Единая система S-20
Базовый комплект ПО
PERCo-SN01

РУКОВОДСТВО АДМИНИСТРАТОРА

Единая система S-20
Базовый комплект ПО

PERCo-SN01

Руководство администратора

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Единая система безопасности PERCo-S-20 (далее – система) предназначена для обеспечения безопасности объектов, повышения контроля трудовой и технологической дисциплины, а также автоматизации рабочих процессов на предприятии.

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.

1 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.

Так как передача данных в системе построена на основе сети Ethernet, то конфигурирование и проектирование системы на конкретном предприятии не должно вызвать осложнений. Поэтому можно с успехом использовать существующую инфраструктуру. Однако, исходя из специфичности решаемых системой PERCo-S-20 задач, настоятельно рекомендуется разделение существующей или создание отдельной сети Ethernet для контроллеров и серверов системы безопасности. При этом остальные модули ПО могут находиться в сети предприятия.

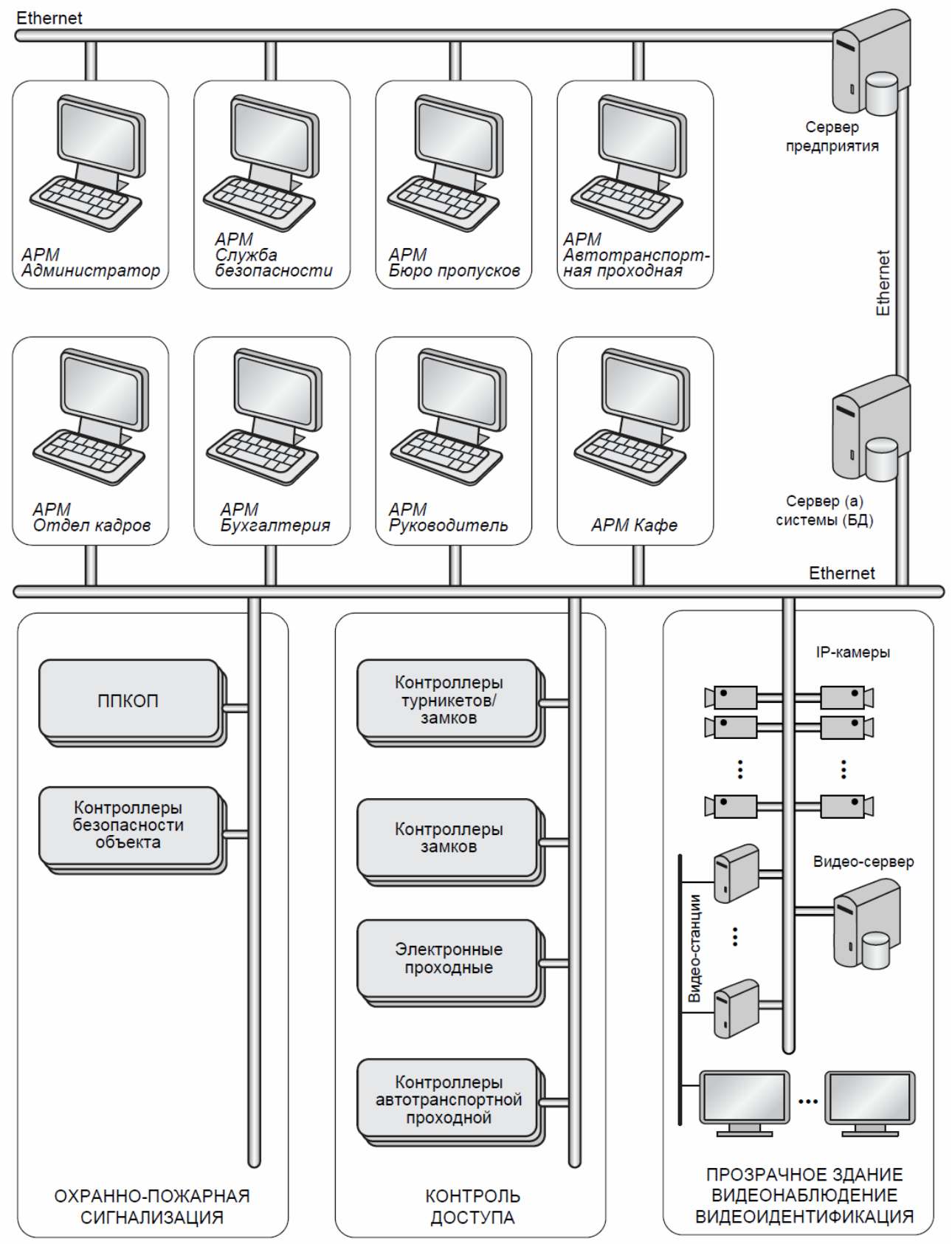


Рис. 1 Структурная схема системы PERCo-S-20

2 ПОРЯДОК ПОДГОТОВКИ СИСТЕМЫ К РАБОТЕ

Для осуществления подготовки системы к работе выполните следующие действия:

1. Разработайте структурную схему системы.
2. Выберите компьютеры, где будет установлен сервер системы и сервер БД, и будут работать модули ПО PERCo-S-20.
3. Проведите инсталляцию ПО в соответствии с разработанной схемой.
4. Запустите **Центр управления PERCo-S-20**. На данном этапе осуществите подключение к серверу БД и создание базы данных.
   - Для запуска сервера системы и создания-управления базой данных необходимо и достаточно установить только **Базовую версию ПО**.
   - Запуск Центра управления серверами системы PERCo-S-20 производится путем открытия файла **MainCenter17k.cpl** (или ярлык **Центр управления PERCo-S-20** на рабочем столе). После открытия файла на вкладке **Настройка серверов** запустите **FireBird SQL сервер** и **Сервер системы**. Далее перейдите на вкладку **Создание и управление БД**, где в режиме **Создание базы данных** задайте расположение БД и ее архивов и затем щелкните на кнопке **Создать базу**.
5. Запустите **Консоль управления PERCo-S-20** (для регистрации подразделов программы) с помощью **Console17k.exe** (или ярлык **Консоль управления PERCo-S-20** на рабочем столе).
6. Задайте права доступа пользователей к программному обеспечению системы. На данном этапе определите пользователей системы, задайте их права доступа к подразделам программного обеспечения и присвойте им индивидуальные пароли.
7. Настройте контроллеры в соответствии с топологией Вашей сети Ethernet. При необходимости настройте DHCP сервер.
8. Проведите 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.

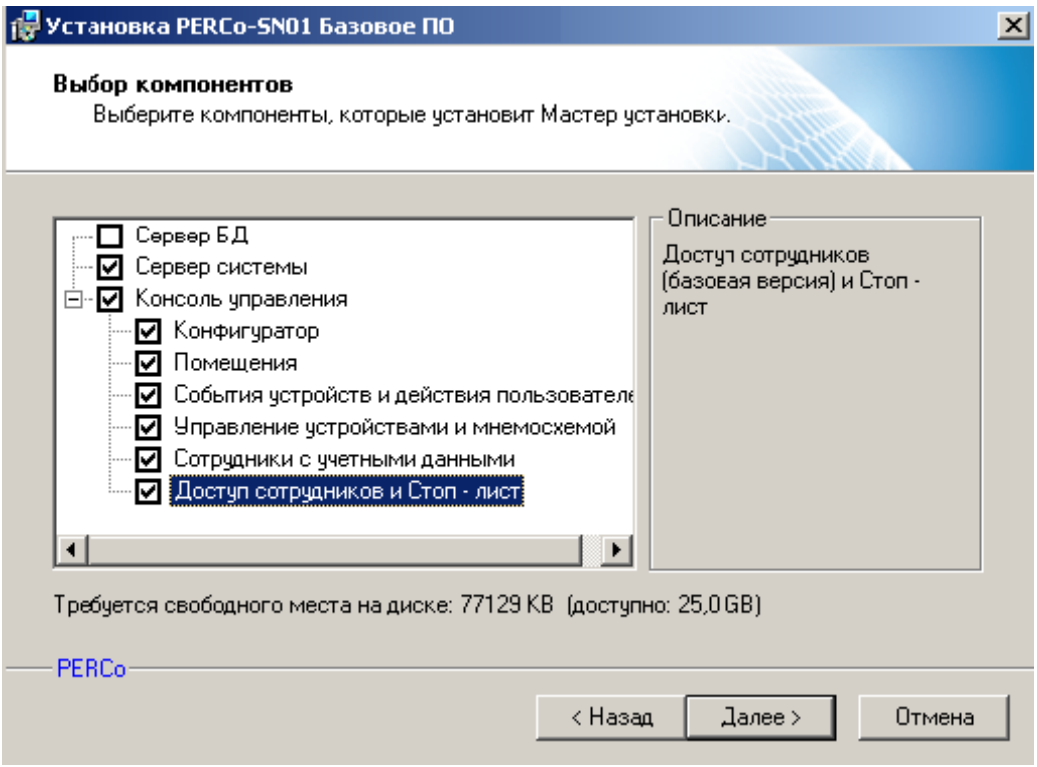
После проведения всех необходимых операций по настройке системы администратору рекомендуется задать себе пароль для входа в нее. Данная процедура необходима для установки эксклюзивного права администратора изменять настройки системы.

3 ИНСТАЛЛЯЦИЯ ПО

Перед началом инсталляции программного обеспечения ознакомьтесь с разработанной структурной схемой системы безопасности. Определите, на какие PC и какие модули программного обеспечения необходимо проинсталлировать.

3.1 Инсталляция PERCo-SN01 «Базовое ПО»

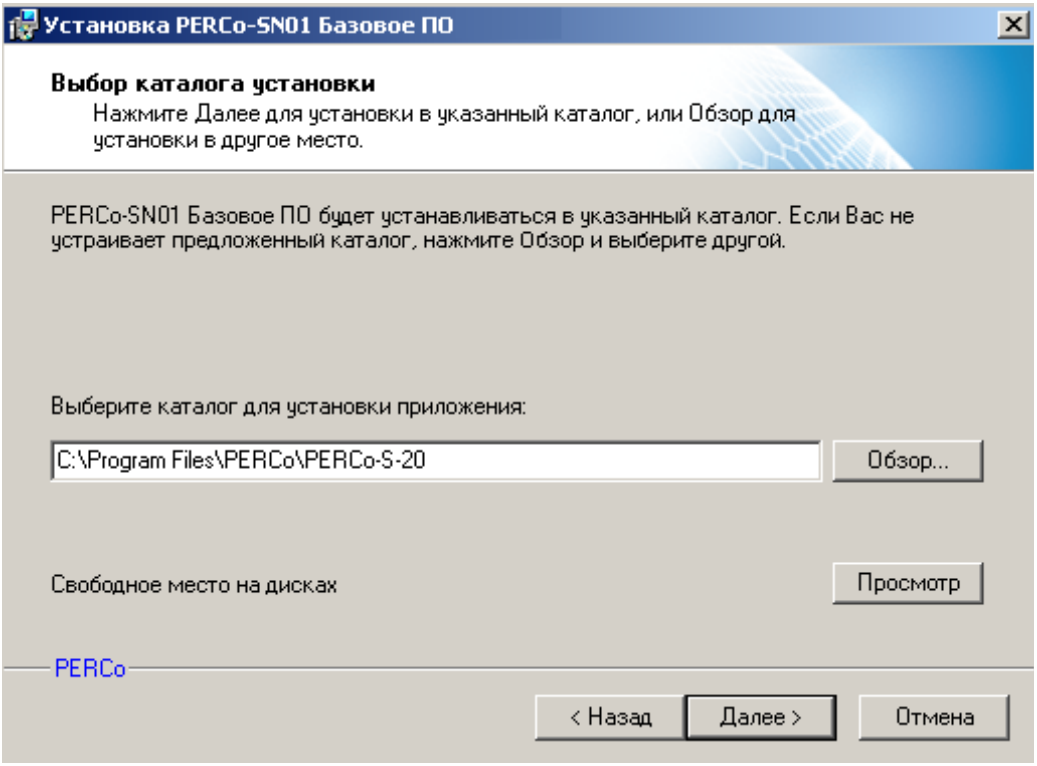
Вставьте компакт диск с дистрибутивом в привод CD-ROM. Должен автоматически запуститься инсталляционный модуль SetupBase.exe. Если этого не происходит – запустите данный модуль вручную. Следуйте указаниям мастера установки. Внимательно ознакомьтесь с предлагаемой информацией и лицензионным соглашением. 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 PC. 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 разделе *«Управление серверами»* данного Руководства администратора.

3.2 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

4 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.

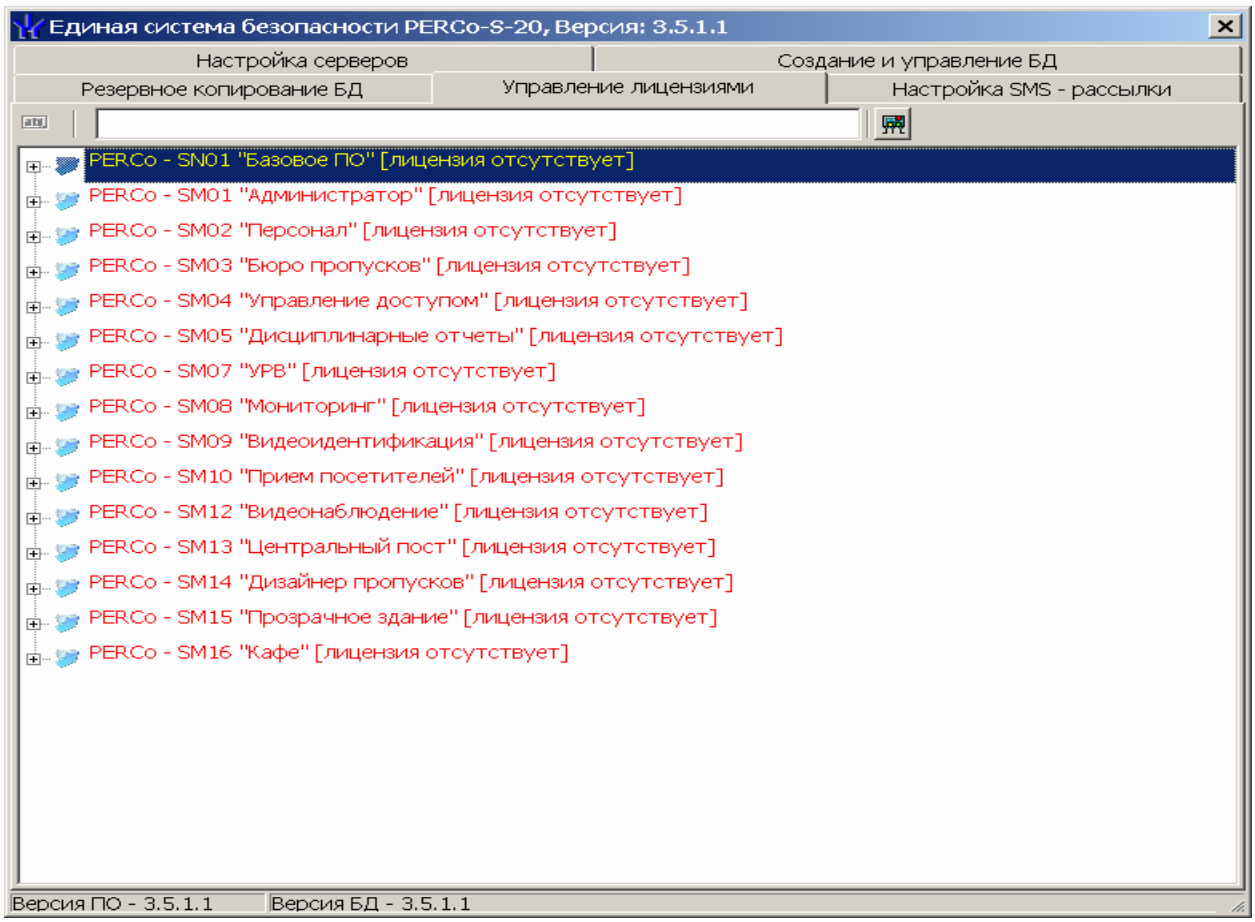
Для упрощения процедуры регистрации программного обеспечения, а также для ознакомления с его возможностями, в течение 30 дней с момента первого запуска программное обеспечение работает в ознакомительном режиме.

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 неактивированным 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 ее в компанию PERCo.

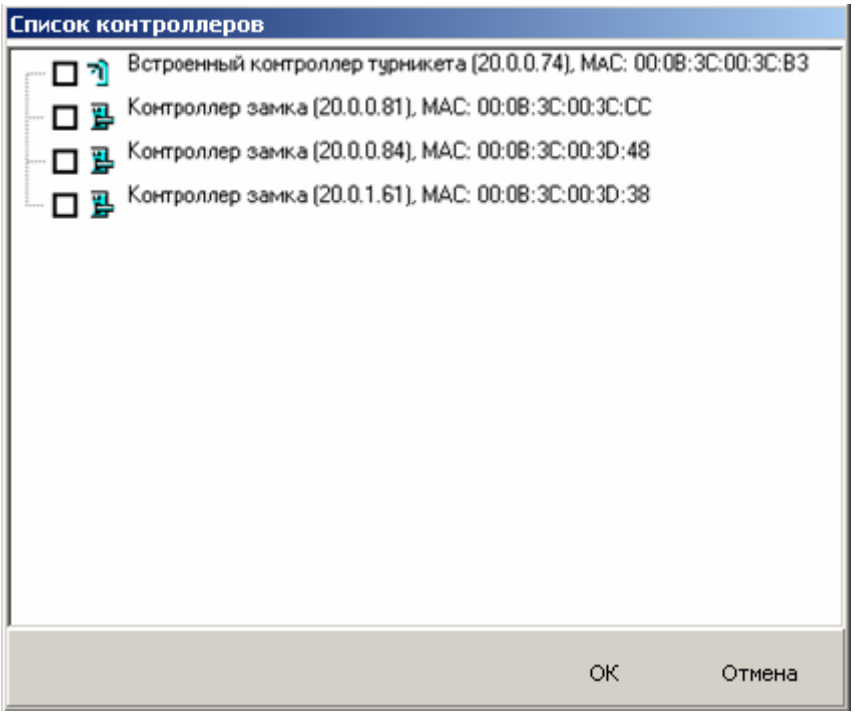
После получения лицензионного соглашения, содержащего ключи активации, Вам необходимо ввести их в программное обеспечение. Ввод ключей активации производится в модуле **Центр управления PERCo-S-20**, входящем в состав **PERCo-SN01 Базовое ПО**. Более подробная информация о работе с этим модулем приведена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

Для запуска **Центра управления серверами 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**:

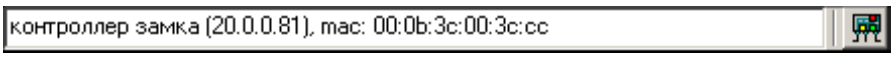


Для ввода лицензий укажите контроллер, MAC-адрес которого содержится в лицензионном соглашении. Для этого щелкните на кнопке, расположенной в верхней части окна.

Откроется окно выбора:



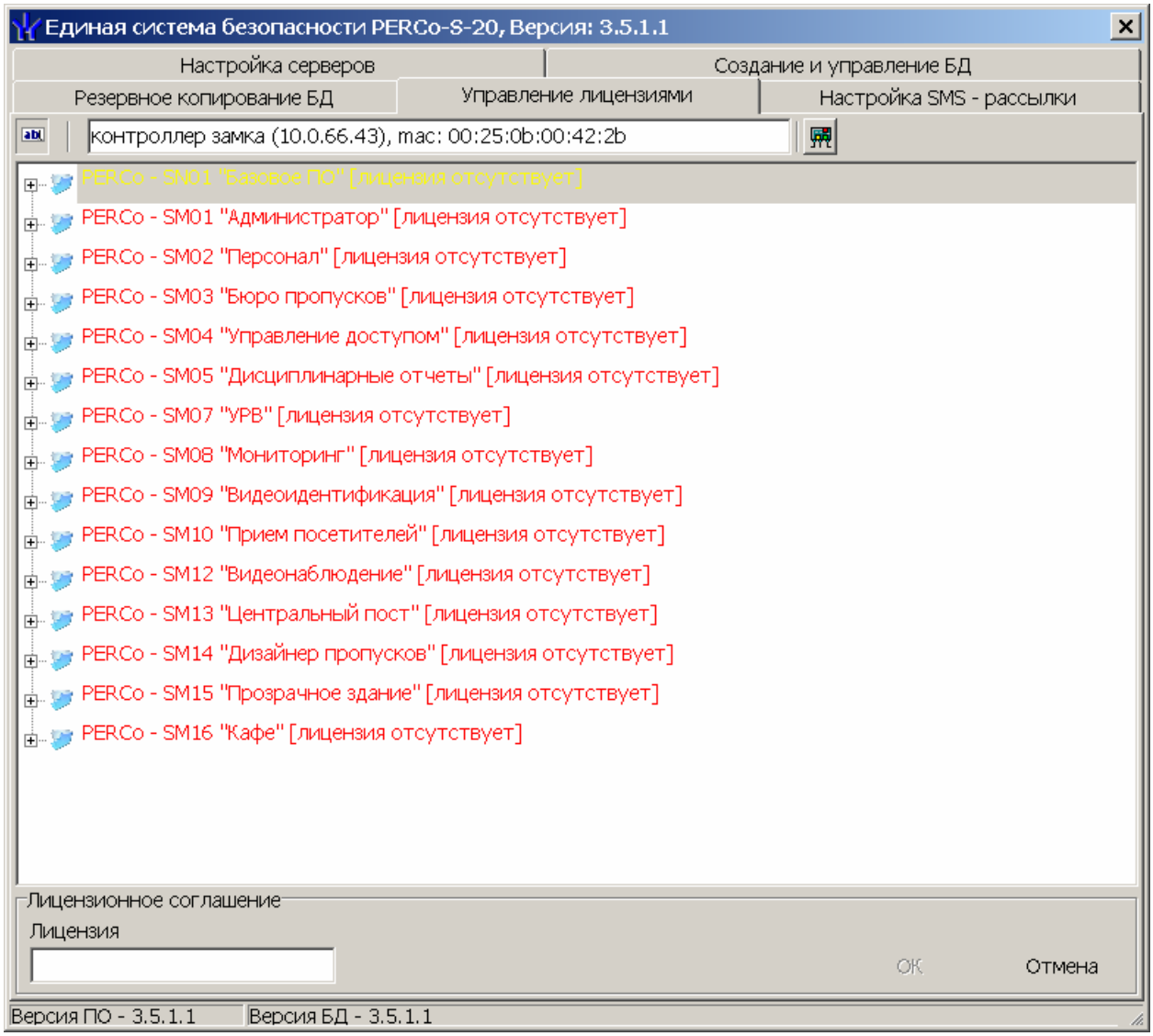
В этом окне отметьте выбранный Вами раньше контроллер и щелкните на кнопке **OK**, что приведет к закрытию диалогового окна и отображению имени выбранного контроллера в верхней части рабочего окна:



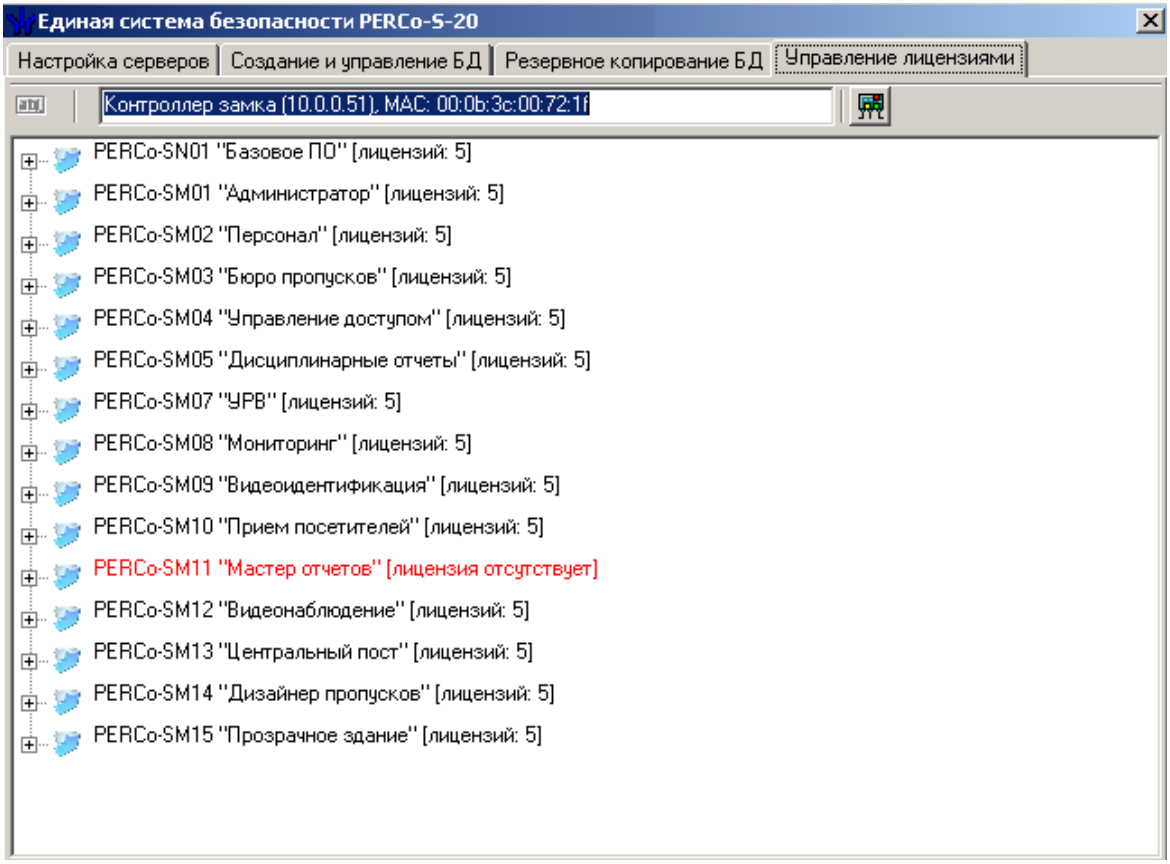
После выбора контроллера выделите в списке тот программный модуль, лицензию на который Вы собираетесь ввести, и щелкните на кнопке **Изменить код активации**  . При этом становится доступным строка ввода ключа активации:

Примечание

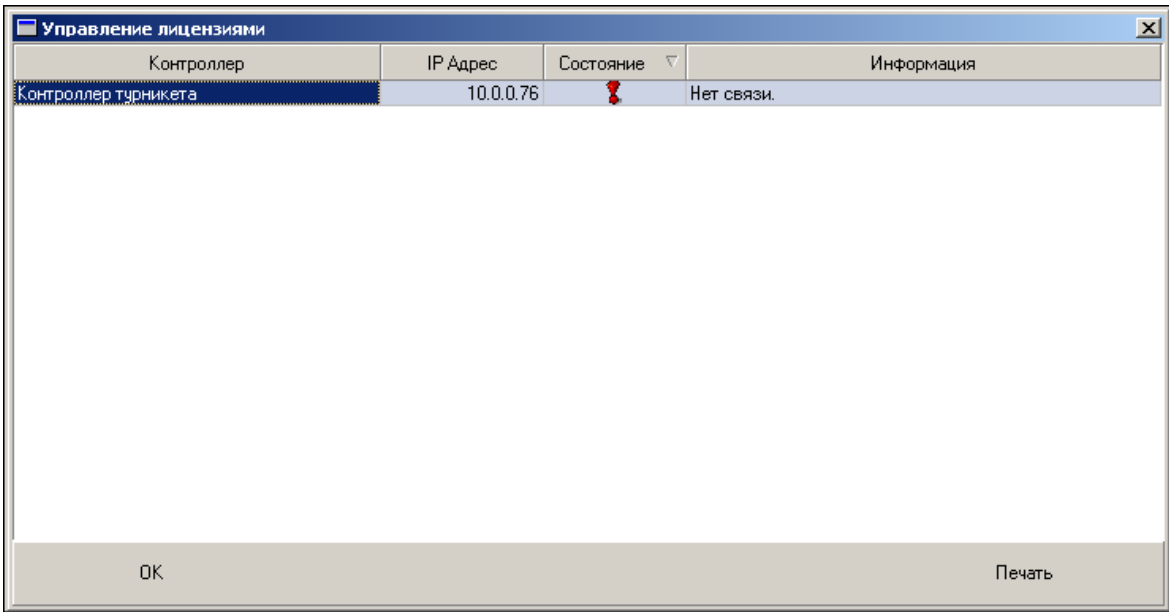
Код активации вводится без разделителей. Выбранный Вами контроллер должен находиться во включенном состоянии и быть подключенным к программному обеспечению. Для проверки наличия связи между программным обеспечением и выбранным контроллером можно воспользоваться разделом **Конфигуратор Консоли управления**.



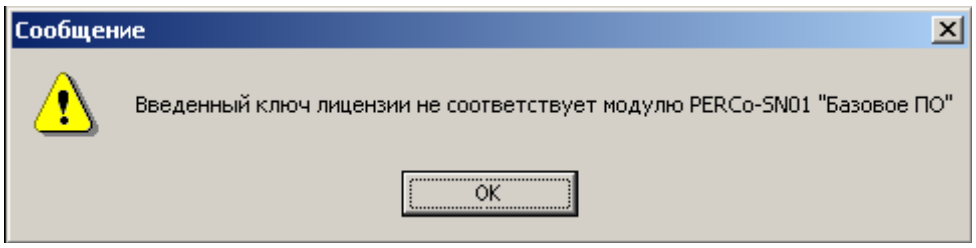
Введите код активации и нажмите кнопку **ОК**. После этого программное обеспечение автоматически осуществит проверку введенного Вами кода активации. При положительном ответе рядом с названием выбранного модуля отображается информация о количестве активированных рабочих мест.



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, и что Вы не ошиблись при вводе ключа активации. Повторите попытку.

Примечание

Выбранный Вами контроллер всегда будет использоваться во время проверки введенных ключей активации! В случае отсутствия связи с контроллером система автоматически перейдет в 30-тидневный режим ознакомления.

5 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:

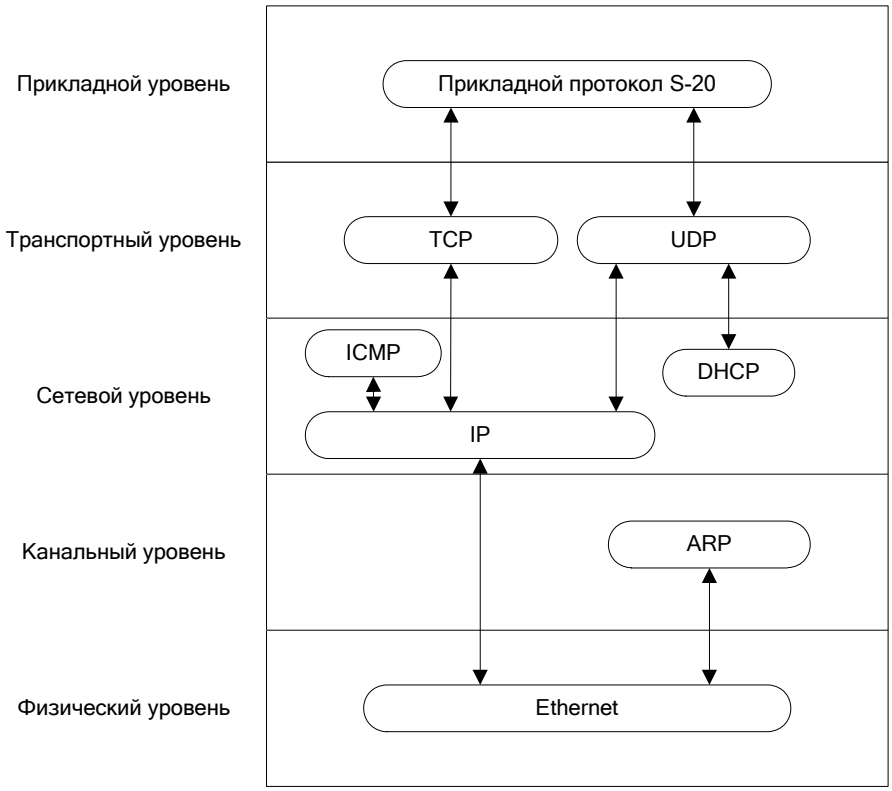


Рис. 2 Стек протоколов, используемых для обмена в системе

Также для передачи данных используются следующие порты:

Таблица 1 Порты

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

Перечисленные в таблице порты должны быть свободны и не использоваться другими системами и службами в сети предприятия. Также, если Вы используете

персональные или встроенные в Windows XP Farewall-ы, то в их конфигурации должны быть учтены эти данные.

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):

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

b) 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 удается, то вероятнее всего на пути следования IP-пакетов находится сетевое коммутирующее оборудование, делящее IP-пакеты на фрагменты размером меньше 576 байт. Проверьте настройки этого оборудования, при возможности увеличьте размер MTU. 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.

5.1 Настройка контроллера

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

Для этого необходимо:

1. Задать IP-адрес и выбрать режим получения адреса, согласовав его с работой вашей сети.
2. Сконфигурировать контроллер с помощью раздела ПО **Конфигуратор** (см. *«Руководство оператора»* по разделу ПО *«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 «x») 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 необходимо учитывать при задании сетевых настроек и последующей конфигурации самой системы PERCo-S-20, это необходимость обеспечения:

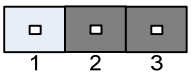
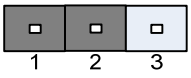
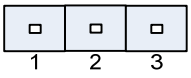
- уникальности сетевых адресов контроллеров в своей сети;
- предотвращения смены контроллерами своих IP-адресов после конфигурации системы PERCo-S-20, т.е. резервирование IP-адресов в сервере DHCP.

5.2 Режимы получения адреса

Режим работы по получению контроллером адреса задается с помощью устанавливаемых на плате контролера 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.

Таблица 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

5.2.1 Настройка без DHCP

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

Для обеспечения этого условия:

1. Добавьте (см. Рис. 3) 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.

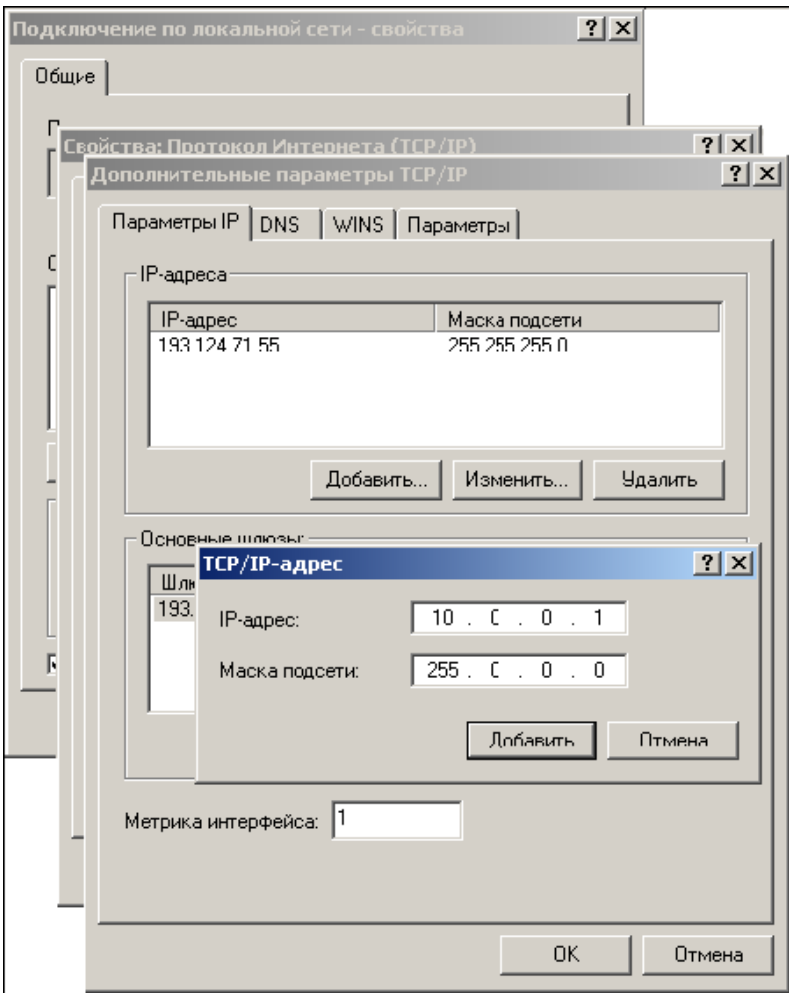


Рис. 3 Добавление нового IP-адреса

2. Установите перемычку по 3-му варианту (см. Таблица 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 в соответствии с разделом *«Конфигурация контроллеров».*
   У контроллера достаточно сконфигурировать только сетевые настройки.
5. Установите контроллер на выбранное место работы.

