Единая система S–20
Модуль «Администратор»

PERCo-SM01

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Версия ПО: 3.9.6.6

СОДЕРЖАНИЕ

1 Введение

Сетевой модуль ***PERCo-SM01 «Администратор»*** предназначен для организации рабочего места администратора системы безопасности предприятия (организации).

Модуль является дополнительным компонентом расширенного сетевого ПО системы контроля доступа ***PERCo-S-20***.

Модуль ***PERCo-SM01 «Администратор»*** состоит из следующих разделов:

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

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

Отличия раздела от версии, входящей в модуль ***PERCo-SN01 «Базовое ПО»***:

- Возможность настройки параметров подсистемы пожарной сигнализации.
- Возможность настройки параметров видеоподсистемы и камер.
- Задание реакции системы безопасности на события устройств.

«Планировщик заданий» предназначен для создания заданий, выполняемых сервером системы автоматически по расписанию или при выполнении определенного условия. Заданием может являться набор команд по управлению устройствами системы или отправка SMS-сообщений.

«Отчет по SMS» предназначен для просмотра и печати отчетов об отправке SMS-сообщений в процессе выполнения заданий, созданных в разделе ***«Планировщик заданий»***.

2 «Консоль управления»

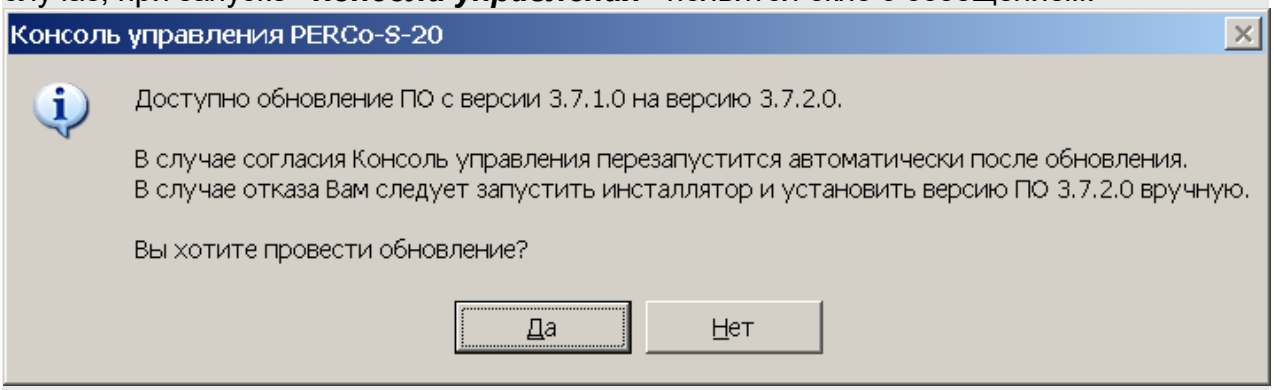
2.1 Запуск консоли

«Консоль управления» представляет собой программную оболочку, обеспечивающую доступ и навигацию оператора по установленным на ПК разделам ПО, связь с сервером системы, получение и сохранение информации из БД системы.

Примечание:

Для версий сетевого ПО выпущенных позднее версии 3.6.3.0, в системе реализована функция автоматического обновления. Функция позволяет обновить ПО ***«Консоли управления»*** и всех установленных на ПК сетевых модулей.

Процедура обновления будет запущена автоматически после подключения к серверу системы, если на сервере системы установлена более поздняя версия ПО. В этом случае, при запуске ***«Консоли управления»*** появится окно с сообщением:

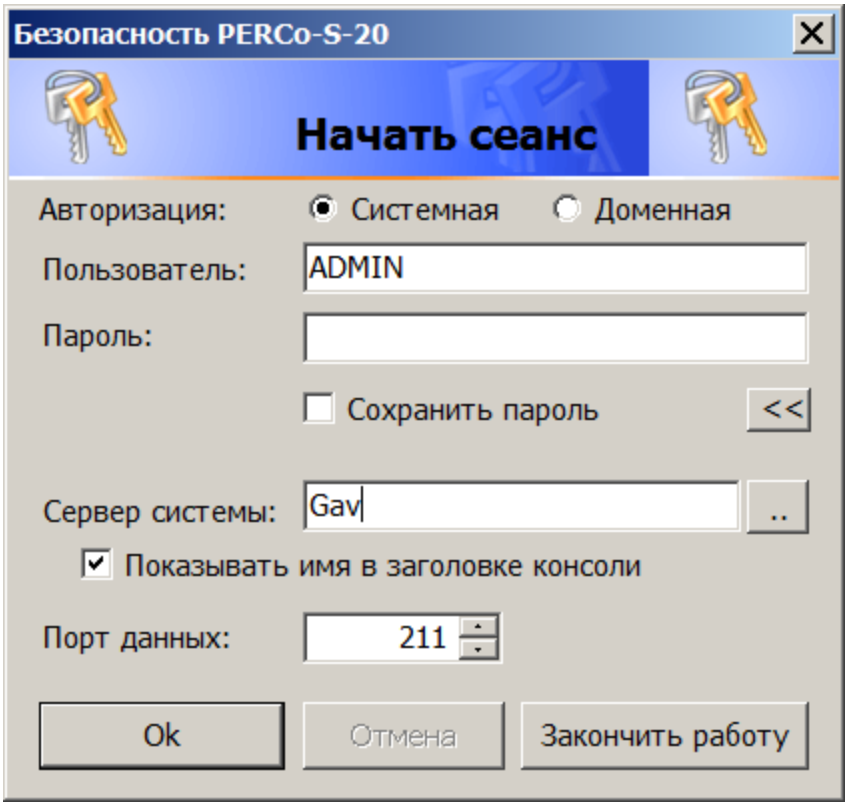


Для начала обновления нажмите кнопку **Да**.

Для запуска консоли выполните следующие действия:

1. Нажмите иконку **Консоль управления PERCo-S-20** на рабочем столе компьютера. Или нажмите кнопку **Пуск (Start)** и выберите последовательно: **Программы (All Programs) > PERCo > PERCo-S-20,** в открывшемся меню нажмите пункт **Консоль управления PERCo-S-20**.
2. Начнется запуск программы, на экране появится заставка Единой системы ***PERCo-S-20*** с указанием версии установленной ***«Консоли управления»***:

3. По окончании загрузки откроется окно **Безопасность PERCo-S-20 Начать сеанс**:



- **Авторизация** – переключатель позволяет выбрать тип учетной записи оператора, используемой при авторизации в системе. В разделе ***«Назначение прав доступа операторов»*** предусмотрена возможность создания учетных записей двух типов:
  - **Системная** – если запись создана непосредственно в разделе;
  - **Доменная** – если запись импортирована из БД службы каталогов *MS Active Directory*. При выборе этого типа учетной записи нет необходимости вводить имя (логин) и пароль.
- **Пользователь** – поле для ввода имени оператора (логина). По умолчанию, в поле отображается имя оператора, последим совершившим удачный вход в систему.
- **Пароль** – поле ввода пароля оператора.
- **Сохранить пароль** – если флажок установлен, то после правильного ввода имени и пароля оператора, в случае успешного входа в систему, при последующих запусках ***«Консоли управления»*** они запрашиваться не будут. Если флажок снят, то имя пользователя и пароль запрашиваются при каждом входе в систему.

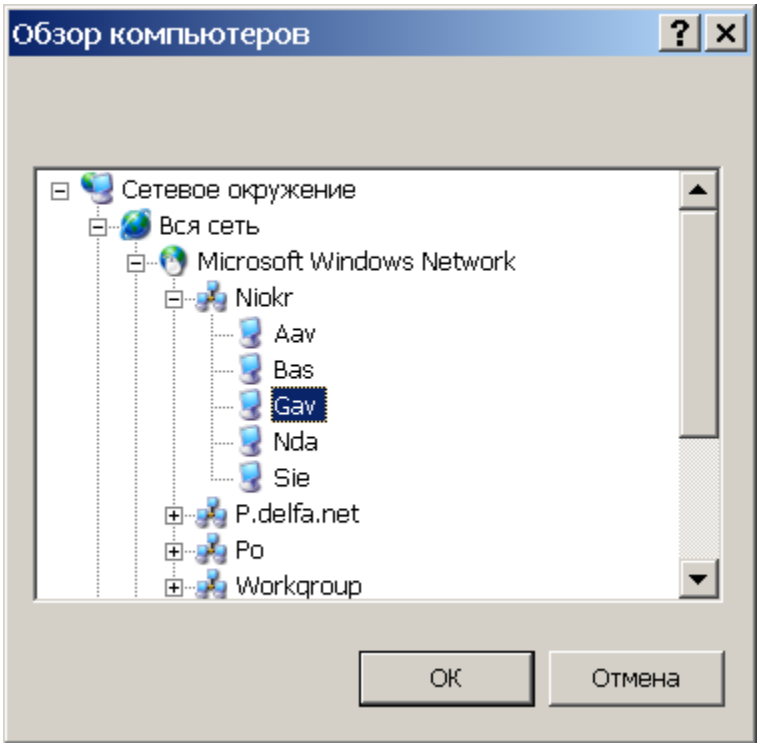
Примечание:

Если флажок **Сохранить пароль** был установлен, (при запуске системы окно **Безопасность PERCo-S-20 Начать сеанс** не открывается), и возникла необходимость сменить оператора, то после входа в систему необходимо нажать кнопку **Закончить сеанс** на панели инструментов ***«Консоли управления»***, в открывшемся окне снять флажок **Сохранить пароль** и нажать кнопку **ОК**.

После этого при запуске откроется окно **Безопасность PERCo-S-20 Начать сеанс**.

- << / >> – кнопка позволяет скрыть/открыть дополнительные поля ввода **Сервер системы** и **Порт данных**.

- **Сервер системы** – поле для ввода имени или IP-адреса компьютера, на котором установлен сервер системы. (Если сервер системы установлен на этом же компьютере, введите в строке: `localhost`.)
- **Показывать имя в заголовке консоли** – при установке флажка в строке заголовка ***«Консоли управления»*** будет отображаться имя или IP-адреса компьютера, на котором установлен сервер системы.
-  – кнопка позволяет открыть окно **Обзор компьютеров** для указания компьютера, на котором установлен сервер системы безопасности в локальной сети:

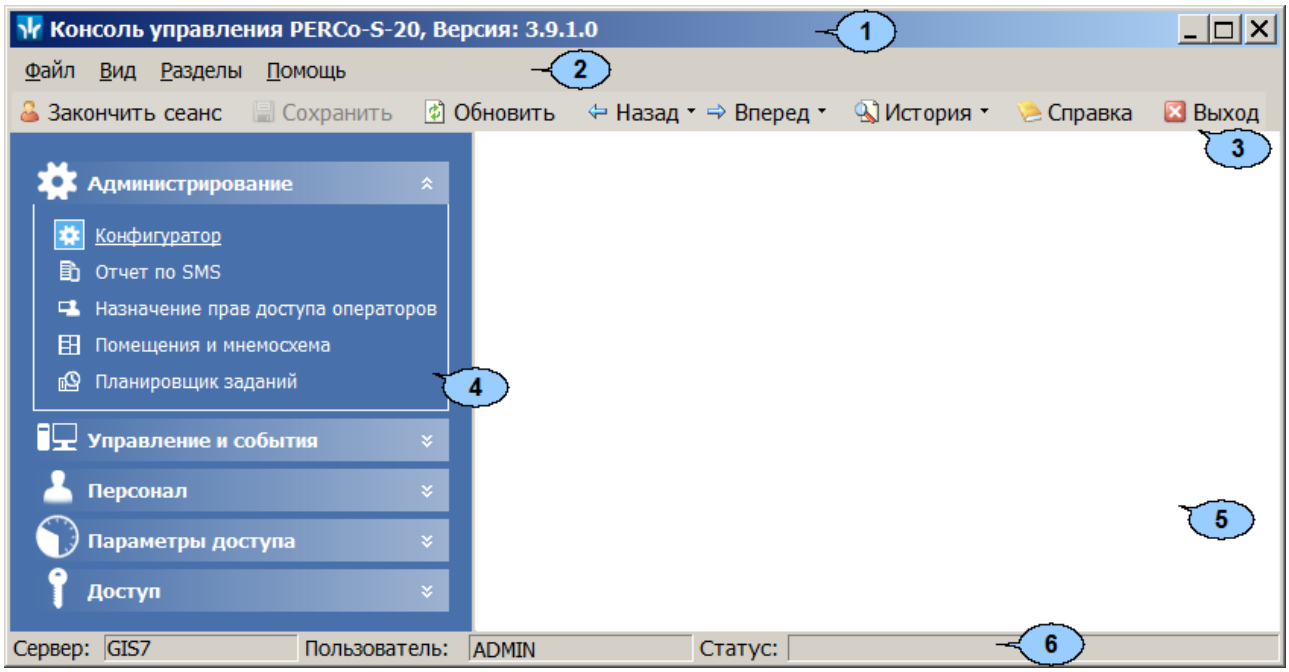


- **Порт данных** – строка позволяет указать порт, по которому будет осуществляться обмен данными с сервером системы. Порт должен совпадать с указанным в ***«Центре управления PERCo-S-20»*** (см. *«Руководство администратора PERCo-S-20»*). По умолчанию установлен порт `211`.

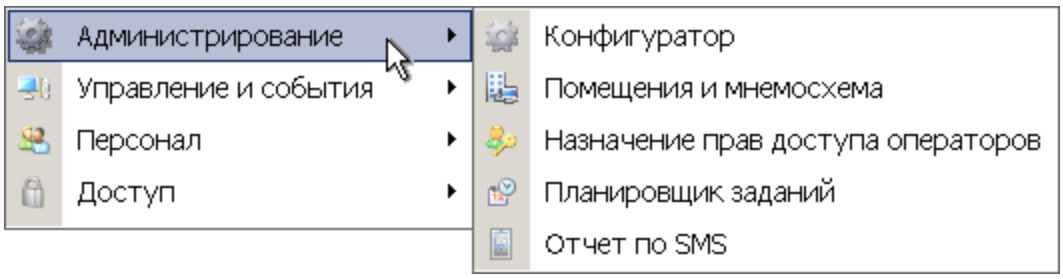
4. В строки **Пользователь** и **Пароль** введите имя и пароль, назначенные вам администратором системы. Пароль должен вводиться латиницей, проверьте раскладку клавиатуры. После трех неудачных попыток ввода приложение будет закрыто. Для уточнения имени и пароля обратитесь к администратору системы безопасности. Если ***«Консоль управления»*** запускается впервые, то необходимо также указать компьютер, на котором расположен сервер системы безопасности.
5. Нажмите кнопку **ОК**. Откроется рабочее окно «***Консоли управления»***.

2.2 Элементы управления

Рабочее окно ***«Консоли управления»*** имеет следующий вид:



1. Строка заголовка окна. В строке указана версия запущенной ***«Консоли управления»*** и имеются следующие кнопки для управления окном:
   – кнопка **Свернуть** позволяет скрыть окно программы на панель задач;
   / – кнопка **Развернуть/ Свернуть в окно** позволяет развернуть окно программы на весь экран/ свернуть в локальное окно с возможностью регулирования его размеров;
   – кнопка **Закрыть** позволяет завершить работу программы и закрыть окно.
2. Основное меню состоит из следующих пунктов:
   - **Файл** – меню данного пункта содержит команду **Выход F10**, позволяющую завершить работу программы.
   - **Вид** – меню данного пункта содержит команду **Панель навигатора F11**, позволяющую скрыть или открыть панель навигатора.
   - **Разделы** – меню данного пункта содержит список групп разделов со списками команд для перехода к одному из установленных на компьютере разделов:



Примечание:

Состав доступных оператору разделов определяется выданными ему в разделе ***«Назначение прав доступа операторов»*** полномочиями на разделы.

- **Помощь** – меню данного пункта содержит следующие команды:
  Справка F1 – команда позволяет вызвать контекстную справку по открытому в рабочей области разделу:

Домашняя страница Shift+Ctrl+F1 – команда позволяет при наличии подключения к сети *Internet* открыть в браузере сайт компании ***PERCo***: http://www.perco.ru/.

Служба поддержки Ctrl+F1 – команда позволяет при наличии подключения к сети *Internet* отправить по электронной почте письмо в службу поддержки компании ***PERCo*** по адресу: soft@perco.ru. Адрес службы поддержки, тема письма и строка приветствия при этом будут вставлены автоматически.

О программе – команда позволяет открыть окно **О программе...** с информацией о версии запущенной ***«Консоли управления»*** и установленных на ПК модулях ПО.

3. Панель инструментов содержит следующие кнопки:

Закончить сеанс – кнопка позволяет сменить оператора, то есть запустить ***«Консоли управления»*** под другой учетной записью.

Сохранить – кнопка позволяет сохранить измененные данные в базе данных программы. кнопка доступна, если какие-либо данные не были сохранены.

Обновить – кнопка позволяет обновить данные, отображаемые в рабочем окне открытого раздела, из базы данных программы. Перед обновлением необходимо сохранить измененные данные, нажав кнопку **Сохранить** панели инструментов, в противном случае данные будут потеряны.

Назад – кнопка позволяет вернуться к разделу, открытому ранее. При нажатии стрелки справа от кнопки откроется меню, позволяющее выбрать один из открытых ранее разделов.

Вперед – кнопка позволяет перейти к разделу, открытому после текущего. При нажатии стрелки справа от кнопки откроется меню, позволяющее выбрать один из открытых позднее разделов.

История – при нажатии стрелки справа от кнопки откроется меню, позволяющее перейти к одному из разделов открытых в ходе текущей сессии.

Справка (**F1**) – кнопка позволяет вызвать контекстную справку по открытому разделу.

Выход (**F10**) – кнопка позволяет завершить работу программы.

4. Панель навигатора содержит кнопки, предназначенные для открытия доступных оператору разделов программного обеспечения. Кнопки объединены в группы по назначению разделов. Кнопки разделов имеют два варианта отображения: в виде крупных или в виде мелких значков. При нажатии правой кнопкой мыши на панели навигатора откроется контекстное меню, содержащее следующие пункты:

Мелкие значки – пункт позволяет отображать мелкие значки для выбранной группы разделов.

Крупные значки – пункт позволяет отображать крупные значки для выбранной группы разделов.

Все мелкие значки – пункт позволяет отображать мелкие значки для всех разделов.

Все крупные значки – пункт позволяет отображать крупные значки для всех разделов.

Развернуть все – пункт позволяет раскрыть списки разделов, входящих во все группы. (Для раскрытия списка разделов, входящих в одну группу, используйте кнопку в заголовке группы.)

Свернуть все – пункт позволяет скрыть списки разделов, входящих во все группы. (Для скрытия списка разделов, входящих в одну группу, используйте кнопку в заголовке группы.)

Примечание:

Расположение групп разделов на панели навигатора можно изменять, перетаскивая группу в нужное место. Для этого нажмите на заголовок группы левой кнопкой мыши и, не отпуская кнопки, наведите указатель мыши на название той группы, перед которой хотите расположить выделенную, после чего отпустите кнопку мыши.

5. Рабочая область ***«Консоли управления»***, в которой отображается рабочее окно открытого раздела.
6. Строка состояния, в которой отображаются:
   - **Сервер** – имя или IP-адреса компьютера, на котором установлен сервер системы;
   - **Пользователь** – имя оператора;
   - **Статус** – состояние программы в поле.

2.3 Выбор раздела

Для открытия раздела произведите одно из следующих действий:

- Нажмите кнопку раздела на панели навигатора, при необходимости предварительно развернув список разделов, входящих в группу.
- В меню **Разделы** выберите группу, в которую входит раздел, затем в открывшемся списке разделов, входящих в группу, выберите нужный раздел.

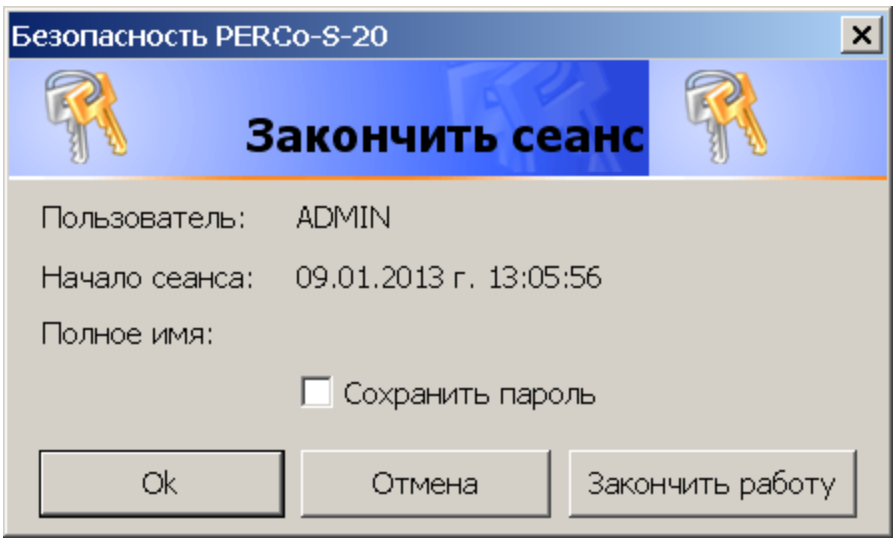
Примечание:

«Консоль управления» запоминает свое состояние при выходе из программы. При следующем запуске в рабочей области будет открыто окно последнего использовавшегося раздела.

2.4 Закрытие консоли

Для завершения работы ***«Консоли управления»*** произведите одно из следующих действий:

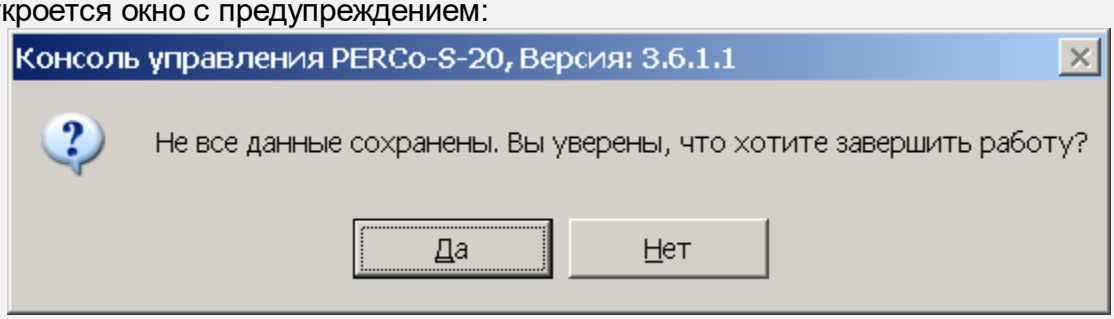
- Нажмите кнопку в строке заголовка окна программы.
- Выберите пункт **Выход F10** в меню **Файл**.
- Нажмите кнопку **F10** на клавиатуре.
- Нажмите кнопку **Выход** на панели инструментов программы.
- Нажмите кнопку **Закончить сеанс** на панели инструментов программы и в открывшемся окне **Безопасность PERCo-S-20. Закончить сеанс** нажмите кнопку **Закончить работу**.



ОК – кнопка позволяет закончить сеанс работы пользователя и открыть окно **Безопасность PERCo-S-20. Начать сеанс** для входа в систему другого пользователя.
Отмена – кнопка позволяет вернуться к работе.
Закончить работу – кнопка позволяет завершить работу программы.
Сохранить пароль – при установке флажка система не будет запрашивать имя и пароль пользователя при входе в систему. При снятии флажка при входе в систему будет открываться окно **Безопасность PERCo-S-20. Начать сеанс**.

Примечание:

Если какие-то данные не были сохранены в базе данных системы безопасности, откроется окно с предупреждением:



Для завершения работы без сохранения данных нажмите **Да**.
Для сохранения данных нажмите кнопку **Нет**, затем нажмите кнопку **Сохранить** на панели инструментов, после чего повторите одно из действий для завершения работы программы.

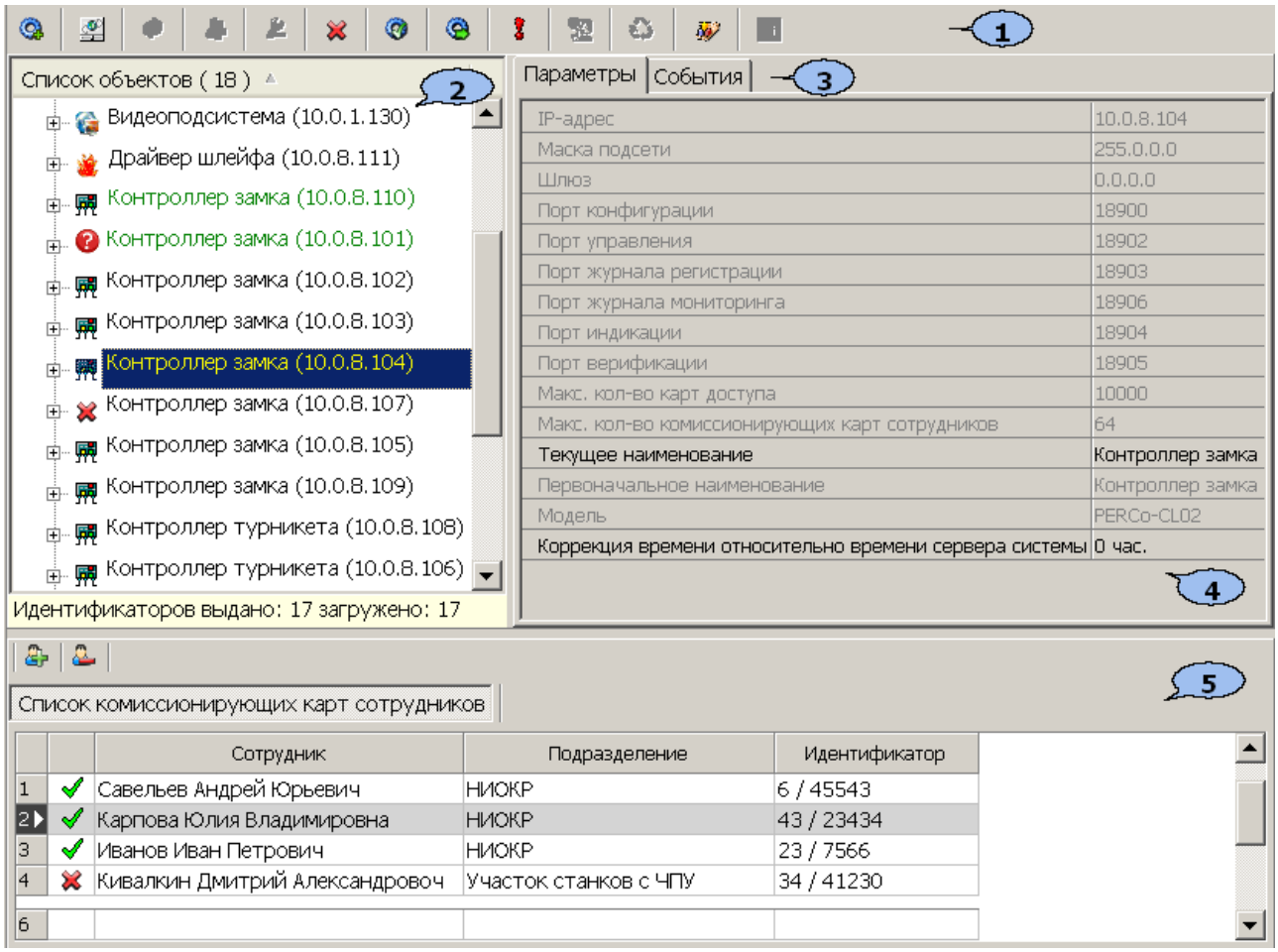
3 Раздел «Конфигуратор»

3.1 Назначение

Раздел «***Конфигуратор»*** (Расширенная версия) предназначен для конфигурации системы, добавления в нее новых устройств, настройки параметров их работы, а также задания реакций на события, регистрируемые в системе. Так же для контроллеров доступа предусмотрена возможность создания списки комиссионирующих карт. Для контроллеров второго уровня списков карт аварийного доступа и для ППКОП списков карт и PIN-кодов постановки и снятия шлейфов сигнализации на охрану.

3.2 Рабочее окно раздела

Рабочее окно раздела имеет следующий вид:



1. Панель инструментов раздела

   Провести конфигурацию **(Ctrl+K)** – кнопка позволяет произвести автоматический поиск устройств в сети и добавление их в конфигурацию системы.

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

Обновить конфигурацию (Ctrl+Alt+K) – кнопка позволяет для контроллера ***PERCo-CT/L04*** привести в соответствие информацию, отображаемую в разделе, с установленной конфигурацией контроллера. Такая процедура может потребоваться после изменения конфигурации при помощи перемычек на плате контроллера или после изменения состава подключенных контроллеров второго уровня.

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

Удалить/ Восстановить (Ctrl+D) – кнопка позволяет удалить из конфигурации устройство, выделенное в рабочей области раздела устройство. Кнопка доступна, если выделенное устройство ранее было исключено из конфигурации при помощи кнопки **Исключить из конфигурации**. Так же кнопка позволяет восстановить скрытое ранее устройство.

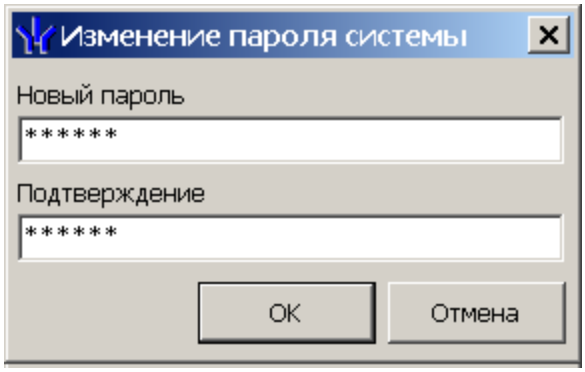
Исключить из конфигурации/ Включить в конфигурацию (Ctrl +O) – кнопка позволяет временно исключить выделенное в рабочей области устройство из конфигурации. Для включения в конфигурацию ранее исключенного устройства (отмеченное в списке объектов значком), выделенное в рабочей области и повторно нажмите кнопку.

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

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

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

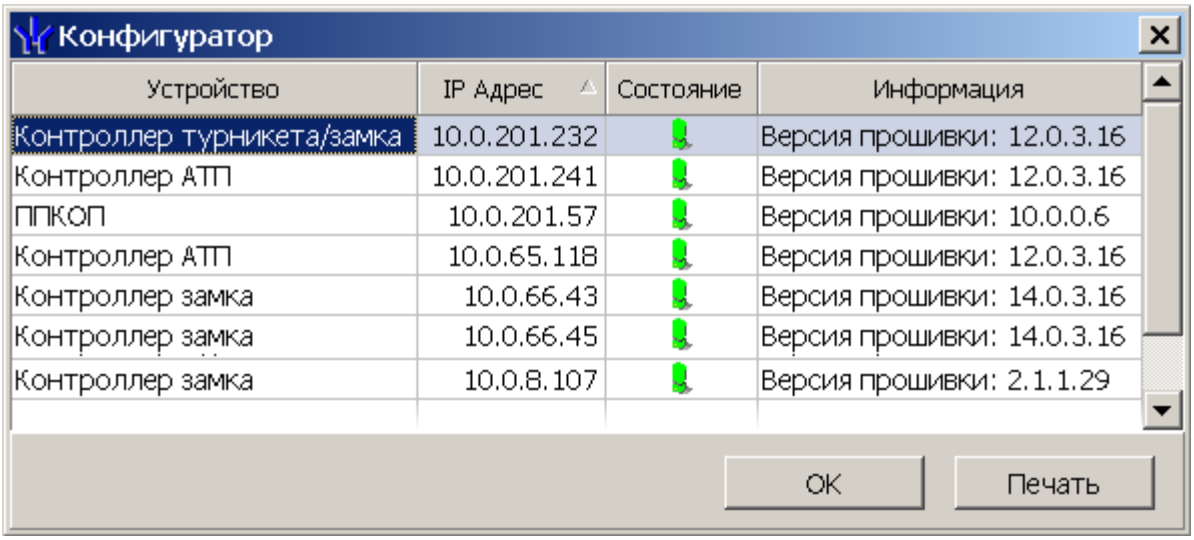
Изменение пароля (Ctrl+P) – кнопка позволяет изменить пароль доступа к контроллерам системы безопасности. Кнопка доступна при выборе в рабочей области корневого элемента списка объектов (по умолчанию «*Система безопасности»*). При нажатии кнопки откроется окно **Изменение пароля системы**:



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

Изменение сетевых настроек (**Ctrl+T**) – кнопка позволяет изменить сетевые настройки выбранного в рабочей области контроллера. Кнопка доступна после исключения выбранного контроллера из конфигурации, то есть при нажатии кнопки **Исключить из конфигурации** .

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



Кнопка **Печать** окна **Конфигуратор** позволяет распечатать представленный список контроллеров.

Получить состояние TCP/IP портов – кнопка позволяет получить диагностическую информацию о состоянии портов выбранного в рабочей области контроллера. Кнопка доступна после исключения выбранного контроллера из конфигурации, то есть при нажатии кнопки **Исключить из конфигурации** (данная кнопка никогда не доступна для встроенного контроллера электронной проходной ***PERCo-KT02.x***).

Кнопка **Копирование параметров между шлейфами и реле аппаратуры "Болид"** – позволяет переносить заданную конфигурацию, заданную на одном шлейфе или реле на другие.

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

Выделение устройства зеленым цветом указывает на то, что параметры устройства были изменены, но не переданы в устройство. Выделение устройства красным означает, что оно скрыто (скрытые устройства отображаются при нажатии кнопки **Отображать скрытые устройства** на панели инструментов).

Значок рядом с наименованиями устройств указывает на его тип и состояние:

– устройство исключено из конфигурации системы безопасности;

– устройство включено в конфигурацию системы безопасности, но не доступно или ему не переданы параметры;

, – устройство является контроллером доступа или ППКОП;

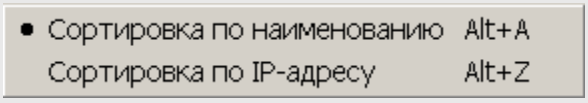
– устройство является видеоподсистемой, включенной в конфигурацию системы безопасности;

– устройство является камерой, добавленной в видеоподсистему;

, , , , , , , , . – ресурсы устройств.

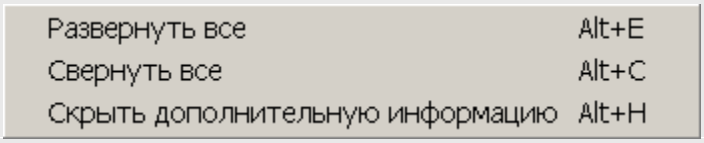
Примечание:

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



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

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



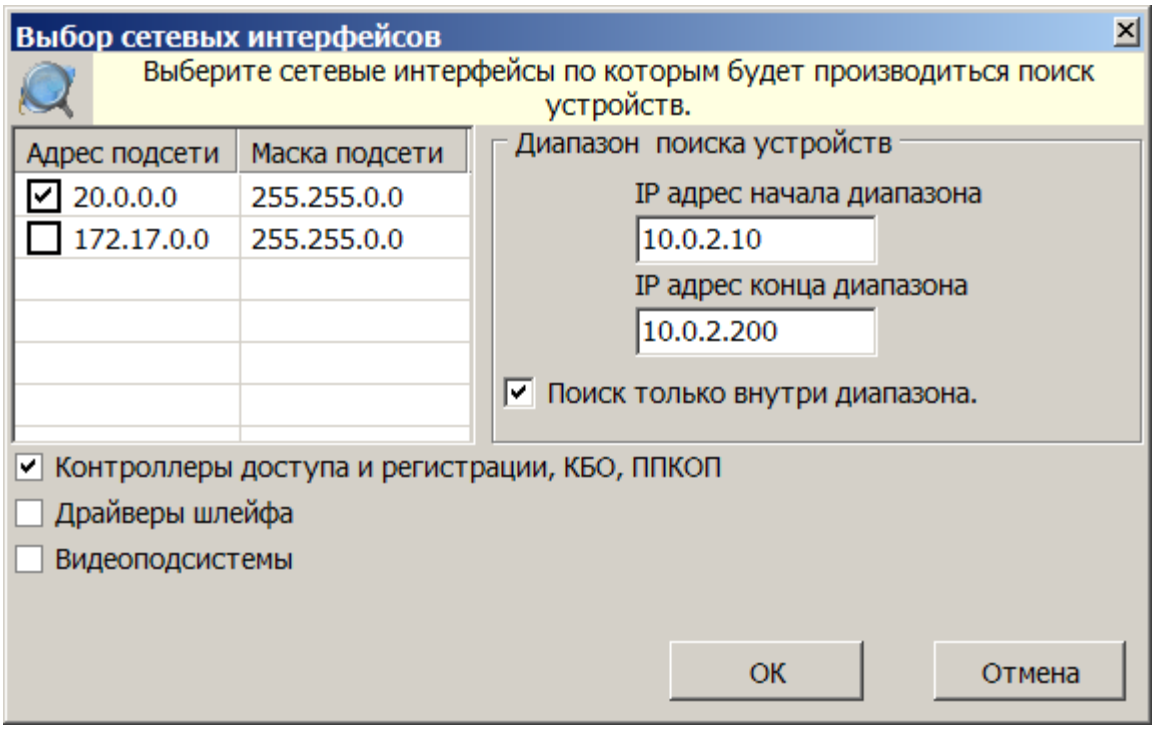
Меню позволяет развернуть, свернуть списки ресурсов для всех устройств, а также открыть и скрыть панель ввода дополнительных данных.

3. Выбор вкладки панели настройки
   - **Параметры.** Вкладка позволяет настроить параметры функционирования устройства или ресурса, выделенного в рабочей области раздела.
   - **События.** На вкладке отображается список событий, регистрируемых системой безопасности для устройства или ресурса, выделенного в рабочей области раздела. Также на вкладке можно задать реакцию системы на любое из событий.
   - **Камера СКУД** Вкладка доступна для ресурса контроллера Считыватель и предназначена для выбора камеры подсистемы ***«Камера СКУД»***.
4. Рабочая область вкладки панели настройки.
5. Панель ввода дополнительных данных. Для открытия и скрытия панели используйте контекстное меню рабочей области раздела или сочетание клавиш **Alt+H**. Значок ✖ в строке с данными сотрудника или PIN-кодом в рабочей области вкладки означает, что данные не были переданы в контроллеры, значок ✔ означает, что данные переданы успешно.

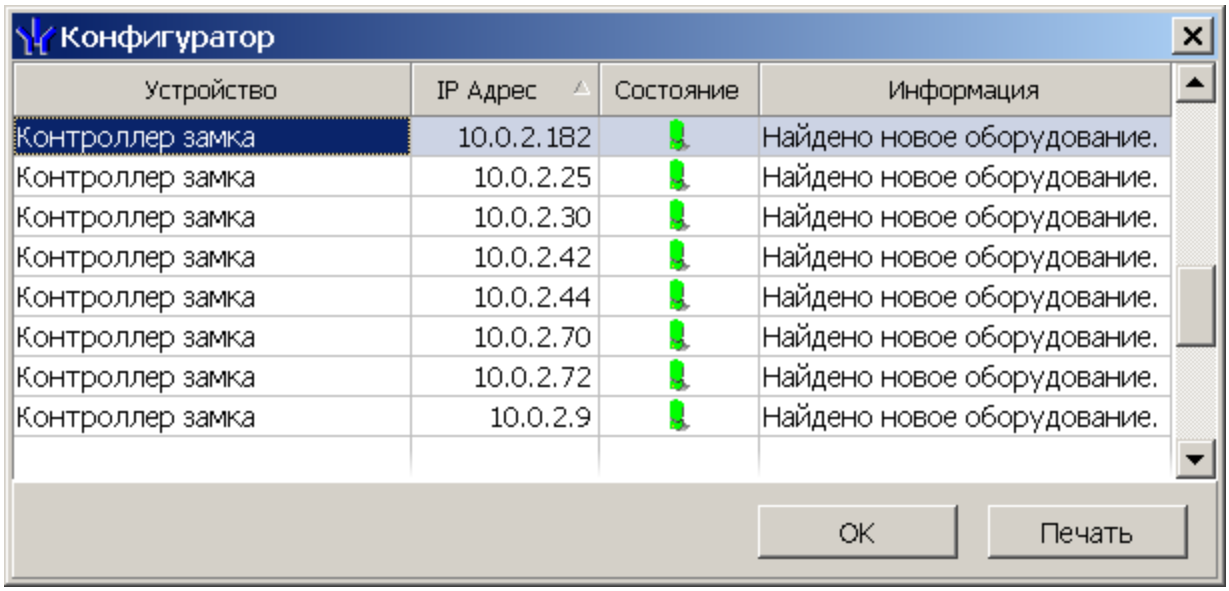
3.3 Автоматическая конфигурация

Для проведения автоматического поиска устройств в локальной сети:

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



2. В рабочей области открывшегося окна отметьте сетевой интерфейс ПК, с которого будут рассылаться запросы на устройства. Поиск производится широковещательной рассылкой запросов в подсети сетевого интерфейса.
3. В нижней части окна отметьте флажками типы искомых устройств.
4. При необходимости адресной отправки запросов на устройств внутри диапазона IP-адресов, укажите в соответствующих полях первый и последний IP-адрес диапазона. В этом случае поиск производится широковещательной рассылкой запросов в подсети сетевого интерфейса и адресно в указанном диапазоне IP-адресов.
5. Для проведения только адресной отправки запросов внутри диапазона IP-адресов установите флажок **Поиск только внутри диапазона**.
6. Нажмите кнопку **ОК**. Окно **Выбор сетевых интерфейсов** будет закрыто, начнется поиск устройств.
7. После завершения поиска откроется окно **Конфигуратор** со списком найденных устройств:

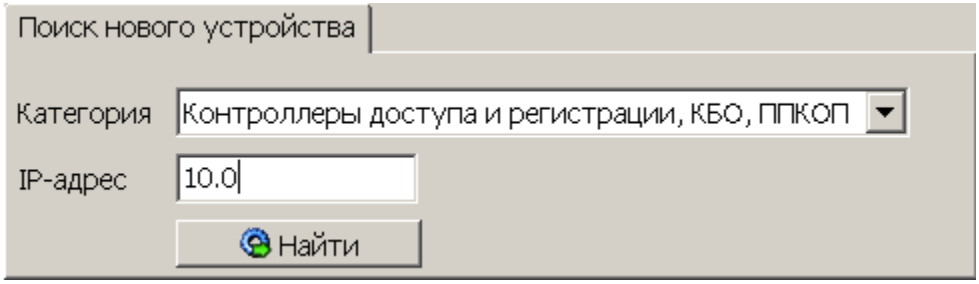


8. Кнопка **Печать** в открывшемся окне позволяет распечатать список найденных устройств.
9. Нажмите кнопку **ОК** (или в заголовке окна). Все найденные устройства будут добавлены в рабочую область раздела и отмечены значками .
10. Если какое-либо из найденных устройство необходимо исключить из конфигурации, выделите его в рабочей области и нажмите кнопку **Исключить из конфигурации** на панели инструментов раздела. Значок устройства изменится на .
11. Для настройки параметров выделите устройство или ресурс в рабочей области раздела и на вкладке **Параметры** панели настройки измените необходимые параметры.
12. Для настройки реакций на события выделите устройство или ресурс в рабочей области раздела и на вкладке **События** панели настройки добавьте необходимые реакции.
13. Выделите в рабочей области раздела корневой элемент (по умолчанию *«Система безопасности»*). На вкладке **Параметры** произведите настройку параметров системы в целом.
14. Для передачи параметров в устройства нажмите кнопку **Передать параметры** на панели инструментов раздела. В случае успешной передачи параметров в устройство значок рядом с его названием в списке объектов изменится на значок, соответствующий типу устройства.

3.4 Добавление нового устройства

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

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

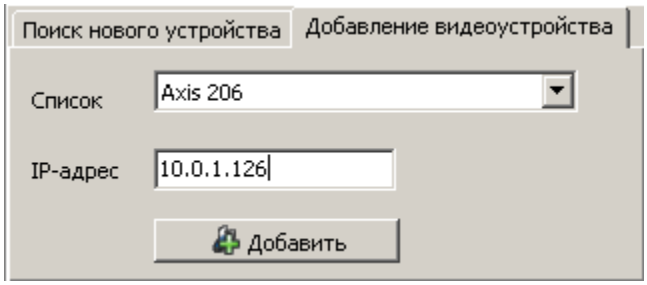


2. Используя раскрывающийся список **Категория**, укажите тип добавляемого устройства:
   - **Контроллеры доступа и регистрации, КБО, ППКОП** – для добавления контроллера доступа, регистрации или ППКОП.

Примечания:

- Порядок конфигурирования видеоподсистемы описан в руководстве администратора системы.
- Список поддерживаемых видеоподсистемой камер наблюдения представлен на сайте компании ***PERCo***, по адресу www.perco.ru, в разделе **Главная> Продукция> Комплексные системы безопасности> Видеокамеры**. Для поддержки некоторых моделей камер требуется установка дополнительных драйверов.

