РУКОВОДСТВО АДМИНИСТРАТОРА

Единая система **S-20**

Расширенная версия ПО

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Единая система безопасности PERCo-S-20 (далее — **система**) предназначена для обеспечения безопасности объектов, повышения контроля трудовой и технологической дисциплины, а так же 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.

СОСТАВ СИСТЕМЫ PERCO-S-20

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

1.Оперативного управления и наблюдения.

2.Управленческой части.

К первой части можно отнести контроллеры, пожарную сигнализацию, системы видеонаблюдения, АРМы службы безопасности и мониторинга. Ко второй - АРМы, не требующие оперативного контроля, такие как бюро пропусков, табельный учет и т.д.

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, сервера системы и серверов. При этом остальные модули ПО могут находиться в сети предприятия.

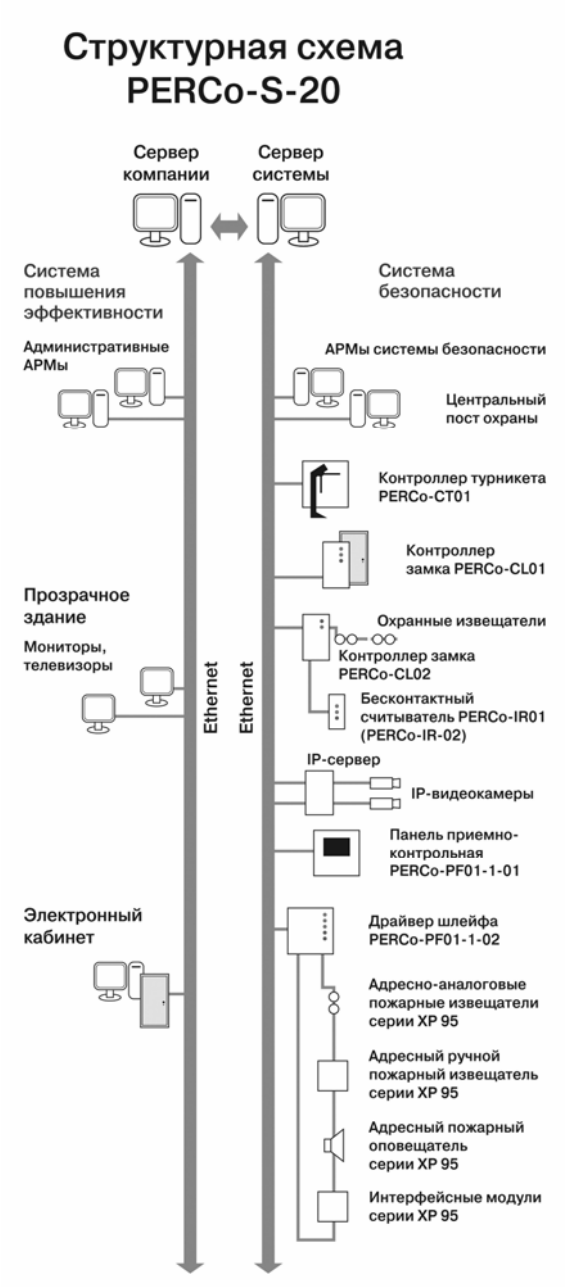


Рис. 1. Структурная схема системы PERCo-S-20

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 версии ПО.

Запуск Центра управления серверами системы PERCo-S-20 производится путём открытия файла MainCenter17k.cpl. 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 её архивов и после щелкните на кнопке «Создать базу».

5.Запустите модуль «Консоль управления» (для регистрации подразделов программы) с помощью Console17k.exe (или ярлык Консоль 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.

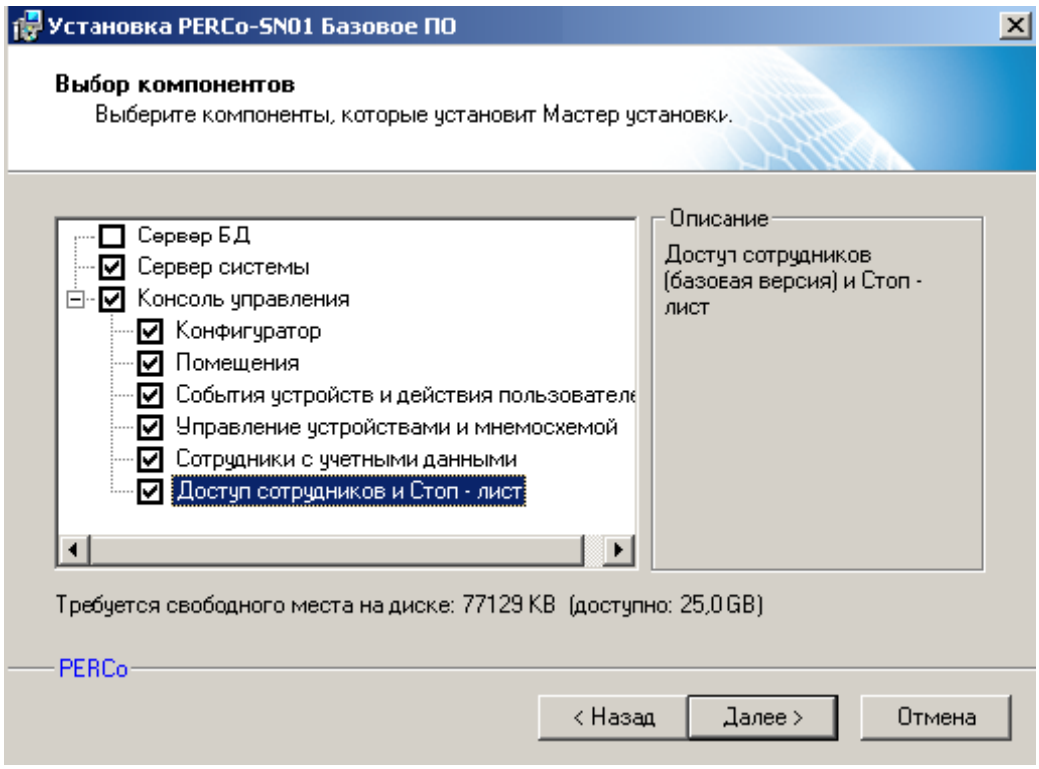
После проведения всех необходимых операций по настройке системы администратору рекомендуется задать себе пароль для входа в нее. Данная процедура необходима для установки эксклюзивного права администратора изменять настройки системы.

ИНСТАЛЯЦИЯ ПО

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

Инсталляция PERCo-SN01 «Расширенное ПО»

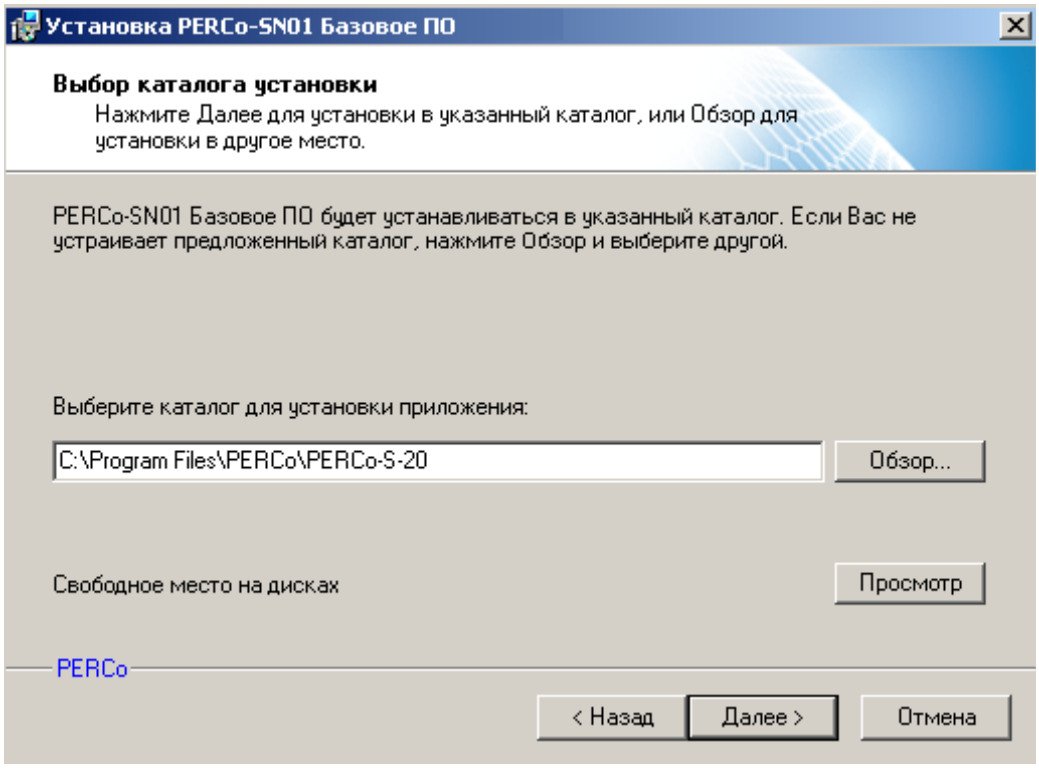
Вставьте компакт диск с дистрибутивом в привод CD-ROM. Должен автоматически запуститься инсталляционный модуль SetupBase.exe. Если этого не происходит — запустите данный модуль вручную. Следуйте указаниям мастера установки. Внимательно ознакомьтесь с предлагаемой информацией и лицензионным соглашением. 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 установки сервера управления базой данных Firebird 2.5.



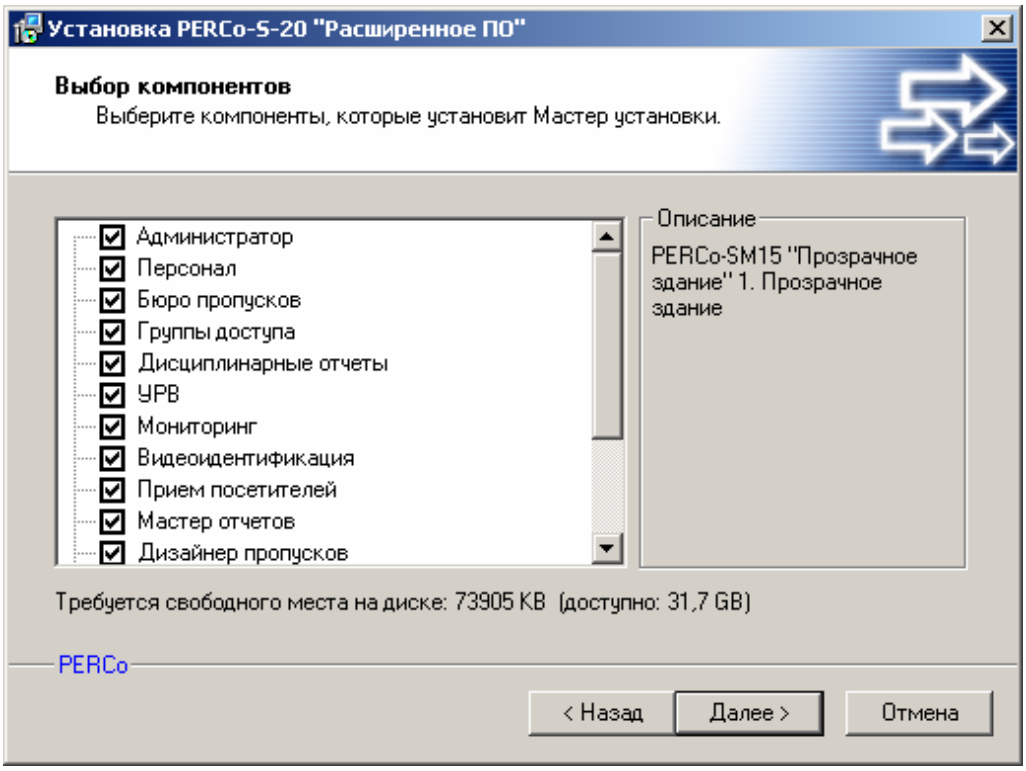
В открывшемся диалоговом окне укажите каталог, в который будет произведена установка программного обеспечения, и щелкните на кнопке Далее.

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.

Инсталляция сетевых модулей

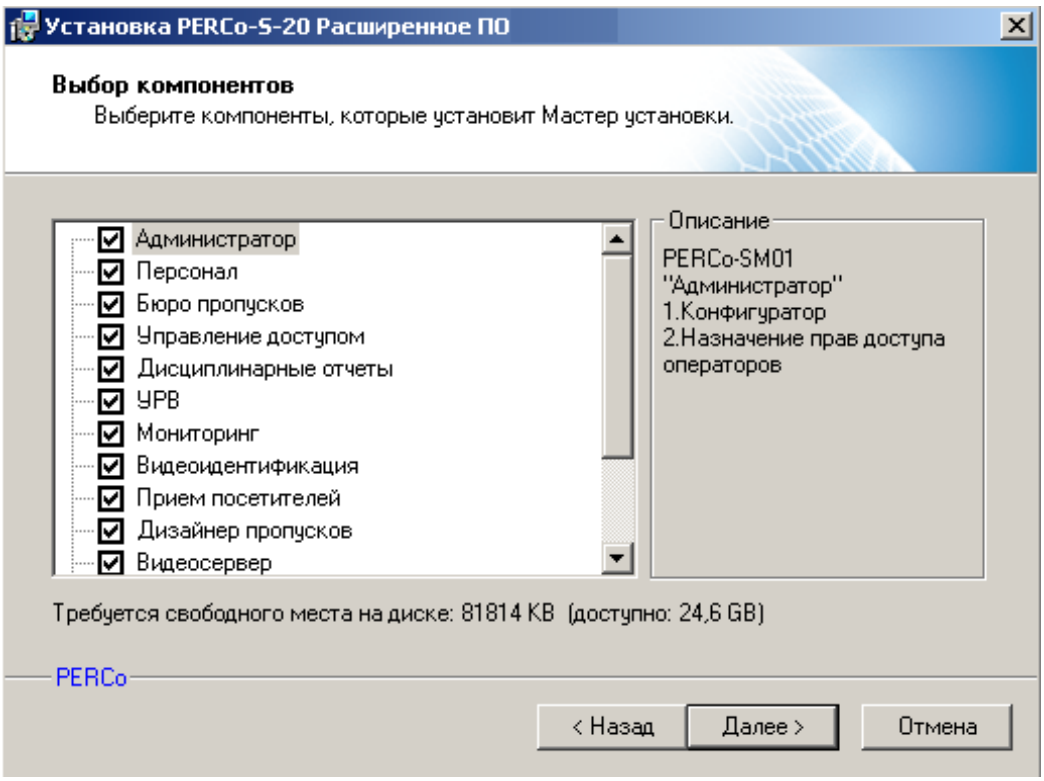
Вставьте компакт диск с дистрибутивом в привод CD-ROM. Должен автоматически запуститься инсталляционный модуль **SetupExtend.exe**. Если этого не происходит, запустите данный модуль вручную. Следуйте указаниям мастера установки. Внимательно ознакомьтесь с предлагаемой информацией и лицензионным соглашением. 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. Нажмите кнопку **Далее**.

ПРИМЕЧАНИЕ

Видеосервер необходим для функционирования сетевых модулей **Видеоидентификация**, **Прием посетителей**, **Видеонаблюдение**, **Центральный пост охраны**, **Прозрачное здание**. Более подробная информация о системе видеонаблюдения приведена в соответствующем разделе данного руководства.



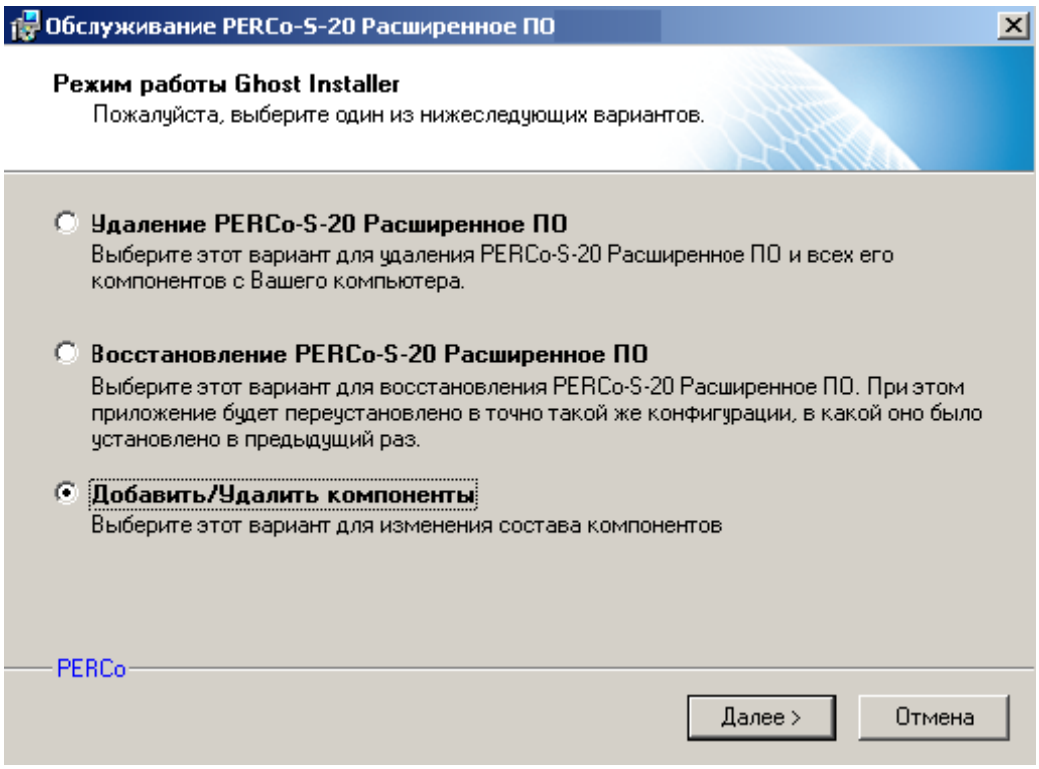
В открывшемся диалоговом окне укажите каталог в который будет произведена установка программного обеспечения и щелкните на кнопке **Далее**.

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

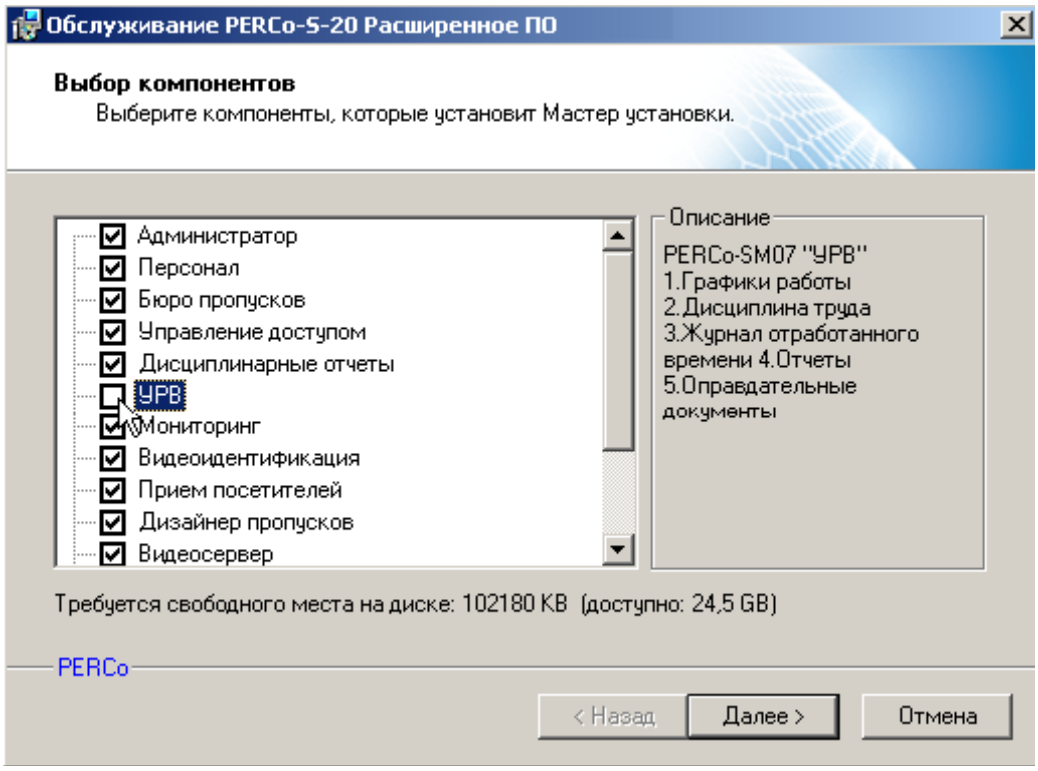
Изменяя или обновляя состав задействованных системных модулей, установите сначала базовое программное обеспечение, если его компоненты используются, а затем расширенное. После удаления расширенной версии следует переустановить базовую.

Удаление модулей

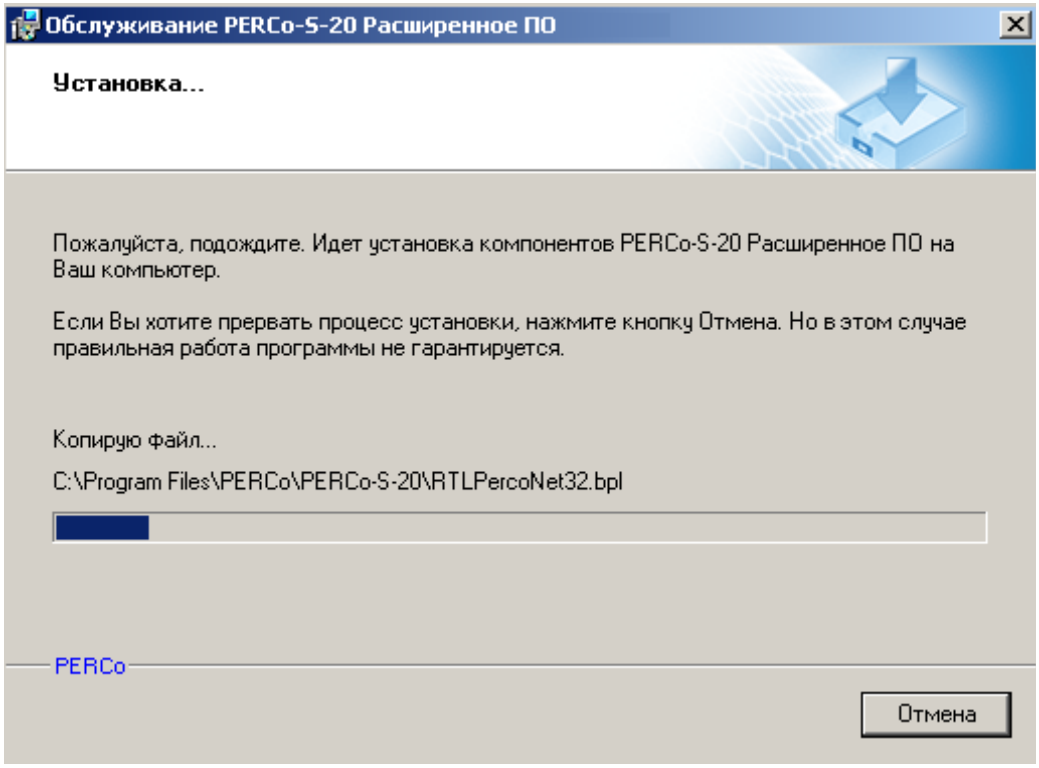
Вставьте компакт диск с дистрибутивом в привод CD-ROM. Должен автоматически запуститься инсталляционный модуль **SetupExtend.exe**. Если этого не происходит, запустите данный модуль вручную. Откроется окно:



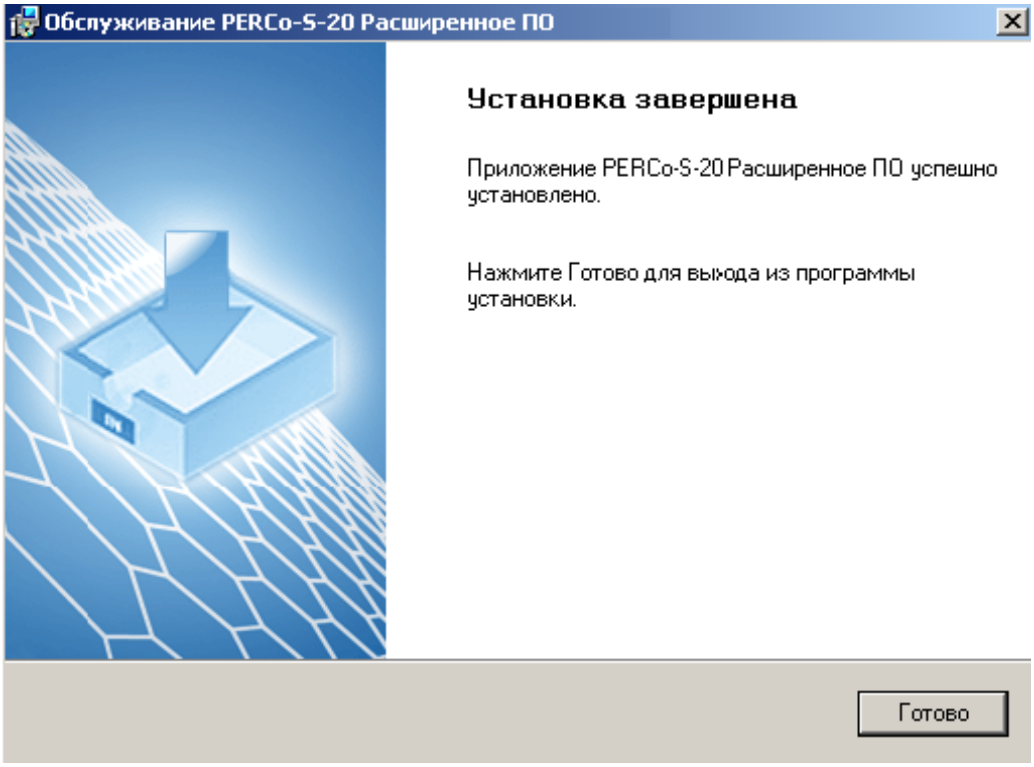
Выберите **Добавить/Удалить компоненты** и щелкните **Далее.** В открывшемся окне снимите метки рядом с теми модулями, которые хотите удалить:



Щелкните на кнопке **Далее**. Откроется окно, отображающее процесс переустановки всех модулей, кроме выбранных:



По окончании мастер установки сообщит об окончании операции:



Завершите процесс щелчком на копке **Готово**.

ПРИМЕЧАНИЕ

Для восстановления модулей вместо **Добавить/Удалить компоненты** выберите «**Восстановление…**».

ЛИЦЕНЗИИ

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

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

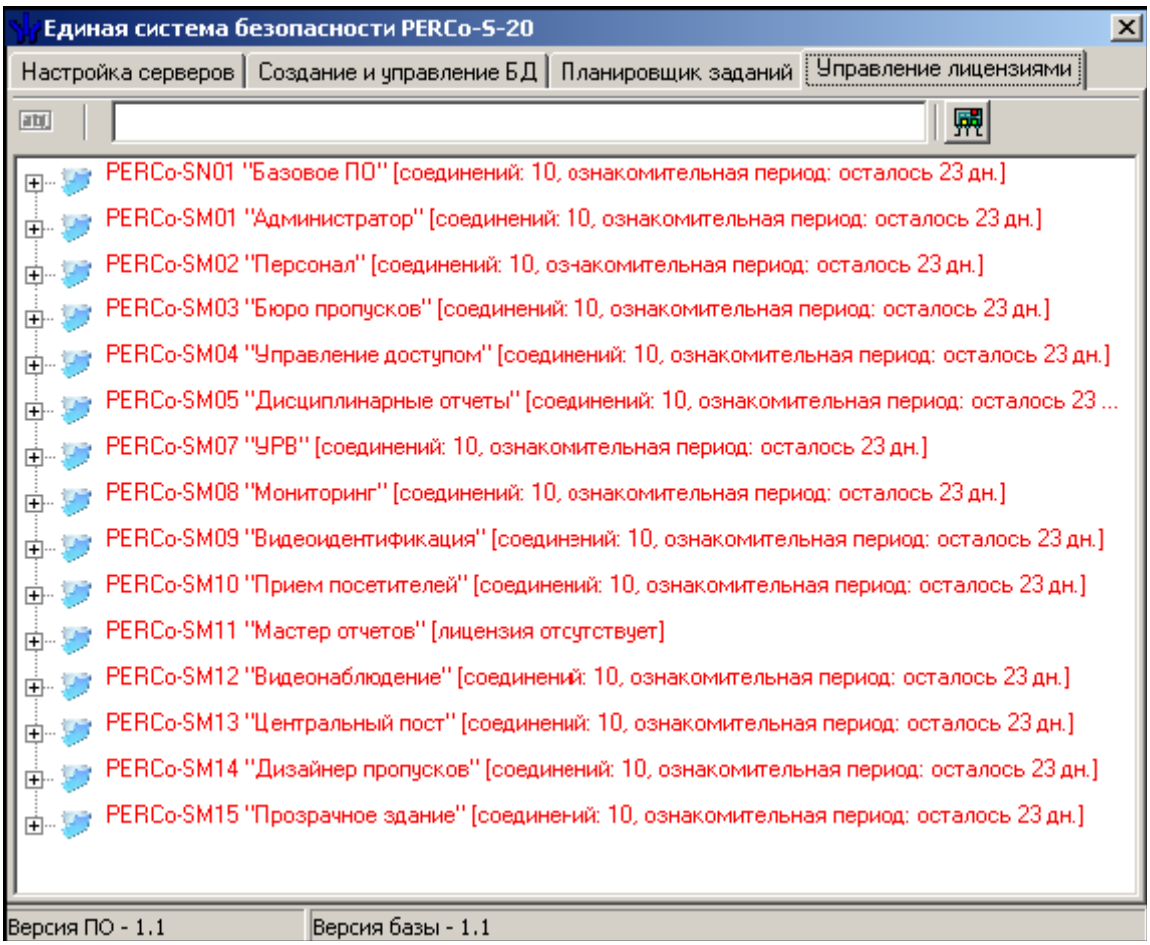
Для упрощения процедуры регистрации программного обеспечения, а так же для ознакомления с его возможностями, в течение 30 дней с момента первого запуска программное обеспечение работает в ознакомительном режиме.

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

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

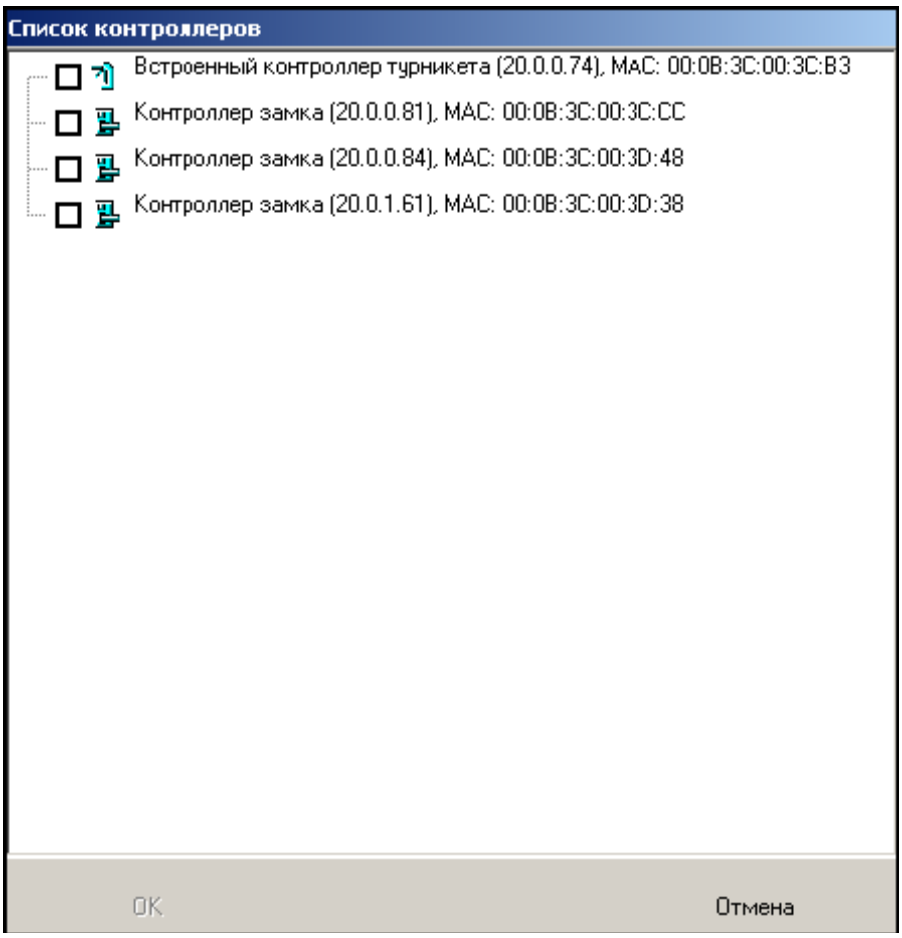
После получения лицензионного соглашения содержащего ключи активации вам необходимо ввести их в программное обеспечение. Ввод ключей активации производится в модуле Центр управления PERCo-S-20, входящем в состав **PERCo-SN01 «Базовое ПО»**. Более подробная информация о работе с этим модулем приведена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

Для запуска центра управления 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**:

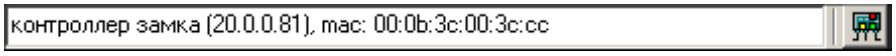


Для ввода лицензий укажите контроллер, MAC адрес которого содержится в лицензионном соглашении. Для этого щелкните на кнопке , расположенной в верхней части окна.

Откроется окно выбора:



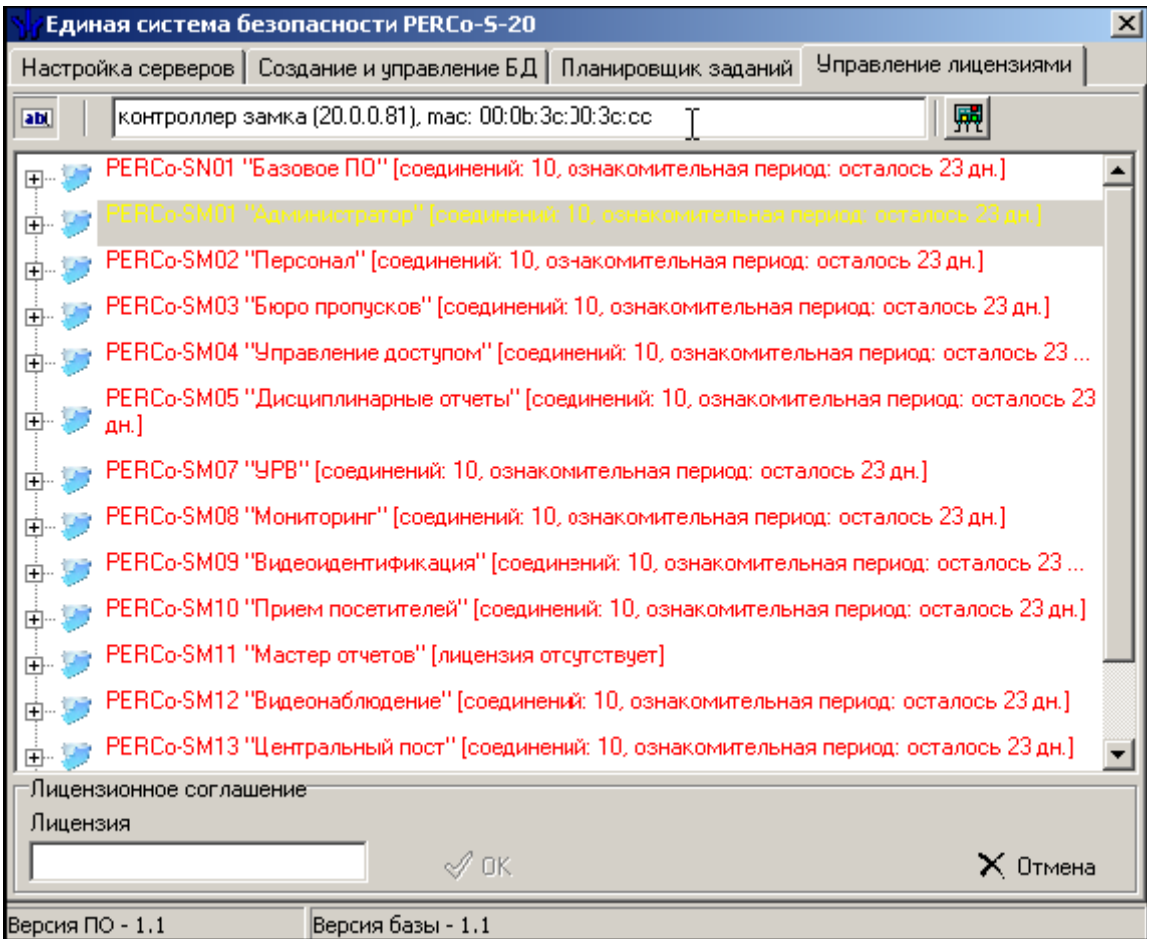
В этом окне отметьте выбранный вами раньше контроллер и щелкните на кнопке **«OK»**, что приведет к закрытию диалогового окна и отображению имени выбранного контроллера в верхней части рабочего окна:



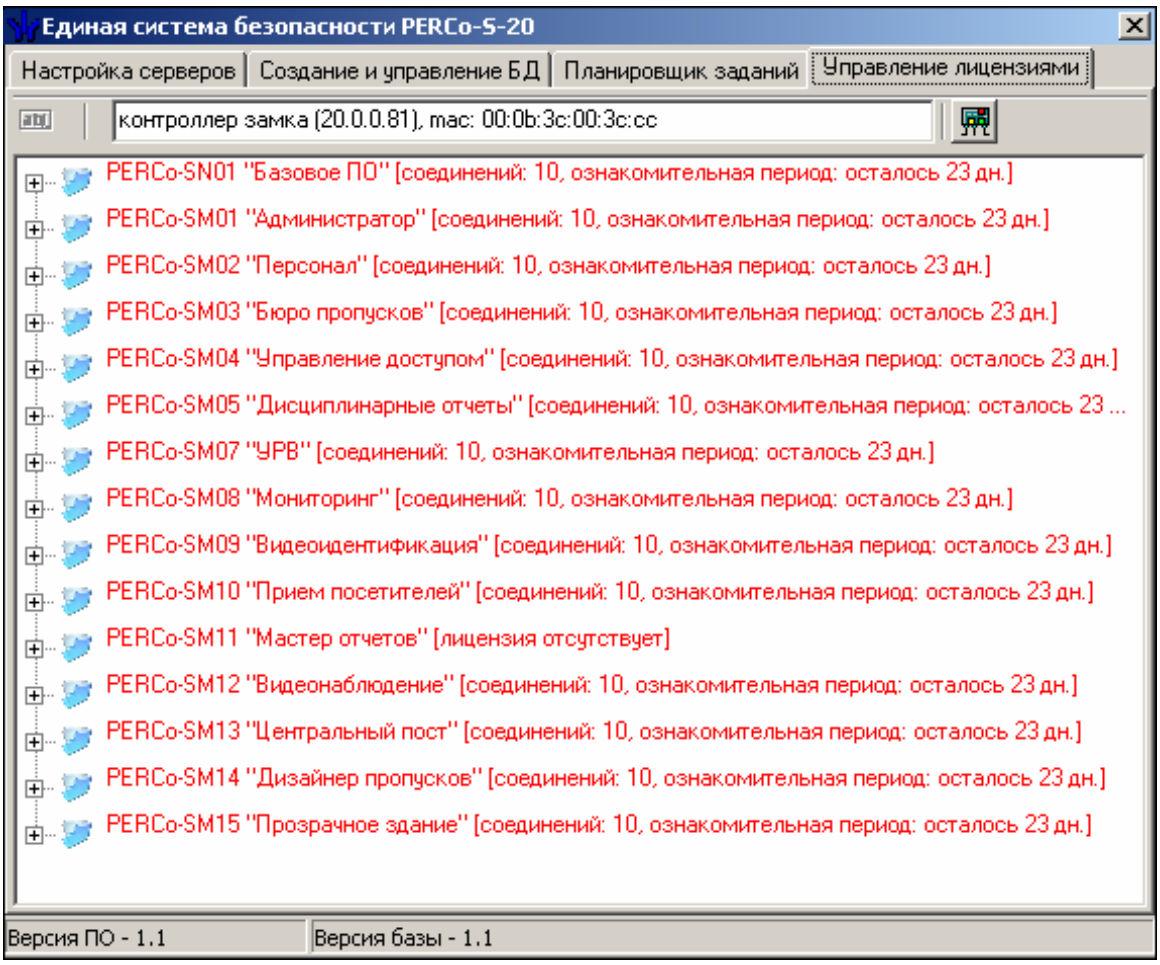
После выбора контроллера выделите в списке тот программный модуль, лицензию на который вы собираетесь ввести, и щелкните на кнопке  . При этом становится доступным строка ввода ключа активации:

ПРИМЕЧАНИЕ

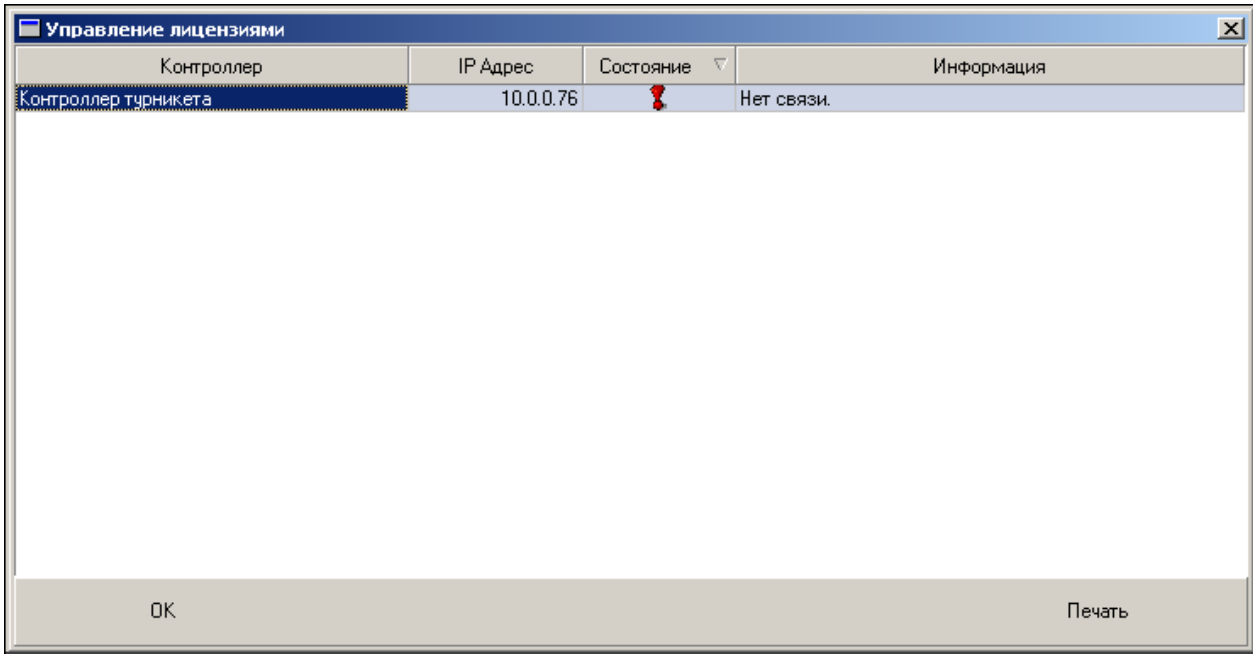
Код активации вводится без разделителей. Выбранный вами контроллер должен находиться во включенном состоянии, и быть подключенным к программному обеспечению. Для проверки наличия связи между программным обеспечением и выбранным контроллером можно воспользоваться модулем «Мониторинг».



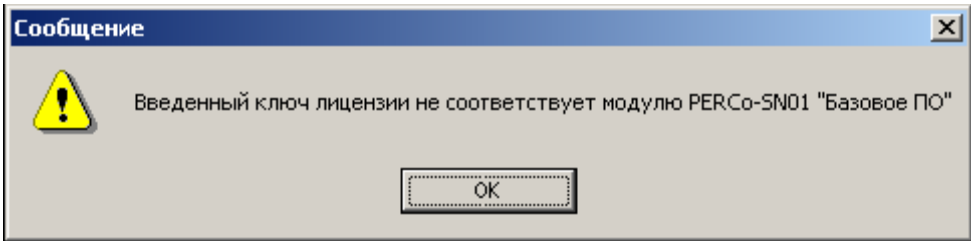
Введите код активации и нажмите кнопку  . После этого программное обеспечение автоматически осуществит проверку введенного вами кода активации. При положительном ответе рядом с названием выбранного модуля отображается информации о количестве активированных рабочих мест.



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



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



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

ПРИМЕЧАНИЕ

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

ОБЩИЕ СВЕДЕНИЯ

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

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

Для обмена данными в системе используется следующий стек протоколов

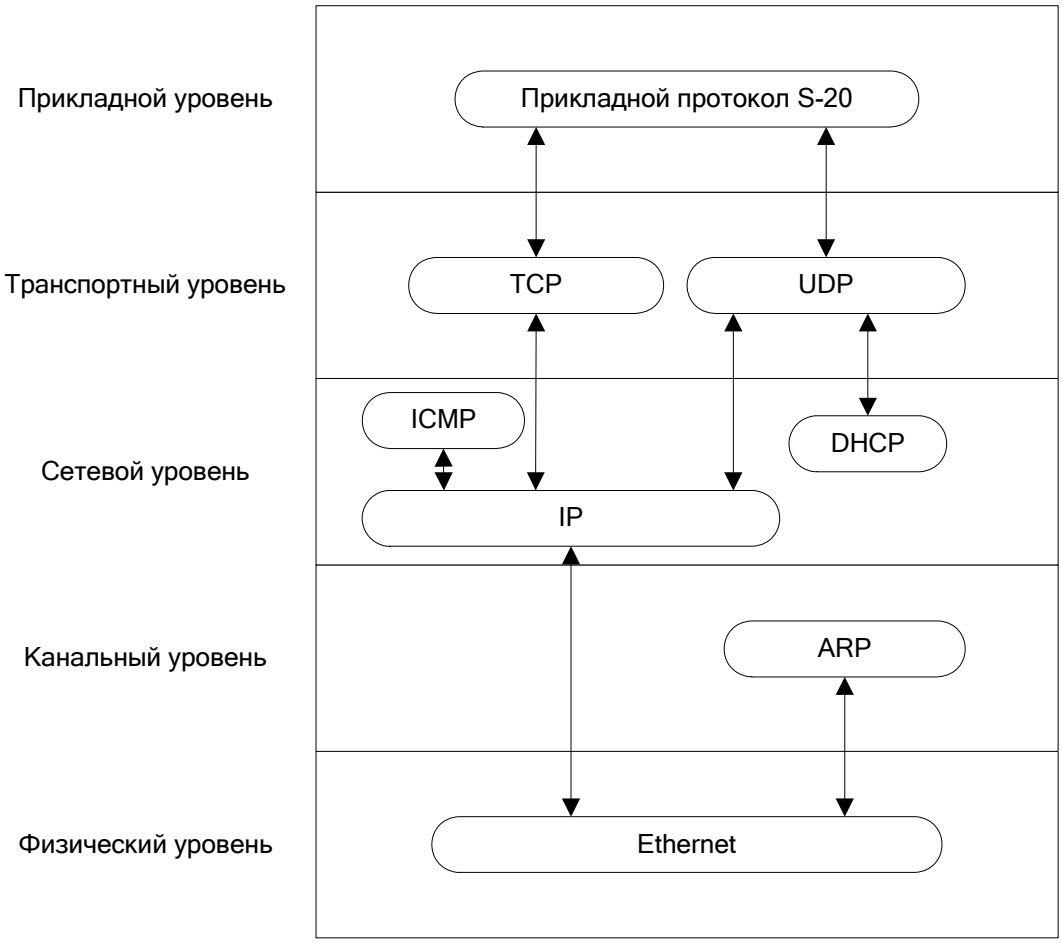


Рис. 2. Стек протоколов, используемых для обмена в системе

Также, для передачи данных используются следующие порты:

Табл. 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 Farewall-ы или встроенные в Windows XP, то в их конфигурации должны учесть 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, фрагментирующее IP-пакеты, которые 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.

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 **Конфигуратор** (см. Руководство оператора по разделу **Конфигуратор**), определив его целевые параметры.

Каждый контроллер имеет следующие предопределенные (заводские) сетевые настройки:

IP-адрес : 10.x.x.x

Шлюз: 10.0.0.1

Маска сети : 255.0.0.0

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

Конкретные для каждого контроллера значения (вместо символа «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.

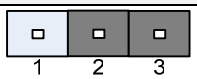
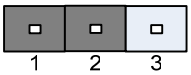
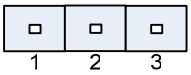
Режимы получения адреса

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.

.

Табл. 1. Варианты перемычек на контроллерах

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

Настройка без DHCP

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

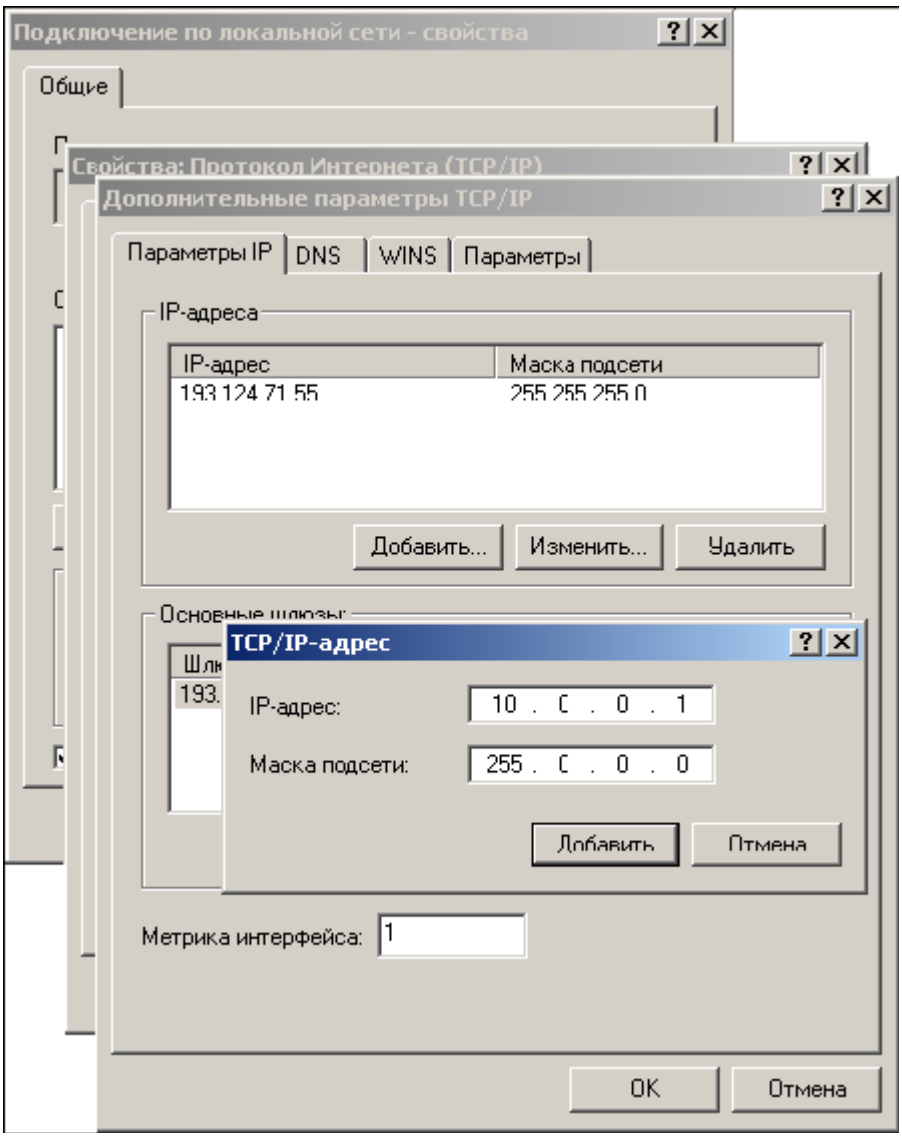


Рис. 4. Добавление нового IP-адреса

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

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

4. Включите контроллер. Произведите настройку согласно п. «***Конфигурация контроллеров***».

У контроллера достаточно сконфигурировать только сетевые настройки.

5. Установите контроллер на выбранное место работы.

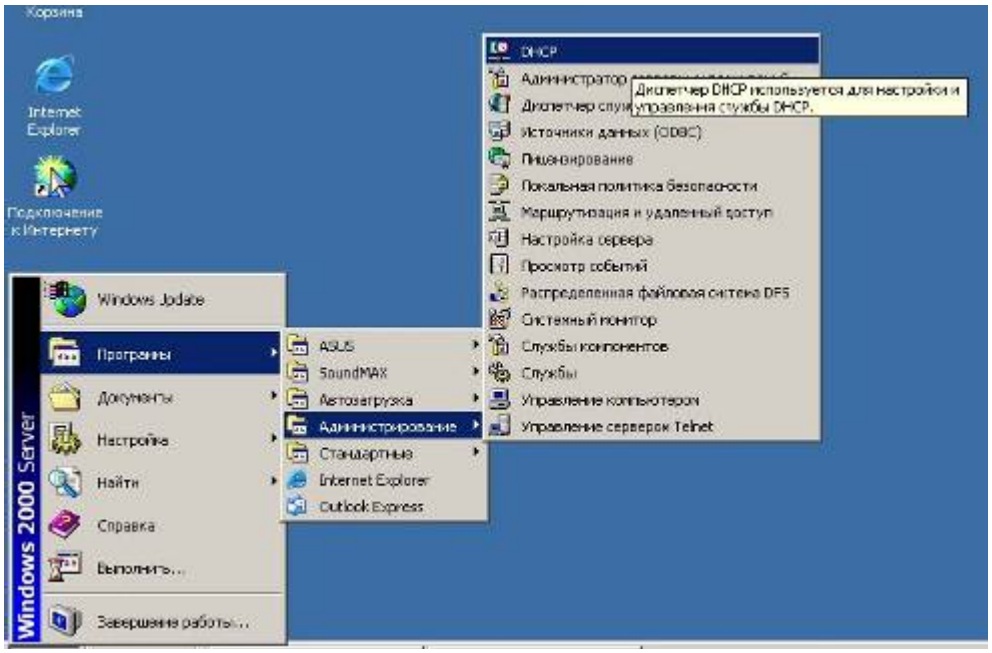
Настройка с DHCP

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

ОС Windows

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

1. Запустите DHCP сервер:

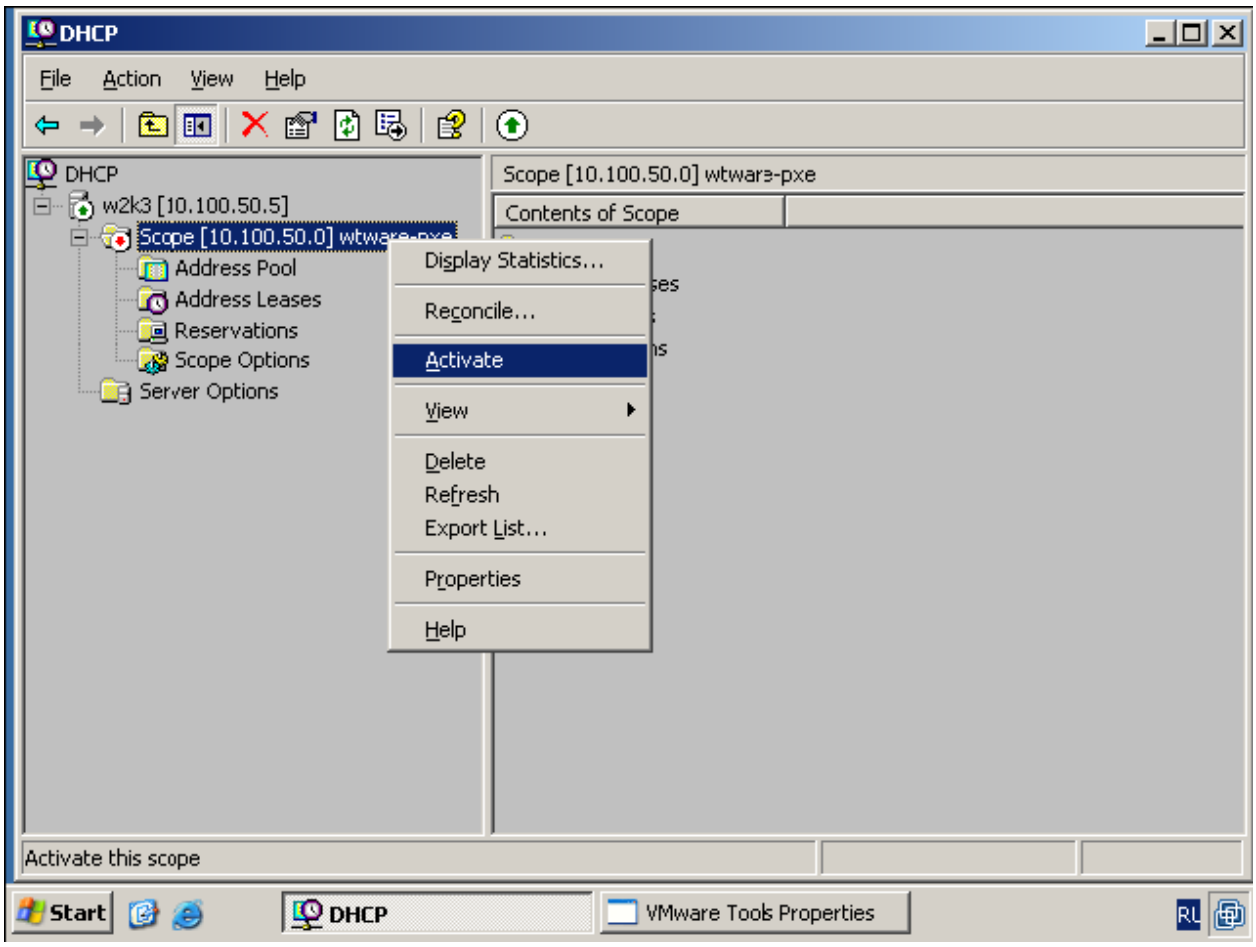


2. Создайте область адресов для контроллеров системы PERCo-S-20:

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

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

3. Последний и обязательный шаг – активация области:



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

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

5. Для удобства добавьте описание.