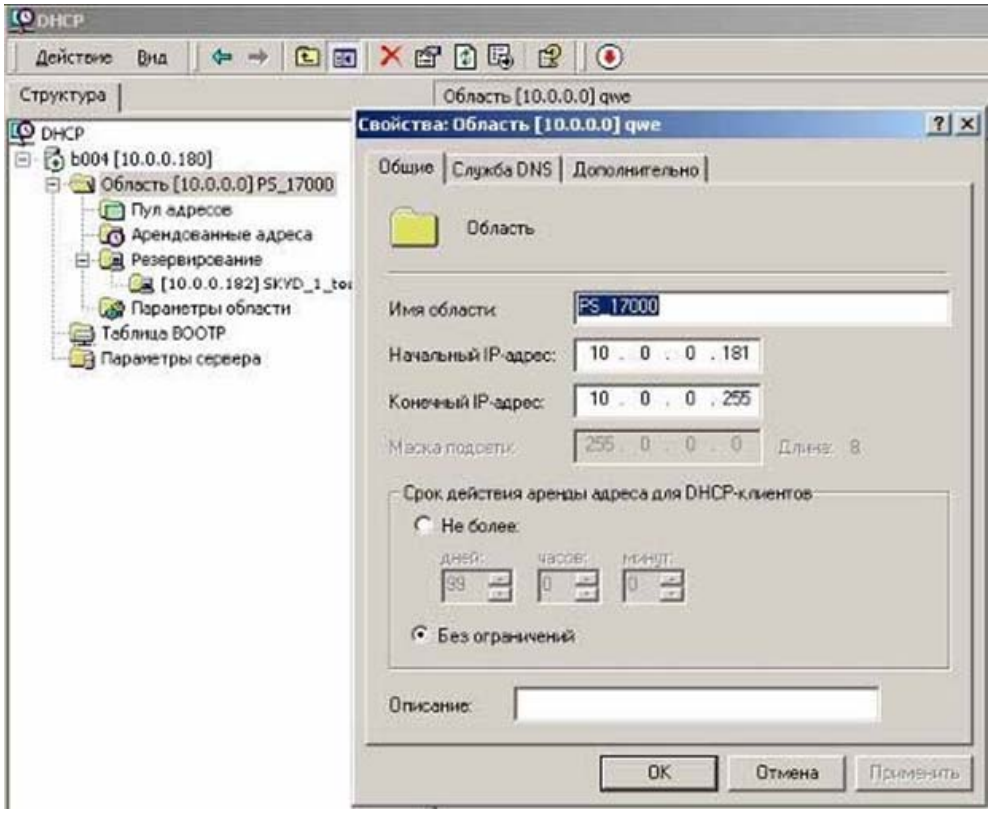
5.2.2 Настройка с DHCP

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

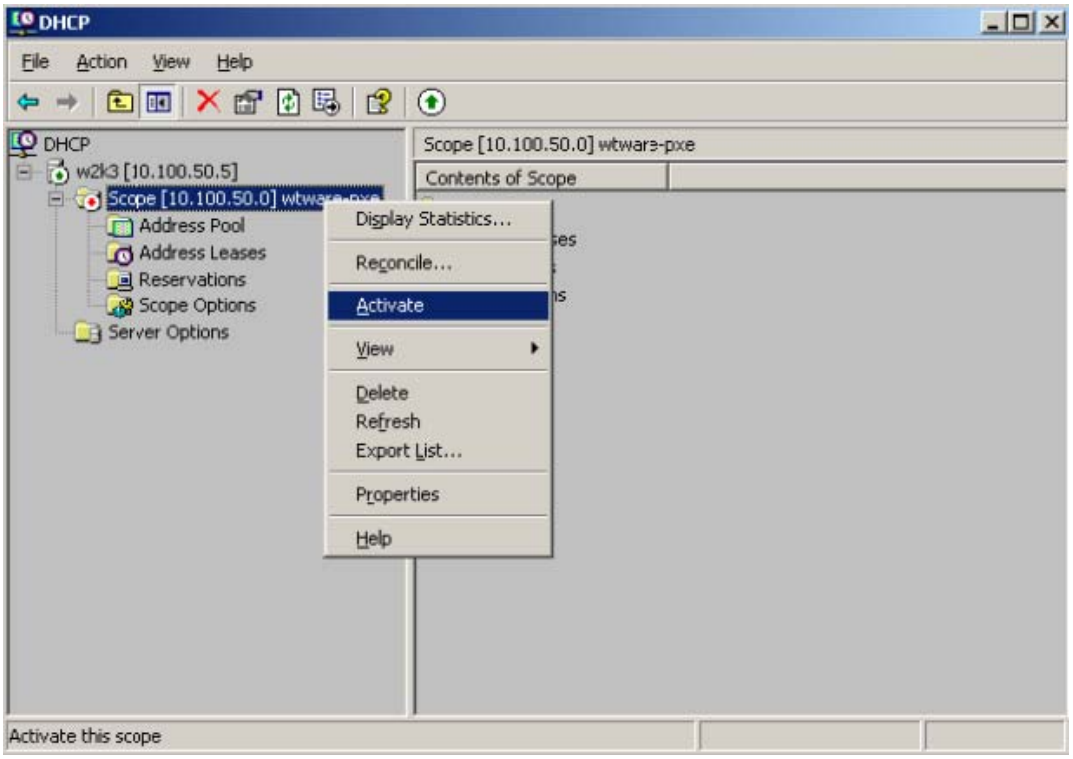
Описание настройки приведено на примере *Windows 2000*. Для других операционных систем смысл остается таким же.

1. Запустите DHCP сервер. Для этого выберите последовательно: **Пуск** → **Программы** → **Администрирование** → **DHCP.**
2. Создайте область адресов для контроллеров системы *PERCo-S-20*:



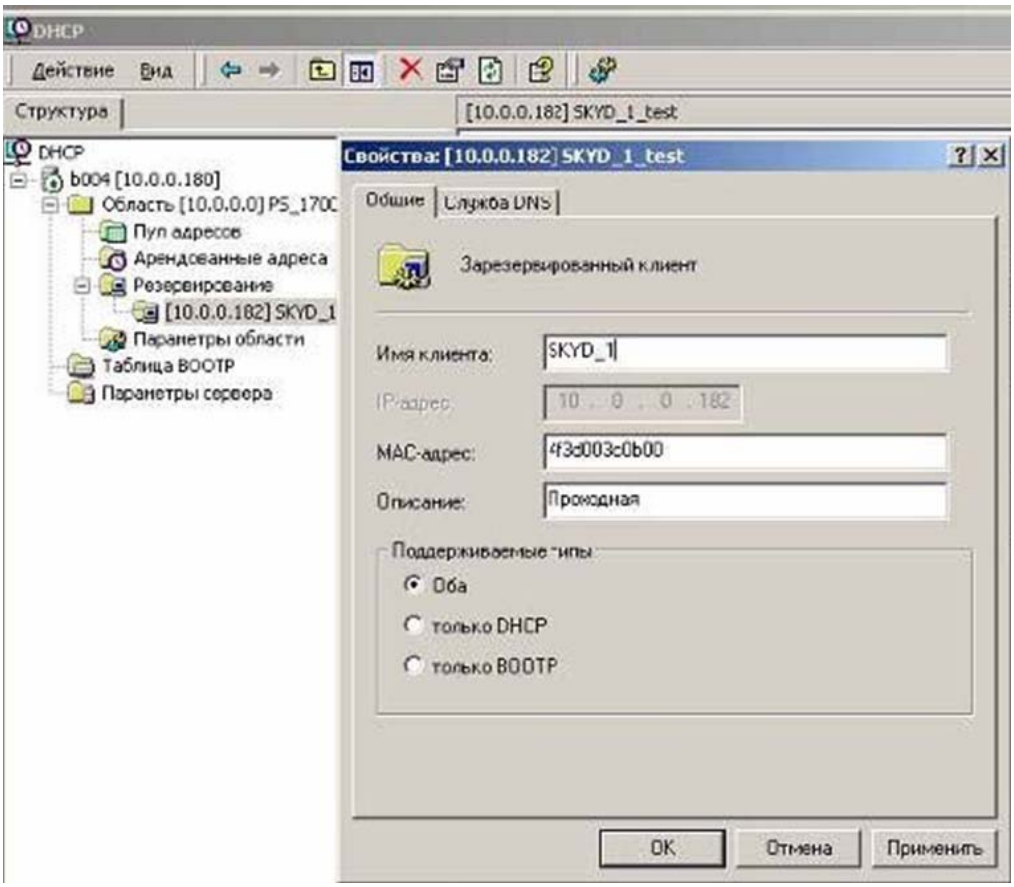
Название области и описание могут быть любыми. Это информация не для системы, а для системного администратора. Лучше, если название достаточно информативно, чтоб не вспоминать потом, что настраивается в этой области.
Рекомендуется делать область несколько больше, чем число контроллеров, которое планируется 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 соответствие с MAC-адресом контроллера, указанном в паспорте.
5. Для удобства добавьте описание.



Данную операцию необходимо будет повторить для всех контроллеров, которые планируется установить в Вашей сети.

6. Установите перемычки по 2-му варианту (см. Таблица 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`).

6 УПРАВЛЕНИЕ СЕРВЕРАМИ

Для управления сервером PERCo-S-20 запустите *Панель управления Windows*. Для этого выберите последовательно: **Пуск** → **Настройка** → **Панель управления**. Нажмите на *Панели управления* иконку:

– для управления сервером системы PERCo-S-20 и сервером баз данных (Рис. 4).

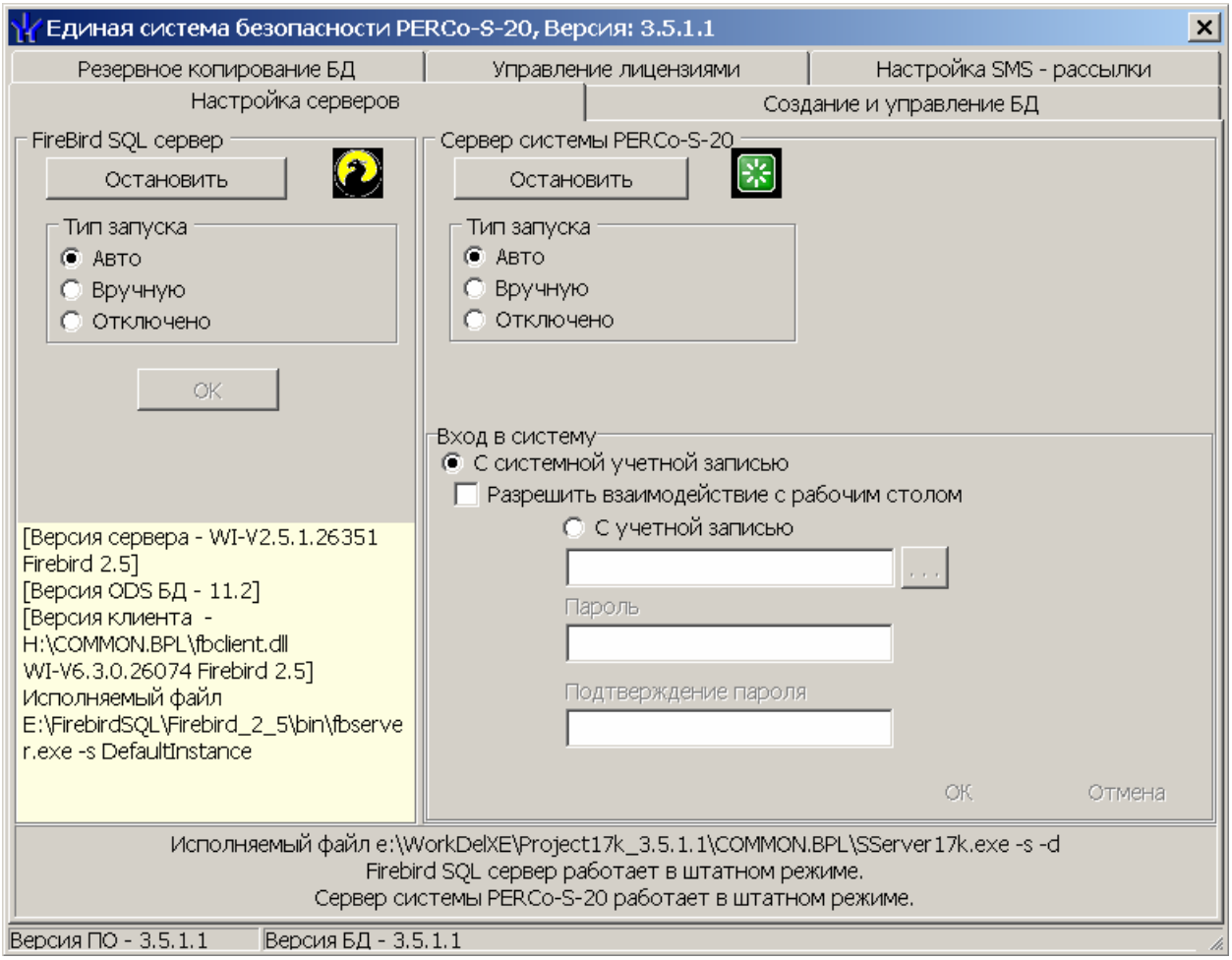


Рис. 4 Центр управления серверами системы PERCo-S-20

Вход в систему в режиме, когда отмечен переключатель **С учетной записью**, позволяет настроить почтовую рассылку сообщений о создании резервных копий базы данных (см. п. *«Планировщик заданий»*).

6.1 Создание и управление БД

Вкладка **Создание и управление БД** предназначена для создания и управления настройками базы данных единой системы безопасности *PERCo-S-20*.

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

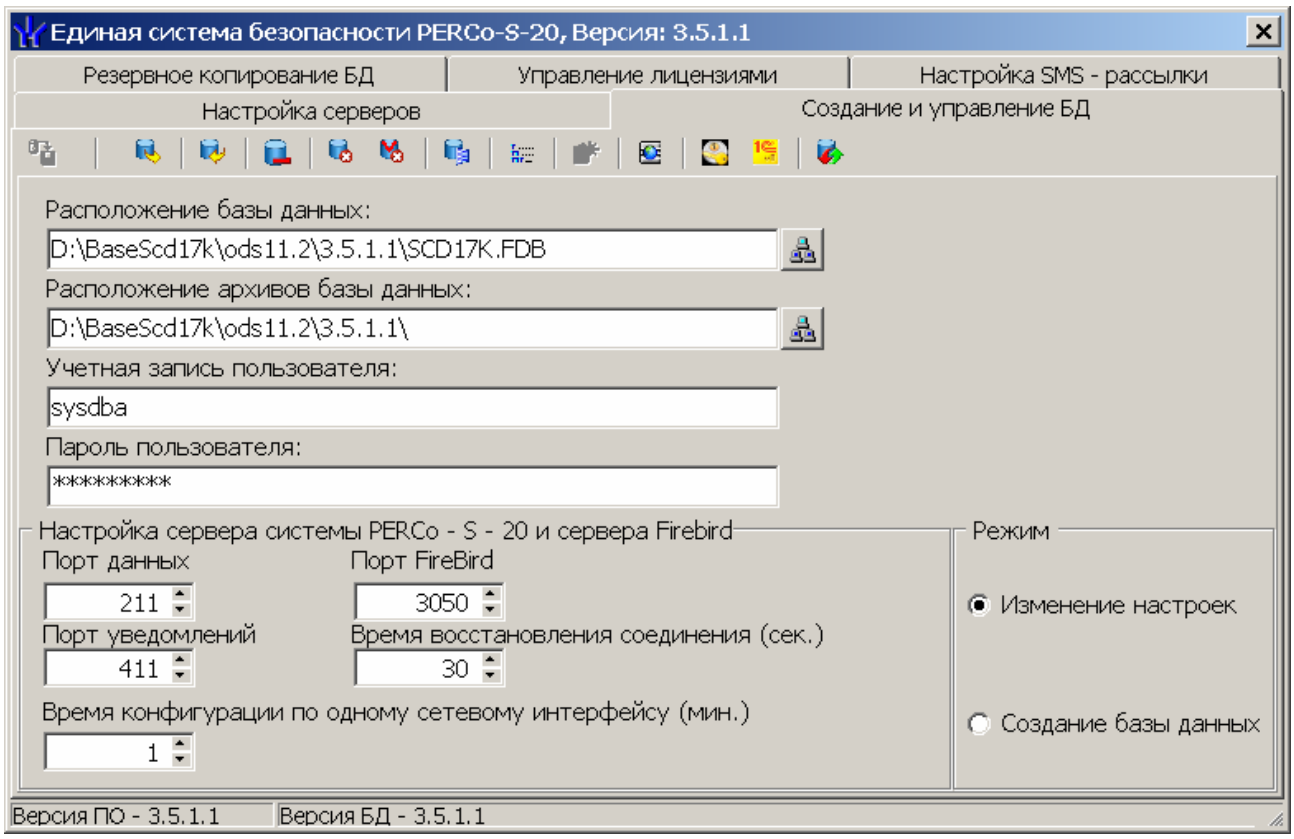


Рис. 5 Создание и управление БД

Доступны следующие кнопки на панели инструментов вкладки:

– Кнопка **Сохранение настроек базы данных** (**Ctrl**+**S**) позволяет сохранить изменения, внесенные в параметры базы данных.

– Кнопка **Сохранение базы данных, оптимизация и проверка целостности** (**Ctrl**+**B**) позволяет сохранить резервную копию базы данных. (См. *«Сохранение базы данных»*)

– Кнопка **Восстановление БД** (**Ctrl**+**R**) позволяет восстановить базу данных из резервной копии.

– Кнопка **Удаление данных мониторинга** (**Ctrl**+**D**) позволяет удалить данные из журнала мониторинга за указанный период.

– Кнопка **Удаление данных по событиям** (**Ctrl**+**E**) позволяет удалить данные из журнала регистрации за указанный период.

– Кнопка **Удаление данных по видеоидентификации** (**Ctrl**+**O**) позволяет удалить данные из журнала верификации за указанный период.

Примечание

Удаление данных с использованием кнопок , , не влияет на размер файла базы данных. Для уменьшения размера файла после удаления данных из журналов базу необходимо оптимизировать, то есть сохранить оптимизированную резервную копию, а затем загрузить ее вместо используемой ранее. (См. *«Очистка базы данных»*)

– Кнопка **Настройки сервера БД** (**Alt**+**N**)

– Кнопка **Оптимизация индексов** (**Ctrl**+**I**) позволяет оптимизировать работу программного обеспечения с базой данных. Рекомендуется проводить раз в неделю.

– Кнопка **Создание базы данных** (**Ctrl**+**N**) позволяет создать новую базу данных.

– Кнопка **Обновление версии базы данных** (**Ctrl**+**U**) позволяет привести в соответствие версию базы данных с версией программы.

Примечание

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

– Кнопка **Восстановление предыдущего пароля устройств** (**Alt**+**R**)

– Кнопка **Настройка работы с 1С** (**Ctrl**+**1**)

– Кнопка **Проверка целостности базы данных** (**Alt**+**B**) позволяет проверить файл базы данных на наличие ошибок.

Рабочая область вкладки:

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.

Панель **Настройки сервера системы и сервера FireBird** На панели расположены параметры, определяющие значения портов ввода/вывода, которые используются программным обеспечением для связи между программными модулями и БД.

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).

Панель **Режим**

6.1.1 Создание базы данных

Щелкнув на иконке из Панели управления, запустите **Центр управления серверами PERCo-S-20.**

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

Для создания базы данных:

1. Перейдите на вкладку **Создание и управление БД** (Рис. 5):

2. На панели **Режим** установите переключатель в положение **Создание базы данных** (См. Рис. 6)..

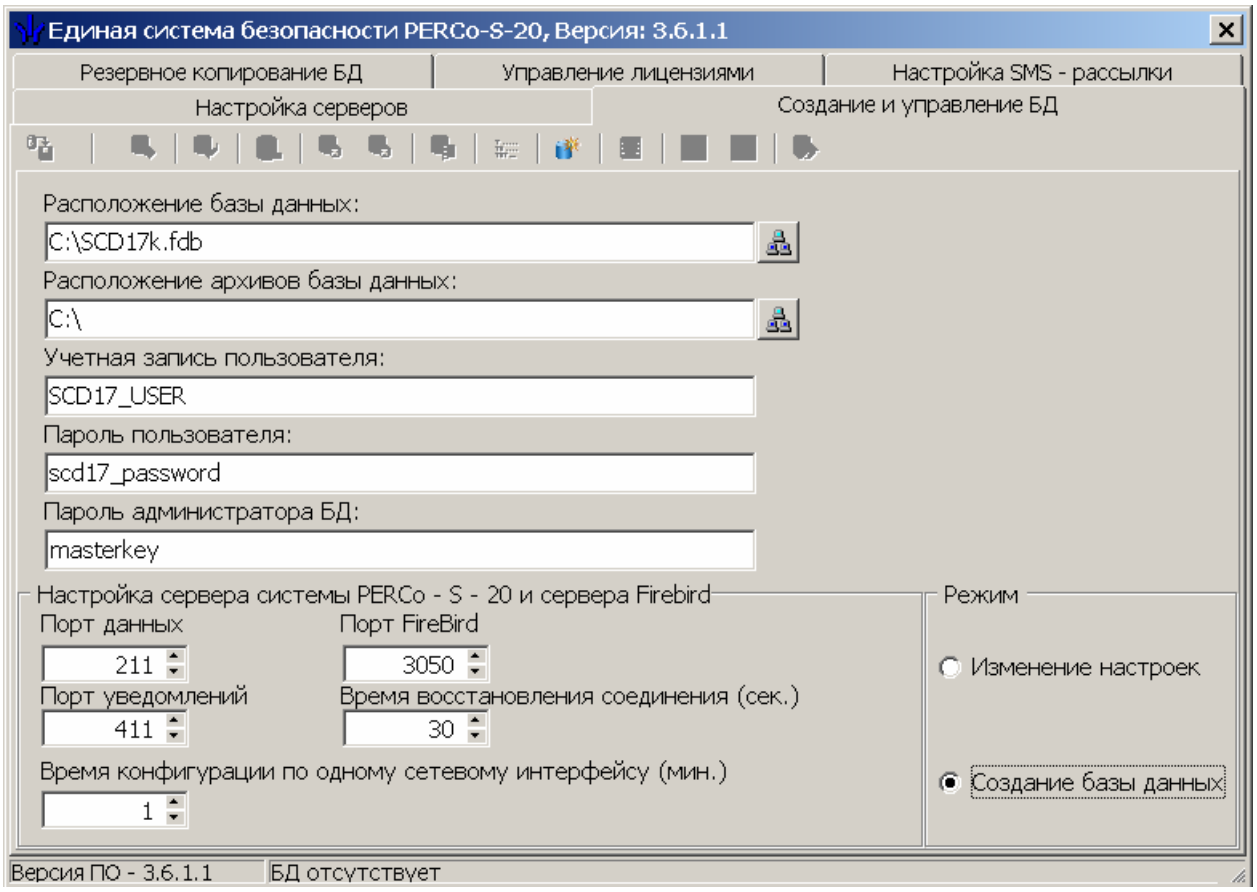


Рис. 6 Создание базы данных

3. В строке **Расположение базы данных** 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.
4. В строке **Расположение архивов базы данных** укажите путь и название файла, который будет создаваться при резервном копировании (сохранении при помощи кнопки), базы данных. Это путь к директории, где будут создаваться архивные копии файла базы данных. Имя самого файла базы данных и архива лучше не изменять. По умолчанию название файла резервной копии `Backup1.fbk`. 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.
5. В строке **Учетная запись пользователя** задайте имя пользователя, который будет создателем и владельцем файла базы данных В строке **Пароль пользователя** задайте пароль пользователя для доступа к БД.

Примечание

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

6. В строке **Пароль администратора БД** задайте пароль администратора БД.
7. После ввода всех характеристик нового файла баз данных нажмите кнопку **Создать базу данных** .
8. При удачном завершении откроется окно с сообщением. Нажмите **ОК**. Новая база данных создана.

После создания базы можно работать с любым разделом программного обеспечения системы PERCo-S-20. Поля данных на вкладке заполнятся введенными параметрами.

6.1.2 Сохранение резервной копии базы данных

При нажатии на кнопку **Сохранение базы данных** – происходит создание полной резервной копии базы данных. Выбор места расположения резервной копии БД определяется в строке **Расположение архивов базы данных** на этапе создания БД. По умолчанию название файла резервной копии `Backup1.fbk`.

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.

6.1.3 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 то же 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.

6.1.4 Очистка базы данных

Рекомендуется проводить очистку базы данных не реже одного раза в квартал после завершения формирования всех необходимых отчетов. События мониторинга рекомендуется удалять не реже одного раза в месяц. Это позволяет уменьшить размер файла базы данных и ускорить работу программных модулей системы безопасности.

Для очистки базы данных произведите следующие действия.

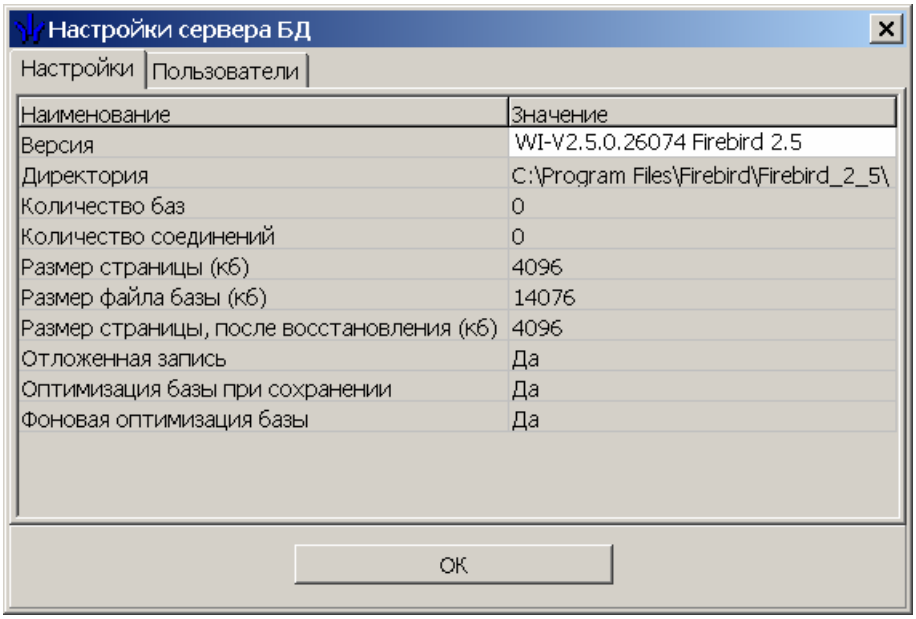
1. Перейдите на вкладку **Создание и управление БД.**
2. Для удаления данных по мониторингу нажмите кнопку **Удаление данных по мониторингу** на панели инструментов вкладки.
3. В открывшемся окне **Удаление данных мониторинга** установите с помощью полей ввода дат **Начало периода** и **Конец периода** за который будут удалены данные. Нажмите кнопку **ОК**. Данные из журнала мониторинга будут удалены.
4. Для удаления данных о событиях нажмите кнопку **Удаление данных по событиям** на панели инструментов вкладки.
5. В открывшемся окне **Удаление данных по событиям** установите с помощью полей ввода дат **Начало периода** и **Конец периода** за который будут удалены данные. Нажмите кнопку **ОК**. Данные из журнала регистрации будут удалены.
6. Для удаления данных по верификации нажмите кнопку **Удаление данных по видеоидентификации** на панели инструментов вкладки.
7. В открывшемся окне **Удаление данных по видеоидентификации** установите с помощью полей ввода дат **Начало периода** и **Конец периода** за который будут удалены данные. Нажмите кнопку **ОК**. Данные из журнала верификации будут удалены.
8. Для оптимизации размера файла базы данных после удаления данных из журналов необходимо нажать кнопку **Сохранение базы данных, оптимизация и проверка целостности** на панели инструментов вкладки. Резервная копия файла будет создана в папке указанной в строке **Расположение архивов базы данных**.
9. После этого необходимо обновить базу данных из сохраненной резервной копии. Для этого нажмите кнопку **Восстановление БД** на панели инструментов вкладки.
10. Система готова к работе с обновленной базой данных.

6.1.5 Настройки сервера базы данных

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

Окно включает две вкладки **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.

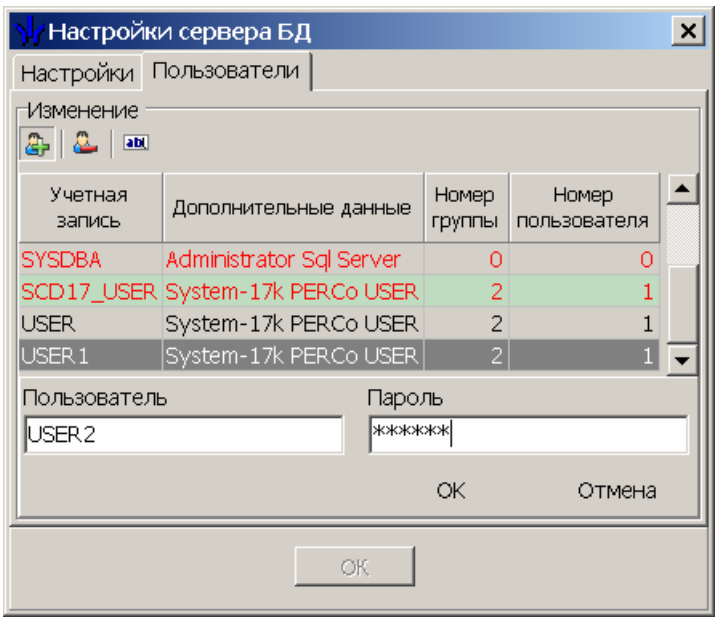
Размер страницы, после восстановления – при восстановлении БД, особенно при переносе на другой носитель, размер страницы может быть не кратным размеру кластера жесткого диска. Поэтому для оптимизации производительности рекомендуется устанавливать его кратным размеру кластера.

Отложенная запись – все изменения, проходящие с данными 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, установив «Нет» в данном параметре, 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 вкладке **Пользователи** предоставляется возможность изменить пароль администратора БД. Рекомендуется заменить пароль «masterkey», являющийся общеизвестным, на пароль, известный только администратору системы (пароли регистрозависимы).

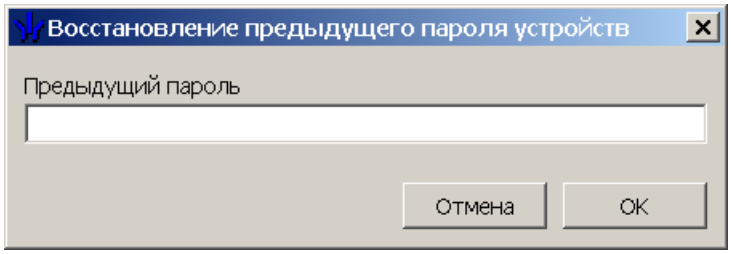


6.1.6 Восстановление предыдущего пароля устройств

Восстановление предыдущего пароля устройств может быть необходимо в следующей ситуации:

- После установки пароля и нормального функционирования системы вы создали резервную копию БД. Затем по возникшей необходимости Вы сменили пароль для связи с устройствами системы и передали им параметры. После этого Вы восстановили БД из резервной копии.
- В результате этих действий в программном обеспечении будет использоваться пароль, сохраненный в резервной копии БД и отличный от пароля, сохраненного в контроллерах системы. 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, установленный на данный момент в контроллерах системы, и нажать на кнопку **ОК**:



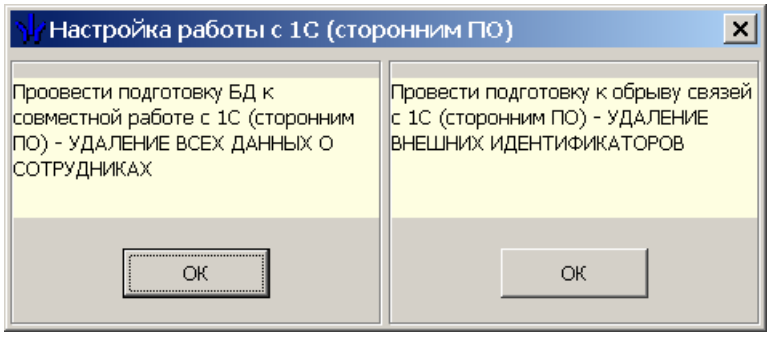
Примечание

При восстановлении пароля все ***Консоли управления*** должны быть закрыты.

После восстановления пароля необходимо завершить работу с **Центром управления серверами.** Запустить **Консоль управления** с установленным модулем **Конфигуратор** и передать измененные параметры в контроллеры системы.

6.1.7 Настройка работы с 1С

Данная функция используется только при работе ПО с модулем интеграции с 1С.



- Проведение подготовки 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.

Примечание

Данная операция не является обязательной для последующей интеграции ПО с 1С и выполняется по необходимости.

- Проведение подготовки 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 и в S-20 не будут синхронизироваться между собой.

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

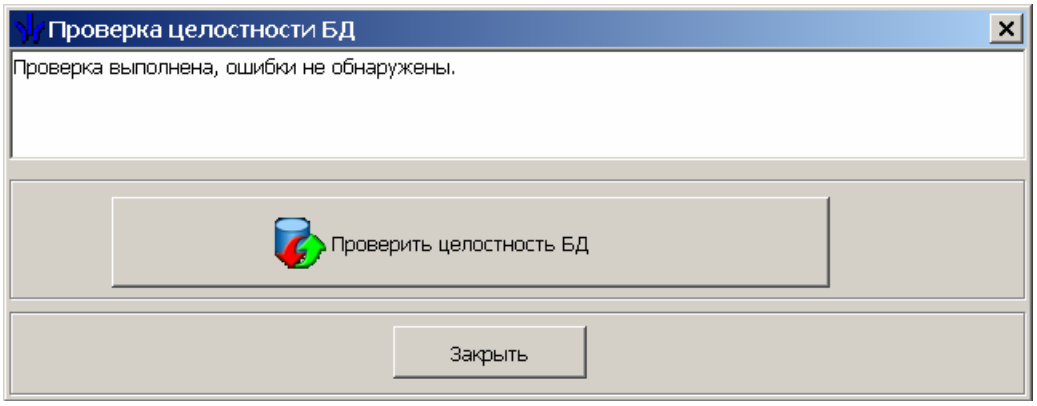
- О сотрудниках
- Учетных данных (подразделения и должности)
- Графики работы, праздничные дни и ночное время
- Оправдательные документы и документы на сверхурочные
- Справочник документов

После обрыва связей все эти действия снова становятся доступными.

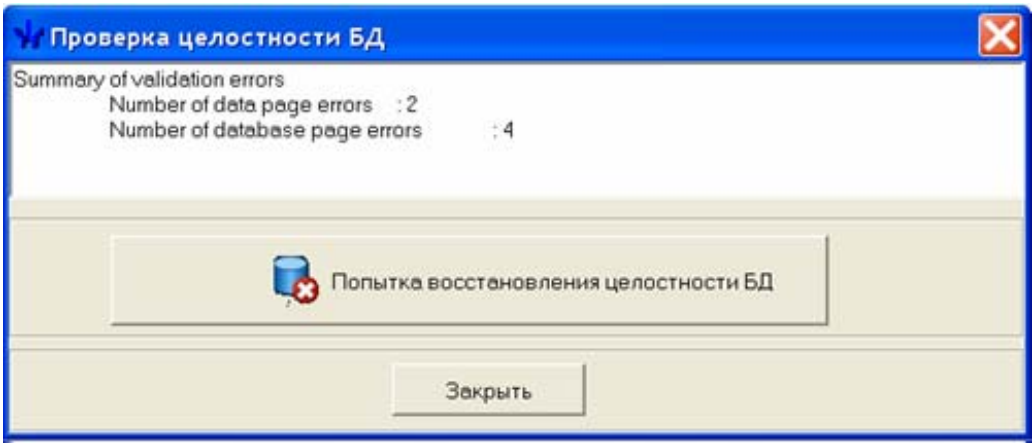
6.1.8 Проверка целостности базы данных

Данная функция используется с целью проверки базы данных на наличие ошибок.

После нажатия на кнопку **Проверить целостность БД** будет произведена проверка БД. В случае отсутствия ошибок появится надпись: *«Проверка выполнена, ошибки не обнаружены»*.