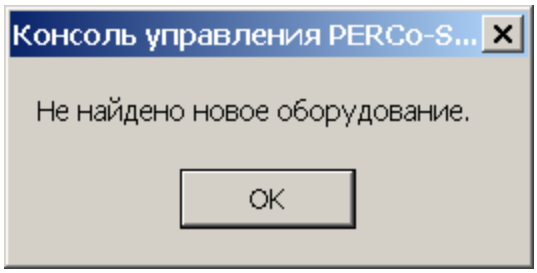
   - **Видеоподсистемы** – для добавления сервера видеоподсистемы с файлами видеоархива.
   - **Камеры и видеосервера видеоподсистемы** – для добавления камер. При выборе пункта становится доступна вкладка **Добавление видеоустройства**. Для добавления камеры в видеоподсистему в раскрывающемся списке **Список** укажите модель камеры, в поле ввода **IP-адрес** укажите адрес и нажмите кнопку **Добавить**.



   - **Камеры стандарта ONVIF видеоподсистемы** – для добавления камер поддерживающих стандарт ONVIF.
   - **Модули управления ИСО "Орион"** – для интеграциеии оборудования *ИСО «Орион»*. При этом в поле **IP-адрес** необходимо указать сетевой адрес ПК на котором установлен ***«Модуль управления ИСО Орион»***. Описание процедуры интеграции с оборудованием *ИСО «Орион»* приведено в руководстве администратора системы.

3. В строку **IP-адрес** введите сетевой адрес искомого устройства. Нажмите ставшую при этом доступной кнопку **Найти**.

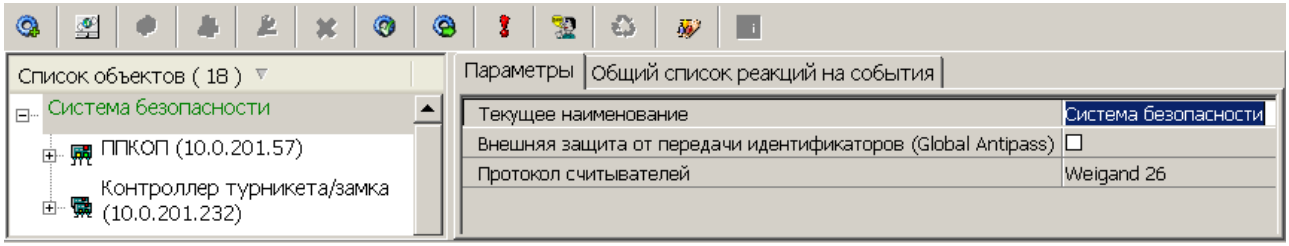
4. В случае успешного поиска откроется окно **Конфигуратор**, содержащее искомое устройство и указывающее состояние связи с ним. Для закрытия окна нажмите кнопку **ОК**. Найденное устройство будет добавлено в рабочую область раздела, отмеченное значком .
5. Если устройство не было найдено, откроется окно с сообщением:



6. Закройте окно, нажав кнопку **ОК**, затем проверьте состояние устройства его подключение к сети *Ethernet*, устраните найденные неполадки, после чего повторите поиск, нажав кнопку **Найти**.
7. Для настройки параметров выделите устройство или его ресурс в рабочей области раздела, затем на вкладке **Параметры** панели настройки измените необходимые параметры.
8. Для настройки реакций на события выделите устройство или его ресурс в рабочей области раздела, затем на вкладке **События** панели настройки добавьте необходимые реакции.
9. Для передачи новых параметров в устройство нажмите кнопку **Передать параметры** на панели инструментов раздела. Устройство будет включено в состав системы безопасности.

3.5 Настройка системы безопасности

Настройки системы безопасности доступны при выборе в рабочей области корневого элемента списка объектов (по умолчанию «*Система безопасности*»):

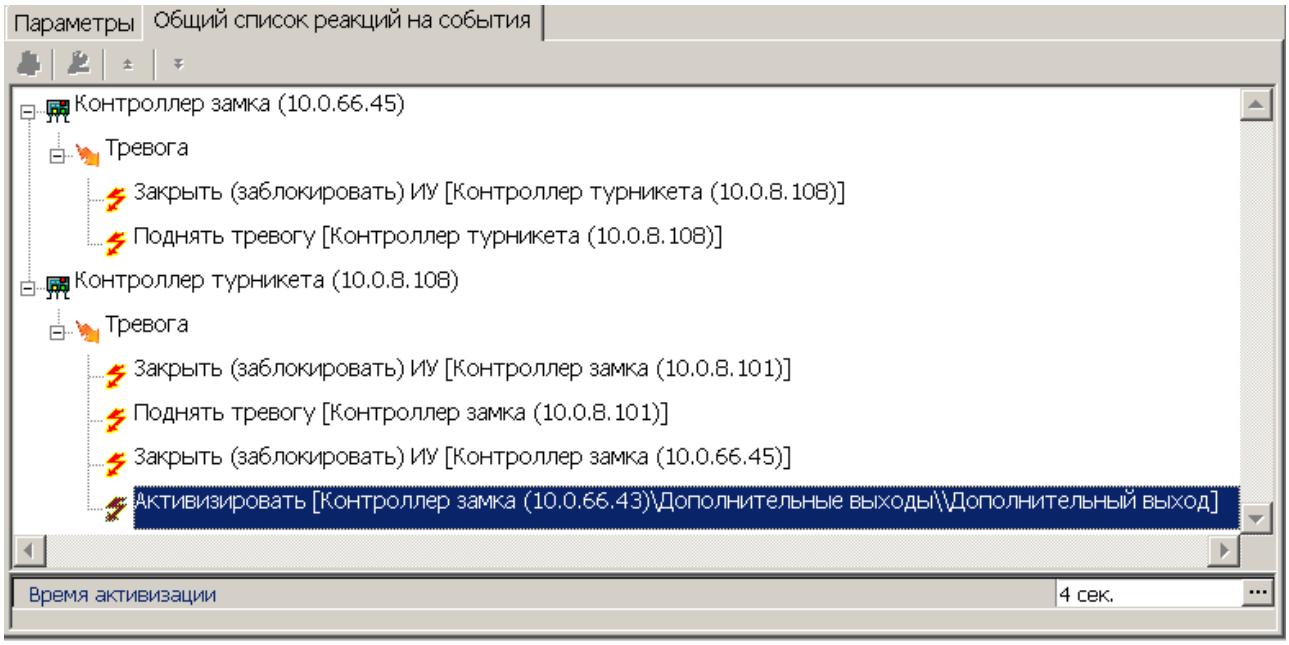


На вкладке **Параметры** доступны следующие параметры системы в целом:

- Строка **Текущее наименование** позволяет изменить описательное название системы безопасности. Значение по умолчанию – *Система безопасности*.
- Флажок **Внешняя защита от передачи идентификаторов (Global Antipass)**. При установке флажка будет включена функция системы безопасности, заключающаяся в контроле нарушений последовательности прохождения (регистрации) сотрудников через точки прохода и направления прохода. Последовательность прохождения точек прохода определяется взаимным расположением пространственных зон с учетом их вложенности (то есть нельзя войти в помещение, не войдя в здание).
- Раскрывающийся список **Протокол считывателей** позволяет выбрать один из форматов хранения:
  - **Сокращенный** (4 байта)

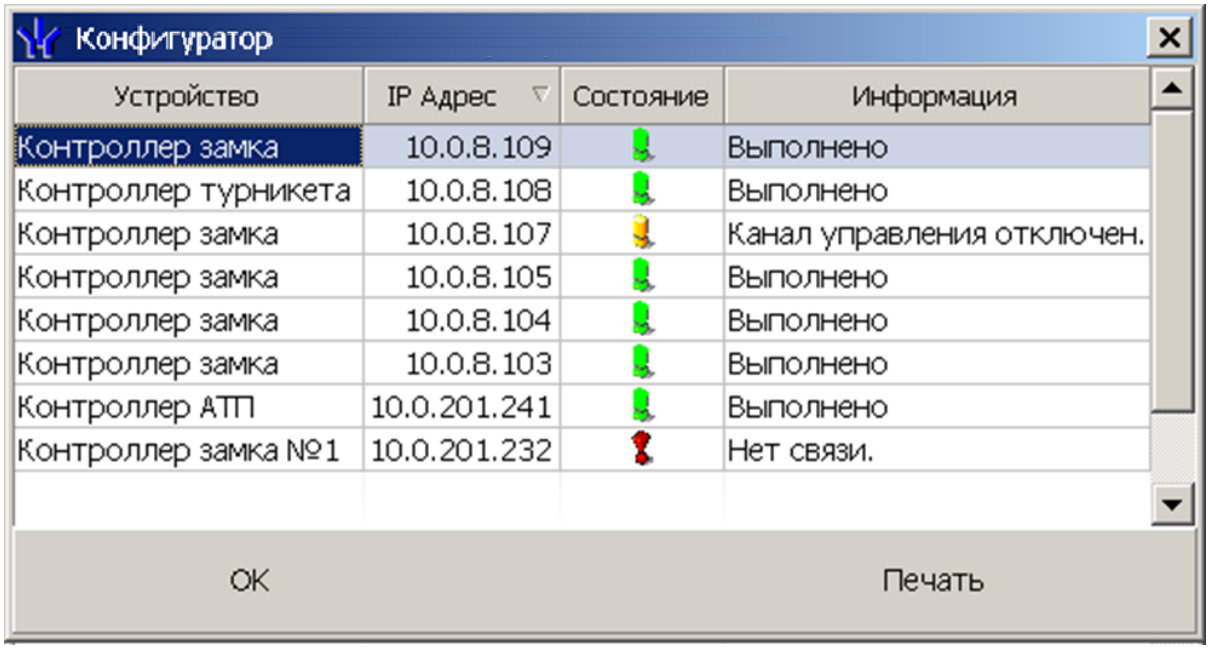
- **Wiegand 26** (3 байта, установлен по умолчанию) Номер карты делится на два числа - серия (1 байт, максимальное значение 255) и номер (2 байта, максимальное значение 65535). В таблицах ПО идентификатору отведено два столбца: **Код семейства**и **Номер**.
- **Универсальный** (8 байт. то есть полностью может быть сохранен идентификатор карты формат E-marin). Значение идентификатора – единое число. Во всех таблицах ПО идентификатору выделен один столбец **Идентификатор** (или **Одним числом**)

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



3.6 Состояние связи с контроллерами

При проведении автоматической конфигурации системы, добавлении или восстановлении устройств, а так же после неудачной передаче параметров в устройства с помощью кнопок панели инструментов раздела: **Передать параметры** и **Передать измененные параметры** открывается окно **Конфигуратор**. В окне отображается диагностическая информация о связи с устройствами.



Окно содержит следующие элементы:

- **Устройство** – в столбце указан тип устройства.
- **IP-адрес** – в столбце указан адрес устройства в сети.
- **Состояние** – в столбце отображено состояние связи с устройством:
  - – устройство найдено, связь с ним установлена, параметры переданы.
  - – санкционированное отключение связи.
  - – несанкционированная потеря связи с устройством, либо устройство не найдено, параметры не были переданы.
- **Информация** – в столбце выводится результат передачи данных в устройство.
- **ОК** – кнопка позволяет закрыть окно.
- **Печать** – кнопка позволяет распечатать результаты передачи данных.

3.7 Удаление и восстановление устройства

Удаления устройства

Внимание!

Прежде чем удалять устройство из конфигурации необходимо убедиться, что оно не связано ни с одним помещением в разделе ***«Помещения и мнемосхема»***.
В обратном случае удалить устройство из конфигурации будет нельзя, его можно будет только скрыть с возможностью последующего восстановления.

Для удаления устройства

1. Выделите устройство в рабочей области раздела.

2. Исключите устройство из конфигурации, нажав кнопку **Исключить из конфигурации** на панели инструментов раздела. Значок рядом с наименованием устройства примет вид .
3. Нажмите кнопку **Удалить** на панели инструментов раздела. В открывшемся окне **Подтверждение** для подтверждения удаления нажмите кнопку **Да**. Устройство будет удалено из конфигурации системы и исчезнет из рабочей области раздела.
4. Если устройство связано с помещением, появится окно **Подтверждение** с предложением скрыть устройство. Нажмите **Да,** если хотите скрыть устройство. Устройство будет отображаться в рабочей области раздела, выделенное красным цветом, при нажатой кнопке **Отображать скрытые устройства** .

Восстановление устройства

Примечание:

Восстановить можно только скрытое устройство. Удаленное ранее устройство необходимо заново добавлять в конфигурацию.

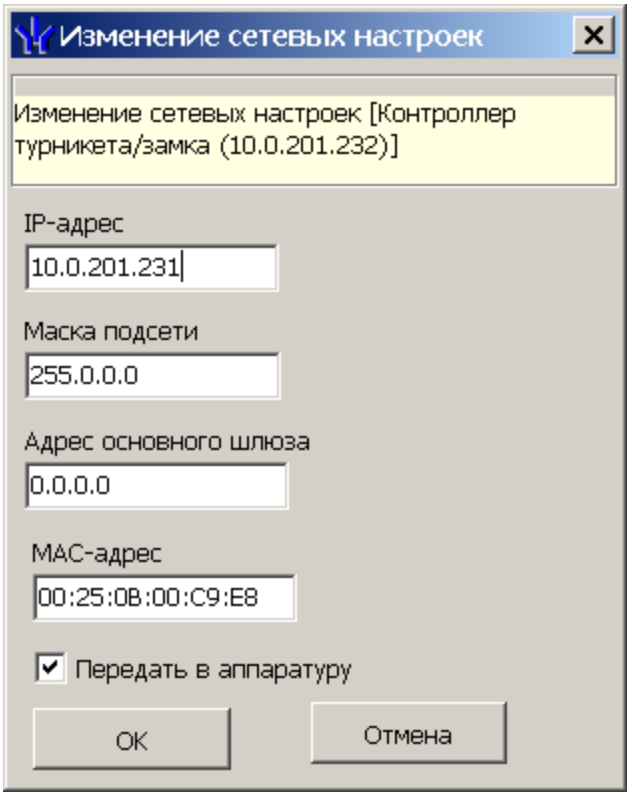
Для восстановления скрытого устройства:

1. Нажмите кнопку **Отображать скрытые устройства** на панели инструментов раздела. В рабочей области раздела станут видны скрытые устройства, они будут выделены красным цветом.
2. Выделите в рабочей области скрытое устройство, которое необходимо восстановить и нажмите кнопку **Восстановить**. В открывшемся окне **Подтверждение** нажмите кнопку **Да**. Название устройства сменит цвет с красного на черный.
3. Для включения устройства в конфигурацию системы нажмите кнопку **Включить в конфигурацию** на панели инструментов раздела. Значок рядом с наименованием устройства примет вид . Откроется окно **Конфигуратор** с информацией о состоянии связи с устройством. В открывшемся окне нажмите кнопку **ОК**.
4. На панели инструментов раздела нажмите кнопку **Передать параметры**. После передачи параметров значок рядом с наименованием устройства примет вид, соответствующий типу устройства.

3.8 Изменение сетевых настроек

Каждый контроллер имеет свои собственные настройки в сети, что упрощает поиск контроллеров, подключение их друг к другу, связи между ними. Для изменения сетевых настроек:

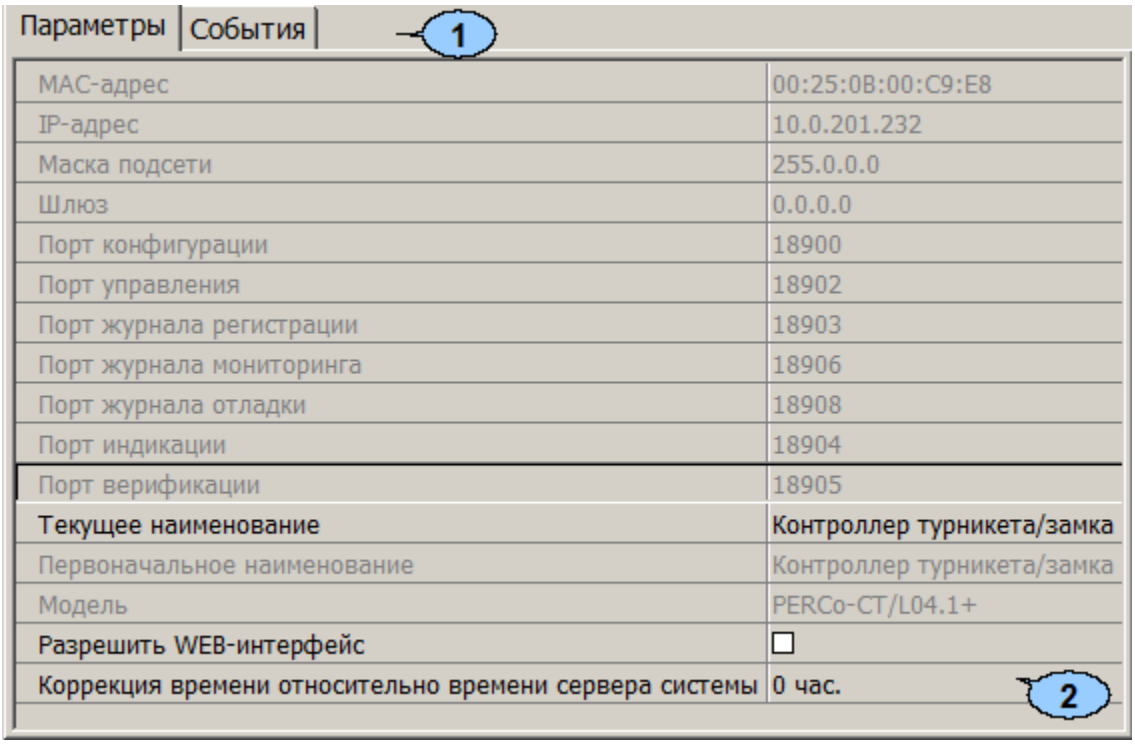
1. Выделите в рабочей области раздела контроллер, сетевые настройки которого необходимо изменить.
2. Исключите контроллер из конфигурации системы безопасности. Для этого нажмите кнопку **Исключить из конфигурации** на панели инструментов раздела.
3. Нажмите кнопку **Изменение сетевых настроек** на панели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



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

3.9 Вкладка «Параметры»

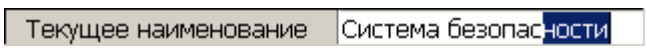
Вкладка предназначена для настройки параметров устройств системы и их ресурсов. Вкладка имеет следующий вид:



1. Выбор вкладки панели настройки.
   - **Параметры**
   - **События**
   - **Камера СКУД**
2. Рабочая область вкладки содержит список параметров и характеристик, доступных для устройства ресурса, выделенного в рабочей области раздела. Выделение параметра синим цветом указывает на то, что значение параметра было изменено но внесенные изменения не были переданы в устройство.

Для настройки параметра устройства или его ресурса, выделенного в рабочей области раздела, нажмите правой кнопкой мыши в правом столбце рабочей области вкладки в строке с наименованием параметра, который необходимо изменить. Используются следующие способы ввода значений параметров:

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

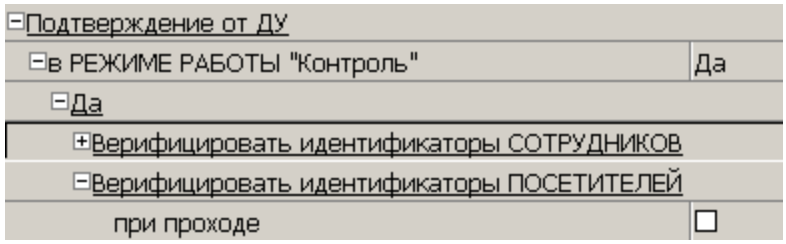


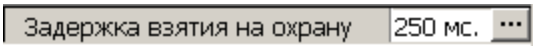
Раскрывающийся список позволяет выбрать одно из предложенных значений параметра. Для раскрытия списка необходимо нажать кнопку справа от установленного ранее значения.

Окошко для флажка позволяет включить или выключить параметр, установив или сняв флажок.

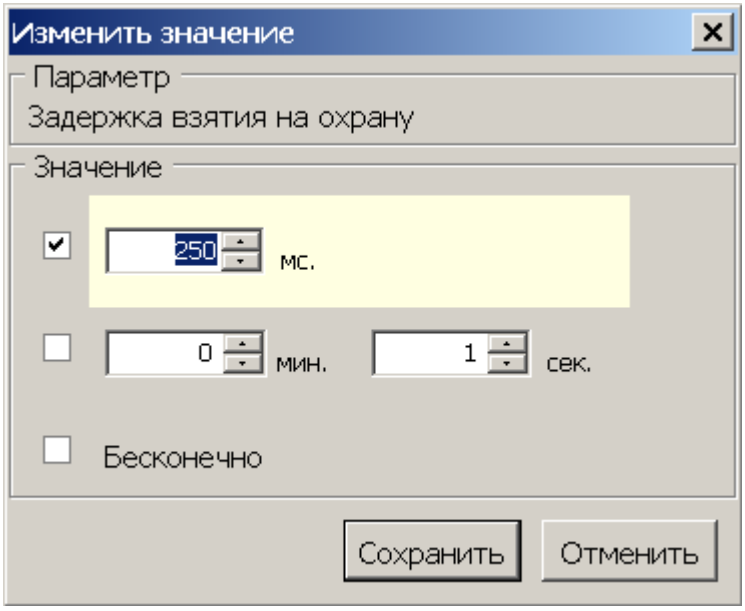
Счетчик позволяет установить числовое значение параметра. Для увеличения/ уменьшения значения параметра используйте кнопки, либо введите значение параметра с помощью клавиатуры.

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





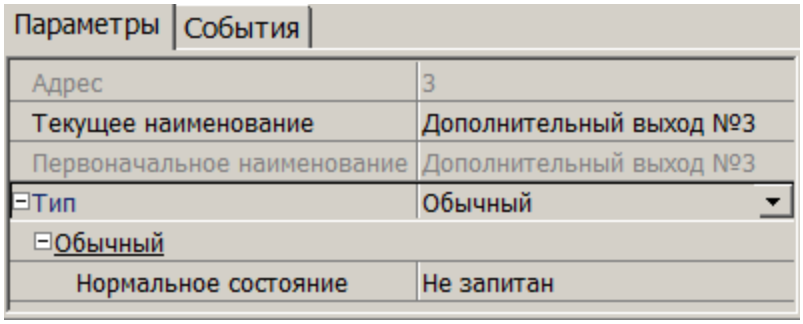
С использованием дополнительного окна. Для открытия окна необходимо нажать кнопку ... справа от установленного ранее значения параметра.



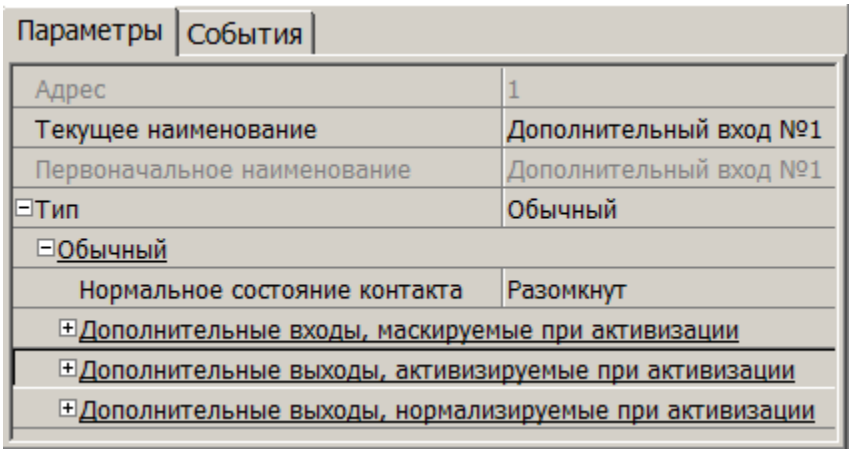
3.9.1 Конфигурирование картоприемника

В системе предусмотрена возможность автоматического изъятия временных карт посетителей с использованием картоприемника производства компании ***PERCo***. После монтажа и включения картоприемника необходимо произвести его конфигурирование в сетевом ПО системы, для этого:

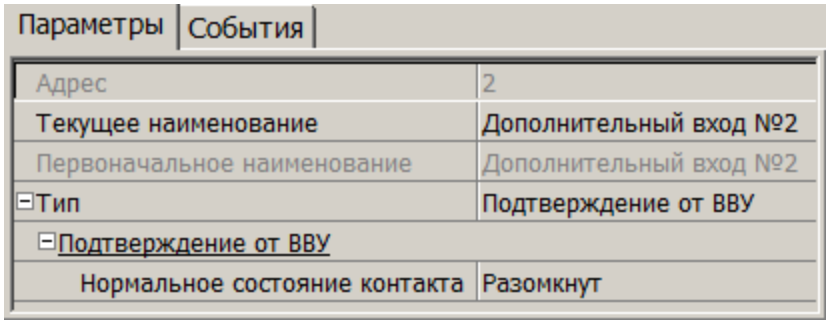
1. Запустите ***«Консоль управления»*** и откройте раздел ***«Конфигуратор»***.
2. Выделите в рабочей области раздела контроллер, к которому подключен картоприемник. Раскройте список его ресурсов.
3. Выделите ресурс **Дополнительный выход №3**. Номер выхода должен соответствовать выходу контроллера, к которому физически подключен вход *«Изъять карту»* картоприемника. На панели **Параметры**:
   - для параметра **Тип** установите значение **Обычный**;
   - для параметра **Нормальное состояние** оставьте значение **Не запитан**:



4. При необходимости настройте реакцию системы на сигнал от картоприемника *«Авария»*. Для этого выделите ресурс **Дополнительный вход №1**. Номер входа должен соответствовать входу контроллера, к которому физически подключен выход *«Авария»* картоприемника. На панели **Параметры**:
   - для параметра **Тип** выберите **Обычный**.
   - для параметра **Нормальное состояние контакта** установите значение **Разомкнут**.
   - настройте нужную реакцию, используя параметры активизации или нормализации выходов:



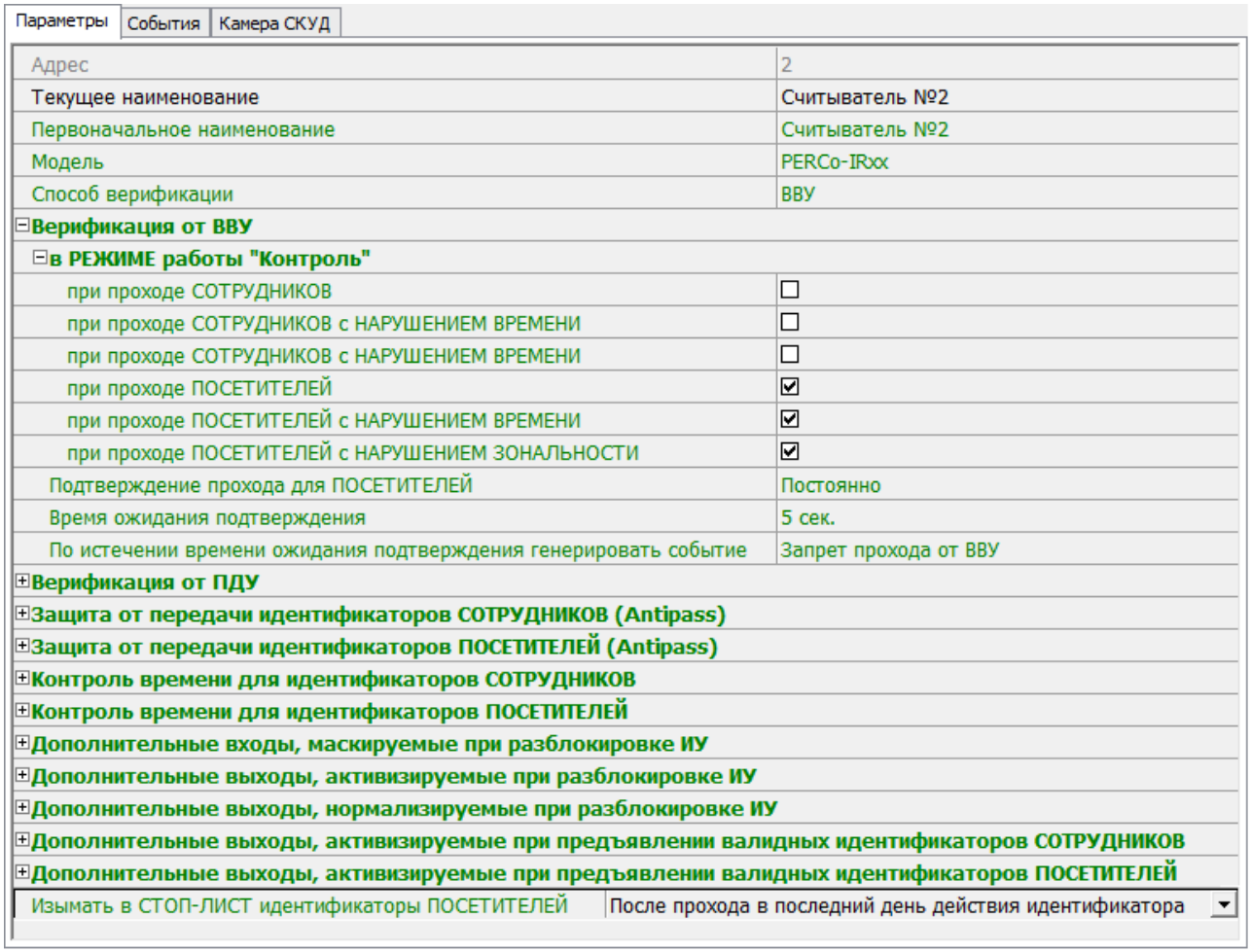
5. Выделите ресурс **Дополнительный вход №2**. Номер входа должен соответствовать входу контроллера, к которому физически подключен выход *«Карта изъята»* картоприемника. На панели **Параметры**:
   - для параметра **Тип** выберите **Подтверждение от ВВУ**.
   - для параметра **Нормальное состояние контакта** установите значение **Разомкнут**:



Примечание:

Для контроллеров с версией прошивки x.0.0.19 и ниже недоступно значение параметра **Тип: Подтверждение от ВВУ** для ресурса **Дополнительный вход №…**. В этом случае выход картоприемника *«Карта изъята»* подключается к входу управления контроллера *DU A* или *DU B* и дополнительно не конфигурируется в ПО. Тот же метод подключения может использоваться в том случае, если все дополнительные входы контроллера заняты.

6. Выделите ресурс **Считыватель №2**. Номер считывателя должен соответствовать выходному считывателю, в направлении которого установлен картоприемник. На панели **Параметры**:
   - для параметра **Способ верификации** установите значение **ПДУ**.
   - в раскрывшемся списке отметьте флажками параметры: **при проходе ПОСЕТИТЕЛЕЙ**; **при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ**; **при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**. В этом случае подтверждением для контроллера доступа будет сигнал от картоприемника *«Карта изъята»*:
   - для параметра **Подтверждение прохода для ПОСЕТИТЕЛЕЙ** установите требуемое значение.
   - для параметра **Время ожидания подтверждения** установите требуемое значение времени, в течение которого контроллер должен ожидать сигнал *«Карта изъята»*.
   - для параметра **Дополнительные выходы активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ** установите **Критерий активизации** в положение **На время срабатывания**.
   - Затем установите флажок **Дополнительный выход №3**:



7. Для передачи измененных параметров в контроллер нажмите на панели инструментов раздела кнопку **Передать параметры**.

3.9.2 Конфигурирование алкотестера

В системе предусмотрена возможность подтверждения или запрета прохода по команде от внешнего верифицирующего устройства (ВВУ), например алкотестера, подключенного к контроллеру.

После монтажа и подключения ВВУ необходимо произвести его конфигурирование в сетевом ПО системы, для этого:

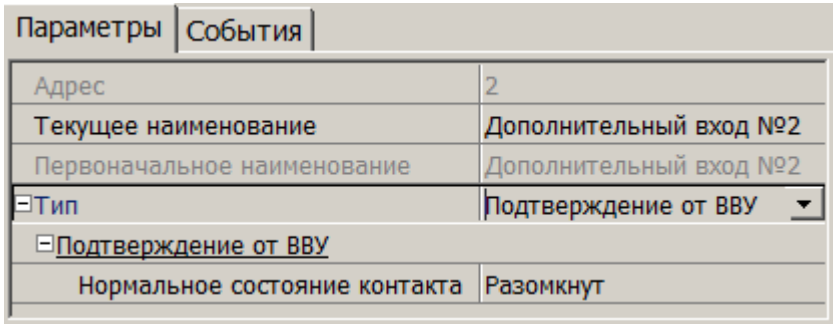
1. Запустите ***«Консоль управления»*** и откройте раздел ***«Конфигуратор»***.
2. Выделите в рабочей области раздела контроллер, к которому подключено ВВУ. Раскройте список его ресурсов.
3. Выделите ресурс **Дополнительный вход №1**. На панели **Параметры**:
   - для параметра **Тип** установите значение **Подтверждение от ВВУ**;
   - для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели).

Примечание:

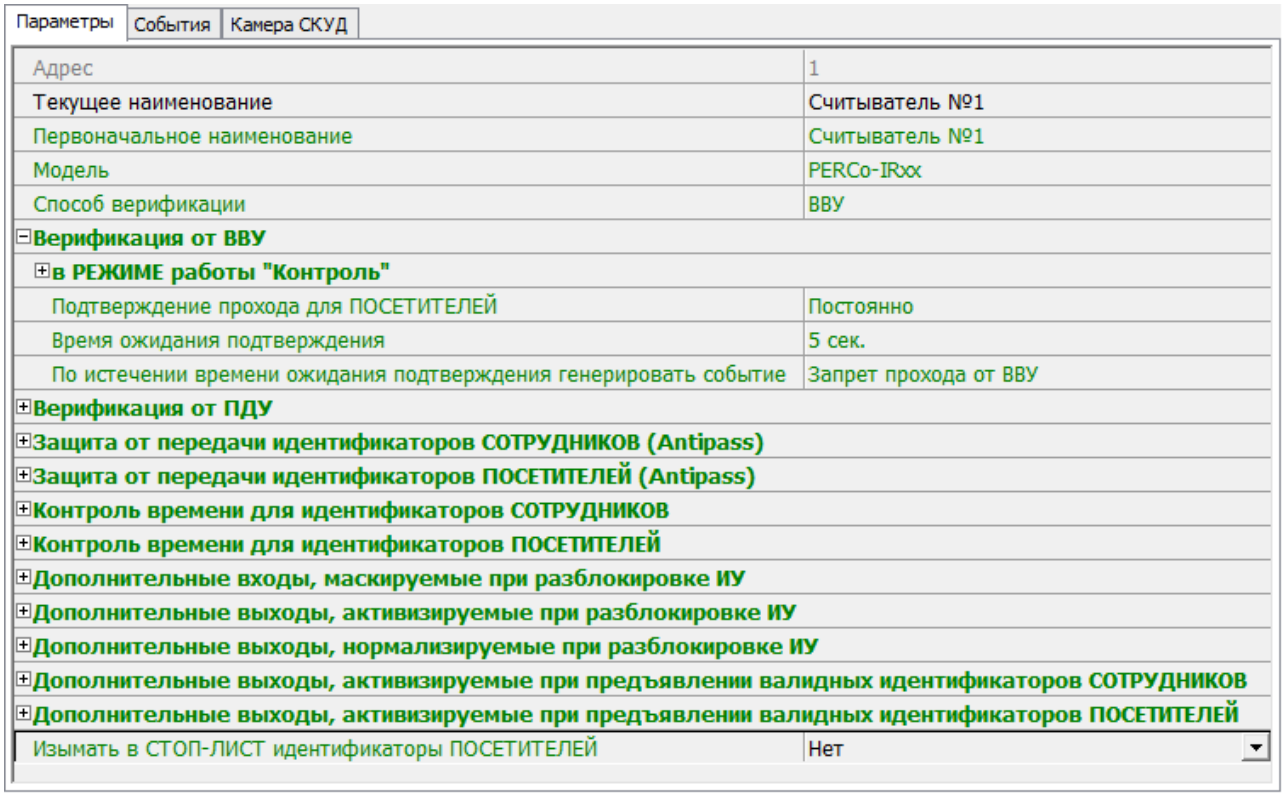
Если к контроллеру подключен только один выход ВВУ, то **Дополнительный вход №1** конфигурируется в зависимости от типа управляющего сигнала. **Дополнительныйвход №2** при этом не используется.

4. Выделите ресурс **Дополнительный вход №2**. На панели **Параметры**:
   - для параметра **Тип** установите значение **Запрет от ВВУ**;

- для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели):



5. Выделите ресурс **Считыватель №1.** Номер считывателя должен соответствовать считывателю, в направлении которого установлено ВВУ. На панели **Параметры**:
   - для параметра **Способ верификации** установите значение **ВВУ**;
   - в раскрывшемся списке отметьте флажками параметры: **при проходе СОТРУДНИКОВ** и при необходимости **при проходе ПОСЕТИТЕЛЕЙ**;
   - для параметра **Подтверждение прохода для ПОСЕТИТЕЛЕЙ** установите требуемое значение;
   - для параметра **Время ожидания подтверждения** установите требуемое значение времени, в течение которого контроллер должен ожидать управляющий сигнал от ВВУ;
   - для параметра **По истечении времени ожидания подтверждения генерировать событие** установите значение **Запрет прохода от ВВУ**, если к контроллеру подключены два выхода ВВУ (для управляющих сигналов разрешения и запрета прохода). **Отказ от прохода, нет ответа от ВВУ**, если подключен только один выход разрешения прохода.



6. Для передачи измененных параметров в контроллер нажмите на панели инструментов раздела кнопку **Передать параметры**  .

3.9.3 Конфигурирование алкотестера для двух направлений

Один алкотестер (или другое ВВУ) может использоваться для подтверждения или запрета возможности прохода в обоих направлениях. Для этого алкотестер (ВВУ) должен быть установлен в месте, доступном при проходе в обоих направлениях.

Для предотвращения несанкционированного прохода, при предъявлении карты доступа для другого направления прохода, необходимо изменить схему подключения считывателей карт доступа. Считыватели должны подключаться через дополнительные выходы контроллера. Пример схемы подключения см. в *«Руководстве по эксплуатации»* на контроллер ***PERCo-CT/L04***.

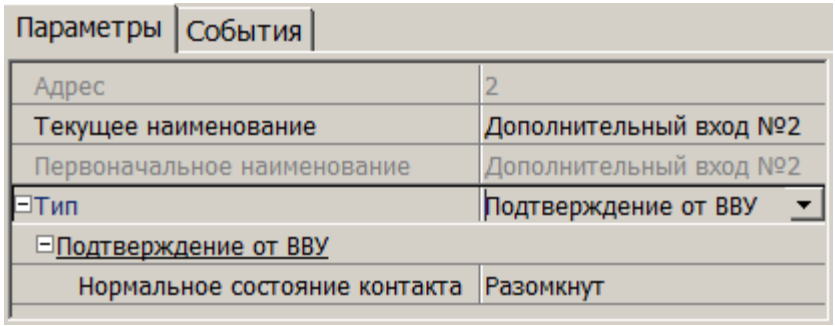
После монтажа и подключения ВВУ необходимо произвести его конфигурирование в сетевом ПО системы, для этого:

1. Запустите ***«Консоль управления»*** и откройте раздел ***«Конфигуратор»***.
2. Выделите в рабочей области раздела контроллер, к которому подключено ВВУ. Раскройте список его ресурсов.
3. Выделите ресурс **Дополнительный вход №1**. На панели **Параметры**:
   - для параметра **Тип** установите значение **Подтверждение от ВВУ**;
   - для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели).

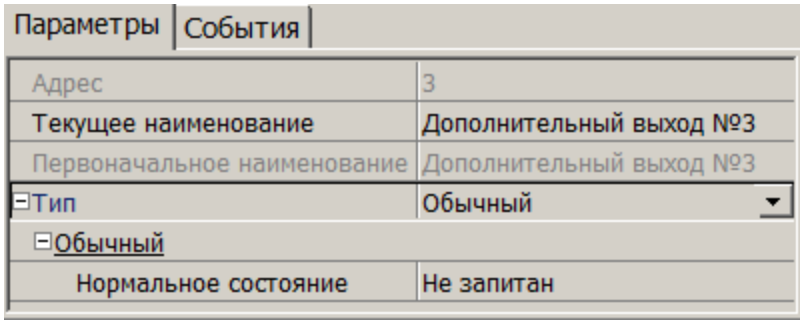
Примечание:

Если к контроллеру подключен только один выход ВВУ, то **Дополнительный вход №1** конфигурируется в зависимости от типа управляющего сигнала. **Дополнительныйвход №2** при этом не используется.

4. Выделите ресурс **Дополнительный вход №2**. На панели **Параметры**:
   - для параметра **Тип** установите значение **Запрет от ВВУ**;
   - для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели):



5. Выделите ресурс **Дополнительный выход №3**. Реле для отключения считывателя №1. На панели **Параметры**:
   - для параметра **Тип** установите значение **Обычный**;
   - для параметра **Нормальное состояние** оставьте значение **Не запитан**:



6. Выделите ресурс **Дополнительный выход №4**. Реле для отключения считывателя №2. На панели **Параметры**:
   - для параметра **Тип** установите значение **Обычный**;
   - для параметра **Нормальное состояние** оставьте значение **Не запитан**.
7. Выделите ресурс **Считыватель №1**. На панели **Параметры**:
   - для параметра **Способ верификации** установите значение **ВВУ**;
   - в раскрывшемся списке отметьте флажками параметры: **при проходе СОТРУДНИКОВ** и при необходимости **при проходе ПОСЕТИТЕЛЕЙ**;
   - для параметра **Подтверждение прохода для ПОСЕТИТЕЛЕЙ** установите требуемое значение;
   - для параметра **Время ожидания подтверждения** установите требуемое значение времени, в течение которого контроллер должен ожидать управляющий сигнал от ВВУ;
   - для параметра **По истечении времени ожидания подтверждения генерировать событие** установите значение **Запрет прохода от ВВУ**, если к контроллеру подключены два выхода ВВУ (для управляющего сигнала разрешения и запрета прохода). **Отказ от прохода, нет ответа от ВВУ** в ином случае.
   - для параметра **Дополнительные выходы активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ** и при необходимости для параметра **Дополнительные выходы активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ**:
     - установите **Критерий активизации** в положение **На время срабатывания**,
     - установите флажок **Дополнительный выход №3**:

Параметры | События | Камера СКУД

Адрес	1
Текущее наименование	Считыватель №1
Первоначальное наименование	Считыватель №1
Модель	PERCo-IRxx
Способ верификации	ВВУ
Верификация от ВВУ	
в РЕЖИМЕ работы "Контроль"	
при проходе СОТРУДНИКОВ	☐
при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ	☐
при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ	☐
при проходе ПОСЕТИТЕЛЕЙ	☑
при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ	☑
при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	☑
Подтверждение прохода для ПОСЕТИТЕЛЕЙ	Постоянно
Время ожидания подтверждения	5 сек.
По истечении времени ожидания подтверждения генерировать событие	Запрет прохода от ВВУ
Верификация от ПДУ	
Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)	
Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)	
Контроль времени для идентификаторов СОТРУДНИКОВ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Охрана"	Нет
Контроль времени для идентификаторов ПОСЕТИТЕЛЕЙ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
Дополнительные входы, маскируемые при разблокировке ИУ	
Дополнительные выходы, активизируемые при разблокировке ИУ	
Дополнительные выходы, нормализируемые при разблокировке ИУ	
Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ	
Критерий активизации	На время срабатывания
Дополнительный выход №3	☑
Дополнительный выход №4	☐
Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ	
Критерий активизации	На время срабатывания
Дополнительный выход №3	☑
Дополнительный выход №4	☐
Изымать в СТОП-ЛИСТ идентификаторы ПОСЕТИТЕЛЕЙ	Нет

8. Выделите ресурс **Считыватель №2**. На панели **Параметры** установите значение параметров, аналогичное установленному для считывателя №1. За исключением параметра **Дополнительные выходы активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ** и при необходимости для параметра **Дополнительные выходы активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ**:
   - установите **Критерий активизации** в положение **На время срабатывания**,
   - установите флажок **Дополнительный выход №4**.
9. Для передачи измененных параметров в контроллер нажмите на панели инструментов раздела кнопку **Передать параметры** .

3.9.4 Биометрический контроллер Suprema BioEntry W2

В системе предусмотрена возможность проведения интеграции с биометрическими контроллерами, разработанными компанией ***Suprema***.