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

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

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

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

ОС Linux

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

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

Примерный вариант файла конфигурации показан ниже:

```
# Подсеть 10.100.0.0, маска сети 255.255.255.0

subnet 10.100.0.0 netmask 255.255.255.0 {

# маска подсети 255.255.255.0
```

```
option subnet-mask 255.255.255.0;
…
# диапазон адресов для контроллеров
# 10.100.0.10-10.100.0.254
range 10.100.0.10 10.100.0.254;
…
#описание контроллеров (proxod_1, …, office_room_101)
# обратите внимание на то, что вы должны использовать
# IP-адрес из указанного Вами диапазона

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

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

КОНФИГУРАЦИЯ КОНТРОЛЛЕРОВ

Конфигурация устройств системы безопасности

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

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

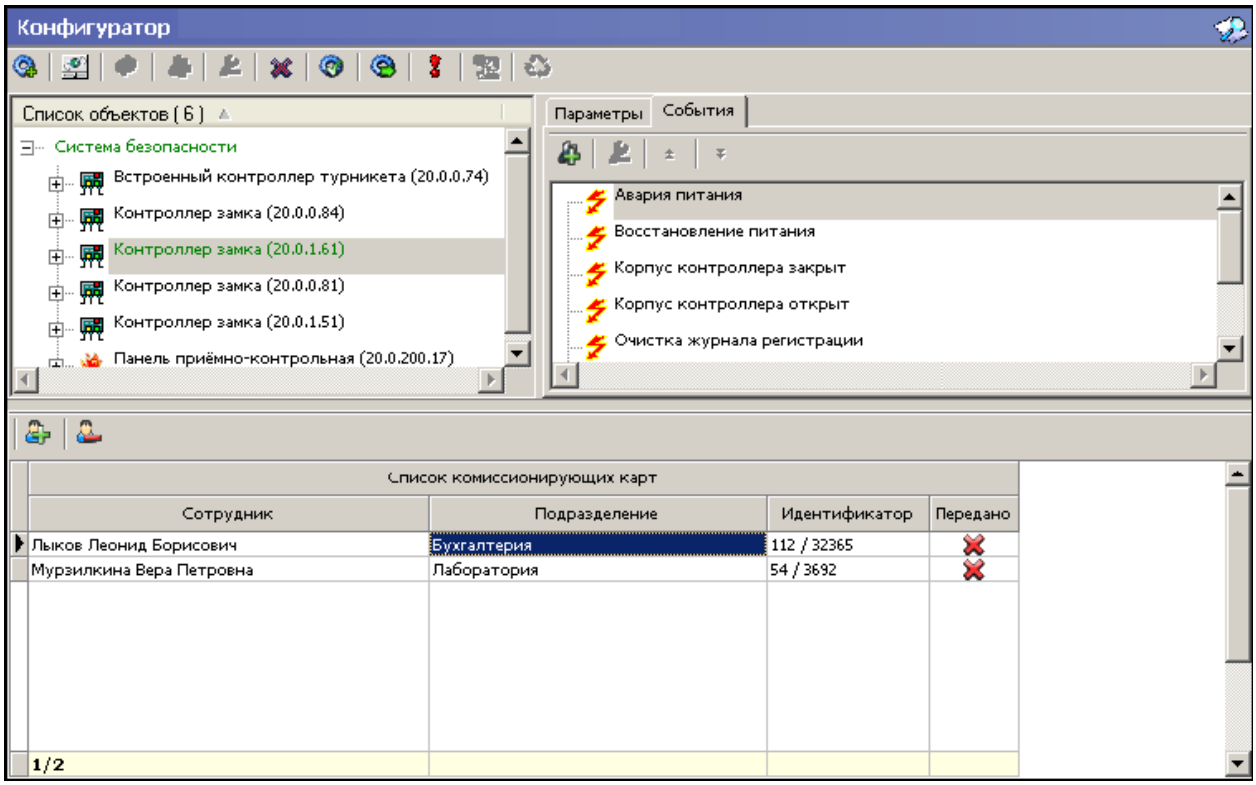
ПРИМЕЧАНИЕ

Автоматическая конфигурация контроллеров системы безопасности поддерживается только контроллерами управления доступом и видеосерверами. Конфигурация контроллеров пожарной сигнализации происходит только через добавление каждого контролера в ручном режиме.

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

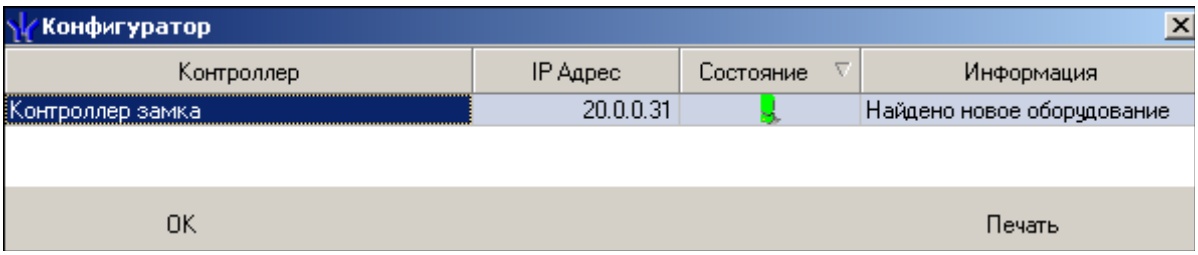
Если все выше сказанное выполнено, произведен монтаж контроллеров системы, при помощи команды “ping” проверено прохождение IP-пакетов с компьютера с установленным сервером системы, можно приступить к проведению конфигурации системы безопасности.

Для этого необходимо запустить «Консоль управления» на компьютере, на котором был проинсталлирован раздел **Конфигуратор**.



Подробная информация о назначении элементов меню раздела **Конфигуратор** приведена в Руководстве пользователя сетевого модуля **Администратор**.

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



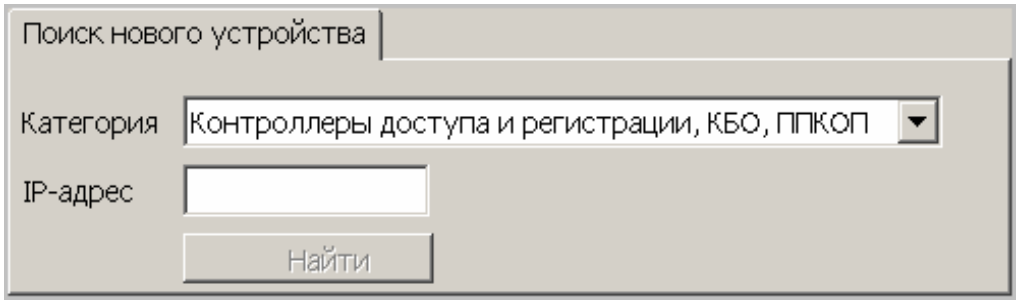
Проанализируйте полученную информацию, а именно проверьте все ли контроллеры были найдены в результате проведения конфигурации.

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

Если контроллер так и остался ненайденным, попробуйте добавить его в конфигурацию вручную.

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

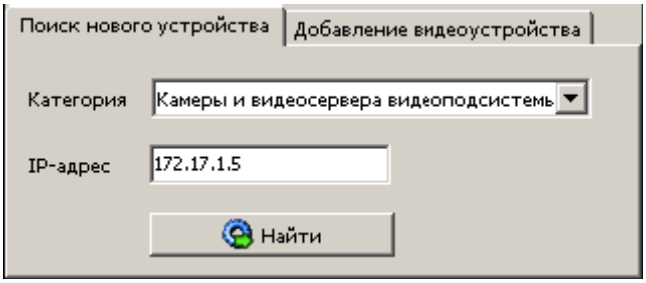
Для этого войдите в раздел **Конфигуратор** и щелкните на кнопке **Добавить новое устройство** —  . При этом в нижней части рабочего окна откроется дополнительная панель поиска:



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

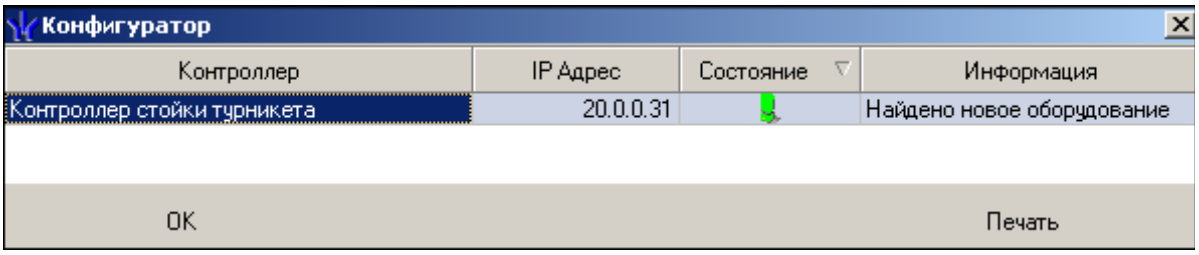
- **Контроллер доступа и регистрации, КБО, ППКОП –** в случае, если вы хотите добавить контроллер управления доступом или регистрации, контроллер безопасности объекта (КБО) или прибор приемно-контрольный охранно-пожарный (ППКОП).
- **Панели приемно-контрольные**. В случае если вы хотите добавить панель управления PERCo PF01, работающие в режиме АПКП.
- **Панели индикации выносные**. В случае если вы хотите добавить панель управления PERCo PF01, работающие отображения, то есть дополнительной панели отображения.
- **Видеоподсистемы**. В случае если вы хотите добавить видеоподсистему.
- **Камеры и видеосервера видеоподсистемы**

  которые можно добавить без поиска, используя вкладку Добавление видеоустройства.



В поле IP-адрес укажите IP-адрес устройства в формате XXX.XXX.XXX.XXX

Значенияия этих параметров, автоматически становится доступной кнопка **Найти**. Нажмите на нее, программное обеспечение проведет проверку возможности подключения к заданному вами устройству. Итоги этой проверки будут отображены в диалоговом окне:



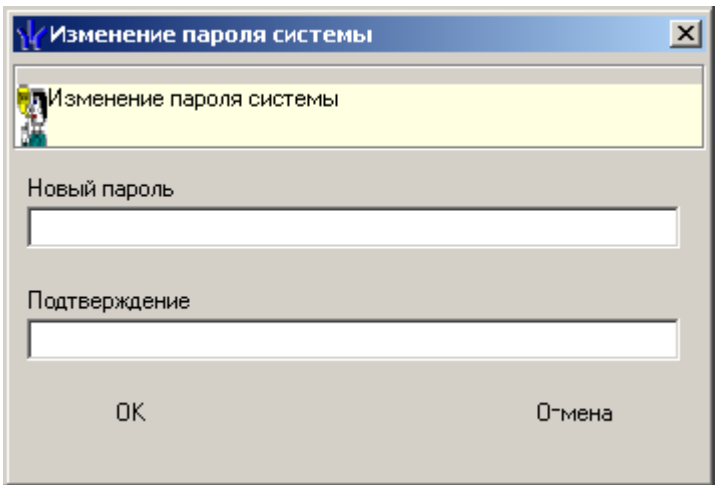
Нажмите на кнопку «**ОК**». Найденное оборудование будет добавлено в конфигурацию системы.

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

Задание пароля связи с контроллерами

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

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



ПРИМЕЧАНИЕ

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

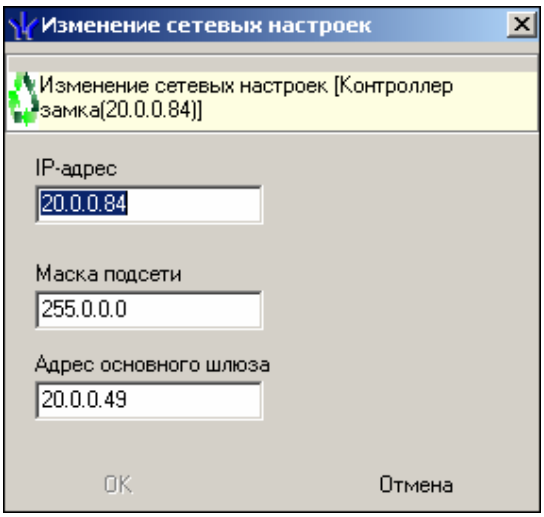
После ввода пароля необходимо передать измененные параметры!

Изменение сетевых настроек

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

Для изменения сетевых настроек:

1. Выделите контроллер, чьи сетевые настройки подлежат изменению.
2. Исключите контроллер из конфигурации, нажав на  .
3. Щелкните на кнопке **Изменение сетевых настроек** —  . Откроется окно:



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

Описание параметров функционирования контроллеров управления доступом

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

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

Дополнительный вход

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

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

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

1. При условии, что к данному дополнительному входу не подключено никакое внешнее оборудование, менять параметры работы входа не нужно.

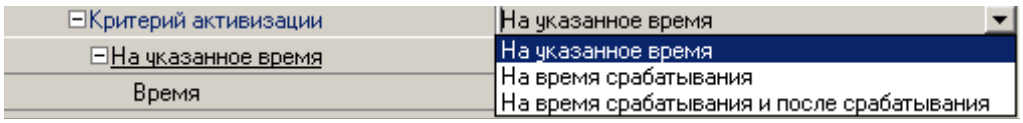
2. **Нормальное состояние контакта** (нормально замкнут или нормально разомкнут). Этот параметр зависит от типа подключенного оборудования и указывает системе на то, какое значение уровня сигнала на входе она должна воспринимать как нормальное.

3. Тип входа – **Обычный.** Означает что к данному дополнительному входу подключено внешнее оборудование, состояние которого должно анализироваться контроллером. При выборе этого типа можно так же указать алгоритм действий контроллера при получении управляющего воздействия от подключенного оборудования, а именно:

Нормальное состояние контакта	Разомкнут
⊟Тип	Обычный
⊟Обычный	
⊟Дополнительные выходы, активизирчемые при активизации	
Дополнительный выход №(1)	☐
⊟Критерий активизации	На указанное время
⊟На чказанное время	
Время	0 мс.
⊟Дополнительные выходы, нормализирчемые при активизации	
Дополнительный выход №(1)	☐
⊟Критерий нормализации	На время срабатывания и после срабатывания
⊟На время срабатывания и после срабатывания	
Время	250 мс.
⊟Дополнительные выходы, реагирчющие через грчппч ресчрсов	
Дополнительный выход №(1)	☐

- **Дополнительные выходы, активизируемые при активизации**. Этот параметр позволяет указать, какие именно дополнительные выходы данного контроллера должны быть активизированы при получении управляющего

сигнала от подключенного к дополнительному входу оборудования. Для выбора необходимо поставить «галочку» напротив тех дополнительных выходов, которые должны быть активизированы. Кроме этого, необходимо будет указать временной критерий активизации, который может быть трех видов:

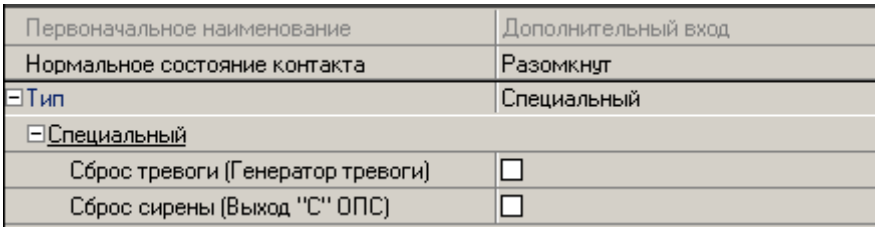


- ✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время.
- ✓ **На время срабатывания –** выбранные дополнительные выходы будут активизированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
- ✓ **На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

• **Дополнительные выходы нормализируемые при активизации.** Этот параметр позволяет указать, какие именно выходы данного контроллера должны быть нормализованы при получении управляющего сигнала от подключенного к тестовому входу оборудования. Для выбора необходимо поставить «галочку» напротив тех выходов, которые должны быть нормализованы. Задание остальных параметров нормализации дополнительных выходов полностью идентично заданию параметров активизации.

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

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



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

Возможны два варианта:

✓ **Сброс тревоги (Генератор тревоги).** В этом случае при возникновении тревоги из-за ситуации, описанной в генераторе тревоги, получение управляющего сигнала на выбранный дополнительный вход приведет к ее сбросу.

✓ **Сброс сирены (Выход «С» ОПС).** Аналогично предыдущему, за исключением того, что будет выключена сирена, подключенная к выходу «С» ОПС.

Дополнительный выход

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

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

Выход №4 и №7 для PERCo-CL02 и PERCo-CL03, которые на самом деле есть звуковые оповещатели, и использовать их для других целей проблематично. В техническом описании они идут обособлено, а в ПО определяются как обычные выходы.

В зависимости от того, какое внешнее оборудование подключено к описываемому дополнительному выходу и какому алгоритму работы оно подчиняется, существуют следующие варианты описания параметров работы выхода:

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

2. Тип дополнительного выхода – **Обычный.**

Первоначальное наименование	Дополнительный выход
⊟Тип	Обычный
⊟Обычный	
Нормальное состояние	Не запитан

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

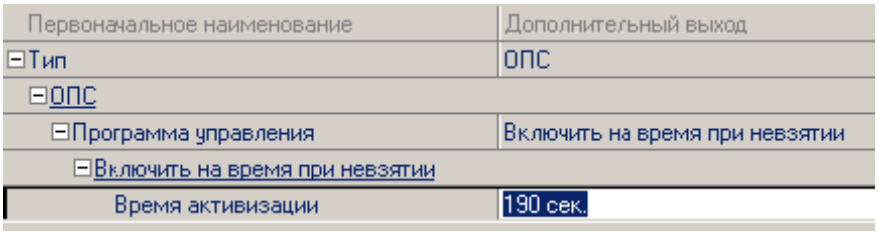
3. Тип дополнительного выхода – **Выход генератора тревоги.**

Первоначальное наименование	Дополнительный выход
⊟Тип	Генератора тревоги
⊟Генератора тревоги	
Нормальное состояние	Не запитан
Время активизации	121 сек.

В этом случае решение об активизации дополнительного выхода принимается исключительно контроллером в соответствии с параметрами, указанными в его генераторе тревоги. Этот дополнительный выход будет использоваться исключительно для индикации перехода контроллера в состояние «Тревога». Так же необходимо указать нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/не запитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий. Кроме этого, необходимо указать время активизации дополнительного выхода, время, до истечения которого выход не изменит

своего состояния. Как правило, в этом случае к такому дополнительному выходу подключают тревожный оповещатель (сирена, проблесковая лампа).

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



В этом случае дополнительный выход предназначен для управления СО, ЗО, а так же для передачи тревожных извещений на ПЦН при активизации ШС, дополнительных входов или контакта ИУ, входящих в группу ресурсов.

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

Возможны следующие варианты программ управления дополнительным выходом:

✓ **Не управлять.** Дополнительный выход не используется как элемент системы охранной сигнализации.

✓ **Включить при тревоге**. В случае возникновения тревоги произойдет замыкание контакта дополнительного выхода.

✓ **Выключить при тревоге**. В случае возникновения тревоги произойдет размыкание контакта дополнительного выхода.

✓ **Включить на время при тревоге**. В случае возникновения тревоги произойдет замыкание контакта дополнительного выхода на время указанное в параметре время активизации.

✓ **Выключить на время при тревоге**. В случае возникновения тревоги произойдет размыкание контакта дополнительного выхода на время указанное в параметре время активизации.

✓ **Мигать из состояния выключено при тревоге**. В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода разомкнуты. В случае возникновения тревоги произойдет попеременное замыкание – размыкание контактов дополнительного выхода.

✓ **Мигать из состояния включено при тревоге**. В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода замкнуты. В случае возникновения тревоги произойдет попеременное размыкание - замыкание контактов дополнительного выхода.

✓ **Мигать на время из состояния выключено при тревоге**. В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода разомкнуты. В случае возникновения тревоги произойдет попеременное замыкание – размыкание контактов дополнительного выхода на время, указанное в параметре «Время активизации».

✓ **Мигать на время из состояния включено при тревоге**. В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода замкнуты. В случае возникновения тревоги произойдет попеременное размыкание – замыкание контактов дополнительного выхода на время, указанное в параметре «Время активизации».

✓ **Лампа –** программа управления, указывающая на то, что к данному дополнительному выходу подключен световой оповещатель тревожной ситуации.

✓ **ПЦН –** программа управления, указывающая на то, что данный дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН).

✓ **ПЦН (старая тактика) –** программа управления, указывающая на то, что данный дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН) по старой тактике передачи тревожного оповещения.

✓ **Сирена –** программа управления, указывающая на то, что к данному дополнительному выходу подключен звуковой оповещатель тревожной ситуации.

✓ **Включить на время перед взятием** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре «Время активизации», перед началом взятия шлейфа на охрану.

✓ **Выключить на время перед взятием** - программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре «Время активизации», перед началом взятия шлейфа на охрану.

✓ **Включить на время при взятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре «Время активизации», при взятия шлейфа на охрану.

✓ **Выключить на время при взятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре «Время активизации», при взятия шлейфа на охрану.

✓ **Включить при взятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода при взятии шлейфа на охрану.

✓ **Выключить при взятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода при взятии шлейфа на охрану.

✓ **Включить на время при снятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре «Время активизации», при снятии шлейфа с охраны.

✓ **Выключить на время при снятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре «Время активизации», при снятии шлейфа с охраны.

✓ **Включить при снятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода при снятии шлейфа с охраны.

✓ **Выключить при снятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода при снятии шлейфа с охраны.

✓ **Включить на время при невзятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода при невозможности взятия шлейфа на охрану.

✓ **Выключить на время при невзятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода при невозможности взятия шлейфа на охрану.

ПРИМЕЧАНИЕ

При установке типа дополнительного выхода как ОПС или генератора тревоги, попытка активировать или нормализовать этот выход из **Управления устройствами и мнемосхемой** приведет к ошибке – «Несоответствие типа ресурса».

Исполнительное устройство

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

Для контроллера управления замком:

Первоначальное наименование	Замок
Нормальное (т.е заблокированное) состояние контакта (вход ИУ)	Нормально замкнут
Нормальное состояние "Закрыто" выхода ИУ	Не запитан
Нормализация выхода ИУ	После "Открытия"
Режим работы выхода управления ИУ	Потенциальный
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа карты)	4 сек.
Регистрация прохода по предъявлению карты	☐
Защита от передачи карт (Antipass)	Нет
⊟ Дополнительные выходы, реагирующие через группу ресурсов	
Дополнительный выход №(1)	☑
Дополнительный выход №(2)	☐
Дополнительный выход №(3)	☐
Дополнительный выход №(4)	☐

Для контроллера управления турникетом:

Первоначальное наименование	Стойка турникета
Прямое направление прохода	☑
Нормальное (т.е заблокированное) состояние контакта (вход ИУ)	Нормально замкнут
Нормальное состояние "Закрыто" выхода ИУ	Не запитан
Нормализация выхода ИУ	После "Открытия"
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа карты)	4 сек.
Регистрация прохода по предъявлению карты	☐
Защита от передачи карт (Antipass)	Нет

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

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

2. **Нормальное состояние «Закрыто» выхода ИУ.** Параметр описывает должен ли контроллер подавать напряжение на ИУ в состоянии «Закрыто». Например, для электромагнитных замков в состоянии «Закрыто» необходимо подавать напряжение, а для электромеханических - нет.

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

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

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

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

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

Это нужно для тех случаев, когда контроллер используется как регистрирующие устройство для учета, например, УРВ сотрудников и факт открытие \закрытие двери игнорируется.

8. **Защита от передачи карт** задает режим работы контроллера по контролю за локальным антипасбэком, контролем за повторным входом. При отмеченной опции, контроллер будет блокировать попытки повторного входа/выхода.

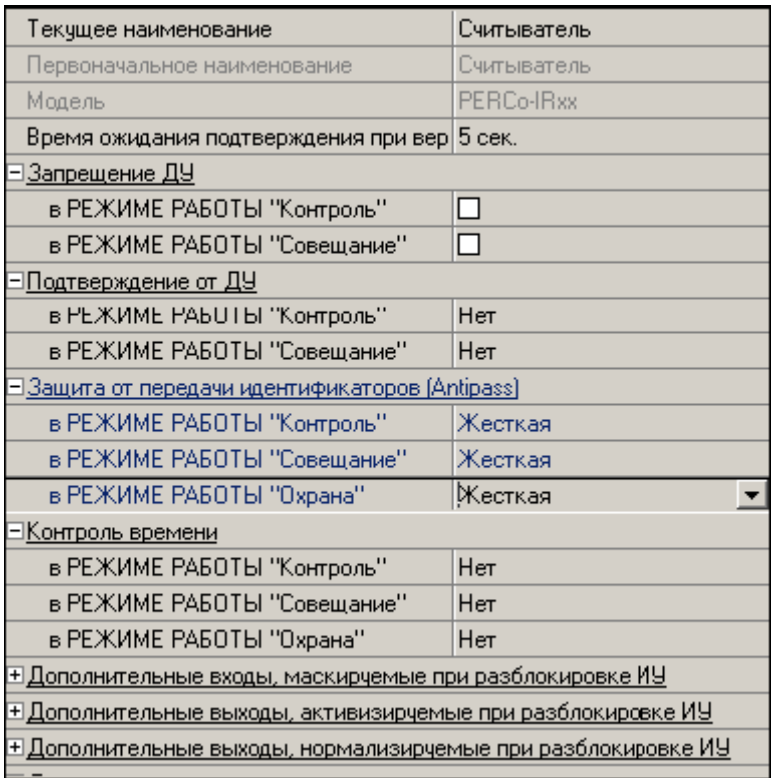
9. **Дополнительные выходы, реагирующие через группу ресурсов**. Параметр указывает, должны ли активизироваться дополнительные выходы при условии, что исполнительное устройство входит в группу ресурсов.

10. **Прямое направление прохода** (только для контроллеров управления турникетом). Данный параметр определяет, в какую сторону будет разблокирован турникет при предъявлении карты к первому считывателю контроллера.

Считыватель

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

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

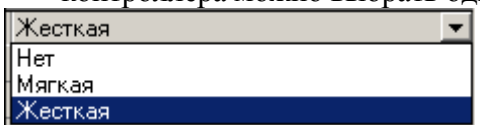


1. **Время ожидания подтверждения от верификации** – временной параметр, который устанавливает время, в течение которого контроллер будет ожидать поднесения комиссионирующей карты или подтверждения от верифицирующего устройства. В качестве верифицирующего устройства может быть использовано ДУ контроллера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

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

3. **Подтверждение от ДУ** – при помощи этого параметра можно указать, что в выбранных режимах доступа при поднесении карты к этому считывающему устройству проход будет разрешен только после получения подтверждения от ДУ.

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



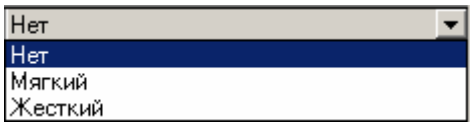
✓ **Нет** – контроллер не будет запрещать двойные проходы по выбранному считывателю.

✓ **Мягкая** – контроллер разрешит повторный проход по карте,

предъявленной к выбранному считывателю, но при этом в журнале мониторинга будет отображено сообщение о проходе с нарушением зональности.

✓ **Жесткая** – контроллер запретит попытку двойного прохода при предъявлении карты к выбранному считывателю. При этом в журнал мониторинга и журнал регистрации будет записано событие о запрете прохода по причине нарушения зональности.

5. **Контроль времени** – параметр, который позволяет задать реакцию контроллера на предъявление карты с учетом текущего времени, дня недели и так далее. Контроль времени задается отдельно для указанных режимов доступа и может иметь следующие значения:



✓ **Нет** – при выборе этого значения контроллер не будет учитывать временные параметры доступа карты для разрешения прохода по предъявленной карте.

✓ **Мягкий** – при выборе этого параметра контроллер разрешит доступ по предъявленной карте, но проведет сравнение текущего времени и даты с временными параметрами доступа предъявленной карты. В случае их нарушения запишет в журнал мониторинга 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 исполнительное устройство. В случае их нарушения запретит проход и запишет в журналы мониторинга и регистрации событие о запрете прохода в связи с нарушением времени.

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

Дополнительные входы, маскирчемые при разблокировке ИУ	
Дополнительный вход №(1)	☐
Критерий маскирования	На указанное время
На указанное время	
Время	10 сек.
Дополнительные выходы, активизирчемые при разблокировке ИУ	
Дополнительный выход №(1)	☐
Дополнительный выход №(2)	☐
Дополнительный выход №(3)	☐
Дополнительный выход №(4)	☐
Критерий активизации	На указанное время
На указанное время	
Время	0 мс.
Дополнительные выходы, нормализирчемые при разблокировке ИУ	
Дополнительный выход №(1)	☐
Дополнительный выход №(2)	☐
Дополнительный выход №(3)	☐
Дополнительный выход №(4)	☐
Критерий нормализации	На указанное время
На указанное время	
Время	0 мс.
Дополнительные выходы, активизирчемые при предъявлении валидных пропусков сотрудников	
Дополнительный выход №(1)	☐
Дополнительный выход №(2)	☐
Дополнительный выход №(3)	☐
Дополнительный выход №(4)	☐
Критерий активизации	На указанное время
На указанное время	
Время	0 мс.
Дополнительные выходы, активизирчемые при предъявлении валидных пропусков гостей	
Дополнительный выход №(1)	☐
Дополнительный выход №(2)	☐
Дополнительный выход №(3)	☐
Дополнительный выход №(4)	☐
Критерий активизации	На указанное время
На указанное время	
Время	0 мс.

1. Дополнительные входы, маскируемые при разблокировке ИУ. Параметр позволяет указать те входы контроллера, информация об активизации которых не будет восприниматься контроллером в течение указанного времени при разблокировке ИУ. Как правило, данный параметр используется для маскирования тестового входа, к которому подключен датчик прохода, тем самым, исключая возможность поднятия ложной тревоги при санкционированном проходе.

2. Дополнительные выходы, активизируемые при разблокировке ИУ. Параметр позволяет указать те выходы контроллера, которые будут активизированы при разблокировке ИУ на время указанное ниже

3. Дополнительные выходы, нормализируемые при разблокировке ИУ. Параметр позволяет указать те выходы контроллера, которые будут нормализованы при разблокировке ИУ на время указанное ниже.

4. Дополнительные выходы, активизируемые при предъявлении валидных пропусков сотрудников. Этот параметр позволяет указать те выходы, которые будут активизированы в случае предъявления пропуска сотрудника, имеющего право на проход в соответствии с действующим режимом работы на время

указанное ниже. Этот параметр может быть использован в случае, если к этим выходам подключено устройство сбора карт или дополнительная индикация, информирующая работников охраны о статусе предъявленной карты.

5. **Дополнительные выходы, активизируемые при предъявлении валидных пропусков гостей.** Этот параметр позволяет указать те выходы, которые будут активизированы в случае предъявления пропуска гостя, имеющего право на проход в соответствии с действующим режимом работы на время указанное ниже. Этот параметр может быть использован в случае, если к этим выходам подключено устройство сбора карт или дополнительная индикация, информирующая работников охраны о статусе предъявленной карты.

Генератор тревоги

В зависимости от структуры системы безопасности, ее задач, местоположения контроллера управления доступом, текущего режима работы те или иные события и действия пользователей системы могут как приводить к генерации тревоги, так и восприниматься как нормальный режим работы.

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

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

1. **Генерация тревоги при предъявлении пропуска.** Этот параметр позволяет указать будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» при предъявлении пропусков с указанными параметрами доступа.
2. **Генерация тревоги при несанкционированной разблокировке ИУ.** Этот параметр позволяет указать будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» в случае разблокировки ИУ при помощи ключа (то есть разблокировке ИУ без команды от контроллера) в выбранных режимах работы.

3. **Генерация тревоги по недопустимо долгому открытию ИУ.** Этот параметр позволяет указать будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» в случае, если после открытия ИУ оно не было приведено в исходное состояние в течение времени большего, чем указано в параметрах этого ИУ. Другими словами, должен ли контроллер перейти в состояние «Тревога», если после прохода через дверь, она осталось открытой.
4. **Дополнительные входы, активизирующие генерацию тревоги.** Параметр, позволяющий выбрать те дополнительные входы контроллера, активизация которых будет приводить к переходу контроллера в состояние «Тревога». Это может быть использовано, например, при подключении к этому тестовому входу кнопки тревожной сигнализации.
5. **Тихая тревога.** Параметр, который позволяет отключить активизацию дополнительного выхода контроллера, помеченного как «Выход генерации тревоги».

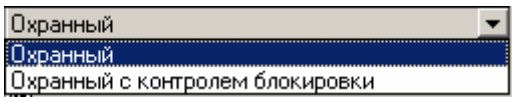
Шлейф сигнализации

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

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

Первоначальное наименование	Шлейф сигнализации
Тип	Охранный
Автоматическое перевзятие	☑
Тихая тревога	☑
Повторное включение сирены	☐
Длительность нарушения	70 мс.
Задержка взятия на охрану	0 мс.
Задержка управления выходом "С"	0 мс.
Задержка управления выходом "Л"	0 мс.
Задержка восстановления нарушенного шлейфа в снятом состоянии	0 мс.
Тип извещателя	Без питания по шлейфу
⊟ Дополнительные выходы	
Дополнительный выход №(1)	☐
Дополнительный выход №(2)	☐
Дополнительный выход №(3)	☐
Дополнительный выход №(4)	☐

1. **Тип.** Дает возможность указать тип шлейфа охранной сигнализации.



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

2. Автоматическое перевзятие. При включенной опции, при постановке на охрану шлейфа охранной сигнализации, в случае невозможности взятия шлейфа на охрану, контроллер автоматически будет пытаться взять шлейф **на охрану повторно.**

3. Тихая тревога. При включении этой опции, если в состав шлейфа включены дополнительные релейные выходы, работающие по программам «Сирена» или «Лампа», то эти программы не будут активизированы.

4. Повторное включение сирены. Параметр указывает, должен ли контроллер повторно включить сирену при условии повторного нарушения шлейфа.

5. Длительность нарушения. Временной параметр, в течение которого нарушение шлейфа не будет считаться тревожным.

6. Задержка взятия на охрану – интервал времени, по истечению которого контроллер начнет анализировать состояние шлейфа охранной сигнализации для постановки на охрану. Как правило, это время устанавливают отличным от нуля в ситуации, когда место постановки на охрану находится так же под контролем этого шлейфа. И после постановки на охрану необходимо время для того, чтобы покинуть охраняемое помещение.

7. Задержка управления выходом «С» – указывает время, в течении которого контроллер не будет активизировать выход с программой управления «Серена» после нарушения шлейфа.

8. Задержка управления выходом «Л» – указывает время, в течении которого контроллер не будет активизировать выход с программой управления «Лампа» после нарушения шлейфа.

9. **Тип извещателя** – контроллер поддерживает работу с двумя типами извещателей по питанию:

- ✓ **Без питания по шлейфу**
- ✓ **С питанием по шлейфу**

10. Дополнительные выходы. Дополнительные выходы этого контроллера, которые будут использованы в соответствии с указанной у них программой.

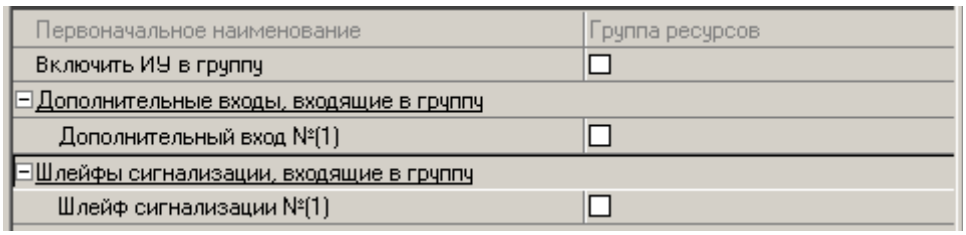
ПРИМЕЧАНИЕ

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

Группы ресурсов

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

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



1. Включить ИУ в группу. Параметр, указывающий на то, входит ли исполнительное устройство в эту группу. То есть, если исполнительное устройство добавлено в группу, при постановке на охрану контроллер будет контролировать его состояние. В противном случае открытие двери не будет приводить к возникновению тревоги после постановки группы ресурсов на охрану. Это может быть использовано в том случае, когда ресурсы контроллера используются не только для контроля помещения, доступ в которое он контролирует.

2. Дополнительные входы, входящие в группу. Параметр позволяет указать дополнительные входы контроллера, которые будут так же контролироваться контроллером при постановке группы ресурсов на охрану**.**

3. Шлейфы сигнализации, входящие в группу. Параметр позволяет указать, какие шлейфы сигнализации входят в выбранную группу ресурсов.

Защита от передачи идентификаторов

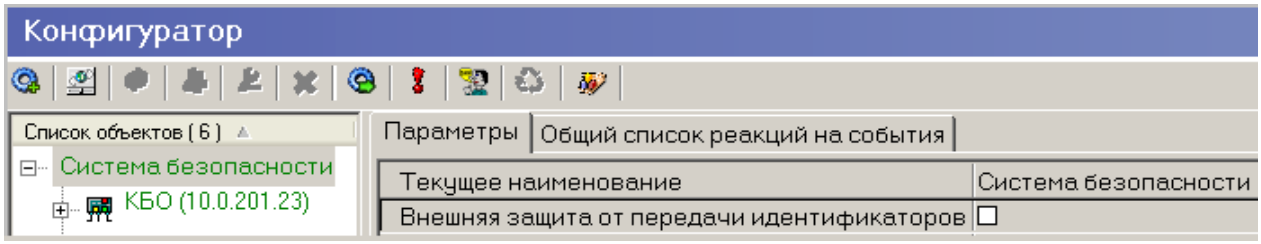
Контроллеры системы PERCo-S-20 поддерживают режим защиты от передачи идентификаторов, т.е. запрет повторного входа без предварительного выхода.

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

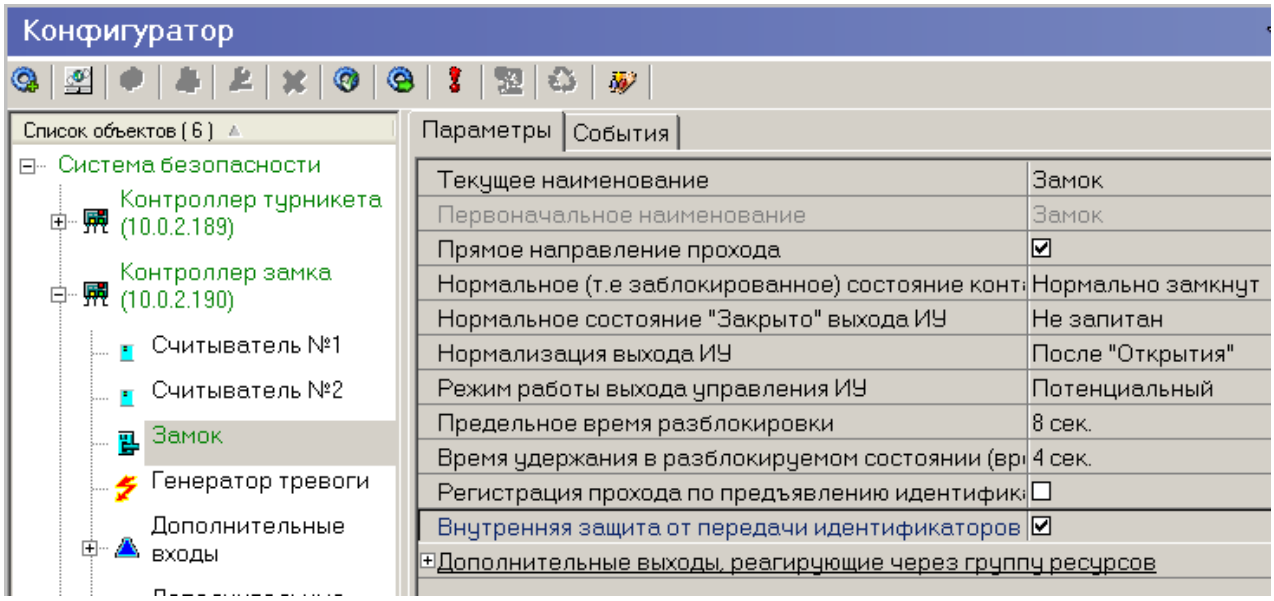
1. Происходит широковещательная рассылка контроллерам своей подсети.