В случае обнаружения ошибок:



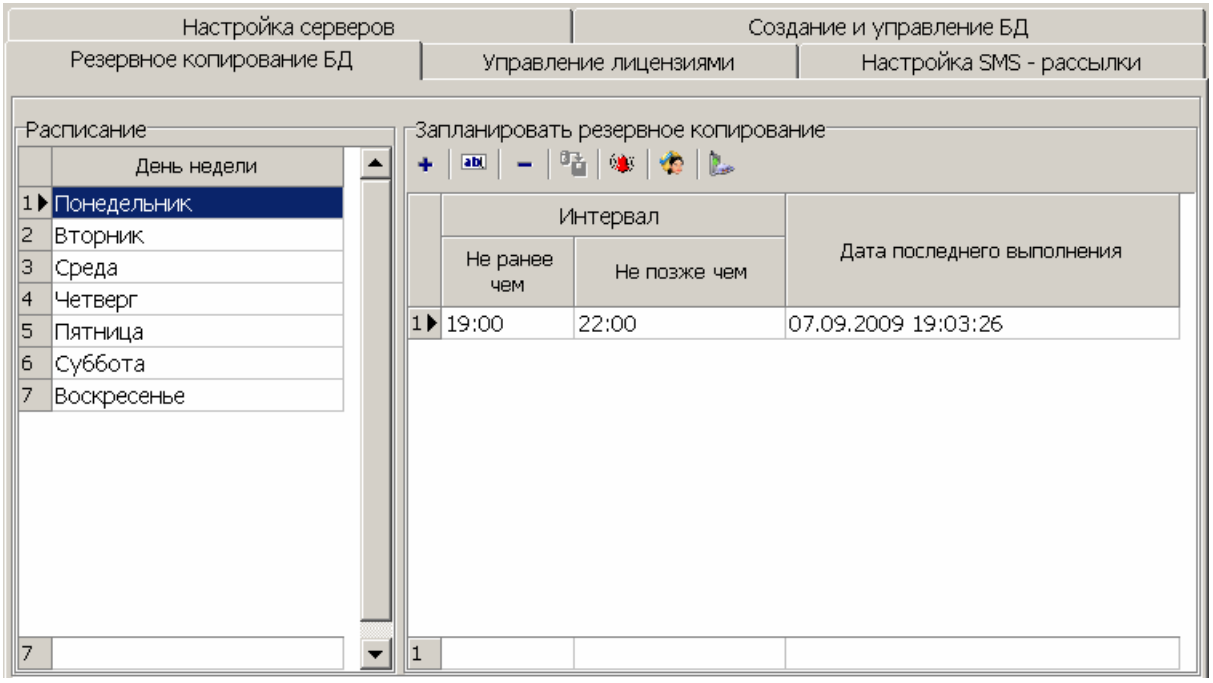
После нажатия на кнопку **Попытка восстановления целостности БД** при успешном восстановлении появится сообщение об успешном восстановлении. Нажмите **ОК**. Испорченный файл базы данных будет сохранен с расширением `.bad`.

Если же восстановить целостность БД не удается, то необходимо воспользоваться последней сохраненной резервной копией данной БД.

6.2 Резервное копирование БД

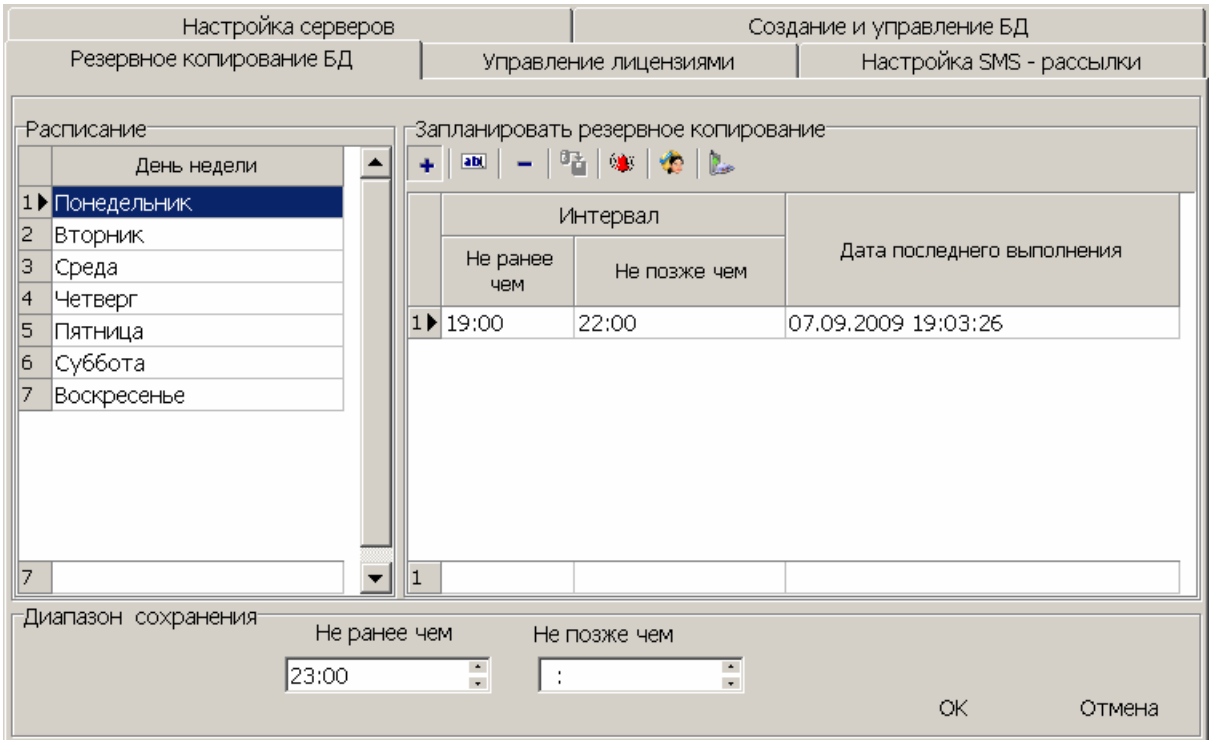
Одной из основных проблем обслуживания информационных систем является своевременное создание резервных копий базы данных. К сожалению, сбои в работе персональных компьютеров, жестких дисков не редкость.

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 закладке **Планировщик заданий** 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 закладке **Создание и управление БД** данного модуля.

Для создания расписания необходимо выбрать день недели и нажать на кнопку **Добавление**  . В нижней части окна откроется панель ввода:

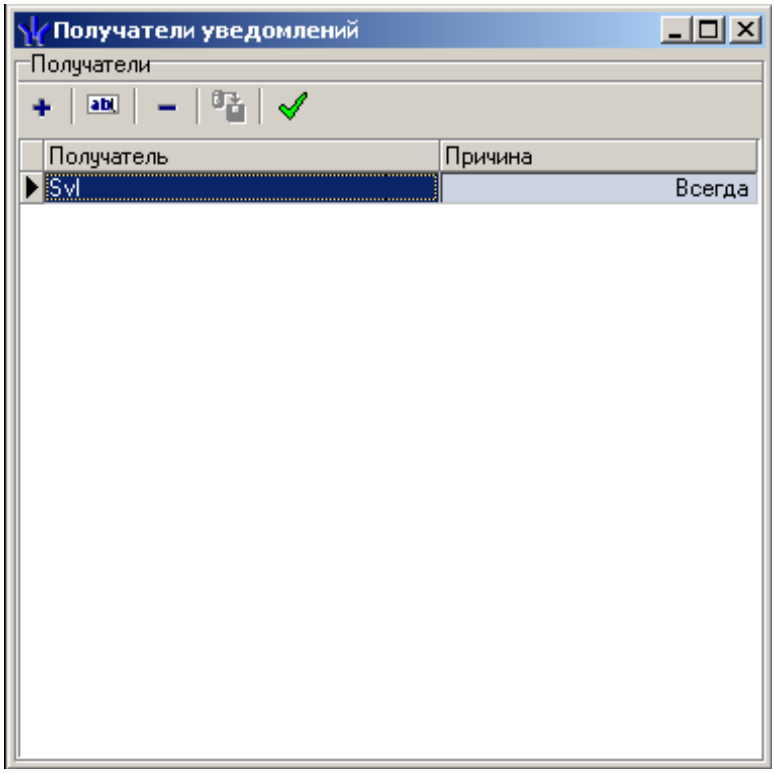


В этой панели необходимо указать интервал времени, в течение которого сервер системы проведет создание резервной копии БД. При условии работы системы в круглосуточном режиме рекомендуем установить этот интервал в ночное время.

После завершения ввода временного интервала и нажатия на кнопку **ОК** необходимо сохранить внесенные данные.

Для изменения временного интервала необходимо воспользоваться кнопкой **Редактирование** , для удаления - кнопкой **Удаление** .

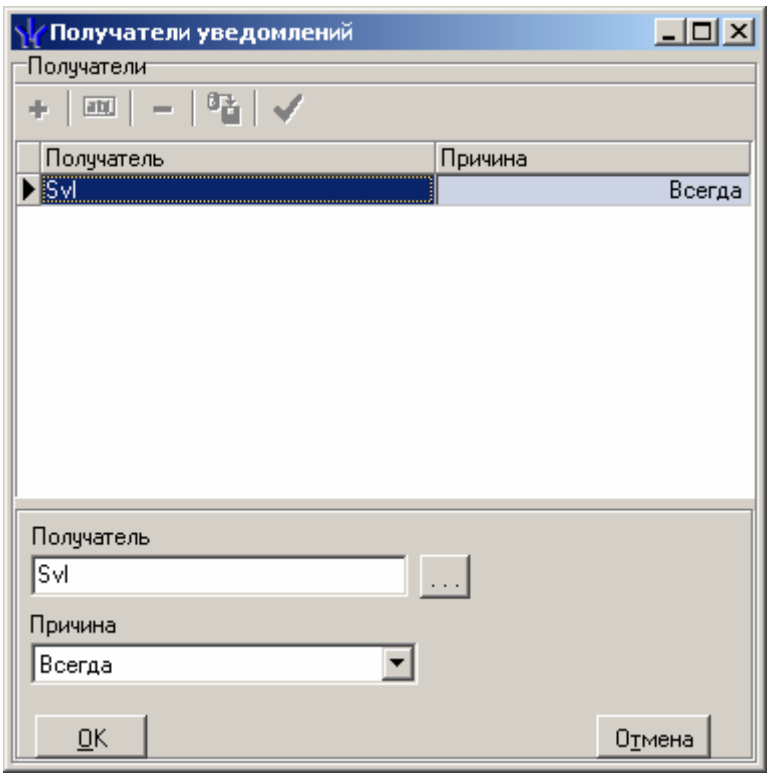
При создании резервной копии базы данных существует возможность рассылки уведомлений о результатах выполнения. Для задания списка рассылки необходимо воспользоваться кнопкой **Настроить сетевую рассылку уведомлений** . Нажатие на нее приведет к открытию диалогового окна, отображающего текущее состояние списка рассылки:



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

Кнопка **Тестирование уведомлений** позволяет протестировать работу данной функции. При нажатии на эту кнопку выделенному сотруднику будет отправлено тестовое сообщение.

Для добавления нового получателя уведомлений необходимо воспользоваться кнопкой **Добавить нового получателя** . При нажатии на нее в нижней части окна отобразиться панель ввода:

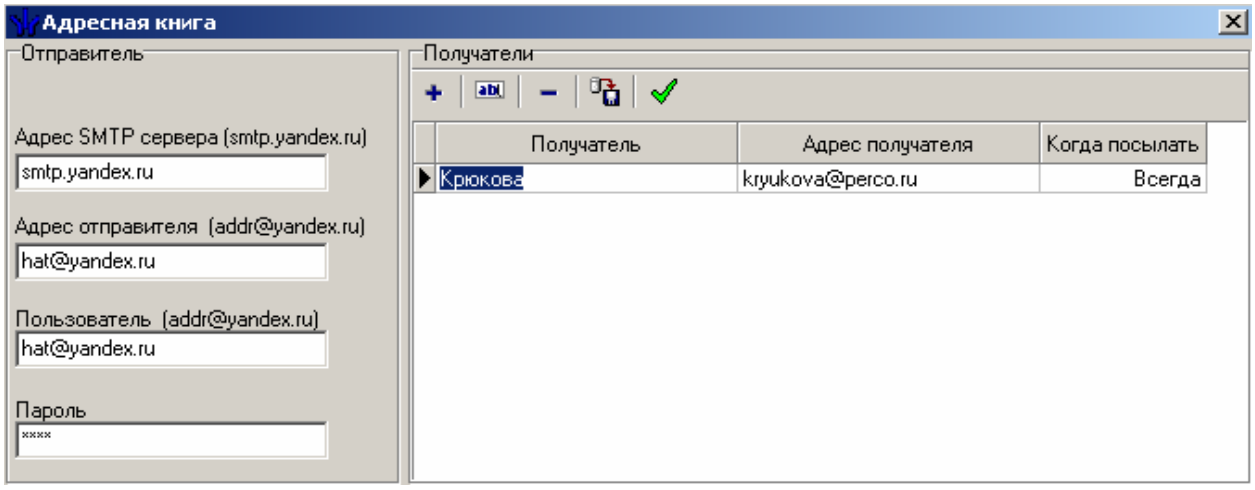


В этой панели необходимо ввести имя компьютера, на которое будет отправлено сообщение и причину отправки, которую необходимо выбрать из списка. Доступны два варианта:

- **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 сможет создать резервную копию базы данных.

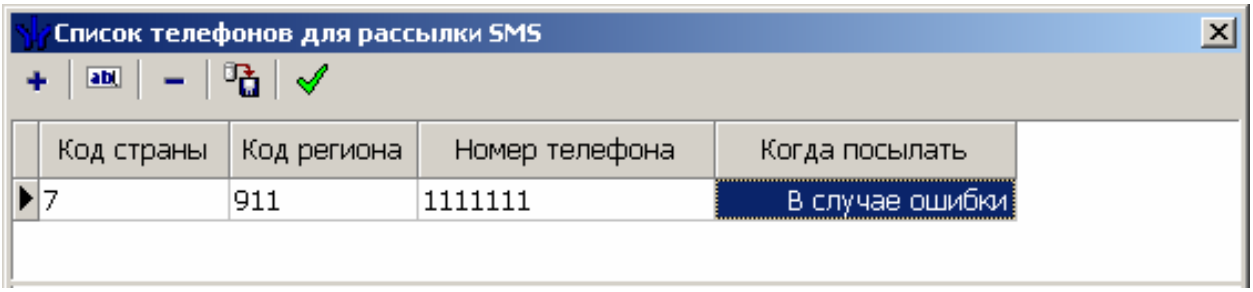
После завершения ввода необходимо нажать на кнопку **ОК** и сохранить внесенные изменения.

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



Функциональные элементы этого окна аналогичны описанным выше функциональным элементам окна настройки сетевой рассылки уведомлений.

Кнопкой **Настройка SMS-рассылки** – открывается окно настройки рассылки уведомлений о создании резервной копии БД с помощью SMS-сообщений:



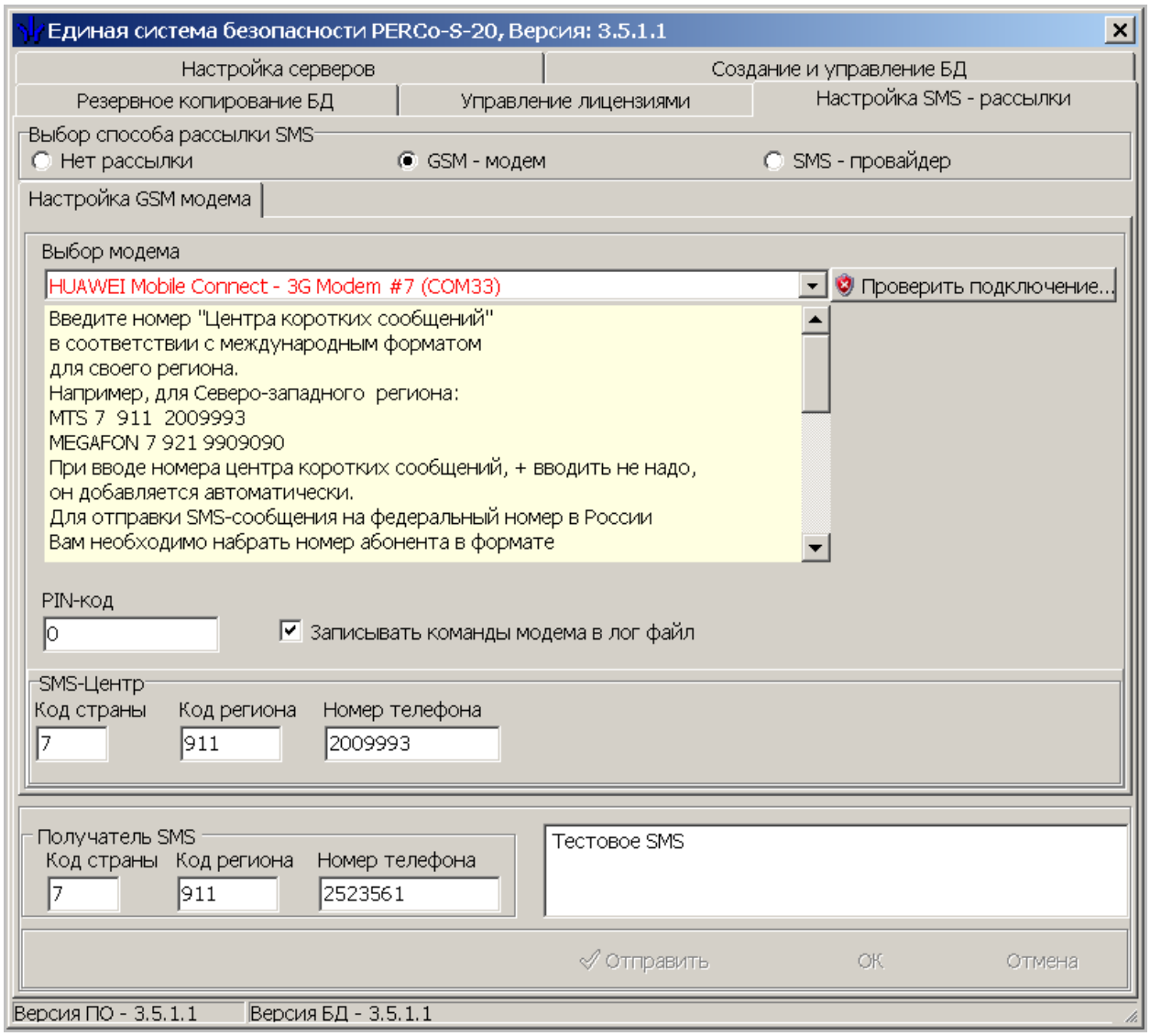
Функциональные элементы этого окна аналогичны описанным выше функциональным элементам окна настройки сетевой рассылки уведомлений.

6.3 Настройка SMS – рассылки

Для рассылки SMS-уведомлений о сохранении БД, а также для SMS-рассылки, настраиваемой непосредственно в разделах **Консоли управления** (SMS-сообщений на телефоны сотрудников при необходимости, при предъявлении карт доступа или наступлении иного события и т.д.) на вкладке **Настройка SMS-рассылки** необходимо выбрать способ рассылки:

- **Рассылка с помощью GSM - модема.** В этом случае рассылка уведомлений и SMS – сообщений будет производиться через модем, подключенный к USB-порту компьютера, где установлен Сервер системы. Необходимо настроить модем, как указано ниже в пункте < Настройка GSM – Модема >.
- **Рассылка с помощью SMS – провайдера.** В этом случае рассылка уведомлений и SMS – сообщений будет производиться через Internet-шлюз, т.е. требуется наличие постоянного подключения к Internet. Необходимо настроить шлюз, как указано ниже в пункте < Настройка SMS – провайдера >.
- **Нет рассылки.** В этом случае рассылка уведомлений и SMS – сообщений будет недоступна.

6.3.1 Настройка GSM – модема



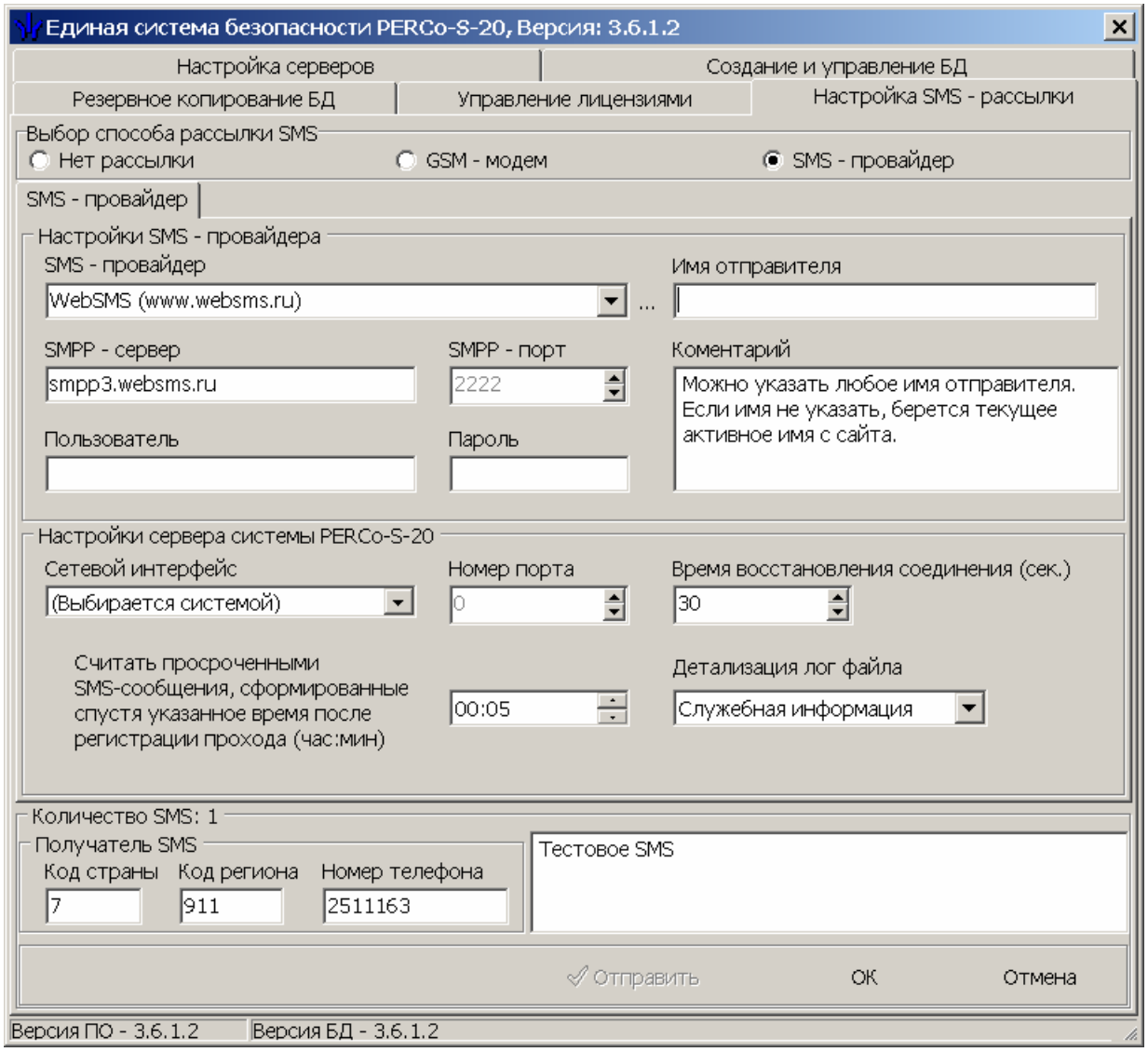
В качестве модема может выступать обычный сотовый телефон со встроенным модемом и возможностью подключением через USB порт компьютера, для рассылки уведомлений о сохранении данных его должно хватить, для более массовой рассылки рекомендуется использовать внешний USB-модем.

Порядок настройки:

- Внимательно прочитать документацию по установке модема и установить ПО в соответствии с рекомендациями производителя (при корректной установке в **Панели управления** –> **Телефон и модем** должна появится запись об установленном модеме).
- Запустить **Центр управления PERCo S-20**, перейти на вкладку **Настройка SMS-рассылки**, выбрать способ рассылки **SMS GSM-модем** и заполнить данные в поле **Выбор модема**.
- PIN-код вводить нужно только, если ваша SIM-карта защищена.
- Записывать команды модема в лог-файл необходимо при возникновении ошибок при использовании модема, для последующей отсылки лог-файла в адрес 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 нее для проверки корректности настроек, при корректном вводе получатель SMS должен получить тестовое SMS с набранным текстом.

6.3.2 Настройка SMS – провайдера



Порядок настройки:

1. Запустите **Центр управления PERCo S-20** и перейдите на вкладку **Настройка SMS-рассылки**. Установите способ рассылки **SMS-провайдер**.
2. Выберите из раскрывающегося списка **SMS – провайдер** того провайдера через которого будет осуществляться рассылка.
3. Перейдите на сайт SMS – провайдера, нажав кнопку ... справа от списка **SMS-провайдер**. Зарегистрируйтесь и получите тестовую учетную запись для пробной рассылки.
4. Введите в полях **Пользователь** и **Пароль** регистрационную информацию, полученную для тестовой учетной записи.
5. Укажите **Имя отправителя**.
6. Введите для отправки тестового SMS-сообщения телефон получателя и текст SMS.

После завершения ввода настроек станет доступна кнопка **Отправить**, следует нажать на нее для проверки корректности настроек, при корректном вводе получатель SMS должен получить SMS с тестовым текстом.

Имеется также ряд параметров, позволяющий более тонко настроить взаимодействие с SMS-провайдером:

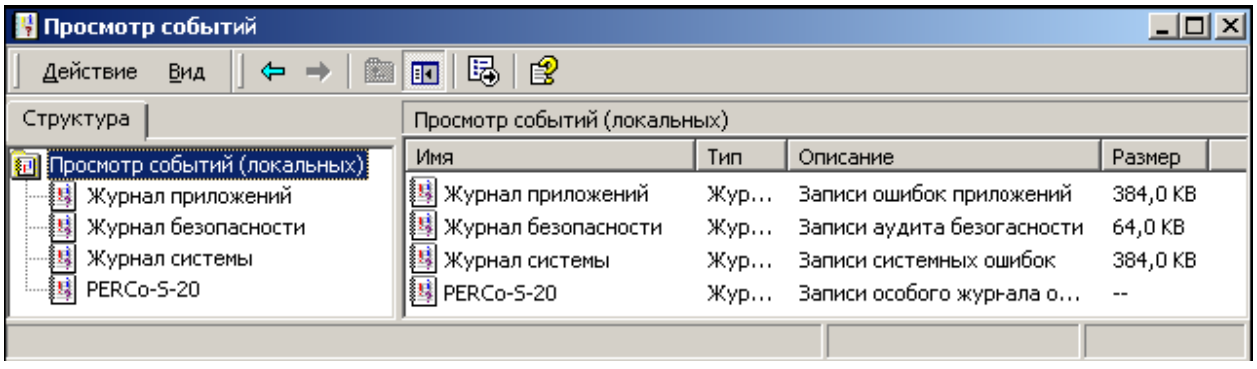
- **Сетевой интерфейс** – параметр, указывающий, с какого сетевого интерфейса будет осуществляться подсоединение к SMS-провайдеру.
- **Номер порта** – параметр, указывающий, с какого порта будет осуществляться подсоединение к SMS-провайдеру.
- **Время восстановления соединения (сек.)** - параметр, указывающий через какое время Сервер системы попытается восстановить разорванное соединение с SMS-провайдером.
- **Считать просроченными SMS-сообщения, сформированные спустя указанное время после регистрации прохода (час:мин)** – параметр, используемый при формировании SMS-сообщений. Если контроллер СКУД зарегистрировал проход, а связь с Сервером системы отсутствовала и была восстановлена через указанное время или позже, то SMS-сообщения, сформированные на основании такого прохода, будут считаться просроченными и не будут отправлены конечному получателю.
- **Детализация лог-файла** – параметр, указывающий, с какой степенью детализации следует выводить информацию в лог-файл при взаимодействии с SMS-провайдером.

6.4 Сообщения об ошибках

Учитывая, что сервер системы выполнен в виде стандартного сервиса *Windows*, информация о возникшей ошибке не может быть выведена в диалоговое окно.

Сообщения о внутренних ошибках и дополнительная информация записывается в журнал, доступный для просмотра через панель управления *Windows*.

Для просмотра событий необходимо открыть панель управления *Windows* (**Пуск** → **Настройка** → **Панель управления**), далее открыть панель **Администрирование** и запустить **Просмотр событий**.



Информация об ошибках и внутренних сообщения записывается в журнал *PERCo-S-20*.

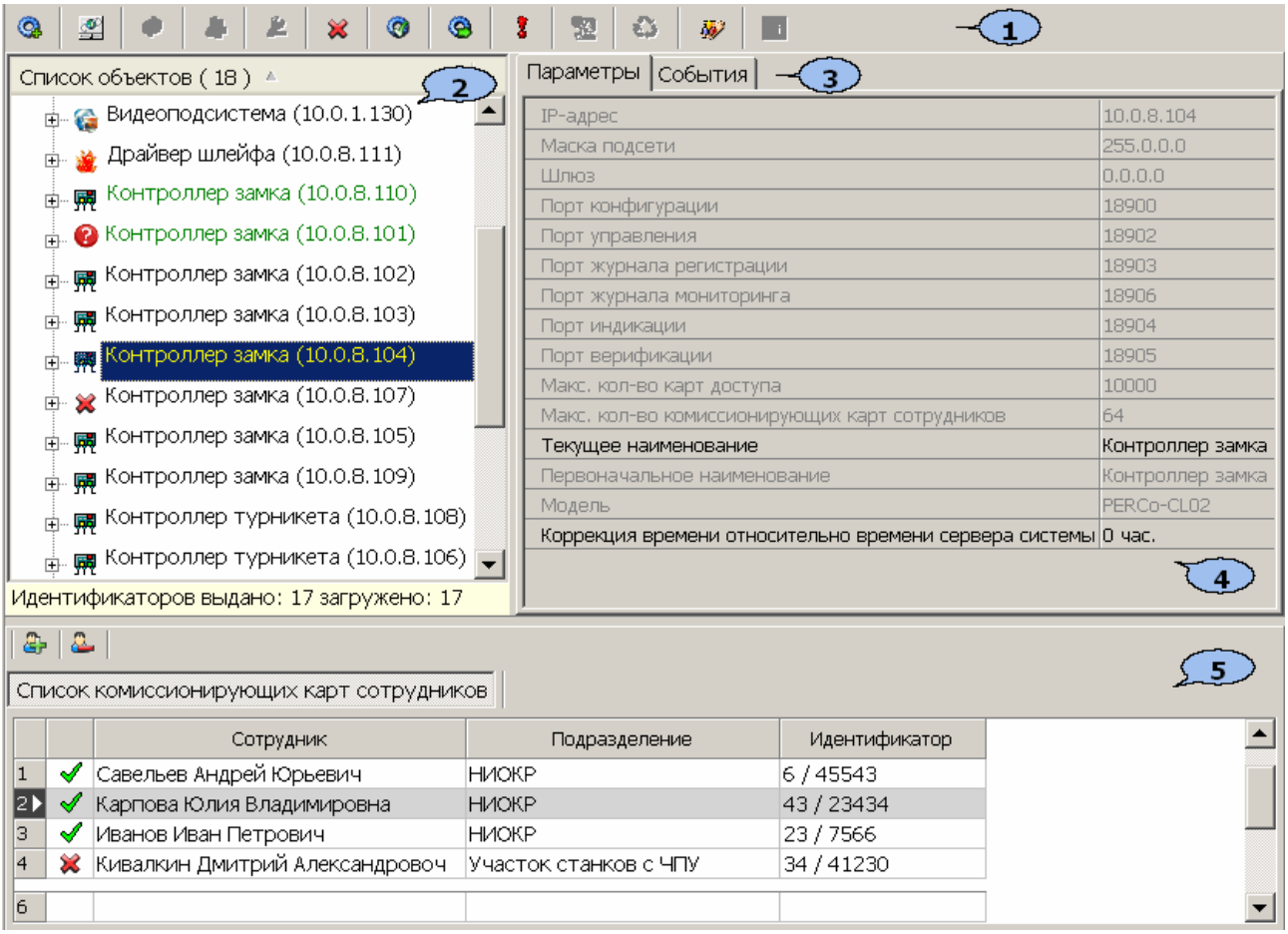
7 КОНФИГУРАЦИЯ СИСТЕМЫ БЕЗОПАСНОСТИ

Конфигурация системы безопасности производится в разделе «*Конфигуратор*». Раздел предназначен для описания параметров функционирования устройств и программного обеспечения системы безопасности *PERCo-S-20*. Раздел позволяет:

- Включать и исключать устройства из состава системы.
- Настраивать параметры работы устройств.
- Устанавливать реакции системы на события устройств.
- Создавать списки комиссионирующих карт.
- Создавать списки карт аварийного доступа для контроллеров второго уровня.

7.1 Рабочее окно раздела «Конфигуратор»

Рабочее окно раздела состоит из следующих элементов:



1. Панель инструментов раздела

   – Кнопка **Провести конфигурацию** (**Ctrl**+**K**) позволяет произвести автоматический поиск устройств в сети и подключение их к серверу системы.

   – Кнопка **Добавить новое устройство** (**Ctrl**+**F**) позволяет открыть панель **Поиск нового устройства** для подключения устройства известного типа по его IP-адресу.

   – Кнопка **Обновить конфигурацию** (**Ctrl**+**Alt**+**K**) позволяет для контроллера PERCo-CT/L04 привести в соответствие информацию, отображаемую в системе, с физическим состоянием контроллера. Такая процедура может потребоваться после изменения его конфигурации при помощи перемычек или после изменения состава подключенных

контроллеров второго уровня. Также кнопка позволяет обновить конфигурацию драйвера шлейфа PERCo-PF01-01-02 адресной пожарной сигнализации.

– Кнопка **Добавить группу ресурсов** (**Ctrl**+**N**) позволяет добавить до 7 групп ресурсов. Кнопка доступна при выборе в рабочей области раздела ресурса контроллера **Группа ресурсов**.

– Кнопка **Удалить** (**Ctrl**+**D**) позволяет удалить из конфигурации устройство, выделенное в рабочей области раздела. Кнопка доступна, если выделенное устройство ранее было исключено из конфигурации при помощи кнопки .

– Кнопка **Исключить из конфигурации** (**Ctrl**+**O**) позволяет временно исключить выделенное в рабочей области устройство из конфигурации. Для включения в конфигурацию ранее исключенного устройства нажмите кнопку еще раз.

– Кнопка **Передать параметры** (**Ctrl**+**H**) позволяет передать параметры в устройство, выделенное в рабочей области раздела. При выборе корневого элемента списка объектов (по умолчанию *«Система безопасности»*) соответствующие параметры будут переданы во все устройства, включенные в конфигурацию.

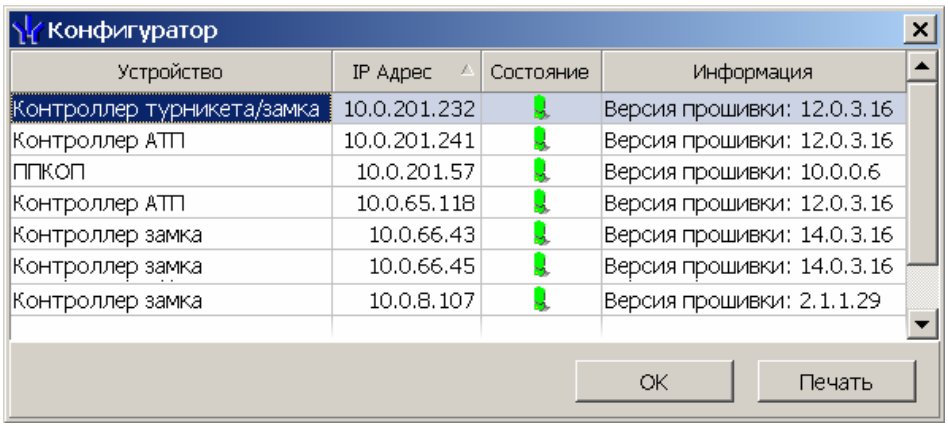
– Кнопка **Передать измененные параметры** (**Ctrl**+**Alt**+**H**) позволяет передать только измененные параметры в устройство, выделенное в рабочей области раздела. Кнопка доступна в случае, если параметры устройства были изменены. При выборе корневого элемента списка объектов (по умолчанию *«Система безопасности»*) будут переданы измененные параметры для всех устройств, включенных в конфигурацию.

– Кнопка **Отображать скрытые устройства** (**Ctrl**+**Alt**+**V**) позволяет просматривать в рабочей области скрытые устройства.

– Кнопка **Изменение пароля** (**Ctrl**+**P**) позволяет изменить пароль доступа к контроллерам системы безопасности. Кнопка доступна при выборе в рабочей области корневого элемента списка объектов (по умолчанию «*Система безопасности»*).

– Кнопка **Изменение сетевых настроек** (**Ctrl**+**T**) позволяет изменить сетевые настройки выбранного в рабочей области контроллера.

– Кнопка **Получить информацию о версиях прошивок** (**Shift**+**Ctrl**+**V**) позволяет открыть окно **Конфигуратор** для просмотра списка контроллеров системы безопасности с указанием версий установленных прошивок:



Кнопка **Печать** позволяет распечатать список.

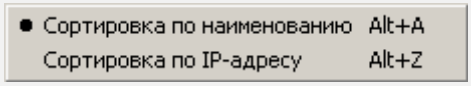
– Кнопка **Получить состояние TCP/IP портов** позволяет получить диагностическую информацию о состоянии портов выбранного в рабочей области контроллера. Кнопка доступна после исключения выбранного контроллера из конфигурации, то есть при нажатии кнопки . Кнопка никогда не доступна для контроллеров CL01, CL02, CL03, CT01, CT02 (встроенного контроллера электронной проходной KT02).

2. Рабочая область раздела **Список объектов** содержит раскрывающийся многоуровневый список устройств и их ресурсов.