После монтажа и подключения биометрического контроллера необходимо произвести его конфигурацию в сетевом ПО системы, для этого:

1. Запустите ***«Консоль управления»*** и откройте раздел ***«Конфигуратор»***.
2. Выделите в рабочей области раздела ресурс **Биометрическая система SUPREMA**, к которому подключен биометрический контроллер, и раскройте список его собственных ресурсов.
3. Выделите ресурс **Контроллер BioEntry W2**. На вкладке **Параметры**:
   - для параметра **Уровень безопасности** установите требуемый уровень безопасности при использовании верификации по отпечатку пальца;
   - для параметра **Таймаут сканирования пальца** установите время, которое будет выделяться системой на поднесение одного пальца при вводе отпечатков. Параметр задаётся в интервале от 3 до 20 секунд;
   - для параметра **Таймаут верификации пальцем** (используется в режиме доступа **карта и палец**) установите время, в течение которого будет ожидаться поднесение пальца для сканирования отпечатков (отсчёт времени начинается после того, как была предъявлена считывателю карта доступа). Параметр может быть задан в интервале от 1 до 20 секунд;
   - для параметра **Таймаут поиска отпечатков** установите время, которое будет отводиться для поиска отпечатка в памяти контроллера. Если за отведенное время отпечаток не будет найден, то аутентификация будет отклонена. Параметр может быть задан в интервале от 1 до 20 секунд;
   - для параметра **Чувствительность сканера** установите чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности обеспечивается высокое качество и скорость сканирования, при низком заданном уровне чувствительности – уменьшается влияние факторов внешней среды (температуры и влажности воздуха, освещённости помещения, чистоты сканируемой поверхности подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию. Понижение заданного уровня чувствительности сканера осуществляется при необходимости в зависимости от условий эксплуатации. Параметр может быть задан в интервале от 1 до 7, где значение "1" – соответствует самой низкой чувствительности, а значение "7" – самой высокой;
   - для параметра **Алгоритм поиска отпечатков** установите автоматический алгоритм (рекомендован производителем) поиска отпечатков пальцев;
   - для параметра **Режим датчика** установите режим работы считывающего датчика – либо он работает всегда, либо включается автоматически, если обнаруживает палец;
   - для параметра **Режим авторизации** установите режим доступа:
     - **частный режим доступа** – в этом случае параметры доступа устанавливаются для отдельного сотрудника/посетителя в рамках СКУД;
     - **общий режим доступа** – в этом случае параметры доступа устанавливаются в рамках биометрического контроллера и будут применяться для всех пользователей, взаимодействующих ним;
   - для параметра **Режим доступа** определите режим доступа при общем режиме авторизации (отображается, только если выбран «**Общий**» режим авторизации):

- **Палец** – для верификации требуется пройти процедуру сканирования отпечатка пальца;
- **Карта** – для верификации требуется предъявить считывателю карту доступа;
- **Карта и палец** – для верификации требуется предъявить считывателю карту доступа, после чего пройти процедуру сканирования отпечатка пальца;
- **Карта или палец** – для верификации требуется предъявить считывателю карту доступа или пройти процедуру сканирования отпечатка пальца;

- для параметра **Схема входных портов** необходимо назначить на входные порты **«Кнопку выхода»** и **«Датчик прохода»** (**«Датчик открытия\закрытия двери»**):
  - **Нет;**
  - **Кнопка выхода – порт 0;**
  - **Кнопка выхода – порт 1;**
  - **Датчик прохода – порт 0;**
  - **Датчик прохода – порт 1;**
  - **Кнопка выхода – порт 0; Датчик прохода – порт 1;**
  - **Кнопка выхода – порт 1; Датчик прохода – порт 0;**

Примечание:

Категорически не рекомендуется подключать датчик прохода и кнопку выхода на один и тот же вход контроллера.

- для параметра **Параметры кнопки выхода (Нормальное состояние)** выберите нормальное состояние входного порта, на который назначена **«Кнопка выхода»**:
  - **Нормально открыто,**
  - **Нормально закрыто;**

Примечание:

Нормальным состоянием кнопки выхода считается то состояние, в котором находится кнопка при заблокированной двери. Соответственно, если конструктивно предусмотрено, что при нажатии кнопки выхода размыкается контакт реле и дверь разблокируется (т.е. – переходит из нормального состояния в состояние разблокировки), то необходимо из раскрывающегося списка выбрать **Нормально закрыто**.

- для параметра **Параметры датчика прохода (Нормальное состояние)** выберите нормальное состояние входного порта, на который назначен **«Датчик прохода»**:
  - **Нормально открыто,**
  - **Нормально закрыто;**
- для параметра **Порядок байтов идентификатора карты** выберите порядок следования байтов идентификатора карты:
  - **От старшего байта к младшему,**
  - **От младшего байта к старшему;**

Примечание:

Нормальным состоянием датчика прохода (геркона) считается то состояние, в котором находится датчик при закрытой двери. Соответственно, если датчик прохода конструктивно расположен так, что при закрытой двери датчик нормально замкнут, то необходимо из раскрывающегося списка для датчика прохода выбрать **Нормально закрыто**.

- параметр **Настройки Wiegand (Режим)** – позволяет задать режим работы интерфейса *Wiegand* контроллера ***Suprema***:
  - **Вход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как вход. В этом режиме контроллер ***Suprema*** работает как обычный контроллер доступа, ожидая поступления данных по интерфейсу *Wiegand*;
  - **Выход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как выход. В этом режиме контроллер ***Suprema*** работает совместно с контроллером ***PERCo*** в составе СКУД (может производить аутентификацию и управление подключённым по интерфейсу *Wiegand* оборудованием (замком и т.д.));
- параметр **Использовать аутентификацию** – при установке флажка контроллером ***Suprema*** при предъявлении карты/пальца будет производиться предварительная аутентификация. В случае успешной предварительной аутентификации данные будут переданы в контроллер ***PERCo*** для повторной аутентификации (загорится зелёная индикация). В случае ошибки предварительной аутентификации данные в контроллер ***PERCo*** передаваться не будут – необходимо провести повторную успешную аутентификацию. Если флажок не выставлен, то процедура аутентификации будет производится только контроллером ***PERCo***.
- параметр **Управление замком** – если флажок не установлен (по умолчанию), то управление замком осуществляется контроллером компании ***PERCo***. Если флажок установлен, то контроллер ***Suprema*** получает возможность управлять замком. Обязательным условием передачи функций управления замком контроллеру ***Suprema*** является установка флажка **Использовать аутентификацию**.

Примечание:

Параметры **Использовать аутентификацию** и **Управление замком** доступны для редактирования в случае, если выбрано значение **Выход** в **Настройки Wiegand (Режим)**.

- для параметра **Коррекция времени относительно времени сервера системы** задайте коррекцию времени (параметр позволяет согласовать работу, если контроллер и сервер системы находятся в разных часовых поясах). Значение коррекции может быть задано в интервале от минус 12 до плюс 14 часов;

4. Выделите ресурс **Замок**. На вкладке **Параметры**:
   - параметр **Блокировать замок при закрытии двери** – при установке флажка дверь будет заблокирована сразу после закрытия;
   - параметр **Блокировать замок по таймауту, только если дверь закрыта** – при установке флажка замок будет заблокирован по истечении **Времени удержания в разблокированном состоянии** только после закрытия двери. Если флажок не установлен – замок будет заблокирован даже если дверь открыта;

- для параметра **Время удержания в разблокированном состоянии** установите время, которое должно пройти от разблокировки замка до его блокировки после успешной аутентификации. За это время необходимо открыть дверь – иначе замок заблокируется. Параметр может быть задан в интервале от 1 до 30 секунд или от 1 до 15 минут;
- для параметра **Предельное время разблокировки** установите максимальное разрешенное время для нахождения двери в открытом состоянии. Если дверь не закрыть за отведенное время – будет сгенерирован сигнал тревоги. Параметр может быть задан в интервале от 1 до 30 секунд или от 1 до 15 минут;
- параметр **Генерация тревоги по взлому двери** – при установке флажка сигнал тревоги будет автоматически сгенерирован в случае, если был зафиксирован факт открытия двери без команды на открытие от контроллера;
- параметр **Генерация тревоги по удержанию двери** – при установке флажка сигнал тревоги будет автоматически сгенерирован в случае, если истекло **Предельное время разблокировки** и дверь не была закрыта;
- параметр **Регистрация прохода по предъявлению идентификатора/ пальца** – если флажок установлен, то событие совершения прохода регистрируется сразу после поднесения карты доступа/сканирования пальца без ожидания сигнала от датчика прохода. Если флажок не выставлен, то событие совершения прохода регистрируется после поднесения карты доступа/ сканирования пальца и срабатывания датчика прохода.

5. Для передачи измененных параметров в контроллер нажмите на панели инструментов раздела кнопку **Передать параметры**  .

3.10 Вкладка «События»

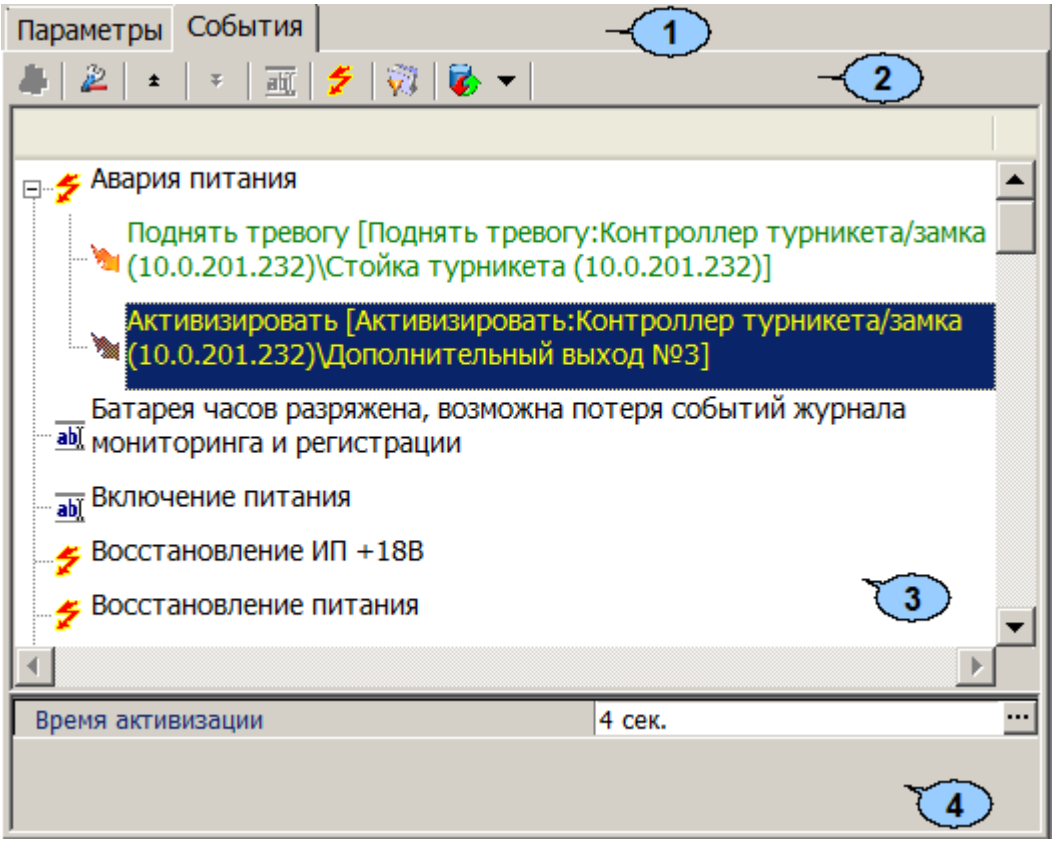
На вкладке **События** перечислен список событий мониторинга, регистрируемых устройством, выделенным в рабочей области раздела. В разделе реализована возможность настроить реакцию системы на любое из этих событий.

Реакция системы это предварительно заданная оператором последовательность команд, автоматически выполняемая устройствами системы.

Внимание!

Команды, определенные как реакция на событие, будут выполняться только при запущенном сервере системы безопасности и наличии связи с соответствующими устройствами.

Вкладка имеет следующий вид:



1. Выбор вкладки панели настройки.
   - **Параметры**
   - **События**
   - **Камера СКУД**
2. На вкладки доступны следующие инструменты:

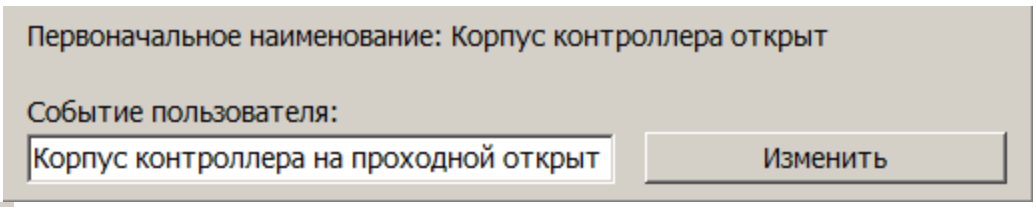
Добавить реакцию на событие (**Alt+N**) – кнопка позволяет открыть окно **Выбор реакции на событие** для выбранного в рабочей области панели события.

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

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

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

Изменить наименование события (**Shift+E**) – кнопка позволяет изменить название события, выделенного в рабочей области вкладки. При нажатии открывается дополнительная панель для ввода названия:



Показать события поддерживающие реакции (**Alt+R**) – кнопка позволяет отобразить в рабочей области вкладки только те события ресурса, на которые может быть задана реакция системы.

Показать измененные события (**Alt+C**) – кнопка позволяет отобразить в рабочей области вкладки только те события ресурса, названия которых были изменены.

Вернуть прежнее наименование событию объекта – при нажатии стрелки справа от кнопки открывается дополнительное меню команд:

- **Вернуть первоначальное наименование событию объекта** (**Shift +B**) – команда позволяет вернуть событию, выделенному в рабочей области вкладки, название, заданное по умолчанию.
- **Вернуть первоначальное наименование всем событиям объекта** (**Alt+B**) – команда позволяет вернуть всем событиям ресурса, выделенного в рабочей области раздела, названия, заданные по умолчанию.

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

   – событие (мониторинга), регистрируемое устройством или ресурсом, поддерживающее возможность задания реакции системы;

   – событие регистрируемое устройством или ресурсом системы;

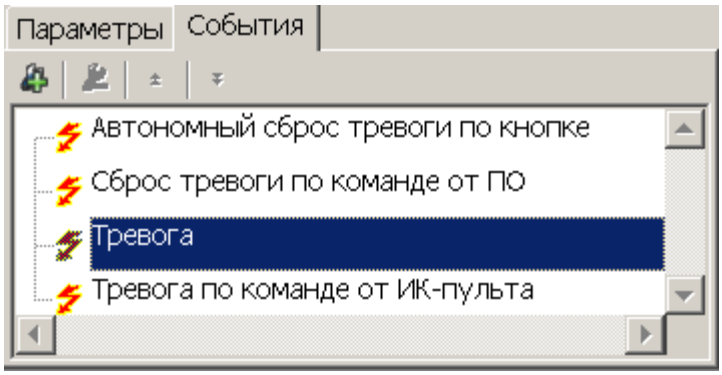
   – установленная для события команда.

4. Панель для настройки дополнительных параметров команд.

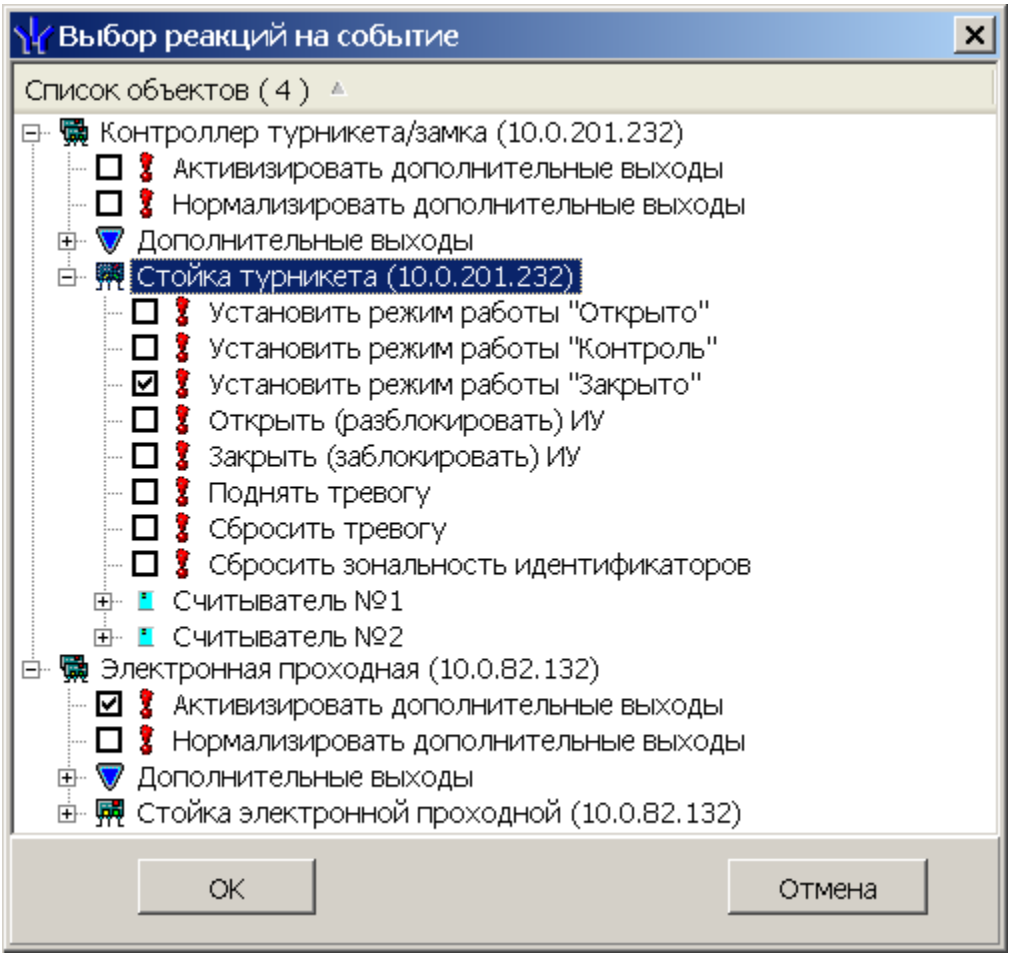
3.10.1 Задание реакции на событие

Для настройки реакции системы на регистрируемое событие мониторинга устройства или ресурса:

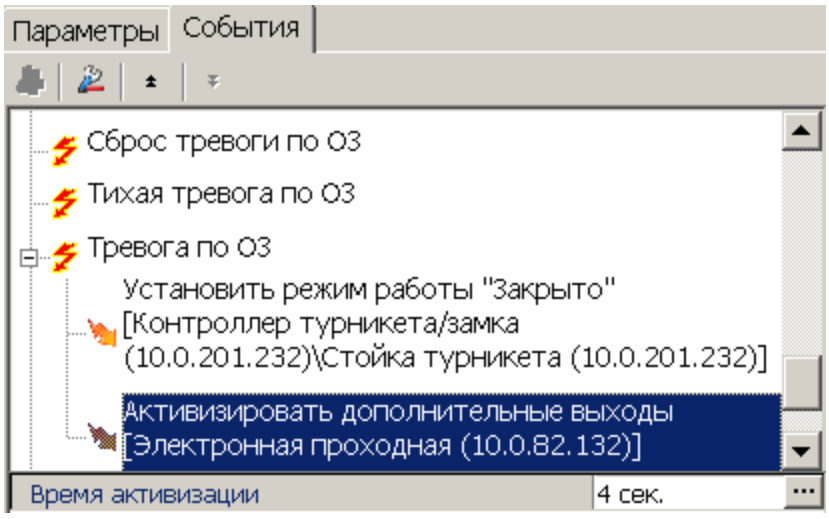
1. Выделите устройство или ресурс, на событие которого необходимо задать реакцию системы в рабочей области раздела.
2. На панели настройки перейдите на вкладку **События**:



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



4. В открывшемся окне отметьте в раскрывающемся многоуровневом списке устройств системы флажками нужные команды. Можно задать одновременно несколько команд, как для одного, так и у нескольких устройств и ресурсов. Нажмите кнопку **ОК**.
5. Окно **Выбор реакций на событие** будет закрыто. Отмеченные команды будут добавлены в рабочую область вкладки **События** для выделенного события:

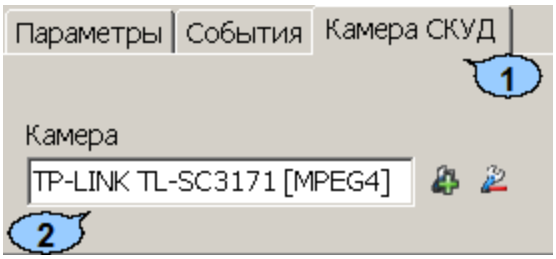


6. Установите последовательность выполнения команд, используя кнопки **Переместить вверх/вниз** ± / ∓ в инструментах панели.
7. При необходимости установите длительность выполнения команды на панели для ввода дополнительных параметров.

8. Для удаления выделенной в рабочей области реакции на событие нажмите кнопку **Удалить реакцию на событие**. В открывшемся окне подтверждения нажмите **Да**.
9. Нажмите кнопку **Сохранить** на панели инструментов ***«Консоли управления»***.

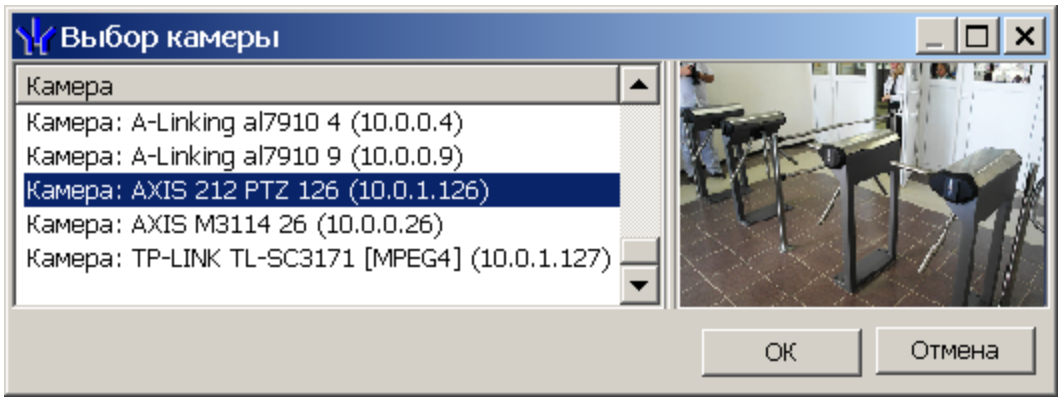
3.11 Вкладка «Камера СКУД»

Вкладка доступна только для ресурса контроллера **Считыватель №...**. На вкладке имеется возможность выбрать одну из камер видеоподсистемы системы безопасности для записи событий прохода в направлении выбранного считывателя. Выбранная камера отображается в поле **Камера**. При этом одна видеокамера может использоваться при работе с несколькими считывателями.



1. Выбор вкладки панели настройки.
   - **Параметры**
   - **События**
   - **Камера СКУД**
2. На вкладки доступны следующие инструменты:

   Добавит камеру – кнопка позволяет открыть окно **Выбор камеры**. Для выбора камеры, которая будет использоваться, как камера СКУД для считывателя выделите нужную камеру в рабочей области **Камеры**. Для удобства выбора камеры в правой части окна отображается изображение с выделенной камеры. Нажмите кнопку **ОК**, окно **Выбор камеры** будет закрыто, выбранная камера появится в поле **Камера** вкладки **Камера СКУД**.



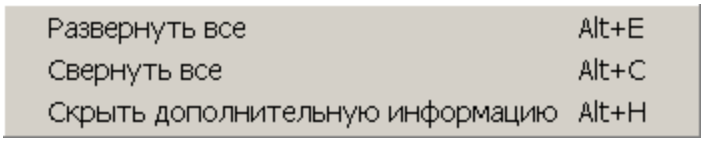
   Удалить камеру – кнопка позволяет удалить камеру СКУД, выбранную в поле **Камера** у считывателя.

Примечание:

Для отключения камеры от всех считывателей выделите ее в рабочей области раздела, перейдите на вкладку **Параметры** и снимите флажок у параметра **Использовать, как камеру СКУД**.

3.12 Панель ввода дополнительных данных

Для открытия и скрытия панели ввода дополнительных данных используйте пункт контекстного меню **Показать/скрыть дополнительную информацию**. Контекстное меню появляется при нажатии правой кнопкой мыши в рабочей области раздела:



Примечание:

Для контроллеров ***PERCo-CT/L04.2*** панель дополнительных данных не доступна. Настройка комиссионирующих карт, карт водителя и охранника, осуществляется в разделе ***«Доступ сотрудников»***на панели **Параметры доступа** вкладки **Помещения и устройства**.

Содержание панели ввода дополнительных данных зависит от типа контроллера, выбранного в рабочей области раздела:

- Для контроллеров доступа на панели расположена вкладка **Список комиссионирующих карт сотрудников**.
- Для контроллера ***PERCo-CT/L04*** в конфигурации *«Контроллер АТП»* на панели расположена вкладка **Список карт, имеющих право на досмотр** (см. *Руководство по эксплуатации* ***PERCo-CT/L04***).
- Для контроллера ППКОП ***PERCo-PU-01*** на панели находятся две вкладки **Список карт для постановки шлейфов на охрану** и **Список PIN-кодов для постановки шлейфов на охрану** (см. *Руководство по эксплуатации* ***PERCo-PU-01***).
- Для контроллеров второго уровня ***PERCo-CL201*** на панели находятся две вкладки: **Список комиссионирующихкарт сотрудников** и **Список карт аварийногодоступа**(см. *Руководство по эксплуатации* ***PERCo-CL201***).

При этом списки карт и PIN-кодов создаются независимо для каждого контроллера.

3.12.1 Список комиссионирующих карт

КомиссионированиеКомиссионирование***.*** Процедура подтверждения прав предъявленной карты посредством предъявления второй, комиссионирующей карты.

Комиссионирующей картой может служить любая карта, выданная сотруднику и внесенная в **Список комиссионирующих карт сотрудников**. Список комиссионирующих карт создается независимо для каждого контроллера.

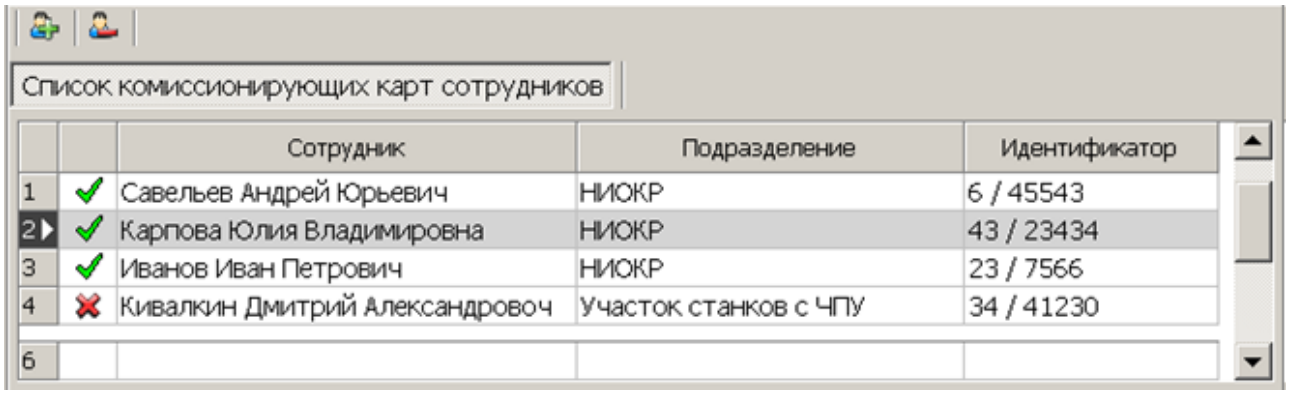
Примечание:

Для одного контроллера можно ввести не более 192 комиссионирующих карт, для каждого контроллера второго уровня ***PERCo-CL201*** – не более 64 комиссионирующих карт.

Для контроллера ***PERCo-CT/L04*** в конфигурации *«Контроллер АТП»* процедура подтверждения прав предъявленной карты может осуществляться картой охранника, имеющей право на досмотр, то есть внесенной в **Список карт, имеющих право на досмотр**.

Для внесения карты сотрудника (охранника) в список комиссионирующих карт (имеющих право на досмотр) для контроллера:

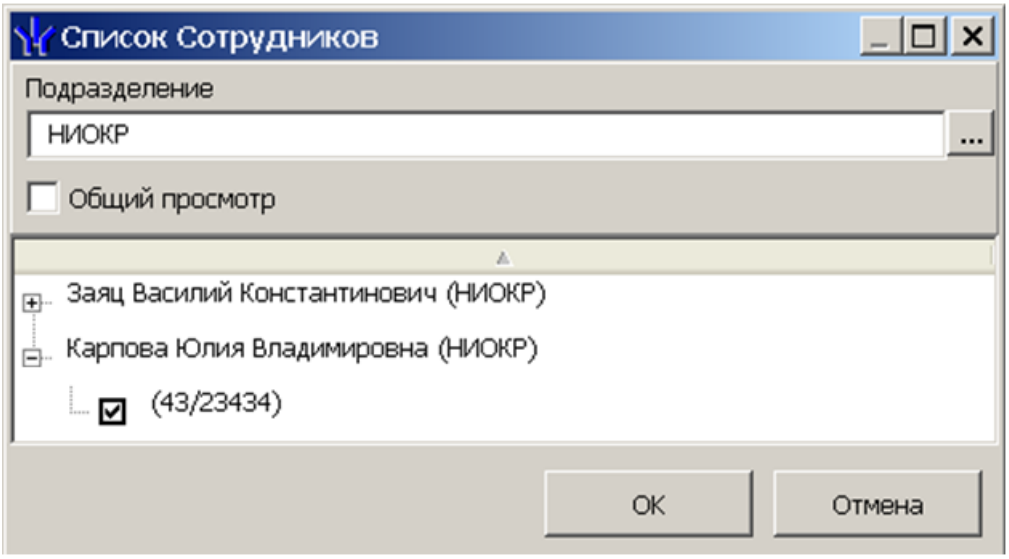
1. В рабочей области раздела выделите нужный контроллер или ресурс контроллера **Контроллер ИУ**. Откроется панель **Список комиссионирующих карт сотрудников, (Список карт, имеющих право на досмотр)**:



Добавить в список (**Shift+Alt+N**) – Кнопка позволяет добавить карту сотрудника (охранника) в список комиссионирующих (имеющих право на досмотр) карт.

Удалить из списка (**Shift+Alt+D**) – Кнопка позволяет удалить выделенную в рабочей области вкладки карту сотрудника (охранника) из списка комиссионирующих (имеющих право на досмотр) карт.

2. Если панель не открылась, нажмите правую кнопку мыши и в открывшемся контекстном меню выберите пункт **Показать дополнительную информацию**.
3. Для добавления карт нажмите кнопку **Добавить в список** на открывшейся панели. Откроется окно **Список сотрудников**:



4. В открывшемся окне отметьте флажками в раскрывающемся многоуровневом списке идентификаторы карт сотрудников, которые необходимо внести в список. Нажмите кнопку **ОК**. (Для выбора подразделения используйте кнопку ..., для просмотра всех сотрудников предприятия установите флажок **Общий просмотр**.) Отмеченные сотрудники будут добавлены в рабочую область панели.

5. Для удаления карты из **Списка комиссионирующих карт сотрудников, (Списка карт, имеющих право на досмотр)**, выделите ее в рабочей области панели и нажмите кнопку **Удалить из списка**. В открывшемся окне **Сообщение** нажмите **Да**.
6. Для сохранения списка в в БД системы нажмите кнопку **Сохранить** на панели инструментов ***«Консоли управления»***.
7. Для передачи прав карт в контроллер нажмите кнопку **Передать измененные параметры** на панели инструментов раздела.

3.12.2 Список карт аварийного доступа

При использовании контроллеров ***PERCo-CT/L04*** и ***PERCo-CT03*** к ним можно подключить до восьми замковых контроллеров второго уровня ***PERCo-CL201***. Карты аварийного доступа предназначены для прохода через контроллер второго уровня в случае отсутствия связи между ним и основным контроллером, к которому он подключен.

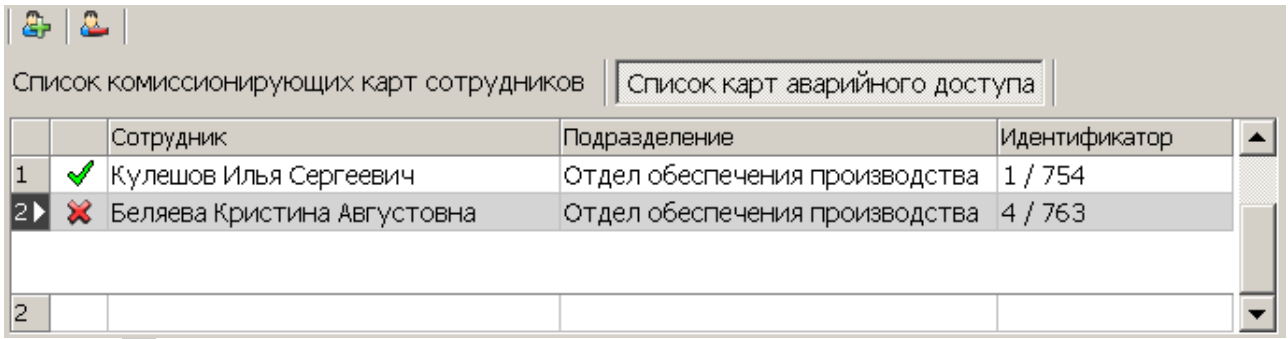
Примечание:

В список карт аварийного доступа одного контроллера может входить не более 128 карт.

Картой аварийного доступа может служить карта, выданная сотруднику, имеющая право доступа через выбранный контроллер второго уровня и внесенная в **Список карт аварийного доступа**. Список аварийных карт создается независимо для каждого контроллера второго уровня.

Для внесения карты сотрудника в список карт аварийного доступа:

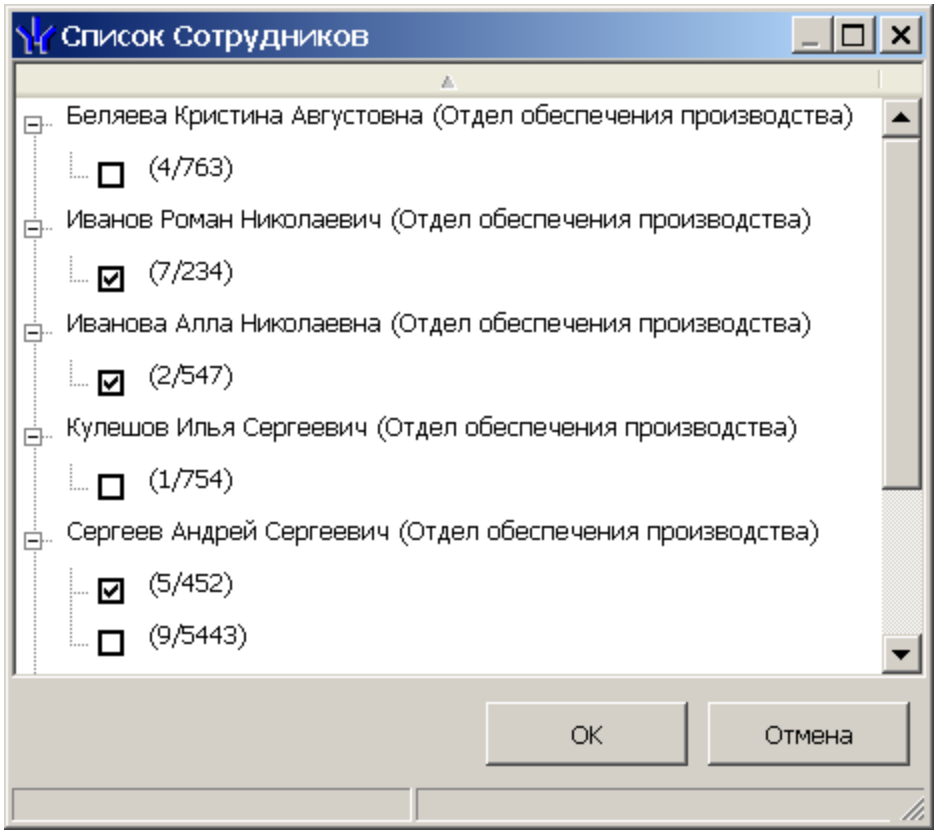
1. В рабочей области раздела выделите нужный ресурс контроллера **Контроллер замка,** соответствующий контроллеру второго уровня. Откроется панель ввода дополнительных данных.
2. Если панель не открылась, нажмите правую кнопку мыши и в открывшемся контекстном меню выберите пункт **Показать дополнительную информацию**.
3. На открывшейся панели перейдите на вкладку **Список карт аварийного доступа**:



Добавить в список (**Shift+Alt+N**) – кнопка позволяет добавить карту сотрудника в список карт аварийного доступа.

Удалить из списка (**Shift+Alt+D**) – кнопка позволяет удалить выделенную в рабочей области вкладки карту сотрудника из списка карт аварийного доступа.

4. Для добавления карт нажмите кнопку **Добавить в список**. Откроется окно **Список сотрудников**. В списке приводится список сотрудников, имеющих право прохода через выбранный контроллер второго уровня:



5. Для удаления карты из **Списка карт аварийного доступа**, выделите ее в рабочей области вкладки и нажмите кнопку **Удалить из списка**. В открывшемся окне **Сообщение** нажмите **Да**.
6. Для сохранения списка в в БД системы нажмите кнопку **Сохранить** на панели инструментов ***«Консоли управления»***.
7. Для передачи прав карт в контроллер нажмите кнопку **Передать измененные параметры** на панели инструментов раздела.

3.12.3 Список карт для постановки шлейфов на охрану

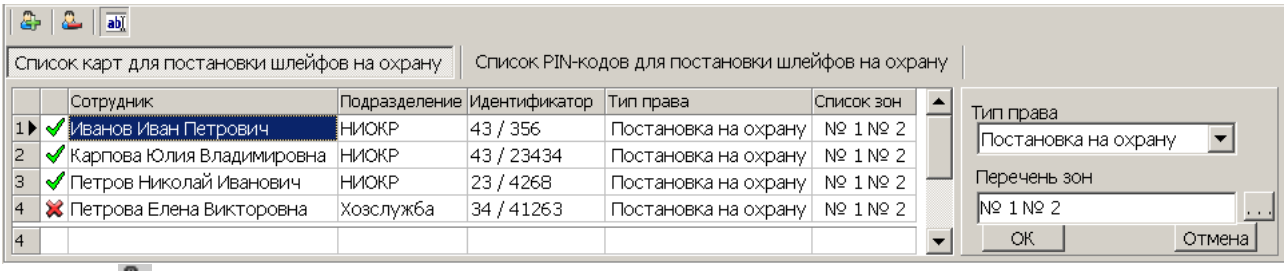
Создание списка карт для постановки и снятия с охраны пожарных и охранных зон сигнализации доступно только для контроллеров ключей постановки и снятия с охраны пожарных и охранных зон сигнализации ППКОП ***PERCo-PU01*** (см. *«Руководство по эксплуатации на ППКОП»*). Список карт создается независимо для каждого контроллера.

Примечание:

Для одного контроллера можно ввести в сумме не более 200 карт постановки на охрану и PIN-кодов, причем нельзя использовать один PIN-код для разных групп сотрудников.

Для внесения карты сотрудника в список:

1. В рабочей области раздела выделите контроллер ППКОП. Откроется панель **Список карт для постановки шлейфов на охрану**. Если панель не открылась, нажмите правую кнопку мыши и в открывшемся контекстном меню выберите пункт **Показать дополнительную информацию**:

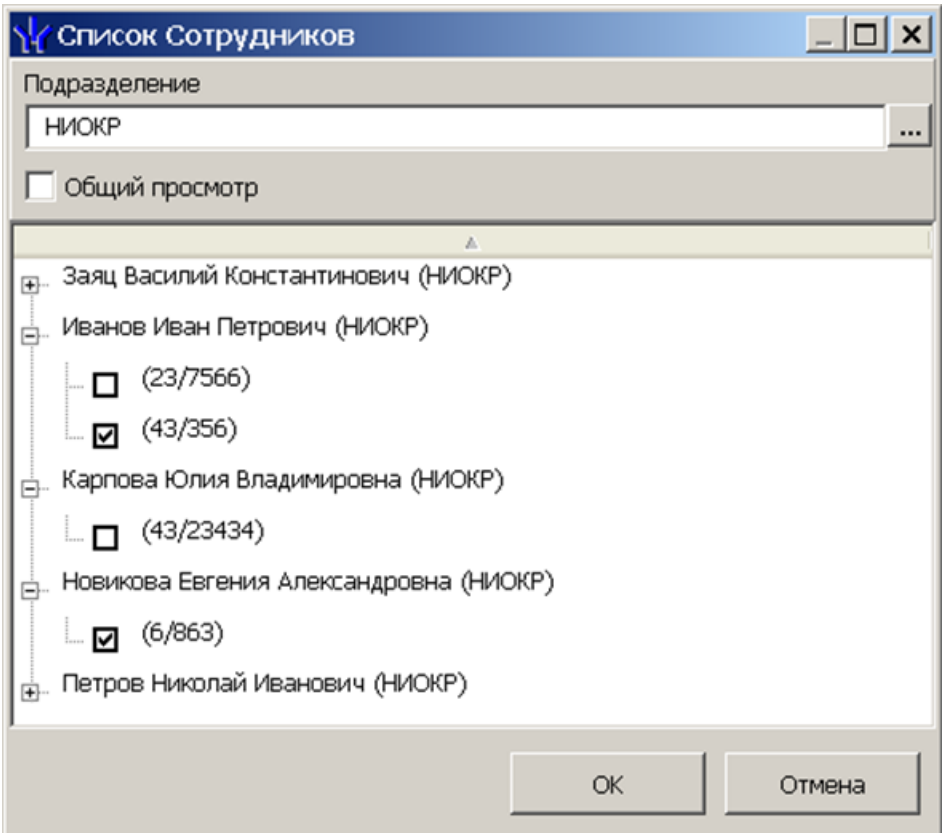


Добавить в список (**Shift+Alt+N**) – кнопка позволяет добавить карту в список карт имеющих право постановки шлейфов, включенных в ОЗ, перечисленные в списке **Перечень зон** на охрану.

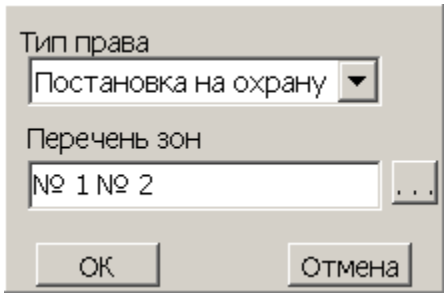
Удалить из списка (**Shift+Alt+D**) – кнопка позволяет удалить выделенную в рабочей области вкладки карту сотрудника (охранника) из списка карт имеющих право постановки на охрану.

Изменить – кнопка позволяет изменить права выделенной в рабочей области вкладки карты.

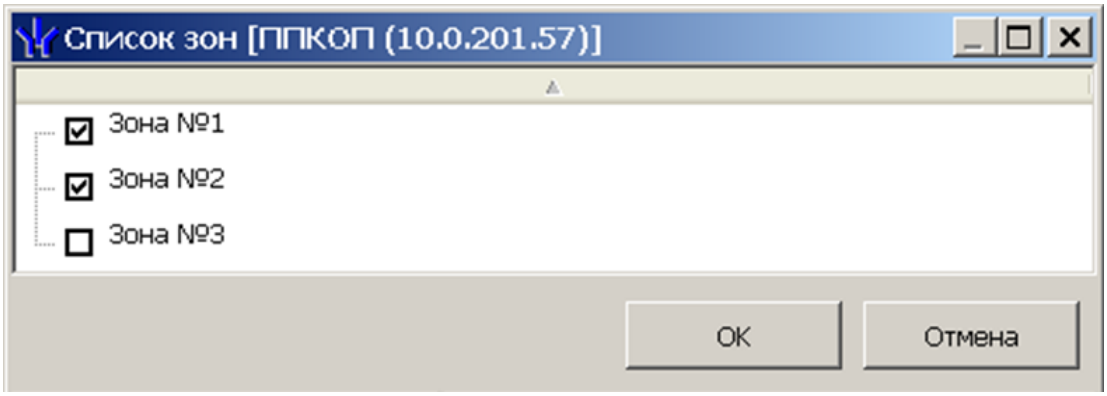
2. Для добавления карт нажмите кнопку **Добавить в список** на открывшейся панели. Откроется окно **Список сотрудников**:



3. В открывшемся окне отметьте флажками в раскрывающемся многоуровневом списке идентификаторы карт сотрудников, которые необходимо внести в список. Нажмите кнопку **ОК**. (Для выбора подразделения используйте кнопку ..., для просмотра всех сотрудников предприятия установите флажок **Общий просмотр**). Отмеченные сотрудники будут добавлены в рабочую область панели, откроется панель задания прав (если необходимо редактировать права, нажмите кнопку **Изменить** для открытия панели):



4. Для настройки прав карты выделите строку с данными сотрудника и выберите в раскрывающемся списке **Тип права**:
   - **Постановка на охрану**
   - **Снятие с охраны**
   - **Постановка и снятие с охраны**
5. Для выбора зон сигнализации, управление которыми будет доступно по карте, выделите строку с данными сотрудника и нажмите кнопку ... справа от строки **Перечень зон.** Откроется окно **Список зон ППКОП…**:



6. В открывшемся окне отметьте флажками зоны, управление которыми будут доступно по карте. Нажмите кнопку **ОК**.
7. Нажмите кнопку **ОК** на панели задания прав, панель будет закрыта.
8. Для удаления карты из **Списка карт для постановки шлейфов на охрану** выделите ее в рабочей области панели и нажмите кнопку **Удалить из списка**. В открывшемся окне **Сообщение** нажмите **Да**.
9. Для сохранения списка в БД системы нажмите кнопку **Сохранить** на панели инструментов ***«Консоли управления»***.
10. Для передачи прав карт в контроллер нажмите кнопку **Передать измененные параметры** на панели инструментов раздела.