2. Выбирается первый контроллер другой подсети, и ему передаются данные. В случае невозможности передачи ему, выбирается следующий контроллер этой подсети и т.д. Затем эта же процедура проводится и с другими подсетями.
3. Контроллер в другой подсети, получив данные, распространяет их широковещательно по всем контроллерам своей подсети.
4. В результате этих действий контроллеров каждый контроллер знает, на каком из уровней доступа (безопасности) находится владелец предъявленной карты.

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

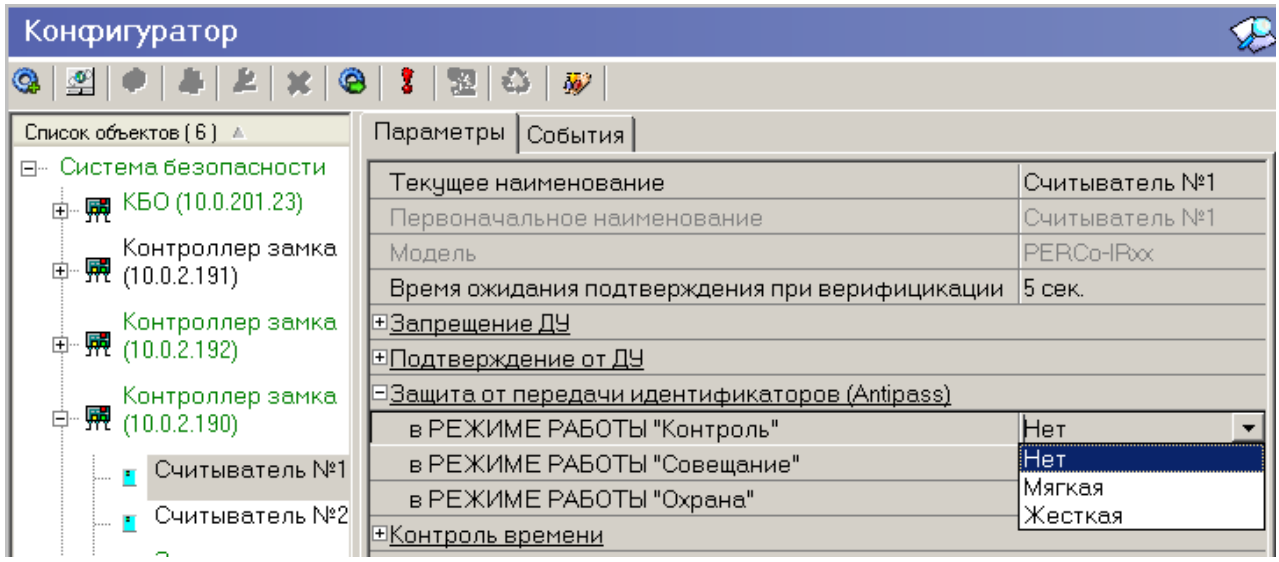
✓ **для системы безопасности в целом:** отметьте флажок Внешняя защита от передачи идентификаторов (Global Antipass) в панели параметров



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

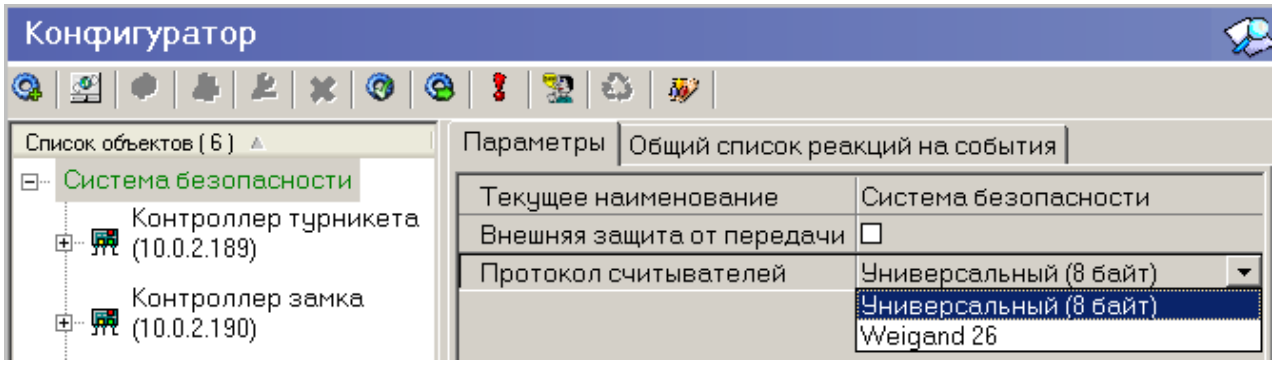


✓ **для отдельного считывателя:** установите у считывателя в параметре Защита от передачи идентификаторов (Antipass) значение Жесткая: для требуемых режимов работы



Протокол работы со считывателями

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



Имеется два значения этого параметра:

✓ **Универсальный (8 байт)** — протокол считывателя, по которому контроллер воспринимает 64 бита кода идентификатора доступа.

✓ **Widgand 26** – протокол считывателя, по которому контроллер воспринимает 26 бит кода идентификатора доступа.

✓ **Сокращенный (4 байта)** - протокол считывателя, по которому контроллер воспринимает 32 бита кода идентификатора доступа.

Описание параметров функционирования контроллеров ППКОП (КБО)

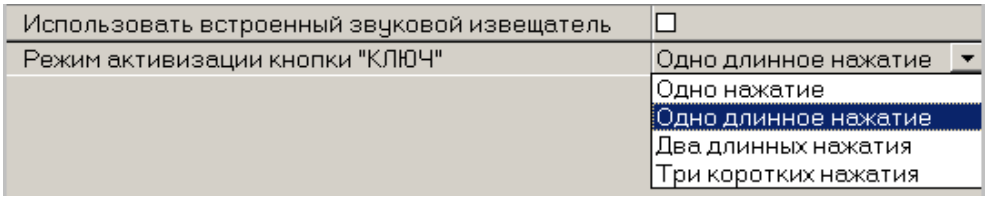
Подробная информация о параметрах функционирования контроллера ППКОП (КБО) системы безопасности PERCo-S-20 приведена в техническом описании системы безопасности.

Контроллер ППКОП (КБО) — предназначен для контроля состояния шлейфов сигнализации (ШС), пожарных или охранных, выдачи тревожных сообщений на пост центрального наблюдения (ПЦН), световое оповещение (СО) и звуковое оповещение (ЗО), управления дополнительным оборудованием, сохранению событий, произошедших в системе, в энергонезависимой памяти и передаче их ПО. Дополнительно панель КБО обеспечивает управление одним электромагнитным или электромеханическим замком и имеет энергонезависимую память на 200 карт доступа и 8000 событий.

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

Контроллер

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



1. **Использовать встроенный звуковой извещатель** — параметр, управляющий

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

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

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

Дополнительный выход

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

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

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

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

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

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

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

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

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

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

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

для ППКОП:

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

для КБО:

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

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

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

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

- ✓ **Включить при пожаре.** В случае перехода одной из зон в режим «ПОЖАР» произойдет замыкание контакта дополнительного выхода.
- ✓ **Мигать при пожаре.** В случае перехода одной из зон в режим «ПОЖАР» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Включить при внимании и пожаре.** В случае перехода одной из зон в режим «ВНИМАНИЕ» или «ПОЖАР» произойдет замыкание контакта дополнительного выхода.
- ✓ **Мигать при внимании и пожаре.** В случае перехода одной из зон в режим «ВНИМАНИЕ» или «ПОЖАР» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Включить при тревоге.** В случае перехода одной из зон в режим «ТРЕВОГА» произойдет замыкание контакта дополнительного выхода.
- ✓ **Мигать при тревоге.** В случае перехода одной из зон в режим «ТРЕВОГА» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Лампа 1** – программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы все зоны изменили свой режим.
- ✓ **Лампа 2** – программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы хотя бы одна из зон изменила свой режим.
- ✓ **ПЦН 1** – программа управления, указывающая на то, что дополнительный

выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы все зоны изменили свой режим.

✓ **ПЦН 2** – программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы все зоны изменили свой режим.

✓ **Сирена** – программа управления, указывающая на то, что к дополнительному выходу подключен звуковой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы хотя бы одна из зон изменила свой режим.

✓ **Включить перед взятием** – Перед переходом одной из зон в режим «ВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.

✓ **Включить при взятии** — При переходе одной из зон в режим «ВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.

✓ **Включить при снятии** – Перед переходом одной из зон в режим «СНЯТА» произойдет замыкание контакта дополнительного выхода.

✓ **Включить при автоперевзятии** – При переходе одной из охранных зон в режим «АВТОПЕРЕВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.

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

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

Шлейф сигнализации

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

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

1. Тип шлейфа сигнализации — Охранный

Текущее наименование	Шлейф сигнализации №1
Адрес	1
Первоначальное наименование	Шлейф сигнализации №1
⊟Тип	Охранный
⊟Охранный	
Контроль вскрытия корпуса 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

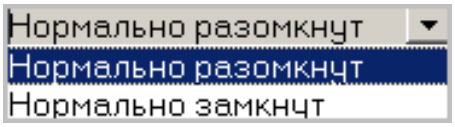
✓ **Задержка взятия на охрану** — параметр, определяющий для шлейфа время, через которое панель предпринимает попытку взять шлейф на охрану после поступления соответствующей команды.

✓ **Задержка восстановления нарушенного шлейфа в снятом состоянии** — если данный параметр установлена в 0, то шлейф в состоянии «СНЯТ» не контролируется. В противном случае продолжается отслеживание шлейфа в режиме «Снят». Если при этом шлейф перейдет в состояние «НАРУШЕНИЕ», то в журнал регистраций записывается событие «Неисправность снятого 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 регистраций будет записано сообщение «Нормализация снятого ОШС». Состояние выходов и встроенная звуковая индикация панели не изменяются.

2. Тип шлейфа сигнализации — **Пожарный**

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

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



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

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

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

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

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

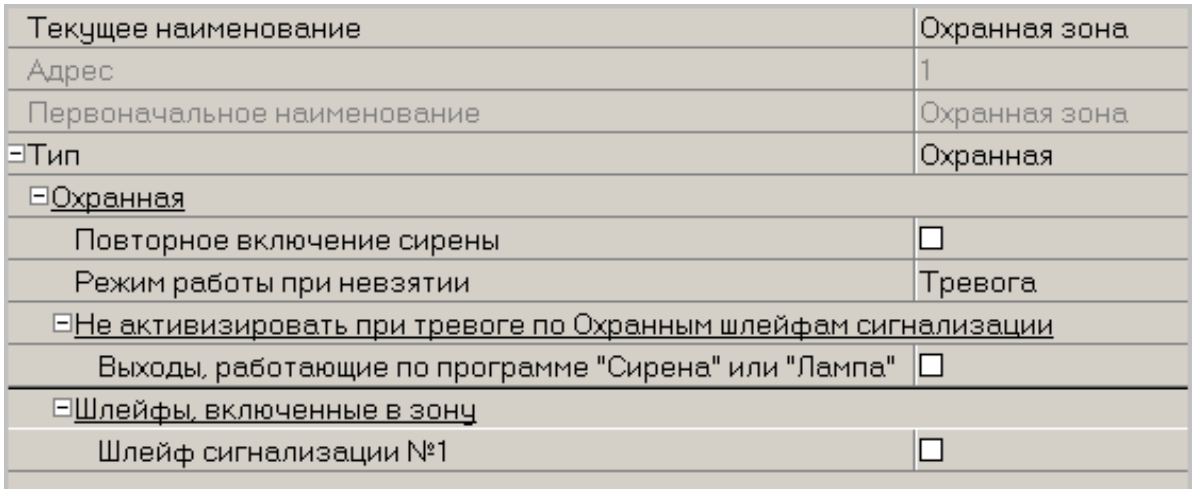
✓ **Длительность нарушения** - параметр, определяющий для шлейфа время интегрирования

Зоны сигнализации

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

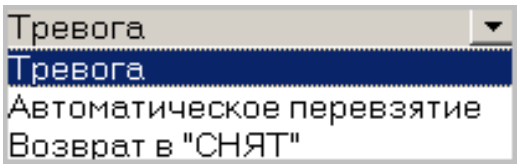
В зависимости от алгоритма работы шлейфов сигнализации существуют следующие варианты описания параметров работы зоны:

1. Тип зоны сигнализации — Охранная



✓ **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 производится повторная попытка взятия до тех пор, пока взятие не произойдет.
- **Возврат в режим снят** — зона перейдет в режим «СНЯТА».

✓ **Не активизировать при тревоге по охранным шлейфам сигнализации дополнительные выходы, работающие по программе «Сирена» или «Лампа»** - параметр указывает, должна ли панель в случае тревоги в данной зоне запрещать активизацию дополнительных выходов, работающие по программе управления «Сирена» или «Лампа».

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

2. Тип зоны сигнализации - **Пожарная**

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

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

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

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

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

3. Тип зоны сигнализации — **КТС**

Текущее наименование	Зона №3
Адрес	3
Первоначальное наименование	Зона №3
⊟Тип	КТС
⊟КТС	
⊟Шлейфы, активизирующие зону	
Шлейф сигнализации №3	☑

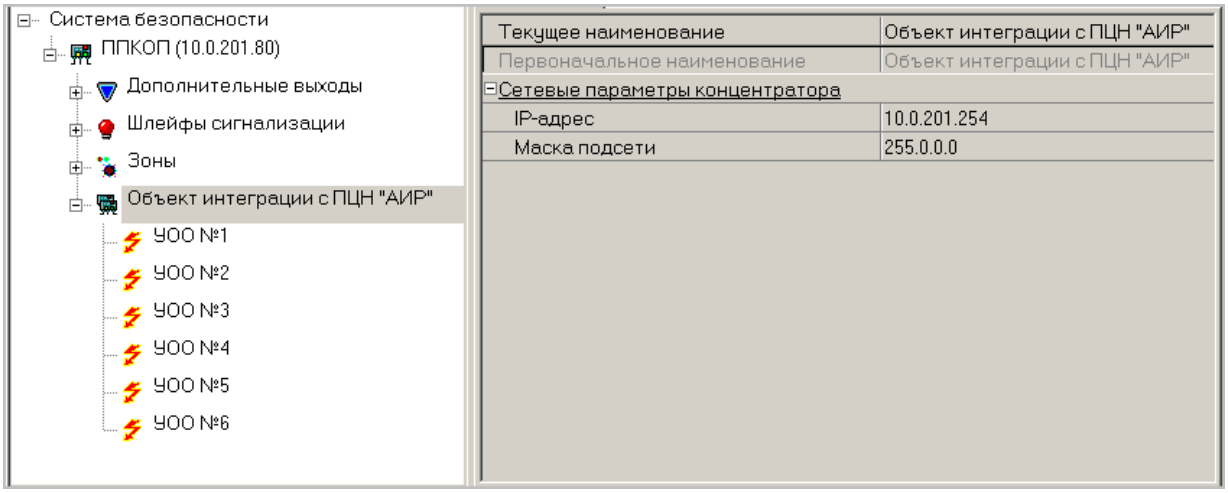
✓ Шлейфы, активизирующие зону **- список шлейфов КТС, контролируемых в данной зоне.**

Интеграция ППКОП с ПЦН «АИР»

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

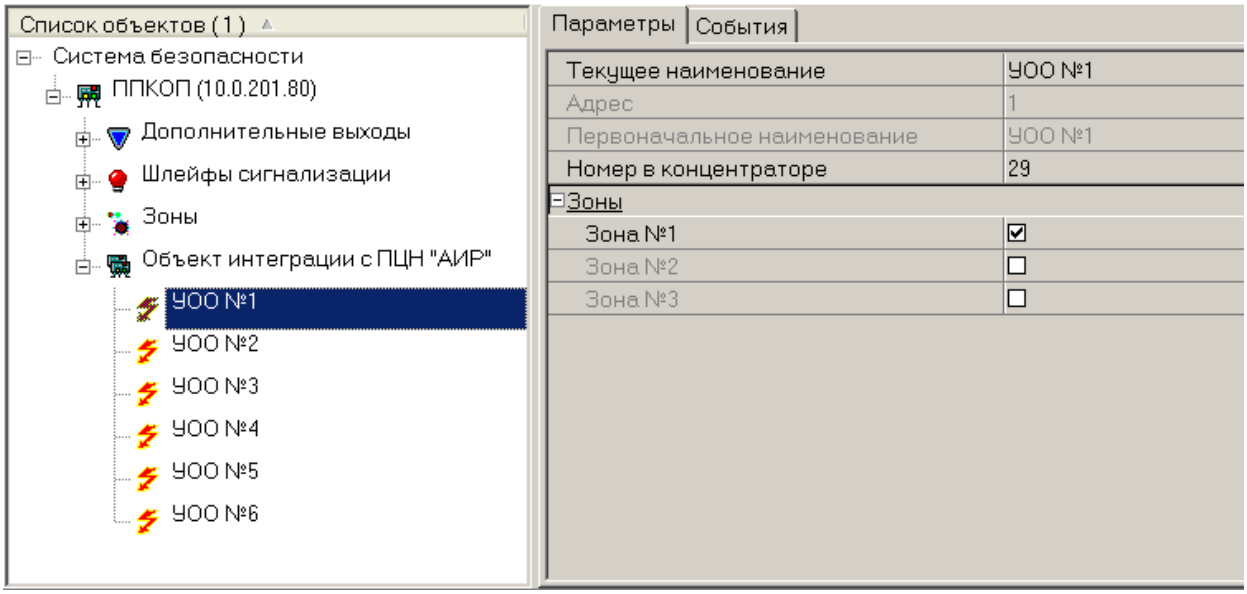
Для включения интеграции следует задействовать параметр «Включить интеграцию с ПЦН «АИР» на контроллере ППКОП.

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 охраняемые зоны.

Задание реакции на события

Единая система безопасности PERCo-S-20 позволяет автоматизировать реакцию на происходящие события в системе. Кроме возможности указания перекрестных ссылок (активизация выхода при срабатывании тестового входа, возможность активизации релейного выхода при разблокировке ИУ и т.д.) в рамках параметров функционирования контроллера система безопасности позволяет задать алгоритмы, сценарии работы системы на уровне программного обеспечения. То есть программное обеспечение позволяет связать в единую систему взаимодействие между разными устройствами. Например, при срабатывании охранного шлейфа на одном контроллере заблокировать все двери на пути возможного отхода, включить запись с камер видеонаблюдения, установленных в этом помещении, открыть все исполнительные устройства в случае возникновения пожара и так далее.

При задании реакций на события нужно не забывать о том, что заданные действия будут выполняться только при условии работающего программного обеспечения системы, а именно сервера системы. Это обусловлено механизмом обработки этих параметров.

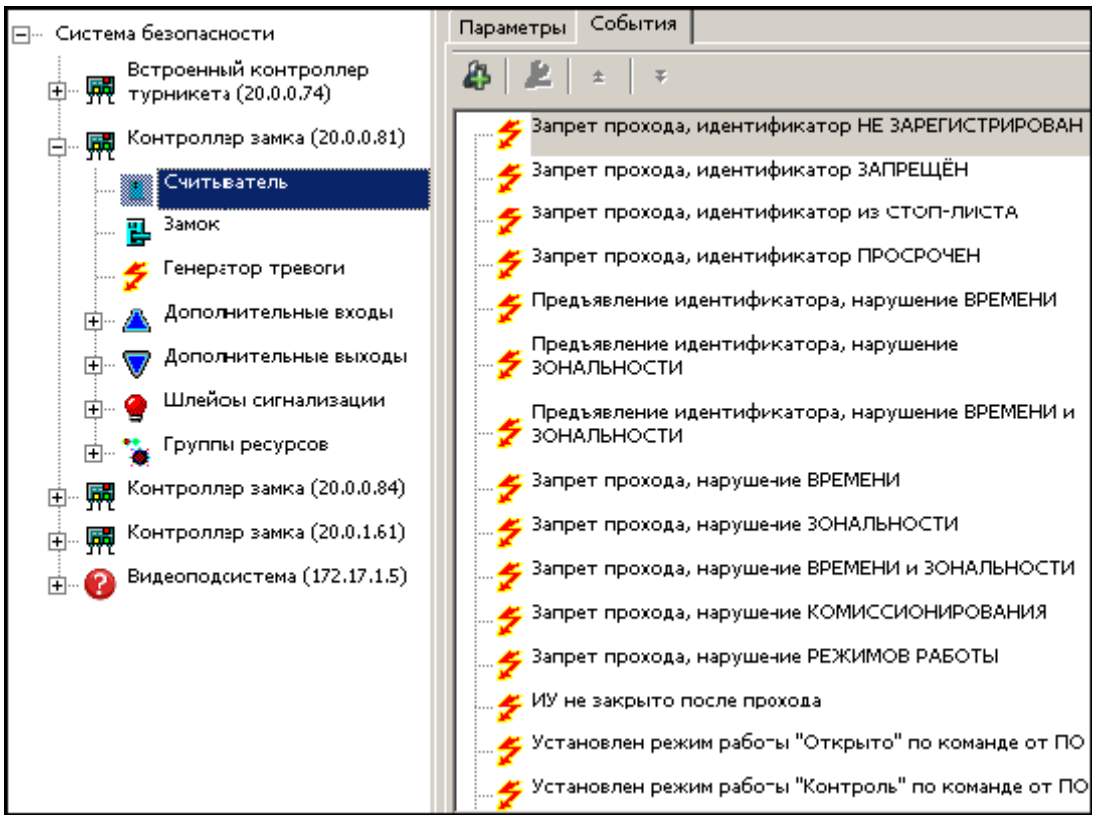
Для задания реакций на события устройства необходимо выбрать это устройство в главном окне раздела **Конфигуратор** и открыть вкладку **События**. На вкладке перечисляется список всех событий, которые могут быть зарегистрированы на выбранном устройстве, с возможностью задания для каждого события реакции на него. Более подробная информация о действиях по заданию реакции на события приведена в Руководстве пользователя в разделе К**онфигуратор**.

Рассмотрим на примере:

Необходимо известить охранника на проходной о факте предъявления карты доступа включенной в СТОП-лист и сделать видеозапись человека, предъявившего эту карту.

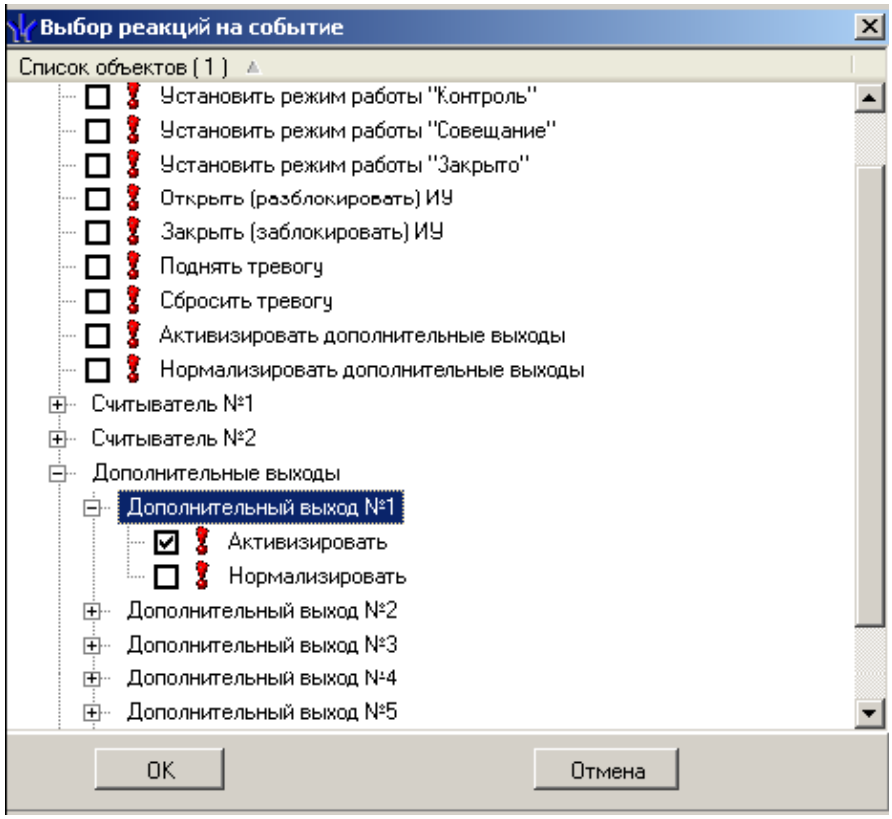
Для этого необходимо подключить к релейному выходу контроллера, расположенного наиболее близко к охраннику, световой оповещатель и установить его в помещении, где находится охранник. Его задача информировать охранника о случае поднесения карты доступа включенной в СТОП-лист. Для осуществления видеозаписи необходимо установить видеокамеру, направленную на место предъявления карты и подключить ее к системе. (Для подключения видеокамер к системе безопасности PERCo-S-20 необходимо приобрести модуль **Видеонаблюдение**).

Далее необходимо выбрать считыватель, на который возможно поднесение карты включенной в СТОП-лист, в главном окне раздела **Конфигуратор**, открыть вкладку **События** и выбрать событие «Запрет прохода, идентификатор из СТОП-листа»:



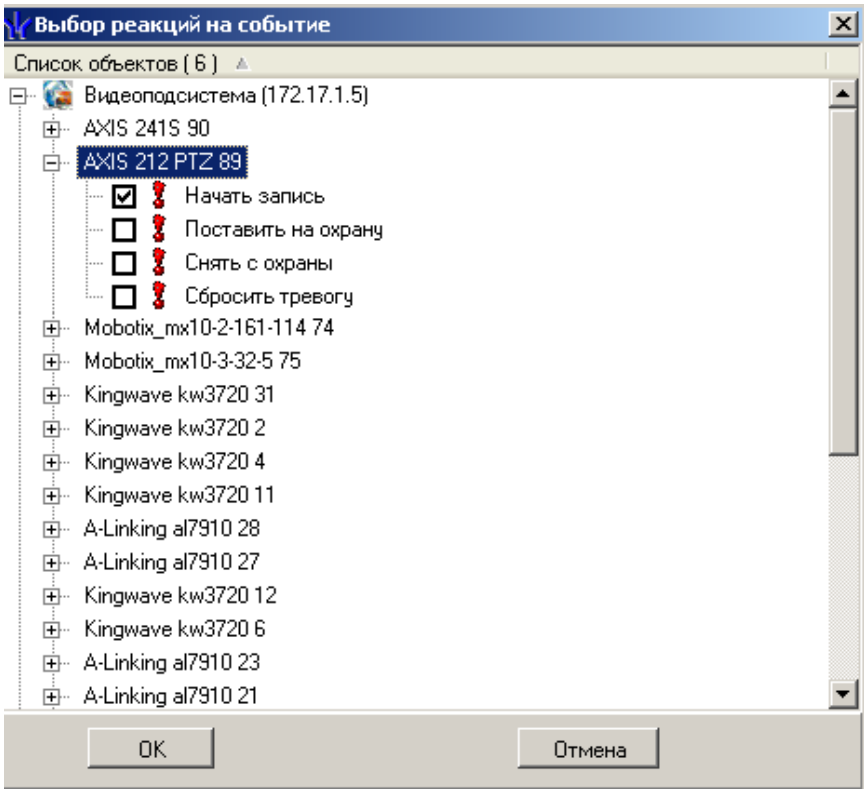
Далее нажать на кнопку **Добавить реакцию на событие** —  .

В появившемся диалоговом окне выбрать релейный выход, к которому подключен оповещатель, и щелкнуть по кнопке «**ОК**».



Этими действиями вы уже указали, что при предъявлении идентификатора, добавленного в СТОП-лист, необходимо активизировать оповещатель.

Далее необходимо в дереве объектов выбрать **Видеоподсистема** и камеру, которая установлена в месте предъявления карты доступа, и отметить команду **Начать запись**:



Нажав на кнопку «**ОК**», вы сохраните эти данные. Теперь необходимо сохранить все внесенные изменения и передать измененные параметры в аппаратуру.

Аналогичным образом при помощи описанного механизма задания реакций системы на происходящие события вы можете создать любые комбинации действий и ответных действий необходимые вам для корректной работы системы безопасности на вашем предприятии.

ПРИМЕЧАНИЕ

Так как заданные алгоритмы работы выполняются автоматически, будьте очень внимательны! Не создавайте циклических ссылок! Остановить выполнение алгоритма можно будет только внесением изменений в конфигурацию системы и повторной передачей параметров!

Описание параметров системы пожарной сигнализации

Подробная информация о параметрах функционирования контроллеров системы пожарной сигнализации PERCo-S-20-PF приведена в техническом описании системы пожарной сигнализации и в текущем разделе данного руководства.

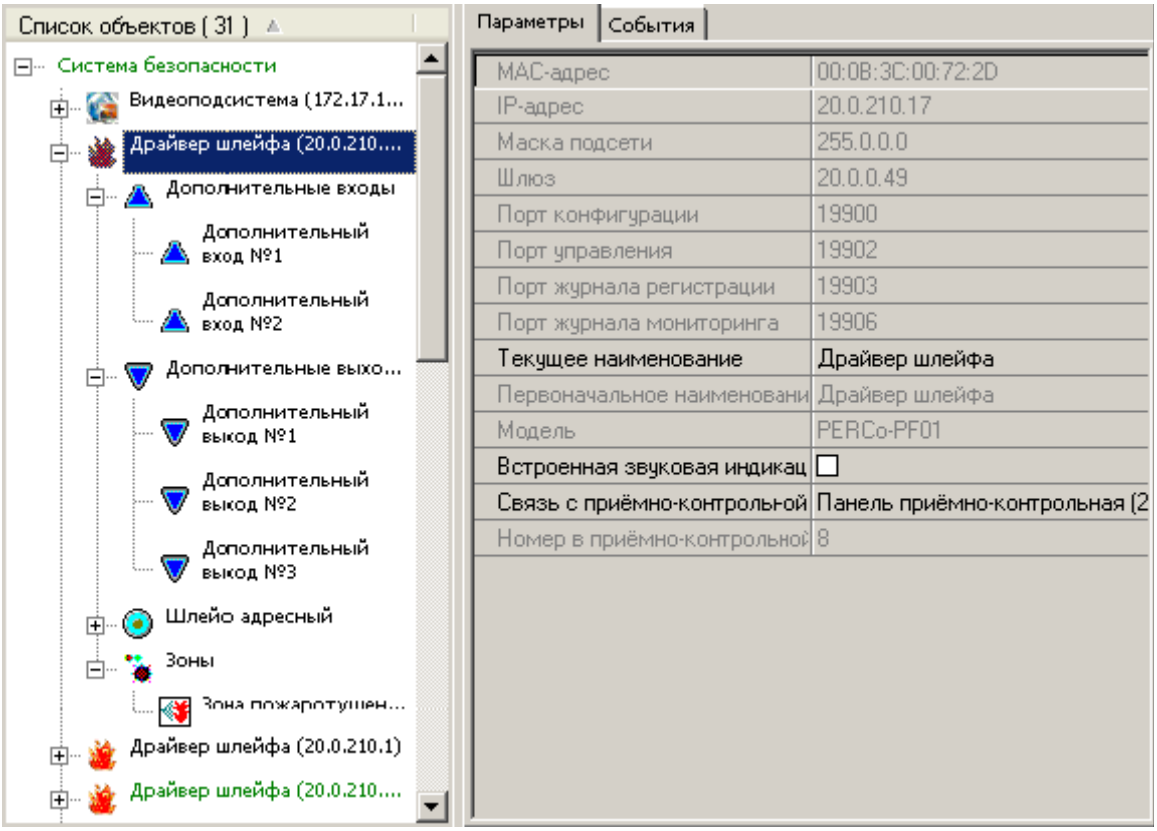
Ниже будут приведены общие рекомендации, проиллюстрированные примерами задания тех или иных параметров контроллеров.

Драйвер шлейфа PERCo-PF01

Драйвер шлейфа предназначен для подключения к нему одного адресного шлейфа пожарных извещателей серии XP95 производства компании Apollo Fire Detect. Список поддерживаемых извещателей приведен в техническом описании на систему пожарной сигнализации.

Кроме этого драйвер шлейфа имеет два дополнительных входа, предназначенных для подключения дополнительного оборудования и трех релейных выходов, которые могут быть использованы для подключения тревожных оповещателей.

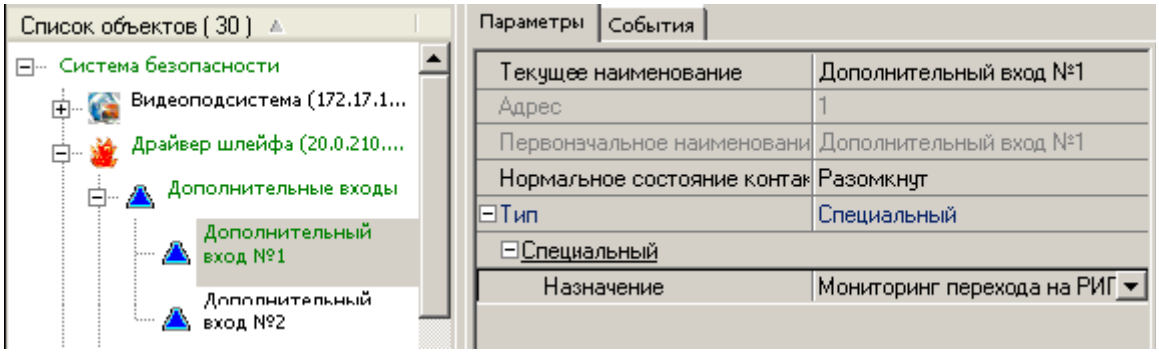
Каждый драйвер поддерживает до 31 зоны пожарной сигнализации с возможностью группировки адресных пожарных извещателей по этим зонам. При этом драйвер шлейфа поддерживает одну зону УПА (устройство пожарной автоматики) – зону, для которой могут быть заданы параметры автоматической передачи сигнала на пуск УПА. Более подробная информация о технических параметрах приведена в техническом описании на систему пожарной сигнализации.



Ниже будет приведено описание параметров функционирования устройств, входящих в состав драйвера шлейфа.

Дополнительные входы

Драйвер шлейфа в своем составе имеет два дополнительных входа, которые могут быть использованы для подключения дополнительного оборудования, влияющего на работу системы пожарной сигнализации.



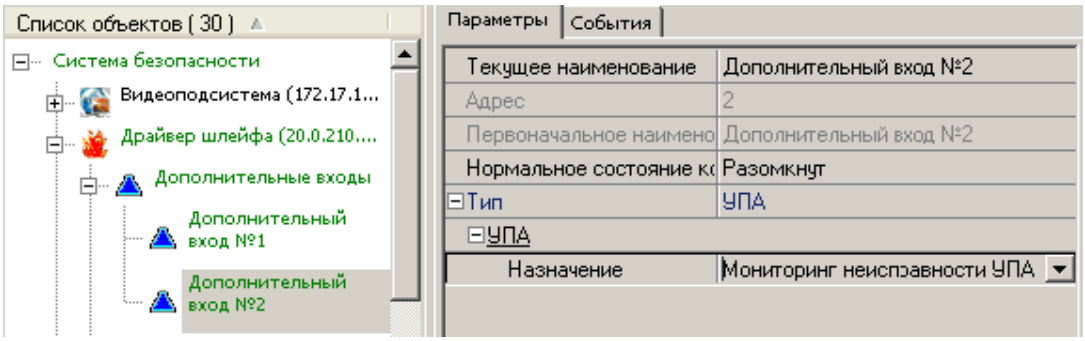
Дополнительный вход №1 зарезервирован для подключения информационной линии от резервного источника питания, сигнализирующей о переходе питания на резервный источник, то есть на питание от аккумуляторов.

При описании параметров функционирования данного входа необходимо указать нормальное состояние контакта. Состояние может быть двух типов:

- **Разомкнут**. В этом случае при нормальной работе источника питания цепь сигнальной линии должна быть разомкнута.
- **Замкнут**. В этом случае при нормальной работе источника питания цепь сигнальной линии должна быть замкнута.

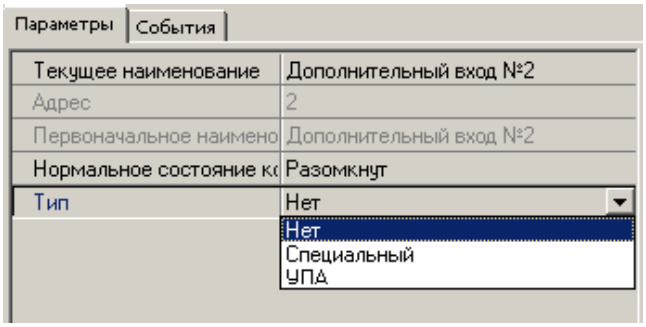
Перед выбором параметров функционирования дополнительного входа №1 внимательно ознакомьтесь с техническим описанием используемого источника питания.

Дополнительный вход №2 – дополнительный вход, который может быть использован для подключения дополнительного оборудования, влияющего на работу системы пожарной сигнализации, в зависимости от типа подключаемого оборудования необходимо задать параметры его функционирования:



- **Нормальное состояние контакта.** Параметр описывает состояние линии в нормальном состоянии и зависит от типа подключенного оборудования и особенностей его функционирования.

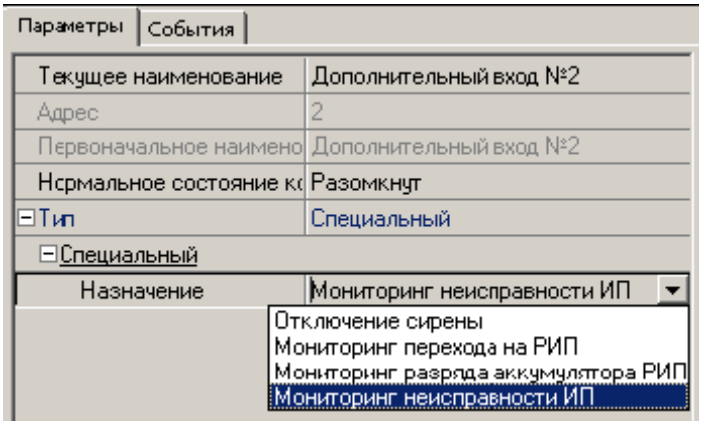
Параметр «**Тип**» позволяет указать, для каких целей будет использоваться информация, получаемая от подключенного к данному входу оборудования:



В зависимости от выбора параметра «**Тип**» становятся доступными дополнительные параметры функционирования дополнительного входа. При выборе значения параметра «**Тип**» равным «Нет» дополнительные параметры не задаются, этот вход не используется в системе пожарной сигнализации.

Допустимые значения параметра «**Тип**»:

- **Специальный.** Означает, что оборудование, подключенное к данному входу, используется для мониторинга состояния подключенного оборудования и в качестве управляющего оборудования:



Доступны следующие варианты назначения параметра **«Назначение»** дополнительного входа:

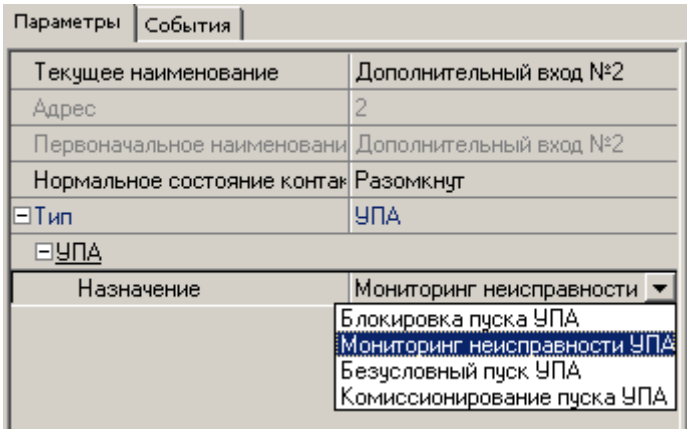
✓ **Отключение сирены.** Срабатывание оборудования, подключенного к данному входу, будет приводить к отключению сирены, вне зависимости от причины ее включения.

✓ **Мониторинг перехода на РИП (резервный источник питания).** Означает, что к данному входу подключено оборудование, сигнализирующее о том, что источник питания перешел на работу от аккумуляторов.

✓ **Мониторинг разряда аккумулятора РИП.** Означает, что к данному входу подключено оборудование, сигнализирующее о том, что аккумуляторы резервного источника питания разряжены.

✓ **Мониторинг неисправности ИП.** Означает, что к данному входу подключено оборудование, сигнализирующее о неисправности источника питания.

- **УПА** – означает, что оборудование, подключенное к данному входу, используется для мониторинга состояния УПА.



Доступны следующие варианты назначения параметра «Действие» дополнительного входа:

✓ **Блокировка пуска УПА (устройство пожарной автоматики)** – указывает драйверу шлейфа на то, что к дополнительному входу подключено оборудование, дающее команду на блокирование пуска УПА. Например, это может быть специальная кнопка, используемая для блокировки пуска газового УПА при условии нахождения людей в зоне.

✓ **Мониторинг неисправности УПА** – указывает драйверу АСПС на то, что к данному входу подключено дополнительное оборудование, информирующее о неисправности устройства пожарной автоматики. При поступлении сигнала драйвер системы сообщает в программное обеспечение и панель приемно-контрольную о неисправности УПА и невозможности его пуска в случае возникновения пожара.

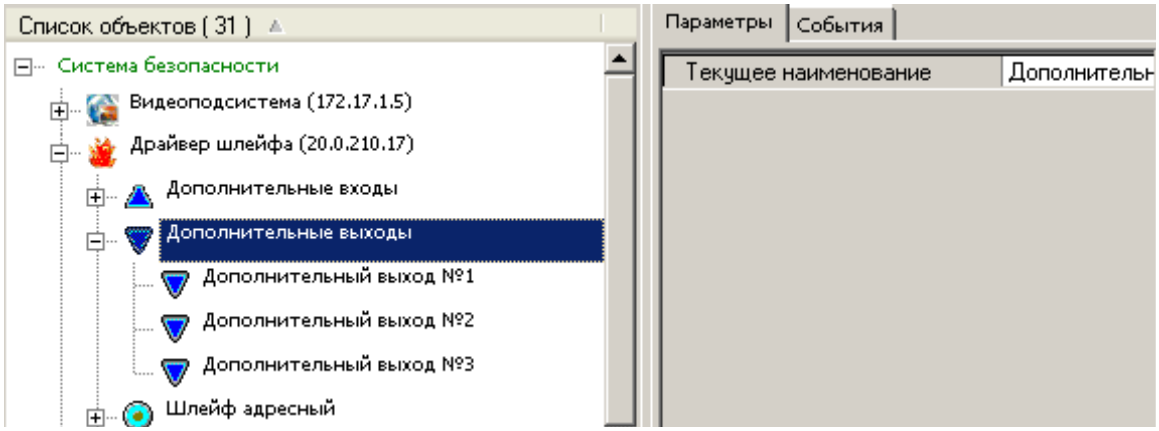
✓ **Безусловный пуск УПА** – указывает драйверу шлейфа на то, что к данному входу подключено дополнительное оборудование (кнопка), срабатывание которого (нажатие) приводит к безусловной подаче сигнала на пуск системы УПА.

✓ **Комиссионирование пуска УПА** – указывает драйверу шлейфа на то,

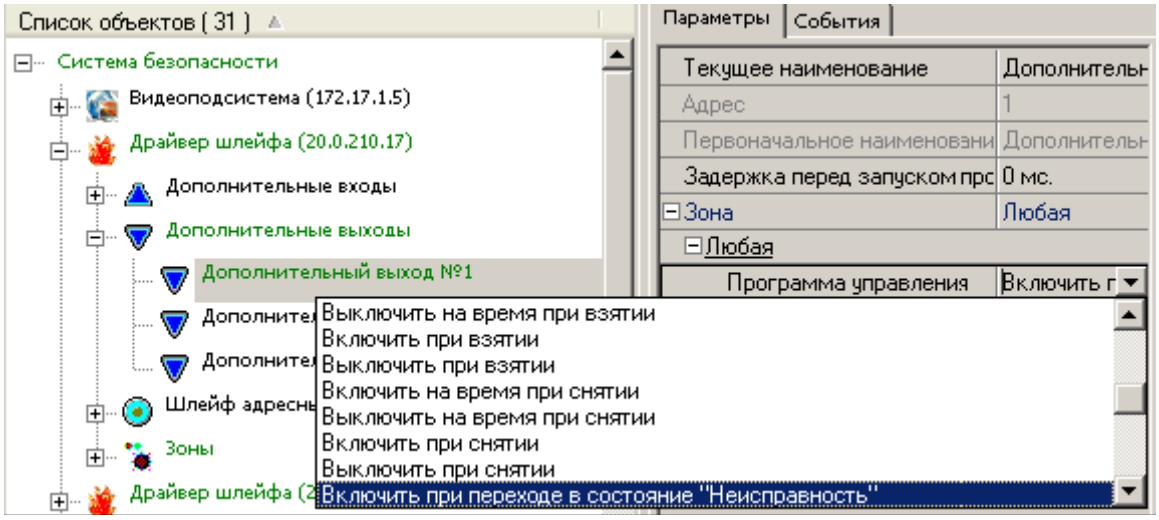
что к данному входу подключено дополнительное оборудование (кнопка), подтверждающая пуск УПА. Другими словами, при условии возникновения пожара и выполнения всех необходимых условий для автоматического пуска УПА, пуск будет произведен, только после нажатия этой кнопки, в противном случае пуска не будет.

Дополнительные выходы

Драйвер шлейфа в своем составе имеет три дополнительных выхода, предназначенных для управления дополнительным оборудованием и передачи оповещений на Центральный пост охраны наблюдения:



В зависимости от структуры системы устройства подключенного к описываемому релейному выходу и его алгоритма работы существуют следующие варианты описания параметров работы релейных выходов:



- **Задержка перед запуском программы управления.** Временной параметр, устанавливающий таймаут между событием, реакцией на которое должна стать активизация дополнительного выхода, и самой активизацией.

- **Зона.** Параметр, определяющий использование данного выхода и его логическую привязку к той или иной зоне сигнализации или УПА. Возможны следующие варианты:

  ✓ **Нет** – данный выход не используется, к нему не подключено дополнительное оборудование.

  ✓ **Любая** – данный вход будет выполнять заданную программу при

возникновении события приводящего к ее активации в любой из зон сигнализации или зоне пожаротушения.

✓ **Сигнализации** – данный выход будет выполнять заданную программу при возникновении события приводящего к ее активации в выбранной зоне сигнализации.

✓ **УПА** - данный вход будет выполнять заданную программу при возникновении события приводящего к ее активации в зоне УПА.

- **Программа управления.** Параметр, определяющий какую из встроенных программ управления должен выполнить контроллер. Возможны следующие варианты программ:

- Для зон **Любая и Сигнализации** возможны следующие варианты программ:

✓ **Включить при пожаре.** В случае возникновения пожара произойдет замыкание контакта релейного выхода.

✓ **Выключить при пожаре.** В случае возникновения пожара произойдет размыкание контакта релейного выхода.

✓ **Включить на время при пожаре.** В случае возникновения пожара произойдет замыкание контакта релейного выхода на время, указанное в параметре «Время активизации».

✓ **Выключить на время при пожаре.** В случае возникновения пожара произойдет размыкание контакта релейного выхода на время, указанное в параметре «Время активизации».

✓ **Мигать из состояния выключено при пожаре.** В этом случае, в ситуации отсутствия пожара, контакты релейного выхода разомкнуты. В случае возникновения пожара произойдет попеременное замыкание - размыкание контактов релейного выхода.

✓ **Мигать из состояния включено при пожаре**. В этом случае в ситуации отсутствия пожара контакты релейного выхода замкнуты. В случае возникновения пожара произойдет попеременное размыкание - замыкание контактов релейного выхода.

✓ **Мигать на время из состояния выключено при пожаре.** В этом случае в ситуации отсутствия пожара контакты релейного выхода разомкнуты. В случае возникновения пожара произойдет попеременное замыкание-размыкание контактов релейного выхода на время, указанное в параметре «Время активизации».

✓ **Мигать на время из состояния включено при пожаре.** В этом случае в ситуации отсутствия пожара контакты релейного выхода замкнуты. В случае возникновения пожара произойдет попеременное размыкание-замыкание контактов релейного выхода на время, указанное в параметре «Время активизации».

✓ **Лампа –** программа управления, указывающая на то, что к данному релейному выходу подключен световой оповещатель пожара.

✓ **ПЦН –** программа управления, указывающая на то, что данный релейный выход используется для передачи извещения о пожаре на пост центрального наблюдения (ПЦН).

✓ **ПЦН (старая тактика) –** программа управления, указывающая на то, что данный релейный выход используется для передачи извещения о пожаре на пост центрального наблюдения (ПЦН) по старой тактике передачи тревожного оповещения.

✓ **Сирена –** программа управления, указывающая на то, что к данному релейному выходу подключен звуковой оповещатель пожара.

✓ **Включить на время при взятии** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода на время указанное в параметре «Время активизации», после взятия шлейфа пожарной сигнализации на дежурство.

✓ **Выключить на время при взятии** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода на время указанное в параметре «Время активизации», после взятия шлейфа пожарной сигнализации на дежурство.

✓ **Включить при взятии** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода после взятия шлейфа пожарной сигнализации на дежурство.

✓ **Выключить при взятии** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода после взятия шлейфа пожарной сигнализации на дежурство.

✓ **Включить на время при снятии** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода на время, указанное в параметре «Время активизации», после снятия шлейфа пожарной сигнализации с дежурства.

✓ **Выключить на время при снятии** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода на время, указанное в параметре «Время активизации», после снятия шлейфа пожарной сигнализации с дежурства.

✓ **Включить при снятии** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода после снятия шлейфа пожарной сигнализации с дежурства.

✓ **Выключить при снятии** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода после снятия шлейфа пожарной сигнализации с дежурства.

✓ **Включить при переходе в состояние «Неисправность»** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода в случае обнаружения неисправности в шлейфе пожарной сигнализации.

✓ **Выключить при переходе в состояние «Неисправность»** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода в случае обнаружения неисправности в шлейфе пожарной сигнализации.

✓ **Включить на время при переходе в состояние «Неисправность»** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода на время, указанное в параметре «Время активизации», в случае обнаружения неисправности в шлейфе пожарной сигнализации.

✓ **Выключить на время при переходе в состояние «Неисправность»** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода на время, указанное в параметре «Время активизации», в случае обнаружения неисправности в шлейфе пожарной сигнализации.

✓ **Мигать при переходе в состояние «Неисправность» из состояния выключено**. В этом случае в ситуации отсутствия неисправности в шлейфе пожарной сигнализации контакты релейного выхода разомкнуты. В случае возникновения неисправности произойдет попеременное замыкание – размыкание контактов дополнительного выхода.

✓ **Мигать из состояния включено при неисправности**. В этом случае в ситуации отсутствия неисправности в шлейфе пожарной сигнализации контакты релейного выхода замкнуты. В случае возникновения неисправности произойдет попеременное размыкание – замыкание контактов дополнительного выхода.

✓ **Мигать на время из состояния выключено при неисправности**. В этом случае в ситуации отсутствия неисправности в шлейфе пожарной сигнализации контакты релейного выхода разомкнуты. В случае возникновения неисправности произойдет попеременное замыкание – размыкание контактов дополнительного выхода в течение времени, указанного в параметре «Время активизации».

✓ **Мигать на время из состояния включено при неисправности**. В этом случае в ситуации отсутствия неисправности в шлейфе пожарной сигнализации контакты релейного выхода замкнуты. В случае возникновения неисправности произойдет попеременное размыкание – замыкание контактов дополнительного выхода в течение времени, указанного в параметре «Время активизации».

✓ **Включить при внимании** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода в случае возникновения ситуации «Внимание».

✓ **Выключить при внимании -** программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время в случае возникновения ситуации «Внимание».

✓ **Включить на время при внимании** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре «Время активизации», в случае возникновения ситуации «Внимание».

✓ **Выключить на время при внимании** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре «Время активизации», в случае возникновения ситуации «Внимание».

✓ **Мигать из состояния выключено при внимании**. В этом случае в ситуации отсутствия состояния «Внимание» в шлейфе пожарной сигнализации контакты релейного выхода разомкнуты. В случае возникновения ситуации «Внимание» произойдет попеременное замыкание – размыкание контактов дополнительного выхода.

✓ **Мигать из состояния включено при внимании**. В этом случае в ситуации отсутствия состояния «Внимание» в шлейфе пожарной сигнализации контакты релейного выхода замкнуты. В случае возникновения ситуации «Предтревога» произойдет попеременное размыкание – замыкание контактов дополнительного выхода.

✓ **Мигать на время из состояния выключено при внимании**. В этом случае в ситуации отсутствия состояния «Внимание» в шлейфе пожарной сигнализации контакты релейного выхода разомкнуты. В случае возникновения ситуации «Внимание» произойдет попеременное замыкание – размыкание контактов дополнительного выхода в течение времени, указанном в параметре «Время активизации».

✓ **Мигать на время из состояния включено при внимании**. В этом случае в ситуации отсутствия состояния «Предтревога» в шлейфе пожарной сигнализации контакты релейного выхода замкнуты. В случае возникновения ситуации «Внимание» произойдет попеременное размыкание – замыкание контактов дополнительного выхода в течение времени, указанном в параметре «Время активизации».