   Выделение устройства зеленым цветом означает, что параметры устройства были изменены, но не переданы. Выделение устройства красным означает, что оно скрыто (скрытые устройства отображаются при нажатии кнопки в панели инструментов) .Значки рядом с наименованиями устройств означают:
   – устройство исключено из конфигурации системы безопасности,
   – устройство включено в конфигурацию системы безопасности, но не доступно, или ему не переданы параметры,
   , , – устройство является контроллером, включенным в конфигурацию системы безопасности,
   – устройство является видеоподсистемой, включенной в конфигурацию системы безопасности,
   – устройство является драйвером шлейфа PERCo-PF01-01-02 адресной пожарной сигнализации, включенным в конфигурацию системы безопасности.

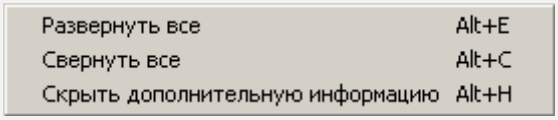
Примечание

1. В рабочей области раздела реализована сортировка по наименованию устройств или по их IP-адресу. Для выбора типа сортировки нажмите правой кнопкой мыши на заголовке рабочей области **Список объектов** и выберите тип в открывшемся контекстном меню:



Используйте стрелку рядом с заголовком рабочей области для выбора прямого ( ) или обратного ( ) порядка сортировки устройств.

2. При нажатии правой кнопкой мыши в рабочей области раздела откроется контекстное меню:



Меню позволяет развернуть, свернуть списки ресурсов для всех устройств, а также открыть и скрыть панель ввода дополнительных данных.

3. Выбор вкладки панели настройки

   - **Параметры.** Вкладка позволяет настроить параметры функционирования устройства или ресурса, выделенного в рабочей области **Список объектов**. Описание параметров приводится в *«Руководстве по эксплуатации»* на устройство.
   - **События.** На вкладке отображается список событий, регистрируемых системой безопасности для устройства или ресурса, выделенного в рабочей области **Список объектов**. Также на вкладке можно задать

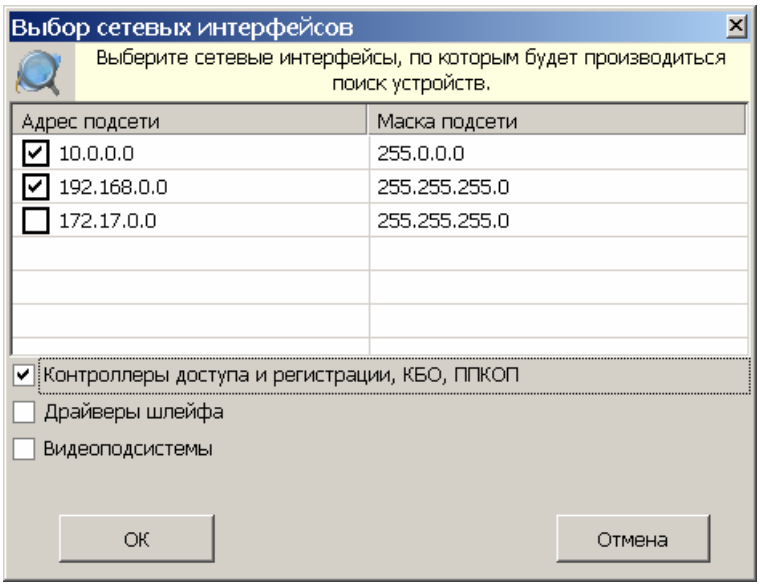
реакцию системы на любое из событий. Описание событий и реакций на события приводится в *«Руководстве по эксплуатации»* на устройство.

4. Рабочая область вкладки панели настройки.
5. Панель ввода дополнительных данных. Для открытия и скрытия панели используйте контекстное меню рабочей области раздела или сочетание клавиш **Alt+H**.
   Значок ✖ в строке с данными сотрудника или PIN-кодом в рабочей области вкладки означает, что данные не были переданы в контроллеры, значок ✔ означает, что данные переданы успешно.

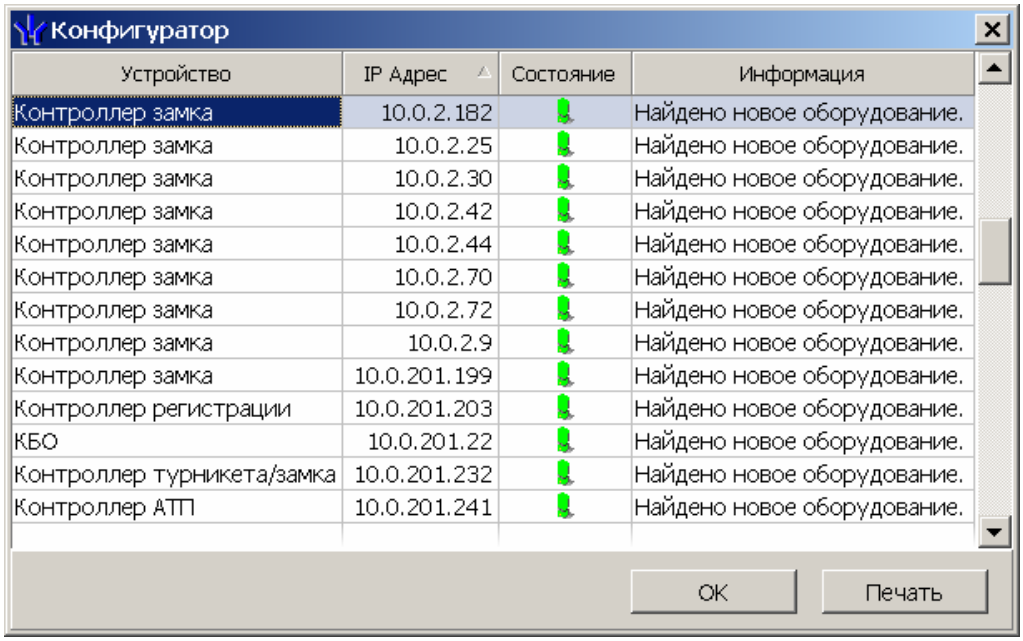
7.2 Автоматическая конфигурация

Для проведения автоматического поиска устройств в локальной сети:

1. Нажмите кнопку  на панели инструментов раздела. Откроется окно **Выбор сетевых интерфейсов**:



2. В рабочей области открывшегося окна отметьте флажками адреса подсетей, в которых будет производиться поиск устройств. В нижней части окна отметьте флажками типы искомых устройств. Нажмите кнопку **ОК**. Начнется поиск устройств.
3. После завершения поиска откроется окно **Конфигуратор** со списком найденных устройств:

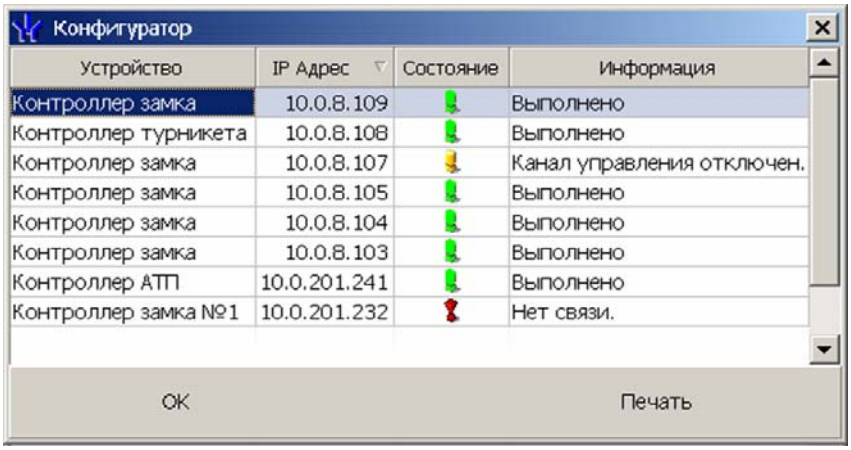


Кнопка **Печать** позволяет распечатать список найденных устройств.

4. Нажмите кнопку **ОК** (или ☒ в заголовке окна). Все найденные устройства будут добавлены в рабочую область раздела **Список объектов** и отмечены значками ❓.
5. Если какое-либо из найденных устройство необходимо исключить из конфигурации, выделите его в рабочей области и нажмите кнопку ✖ на панели инструментов.
6. Для настройки параметров выделите устройство или ресурс в рабочей области раздела и на вкладке **Параметры** панели настройки измените необходимые параметры.
7. Для настройки реакций на события выделите устройство или ресурс в рабочей области раздела и на вкладке **События** панели настройки добавьте необходимые реакции.
8. Выделите в рабочей области раздела **Список объектов** корневой элемент (по умолчанию *«Система безопасности»*) и нажмите кнопку на панели инструментов раздела. В устройства будут переданы параметры конфигурации. Значки устройств в рабочей области изменят свой вид, в зависимости от типа: , , , .

7.3 Состояние связи с устройствами

В случае, если серверу системы не удастся передать параметры в устройства, откроется окно **Конфигуратор** с описанием состояния связи.



Устройство – в столбце указан тип устройства.
IP-адрес – в столбце указан адрес устройства в сети.
Состояние – в столбце отображено состояние связи с устройством:

– связь установлена,

– санкционированное отключение связи,

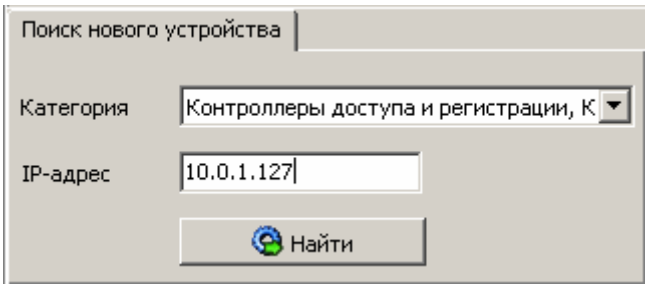
– несанкционированная потеря связи.

Информация – в столбце выводится результат передачи данных в устройство.
ОК – кнопка позволяет закрыть окно.
Печать – кнопка позволяет распечатать результаты передачи данных.

7.4 Добавление нового устройства

Если устройство не было найдено при автоматической конфигурации или необходимо добавить в систему только определенные устройства с известными IP-адресами, то можно добавить их вручную. Для добавления нового устройства:

1. Нажмите кнопку  на панели инструментов раздела. Откроется панель **Поиск нового устройства**:



2. В строку **IP-адрес** введите адрес искомого устройства. Нажмите ставшую доступной кнопку **Найти**.

Примечание

IP-адрес контроллера указан в паспорте и на плате устройства.

Для подключения к контроллеру по сети *Ethernet* необходимо, чтобы компьютер находился в одной подсети с контроллером.

3. Нажмите **ОК** в появившемся диалоговом окне **Сообщение**. Найденное устройство будут добавлено в рабочую область раздела **Список объектов** и отмечено значками .
4. Для настройки параметров выделите устройство или его ресурс в рабочей области раздела и на вкладке **Параметры** панели настройки измените необходимые параметры.
5. Для настройки реакций на события выделите устройство или его ресурс в рабочей области раздела и на вкладке **События** панели настройки добавьте необходимые реакции.
6. Для передачи новых параметров в устройство нажмите кнопку на панели инструментов раздела.

7.5 Удаление и восстановление устройства

Внимание!

Прежде чем удалять устройство из конфигурации, необходимо убедиться, что оно не связано ни с одним помещением в разделе *«Помещения и мнемосхема»* модуля *PERCo-SN01 «Базовое ПО»*.

В обратном случае удалить устройство из конфигурации будет нельзя, его можно будет только скрыть. Отобразить скрытые ранее устройства в рабочей области **Список объектов** можно при помощи кнопки , при этом они выделяются красным цветом.

Для удаления устройства

1. Выделите устройство в рабочей области раздела **Список объектов**.
2. Исключите устройство из конфигурации, нажав кнопку в панели инструментов раздела.
3. Удалите устройство, нажав кнопку в панели инструментов раздела. В открывшемся окне **Сообщение** для подтверждения нажмите кнопку **Да**.
4. Если устройство связано с помещением, появится окно **Сообщение** с предложением скрыть устройство. Нажмите **Да,** если хотите скрыть устройство.

Восстановить можно только скрытое устройство. Удаленное устройство необходимо заново добавлять в конфигурацию. Для восстановления скрытого устройства:

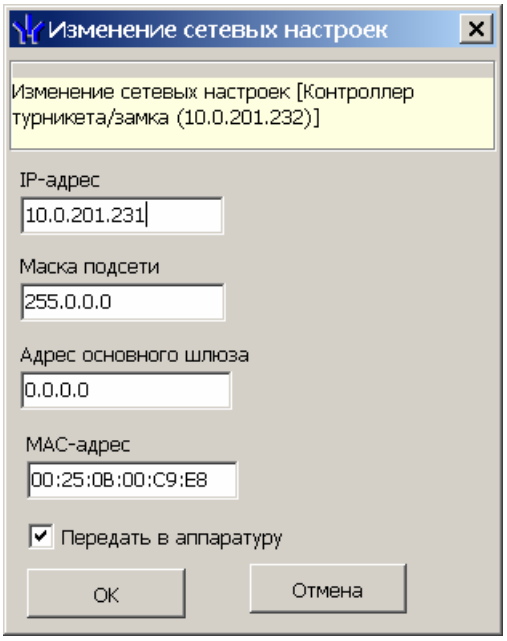
1. Нажмите кнопку на панели инструментов раздела. В рабочей области раздела станут видны скрытые устройства, выделенные красным.
2. Выделите в рабочей области скрытое устройство, которое необходимо восстановить и нажмите кнопку . В открывшемся окне **Сообщение** нажмите кнопку **Да**.
3. Для включения устройства в конфигурацию нажмите кнопку на панели инструментов раздела.
4. Для передачи параметров в устройство нажмите кнопку в панели инструментов раздела.

7.6 Изменение сетевых настроек

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

Для изменения сетевых настроек:

1. Выделите в рабочей области **Список объектов** раздела контроллер, сетевые настройки которого необходимо изменить.
2. Исключите контроллер из конфигурации системы безопасности. Для этого нажмите кнопку  на панели инструментов.
3. Для изменения сетевых настроек нажмите кнопку  Откроется окно **Изменение сетевых настроек**:



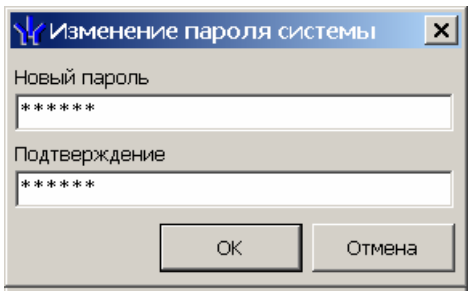
4. В открывшемся окне измените необходимые сетевые настройки контроллера. Если измененные настройки необходимо передать в контроллер сразу после закрытия окна установите флажок **Передать в аппаратуру**.
5. Нажмите кнопку **ОК** для применения измененных настроек или кнопку **Отмена**, для отмены изменений.
6. Если в окне **Изменение сетевых настроек** флажок **Передать в аппаратуру** не был установлен, то для передачи измененных настроек в контроллер необходимо дополнительно нажать кнопку  или  на панели инструментов.

7.7 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:

1. Выберите в рабочей области раздела корневого элемента списка объектов (по умолчанию «*Система безопасности*»).
2. Нажмите кнопку  на панели инструментов. Откроется окно **Изменение пароля системы**:



3. В поля **Новый пароль** и **Подтверждение** введите пароль и нажмите кнопку **ОК**.

Примечание

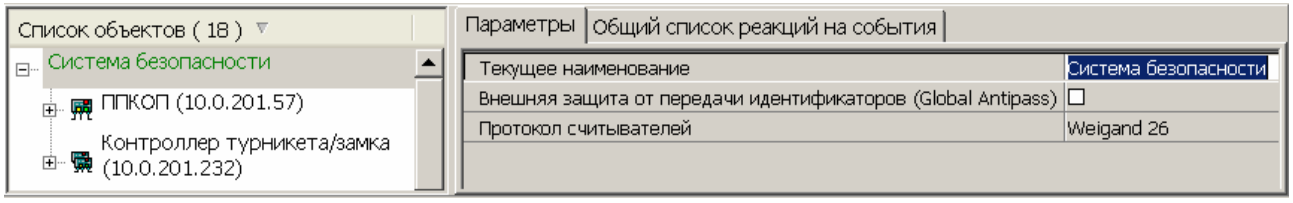
Длина пароля не должна превышать 10 символов. Для создания пароля можно использовать латинский алфавит и цифры.

4. Передайте измененный пароль в контроллеры. Для этого нажмите кнопку или на панели инструментов.

7.8 Параметры системы безопасности

Для настройки параметров системы безопасности в области **Список объектов** выберите корневой элемент (по умолчанию «*Система безопасности*»).

На вкладке **Параметры** будут доступны следующие параметры:



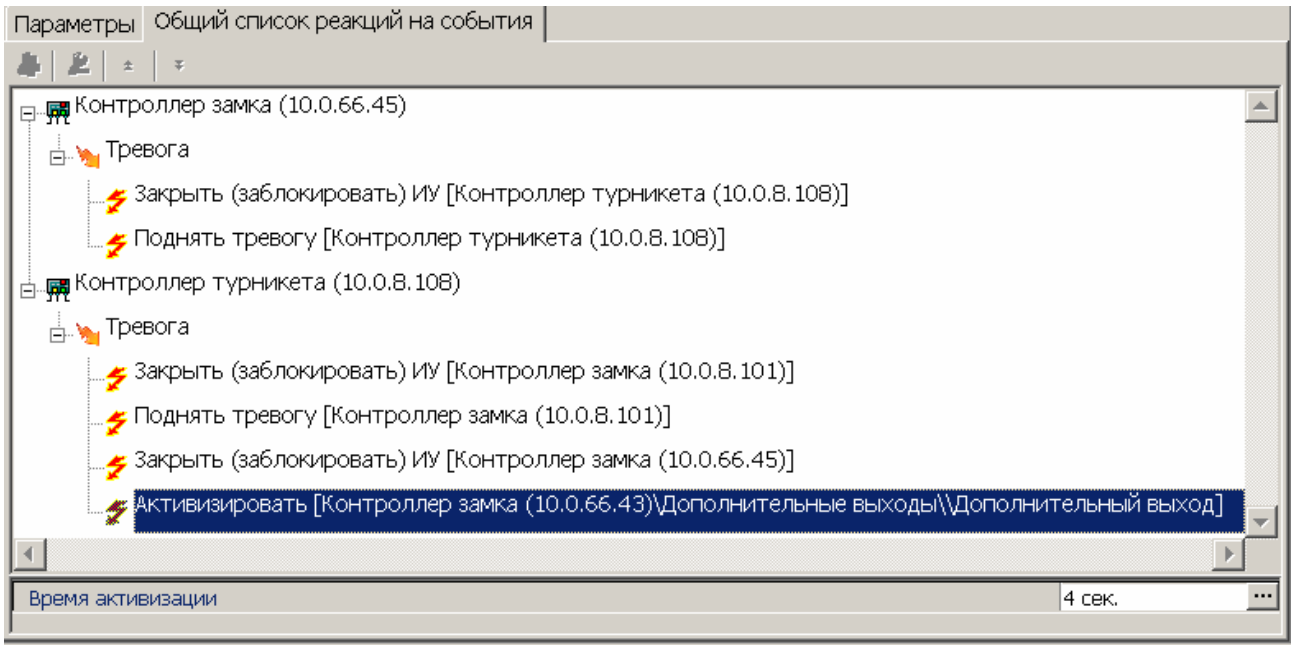
Поле ввода **Текущее наименование** позволяет ввести название системы безопасности.

Внешняя защита от передачи идентификаторов (Global Antipass). При установке флажка система безопасности будет контролировать последовательность прохождения (регистрации) сотрудников (посетителей) через точки прохода, с учетом направления прохода. Последовательность прохождения точек прохода определяется взаимным расположением пространственных зон с учетом их вложенности. (То есть нельзя войти в помещение, не войдя в здание.)

Протокол считывателей. Раскрывающийся список позволяет выбрать формат хранения идентификаторов в системе. Доступны следующие форматы:

- **Сокращенный (4 байта);**
- **Wiegand 26** (установлен по умолчанию);
- **Универсальный (8 байт).**

На вкладке **Общий список реакций на события** отображается список устройств, для событий которых в системе установлены какие-либо реакции, с указанием этих реакций в виде раскрывающегося списка. При двойном нажатии левой кнопкой мыши на устройстве в рабочей области вкладки отобразится полный список событий этого устройства.



7.9 Вкладка «Параметры»

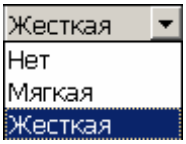
На вкладке выводится список параметров и характеристик, доступных для устройства или ресурса устройства, выделенного в рабочей области раздела.

Выделение параметров синим цветом означает, что значения параметров были изменены, и внесенные изменения не были переданы в устройства.

Для настройки параметра нажмите правой кнопкой мыши в правом столбце рабочей области вкладки в строке с наименованием параметра. Используются следующие способы ввода значений параметров:

Поле ввода позволяет ввести данные (наименование, значение) при помощи клавиатуры.

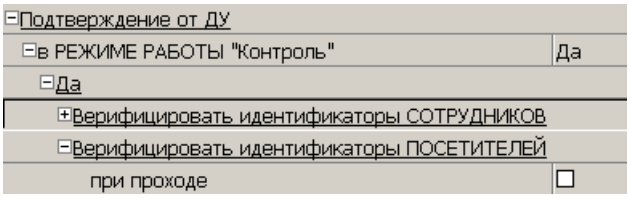
Раскрывающийся список позволяет выбрать одно из предложенных значений параметра. Для раскрытия списка необходимо нажать кнопку справа от установленного ранее значения.



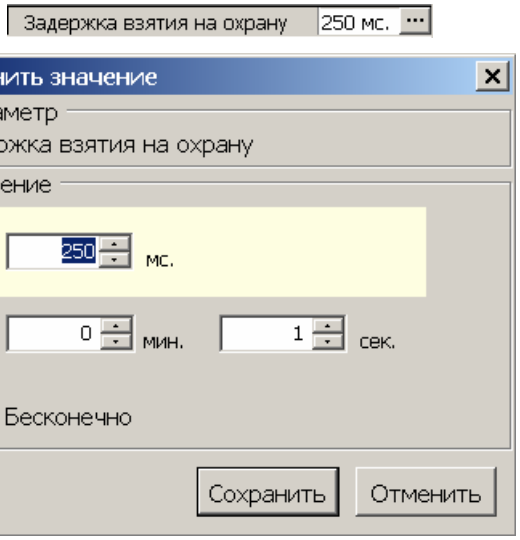
Флажок. Установка или снятие флажка позволяет включить или выключить необходимый параметр.

Счетчик позволяет установить числовое значение параметра. Для увеличения / уменьшения значения параметра используйте кнопки, либо введите значение параметра с помощью клавиатуры.

Раскрывающийся многоуровневый список позволяет получить доступ к группе параметров при нажатии на значок ⊞ для их настройки, либо скрыть их, нажав значок ⊟.



С использованием дополнительного окна Для открытия окна необходимо нажать кнопку ··· справа от установленного ранее значения параметра.



7.10 Вкладка «События»

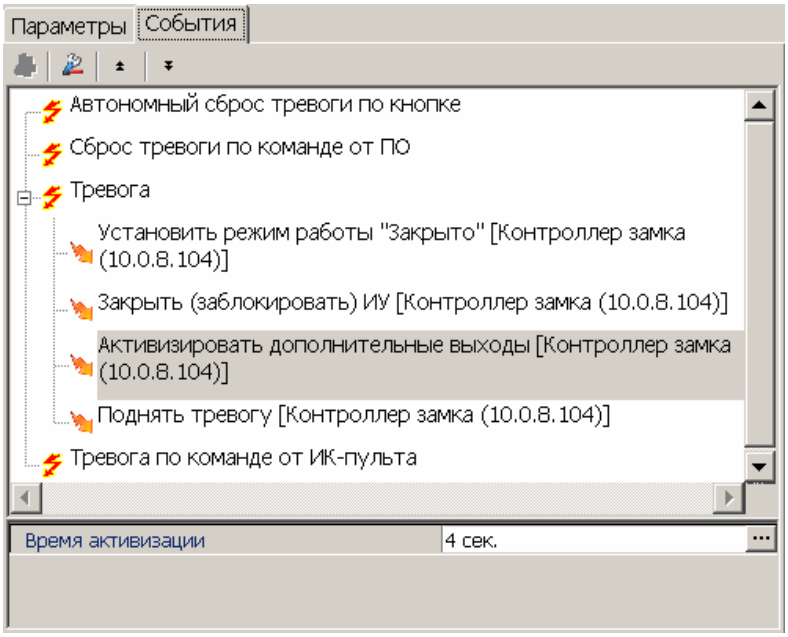
В процессе работы контроллер записывает в журнал регистрации события, связанные с каждым из ресурсов. Список возможных событий каждого ресурса приведен на вкладке **События**. В системе реализована возможность задать реакцию на любое из этих событий.

Например, вы можете задать автоматическое включение записи на камере видеонаблюдения при предъявлении запрещенной карты доступа, или автоматически открыть дверь, разблокировать турникеты при срабатывании пожарных извещателей.

Внимание!

Заданные в виде реакций на события действия будут выполняться только при запущенном сервере системы безопасности и наличием связи с соответствующим устройством.

7.10.1 Описание вкладки



На вкладки **События** доступны следующие инструменты:

– Кнопка **Добавить реакцию на событие** (**Alt+N**) позволяет открыть окно **Выбор реакции на событие** для выбранного в рабочей области панели события.

– Кнопка **Удалить реакцию на событие** (**Alt+D**) позволяет удалить выбранную в рабочей области реакцию на событие.

– Кнопка **Переместить вверх** (**Ctrl+Up**) позволяет переместить выбранную в рабочей области реакцию на событие вверх в порядке следования реакций.

– Кнопка **Переместить вниз** (**Ctrl+Down**) позволяет переместить выбранную в рабочей области реакцию на событие вниз в порядке следования реакций.

В рабочей области вкладки **События** значками отмечены:

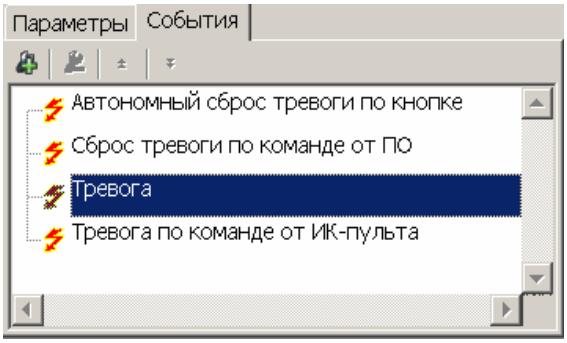
– Регистрируемое устройством или ресурсом событие.

– Установленная на событие реакция со стороны системы. Для некоторых реакций доступна панель для задания дополнительных параметров.

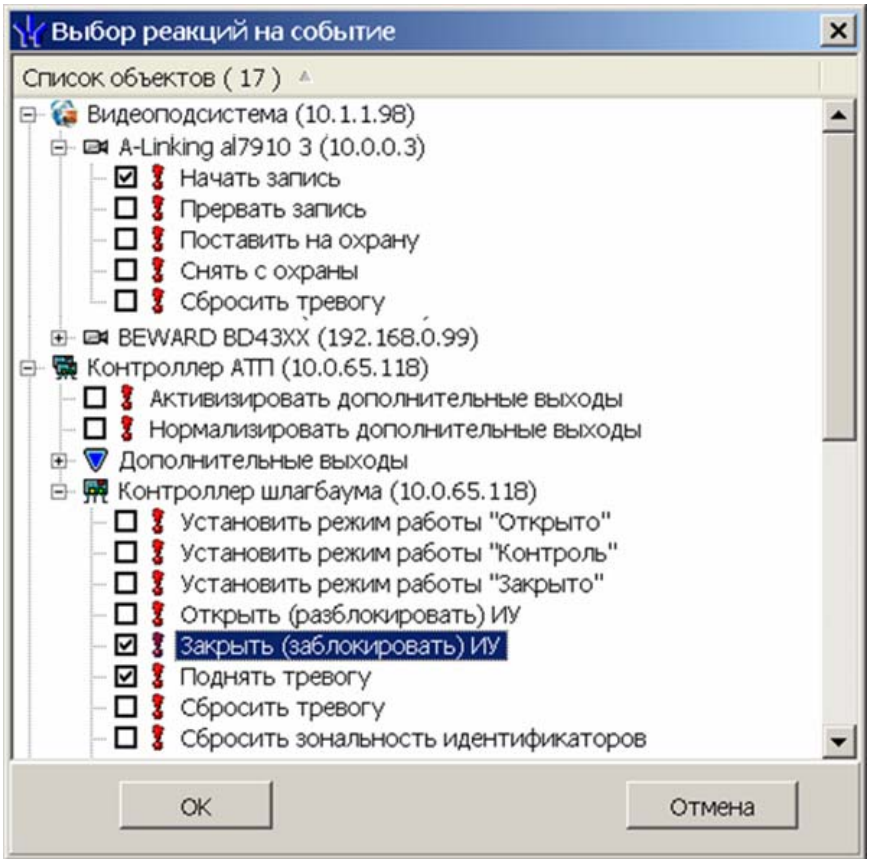
7.10.2 Задание реакции на событие

Для задания реакции на событие устройства или ресурса:

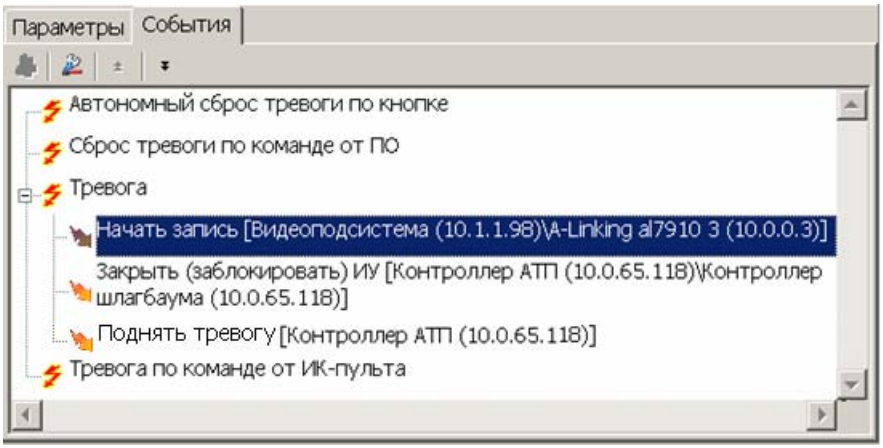
1. Выделите устройство или ресурс, на событие которого необходимо задать реакцию системы, в рабочей области раздела **Список объектов**.
2. На панели настройки перейдите на вкладку **События**.



3. Выделите событие, на которое необходимо задать реакцию системы, и нажмите кнопку  . Откроется окно **Выбор реакций на событие**:



4. В открывшемся окне отметьте в раскрывающемся многоуровневом списке устройств системы безопасности флажками требуемые реакции на события. Можно задать одновременно несколько реакций на событие, как у одного, так и у нескольких устройств и ресурсов. Нажмите кнопку **ОК**.
5. Отмеченные реакции будут добавлены в рабочую область вкладки **События** для выделенного события.



6. Установите порядок следования реакций на события, используя кнопки , в инструментах панели.
7. При необходимости установите длительность реакции на панели для ввода дополнительных параметров.
8. Для удаления выделенной в рабочей области реакции на событие нажмите кнопку . В открывшемся окне подтверждения нажмите **Да**.
9. Нажмите кнопку **Сохранить** на панели инструментов *«Консоли управления»*.

8 ПАРАМЕТРЫ УСТРОЙСТВ

8.1 Описание параметров контроллеров доступа

В зависимости от типа контроллера наличие и количество ресурсов может различаться. В таблице 3 представлен перечень ресурсов контроллера в разных вариантах конфигурации.

Для доступа к списку ресурсов контроллера нажмите на ⊞ рядом с названием контроллера в области **Список объектов** раздела **Конфигуратор**. Откроется список доступных ресурсов контроллера, сгруппированных по типам:

- Дополнительные входы;
- Дополнительные выходы;
- Шлейфы сигнализации;
- Охранные зоны;
- Контроллер *И*У (замка, турникета, шлагбаума);

Если к контроллеру подключены несколько исполнительных устройств или замковые контроллеры *PERCo-CL201,* то в списке ресурсов будет отображаться несколько контроллеров *И*У. Каждый контроллер *И*У также обладает своим списком ресурсов:

- Считыватель;
- ИУ (замок, турникет, шлагбаум);
- Генератор тревоги;
- ОЗ.

Таблица 3 Ресурсы контроллеров

Модель	Доп. вход	Доп. выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считы-ватель	ИУ	Ген. тревоги	ОЗ
Контроллеры									
CL201	0	0	0	0	-	1	замок	1	1
CT/L04 (1*)	2	4	2	2	0	2	замок	1	1
CT/L04 (2)	2	4	2	2	8	2	замок	1	1
CT/L04(3)	2	4	2	2	8	2	2 замка	2	2
CT/L04(4)	2	2	0	0	0	2	турникет	1	0
CT/L04(5)	2	2	0	0	8	2	турникет	1	0
CT/L04(6)	2	2	0	0	0	2	шлагбаум	1	0
CT/L04(7)	2	2	0	0	8	2	шлагбаум	1	0
CL05	0	1	0	0	0	1	замок	1	1
Электронные проходные									
KT02.3, KT02.7, KT05.3, KTC01.3, KR05.3, KR05.4	2	2	0	0	8	2	турникет	1	0

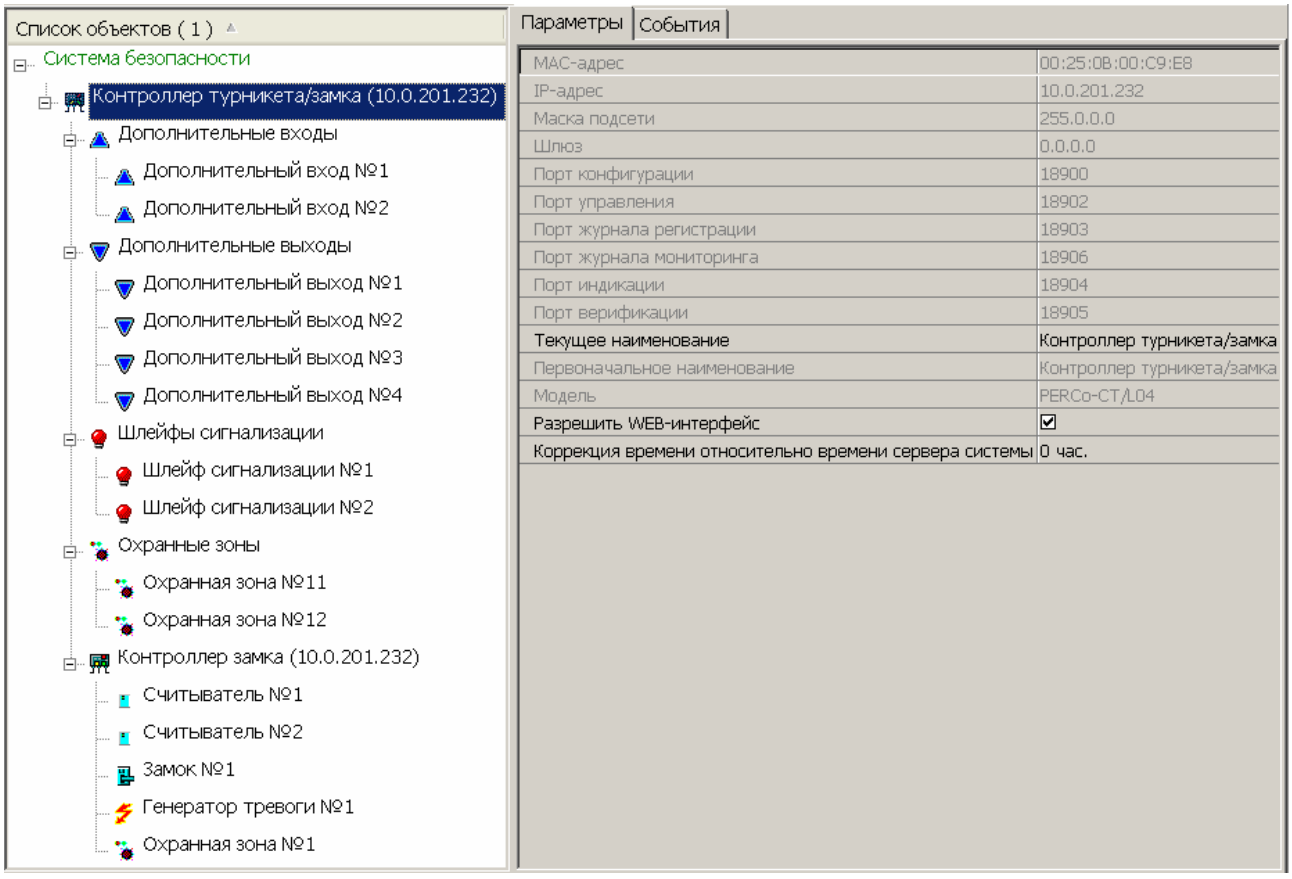
*Для контроллера PERCo-CT/L04 в скобках указан вариант конфигурации.