3.12.4 Список PIN-кодов для постановки шлейфов на охрану

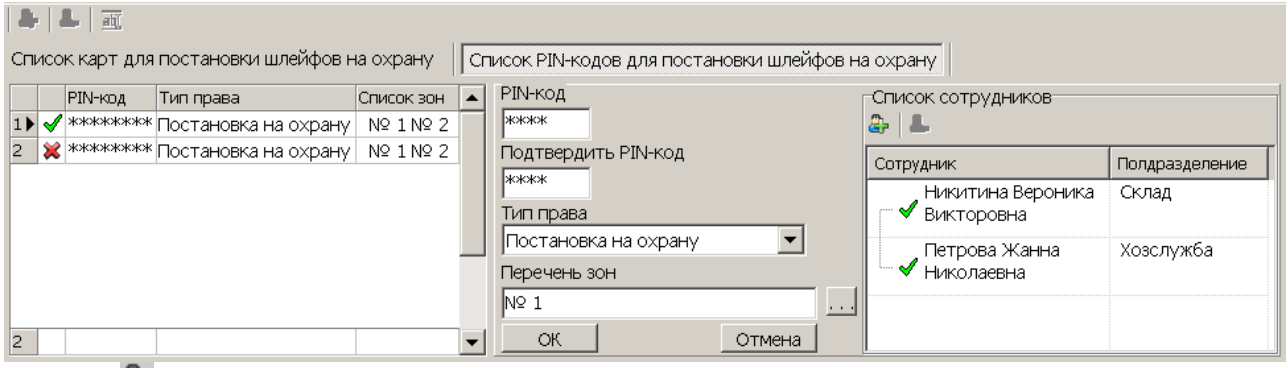
Создание списка PIN-кодов для постановки и снятия с охраны пожарных и охранных зон сигнализации доступно только для контроллеров ППКОП ***PERCo-PU01***. Ввод PIN-кода осуществляется при помощи БУИ ***PERCo-AU02 1-01***, подключенного к контроллеру. Список PIN-кодов создается независимо для каждого контроллера.

Примечания:

- PIN-кодом может служить комбинация из 4–8 цифр от 1 до 8.
- Для одного контроллера можно ввести в сумме не более 200 карт постановки на охрану и PIN-кодов, причем нельзя использовать один PIN-код для разных групп сотрудников.

Для добавления в список нового PIN-кода:

1. В рабочей области раздела выделите контроллер ППКОП. На открывшейся панели перейдите на вкладку **Список PIN-кодов для постановки шлейфов на охрану**. Если панель не открылась, нажмите правую кнопку мыши и в открывшемся контекстном меню выберите пункт **Показать дополнительную информацию**:

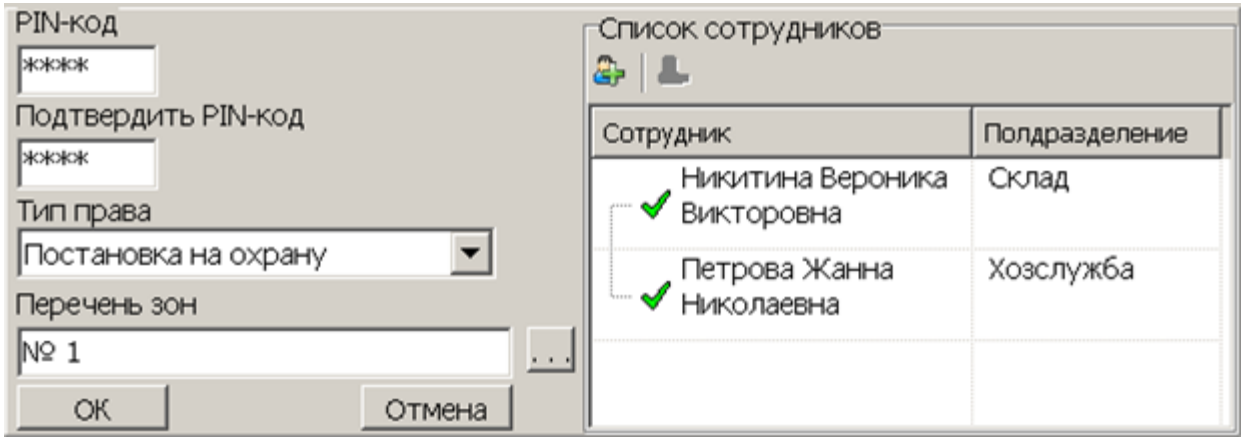


Добавить в список (**Shift+Alt+N**) – кнопка позволяет добавить новый PIN-код.

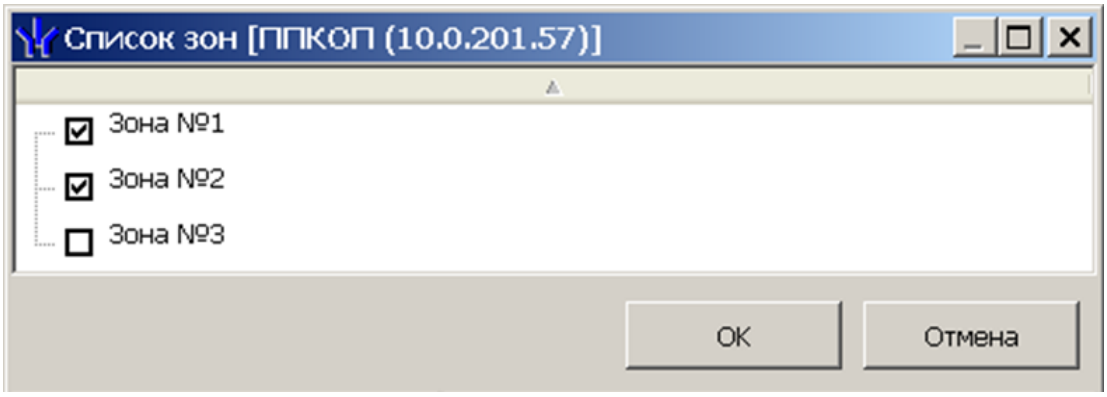
Удалить из списка (**Shift+Alt+D**) – кнопка позволяет удалить PIN-код, выделенный в рабочей области вкладки.

Изменить – кнопка позволяет изменить права PIN-кода, выделенного в рабочей области вкладки.

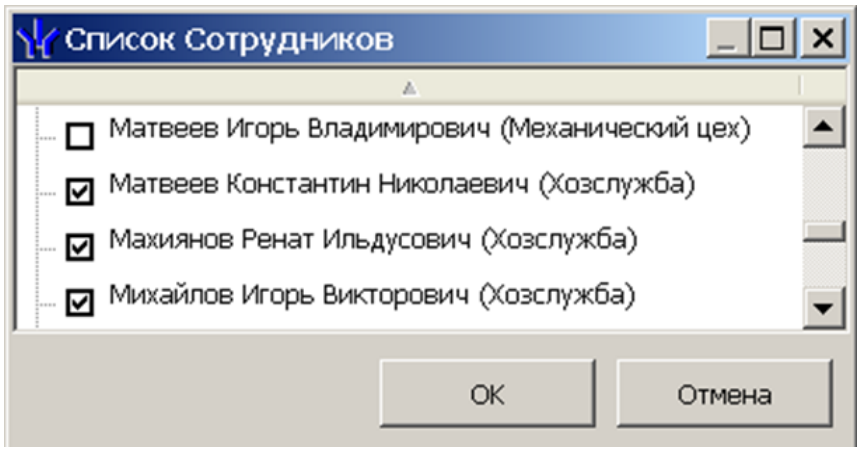
2. Для добавления нового PIN-кода нажмите кнопку **Добавить в список**. Откроется панель задания PIN-кода (если необходимо редактировать права PIN-кода нажмите кнопку **Изменить** для открытия панели):



3. В поля **PIN-код** и **Подтвердить PIN-код** введите комбинацию из 4–8 цифр от 1 до 8, которая будет являться PIN-кодом.
4. Для установки прав PIN-кода выберите в раскрывающемся списке **Тип права**:
   - **Постановка на охрану**
   - **Снятие с охраны**
   - **Постановка и снятие с охраны**
5. Для выбора зон сигнализации, управляемых с использованием PIN-кода, нажмите кнопку справа от строки **Перечень зон.** Откроется окно **Список зон ППКОП…**:



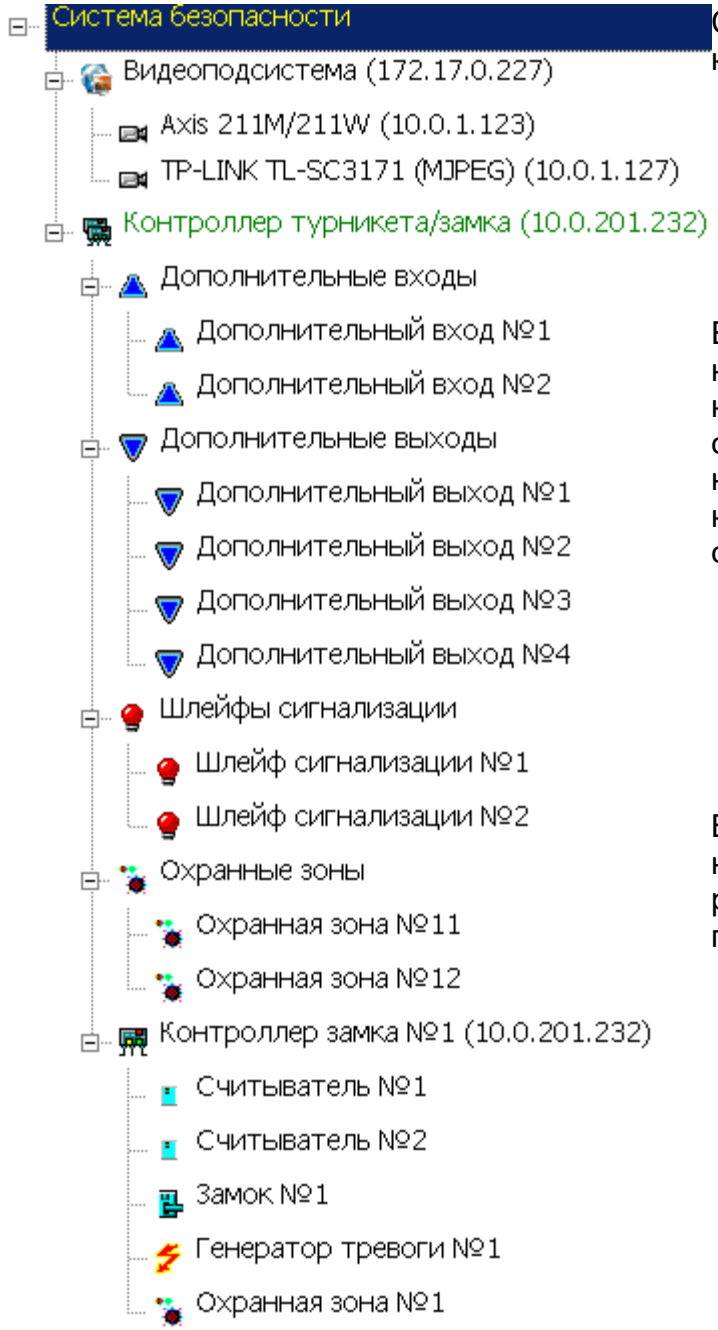
6. В открывшемся окне отметьте флажками зоны, управление которыми будет доступно с использованием PIN-кода. Нажмите кнопку **ОК**.
7. Нажмите кнопку **Добавить в список** в области **Список сотрудников**. Откроется окно **Список сотрудников**:



8. В открывшемся окне отметьте флажками сотрудников, которым будет сообщен PIN-код. Нажмите кнопку **ОК**. Окно будет закрыто, отмеченные сотрудники будут добавлены в область **Список сотрудников**.
9. Нажмите кнопку **ОК** на панели задания PIN-кода, панель будет закрыта. Новый PIN-код появится в рабочей области панели.
10. Для удаления PIN-кода выделите его в рабочей области панели и нажмите кнопку **Удалить из списка**. В открывшемся окне **Сообщение** нажмите **Да**.
11. Для сохранения списка в в БД системы нажмите кнопку **Сохранить** на панели инструментов ***«Консоли управления»***.
12. Для передачи PIN-кодов в контроллер нажмите кнопку **Передать измененные параметры** на панели инструментов раздела.

3.13 Параметры ресурсов

Для настройки параметров ресурсов контроллера перейдите в раздел ***«Конфигуратор»*** Для доступа к списку ресурсов контроллера в области **Список объектов** нажмите на ⊞ рядом с названием контроллера. Выделите в списке необходимый ресурс и перейдите на вкладку **Параметры** на панели настройки.



Список доступных ресурсов контроллера, сгруппирован по типам:

- **Дополнительные входы**;
- **Дополнительные выходы**;
- **Шлейфы сигнализации**;
- **Зоны** (охранные, пожарные);
- **Контроллер ИУ** (замка, турникета, шлагбаума);

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

- **Считыватель**;
- ИУ (**Замок**, **Турникет**, **Шлагбаум**);
- **Генератор тревоги**;
- Зона (**Охранная зона**, **Пожарная зона**).

В зависимости от типа контроллера наличие и количество ресурсов может различаться. В таблице представлен перечень ресурсов контроллеров.

3.13.1 Ресурсы контроллеров и ЭП PERCo серии x.1

Ресурсы контроллеров и ЭП PERCo серии x.1

Модель*	Доп. вход	Доп. выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считы-ватель	ИУ	Ген. тревоги	ЗС
Контроллеры PERCo									
CL201	0	0	0	0	-	1	замок	1	1
CT/L04 (1)	2	4	2	2	0	2	замок	1	1
CT/L04 (2)	2	4	2	2	8	2	замок	1	1
CT/L04 (3)	2	4	2	2	8	2	2 замка	2	2
CT/L04 (4)	2	2	0	0	0	2	турникет	1	0
CT/L04 (5)	2	2	0	0	8	2	турникет	1	0
CT/L04 (6)	2	2	0	0	0	2	шлагбаум	1	0
CT/L04 (7)	2	2	0	0	8	2	шлагбаум	1	0
CL05	0	1	0	0	0	1	замок	1	1
Контроллер ЭП PERCo									
CT03(1)	2	2	0	0	0	2	турникет	1	0
CT03(2)	2	2	0	0	8	2	турникет	1	0
Контроллер регистрации PERCo									
CR01	-	-	-	-	-	2	-	-	-
Контроллеры ППКОП PERCo									
PU01**	-	6	8	8	-	-	-	-	-
CS01	-	5	3	2	-	1	замок	1	-

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

**Предусмотрена возможность подключения считывателя ключей для постановки и снятия ОЗ с охраны. Считыватель не отображается в списке ресурсов. Конфигурация происходит автоматически на аппаратном уровне.

Варианты конфигурации контроллера ***PERCo-CT/L04***:

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

Варианты конфигурации ЭП:

1. Электронная проходная.
2. Электронная проходная с подключением до восьми контроллеров замка второго уровня ***PERCo-CL201.***

3.13.2 Ресурсы контроллеров и ЭП PERCo серии x.2

Ресурсы контроллеров и ЭП PERCo серии x.2

Модель	Доп. вход	Доп. выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считы-ватель	ИУ	Ген. тревоги	ОЗ
Контроллеры доступа									
CL201	0	0	0	0	-	1	L	1	1
CT/L04.2 (1)	4	4	0	0	до 8	2	T	1	0

Модель	Доп. вход	Доп. выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считы-ватель	ИУ	Ген. тревоги	ОЗ
CT/L04.2 (2)	2	3	0	0	до 8	3	T+L	2	1
CT/L04.2 (3)	0	2	0	0	до 8	4	T+L+L	3	2
CT/L04.2 (4)	2	3	0	0	до 8	4	T+2L	2	1
CT/L04.2 (5)	5	4	0	0	до 8	2	G	1	0
CT/L04.2 (6)	3	3	0	0	до 8	3	G+L	2	1
CT/L04.2 (7)	1	2	0	0	до 8	4	G+L+L	3	2
CT/L04.2 (8)	3	3	0	0	до 8	4	G+2L	2	1
CT/L04.2 (9)	5	8	2	2	до 8	1	L	1	1
CT/L04.2 (10)	6	8	1	1	до 8	1	L	1	1
CT/L04.2 (11)	7	8	0	0	до 8	1	L	1	1
CT/L04.2 (12)	3	7	2	2	до 8	2	L+L	2	2
CT/L04.2 (13)	4	7	1	1	до 8	2	L+L	2	2
CT/L04.2 (14)	5	7	0	0	до 8	2	L+L	2	2
CT/L04.2 (15)	2	6	1	1	до 8	3	L+L+L	3	3
CT/L04.2 (16)	3	6	0	0	до 8	3	L+L+L	3	3
CT/L04.2 (17)	0	4	0	0	до 8	4	L+L+L+L	4	4
CT/L04.2 (18)	5	8	2	2	до 8	2	2L	1	1
CT/L04.2 (19)	6	8	1	1	до 8	2	2L	1	1
CT/L04.2 (20)	7	8	0	0	до 8	2	2L	1	1
CT/L04.2 (21)	4	7	1	1	до 8	3	2L+L	2	2
CT/L04.2 (22)	5	7	0	0	до 8	3	2L+L	2	2
CT/L04.2 (23)	3	6	0	0	до 8	4	2L+L+L	3	3
CT/L04.2 (24)	4	7	1	1	до 8	4	2L+2L	2	2
CT/L04.2 (25)	5	7	0	0	до 8	4	2L+2L	2	2
CL05.2	1/1		0	0	-	1	L	1	1
Контроллер регистрации									
CR01.2	-	-	-	-	-	2	-	-	-
Электронные проходные									
CT03 (1)	4	4	0	0	до 8	2	IP-Stile	1	0
CT03 (2)	2	3	0	0	до 8	2	IP-Stile+IC	1	0
CT03 (3)	4	3	0	0	до 8	2	IP-Stile +AP	1	0
CT03 (4)	2	2	0	0	до 8	2	IP-Stile+IC +AP	1	0

Принятые в таблице сокращения:

L – односторонний замок;
2L – двусторонний замок;
T – турникет;
G – шлагбаум;
IP-Stile – электронная проходная;
IC – встроенный картоприемник;
AP – встроенное устройство «Антипаника".

Варианты шаблонов конфигурации контроллера ***PERCo-CT/L04.2*** (к любой конфигурации возможно подключить до восьми контроллеров замка ***PERCo-CL201***):

1. Контроллер для управления турникетом.
2. Контроллер для управления турникетом и одним односторонним замком.
3. Контроллер для управления турникетом и двумя односторонними замками.
4. Контроллер для управления турникетом и одним двусторонним замком.
5. Контроллер для управления автотранспортной проходной (АТП).
6. Контроллер для управления АТП и одним односторонним замком.
7. Контроллер для управления АТП и двумя односторонними замками.
8. Контроллер для управления АТП и одним двусторонним замком.

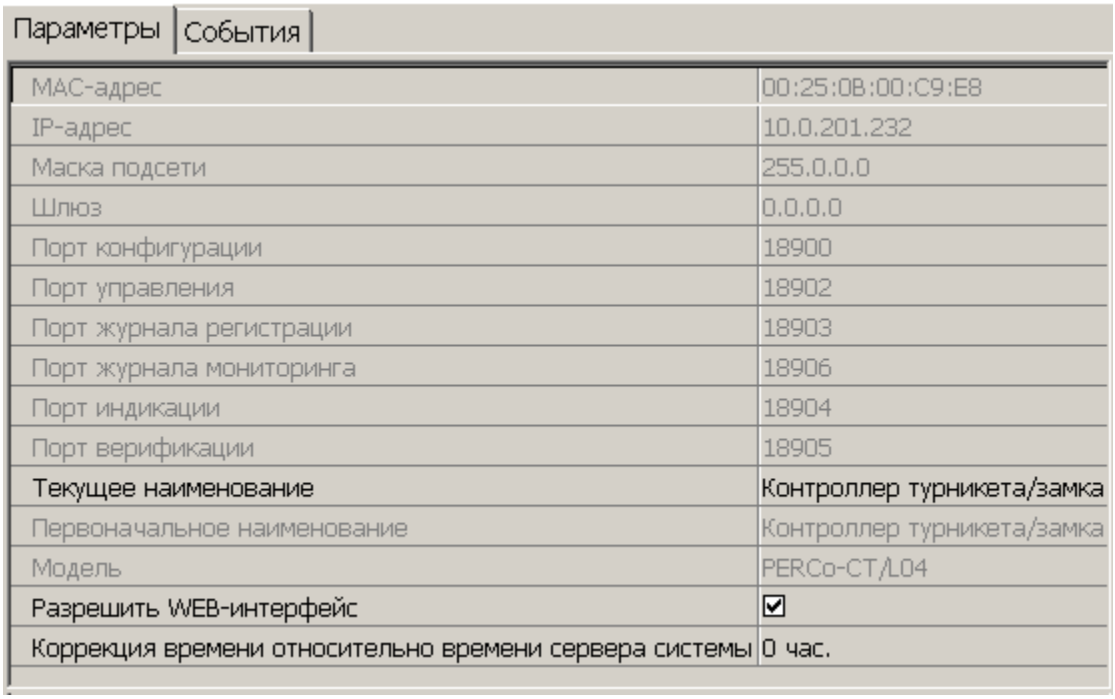
9. Контроллер для управления одним односторонним замком с двумя ШС.
10. Контроллер для управления одним односторонним замком с одним ШС.
11. Контроллер для управления одним односторонним замком.
12. Контроллер для управления двумя односторонними замками с двумя ШС.
13. Контроллер для управления двумя односторонними замками с одним ШС.
14. Контроллер для управления двумя односторонними замками.
15. Контроллер для управления тремя односторонними замками с одним ШС.
16. Контроллер для управления тремя односторонними замками.
17. Контроллер для управления четырьмя односторонними замками.
18. Контроллер для управления одним двусторонним замком с двумя ШС.
19. Контроллер для управления одним двусторонним замком с одним ШС.
20. Контроллер для управления одним двусторонним замком.
21. Контроллер для управления одним двусторонним и одним односторонним замками с одним ШС.
22. Контроллер для управления одним двусторонним и одним односторонним замками.
23. Контроллер для управления одним двусторонним и двумя односторонним замками.
24. Контроллер для управления двумя двусторонними замками с одним ШС.
25. Контроллер для управления двумя двусторонними замками.

Варианты шаблонов конфигурации ЭП ***PERCo-CT03*** (к любой конфигурации возможно подключить до восьми контроллеров замка ***PERCo-CL201***):

1. Электронная проходная.
2. Электронная проходная со встроенным картоприемником.
3. Электронная проходная со встроенным устройством «Антипаника».
4. Электронная проходная со встроенными картоприемником и устройством «Антипаника».

3.13.3 Контроллер доступа

Доступны следующие параметры:



Текущее наименование. Поле ввода позволяет ввести описательное название контроллера.

Разрешить Web-интерфейс. После установки параметра появляется возможность подключения к web-интерфейсу контроллера. По умолчанию доступ к web-интерфейсу запрещен. Доступ к web-интерфейсу будет возможен после остановки сервера системы или исключения контроллера из конфигурации системы в ПО.

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

3.13.4 Контроллер регистрации (LICON)

Доступны следующие параметры:

Параметры | События

MAC-адрес	00:25:0B:00:67:FD
IP-адрес	10.0.103.253
Маска подсети	255.0.0.0
Шлюз	0.0.0.0
Порт конфигурации	18900
Порт управления	18902
Порт журнала регистрации	18903
Порт журнала мониторинга	18906
Порт индикации	18904
Порт персонализации	18907
Макс. кол-во идентификаторов	5120
Текущее наименование	Контроллер регистрации
Первоначальное наименование	Контроллер регистрации
Модель	PERCo-CR01
Разрешить WEB-интерфейс	☑
Прямое направление прохода	☑
Контроль повторного предъявления идентификаторов	☑
Защита от передачи идентификаторов (Antipass)	Нет
Время ожидания персонализации	5 сек.
Время отображения персонализации	5 сек.
⊞ Локализация отображаемых строк:	

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

Разрешить Web-интерфейс. После установки параметра появляется возможность подключения к web-интерфейсу контроллера. По умолчанию доступ к web-интерфейсу запрещен. Доступ к web-интерфейсу будет возможен после остановки сервера системы или исключения контроллера из конфигурации системы в ПО.

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

Прямое направление прохода. Параметр позволяет указать, в направлении какого из считывателей проход считается входом. При установленном параметре правый считыватель считается входным, левый выходным. При снятом – наоборот.

Примечание:

При изменении прямого направления прохода подписи указателей *«Вход»* и *«Выход»* на ЖКИ не меняются. Изменить текст надписей указателей можно в раскрывающемся меню **Локализация отображаемых строк.**

Контроль повторного предъявления идентификаторов (Antipass). При установленном параметре контроллер отслеживает случаи повторного предъявления одной и той же карты доступа к тому же считывателю.

Примечание:

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

Защита от передачи идентификаторов (Antipass). Раскрывающийся список позволяет определить реакцию системы в случае повторного предъявления одной и той же карты доступа к считывателю, то есть при работе функции системы *Antipass*. Возможен выбор одного из следующих вариантов:

- **Нет** – реакция не задана.
- **Мягкая** – регистрируется событие *«Проход с нарушением зональности»*..
- **Жесткая** – при нарушении локальной зональности (*Antipass*) – проход по карте разрешается, при этом регистрируется событие *«Проход с нарушением зональности»*; при нарушении глобальной зональности (*Global Antipass*) регистрируется событие *«Запрет прохода по причине нарушения зональности».*

Время ожидания персонализации. Поле ввода позволяет задать время, в течение которого контроллер ожидает получения от сервера системы персональной информации (ФИО), связанной с предъявленной картой доступа. В случае невозможности получения информации на ЖКИ отображается идентификатор карты.

Время отображения персонализации. Поле ввода позволяет задать время, в течение которого на ЖКИ контроллера отображается персональная информация, связанная с предъявленной картой доступа.

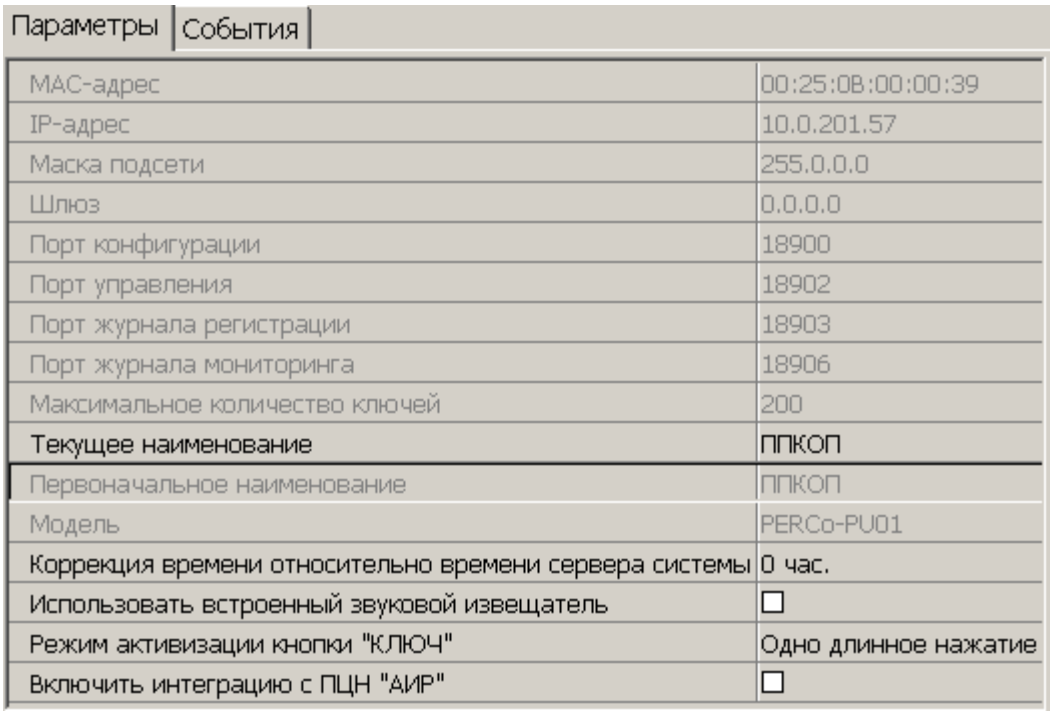
Локализация отображаемых строк. Раскрывающийся список позволяет изменить содержание сообщений, отображаемых на ЖКИ контроллера.

Контроллер регистрации имеет два встроенных считывателя. Для считывателей доступно поле ввода **Текущее наименование**, позволяющее изменить описательное название считывателей. По умолчанию: *«Считыватель №…».*

3.13.5 ППКОП (КБО)

Контроллеры ППКОП (КБО) предназначены для контроля состояния ОШС и ПШС, выдачи тревожных сообщений на пост центрального наблюдения (ПЦН), световое и звуковое оповещение, управления дополнительным оборудованием. Дополнительная информация о функционировании контроллеров ППКОП (КБО) приведена в их *«Руководстве по эксплуатации»*.

Доступны следующие параметры:



Текущее наименование Поле ввода позволяет ввести описательное название контроллера.

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

Использовать встроенный звуковой извещатель. По умолчанию флажок установлен и встроенный звуковой индикатор БУИ ППКОП (КБО) включен. При снятии флажка звуковой индикатор отключен и используется только для КБО по части СКУД.

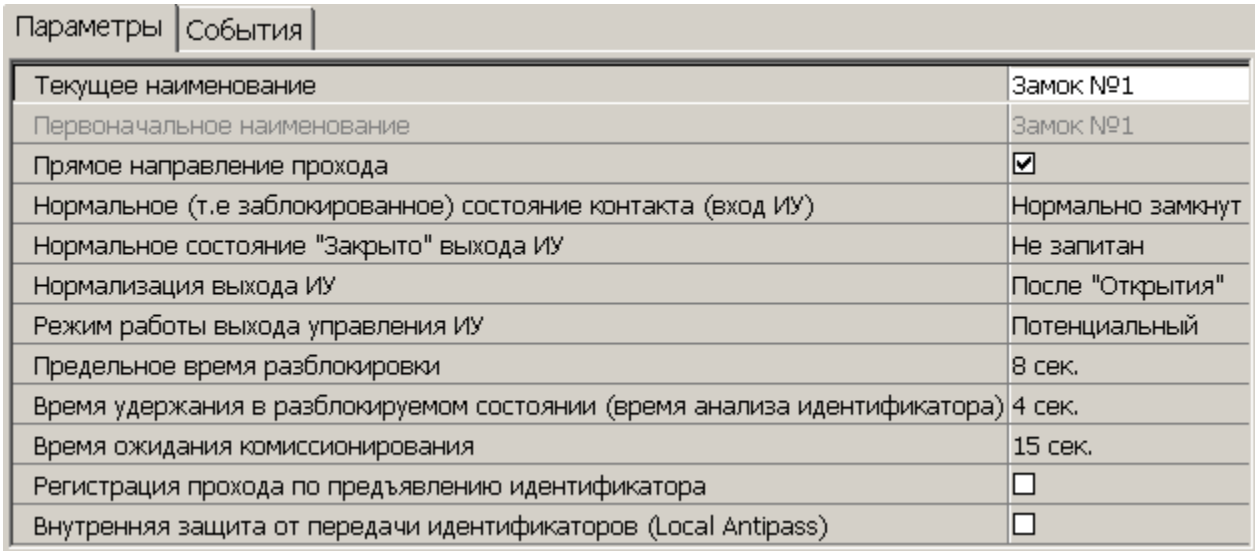
Режим активизациикнопки "КЛЮЧ". Раскрывающийся список позволяет выбрать способ разблокирования кнопок БУИ. Доступны следующие варианты:

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

Включить интеграцию с ПЦН «АИР» (для ППКОП). При установке флажка появляется возможность передавать тревожные сообщения на внешний пульт центрального наблюдения (ПЦН) и добавляется ресурс Объект интеграции с ПЦН «АИР».

3.13.6 ИУ (Замок/Турникет/ Шлагбаум)

Доступны следующие параметры:



Параметры | События

Текущее наименование	Замок №1
Первоначальное наименование	Замок №1
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"
Режим работы выхода управления ИУ	Потенциальный
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа идентификатора)	4 сек.
Время ожидания комиссионирования	15 сек.
Регистрация прохода по предъявлению идентификатора	☐
Внутренняя защита от передачи идентификаторов (Local Antipass)	☐

Текущее наименование. Поле ввода позволяет ввести описательное название ИУ.

Прямое направление прохода. Параметр позволяет указать, в направлении какого из считывателей проход считается входом.

- По умолчанию параметр установлен, и нумерация считывателей соответствует положению перемычки *«номер считывателя» (XP2)* на плате считывателя.
- Если параметр отключен, то тот считыватель, который в соответствии с его перемычкой должен иметь номер 1, в контроллере будет опознан как считыватель номер 2, и соответственно наоборот, считыватель номер 2 в контроллере будет опознан как считыватель номер 1.

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

Нормальное состояние «Закрыто» выхода ИУ (*Не запитан*/ *Запитан*) (Не доступен в конфигурации *«Контроллер АТП»*). Параметр указывает, активизирован ли выход управления ИУ (подано управляющее напряжение на реле или транзистор) при заблокированном ИУ.

Нормализация выхода ИУ (*После «Открытия»*/ *После «Закрытия»*). Параметр определяет, в какой момент нормализуется состояние выхода управления ИУ.

Режим работы выхода управления ИУ (Доступен только в конфигурации *«Контроллер управления дверьми»*) Описывает логику управления подключенным ИУ.

- **Потенциальный**
- **Импульсный** – режим управления применяется только для замков, поддерживающих этот режим. Рекомендуется использовать для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки «CISA»).

Время управляющего импульса. Параметр доступен при выборе импульсного режима работы выхода ИУ и определяет длительность импульса управления ИУ.

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

Время удержания в разблокированном состоянии (**Время анализа идентификатора**). Время, на которое открывается ИУ.

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

Регистрация прохода по предъявлению идентификатора (Не доступен в конфигурации *«Контроллер АТП»*). При установке параметра контроллер будет считать проход совершившимся сразу после предъявления карты доступа, независимо от того, будет ли реально совершен проход через ИУ или нет.

Внимание!

При установке параметра **Регистрация прохода по предъявлению идентификатора** недопустимо у ресурсов **Считыватель** для обоих направлений прохода:

- Устанавливать для параметра **Подтверждение разрешения** значение отличное от **Нет**. То есть запрещено проведение процедуры верификации от ПДУ или ВВУ.
- Проводить процедуру верификации из ПО.

Обратное может привести к некорректной работе функции контроля зональности (Antipass).

Так же при установке этого параметра не рекомендуется устанавливать для параметра **Защита от передачи идентификаторов** значение **Жесткая**.

Отсутствие датчиков проезда (Доступен только в конфигурации *«Контроллер АТП»*). При установке параметра контроллер будет считать проезд совершившимся сразу после предъявления карты доступа, независимо от того, будет ли реально совершен проход через ИУ или нет. ИУ будет открыто на Время удержания в разблокированном состоянии.

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

Внутренняя защита от передачи идентификаторов (Local Antipass). При установленном параметра контроллер отслеживает случаи повторного предъявления одной и той же карты доступа к тому же считывателю.

Fire Alarm в РЕЖИМЕ РАБОТЫ «ОХРАНА» – При установленном флажке, по команде от устройства *Fire Alarm,* аварийная разблокировка (открытие) ИУ, находящегося в составе ОЗ, будет производится при взятой на охрану ОЗ. При снятом параметре (по умолчанию) в РКД *«Охрана»* сигналы на входах **Тип: Fire Alarm** игнорируются.

3.13.7 Считыватель

Ресурс связан с контроллером ИУ и позволяет настроить с помощью ПО параметры функций верификации, контроля по времени, защиты от передачи карт доступа (Antipass). Доступны следующие параметры:

Адрес	4
Текущее наименование	Считыватель №4
Первоначальное наименование	Считыватель №4
Модель	PERCo-IRxx
Способ верификации	Нет
Верификация от ВВУ	
в РЕЖИМЕ работы "Контроль"	
Подтверждение прохода для ПОСЕТИТЕЛЕЙ	Постоянно
Время ожидания подтверждения	5 сек.
По истечении времени ожидания подтверждения генерировать событие	Запрет прохода от ВВУ
Верификация от ПДУ	
в РЕЖИМЕ работы "Контроль"	
Подтверждение прохода для ПОСЕТИТЕЛЕЙ	Постоянно
Время ожидания подтверждения	5 сек.
Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)	
Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)	
Контроль времени для идентификаторов СОТРУДНИКОВ	
Контроль времени для идентификаторов ПОСЕТИТЕЛЕЙ	
Дополнительные входы, маскируемые при разблокировке ИУ	
Дополнительные выходы, активизируемые при разблокировке ИУ	
Дополнительные выходы, нормализируемые при разблокировке ИУ	
Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ	
Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ	
Изымать в СТОП-ЛИСТ идентификаторы ПОСЕТИТЕЛЕЙ	Нет

Текущее наименование. Поле ввода позволяет ввести описательное название считывателя.

Способ верификации. Параметр позволяет указать будет ли при предъявлении карты доступа считывателю в РКД *«Контроль»* формироваться запрос на верифицирующее устройство. В качестве верифицирующих устройств могут использоваться: ПДУ, картоприемник, алкотестер (алкометр) или другое оборудование.

- **Нет.** Подтверждение от верифицирующего устройства не требуется.

Примечание:

Если для параметра **Подтверждение разрешения прохода** установлено значение отличное от **Нет**, то в случае прохода с верификацией от ПО и отсутствия связи с верифицирующим устройством доступ может быть подтвержден кнопкой ПДУ.

- **От ПДУ.** Для настройки картоприемника и верификации от ПДУ или ПО. Имеется возможность гибко настроить условия проведения верификации независимо для карт доступа сотрудников и посетителей в следующих случаях:
  - **при проходе** – верификация проводится при каждой попытке прохода;
  - **при проходе с НАРУШЕНИЕМ ВРЕМЕНИ** – верификация проводится при попытке прохода в случае нарушения времени (параметр **Контроль времени для идентификаторов** должен быть установлен на значение **Жесткий**).

- **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ** – верификация проводится в случае попытке повторного входа без предварительного выхода (параметр **Защита от передачи идентификаторов** должен быть установлен на значение **Жесткая**).

- **Софт.** Для верификации от оператора с помощью раздела ***«Верификация»*** ПО ***PERCo-S-20.***
- **От ВВУ**. Для верификации от алкотестера (алкометра) или другого оборудования. Имеется возможность настроить запуск процедуры верификации при предъявлении карт доступа независимо для сотрудников и посетителей.
- **При доступности Софт, иначе ПДУ;**
- **ПДУ или Софт;**
- **Сначала ПДУ, затем Софт;**
- **Сначала ВВУ, затем ПДУ;**
- **Сначала ВВУ, затем софт;**
- **При доступности софт, иначе ВВУ.**

Подтверждение прохода для ПОСЕТИТЕЛЕЙ. Параметр позволяет выбрать дополнительное условие проведения процедуры верификации для посетителей.

- **Постоянно.** Верификация проводится независимо от срока действия карты.
- **В последний день действия идентификатора.** Верификация проводится в случае, если дата предъявления совпадает с датой окончания срока действия карты.

Время ожидания подтверждения. Параметр позволяет установить время, в течение которого контроллер ожидает подтверждение запроса от верифицирующего устройства.

По истечении времени ожидания подтверждения генерировать событие. Параметр позволяет выбрать событие, регистрируемое в случае отсутствия подтверждения прохода от ВВУ:

- **Запрет прохода от ВВУ**. Рекомендуется в случае подключения ВВУ, имеющего только один выход разрешения прохода.
- **Отказ от прохода, нет ответа от ВВУ**. Рекомендуется в случае подключения ВВУ, имеющего выходы как для разрешения прохода, так и для запрета прохода.

Внимание!

Для **ПДУ** по истечении **времени ожидания подтверждения** автоматически будет генерироваться событие **Запрет прохода от ПДУ**.

Защита от передачи идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ (Antipass). Параметр позволяет для выбранных РКД определить реакцию контроллера на предъявление карты доступа сотрудника/ посетителя к считывателю в случае нарушения им функции контроля зональности (Antipass). Для каждого из указанных РКД контроллера можно выбрать один из видов контроля:

- **Нет**. Контроллер не учитывает зональность идентификатора карты для разрешения доступа.
- **Мягкая.** Контроллер разрешит доступ по карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение зональности»,* после совершения прохода регистрируется событие «*Проход по карте с несоответствием текущему местоположению»*.

- **Жесткая.** Контроллер запретит доступ по карте, при этом передается событие мониторинга *«Предъявление карты с нарушением зональности»* и регистрируется событие *«Запрет прохода по причине нарушения зональности».* Если для считывателя установлен параметр **Подтверждение от ДУ** (или верификация от ПО), то будет запущена процедура верификации.

Контроль времени для идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ. Параметр позволяет для выбранных РКД определить реакцию контроллера на предъявление карты доступа сотрудника/ посетителя к считывателю в случае нарушения установленного критерия доступа по времени. Для каждого из указанных РКД контроллера можно выбрать один из видов контроля:

- **Нет.** Контроллер не отслеживает временные критерии прав доступа карты.
- **Мягкий.** Контроллер разрешит доступ по предъявленной карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение времени»*, после совершения прохода регистрируется событие «*Проход по карте с несоответствием временным критериям доступа»*.
- **Жесткий.** Контроллер запретит доступ по карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение времени»* и регистрируется событие «*Запрет прохода, несоответствие временным критериям доступа»*. Если для считывателя установлен параметр **Подтверждениеот ДУ** (или верификация от ПО), то будет запущена процедура верификации.

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

Временной **Критерий маскирования**:

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

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

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

Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ. Параметр позволяет указать выходы, активизируемые при предъявлении карты доступа сотрудника/ посетителя, которой выданы права доступа на контроллер (карта не заблокирована и ее срок действия не истек). Этот параметр может быть использован в случае, если к дополнительным выходам подключена индикация, информирующая оператора о статусе предъявленной карты. Для выбора отметьте те дополнительные выходы, которые должны быть активизированы. Укажите временной критерий активизации.

Временной **Критерий активизации/нормализации**:

- **На указанное время**. Выход активизируется/ нормализуется на указанное время. Отсчет времени начинается с момента предъявления карты доступа, независимо от того, будет разрешен проход или нет.
- **На время срабатывания.**Выход активизируется/ нормализуется на указанное время. Отсчет времени начинается с момента разблокирования ИУ. Выход возвращается в исходное состояние при блокировании ИУ, либо по истечении **Времени удержания в разблокированном состоянии**.
- **На время срабатывания и после срабатывания.** Выбор этого параметра является комбинацией двух предыдущих. Выход активизируется/ нормализуется на указанное время, начиная с момента разблокирования ИУ и до момента его блокирования, плюс указанное время, либо, если проход не был совершен, до истечения **Времени удержания в разблокированном состоянии**.

Изымать в СТОП-ЛИСТ идентификаторы ПОСЕТИТЕЛЕЙ. Функция доступна только при наличии связи контроллера с сервером системы. Параметр позволяет выбрать условие, при котором идентификатор предъявленной карты доступа посетителя автоматически заносится в СТОП-лист, то есть в список карт запрещенных к использованию.

- **Нет**. Идентификатор не заносится в СТОП-лист.
- **После любого прохода**. Идентификатор заносится в СТОП-лист при первом предъявлении.
- **После прохода в последний день действия идентификатора**. Идентификатор заносится в СТОП-лист если дата предъявления совпадает с датой окончания срока действия карты.

3.13.8 Генератор тревоги

Ресурс связан с контроллером ИУ и позволяет выделить события, которые должны приводить к генерации тревоги в контроллере, и соответствующему управлению выделенным выходом тревоги (один из релейных выходов контроллера для которого выбран **Тип: Генератор тревоги**). Доступны следующие параметры:

Параметры | События

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

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

Генерация тревоги при предъявлении идентификатора. Параметр позволяет указать события, связанные с предъявлением карт доступа, при регистрации которых произойдет генерация тревоги. Для каждого события есть возможность выбрать тип тревоги:

- **Нет**
- **Тихая.** Тревога генерируется, но при этом не активизируются выходы, для которых выбран **Тип: Генератор тревоги**.
- **Громкая.** Генерируется тревога.

Генерация тревоги при несанкционированной разблокировке ИУ. Параметр позволяет для РКД *«Контроль»* и *«Закрыто»* указать, будет ли генерироваться тревога в случае механической разблокировки ИУ при помощи ключа, то есть без команды от контроллера.