- Для зоны УПА возможны следующие варианты программ управления:

✓ **Включить при пуске УПА –** программа управления, указывающая на необходимость замкнуть контакты релейного выхода при подаче управляющего сигнала на пуск УПА (устройства пожарной автоматики).

✓ **Выключить при пуске УПА –** программа управления, указывающая на необходимость разомкнуть контакты релейного выхода при подаче управляющего сигнала на пуск УПА (устройства пожарной автоматики).

✓ **Включить на время при пуске УПА –** программа управления, указывающая на необходимость замкнуть контакты релейного выхода на время, указанное в параметре «Время активизации», при подаче управляющего сигнала на пуск УПА.

✓ **Выключить на время при пуске УПА –** программа управления, указывающая на необходимость разомкнуть контакты релейного выхода на время, указанное в параметре «Время активизации», при подаче управляющего сигнала на пуск УПА**.**

✓ **Мигать на время из состояния выключено при пуске УПА -** в этом случае в ситуации до подачи управляющего сигнала на пуск УПА контакты релейного выхода разомкнуты. В случае подачи сигнала на пуск УПА произойдет попеременное замыкание – размыкание контактов дополнительного выхода в течение времени, указанном в параметре «Время активизации».

✓ **Мигать на время из состояния включено при пуске УПА -** в этом случае в ситуации до подачи управляющего сигнала на пуск УПА контакты релейного выхода замкнуты. В случае подачи сигнала на пуск УПА произойдет попеременное размыкание – замыкание контактов дополнительного выхода в течение времени, указанном в параметре «Время активизации».

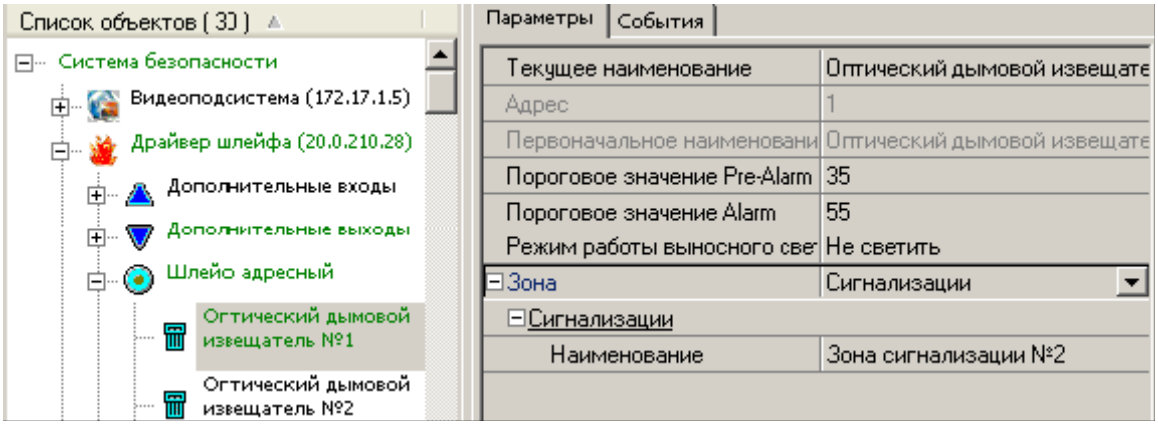
Шлейф адресный

Драйвер шлейфа предназначен для подключения к нему одного адресного шлейфа пожарных извещателей серии XP95 производства компании Apollo Fire Detect. Список поддерживаемых извещателей приведен в техническом описании на систему пожарной сигнализации.

Количество адресных – аналоговых извещателей не может превышать 126 штук в одном шлейфе. Каждый адресный извещатель имеет свой уникальный адрес, который выставляется в нем при помощи специальной перфорированной пластины. При проведении конфигурации драйвера шлейфа, адреса подключенных адресных извещателей соответствуют адресам установленным при помощи перфорированной пластины или джампера.

Для нормального функционирования драйвера шлейфа и всей системы пожарной сигнализации необходимо задать параметры функционирования каждого извещателя. Количество задаваемых параметров и их значения зависят от типа извещателя.

Для большинства извещателей не требуется вносить изменения в его параметры. Изменения вносятся лишь в том случае, если условия эксплуатации отличаются от общепринятых. Более подробная информация о задаваемых параметрах функционирования извещателей приведена в технической документации на них.



Ниже приводится описание параметров функционирования «Оптического дымового извещателя»:

- **Текущее наименование** – мнемоническое имя устройства, при возникновении событий связанных с этим извещателем в качестве его названия будет отображаться введенной значение.

- **Пороговое значение PreAlarm (Предтревога)** – значение, по достижению которого драйвер шлейфа выдаст сообщение о состоянии «Предтревога» на этом извещателе и начнет выполнять внутреннюю программу по обработке данной ситуации.

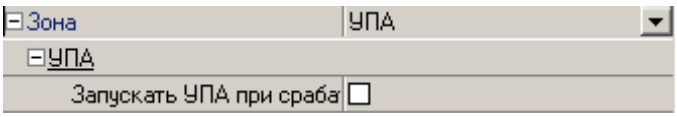
- **Пороговое значение Alarm (Пожар)** – значение, по достижению которого драйвер шлейфа выдаст сообщение о состоянии «Пожар» на этом извещателе и начнет выполнять внутреннюю программу по обработке данной ситуации.

- **Режим работы выносного светодиода** – параметр, определяющий работу светодиода установленного на корпусе извещателя. В зависимости от типа установленной базы извещателя вместо выносного светодиода могут быть установлен сирена или дополнительный выход, для подключения дополнительного оборудования (оповещателей). Таким образом, задавая логику работы второго светодиода

автоматически задается логика работы базы извещателя.

- **Зона** – параметр, позволяющий указать к какой зоне сигнализации относится выбранный извещатель. Возможны следующие варианты:

  ✓ **УПА.** Показания данного извещателя будут использоваться для принятия решения по подаче сигнала на пуск устройства пожарной автоматики. При выборе этого параметра возникает возможность установить дополнительный параметр функционирования выбранного извещателя:



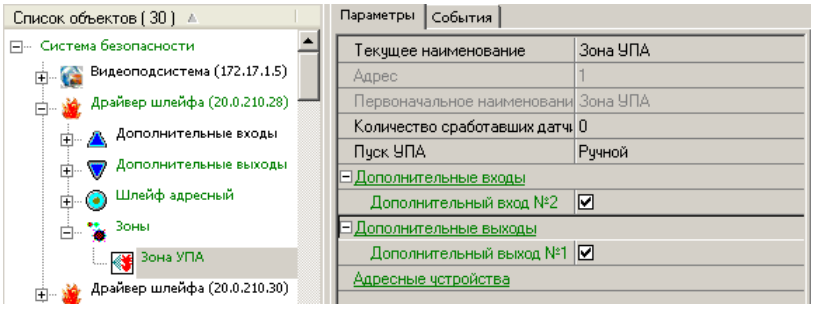
  При отмеченном флажке Запускать УПА при срабатывании**,** в случае получения сигнала «Пожар» с этого извещателя, драйвер шлейфа автоматически начнет выполнять заданный алгоритм передачи сигнала на пуск устройства пожарной автоматики. При этом драйвер шлейфа проигнорирует условие по срабатыванию заданного количества извещателей, необходимых для пуска УПА.

  ✓ **Сигнализации.** Данный извещатель принадлежит к выбранной зоне пожарной сигнализации. Соответственно при его срабатывание драйвер шлейфа передаст информацию на ППК о срабатывании извещателя в зоне сигнализации № X.. При этом на ЖК-дисплее ППК будет отображен номер извещателя и название соответствующей зоны сигнализации.

Зона УПА

Каждый драйвер шлейфа, входящий в единую систему безопасности PERCo-S-20, поддерживает одну зону УПА. Зона УПА – это территория предприятия, на которой установлена система автоматического пожаротушения совместно пожарными извещателями.

Так как не все извещатели, установленные в шлейфе пожарной сигнализации, установлены в этой зоне, укажите в параметрах каждого извещателя, входит ли он в зону УПА.



В параметрах зоны УПА автоматически отображаются извещатели, дополнительные входы и выходы, в параметрах которых указано, что они входят в эту зону.

Основным параметром функционирования зоны УПА является задание количества сработавших датчиков необходимых для пуска УПА. Количество сработавших датчиков не может быть больше общего количества извещателей входящих в зону УПА.

- **Пуск УПА** – параметр, задающий логику пуска. Доступны следующие варианты:

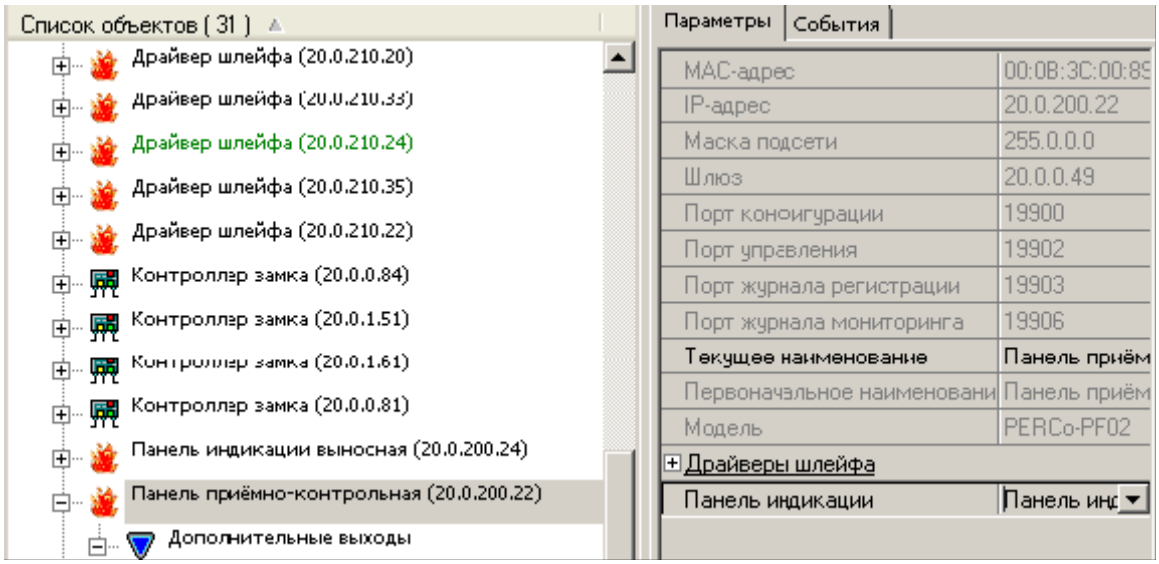
✓**Ручной.** При задании этого параметра драйвер шлейфа передает сообщение на приемно-контрольную панель (ППК), о необходимости пуска устройства пожарной автоматики (УПА), при этом на ППК загорается индикация о необходимости пуска УПА и отображается сообщение на ЖК-дисплее. Для пуска УПА нажмите соответствующую кнопку на ППК.

✓**Автоматический** (с комиссионированием /без комиссионирования). При задании этого параметра драйвер шлейфа автоматически выполняет заданный алгоритм передачи сигнала на пуск УПА.

Панель приемно-контрольная (ППК) PERCo-PF02

Панель приемно-контрольная предназначена для отображения информации о состоянии адресных шлейфов пожарной сигнализации, управления пуском УПА и индикации тревожных ситуаций. ППК поддерживает работу с 32 драйверами шлейфа. Суммарное количество драйверов шлейфа и ППК в системе безопасности не может быть больше 1024.

Основным параметром функционирования ППК является указания списка драйверов шлейфа, информация о состоянии которых будет отображаться на ППК:



Выбор драйвера шлейфа осуществляется из списка. В этом списке присутствуют все драйвера шлейфа включенные в конфигурацию системы безопасности. Каждый драйвер шлейфа может быть выбран только один раз.

ПРИМЕЧАНИЕ

Четыре зоны для управления пуском УПА с консоли ППК, берутся с ДШ №1-№4 (то есть первые четыре из предлагаемого списка на 32 ДШ).

После выбора списка драйверов шлейфа, контролируемых данной панелью, необходимо указать наименование зон пожарной сигнализации для каждого из выбранных драйверов. Вводимые названия (максимальная длина 15 символов) будут отображаться на ЖК-индикаторе панели управления при отображении событий поступающих от драйверов шлейфов.

При наличии в системе второй панели управления, работающей в режиме отображения информации, необходимо выбрать ее из выпадающего списка. Выбранная панель будет дублировать текущую панель управления в рамках отображения информации.

Кроме этого, ППК имеет два дополнительных входа предназначенных для подключения дополнительного оборудования и пять релейных выходов, которые могут быть использованы для подключения тревожных оповещателей.

Ниже приведется описание параметров функционирования ресурсов, входящих в состав ППК.

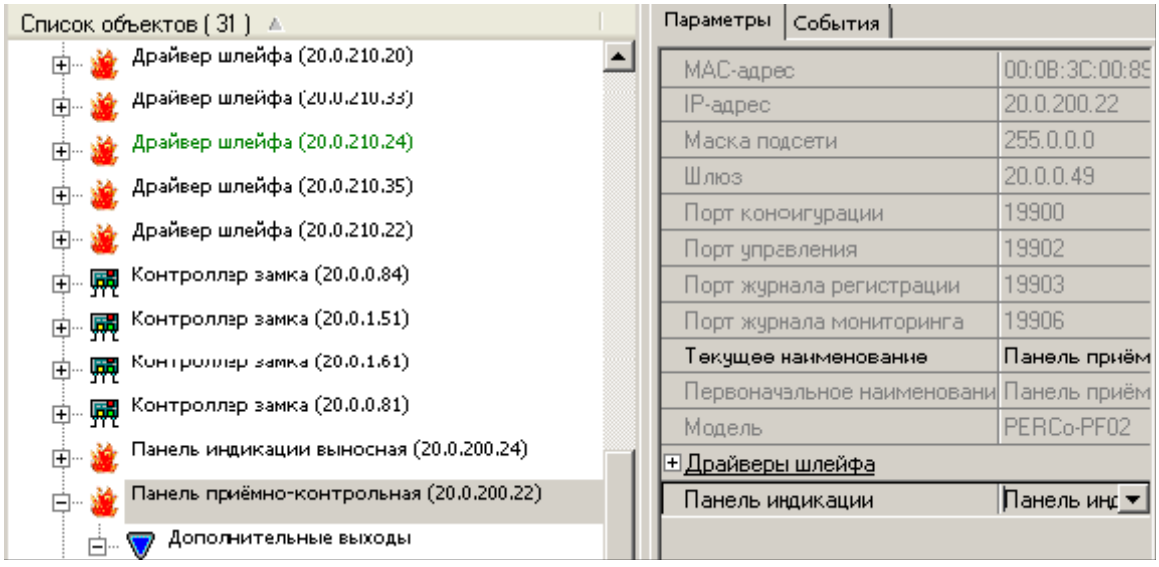
Дополнительные входы

ППК в своем составе имеет два дополнительных входа, которые должны быть использованы для подключения оборудования отвечающего за мониторинг состоянии источника питания панели управления. Информация о назначении входов, правилах подключения дополнительного оборудования находится в технической документации на ППК.

Дополнительные выходы

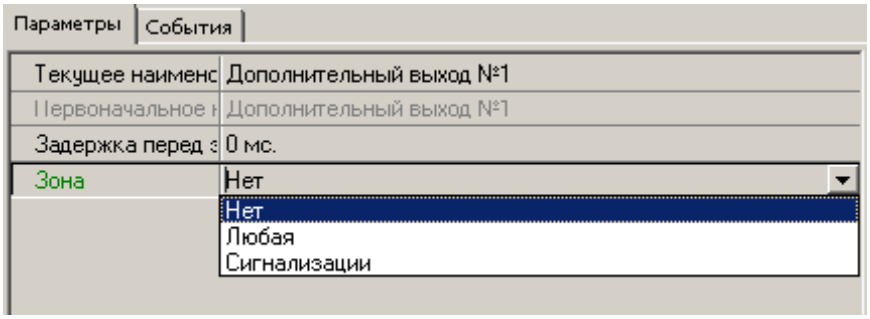
ППК в своем составе имеет пять дополнительных выходов, предназначенных для управления дополнительным оборудованием и передачи оповещений на Центральный пост охраны.

В зависимости от структуры системы, устройства подключенного к описываемому релейному выходу и его алгоритма работы существуют следующие варианты описания параметров работы релейных выходов:



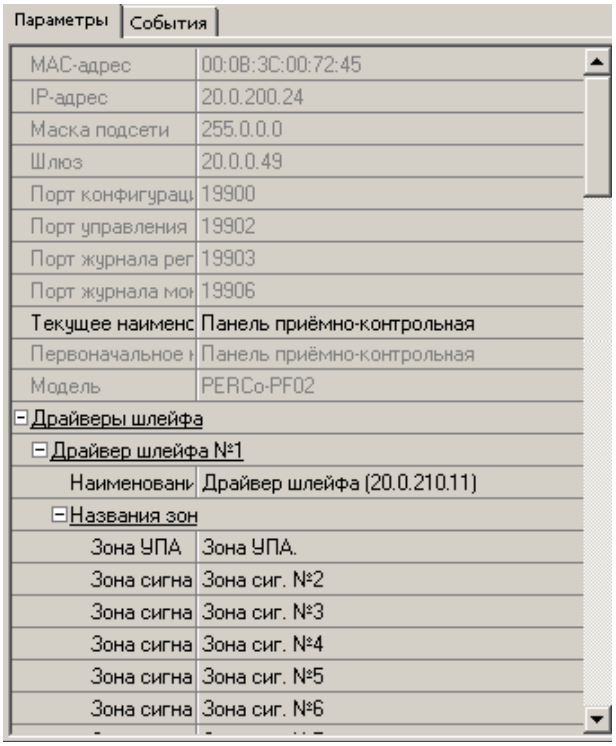
- **Задержка перед запуском программы управления** – временной параметр, устанавливающий таймаут между событием, реакцией на которое должна стать активизация дополнительного выхода и самой активизацией.

- **Зона** – параметр, определяющий зону пожарной сигнализации, по получению события из которой, панель управления шлейфа, выполнит заданную программу управления на выбранном релейном выходе. Возможны следующие варианты параметра:

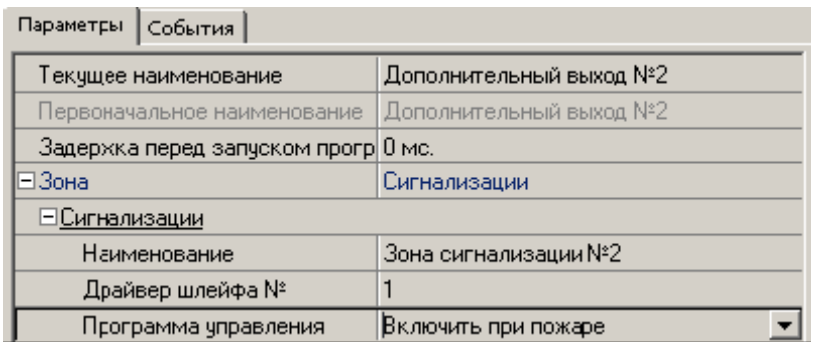


✓**Нет** – данный выход не используется.

✓**Любая** – при задании этого параметр, панель управления выполнит заданную программу управления при получении сообщения из любого из установленных драйверов шлейфов в любой его зоне, кроме зоны УПА.



✓**Сигнализации.** При задании этого параметра, панель управления выполнит заданную программу управления выходом при получении сообщения о пожаре или неисправности от выбранного драйвера шлейфа и выбранной зоны драйвера.



Номер драйвера соответствует порядковому номеру драйвера шлейфа в данной панели управления. Наименование соответствует наименованию зоны сигнализации в выбранном драйвере.

- **Программа управления** – параметр, определяющий какую из встроенных программ управления должен выполнить контроллер. Возможны следующие варианты программ:

  - ✓ **Включить при пожаре.** В случае возникновения пожара произойдет замыкание контакта релейного выхода.
  - ✓ **Выключить при пожаре.** В случае возникновения пожара произойдет размыкание контакта релейного выхода.
  - ✓ **Включить на время при пожаре.** В случае возникновения пожара произойдет замыкание контакта релейного выхода на время, указанное в параметре «Время активизации».
  - ✓ **Выключить на время при пожаре.** В случае возникновения пожара произойдет размыкание контакта релейного выхода на время, указанное в параметре «Время активизации».
  - ✓ **Мигать из состояния выключено при пожаре.** В этом случае, в ситуации отсутствия пожара, контакты релейного выхода разомкнуты. В случае возникновения пожара произойдет попеременное замыкание - размыкание контактов релейного выхода.
  - ✓ **Мигать из состояния включено при пожаре**. В этом случае в ситуации отсутствия пожара контакты релейного выхода замкнуты. В случае возникновения пожара произойдет попеременное размыкание - замыкание контактов релейного выхода.
  - ✓ **Мигать на время из состояния выключено при пожаре.** В этом случае в ситуации отсутствия пожара контакты релейного выхода разомкнуты. В случае возникновения пожара произойдет попеременное замыкание-размыкание контактов релейного выхода на время, указанное в параметре «Время активизации».
  - ✓ **Мигать на время из состояния включено при пожаре.** В этом случае в ситуации отсутствия пожара контакты релейного выхода замкнуты. В случае возникновения пожара произойдет попеременное размыкание-замыкание контактов релейного выхода на время, указанное в параметре «Время активизации».
  - ✓ **Лампа –** программа управления, указывающая на то, что к данному релейному выходу подключен световой оповещатель пожара.
  - ✓ **ПЦН –** программа управления, указывающая на то, что данный релейный выход используется для передачи извещения о пожаре на пост центрального наблюдения (ПЦН).
  - ✓ **ПЦН (старая тактика) –** программа управления, указывающая на то, что данный релейный выход используется для передачи извещения о пожаре на пост центрального наблюдения (ПЦН) по старой тактике передачи тревожного оповещения.
  - ✓ **Сирена –** программа управления, указывающая на то, что к данному релейному выходу подключен звуковой оповещатель пожара.
  - ✓ **Включить на время при взятии** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода на время указанное в параметре «Время активизации», после взятия шлейфа пожарной сигнализации на дежурство.

✓ **Выключить на время при взятии** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода на время указанное в параметре «Время активизации», после взятия шлейфа пожарной сигнализации на дежурство.

✓ **Включить при взятии** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода после взятия шлейфа пожарной сигнализации на дежурство.

✓ **Выключить при взятии** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода после взятия шлейфа пожарной сигнализации на дежурство.

✓ **Включить на время при снятии** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода на время, указанное в параметре «Время активизации», после снятия шлейфа пожарной сигнализации с дежурства.

✓ **Выключить на время при снятии** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода на время, указанное в параметре «Время активизации», после снятия шлейфа пожарной сигнализации с дежурства.

✓ **Включить при снятии** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода после снятия шлейфа пожарной сигнализации с дежурства.

✓ **Выключить при снятии** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода после снятия шлейфа пожарной сигнализации с дежурства.

✓ **Включить при переходе в состояние «Неисправность»** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода в случае обнаружения неисправности в шлейфе пожарной сигнализации.

✓ **Выключить при переходе в состояние «Неисправность»** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода в случае обнаружения неисправности в шлейфе пожарной сигнализации.

✓ **Включить на время при переходе в состояние «Неисправность»** – программа управления, указывающая на необходимость замкнуть контакты релейного выхода на время, указанное в параметре «Время активизации», в случае обнаружения неисправности в шлейфе пожарной сигнализации.

✓ **Выключить на время при переходе в состояние «Неисправность»** – программа управления, указывающая на необходимость разомкнуть контакты релейного выхода на время, указанное в параметре «Время активизации», в случае обнаружения неисправности в шлейфе пожарной сигнализации.

✓ **Мигать при переходе в состояние «Неисправность» из состояния выключено**. В этом случае в ситуации отсутствия неисправности в шлейфе пожарной сигнализации контакты релейного выхода разомкнуты. В случае возникновения неисправности произойдет попеременное замыкание – размыкание контактов дополнительного выхода.

✓ **Мигать из состояния включено при неисправности**. В этом случае в ситуации отсутствия неисправности в шлейфе пожарной сигнализации контакты релейного выхода замкнуты. В случае возникновения неисправности произойдет попеременное размыкание – замыкание контактов дополнительного выхода.

✓ **Мигать на время из состояния выключено при неисправности**. В этом случае в ситуации отсутствия неисправности в шлейфе пожарной сигнализации контакты релейного выхода разомкнуты. В случае возникновения неисправности произойдет попеременное замыкание – размыкание контактов дополнительного выхода в течение времени, указанного в параметре «Время активизации».

✓ **Мигать на время из состояния включено при неисправности**. В этом случае в ситуации отсутствия неисправности в шлейфе пожарной сигнализации контакты релейного выхода замкнуты. В случае возникновения неисправности произойдет попеременное размыкание – замыкание контактов дополнительного выхода в течение времени, указанного в параметре «Время активизации».

✓ **Включить при внимании** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода в случае возникновения ситуации «Внимание».

✓ **Выключить при внимании -** программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время в случае возникновения ситуации «Внимание».

✓ **Включить на время при внимании** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре «Время активизации», в случае возникновения ситуации «Внимание».

✓ **Выключить на время при внимании** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре «Время активизации», в случае возникновения ситуации «Внимание».

✓ **Мигать из состояния выключено при внимании**. В этом случае в ситуации отсутствия состояния «Внимание» в шлейфе пожарной сигнализации контакты релейного выхода разомкнуты. В случае возникновения ситуации «Внимание» произойдет попеременное замыкание – размыкание контактов дополнительного выхода.

✓ **Мигать из состояния включено при внимании**. В этом случае в ситуации отсутствия состояния «Внимание» в шлейфе пожарной сигнализации контакты релейного выхода замкнуты. В случае возникновения ситуации «Внимание» произойдет попеременное размыкание – замыкание контактов дополнительного выхода.

✓ **Мигать на время из состояния выключено при внимании**. В этом случае в ситуации отсутствия состояния «Внимание» в шлейфе пожарной сигнализации контакты релейного выхода разомкнуты. В случае возникновения ситуации «Внимание» произойдет попеременное замыкание – размыкание контактов дополнительного выхода в течение времени, указанном в параметре «Время активизации».

✓ **Мигать на время из состояния включено при внимании**. В этом случае в ситуации отсутствия состояния «Внимание» в шлейфе пожарной сигнализации контакты релейного выхода замкнуты. В случае возникновения ситуации «Внимание» произойдет попеременное размыкание – замыкание контактов дополнительного выхода в течение времени, указанном в параметре «Время активизации».

Описание параметров видеоподсистемы

Подсистема видеонаблюдения единой системы безопасности PERCo-S-20 состоит из следующих элементов:

✓**Сервер видеонаблюдения** - раздел, предназначенный для обеспечения работы системы безопасности с камерами видеонаблюдения, ведения архива видеонаблюдения.

✓**Видеоконтроль/Видеонаблюдение PERCo-SM12** – раздел, предназначенный для отображения видеоинформации с камер видеонаблюдения на рабочем месте оператора. Управления видеокамерами, просмотра видеоархива.

✓**Прозрачное здание PERCo-SM15** – раздел, предназначенный для отображения видеоинформации с камер подключенных к системе видеонаблюдения на рабочих местах руководителей предприятия.

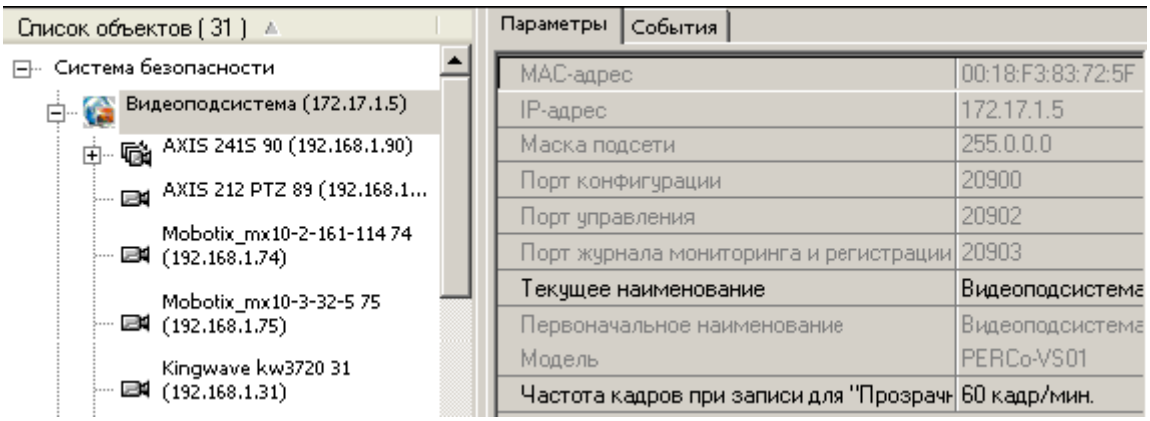
✓**Верификация/идентификация PERCo-SM09 Видеоидентификация, Прием посетителей PERCo-SM10** – разделы, предназначенные для контроля и управления входом в помещения, контролируемые подсистемой контроля доступа с одновременным отображением и записью видеоинформации с камер видеонаблюдения.

Для функционирования этих программных модулей необходимо описать параметры работы всей подсистемы видеонаблюдения. Описание настроек работы сервера видеонаблюдения приведено в соответствующей главе данного руководства.

Ниже приводится описание параметров работы видеоподсистемы и видеокамер.

Видеоподсистема

В данном случае под видеоподсистемой понимается программный модуль **Сервер видеонаблюдения**, который отображается в дереве устройств системы:



В качестве параметров работы должны быть заданы:

- **Текущее название** - название, которое будет отображаться в дальнейшем в

журналах мониторинга и регистрации.

- **Частота кадров при записи для «Прозрачного здания» -** параметр, указывающий количество записываемых кадров в минуту. Этот параметр имеет смысл только в случае использования программного модуля Прозрачное здание. И влияет на частоту записываемых кадров с камер видеонаблюдения, у которых установлен параметр «Использовать в прозрачном здании». При установке этого параметра необходимо учитывать трафик локальной сети. Рекомендованное значение не более 1 кадра в секунду.

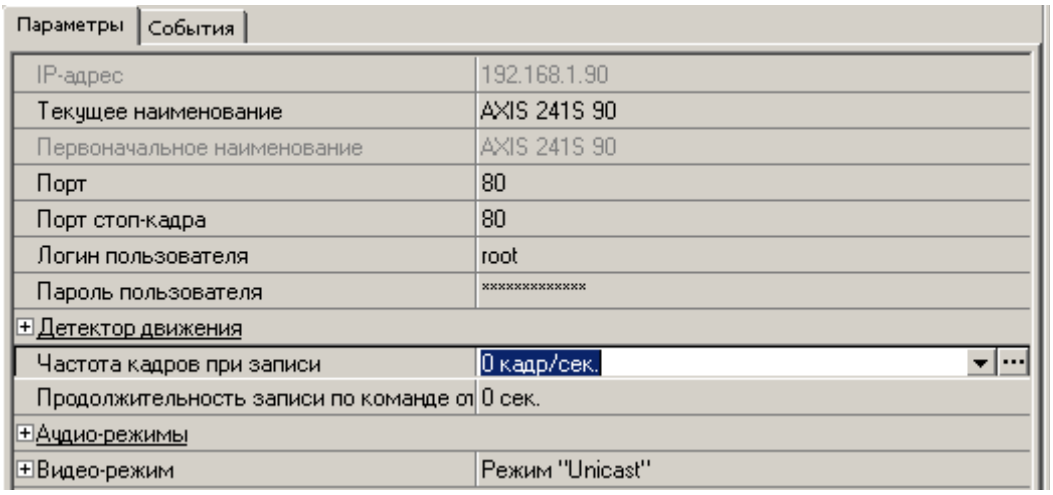
Может быть задано только его название, которое будет отображаться в дальнейшем в журналах мониторинга и регистрации.

Также в панели параметров отображаются неизменяемые параметры работы сервера видеонаблюдения.

Видеокамеры

Ниже приводится описание параметров функционирования камер видеонаблюдения, необходимых для их функционирования в системе безопасности PERCo-S-20.

В зависимости от типа используемой видеокамеры, меняется и список ее параметров.



- **Текущее наименование** – параметр, задающий мнемоническое наименование выбранной камеры видеонаблюдения. Введенной значение будет использоваться в журналах мониторинга и регистрации.

- **Порт, Порт стоп-кадра** – параметры, указывающий номер порта, используемый для связи с выбранной камерой. Более подробная информация представлена в технической документации на выбранную виде камеру.

- **Логин пользователя, Пароль пользователя** – параметры, задающие имя и пароль пользователя, от имени которого будет осуществляться подключение к выбранной видеокамере. Задание имени пользователя и пароля необходимо для предотвращения доступа к видеокамере других пользователей.

- **Детектор движения** — параметры, определяющие продолжительность записи и порт, имеющие отношение к детектору движения.

- **Частота кадров при записи** – параметр, задающий частоту записываемой видеоинформации при получении команды Начать запись.

- **Продолжительность записи** – время, в течение которого видеосервер будет осуществлять запись с выбранной камеры при поступлении команды «Начать запись». Команда о начале записи может быть подана в двух случаях: Оператором системы из программных модулей Мониторинг и Центральный пост; Как результат выполнения заданной реакции системы на произошедшее событие.

- **Аудио-режимы** — параметры режима работы видеокамеры. Наличие режима Downstream позволяет записывать и воспроизводить звук, полученный со встроенного микрофона камеры. Если этот режим выбран, необходимо включить передачу аудио и выбрать формат данных в веб-интерфейсе камеры.

- **Видео-режим** - параметры режима работы видеокамеры. Наличие того или иного режима зависит от типа камеры, версии sdk и прошивки камеры.

  Http — в этом режиме камера работает через протокол http в формате mjpeg. В этом режиме камера ограничивает количество подключений (Ограничения ресурсов используемой камеры)

  Unicast — в этом режиме камера работает либо через протокол RTSP/RTP/RTCP в формате mpeg4 или по нестандартному протоколу в формате mpeg4, поддерживаемому камерой. В этом режиме количество подключений также ограничено ресурсами камеры.

  Multicast - в этом режиме камера работает либо через протокол RTSP/RTP/RTCP в формате mpeg4, либо по нестандартному протоколу в формате mpeg4, поддерживаемому камерой. В отличии от Unicast, количество подключений к камере в этом режиме неограничено.

  Tunnelled — режим туннелирования RTSP через http. Используется при невозможности подключения через Unicast, количество подключений также ограничено.

ПОМЕЩЕНИЯ И МНЕМОСХЕМА

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

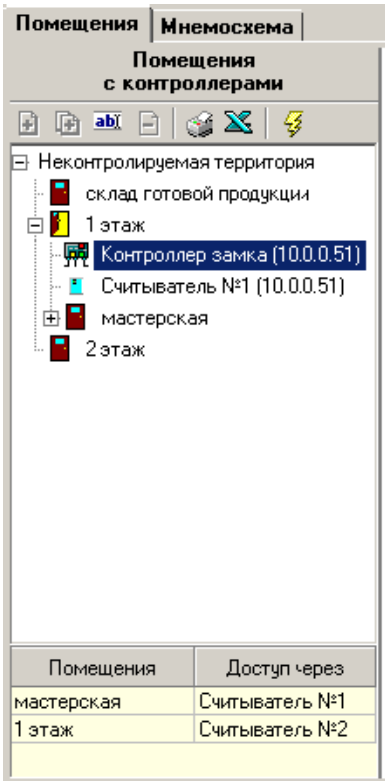
Под помещениями в системе безопасности подразумевается иерархическая структура помещений предприятий (организации). Эта информация необходима для определения уровней доступа, указания какие контроллеры контролируют доступ в какие помещения, привязки шлейфов охранно-пожарной сигнализации, видеокамер,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

Помещения

В 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. Так же справедливо и обратное, нельзя выйти с территории предприятия, не совершив предварительного входа.

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

Мнемосхема

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

Существует два варианта создания мнемосхем:

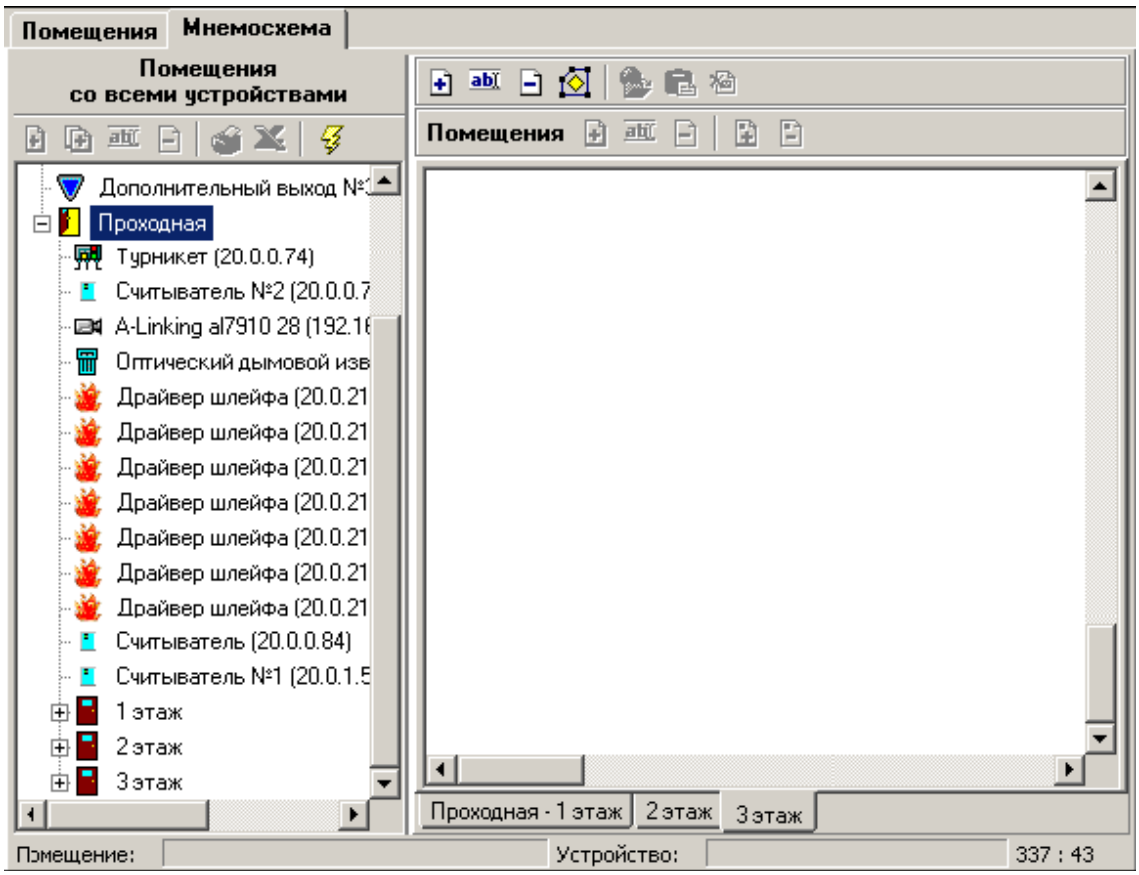
- ✓Создание мнемосхемы без использования графических изображений территории предприятия. В этом случае графические изображения располагаются на автоматически созданном белом квадрате с размером 1600x1600 пикселей. Использование такого подхода оправдано только в том случае, если территория предприятия небольшая или система безопасности состоит только из турникетов установленных на проходной.
- ✓Создание мнемосхем с использованием графических изображений территории предприятия. В этом случае размер каждой мнемосхемы определяется размером загружаемого изображения, который не может превышать 1600x1600 пикселей.

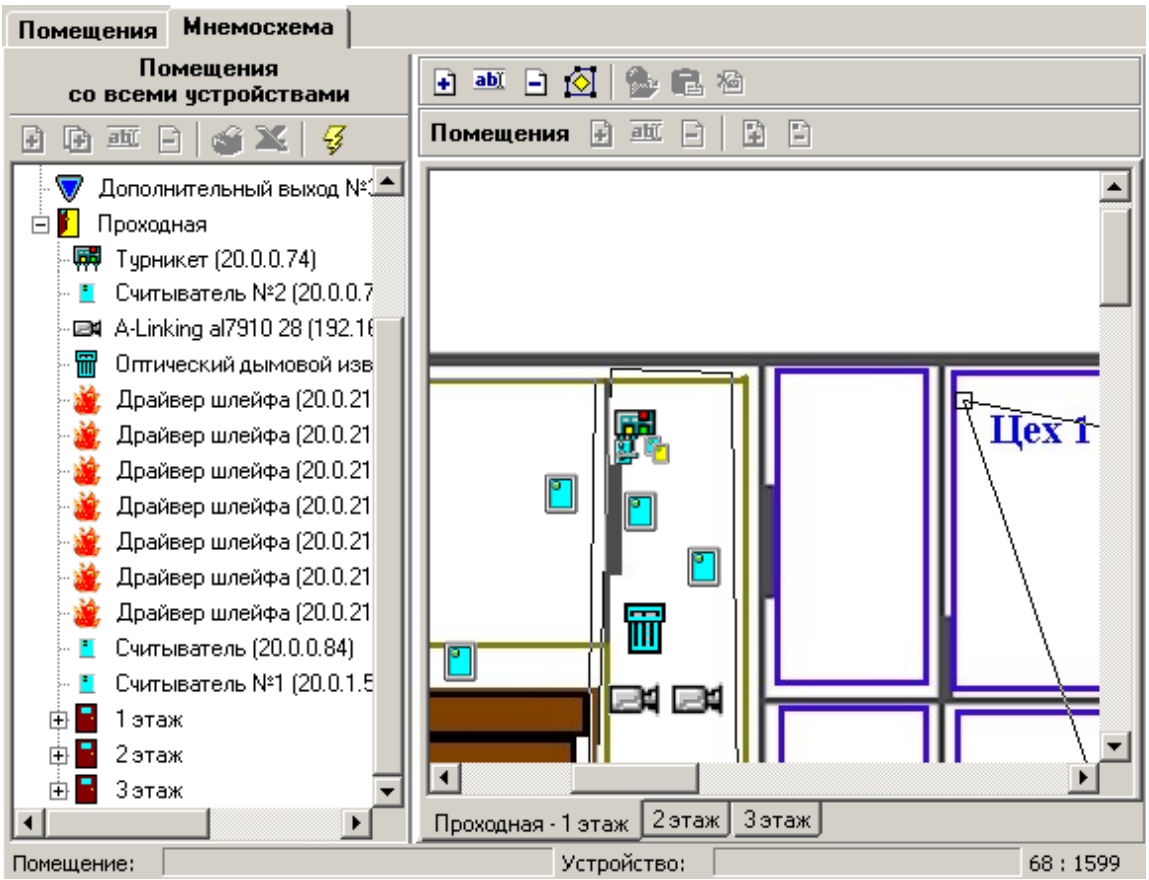
Далее рассмотрим создание мнемосхем с использованием графических планов. Создание без графических планов полностью аналогично.

Для создания мнемосхемы предприятия (поэтажных планов) 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.

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.

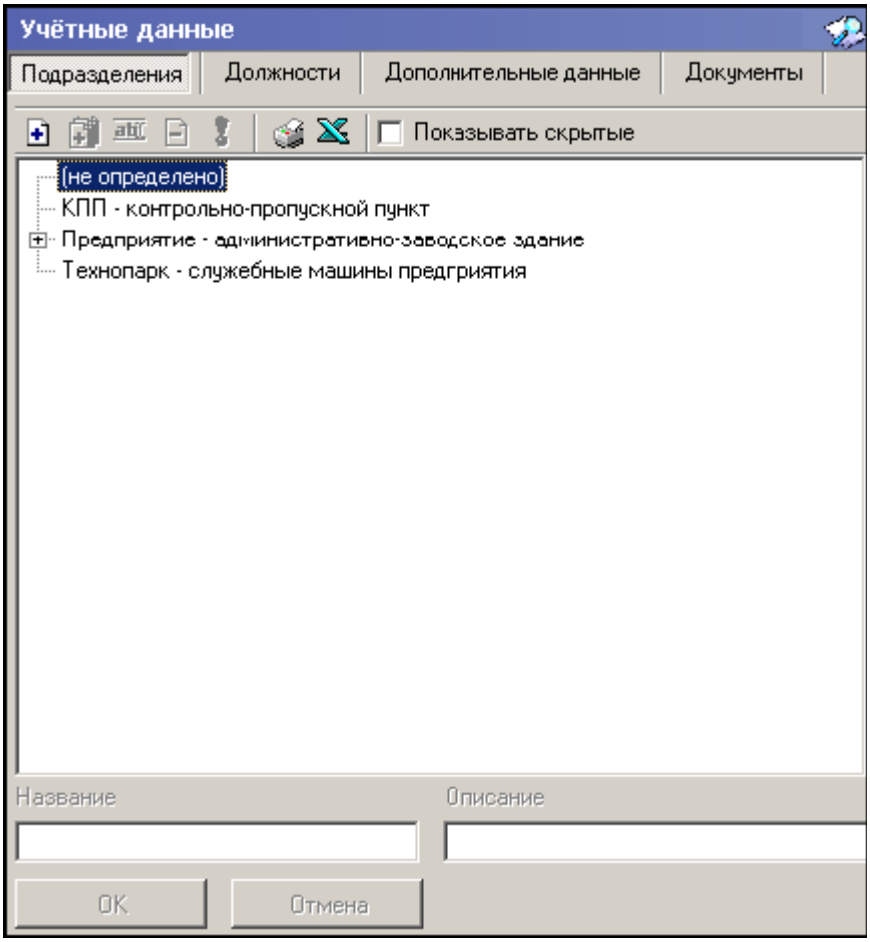
Учётные данные

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

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

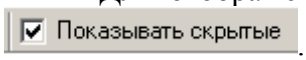
Подробная информация о правилах работы с этим разделом приведена в Руководстве пользователя в разделе **Учетные данные**.

Справочник Подразделения



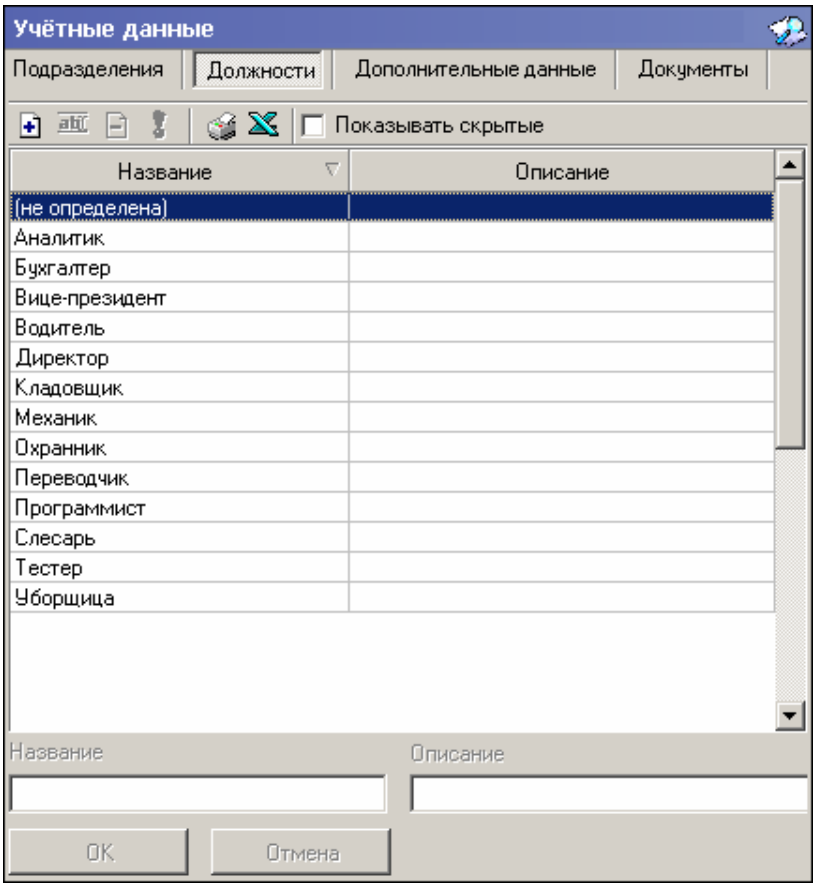
Справочник **Подразделения** предназначен для создания и редактирования структуры подразделений предприятия в соответствии с его штатным расписанием. Эта информация в дальнейшем используется при вводе данных о сотрудниках предприятия и при составлении отчетов по сотрудникам.

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

Для отображения/восстановления скрытых подразделений необходимо отметить 

.

Справочник Должности

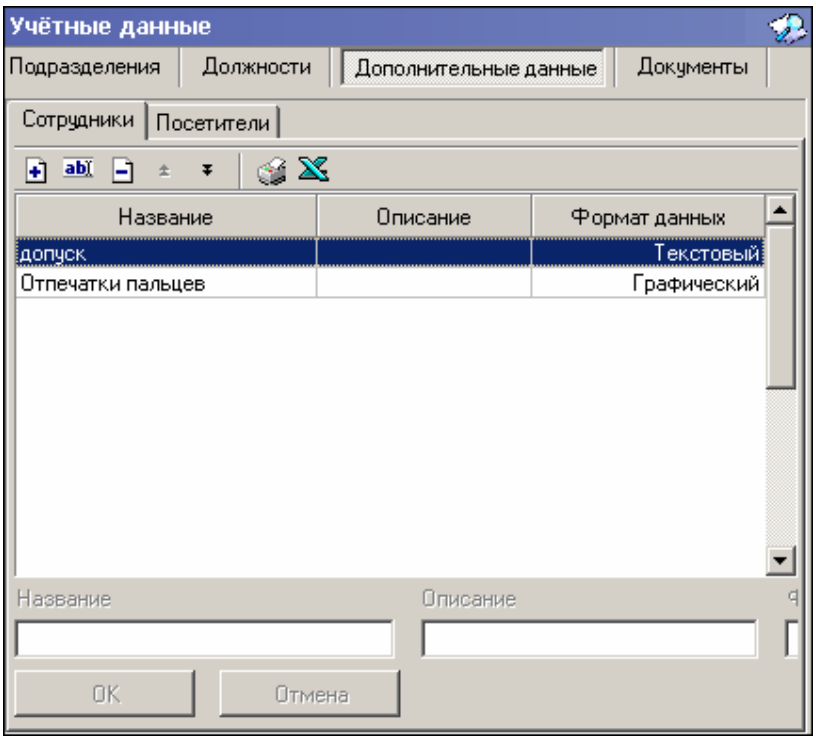


Справочник Должности по своему назначению аналогичен справочнику подразделений. В отличие от справочника Подразделения он представлен не в виде иерархического дерева, а в виде линейного списка.

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

Справочник Дополнительные данные

В отличие от двух предыдущих, справочник **Дополнительные данные** предназначен не для занесения справочной информации, а для создания структуры отображения дополнительной информации о сотрудниках.

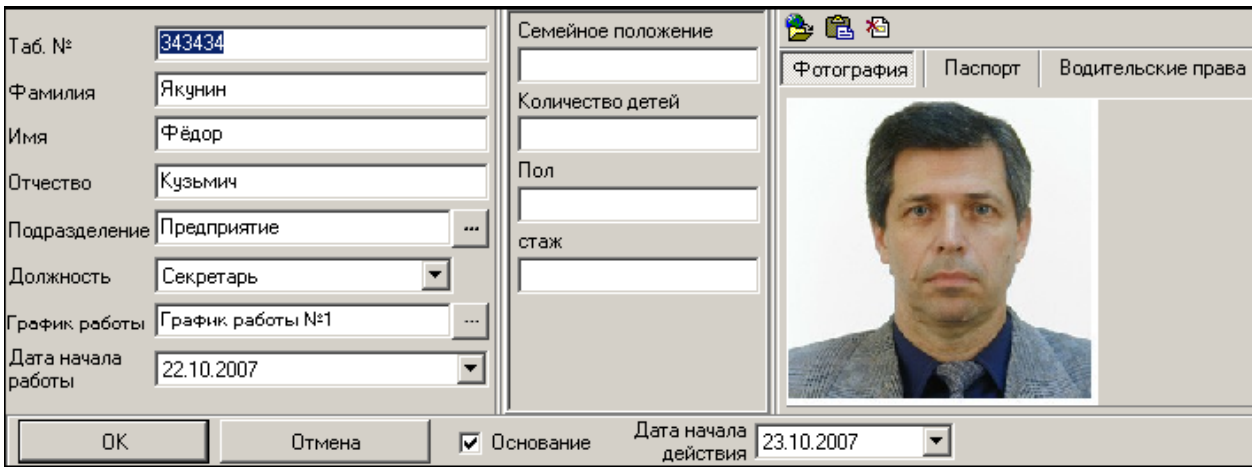


Кроме предопределенных данных о сотрудниках может возникнуть необходимость ввода дополнительной информации о работниках предприятия, например, данных о дате рождения, месте проживания, домашнем телефоне и так далее.

Работая с этим справочником, можно создать список дополнительных полей, которые будут отображаться при вводе информации о сотруднике предприятия или посетителе. Вводимые данные могут быть двух типов:

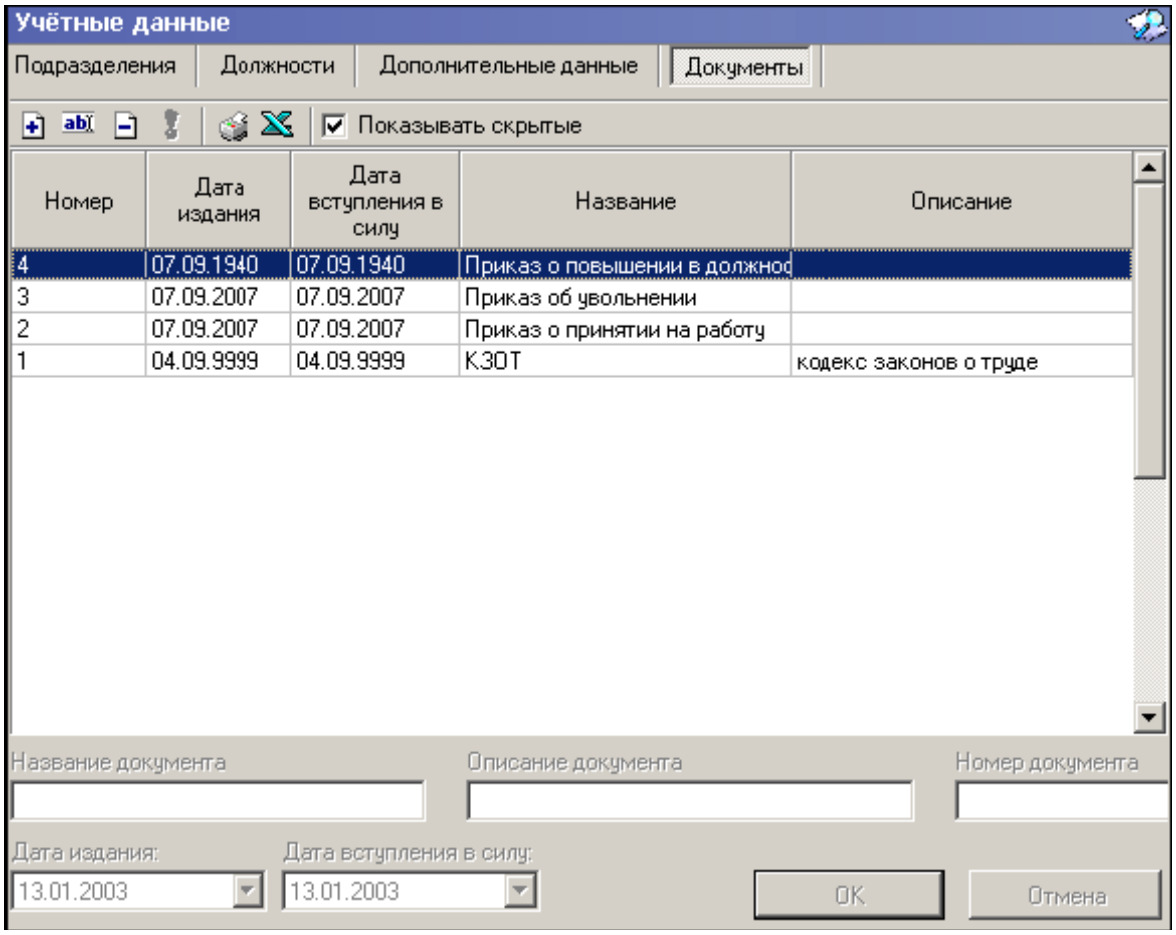
- ✓**текстовый** – позволяет хранить любую информацию в текстовом виде;
- ✓**графический** – позволяет вводить дополнительную графическую информацию о сотруднике, помимо фотографии.

После ввода и сохранения этой информации при добавлении нового сотрудника или при редактировании существующего становятся доступны введенные дополнительные поля:



Справочник Документы

Как правило, любое действие по приему на работу сотрудника, по его увольнению, по переходу в другое подразделение, смену должности сопровождается выпуском соответствующего приказа или распоряжения. Это так же определяется требованиями трудового кодекса.



Справочник **Документы** позволяет хранить информацию о таких документах, соответственно указывая их как основание при внесении изменений в учетные данные сотрудников.

ПРИМЕЧАНИЕ

Программное обеспечение не хранит сами документы! Оно позволяет только вносить информацию о дате внесения изменений, названия документа, на основании которого эти изменения были произведены.

Сотрудники

Раздел **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, ведении единой базы сотрудников приведена в Руководстве оператора в разделе **Сотрудники**.

ПАРАМЕТРЫ ДОСТУПА