Варианты конфигурации контроллера PERCo-CT/L04:

1. Контроллер для управления одной двухсторонней дверью.
2. Контроллер для управления одной двухсторонней дверью с подключением до 8 контроллеров замка *PERCo-CL201*.
3. Контроллер для управления двумя односторонними дверьми с подключением до 8 контроллеров замка *PERCo-CL201*.
4. Контроллер для управления турникетом.
5. Контроллер для управления турникетом с подключением до 8 контроллеров замка *PERCo-CL201*.
6. Контроллер автотранспортной проходной.
7. Контроллер автотранспортной проходной с подключением до 8 контроллеров замка *PERCo-CL201*.

Для настройки параметров выделите в списке необходимый ресурс и перейдите на вкладку **Параметры** в правой части экрана.

8.1.1 Контроллер



Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название контроллера.

Разрешить Web-интерфейс. Флажок определяет, будет ли поддерживаться возможность конфигурации контроллера через Web-интерфейс.

- Флажок снят. Доступ к контроллеру через Web-интерфейс запрещен.
- Флажок установлен. Доступ к контроллеру через Web-интерфейс разрешен.

Примечание

По умолчанию при подключении к контроллеру Web-интерфейс отключен.

Доступ через Web-интерфейс будет возможен после остановки сервера системы *PERCo-S-20* или удалении контроллера из списка объектов. Для остановки сервера: выйдите из *«Консоли управления PERCo-S-20»*; запустите *«Центр управления PERCo-S-20»*; перейдите на вкладку **Настройка серверов**; в области **Сервер системы PERCo-S-20** нажмите кнопку **Остановить**; индикатор справа от кнопки станет красным, сервер будет остановлен.

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

На вкладке **События** можно установить следующие реакции данного ресурса на события системы:

Активизировать дополнительные выходы. Приводит к активизации всех релейных выходов выбранного контроллера, для которых выбран **Тип**: **Обычный**.

Нормализовать дополнительные выходы. Приводит к нормализации всех релейных выходов данного контроллера, для которых выбран **Тип**: **Обычный**.

8.1.2 Дополнительный вход

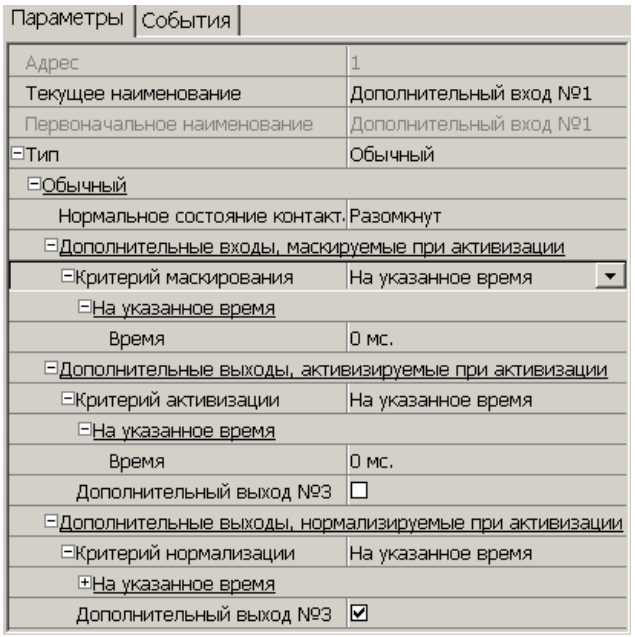
Дополнительные входы контроллеров могут быть использованы для наблюдения за состоянием внешнего оборудования, подключенного к ним, и для подключения кнопок сброса тревоги и активизации режима **FireAlarm** турникета.

Для настройки ресурса доступны следующие параметры:

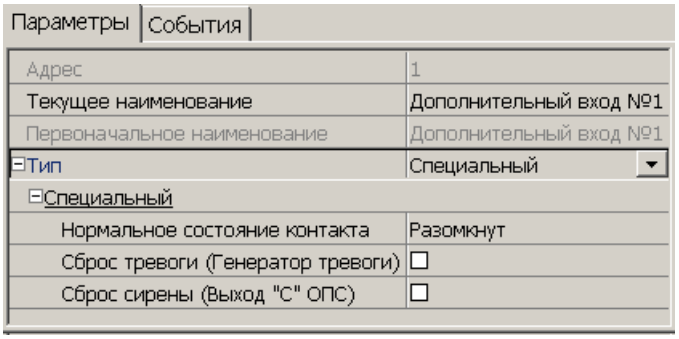
Текущее наименование. Поле ввода позволяет ввести описательное название входа.

Тип. Раскрывающийся список позволяет выбрать следующие типы входа:

- **Нет.** К данному входу не подключено никакое внешнее оборудование.
- **Обычный.** К данному входу подключено внешнее оборудование, состояние которого должно контролироваться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.



- **Специальный.** Предназначен для автономного сброса тревоги, выключения сирены либо перевода турникета в режим **FireAlarm** при поступлении управляющего сигнала на этот дополнительный вход.



Нормальное состояние контакта (*Разомкнут / Замкнут*). Этот параметр зависит от типа подключенного оборудования и указывает контроллеру на то, какое значение уровня сигнала на данном дополнительном входе он должен воспринимать как нормальное.

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 флажками те дополнительные входы, которые должны быть маскированы. Укажите временной критерий маскирования.

Дополнительные выходы, активизируемые при активизации. Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Укажите временной критерий активизации.

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

Временной **Критерий маскирования/активизации/нормализации**:

- **На указанное время.** Выбранные дополнительные входы будут маскированы на указанное время.
- **На время срабатывания.** Выбранные дополнительные входы будут маскированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
- **На время срабатывания и после срабатывания.** Выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал, плюс указанное вами время.

Сброс тревоги (Генератор тревоги). При установке флажка получение управляющего сигнала на данном дополнительном входе приведет к сбросу тревоги.

Сброс сирены (Выход «С» ОПС). При установке флажка получение управляющего сигнала на данном дополнительном входе приведет к выключению сирены, подключенной к выходу, работающему по программе «Сирена».

FireAlarm. Режим работы турникета в случае возникновения пожара. Турникет в этом режиме разблокирован для прохода в обоих направлениях. Для активизации режима необходимо подать управляющий сигнал на **Дополнительный вход**, сконфигурированный как **Специальный**. При этом ни один из флажков **Сброс тревоги (Генератор тревоги), Сброс сирены (Выход «С» ОПС),** не должен быть установлен.

8.1.3 Дополнительный выход

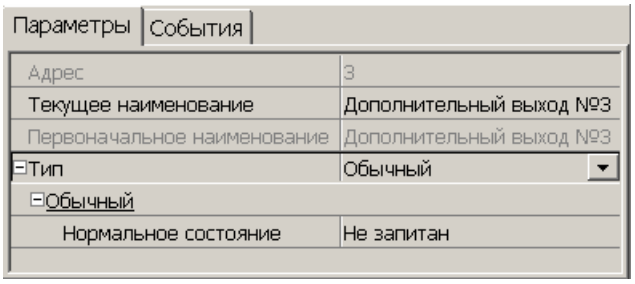
Дополнительные выходы могут быть использованы для управления любым дополнительным оборудованием в рамках системы *PERCo-S-20*.

Для настройки ресурса доступны следующие параметры:

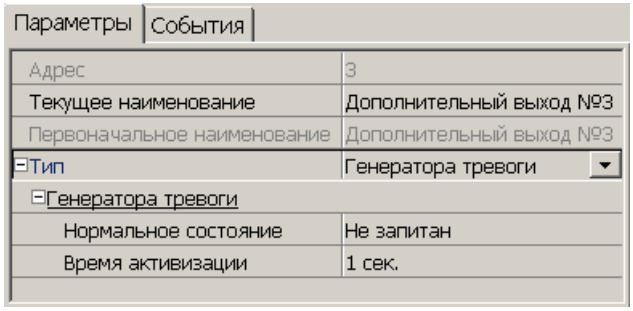
Текущее наименование. Поле ввода позволяет ввести описательное название выхода.

Тип. Раскрывающийся список позволяет выбрать следующие типы выхода:

- **Нет.** К данному выходу не подключено никакое внешнее оборудование.
- **Обычный.** К выходу подключено дополнительное оборудование, логика управления которым описывается через описание других устройств системы (за исключением генератора тревоги).

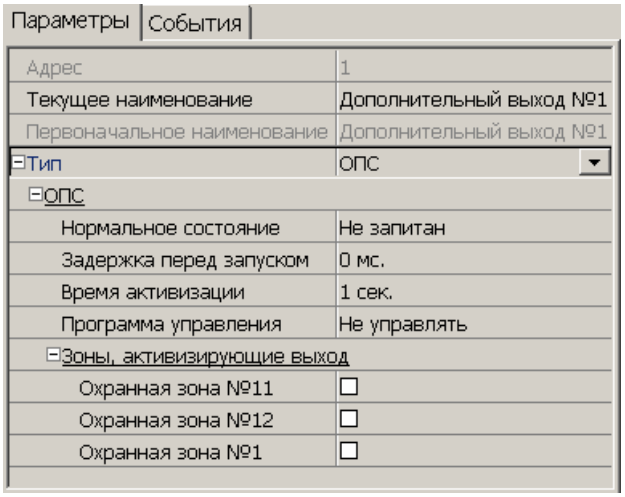


- **Генератор тревоги.** Решение об активизации дополнительного выхода принимается в соответствии с параметрами, указанными в генераторе тревоги. Этот дополнительный выход будет использоваться для индикации перехода в состояние *«Тревога».*



- **ОПС.** Выход предназначен для управления световым оповещением, звуковым оповещением, а также для передачи тревожных извещений на пульт центрального наблюдения при изменении режимов и состояний охранной зоны. Программа управления задает логику работы контроллера по управлению этим дополнительным выходом. Инициатором активизации выхода являются изменения режимов и состояний охранных зон, отмеченных как **Зоны, активизирующие выход**. После возникновения события,

инициирующего активизацию выхода (в соответствии с заданной программой), начинается отсчет задержки, указанной в параметре **Задержка перед запуском**, после чего выход активизируется. В зависимости от параметра **Программа управления** выход может быть запитан (не запитан) постоянно (пока ресурс панели находится в текущем режиме), либо изменять свое физическое состояние (мигать) из нормализированного на противоположное. Нормализация выхода происходит либо по истечению времени, указанному в параметре **Время активизации** (если оно не бесконечное), либо по сбросу панели, либо после выключения ее питания.



Нормальное состояние (*Не запитан / Запитан*). Параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий.

Задержка перед запуском. Промежуток времени между изменением состояния ОЗ и запуском программы управления выходом.

Время активизации. Время, в течение которого при наличии активизирующего управляющего воздействия выход меняет свое состояние из нормализированного на противоположное. Как правило, в этом случае к такому дополнительному выходу подключают тревожный оповещатель (сирена, проблесковая лампа).

Программа управления. Режим работы выхода после активизации. Доступны следующие программы:

- **Не управлять.**
- **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 замыкание/размыкание 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 **хотя бы одна из зон** изменила 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.

Зоны, активизирующие выход. Параметр позволяет выбрать охранные зоны, нарушение которых приведет к активизации выхода.

Примечание

После включения питания все выходы нормализуются.

На вкладке **События** можно установить следующие реакции данного ресурса на события системы:

Активизировать. Приводит к переводу выбранного релейного выхода в активное состояние на время, установленное параметром **Время активизации** для данного выхода.

Нормализовать. Приводит к переводу выбранного релейного выхода в нормальное (исходное) состояние.

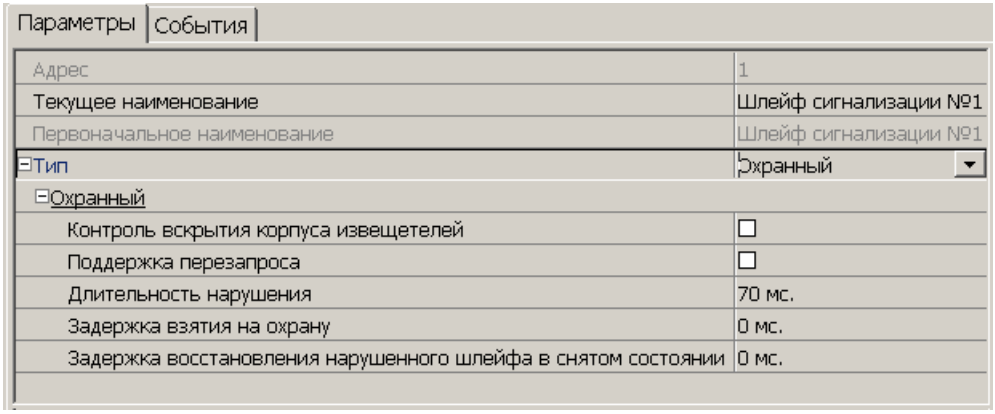
8.1.4 Шлейф сигнализации

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. Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название шлейфа сигнализации.

Тип. Раскрывающийся список позволяет выбрать тип ШС:

- **Нет.** ШС не подключен.
- **Охранный.** Подключен охранный ШС.



Контроль вскрытия корпуса извещателей. При установке флажка шлейф контролирует вскрытие корпусов извещателей.

Поддержка перезапроса. При установке флажка контроллер после срабатывания извещателей снимает питание со шлейфа и перепроверяет его состояние.

Длительность нарушения. Параметр определяет время интегрирования для шлейфа, то есть максимальное время нарушения, не приводящее к переходу в режим *«Тревога»*.

Задержка взятия на охрану. Параметр определяет время, через которое панель предпринимает попытку взять шлейф на охрану после поступления соответствующей команды. Время, определяемое значением этого параметра, может быть использовано как «задержка на выход» для шлейфов входных зон.

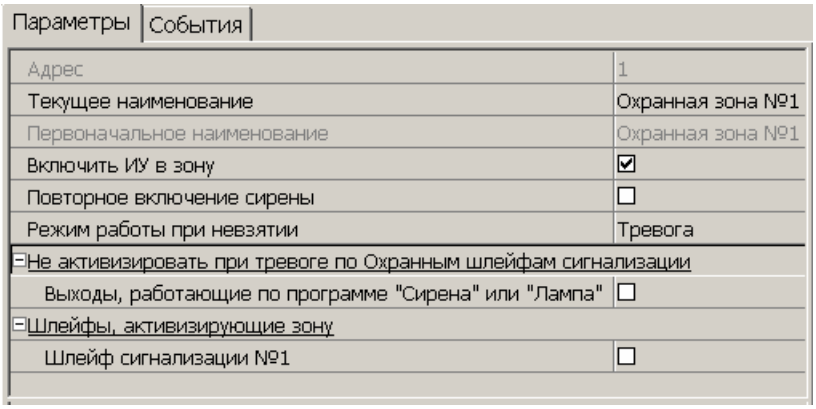
Задержка восстановления нарушенного шлейфа в снятом состоянии:

- Если данный параметр установлен 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 также записывается событие *«Неисправность снятого ОШС»*, 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 также будет записано сообщение *«Нормализация снятого ОШС»*. Состояние выходов и встроенная звуковая индикация панели не изменяются.

8.1.5 Охранная зона

Охранная зона – это логическая структура, которая позволяет создать комбинации ресурсов контроллера, которые одновременно будут ставиться на охрану.

Для настройки ресурса доступны следующие параметры:



Включить ИУ в зону. При установке флажка ИУ будет включено в охранную зону. Если ИУ добавлено в зону, то при постановке на охрану контроллер будет контролировать его состояние.

Повторное включение сирены. При установке флажка активизация дополнительного выхода, управляемого по программе *«Сирена»,* происходит при каждом нарушении 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 на охрану до тех пор, пока постановка на охрану не произойдет.
- **Возврат в «Снята».** Зона перейдет в режим *«Снята».*

Не активизировать при тревоге по охранным шлейфам сигнализации:

- **Выходы, работающие по программе Сирена или Лампа.** При установке флажка в случае тревоги в данной зоне будет запрещена активизация дополнительных выходов, работающие по программе управления **Сирена** или **Лампа**.

Шлейфы, активизирующие зону. Параметр позволяет указать флажками шлейфы сигнализации, которые будут входить в ОЗ и состояние которых будет отслеживаться контроллером при постановке зоны на охрану.

На вкладке **События** можно установить следующие реакции данного ресурса на события системы:

Поставить на охрану/контроль. Приводит к постановке выбранной ОЗ на охрану. Если в состав выбранной охранной зоны входит ИУ, то ИУ 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 (взломе) 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 «невзятие» через время задержки, задаваемое при конфигурации. Для

взятого на охрану ШС контроллер отслеживает сопротивление в его линии и принимает решение о его состоянии.

Снять с охраны/контроля. Происходит снятие охранной зоны с охраны. Если в состав охранной зоны входит ИУ, то контроллер переходит в режим доступа *«Контроль»*. Если в состав ОЗ входит ШС, контроллер перестает отслеживать сопротивление в его линии.

Сбросить тревогу. Приводит к сбросу тревоги и прекращению выполнения алгоритма обработки тревожной ситуации.

8.1.6 Контроллер ИУ

На вкладке **События** можно установить следующие реакции данного ресурса на события системы:

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.

Установить режим работы «Контроль». Приводит к блокировке всех исполнительных устройств выбранного контроллера. При нажатии на кнопку ПДУ для данного направления или при поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ разблокируется на время, определяемое параметром **Время удержания в разблокированном состоянии (время анализа карты).** Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии в зависимости от значения параметра, устанавливаемого в конфигурации ИУ.

Установить режим работы «Совещание». Аналогично режиму работы «Контроль», за исключением индикации на считывателях и блоке внутренней индикации. Более подробно об индикации режимов доступа изложено в техническом описании системы безопасности.

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 (открытое механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.

Открыть (разблокировать) ИУ. Приводит к разблокированию ИУ.

Закрыть (заблокировать) ИУ. Приводит к блокированию ИУ.

Поднять тревогу. Приводит к включению механизма реакции контроллера на возникновение тревожной ситуации. Параметры обработки тревожной ситуации для выбранного контроллера описываются в «*Генераторе тревоги*».

Сбросить тревогу. Приводит к прекращению выполнения контроллером механизма обработки тревожной ситуации.

Сбросить зональность идентификаторов. После получения данной команды контроллер будет игнорировать нарушение зональности при первом предъявлении для каждого из зарегистрированных в контроллере идентификаторов.

8.1.7 Считыватель

Ресурс связан с контроллером ИУ и позволяет настроить с помощью ПО параметры функции верификации, контроля времени, защиты от передачи идентификаторов (Antipass):

Для настройки ресурса доступны следующие параметры:

Параметры | События

Адрес	1
Текущее наименование	Считыватель №1
Первоначальное наименование	Считыватель №1
Модель	PERCo-IRxx
⊟Запрещение ДУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	☐
в РЕЖИМЕ РАБОТЫ "Совещание"	☐
⊟Подтверждение от ДУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
Время ожидания подтверждения при верифицикации	5 сек.
⊟Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Охрана"	Нет
⊟Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
⊞Контроль времени для идентификаторов СОТРУДНИКОВ	
⊞Контроль времени для идентификаторов ПОСЕТИТЕЛЕЙ	
⊟Дополнительные входы, маскируемые при разблокировке ИУ	
⊟Критерий маскирования	На указанное время
⊟На указанное время	
Время	0 мс.
⊟Дополнительные выходы, активизируемые при разблокировке ИУ	
⊟Критерий активизации	На указанное время
⊟На указанное время	
Время	0 мс.
⊟Дополнительные выходы, нормализируемые при разблокировке ИУ	
⊟Критерий нормализации	На указанное время
⊟На указанное время	
Время	0 мс.
⊞Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ	
⊞Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ	
Изымать в СТОП-ЛИСТ идентификаторы ПОСЕТИТЕЛЕЙ после прохода	☐

Текущее наименование. Поле ввода позволяет ввести описательное название считывателя.

Запрещение ДУ. При установке флажка для выбранного режима блокируется возможность управления ИУ с помощью ДУ контроллера в направлении данного считывателя.

Подтверждение от ДУ (Верификация). При помощи этого параметра можно указать, будет ли в выбранных режимах доступа при поднесении идентификатора к данному считывателю формироваться запрос на подтверждение от ДУ.

- **Нет.** Подтверждение не требуется.
- **Да.** Имеется возможность гибко настроить условия верификации идентификаторов отдельно для сотрудников и посетителей в следующих случаях:
    - **при проходе** – верификация будет осуществляться при попытке прохода без каких-либо нарушений
    - **при проходе с НАРУШЕНИЕМ ВРЕМЕНИ** – верификация будет осуществляться при попытке прохода с нарушением времени (параметр **Контроль времени** должен быть установлен на значение **Жесткий**).
    - **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ** – верификация будет осуществляться при попытке повторного прохода без предварительного прохода в обратную сторону (параметр **Защита от передачи идентификаторов** должен быть установлен на значение **Жесткая**).

Время ожидания подтверждения при верификации. Параметр позволяет установить время, в течение которого контроллер будет ожидать подтверждение от верифицирующего устройства. В качестве верифицирующего устройства может быть использовано ДУ контроллера (ПДУ) или картоприемник.

Защита от передачи идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ (Antipass). Параметр позволяет для выбранных режимов определить реакцию контроллера в случае попытки повторного прохода сотрудника/посетителя без предварительного прохода в обратную сторону. Для каждого из указанных режимов работы контроллера можно выбрать один из вариантов защиты:

- **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 мониторинга записывается факт предъявления карты с нарушением местоположения, а после прохода в журнал регистрации записывается событие о проходе с нарушением зональности.
- **Жесткая.** Контроллер либо запретит попытку повторного прохода при предъявлении идентификатора к выбранному считывателю и при этом в журнал мониторинга записывается факт предъявления карты с нарушением местоположения, а в журнал регистрации записывается событие о запрете прохода по причине нарушения зональности, либо будет запущена процедура верификации.

Контроль времени для идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ. Параметр позволяет для выбранных режимов определить реакцию контроллера на предъявление карты сотрудника/посетителя с учетом временного критерия. Для каждого из указанных режимов работы контроллера можно выбрать один из видов контроля:

- **Нет.** Контроллер не учитывает временные параметры доступа карты для разрешения прохода.
- **Мягкий.** Контроллер разрешит доступ по предъявленной карте, но проведет сравнение текущего времени и даты с временными параметрами доступа предъявленной карты. В случае их нарушения в журнал мониторинга записывается факт предъявления карты с нарушением местоположения, а после прохода в журнал регистрации записывается событие о проходе с нарушением времени.

- **Жесткий.** При выборе этого параметра контроллер проведет сравнение текущего времени и даты с временными параметрами доступа предъявленной карты. В случае их совпадения (то есть владелец карты не нарушает режим доступа) контроллер разрешит проход через ИУ. В случае их нарушения контроллер либо запретит проход и запишет в журнал мониторинга факт предъявления карты с нарушением местоположения, а в журнал регистрации событие о запрете прохода в связи с нарушением времени, либо будет запущена процедура верификации.

Дополнительные входы, маскируемые при разблокировке ИУ. Параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы (т.е. не воспринимать управляющий сигнал от внешнего оборудования) при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных входов, которые должны быть маскированы. Укажите временной критерий маскирования.

Временной **Критерий маскирования**:

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

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

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

Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ. Параметр позволяет указать те дополнительные выходы, которые будут активизированы на указанное время в случае предъявления незаблокированного и с неистекшим сроком действия идентификатора сотрудника/посетителя. Этот параметр может быть использован в случае, если к дополнительным выходам подключена индикация, информирующая работников охраны о статусе предъявленной карты. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Укажите временной критерий активизации.

Временной **Критерий активизации/нормализации**:

- **На указанное время.** Выбранные дополнительные выходы будут активизированы / нормализированы на указанное время, начиная с момента предъявления идентификатора, независимо от того, будет или нет разрешен проход.
- **На время срабатывания.** Выбранные дополнительные выходы будут активизированы / нормализированы на указанное время, начиная с момента

разблокирования ИУ и до момента его блокирования, либо, если проход не был совершен, то до истечения времени анализа идентификатора.

- **На время срабатывания и после срабатывания.** Выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы / нормализированы на указанное время, начиная с момента разблокирования ИУ и до момента его блокирования, плюс указанное вами время, либо, если проход не был совершен, до истечения времени анализа идентификатора.

Изымать в СТОП-ЛИСТ идентификаторы ПОСЕТИТЕЛЕЙ после прохода. При установке флажка идентификаторы посетителей после совершения прохода будут помещаться в список идентификаторов запрещенных к проходу.

На вкладке **События** можно установить следующие реакции данного ресурса на события системы:

Установить режим работы «Открыто». Приводит к установлению режима работы *«Открыто»* для ИУ, связанного с данным считывателем.

Установить режим работы «Контроль». Приводит к установлению режима работы *«Контроль»* для ИУ, связанного с данным считывателем.

Установить режим работы «Совещание». Приводит к установлению режима работы *«Совещание»* для ИУ, связанного с данным считывателем.

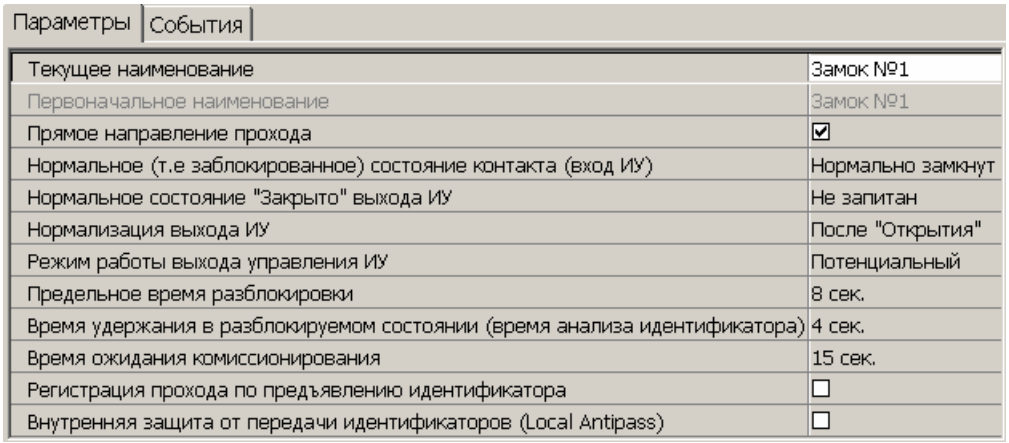
Установить режим работы «Закрыто». Приводит к установлению режима работы *«Закрыто»* для ИУ, связанного с данным считывателем.

Открыть (разблокировать) ИУ. Приводит к разблокировке ИУ, связанного с этим считывателем на время, установленное параметром **Время разблокировки** для данного считывателя.

Закрыть (заблокировать) ИУ. Приводит к закрытию ИУ, связанного с данным считывателем.

8.1.8 ИУ (Замок/Турникет/ Шлагбаум)

Для настройки ресурса доступны следующие параметры:



Текущее наименование. Поле ввода позволяет ввести описательное название ИУ.

Прямое направление прохода. Параметр определяет, какой из считывателей считается входным, а какой выходным.

- Если флажок установлен, то нумерация считывателей соответствует состоянию перемычки «номер считывателя».

- Если флажок не установлен, то тот считыватель, который в соответствии с состоянием его перемычки должен иметь номер 1, в контроллере будет опознан как считыватель номер 2, и соответственно наоборот, считыватель номер 2, в контроллере будет опознан как считыватель номер 1.

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

Нормальное состояние «Закрыто» выхода ИУ (*Не запитан / Запитан*) (Не доступен в конфигурациях 6, 7 «Контроллер АТП»). Параметр описывает, активизировано ли реле управления ИУ в состоянии *«Закрыто»*.

Нормализация выхода ИУ (*После «Открытия» / После «Закрытия»*). В какой момент нормализуется состояние выхода управления исполнительным устройством.

Режим работы выхода управления ИУ (*Потенциальный / Импульсный*). (Доступен только в конфигурациях 1-3 «Контроллер управления дверьми») Описывает логику управления подключенным исполнительным устройством. Импульсный режим управления применяется только для замков, поддерживающих этот режим. Рекомендуется использовать для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки «CISA»).

Время управляющего импульса. Параметр доступен при выборе импульсного режима работы выхода исполнительного устройства. Определяет время управляющего импульса.

Предельное время разблокировки. Параметр позволяет указать время, по истечении которого контроллер сформирует сообщение *«ИУ не закрыто после прохода по идентификатору»* по причине того, что ИУ не заблокировано.

Время удержания в разблокированном состоянии (время анализа идентификатора). Время, на которое открывается ИУ, а также время, в течение которого необходимо повторно предъявить карту, имеющую право постановки на охрану, для постановки ИУ на охрану.

Время ожидания комиссионирования/Время досмотра/Время ожидания подтверждения проезда картой водителя (сотрудника). Параметр позволяет ограничить интервал времени между предъявлением карт пользователя (сотрудника/ посетителя/ служебного ТС) и комиссионирующей карты (сотрудника/ охранника/ водителя), в случае если в правах карты пользователя установлен доступ с комиссионированием/ доступ с досмотром/ подтверждение проезда картой водителя.

Регистрация прохода по предъявлению идентификатора (Не доступен в конфигурациях 6, 7 «Контроллер АТП»). При установке флажка контроллер будет считать проход совершившимся сразу после поднесения идентификатора, независимо от того, будет ли реально совершен проход через ИУ.

Отсутствие датчиков проезда (Доступен только в конфигурациях 6, 7 «Контроллер АТП»). При установке флажка контроллер будет считать проезд совершившимся сразу после поднесения идентификатора, ИУ будет открыто на **Время удержания в разблокированном состоянии.**

Задержка восстановления датчиков проезда (Доступен только в конфигурациях 6, 7 «Контроллер АТП») Параметр определяет промежуток времени между моментом нормализации датчика проезда и подачей команды на закрытие ИУ. Рекомендуемое время 0,5-3 сек.

Внутренняя защита от передачи идентификаторов (Local Antipass). При установке флажка контроллер будет отслеживать случаи повторного предъявления идентификатора.

8.1.9 Генератор тревоги

Ресурс связан с контроллером ИУ и позволяет установить с помощью параметров события, приводящие к переходу системы в состояние *«Тревога СКУД»*. Для настройки ресурса доступны следующие параметры:

Параметры | События

Текущее наименование	Генератор тревоги №1
Первоначальное наименование	Генератор тревоги №1
⊟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 "Закрыто"	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

Текущее наименование. Поле ввода позволяет ввести описательное название генератора тревоги.

Генерация тревоги при предъявлении идентификатора. Параметр позволяет указать события, при которых контроллер переходит в состояние *«Тревога»* при предъявлении идентификатора:

Тип тревоги:

- **Нет.** Контроллер не переходит в состояние *«Тревога»* при выбранном событии.
- **Тихая.** Контроллер переходит в состояние *«Тревога»,* но при этом выходы, **Тип** которых выбран, как **Генератор тревоги,** не активизируются.
- **Громкая.** Контроллер переходит в состояние *«Тревога».*

Генерация тревоги при несанкционированной разблокировке ИУ. Параметр позволяет для выбранных режимов доступа указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние *«Тревога»* в случае механической разблокировки ИУ при помощи ключа, то есть без команды от контроллера.

Генерация тревоги по недопустимо долгому открытию ИУ. Параметр позволяет для выбранных режимов доступа указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние *«Тревога»* в случае, если после открытия ИУ оно не было нормализовано в течение **Предельного времени разблокировки**, заданного в параметрах этого ИУ.

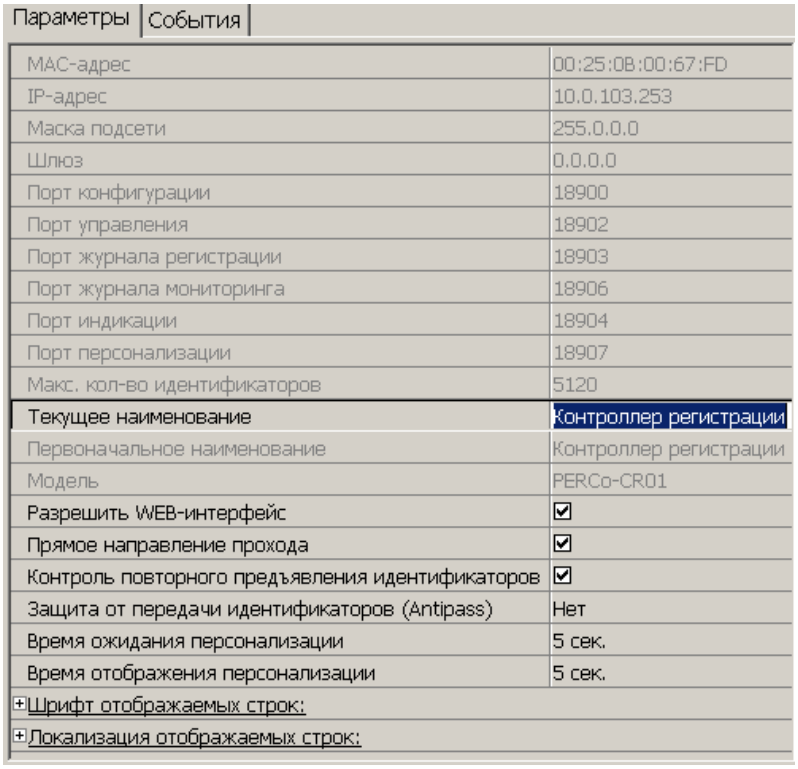
Генерация тревоги по датчику вскрытия корпуса контроллера. Параметр, который позволяет указать, будет ли контроллер автоматически генерировать тревожное событие, если его корпус был вскрыт.

8.2 Описание параметров контроллера регистрации (CR01 LICON)

8.2.1 Параметры контроллера

Контроллер регистрации *PERCo-CR01 LICON* предназначен для организации учета рабочего времени и контроля трудовой дисциплины.

Контроллер регистрации имеет следующие параметры настройки:



Текущее наименование Поле ввода позволяет ввести описательное название контроллера. По умолчанию: «Контроллер регистрации».

Разрешить Web-интерфейс Флажок определяет, будет ли поддерживаться возможность доступа к контроллера через Web-интерфейс.

- Флажок снят. Доступ к контроллеру через Web-интерфейс запрещен.
- Флажок установлен. Доступ к контроллеру через Web-интерфейс разрешен.

Примечание

Доступ будет возможен после остановки сервера системы PERCo-S-20. Для остановки сервера: выйдите из «Консоли управления PERCo-S-20»; запустите «Центр управления PERCo-S-20»; перейдите на вкладку **Настройка серверов**; в области **Сервер системы PERCo-S-20** нажмите кнопку **Остановить**; индикатор справа от кнопки станет красным, сервер будет остановлен.

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

Прямое направление прохода Флажок определяет, какой из считывателей считается входным, а какой выходным.

- Флажок снят. Левый считыватель считается входным, правый выходным.
- Флажок установлен. Правый считыватель считается входным, левый выходным.

Примечание

Подписи указателей «Вход» и «Выход» на ЖКИ при этом не меняются. Изменить текст надписей указателей можно в раскрывающемся меню **Локализация отображаемых строк.**

Контроль повторного предъявления идентификаторов Флажок позволяет определить реакцию контроллера в случае повторного предъявления считывателю идентификатора.

- Флажок снят. Контроллер не отслеживает повторное предъявление идентификатора.
- Флажок установлен. Контроллер следит за повторным предъявлением идентификатора.

Примечание

Флажок **Контроль повторного предъявления идентификаторов** автоматически устанавливается при активизации функции **Внешняя защита от передачи идентификаторов (Global Antipass)** для системы безопасности в целом.

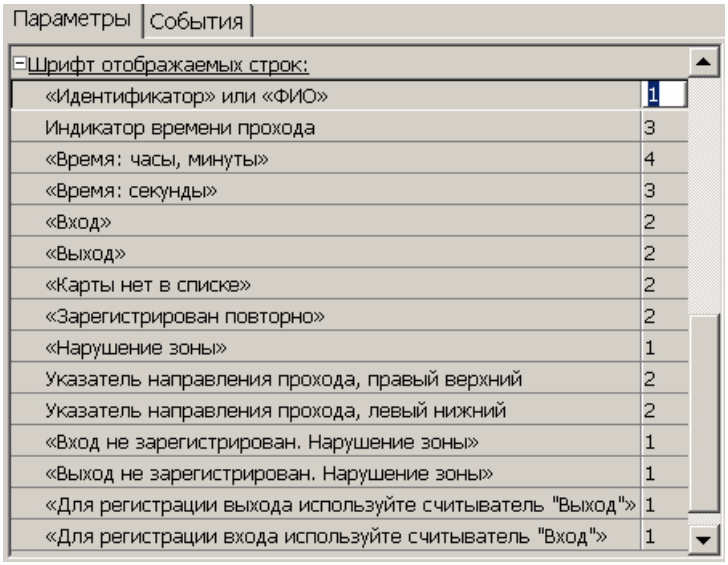
Защита от передачи идентификаторов (Antipass) Раскрывающийся список позволяет определить реакцию контроллера в случае повторного предъявления идентификатора считывателю. Можно выбрать один из способов защиты:

- **Нет** – контроллер не отслеживает повторное предъявление идентификатора.
- **Мягкая** – контроллер зарегистрирует событие о проходе с нарушением зональности.
- **Жесткая**:
  - при нарушении локальной зональности – контроллер зарегистрирует событие о проходе с нарушением зональности;
  - при нарушении глобальной зональности – контроллер зарегистрирует событие о запрете прохода по причине нарушения зональности.