Генерация тревоги по недопустимо долгому открытию ИУ. Параметр позволяет для РКД *«Контроль»* указать, будет ли генерироваться тревога в случае, если после открытия ИУ оно не было нормализовано в течение **Предельного времени разблокировки**, заданного в параметрах этого ИУ.

Генерация тревоги по датчику вскрытия корпуса контроллера. Параметр позволяет указать, будет ли генерироваться тревога в случае вскрытия корпуса контроллера.

3.13.9 Дополнительный вход

Дополнительные входы контроллеров могут быть использованы для наблюдения за состоянием внешнего оборудования, подключенного к ним. Входы могут использоваться для подключения кнопки сброса тревоги, ВВУ, устройства для подачи команды аварийной разблокировки *FireAlarm* и др.

Доступны следующие параметры:

Тип. Раскрывающийся список позволяет выбрать один из следующих типов:

- **Нет.** К данному входу не подключено никакое внешнее оборудование.
- **Обычный.** К данному входу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
- **Специальный**. Предназначен для автономного сброса тревоги, выключения сирены.
- **FireAlarm**. Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ *Fire Alarm*. Тип входа **FireAlarm** не может быть изменён для входов контроллеров и ЭП ***PERCo*** серии x.2, для которых он установлен по умолчанию. В этом случае дополнительный вход обозначается как **Вход FireAlarm.**
- **Подтверждение от ВВУ.** Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае разрешения прохода.
- **Запрет от ВВУ.** Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае запрета прохода.

В зависимости от выбранного типа остальные параметры выхода могут различаться.

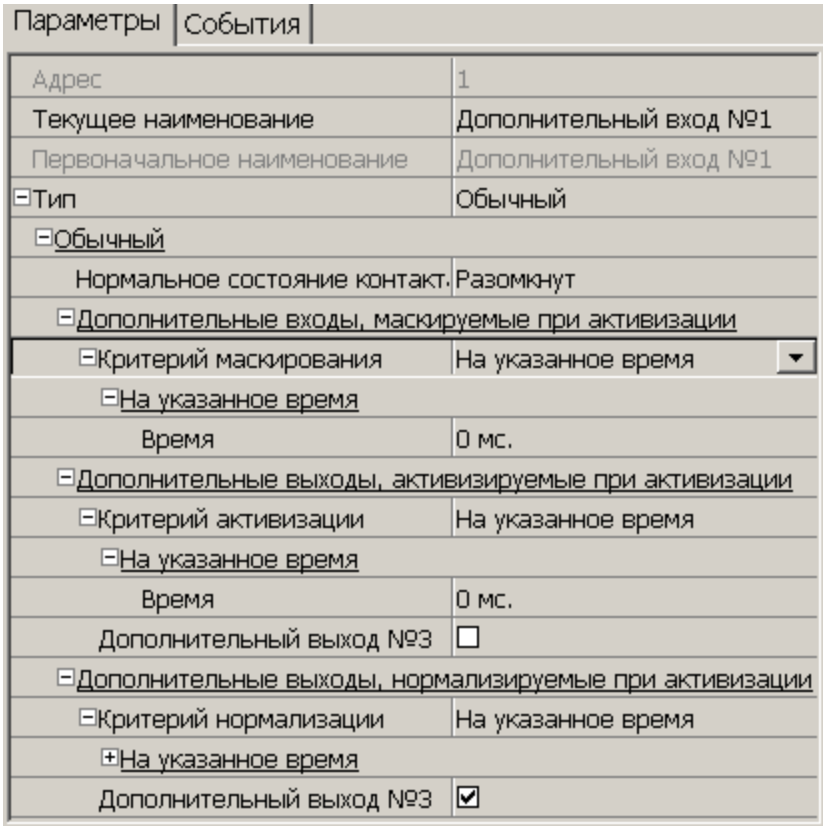
Нормальное состояние контакта (*Разомкнут/ Замкнут*). Параметр не доступен для входа **Тип: FireAlarm**. Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

Для типов **Подтверждение от ВВУ** и **Запрет от ВВУ** доступны следующие параметры:

- **Номер ИУ.** Параметр задаёт номер ИУ, к которому привязывается считыватель.
- **Направление.** Параметр задаёт направление ИУ, к которому привязывается считыватель.

Тип входа «Обычный»

Доступны следующие параметры:



Дополнительные входы, маскируемые при активизации. Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы (т.е. не воспринимать управляющий сигнал от внешнего оборудования) при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные входы, которые должны быть маскированы. Укажите временной критерий маскирования.

Дополнительные выходы, активизируемые при активизации. Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть активизированы. Укажите временной критерий активизации. Следует заметить, что активизация релейного выхода, привязанная к активизации дополнительного входа, не учитывает возможного шунтирования этого входа. Это очень важно для случаев применения в системе датчиков контроля зоны прохода.

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

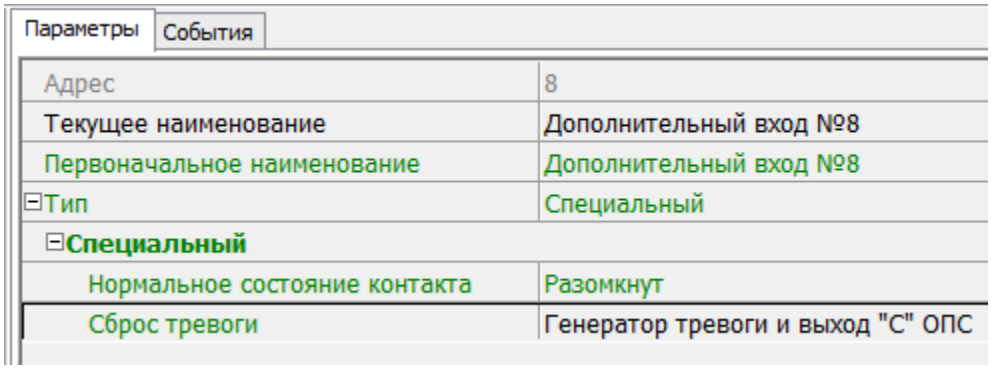
Временной **Критерий маскирования/активизации/нормализации**:

- **На указанное время.** Выбранные дополнительные входы будут маскированы на указанное время.

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

Тип входа «Специальный»

Доступны следующие параметры:



Сброс тревоги. Параметр определяет реакцию на получение управляющего сигнала:

- **Генератор тревоги.** При установке параметра получение управляющего сигнала на данном дополнительном входе приведет к сбросу тревоги.
- **Выход «С» ОПС.** При установке параметра получение управляющего сигнала на данном дополнительном входе приведет к выключению сирены, подключенной к выходу, работающему по программе «Сирена».
- **Генератор тревоги и выход «С» ОПС.**

Примечание:

Если ни один из параметров **Сброс тревоги (Генератор тревоги)** и **Сброс сирены (Выход «С» ОПС)** не установлен, то этот вход будет сконфигурирован как вход *Fire Alarm*.

Тип входа «Подтверждение от ВВУ»

Доступны следующие параметры:

Адрес	2
Текущее наименование	Дополнительный вход №2
Первоначальное наименование	Дополнительный вход №2
⊟Тип	Подтверждение от ВВУ
⊟**Подтверждение от ВВУ**	
Нормальное состояние контакта	Разомкнут
Контроллер	Контроллер замка CL201 №1
Считыватель	Считыватель CL201 №1
⊟**Дополнительные входы, маскируемые при активизации**	
⊟Критерий маскирования	На указанное время
⊟**На указанное время**	
Время	0 мс.
⊟**Дополнительные выходы, активизируемые при активизации**	
⊟Критерий активизации	На указанное время
⊟**На указанное время**	
Время	0 мс.
⊟**Дополнительные выходы, нормализируемые при активизации**	
⊟Критерий нормализации	На указанное время
⊟**На указанное время**	
Время	0 мс.

Нормальноесостояниеконтакта(*Разомкнут/ Замкнут*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

Контроллер. Параметр позволяет определить устройство, от которого будет ожидаться сигнал подтверждения прохода. В этом качестве могут выступать так же контроллеры второго уровня ***PERCo-CL201.1.***

Считыватель. Параметр позволяет определить устройство, с помощью которого необходимо провести подтверждение прохода.

Дополнительные входы, маскируемые при активизации. Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы (т.е. не воспринимать управляющий сигнал от внешнего оборудования) при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные входы, которые должны быть маскированы. Укажите временной критерий маскирования.

Дополнительныевыходы, активизируемыепри активизации.Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть активизированы. Укажите временной критерий активизации. Следует заметить, что активизация релейного выхода, привязанная к активизации дополнительного входа, не учитывает возможного шунтирования этого входа. Это очень важно для случаев применения в системе датчиков контроля зоны прохода.

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

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

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

Тип входа «Запрет от ВВУ»

Доступны следующие параметры:

Адрес	2
Текущее наименование	Дополнительный вход №2
Первоначальное наименование	Дополнительный вход №2
⊟Тип	Запрет от ВВУ
⊟**Запрет от ВВУ**	
Нормальное состояние контакта	Разомкнут
Контроллер	Контроллер замка CL201 №1
Считыватель	Считыватель CL201 №1
⊟**Дополнительные входы, маскируемые при активизации**	
⊟Критерий маскирования	На указанное время
⊟**На указанное время**	
Время	0 мс.
⊟**Дополнительные выходы, активизируемые при активизации**	
⊟Критерий активизации	На указанное время
⊟**На указанное время**	
Время	0 мс.
⊟**Дополнительные выходы, нормализируемые при активизации**	
⊟Критерий нормализации	На указанное время
⊟**На указанное время**	
Время	0 мс.

Нормальное состояние контакта (*Разомкнут/ Замкнут*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

Контроллер. Параметр позволяет определить устройство, от которого будет ожидаться сигнал запрета прохода. В этом качестве могут выступать так же контроллеры второго уровня ***PERCo-CL201.1.***

Считыватель. Параметр позволяет определить устройство, с помощью которого, в случае необходимости, возможно провести запрет прохода.

Нормальное состояние контакта (*Разомкнут/ Замкнут*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

Дополнительные входы, маскируемые при активизации. Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы (т.е. не воспринимать управляющий сигнал от внешнего оборудования) при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные входы, которые должны быть маскированы. Укажите временной критерий маскирования.

Дополнительные выходы, активизируемые при активизации. Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть активизированы. Укажите временной критерий активизации. Следует заметить, что активизация релейного выхода, привязанная к активизации дополнительного входа, не учитывает возможного шунтирования этого входа. Это очень важно для случаев применения в системе датчиков контроля зоны прохода.

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

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

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

3.13.10 Дополнительный выход

Дополнительные выходы могут быть использованы для управления любым дополнительным оборудованием в рамках системы. Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название выхода.

Тип. Раскрывающийся список позволяет выбрать следующие типы выхода:

- **Нет.** К данному выходу не подключено никакое внешнее оборудование.
- **Обычный.** К выходу подключено дополнительное оборудование, логика управления которым описывается через описание других устройств системы (за исключением ресурса **Генератор тревоги**).
- **Генератор тревоги.** Решение об активизации дополнительного выхода принимается в соответствии с параметрами, заданными для ресурса **Генератор тревоги**.

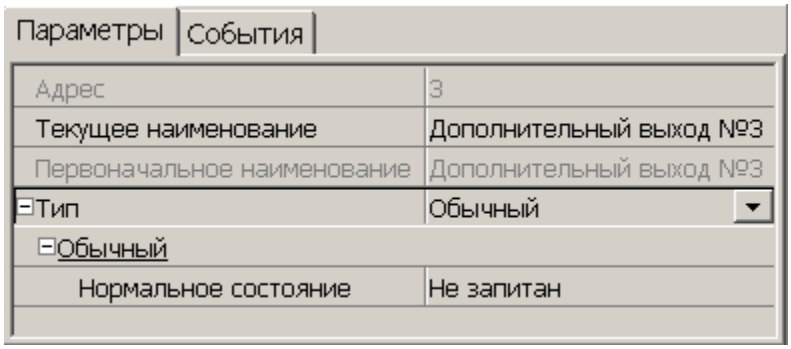
- **ОПС.** Выход предназначен для управления световым или звуковым оповещателем, а также для передачи тревожных извещений на пульт центрального наблюдения (ПЦН) при изменении режима ОЗ.

Примечание:

После включения питания все выходы нормализуются.

Тип выхода «Обычный»

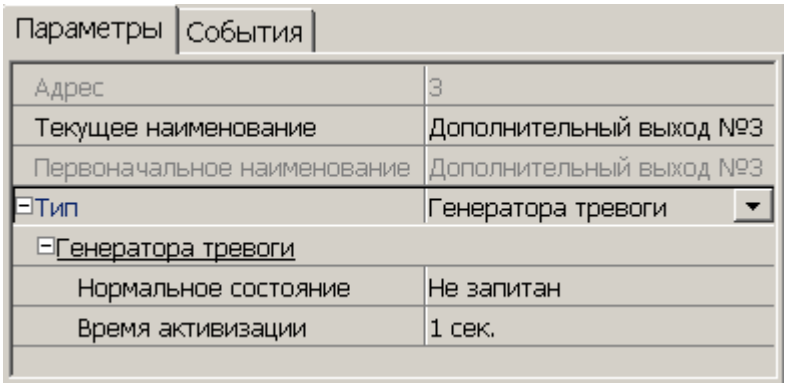
Доступны следующие параметры:



Нормализованное состояние (*Не запитан/ Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода. Для выходов №1 и № 2 нормализованное состояние: **Не запитан**.

Тип выхода «Генератор тревоги»

Доступны следующие параметры:



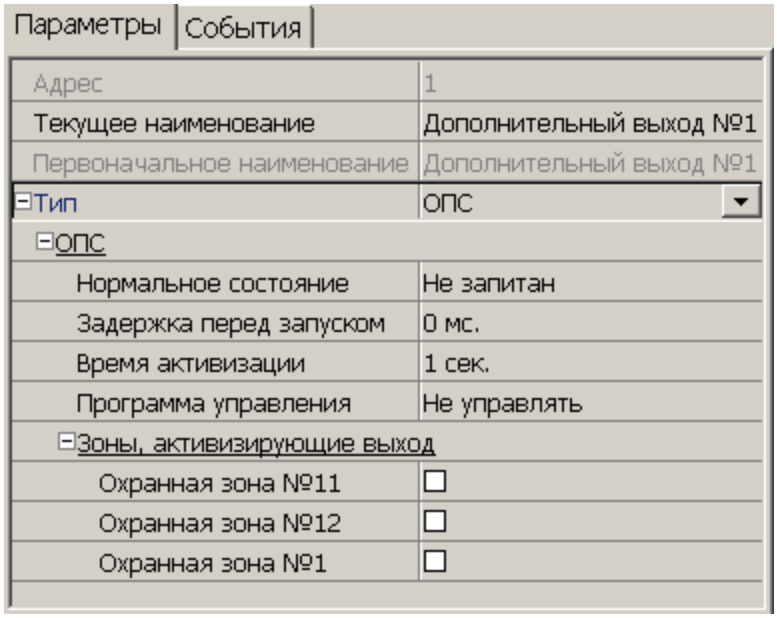
Нормализованное состояние (*Не запитан/ Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода. Для выходов №1 и № 2 нормализованное состояние: **Не запитан**.

Время активизации. Время на которое выход, при наличии активизирующего управляющего воздействия, меняет свое состояние из нормализированного на противоположное.

Тип выхода «ОПС»

Программа управления задает логику работы контроллера по управлению этим дополнительным выходом. Инициатором активизации выхода является изменение режима ОЗ, отмеченных как **Зоны, активизирующие выход**. После возникновения события, инициирующего активизацию выхода, он активизируется. В зависимости от параметра **Программа управления** выход может быть *запитан/ не запитан* постоянно (пока ресурс панели находится в текущем режиме), либо изменять свое физическое состояние (мигать) из нормализированного на противоположное. Нормализация выхода происходит либо по истечению времени, указанному в параметре **Время активизации** (если оно не бесконечное), либо по сбросу панели, либо после выключения ее питания.

Доступны следующие параметры:



Нормализованное состояние (*Не запитан/ Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода. Для выходов №1 и № 2 нормализованное состояние: **Не запитан**.

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

Время активизации. Время на которое выход, при наличии активизирующего управляющего воздействия, меняет свое состояние из нормализированного на противоположное.

Примечание:

Для программ *«Лампа 1»*, *«Лампа 2»*, *«ПЦН 1»* и *«ПЦН 2»* рекомендуется устанавливать **Время активизации: Бесконечно**.

Программа управления. Раскрывающийся список позволяет выбрать режим работы выхода после его активизации.

Зоны, активизирующие выход. Параметр позволяет выбрать ОЗ, нарушение которых приведет к активизации выхода (запуску выбранной для него программы управления). Для программ *«Лампа 1»*, *«ПЦН 1»* и *«ПЦН 2»* активизация выхода произойдет только при переходе в данный режим всех ОЗ, указанных в параметре **Зоны, активизирующиевыход** (логическое «И»). Во всех остальных случаях для активизации выхода достаточно поступления сигнала об изменении режима любой из ОЗ, указанных в параметре (логическое «ИЛИ»).

Программы управления выходом «ОПС»

При управлении выходом отслеживается режим работы ОЗ, отмеченных в списке **Зоны, активирующие выход**. Доступны следующие программы управления выходом :

- **Включить при тревоге.** В случае перехода хотя бы одной из ОЗ в режим *«ТРЕВОГА»* выход будет активизирован на **Время активизации**.
- **Мигать при тревоге.** В случае перехода хотя бы одной из ОЗ в режим *«ТРЕВОГА»* выход будет активизироваться с частотой 1Гц.
- **Лампа 1**. Программа управления световым оповещателем тревожной ситуации. Для смены режима требуется, чтобы все ОЗ изменили свое состояние.
- **Лампа 2.** Программа управления световым оповещателем тревожной ситуации. Для смены режима требуется, чтобы хотя бы одна ОЗ изменила свое состояние.
- **ПЦН 1.** Программа для передачи тревожных извещений на пост центрального наблюдения (ПЦН). В случае перехода всех ОЗ в режим *«ОХРАНА»* выход будет активизирован. Передача тревожных извещений на ПЦН
- **ПЦН 2.** Программа для передачи тревожных извещений на пост центрального наблюдения (ПЦН). В случае перехода всех ОЗ в режим *«ОХРАНА»* или в режим *«СНЯТА»* выход будет активизирован.
- **Сирена.** Программа управления звуковым оповещателей тревожной ситуации. В случае перехода хотя бы одной из ОЗ в режим *«ТРЕВОГА»* выход будет активизирован на **Время активизации**.
- **Вкл. перед взятием для ИУ в импульсномрежиме управления.**Если для ИУ установлен **Режим работы выхода управления ИУ: Импульсный**, то при постановке на охрану введена задержка на 4 секунды, действующая между вторым поднесением карты и постановкой на охрану, чтобы можно было открыть и снова закрыть дверь для сброса механизма самовзвода замка. Данная программа служит для возможности индикации данной задержки.
- **Включить при взятии.** В случае перехода хотя бы одной из ОЗ в режим *«ОХРАНА»* выход будет активизирован на **Время активизации**.
- **Включить при снятии.** В случае перехода хотя бы одной из ОЗ в режим *«СНЯТА»* выход будет активизирован на **Время активизации**.

Для ППКОП кроме этого доступны программы:

Примечание:

Режимы работы *«ВЗЯТИЕ», «АВТОПЕРЕВЗЯТИЕ», «ВНИМАНИЕ», «ПОЖАР», «НЕИСПРАВНОСТЬ»* доступны только для ППКОП.

- **Включить при неисправности**. В случае перехода ППКОП в состояние *«Неисправность»* выход будет активизирован на **Время активизации**.
- **Мигать при неисправности**. В случае перехода ППКОП в состояние *«Неисправность»* выход будет активизироваться с частотой 1Гц.
- **Включить при пожаре**. В случае перехода хотя бы одной из ПЗ в состояние *«Пожар»* выход будет активизирован на **Время активизации**.
- **Мигать при пожаре**. В случае перехода хотя бы одной из ПЗ в состояние *«Пожар»* выход будет активизироваться с частотой 1Гц.
- **Включить при внимании и пожаре**. В случае перехода хотя бы одной из ПЗ в состояние *«Внимание»* или *«Пожар»* выход будет активизирован на **Время активизации**.
- **Мигать при внимании и пожаре**. В случае перехода хотя бы одной из ПЗ в состояние *«Внимание»* или *«Пожар»* выход будет активизироваться с частотой 1Гц.

- **Включить перед взятием.** В случае перехода хотя бы одной из ПЗ в состояние *«Взятие»* выход будет активизирован на **Время активизации**.
- **Включить при автоперевзятии.** В случае перехода хотя бы одной из ПЗ в состояние *«Автоперевзятие»* выход будет активизирован на **Время активизации**.

В таблицах используются следующие обозначения:

В столбце **Зоны** указано условие смены режима работы выхода:

OR – для смены режима необходимо, чтобы хотя бы одна из ОЗ или ПЗ, отмеченных в списке **Зоны, активирующиевыход** изменила свое состояние.

AND – для смены режима необходимо, чтобы все ОЗ или ПЗ, отмеченные в списке **Зоны, активирующие выход**, перешли в одно и то же состояние.

В таблице указаны следующие режимы работы выхода:

0 – выход нормализован.

N – состояние выхода не изменяется.

∞ – выход активизирован постоянно.

такт – выход активизирован в течение времени, определенного параметром**Время активизации**.

tзад – выход активизируется на 4 сек перед переходом ОЗ в режим *«ОХРАНА».*

1Гц, 2Гц – выход активизируется с частотой 1Гц или 2Гц, соответственно, в течение времени, определенного параметром **Время активизации**.

Программы управления выходами для контроллеров доступа

Название программы	Зоны	Режим ОЗ		
		Снята	Охрана	Тревога
Включить при тревоге	OR	0	0	такт
Мигать при тревоге	OR	0	0	1Гц
Лампа 1	AND	0	∞	1Гц
Лампа 2	OR	0	∞	1Гц
ПЦН 1	AND	0	∞	0
ПЦН 2	AND	∞	∞	0
Сирена	OR	0	0	такт
Вкл. перед взятием для ИУ в импульсном режиме управления	OR	0	tзад	0
Вкл. при взятии	OR	0	такт	0
Вкл. при снятии	OR	такт	0	0
Вкл. при автоперевзятии	Не используется			

Программы управления выходами для ППКОП

Название программы	Зоны	Режим зоны							Неисправность ППКОП
		Снята	Взятие	Автоперевзятие	Охрана	Тревога	Внимание	Пожар	Неисправность	
Включить при неисправности	OR	0	N	N	N	N	N	N	такт	такт
Мигать при неисправности	OR	0	N	N	N	N	N	N	1Гц	1Гц
Включить при пожаре	OR	N	N	N	0	N	N	такт	N	N
Мигать при пожаре	OR	N	N	N	0	N	N	1Гц	N	N
Включить при внимании и пожаре	OR	0	N	N	0	N	такт	такт	N	N
Мигать при внимании и пожаре	OR	0	N	N	0	N	1Гц	1Гц	N	N
Включить при тревоге	OR	0	N	N	0	такт	N	N	N	N
Мигать при тревоге	OR	0	N	N	0	1Гц	N	N	N	N
Лампа 1	AND	0	2Гц	N	∞	1Гц	N	N	N	N
Лампа 2	OR	0	2Гц	N	∞	1Гц	N	N	N	N
ПЦН 1	AND	0	0	N	∞	0	N	N	N	N
ПЦН 2	AND	∞	0	N	∞	0	N	N	N	N
Сирена	OR	0	N	N	0	такт	N	N	N	N
Вкл. перед взятием	OR	0	такт	N	0	0	N	N	N	N
Вкл. при взятии	OR	0	N	N	такт	0	N	N	N	N
Вкл. при снятии	OR	такт	0	N	0	0	N	N	N	N
Вкл. при автоперевзятии	OR	0	N	такт	0	0	N	N	N	N

3.13.11 Шлейф сигнализации

Контроллеры имеют возможность подключения стандартных ШС для организации ОЗ и ПЗ. Для настройки ресурса доступны следующие параметры:

Текущее наименование. Поле ввода позволяет ввести описательное название ШС.

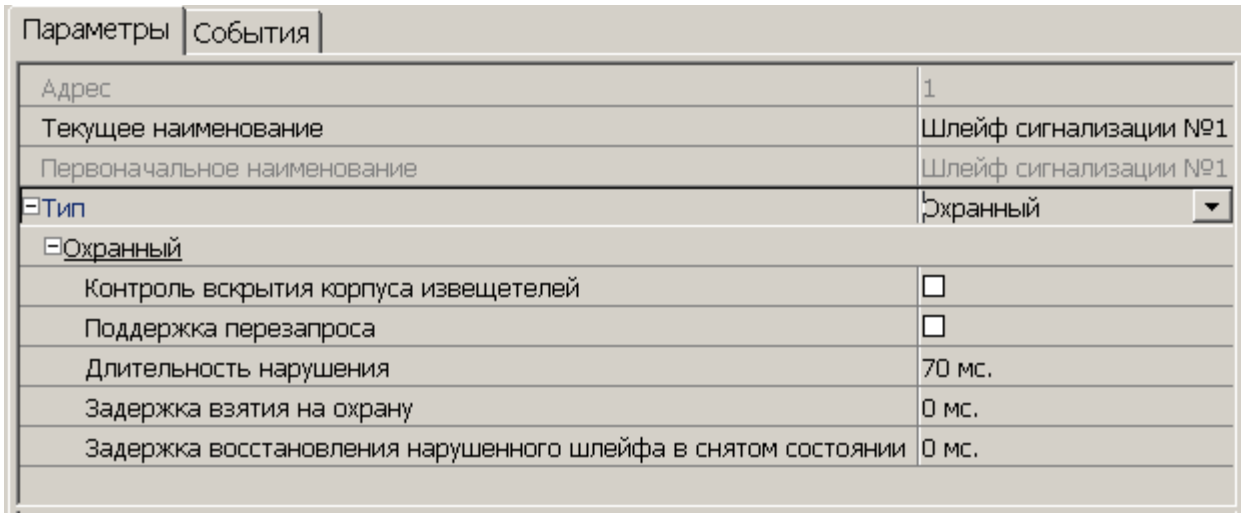
Тип. Раскрывающийся список позволяет выбрать тип ШС:

- **Нет** – ШС отключен.
- **Охранный** – Подключен охранный ШС.
- **Пожарный** – (только для ППКОП) Подключен пожарный ШС.
- **КТС** – (только для ППКОП) Подключена пожарный КТС.

Тип шлейфа «Охранный» (ОШС)

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

Доступны следующие параметры:



Контроль вскрытия корпуса извещателя. При установке параметра контроллер отслеживает вскрытие корпуса извещателя ШС.

Поддержка перезапроса. При установке параметра контроллер после срабатывания извещателей на несколько секунд снимает питание с ШС, после чего повторно проверяет его состояние.

Длительность нарушения. Параметр определяет время интегрирования для ШС (70/300 мс), то есть максимальное время нарушения, не приводящее к переходу в режим *«ТРЕВОГА»*.

Задержка взятия на охрану. Параметр определяет время, по истечению которого контроллер предпринимает попытку взять ШС на охрану после поступления соответствующей команды. Время, определяемое значением этого параметра, может быть использовано как «задержка на выход» для ШС входных зон.

Внимание!

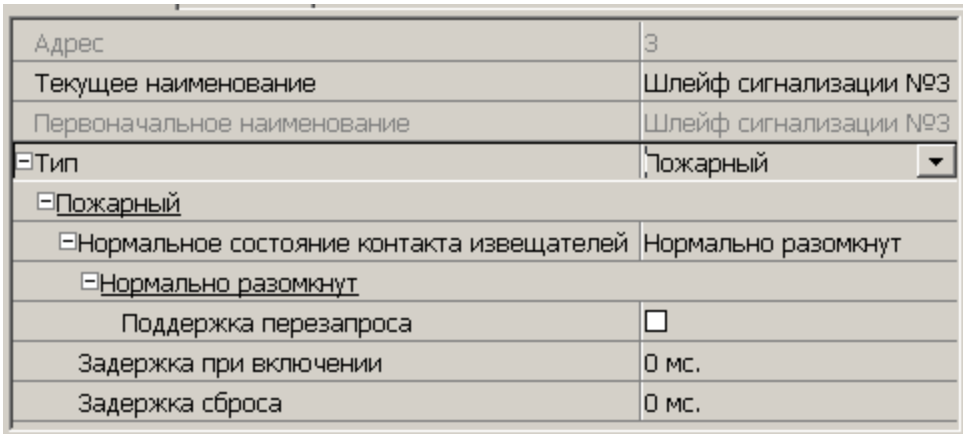
В версиях прошивки x.0.0.19 и старше установленное в ПО ***PERCo-S-20*** значение параметра **Задержка взятия на охрану** игнорируется и всегда считается равным **0**.

Задержка восстановления нарушенного шлейфа в снятом состоянии:

- Если для параметра установлено значение: **0**, то ШС в режиме *«СНЯТ»* не контролируется.
- В противном случае в режиме *«СНЯТ»* продолжается отслеживание состояния ШС.
  - Если ШС перейдет в состояние *«нарушение»*, то регистрируется событие *«Неисправность снятого ОШС»*. Состояние выходов ОПС не изменяется.
  - Если после этого ШС возвращается в состояние *«норма»* и продержится этом состоянии время, указанное в этом параметре, то регистрируется событие *«Нормализация снятого ОШС»*. Состояние выходов ОПС не изменяется.

Тип шлейфа «Пожарный» (ПШС)

Доступны следующие параметры:



Текущее наименование.Поле ввода позволяет ввести произвольное описательное название ресурса.

Нормальное состояние контактов извещателей (*Нормально разомкнут*/ *Нормально замкнут*) – параметр, определяющий нормализованное состояние контакта извещателей, подключенных к ШС.

Поддержка перезапроса – параметр, определяющий, надо или нет после срабатывания извещателей снимать питание с ШС и перепроверять его состояние.

Задержка при включении – параметр, определяющий время задержки до начала измерений сопротивления ШС после подачи на него питания при перезапросе и взятии.

Задержка сброса – параметр, определяющий время нахождения ШС в режиме *«Сброс»* (без питания).

3.13.12 Зона сигнализации

Зона сигнализации – это часть территории объекта, на которой физически расположены один или несколько ШС.

Проникновение в зону сигнализации, сконфигурированную как *охранная зона* (ОЗ), приводит к нарушению охранного ШС и переход данной ОЗ в режим *«ТРЕВОГА»*.

Возникновение пожара (задымления, превышение определенного порога температуры, открытое пламя и т.д.) в зоне сигнализации, сконфигурированной как пожарная зона (ПЗ), приводит к изменению состояния входящего в нее пожарного ШС и переход данной ПЗ в режим *«ВНИМАНИЕ»* или *«ПОЖАР»*.

Для настройки зон сигнализации доступны следующие параметры:

Текущее наименование.Поле ввода позволяет ввести описательное название зоны.

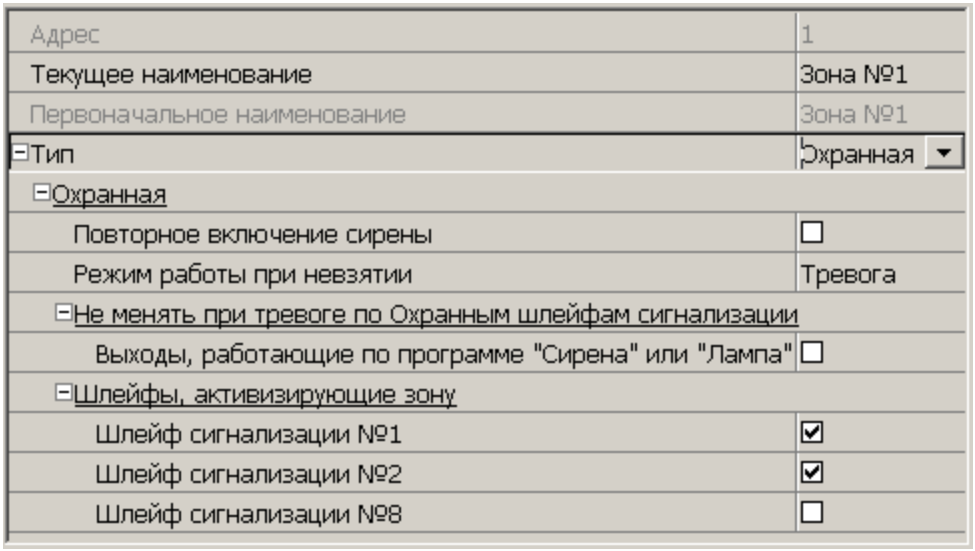
Тип. Раскрывающийся список позволяет выбрать тип зоны сигнализации:

- **Нет** – зона не сконфигурирована.
- **Охранная** – зона сконфигурирована как ОЗ.
- **Пожарная** – (только для ППКОП) зона сконфигурирована как ПЗ.
- **КТС** – (только для ППКОП) зона сконфигурирована для шлейфов КТС.

Тип зоны «Охранная» (ОЗ)

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

Доступны следующие параметры:



Включить ИУ в зону. При установке параметра ИУ, подключенное к контроллеру будет включено в ОЗ. В РКД *«Охрана»* при регистрации события *«Взлом ИУ»* ОЗ перейдет в режим *«ТРЕВОГА»*.

Повторное включение сирены. При установке параметра активизация дополнительного выхода, для которого установлен **Тип: ОПС** и выбрана программа управления *«Сирена»,* происходит при каждом переходе ИУ или одного из ШС в состояние *«нарушение»*, даже если ОЗ уже находится в режиме *«ТРЕВОГА»*.

Режим работы при невзятии. Параметр указывает действие, которое будет происходить при невозможности взятия ОЗ на охрану. Имеются следующие значения:

- **Тревога.** ОЗ будет переведена в режим *«ТРЕВОГА»*.
- **Автоматическое перевзятие**. Производится повторная попытка взятия на охрану до тех пор, пока постановка на охрану не произойдет.
- **Возврат в «Снята»**. ОЗ перейдет в режим *«СНЯТА»*.

Внимание!

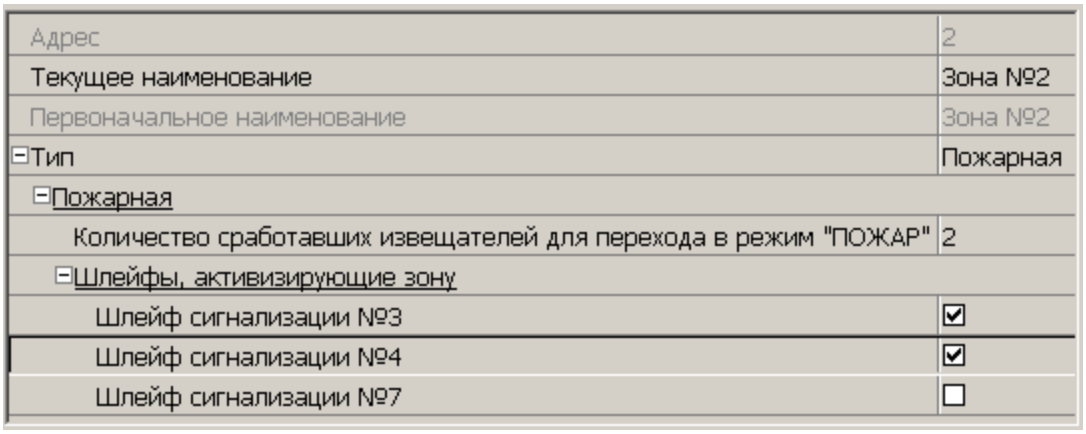
В версиях прошивки x.0.0.19 и старше установленное в ПО ***PERCo-S-20*** значение параметра **Режим работы при невзятии** игнорируется и всегда считается равным **Возврат в «Снята»**.

Тихая тревога. При установке параметра в случае перехода ОЗ в режим *«ТРЕВОГА»* запрещена активизация дополнительных выходов, для которого установлен **Тип: ОПС** и выбрана программа управления *«Включить при тревоге»*.

Шлейфы, активизирующиезону. Параметр позволяет отметить ШС, которые будут входить в ОЗ и состояние которых будет отслеживаться контроллером в режиме ОЗ *«ОХРАНА».* В ОЗ могут входить ШС, для которых выбран **Тип: Охранный**. При этом каждый ШС может входить только в одну ОЗ.

Тип зоны «Пожарная» (ПЗ)

Доступны следующие параметры:



Количество сработавших извещателей для перехода в режим "ПОЖАР" (*«1»/ «2»*) – параметр, задающий минимальное количество извещателей, срабатывание которых переводит данную ПЗ в режим *«Пожар»*.

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

- **Никогда –** изменения режимов работы ПЗ не влияют на состояние 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. Параметр позволяет отметить флажками ПШС, которые будут входить в ПЗ и состояние которых будет отслеживаться контроллером при постановке ПЗ на контроль (переводе в режим *«Норма»*). В ОЗ могут входить ШС, для которых выбран **Тип: Пожарный**. При этом каждый ШС может входить только в одну ОЗ.

3.13.13 Интеграция ППКОП с ПЦН «АИР»

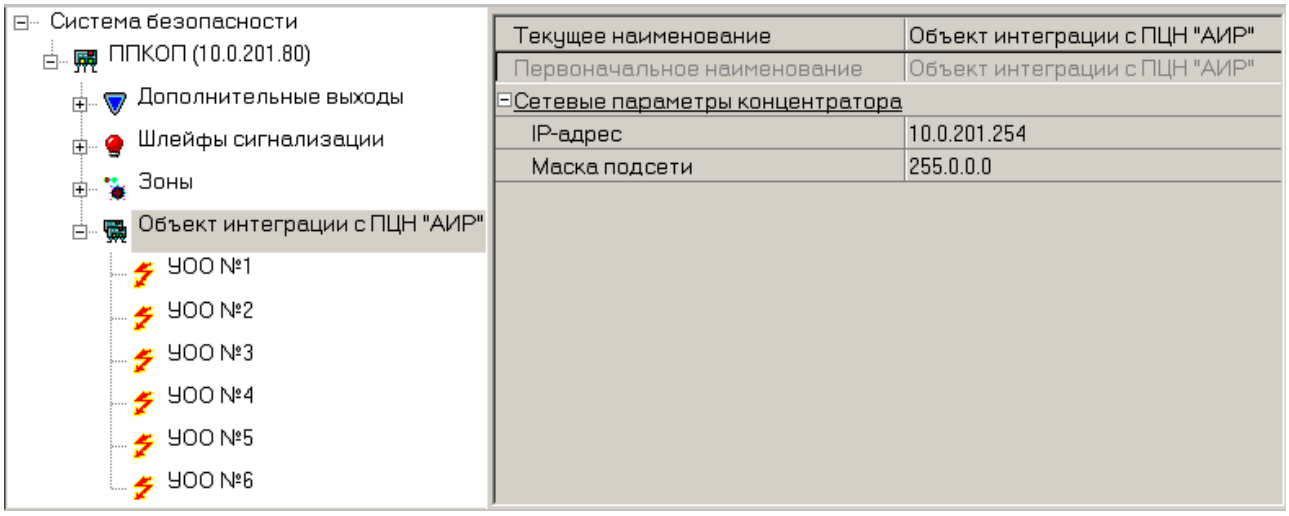
В системе предусмотрена возможность проведения интеграции ППКОП с оборудованием автоматизированной системы передачи извещений *«Ахтуба»*, разработанной научно-производственным центром *«АИР»*. Это дает возможность передавать тревожные сообщения на внешний пульт центрального наблюдения (ПЦН), предназначенный для охраны объектов через широкополосные каналы передачи информации: *Internet*, GSM.

В разделе использованы следующие сокращения:

УОО – устройство охранное объектовое,

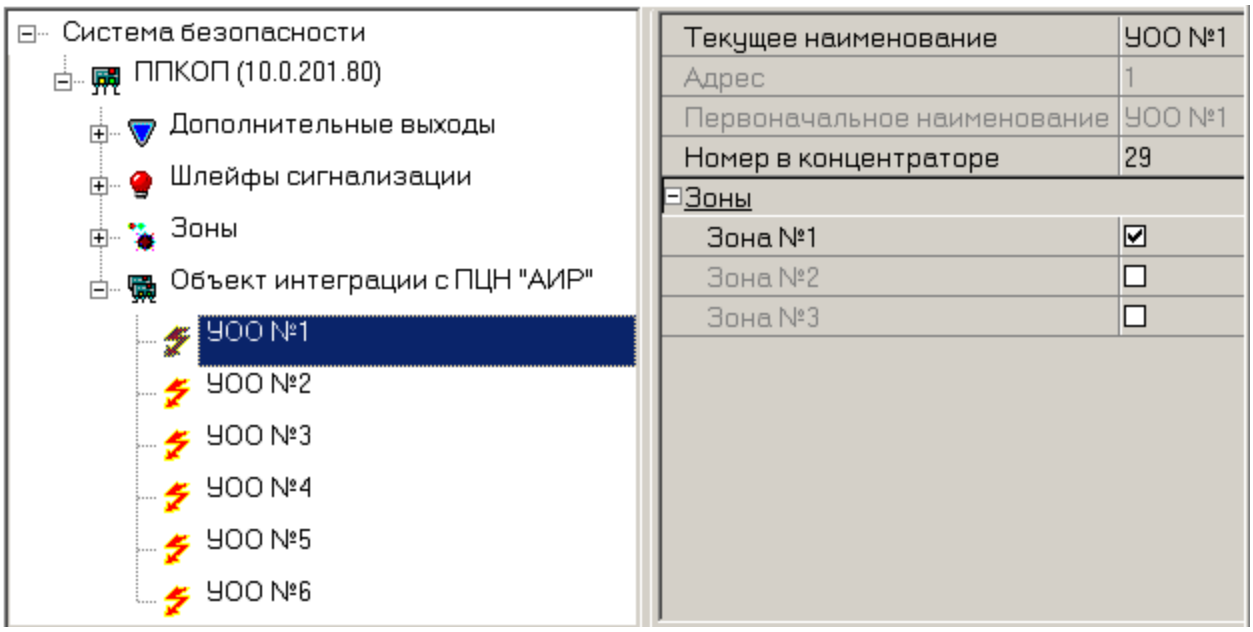
КТС – кнопка тревожной сигнализации.

Для включения интеграции следует установить флажок у параметра ППКОП **Включить интеграцию с ПЦН «АИР»**. После этого для ППКОП будет добавлена группа ресурсов **Объект интеграции с ПЦН "АИР"** содержащая шестью ресурсов УОО.



Для группы ресурсов **Объект интеграции с ПЦН "АИР** доступны следующие параметры:

- **Сетевые параметры концентратора**
  - **IP-адрес**
  - **Маска подсети**

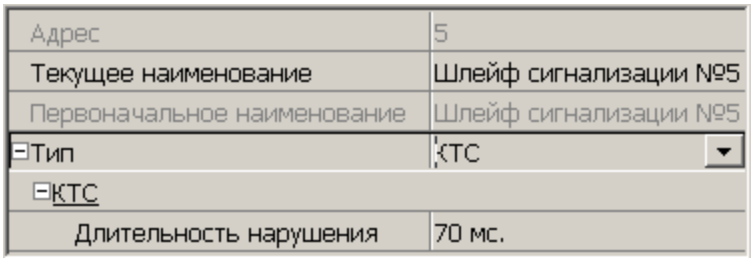


Для каждого УОО доступны следующие параметры:

- **Номер в концентраторе** – номер УОО в адресном пространстве концентратора.
- **Зоны** – список зон **КТС** УОО. При этом каждая зона КТС может входить только в одно УОО.

Тип шлейфа «КТС»

Доступны следующие параметры:

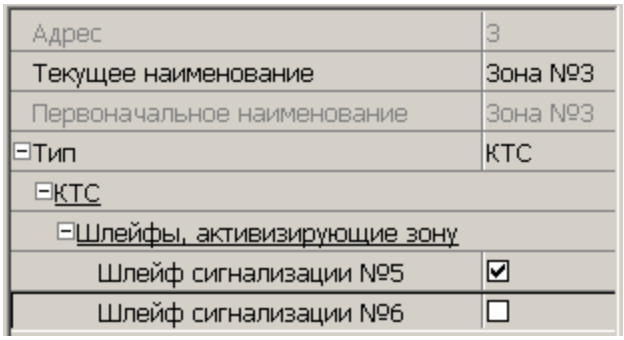


Текущее наименование.Поле ввода позволяет ввести произвольное описательное название ресурса.

Длительность нарушения – параметр, определяет время интегрирования ШС.

Тип зоны «КТС»

Доступны следующие параметры:



Шлейфы, активизирующие зону. Параметр позволяет отметить флажками ШС, которые будут входить в зону КТС и состояние которых будет отслеживаться контроллером при переводе зоны КТС в режим *«Охрана»*. В ОЗ могут входить ШС, для которых выбран **Тип: КТС**. При этом каждый ШС может входить только в одну ОЗ.