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

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

После подготовки 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 так же 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:

Временные зоны

Временная зона — это совокупность **временных интервалов** (до 4-х) в пределах календарных суток, в течение которых возможно:

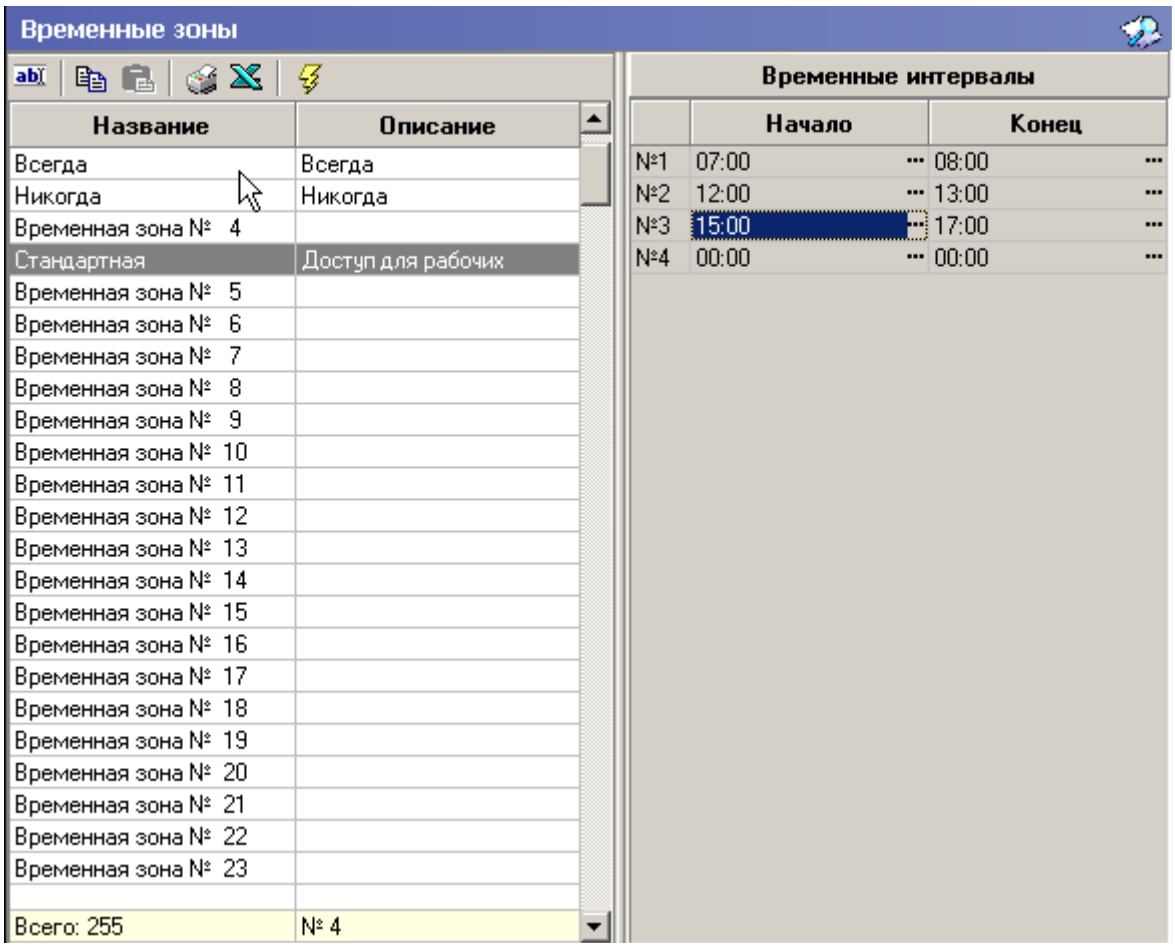
- разрешение доступа по пользовательской карте;
- постановка/снятие помещения на охрану.

Временные интервалы представляют собой отрезки времени с точностью до минуты, в течение которых доступ заданным категориям сотрудников (посетителей) на определенные объекты разрешен. Сотруднику может быть разрешен доступ на объект в соответствии с любой из временных зон.

Рассмотрим на примере использование временной зоны в качестве критерия доступа. Нам необходимо создать временной критерий доступа, в соответствии с которым будет разрешен доступ на территорию предприятия в любой день недели в течение следующего времени:

- 7:00 – 8:00 – для входа на территорию предприятия;
- 12:00 – 13:00 – для обеспечения входа и выхода на обед;
- 17:00 – 18:00 – для обеспечения выхода сотрудников с предприятия.

Для этого отредактируем название любой из неиспользуемых временных зон, назовем ее «Стандартная», в описании укажем, что она предназначается для рабочих специальностей, и введем в панели свойств необходимые нам интервалы:



Следует обратить внимание на то, что нам для описания такого графика работы необходимо было всего 3 интервала, при этом 4-ый интервал остается неиспользованным.

Временные зоны, как уже указывалось выше, могут быть использованы для задания прав доступа сотрудников/посетителей предприятия. Задание временной зоны в качестве временного критерия доступа означает, что данный сотрудник может осуществить доступ в выбранные помещения в течение указанных временных интервалов в любой день недели.

Как правило, выбор временной зоны в качестве критерия доступа очень редкое явление. Но при этом нужно помнить о том, что временные зоны служат основой для создания графиков доступа на предприятие и используются напрямую или косвенно во всех остальных временных критериях доступа.

Типы праздников

В соответствии с действующим законодательством и принятыми правилами работы на каждом предприятии существуют так называемые праздничные дни. Это дни, в которые предприятие не работает или работает по сокращенному графику.

Для обеспечения корректного доступа в такие дни система безопасности PERCo-S-20 позволяет указать на весь календарный год, какие дни будут выходными, и в какие из дней года работа будет идти по укороченному графику работы.

По умолчанию в системе праздничными днями считаются государственные праздники.

Дата	Тип	Описание
01.01.2008	1	Новогодние каникулы
02.01.2008	1	Новогодние каникулы
03.01.2008	1	Новогодние каникулы
04.01.2008	1	Новогодние каникулы
07.01.2008	1	Рождество
23.02.2008	1	День защитника Отечества
08.03.2008	1	Женский день
01.05.2008	1	День весны
09.05.2008	1	День победы
12.06.2008	1	День независимости
04.11.2008	1	День примирения
31.12.2008	1	Новый год

Вы можете внести любые изменения в этот список.

Кроме назначения даты конкретного праздника необходимо указать его тип. Тип праздника – это логическое название, которое позволяет создать совокупности дней с доступом по определенному правилу.

Недельные графики

Недельный график представляет собой совокупность временных зон, заданных для каждого дня недели, в том числе и для 8 типов праздничных дней.

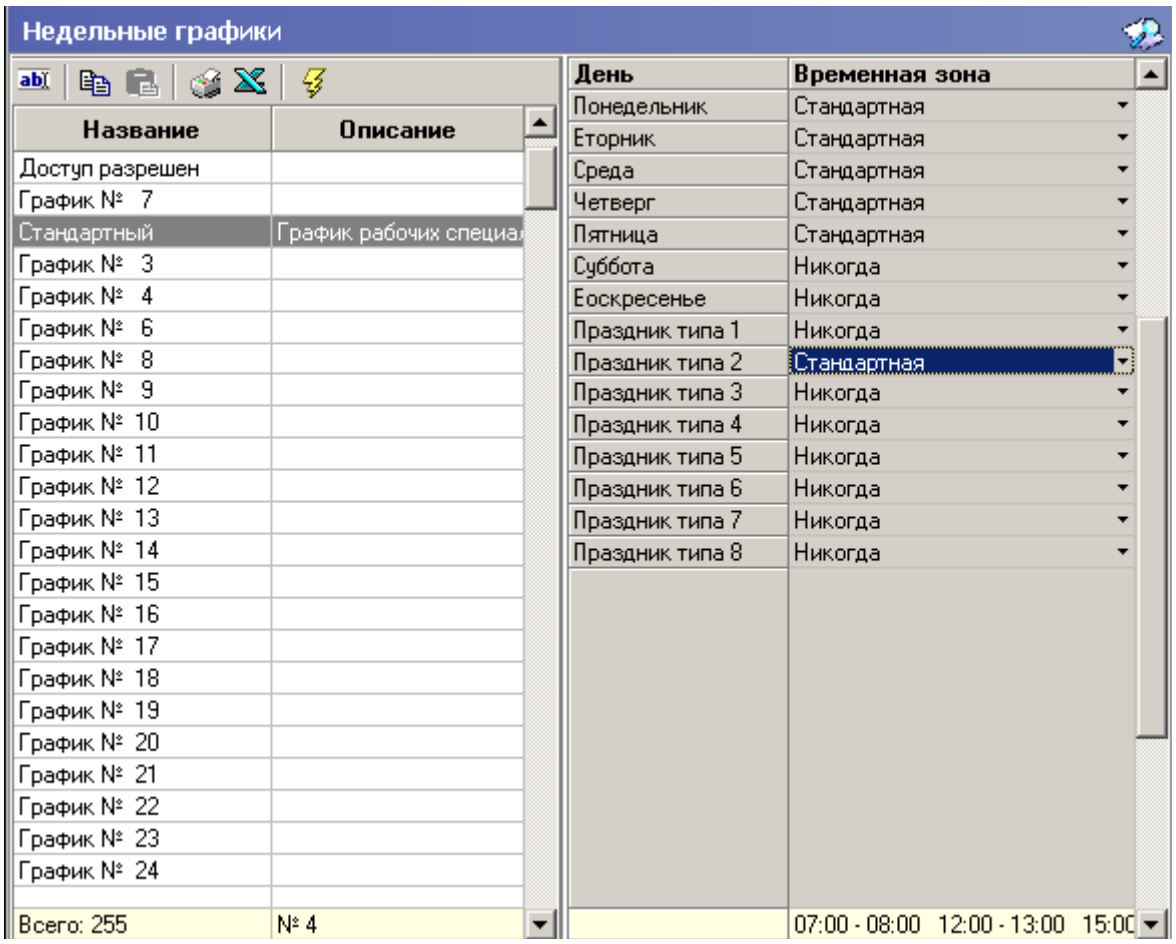
Доступ сотруднику на объект может быть определен в соответствии с любым из недельных графиков.

Создавая недельные графики, вы должны понимать, что задание прав доступа по недельному графику определяет время, в течение которого будет разрешен доступ на предприятие вне зависимости от конкретной даты.

Рассмотрим на примере создание недельного графика для сотрудников, которые работают каждую неделю, с понедельника по пятницу, по временной зоне «Стандартная». При этом доступ в субботу и воскресенье им запрещен. Также в предпраздничные дни их рабочий день не сокращается.

В календаре праздничных дней необходимо указать, что все календарные дни перед праздником будут иметь второй тип.

Выберем один из неиспользованных недельных графиков и изменим его название на «Стандартный», в описании укажем, что это недельный график рабочих специальностей:



Далее зададим на все дни недели с понедельника по пятницу временную зону «Стандартная». Так же для второго типа праздника (мы помним, что у рабочих специальностей нет сокращенного рабочего дня) укажем временную зону «Стандартная».

Сохраним сделанные изменения. Теперь при указании в качестве графика доступа недельного графика «Стандартный», сотрудники смогут входить на территорию предприятия только по рабочим дням недели и в предпраздничные дни в течение следующего времени:

- 7:00 – 8:00 – для входа на территорию предприятия;
- 12:00 – 13:00 – для обеспечения входа и выхода на обед;
- 17:00 – 18:00 – для обеспечения выхода сотрудников с предприятия.

Скользящие посуточные графики

Как правило, на производственных предприятиях графики работы не ограничиваются недельной цикличностью. Периодичность работы сотрудников может равняться и нескольким дням и неделям. Для поддержки таких сложных графиков работы в системе безопасности предусмотрены два типа скользящих графиков.

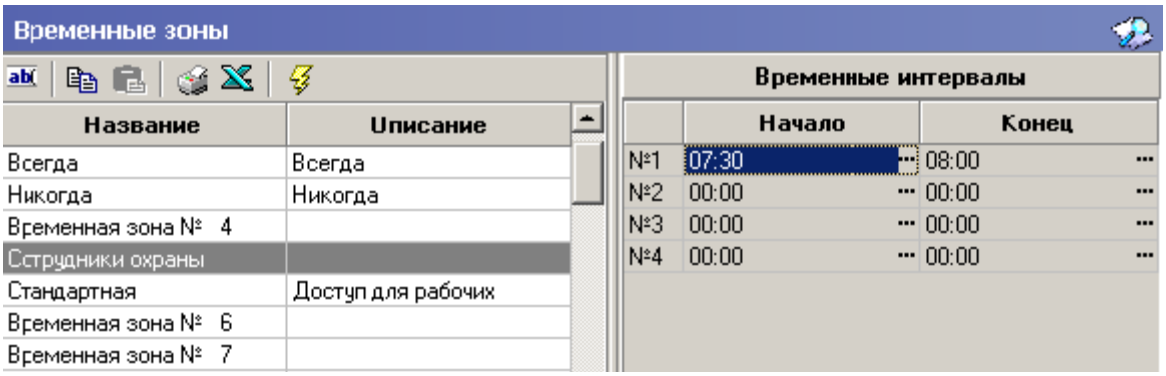
Скользящий посуточный график – это совокупность временных зон доступа установленных на каждый день графика и даты начала графика. Максимальное количество дней в скользящем посуточном графике равно 30. Всего в системе может быть 255 таких графиков.

Идея скользящего посуточного графика заключается в его циклическом повторении. При этом нужно не забывать, что нерабочие дни графика так же должны быть в него включены для определения повторяемости.

Рассмотрим это на примере:

На предприятии работники службы охраны работают по графику сутки через двое. Они заступают на дежурство в 8:00 и заканчивают дежурство в 8:00 следующего дня, день окончания работы и следующий день у них выходной. Для описания такого графика работы необходимо создать временную зону:

Временная зона первого дня содержит только один интервал с 7:30 до 8:00 – это время, в течение которого работник должен прийти на работу. Назовем ее «Сотрудники охраны».

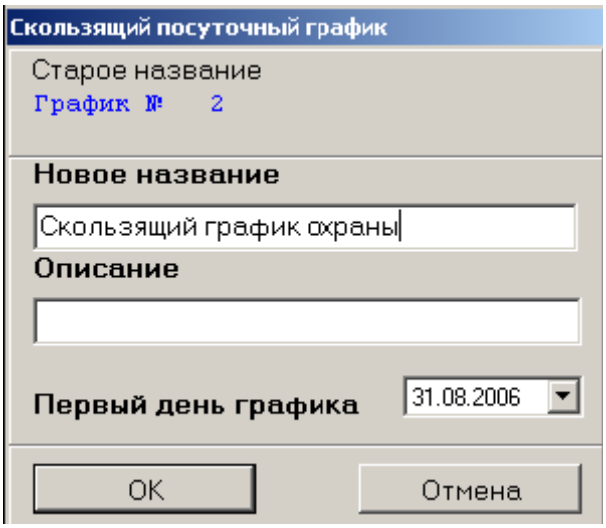


Теперь можно перейти к созданию собственно посуточного скользящего графика доступа.

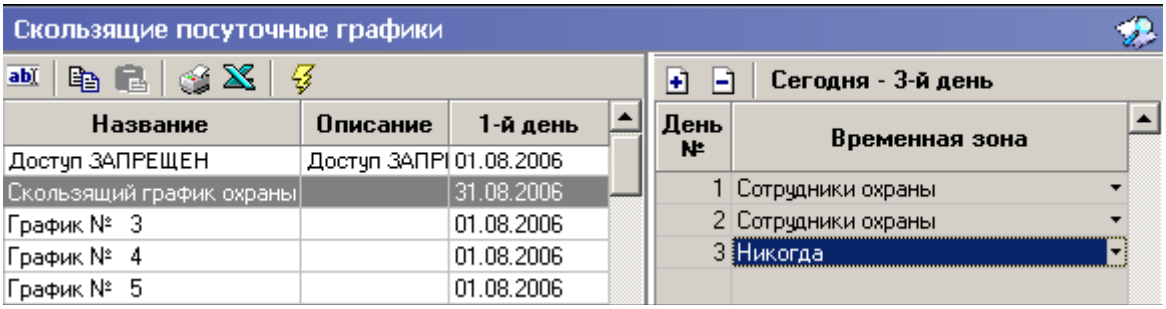
1. Необходимо выбрать любой незадействованный скользящий посуточный график работы и изменить его данные.

1. Указать название, например «Скользящий график охраны».

2. Указать дату начала этого графика – дата начала указывает, с какого числа система должна автоматически отсчитывать его периодичность. Например, он начинается с 5 марта.



3. Далее необходимо в панели свойств графика добавить необходимое количество дней. В нашем случае оно равно трем. И для первых двух дней (время прихода на работу и ухода у охранников совпадает) указать созданную временную зону «Сотрудники охраны».



4. Сохранить сделанные изменения.

Скользящие понедельные графики

Вторым типом графиков, обеспечивающих сменный режим работы, являются скользящие понедельные графики.

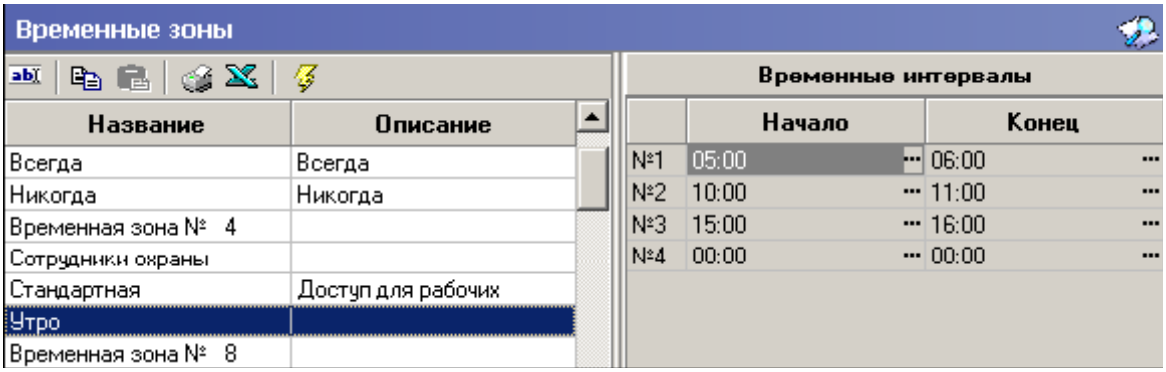
Скользящий понедельный график – это совокупность недельных графиков доступа и даты начала графика. Максимальное количество недельных графиков в скользящем понедельном графике равно 51. Всего в системе может быть 255 таких графиков.

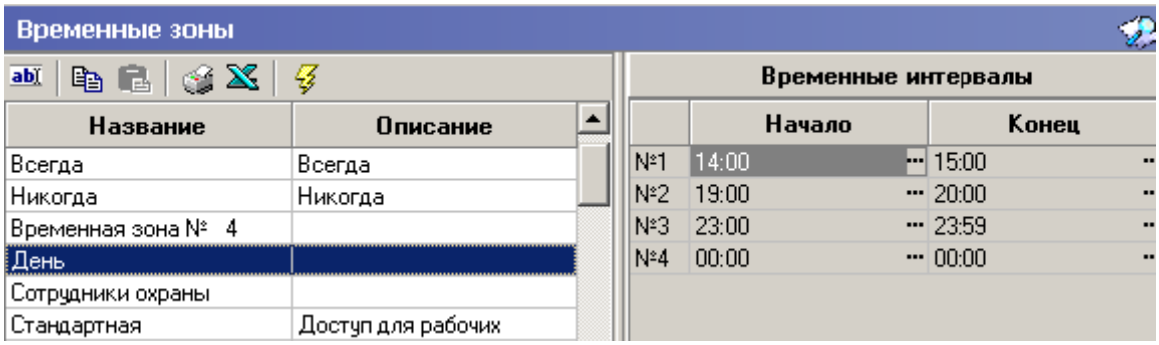
Принцип создания и использования скользящих понедельных графиков полностью аналогичен принципам работы со скользящими посуточными графиками, за исключением того, что датой начала такого графика может служить только понедельник и в качестве основной единицы графика используется не день, а неделя.

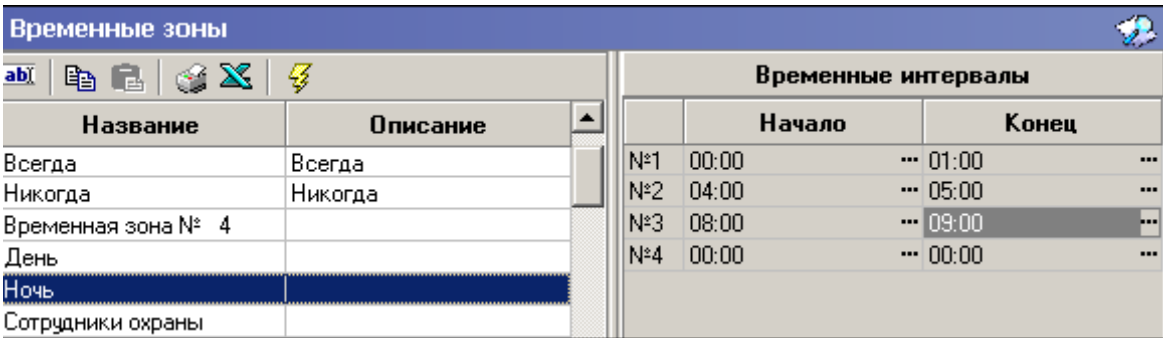
Рассмотрим на примере:

Есть группа сотрудников, которая работает первую неделю с 6 утра до 15 дня по рабочим дням, следующую неделю они работают с 15 дня до 24 часов и третью неделю - с нуля часов до 6 утра.

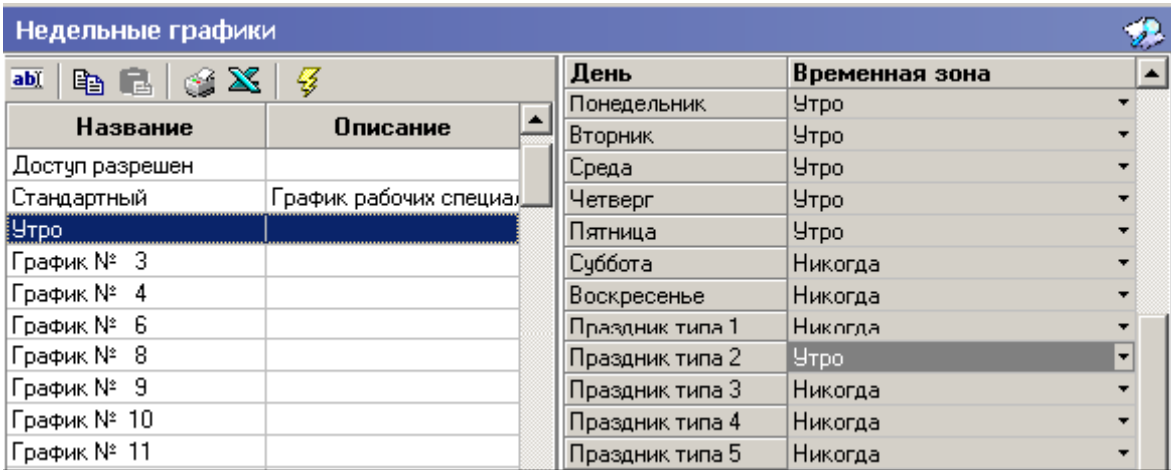
Для описания такого графика работы нам необходимо создать временные зоны, удовлетворяющие каждому варианту работы:

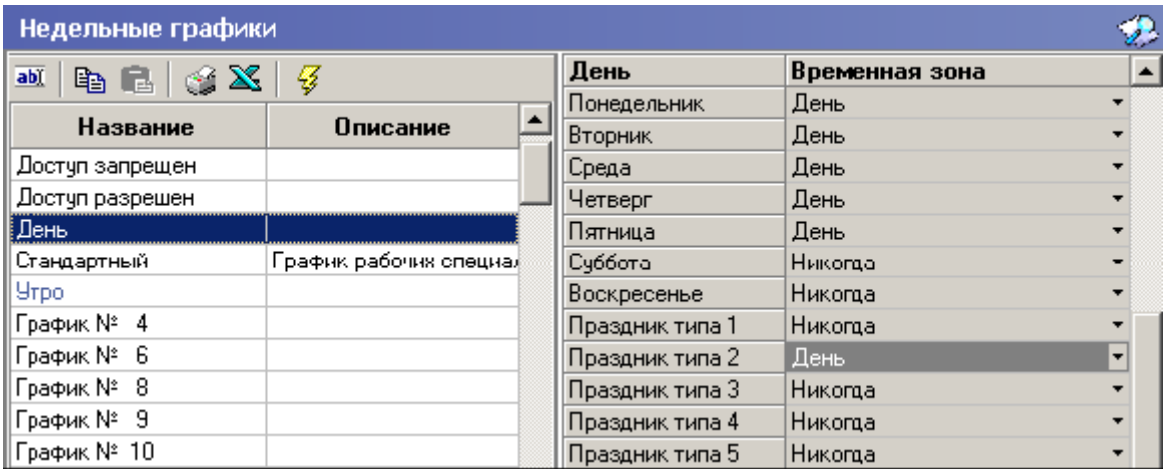


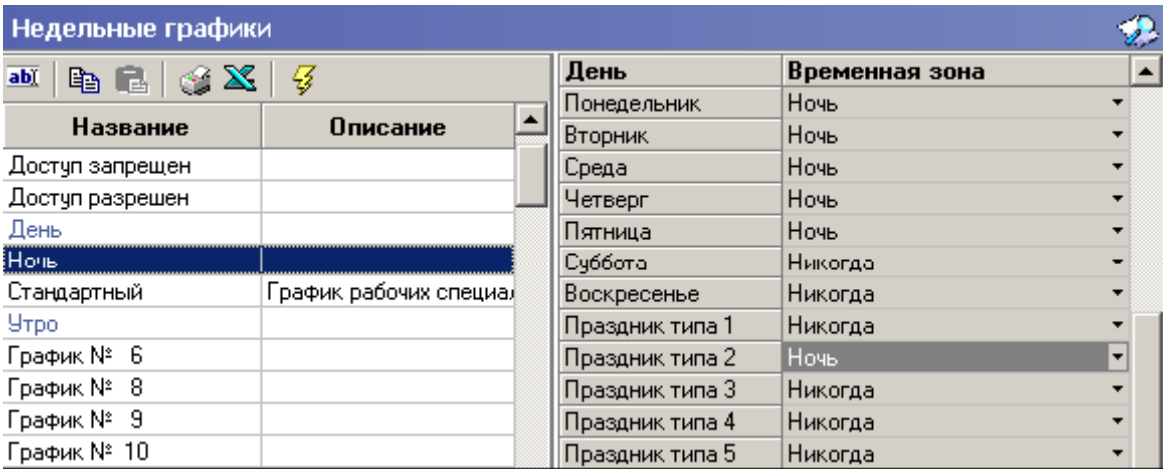




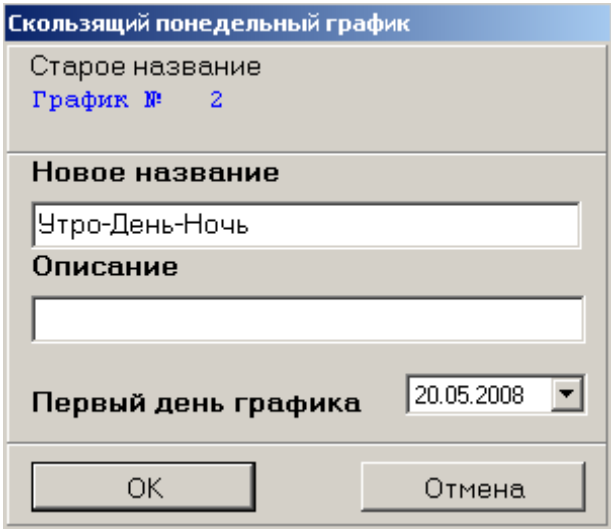
После создания временных зон необходимо создать соответствующие недельные графики работы:



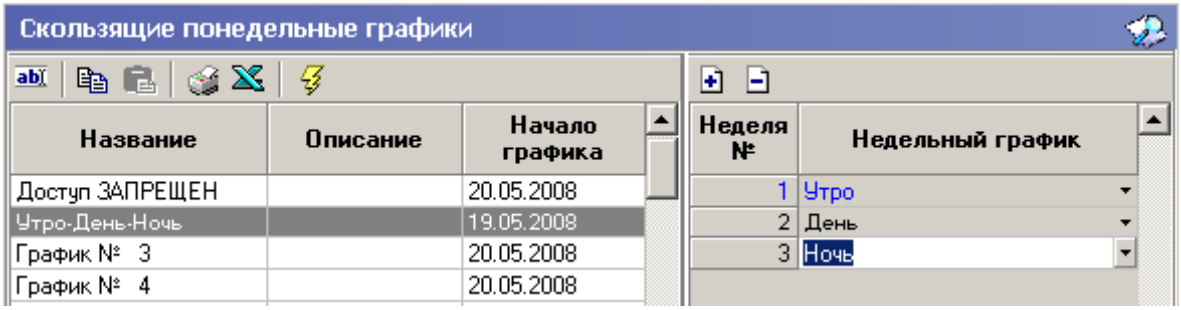




После создания и сохранения созданных временных зон и недельных графиков необходимо перейти к созданию скользящего недельного графика. Для этого необходимо выбрать незадействованный график и изменить его параметры:



Далее задайте длительность графика работы равной трем неделям. Для этого необходимо добавить три недельных графика в панели параметров и указать для них созданные недельные графики:



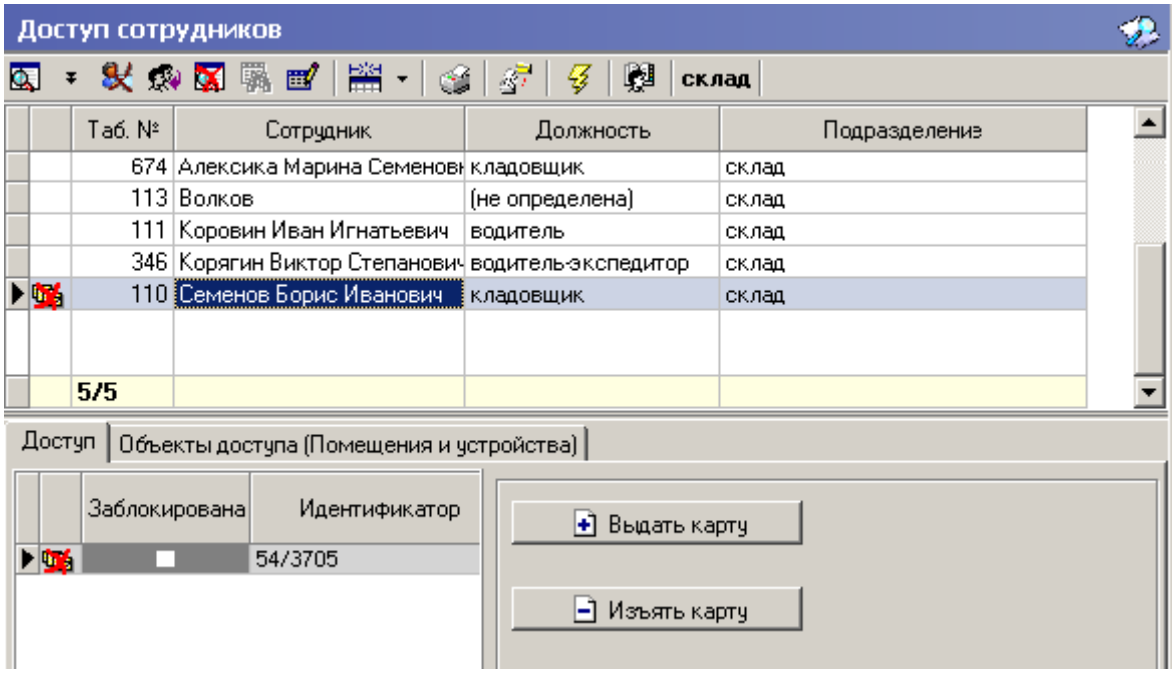
Сохраните введенные изменения.

Доступ сотрудников

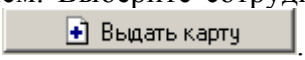
После создания всех необходимых графиков доступа можно переходить к выдаче карт доступа и назначению прав доступа сотрудников предприятия.

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.

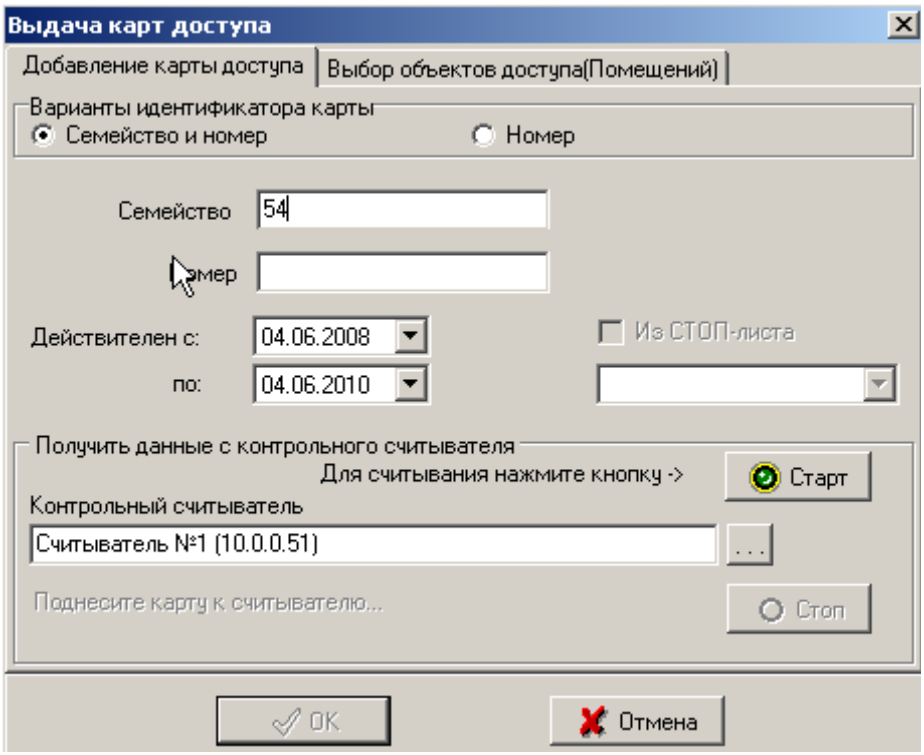


Выберите подразделение, к выдаче карт доступа сотрудникам которого вы хотите приступить. Для этого воспользуйтесь кнопкой  , название выбранного подразделения отобразится рядом.

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

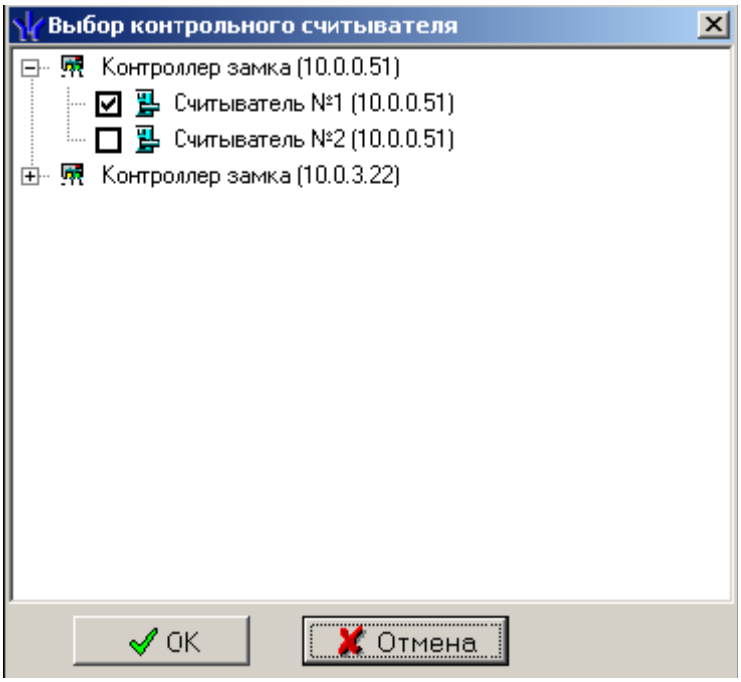
.

В появившемся диалоговом окне задайте необходимые параметры.



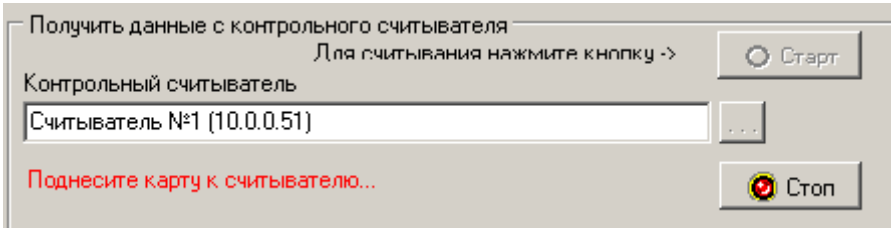
При вводе параметров необходимо обратить внимание на то, что срок действия карты доступа автоматически контролируется контроллерами. По истечению этого срока доступ по этой карте будет автоматически запрещен.

- **Получить данные с контрольного считывателя.** Для этого 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 

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 

.

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

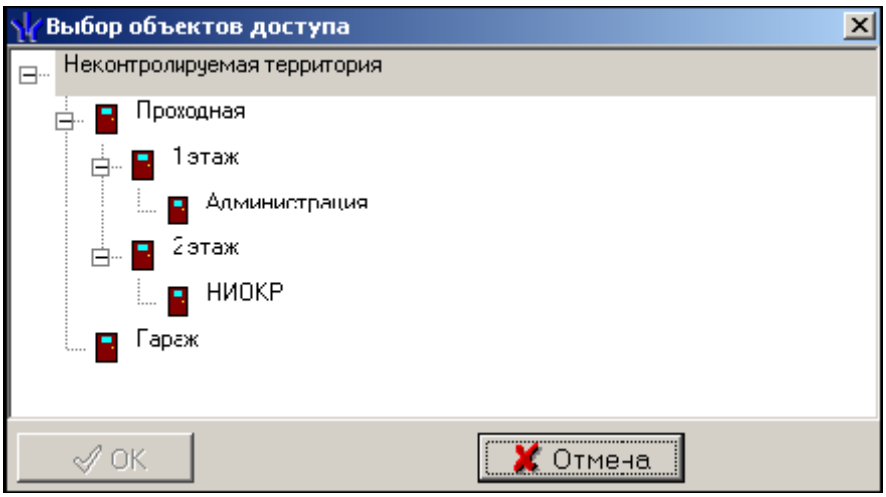
ПРИМЕЧАНИЕ

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.

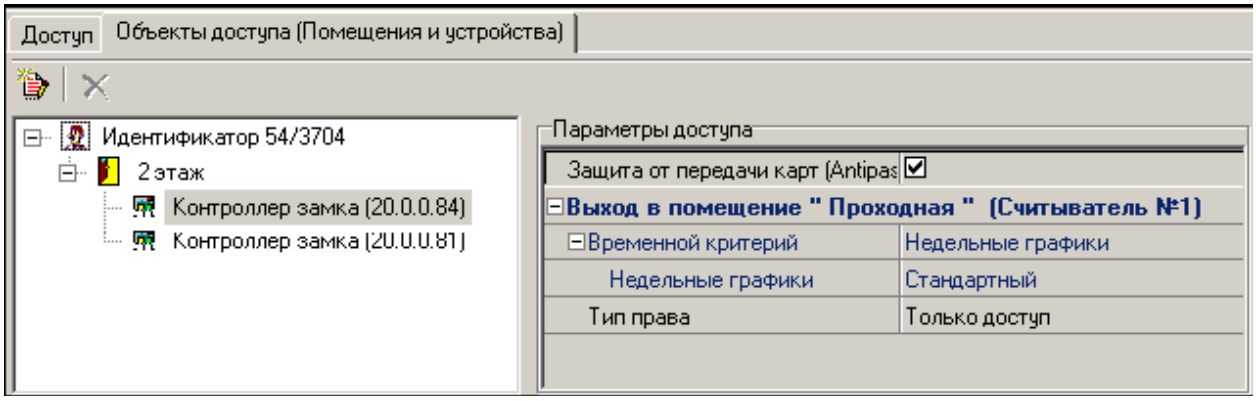
После выдачи карт доступа можно перейти к указанию прав доступа. Раздел **Доступ сотрудников** позволяет задавать права доступа не только каждому сотруднику в отдельности, но и поддерживает групповые операции. Таким образом, вы можете выделить группу сотрудников при помощи клавиши **Shift** и мышки и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



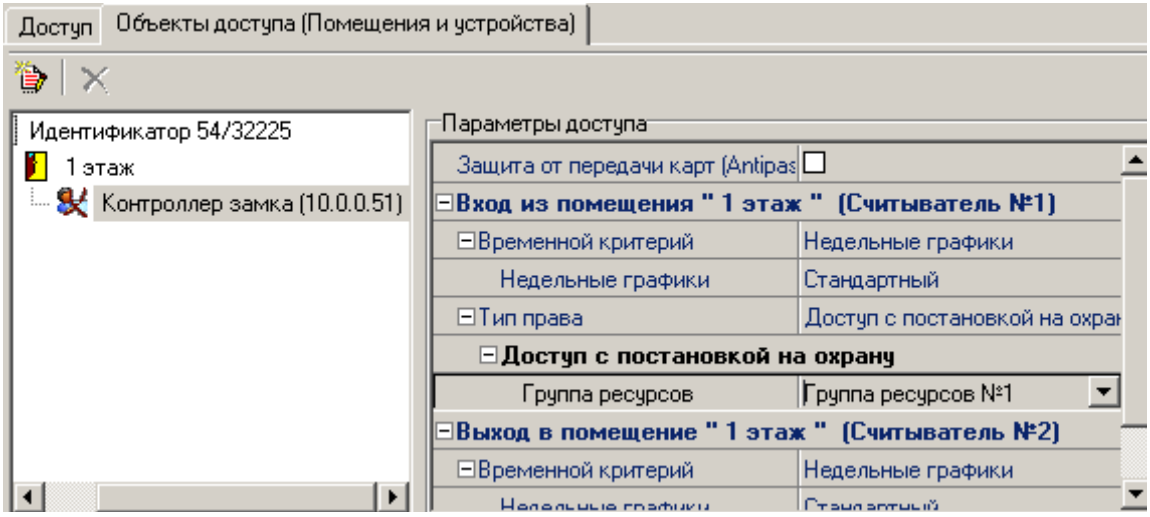
После завершения выбора объектов, в которые разрешен доступ, необходимо указать параметры доступа. Для этого необходимо выбрать поочередно каждый контроллер, отображенный в окне разрешенных объектов доступа и указать параметры доступа.

Так, например, для контроллера турникета, контролирующего вход на первый этаж, мы в нашем случае указали, что доступ через него разрешен по недельному графику, а именно по графику «Стандартный»:



Кроме этого, мы указали, что владелец упомянутой карты доступа будет подвержен контролю на случай повторного входа/выхода через этот контроллер.

Для замкового контроллера, контролирующего вход на опытный участок, мы задали следующие параметры:



В соответствии с этими параметрами, 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.

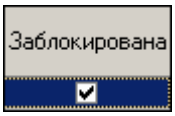
Кроме этого, владельцу этой карты доступа мы предоставили право постановки и снятия с охраны группы ресурсов №1. Тем самым, разрешив ему ставить/снимать помещение опытного участка с охраны.

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 отметить мышкой квадратик в поле

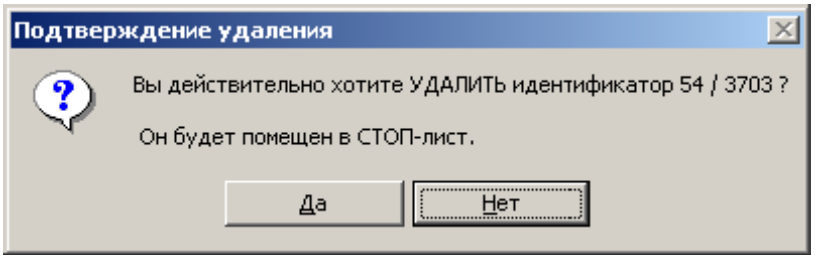
«Заблокировано». Программное обеспечение автоматически передаст данные в контроллеры. С этого момента выбранная карта доступа будет заблокирована для доступа:



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 выхода из строя, 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.

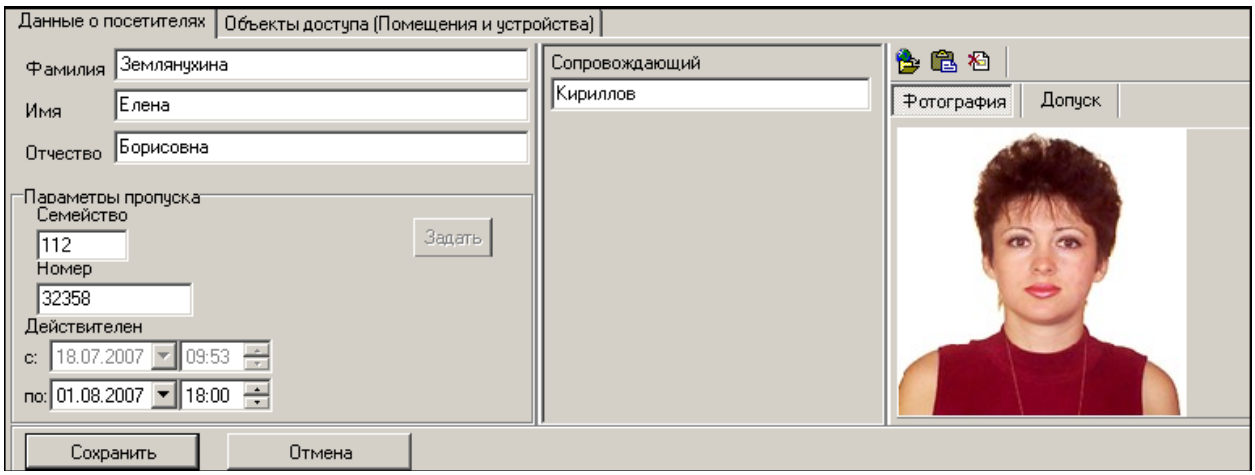
После ввода причины занесения карты доступа в «Стоп – лист» программное обеспечение автоматически передаст данные в контроллеры системы, тем самым запретив доступ по этой карте.

Доступ посетителей

На любом предприятии во время работы встает необходимость в разрешении доступа не только сотрудников, но и посетителей. Для организации доступа посетителей в системе безопасности PERCo-S-20 существует раздел **Доступ посетителей**.

По своим функциональным возможностям, принципам работы он полностью аналогичен модулю **Доступ сотрудников** и **Сотрудники**. Далее рассмотрим отличительные особенности этого раздела.

1. Кроме задания прав доступа в этом разделе так же задаются и данные о самом посетителе, его фамилия, имя, отчество, фотография и так же те дополнительные данные, которые были указаны в справочнике дополнительных данных посетителей.



2. Срок действия пропуска посетителя указывается с точностью до минуты и автоматически отслеживается контроллерами системы безопасности.

ПРИМЕЧАНИЕ

Задание дат и временных критериев производится по дате и времени на компьютере пользователя, а контроль времени производит контроллер по времени сервера. При несовпадении времени сервера и времени, установленном на компьютере пользователя, выставленное время действия карт будет неактуально.

3. При указании прав доступа посетителей невозможно задать права на постановку/снятие с охраны помещений.

МОНИТОРИНГ И УПРАВЛЕНИЕ УСТРОЙСТВАМИ

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

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

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

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

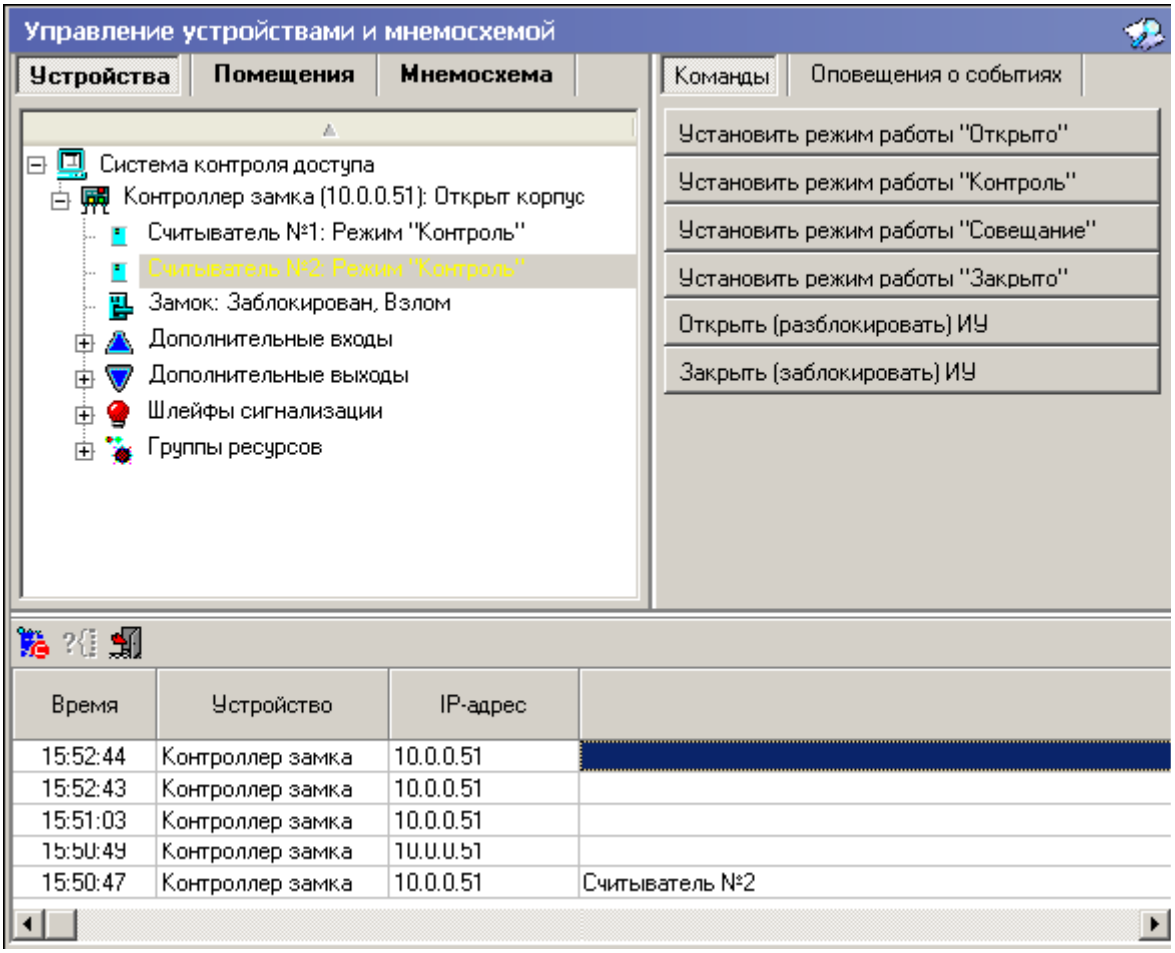
Отличительной особенность единой системы безопасности PERCo-S-20 является то, что контроллеры системы самостоятельно сообщают программному обеспечению обо всех событиях, тем самым скорость доставки и отображения информации превосходит аналогичные системы.

Ниже приведена общая информация о возможностях разделов. Информация об интерфейсе пользователя приведена в соответствующих Руководствах пользователя. В

этом документе мы остановимся на ключевых моментах, необходимых при настройке рабочего места.

Управление устройствами

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



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

Табл. 3 Пиктограммы обозначения состояния устройства

Устройство системы	Название состояния	Мнемосхема	Событие	Примечания
Контроллер	Нормальное состояние			
	Авария питания	П	Авария питания	Авария питания на контроллере, на котором появился знак аварии питания
	Тревога		Тревога	Тревога на контроллере, на котором появился знак тревоги
	Корпус открыт	К	Корпус контроллера открыт	Корпус контроллера, на котором появился знак открытия контроллера, открыт
	Неисправность	Н	Ошибка принятого сообщения	Тревога на контроллере, на котором появился знак тревоги
Считыватель	Режим работы «Открыто»		Изменение режима доступа по команде оператора	Режим доступа «Открыто»
	Режим работы «Контроль»		Изменение режима доступа по команде оператора	Режим доступа «Дневной»
	Режим работы «Совещание»		Изменение режима доступа по команде оператора	Режим доступа «Конференция»
	Режим работы «Закрыто»		Изменение режима доступа по команде оператора	Режим доступа «Ночной»
	Режим работы «Охрана»		Изменение режима доступа на режим доступа «Охрана»	Режим доступа «Охрана»

Устройство системы	Название состояния	Мнемосхема	Событие	Примечания
	Запрет прохода по карте		Предъявление карты / Запрет прохода	Идентификатор не зарегистрирован Идентификатор запрещён Идентификатор из «стоп-листа» Идентификатор просрочен Нарушение комиссионирования Нарушение РКД Несоответствие временным критериям доступа Несоответствие текущему местоположению Несоответствие временным критериям доступа и текущему местоположению
ИУ	Разблокирован		Исполнительное устройство разблокировано	Исполнительное устройство на контроллере, на котором появляется знак разблокировки ИУ, разблокировано
	Заблокирован		Исполнительное устройство заблокировано	Исполнительное устройство на контроллере, на котором появляется знак блокировки ИУ, заблокировано
	Не заблокирован после прохода		Исполнительное устройство не закрыто после прохода от ДУ	Исполнительное устройство, на котором появляется знак разблокировки ИУ, разблокировано
	Взлом		Несанкционированный проход через исполнительное устройство (взлом ИУ)	
	Взят на охрану		«Взят» на охрану	Ресурс ИУ
	Тревога		«Нарушение» ресурса, состояние «Тревога»	Ресурс ИУ

Устройство системы	Название состояния	Мнемосхема	Событие	Примечания
Вход	Активизирован		Активизация входа	Активируется вход на контроллере, на котором появляется знак активизации входа
	Нормализован		Нормализация входа	Нормализуется вход на контроллере, на котором появляется знак нормализации входа
	Взят на охрану		«Взят» на охрану	Ресурс дополнительный вход
	Тревога		«Нарушение» ресурса, состояние «Тревога»	Ресурс дополнительный вход
Выход	Активизирован		Активизация выхода	Активируется выход на контроллере, на котором появляется знак активизации выхода
	Нормализован		Нормализация выхода	Нормализуется выход на контроллере, на котором появляется знак нормализации выхода
ШОС	Неисправен		Неисправность снятого шлейфа сигнализации (ШС)	На шлейфе сигнализации (ШС) существует неисправность, требующая исправления
	Нормализован		Нормализация снятого ШС	Нормализуется шлейф сигнализации на контроллере, на котором появляется знак нормализации ШС
	Взят на охрану		«Взят» на охрану	Ресурс ШС
	Тревога		«Нарушение» ресурса, состояние «Тревога», то есть ресурс был взломан, был совершен несанкционированный проход	Ресурс ШС
Группа ресурсов	Без названия			

Устройство системы	Название состояния	Мнемосхема	Событие	Примечания
	Взята на охрану		Группа ресурсов взята на охрану по идентификатору Группа ресурсов взята на охрану по идентификатору с подтверждением Группа ресурсов взята на охрану по команде оператора	
	Невзятие на охрану		Невзятие группы ресурсов	Нарушение состояния ресурса ИУ
	Тревога		Тревога	
			Нет связи — для всех устройств, как в деревьях,	
Извещатели	Пожар		Извещатель АУ перешел в состояние "Пожар"	
	Блокирован		Извещатель АУ блокирован	
	Разблокирован		Извещатель АУ разблокирован	
	Неисправность		Любая неисправность	
Панели				
Драйвер шлейфа				
	УПА запущена		Пуск УПА (установка пожаротушения автоматическая)	
	Взят на контроль		Адресный шлейф взят на контроль	
Общие для драйвера и панели	Открыт корпус		Корпус контроллера открыт	

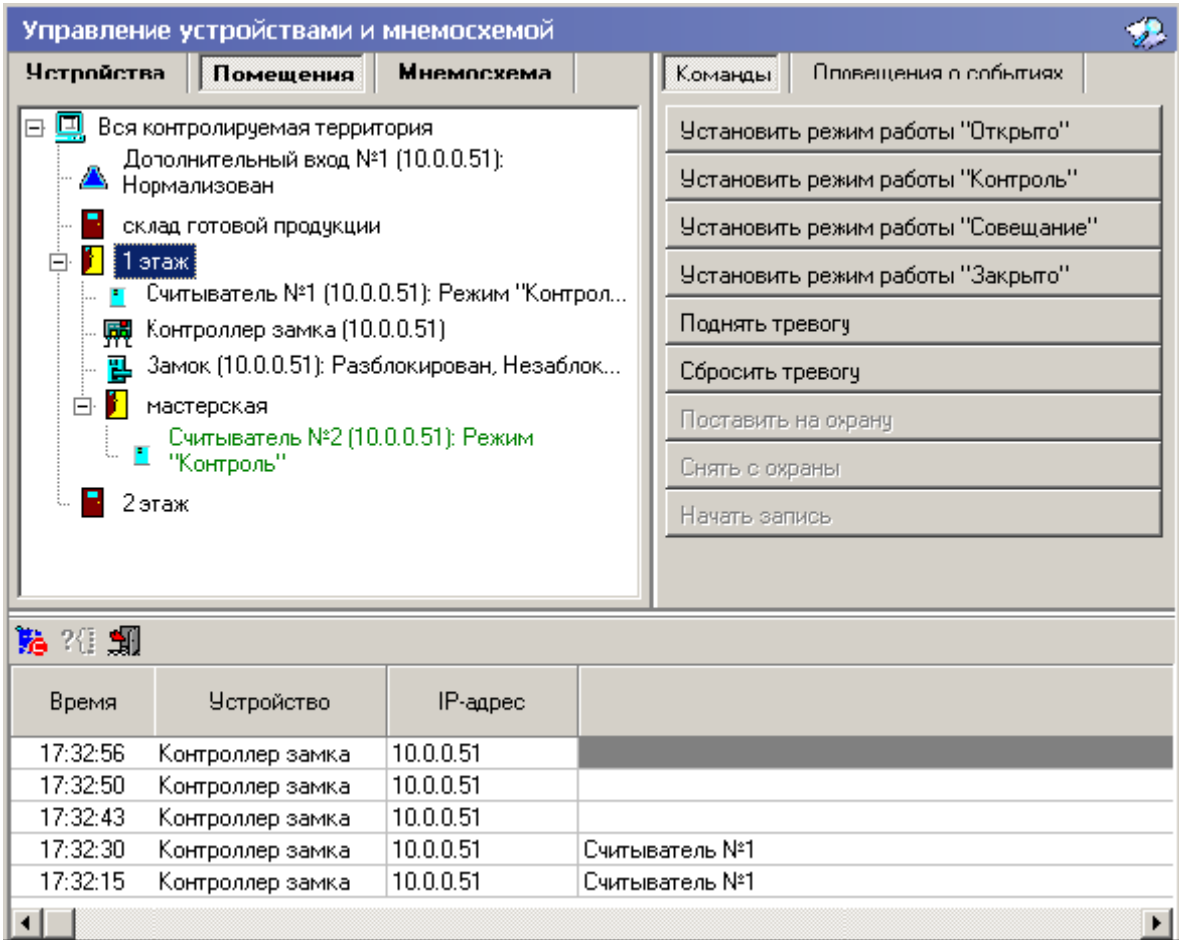
Устройство системы	Название состояния	Мнемосхема	Событие	Примечания
	Неисправность	Н	Любая неисправность	
	Авария питания	П	Переход на резерв ИП. Разряд батареи ИП. Неисправность ИП	
Доп. выходы драйвера и панелей	Активизирован		Активизация выхода	
	Нормализован		Нормализация выхода	
Доп. входы драйвера	Активизирован		Активизация входа	
	Нормализован		Нормализация входа	

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 дереве объектов доступа.

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

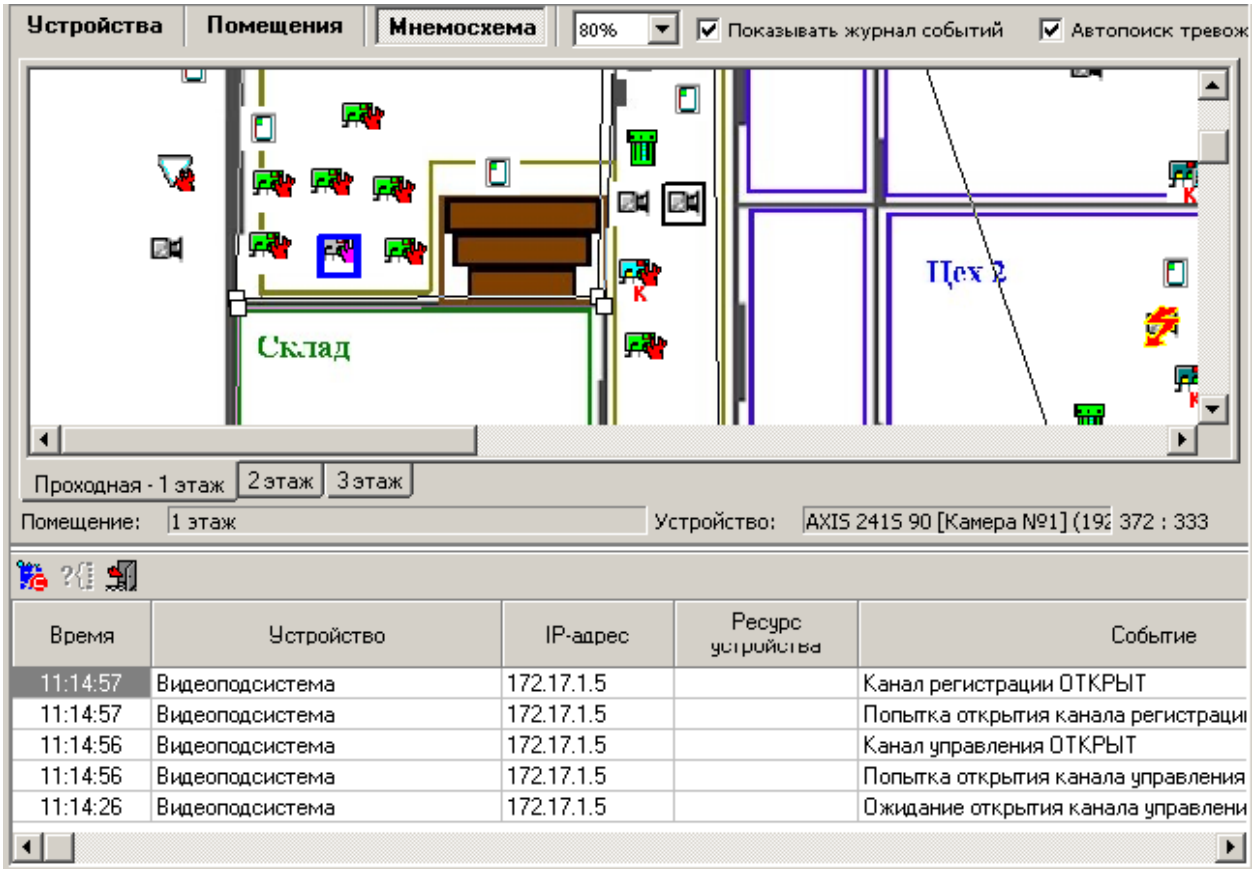


При выборе такого варианта отображения в дереве объектов доступа отображаются только те устройства, которые были установлены и размещены в конкретных помещениях. Соответственно при отображении информации о состоянии устройств автоматически отображается помещение, в котором произошло то или иное событие.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

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

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.

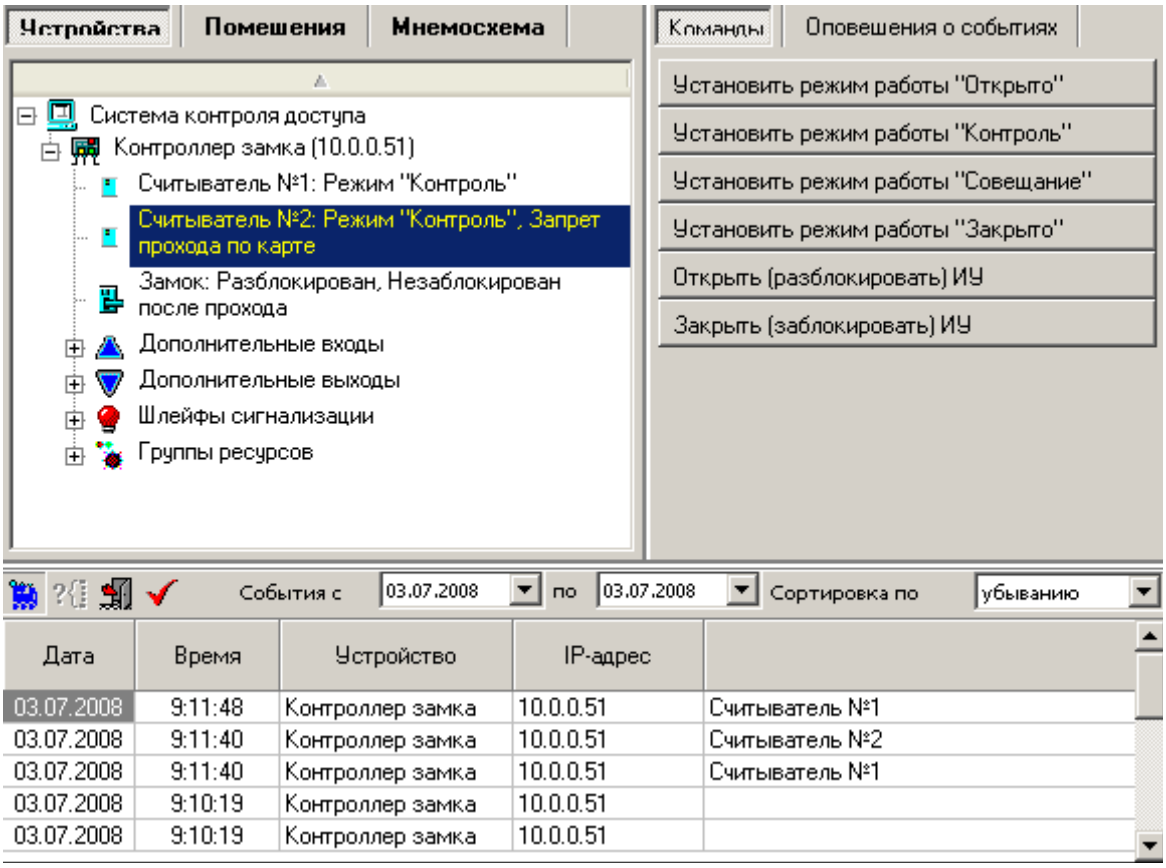
Просмотр событий мониторинга

При работе системы безопасности может возникнуть необходимость в просмотре зарегистрированных событий мониторинга. Это может быть необходимо для проведения служебных расследований, проведение пусконаладочных работ и так далее.

Для просмотра событий необходимо остановить работу модуля «Мониторинг и управление», в противном случае вновь поступающие события не дадут возможности просмотреть ранее полученные данные.

Для остановки работы раздела необходимо воспользоваться кнопкой **Остановить мониторинг** —  .

После ее нажатия раздел **Управление устройствами и мнемосхемой** примет следующий вид:



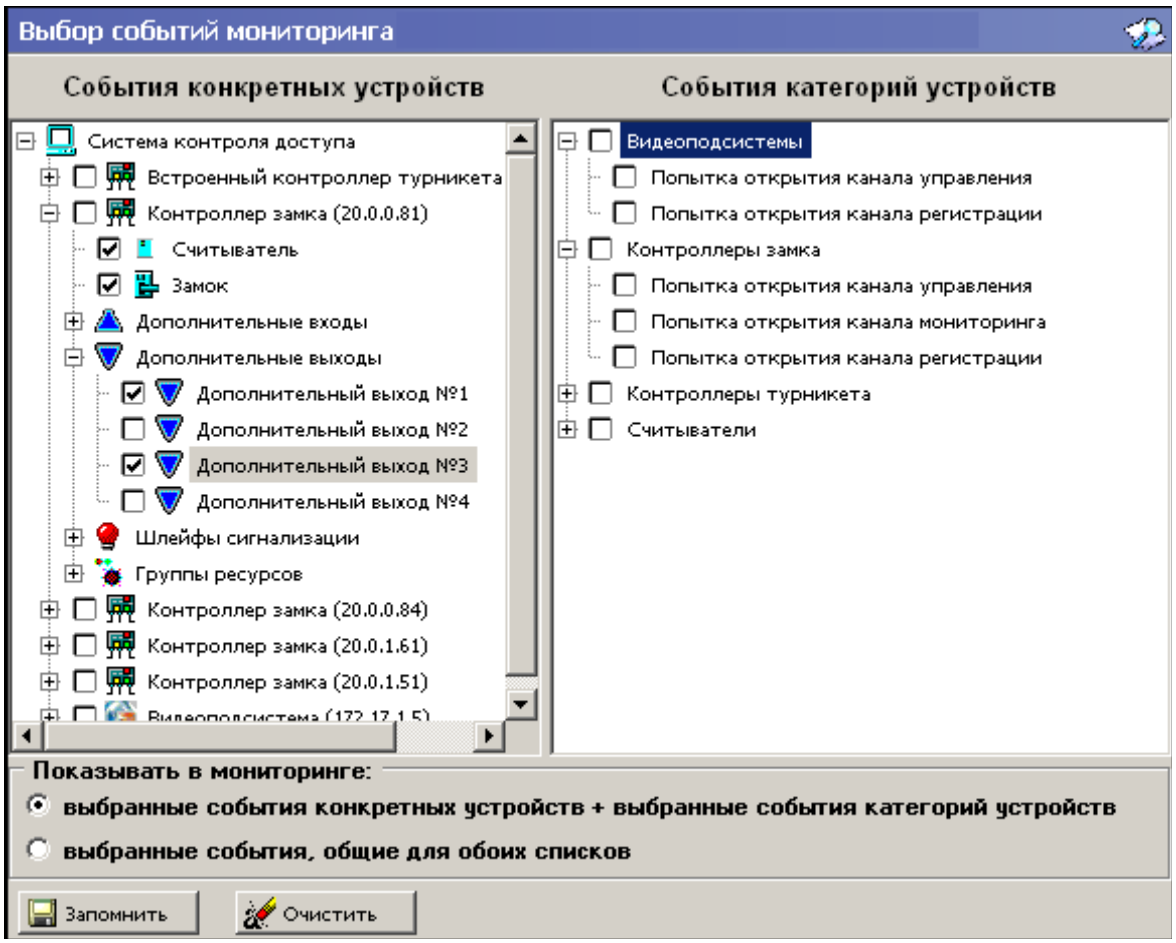
Теперь выберите события мониторинга за интересующий вас период, воспользовавшись двумя выпадающими календарями и отсортируйте события по возрастанию или убыванию.

Для обеспечения более сложных выборок по устройствам и/или типу зарегистрированных событий воспользуйтесь модулем «Выбор событий и устройств мониторинга», подробная информация по которому приведена в данном руководстве.

Выбор событий мониторинга

Как правило, в зависимости от задач и сложности системы безопасности предприятия каждый из постов охраны наблюдает за определенной частью предприятия. Соответственно для уменьшения информационной нагрузки на сотрудников охраны необходимо иметь возможность контролировать процесс поступления информации на каждый пост охраны.

Для определения типа событий и устройств, информация о которых отображается на каждом конкретном посту охраны, предназначен раздел **Выбор событий мониторинга.**



ПРИМЕЧАНИЕ

Условия выбора конкретных устройств и типов событий сохраняются локально на каждом рабочем месте. Это позволяет гибко настраивать работу постов охраны.

В левой части окна необходимо выбрать те контроллеры, информация о которых должна отображаться на данном рабочем месте сотрудников охраны. В правой части окна можно так же выбрать те события, которые должны отображаться на этом рабочем месте. Таким образом, можно точно указать какие именно события и каких устройств будут отображаться на посту охраны.

После завершения работы необходимо сохранить введенные данные. Для этого необходимо воспользоваться кнопкой **Запомнить**.

ЦЕНТРАЛЬНЫЙ ПОСТ ОХРАНЫ

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.

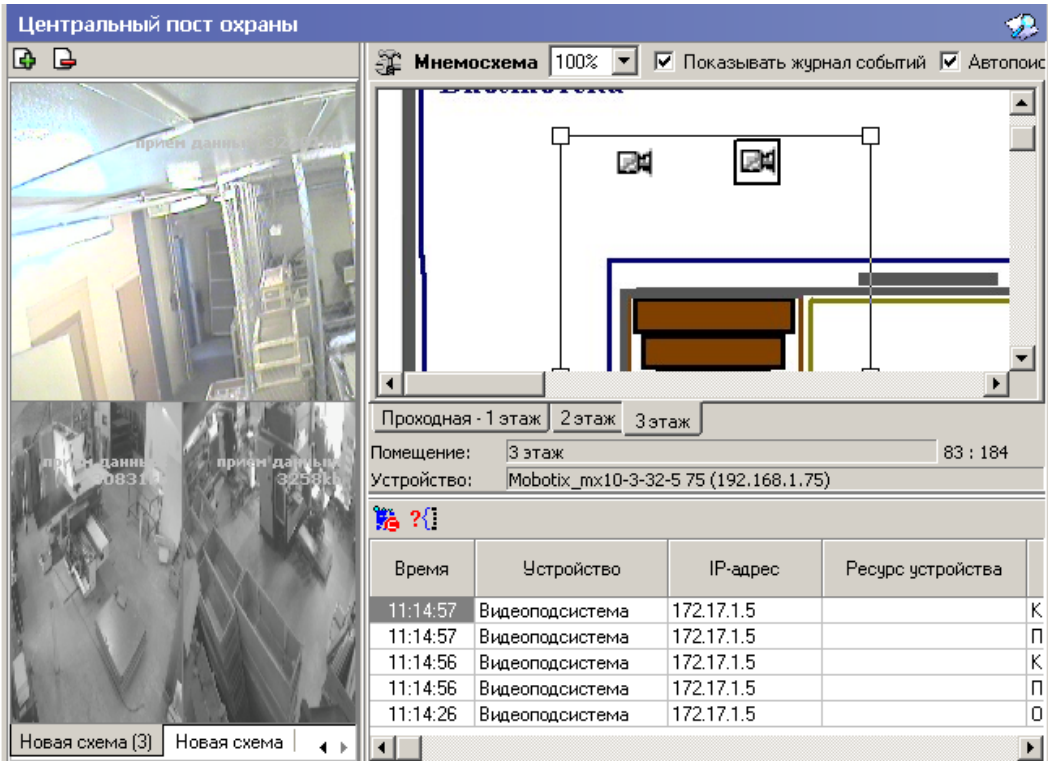
Выше было приведено описание раздела **Выбор событий мониторинга,** позволяющего организовать рабочее место работника службы безопасности.

В этой главе будет описан раздел **Центральный пост охраны,** позволяющий не только отображать информацию о состоянии объектов системы, но так же информацию с видеокамер, входящих в подсистему видеонаблюдения. Для управления объектами системы безопасности предназначены их графические представления на мнемосхеме предприятия.

Кроме стандартных функций управления объектами системы, отображения информации об их состоянии, отображении видеоинформации, программное обеспечение раздела **Центральный пост охраны** позволяет оператору системы принимать решения о разрешении/запрещении доступа, постановке/снятия с охраны на особо важных объектах.

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. Используя это обстоятельство, раздел **Центральный пост охраны** позволяет автоматически отображать видеоинформацию с камер наблюдения, установленных в месте возникновения тревожной ситуации.

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

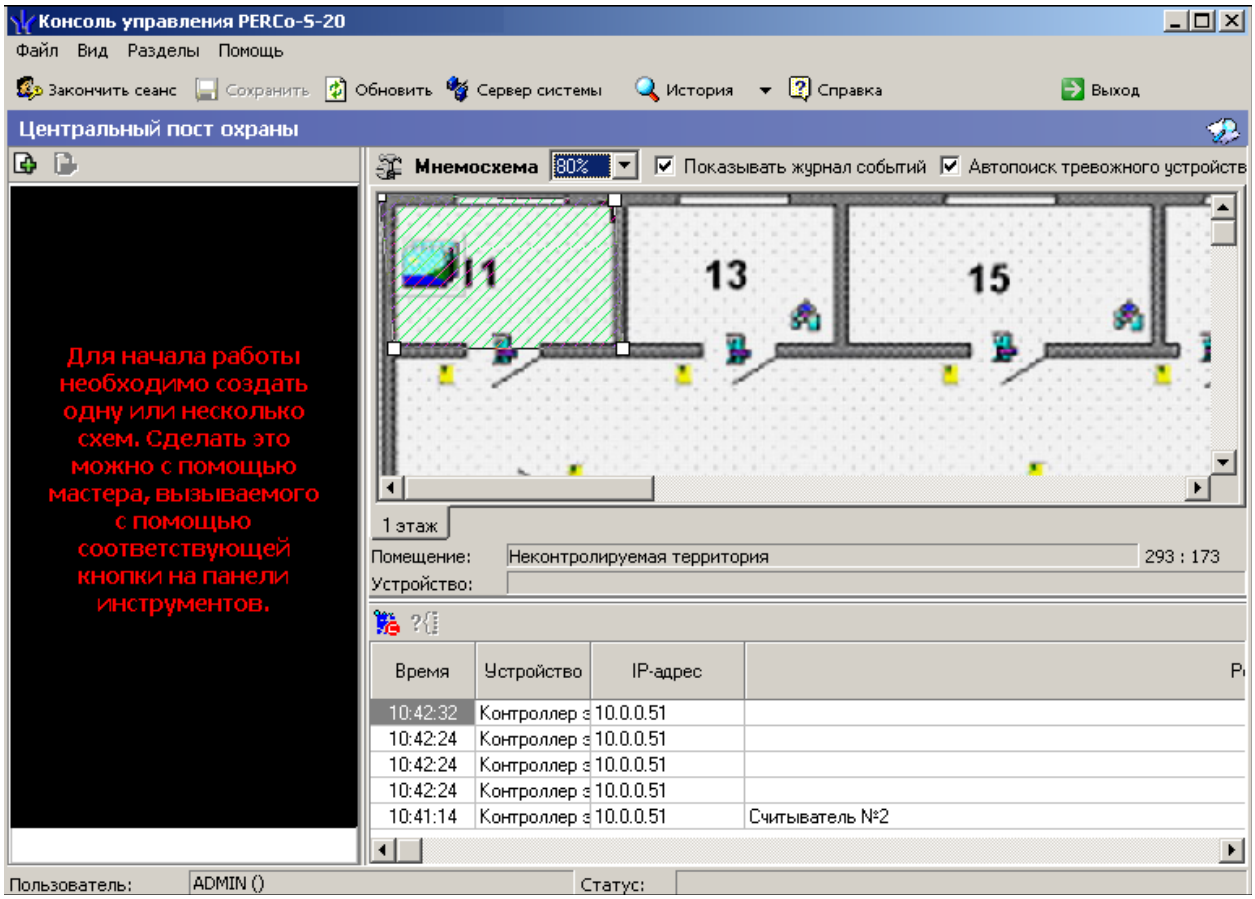


Для организации рабочего места необходимо:

1. Создать мнемосхемы контролируемой территории.
2. Разместить на них устройства системы безопасности.
3. Разместить на мнемосхемах камеры видеонаблюдения.
4. Определить каким образом участки контролируемой территории будут контролироваться на каждом рабочем месте.
5. Определить на каком рабочем месте будет осуществляться работа модуля.
6. Проверить наличие связи (прохождение IP пакетов) между выбранным рабочим местом и компьютером, на котором установлен сервер системы, контроллерами, точки доступа которых будут контролироваться, и видеокамерами, информация с которых будет сопоставлена выбранным точкам доступа.
7. Провести инсталляцию раздела **Центральный пост охраны** на выбранном компьютере.
8. Описать конфигурацию раздела **Центральный пост охраны**.

Конфигурация модуля

При первом запуске раздел имеет следующий вид:



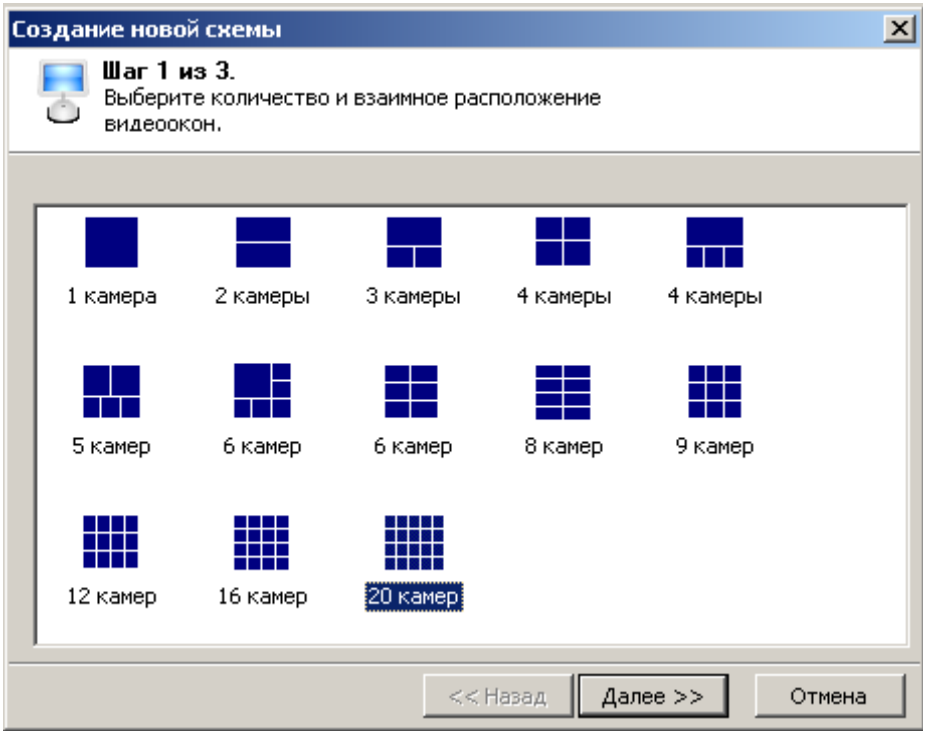
Он состоит из трех окон:

- **Мнемосхема предприятия** – графическое представление планов контролируемой территории с размещенными на них объектами системы безопасности.

- **Журнал событий** – представленные в табличном виде события мониторинга, зарегистрированные системой.
- **Окно отображения видеоинформации** – окно, предназначенное для отображения видеоинформации с выбранных камер видеонаблюдения, а так же автоматического отображения видеоинформации с камер, расположенных в месте возникновения тревожной ситуации.

Конфигурация видеонаблюдения

Для создания новой конфигурации окна отображения видео необходимо воспользоваться кнопкой **Мастер создания новой схемы** —  . При этом появится следующее диалоговое окно:

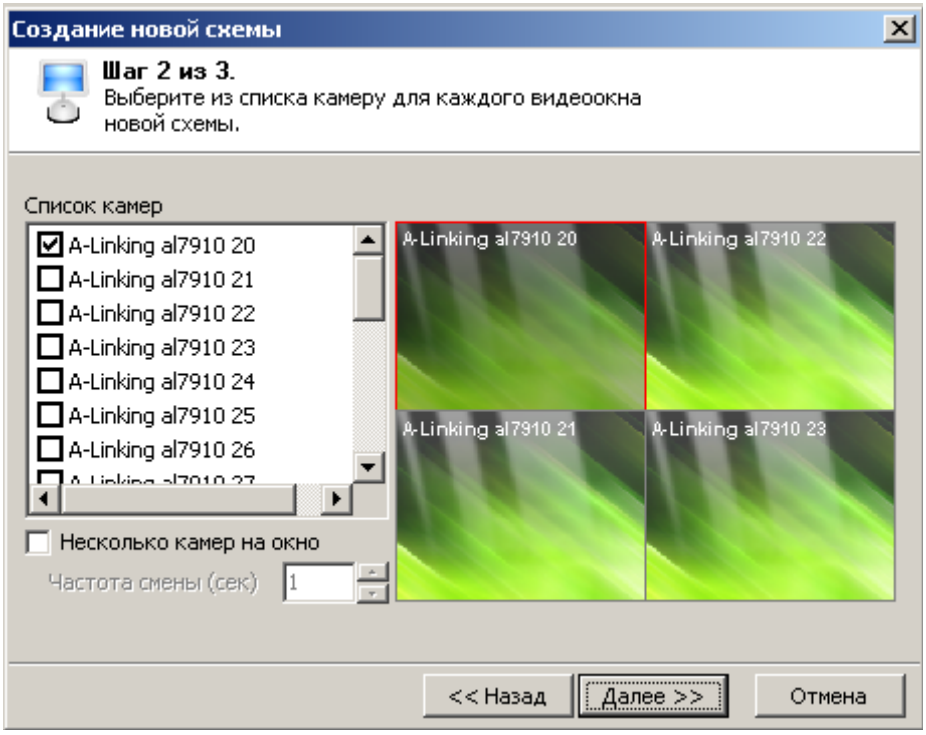


В этом диалоговом окне вы должны выбрать одну из предлагаемых схем расположения окон отображения видеоинформации, в зависимости от количества камер видеонаблюдения которые должны отображаться.

ПРИМЕЧАНИЕ

Максимальное количество камер в одной схеме равно 20.

Выбрав схему расположения камер необходимо нажать на кнопку **Далее**:

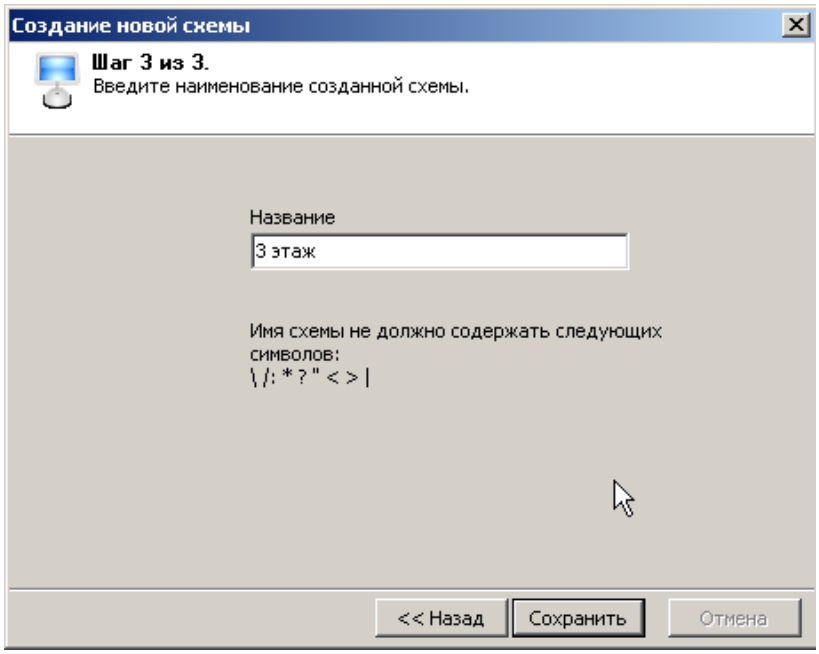


На этом шаге создания схемы отображения укажите, какие именно камеры видеонаблюдения будут отображаться в создаваемой схеме.

Для этого при помощи мыши выделить нужное окно на схеме (выбранное окно имеет красную рамку) и выбрать нужную камеру из раскрывающегося списка, расположенного в верхней части окна:

Для этого при помощи мыши выделите нужное окно вывода на схеме (выбранное окно имеет красную рамку) и отметьте нужную камеру в списке слева. Отметкой флажка **Несколько камер на окно** можно задать смену вывода изображений с нескольких камер в одном окне. Камеры будут меняться с частотой, введенной в поле **Частота смены**.

После окончания выбора камер видеонаблюдения необходимо нажать на кнопку **Далее**:



В появившемся диалоговом окне необходимо задать название схемы. Задаваемое название будет отображаться в нижней части окна модуля «Центральный пост охраны» в качестве заголовка закладки:

При необходимости создания нескольких схем, описанные выше действия необходимо повторить.

Конфигурация верификации

Раздел **Центральный пост охраны** позволяет организовать рабочее место сотрудника службы безопасности по контролю за входом в особо охраняемые помещения, за нарушениями трудовой дисциплины, правами доступа, доступом посетителей и контролем за фактами постановки/снятия с охраны помещений.

Все действия оператора, информация о фактах предъявления карт доступа, видеоинформация автоматически записываются разделом и доступны для последующего просмотра и анализа.

Для организации рабочего места необходимо:

1. Определить какие точки доступа и в каких ситуациях будут контролироваться разделом **Центральный пост охраны**.
2. Определить на каком рабочем месте будет осуществляться работа модуля.
3. Проверить наличие связи (прохождение IP пакетов) между выбранным рабочим местом и компьютером, на котором установлен сервер системы, контроллерами, точки доступа которых будут контролироваться, и видеокамерами, информация с которых будет сопоставлена выбранным точкам доступа.
4. Провести инсталляцию модуля **Центральный пост охраны** на выбранном компьютере.
5. Описать конфигурацию раздела **Центральный пост охраны**.

ПРИМЕЧАНИЕ

Конфигурация схем работы раздела **Центральный пост охраны** записывается локально на каждом рабочем месте. Таким образом, в случае наличия в системе нескольких рабочих мест необходимо создать конфигурации работы на каждом рабочем месте.

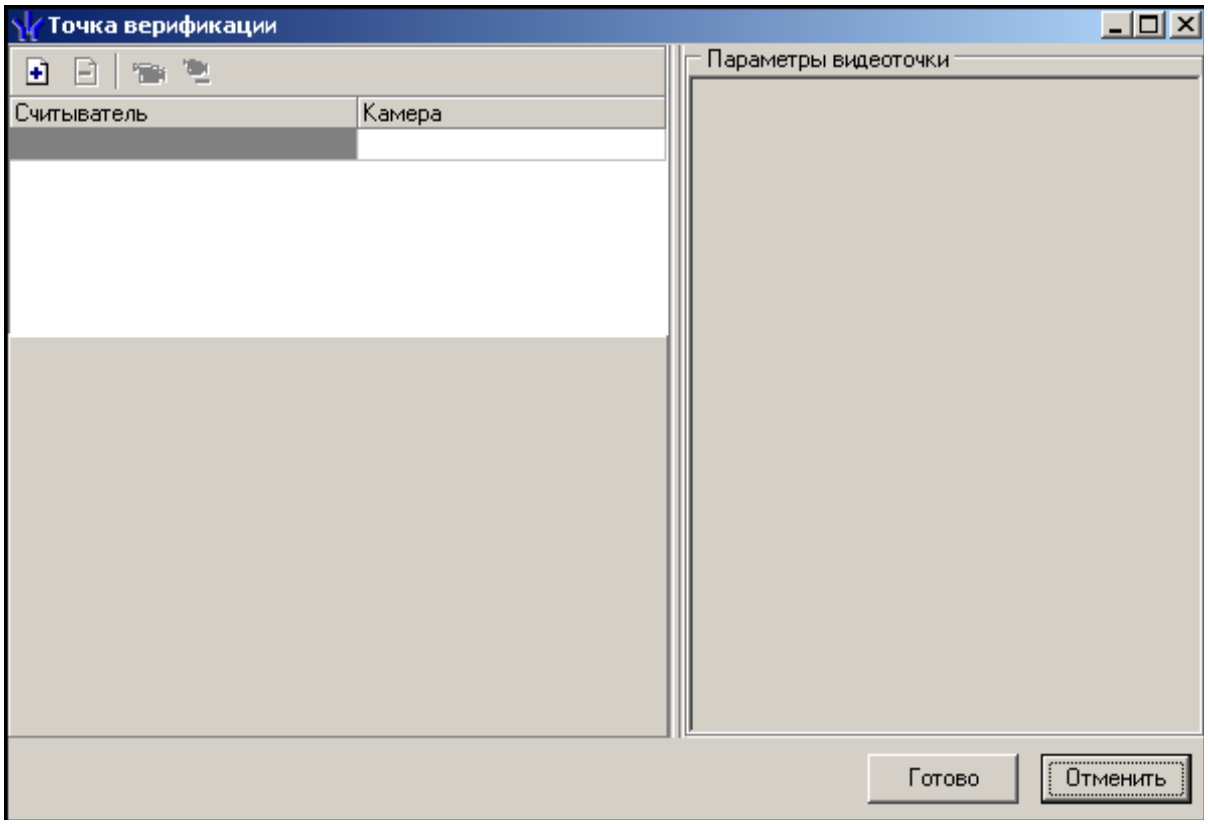
ПРИМЕЧАНИЕ

Контроль за предъявлением карт доступа в режиме верификации для выбранного считывателя может осуществляться только из одного раздела **Центральный пост охраны или Верификация**. Не возможно организовать несколько рабочих мест операторов раздела **Центральный пост охраны или Верификация,** контролирующих одно и то же устройство.

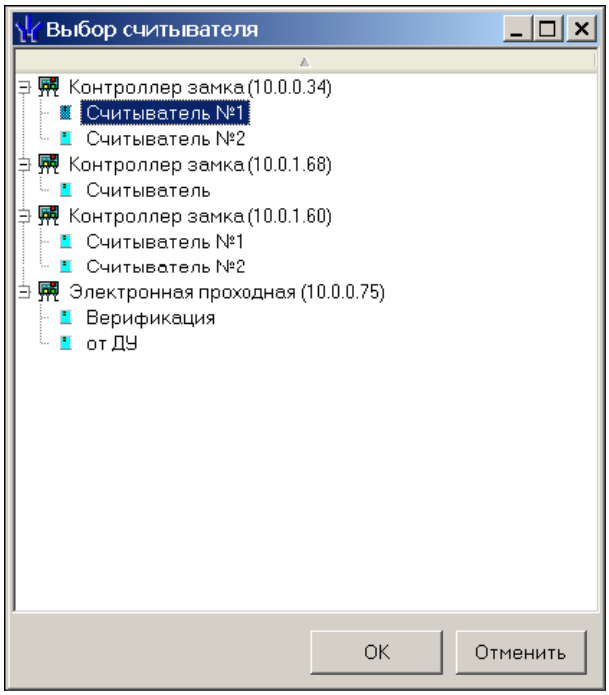