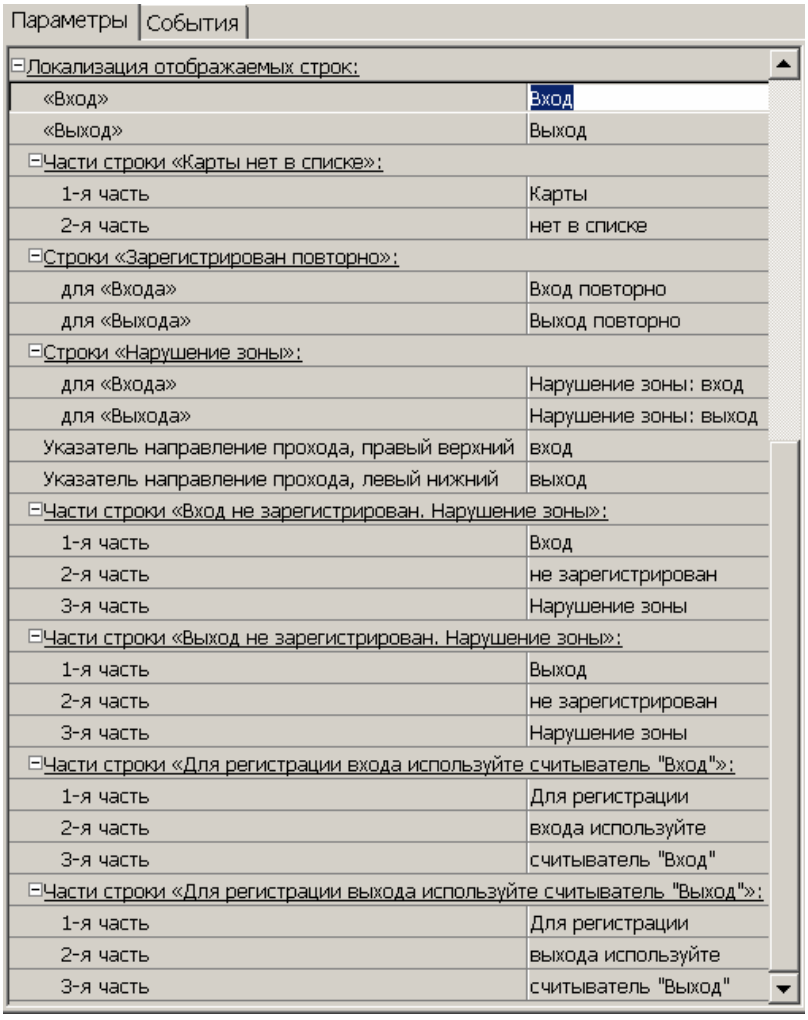
Время ожидания персонализации Поле ввода позволяет задать время, в течение которого контроллер ожидает получения от сервера системы персональной информации (ФИО), связанной с предъявленным идентификатором. В случае невозможности получения такой информации за указанное время, контроллер будет отображать на ЖКИ номер идентификатора.

Время отображения персонализации Поле ввода позволяет задать время, в течение которого контроллер будет отображать на ЖКИ персональную информацию, связанную с предъявленным идентификатором.

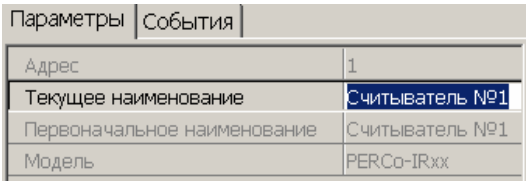
Шрифт отображаемых строк В меню можно выбрать номер шрифта из числа загруженных в контроллер, для сообщений, отображаемых на ЖКИ:



Локализация отображаемых строк В меню можно изменить содержание сообщений, отображаемых на ЖКИ:



Контроллер регистрации имеет два считывателя. Вкладка настройки параметров считывателя имеет следующий вид:

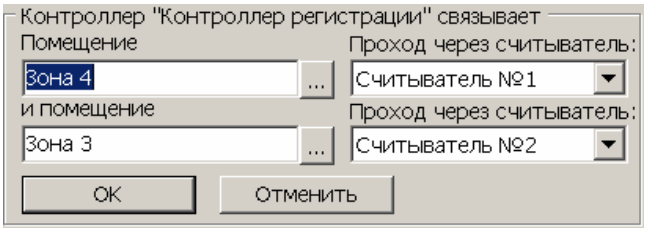


Текущее наименование Поле ввода позволяет ввести описательное название считывателя. По умолчанию: *«Считыватель №…».*

8.2.2 Размещение контроллера на схеме помещений

В разделе ПО **Помещения и мнемосхема** необходимо указать расположение контроллера регистрации.

1. В разделе ПО **Помещения и мнемосхема** перейдите на вкладку **Помещения**.
2. В окне **Помещения с контроллерами** выберите помещение, в котором будет размещен контроллер регистрации.
3. В окне **Доступные контроллеры** выберите контроллер регистрации.
4. Нажмите кнопку  . Откроется панель ввода **Контроллер «…» связывает.**



Примечание

Названия помещений «Зона 3» и «Зона 4» приведены в качестве примера.

5. Определите, какой из считывателей будет считаться входным. Нажмите **ОК**.
6. Панель будет закрыта. Контроллер регистрации появится в окне **Помещения и мнемосхема** в выбранном помещении.

8.2.3 Функция локального контроля зональности Antipass

Antipass – Функция системы безопасности, заключающаяся в контроле повторного прохождения (регистрации) через одну точку прохода в том же направлении с использованием одного и того же идентификатора.

Для включения функции локального контроля зональности в разделе ПО **Конфигуратор** на вкладке **Параметры** контроллера регистрации необходимо:

1. Установите флажок **Контроль повторного предъявления идентификаторов**.
2. В раскрывающемся списке **Защита от передачи идентификаторов (Antipass)** выберите один из способов защиты:
   - **Мягкая**
   - **Жесткая**

8.2.4 Функция глобального контроля зональности Global Antipass

Внимание!

Для работы функции **Внешняя защита от передачи идентификаторов (Global Antipass)** необходимо указать расположение контроллера

регистрации на схеме помещений в разделе ПО **Помещения и мнемосхема**.

Global Antipass – Функция системы безопасности, заключающаяся в контроле нарушений последовательности прохождения (регистрации) сотрудников через точки прохода, с учетом направления прохода. Последовательность прохождения точек прохода определяется взаимным расположением пространственных зон с учетом их вложенности. (То есть нельзя войти в помещение, не войдя в здание.)

Для включения функции глобального контроля зональности **(Global Antipass)** необходимо:

1. Включите функцию локальной зональности (**Antipass**).
2. Установить флажок **Внешняя защита от передачи идентификаторов (Global Antipass)** в разделе ПО **Конфигуратор** на вкладке **Параметры** системы безопасности.

8.3 Описание параметров 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, сохранения событий, произошедших в системе, в энергонезависимой памяти, и передаче их в 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.

8.3.1 Контроллер

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

Поле ввода **Текущее наименование** позволяет ввести описательное название контроллера.

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

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.

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**

8.3.2 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:

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

1. **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/не запитан**. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий.

2. **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». Также 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 свое состояние из нормализированного на противоположное. Как правило, в этом случае к такому дополнительному выходу подключают тревожный оповещатель (сирена, проблесковая лампа).

3. **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 также 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 отсчет задержки, указанной в параметре «Задержка перед запуском» (если задержка ненулевая), по окончанию которой выход активизируется. В зависимости от программы управления выход может быть запитан (не запитан) постоянно (пока ресурс панели находится в текущем режиме), либо изменять свое физическое состояние (мигать) из нормализированного на противоположное. Нормализация выхода происходит либо по истечению времени, указанному в параметре «Время активизации» (если оно не бесконечное), либо по сбросу панели, либо после выключения ее питания. 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 замыкание/размыкание 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 замыкание/размыкание 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 замыкание/размыкание 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 замыкание/размыкание контактов дополнительного выхода.

8.3.3 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 извещетелей	☐
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.

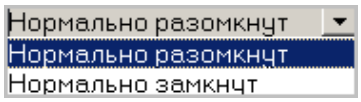
Задержка взятия на охрану – параметр, определяющий для шлейфа время, через которое панель предпринимает попытку взять шлейф на охрану после поступления соответствующей команды.

Задержка восстановления нарушенного шлейфа в снятом состоянии – если в данном параметре установлено значение «0 мс», 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 также записывается событие «Неисправность снятого ОШС», состояние выходов и встроенная звуковая индикация панели не изменяются. Если после этого нормальное состояние шлейфа восстановится и продержится в течение времени, указанном в этом параметре, то шлейф выйдет из состояния «НАРУШЕНИЕ» и в журнал регистрации 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 ППКОП).**

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.

8.3.4 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 определенного 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).

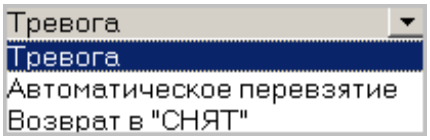
В зависимости от алгоритма работы шлейфов сигнализации существуют следующие варианты описания параметров работы зоны:

1. **Тип** зоны сигнализации – **Охранная**

Текущее наименование	Охранная зона
Адрес	1
Первоначальное наименование	Охранная зона
⊟Тип	Охранная
⊟Охранная	
Повторное включение сирены	☐
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 сирены – 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, работающих 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	☑

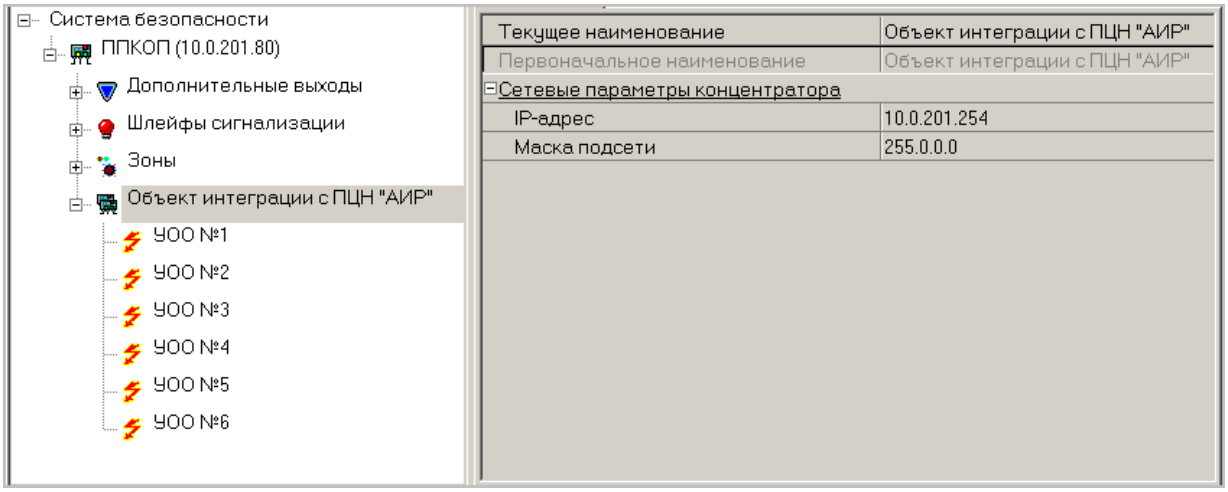
Шлейфы, активизирующие зону – список шлейфов КТС, контролируемых в данной зоне.

8.4 Интеграция ППКОП с ПЦН «АИР»

Включение интеграции 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.

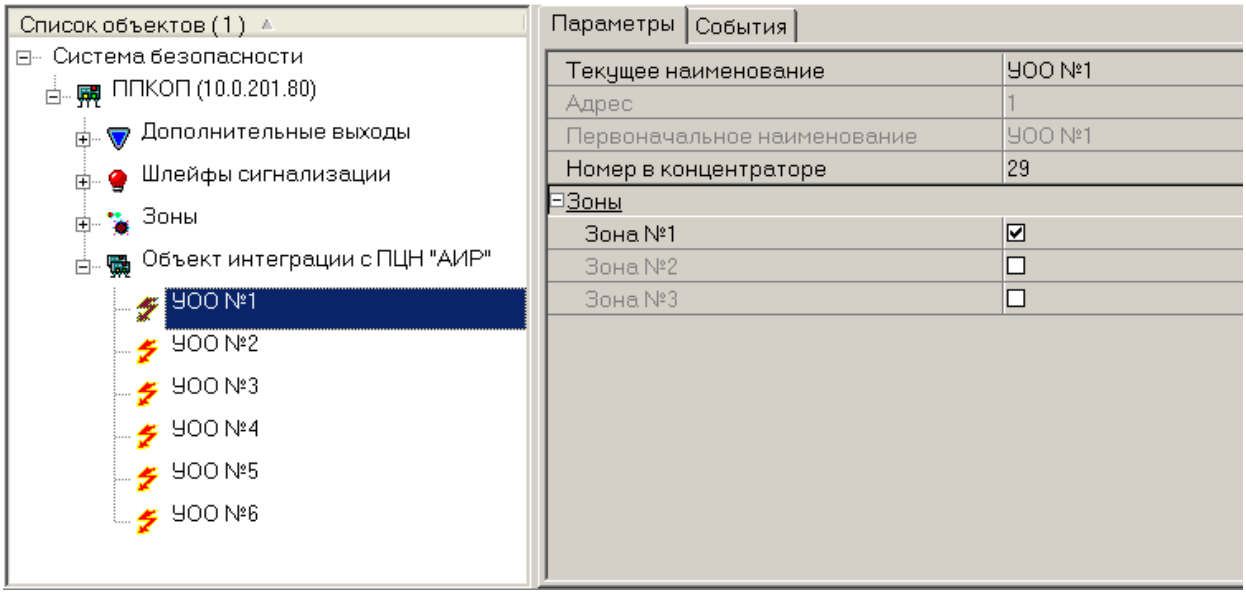
Для включения интеграции следует задействовать параметр **«Включить интеграцию с ПЦН «АИР»** на контроллере ППКОП.

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



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 охраняемых зон.

9 ПОМЕЩЕНИЯ И МНЕМОСХЕМА

Нормальное функционирование системы безопасности невозможно без привязки объектов системы к помещениям предприятия, его территории. Привязка объектов системы осуществляется в разделе ПО **Помещения и мнемосхемы**.

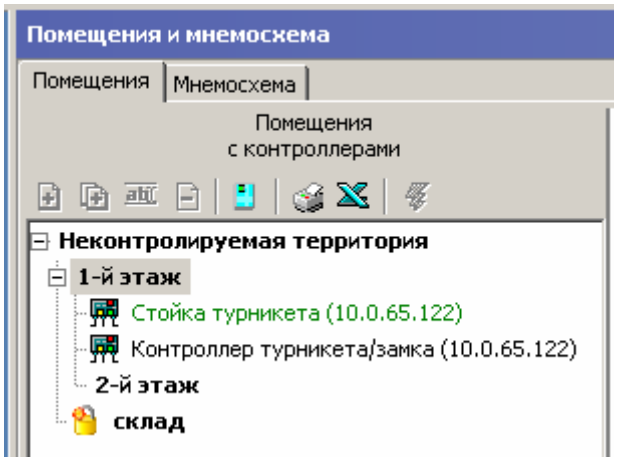
Под помещениями в системе безопасности подразумевается иерархическая структура помещений предприятия (организации). Эта информация необходима для определения уровней доступа, указания, какие контроллеры контролируют доступ в какие помещения, привязки шлейфов охранно-пожарной сигнализации, дополнительных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

9.1 Помещения

В данном подразделе список помещений строится в виде древовидной структуры. Максимальное количество вложений 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 зоны (территория вне предприятия) контролируется контроллером стойки турникета. В случае задания включения защиты от передачи карт вход на первый этаж без предварительного выхода будет невозможен. Также справедливо будет 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.

9.2 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:

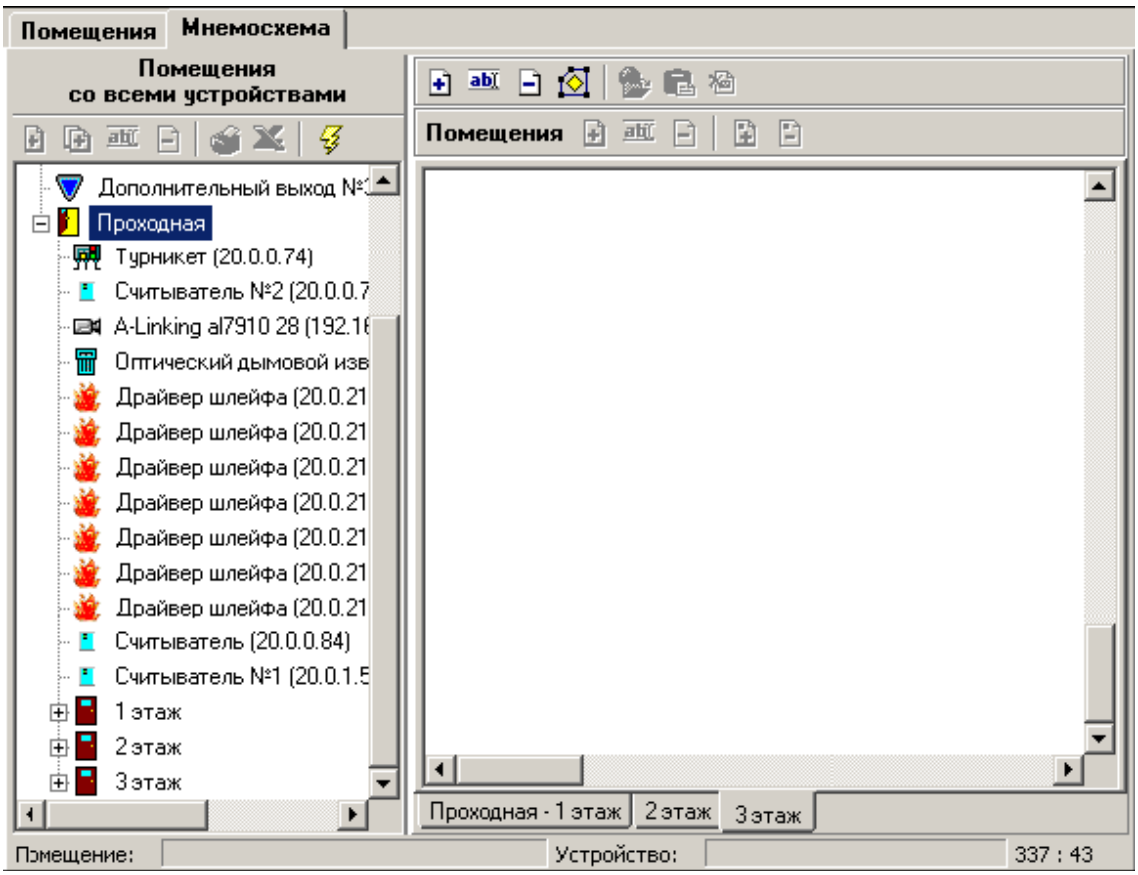
- Создание мнемосхемы без использования графических изображений территории предприятия. В этом случае графические изображения располагаются на автоматически созданном белом квадрате с размером 1600x1600 пикселей. Использование такого подхода оправдано только в том случае, если территория предприятия 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.

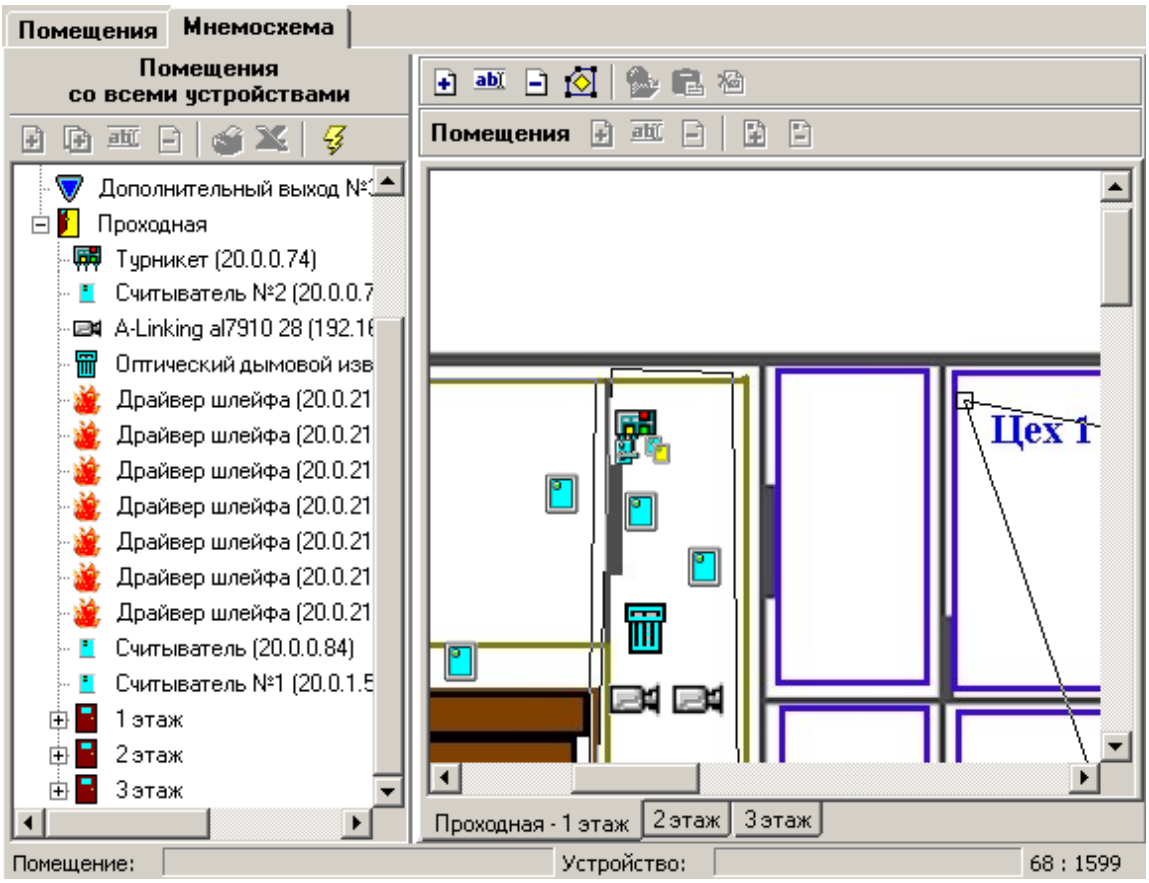
Далее рассмотрим создание мнемосхем с использованием графических планов. Создание без графических планов полностью аналогично.

Для создания мнемосхемы предприятия (поэтажных планов) вам в первую очередь необходимо подготовить 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.

10 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 Т-12 и Т13.

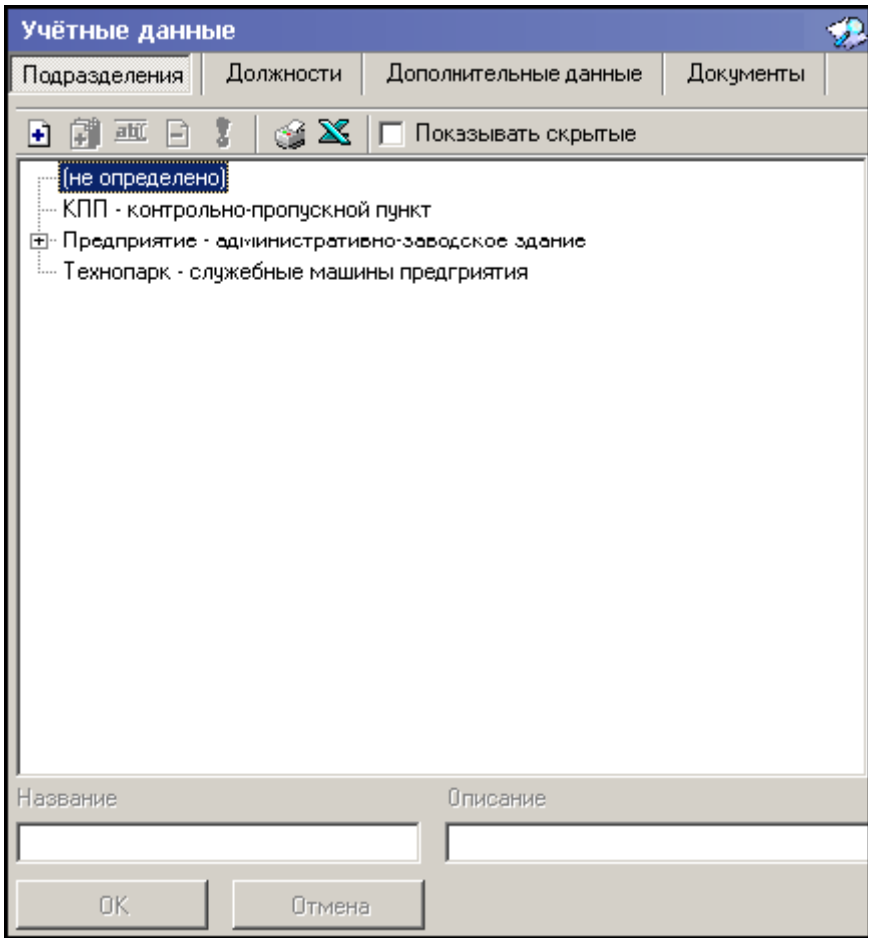
10.1 Учетные данные

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

Раздел ПО **Учетные данные** позволяет создавать и изменять справочные данные о структуре подразделений предприятия, должностях, дополнительные сведения о сотрудниках.

Подробная информация о правилах работы с этим разделом ПО приведена в Руководстве пользователя в разделе **Учетные данные**.

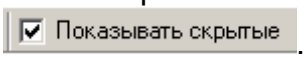
10.1.1 Справочник «Подразделения»



Справочник **Подразделения** предназначен для создания и редактирования структуры подразделений предприятия в соответствии с его штатным расписанием.

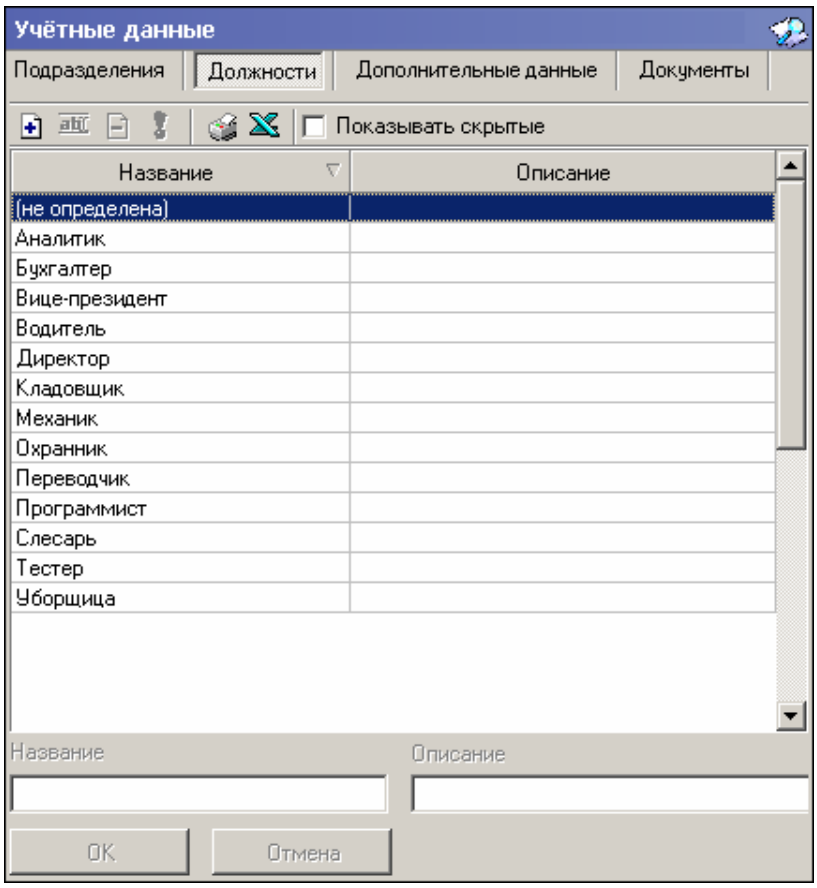
Эта информация в дальнейшем используется при вводе данных о сотрудниках предприятия и при составлении отчетов по сотрудникам.

В процессе корректировки структуры подразделений ненужные подразделения можно удалить (кнопка ), однако если в подразделении числятся (числились) сотрудники (в т.ч. и ранее уволенные), то такое подразделение удалить нельзя, можно только перевести в категорию «скрытых» подразделений (в списке выделяются красным цветом). 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 скрытия/отображения скрытых подразделений необходимо снять/поставить флажок 

. Чтобы восстановить в структуре скрытое ранее подразделение, необходимо воспользоваться кнопкой  .

10.1.2 Справочник «Должности»



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.

10.2 Сотрудники

Раздел ПО **Сотрудники** облегчает работу по упорядочиванию, ведению и оперативному внесению изменений в учетные данные сотрудников, что значительно сокращает объем рутинной работы и повышает эффективность работы сотрудников отделов кадров (отделов персонала).

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

11 ПАРАМЕТРЫ ДОСТУПА СОТРУДНИКОВ

Для нормального функционирования системы безопасности недостаточно провести конфигурацию устройств системы, задать принципы ее работы и ввести данные о сотрудниках. Необходимо также 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 на охрану /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 необходимой информации необходимо сначала заполнить справочники временных критериев доступа. Под временными параметрами доступа понимаются интервалы времени, привязанные к суткам, дням недели, в течение которых разрешен доступ на территорию предприятия и его внутренние помещения, а также действия по постановке/снятию с охраны помещений и групп ресурсов.

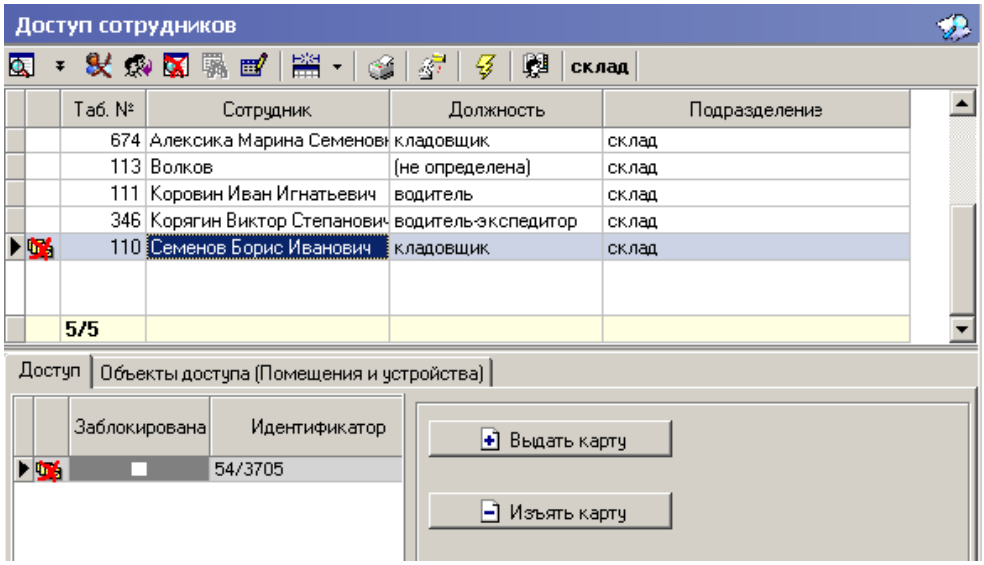
После их создания можно переходить к выдаче карт доступа и назначению прав доступа сотрудников.

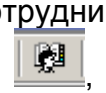
Система безопасности PERCo-S-20 поддерживает следующие типы временных графиков доступа сотрудников и посетителей предприятия:

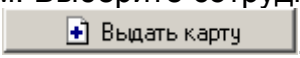
После создания всех необходимых графиков доступа можно переходить к выдаче карт доступа и назначению прав доступа сотрудников предприятия.

Примечание

Перед началом работы убедитесь, что Вами уже разработаны необходимые графики доступа сотрудников и подготовлены все необходимые административные документы, определяющие права и время доступа сотрудников.

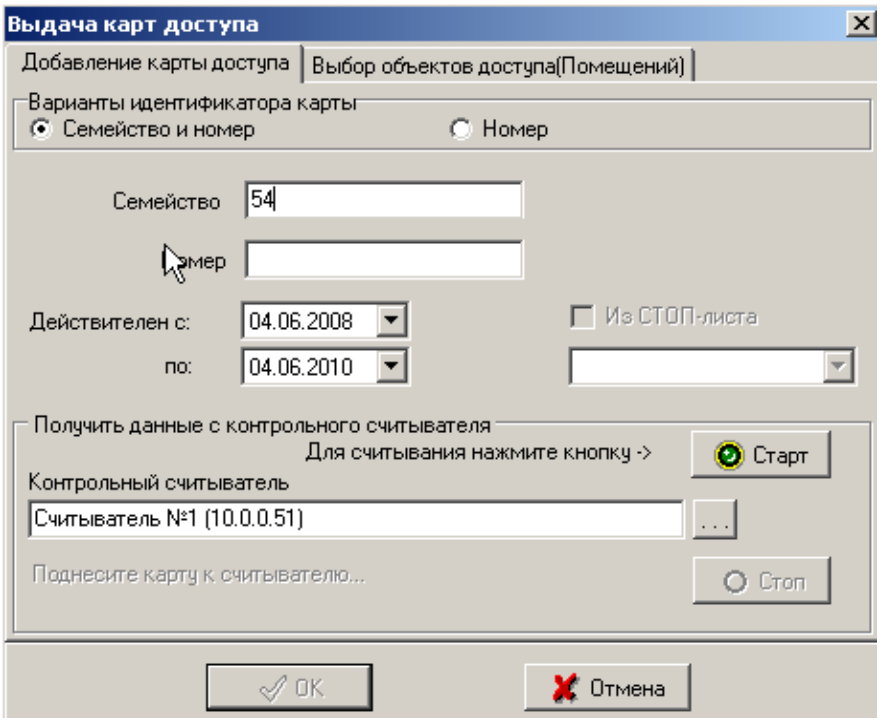


Выберите подразделение, к выдаче карт доступа сотрудникам которого Вы хотите приступить. Для этого воспользуйтесь кнопкой  , название выбранного подразделения отобразится рядом.

После выбора подразделения становится доступен список всех сотрудников, работающих в нем. Выберите сотрудника, которому Вы хотите выдать карту доступа и нажмите кнопку 

.

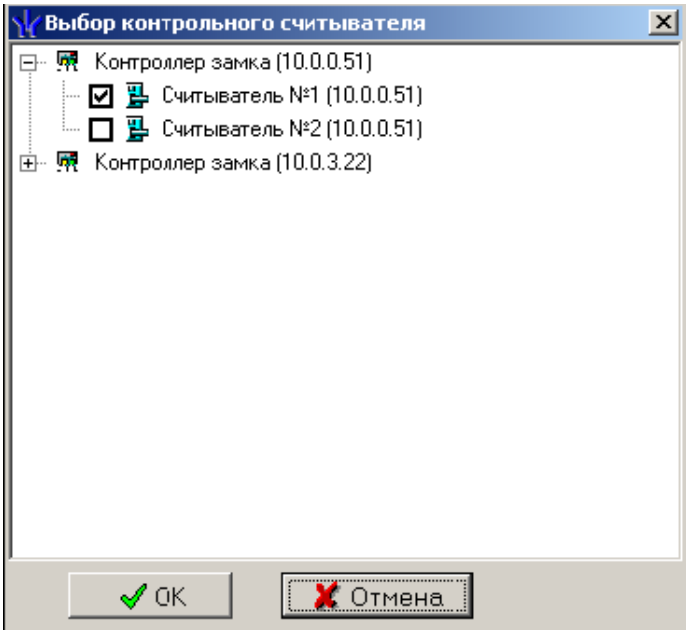
В появившемся диалоговом окне задайте необходимые параметры.



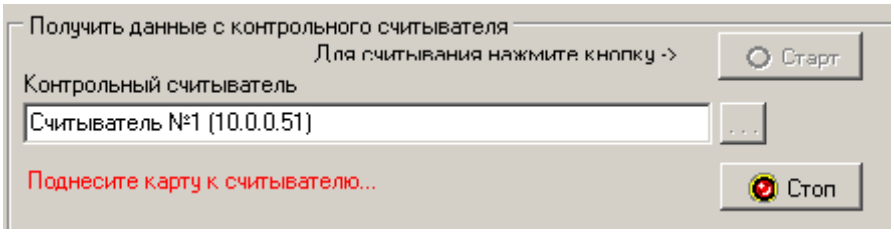
При вводе параметров необходимо обратить внимание на то, что срок действия карты доступа автоматически контролируется контроллерами. По истечению этого срока доступ по этой карте будет автоматически запрещен.

Поле Получить данные с контрольного считывателя. Для получения данных с помощью контрольного считывателя справа от поля ввода Контрольный считыватель щелкните на кнопке 

. Откроется окно **Выбор контрольного считывателя**, в котором отметьте считыватель, удобный для выполнения функции контрольного.



После подтверждения выбора кнопкой **ОК**, щелкните на кнопке Старт на панели контрольного считывателя



и поднесите выдаваемую карту к контрольному считывателю. В полях ввода семейства и номера карты отобразятся данные выдаваемой карты доступа. Считыватель выводится из режима работы контрольного считывателя щелчком на кнопке Стоп.