3.13.14 Приборы ИСО «Орион»

Для приборов ИСО «Орион» доступны следующие общие параметры:

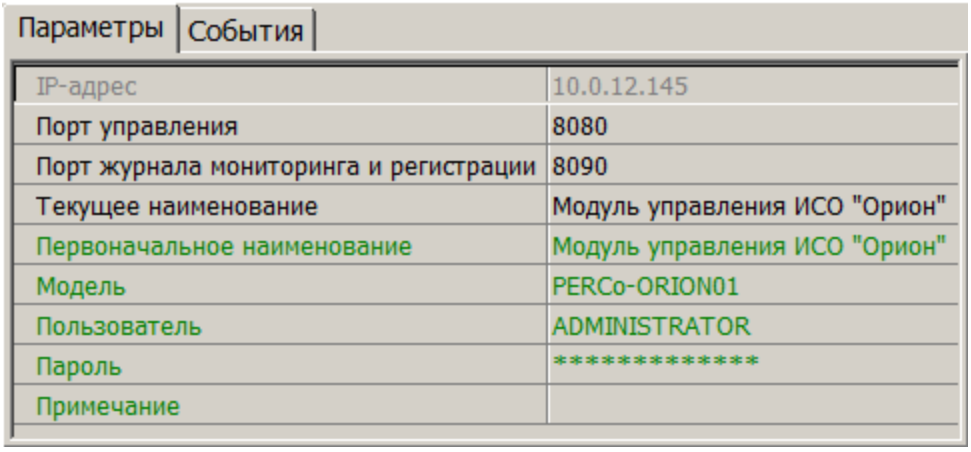
Текущее наименование – описательное название прибора, которое может быть изменено пользователем.

Первоначальное наименование – наименование прибора в системе по умолчанию.

Модель – модель прибора.

Примечание – дополнительная информация о приборе, которая может быть добавлена пользователем.

Модуль управления ИСО "Орион"



IP-адрес – IP–адрес ПК, на котором установлен ***«Модуль управления ИСО Орион»*** и запущен XML-RPC-сервер.

Примечание:

Для подключения к XML-RPC-серверу параметры **Порт управления**, **Пользователь**, **Пароль** должны совпадать с указаны в соответствующих параметрах `XMLIPPORT`, `LOGIN`, `PASSWORD` раздела реестра: `"HKEY_LOCAL_MACHINE\SOFTWARE\BOLID\ORION_PRO\ORICORE"` ПК, на котором установлен ***«Модуль управления ИСО Орион»***.

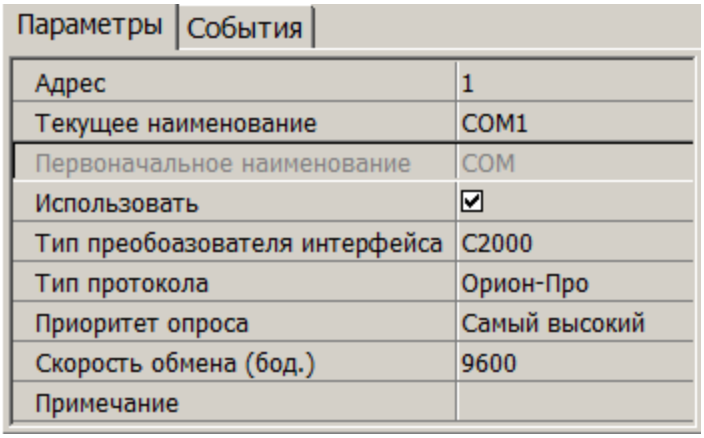
Порт управления (по умолчанию 8080) – номер IP–порта XML-RPC-сервера для обмена данными с сервером системы.

Порт журнала мониторинга и регистрации (по умолчанию 8090) – номер IP–порта сервера системы для приема событий, регистрируемых приборами ИСО «Орион» от XML-RPC-сервера.

Пользователь – имя пользователя для доступа к XML-RPC-серверу.

Пароль – пароль для доступа к XML-RPC-серверу.

COM1, COM2, ...



Адрес – номер COM-порта ПК, к которому физически подключено оборудование ИСО «Орион».

Использовать – при снятии флажка будет остановлен обмен данными с устройствами ИСО «Орион», входящими в группу ресурсов.

Тип преобразователя интерфейса – параметр позволяет указать тип преобразователя интерфейса, соответствующий установленному оборудованию:

- **ПИ-ГР** – значение необходимо выбрать в случае, если пульт *С2000М* (*С2000*), работающий в режиме ПИ, подключен по COM-порту. В этом режиме ядро опроса будет посылать дополнительные команды управления приемом-передачей.
- **С2000-ПИ** – значение необходимо выбрать в случае подключения оборудования ИСО «Орион» через *С2000* USB-конвертер.
- **С2000** – значение необходимо выбрать в случае подключения через пульт *С2000М* (*С2000*) в режиме компьютер.

Примечание:

Для параметра Тип преобразователя интерфейса:

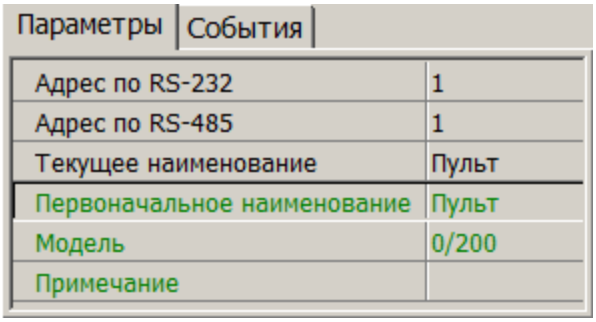
- Значения **С2000-ПИ** и **С2000** выбираются при использовании преобразователей интерфейсов с автоматическим переключением приема/передачи сигнала. В этом случае дополнительные команды не генерируются.
- При подключении *С2000М* (*С2000*) через *С2000USB*, необходимо выбрать пункт **ПИ-ГР** или **С2000**, в зависимости от настроек.

Тип протокола (*Орион-Про*/ *Орион*) – протокол обмена данными между устройствами ИСО «Орион» и XML-RPC-сервером по COM-порту.

Приоритет опроса – параметр позволяет выбрать значение приоритета опроса модулем ИСО «Орион» оборудования, которое подключено к этому порту.

Скорость обмена (бод.) (*9600*/ *19200*) – скорость обменна данными между устройствами ИСО «Орион» и XML-RPC-сервером

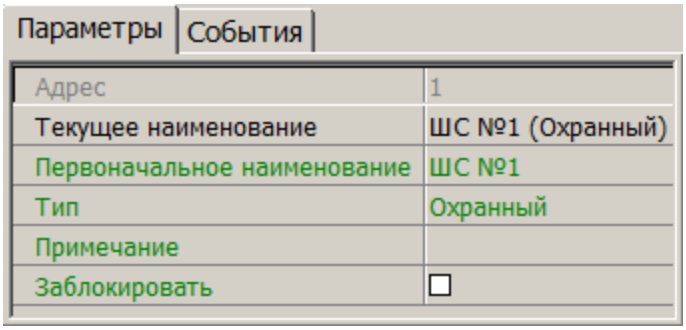
Пульт



Адрес по RS-232 – адрес прибора при передаче данных по интерфейсу RS-232.

Адрес по RS-485 – адрес прибора при передаче данных по интерфейсу RS-485.

ШС



Заблокировать – при установке флажка возможность снятия ШС с охраны/контроля будет заблокирована.

Примечание:

Описание режима работы ШС в зависимости от выбранного типа конфигурации и используемого прибора приводится в эксплуатационной документации конкретного прибора. Документация доступна на сайте производителя: www.bolid.ru.

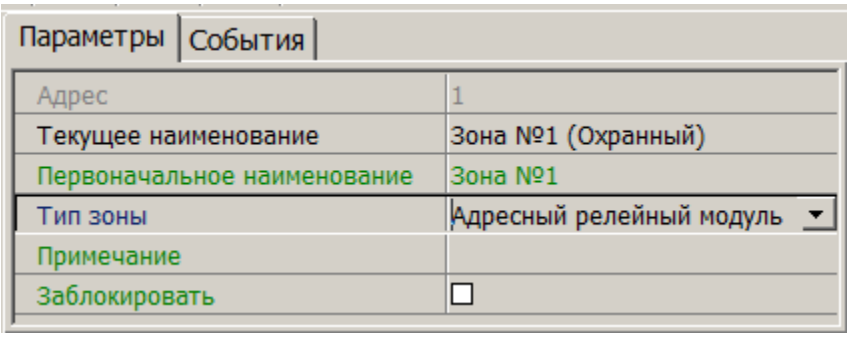
Тип – раскрывающийся список позволяет выбрать вариант конфигурации ШС в зависимости от типа подключенного оборудования:

- **Охранный**
- **Пожарный**
- **Ademco (Приемник)**
- **Ademco (Радиоповторитель)**
- **Автоматическое управление второго рабочего насоса**
- **Автоматическое управление жокей-насоса**
- **Автоматическое управление первого рабочего насоса**
- **Автоматическое управление резервного насоса**
- **Агрегат 1**
- **Агрегат 2**
- **Агрегат 3**
- **Агрегат 4**
- **Адресно-аналоговый дымовой**
- **Адресно-аналоговый тепловой**
- **Влагоизмерительный**
- **Входной**
- **Выход Р1**
- **Выход Р2**
- **Выход Р3**
- **Выход Р4**
- **Выходное напряжение**
- **Выходной ток**
- **Давление**
- **Давление в системе**
- **ДД запуска**
- **Дистанционный пуск**
- **Дистанционный пуск Потока**
- **Дренажный приямок**
- **Дренчерная завеса**
- **Закрытие электрозадвижки**
- **Запуск второго рабочего насоса**
- **Запуск жокей-насоса**
- **Запуск первого рабочего насоса**
- **Запуск резервного насоса**
- **Зоны УОП**
- **Контроль состояния прибора**
- **Контроль ШС**
- **Масса**
- **Основной ввод АВР**
- **Основной резервуар**
- **Открытие электрозадвижки**
- **Питание второго рабочего насоса**
- **Питание жокей-насоса**
- **Питание первого рабочего насоса**
- **Питание резервного насоса**
- **Питание электрозадвижки**
- **Пожарный адресно-пороговый**
- **Проверка 220В**
- **Проверка АКБ**
- **Проверка ЗУ**
- **Программируемый технологический**
- **Режим автоматического запуска**
- **Режим запуска**
- **Режим прибора**
- **Резервный ввод АВР**
- **Резервный резервуар**
- **Ручной пуск**
- **Ручной пуск (АСПТ)**
- **Ручной пуск (Поток)**
- **Ручной пуск (Рупор)**
- **СДУ**
- **Состояние КЦ1**
- **Состояние КЦ10**
- **Состояние КЦ11**
- **Состояние КЦ12**
- **Состояние КЦ13**
- **Состояние КЦ14**
- **Состояние КЦ15**
- **Состояние КЦ16**
- **Состояние КЦ17**
- **Состояние КЦ18**
- **Состояние КЦ2**
- **Состояние КЦ3**

- **Источник 26 В**
- **Источник ОП**
- **Источник питания 27 В**
- **Источник РП**
- **Контроль дистанционного запуска РО (речевого оповещения)**
- **Контроль ЗУ**
- **Контроль источника ОП (220В)**
- **Контроль источника РП (АКБ)**
- **Контроль неисправности АУП («М\Д»)**
- **Состояние КЦ4**
- **Состояние КЦ5**
- **Состояние КЦ6**
- **Состояние КЦ7**
- **Состояние КЦ8**
- **Состояние КЦ9**
- **Состояние устройства**
- **Технологический**
- **Тревожная кнопка**
- **Цепь ДС дверей**

Зона

Ресурс доступен для категории приборов **Адресно-аналоговые подсистемы (КДЛ)**.

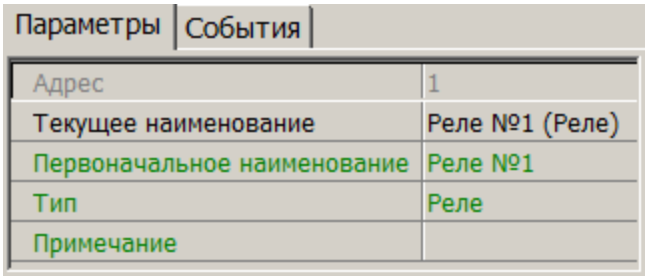


Тип зоны – раскрывающийся список позволяет выбрать тип зоны:

- **Шлейф** (варианты конфигурации ШС указаны выше)
- **Адресный релейный модуль**

Заблокировать– При установке флажка возможность снятия ШС или адресного релейного модуля с охраны/ контроля будет заблокирована.

Реле



Примечание:

Описание режима работы реле в зависимости от выбранного типа конфигурации и используемого прибора приводится в эксплуатационной документации конкретного прибора. Документация доступна на сайте производителя: www.bolid.ru.

Тип – раскрывающийся список позволяет выбрать вариант конфигурации реле в зависимости от типа подключенного оборудования:

- **Адресный релейный модуль**
- **Выход КПБ (АСПТ)**
- **ЗО (Сирена)**
- **Контролируемый выход**

- **Пуск 1**
- **Пуск 2**
- **Пуск 3**
- **Пуск 4**
- **Пусковая цепь**
- **Реле**
- **Речевое оповещение**
- **СО1 (УХОДИ)**
- **СО2 (НЕ ВХОДИ)**
- **СО3 (Автоматика отключена)**

3.13.15 Интеграция с контроллерами «Suprema»

В системе предусмотрена возможность проведения интеграции с биометрическими контроллерами ***«BioEntry Plus»*** и ***«BioEntry W2»***, разработанными компанией **«Suprema»**. Биометрические контроллеры доступа имеют возможность подключения по сети Ethernet с использованием стека протоколов TCP/IP. Биометрические технологии дополняют стандартный метод верификации, основанный на использовании бесконтактных карт и позволяют усилить контроль доступа на территорию предприятия при проходе сотрудников и посетителей с целью предотвращения случаев прохода по чужой/поддельной бесконтактной карте доступа.

Совместно с контроллерами могут использоваться настольные биометрические сканеры линейки ***«BioMini»***, подключаемые по интерфейсу USB.

Для настройки параметров работы в СКУД доступны следующие устройства **«Suprema»**:

Контроллер BioEntry Plus;

КонтроллерBioEntry W2;

Замок;

Биометрическийсчитыватель.

Для устройств, разработанных компанией **«Suprema»**, доступны следующие общие параметры:

Текущее наименование – описательное название прибора, которое может быть изменено пользователем;

Первоначальное наименование – наименование прибора в системе по умолчанию.

Контроллер BioEntry Plus

Параметры | События

IP-адрес	172.17.108.208
Маска подсети	255.255.0.0
Шлюз	172.17.0.74
Макс. кол-во сотрудников/посетителей	5000
Макс. кол-во отпечатков пальцев	10000
Текущее наименование	Контроллер BioEntry Plus
Порт	51211
Первоначальное наименование	Контроллер BioEntry Plus
Модель	BioEntry Plus
Серийный номер	539301863
Уровень безопасности	Нормальный
Таймаут сканирования пальца	10 сек.
Таймаут верификации пальцем	5 сек.
Таймаут поиска отпечатка	5 сек.
Чувствительность сканера	3
Алгоритм поиска отпечатков	Автоматический
Режим авторизации	Частный
Схема входных портов	Кнопка выхода - порт 0; Датчик прохода - порт 1
Параметры кнопки выхода	
Нормальное состояние	Нормально открыто
Параметры датчика прохода	
Нормальное состояние	Нормально открыто
Порядок байт идентификатора карты	От старшего байта к младшему
Настройки Wiegand	
Режим	Вход
Коррекция времени относительно времени сервера системы	0 час.

IP-адрес.

Маска подсети.

Шлюз.

Макс. кол-во сотрудников/посетителей – определяет максимально допустимое количество сотрудников/посетителей, информация о которых может храниться в контроллере.

Макс. кол-во отпечатков пальцев – определяет максимально допустимое количество отпечатков пальцев, информация о которых может храниться в контроллере.

Порт – порт контроллера, который необходимо использовать для подключения.

Модель – отображает официальное наименование модели устройства.

Серийный номер – серийный номер устройства.

Уровень безопасности – уровень безопасности, устанавливаемый при использовании верификации по отпечатку пальца:

- Нормальный,
- Безопасный,
- Наиболее безопасный.

Чем выше установленный уровень безопасности – тем больше характерных точек будет считываться с отсканированного изображения папиллярных узоров отпечатка пальца, а значит – снизится вероятность ложного срабатывания (прохода по чужому/поддельному отпечатку). Однако, чем выше установленный уровень безопасности, тем выше вероятность отказа при сканировании отпечатков. Отказы могут возникать вследствие возникновения ошибок сканирования, связанных с более высоким влиянием на процедуру сканирования влажности и температуры воздуха, загрязнённости сканируемой поверхности пальцев и т.д. В этом случае для успешной верификации потребуется повторно пройти процедуру сканирования отпечатков.

Таймаут сканирования пальца – время, которое выделяется системой на поднесение одного пальца при вводе отпечатков. Параметр может быть задан в интервале от 3 до 20 секунд.

Таймаут верификации пальцем (используется в режиме доступа **карта и палец**) – интервал времени, в течение которого ожидается поднесение пальца для сканирования отпечатков, при этом отсчёт времени интервала начинается после того, как была предъявлена считывателю карта доступа. Параметр может быть задан в интервале от 1 до 20 секунд.

Таймаут поиска отпечатков – время поиска отпечатка в памяти контроллера. Если за отведенное время отпечаток не будет найден, то аутентификация будет отклонена. Параметр может быть задан в интервале от 1 до 20 секунд.

Чувствительность сканера – определяет чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности – обеспечивается высокое качество и скорость сканирования, при низком заданном уровне чувствительности – уменьшается влияние факторов внешней среды (температуры и влажности воздуха, освещённости помещения, чистоты сканируемой поверхности подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию. Понижение заданного уровня чувствительности сканера осуществляется при необходимости в зависимости от условий эксплуатации. Параметр может быть задан в интервале от 1 до 7, где значение 1 – соответствует самой низкой чувствительности, а значение 7 – самой высокой.

Алгоритм поиска отпечатков – позволяет выбрать алгоритм поиска отпечатков пальца. Выбор алгоритма влияет на скорость верификации по отпечатку пальца:

- **Автоматический (рекомендован производителем),**
- **Нормальный,**
- **Быстрый,**
- **Очень быстрый.**

Выбор **алгоритма поиска отпечатков** определяет тот объём памяти контроллера, который будет выделяться для поиска совпадения отсканированного отпечатка с отпечатком в базе данных. Если в базе данных контроллера большое количество разных отпечатков, то для быстрого поиска совпадений потребуется больший объём памяти контроллера. Однако, выделение большего объёма памяти контроллера для поиска совпадений может замедлить остальные параллельно происходящие процессы поиска совпадений, например, если к контроллеру подключены несколько считывателей, на которых в этот же момент времени происходит верификация по отпечаткам пальцев.

Режим авторизации – параметр определяет режим авторизации:

- **частный режим доступа** – в этом случае параметры доступа устанавливаются для отдельного сотрудника/посетителя в рамках СКУД;
- **общий режим доступа** – в этом случае параметры доступа устанавливаются в рамках биометрического контроллера и будут применяться для всех пользователей, взаимодействующих ним.

Режим доступа – определяет режим доступа при общем режиме авторизации (отображается, только если режим авторизации выставлен как **«Общий»**):

- **Палец** – для верификации требуется пройти процедуру сканирования отпечатка пальца;
- **Карта** – для верификации требуется предъявить считывателю карту доступа;
- **Карта и палец** – для верификации требуется предъявить считывателю карту доступа, после чего пройти процедуру сканирования отпечатка пальца;
- **Карта или палец** – для верификации требуется предъявить считывателю карту доступа или пройти процедуру сканирования отпечатка пальца.

Примечание:

Параметр **Режим доступа** доступен для редактирования в случае, если выбран **Общий** режим авторизации.

Схема входных портов – позволяет назначить на входные порты **«Кнопку выхода»** и **«Датчик прохода» («Датчик открытия\закрытия двери»)**:

- **Нет;**
- **Кнопка выхода – порт 0;**
- **Кнопка выхода – порт 1;**
- **Датчик прохода – порт 0;**
- **Датчик прохода – порт 1;**
- **Кнопка выхода – порт 0; Датчик прохода – порт 1;**
- **Кнопка выхода – порт 1; Датчик прохода – порт 0.**

Примечание:

Категорически не рекомендуется подключать датчик прохода и кнопку выхода на один и тот же вход контроллера.

Параметры кнопки выхода (Нормальное состояние) – нормальное состояние входного порта, на который назначена **«Кнопка выхода»**:

- **Нормально открыто,**
- **Нормально закрыто.**

Примечание:

Нормальным состоянием кнопки выхода считается то состояние, в котором находится кнопка при заблокированной двери. Соответственно, если конструктивно предусмотрено, что при нажатии кнопки выхода размыкается контакт реле и дверь разблокируется (т.е. – переходит из нормального состояния в состояние разблокировки), то необходимо из раскрывающегося списка выбрать **Нормально закрыто**.

Параметры датчика прохода (Нормальное состояние) – нормальное состояние входного порта, на который назначен **«Датчик прохода»**:

- **Нормально открыто,**
- **Нормально закрыто.**

Порядок байтов идентификатора карты – определяет порядок следования байтов идентификатора карты:

- **От старшего байта к младшему,**
- **От младшего байта к старшему.**

Примечание:

Нормальным состоянием датчика прохода (геркона) считается то состояние, в котором находится датчик при закрытой двери. Соответственно, если датчик прохода конструктивно расположен так, что при закрытой двери датчик нормально замкнут, то необходимо из раскрывающегося списка для датчика прохода выбрать **Нормально закрыто**.

- **Настройки Wiegand (Режим)** – позволяет задать режим работы интерфейса *Wiegand* контроллера ***Suprema***:
  - **Вход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как вход. В этом режиме контроллер ***Suprema*** работает как обычный контроллер доступа, ожидая поступления данных по интерфейсу *Wiegand*;
  - **Выход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как выход. В этом режиме контроллер ***Suprema*** работает совместно с контроллером ***PERCo*** в составе СКУД (может производить аутентификацию и управление подключённым по интерфейсу *Wiegand* оборудованием (замком и т.д.)).

- **Использовать аутентификацию** – при установке флажка контроллером ***Suprema*** при предъявлении карты/пальца будет производиться предварительная аутентификация. В случае успешной предварительной аутентификации данные будут переданы в контроллер ***PERCo*** для повторной аутентификации (загорится зелёная индикация). В случае ошибки предварительной аутентификации данные в контроллер ***PERCo*** передаваться не будут – необходимо провести повторную успешную аутентификацию. Если флажок не выставлен, то процедура аутентификации будет производится только контроллером ***PERCo***.
- **Управление замком** – если флажок не установлен (по умолчанию), то управление замком осуществляется контроллером компании ***PERCo***. Если флажок установлен, то контроллер ***Suprema*** получает возможность управлять замком. Обязательным условием передачи функций управления замком контроллеру ***Suprema*** является установка флажка **Использовать аутентификацию**.

Примечание:

Параметры **Использовать аутентификацию** и **Управление замком** доступны для редактирования в случае, если выбрано значение **Выход** в **Настройки Wiegand (Режим).**

Коррекция времени относительно времени сервера системы – параметр позволяет задать коррекцию времени (параметр позволяет согласовать работу, если контроллер и сервер системы находятся в разных часовых поясах). Значение коррекции может быть задано в интервале от минус 12 до плюс 14 часов.

Контроллер BioEntry W2

Параметры | События

IP-адрес	172.17.106.206
Маска подсети	255.255.0.0
Шлюз	172.17.0.54
Макс. кол-во сотрудников/посетителей	100000
Макс. кол-во отпечатков пальцев	200000
Текущее наименование	Контроллер BioEntry W2
Порт	51211
Первоначальное наименование	Контроллер BioEntry W2
Модель	BioEntry W2
Серийный номер	544108028
Уровень безопасности	Нормальный
Таймаут сканирования пальца	10 сек.
Таймаут верификации пальцем	5 сек.
Таймаут поиска отпечатка	5 сек.
Чувствительность сканера	3
Алгоритм поиска отпечатков	Автоматический
Режим датчика	Включается автоматически
⊟Режим авторизации	Общий
⊟**Общий**	
Режим доступа	Палец
Схема входных портов	Кнопка выхода - порт 0; Датчик прохода - порт 1
⊟**Параметры кнопки выхода**	
Нормальное состояние	Нормально открыто
⊟**Параметры датчика прохода**	
Нормальное состояние	Нормально открыто
Порядок байт идентификатора карты	От старшего байта к младшему
⊟**Настройки Wiegand**	
⊟Режим	Выход
⊟**Выход**	
Использовать аутентификацию	☑
Управление замком	☐
Коррекция времени относительно времени сервера системы	0 час.

IP-адрес.

Маска подсети.

Шлюз.

Макс. кол-во сотрудников/посетителей – определяет максимально допустимое количество сотрудников/посетителей, информация о которых может храниться в контроллере.

Макс. кол-во отпечатков пальцев – определяет максимально допустимое количество отпечатков пальцев, информация о которых может храниться в контроллере.

Порт – порт контроллера, который необходимо использовать для подключения.

Модель – отображает официальное наименование модели устройства.

Серийный номер – серийный номер устройства.

Уровень безопасности – уровень безопасности, устанавливаемый при использовании верификации по отпечатку пальца:

- **Нормальный,**
- **Безопасный,**
- **Наиболее безопасный.**

Чем выше установленный уровень безопасности – тем больше характерных точек будет считываться с отсканированного изображения папиллярных узоров при прикладывании пальца, а значит – снизится вероятность ложного срабатывания (прохода по чужому/поддельному отпечатку). Однако, чем выше установленный уровень безопасности, тем выше вероятность отказа при сканировании отпечатков. Отказы могут возникать вследствие возникновения ошибок сканирования, связанных с более высоким влиянием на процедуру сканирования влажности и температуры воздуха, загрязнённости сканируемой поверхности пальцев и т.д. В этом случае для успешной верификации потребуется повторно пройти процедуру сканирования отпечатков.

Таймаут сканирования пальца – время, которое выделяется системой на поднесение одного пальца при вводе отпечатков. Параметр может быть задан в интервале от 3 до 20 секунд.

Таймаут верификации пальцем (используется в режиме доступа ***карта и палец***) – интервал времени, в течение которого ожидается поднесение пальца для сканирования отпечатков, при этом отсчёт времени интервала начинается после того, как была предъявлена считывателю карта доступа**.** Параметр может быть задан в интервале от 1 до 20 секунд.

Таймаут поиска отпечатков – время поиска отпечатка в памяти контроллера. Если за отведенное время отпечаток не будет найден, то аутентификация будет отклонена. Параметр может быть задан в интервале от 1 до 20 секунд.

Чувствительность сканера – определяет чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности – обеспечивается высокое качество и скорость сканирования, при низком заданном уровне чувствительности – уменьшается влияние факторов внешней среды (температуры и влажности воздуха, освещённости помещения, чистоты сканируемой поверхности подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию. Понижение заданного уровня чувствительности сканера осуществляется при необходимости в зависимости от условий эксплуатации. Параметр может быть задан в интервале от 1 до 7, где значение "1" – соответствует самой низкой чувствительности, а значение "7" – самой высокой.

Алгоритм поиска отпечатков – выбор алгоритма влияет на скорость верификации по отпечатку пальца:

- **Автоматический (рекомендован производителем),**
- **Нормальный,**
- **Быстрый,**
- **Очень быстрый.**

Выбор **алгоритма поиска отпечатков** определяет тот объём памяти контроллера, который будет выделяться для поиска совпадения отсканированного отпечатка с отпечатком в базе данных. Если в базе данных контроллера большое количество разных отпечатков, то для быстрого поиска совпадений потребуется больший объём памяти контроллера. Однако, выделение большего объёма памяти контроллера для поиска совпадений может замедлить остальные параллельно происходящие процессы поиска совпадений, например, если к контроллеру подключены несколько считывателей, на которых в этот же момент времени происходит верификация по отпечаткам пальцев.

Режим датчика – параметр определяет режим работы считывающего датчика, либо он работает всегда, либо включается автоматически, если обнаруживает палец;

Режим авторизации – параметр определяет режим авторизации:

- **частный режим доступа** – в этом случае параметры доступа устанавливаются для отдельного сотрудника/посетителя в рамках СКУД;
- **общий режим доступа** – в этом случае параметры доступа устанавливаются в рамках биометрического контроллера и будут применяться для всех пользователей, взаимодействующих ним.

Режим доступа – определяет режим доступа при общем режиме авторизации (отображается, только если режим авторизации выставлен как **«Общий»**):

- **Палец** – для верификации требуется пройти процедуру сканирования отпечатка пальца;
- **Карта** – для верификации требуется предъявить считывателю карту доступа;
- **Карта и палец** – для верификации требуется предъявить считывателю карту доступа, после чего пройти процедуру сканирования отпечатка пальца;
- **Карта или палец** – для верификации требуется предъявить считывателю карту доступа или пройти процедуру сканирования отпечатка пальца.

Примечание:

Параметр **Режим доступа** доступен для редактирования в случае, если выбран **Общий** режим авторизации.

Схема входных портов – позволяет назначить на входные порты **«Кнопку выхода»** и **«Датчик прохода» («Датчик открытия\закрытия двери»)**:

- **Нет;**
- **Кнопка выхода – порт 0;**
- **Кнопка выхода – порт 1;**
- **Датчик прохода – порт 0;**
- **Датчик прохода – порт 1;**
- **Кнопка выхода – порт 0; Датчик прохода – порт 1;**
- **Кнопка выхода – порт 1; Датчик прохода – порт 0.**

Примечание:

Категорически не рекомендуется подключать датчик прохода и кнопку выхода на один и тот же вход контроллера.

Параметры кнопки выхода (Нормальное состояние) – нормальное состояние входного порта, на который назначена **«Кнопка выхода»**:

- **Нормально открыто,**
- **Нормально закрыто.**

Примечание:

Нормальным состоянием кнопки выхода считается то состояние, в котором находится кнопка при заблокированной двери. Соответственно, если конструктивно предусмотрено, что при нажатии кнопки выхода размыкается контакт реле и дверь разблокируется (т.е. – переходит из нормального состояния в состояние разблокировки), то необходимо из раскрывающегося списка выбрать **Нормально закрыто**.

Параметры датчика прохода (Нормальное состояние) – нормальное состояние входного порта, на который назначен **«Датчик прохода»**:

- **Нормально открыто,**
- **Нормально закрыто.**

Порядок байтов идентификатора карты – определяет порядок следования байтов идентификатора карты:

- **От старшего байта к младшему,**
- **От младшего байта к старшему.**

Примечание:

Нормальным состоянием датчика прохода (геркона) считается то состояние, в котором находится датчик при закрытой двери. Соответственно, если датчик прохода конструктивно расположен так, что при закрытой двери датчик нормально замкнут, то необходимо из раскрывающегося списка для датчика прохода выбрать **Нормально закрыто**.

- **Настройки Wiegand (Режим)** – позволяет задать режим работы интерфейса *Wiegand* контроллера ***Suprema***:
  - **Вход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как вход. В этом режиме контроллер ***Suprema*** работает как обычный контроллер доступа, ожидая поступления данных по интерфейсу *Wiegand*;
  - **Выход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как выход. В этом режиме контроллер ***Suprema*** работает совместно с контроллером ***PERCo*** в составе СКУД (может производить аутентификацию и управление подключённым по интерфейсу *Wiegand* оборудованием (замком и т.д.)).

- **Использовать аутентификацию** – при установке флажка контроллером ***Suprema*** при предъявлении карты/пальца будет производиться предварительная аутентификация. В случае успешной предварительной аутентификации данные будут переданы в контроллер ***PERCo*** для повторной аутентификации (загорится зелёная индикация). В случае ошибки предварительной аутентификации данные в контроллер ***PERCo*** передаваться не будут – необходимо провести повторную успешную аутентификацию. Если флажок не выставлен, то процедура аутентификации будет производится только контроллером ***PERCo***.

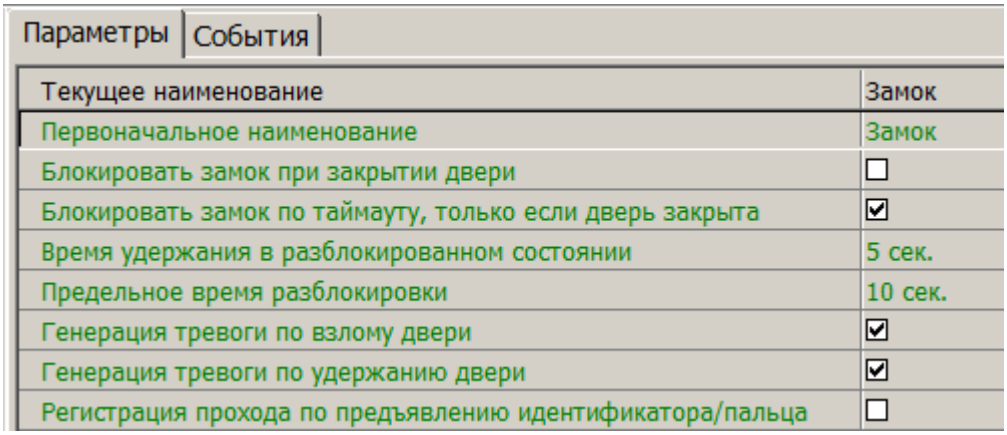
- **Управление замком** – если флажок не установлен (по умолчанию), то управление замком осуществляется контроллером компании ***PERCo***. Если флажок установлен, то контроллер ***Suprema*** получает возможность управлять замком. Обязательным условием передачи функций управления замком контроллеру ***Suprema*** является установка флажка **Использовать аутентификацию**.

Примечание:

Параметры **Использовать аутентификацию** и **Управление замком** доступны для редактирования в случае, если выбрано значение **Выход** в **Настройки Wiegand (Режим).**

Коррекция времени относительно времени сервера системы – параметр позволяет задать коррекцию времени (параметр позволяет согласовать работу, если контроллер и сервер системы находятся в разных часовых поясах). Значение коррекции может быть задано в интервале от минус 12 до плюс 14 часов.

Замок



Блокировать замок при закрытии двери – при установке флажка дверь будет заблокирована сразу после закрытия.

Блокировать замок по таймауту, только если дверь закрыта – при установке флажка замок будет заблокирован по истечении **Времени удержания в разблокированном состоянии** только после закрытия двери. Если флажок не установлен – замок будет заблокирован, даже если дверь открыта.

Время удержания в разблокированном состоянии – устанавливает время, которое должно пройти от разблокировки замка до его блокировки после успешной аутентификации. За это время необходимо открыть дверь – иначе замок заблокируется. Параметр может быть задан в интервале от 1 до 30 секунд или от 1 до 15 минут.

Предельное время разблокировки – максимальное разрешенное время для нахождения двери в открытом состоянии. Если дверь не закрыть за отведенное время – будет сгенерирован сигнал тревоги. Параметр может быть задан в интервале от 1 до 30 секунд или от 1 до 15 минут.

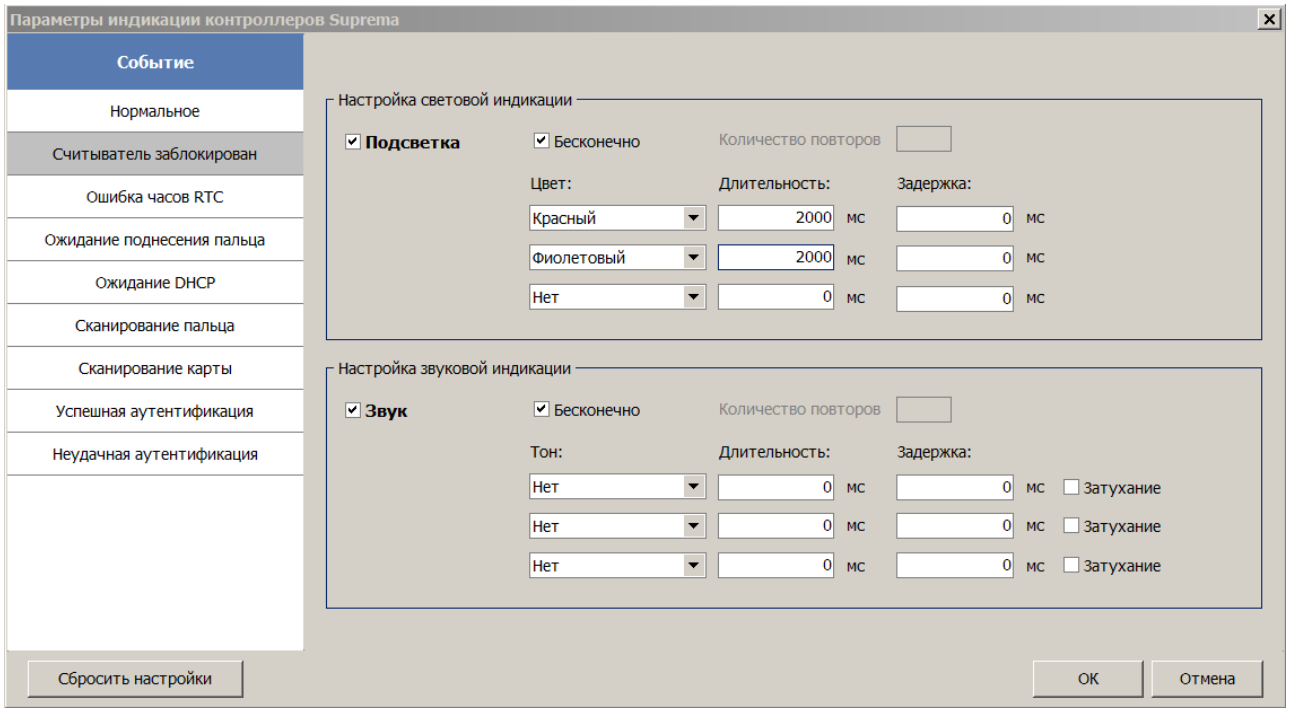
Генерация тревоги по взлому двери – при установке флажка сигнал тревоги будет автоматически сгенерирован в случае, если был зафиксирован факт открытия двери без команды на открытие от контроллера.

Генерация тревоги по удержанию двери – при установке флажка сигнал тревоги будет автоматически сгенерирован в случае, если истекло Предельное время разблокировки и дверь не была закрыта.

Регистрация прохода по предъявлению идентификатора/ пальца – если флажок установлен, то событие совершения прохода регистрируется сразу после поднесения карты доступа/сканирования пальца без ожидания сигнала от датчика прохода. Если флажок не выставлен, то событие совершения прохода регистрируется после поднесения карты доступа/ сканирования пальца и срабатывания датчика прохода.

Параметры индикации контроллеров «Suprema»

Для того, чтобы настроить параметры индикации биометрических контроллеров ***Suprema***, необходимо перейти в раздел ***«Конфигуратор»*** и выбрать ***Биометрическая система SUPREMA.*** На вкладке **Параметры** для параметра **Параметры индикации** необходимо с помощью кнопки ... вызвать диалоговое окно **Параметры индикации контроллеров Suprema:**



В данном окне предоставляется возможность настроить цветовую индикацию и звуковые сигналы контроллера **Suprema** для следующего списка событий:

- **Нормальное** – событие возникает в случае нормальной работы контроллера (режим работы "Контроль");
- **Считыватель заблокирован** – событие возникает в случае блокировки контроллера (режим работы "Закрыто");

- **Ошибка часов RTC (Real Time Clock)** – событие возникает в случае несовпадения внутреннего времени контроллера со временем сети;
- **Ожидание поднесения пальца** – событие возникает в случае, если был выбран тип прав доступа «Доступ по карте и пальцу» после предъявления карты;
- **Ожидание DHCP (Dynamic Host Configuration Protocol)** – событие возникает в случае ожидания получения IP-адреса от DHCP-сервера;
- **Сканирование пальца** – событие возникает в случае добавления отпечатков пальцев, как идентификатора сотруднику или посетителю (если контроллер выбран как устройство для получения идентификатора);
- **Сканирование карты** – событие возникает в случае добавления карты доступа, как идентификатора сотруднику или посетителю (если контроллер выбран как устройство для получения идентификатора);
- **Успешная аутентификация** – событие возникает в случае успешной идентификации;
- **Неудачная аутентификация** – событие возникает в случае ошибки идентификации.

Область **Настройка световой индикации** – отображает параметры настройки цветовой индикации контроллера для выбранного события из списка событий:

- **Подсветка** – при установке флажка для индикации выбранного события будет использоваться подсветка;
- **Бесконечно** – при установке флажка подсветка будет производиться бесконечно;
- **Количество повторов** – позволяет задать количество повторений подсветки.

Примечание:

Параметры **Бесконечно / Количество повторов** являются взаимоисключающими.

- **Цвет** – параметр позволяет выбрать цвета индикации (не более трёх);
- **Длительность** – параметр позволяет задать длительность свечения индикации тем или иным цветом;
- **Задержка** – параметр позволяет задать задержку перед началом свечения тем или иным цветом от начала цикла индикации.

Область **Настройка звуковой индикации** – отображает параметры настройки звуковых сигналов контроллера для выбранного события из списка событий:

- **Звук** – при установке флажка для индикации выбранного события будет использоваться звук;
- **Бесконечно** – при установке флажка звук будет воспроизводиться бесконечно;
- **Количество повторов** – позволяет задать количество повторений звучания.

Примечание:

Параметры **Бесконечно / Количество повторов** являются взаимоисключающими.

- **Тон** – параметр позволяет выбрать тон звучания;
- **Длительность** – параметр позволяет задать длительность звучания индикации тем или иным тоном;

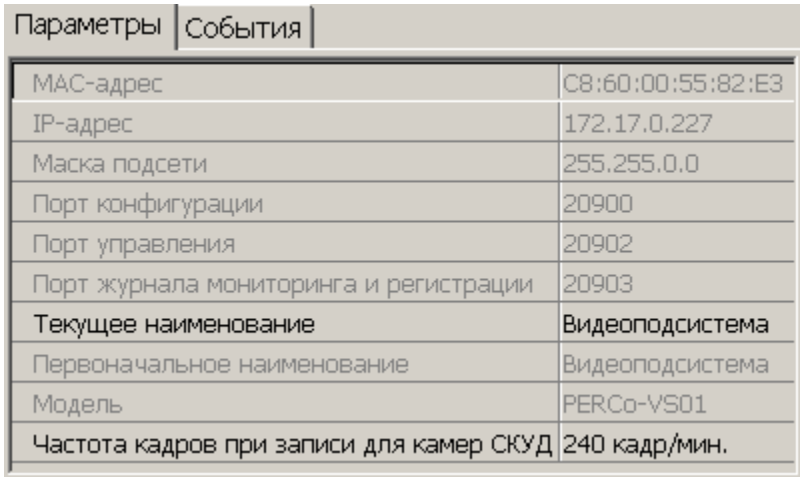
- **Задержка** – параметр позволяет задать задержку перед началом звучания индикации тем или иным тоном от начала цикла индикации.

В случае, если необходимо сбросить настройки индикации до стандартных значений, нажмите на кнопку **Сбросить настройки**.

Для того, чтобы сохранить изменения индикации, нажмите на кнопку **ОК**, в противном случае на кнопку **Отмена**.

3.13.16 Видеоподсистема

Для настройки параметров видеоподсистемы перейдите в раздел ***«Конфигуратор»*** и выделите в рабочей области раздела элемент **Видеоподсистема**. На панели настроек перейдите на вкладку **Параметры**. Рабочая область вкладки примет следующий вид:



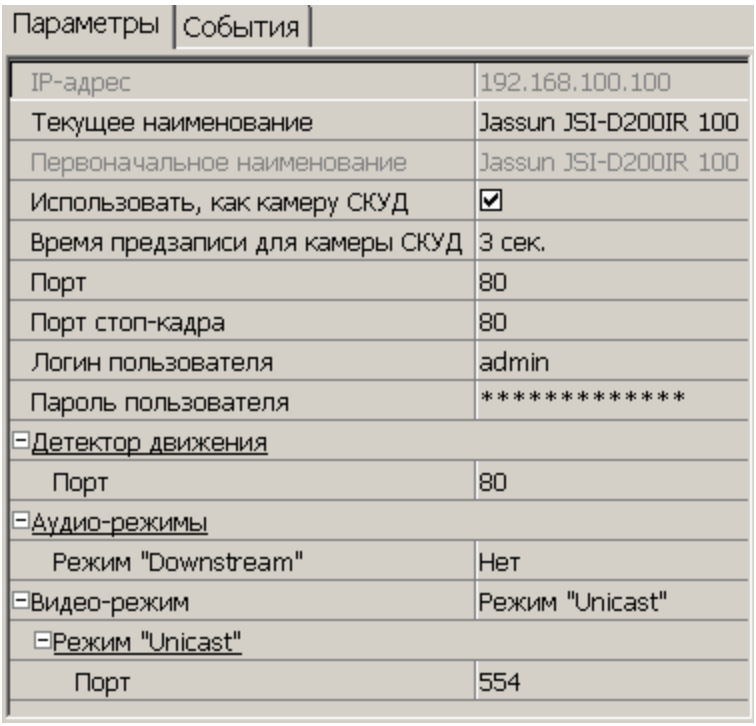
Для настройки доступны следующие параметры видеоподсистемы:

Текущее название – поле для ввода описательное название видеоподсистемы.