Конфигурация верификации — совокупность точек верификации, каждая из которых состоит из считывателя (обязательный элемент конфигурации) и камеры (если

таковые присутствуют в конфигурации системы безопасности). В конфигурации можно создать не более 8 точек верификации.

Для создания (изменения) конфигурации щелкните на кнопке Верифицируемые считыватели —  . В открывшемся диалоговом окне создайте (измените) список точек верификации:



Для добавления считывателя необходимо нажать на кнопку  . При этом появится следующее диалоговое окно:



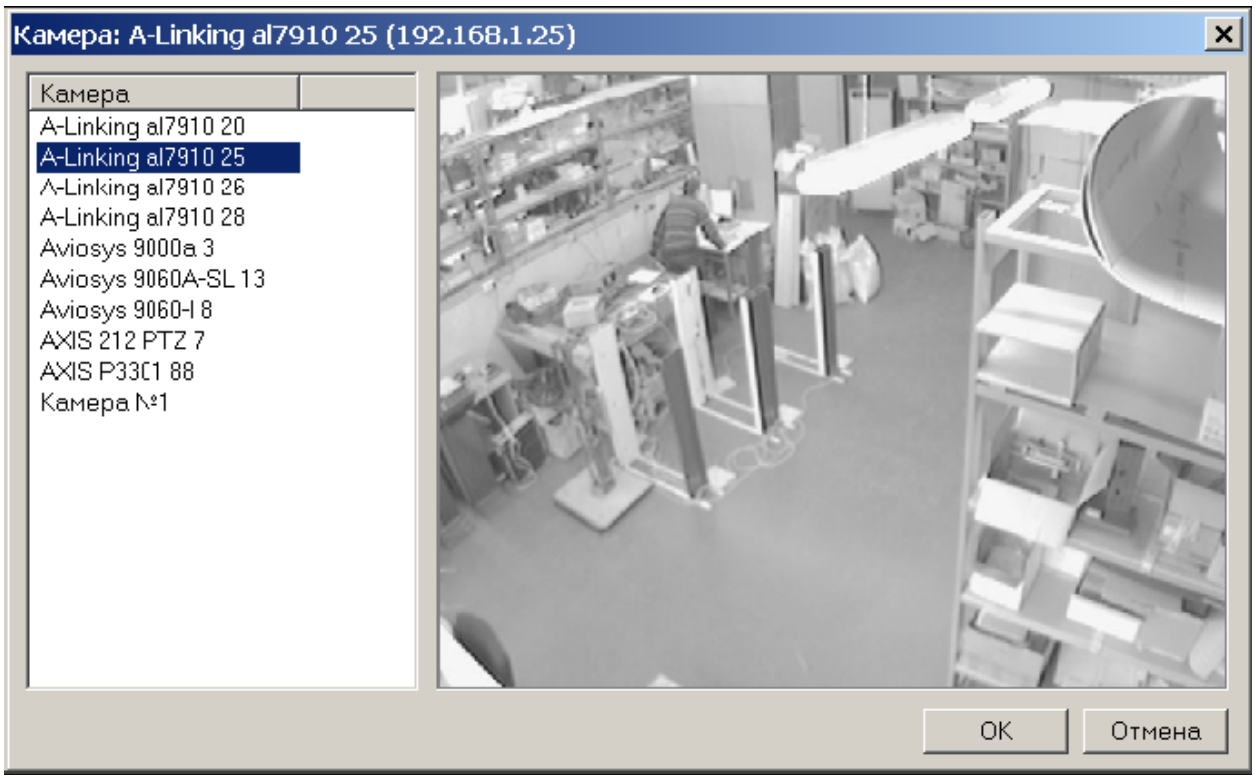
В этом окне вы выбираете тот считыватель, проход через который будет контролироваться создаваемой точкой верификации.

Для удаления точки верификации воспользуйтесь кнопкой  .

После создания точки верификации в нее можно добавить видеокамеру, которая позволит оператору дистанционно контролировать ситуацию в месте установки считывателя.

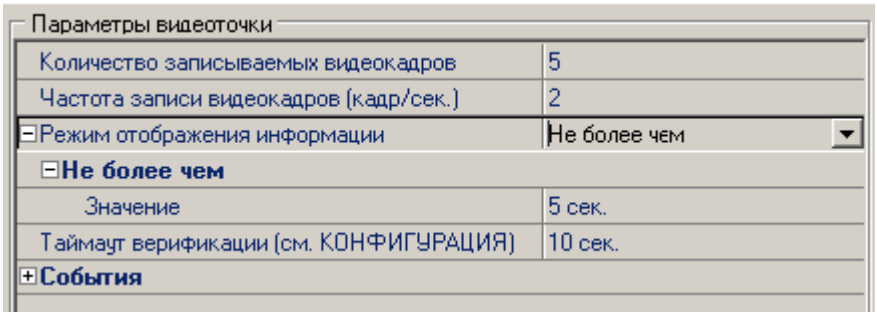
Для этого щелкните на кнопке  , расположенной в графе Камера.

После этого в окне выбора будет отображен список всех видеокамер, входящих в конфигурацию системы безопасности:



Для удобства выбора в правой части окна при выборе камеры автоматически выводится видеоизображение. Для добавления камеры в точку верификацию выберите нужную и воспользуйтесь кнопкой «ОК».

После добавления всех необходимых считывателей и видеокамер укажите, в каких ситуациях и как должен работать раздел при предъявлении карты доступа к каждому из выбранных считывателей. Для этого выберите поочередно каждый из добавленных считывателей и в правой части окна задайте необходимые параметры.



1. **Количество записываемых видеокадров** – параметр, задающий количество записываемых видеокадров с выбранной видеокамеры при предъявлении карты

доступа к выбранному считывателю.

2. **Частота записи видеокадров** – параметр, задающий интервал записи видеокадров.

ПРИМЕЧАНИЕ

Необходимо правильно рассчитывать количество записываемых кадров и их частоту, исходя из частоты и продолжительности проходов, так как указанное количество кадров будет записываться независимо от того, осуществляется или нет следующий проход

3. **Режим отображения информации** – параметр, указывающий в течение какого времени должна в рабочем окне будет отображаться видеоинформация с указанной камеры. Доступны два варианта значения параметра:

a) **Постоянный.** В этом случае в рабочем окне раздела **Верификация** постоянно отображается видеоинформация с выбранной камеры. Вне зависимости от того, была предъявлена карта к выбранному считывателю или нет.

b) **Не более чем**. В этом случае видеоинформация отображается, начиная с момента предъявления карты к считывателю и до истечения времени, указанного в параметре «Значение».

4. **Таймаут верификации** – не изменяемый в данном окне параметр, указывающий время, в течение которого контроллер будет ожидать действий оператора раздела **Верификация**. Значения этого параметра задаются при описании параметров работы выбранного считывателя и описаны в соответствующем разделе данного руководства.

Далее укажите, какие именно события подлежат верификации со стороны оператора раздела **Верификация**. Для этого раскройте параметр «События» выбранного считывателя:

Отслеживание фактов предъявления карт доступа сотрудников описывается в группе «События – Сотрудников». Доступны для отслеживания следующие события, связанные с предъявлением карты сотрудника:

1. **Проход** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем.

2. **Проход с нарушением времени** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемой этим считывателем. При этом время предъявления карты не соответствует временному критерию доступа данной карты.

3. **Проход с нарушением зональности** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем. При этом владелец этой карты нарушил правила «антипасбека», то есть пытается совершить повторный вход в помещение.

4. **Постановка на охрану** – событие, возникающее при попытке постановки помещения на охрану при помощи карты доступа.

5. **Снятие с охраны** – событие, возникающие при попытке снятия помещения с охраны при помощи карты доступа.

Отслеживание фактов предъявления карт доступа посетителей описывается в группе **«События – Посетителей»**. Доступны для отслеживания следующие события, связанные с предъявлением карты посетителя:

1. **Проход** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем.

2. **Проход с нарушением времени** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемой этим считывателем. При этом время предъявления карты не соответствует временному критерию доступа данной карты.

3. **Проход с нарушением зональности** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем. При этом владелец этой карты нарушил правила «антипасбека», то есть пытается совершить повторный вход в помещение.

Отслеживание фактов предъявления карт доступа, не имеющих права на проход через исполнительное устройство, управляемое выбранным считывателем описывается в группе **«События – Уведомляющие события»**. Для отслеживания доступны следующие события:

1. **Идентификатор не зарегистрирован** – событие, возникающее при предъявлении карты доступа, которая не внесена в списки карт системы. То есть эта карта доступа никогда не выдавалась сотрудникам или посетителям предприятия или была выдана, а в последствии была удалена из всех списков.

2. **Идентификатор заблокирован** – возникает в случае предъявления карты доступа, которая была заблокирована. Подробно о блокировке карт доступа смотрите раздел **«*Параметры доступа*»** данного руководства.

3. **Идентификатор из «СТОП - листа»** - событие, возникающее при

предъявлении карты доступа занесенной в стоп лист. Подробно о занесении карты доступа в СТОП – лист смотрите раздел **«*Параметры доступа*»** данного руководства.

4. **Идентификатор просрочен** – событие, возникающее при предъявлении карты доступа с истекшим сроком действия. Подробно о сроке действия карт доступа смотрите раздел **«*Параметры доступа*»** данного руководства.

5. **Нарушение режимов доступа** – событие, возникающее при предъявлении карты доступа в режиме «Закрыто» или в режиме «Охрана» при условии, что данная карта доступа не имеет права на снятие помещения с охраны.

Среди отслеживаемых событий есть два, не связанных с предъявлением идентификатора:

1. **Взлом ИУ** - событие, возникающее при несанкционированном проходе через ИУ.

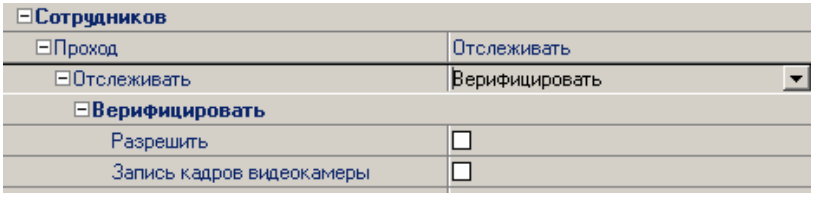
2. **Проход от ДУ** - событие, возникающее при проходе через ИУ после нажатия кнопки ДУ, приводящее к разблокировке ИУ.

Для событий связанных с предъявлением карт доступа сотрудников и посетителей могут быть заданы следующие параметры работы:

- **Не отслеживать** – в этом случае раздел никак не реагирует на предъявление карты доступа.

- **Отслеживать** – в этом случае будет отслеживаться предъявление карты доступа в зависимости от следующих установленных параметров:

✓**Не верифицировать** – при установке этого параметра будет только отображаться информация о владельце предъявленной карты доступа и видеоинформацию с видеокамеры при условии, что она установлена.



✓**Верифицировать** – при установке этого параметра будет отображать информация о владельце предъявленной карты доступа и видеоинформация с видеокамеры при условии, что она установлена. При этом решение о разрешении прохода должен принять оператор, используя кнопку разрешающую или запрещающую проход.

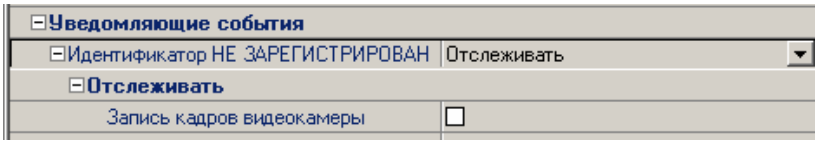
Кроме этого в режиме верификация могут быть установлены следующие параметры:

- **Разрешить** – в этом случае по истечении таймаута верификации раздел автоматически разрешит проход без вмешательства оператора. При этом оператор в течение этого времени может самостоятельно принять нужное для него решение путем нажатия соответствующих кнопок.

- **Запись кадров видеокамеры** – при выборе этого параметра раздел Верификация будет записывать видеоизображение в количестве и с частотой, указанными в параметрах точки верификации.

Для событий представленных в группе «Уведомляющие события» могут быть заданы следующие параметры работы раздела **Верификация**:

- **Не отслеживать** – в этом случае раздел Верификация никак не реагирует на предъявление карты доступа вызвавшей данное событие.



- **Отслеживать** – в этом случае раздел Верификация будет отслеживать предъявление карты доступа вызвавшей это событие, и работать в зависимости от следующих установленных параметров:

- **Запись кадров видеокамеры** – при выборе этого параметра, раздел Верификация будет записывать видеоизображение в количестве и с частотой указанными в параметрах точки верификации.

Для завершения действий по созданию конфигурации раздела **Верификация** нажмите на кнопку **Готово**.

Управление

Управление устройствами в разделе **Центральный пост охраны** осуществляется аналогично разделам **Управление устройствами** и **Мнемосхема**.

Управление отображением видеоинформации осуществляется следующими способами

1. Переключение между схемами отображения видеоинформации.
2. Двойной щелчок левой клавишей мыши на пиктограмме нужной камеры видеонаблюдения расположенной на мнемосхеме территории. При этом изображение с этой камеры автоматически выводится во вновь созданном окне просмотра видеоизображения.

Автоматически при регистрации тревожного события в помещении (пожар, тревога по нарушению охранных датчиков). При этим изображение с видеокамер установленных в месте возникновения тревоги автоматически выводится в окне отображения видеоинформации.

УПРАВЛЕНИЕ СЕРВЕРАМИ

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

 — для управления сервером системы PERCo-S-20 и сервером баз данных (Рис. 1).

 — для управления видеосервером системы PERCo-S-20 (Рис.) при условии приобретения хотя бы одного из разделов: **Прозрачное здание**, **Видонаблюдение**, **Верификация/Идентификация.**

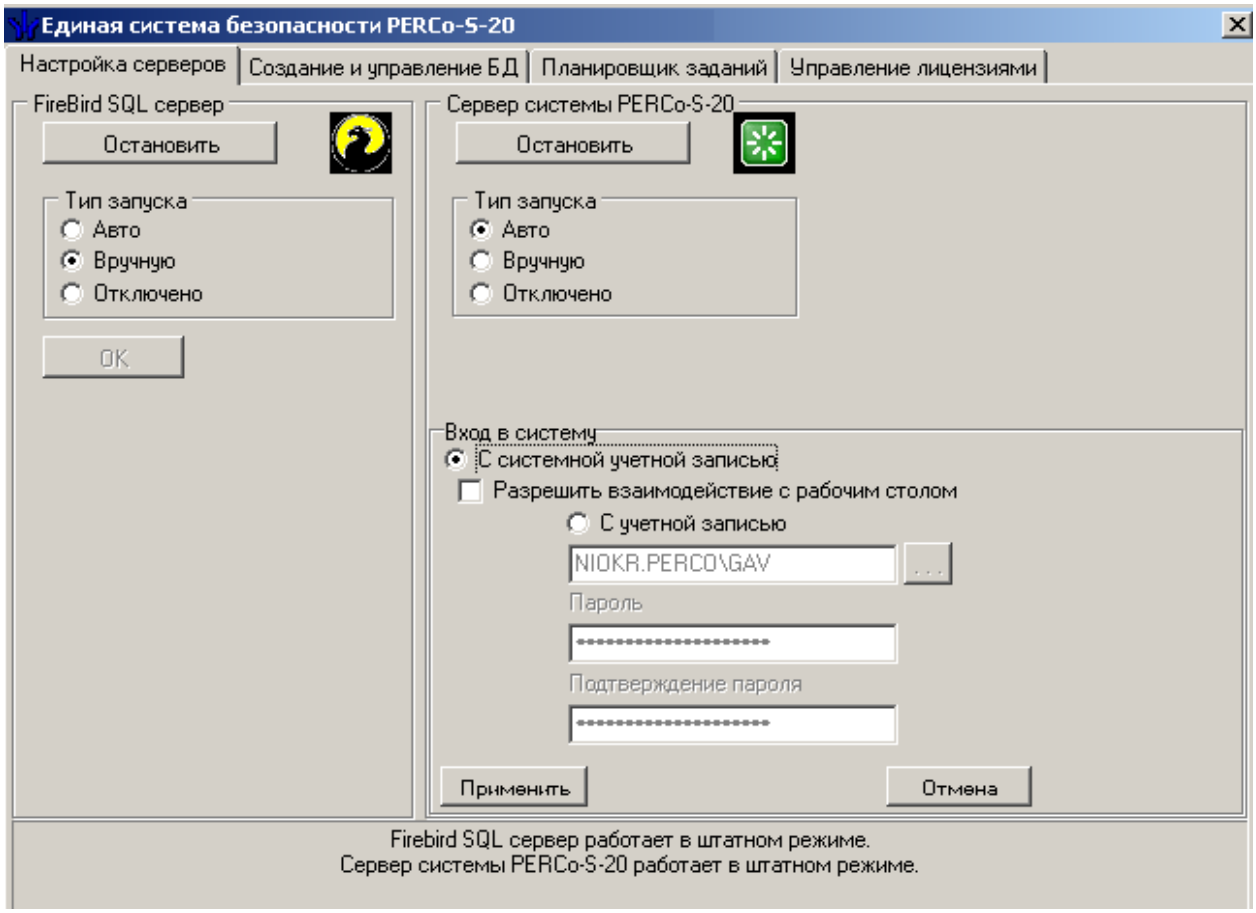


Рис. 5. Центр управления серверами системы PERCo-S-20

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).

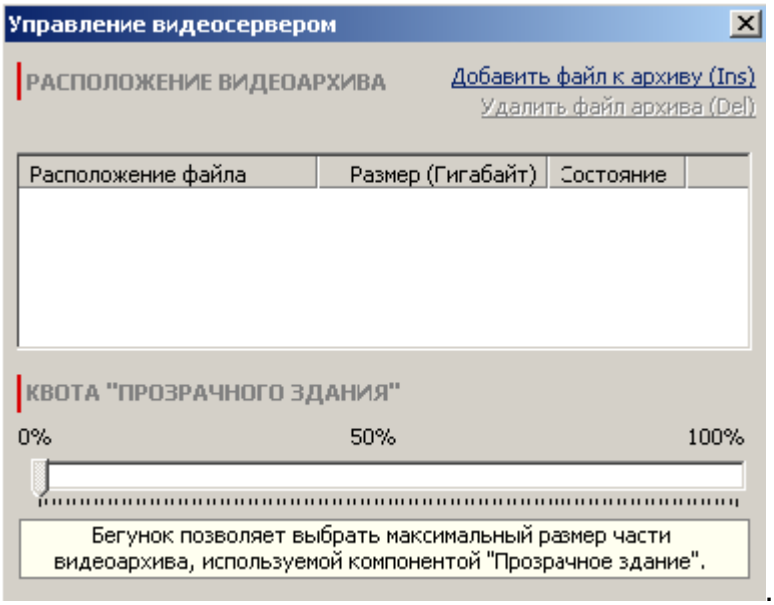
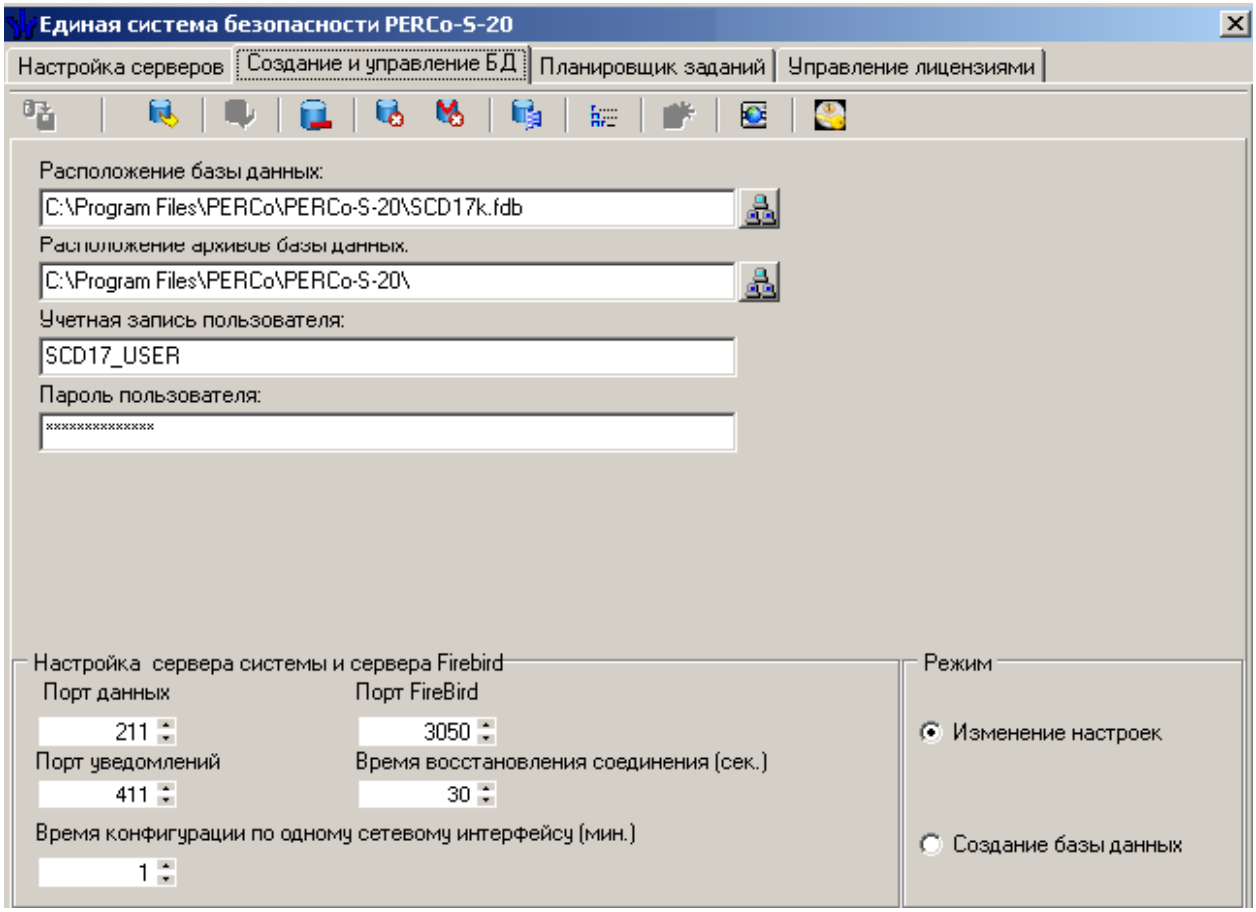


Рис. 6. Управление видеосервером

База данных

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.

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



1. **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.

2. **Расположение архивов базы данных.** В этой строке указывается путь к каталогу, в котором будут размещаться архивные копии базы данных. Правила ввода пути аналогичны предыдущим.

3. **Учетная запись пользователя.** Этот параметр задает имя пользователя, от которого будет осуществляться доступ к файлу базы данных.

4. **Пароль пользователя.** Этот параметр задает пароль пользователя, от имени которого будет происходить обращение к файлу базы данных.

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

6. **Время восстановления (сек.)** - время, через которое Сервер системы попытается восстановить связь с любым контроллером системы в случае ее неожиданной потери.

7. **Время конфигурации по одному сетевому интерфейсу (мин.)** – предельный минимум времени, отведенный на конфигурацию по одному адресу и маске подсети. Пользователь может изменить его по своему усмотрению, но значение не может быть меньше предопределенного (1 мин).

Создание базы данных

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

Убедитесь (см. Рис. 1), что Firebird SQL Server и Сервер системы запущены. Информация об этом расположена в нижней части окна.

Для создания базы данных перейдите на вкладку **Создание и управление БД** (Рис. 3):

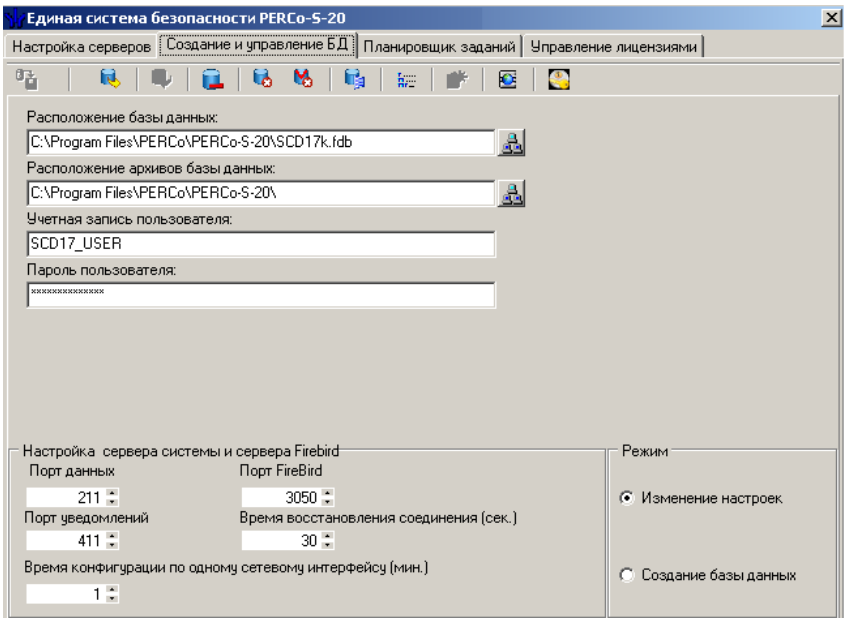


Рис. 7 Создание и управление БД

Выберите режим работы **Создание базы данных**. Заполните соответствующие поля (Рис. 7).

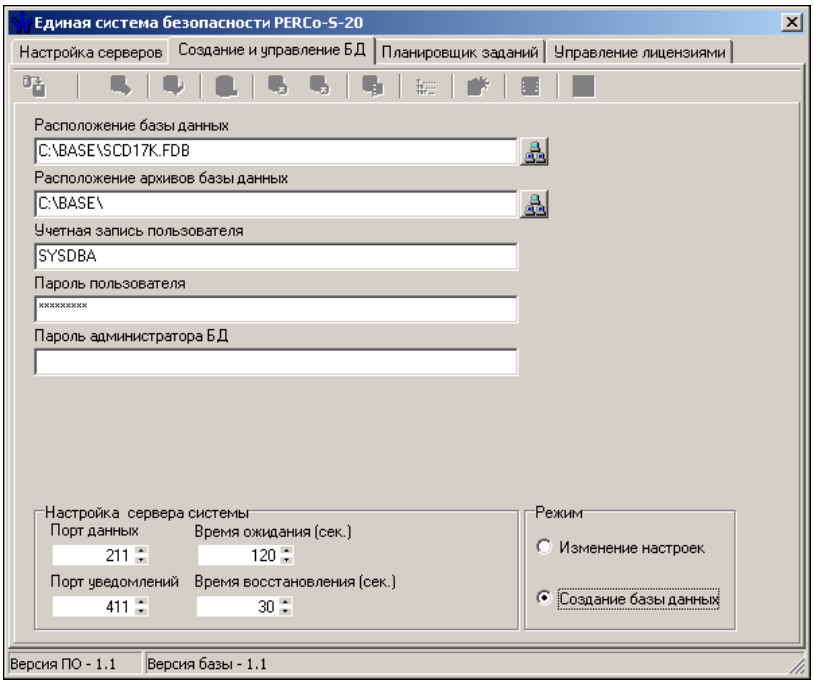


Рис. 8 Создание базы данных

Заполните параметры базы данных:

1. Укажите путь к тому месту, где будет создан файл базы данных. Это путь к компьютеру, где был ранее установлен SQL-сервер Firebird 2.0. Папку, в которой вы создаете файл базы данных, для повышения безопасности не рекомендуется предоставлять в общее пользование. Если база находится на том же компьютере, что и сервер управления, вы можете выбрать путь с помощью кнопки  , если нет, то кнопка будет неактивной, и вы должны ввести путь вручную.

2. Укажите путь к архиву базы данных. Это путь к директории, где будут создаваться архивные копии файла базы данных. Имя самого файла базы данных и архива лучше не изменять. Имя директории может вводиться вручную (тогда это директория на компьютере, где находится SQL-сервер) или выбираться нажатием на кнопку  . В этом случае можно выбирать директорию, к которой предоставлен общий доступ с любого компьютера сети. Если SQL-сервер запущен как сервис, то данному сервису должен быть предоставлен полный доступ к директории. Если SQL-сервер запущен как приложение, то учетной записи, под которой он запущен, должны быть предоставлены права на директорию.

3. Введите имя пользователя, который будет создателем и владельцем файла базы данных (оставьте предопределенное).

4. Введите пароль пользователя для доступа к БД (оставьте предопределенный).

ПРИМЕЧАНИЕ

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

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

После создания базы можно работать с любым разделом программного обеспечения системы PERCo-S-20. Поля данных на вкладке заполнятся введенными параметрами. И станут доступными следующие элементы управления (Рис. 9):

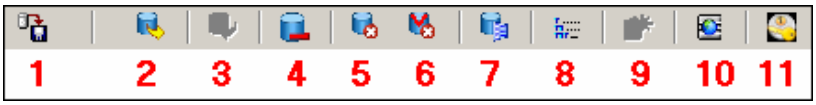


Рис. 9. Элементы управления базой данных

1 — Сохранение настроек базы данных

2 — Сохранение базы данных оптимизация и проверка целостности (см. *«Сохранение базы данных»*)

3 — Восстановление БД

4 — Удаление данных мониторинга

5 — Удаление данных по событиям

6 — Удаление данных по видеоидентификации

7 — Настройки сервера БД

8 — Оптимизация индексов

9 — Создание базы данных

10 — Обновление версии базы данных

11 — Восстановление предыдущего пароля устройств

Сохранение настроек базы данных

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

Сохранение базы данных

При нажатии на кнопку **Сохранение базы данных** — происходит создание полной резервной копии базы данных. Выбор места расположения резервной копии БД определяется на этапе создания (см. «***Создание базы данных***»). Однако резервные копии БД можно делать и в другом месте. Для внесения изменений необходимо произвести следующие действия:

1. Выбирается имя компьютера, на котором установлен Сервер БД, т.е. указывается имя компьютера, где расположен SQL-сервер Firebird 2.0.

2. Вводится путь к файлу базы данных. Необходимость менять путь к базе может возникнуть при переносе базы. Если “Консоль администратора БД” запущена на том же компьютере, где установлен SQL-сервер Firebird 2.0, то Вы можете выбрать путь с помощью кнопки , если нет, то кнопка будет не активна, и Вы должны ввести путь вручную.

3. Указывается директория, в которой сохраняются архивные файлы. Имя директории может вводиться вручную (тогда это директория на компьютере, где находится SQL-сервер) или выбираться нажатием на кнопку . В этом случае

можно выбрать директорию, к которой предоставлен общий доступ с любого компьютера сети (не рекомендуется, т.к. замедляется создание архивов и их восстановление). Рекомендуется иметь второй HDD на компьютере с сервером Firebird и сохранять архивы на диск отличный от диска, где находится БД.

4. Указывается пользователь, от имени которого создается база данных, и его пароль.

Восстановление базы данных из резервной копии

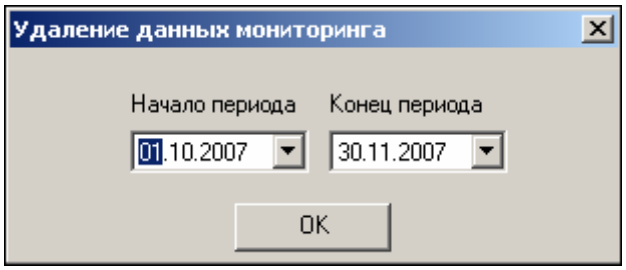
Восстановление данных из архива выполняется при помощи нажатия кнопки **Восстановление базы данных** —  .

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

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

Удаление данных мониторинга

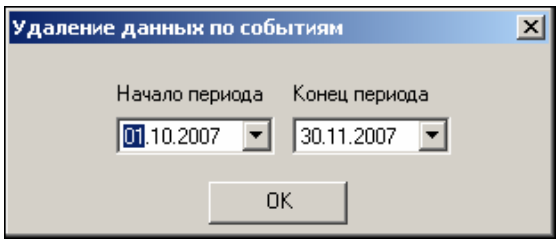
Удаление данных по мониторингу можно выполнить после нажатия кнопки —  :



Эти действия необходимо проводить периодически. Это позволяет уменьшить размер файла базы данных и ускорить работу программных модулей системы безопасности. Мы рекомендуем проводить эти действия один раз в месяц.

Удаление данных о событиях

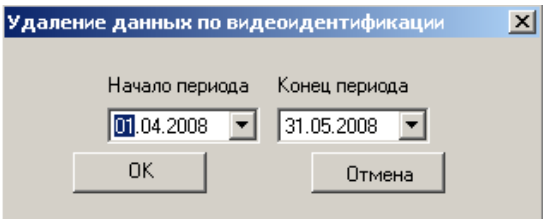
Удаление данных о проходах становится возможным после нажатия кнопки —  :



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

Удаление данных по видеоидентификации

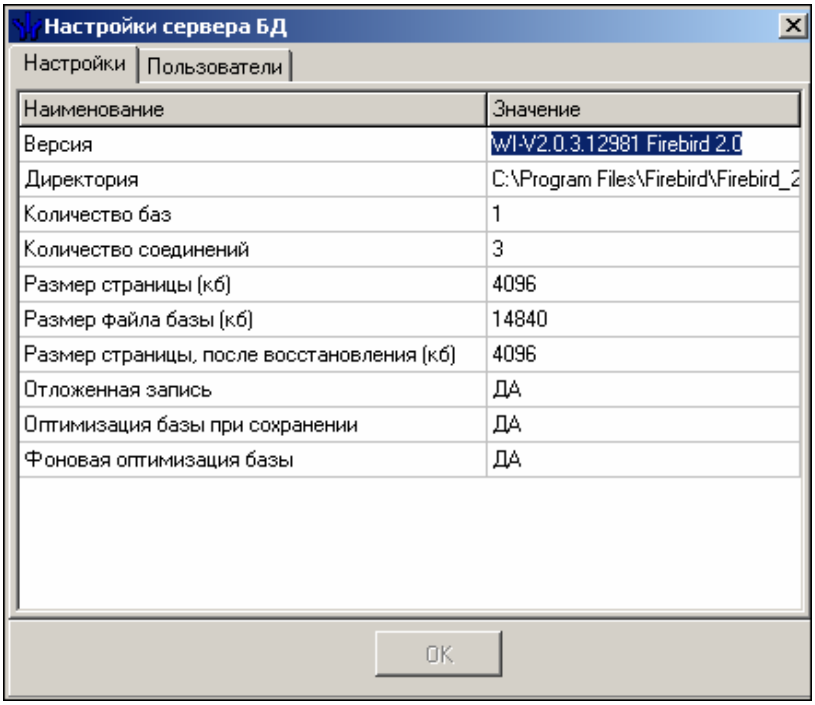
Удаление данных по видеоиндентификации становится возможным после щелчка на кнопке —  :



Эти действия также аналогичны действиям, описанным выше, за исключением того, что удаляются данные верификации, зарегистрированные в системе и записанные в журнале верификации. Рекомендуется проводить эти действия не реже одного раза в квартал, после завершения формирования всех необходимых отчетов за удаляемый период.

Настройки сервера базы данных

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



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

Вкладка **Настройки** включает следующие позиции:

- **Версия** SQL-сервера Firebird, для сведения.
- **Директория** - место установки SQL-сервера Firebird.
- **Количество баз** – информационный параметр.
- **Количество соединений** – информационный параметр.
- **Размер страницы** - по умолчанию файл БД создается с размерами страницы 4096 байт.
- **Размер файла базы** - текущий размер файла базы данных системы PERCo-S-20.
- **Размер страницы, после восстановления** - при восстановлении БД, особенно при переносе на другой носитель, размер страницы может быть не кратным размеру кластера жесткого диска. Поэтому для оптимизации производительности рекомендуется устанавливать его кратным размеру кластера.
- **Отложенная запись** - все изменения, 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», данный параметр, при этом скорость операций с БД уменьшится.
- **Оптимизация базы при сохранении** - данный параметр управляет необходимостью оптимизации БД (см. ниже «Фоновая оптимизация») при сохранении резервной копии БД.
- **Фоновая оптимизация базы** — при работе SQL-сервера создаются разные версии записей. При режиме «Да» они чистятся самим сервером, однако это замедляет его основную деятельность. Следует учесть, что сборка «мусора» происходит при сохранении базы данных, которое рекомендуется делать ежедневно. Поэтому рекомендуется выбирать режим «Нет».

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

Оптимизация индексов базы данных

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

Обновление версии базы данных

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

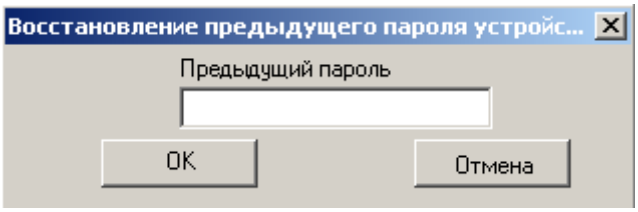
Восстановление предыдущего пароля устройств

Восстановление предыдущего пароля устройств может быть необходимо в следующей ситуации:

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

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

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



ПРИМЕЧАНИЕ

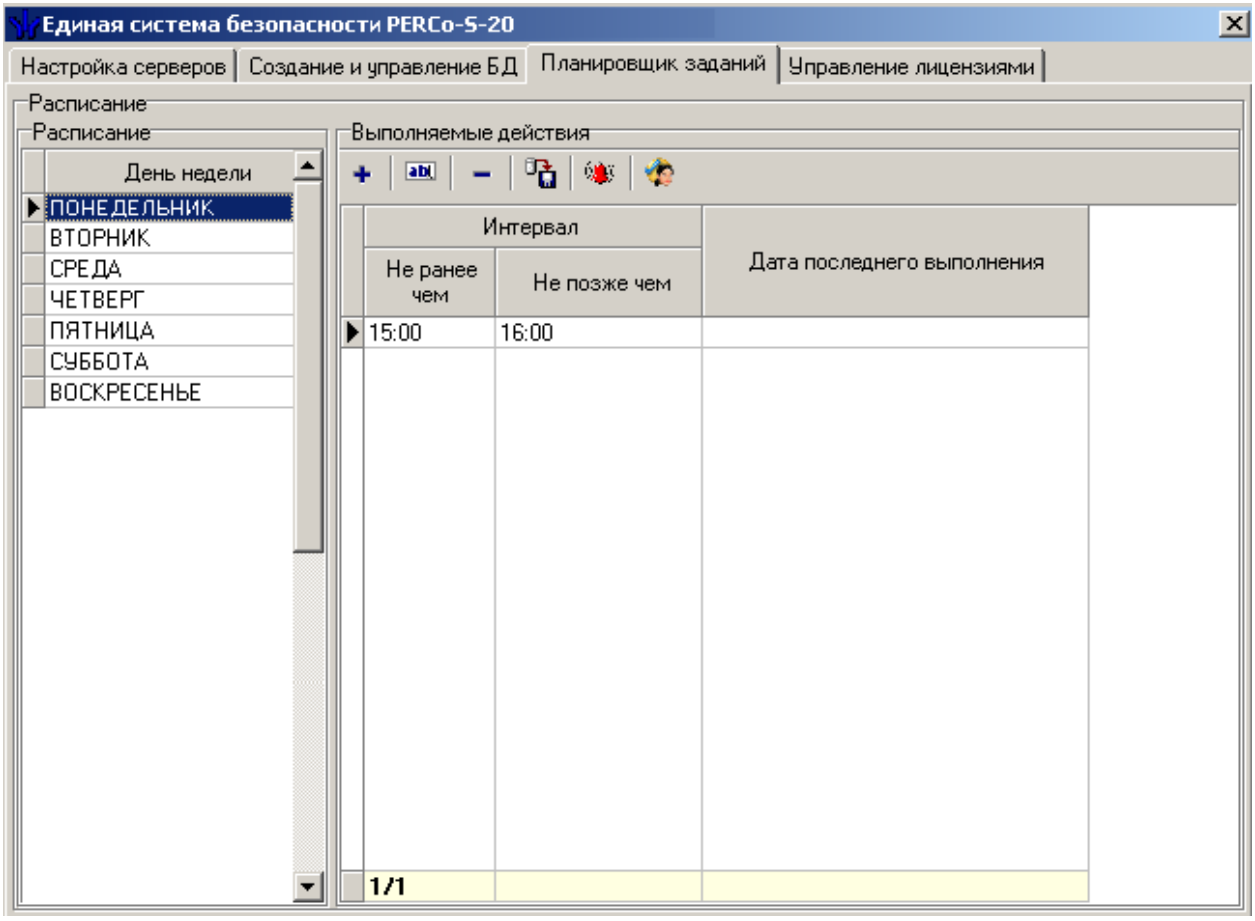
При восстановлении пароля все «Консоли управления» должны быть закрыты.

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

Планировщик заданий

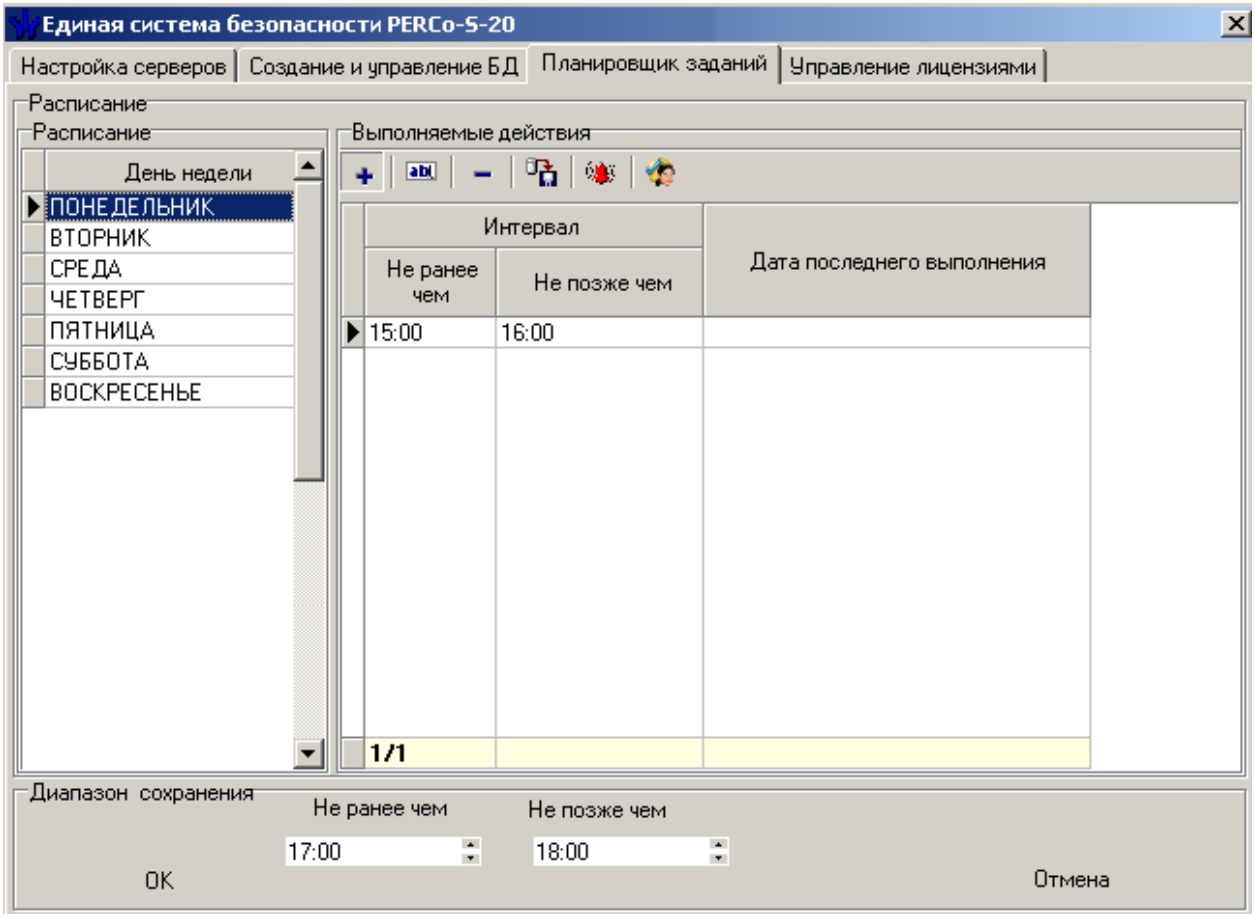
Одной из основных проблем обслуживания информационных систем является своевременное создание резервных копий базы данных. К сожалению, сбои в работе персональных компьютеров, жестких дисков не редкость.

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  . В нижней части окна откроется панель ввода:

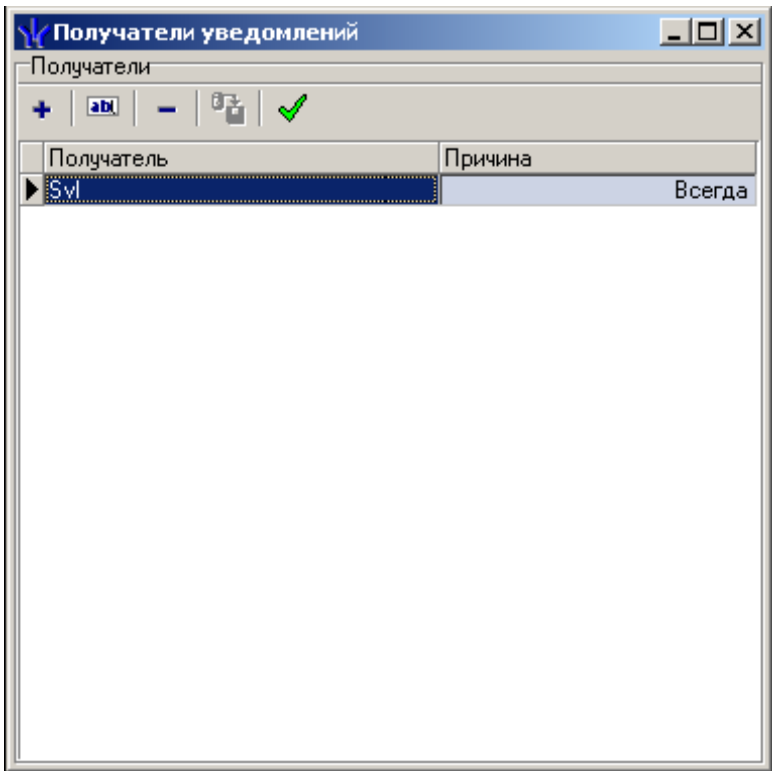


В этой панели необходимо указать интервал времени, в течение которого сервер системы проведет создание резервной копии БД. При условии работы системы в круглосуточном режиме рекомендуем установить этот интервал в ночное время.

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

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

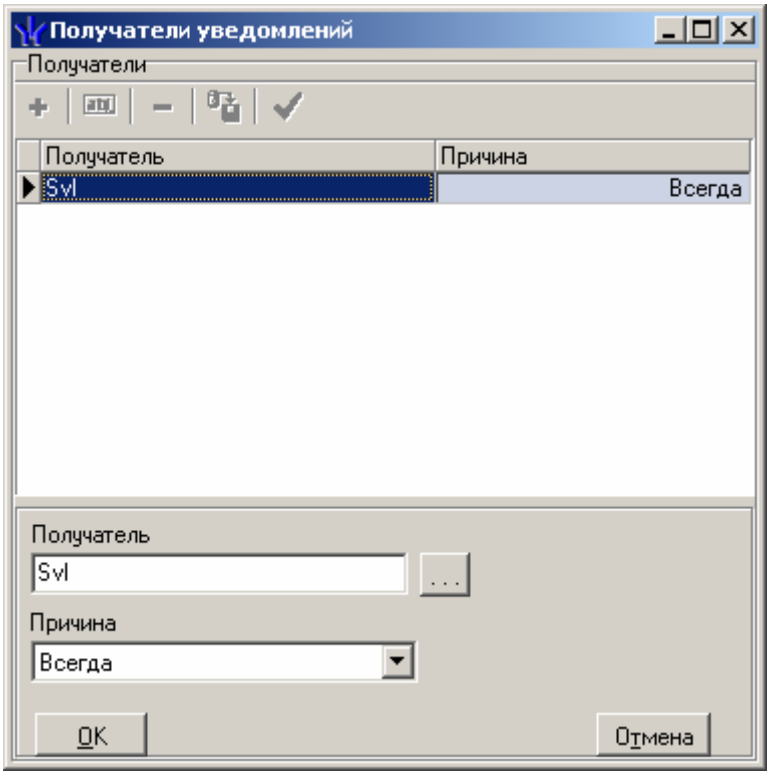
При создании резервной копии базы данных существует возможность рассылки уведомлений о результатах выполнения. Для задания списка рассылки необходимо воспользоваться кнопкой  . Нажатие на нее приведет к открытию диалогового окна, отображающего текущее состояние списка рассылки:



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

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

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

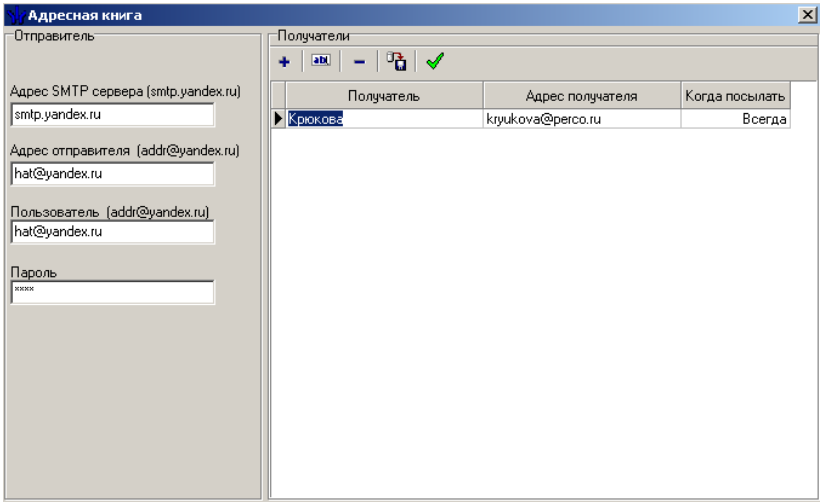


В этой панели необходимо ввести имя компьютера, на которое будет отправлено сообщение и причину отправки, которую необходимо выбрать из списка. Доступны два варианта:

- **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 может 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.

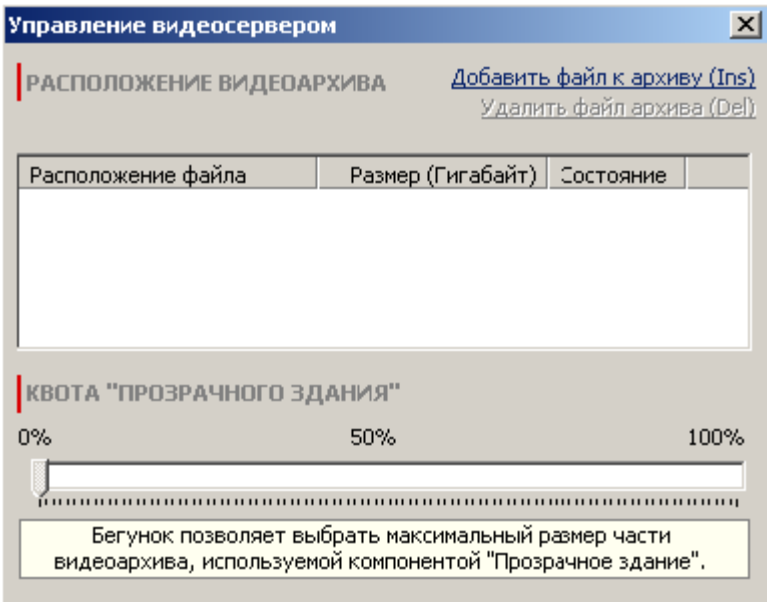


Функциональные элементы окна настройки аналогичны описанным выше функциональным элементам окна настройки рассылки по сети.

Сервер видеонаблюдения

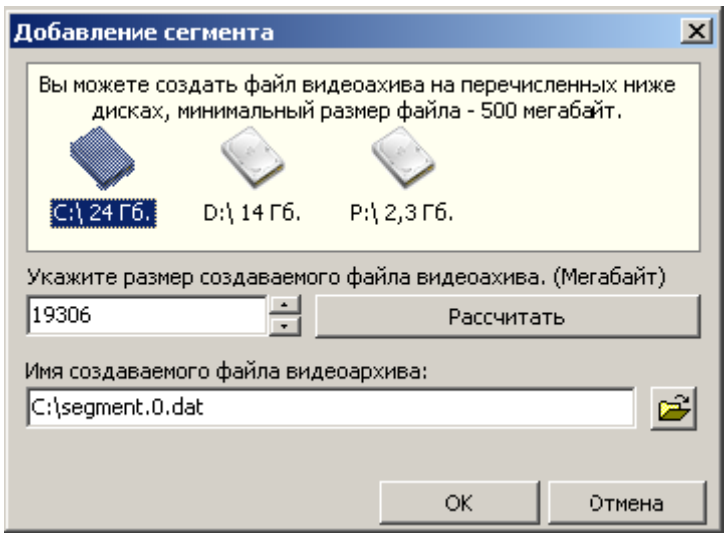
Программный модуль, предназначенный для создания систем Видеонаблюдения, Прозрачное здание и Верификация / Видеоидентификация.

Для управления сервером видеонаблюдения PERCo-S-20 запустите Панель управления Windows (**Пуск → Настройка → Панель управления**), дважды щелкните на значке  :



В этом окне необходимо задать место расположение файла видеоархива, в котором сервер видеонаблюдения будет сохранять видеоинформацию.

Для добавления файла видеоархива необходимо щелкнуть на Добавить файл к архиву (Ins):

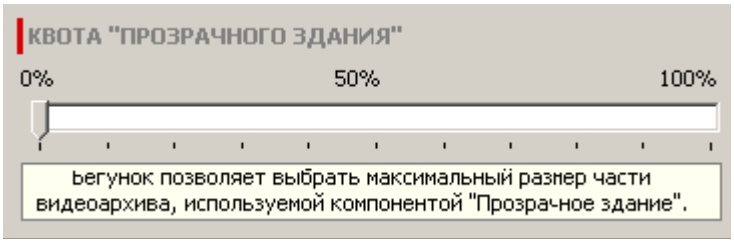


В появившемся диалоговом окне выбрать логический диск, на котором будет храниться файл видеоархива. Ниже программа выводит размер предполагаемого файла. Кнопка **Рассчитать** позволяет определить какое количество камер и длительность записи будет возможно сохранить в этом файле.

ПРИМЕЧАНИЕ

Архив системы **Видеонаблюдения** имеет циклическую структуру. После заполнения старая информация будет автоматически перезаписываться!

Ниже расположен бегунок, позволяющий определить, какая часть видеоархива будет зарезервирована под использование системы **Прозрачное здание**:

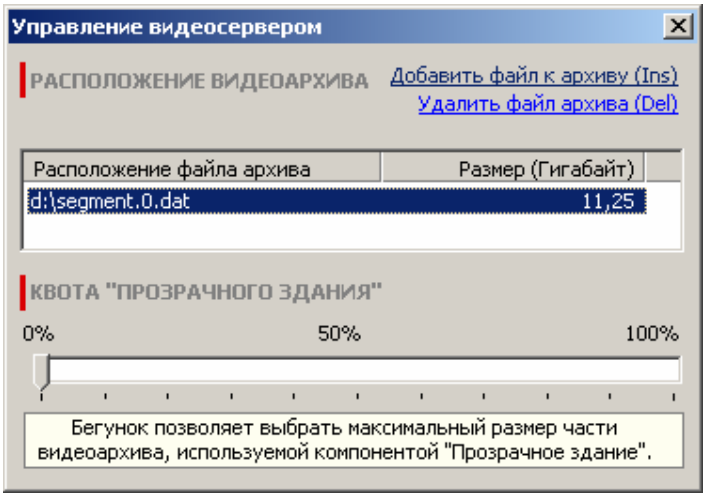


ПРИМЕЧАНИЕ

Часть архива подсистемы **Прозрачное здание** имеет циклическую структуру. После заполнения старая информация будет автоматически перезаписываться!

Система позволяет создать несколько файлов видеоархива, расположенных на разных дисках.

Для удаления файла видеоархива необходимо выделить его в списке файлов:



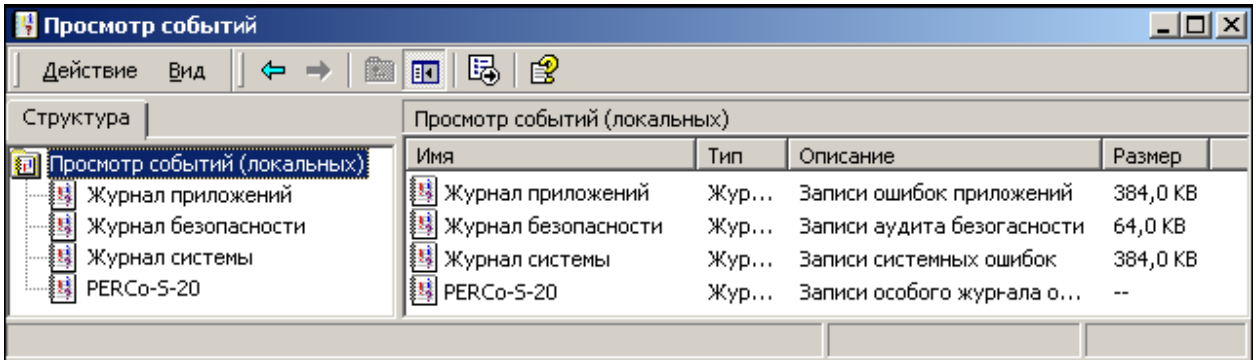
Затем нажать на Удалить файл архива (Del). В появившемся диалоговом окне ответить утвердительно на предупреждение о невозможности последующего восстановления данных.

Сообщения об ошибках

Учитывая, что сервер системы и сервер видеонаблюдения, выполнены в виде стандартных сервисов 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**.

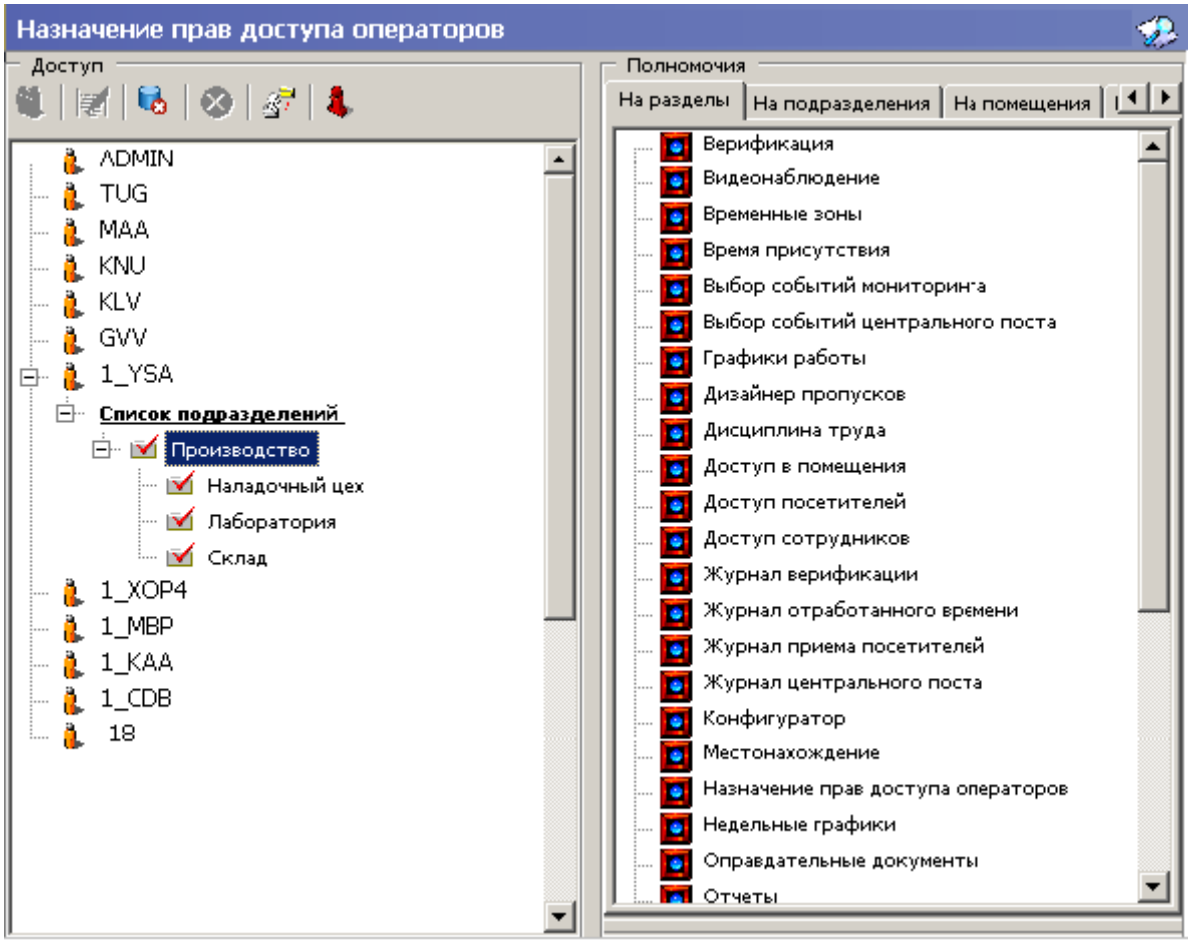


Информация об ошибках и внутренних сообщения записывается в журнал PERCo-S-20.

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 **Назначение прав доступа операторов**:



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

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 для указания списка помещений системы безопасности.

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

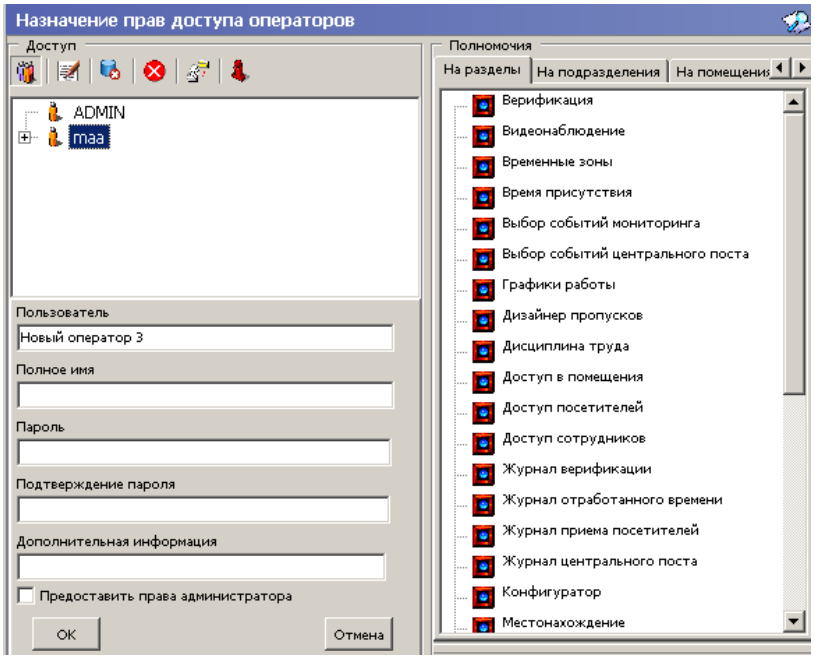
ПРИМЕЧАНИЕ

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.

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:

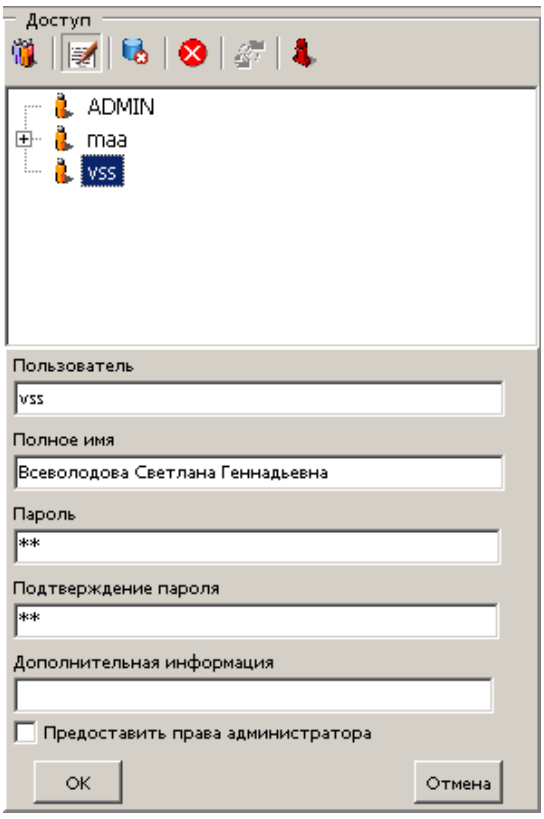
- **Пользователь.** В этой строке указывается имя пользователя, которое он будет вводить при запуске программного обеспечения.
- **Полное имя.** В этой строке указывается полное имя пользователя.
- **Пароль.** В этой строке указывается пароль пользователя.
- **Подтверждение пароля.** Указывается тот же самый пароль для избегания ошибки ввода.
- **Дополнительная информация.** В этой строке ввода можно ввести любую дополнительную информацию об операторе.

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

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.

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  . При этом появится диалоговое окно с запросом подтверждения удаления оператора.

Предоставление прав доступа оператору

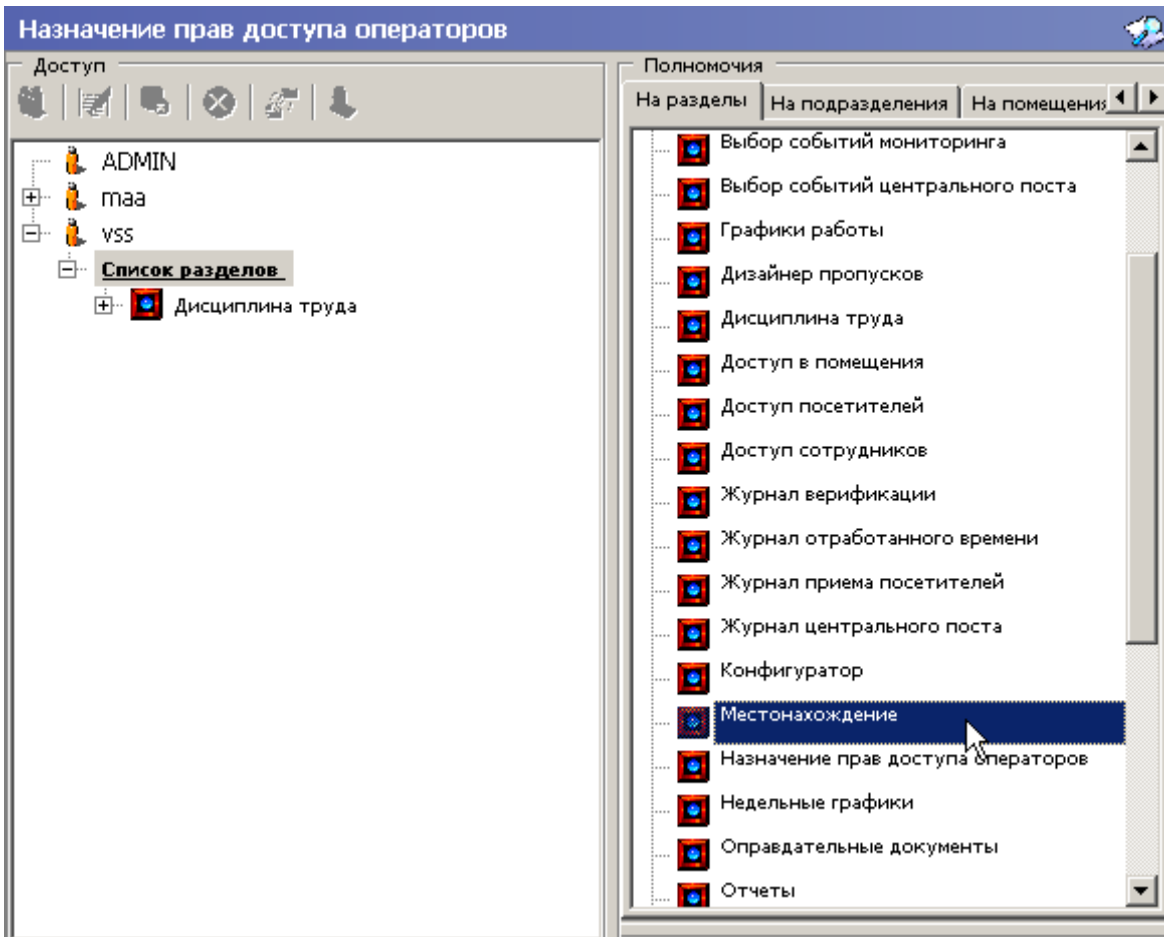
Для предоставления прав доступа оператору необходимо выделить его в списке операторов системы при помощи левой клавиши мыши и выбрать соответствующую закладку в левой части рабочего окна.

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.

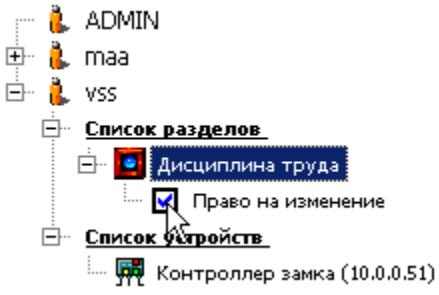
После этого название добавленного раздела программного обеспечения отобразится под оператором:



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.



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.

Права доступа на помещения

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

Механизм предоставления права доступа оператору полностью аналогичен описанному выше.

Права доступа на управление устройствами

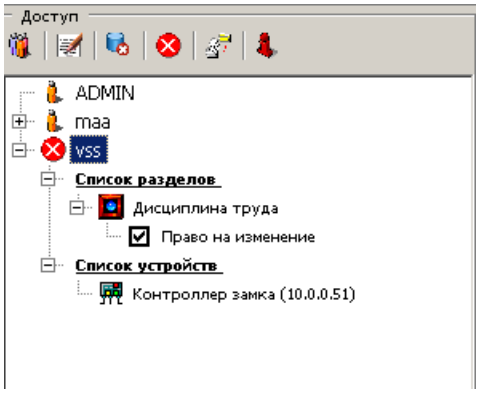
Вкладка **На устройства** дает возможность указать, какими именно устройствами, входящими в систему безопасности, будет разрешено управлять оператору.

Механизм предоставления права оператору полностью аналогичен описанному выше.

Запрещение прав оператора

Для запрещения любого права оператора необходимо выбрать это право и нажать на кнопку  . При этом это право будет удалено из списка разрешенных.

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



После этого доступ оператора к программным разделам будет запрещен.

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

ПРИМЕЧАНИЕ

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

СИСТЕМА ПОЖАРНОЙ СИГНАЛИЗАЦИИ

Одной из составных частей единой система безопасности предприятия PERCo-S-20, является адресная система пожарной сигнализации (АСПС) PERCo-S-20-PF.

АСПС предназначена для раннего обнаружения пожара, извещения о пожаре уполномоченного персонала и сотрудников предприятия. Кроме этого, АСПС имеет возможность выдачи сигналов на пуск системы пожаротушения, систем оповещения и эвакуации, подключения и отключения технологического оборудования.

Подробное описание технических характеристик АСПС, требований к используемому оборудованию, условия эксплуатации приведены в техническом описании на адресную систему пожарной сигнализации PERCo-S-20-FIRE.

Порядок описание параметров функционирования АСПС приведен в разделе «***Конфигурация контроллеров***» данного руководства.

Ниже приводится общее описание построения системы пожарной сигнализации с точки зрения ее функционирования в составе единой системы безопасности PERCo-S-20.

Адресная система пожарной сигнализации состоит из следующих элементов:

1. Драйвер шлейфа PERCo -PF01.
2. Адресный пожарный контрольный прибор (АПКП) - PERCo -PF02.

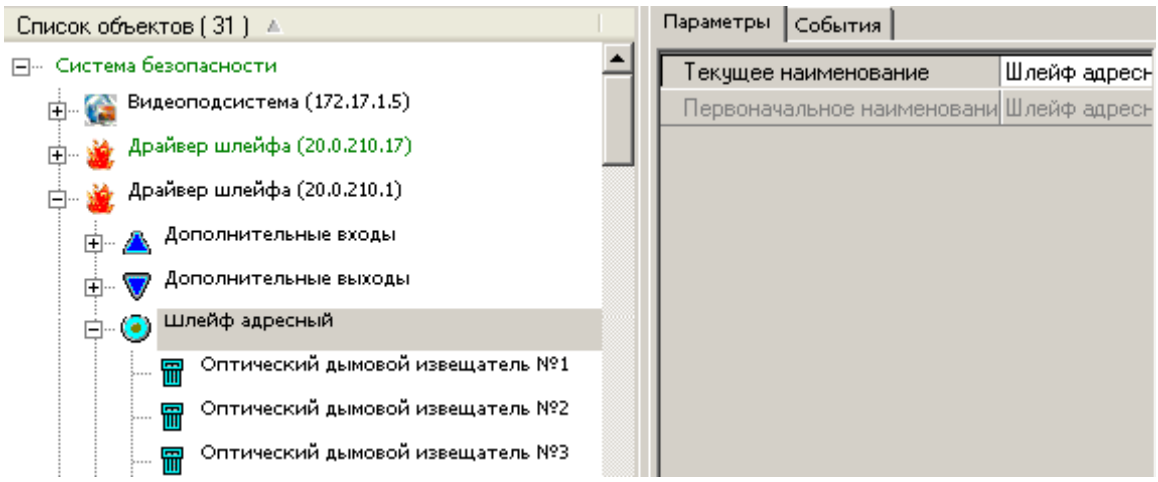
Драйвер шлейфа предназначен для подключения к нему одного адресного шлейфа пожарных извещателей серии XP95 производства компании Apollo Fire Detect. Список поддерживаемых извещателей приведен в техническом описании на систему пожарной сигнализации.

Кроме этого, драйвер шлейфа имеет два дополнительных входа предназначенных для подключения дополнительного оборудования и трех релейных выходов, которые могут быть использованы для подключения тревожных оповещателей.

Адресный пожарный контрольный прибор предназначен для отображения информации о состоянии адресных шлейфов пожарной сигнализации, и управления пуском системы пожаротушения и индикации тревожных ситуаций. АПКП поддерживает работу с 32 драйверами шлейфа и управление 4 зонами пожаротушения. Суммарное количество драйверов шлейфа и АПКП в системе безопасности не может быть больше 1024.

После проведения монтажа системы пожарной сигнализации необходимо провести конфигурацию систему. Порядок проведения конфигурации описан в разделе «***Конфигурация контроллеров***» данного руководства.

При конфигурации контроллеров пожарной сигнализации, драйвер шлейфа автоматически опрашивает все адресное пространство шлейфа сигнализации. Список подключенных извещателей отображается в виде подчиненного дерева объектов у каждого из драйверов:



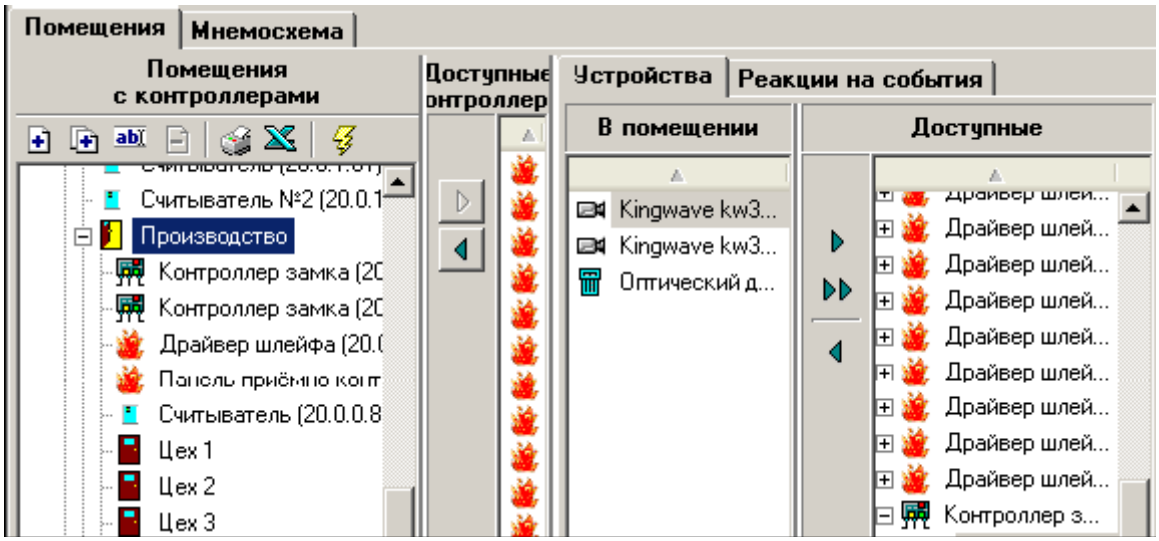