Следует помнить, что если карта с таким номером или семейством уже зарегистрирована, то программа выдаст соответствующее предупреждение, и новый пропуск не будет зарегистрирован.

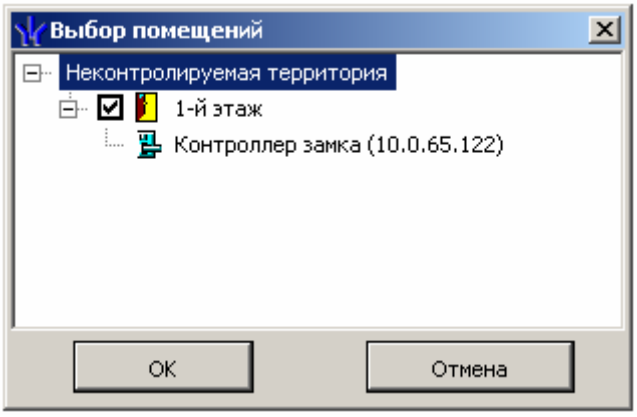
Примечание

В случае проведения повторной конфигурации необходимо заново указать контроллер, выступающий в качестве контрольного считывателя, даже если указан именно тот контроллер, с которым работали раньше.

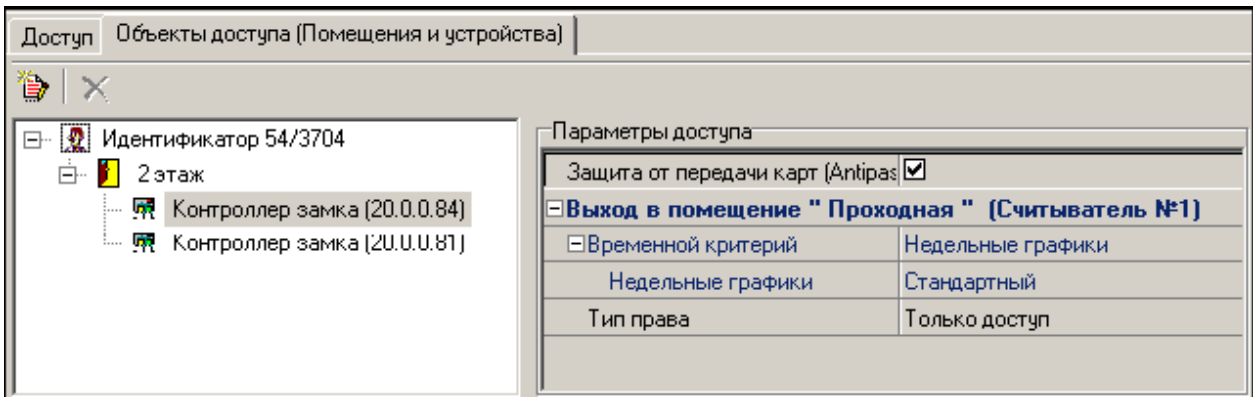
Проделайте всю эту процедуру со всеми остальными сотрудниками. Сохраните сделанные изменения.

После выдачи карт доступа можно перейти к указанию прав доступа. Раздел ПО **Доступ сотрудников** позволяет задавать права доступа не только каждому сотруднику в отдельности, но и поддерживает групповые операции. Таким образом, Вы можете выделить группу сотрудников при помощи клавиши **Shift** и мыши и тем самым задать для них одинаковые права доступа.

В диалоговом окне выбора объектов доступа (вызывается кнопкой ) Вы можете сразу указать те помещения, в которые будет разрешен доступ сотруднику (выбранным сотрудникам):

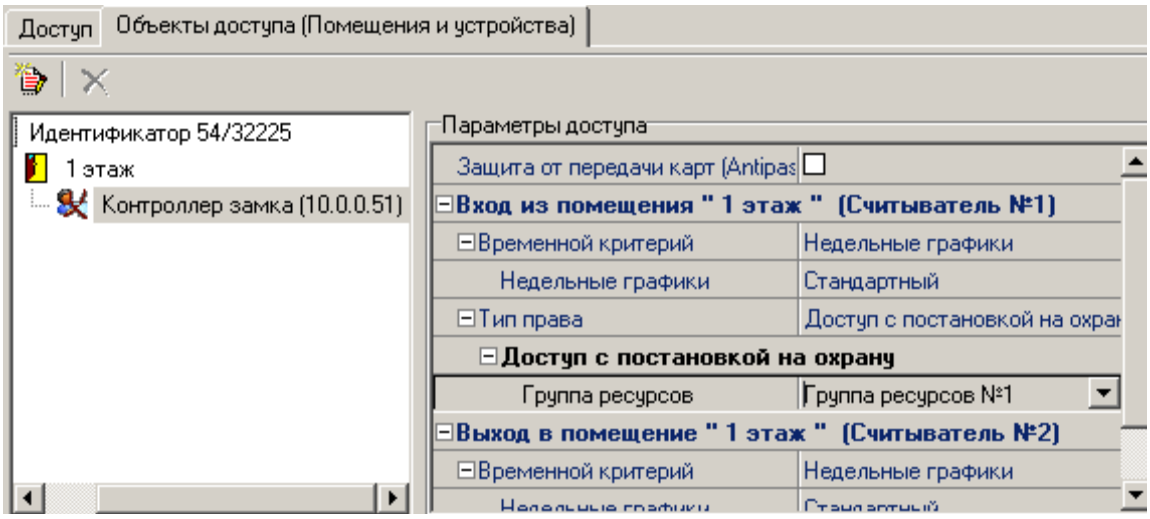


После завершения выбора объектов, в которые разрешен доступ, необходимо указать параметры доступа. Для этого необходимо выбрать поочередно каждый контроллер, отображенный в окне разрешенных объектов доступа, и указать параметры доступа.



Кроме этого для каждого контроллера можно включить или выключить функцию **Antipass** для контроля повторного входа или выхода через точку прохода.

В качестве примера рассмотрим права доступа заданные идентификатору для прохода через замковый контроллер, контролирующий проход на первый этаж:

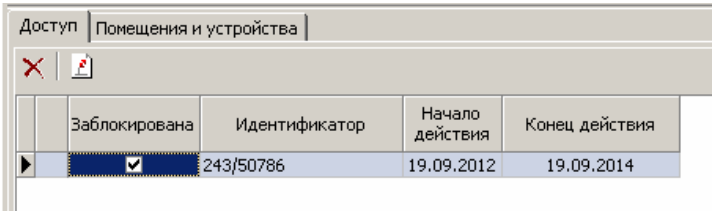


В соответствии с заданными правами, сотрудник, владеющей этой картой доступа, имеет право доступа на 1 этаж по недельному графику *«Стандартный»*. Так как данный контроллер контролирует только вход в это помещение, и выход из него не контролируется системой, мы не установили защиту от передачи карт, как не имеющую смысла. Кроме этого, владельцу этой карты доступа предоставлено право постановки и снятия с охраны группы ресурсов (охранной зоны), связанной с данным контроллером.

После завершения задания прав доступа необходимо сохранить сделанные изменения и передать их в контроллеры.

Как правило, на работающем предприятии возникают ситуации, когда сотрудник временно отсутствует на рабочем месте, находится в командировке, в отпуске. Соответственно доступ по его карте доступа должен быть заблокирован для предотвращения фактов незаконного проникновения на территорию предприятия.

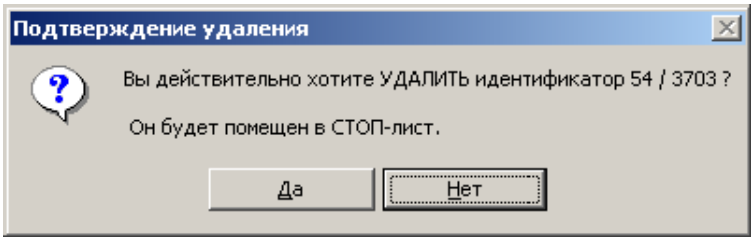
Для блокировки карты доступа необходимо выбрать соответствующего сотрудника в списке сотрудников предприятия и задать параметр в окошке столбца **Заблокирована** на вкладке **Доступ** и в вызванном диалоговом окне подтвердить свое намерение. Программное обеспечение автоматически передаст данные в контроллеры. С этого момента выбранная карта доступа будет заблокирована для доступа:



Для разрешения доступа необходимо снять пометку в поле «Заблокирована». Программное обеспечение автоматически передаст необходимые данные в контроллеры и доступ по карте будет разрешен.

В случае утери карты доступа в результате ее хищения или повреждения для предотвращения доступа на предприятия посторонних лиц необходимо изъять карту доступа и занести ее в «СТОП – лист». Для этого необходимо выбрать сотрудника, утерявшего карту доступа, выбрать в списке утерянную карту и нажать на кнопку

В появившемся диалоговом окне ответить утвердительно на предложение о внесении карты доступа в СТОП – лист:



Программное обеспечение попросит Вас внести причину внесения карты доступа в стоп лист, это позволит в дальнейшем определить, при каких обстоятельствах была утеряна карта.

После ввода причины занесения карты доступа в «СТОП – лист» программное обеспечение автоматически передаст данные в контроллеры системы, тем самым запретив доступ по этой карте.

12 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**.

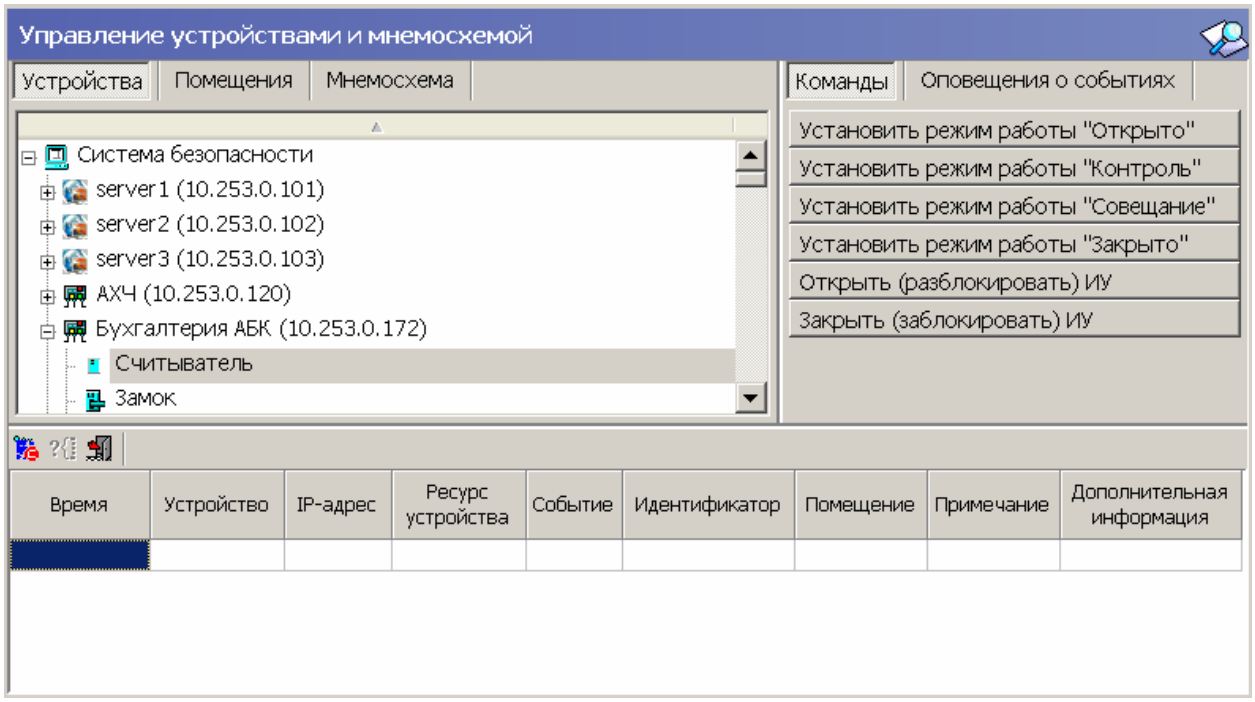
Программное обеспечение единой системы безопасности *PERCo-S-20* предоставляет возможность создания рабочих мест сотрудников отдела безопасности для контроля за состоянием охраняемых объектов.

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 ПО. Информация об интерфейсе пользователя приведена в соответствующих Руководствах пользователя. В этом документе мы остановимся на ключевых моментах, необходимых при настройке рабочего места.

12.1 Управление устройствами

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



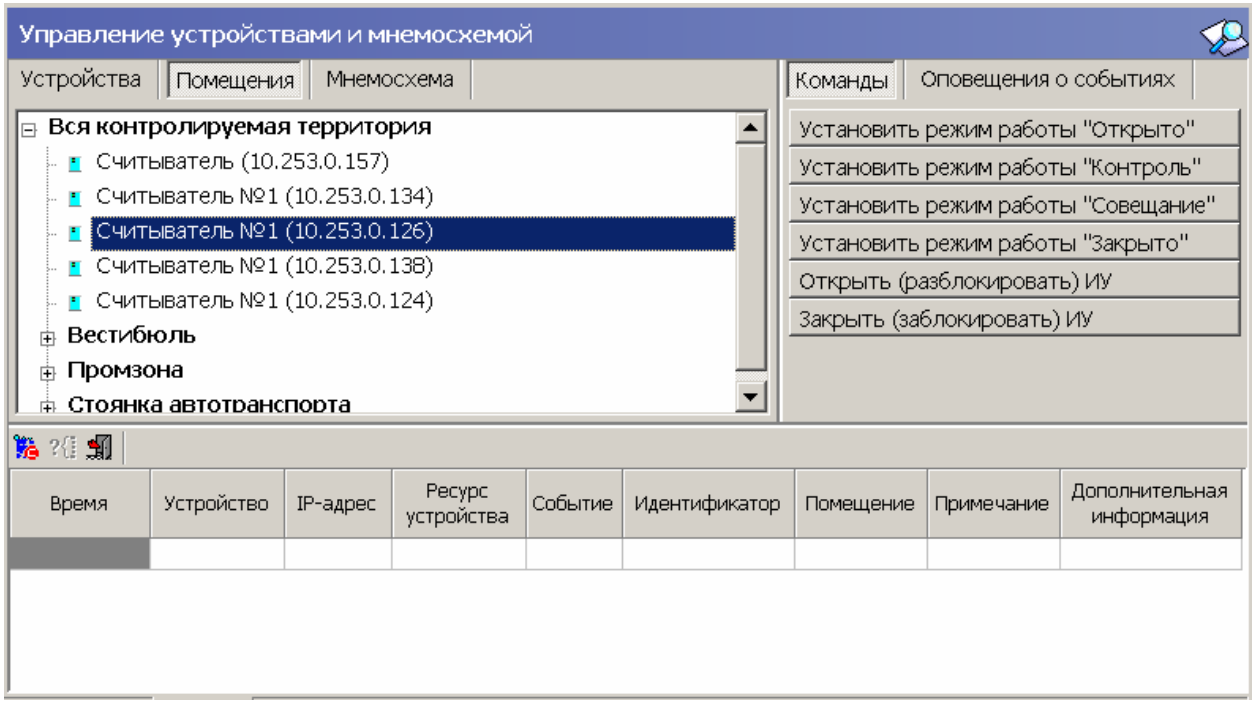
Состояние устройств в дереве объектов системы отображается в надписях возле пиктограмм, обозначающих тип устройств, например: *Замок №1: Заблокирован*. Если нет связи с контроллером, то тогда вместо его пиктограммы высвечивается ?.

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

Для управления любым устройством необходимо выбрать это устройство в дереве объектов системы, при этом в правой части окна автоматически отобразится список доступных команд управления для выбранного устройства.

Для удобства восприятия информации о состоянии устройств системы безопасности и управления ими программное обеспечение предлагает возможность отображения устройств не в дереве объектов системы, а в дереве объектов доступа, для этого нужно перейти на вкладку **Помещения**.

Подробно о создании дерева объектов доступа и помещениях изложено в разделе **Помещения и мнемосхема** данного руководства.

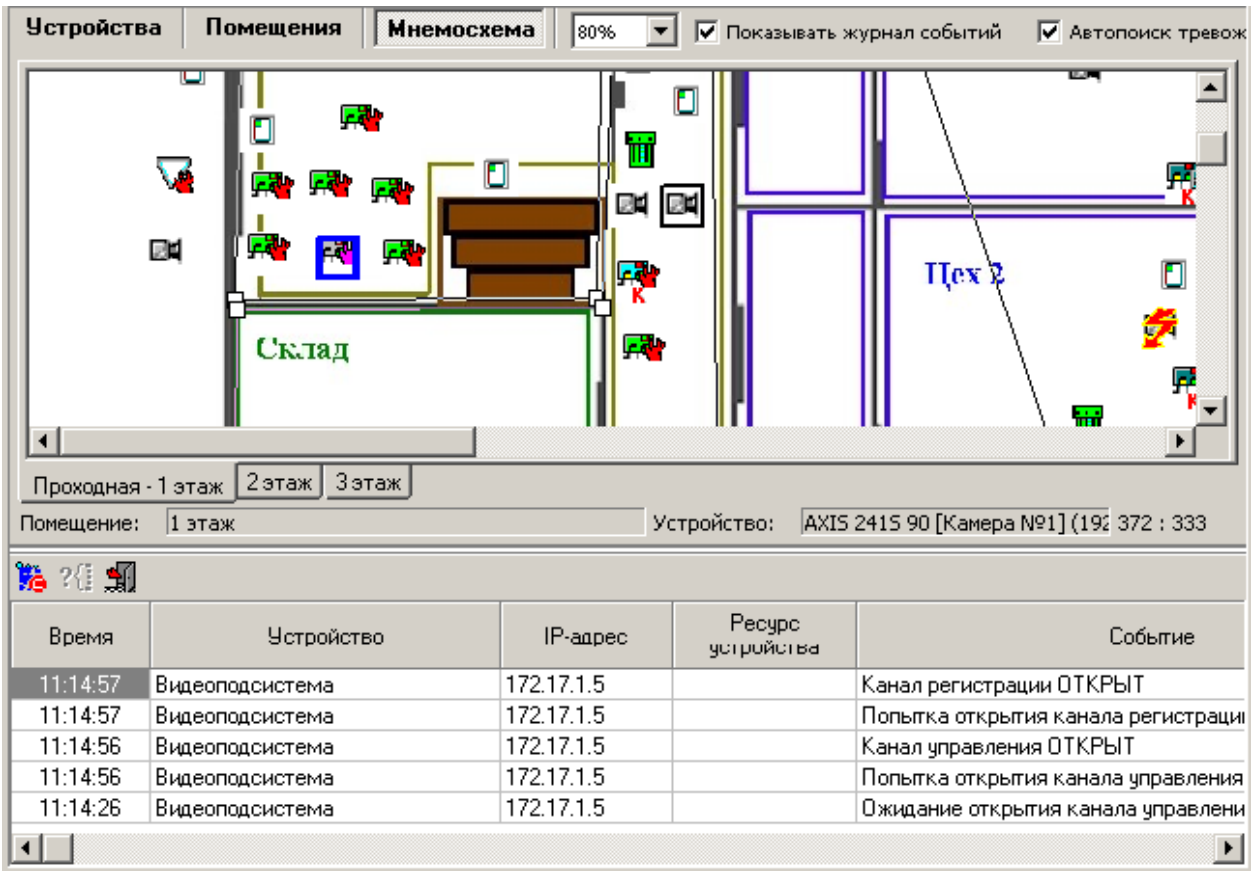


При выборе такого варианта отображения в дереве объектов доступа отображаются только те устройства, которые были установлены и размещены в конкретных помещениях. Соответственно при отображении информации о состоянии устройств автоматически отображается помещение, в котором произошло то или иное событие. Такой вариант наиболее полно отражает состояние охраняемых объектов.

Отображение событий в табличном виде, и управление устройствами происходит аналогичным образом.

12.2 Мнемосхема

Следующим вариантом отображения информации о состоянии объектов является использование графических планов объектов. Методика создания графических планов объектов и размещения на них объектов системы безопасности изложена в разделе **Помещения и мнемосхемы** данного руководства.



При таком варианте представления, информации о состоянии объектов системы отображается в виде пиктограмм, расположенных на графических планах предприятия. При этом изменение состояния объекта системы приводит к автоматическому открытию соответствующего плана предприятия.

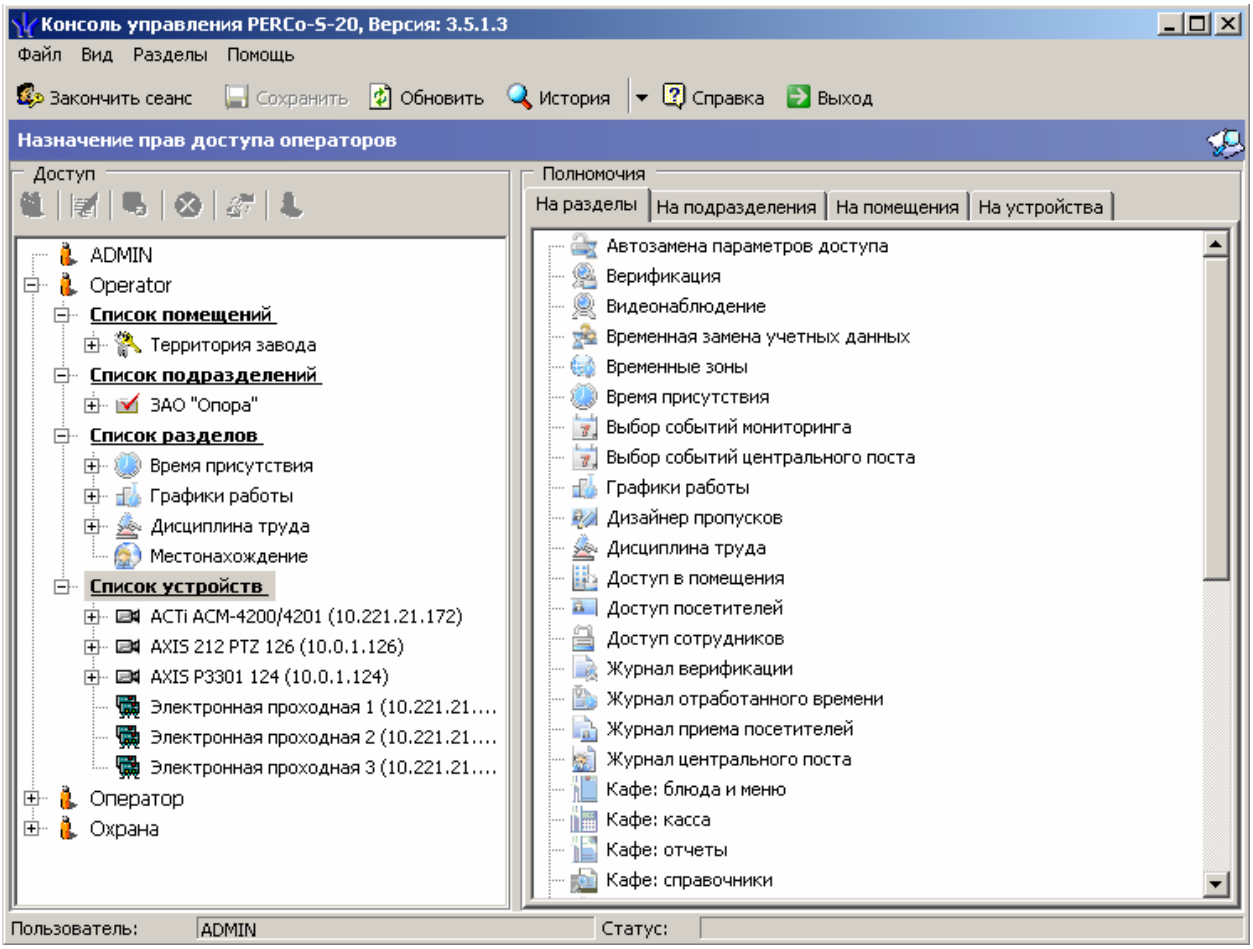
Для управления объектами системы необходимо воспользоваться правой кнопкой мыши. При этом в контекстном меню отображаются команды доступные для выбранного объекта.

Отображение событий в табличном виде происходит аналогичным образом.

13 НАЗНАЧЕНИЕ ПРАВ ДОСТУПА ОПЕРАТОРОВ

Одним из важнейших свойств системы безопасности является разграничение прав пользователей программного обеспечения к разделам ПО и устройствам, входящим в состав системы безопасности.

Для определения прав операторов программного обеспечения предназначен раздел ПО **Назначение прав доступа операторов**:



Этот раздел ПО предназначен для ведения списка операторов системы, установки для них паролей, определения для каждого из них прав на работу с разделами ПО, подразделениями, помещениями и устройствами системы, оперативного управления их правами.

Рабочая область раздела состоит из двух частей:

- Левая часть содержит список всех зарегистрированных пользователей с указанием прав каждого из них.
- Правая часть представлена в виде многостраничного блокнота с информацией о разделах ПО и объектах системы, на которые могут быть предоставлены права доступа операторам системы:
  - **На разделы**. Страница содержит список всех разделов системы безопасности.
  - **На подразделения**. Страница содержит список всех подразделений, введенных в систему.
  - **На помещения**. Страница содержит дерево помещений со списком помещений системы безопасности.

- **На устройства**. Страница содержит список устройств системы для предоставления прав на управление ими.

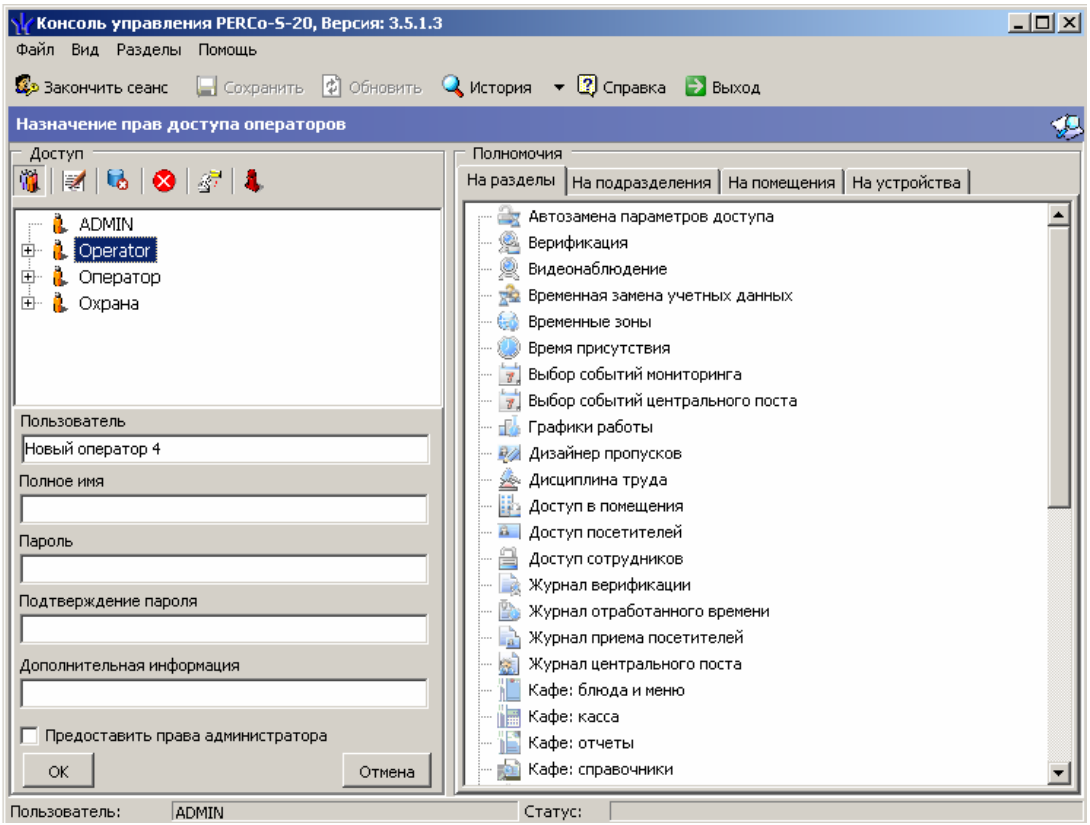
Примечание

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.

13.1 Добавление нового оператора

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 оператора программного обеспечения необходимо нажать на кнопку  . При этом в нижней части окна откроется дополнительная панель для ввода данных:



Необходимо указать следующие данные на оператора:

- **Пользователь.** В этой строке указывается имя пользователя, которое он будет вводить при запуске программного обеспечения.
- **Полное имя.** В этой строке указывается полное имя пользователя.
- **Пароль.** В этой строке указывается пароль пользователя.
- **Подтверждение пароля.** Указывается тот же самый пароль для избегания ошибки ввода.

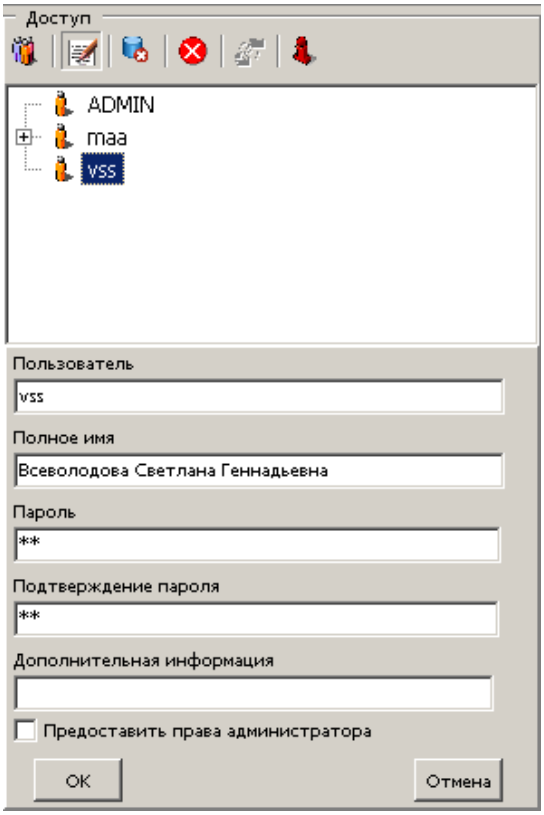
- **Дополнительная информация.** В этой строке ввода можно ввести любую дополнительную информацию об операторе.

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 также иметь возможность управлять любым устройством, входящим в систему безопасности.

По завершению ввода данных об операторе необходимо нажать на кнопку **ОК**, что приведет к закрытию панели ввода и отображению информации о введенном операторе в левой части рабочего окна.

13.2 Редактирование и удаление оператора

Для внесения изменений в данные оператора необходимо выбрать его из списка операторов системы при помощи левой клавиши мыши и нажать на кнопку  . При этом откроется панель редактирования данных оператора, аналогичная описанной выше:



Для удаления оператора из списка необходимо так же выделить его в списке операторов системы и нажать на кнопку **Удалить пользователя**  . При этом появится диалоговое окно с запросом подтверждения удаления оператора.

13.3 Предоставление прав доступа оператору

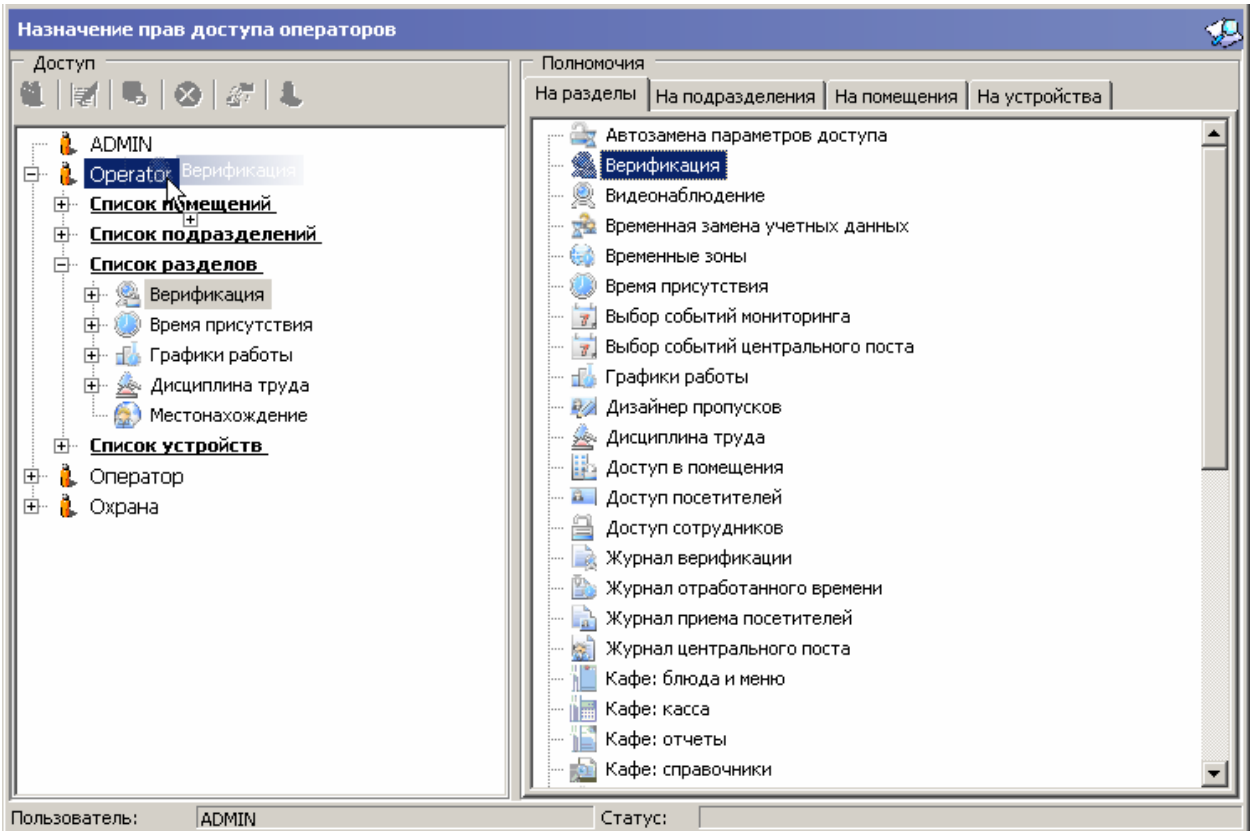
Для предоставления прав доступа оператору необходимо выделить его в списке операторов системы при помощи левой клавиши мыши и выбрать соответствующую закладку в левой части рабочего окна.

13.3.1 Права доступа на разделы ПО

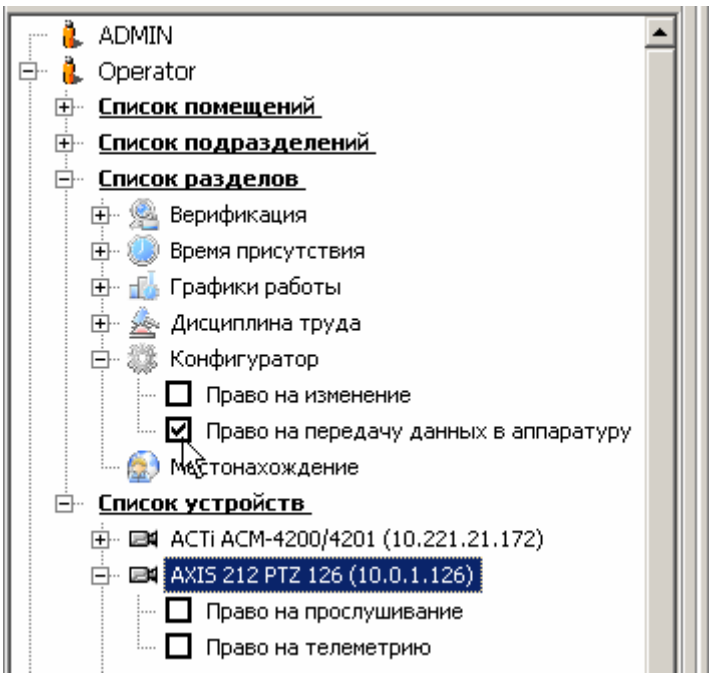
На вкладке **На разделы** представлен список всех разделов программного обеспечения, к которым может быть предоставлен доступ выбранному оператору.

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

После этого название добавленного раздела программного обеспечения отобразится под оператором:



Перетаскивание названия программного модуля определяет, что данный оператор имеет право на вход в этом модуль и просмотр имеющейся там информации. Кроме этого для модуля 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.
Для **предоставления** дополнительных прав отметьте соответствующие права.



13.3.2 Права доступа на подразделения

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

Механизм предоставления прав полностью аналогичен описанному выше. При этом при перетаскивании подразделения, имеющего вложенные подразделения, автоматически будут добавлены все вложенные подразделения.

13.3.3 Права доступа на помещения

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

Механизм предоставления права доступа оператору полностью аналогичен описанному выше.

