;*
- *область установок конфигурации;*
- *область программ;*
- *область текущих установок.*

6.9. *Изменение режима работы (РР) по команде от ПО.* Событие регистрируется контроллером при изменении режима работы оператором из программного обеспечения.

6.10. *Изменение РР на/с РР «Охрана».* Событие возникает при постановке/снятии с охраны группы ресурсов, в которую входит ИУ. Выход из РР «Охрана» производится в РР «Контроль».

6.11. *Изменение РР по команде от ИК.* Событие регистрируется при смене режима контроля доступа в результате команды получаемой контроллером управления доступом от ИК пульта управления.

6.12. *Тревога по команде от ИК-пульта.* Событие регистрируется при получении команды поднятия тревоги от ИК пульта управления..

6.13. *Авария или восстановление питания.* Авария возникает в случае понижения напряжения питания контроллера ниже уровня 10 вольт. Восстановление происходит в случае установления нормального уровня напряжения - 12 вольт.

6.14. *Тревога или сброс тревоги по команде от ПО.* События связаны с возникновением тревожной ситуации в системе (см. параметры генератора тревоги) и сбросом сигнала тревоги оператором системы под управлением ПО "Управление системой" или активизацией дополнительного входа сброса тревоги.

6.15. *Тревога по вскрытию корпуса извещателя.* Событие происходит в случае вскрытия корпуса извещателя, подключенного к шлейфам ОПС, при условии, что извещатель имеет датчик вскрытия корпуса.

6.16. *Корпус извещателя закрыт.* Событие возникает при закрытии предварительно открытого корпуса извещателя, подключенного к шлейфам ОПС, при условии, что извещатель имеет датчик вскрытия корпуса.

7. События, связанные с изменениями состояний группы ресурсов

7.1. *ГР взята на охрану по идентификатору.* Событие возникает при взятии на охрану всей группы ресурсов по идентификатору с соответствующими правами. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Охрана».

7.2. *ГР снята с охраны по идентификатору.* Событие возникает при снятии с охраны группы ресурсов по идентификатору с соответствующими правами. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Контроль».

7.3. *Попытка взятия ГР на охрану (невозможно взять) по идентификатору.* Событие возникает при попытке взятия на охрану по идентификатору группы ресурсов:

- *нарушение состояния дополнительного входа.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние дополнительного входа было не нормализовано. Например, датчик движения, подключенный к данному дополнительному входу, находится в активном состоянии;
- *нарушение состояния ресурса ИУ.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние ресурса ИУ было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе постановки группы ресурсов на охрану было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВЕРИФИКАЦИИ.* Событие возникает, если в процессе постановки группы ресурсов на охрану не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение ВРЕМЕНИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану группы ресурсов без ИУ и являющегося нарушителем по времени;
- *нарушение ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану группы ресурсов и являющегося нарушителем зональности;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану группы ресурсов и являющегося нарушителем и по времени и зональности;
- *отказ от постановки.* Событие возникает, если после поднесения к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану группы ресурсов и до истечения времени удержания ИУ в открытом состоянии, этот идентификатор не был поднесен повторно.

7.4. *Попытка снятия ГР с охраны (невозможно снять) по идентификатору.*
Событие возникает при попытке снятия с охраны по идентификатору группы ресурсов:

- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе снятия группы ресурсов с охраны было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВЕРИФИКАЦИИ.* Событие возникает, если в процессе снятия группы ресурсов с охраны не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение ВРЕМЕНИ.* Событие возникает при поднесении к контроллеру,

находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и являющегося нарушителем по времени;

- *нарушение ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и являющегося нарушителем зональности;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и являющегося нарушителем и по времени и по зональности;
- *отказ от снятия.* Событие возникает, если после поднесения к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и до истечения времени удержания ИУ в открытом состоянии этот идентификатор не был поднесен повторно.

7.5. *Невзятие ГР на охрану по идентификатору.* Событие возникает, если после попытки взятия группы ресурсов на охрану по идентификатору один или несколько из входящих в нее ресурсов окажется в состоянии «невзятие».

7.6. *ГР взята на охрану по идентификатору, подтверждение от ВЕРИФИКАЦИИ.* Событие возникает при взятии на охрану всех ресурсов группы ресурсов по идентификатору с соответствующими правами и с подтверждением от верифицирующего устройства. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Охрана».

7.7. *ГР снята с охраны по идентификатору, подтверждение от ВЕРИФИКАЦИИ.* Событие возникает при снятии с охраны группы ресурсов по идентификатору с соответствующими правами и с подтверждением от верифицирующего устройства. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Контроль».

7.8. *ГР взята на охрану по команде от ПО.* Событие возникает при взятии на охрану всей группы ресурсов по команде оператора ПК. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Охрана».

7.9. *ГР снята с охраны по команде от ПО.* Событие возникает при снятии с охраны группы ресурсов по команде оператора ПК. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Контроль».

7.10. *Попытка взятия ГР на охрану (невозможно взять) по команде от ПО.* Событие возникает при попытке взятия на охрану по команде оператора ПК группы ресурсов:

- *нарушение состояния дополнительного входа.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние данного дополнительного входа было не нормализовано;
- *нарушение состояния ИУ.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние ресурса ИУ было не нормализовано.

7.11. *Невзятие ГР на охрану по команде от ПО.* Событие возникает, если после попытки взятия группы ресурсов на охрану по команде оператора ПК один или несколько из входящих в нее ресурсов окажутся в состоянии «невзятие».

7.12. *Тихая тревога по ГР.* Событие возникает, если один или несколько ресурсов, входящих в группу ресурсов, перейдут в состояние «Тихая тревога».

7.13. *Тревога по ГР.* Событие возникает, если один или несколько ресурсов, входящих в группу ресурсов, перейдут в состояние «Тревога».

7.14. *Сброс тревоги по ГР по команде от ПО.* Событие возникает, при начале процедуры сброса тревоги всей группы ресурсов по команде оператора от ПК.

7.15. *Взятие ГР на охрану по идентификатору.* Событие возникает при начале процедуры взятия на охрану всей группы ресурсов по идентификатору с соответствующими правами (идет задержка взятия).

7.16. *Взятие группы ресурсов на охрану по команде оператора.* Событие возникает при начале процедуры взятия на охрану всей группы ресурсов по команде оператора (идет задержка взятия).

8. События, связанные с изменением текущего состояния ресурсов, входящих в группу ресурсов

8.1. *Невзятие на охрану ресурса "Шлейф сигнализации".* Событие возникает, если в момент взятия группы ресурсов на охрану состояние входящего в нее ШС окажется не нормализованным. ШС перейдет в состояние «невзятие».

8.2. *Взят на охрану ресурс.* Событие возникает при переходе ресурса в состояние «взят» с указанием типа ресурса:

- ресурс "Дополнительный вход";
- ресурс "ИУ";
- ресурс "Шлейф сигнализации".

8.3. *Взятие на охрану ресурса.* Событие возникает в момент взятия группы ресурсов на охрану: для ИУ – всегда, для ШС - если установлено не нулевое значение параметра «Задержка взятия на Охрану»:

- ресурс "ИУ";
- ресурс "Шлейф сигнализации".

8.4. *Снят с охраны ресурс.* Событие возникает при переходе ресурса в состояние «снят» с указанием типа ресурса:

- ресурс "Дополнительный вход";
- ресурс "ИУ";
- ресурс "Шлейф сигнализации".

8.5. *Неисправность снятого ресурса "Шлейф сигнализации".* Событие возникает, если величина сопротивления ШС, у которого параметр «задержка восстановления нарушенного ШС в снятом состоянии» отличен от значений 0 либо 255, и не

находящегося в режиме «Охрана», не находится в пределах от 2 до 10 кОм, либо изменилось более чем на 10% в течение часа.

8.6. *Нормализация снятого ресурса "Шлейф сигнализации"*. Событие возникает при нормализации состояния ШС, находившегося в состоянии «неисправность снятого ШС».

8.7. *Нарушение ресурса, состояние «Тревога»*. Событие возникает при переходе ресурса в состояние «Тревога»:

- ресурс *"Дополнительный вход"*
- ресурс *"ИУ"*
- ресурс *"Шлейф сигнализации"*

8.8. *Нарушение ресурса, состояние «Тихая тревога»*. Событие возникает при переходе ресурса в состояние «Тихая тревога»:

- ресурс *"Шлейф сигнализации"*

8.9. *Восстановление ресурса*. Событие возникает при нормализации состояния ресурса, находящегося в состоянии «Тревога» с указанием типа ресурса:

- ресурс *"Шлейф сигнализации"*

8.10. *Сброс тревоги ресурса*. Событие возникает при сбросе тревоги по ресурсу:

- ресурс *"Дополнительный вход"*
- ресурс *"ИУ"*;
- ресурс *"Шлейф сигнализации"*

8.11. *Автономный сброс сирены*. Событие возникает при сбросе сирены по входу автономного сброса сирены.