В данном случае шлейф пожарной сигнализации содержит оптические дымовые и температурные извещатели. Адрес извещателя отображаемый в его параметрах соответствует адресу установленному при монтаже при помощи соответствующей пластины.

После описания параметров работы извещателей и передачи этих данных в аппаратуру (см. раздел «***Описание параметров пожарной сигнализации***») необходимо разместить адресные пожарные извещатели в дереве помещений (см. раздел ***Помещения и мнемосхема***). При размещении извещателей необходимо руководствоваться составленной ранее схемой пожарной сигнализации и обратить внимание на соответствие адресов извещателей установленных в помещении адресам извещателей полученным при конфигурации системы.

В случае их несовпадения необходимо внести необходимые изменения и повторить конфигурацию системы пожарной сигнализации.

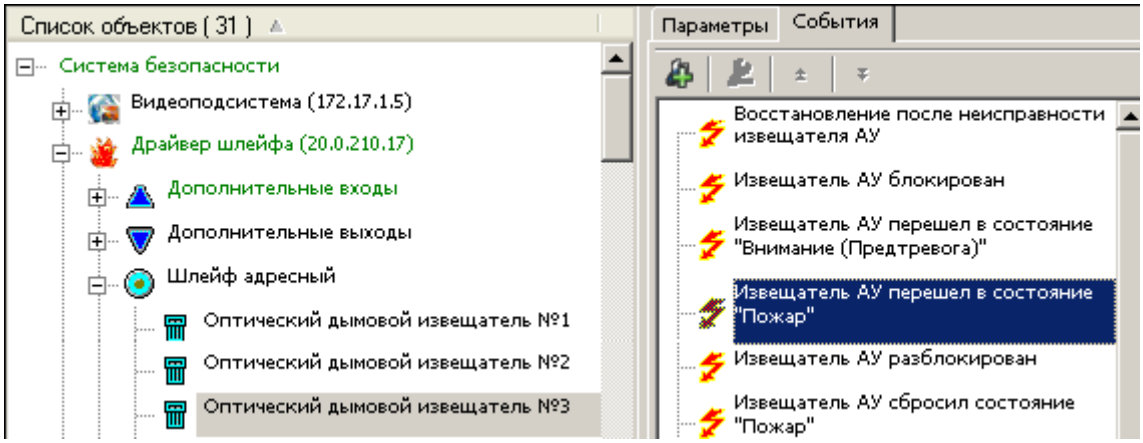
Использование адресных пожарных извещателей дает возможность точно определить место возникновения пожара и тем самым организовать возможность оповещения и эвакуации сотрудников предприятия.

Для организации этого необходимо задать реакцию системы безопасности на событие возникновения пожара на извещателе.

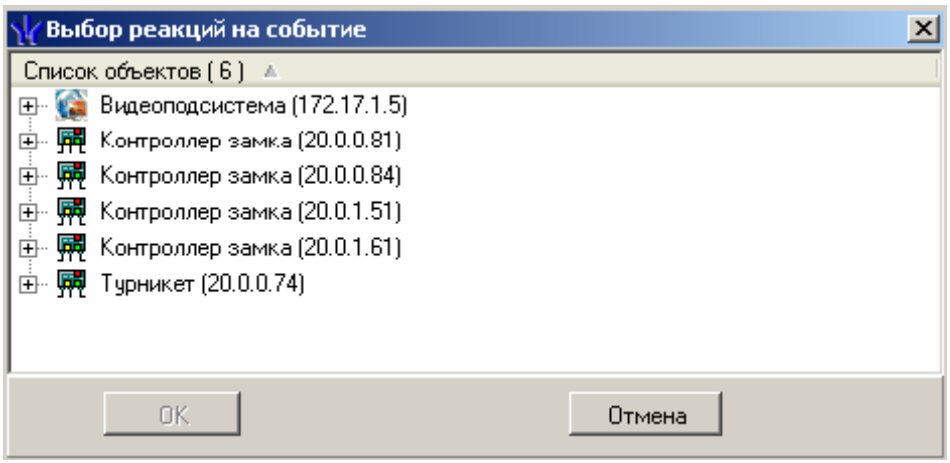


Так, например, в данном случае оптический дымовой извещатель №3 расположен в помещении «Производство». Доступ в это помещение контролирует «Контроллер замка (20.0.0.81)». Для обеспечения эвакуации людей из этого помещения нам необходимо, в случае срабатывания пожарного извещателя разблокировать дверь помещения или

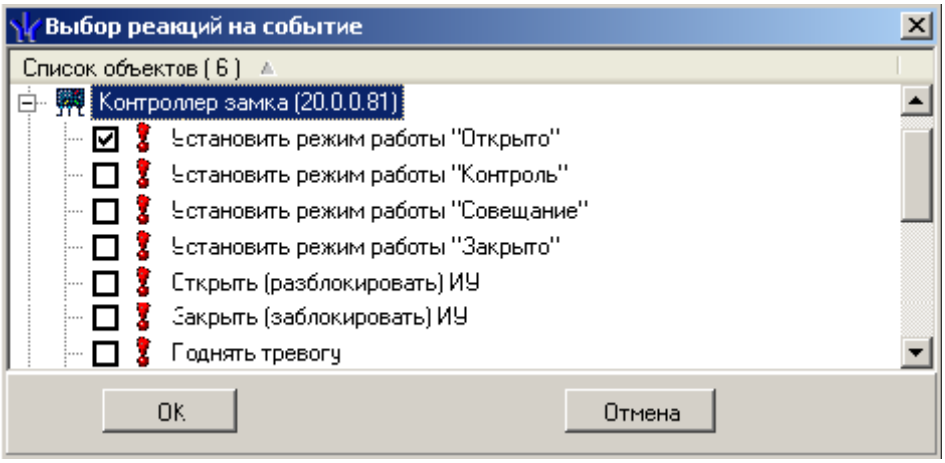
другими словами перевести контроллер в состояние «Открыто». Для реализации этого выберите в разделе Конфигуратор оптический дымовой извещатель и перейдите на вкладку События:



Выберите событие «Извещатель АУ перешел в состояние «Пожар»» и нажмите на кнопку  . При этом появится диалоговое окно со списком объектов системы.



В этом списке выберите «Контроллер замка (20.0.0.81)» и отметьте команду **Установить режим работы «Открыто».**



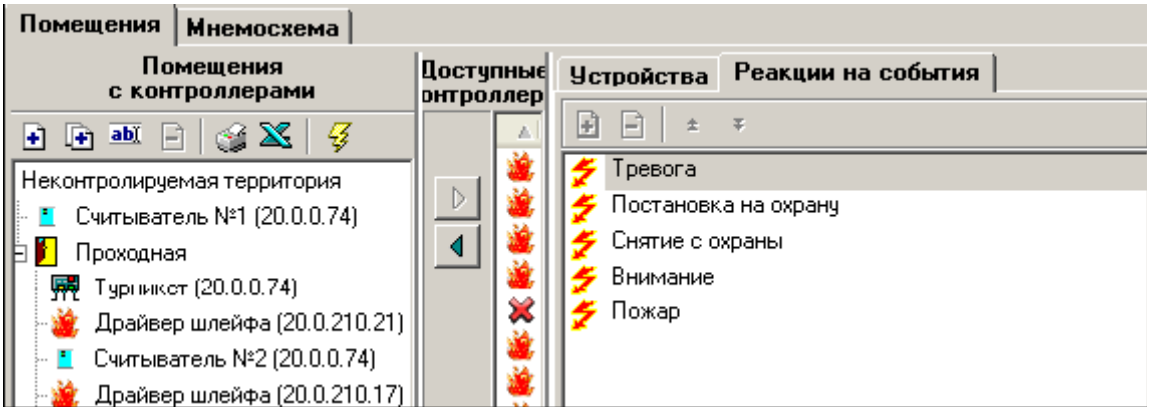
Нажмите кнопку «**ОК**», сохраните и передайте измененные параметры.

ПРИМЕЧАНИЕ

Если в качестве реакции на событие выбрать «Открыть, разблокировать ИУ» это приведет к однократной разблокировке замка на время удержания в открытом состоянии, что не обеспечит беспрепятственной эвакуации сотрудников.

Аналогичным образом может быть настроена реакция на все события, поступающие от системы пожарной сигнализации.

Добавить или удалить реакцию на событие возможно также с использованием вкладки Реакции на события подраздела Помещения.



ВИДЕОНАБЛЮДЕНИЕ

Одной из составных частей единой системы безопасности PERCo-S-20 является подсистема видеонаблюдения.

Подсистема видеонаблюдения является программно аппаратным комплексом, состоящим из следующих частей:

- ✓ **IP видеокамеры, IP видеосервера с подключенными к ним аналоговыми видеокамерами** – оконечные устройства, предназначенные для получения видеоизображения контролируемой территории предприятия.
- ✓ **Видеосервер** – программный модуль, обеспечивающий отображение, запись, **воспроизведение видеоинформации, получаемой от видеокамер.**
- ✓ **Программные модули: Видеонаблюдение, Прозрачное здание** – программные модули, встраиваемые в консоль управления и предназначенные для отображения видеоинформации на компьютерах операторов.

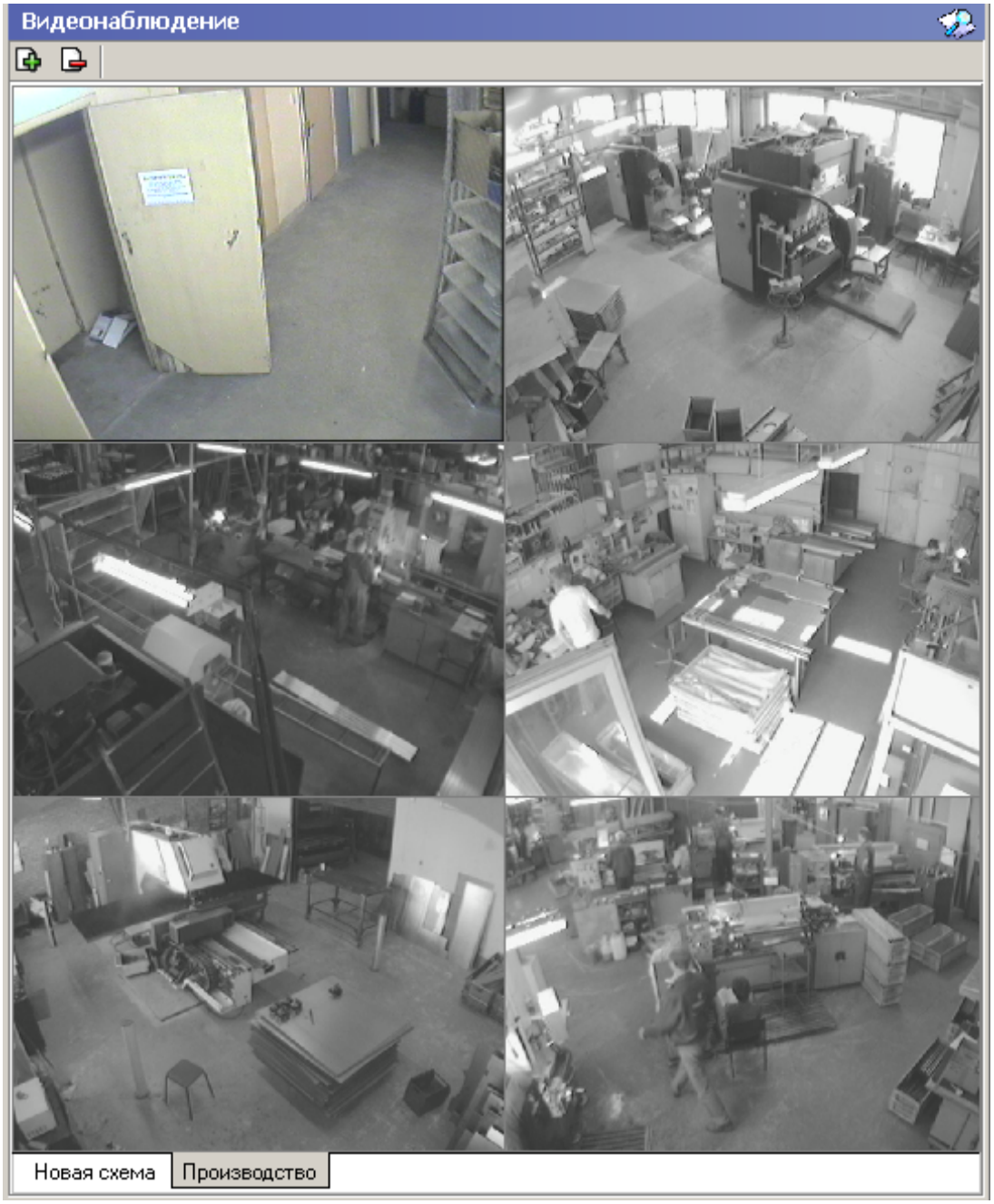
Список поддерживаемых IP видеокамер и видеосерверов приведен в разделе «***Требования к аппаратуре***». Правила их монтажа, подключения описаны в сопроводительной документации к этим изделиям.

Настройка программного модуля сервера видеонаблюдения описана в разделе «***Управление серверами, Сервер видеонаблюдения***» этого руководства.

Описание параметров функционирования IP видеокамер описано в разделе «***Конфигурация контроллеров, Описание параметров видеоподсистемы***» этого руководства.

В этом разделе будут даны рекомендации по конфигурированию раздела **Видеонаблюдение** и общим приемам работы с ним.

Раздел **Видеонаблюдение** предназначен для отображения видеоинформации, получаемой с видеокамер, управления видеокамерами, записи видеоинформации и ее воспроизведения.



Для организации рабочего места необходимо:

1. Определить изображение с каких камер видеонаблюдения и в каких ситуациях будут контролироваться разделом **Видеонаблюдение**.

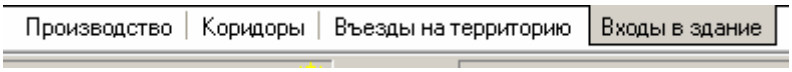
2. Определить, на каком рабочем месте будет осуществляться работа модуля.

3. Проверить наличие связи (прохождение IP пакетов) между выбранным рабочим местом и компьютером, на котором установлен сервер системы и сервер видеонаблюдения, видеокамерами, информация о которых будет отображаться на этом Рабочем месте.

4. Провести инсталляцию модуля **Видеонаблюдение** на выбранном компьютере.

5. Создать схемы работы разделом **Видеонаблюдение.**

Учитывая, что в зависимости от режима работы предприятия, может возникнуть необходимость вести наблюдение за различными помещениями в зависимости от времени суток на одном рабочем месте может быть создано несколько схем отображения видеоинформации. Переключение между ними может осуществлять оператор в соответствии с установленными административными правилами. Для переключения между схемами необходимо воспользоваться закладками расположенными в нижней части рабочего окна:



При условии, что данному оператору это будет разрешено. Об установке прав оператора по работе с этим разделом смотрите соответствующий раздел данного руководства.

Возможность переключения между схемами отображения может быть проиллюстрирована следующим примером.

Например, до начала рабочего дня и после его окончания оператор контролирует вход/выход на территорию предприятия. После начала рабочего дня оператор меняет схему отображения, выбирая другую. И начинает контролировать вход в администрацию предприятия.

Такая организация работы, позволяет уменьшить затраты на организацию дополнительного рабочего места сотрудника безопасности.

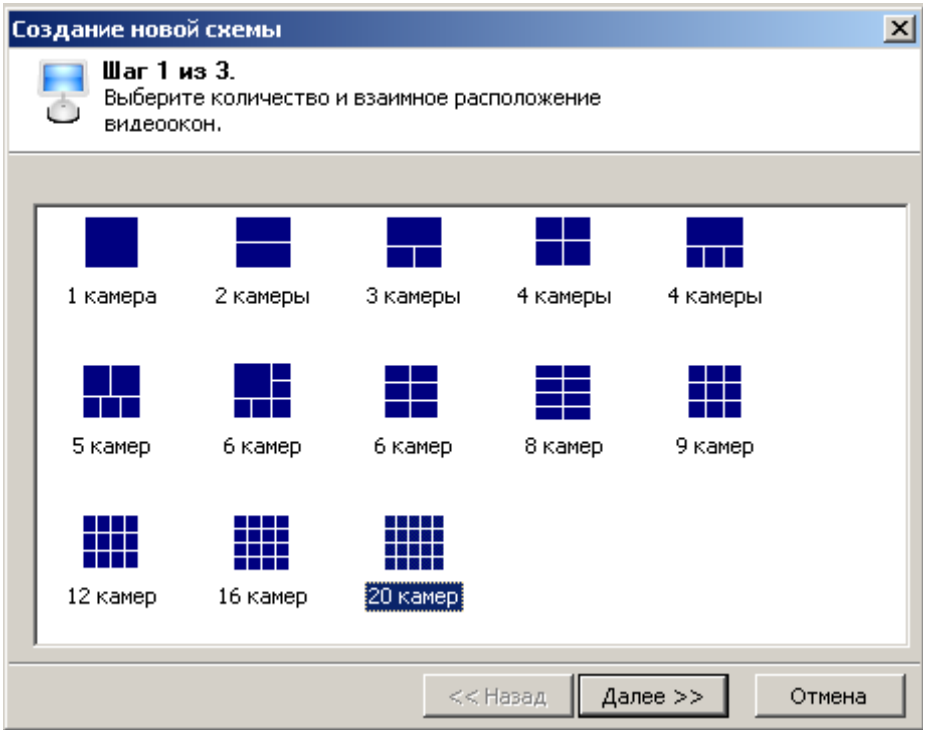
ПРИМЕЧАНИЕ

Схемы отображения видеоинформации раздела **Видеонаблюдение** записывается локально на каждом рабочем месте. Таким образом, в случае наличия в системе нескольких рабочих мест необходимо создать схемы отображения на каждом рабочем месте.

Для удаления схемы отображения раздела **Видеонаблюдение** предназначена кнопка  .

Конфигурация модуля

Для создания новой конфигурации щелкните на кнопке Создать новую схему —  . При этом откроется следующее диалоговое окно:

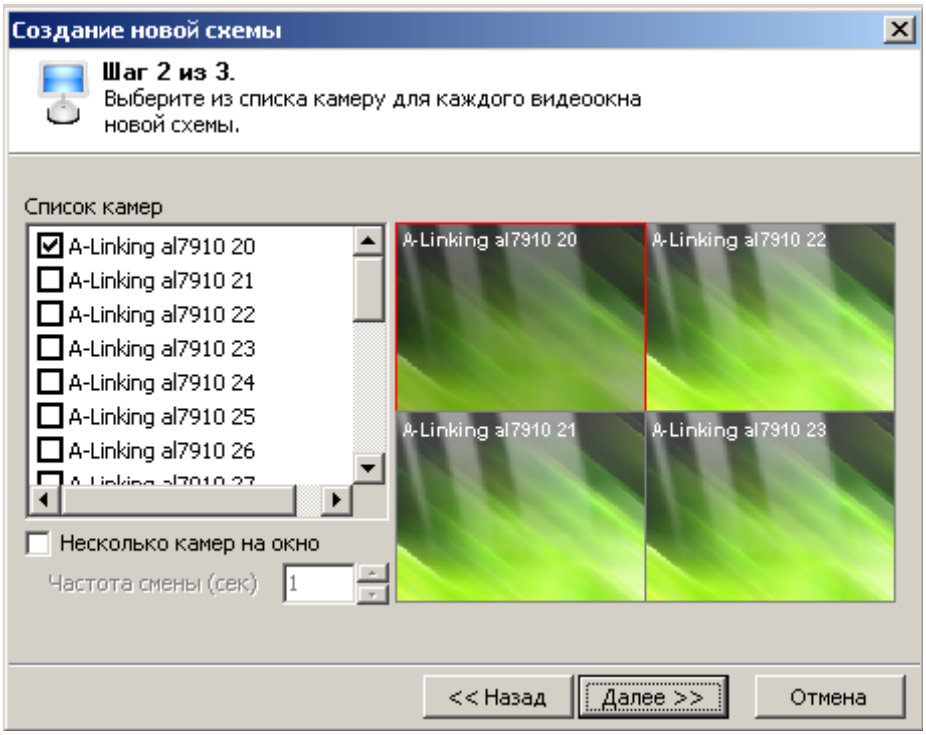


В этом диалоговом окне выберите одну из предлагаемых схем расположения окон отображения видеоинформации, в зависимости от количества камер видеонаблюдения которые должны отображаться.

ПРИМЕЧАНИЕ

Максимальное количество камер в одной схеме равно 20.

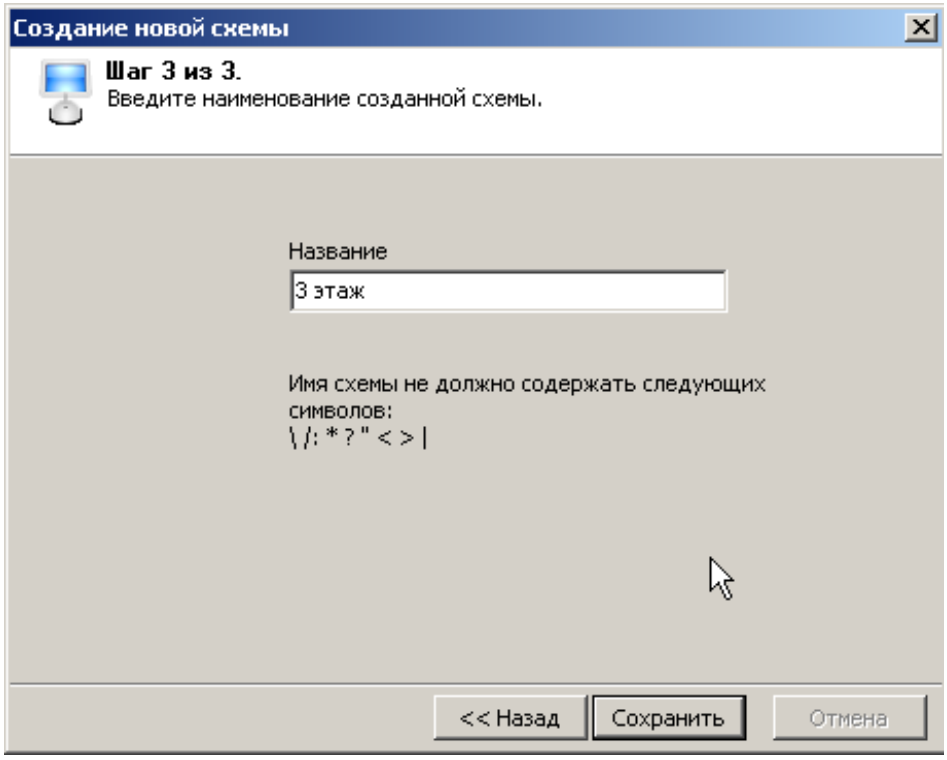
Выбрав схему расположения камер, щелкните на кнопке **Далее**:



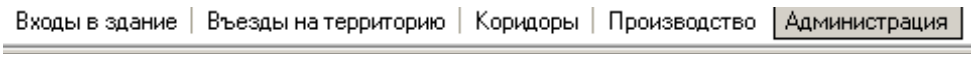
На этом шаге создания схемы отображения укажите, какие именно камеры видеонаблюдения будут отображаться в создаваемой схеме.

Для этого при помощи мыши выделите нужное окно вывода на схеме (выбранное окно имеет красную рамку) и отметьте нужную камеру в списке слева. Отметкой флажка Несколько камер на окно можно задать смену вывода изображений с нескольких камер в одном окне. Камеры будут меняться с частотой, введенной в поле Частота смены.

После окончания выбора камер видеонаблюдения щелкните на кнопке Далее.



В открывшемся диалоговом окне задайте название схемы. Это название будет отображаться в нижней части окна раздела Видеонаблюдения в качестве заголовка вкладки:



При необходимости создания нескольких схем повторите описанные выше действия.

ПРОЗРАЧНОЕ ЗДАНИЕ

Одной из составных частей единой системы безопасности PERCo-S-20 является подсистема видеонаблюдения.

Подсистема видеонаблюдения является программно аппаратным комплексом, состоящим из следующих частей:

- **IP видеокамеры, IP видеосервера с подключенными к ним аналоговыми видеокамерами** – оконечные устройства предназначенные для получения видеоизображения контролируемой территории предприятия.
- **Видеосервер** – раздел, обеспечивающий отображение, запись, воспроизведение видеоинформации, получаемой от видеокамер.
- **Программные модули: Видеонаблюдение, Прозрачное здание** – разделы, встраиваемые в консоль управления и предназначенные для отображения видеоинформации на компьютерах операторов.

Список поддерживаемых IP видеокамер и видеосерверов приведен в разделе «***Требования к аппаратуре***». Правила их монтажа, подключения описаны в сопроводительной документации к этим изделиям.

Настройка программного модуля сервера видеонаблюдения описана в разделе «***Управление серверами, Сервер видеонаблюдения***» этого руководства.

Описание параметров функционирования IP видеокамер описано в разделе «***Конфигурация контроллеров, Описание параметров видеоподсистемы***» этого руководства.

В этом разделе будут даны рекомендации по конфигурированию программного раздела **Прозрачное здание** и общим приемам работы с ним.

Раздел **Прозрачное здание** предназначен для отображения видеоинформации, получаемой с видеокамер, просмотра видеоархива раздела.

В отличие от раздела **Видеонаблюдение** раздел **Прозрачное здание** работает по другому принципу.

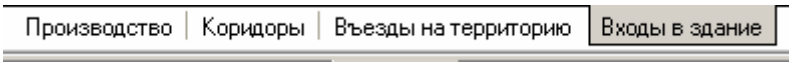
Основной задачей раздела является не наблюдение в режиме реального времени за состоянием охраняемых объектов, а информирование сотрудников предприятия и руководителей о ходе производственного процесса.

В соответствии с этой задачей, для минимизации трафика сети Ethernet изображение с камер видеонаблюдения, используемых в системе **Прозрачное здание**, сначала записывается сервером видеонаблюдения с частотой, не превышающей 1 кадр в секунду, а затем транслируется в раздел **Прозрачное здание**. Таким образом, временная задержка отображения видеоинформации в разделе **Прозрачное здание** составляет 4 – 5 секунд. Более подробно об использовании камер в системе **Прозрачное здание** см. раздел «***Описание параметров видеокамер***» данного руководства.

Для организации рабочего места необходимо:

1. Определить изображение с каких камер видеонаблюдения и в каких ситуациях будут отображаться разделом **Прозрачное здание**.
2. Указать в параметрах выбранных видеокамер, что они используются в системе **Прозрачное здание**.
3. Определить на каком рабочем месте будет осуществляться работа модуля.
4. Проверить наличие связи (прохождение IP пакетов) между выбранным рабочим местом и компьютером, на котором установлен сервер системы и сервер видеонаблюдения.
5. Провести инсталляцию модуля **Прозрачное здание** на выбранном компьютере.
6. Создать схемы работы раздела **Прозрачное здание.**

Учитывая, что в зависимости от режима работы предприятия, может возникнуть необходимость вести наблюдение за различными помещениями в зависимости от времени суток на одном рабочем месте может быть создано несколько схем отображения видеоинформации. Переключение между ними может осуществлять оператор в соответствии с установленными административными правилами. Для переключения между схемами необходимо воспользоваться закладками, расположенными в нижней части рабочего окна:



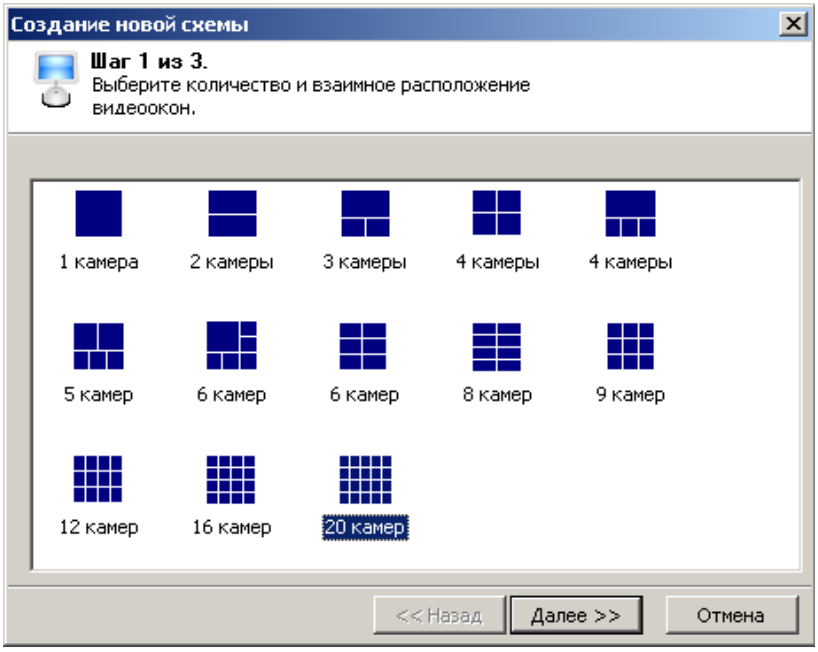
ПРИМЕЧАНИЕ

Схемы отображения видеоинформации раздела **Прозрачное здание** записывается локально на каждом рабочем месте. Таким образом, в случае наличия в системе нескольких рабочих мест необходимо создать схемы отображения на каждом рабочем месте.

Для удаления схемы отображения раздела **Прозрачное здание** предназначена кнопка .

Конфигурация модуля

Для создания новой конфигурации щелкните на кнопке Создать новую схему — . При этом откроется следующее диалоговое окно:

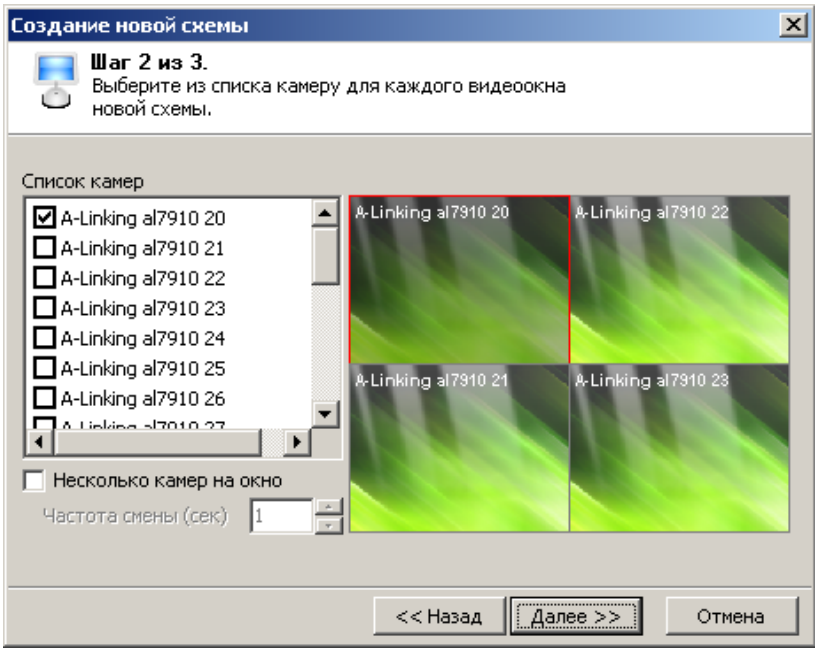


В этом диалоговом окне вы должны выбрать одну из предлагаемых схем расположения окон отображения видеоинформации, в зависимости от количества камер видеонаблюдения которые должны отображаться.

ПРИМЕЧАНИЕ

Максимальное количество камер в одной схеме равно 20.

Выбрав схему расположения камер необходимо нажать на кнопку **Далее**:



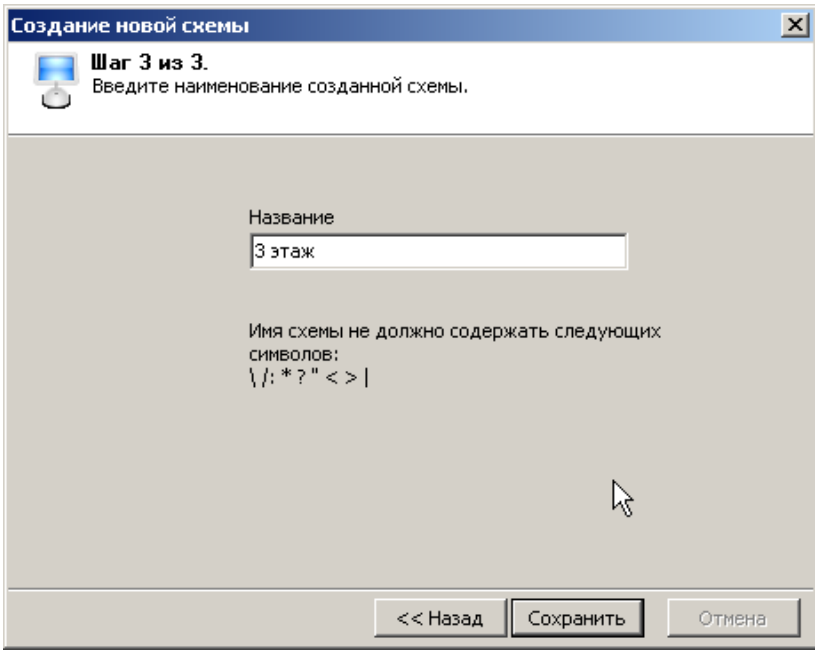
На этом шаге создания схемы отображения укажите, какие именно камеры видеонаблюдения будут отображаться в создаваемой схеме.

Для этого при помощи мыши выделите нужное окно вывода на схеме (выбранное окно имеет красную рамку) и отметьте нужную камеру в списке слева. Отметкой флажка Несколько камер на окно можно задать смену вывода изображений с нескольких камер в одном окне. Камеры будут меняться с частотой, введенной в поле Частота смены.

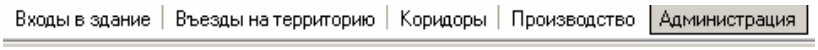
ПРИМЕЧАНИЕ

В списке камер отображаются только те, в параметрах работы которых установлено, что данная камера используется в системе **Прозрачное здание**.

После окончания выбора камер видеонаблюдения необходимо нажать на кнопку **Далее**:



В появившемся диалоговом окне задайте название схемы. Это название будет отображаться в нижней части окна раздела **Прозрачное здание** в качестве заголовка закладки:



При необходимости создания нескольких схем, описанные выше действия необходимо повторить.

ПРИЕМ ПОСЕТИТЕЛЕЙ

Модуль **Прием посетителей** PERCo-SM10 «Прием посетителей» предназначен для организации рабочего места руководителя предприятия, секретаря руководителя, организации рабочего места сотрудника, ведущего прием посетителей. Кроме этого данный программный модуль может быть использован для организации доступа в помещения с особым режимом доступа, например в бухгалтерию.

Раздел **Прием посетителей** позволяет контролировать вход только через одно устройство. При этом он позволяет отображать информацию о владельце предъявленной карты доступа, видеоинформацию с камеры видеонаблюдения при условии, что она установлена и описана в конфигурации системы; записывать информацию о зарегистрированных событиях и действиях оператора. Кроме этого раздел позволяет управлять режимами доступа через выбранное устройство.

Кроме отображения информации о сотруднике, раздел **Прием посетителей** позволяет отображать и записывать видеоинформацию, полученную с выбранных камер.

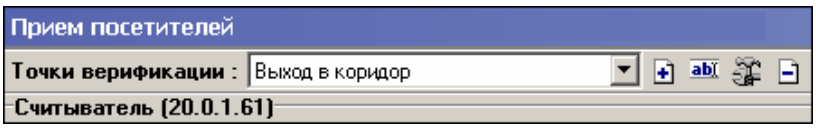
Одновременно раздел **Прием посетителей** позволяет контролировать до 4 точек прохода и 4 камер видеонаблюдения.

Все действия оператора, информация о фактах предъявления карт доступа, видеоинформация автоматически записываются разделом и доступны для последующего просмотра и анализа.

Для организации рабочего места необходимо:

1. Определить какая точка доступа будет контролироваться разделом **Прием посетителей**.
2. Определить на каком рабочем месте будет осуществляться работа модуля.
3. Проверить наличие связи (прохождение IP пакетов) между выбранным рабочим местом и компьютером, на котором установлен сервер системы, контроллером точки доступа, которая будет контролироваться, и видеокамерой, информация с которой будет сопоставлена выбранной точке доступа.
4. Провести инсталляцию модуля **Прием посетителей** на выбранном компьютере.
5. Описать конфигурацию раздела **Прием посетителей.**

Учитывая, что в зависимости от режима работы помещения, может возникнуть необходимость контролировать доступ в различные помещения, на одном рабочем месте может быть создано несколько конфигураций. Переключение между ними может осуществлять оператор в соответствии с установленными административными правилами. Для переключения между конфигурациями необходимо воспользоваться раскрывающимся списком в верхней части рабочего окна при условии, что данному оператору это будет разрешено:



Об установке прав оператора по работе с этим модулем смотрите соответствующий раздел данного руководства.

Возможность переключения между конфигурациями может быть проиллюстрирована следующим примером.

Например, секретарь в приемной контролирует доступ в помещение администрации при отсутствии руководителя, после его прихода она контролирует доступ в его кабинет.Такая организация работы позволяет уменьшить затраты на организацию дополнительного рабочего места.

ПРИМЕЧАНИЕ

Конфигурация схем работы раздела **Прием посетителей** записывается локально на каждом рабочем месте. Таким образом, в случае наличия в системе нескольких рабочих мест необходимо создать конфигурации работы на каждом рабочем месте.

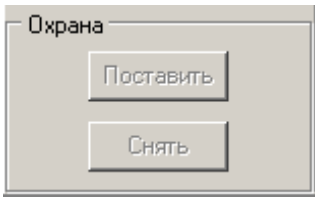
Для удаления конфигурации раздела **Прием посетителей** предназначена кнопка .

Для изменения названия конфигурации кнопка .

Для изменения конфигурации кнопка .

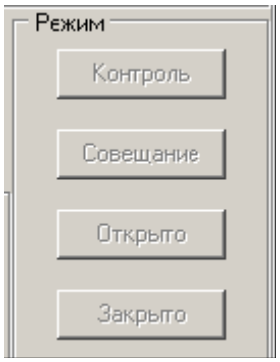
Кнопки **Разрешить**, **Запретить** становятся активными только в случае предъявления карты при условии, что данное предъявление обрабатывается программным модулем, и предназначены для принятия решения оператором.

В группе **Охрана** находятся две кнопки:



- **Поставить** – предназначена для установки режима работы «Охрана» контролируемого помещения.
- **Снять** - предназначена для снятия режима работы «Охрана» контролируемого помещения.

Кнопки управления режимом работы выбранного устройства объединены в группу **Режим**:



- **Контроль.** Приводит к блокировке исполнительного устройства, связанного с выбранным считывателем. При нажатии на кнопку ДУ для данного направления или при поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ разблокируется на время, которое равно времени удержания данного направления ИУ в открытом состоянии. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии.

- **Совещание.** Аналогично режиму работы Контроль за исключением индикации на считывателе и блоке внутренней индикации. Более подробно об индикации режимов доступа изложено в техническом описании системы безопасности.

- **Открыто.** Приводит к разблокировке исполнительного устройства, связанного с выбранным считывателем. Исполнительное устройство остается разблокированным в течение всего времени пока данный режим не будет сменен. Нажатие на кнопки ДУ исполнительного устройства игнорируются. При поднесении карты доступа к считывателю регистрируется событие о проходе или нарушении доступа. При этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.

- **Закрыто.** При включении режима данное направление ИУ блокируется и остается заблокированным в течение всего времени пока режим включен. Нажатие на кнопку ДУ для данного направления игнорируется. Предъявление любой карты вызывает регистрацию события о нарушении прав доступа. Проход через ИУ (открытый механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.

ПРИМЕЧАНИЕ

Контроль за предъявлением карт доступа для выбранного считывателя может осуществляться только из одного раздела **Прием посетителей**. Невозможно организовать несколько рабочих мест операторов раздел **Прием посетителей,** контролирующих одно и то же устройство.

Раздел **Прием посетителей** автоматически обрабатывает следующие события, связанные с предъявлением карт доступа к выбранному считывателю:

События, связанные с предъявлением карты доступа сотрудников:

1. **Проход** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство управляемой этим считывателем.

2. **Проход с нарушением времени** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем. При этом время предъявления карты не соответствует временному критерию доступа данной карты.

3. **Проход с нарушением зональности** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем. При этом владелец этой карты нарушил правила «антипасбека», то есть пытается совершить повторный вход в помещение.

4. **Постановка на охрану** – событие, возникающее при попытке постановки помещения на охрану при помощи карты доступа.

5. **Снятие с охраны** – событие, возникающие при попытке снятия помещения с охраны при помощи карты доступа.

События, связанные с предъявлением карт доступа посетителей:

1. **Проход** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем.

2. **Проход с нарушением времени** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем. При этом время предъявления карты не соответствует временному критерию доступа данной карты.

3. **Проход с нарушением зональности** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем. При этом владелец этой карты нарушил правила «антипасбека», то есть пытается совершить повторный вход в помещение.

События, связанные с предъявлением невалидных или запрещенных карт доступа:

1. **Идентификатор не зарегистрирован** – событие, возникающее при предъявлении карты доступа, которая не внесена в списки карт системы. То есть эта карта доступа никогда не выдавалась сотрудникам или посетителям предприятия или была выдана, а впоследствии была удалена из всех списков.

2. **Идентификатор заблокирован**. Событие возникает в случае предъявления карты доступа, которая была заблокирована. Подробно о блокировке карт доступа смотрите раздел «*Параметры доступа*» данного руководства.

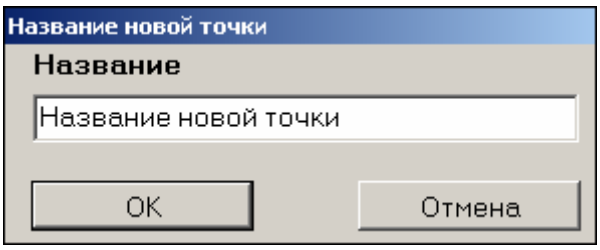
3. **Идентификатор из «СТОП - листа»** - событие, возникающее при предъявлении карты доступа занесенной в стоп лист. Подробно о занесении карты доступа в «СТОП-лист» смотрите раздел «*Параметры доступа*» данного руководства.

4. **Идентификатор просрочен** – событие, возникающее при предъявлении карты доступа с истекшим сроком действия. Подробно о сроке действия карт доступа смотрите раздел «*Параметры доступа*» данного руководства.

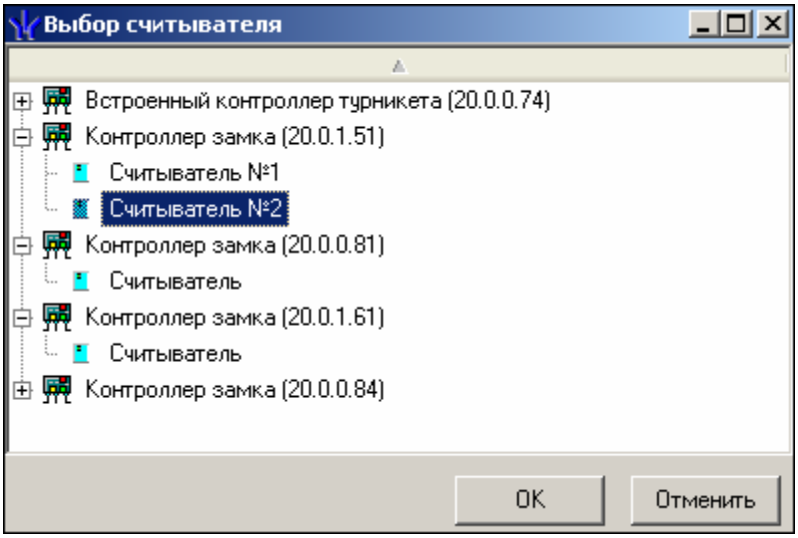
5. **Нарушение режимов доступа** – событие, возникающее при предъявлении карты доступа в режиме «Закрыто» или в режиме «Охрана» при условии, что данная карта доступа не имеет права на снятие помещения с охраны.

Конфигурация модуля

Для создания новой конфигурации необходимо воспользоваться кнопкой **Добавить** —  или горячими клавишами **Ctrl** + **N**. При этом появится следующее диалоговое окно, в котором вам необходимо задать название:

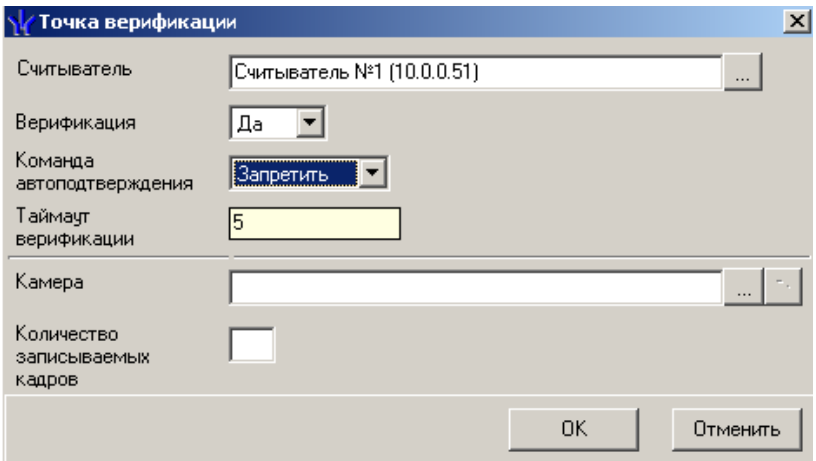


Это название будет отображаться в раскрывающемся списке при выборе текущей конфигурации раздела **Верификация**. После нажатия на кнопку «**ОК**» появится диалоговое окно **Выбор считывателя**:



В этом окне выберите тот считыватель, проход через который будет контролироваться в данной конфигурации.

После выбора считывателя появится следующее диалоговое окно, в котором вы должны указать параметры работы модуля «Прием посетителей» в создаваемой конфигурации:



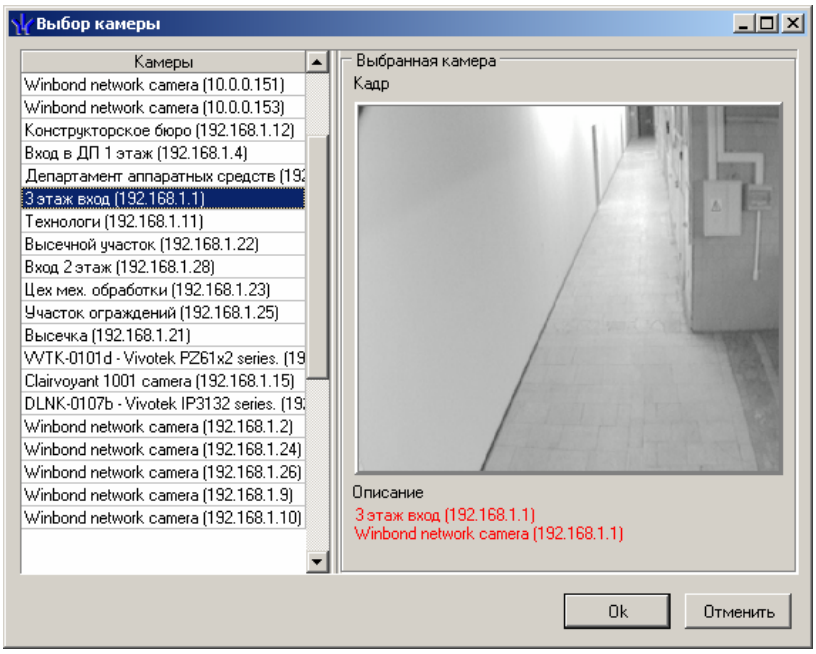
- **Верификация** – параметр, указывающий должен ли раздел Прием посетителей ожидать действий оператора по разрешению прохода в помещение (соответствует значению параметра «ДА»). Или должен только отображать информацию о владельце предъявленной карты, а решение о доступе определяется контроллером доступа, исходя из прав доступа предъявленной карты (соответствует значению параметра «НЕТ»).

- **Команда автоподтверждения – «Разрешить».** В этом случае, по истечении

таймаута верификации, программный модуль автоматически разрешит проход, без вмешательства оператора. «Запретить» – в этом случае, по истечении таймаута верификации, программный модуль автоматически запретит проход, без вмешательства оператора. При этом, оператор в течение этого времени может самостоятельно принять нужное для него решение, путем нажатия соответствующих кнопок.

- **Таймаут верификации** — параметр, определяющий время ожидания подтверждения при верификации, заданный предварительно в параметрах считывателя в разделе Конфигуратор.

- **Камера** – позволяет выбрать камеру видеонаблюдения, информация с которой будет отображаться в рабочем окне раздела. Для ее выбора необходимо воспользоваться кнопкой [...] и в появившемся диалоговом окне выбрать нужную камеру видеонаблюдения:

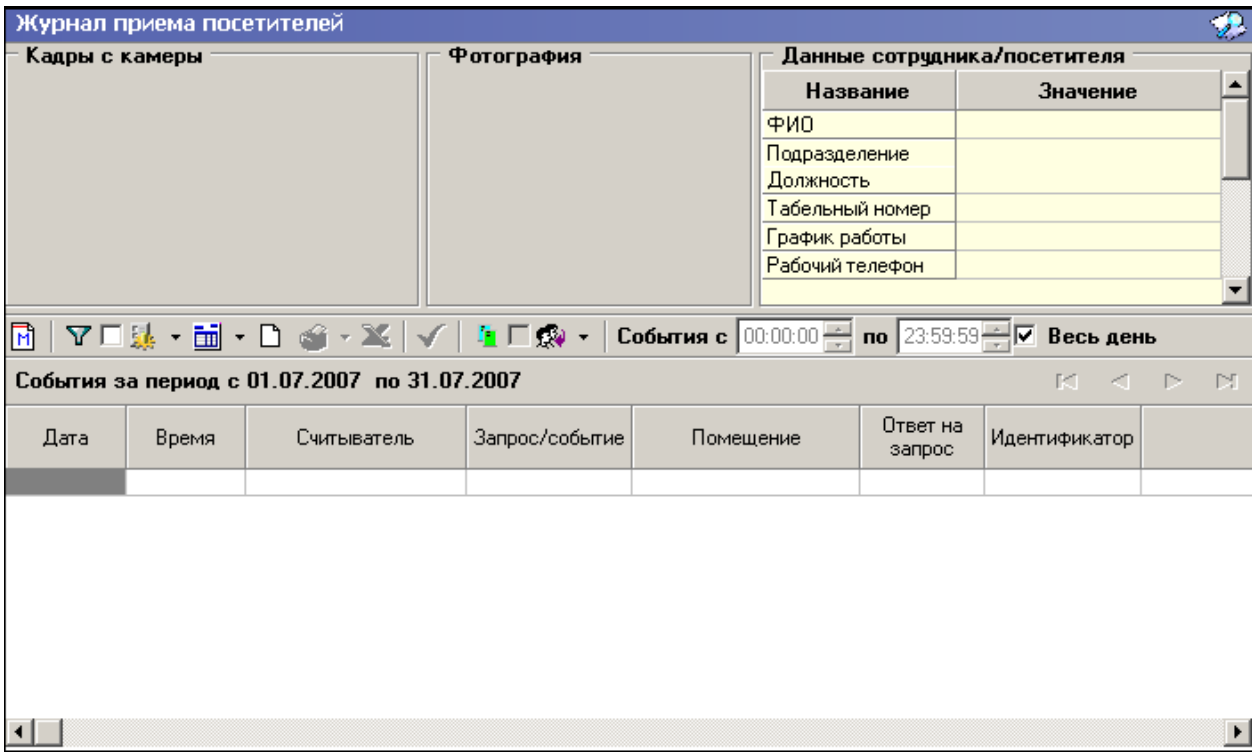


- **Количество записываемых кадров** – параметр, указывающий какое количество кадров будет записано при предъявлении карты доступа к выбранному считывателю.

Для завершения работы по созданию конфигурации необходимо нажать на кнопку «**ОК**». После этого программный раздел **Прием посетителей** автоматически перейдет в режим работы в соответствии с созданной конфигурацией.

Журнал приема посетителя

Раздел **Журнал приема посетителей** предназначен для просмотра данных о фактах предъявления карт доступа к контролируемым считывателям, которые контролируются разделом **Прием посетителей**.



Информация о значении кнопок управления приведена в руководстве оператора по разделу **Журнал приема посетителей**.

Верхняя часть окна предназначена для отображения видеоинформации, записанной при предъявлении карты, фотографии владельца предъявленной карты доступа и его данных.

В нижней части окна расположены события обработанные разделом **Прием посетителей**.

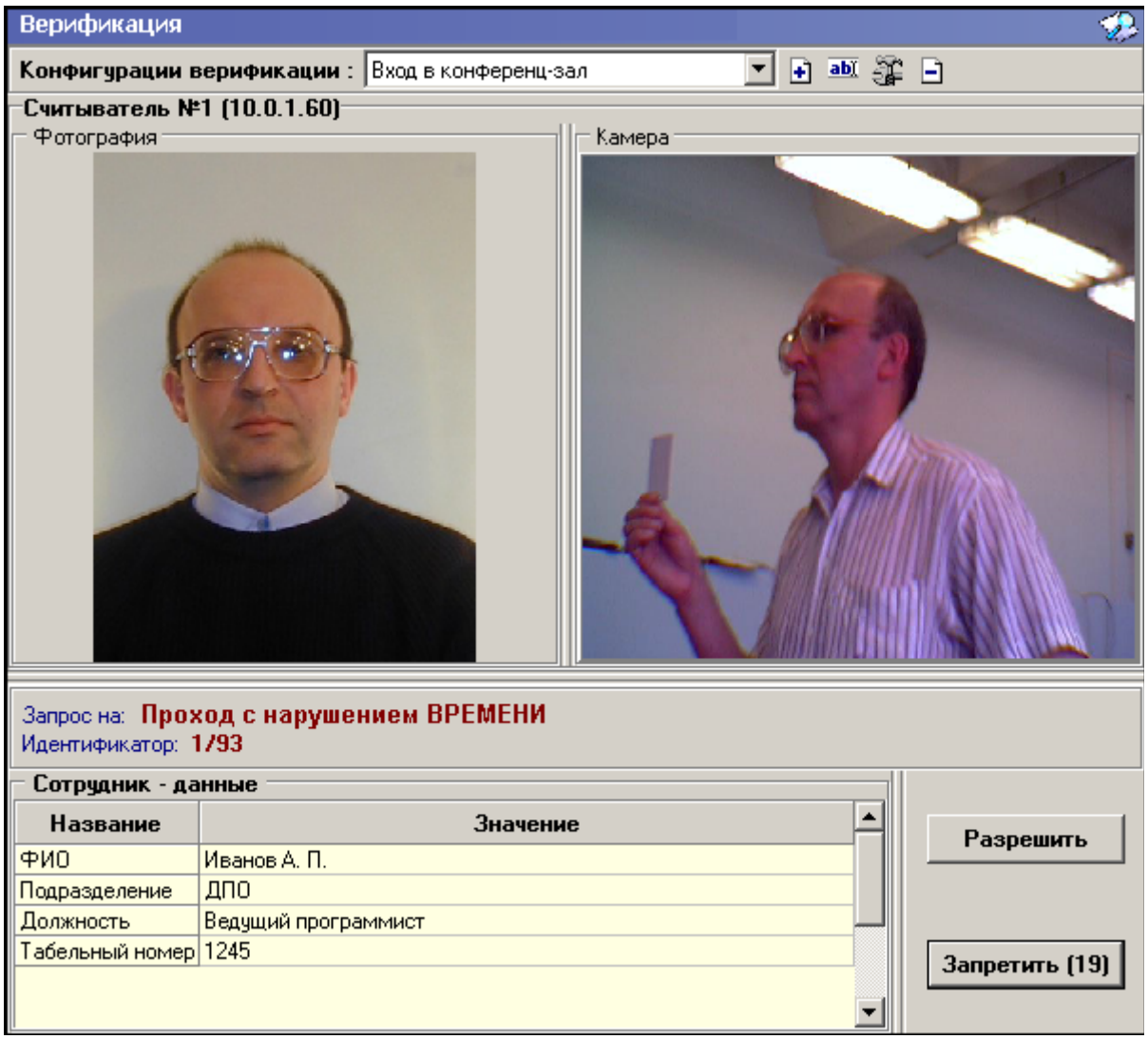
ВЕРИФИКАЦИЯ

Модуль **Верификация** PERCo-SM09 «Видеоидентификация» предназначен для организации рабочего места сотрудника службы безопасности по контролю входа в особо охраняемы помещения, контроля за нарушениями доступа посетителей и контроля за фактами постановки/снятия с охраны помещений. Так же этот раздел может быть использован для отображения информации о владельце предъявленной карты доступа на проходной.

Кроме отображения информации о сотруднике, раздел **Верификация** позволяет отображать и записывать видеоинформацию, полученную с выбранных камер.

Одновременно раздел **Верификация** позволяет контролировать до 4 точек прохода и 4 камер видеонаблюдения.

Все действия оператора, информация о фактах предъявления карт доступа, видеоинформация автоматически записываются разделом и доступны для последующего просмотра и анализа.

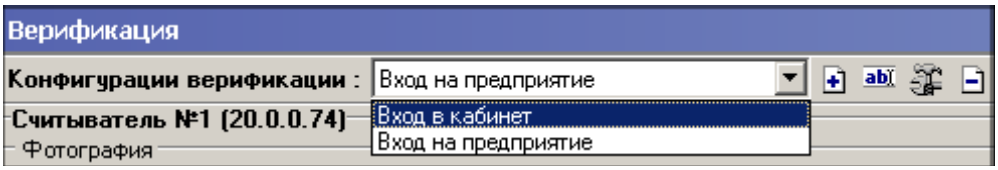


Для организации рабочего места необходимо:

1. Определить какие точки доступа и в каких ситуациях будут контролироваться разделом **Верификация**.
2. Определить на каком рабочем месте будет осуществляться работа модуля.
3. Проверить наличие связи (прохождение IP пакетов) между выбранным рабочим местом и компьютером, на котором установлен сервер системы, контроллерами, точки доступа которых будут контролироваться, и видеокамерами, информация с которых будет сопоставлена выбранным точкам доступа.
4. Провести инсталляцию модуля **Верификация** на выбранном компьютере.
5. Описать конфигурацию раздела **Верификация**.

Учитывая, что в зависимости от режима работы предприятия, может возникнуть необходимость контролировать доступ в различные помещения, на одном рабочем месте может быть создано несколько конфигураций. Переключение между ними может осуществлять оператор в соответствии с установленными административными правилами. Для переключения между конфигурациями необходимо воспользоваться выпадающим

списком в верхней части рабочего окна при условии, что данному оператору это будет разрешено:



Об установке прав оператора по работе с этим разделом смотрите соответствующий раздел данного руководства.

Возможность переключения между конфигурациями может быть проиллюстрирована следующим примером.

Например, до начала рабочего дня и после его окончания оператор контролирует вход/выход на территорию предприятия, проверяя соответствие предъявленного пропуска сотруднику, его предъявившему. После начала рабочего дня оператор меняет конфигурацию раздела, выбирая другую. И начинает контролировать вход в администрацию предприятия.

Такая организация работы позволяет уменьшить затраты на организацию дополнительного рабочего места сотрудника безопасности.

ПРИМЕЧАНИЕ

Конфигурация схем работы раздела **Верификация** записывается локально на каждом рабочем месте. Таким образом, в случае наличия в системе нескольких рабочих мест необходимо создать конфигурации работы на каждом рабочем месте.

Для удаления конфигурации раздела **Верификация** предназначена кнопка .

Для изменения названия конфигурации кнопка .

Для изменения конфигурации кнопка .

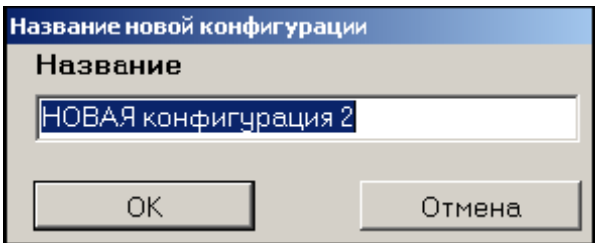
Кнопки **Разрешить**, **Запретить** становятся активными только в случае предъявления карты, при условии, что данное предъявление обрабатывается разделом. И предназначены для принятия решения оператором.

ПРИМЕЧАНИЕ

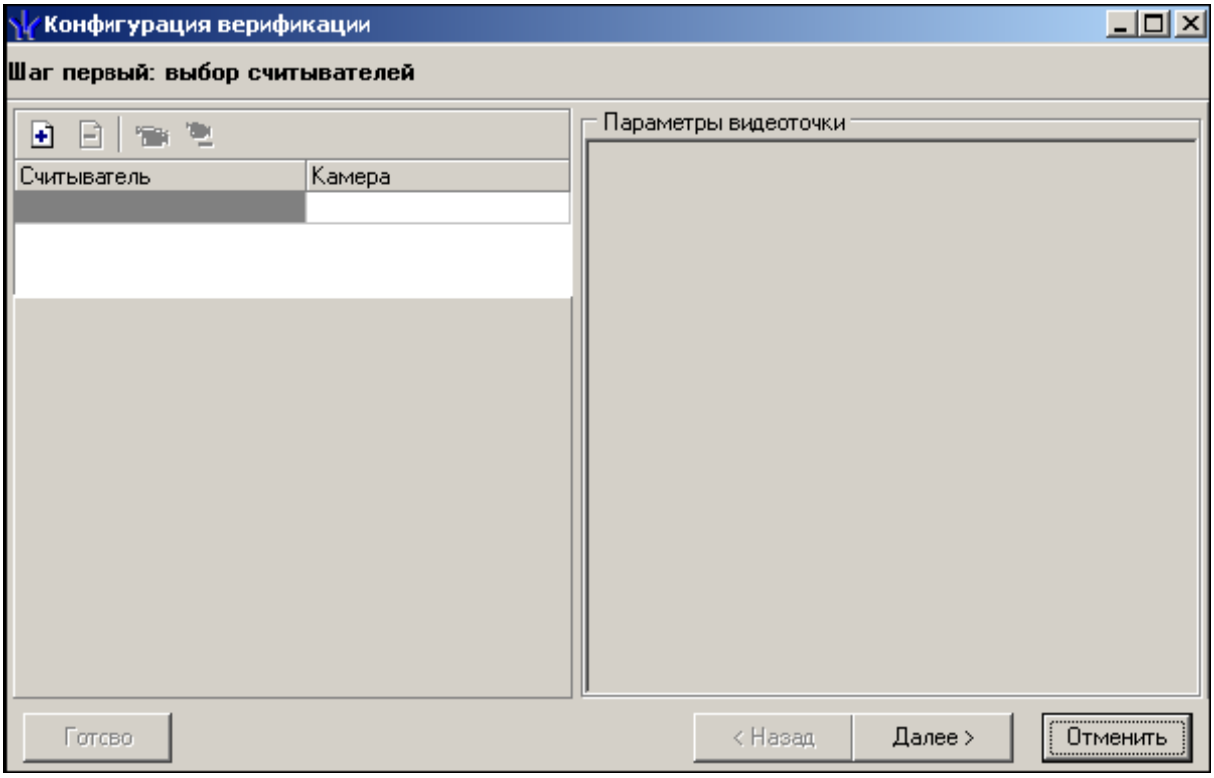
Контроль за предъявлением карт доступа в режиме верификации для выбранного считывателя может осуществляться только из одного раздела **Верификация**. Не возможно организовать несколько рабочих мест операторов раздела **Верификация,** контролирующих одно и то же устройство.

Конфигурация модуля

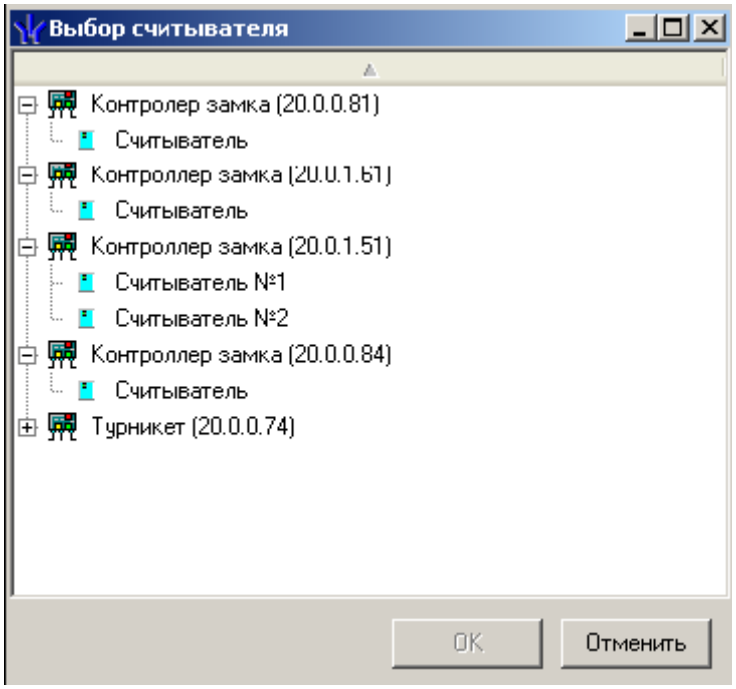