13.3.4 Права доступа на управление устройствами

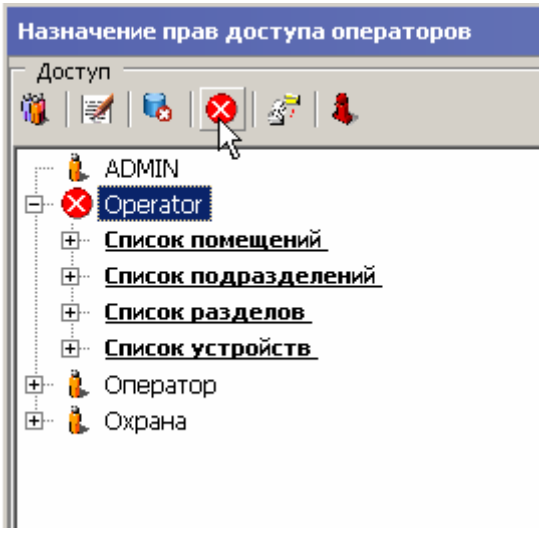
Вкладка **На устройства** дает возможность указать, какими именно устройствами, входящими в систему безопасности, будет разрешено управлять оператору.

Механизм предоставления права оператору полностью аналогичен описанному выше.

13.4 Запрещение прав оператора

Для запрещения любого права оператора необходимо выбрать это право и нажать на кнопку **Удалить**  . При этом появится диалоговое окно с запросом подтверждения данной операции. После нажатия кнопки **ОК** данное право будет удалено из списка разрешенных.

Для временной блокировки оператора необходимо выделить этого оператора и нажать на кнопку **Запретить доступ**  .



После этого доступ оператора к программным разделам будет запрещен.

Для разрешения ранее заблокированного оператора необходимо выделить его в списке и нажать на кнопку **Разрешить доступ** .

Примечание

Внесенные изменения, а также блокировка\разблокировка оператора, вступят в силу только после того, как данный оператор закончит и снова начнет работу под своей учетной записью.

14 СОБЫТИЯ УСТРОЙСТВ И ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ

Раздел **События устройств и действия пользователей** предназначен для получения отчетов о событиях в системе, произошедших на определенных объектах в заданный интервал времени для выбранных сотрудников. При этом имеется возможность выбора значимых событий. Интервал времени задается с точностью до минуты, диапазон просмотра списка событий неограничен. Отчеты могут использоваться для выборочного контроля за перемещением сотрудников по предприятию или для проведения служебных расследований.

14.1 Рабочее окно

Рабочее окно раздела **События устройств и действия пользователей** выглядит следующим образом:

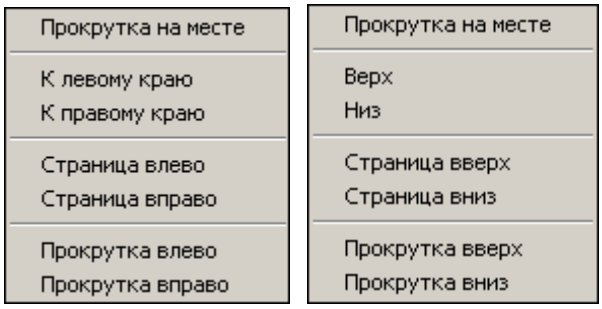
Функциональные элементы раздела:

1. **Настроить выборку**
2. **Настройка столбцов таблицы**
3. **Посмотреть область листа для печати**
4. **Предварительный просмотр и печать**
5. **Экспорт данных** (возможен экспорт в файлы форматов XLS, CSV, OpenOffice Calc)
6. **Получить данные**

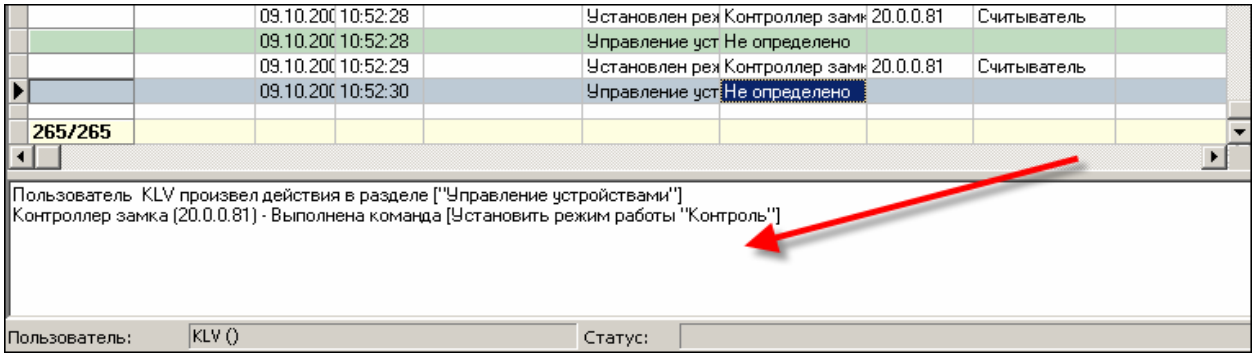
В правой части окна – кнопки для перемещения по списку событий.

При первом запуске программы рабочее окно раздела не заполнено.

Щелчком правой кнопки мыши на область прокрутки внизу и по правому краю рабочего окна вызывается контекстное меню, позволяющее перемещать документ по горизонтали и по вертикали в удобном для пользователя режиме.



Зеленым цветом в списке выделены строки с событиями, связанными с действиями пользователей ПО (операторов). При выделении данной строки внизу рабочего окна открывается дополнительная панель с комментариями по данному событию:

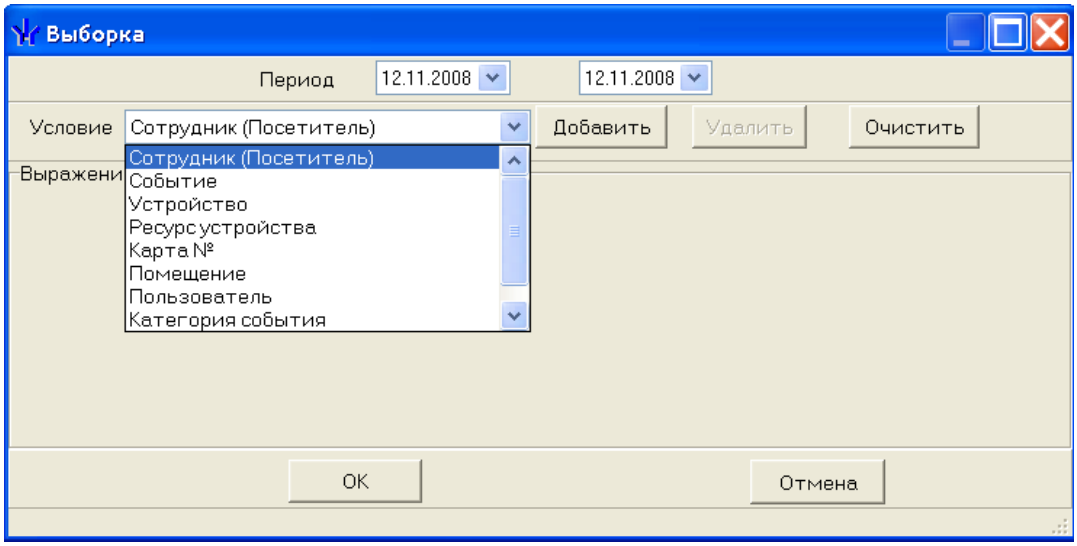


14.2 Выбор периода отчета

Для выбора периода отчета:

1. Нажмите на кнопку **Получить данные** –  .

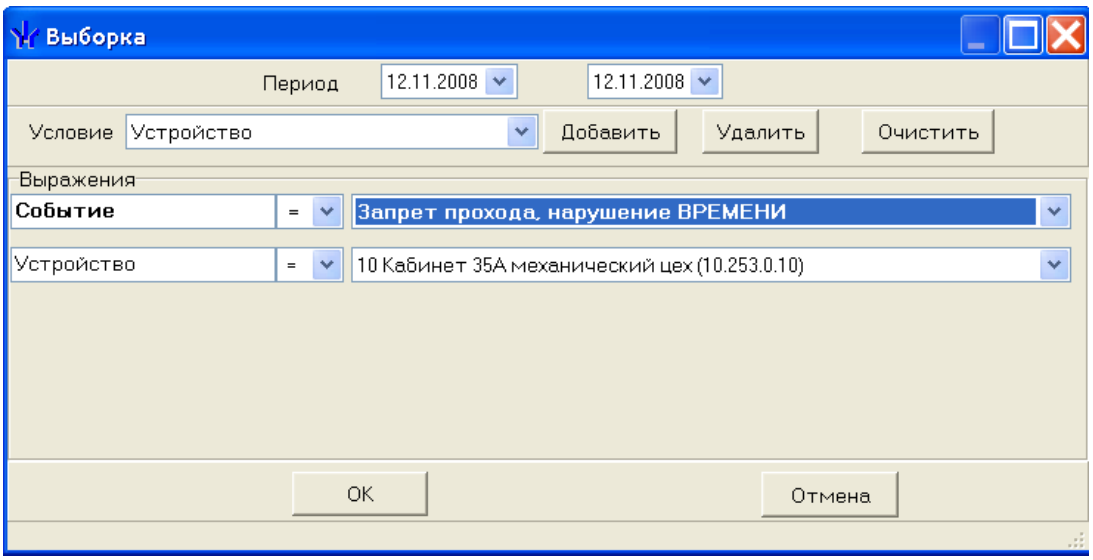
2. Выберите период:



Для получения событий за выбранный период щелкните на кнопке **ОК**. Для отмены выбранного действия щелкните на кнопке **Отмена**.

Также при получении данных можно уточнить, какие данные нужно получить из базы при помощи дополнительных условий.

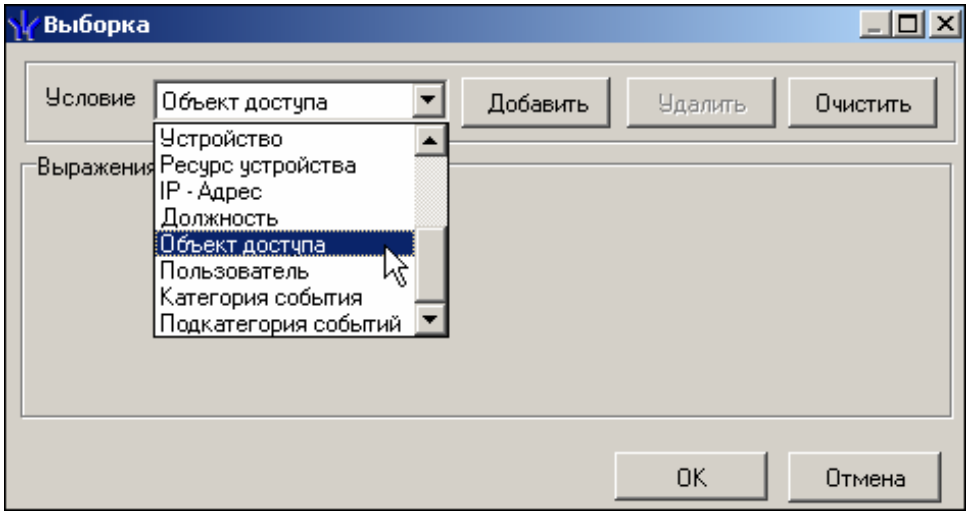
3. Для редактирования параметров используйте кнопки:
   Добавить – для добавления выражения.
   Удалить – для удаления выделенного выражения.
   Очистить – для удаления всех выражений.



14.3 Настройка выборки

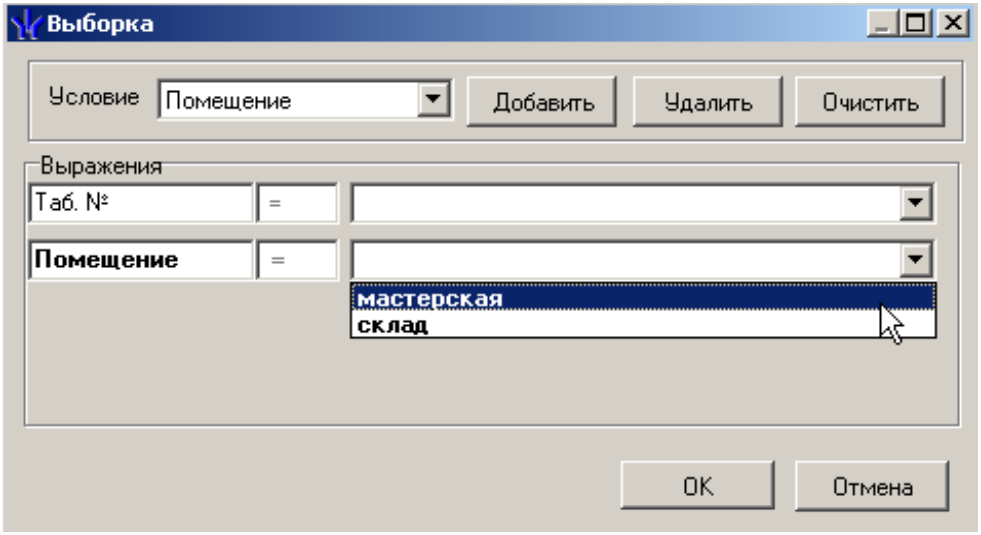
Для настройки выборки:

1. Щелкните на кнопке **Настроить выборку –**  . В окне выберите необходимые условия для выборки:



2. Щелкните на кнопку **Добавить**, в поле **Выражения** добавятся окна для ввода уточняющих параметров выборки.

3. Щелкните по стрелке раскрывающегося списка и выберите необходимое значение условия:



Удалить – для удаления выделенного выражения.
Очистить – для удаления всех выражений.

4. Нажмите на кнопку **ОК** для подтверждения создания выборки.

Около кнопки **Настроить выборку** будет установлен флажок  , а в рабочем окне отобразятся события устройств и действия пользователей, удовлетворяющие условиям выборки.

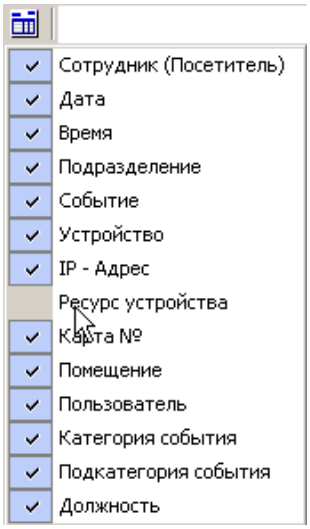
Разница между настройкой получения данных и фильтром в том, что при настройке получения данных данные выбираются из всей базы, а фильтр работает с уже полученными данными. Поэтому при получении данных настройки фильтра стираются.

14.4 Настройка столбцов таблицы

Для настройки столбцов таблицы:

1. Щелкните на кнопке **Настройка столбцов таблицы** –  .

2. Флажками отмечены те столбцы, которые будут отражены в отчете. Чтобы скрыть неиспользуемые столбцы отчета, снимите флажок напротив названия столбца:



15 ТРЕБОВАНИЯ К АППАРАТУРЕ

Объем дискового пространства:

- Сервер системы: 100 Гб.
- Станция: 1 Гб.

Оперативная память:

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

Процессор:

- Сервер системы: не ниже Pentium 4
- Станция: не ниже Celeron 2.5 ГГц

Операционная система

- Для сервера системы: Windows Server 2003 SP1, Windows XP SP3, Windows Vista SP2, Windows 7 SP1, Windows Server 2008, Windows Server 2008 R2
- Станций: Windows 2000 SP4, Windows XP SP3, Windows Vista SP2, Windows 7 SP1
- Для сервера системы допустимо использование 64 битных версий операционных систем.

Сеть: 100 Mbit,

Рекомендуемые GSM USB-модемы:

- Megafon Huawei Modem E1550
- Megafon Huawei Modem E173
- Megafon Huawei Modem E1820
- Megafon Huawei Modem E367
- МТС Huawei Modem E171
- МТС Huawei Modem E156G
- GSM модем TELEOFIS RX101-R USB GPRS (Telit)

ПРИЛОЖЕНИЯ

Приложение 1. 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 ЗАПРЕЩЕН* – доступ предъявленному идентификатору явным образом запрещен в контроллере, то есть предъявленный идентификатор включен в список доступа данного контроллера 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 комиссионирующим 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 комиссионирующим 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 Д*У 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 сопровождающейся санкционированным системой открытием ИУ (к примеру, механической разблокировкой 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 течение 2 мин.;
  - *Нет ответа на выполнение команды по каналу управления* – событие возникает в случае отсутствия ответа от контроллера в течение 6 мин. на выполнение команды сервером системы;

- *канал мониторинга* – служит для получения системой безопасности данных 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 течение 2 мин.;
- *канал регистрации* **–** служит для получения системой безопасности данных 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 течение 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: 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 проведении 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-пульта.* 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 нормализировано. 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 нормализировано. 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 комиссионирующим 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 комиссионирующим 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 нормализировано;
- *нарушение состояния ИУ.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние ресурса ИУ было не нормализировано.

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 нормализированным. 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 ЗАПРЕЩЕН* – доступ предъявленному идентификатору явным образом запрещен в контроллере, то есть предъявленный идентификатор включен в список доступа данного контроллера 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 комиссионирующим 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 комиссионирующим 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 (к примеру, механической разблокировкой 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, 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, 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 течение 2 мин.;
  - *Нет ответа на выполнение команды по каналу управления* – событие возникает в случае отсутствия ответа от контроллера в течение 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 течение 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 течение 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: 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: 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 сбр*ос;
- *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-пульта* (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 «землей» 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 «землей» 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».

3. 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 нормализировано. 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 нормализировано;
- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе взятия ОЗ на охрану было зафиксировано несоответствие с комиссионирующим 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 комиссионирующим идентификатором или комиссионирование 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 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 нормализировано. 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 нормализировано;

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 нормализировано. 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 нормализировано;

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 нормализированных

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 контроль 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 нормализировано;

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 снятие 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 нормализированных.

4. 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 нормализированным. 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.*
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 начато взятие ПШС.
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».

5. 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;

6. 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».

События контроллера регистрации

1. События, связанные с предъявлением идентификаторов

1.1 *Предъявление идентификатора* с причиной:

- *Идентификатор НЕ ЗАРЕГИСТРИРОВАН* – предъявленный идентификатор никогда не передавался в контроллер, то есть ему не назначались параметры контроля в этот контроллер;
- *Идентификатор ЗАПРЕЩЕН* – предъявленный идентификатор явным образом запрещен в контроллере;
- *Идентификатор из СТОП-ЛИСТА* – предъявленный идентификатор занесен в «СТОП-ЛИСТ»;

- *Идентификатор ПРОСРОЧЕН* – у предъявленного идентификатора истек срок действия, указанный в параметрах контроля;

1.2 *Проход* — событие, возникающее при прохода через один из считывателей контроллера без каких-либо выявленных нарушений.

1.3 *Проход* с причиной нарушения:

- *с нарушением ВРЕМЕНИ* – предъявленный идентификатор не удовлетворяет указанному в параметрах контроля временному критерию контроля;
- *с нарушением ЗОНАЛЬНОСТИ* – у данного контроллера установлена «мягкая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, либо установлена «жесткая» защита и была нарушена локальная зональность, то есть была совершена попытка повторного входа/выхода;
- *с нарушением ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ;*

1.4 *Проход не зарегистрирован.*

- *Нарушение ЗОНАЛЬНОСТИ.* У данного контроллера установлена «жесткая» защита от передачи идентификаторов. Предъявленный идентификатор нарушил глобальную зональность;
- *Нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ*. У данного контроллера установлена «жесткая» защита от передачи идентификаторов. Предъявленный идентификатор не удовлетворяет указанному в параметрах временному критерию контроля и нарушил глобальную зональность.

2. События, связанные с изменением текущего состояния контроллера

2.1 *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.

2.2 *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.

2.3 *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.

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

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

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

- *памяти DataFlash;*

- *часов RTC;*
- *шины I2C;*

2.6 *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.*

2.7 Тестирование контроллера

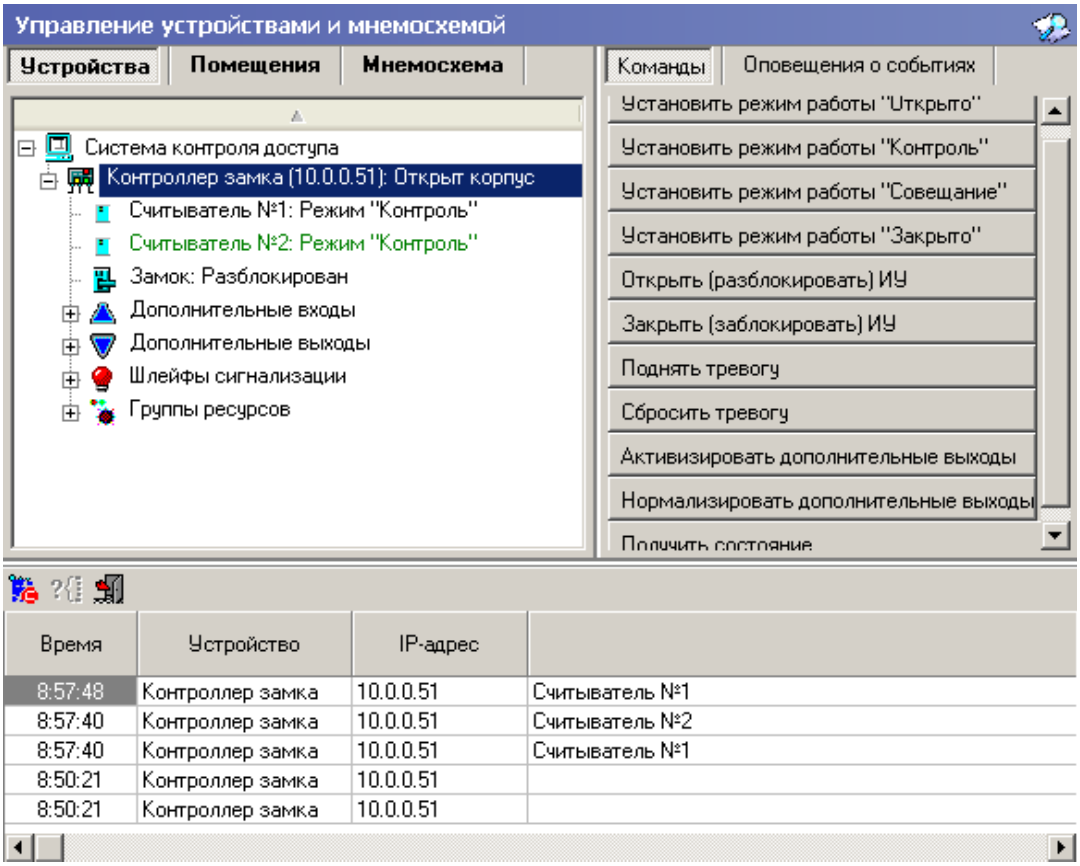
- *начато.* Переход устройства в режим «Тестирование» по команде Web-интерфейса.
- *завершено, неисправностей не выявлено.* Переход устройства в дежурный режим по завершению самодиагностики. Фатальных неисправностей не выявлено.
- *завершено, выявлены неисправности.* Завершение самодиагностики. Выявлены фатальные неисправности.

Приложение 2. Команды управления

Большинство устройств, входящих в единую систему безопасности PERCo-S-20, могут управляться из программного обеспечения. Для управления этими устройствами используются разделы ПО **Мониторинг**, **Центральный пост охраны** и программный модуль **Прием посетителей**.

Ниже приведен список команд управления доступных для каждого типа устройств.

Контроллер управления доступом



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.

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, определяемое параметром **«Время удержания в разблокируемом состоянии (время анализа идентификатора)»**. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии в зависимости от значения параметра, устанавливаемого в конфигурации ИУ.

Установить режим работы «Совещание». Аналогично режиму работы «Контроль», за исключением индикации на считывателях и блоке внутренней индикации. Более подробно об индикации режимов доступа изложено в техническом описании системы безопасности.

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 (открытое механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.

Поднять тревогу. Приводит к включению механизма реакции контроллера на возникновение тревожной ситуации. Параметры обработки тревожной ситуации для выбранного контроллера описываются в «*Генераторе тревоги*».

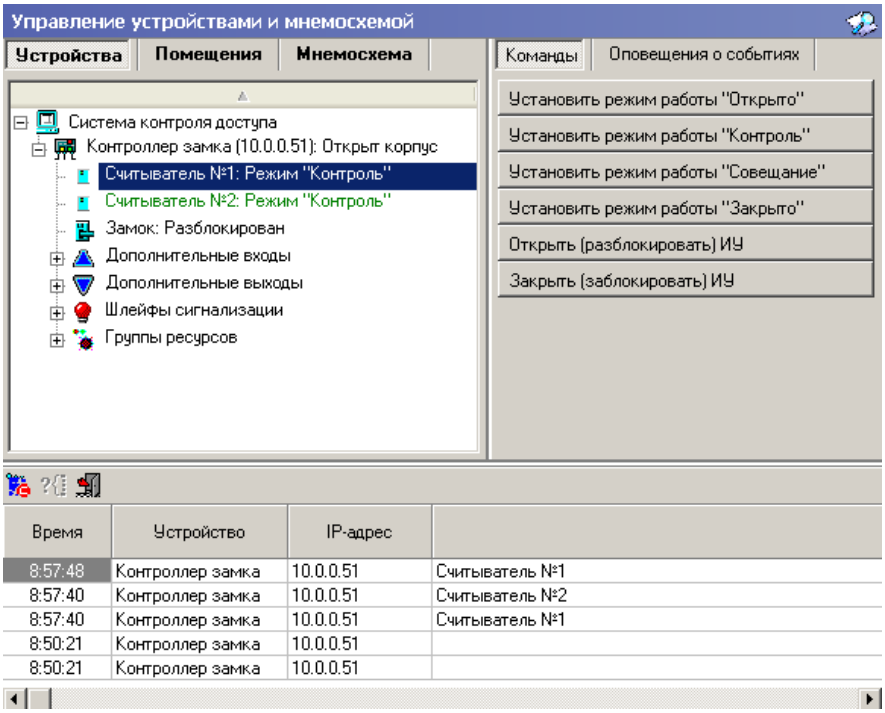
Сбросить тревогу. Приводит к прекращению выполнения контроллером механизма обработки тревожной ситуации.

Активизировать дополнительные выходы. Приводит к активизации всех релейных выходов выбранного контроллера.

Нормализовать дополнительные выходы. Приводит к нормализации всех релейных выходов данного контроллера.

Получить состояние. Выводит на экран отчет о параметрах устройства на момент команды.

Считыватель



Установить режим работы «Открыто». Приводит к установлению режима работы «Открыто» для ИУ, связанного с данным считывателем.

Установить режим работы «Контроль». Приводит к установлению режима работы «Контроль» для ИУ, связанного с данным считывателем.

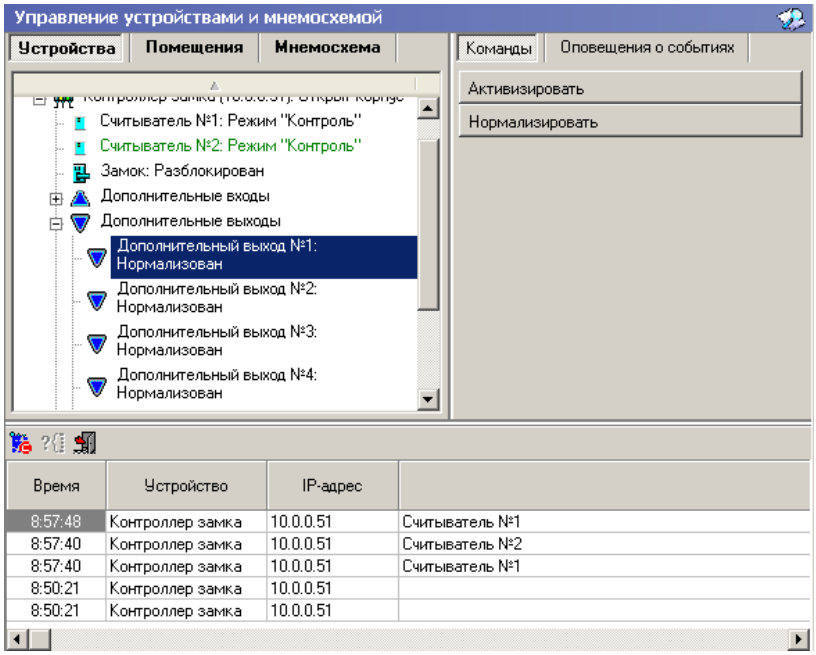
Установить режим работы «Совещание». Приводит к установлению режима работы «Совещание» для ИУ, связанного с данным считывателем.

Установить режим работы «Закрыто». Приводит к установлению режима работы «Закрыто» для ИУ, связанного с данным считывателем.

Открыть (разблокировать) ИУ. Приводит к разблокировке ИУ, связанного с этим считывателем на время, установленное параметром «Время разблокировки» для данного считывателя.

Закрыть (заблокировать) ИУ. Приводит к закрытию ИУ, связанного с данным считывателем.

Дополнительный выход



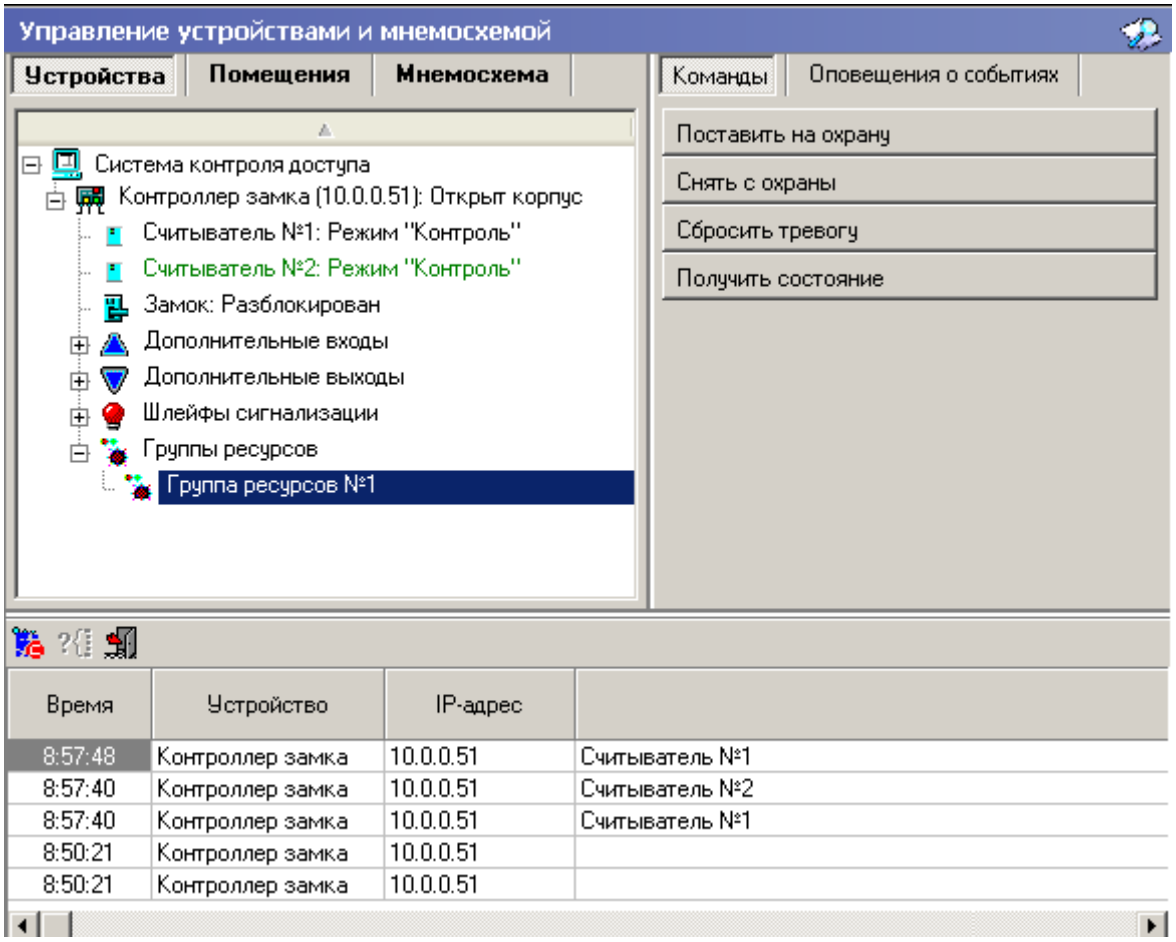
Активизировать. Приводит к переводу выбранного релейного выхода в активное состояние на время, установленное параметром «Время активизации» для данного выхода.

Нормализировать. Приводит к переводу выбранного релейного выхода в нормальное (исходное) состояние.

Примечание

При установке типа релейного выхода как ОПС или генератора тревоги, попытка активизировать или нормализировать этот выход из раздела ПО **Управления устройствами и мнемосхемой** приведет к ошибке – «Несоответствие типа ресурса».

Охранные зоны



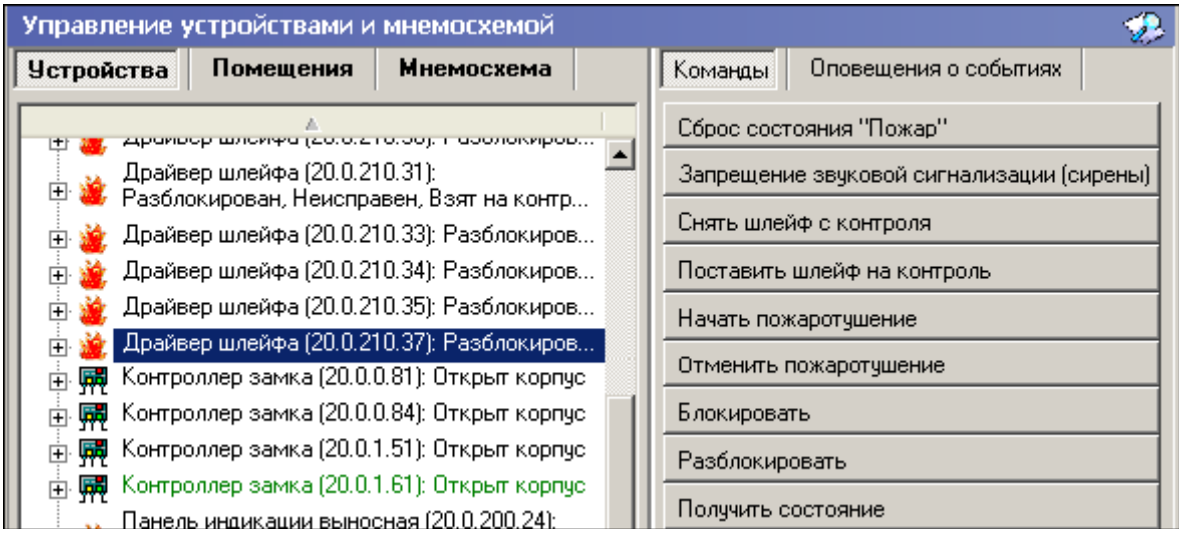
Поставить на охрану. Приводит к постановке выбранной охранной зоны на охрану. Если в состав выбранной охранной зоны входит исполнительное устройство, то ИУ блокируется и остается заблокированным в течение всего времени, пока режим включен. Нажатие на кнопку ДУ игнорируется. Открывание двери в режиме постановки на охрану вызывает регистрацию события о несанкционированном проходе (взломе) 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 «невзятие» через время задержки, задаваемое при конфигурации. Для взятого на охрану ШС контроллер отслеживает сопротивление в его линии и принимает решение о его состоянии.

Снять с охраны. Происходит снятие охранной зоны с охраны. Если в состав охранной зоны входит ИУ, то контроллер переходит в режим доступа «Контроль». Если в состав охранной зоны входит шлейф сигнализации, контроллер перестает отслеживать сопротивление в его линии.

Сбросить тревогу. Приводит к сбросу тревоги и прекращению выполнения алгоритма обработки тревожной ситуации.

Получить состояние. Выводит на экран отчет о параметрах устройства на момент команды.

Контроллер ППК



Сброс состояния «Пожар» – приводит к отключению индикации «Пожар» и прекращению выполнения контроллером подпрограмм состояния «Пожар»

Запрещение звуковой сигнализации (сирены) – приводит к отключению звуковой сигнализации.

Снять шлейф с контроля – приводит к снятию шлейфа с контроля. Используется для профилактических работ, проведения конфигурации и т.д.

Поставить шлейф на контроль – приводит к постановке шлейфа на контроль, драйвер шлейфа начинает анализировать состояния извещателей, подключенных к адресному шлейфу.

Начать пожаротушение – приводит к подаче сигнала на пуск системы пожаротушения в случае, если в зоне пожаротушения был зафиксирован пожар.

Отменить пожаротушение – приводит к отмене подачи сигнала на пуск системы пожаротушения в случае, если в конфигурации задан запуск системы пожаротушения с временной задержкой.

ООО «Завод ПЭРКо»

Тел.: (812) 329-89-24, 329-89-25
Факс: (812) 292-36-08

Юридический адрес:
180600, г. Псков, ул. Леона Поземского, 123 В

Техническая поддержка:

Тел./факс: (812) 321-61-55, 292-36-05

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

turnstile@perco.ru – по вопросам обслуживания турникетов, ограждений

locks@perco.ru – по вопросам обслуживания замков

soft@perco.ru – по вопросам технической поддержки программного обеспечения

www.perco.ru

Утв. 15.08.2011
Кор. 23.09.2013
Отп. 23.09.2013

www.perco.ru

тел: 8 (800) 333-52-53