События КБО и ППКОП

1. События, связанные с перемещением через ИУ (только КБО)

1.1. *Запрет прохода* с причиной:

- *идентификатор НЕ ЗАРЕГИСТРИРОВАН* – предъявленный идентификатор никогда не передавался в контроллер, то есть ему не назначались права доступа в этот контроллер;
- *идентификатор ЗАПРЕЩЁН* - доступ предъявленному идентификатора явным образом запрещен в контроллере, то есть данный контроллер включен в список доступа предъявленного идентификатора с явным запрещением проходов;
- *идентификатор из СТОП-ЛИСТА* - предъявленный идентификатор занесен в «СТОП-ЛИСТ»;

- *идентификатор ПРОСРОЧЕН* — у предъявленного идентификатора истек срок действия, указанный в параметрах доступа;
- *нарушение ВРЕМЕНИ* - у данного контроллера установлен «жесткий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* - у данного контроллера установлена «жесткая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* - это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;
- *нарушение КОМИССИОНИРОВАНИЯ* - было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *запрет по команде от ДУ* - охранник пультом ДУ подал команду на запрет прохода, после того, как контроллер разрешил проход;
- *запрет по команде от ПО* - оператор с ПК подал команду на запрет прохода, после того, как контроллер разрешил проход;
- *отказ в подтверждении от ВЕРИФИКАЦИИ* - не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение РЕЖИМОВ РАБОТЫ* – у данного контроллера установлен такой режим работы, при котором доступ по предъявленному идентификатору запрещен (режимы «ЗАКРЫТО» и «ОХРАНА»);

1.2. *Отказ от прохода* - отказ от предоставленного системой права пройти через ИУ по идентификатору.

1.3. *Проход* — событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером права пройти через него и до истечения времени удержания ИУ в открытом состоянии, без каких-либо выявленных нарушений.

1.4. *Проход с причиной нарушения:*

- *нарушение ВРЕМЕНИ* – у данного контроллера установлен «мягкий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* – у данного контроллера установлена «мягкая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;

- *нарушение КОМИССИОНИРОВАНИЯ* – было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВРЕМЕНИ и КОМИССИОНИРОВАНИЯ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ЗОНАЛЬНОСТИ и КОМИССИОНИРОВАНИЯ* – это комбинация двух причин, описанных выше: *нарушение ЗОНАЛЬНОСТИ* и *нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ВРЕМЕНИ, ЗОНАЛЬНОСТИ и КОМИССИОНИРОВАНИЯ* – это комбинация трех причин, описанных выше: *нарушение ВРЕМЕНИ*, *нарушение ЗОНАЛЬНОСТИ* и *нарушение КОМИССИОНИРОВАНИЯ* ;
- *нарушение ВЕРИФИКАЦИИ* – в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен в другом направлении и по другому считывателю;
- *нарушение ВРЕМЕНИ и ВЕРИФИКАЦИИ* - в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен с *нарушением ВРЕМЕНИ* в другом направлении и по другому считывателю;
- *нарушение ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ* - в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен с *нарушением ЗОНАЛЬНОСТИ* в другом направлении и по другому считывателю;
- *нарушение ВРЕМЕНИ, ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ* - это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ и ВЕРИФИКАЦИИ* и *нарушение ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ*;

1.5. *Проход, подтверждение от ДУ* – событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером с подтверждением от ДУ права прохода и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от ДУ осуществляется при условии, что стоят опции «подтверждения от ДУ» для верификации сотрудников либо посетителей на каждый считыватель:

- *при проходе*
- *при проходе с НАРУШЕНИЕМ ВРЕМЕНИ*
- *при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ*

1.6. *Проход с подтверждением от ДУ и причиной нарушения:*

- *нарушение ВРЕМЕНИ* – предъявленный идентификатор не удовлетворяет

указанному в правах доступа временному критерию доступа;

- *нарушение ЗОНАЛЬНОСТИ* – предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: нарушение ВРЕМЕНИ и нарушение ЗОНАЛЬНОСТИ;]

1.7. *Проход, подтверждение от ВЕРИФИКАЦИИ* - событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером с подтверждением от верифицирующего устройства права прохода и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от верифицирующего устройства осуществляется в соответствии с параметрами, задаваемыми в модуле «ВЕРИФИКАЦИЯ » для верификации сотрудников либо посетителей на каждый считыватель:

- *при проходе;*
- *при проходе с НАРУШЕНИЕМ ВРЕМЕНИ;*
- *при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ;*

1.8. *Проход с подтверждением от ВЕРИФИКАЦИИ* и причиной нарушения:

- *нарушение ВРЕМЕНИ* – предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* – предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ и нарушение ЗОНАЛЬНОСТИ;*

1.9. *ИУ не закрыто после прохода (с фиксацией номера идентификатора).* Событие возникает, если после прохода по идентификатору время активизации состояния контакта ИУ превысило установленное предельное время разблокировки. То есть, например, после открытия дверь остается в открытом состоянии в течение времени большем, чем время удержания в открытом состоянии, установленное для данного контроллера.

1.10. *Проход по команде от ДУ.* Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ДУ права прохода и до истечения времени удержания ИУ в открытом состоянии.

1.11. *Проход по команде от ПК.* Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ПК права прохода и до истечения времени удержания ИУ в открытом состоянии.

1.12. *Проход по команде от ИК - пульта.* Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ИК - пульта права прохода и до истечения времени удержания ИУ в открытом состоянии.

1.13. *Несанкционированный проход через ИУ (взлом ИУ).* Событие, возникающее при активизации состояния контакта ИУ, не сопровождающегося

санкционированным системой открытием ИУ. Механической разблокировки двери, турникета с последующим проходом через него.

2. События, связанные с изменением текущего состояния дополнительных выходов

2.1. *Активизация выхода.* Событие происходит в случае подачи контроллером управляющего сигнала на дополнительный выход. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

2.2. *Нормализация выхода.* Событие происходит в случае снятия контроллером управляющего сигнала с дополнительного выхода. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

2.3. *Запуск задержки активизации выхода.* Только для выхода типа «ОПС». Событие происходит в случае подачи контроллером управляющего сигнала на дополнительный выход, если параметр выхода «Задержка перед запуском» не равен 0. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

2.4. *КЗ на выходе.* Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, в если на выходе обнаружено короткое замыкание.

2.5. *Обрыв на выходе.* Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, если на выходе обнаружен обрыв.

2.6. *Активизация выхода невозможна, КЗ.* Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, если на выходе обнаружено короткое замыкание при попытке контроллера подать управляющий сигнал на данный выход.

2.7. *Восстановление выхода.* Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, если после сброса контроллера на выходе не обнаружены никакие неисправности.

3. События, связанные с изменением текущего состояния корпуса контроллера

3.1. *Корпус контроллера открыт.* Событие происходит в случае вскрытия корпуса контроллера.

3.2. *Корпус контроллера закрыт.* Событие происходит при закрытии корпуса контроллера.

4. События, связанные с работоспособностью сетевых каналов контроллера

Система безопасности взаимодействует с любым контроллером по 3 сетевым каналам. Для нормальной работы контроллера требуется, что бы все 3 сетевых канала были открыты:

- ✓ *канал управления* — служит для передачи команд управления от системы

безопасности к контроллеру. С данным каналом связаны следующие события:

- *Канал управления ОТКРЫТ* — событие возникает при открытии канала управления сервером системы;
 - *Канал управления ЗАКРЫТ* — событие возникает при закрытии канала управления сервером системы;
 - *Канал управления НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала управления сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу управления другим программным обеспечением (например, локальным ПО);
 - *Канал управления неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом управления контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
 - *Канал управления НЕ АВТОРИЗИРОВАН* — событие возникает при невозможности сервера системы получить авторизованный доступ к контроллеру. Причиной, вызывающей такое событие, является наличие установленного пароля в контроллере, отличного от передаваемого пароля на этот контроллер системой безопасности;
 - *Ожидание открытия канала управления* - событие возникает при постановке в очередь сервера системы запроса на открытие канала управления;
 - *Отмена ожидания открытия канала управления* - событие возникает при удалении из очереди сервера системы запроса на открытие канала управления;
 - *Попытка открытия канала управления* — событие уведомляет о начале операции по открытию канала управления сервером системы;
 - *Нарушение связи с каналом управления* — событие возникает при отсутствии связи между сервером системы и каналом управления контроллера в течении 2 мин.;
 - *Нет ответа на выполнение команды по каналу управления* — событие возникает в случае отсутствия ответа от контроллера в течении 6 мин. на выполнение команды сервером системы;
- ✓ *канал мониторинга* — служит для получения системой безопасности журнала мониторинга контроллера. С данным каналом связаны следующие события:
- *Канал мониторинга ОТКРЫТ* — событие возникает при открытии канала мониторинга сервером системы;
 - *Канал мониторинга ЗАКРЫТ* — событие возникает при закрытии канала мониторинга сервером системы;
 - *Канал мониторинга НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала мониторинга сервером системы. Причиной, вызывающей такое

событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу мониторинга другим программным обеспечением (например, локальным ПО);

- *Канал мониторинга неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом мониторинга контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
 - *Попытка открытия канала мониторинга* — событие уведомляет о начале операции по открытию канала мониторинга сервером системы;
 - *Нарушение связи с каналом мониторинга* — событие возникает при отсутствии связи между сервером системы и каналом мониторинга контроллера в течении 2 мин.;
- ✓ *канал регистрации* - служит для получения системой безопасности журнала регистрации контроллера. С данным каналом связаны следующие события:
- *Канал регистрации ОТКРЫТ* — событие возникает при открытии канала регистрации сервером системы;
 - *Канал регистрации ЗАКРЫТ* — событие возникает при закрытии канала регистрации сервером системы;
 - *Канал регистрации НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала регистрации сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу регистрации другим программным обеспечением (например, локальным ПО);
 - *Канал регистрации неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом регистрации контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
 - *Попытка открытия канала регистрации* — событие уведомляет о начале операции по открытию канала регистрации сервером системы;
 - *Нарушение связи с каналом регистрации* — событие возникает при отсутствии связи между сервером системы и каналом регистрации контроллера в течении 2 мин.

5. События, связанные с изменением текущего состояния контроллеров или системы

5.1. *Включение или выключение питания контроллера.* Выключение питания может возникнуть в двух случаях: или при штатном выключении блока питания контроллера, или при аварийном выключении, связанным с аварией сети и разрядом аккумулятора. Включение питания возникает аналогично выключению в двух случаях: или при штатном включении блока питания контроллера, или при восстановлении сетевого питания.

5.2. *Нарушение или восстановление связи с контроллером.* Эти события относятся к разряду диагностических и отражают возможное нарушение и восстановление работоспособности структурных элементов системы. Такие события возникают при нарушении связи между программным обеспечением системы безопасности и контроллером. Через 2 минуты отсутствия связи по одному из каналов контроллера, соединение по всем каналам будет закрыто. События генерируется при нарушении связи с

- *каналом управления;*
- *каналом мониторинга;*
- *каналом регистрации;*

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

5.4. *Переполнение списка идентификаторов.* Событие появляется в случае, если из-за внутренней ошибки программного обеспечения в контроллер передано количество карт доступа, превышающее его ресурсы.

5.5. *Ошибка принятого сообщения.* Событие возникает в случае невозможности контроллера правильно декодировать принятые от программного обеспечения сообщения. Может быть вызвано ошибками сети Ethernet.

5.6. *Сбой физического уровня Ethernet.* Событие происходит в случае обнаружения внутренних ошибок в сети Ethernet.

5.7. *Перезапуск контроллера.* Событие возникает в случае решения контроллера о поведении аппаратного сброса. Данные события носят диагностический характер:

- *внешний сброс;*
- *сброс по WatchDog.*

5.8. *Неисправность контроллера.* Приведенные ниже события носят диагностический характер и содержат информацию о выходе из строя составляющих контроллера:

- *памяти FRAM;*
- *памяти DataFlash;*
- *памяти SRAM;*
- *часов RTC;*
- *шины I²C;*
- *ошибки сопроцессора;*

5.9. *Форматирование памяти событий.* Приведенные ниже события содержат информацию об изменении состояния внутренней памяти контроллера и носят диагностический характер:

- *область журнала событий;*
- *область списка карт;*
- *область установок конфигурации;*
- *область программ;*
- *область текущих установок.*

5.10. *Изменение режима работы (РР) по команде от ПО (только для КБО).* Событие возникает при изменении режима работы оператором из программного обеспечения.

5.11. *Установлен режим работы "Открыто" по команде от ПЗ (только для КБО).* Событие возникает при установке режима работы «Открыто», если пожарная зона перешла в режим «ПОЖАР» или «ВНИМАНИЕ».

5.12. *Изменение РР на/с РР «Охрана» (только для КБО).* Событие возникает при постановке/снятии с охраны охранной зоны, в которую входит ИУ. Выход из РР «Охрана» производится в РР «Контроль».

5.13. *Изменение РР по команде от ИК (только для КБО).* Событие регистрируется при смене режима контроля доступа в результате команды получаемой контроллером управления доступом от ИК пульта управления.

5.14. *Тревога по команде от ИК-пульта (только для КБО).* Событие регистрируется при получении команды поднятия тревоги от ИК пульта управления..

5.15. *Авария или восстановление питания.* Авария возникает в случае понижения напряжения питания контроллера ниже уровня 10 вольт. Восстановление происходит в случае установления нормального уровня напряжения в 12 вольт.

5.16. *Тревога или сброс тревоги по команде от ПО (только для КБО).* События связаны с возникновением тревожной ситуации в системе (см. параметры генератора тревоги) и сбросом сигнала тревоги оператором системы под управлением ПО "Управление системой" или активизацией дополнительного входа сброса тревоги.

5.17. *Автономный сброс тревоги по кнопке.* Событие возникает при нажатии на кнопку «СБРОС» на БУИ.

5.18. *Автономное отключение звука по кнопке.* Событие возникает при нажатии на кнопку «ОТКЛ ЗВУКА» на БУИ.

5.19. *Переход на резерв ИП.* Событие возникает при активизации входа «Переход на РИП», подключенного к резервному источнику питания.

5.20. *Разряд батареи ИП.* Событие возникает при активирован вход «Разряд ИП» или напряжение питания менее 10.5 В при активизированном входе «Переход на РИП».

5.21. *Утечка на землю в ШС.* Событие возникает при условии, что сопротивление между цепью GND на плате контроллера и «землём» меньше 20 кОм.

5.22. *Восстановление после утечки на землю в ШС.* Событие возникает при условии, что сопротивление между цепью GND на плате контроллера и «землём» больше 20 кОм.

5.23. *Кнопки заблокированы.* Событие возникает через 20 с после последнего нажатия на любую кнопку БУИ, при условии, что кнопки БУИ были разблокированы.

5.24. *Кнопки разблокированы.* Событие возникает после выполнения последовательности действий, приводящих к разблокировке кнопок БУИ.

5.25. *Сброс от кнопки запущен.* Событие возникает при начале процедуры сброса, инициированной нажатием на кнопку «СБРОС» на БУИ.

5.26. *Сброс по команде от ПО запущен.* Событие возникает при начале процедуры сброса, инициированной командой оператора от ПО.

5.27. *Нарушение или восстановление связи с БУИ.* События возникают при нарушении или восстановлении связи с БУИ.

5.28. *Неисправность ИП +18В.* Событие возникает в случае выхода напряжения питания ШС за рабочий диапазон.

5.29. *Восстановление ИП +18В.* Событие возникает в случае возврата напряжения питания ШС в рабочий диапазон.

5.30. *Питание нестабильно (только ППКОП).* Событие возникает при частых переключениях питания с основного (~220 В) источника питания на резервный (батарея) источник питания.

5.31. *Питание стабильно (только ППКОП).* Событие возникает при стабилизации источника питания.

5.32. *Нарушение связи с концентратором АИР (только ППКОП).* Событие возникает при нарушении связи с концентратором ПЦН «АИР». Причиной, вызывающей такое событие, может быть физическое отсутствие связи с концентратором в сети либо проблемы с концентратором.

5.33. *Восстановление связи с концентратором АИР (только ППКОП).* Событие возникает при восстановлении связи с концентратором ПЦН «АИР».

6. События, связанные с изменениями состояний зон

6.1. *ОЗ взята на охрану.* Событие возникает при переходе охранной зоны (ОЗ) в режим «ОХРАНА». Если с ОЗ связано ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Охрана». Имеются следующие уточнения:

- *по идентификатору* - если идентификатор имеет соответствующие права.
- *по идентификатору*, подтверждение от ВЕРИФИКАЦИИ - если было подтверждения от верифицирующего устройства.
- *по команде от ПО* - после выполнения команды оператором ПО.