Частота кадров при записи для «Камер СКУД» – параметр предназначен для камер видеоподсистемы, используемых в качестве камер СКУД, то есть для которых установлен флажок у параметра **Использовать как камеру СКУД**. Параметр устанавливает частоту записи кадров с камеры. По умолчанию: 240 кадров в минуту.

3.13.17 Камера

Для настройки параметров камеры перейдите в раздел ***«Конфигуратор»*** и выделите в рабочей области раздела соответствующую камеру . Все добавленные в конфигурацию камеры входят в видеоподсистему. На панели настроек перейдите на вкладку **Параметры**. Рабочая область вкладки примет следующий вид:



Для настройки доступны следующие параметры камеры (в зависимости от типа камеры список параметров может изменяться):

Текущее наименование – поле для ввода описательного названия камеры.

Использовать в "Прозрачном здании" – при установке флажка у параметра кадры с камеры могут транслироваться в разделе ***«Прозрачное здание»***.

Использовать как камеру СКУД – установленный у параметра флажок указывает на то, что камера используется как камера СКУД, по крайней мере, с одним из считывателей системы безопасности (флажок устанавливается автоматически при выборе камеры для считывателя на вкладке **Камера СКУД**). При снятии флажка, после подтверждения оператора, камера будет удалена у всех считывателей.

Время предзаписи для камеры СКУД – Параметр предназначен для камер видеоподсистемы, используемых в качестве камер СКУД, то есть для которых установлен флажок у параметра **Использовать как камеру СКУД**. Параметр определяет время записи видеоинформации с камеры до и после регистрации события, связанного с проходом через ИУ в направлении считывателя. Значение установленное по умолчанию: 3 секунды. При этом в видеоархиве будет сохранена видеоинформация за 3 секунды до регистрации события и 3 секунды после.

Порт, Порт стоп-кадра – параметры, указывающие номера сетевых портов, используемых для связи с камерой.

Логин пользователя, Пароль пользователя – поля для ввода имени и пароль пользователя для доступа к камере.

Детектор движения: Порт – параметр, указывающий номера сетевого порта, используемого для обмена данными при активизации детектора движения.

Аудио-режимы: Downstream

- **Да** – аудио-сигнал со встроенного микрофона камеры транслируется в разделы ПО и может быть сохранен в видеоархиве. Необходимо дополнительно указать сетевой порт для передачи аудио-сигнала.
- **Нет** – передача аудио-сигнала с камеры отключена.

Видео-режим – параметр позволяет выбрать режим работы камеры. Наличие того или иного режима зависит от типа камеры, ее прошивки и версии SDK. Возможен выбор одного из следующих режимов:

- **Http** – обмен данными с камерой производится по протоколу HTTP в формате MJPEG. Количество подключений к камере ограничено ее ресурсами.
- **Unicast** – обмен данными с камерой производится по протоколу RTSP/RTP/ RTCP в формате MPEG-4 или по нестандартному протоколу, поддерживаемому камерой в формате MPEG-4. Количество подключений к камере ограничено ее ресурсами.
- **Multicast** – обмен данными с камерой производится по протокол RTSP/RTP/ RTCP в формате MPEG-4, или по нестандартному протоколу, поддерживаемому камерой в формате MPEG-4. Количество подключений к камере не ограниченно.
- **Tunnelled** – режим туннелирования RTSP через HTTP. Используется при невозможности подключения через Unicast. Количество подключений ограничено.

Дополнительные параметры – параметр доступен только для камер поддерживающих поддерживающих стандарт ONVIF. При выделении строки появится кнопка ..., позволяющая открыть окно **Менеджер поиска и конфигурации камер (стандарт ONVIF)**.

4 Раздел «Планировщик заданий»

4.1 Назначение

Раздел ***«Планировщик заданий»*** предназначен для создания заданий, выполняемых сервером системы автоматически по расписанию или при выполнении определенного условия. Заданием может являться набор команд по управлению устройствами системы или отправка SMS-сообщений.

В разделе доступны для создания следующие типы заданий:

По предъявлению идентификатора – При предъявлении любого из идентификаторов сотрудника из перечисленных на панели **Сотрудники,** одному из считывателей, перечисленных на панели **Считыватели** в промежуток времени, установленный на панели **Расписание**, на номер сотрудника будет отправлено SMS-сообщение с текстом, введенным на панели **Текст SMS** для данного считывателя, а затем будут выполнены команды в установленном на панели **Команды** порядке.

По времени – В установленный на панели **Расписание** промежуток времени начнется выполнение задания. На телефонные номера, заданные на панели **Телефоны,** будут отправлены SMS-сообщения с текстом, введенным на панели **Текст SMS**, и выполнены команды в установленном на панели **Команды** порядке.

По времени и достижению состояний – При достижении устройствами, указанными в столбце **Устройства**, состояний, указанных в столбце **Состояния** панели **Отслеживаемые состояния** (**всех состояний** или **хотя бы одного состояния** устанавливается в раскрывающемся списке **Выполнение команд по достижении:**) в установленный на панели **Расписание** промежуток времени на телефонные номера заданные на панели **Телефоны** будут отправлены SMS-сообщения с текстом, введенным на панели **Текст SMS**, и выполнены команды в установленном на панели **Команды** порядке.

По изменению состояний – При выходе устройств, указанных в столбце **Устройства**, из состояний, указанных в столбце **Состояния** панели **Отслеживаемые состояния** (**всех состояний** или **хотя бы одного состояния** устанавливается в раскрывающемся списке **Выполнение команд по достижении:**) (однократно, при установке флажка **Выполнять только один раз,** или каждый раз) в установленный на панели **Расписание** промежуток времени на телефонные номера заданные на панели **Телефоны** будут отправлены SMS-сообщения с текстом, введенным на панели **Текст SMS**, и выполнены команды в установленном на панели **Команды** порядке.

Отправка SMS по неприходу – При опоздании сотрудника из числа перечисленных на время, превышающее указанное в поле ввода времени **Допустимое опоздание,** на его номер будет отправлено SMS-сообщение с текстом, введенным на панели **Текст SMS.**

Отчет по EMail – С установленной периодичностью на указанные адреса электронной почты отправляется один из отчетов по учету рабочего времени или дисциплине труда формируемый в соответствующем разделе ***«УРВ»*** или ***«Дисциплинарные отчеты»***.

Внимание!

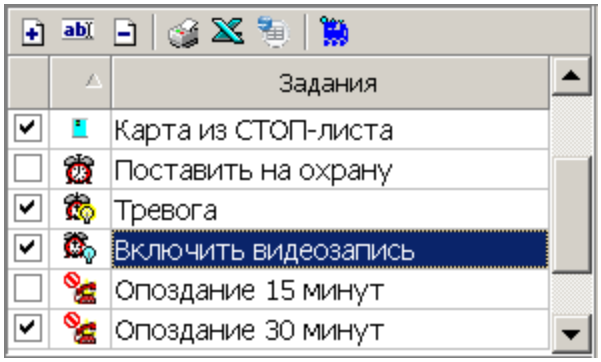
- Для создания задания по отправке отчета *«T13»* необходимо приобрести лицензию на модуль ***PERCo-SM07 «УРВ»***.
- Для создания задания по отправке дисциплинарных отчетов необходимо приобрести лицензию на модуль ***PERCo-SM05 «Дисциплинарные отчеты»***.

4.2 Панели рабочей области

4.2.1 Панель «Задания»

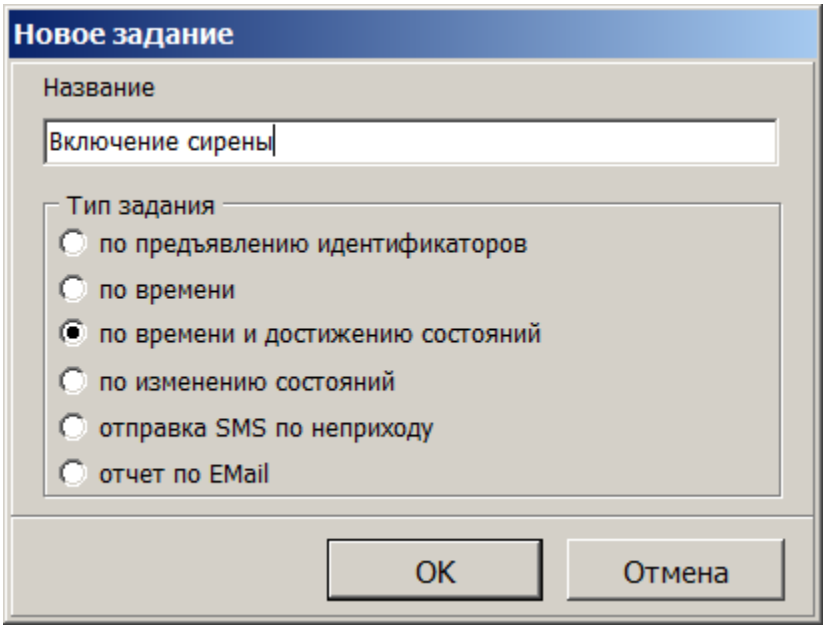
При первом запуске в рабочем окне раздела доступна только панель **Задания**, позволяющая создавать новые задания и управлять уже созданными. Рабочее окно раздела состоит из типовых панелей и его вид зависит от типа задания, выбранного на панели **Задания**.

Панель имеет следующий вид:



Инструменты панели:

Добавить (**Ctrl**+**N**) – кнопка позволяет создать новое задание. При нажатии кнопки откроется окно **Новое задание**:



Для создания нового задания введите название, выберите тип задания, затем нажмите кнопку **ОК**. После этого необходимо настроить параметры задания и активизировать его.

Изменить (**Crtl+E**) – кнопка позволяет изменить название выделенного в рабочей области задания.

Удалить (**Ctrl+D**) – кнопка позволяет удалить выбранное в рабочей области задание. Вся информация о задании также будет удалена из журнала выполнения заданий.

Печать (**Ctrl+P**) – кнопка позволяет распечатать списки заданий, отображаемых в рабочей области, отдельно для каждого типа заданий для разных типов.

Экспорт в Excel (**Ctrl+Y**) – Кнопка позволяет сохранить списки заданий, отображаемых в рабочей области, отдельно для каждого типа заданий в файлы с расширением `.xls`.

Экспорт в OpenOffice Calc – кнопка позволяет сохранить списки заданий, отображаемых в рабочей области, отдельно для каждого типа заданий в файлы с расширением `.ods`.

Журнал (**Ctrl+L**) – кнопка позволяет перейти к журналу выполнения заданий.

Флажок в первом столбце рабочей области панели указывает, что задание активизировано и будет выполнено сервером системы. Для отключения задания снимите флажок.

Внимание!

Активизировать задание можно только в случае, когда задан минимальный набор его параметров.

Значок во втором столбце рабочей области панели указывает на следующие типы заданий:

– по предъявлению идентификаторов,

– по времени,

– по времени и достижению состояний,

– по изменению состояний,

– отправка SMS по неприходу,

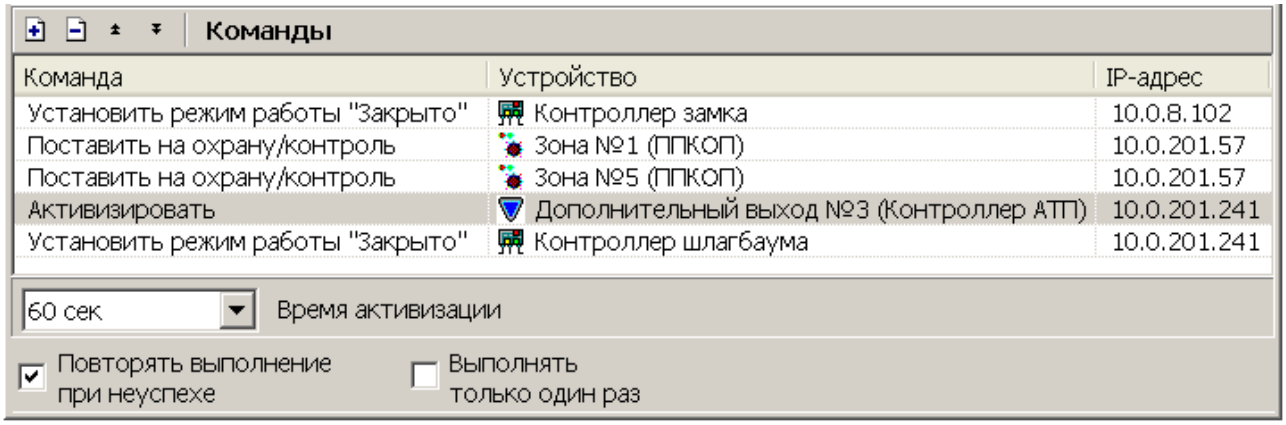
– отчет по почте.

Примечание:

В рабочей области реализованы функции: сортировка по элементам одного или нескольких столбцов, изменение ширины и последовательности столбцов

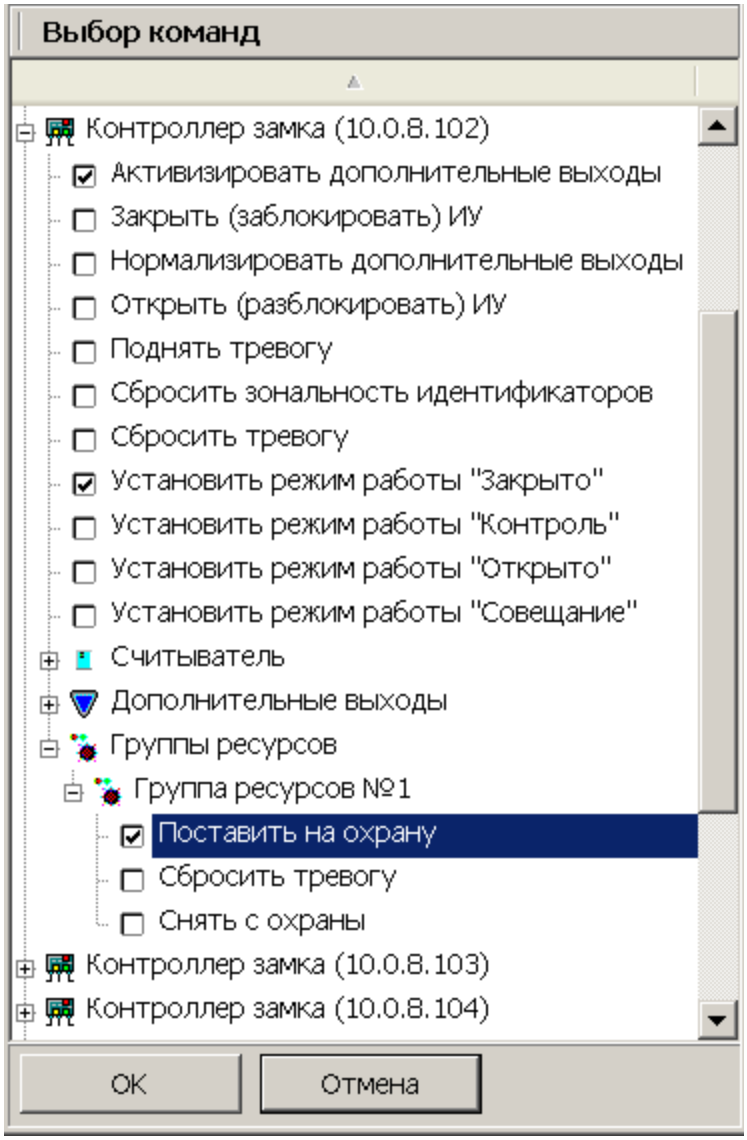
4.2.2 Панель «Команды»

Панель позволяет задавать команды устройствам системы безопасности и устанавливать порядок выполнения этих команд.



Инструменты панели:

Добавить команду – кнопка позволяет задать команды для устройств и их ресурсов. При нажатии кнопки откроется панель **Выбор команд**:



На открывшейся панели отметьте флажками необходимые команды в раскрывающемся многоуровневом списке устройств системы безопасности и их ресурсов, затем нажмите кнопку **ОК**.

Удалить команду – кнопка позволяет удалить выбранную в рабочей области команду.

Переместить вверх, **Переместить вниз** – кнопки позволяют поднять или опустить выбранную в рабочей области команду в очереди выполнения команд. Команды выполняются последовательно сверху-вниз.

Время активизации. Раскрывающийся список позволяет установить длительность выполнения команды. Доступен не для всех команд.

Повторять выполнение при неуспехе. При установке флажка – в случае, если выполнение задания завершилось с ошибкой, сервер системы будет пытаться выполнить его снова.

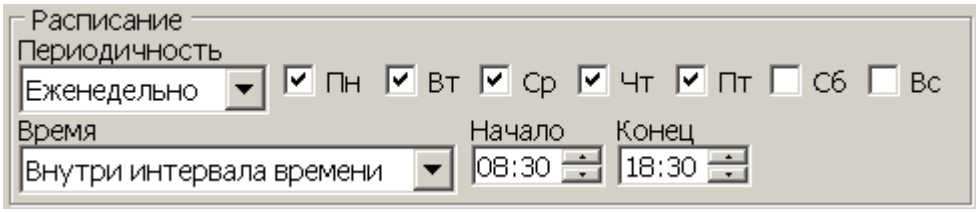
Внимание!

Повторный запуск задания возможен только в промежутке времени, указанном на панели **Расписание**. Перевод задания на следующий день не предусмотрен.

Выполнять только один раз. При установке флажка – задание может быть выполнено не более одного раза в течение суток. (Если задание было изменено, то оно будет считаться новым, и будет запущено заново в установленный временной интервал.)

4.2.3 Панель «Расписание»

Панель имеет следующий вид:



Инструменты панели:

Периодичность. Раскрывающийся список позволяет указать дни недели, на которые назначено задание:

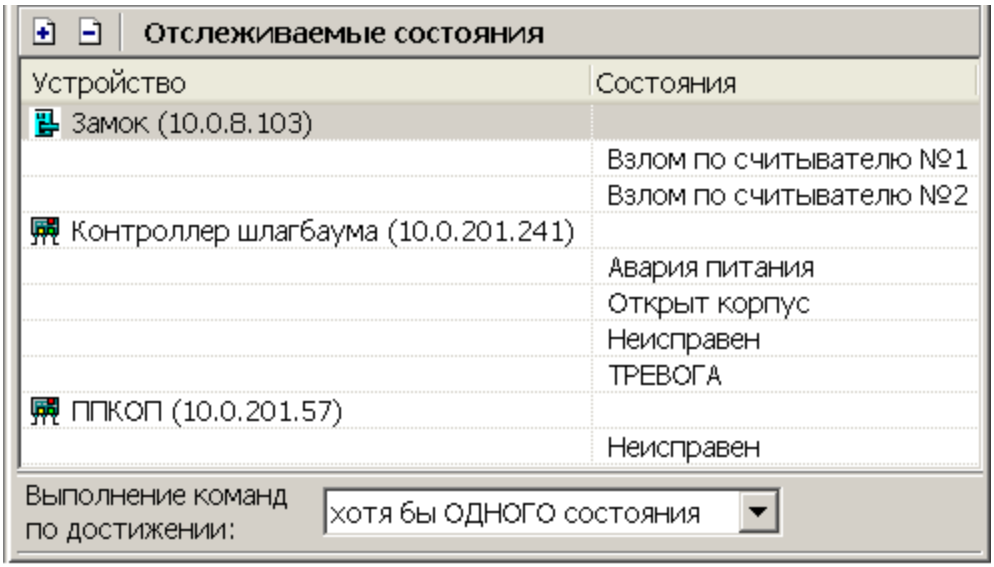
- **Ежедневно.** Задание назначено на каждый день в установленное **Время**.
- **Еженедельно.** Задание назначено на дни недели, отмеченные флажками в установленное **Время**.

Время. Раскрывающийся список позволяет установить промежуток времени, в который возможен запуск задания.

- **Без ограничений.** Задание может быть запущено в любое время в течение суток (**Начало** 00:00, **Конец** 23:59).
- **Внутри интервала времени.** Задание может быть запущено только в интервал времени, установленный в полях ввода времени **Начало**, **Конец**, в течение суток.

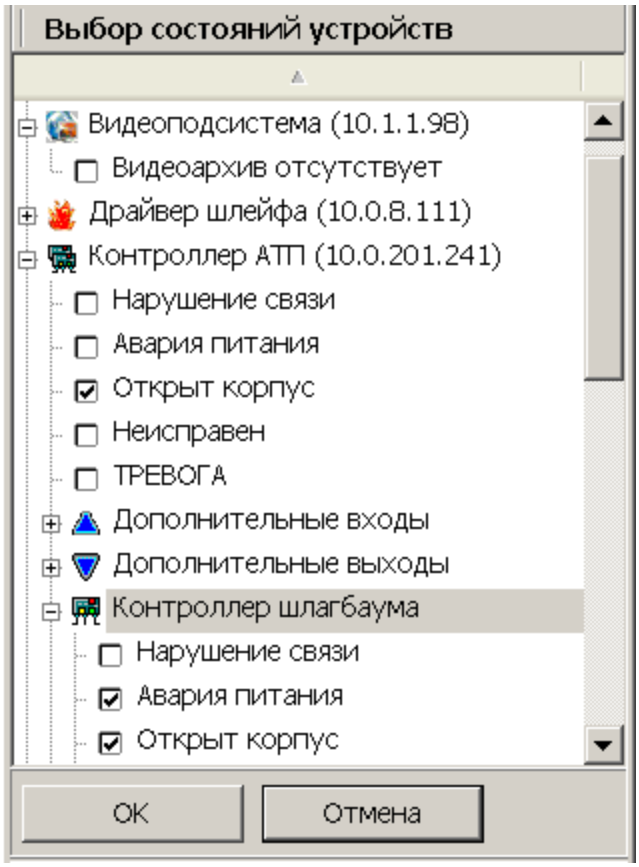
4.2.4 Панель «Отслеживаемые состояния»

Панель имеет следующий вид:



Инструменты панели:

Добавить – кнопка позволяет задать состояния устройств и их ресурсов, отслеживаемые системой, достижение (изменение) которых является условием выполнения задания. При нажатии кнопки откроется панель **Выбор состояний устройств:**



На открывшейся панели отметьте флажками необходимые состояния (регистрируемые события мониторинга) в раскрывающемся многоуровневом списке устройств системы безопасности и их ресурсов, затем нажмите кнопку **ОК**.

Удалить – кнопка позволяет удалить выбранное в рабочей области состояние.

Выполнение команд по достижении: – раскрывающийся список позволяет выбрать зависимость условия запуска выполнения задания от установленных состояний:

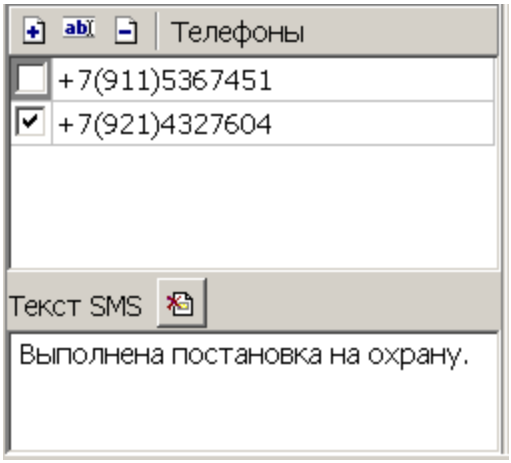
- **ВСЕХ состояний.** Выполнение задания начнется при наступлении всех указанных на панели состояний.
- **Хотя бы ОДНОГО состояния.** Выполнение задания начнется при наступлении одного из установленных на панели состояний.

4.2.5 Панели «Телефоны» и «Текст SMS»

Панель **Телефоны** позволяет задать номера телефонов, а панель **Текст SMS** – ввести текст SMS-сообщения для рассылки при выполнении задания.

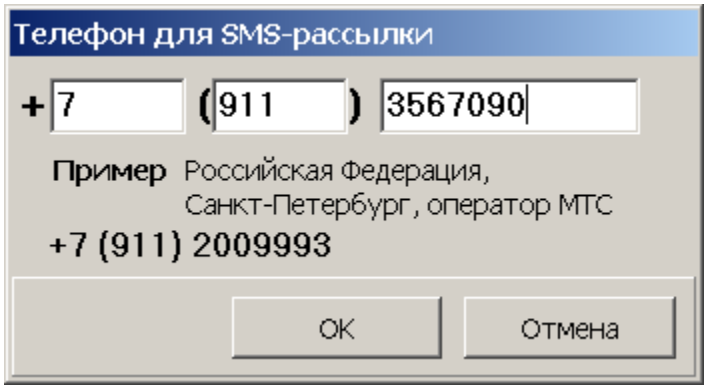
Примечание:

Для отправки SMS-сообщений необходимо чтобы в «***Центре управления»*** на вкладке **Настройка SMS-рассылки** был выбран и настроен способ отправки сообщений, и к системе было подключено соответствующее оборудование.



Инструменты панелей:

Добавить – кнопка позволяет добавить номер телефона для отправки SMS-сообщения. При нажатии кнопки откроется окно **Телефон для SMS-рассылки**:



Введите в соответствующие поля ввода международный код страны, код региона и номер телефона, затем нажмите кнопку **ОК**

Изменить – кнопка позволяет изменить, выбранный в рабочей области номер телефона. При нажатии кнопки откроется окно **Телефон для SMS-рассылки**.

Удалить – кнопка позволяет удалить выбранный в рабочей области номер телефона.

При снятии флажка у номера телефона в рабочей области панели SMS-сообщение на этот номер отсылаться не будет.

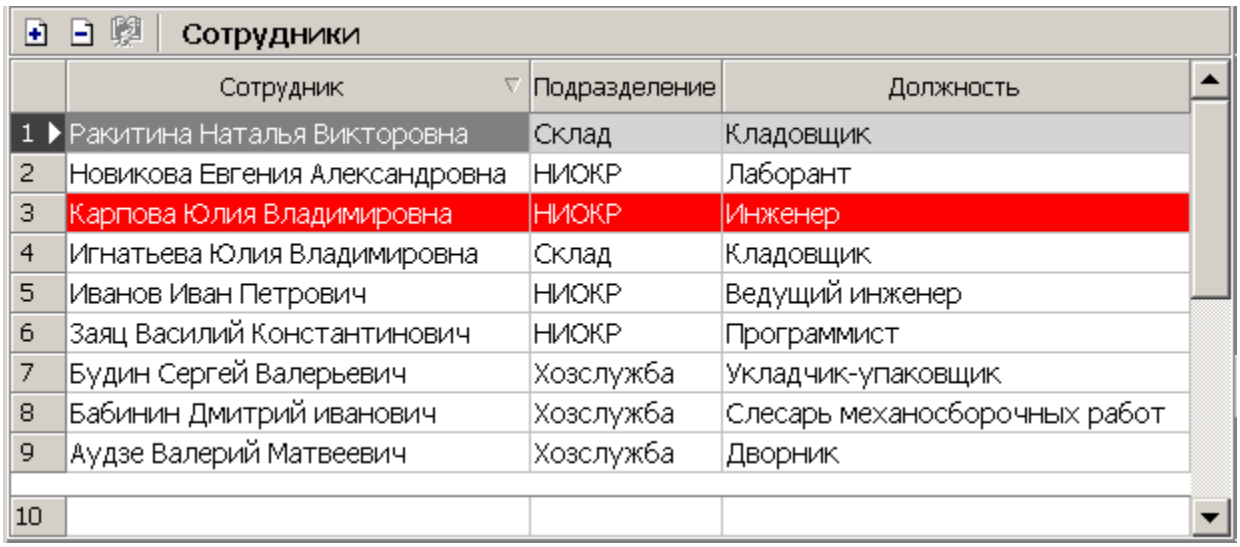
Удалить текст SMS – кнопка позволяет очистить рабочую область панели **Текст SMS**.

Примечание:

SMS-сообщения рассылаются после начала выполнения задания перед исполнением команд. Текст одного SMS-сообщения может содержать не более 35 символов.

4.2.6 Панель «Сотрудники»

Панель предназначена для создания списка сотрудников. Панель имеет следующий вид:



	Сотрудник	Подразделение	Должность
1	Ракитина Наталья Викторовна	Склад	Кладовщик
2	Новикова Евгения Александровна	НИОКР	Лаборант
3	Карпова Юлия Владимировна	НИОКР	Инженер
4	Игнатьева Юлия Владимировна	Склад	Кладовщик
5	Иванов Иван Петрович	НИОКР	Ведущий инженер
6	Заяц Василий Константинович	НИОКР	Программист
7	Будин Сергей Валерьевич	Хозслужба	Укладчик-упаковщик
8	Бабинин Дмитрий иванович	Хозслужба	Слесарь механосборочных работ
9	Аудзе Валерий Матвеевич	Хозслужба	Дворник
10			

Инструменты панели:

Добавить – кнопка позволяет добавить в список сотрудников.

Удалить – кнопка позволяет удалить выбранных в рабочей области сотрудников.

НИОКР **Выбор подразделения** – кнопка и название выбранного в данный момент подразделения. (Кнопка доступна только в режиме добавления сотрудников.) В рабочей области панели отображаются сотрудники выбранного подразделения.

Выделение в рабочей области строки с данными сотрудника красным цветом означает, что для сотрудника не задано ни одного телефона, и ему невозможно отправить SMS-сообщение. Номера телефонов сотрудников задаются в разделе ***«Сотрудники»*** модуля ***SN01 «Базовое ПО»***.

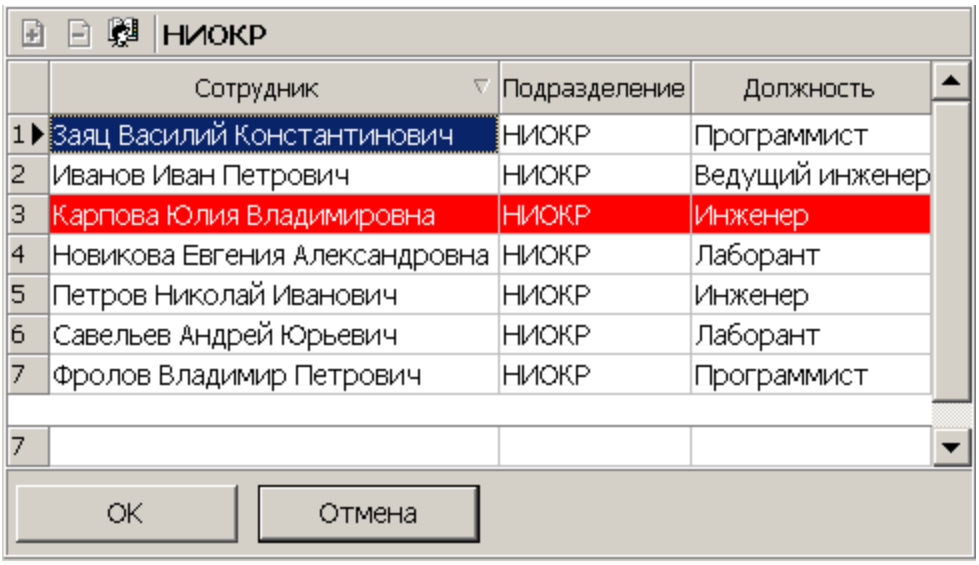
Примечание:

В рабочей области реализованы функции: сортировка по элементам одного или нескольких столбцов, одновременное выделения нескольких элементов и изменение ширины и последовательности столбцов.

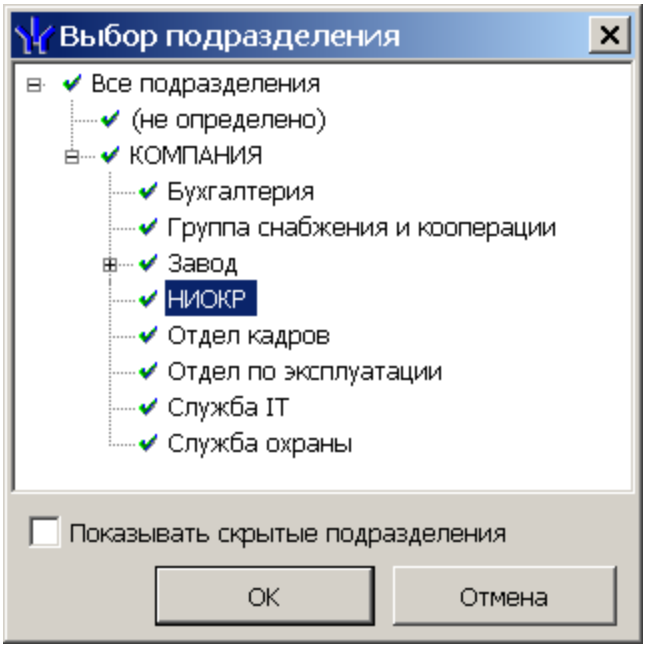
Добавление сотрудников

Для добавления сотрудников произведите последовательно следующие действия:

1. Нажмите кнопку **Добавить** в инструментах панели. Панель перейдет в режим добавления сотрудников:



2. Для выбора подразделения нажмите ставшую доступной кнопку **Выбор подразделения** в инструментах панели. Откроется окно **Выбор подразделения**:

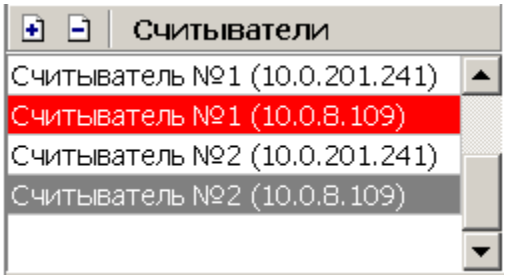


3. В открывшемся окне выберите подразделение, сотрудников которого необходимо добавить в список. Нажмите кнопку **ОК**. При установке флажка **Показывать скрытые подразделения** в списке будут отображаться удаленные подразделения. (Значок ✘ у названия подразделения означает, что у оператора нет прав доступа к данному подразделению.)

4. Окно Выбор подразделения будет закрыто. Список сотрудников этого подразделения будет отображен в рабочей области панели **Сотрудники**.
5. Выделите в рабочей области сотрудников, которых необходимо добавить в список. Нажмите кнопку **ОК**.
6. Выделенные сотрудники будут добавлены в список, панель выйдет из режима добавления сотрудников.
7. При необходимости добавьте сотрудников, выбрав другое подразделение.

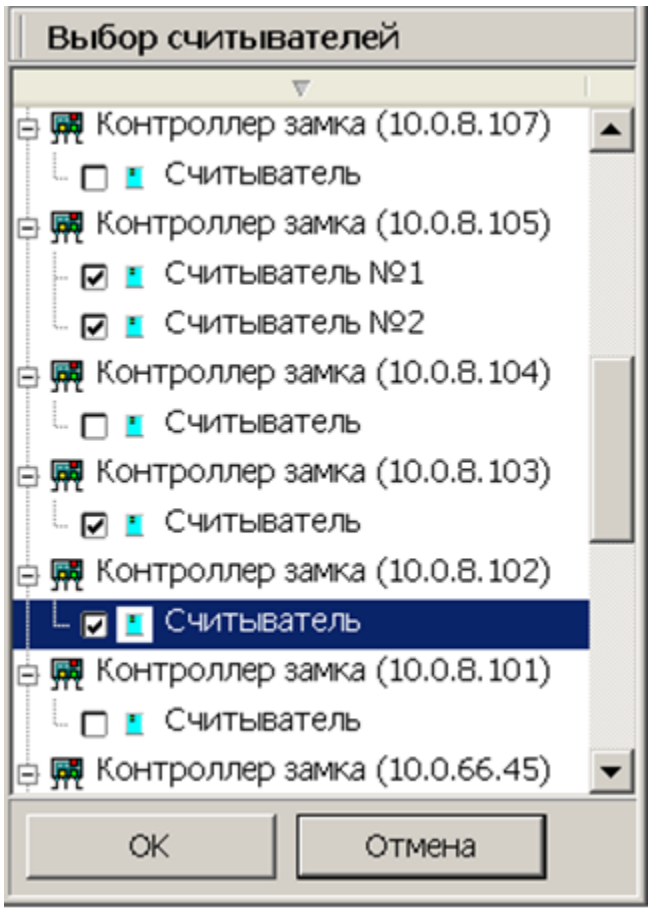
4.2.7 Панель «Считыватели»

Панель **Считыватели** предназначена для выбора считывателей, предъявление идентификаторов к которым будет отслеживаться заданием.



Выделение в рабочей области считывателя красным цветом означает, что для него не введен текст SMS-сообщения.

Добавить – кнопка позволяет добавить на панель новые считыватели. При нажатии кнопки откроется панель **Выбор считывателей**:

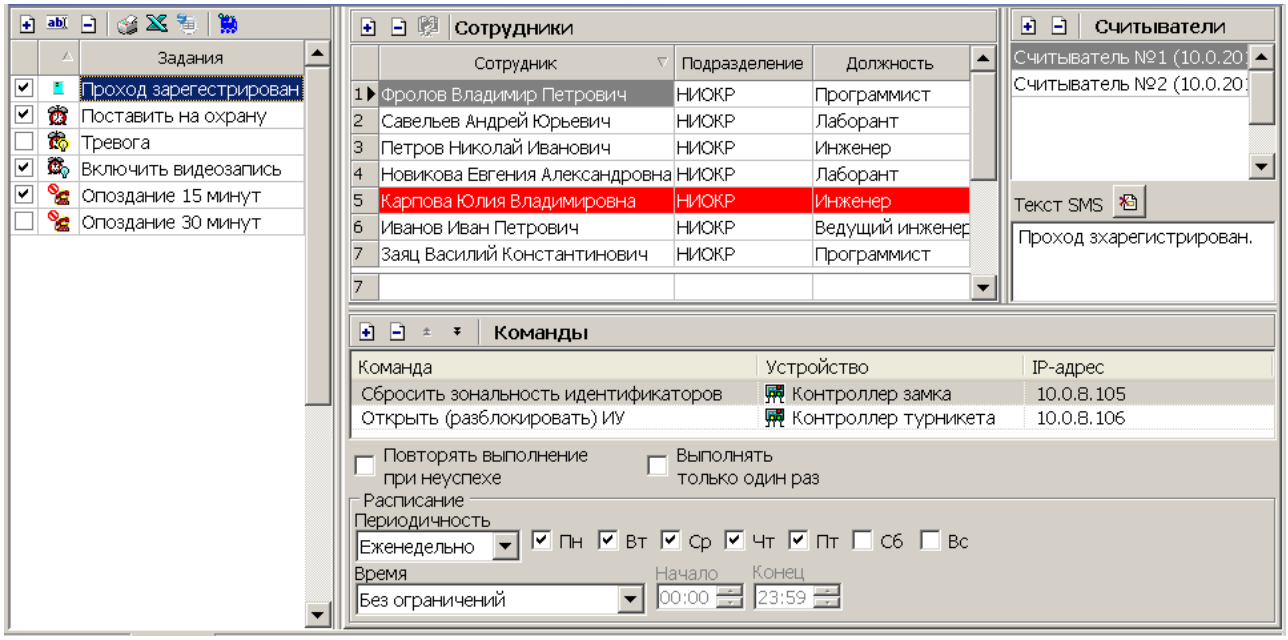


На открывшейся панели в раскрывающемся многоуровневом списке контроллеров системы безопасности отметьте флажками необходимые считыватели, затем нажмите кнопку **ОК**.

Удалить – кнопка позволяет удалить выбранный в рабочей области считыватель.

4.3 Задание по предъявлению идентификаторов

Рабочее окно раздела при настройке параметров задания по предъявлению идентификаторов выглядит следующим образом:

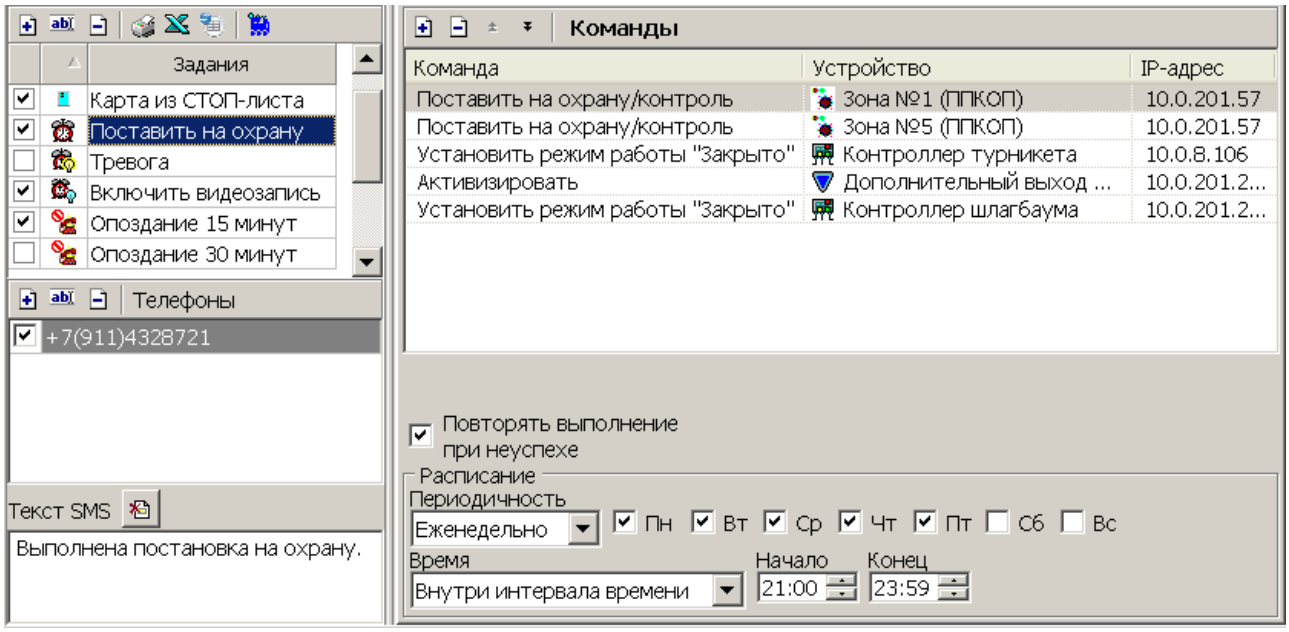


Порядок настройки задания:

1. Нажмите кнопку **Добавить** на панели **Задания** и создайте новое задание, при этом **Тип задания**выберите **По предъявлению идентификаторов**.
2. На панели **Сотрудники** добавьте сотрудников, предъявление идентификаторов которых будет отслеживаться заданием.
3. На панели **Считыватели** добавьте считыватели, предъявление к которым идентификаторов выбранных сотрудников будет отслеживаться заданием.
4. На панели **Текст SMS** введите текст SMS-сообщения независимо для каждого считывателя. Сообщение, связанное со считывателем, будет отправлено в случае начала выполнения задания, на номер телефона сотрудника, предъявившего идентификатор.
5. На панели **Расписание** установите периодичность и время выполнения задания.
6. На панели **Команды** добавьте команды, которые будут выполняться системой в случае запуска задания.
7. Поставьте флажок в строке с названием задания на панели **Задания**.
8. Нажмите кнопку **Сохранить** в панели инструментов ***«Консоли управления»***.

4.4 Задание по времени

Рабочее окно раздела при настройке параметров задания по времени выглядит следующим образом:

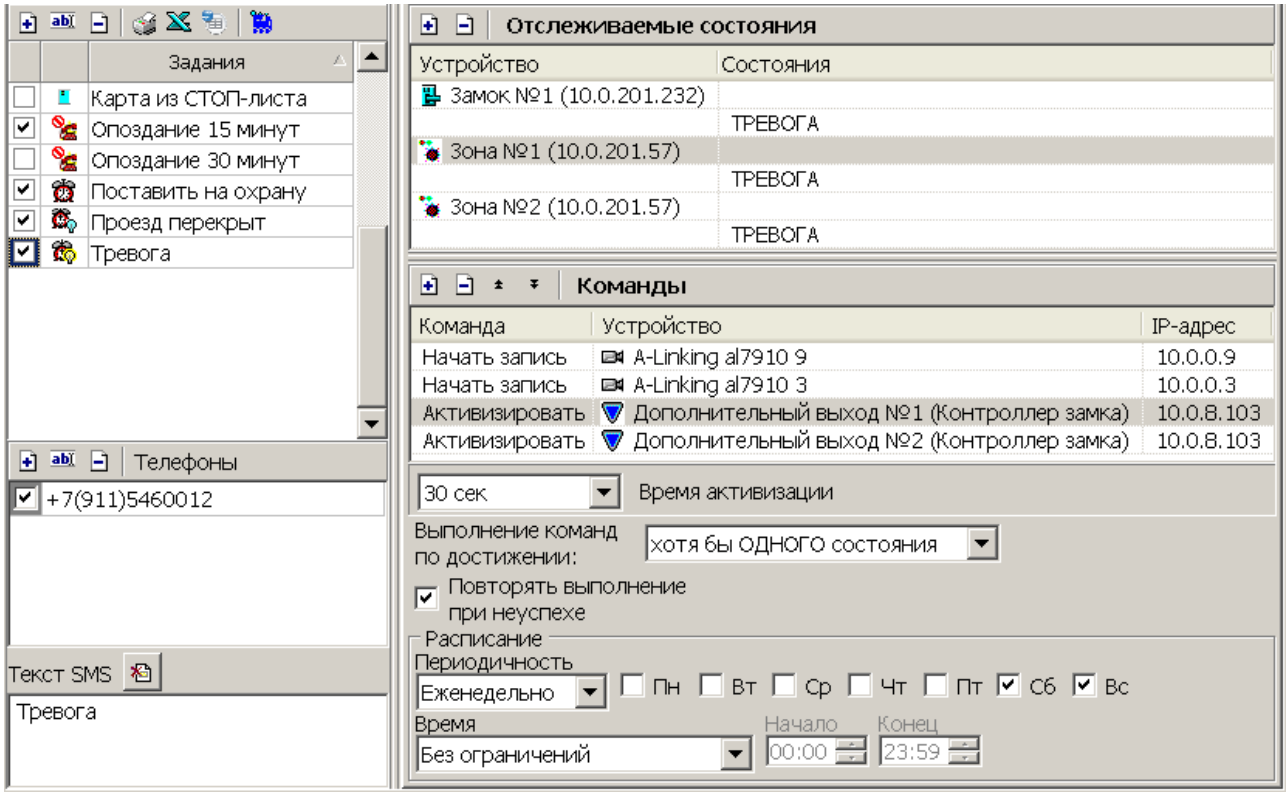


Порядок настройки задания:

1. Нажмите кнопку **Добавить** на панели **Задания** и создайте новое задание, при этом **Тип задания** выберите **По времени**.
2. На панели **Телефоны** задайте телефонные номера, на которые будут рассылаться SMS-сообщения в случае начала выполнения задания.
3. На панели **Текст SMS** введите текст SMS-сообщения.
4. На панели **Расписание** установите периодичность и время выполнения задания.
5. На панели **Команды** добавьте команды, которые будут выполняться системой при запуске задания.
6. Поставьте флажок в строке с названием задания на панели **Задания**.
7. Нажмите кнопку **Сохранить** в панели инструментов ***Консоли управления***.