Для создания новой конфигурации необходимо воспользоваться кнопкой **Добавить** — или горячими клавишами **Ctrl** + **N**. При этом появится следующее диалоговое окно, в котором вам необходимо задать название:



Это название будет отображаться в раскрывающемся списке при выборе текущей конфигурации раздела **Верификация**. После нажатия на кнопку «**ОК**» появится диалоговое окно задания параметров создаваемой конфигурации:



В этом окне необходимо выбрать те считыватели, проход через которые будут контролироваться на данном рабочем месте. Максимально в одной конфигурации может быть добавлено 4 считывателя. Для добавления считывателя необходимо нажать на кнопку  . При этом появится следующее диалоговое окно:



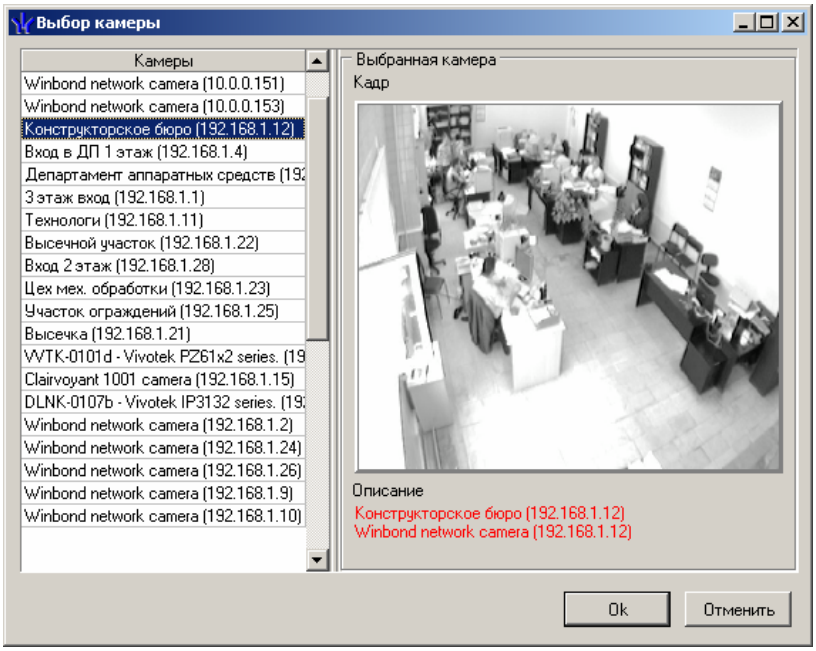
В этом окне вы должны выбрать тот считыватель, проход через который будет контролироваться в данной конфигурации.

Для удаления считывателей добавленных ошибочно необходимо воспользоваться кнопкой  .

После добавления всех считывателей добавьте видеокамеру, которая расположена вблизи этого считывателя и которая позволит оператору дистанционно контролировать ситуацию в месте установки считывателя.

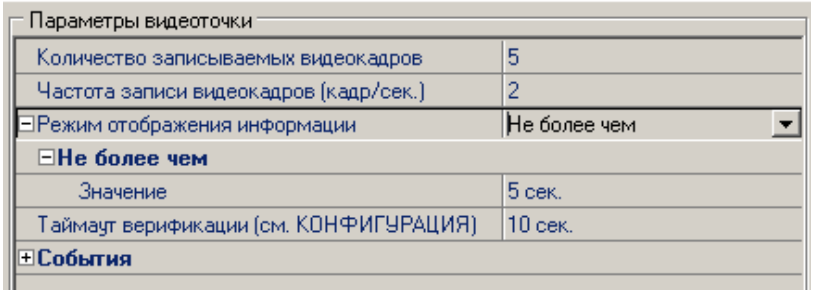
Для этого необходимо воспользоваться кнопкой  , расположенной в графе **Камера**.

При этом в диалоговом окне будет отображен список всех видеокамер входящих в конфигурацию системы безопасности:



Для удобства выбора в правой части окна при выборе камеры автоматически отображается видеоизображение.

После добавления всех необходимых считывателей и видеокамер укажите в каких ситуация и как должен работать раздел **Верификация** при предъявлении карты доступа к каждому из выбранных считывателей. Для этого выберите поочередно каждый из добавленных считывателей и в правой части окна задайте необходимые параметры.



1. **Количество записываемых видеокадров** – параметр, задающий количество записываемых видеокадров с выбранной видеокамеры при предъявлении карты доступа к выбранному считывателю.

2. **Частота записи видеокадров** – параметр, задающий интервал записи видеокадров.

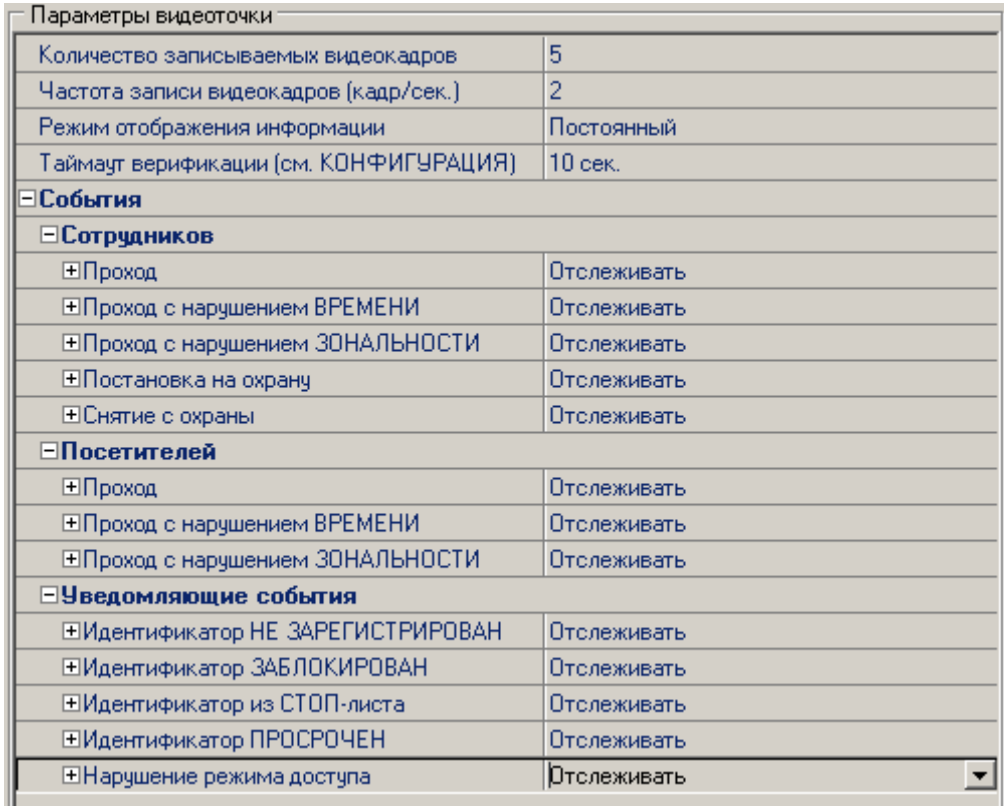
3. **Режим отображения информации** – параметр, указывающий в течение какого времени должна в рабочем окне будет отображаться видеоинформация с указанной камеры. Доступны два варианта значения параметра:

4. **Постоянный** – в этом случае в рабочем окне раздела Верификация отображение информации о карте доступа не ограничено временем.

5. **Не более чем** – в этом случае данные идентификатора отображаются после команды в течении времени, указанного в параметре «Значение».

6. **Таймаут верификации** – неизменяемый в данном окне параметр, указывающий время, в течение которого контроллер будет ожидать действий оператора раздела **Верификация**. Значения этого параметра задаются при описании параметров работы выбранного считывателя и описаны в соответствующем разделе данного руководства.

Далее укажите, какие именно события подлежат верификации со стороны оператора раздела **Верификация**. Для этого раскройте параметр «События» выбранного считывателя:



Отслеживание фактов предъявления карт доступа сотрудников описывается в группе «**События – Сотрудников**». Доступны для отслеживания следующие события, связанные с предъявлением карты сотрудника:

1. **Проход** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем.

2. **Проход с нарушением времени** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемой этим считывателем. При этом время предъявления карты не соответствует временному критерию доступа данной карты.

3. **Проход с нарушением зональности** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем. При этом владелец этой карты нарушил правила «защиты от передачи идентификаторов», то есть пытается совершить повторный вход в помещение.

4. **Постановка на охрану** – событие, возникающее при попытке постановки помещения на охрану при помощи карты доступа.

5. **Снятие с охраны** – событие, возникающие при попытке снятия помещения с охраны при помощи карты доступа.

Отслеживание фактов предъявления карт доступа посетителей описывается в группе «События – Посетителей». Доступны для отслеживания следующие события, связанные с предъявлением карты посетителя:

1. **Проход** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое

этим считывателем.

2. **Проход с нарушением времени** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемой этим считывателем. При этом время предъявления карты не соответствует временному критерию доступа данной карты.

3. **Проход с нарушением зональности** – событие, возникающее при предъявлении карты доступа, имеющей право на проход через исполнительное устройство, управляемое этим считывателем. При этом владелец этой карты нарушил правила «антипасбека», то есть пытается совершить повторный вход в помещение.

Отслеживание фактов предъявления карт доступа, не имеющих права на проход через исполнительное устройство, управляемое выбранным считывателем описывается в группе «События – Уведомляющие события». Для отслеживания доступны следующие события:

1. **Идентификатор не зарегистрирован** – событие, возникающее при предъявлении карты доступа, которая не внесена в списки карт системы. То есть эта карта доступа никогда не выдавалась сотрудникам или посетителям предприятия или была выдана, а в последствии была удалена из всех списков.

2. **Идентификатор заблокирован** – возникает в случае предъявления карты доступа, которая была заблокирована. Подробно о блокировке карт доступа смотрите раздел «*Параметры доступа*» данного руководства.

3. **Идентификатор из «СТОП - листа»** - событие, возникающее при предъявлении карты доступа занесенной в стоп лист. Подробно о занесении карты доступа в СТОП – лист смотрите раздел «*Параметры доступа*» данного руководства.

4. **Идентификатор просрочен** – событие, возникающее при предъявлении карты доступа с истекшим сроком действия. Подробно о сроке действия карт доступа смотрите раздел «*Параметры доступа*» данного руководства.

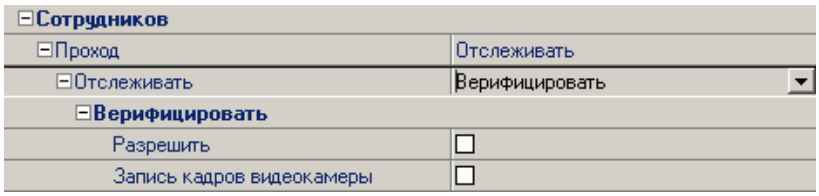
5. **Нарушение режимов доступа** – событие, возникающее при предъявлении карты доступа в режиме «Закрыто» или в режиме «Охрана» при условии, что данная карта доступа не имеет права на снятие помещения с охраны.

Для событий связанных с предъявлением карт доступа сотрудников и посетителей могут быть заданы следующие параметры работы раздела **Верификация**:

- **Не отслеживать** – в этом случае программный раздела Верификация никак не реагирует на предъявление карты доступа.

- **Отслеживать** – в этом случае программный раздела Верификация будет отслеживать предъявление карты доступа и работать в зависимости от следующих установленных параметров:

✓**Не верифицировать** – при установке этого параметра раздела Верификация будет только отображать информацию о владельце предъявленной карты доступа и видеоинформацию с видеокамеры при условии, что она установлена.



✓**Верифицировать** – при установке этого параметра раздел Верификация будет отображать информацию о владельце предъявленной карты доступа и видеоинформацию с видеокамеры при условии, что она установлена. При этом решение о разрешении прохода должен принять оператор путем нажатия той или иной кнопки разрешающей или запрещающей проход.

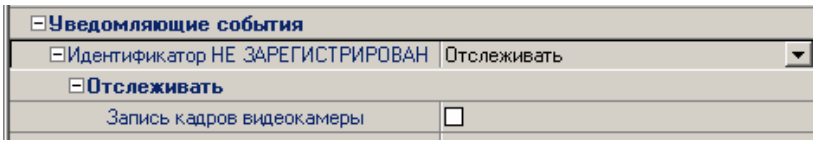
Кроме этого при условии работы программного модуля «Верификация» в режиме верификация могут быть установлены следующие параметры:

- **Разрешить** – в этом случае по истечении таймаута верификации раздел автоматически разрешит проход без вмешательства оператора. При этом оператор в течение этого времени может самостоятельно принять нужное для него решение, используя соответствующие кнопки.

- **Запись кадров видеокамеры** – при выборе этого параметра раздел Верификация будет записывать видеоизображение в количестве и с частотой, указанными в параметрах точки верификации.

Для событий представленных в группе «Уведомляющие события» могут быть заданы следующие параметры работы раздела **Верификация**:

- **Не отслеживать** – в этом случае раздела Верификация никак не реагирует на предъявление карты доступа вызвавшей данное событие.

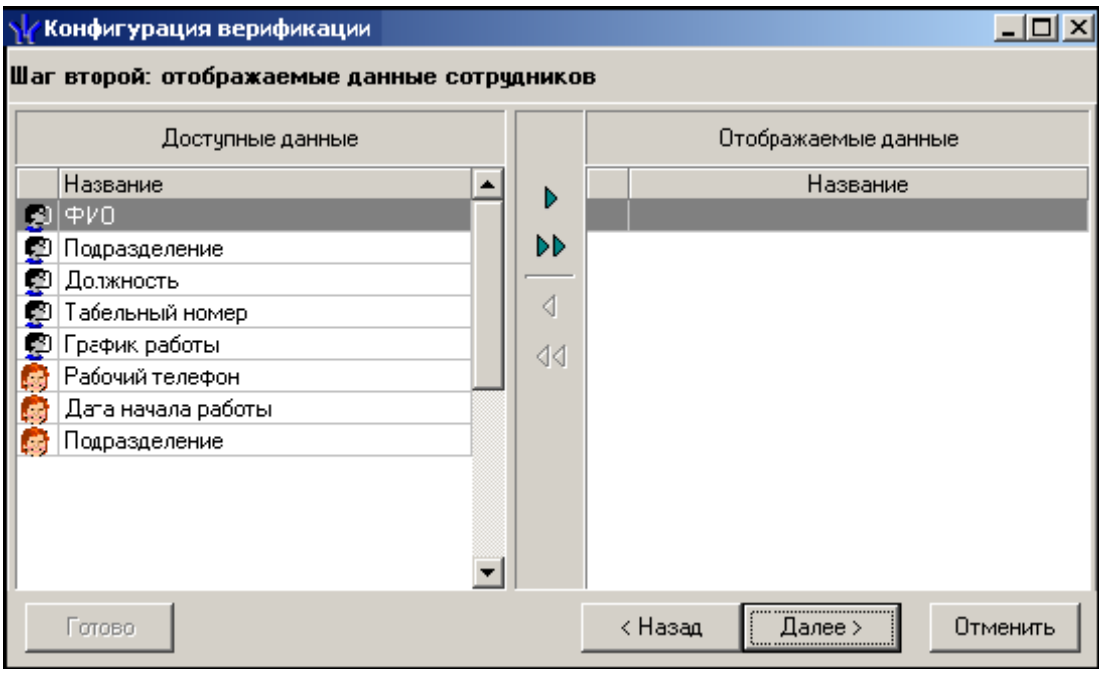


- **Отслеживать** – в этом случае раздел Верификация будет отслеживать предъявление карты доступа вызвавшей это событие, и работать в зависимости от следующих установленных параметров:

- **Запись кадров видеокамеры** – при выборе этого параметра, раздел Верификация будет записывать видеоизображение в количестве и с частотой, указанными в параметрах точки верификации.

После задания параметров работы раздела **Верификация** необходимо нажать на кнопку 

. Вы перейдете на следующий этап задания параметров конфигурации раздела **Верификация**:



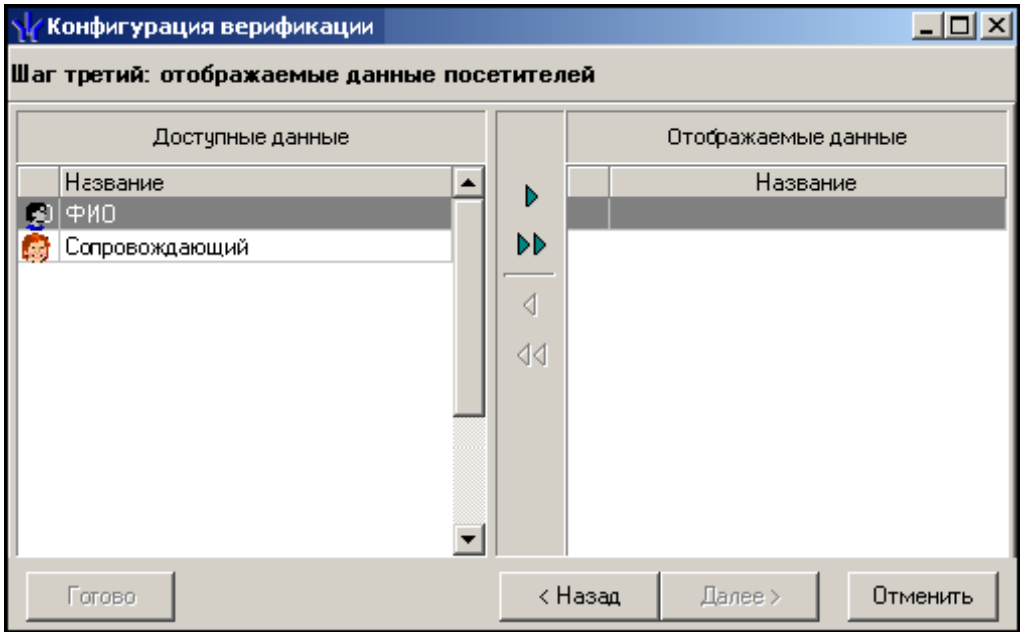
На этом этапе вы определите, какие данные о сотруднике должны отображаться в рабочем окне раздела **Верификация** при предъявлении карты доступа, сотрудника предприятия.

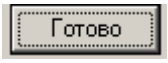
Для выбора данных необходимо выделить их в левой части окна и при помощи стрелок расположенных в центральной части перенести в правую часть окна.

После завершения этой операции необходимо нажать кнопку 

.

В открывшемся окне задайте, какие данные о посетителях предприятия будут отображаться при предъявлении карты доступа посетителя:

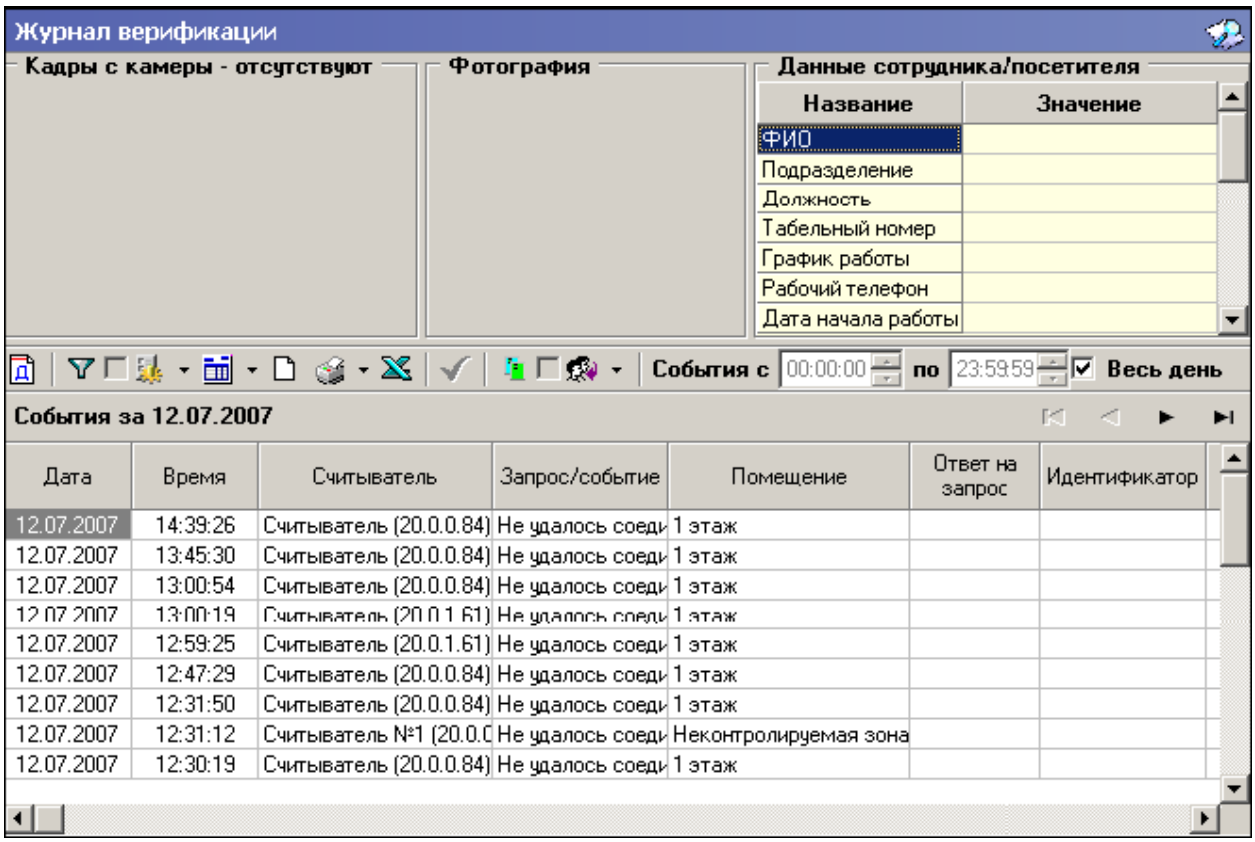


Для завершения действий по созданию конфигурации раздела **Верификация** необходимо нажать на кнопку 

.

Журнал верификации

Раздел **Журнал верификации** предназначен для просмотра данных о фактах предъявления карт доступа к контролируемым считывателям, которые контролируются разделом **Верификация**.



Информация о значении кнопок управления приведена в руководстве оператора по разделу **Журнал верификации**.

Верхняя часть окна предназначена для отображения видеоинформации записанной при предъявлении карты, фотографии владельца предъявленной карты доступа и его данных.

В нижней части окна расположены события обработанные разделом **Верификация**.

ТРЕБОВАНИЯ К АППАРАТУРЕ

Компьютеры:

Объем дискового пространства:

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

Оперативная память:

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

Процессор:

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

Операционная система: Windows 2000 Prof., Windows 2003. Internet Explorer 6.0

Для станции Windows XP, Windows 2000 Prof., Windows 2003. Internet Explorer 6.0

Для сервера системы и сервера видеонаблюдения допустимо использование 64 битных версий операционных систем.

Сеть: 100 Mbit.

ПРИЛОЖЕНИЕ 1. События

События, записываемые в журнал мониторинга и/или регистрации.

События контроллера доступа.

1. События, связанные с перемещением через ИУ

1.1. *Запрет прохода* с причиной:

- *идентификатор НЕ ЗАРЕГИСТРИРОВАН* – предъявленный идентификатор никогда не передавался в контроллер, то есть ему не назначались права доступа в этот контроллер;
- *идентификатор ЗАПРЕЩЁН* - доступ предъявленному идентификатора явным образом запрещен в контроллере, то есть данный контроллер включен в список доступа предъявленного идентификатора с явным запрещением проходов;
- *идентификатор из СТОП-ЛИСТА* - предъявленный идентификатор занесен в «СТОП-ЛИСТ»;
- *идентификатор ПРОСРОЧЕН* — у предъявленного идентификатора истек срок действия, указанный в параметрах доступа;
- *нарушение ВРЕМЕНИ* - у данного контроллера установлен «жесткий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* - у данного контроллера установлена «жесткая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* - это комбинация двух причин, описанных выше: нарушение ВРЕМЕНИ и нарушение ЗОНАЛЬНОСТИ;
- *нарушение КОМИССИОНИРОВАНИЯ* - было зафиксировано несоответствие с 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 сопровождающегося санкционированным системой открытием ИУ. Механической разблокировки двери, турникета с последующим проходом через него.

2. События, связанные с изменением текущего состояния дополнительных входов

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

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

3. События, связанные с изменением текущего состояния дополнительных выходов

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

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

4. События, связанные с изменением текущего состояния корпуса контроллера

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

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

5. События, связанные с работоспособностью сетевых каналов контроллера

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

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

- *Канал мониторинга ОТКРЫТ* — событие возникает при открытии канала мониторинга сервером системы;

- *Канал мониторинга ЗАКРЫТ* — событие возникает при закрытии канала мониторинга сервером системы;

- *Канал мониторинга НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала мониторинга сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу мониторинга другим программным обеспечением (например, локальным ПО);

- *Канал мониторинга неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом мониторинга контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;

- *Попытка открытия канала мониторинга* — событие уведомляет о начале операции по открытию канала мониторинга сервером системы;

- *Нарушение связи с каналом мониторинга* — событие возникает при отсутствии связи между сервером системы и каналом мониторинга контроллера в течении 2 мин.;

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

- *Канал регистрации ОТКРЫТ* — событие возникает при открытии канала регистрации сервером системы;

- *Канал регистрации ЗАКРЫТ* — событие возникает при закрытии канала регистрации сервером системы;

- *Канал регистрации НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала регистрации сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу регистрации другим программным обеспечением (например, локальным ПО);

- *Канал регистрации неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом регистрации контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;

- *Попытка открытия канала регистрации* — событие уведомляет о начале операции по открытию канала регистрации сервером системы;

- *Нарушение связи с каналом регистрации* — событие возникает при отсутствии связи между сервером системы и каналом регистрации контроллера в течении 2 мин.

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

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

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

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

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

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

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

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

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

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

- *памяти FRAM;*
- *памяти DataFlash;*
- *памяти SRAM;*
- *часов RTC;*

- *шины I2C.*

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

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

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

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

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

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

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

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

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

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

7. События, связанные с изменениями состояний группы ресурсов

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

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

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

- *нарушение состояния дополнительного входа.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние дополнительного входа было не нормализовано. Например, датчик движения, подключенный к данному дополнительному входу, находится в активном состоянии;
- *нарушение состояния ресурса ИУ.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние ресурса ИУ было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе постановки группы ресурсов на охрану было зафиксировано несоответствие с 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 являющуюся 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 нормализовано;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.5. *Неисправность снятого ресурса "Шлейф сигнализации".* Событие возникает, если величина сопротивления ШС, у которого параметр «задержка восстановления нарушенного ШС в снятом состоянии» отличен от значений 0 либо 255, и не находящегося в режиме «Охрана», не находится в пределах от 2 до 10 кОм, либо изменилось более чем на 10% в течение часа.

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

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

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

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

- *ресурс "Шлейф сигнализации"*

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

- *ресурс "Шлейф сигнализации"*

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

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

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

События КБО и ППКОП

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

1.1. *Запрет прохода* с причиной:

- *идентификатор НЕ ЗАРЕГИСТРИРОВАН* – предъявленный идентификатор никогда не передавался в контроллер, то есть ему не назначались права доступа в этот контроллер;

- *идентификатор ЗАПРЕЩЁН* - доступ предъявленному идентификатора явным образом запрещен в контроллере, то есть данный контроллер включен в список доступа предъявленного идентификатора с явным запрещением проходов;
- *идентификатор из СТОП-ЛИСТА* - предъявленный идентификатор занесен в «СТОП-ЛИСТ»;
- *идентификатор ПРОСРОЧЕН* — у предъявленного идентификатора истек срок действия, указанный в параметрах доступа;
- *нарушение ВРЕМЕНИ* - у данного контроллера установлен «жесткий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* - у данного контроллера установлена «жесткая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* - это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;
- *нарушение КОМИССИОНИРОВАНИЯ* - было зафиксировано несоответствие с 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. Механической разблокировки двери, турникета с последующим проходом через него.

2. События, связанные с изменением текущего состояния дополнительных выходов

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

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

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

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

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

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

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

3. События, связанные с изменением текущего состояния корпуса контроллера

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

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

4. События, связанные с работоспособностью сетевых каналов контроллера

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- *памяти FRAM;*
- *памяти DataFlash;*
- *памяти SRAM;*
- *часов RTC;*
- *шины I^2C;*
- *ошибки сопроцессора;*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. События, связанные с изменениями состояний зон

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

- *по идентификатору* - если идентификатор имеет соответствующие права.
- *по идентификатору*, подтверждение от ВЕРИФИКАЦИИ - если было подтверждения от верифицирующего устройства.
- *по команде от ПО* - после выполнения команды оператором ПО.
- *по кнопке* - по кнопке на БУИ;
- *безусловно от ПЦН (только для ППКОП) - если ПЦН взял зону на охрану;*
- *по команде оператора ПЦН (только для ППКОП)- если оператор ПЦН взял зону на охрану;*
- по идентификатору с верификацией от ПЦН (только для ППКОП) - *если было подтверждение от ПЦН, как от верифицирующего устройства;*

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

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

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

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

охрану состояние ШС, включенного в эту ОЗ, было не 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 являющуюся 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 любой

и до истечения времени удержания ИУ в открытом состоянии, этот идентификатор не был поднесен повторно.

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

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

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

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

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

- *по команде от ПО* - по команде от оператора ПО;
- *по кнопке* - по кнопке на БУИ;
- *безусловно от ПЦН во время сброса при взятии УОО (только для ППКОП) —*

во время автоматического сброса ПЦН при взятии УОО на охрану;

- *по команде оператора ПЦН во время сброса при взятии УОО (только для ППКОП) - во время сброса ПЦН по команде оператора при взятии УОО на охрану;*

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

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

- *по команде от ПО* - по команде от оператора ПО;

- *по кнопке* - по кнопке на БУИ;

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

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

- *«Неисправность»* - ПЗ перешла в режим «Неисправность»;

- *«Внимание»* - ПЗ перешла в режим «Внимание»;

- *«Пожар»* - ПЗ перешла в режим «Пожар»;

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

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

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

- *по команде оператора ПЦН, нарушены ШС*. Событие возникает, если в процессе взятия ОЗ на охрану по команде оператора ПЦН состояние ШС, включенного в эту ОЗ, было не 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 нормализованных;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.28. *ПШС, сработало 2 извещателя.* Событие возникает, если 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 если осуществлен сброс ПШС по кнопке от БУИ.

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

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

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

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

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

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

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

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

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

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

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

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

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

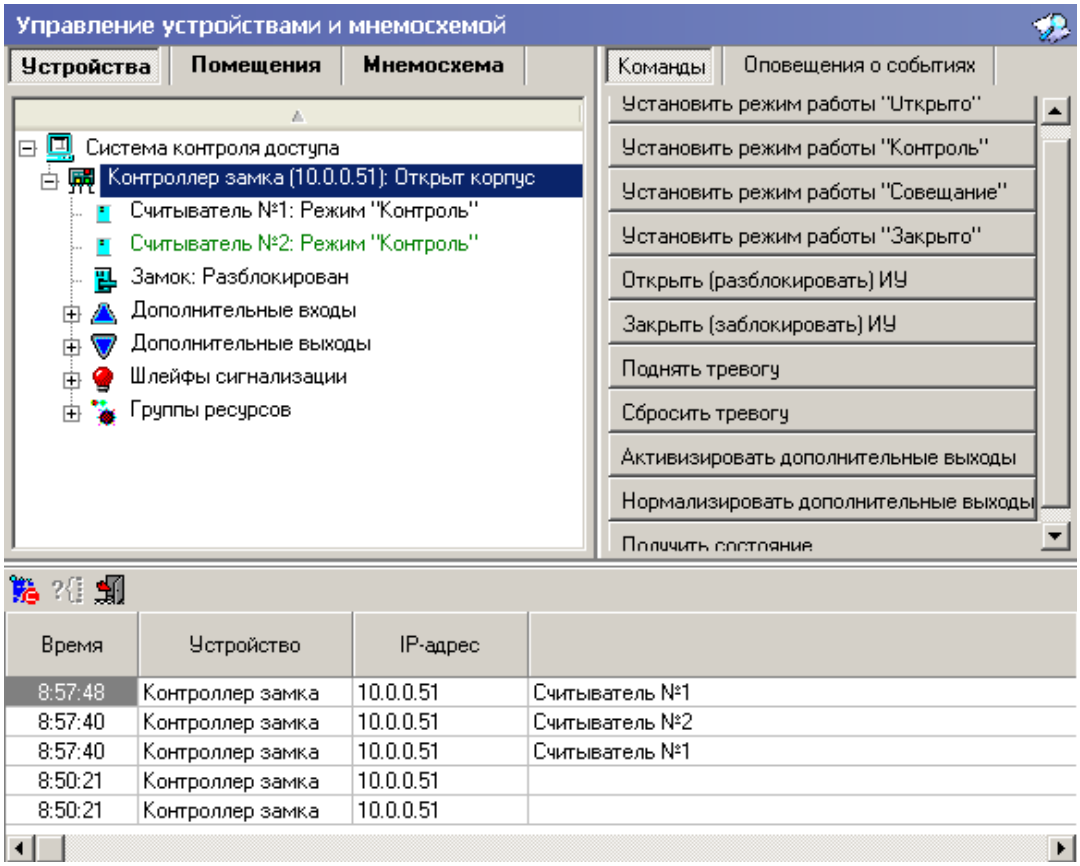
9.4. *Сброс тревоги ИУ*. Событие возникает при снятии ОЗ с охраны, если она до этого находилась в режиме «ТРЕВОГА».

Команды управления

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

Ниже приведен список команд управления доступных для каждого типа устройств.

Контроллер управления доступом



1. **Установить режим работы «Открыто».** Приводит к разблокировке всех исполнительных устройств выбранного контроллера. Исполнительные устройства остаются разблокированными в течение всего времени, пока данный режим не будет сменен. Нажатие на кнопки ДУ исполнительных устройств игнорируются. При предъявлении карт доступа к считывателям данного контроллера регистрируются события о проходе или нарушении доступа. При этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.

2. **Установить режим работы «Контроль».** Приводит к блокировке всех исполнительных устройств выбранного контроллера. При нажатии на кнопку ПУ для данного направления или при поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ

разблокируется на время равное времени удержания данного направления ИУ в открытом состоянии. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии.

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

4. **Установить режим работы «Закрыто»**. При включении режима данное направление ИУ блокируется и остается заблокированным в течение всего времени пока режим включен. Нажатие на кнопку ДУ для данного направления игнорируется. Предъявление любой карты вызывает регистрацию события о нарушении прав доступа. Проход через ИУ (открытый механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.

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

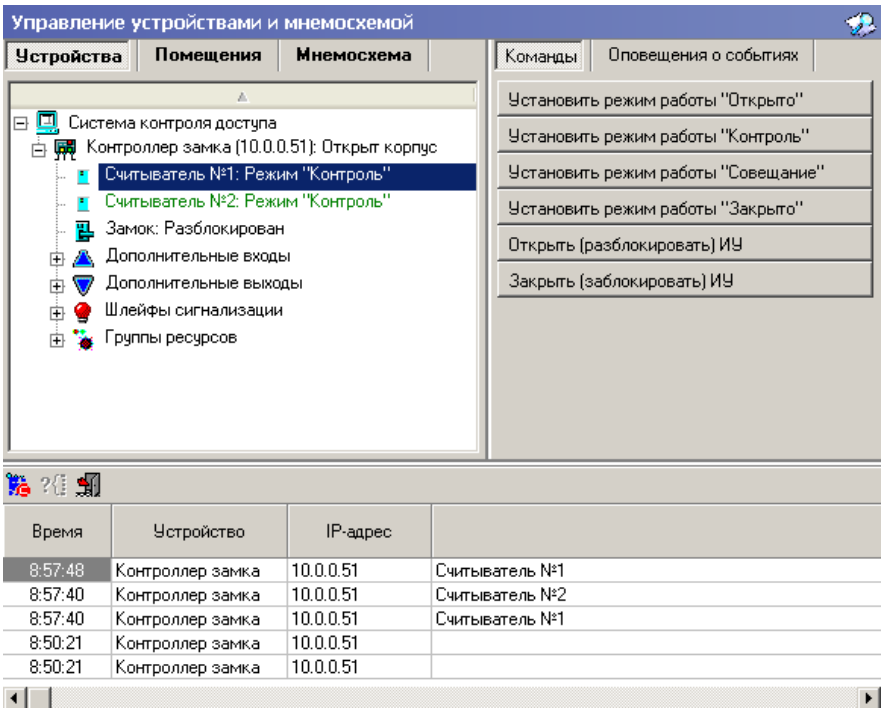
6. **Сбросить тревогу**. Приводит к прекращению выполнения контроллером механизма обработки тревожной ситуации.

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

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

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

Считыватель



1. **Установить режим работы «Открыто».** Приводит к разблокировке

исполнительного устройства, связанного с выбранным считывателем. Исполнительное устройство остается разблокированным в течение всего времени пока данный режим не будет сменен. Нажатие на кнопки ДУ исполнительного устройства игнорируются. При поднесении карты доступа к считывателю регистрируется событие о проходе или нарушении доступа. При этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.

2. **Установить режим работы «Контроль».** Приводит к блокировке исполнительного устройства, связанного с выбранным считывателем. При нажатии на кнопку ДУ для данного направления или при поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ разблокируется на время, которое равно времени удержания данного направления ИУ в открытом состоянии. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии.

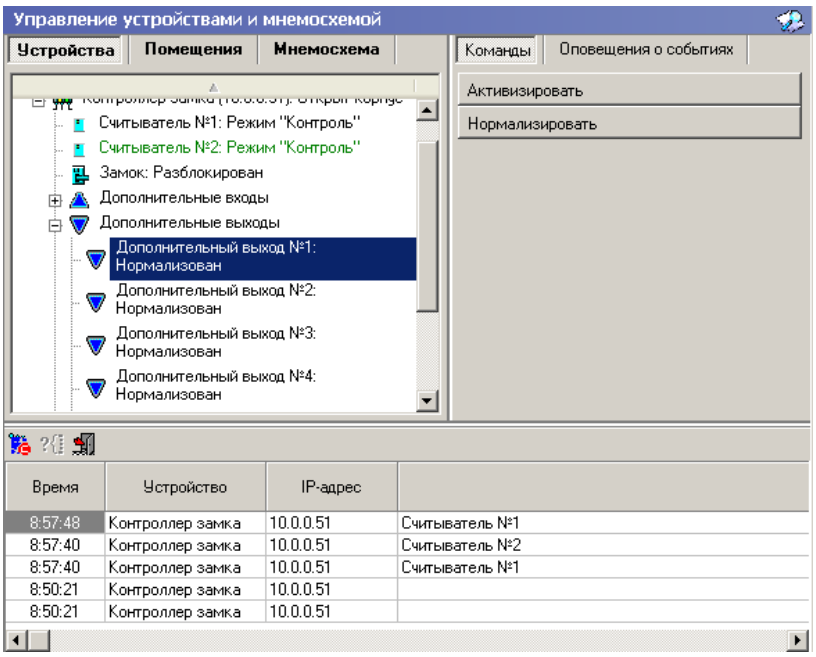
3. **Установить режим работы «Совещание».** Аналогично режиму работы «Контроль» за исключением индикации на считывателе и блоке внутренней индикации. Более подробно об индикации режимов доступа изложено в техническом описании системы безопасности.

4. **Установить режим работы «Закрыто».** При включении режима данное направление ИУ блокируется и остается заблокированным в течение всего времени пока режим включен. Нажатие на кнопку ДУ для данного направления игнорируется. Предъявление любой карты вызывает регистрацию события о нарушении прав доступа. Проход через ИУ (открытый механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.

5. **Открыть (разблокировать) ИУ.** Приводит к разблокировке выбранного считывателя на время удержания в открытом состоянии, заданное при описании параметров функционирования данного ИУ.

6. **Закрыть (заблокировать) ИУ.** Приводит к закрытию выбранного считывателя.

Дополнительный выход



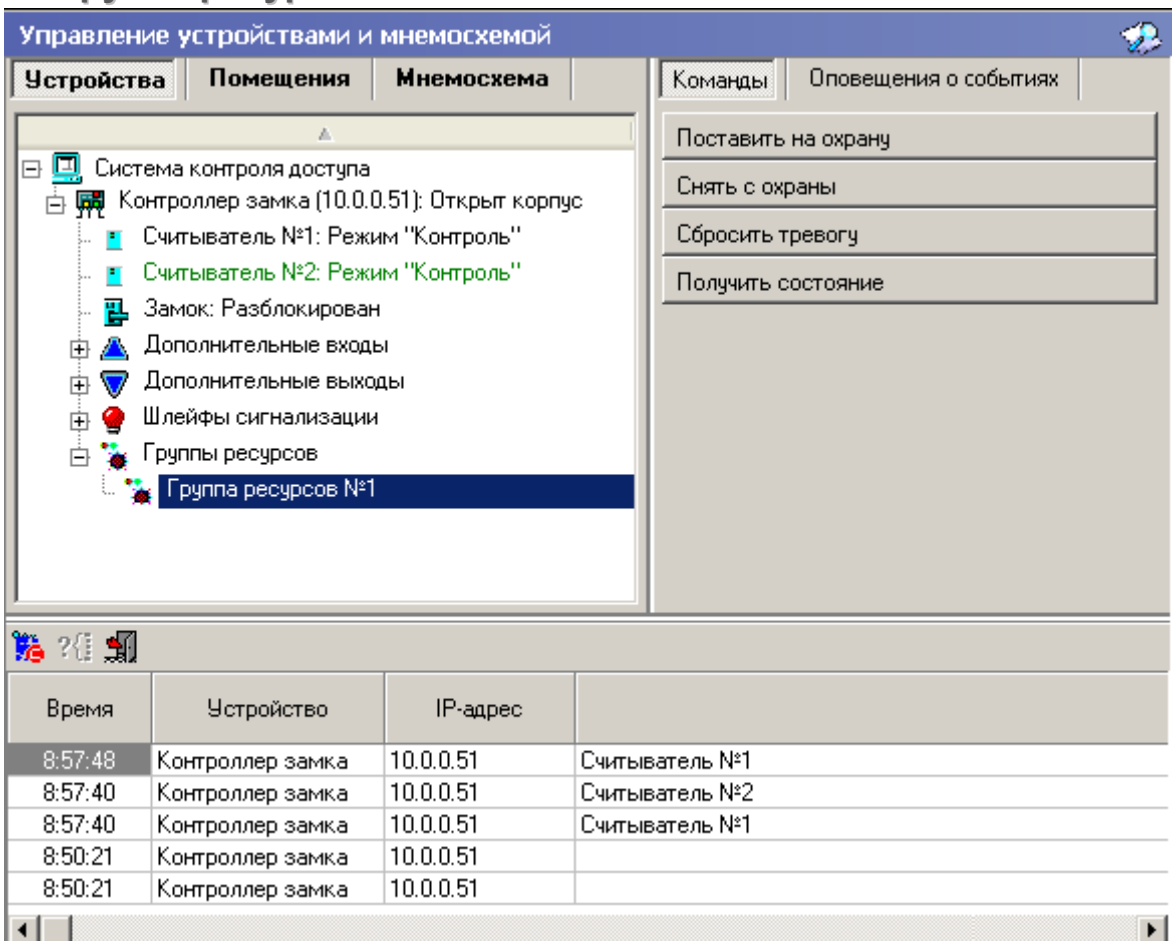
1. **Активизировать**. Приводит к переводу выбранного релейного выхода в активное состояние.

2. **Нормализовать.** Приводит к переводу выбранного релейного выхода в нормальное состояние.

ПРИМЕЧАНИЕ

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

Группа ресурсов



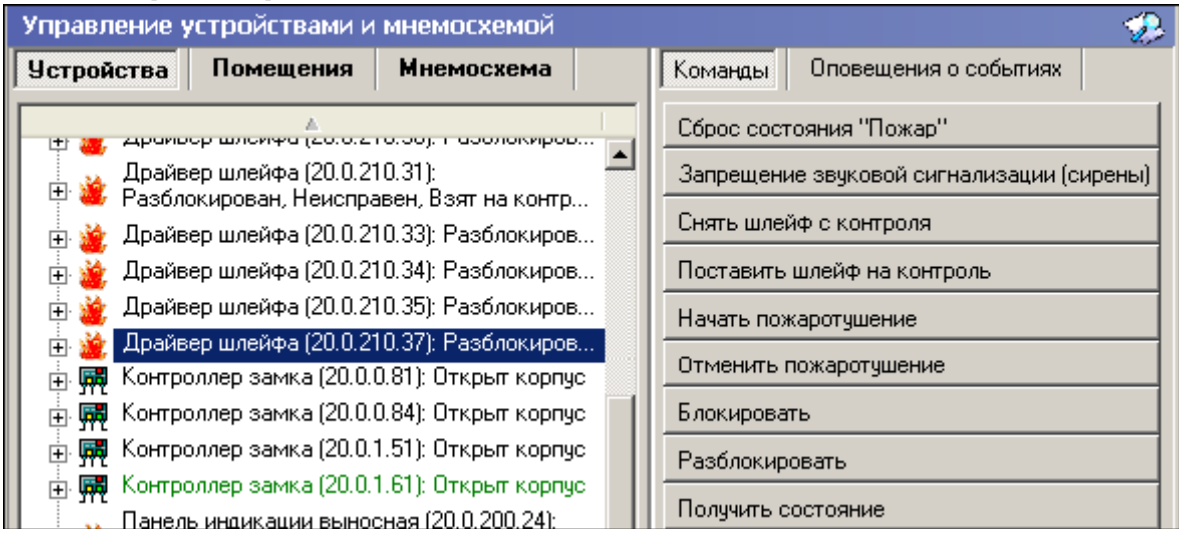
1. **Поставить на охрану**. Приводит к постановке выбранной группы ресурсов на охрану. Если в состав выбранной группы ресурсов входит исполнительное устройство, то ИУ блокируется и остается заблокированным в течение всего времени пока режим включен. Нажатие на кнопку ДУ игнорируется. Открывание двери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

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

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

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

Контроллер ППК



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

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

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

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

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

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