- *по кнопке* - по кнопке на БУИ;
- *безусловно от ПЦН (только для ППКОП)* - если ПЦН взял зону на охрану;
- *по команде оператора ПЦН (только для ППКОП)*- если оператор ПЦН взял зону на охрану;
- по идентификатору с верификацией от ПЦН (только для ППКОП) - *если было подтверждение от ПЦН, как от верифицирующего устройства;*

6.2. *ОЗ снята с охраны.* Событие возникает при переходе охранной зоны (ОЗ) в режим «СНЯТА». Если с ОЗ связано ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Контроль». Имеются следующие уточнения:

- *по идентификатору* - если идентификатор имеет соответствующие права;
- *по идентификатору, подтверждение от ВЕРИФИКАЦИИ* - если было подтверждения от верифицирующего устройства;
- *по команде от ПО* - после выполнения команды оператором ПО.
- *по кнопке* - по кнопке на БУИ;
- *по команде от ПЗ* — если пожарная зона (ПЗ) перешла в режим «ПОЖАР» или «ВНИМАНИЕ». Конкретное условия снятия ОЗ с охраны зависит от значения параметра ПЗ **Переводить ИУ в режим «Открыто»**;
- *безусловно от ПЦН (только для ППКОП)* - если ПЦН снял зону с охраны;
- *по команде оператора ПЦН (только для ППКОП)* - если оператор ПЦН снял зону с охраны;
- по идентификатору с верификацией от ПЦН (только для ППКОП) - *если было подтверждение от ПЦН, как от верифицирующего устройства;*

6.3. *Попытка взятия ОЗ на охрану (невозможно взять) по идентификатору.* Событие возникает при попытке взятия охранной зоны на охрану по идентификатору:

- *нарушение состояния ИУ.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ИУ, связанного с этой ОЗ, было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение состояния ШС.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ШС, включенного в эту ОЗ, было не нормализовано;
- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе взятия ОЗ на охрану было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВЕРИФИКАЦИИ.* Событие возникает, если в процессе взятия ОЗ на охрану не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение ВРЕМЕНИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану

и являющегося нарушителем по времени;

- *нарушение ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и являющегося нарушителем зональности;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и являющегося нарушителем и по времени и зональности;
- *отказ от постановки.* Событие возникает, если после поднесения к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и до истечения времени удержания ИУ в открытом состоянии, этот идентификатор не был поднесен повторно.

6.4. *Попытка снятия ОЗ с охраны (невозможно снять) по идентификатору.* Событие возникает при попытке снятия ОЗ с охраны по идентификатору:

- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе снятия ОЗ с охраны было зафиксировано несоответствие с комисионирующим идентификатором или комисионирование не было выполнено вообще;
- *нарушение ВЕРИФИКАЦИИ.* Событие возникает, если в процессе снятия ОЗ с охраны не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение ВРЕМЕНИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны и являющегося нарушителем по времени;
- *нарушение ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны и являющегося нарушителем зональности;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и являющегося нарушителем и по времени и по зональности;
- *отказ от снятия.* Событие возникает, если после поднесения к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой и до истечения времени удержания ИУ в открытом состоянии, этот идентификатор не был поднесен повторно.

6.5. *Попытка взятия ОЗ на охрану (невозможно взять) по команде от ПО.* Событие возникает при попытке взятия охранной зоны на охрану по команде от оператора ПО:

- *нарушение состояния ИУ.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ИУ, связанного с этой ОЗ, было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение состояния ШС.* Событие возникает, если в процессе взятия ОЗ на

охрану состояние ШС, включенного в эту ОЗ, было не нормализовано;

6.6. *Попытка взятия ОЗ на охрану (невозможно взять) по кнопке.* Событие возникает при попытке взятия охранной зоны на охрану по кнопке на БУИ:

- *нарушение состояния ИУ.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ИУ, связанного с этой ОЗ, было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение состояния ШС.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ШС, включенного в эту ОЗ, было не нормализовано;

6.7. *Тихая тревога по ОЗ.* Событие возникает при переходе ОЗ в режим «ТРЕВОГА» (при нарушении любого ОШС) и если установлен параметр конфигурации зоны **Не активизировать при тревоге по Охранным шлейфам сигнализации выходы, работающие по программам «Сирена» и «Лампа».**

6.8. *Тревога по ОЗ.* Событие возникает при переходе ОЗ в режим «ТРЕВОГА» (при нарушении любого ОШС) и если не установлен параметр конфигурации зоны **Не активизировать при тревоге по Охранным шлейфам сигнализации выходы, работающие по программам «Сирена» и «Лампа».**

6.9. *Сброс тревоги по ОЗ по команде от ПО.* Событие возникает при сбросе тревоги на ОЗ по команде оператора от ПО. Причем ОЗ режим не меняет, а индикация на БУИ для нарушенных ОШС этой зоны будет отличаться от нормализованных

6.10. *Взятие ОЗ на охрану.* Событие возникает при попытке перехода охранной зоны (ОЗ) в режим «ОХРАНА». Имеются следующие уточнения:

- *по идентификатору* - если идентификатор имеет соответствующие права;
- *по команде от ПО* - по команде от оператора ПО;
- *по кнопке* - по кнопке на БУИ;

6.11. *ПЗ снята с контроля.* Событие возникает при снятии с контроля ПЗ и переходе ее в режим «СНЯТА». Имеются следующие уточнения:

- *по команде от ПО* - по команде от оператора ПО;
- *по кнопке* - по кнопке на БУИ;
- *безусловно от ПЦН во время сброса при взятии УОО (только для ППКОП) — во время автоматического сброса ПЦН при взятии УОО на охрану;*
- *по команде оператора ПЦН во время сброса при взятии УОО (только для ППКОП) - во время сброса ПЦН по команде оператора при взятии УОО на охрану;*
- *по идентификатору с верификацией от ПЦН во время сброса при взятии УОО (только для ППКОП) - по идентификатору с подтверждением от ПЦН, как от верифицирующего устройства во время сброса ПЦН по команде оператора при взятии УОО на охрану;*

6.12. *ПЗ взята на контроль.* Событие возникает при взятии на контроля ПЗ и переходе ее в режим «НОРМА». Имеются следующие уточнения:

- *по команде от ПО* - по команде от оператора ПО;
- *по кнопке* - по кнопке на БУИ;
- *автоматически, в составе УОО (только для ППКОП) - при взятии на охрану УОО от ПЦН «АИР» в состав которого входит ПЗ зона;*

6.13. *ПЗ перешла в режим.* Событие возникает при переходе ПЗ в конкретный режим. Имеются следующие уточнения:

- *«Неисправность»* - ПЗ перешла в режим «Неисправность»;
- *«Внимание»* - ПЗ перешла в режим «Внимание»;
- *«Пожар»* - ПЗ перешла в режим «Пожар»;
- *«Норма»* - ПЗ перешла в режим «Норма» после сброса из одного из режимов: «Неисправность», «Внимание» или «Пожар»;

6.14. *Отказ от взятия ОЗ на охрану (только для ППКОП).* Событие возникает при попытке взятия охранной зоны на охрану:

- *по идентификатору с верификацией от ПЦН*, неверный идентификатор. Событие возникает, если в процессе взятия ОЗ на охрану по идентификатору не было подтверждения от ПЦН, как от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *по команде оператора ПЦН, нарушены ШС.* Событие возникает, если в процессе взятия ОЗ на охрану по команде оператора ПЦН состояние ШС, включенного в эту ОЗ, было не нормализовано;

6.15. *Отказ от снятия ОЗ с охраны (только для ППКОП).* Событие возникает при попытке снятия охранной зоны с охраны:

- *по идентификатору в режиме "ТРЕВОГА" с верификацией от ПЦН.* Событие возникает, если в процессе снятия ОЗ с охраны по идентификатору в режиме "ТРЕВОГА" не было подтверждения от ПЦН, как от верифицирующего устройства или верифицирующее устройство выдало запрет;

6.16. *Сброс ОЗ по команде постановки УОО от ПЦН (только для ППКОП).* Событие возникает при постановке на охрану УОО от ПЦН «АИР»;

6.17. *Сброс ПЗ по команде постановки УОО от ПЦН (только для ППКОП).* Событие возникает при постановке на охрану УОО от ПЦН «АИР»;

6.18. *Зона КТС взята на охрану.* Событие возникает при переходе зоны КТС в режим «ОХРАНА». Имеются следующие уточнения:

- *по команде от ПО* - после выполнения команды оператором ПО;
- *при взятии УОО (только для ППКОП) - если ПЦН берет УОО на охрану;*

6.19. *Зона КТС снята с охраны.* Событие возникает при переходе зоны КТС в режим «СНЯТА». Имеются следующие уточнения:

- *по команде от ПО - после выполнения команды оператором ПО;*

6.20. *Тревога по зоне КТС.* Событие возникает при переходе зоны КТС в режим «ТРЕВОГА» при нарушении любого шлейфа КТС;

6.21. *Сброс тревоги по зоне КТС.* Событие возникает при сбросе тревоги на зоне КТС. Причем, зона КТС режим не меняет, а индикация на БУИ для нарушенных шлейфов КТС этой зоны будет отличаться от нормализованных;

7. События, связанные с изменением текущего состояния ШС, входящих в ОЗ, КТС и ПЗ

7.1. *ОШС не взят на охрану, переход в режим "Автоперевзятие".* Событие возникает, если в момент взятия ШС на охрану его состояние окажется не нормализованным. ШС перейдет в состояние «Автоперевзятие».

7.2. *ОШС взят на охрану.* Событие возникает, если ОШС перешел в режим «ОХРАНА».

7.3. *КТС взят на охрану.* Событие возникает, если шлейф КТС перешел в режим «ОХРАНА».

7.4. *ОШС снят с охраны.* Событие возникает, если ОШС перешел в режим «СНЯТ».

7.5. *КТС снят с охраны.* Событие возникает, если шлейф КТС перешел в режим «СНЯТ».

7.6. *Взятие ОШС на охрану.* Событие возникает при переходе ОШС в режим «ВЗЯТИЕ».

7.7. *Взятие КТС на охрану.* Событие возникает при переходе шлейфа КТС в режим «ВЗЯТИЕ».

7.8. *ПШС отключен.* Событие возникает, если была передана новая конфигурация на ПШС, указывающая не использовать данный ПШС.

7.9. *ОШС отключен.* Событие возникает, если была передана новая конфигурация на ПШС, указывающая не использовать данный ОШС.

7.10. *Корпус извещателя вскрыт (ОШС).* Событие возникает, если на одном из охранных извещателей вскрыт корпус .

7.11. *Корпус извещателя закрыт (ОШС).* Событие возникает, если на одном из извещателей корпус закрыт после вскрытия.

7.12. *Неисправность снятого ОШС.* Событие возникает, если происходит нарушения ОШС в режиме «СНЯТ» и параметр конфигурации ОШС **Задержка восстановления нарушенного ОШС в снятом состоянии** отличен от нуля.

7.13. *Нормализация снятого ОШС.* Событие возникает, если происходит нормализация ОШС в режиме «СНЯТ» и параметр конфигурации ОШС **Задержка восстановления нарушенного ОШС в снятом состоянии** отличен от нуля.

7.14. *Нарушение ОШС, переход в режим "Тревога".* Событие возникает, если ОШС перешел в режим «ТРЕВОГА».

7.15. *Нарушение ОШС, переход в режим "Тихая тревога".* Событие возникает, если ОШС перешел в режим «ТРЕВОГА», а в ОЗ, включающей данный шлейф, установлен параметр конфигурации **Не активизировать при тревоге по Охранным шлейфам сигнализации выходы, работающие по программам «Сирена» и «Лампа».**

7.16. *Нарушение КТС, переход в режим "Тревога".* Событие возникает, если шлейф КТС перешел в режим «ТРЕВОГА».

7.17. *Нарушение ОШС в режиме "Тревога".* Событие возникает, если происходит повторное нарушение ОШС в режиме «ТРЕВОГА».

7.18. *Восстановление ОШС в режиме "Тревога".* Событие возникает, если происходит восстановление нарушенного ОШС в режиме «ТРЕВОГА».

7.19. *Сброс тревоги ОШС.* Событие возникает при сбросе тревоги на ОЗ, включающей данный ОШС.

7.20. *Нормализация КТС.* Событие возникает, если шлейф КТС перешел в режим «НОРМА».

7.21. *Сброс тревоги КТС.* Событие возникает при сбросе тревоги на зоне КТС, включающей данный шлейф КТС.

7.22. *Сброс питания нарушенного ОШС при сбросе ОЗ по команде постановки УОО (только для ППКОП).* Событие возникает при сбросе ОЗ, включающей данный ОШС по команде постановки УОО на охрану.

7.23. *Сброс питания нарушенного ПШС при сбросе ПЗ по команде постановки УОО (только для ППКОП).* Событие возникает при сбросе ПЗ, включающей данный ПШС по команде постановки УОО на охрану.

7.24. *ПШС перешел в режим "Норма".* Событие возникает, если ПШС перешел в режим «НОРМА».

7.25. *Неисправность ПШС, КЗ.* Событие возникает, если ПШС перешел в состояние «НЕИСПРАВНОСТЬ» по причине короткого замыкания.

7.26. *Неисправность ПШС, обрыв.* Событие возникает, если ПШС перешел в состояние «НЕИСПРАВНОСТЬ» по причине обрыва.

7.27. *ПШС, сработал 1 извещатель.* Событие возникает, если на ПШС сработал один извещатель.

7.28. *ПШС, сработало 2 извещателя.* Событие возникает, если на ПШС сработало два или более извещателей.

7.29. *Сброс ПШС по команде от ПО.* Событие возникает, если осуществлен сброс ПШС по команде оператора от ПО.

7.30. *Сброс ПШС по кнопке.* Событие возникает, если осуществлен сброс ПШС по кнопке от БУИ.

7.31. *Сброс ПШС при перезапросе.* Событие возникает, если .

7.32. *ПШС взят на контроль.* Событие возникает, если ПШС перешел в режим «ВЗЯТ».

7.33. *ПШС снят с контроля.* Событие возникает, если ПШС перешел в режим «СНЯТ».

7.34. *Взятие ПШС на контроль.* Событие возникает, если .

7.35. *ПШС перешел в режим "Внимание".* Событие возникает, если ПШС перешел в режим «ВНИМАНИЕ».

7.36. *ПШС перешел в режим "Пожар".* Событие возникает, если ПШС перешел в режим «ПОЖАР».

8. События, связанные с Устройствами охранными объектовыми (УОО) (только ППКОП)

8.1. *Сброс УОО начат.* Событие возникает при запуске сброса УОО ПЦН «АИР». Имеются следующие уточнения:

- *безусловно от ПЦН* — если ПЦН сбрасывает УОО;
- *по команде оператора ПЦН* - если оператор ПЦН сбрасывает УОО;
- *по идентификатору с верификацией от ПЦН* – перед постановкой на охрану УОО по идентификатору с верификацией от ПЦН;

9. События, связанные с изменением текущего состояния ИУ, входящих в ОЗ (только КБО)

9.1. *ИУ взят на охрану.* Событие возникает, если ОЗ перешла в режим «ОХРАНА».

9.2. *ИУ снят с охраны.* Событие возникает, если ОЗ перешла в режим «СНЯТА».

9.3. *Нарушение ИУ, переход в режим "Тревога".* Событие возникает, если ОЗ перешла в режим «ТРЕВОГА» из-за несанкционированной разблокировки ИУ.

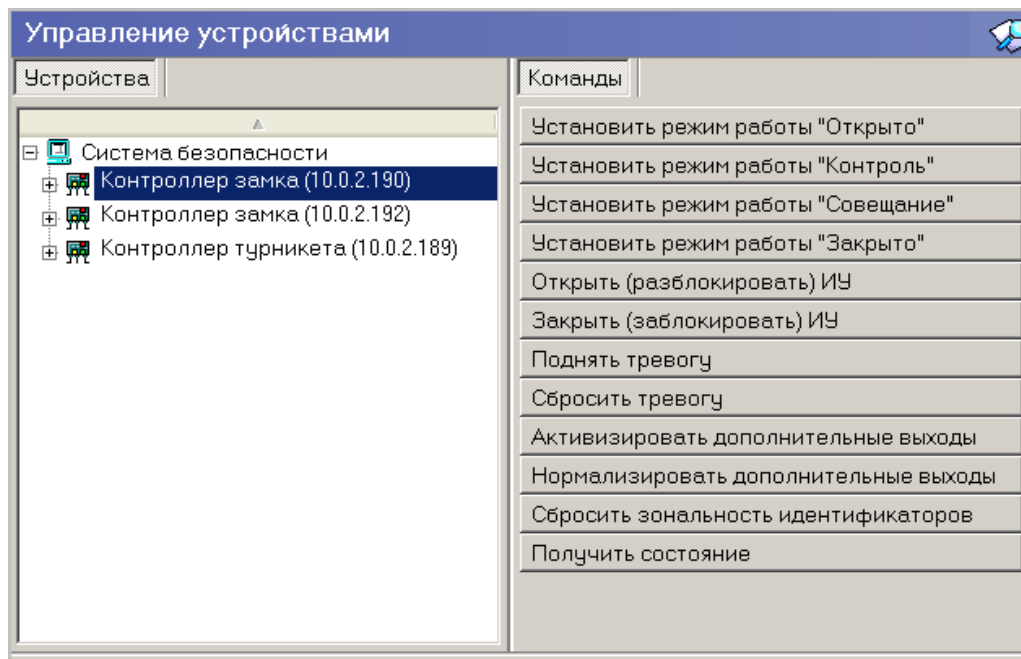
9.4. *Сброс тревоги ИУ.* Событие возникает при снятии ОЗ с охраны, если она до этого находилась в режиме «ТРЕВОГА».

КОМАНДЫ УПРАВЛЕНИЯ

Большинство устройств, входящих в единую систему безопасности PERCo-S-20, могут управляться из программного обеспечения. Для управления этими устройствами используются разделы Управление устройствами.

Ниже приведен список команд управления доступных для каждого типа устройств.

Контроллер управления доступом



1. **Установить режим работы «Открыто».** Приводит к разблокировке всех исполнительных устройств выбранного контроллера. Исполнительные устройства остаются разблокированными в течение всего времени, пока данный режим не будет сменен. Нажатие на кнопки ДУ исполнительных устройств игнорируются. При предъявлении карт доступа к считывателям данного контроллера регистрируются события о проходе или нарушении доступа. При этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.
2. **Установить режим работы «Контроль».** Приводит к блокировке всех исполнительных устройств выбранного контроллера. При нажатии на кнопку ПУ для данного направления или при поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ разблокируется на время равное времени удержания данного направления ИУ в открытом состоянии. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии.
3. **Установить режим работы «Совещание».** Аналогично режиму работы «Контроль» За исключением индикации на считывателях и блоке внутренней индикации. Более подробно об индикации режимов работы изложено в техническом описании системы безопасности.
4. **Установить режим работы «Закрыто».** При включении режима данное направление ИУ блокируется и остается заблокированным в течение всего времени пока режим включен. Нажатие на кнопку ДУ для данного направления игнорируется. Предъявление любой карты вызывает регистрацию события о нарушении прав доступа. Проход через ИУ (открытый механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании

соответствующих опций, включение сигнала тревоги.

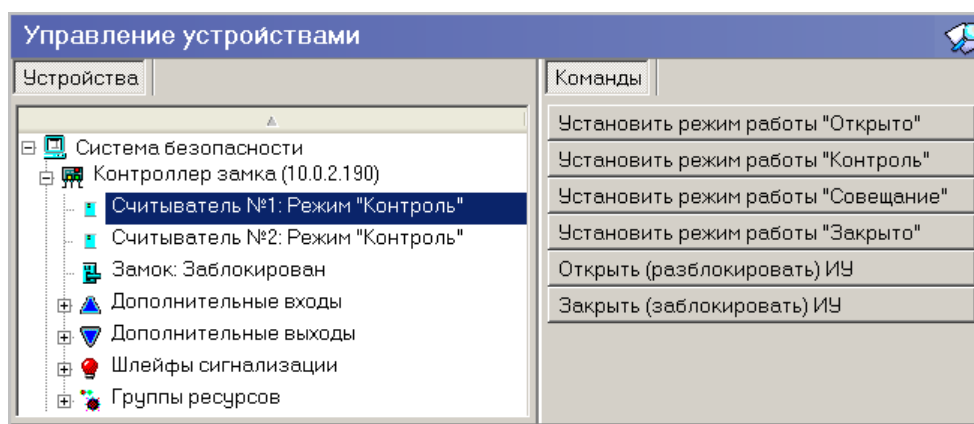
5. **Открыть (разблокировать) ИУ.** Приводит к разблокировке ИУ выбранного контроллера на указанное время .
6. **Заккрыть (заблокировать) ИУ.** Приводит к блокировке ИУ выбранного контроллера на указанное время
7. **Поднять тревогу.** Приводит к включению механизма реакции контроллера на возникновение тревожной ситуации. Параметры обработки тревожной ситуации для выбранного контроллера описываются в «*Генераторе тревоги*».
8. **Сбросить тревогу.** Приводит к прекращению выполнения контроллером механизма обработки тревожной ситуации.
9. **Активизировать дополнительные выходы.** Приводит к активизации всех релейных выходов выбранного контроллера.
10. **Нормализовать дополнительные выходы.** Приводит к нормализации всех релейных выходов данного контроллера.
11. **Сбросить зональность идентификаторов.** Приводит к сбросу зональности всех идентификаторов, связанных с выбранным контроллером. Эта команда тесно связана с параметром ИУ «*Внутренняя защита от передачи идентификаторов*», и имеет смысл, если этот параметр задействован. После выполнения данной команды всем идентификаторам будет присвоена зона 0.
12. **Получить состояние.** Выводит на экран отчет о состоянии контроллера на момент выполнения команды.



ПРИМЕЧАНИЕ

Невозможно воспользоваться командами «Открыть (разблокировать) ИУ» и «Заккрыть (заблокировать) ИУ» при установленных режимах работы «Открыто» и «Заккрыто».

Считыватель



1. **Установить режим работы «Открыто».** Приводит к разблокировке исполнительного устройства, связанного с выбранным считывателем. Исполнительное устройство остается разблокированным в течение всего времени

пока данный режим не будет сменен. Нажатие на кнопки ДУ исполнительного устройства игнорируются. При поднесении карты доступа к считывателю регистрируется событие о проходе или нарушении доступа. При этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.

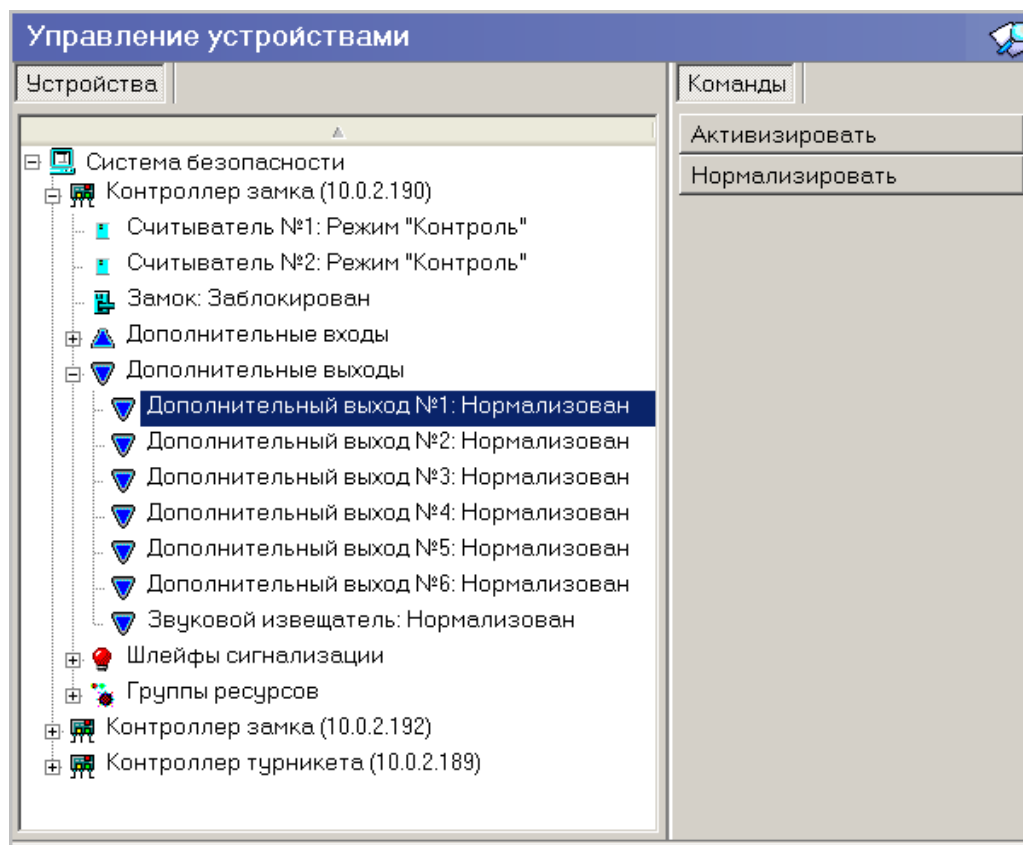
2. **Установить режим работы «Контроль».** Приводит к блокировке исполнительного устройства, связанного с выбранным считывателем. При нажатии на кнопку ДУ для данного направления или при поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ разблокируется на время, которое равно времени удержания данного направления ИУ в открытом состоянии. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии.
3. **Установить режим работы «Совещание».** Аналогично режиму работы «Контроль» за исключением индикации на считывателе и блоке внутренней индикации. Более подробно об индикации режимов работы изложено в техническом описании системы безопасности.
4. **Установить режим работы «Закрето».** При включении режима данное направление ИУ блокируется и остается заблокированным в течение всего времени пока режим включен. Нажатие на кнопку ДУ для данного направления игнорируется. Предъявление любой карты вызывает регистрацию события о нарушении прав доступа. Проход через ИУ (открытый механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.
5. **Открыть (разблокировать) ИУ.** Приводит к разблокировке выбранного считывателя на указанное время.
6. **Закреть (заблокировать) ИУ.** Приводит к блокировке выбранного считывателя на указанное время.



ПРИМЕЧАНИЕ

Невозможно воспользоваться командами «Открыть (разблокировать) ИУ» и «Закреть (заблокировать) ИУ» при установленных режимах работы «Открыто» и «Закрето».

Дополнительный выход



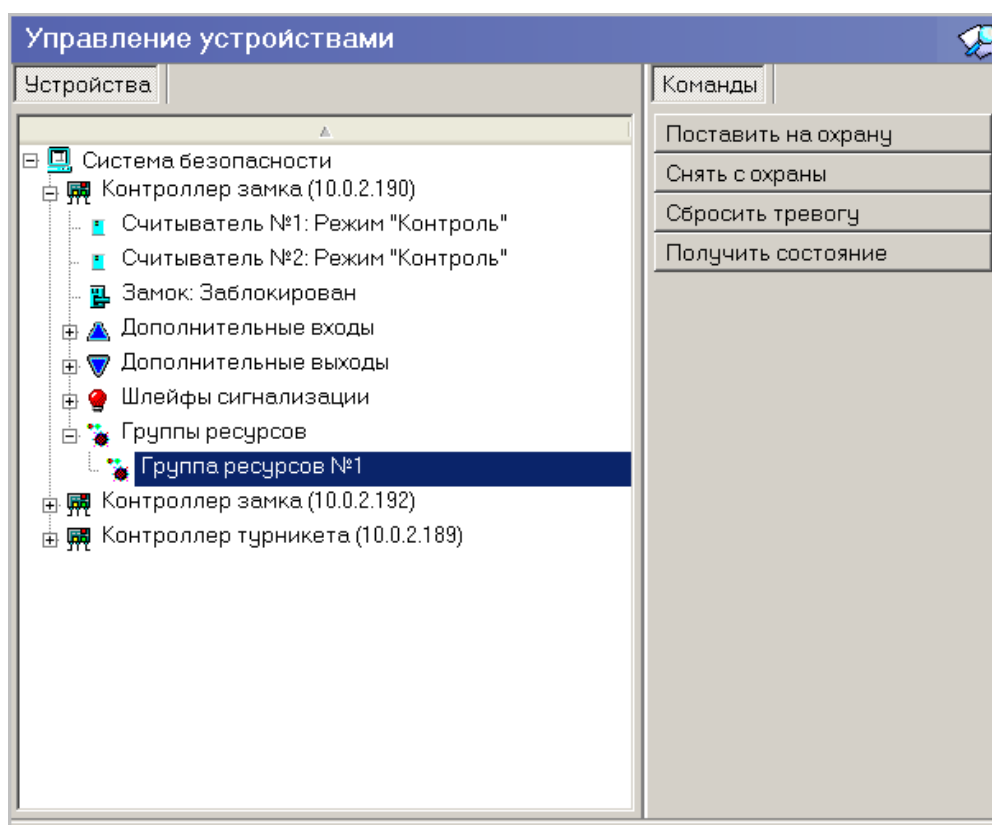
1. **Активизировать.** Приводит к переводу выбранного дополнительного выхода в активное состояние.
2. **Нормализовать.** Приводит к переводу выбранного дополнительного выхода в нормальное состояние.



ПРИМЕЧАНИЕ

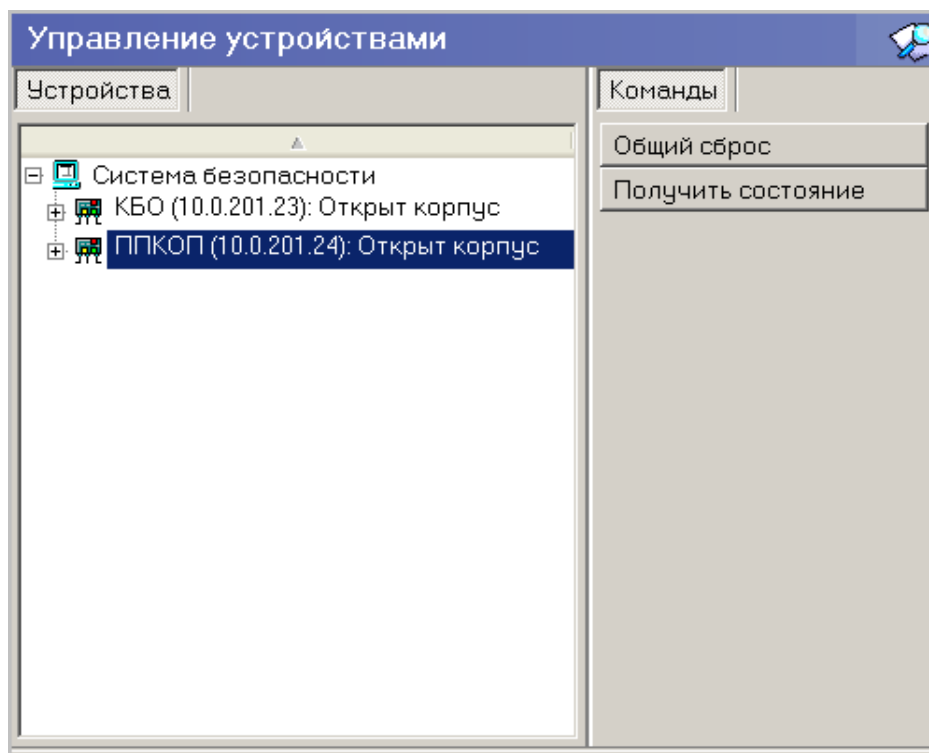
Если тип дополнительного выхода описан как ОПС или генератора тревоги, то попытка активировать или нормализовать этот выход приведет к ошибке – «Несоответствие типа ресурса».

Группа ресурсов



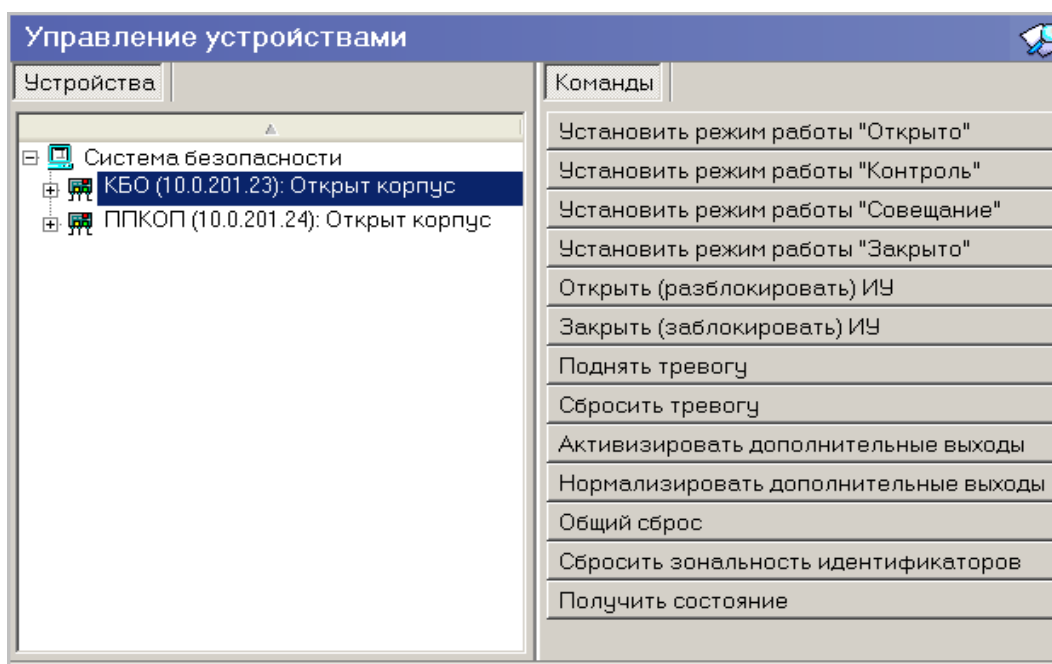
1. **Поставить на охрану.** Приводит к постановке выбранной группы ресурсов на охрану. Если в состав выбранной группы ресурсов входит исполнительное устройство (ИУ), то оно блокируется и остается заблокированным в течение всего времени пока режим включен. Нажатие на кнопку ДУ игнорируется. Открывание двери в режиме постановки на охрану вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги. Если по истечении времени выдачи сигнала тревоги дверь будет закрыта (вход Pass нормализуется), сигнал тревоги выключается. Иначе выдача сигнала тревоги продолжается до закрытия двери. Если в выбранную группу ресурсов входит шлейф охранной сигнализации, то ШС переходит в состояние «на охране». Если сопротивление ШС, устанавливаемого на охрану, не в норме, ШС переходит в состояние «не взятие» через время задержки, задаваемое при конфигурации. Для взятого на охрану ШС контроллер отслеживает сопротивление в его линии и принимает решение о его состоянии.
2. **Снять с охраны.** Происходит снятие группы ресурсов с охраны. Если в состав группы ресурсов входит ИУ, то контроллер переходит в режим работы «Контроль». Если в состав группы ресурсов входит шлейф сигнализации, контроллер перестает отслеживать сопротивление в его линии.
3. **Сбросить тревогу.** Приводит к сбросу тревоги и прекращению выполнения алгоритма обработки тревожной ситуации.
4. **Получить состояние.** Выводит на экран отчет о состоянии группы ресурсов на момент выполнения команды.

Контроллер ППКОП



1. **Общий сброс.** Приводит к сбросу контроллера при котором состояния всех ШС инициализируются, с ПШС снимается питание на время Задержка сброса ПШС, у ОЗ снимается тревога.
2. **Получить состояние.** Выводит на экран отчет о состоянии ресурсов контроллера на момент выполнения команды.

Контроллер КБО



1. **Установить режим работы «Открыто».** Приводит к разблокировке исполнительного устройства (ИУ) выбранного контроллера. ИУ остаются

разблокированными в течение всего времени, пока данный режим не будет изменен. Нажатие на кнопки ДУ исполнительным устройством игнорируются. При предъявлении карт доступа к считывателям данного контроллера регистрируются события о проходе или нарушении доступа. При этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.

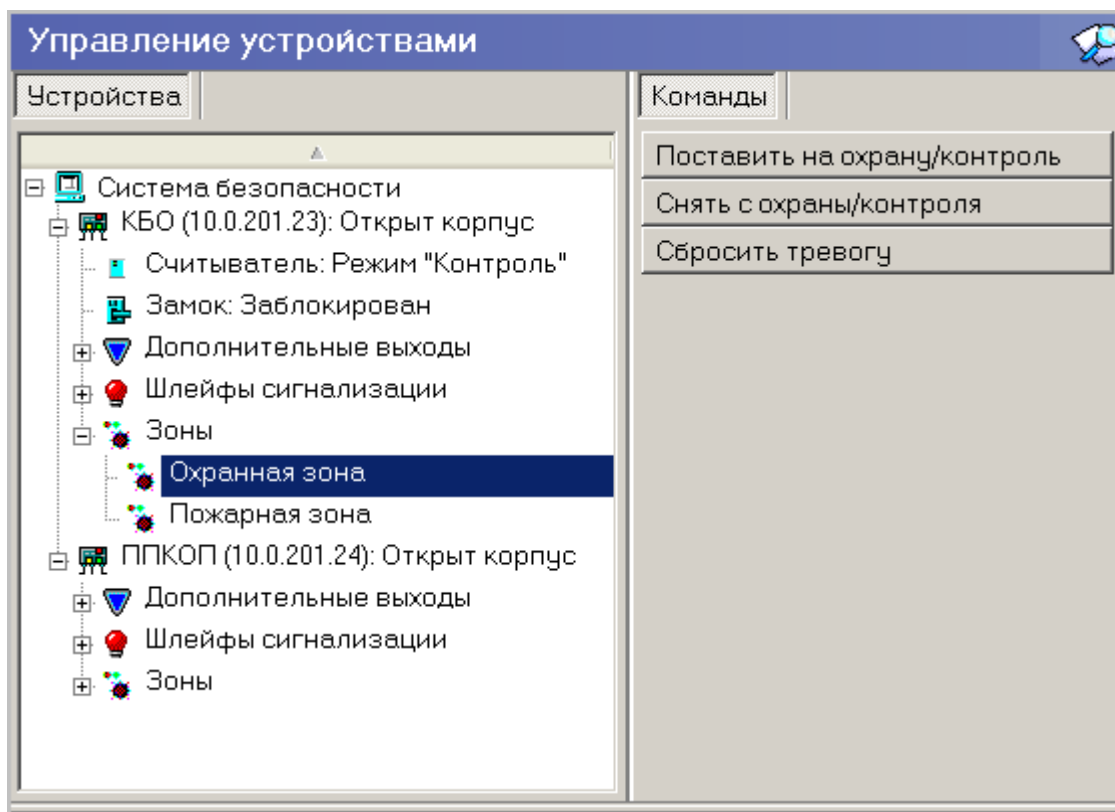
2. **Установить режим работы «Контроль».** Приводит к блокировке ИУ выбранного контроллера. При нажатии на кнопку ПУ для данного направления или при поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ разблокируется на время равное времени удержания данного направления ИУ в открытом состоянии. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии.
3. **Установить режим работы «Совещание».** Аналогично режиму работы «Контроль» За исключением индикации на считывателях и блоке внутренней индикации. Более подробно об индикации режимов работы изложено в техническом описании системы безопасности.
4. **Установить режим работы «Закрото».** Приводит к разблокировке исполнительного устройства (ИУ) выбранного контроллера. ИУ остаются заблокированными в течение всего времени, пока данный режим не будет изменен. Нажатие на кнопку ДУ исполнительным устройством игнорируется. Предъявление любой карты вызывает регистрацию события о нарушении прав доступа. Проход через ИУ (открытый механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.
5. **Открыть (разблокировать) ИУ.** Приводит к разблокировке ИУ выбранного контроллера на указанное время .
6. **Закреть (заблокировать) ИУ.** Приводит к блокировке ИУ выбранного контроллера на указанное время
7. **Поднять тревогу.** Приводит к запуску выбранным контроллером механизма реакции на возникновение тревожной ситуации. Параметры обработки тревожной ситуации для выбранного контроллера описываются в «Генераторе тревоги».
8. **Сбросить тревогу.** Приводит к прекращению выполнения выбранным контроллером механизма обработки тревожной ситуации.
9. **Активизировать дополнительные выходы.** Приводит к активизации всех дополнительных выходов выбранного контроллера.
10. **Нормализовать дополнительные выходы.** Приводит к нормализации всех дополнительных выходов выбранного контроллера.
11. **Сбросить зональность идентификаторов.** Приводит к сбросу зональности всех идентификаторов, связанных с выбранным контроллером. Этот команда тесно

связана с параметром ИУ «Внутренняя защита от передачи идентификаторов», и имеет смысл, если этот параметр задействован. После выполнения данной команды всем идентификаторам будет присвоена зона 0.

12. **Общий сброс.** Приводит к сбросу контроллера при котором состояния всех ШС инициализируются, с ПШС снимается питание на время Задержка сброса ПШС, у ОЗ снимается тревога.

13. **Получить состояние.** Выводит на экран отчет о состоянии ресурсов контроллера на момент выполнения команды.

Зона контроллера ППКОП (КБО)



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

2. **Снять с охраны/контроля.** Происходит снятие зоны с охраны/контроля. Если в состав зоны входит ИУ, то контроллер переходит в режим работы «Контроль». Если в состав зоны входит шлейф сигнализации, контроллер перестает отслеживать сопротивление в его линии.
3. **Сбросить тревогу.** Приводит к сбросу тревоги и прекращению выполнения алгоритма обработки тревожной ситуации.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Инсталляция	Учетные данные
Лицензия	Справочник
Контроллер	Подразделение
Сетевые настройки	Должность
Адрес	Сотрудник
DHCP	Доступ
Конфигурация	Параметры доступа
Параметры контроллеров	Управление устройствами
Тестовый вход	Сервер
Релейный выход	База данных
Исполнительное устройство	Резервная копия БД
Считыватель	Оптимизация индексов БД
Тревога	Пароль
Генератор тревоги	Мониторинг
Шлейф сигнализации	Проход
Группа ресурсов	Аппаратура
Защита от передачи идентификаторов	Событие
Помещение	Команды управления
Персонал	