4.5 Задание по времени и достижению состояний

Рабочее окно раздела при настройке параметров задания по времени и достижению состояния выглядит следующим образом:

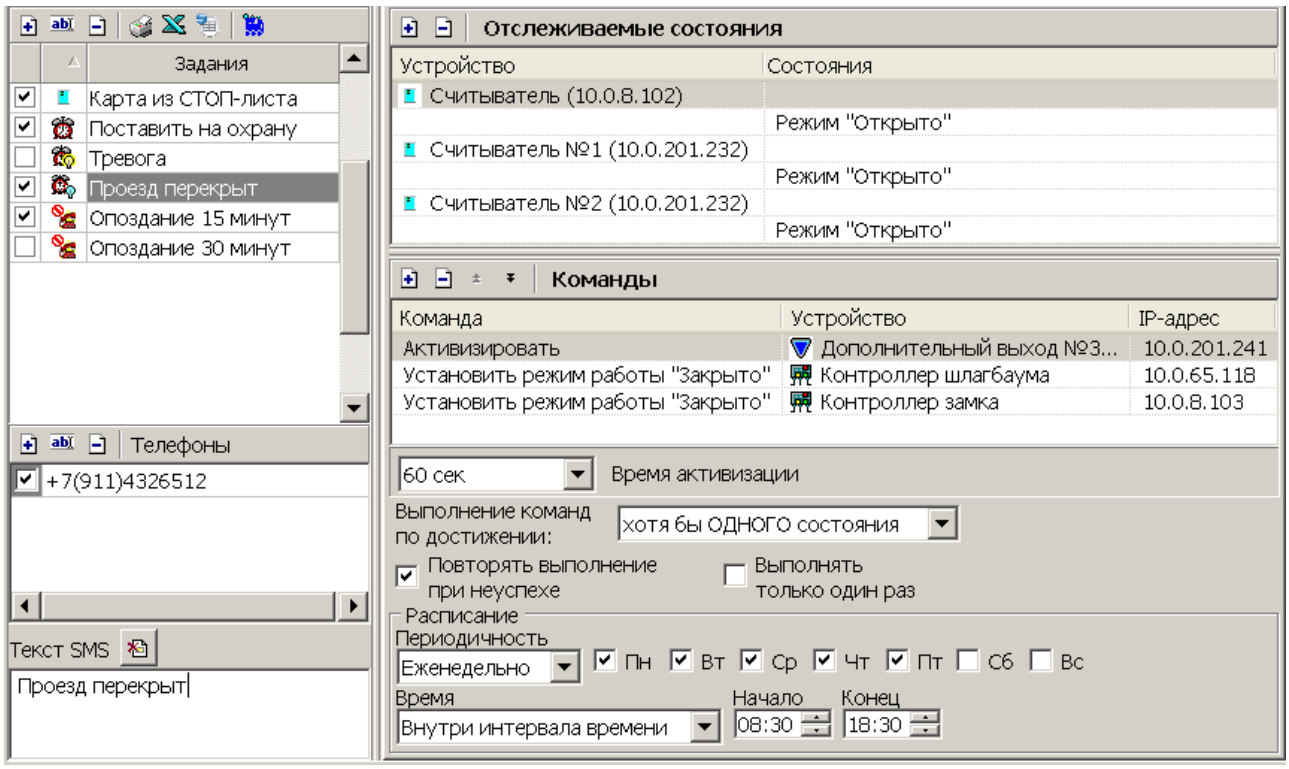


Порядок настройки задания:

1. Нажмите кнопку **Добавить** на панели **Задания** и создайте новое задание, при этом **Тип задания** выберите **По времени и достижению состояния**.
2. На панели **Телефоны** задайте телефонные номера, на которые будут рассылаться SMS-сообщения в случае начала выполнения задания.
3. На панели **Текст SMS** введите текст SMS-сообщения.
4. На панели **Расписание** установите периодичность и время выполнения задания.
5. На панели **Отслеживаемые состояния** добавьте состояния, отслеживаемые системой, достижение которых является условием для начала выполнения задания.
6. На панели **Команды** добавьте команды, которые будут выполняться системой при запуске задания.
7. Поставьте флажок в строке с названием задания на панели **Задания**.
8. Нажмите кнопку **Сохранить** в панели инструментов ***«Консоли управления»***.

4.6 Задание по изменению состояний

Рабочее окно раздела при настройке параметров задания по изменению состояния выглядит следующим образом:



Порядок настройки задания:

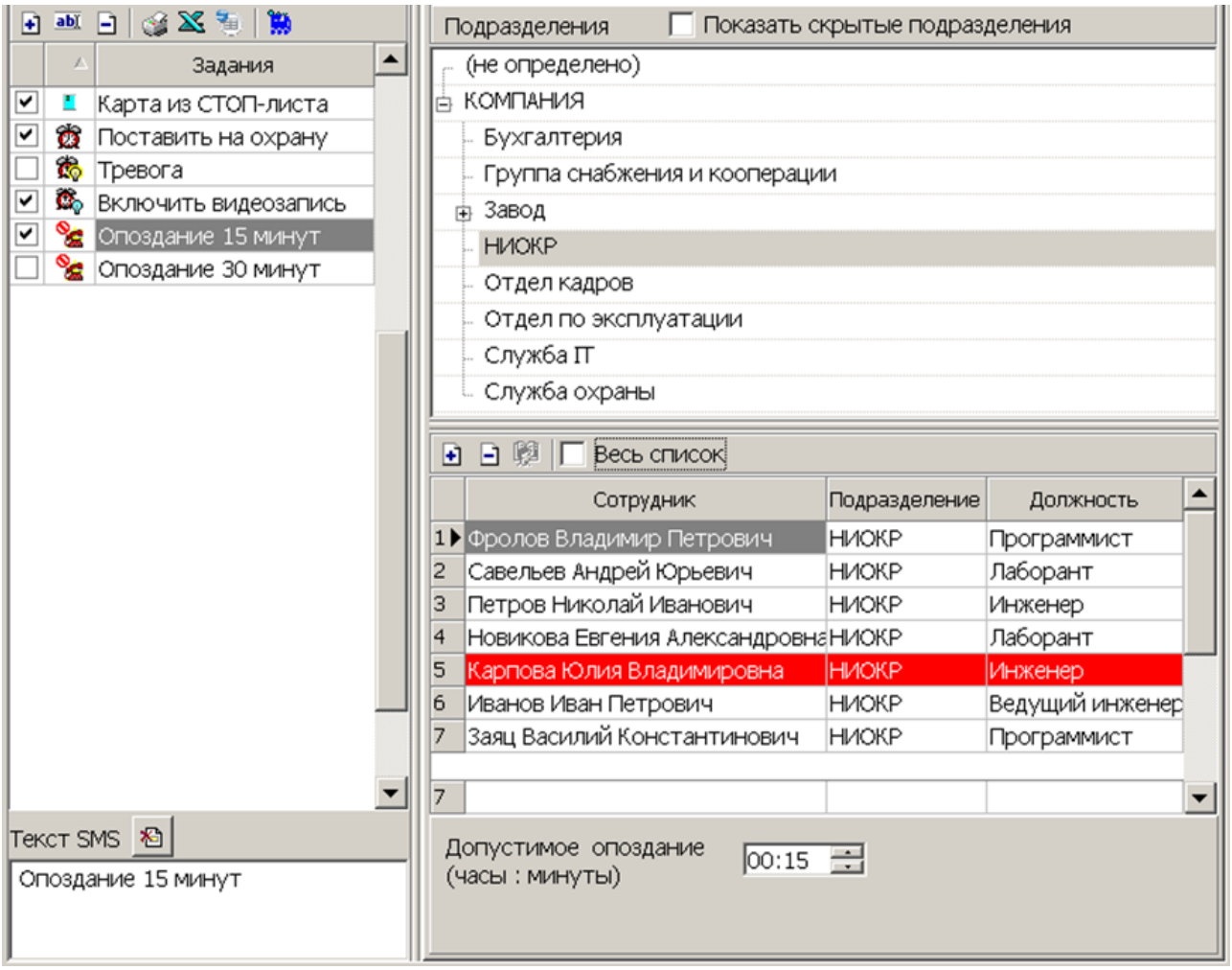
1. Нажмите кнопку **Добавить** на панели **Задания** и создайте новое задание, при этом **Тип задания** выберите **По изменению состояний**.
2. На панели **Телефоны** задайте телефонные номера, на которые будут рассылаться SMS-сообщения в случае начала выполнения задания.
3. На панели **Текст SMS** введите текст SMS-сообщения.
4. На панели **Расписание** установите периодичность и время выполнения задания.
5. На панели **Отслеживаемые состояния** добавьте состояния, отслеживаемые системой, изменение которых является условием для начала выполнения задания.
6. На панели **Команды** добавьте команды, которые будут выполняться системой при запуске задания.
7. Поставьте флажок в строке с названием задания на панели **Задания**.
8. Нажмите кнопку **Сохранить** в панели инструментов ***«Консоли управления»***.

4.7 Задание отправки SMS по неприходу

Примечание:

- Для выполнения задания необходимо, чтобы для каждого сотрудника, включенного в список задания, в разделе ***«Сотрудники»*** модуля ***PERCo-SN01 «Базовое ПО»*** был выбран график работы, отличный от установленного по умолчанию *ГРАФИКА НИКОГДА* с указанием хотя бы одного регистрирующего помещения и задан номер телефона.
- Настройка графиков работы сотрудников возможна в разделе ***«Графики рабочего времени»*** модуля ***PERCo-SN01 «Базовое ПО»***
- Номера телефонов сотрудников задаются в разделе ***«Сотрудники»*** модуля ***SN01 «Базовое ПО»***. Для ввода телефонного номера сотрудника необходимо открыть панель **Телефоны для SMS-отправки** с помощью кнопки в панели инструментов вкладки **Сотрудники**.

Рабочее окно раздела при настройке параметров задания по неприходу выглядит следующим образом:



Порядок настройки задания:

1. Нажмите кнопку **Добавить** на панели **Задания** и создайте новое задание, при этом **Тип задания** выберите **Отправка SMS по неприходу**.

2. На панели **Допустимое опоздание** с помощью поля ввода времени установите максимальное допустимое время опоздания сотрудника. Началом отсчета времени опоздания считается нижняя граница 1-го интервала графика рабочего времени, установленного сотруднику. Приход на работу фиксируется по предъявлению идентификатора сотрудника любому из считывателей, контролирующих проход в одно из регистрирующих помещений.
3. На панели **Текст SMS** введите текст SMS-сообщения. Фамилия, имя и отчество отсутствующего сотрудника помещаются в сообщение автоматически. Текст отправляемого сообщения один и тот же для всех сотрудников. Сообщение будет отправлено сотруднику в случае его опоздания на время, превышающее введенное на панели **Допустимое опоздание**, на номер телефона, указанный для сотрудника.
4. На панели **Сотрудники** добавьте сотрудников, которым будут отправляться SMS-сообщения по неприходу. Каждый сотрудник может входить в список только для одного задания по неприходу. На панели отображаются сотрудники подразделения, выделенного на панели **Подразделения**. При установке флажка **Весь список** в списке будут отображаться сотрудники всех подразделений.
5. Поставьте флажок в строке с названием задания на панели **Задания**.
6. Нажмите кнопку **Сохранить** в панели инструментов ***«Консоли управления»***.

Примечание:

Статистика по отправленным SMS-сообщениям доступна в разделе ***«Отчет по SMS»***.

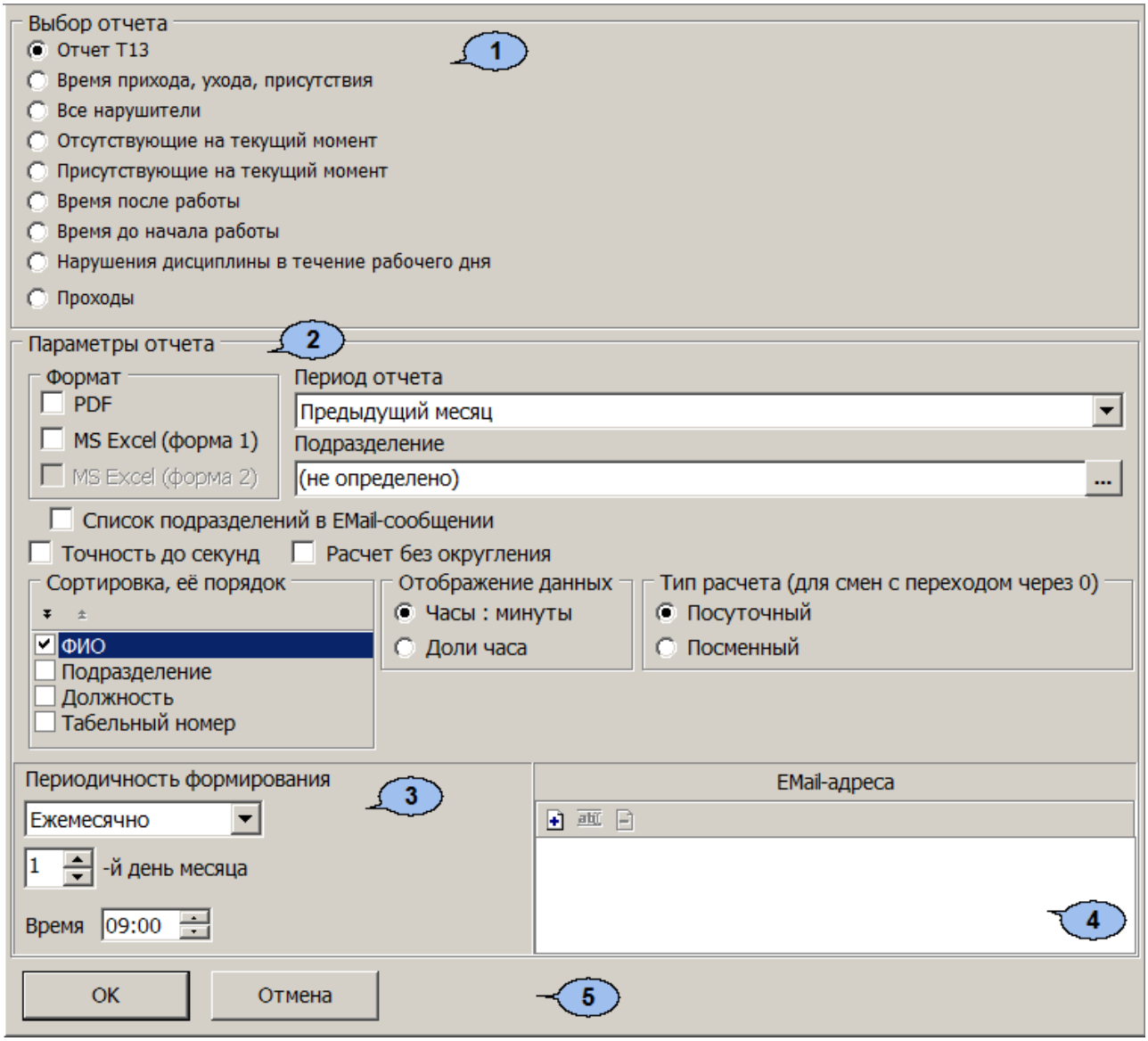
4.8 Задание отправки отчета по EMail

Примечание:

Для выполнения задания необходимо настроить рассылку по электронной почте в разделе ***«Центр управления» PERCo-S-20*** на вкладке **Настройка почтовой рассылки отчетов**.

Панель настройки задания

Панель настройки задания отправки отчета по электронной почте имеет следующий вид:



Внимание!

Наличие тех или иных параметров на панели зависит от выбранного типа отчета.

1. Панель **Выбор отчета** содержит переключатель, позволяющий выбрать один из следующих типов отчетов:
   - **Отчет Т13**
   - **Время прихода, ухода, присутствия**
   - **Все нарушители**
   - **Отсутствующие на текущий момент**
   - **Присутствующие на текущий момент**
   - **Время после работы**
   - **Время до начала работы**
   - **Нарушения дисциплины в течение рабочего дня**
   - **Проходы**
2. Панель **Параметры отчета** содержит параметры настройки для выбранного отчета. При этом для разных отчетов параметры могут отличаться.

   Формат – с помощью флажков позволяет выбрать форматы отчетов.

Период отчета – раскрывающийся список позволяет указать период времени, за который будет составлен отчет. Продолжительность периода отчета не может превышать один месяц.

Подразделение – в поле отображается подразделение, по сотрудникам которого составляется отчет. Для выбора подразделения справа от поля нажмите кнопку **Выбор подразделения** ....

Список подразделений в EMail сообщении – при установке флажка в письме отображается список подразделений по сотрудникам которых сформирован отчет.

Точность до секунды – при установке флажка время в отчетах отображается с точностью до секунд.

Расчет без округления – при установке флажка секунды в отчетах отбрасываются без округления до минут.

Сортировка, ее порядок – позволяет с помощью флажков указать заголовки столбцов по которы будет произведена сортировка данных при составлении отчета.

Показывать нулевые значения – при установке флажка в отчете отображаются нулевые значения времени.

Отображение данных – переключатель позволяет выбрать формат отображения времени в отчете Т13:

- **Часы:минуты**
- **Доли часа**

Тип расчета (для смен с переходом через 0) – переключатель позволяет выбрать способ расчета времени в отчете Т13:

- **посуточный**
- **посменный**

Отображаемые столбцы – на панели в помощью флажков можно отметить столбцы с данными отображаемые в отчете *«Время прихода, время присутствия»*:

- **Время прихода**
- **Время ухода**
- **Время присутствия**

Виды нарушений – на панели в помощью флажков можно отметить виды нарушений трудовой дисциплины, отображаемые в отчете *«Все нарушители»*:

- **Опоздание**
- **Уход раньше**
- **Отсутствие**
- **Прогул**
- **Общее время нарушений**
- **Другие нарушения**

3. Панель **Периодичность формирования** содержит параметры для настройки времени и периодичности формирования и отправки отчета.
4. Панель **EMail-адреса** содержит список электронных адресов, на которые отправляется сформированный при выполнении задания отчет. На панели расположены следующие кнопки:

   Добавить – кнопка позволяет открыть дополнительную панель для ввода нового электронного адреса:

Изменить – кнопка позволяет открыть дополнительную панель для изменения выделенного на панели электронного адреса.

Удалить – кнопка позволяет удалить выделенный на панели электронный адрес.

5. Кнопки **ОК** и **Отмена** позволяют сохранить измененные параметры задания или отменить внесенные в задание изменения.

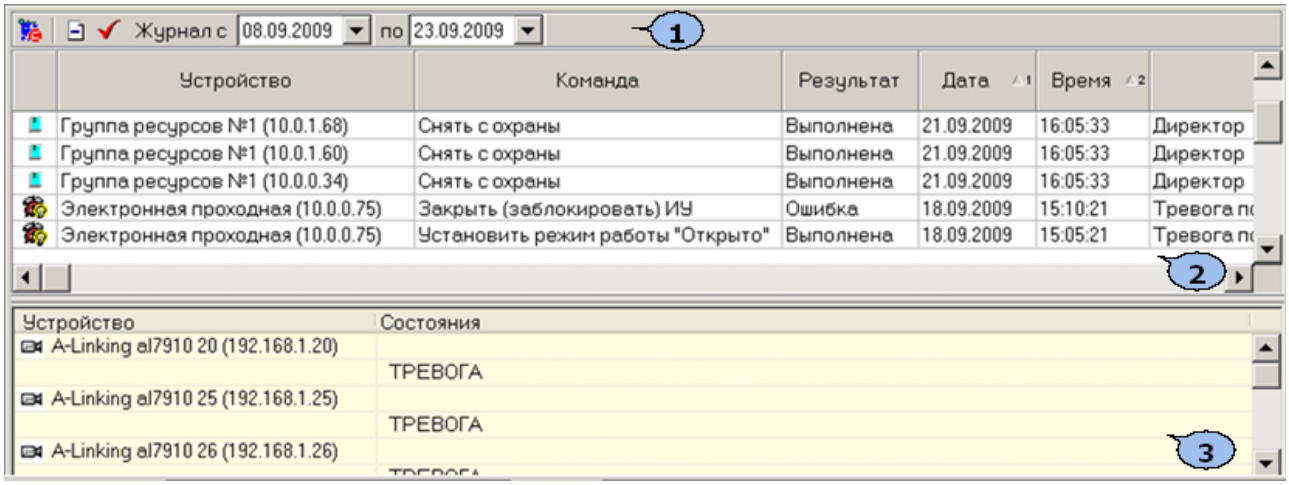
Порядок настройки задания

Порядок настройки задания:

1. Нажмите кнопку **Добавить** на панели **Задания** и создайте новое задание. Введите название задания. Переключатель **Тип задания** установите в положение **Отчет по EMail**. Откроется панель настройки задания.
2. На панели **Выбор отчета** с помощью переключателя выберите один из типов отчета, который будет отправляться по электронной почте.
3. На панели **Параметры отчета**:
   - С помощью раскрывающегося списка **Период отчета установите** промежуток времени, за который составляется отчет.
   - Нажмите кнопку **Выбор подразделения** справа от поля **Подразделение**. В открывшемся окне выберите подразделение, для сотрудников которого составляется отчет.
   - При необходимости установите флажок **Список подразделений в EMail сообщении**.
   - Настройте другие параметры отчета.
4. На панели **Периодичность** установите регулярность формирования отчета и время его отправки на электронный адрес.
5. На панели **EMail-адреса** нажмите кнопку **Добавить**. На открывшейся панели введите электронный адрес, на который будет отправляться отчет, после чего нажмите кнопку **ОК**. При необходимости добавьте другие адреса.
6. Поставьте флажок в строке с названием задания на панели **Задания**.
7. Нажмите кнопку **Сохранить** в панели инструментов ***«Консоли управления»***.

4.9 Журнал выполнения команд

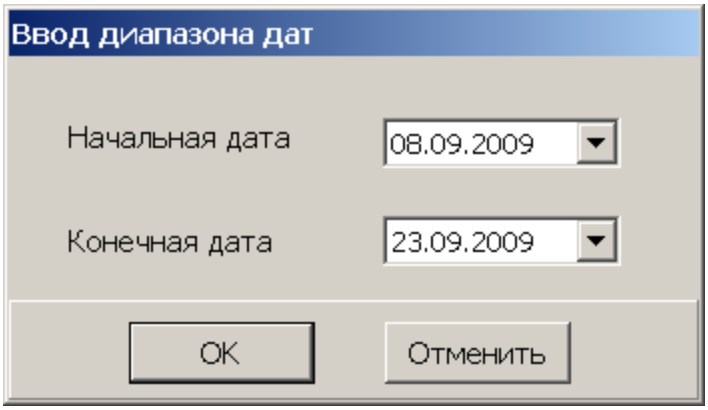
При нажатии кнопки **Журнал** на панели **Задания** рабочее окно раздела примет следующий вид:



1. Панель инструментов окна:

   Задания (**Ctrl+T**) – кнопка позволяет перейти к панели заданий.

   Удалить – кнопка позволяет удалить записи журнала заданий. При нажатии на кнопку откроется окно для установки периода времени, за который необходимо удалить записи:



   Используя поля ввода дат, установите период и нажмите кнопку **ОК**.

   Обновить – кнопка позволяет обновить данные журнала в рабочей области окна.

   Журнал с … по… – поля ввода дат позволяют установить период, за который будут отображаться данные журнала заданий в рабочей области окна. После изменения дат необходимо нажать обновить данных в рабочей области, используя кнопку **Обновить**.

2. Рабочая область. В рабочей области отображается список всех выполненных или не выполненных на данный момент команд.

Примечание:

В рабочей области реализованы функции: сортировка по элементам одного или нескольких столбцов, изменение ширины и последовательности столбцов

3. Панель дополнительных данных. На панели отображаются данные об изменении состояний устройств при выполнении команды, выбранной в рабочей области раздела.

5 Раздел «Отчет по SMS»

5.1 Назначение

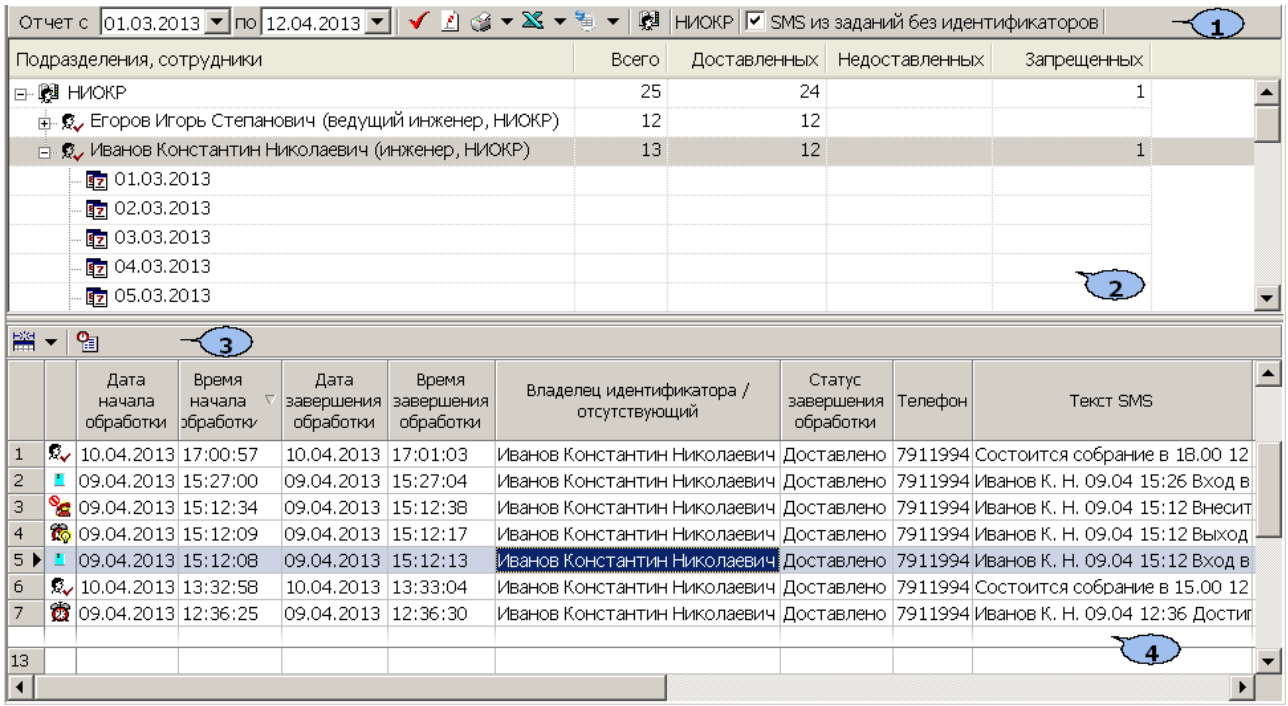
Раздел ***«Отчет по SMS»*** предназначен для просмотра и печати отчетов об отправке SMS-сообщений в процессе выполнения заданий, созданных в разделе ***«Планировщик заданий»***.

В процессе отправки SMS-сообщение может получить один из следующих статусов:

- ***Доставленное*** – сообщение, о доставке которого получено уведомление от оператора связи.
- ***Недоставленное*** – сообщение, о доставке которого не получено уведомление от оператора связи.
- ***Просроченное*** – сообщение, для которого промежуток времени между событием, послужившим причиной создания SMS-сообщения, и моментом его создания превышает время, установленное в параметре **Считать просроченными сообщения, сформированные спустя указанное время после регистрации прохода** на вкладке **Настройка SMS-рассылки** в ***«Центре управления PERCo-S-20»***. (Такая ситуация может возникнуть, например, в случае, если сервер системы был недоступен в момент предъявления идентификатора, по предъявлению которого задана отправка SMS-сообщения.)

5.2 Рабочее окно раздела

Рабочее окно раздела имеет следующий вид:



1. Панель инструментов раздела.

   Отчет с ... по... – поля ввода дат позволяют установить период отчета отображаемого в рабочей области раздела. После изменения периода отчета необходимо нажать кнопку **Обновить** для обновления данных.

   Обновить (**Ctrl+R**) – кнопка позволяет обновить данные в рабочей области.

Сокращенные ФИО – кнопка позволяет показывать фамилию, имя, отчество в сокращенном (Фамилия И.О.) или в полном варианте.

Печать – при нажатии стрелки справа от кнопки открывается меню, позволяющее выбрать один из вариантов отчета для вывода на печать:

- **Подразделения** – отчет по подразделениям;
- **Подразделенияи сотрудники**– отчет по подразделениям и входящим в них сотрудникам;
- **Все данные отчета**– детальный отчет по дням, для всех сотрудников.

Экспорт в MS Excel – при нажатии стрелки справа от кнопки открывается меню, позволяющее выбрать один из видов отчета по отправке SMS за указанный на панели инструментов период для экспорта в файл *MS Office Excel*.

- **Подразделения** – Отчет по подразделениям
- **Подразделения и сотрудники** – Отчет по подразделениям и входящим в них сотрудникам.
- **Все данные отчета** – Детальный отчет по дням, для всех сотрудников.
- **Список SMS** – Отчет для выделенного в рабочей области сотрудника или подразделения.

Экспорт в OpenOffice Calc – при нажатии стрелки справа от кнопки открывается меню, позволяющее выбрать один из видов отчета по отправке SMS за указанный на панели инструментов период для экспорта в файл *OpenOffice Calc*.

- **Подразделения** – отчет по подразделениям;
- **Подразделения и сотрудники** – отчет по подразделениям и входящим в них сотрудникам;
- **Все данные отчета** – детальный отчет по дням, для всех сотрудников;
- **Список SMS** – отчет для выделенного в рабочей области сотрудника или подразделения.

НИОКР **Выбор подразделения**(**Ctrl**+**B**) – кнопка и название выбранного подразделения.

SMS из заданий без идентификаторов – при установке флажка в рабочей области будут отображаться данные об отправке SMS-сообщений заданиями, не связанными с предъявлением идентификаторов сотрудников.

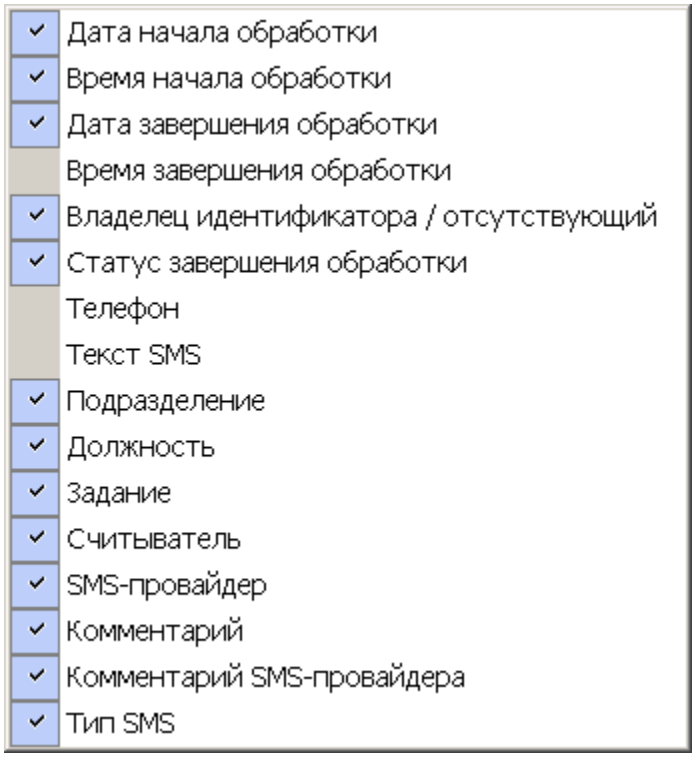
2. Рабочая область. В рабочей области в виде многоуровневого раскрывающегося списка отображаются данные об отправленных, неотправленных и просроченных SMS-сообщениях для сотрудников выбранного подразделения и всех вложенных подразделений Данные приводятся для каждого дня в установленный на панели инструментов период.
   - Красным цветом выделены сотрудники, для которых не задан номер телефонов для отправки SMS-сообщения.
   - Зеленым цветом выделены сотрудники, уволенные на момент построения отчета.

Примечание:

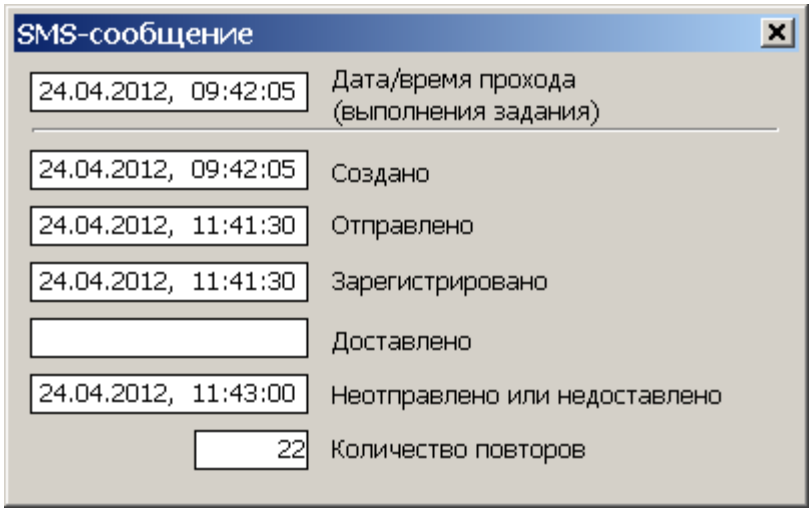
В рабочей области реализованы функции: сортировка по элементам одного или нескольких столбцов, изменение ширины и последовательности столбцов.

3. Инструменты панели дополнительных данных:

Отображение столбцов – при нажатии стрелки справа от кнопки откроется меню, позволяющее выбрать столбцы, отображаемые в рабочей области панели дополнительных данных. Отметьте флажками названия тех столбцов, которые будут отображаться на панели:



Подробно об этапах обработки (**Ctrl+L**) – кнопка позволяет открыть окно **SMS-сообщение** с подробной информацией об этапах обработки выбранного на панели дополнительных данных SMS-сообщения:



- **Дата/время прохода (выполнения задания)** – дата и время события, послужившего причиной создания SMS-сообщения.
- **Создано** – дата и время создания SMS-сообщения.
- **Отправлено** – дата и время отправки SMS-сообщения провайдеру.
- **Зарегистрировано** – дата и время получения уведомления от провайдера о регистрации SMS-сообщения.
- **Доставлено** – дата и время получения уведомления от провайдера о доставке SMS-сообщения.

- **Не отправлено или не доставлено** – дата и время последней неудачной отправки. Причина неудачной отправки отображается в столбце **Комментарий** панели дополнительных данных. Информация о причине может быть сформирована системой (например, если нет связи с провайдером) или получена от провайдера (например, если телефон абонента отключен).
- **Количество повторов** – количество попыток отправки SMS-сообщения.

Примечание:

Если SMS-сообщение не было доставлено, то система в течение 24 часов с момента создания сообщения с интервалом в 5 минут повторяет отправку.

4. Рабочая область панели дополнительных данных. На панели отображается информация о созданных SMS-сообщениях для выбранного в рабочей области сотрудника или подразделения. Значок в первом столбце указывает на раздел, в котором было создано SMS-сообщение. При наведении курсора на значок будет указан тип сообщения.

   Сообщения, созданные в процессе выполнения заданий разделом ***«Планировщик заданий»***:

   «По предъявлению идентификаторов» – сообщение создано в процессе выполнения задания **По предъявлению идентификаторов**.

   «По времени» – сообщение создано в процессе выполнения задания **По времени**.

   «По времени и достижению состояний» – сообщение создано в процессе выполнения задания **По времени и достижению состояний**.

   «По изменению состояний» – сообщение создано в процессе выполнения задания **По изменению состояний**.

   «Уведомление о неприходах» – сообщение создано в процессе выполнения задания **Отправка SMS по неприходу.**

   «Сообщение общей рассылки» – сообщение создано в разделе ***«Сотрудники и ученики»***

   «Тестовое сообщение» – отправлено при тестовой рассылке из «***Центра управления PERCo-S-20»*** при проверке связи с SMS-провайдером.

Примечание:

В рабочей области реализованы функции: сортировка по элементам одного или нескольких столбцов, изменение ширины и последовательности столбцов.

6 Состав видеоподсистемы

В состав видеоподсистемы входят следующие компоненты и программные модули, обеспечивающие работу системы с камерами наблюдения:

- ***«Центр управления видеоподсистемой»*** – компонент, предназначенный для управления сервером видеоподсистемы и файлами видеоархива.
- ***«Видеонаблюдение»*** – модуль ПО, предназначен для организации АРМ оператора видеонаблюдения. Модуль позволяет отображать в режиме реального времени видеоинформацию с камер наблюдения и просматривать видеоархив камер. Запись в формате потокового видео ведется по команде оператора или ПО.
- ***«Прозрачное здание»*** – модуль ПО, предназначен для организации АРМ оператора видеонаблюдения. Модуль позволяет отображать в режиме реального времени видеоинформацию с камер наблюдения и просматривать видеоархив камер. Запись в виде стоп-кадров с отмеченных камер ведется непрерывно.
- ***«Камера СКУД»*** – камера, установленная в точке прохода, таким образом, что в ее поле зрения попадает место предъявления карт доступа считывателю. Запись кадров с камеры производится автоматически при регистрации события, связанного с проходом (или запретом прохода) через ИУ в направлении считывателя. Запись в виде стоп-кадров с отмеченных камер ведется непрерывно.
- ***«Верификация»*** – модуль ПО, предназначен для организации АРМ оператора службы безопасности. Модуль позволяет усилить контроля доступа через точки прохода, за счет проведения оператором процедуры верификации. Видеоинформация с точек верификации поступает в формате потокового видео.

Внимание!

Список поддерживаемых видеоподсистемой камер наблюдения представлен на сайте компании ***PERCo***, по адресу www.perco.ru, в разделе **Главная> Продукция> Комплексные системы безопасности> Видеокамеры**. Для поддержки некоторых моделей камер требуется установка дополнительных драйверов.

7 Конфигурирование видеоподсистемы

Внимание!

Перед проведением конфигурации:

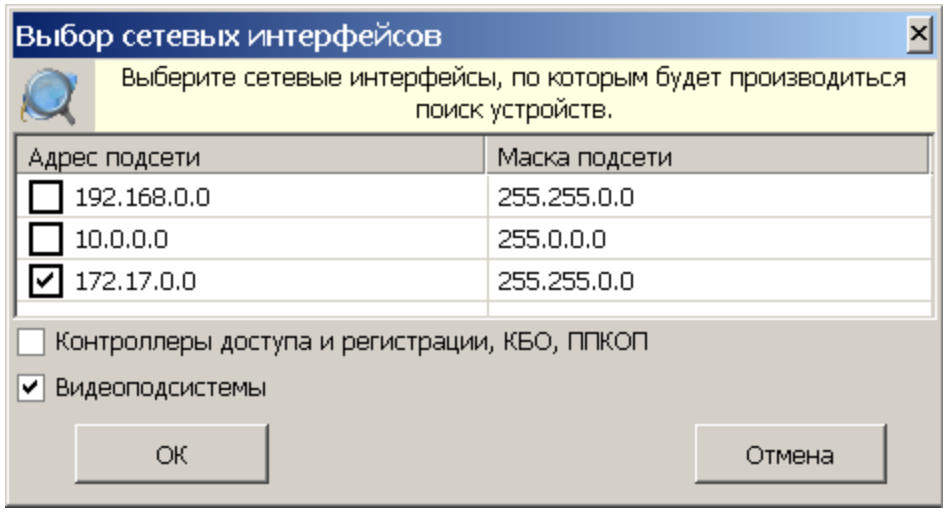
- Установите необходимые драйверы для камер.
- Убедитесь, что сервер видеоподсистемы и камеры наблюдения подключены к сети *Ethernet* и работают в штатном режиме.

При настройке видеоподсистемы придерживайтесь следующей последовательности действий:

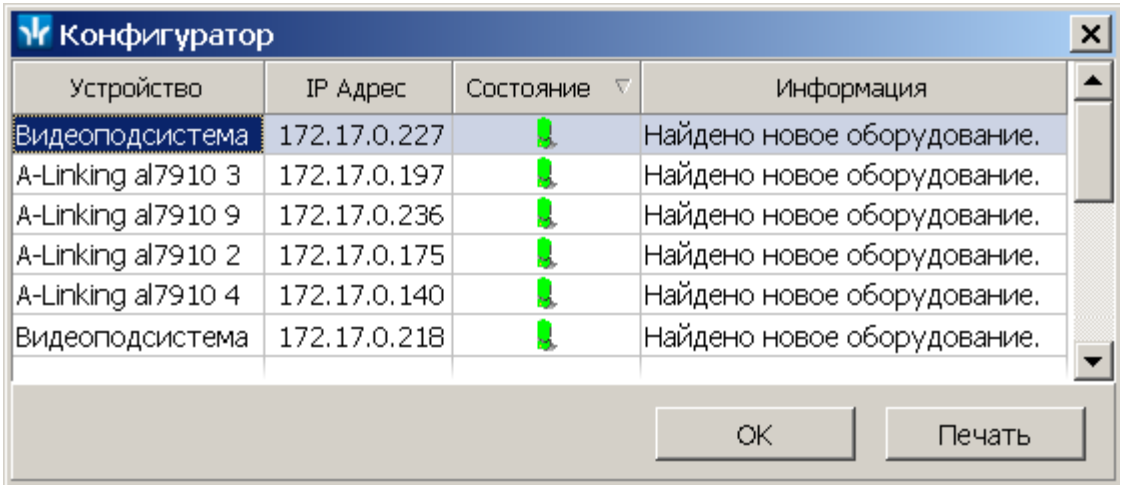
1. Убедитесь, что установлен модуль сетевого ПО: **Сервер видеоподсистемы** и запущена соответствующая служба.
2. Запустите ***«Центр управления видеоподсистемой»***, перейдите на вкладку **Видеоархив** и создайте хотя бы один файл видеоархива.
3. Запустите ***«Консоль управления»*** и перейдите в раздел ***«Конфигуратор»***.

Автоматический поиск устройств видеоподсистемы

4. Для проведения автоматического поиска в сети видеоподсистемы и камер наблюдения нажмите кнопку **Провести конфигурацию** на панели инструментов раздела. Откроется окно **Выбор сетевых интерфейсов**:



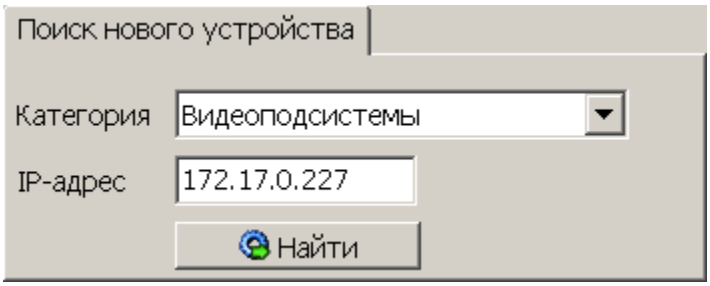
5. В открывшемся окне отметьте подсети, в которых будет произведен поиск устройств, и установите флажок **Видеоподсистемы**. Нажмите кнопку **ОК**. По окончании поиска откроется окно **Конфигуратор** со списком найденных устройств:



6. В открывшемся окне нажмите кнопку **ОК**. Все найденные устройства будут добавлены в рабочую область раздела и отмечены значками .
7. Если какое-либо из найденных устройств необходимо исключить из конфигурации, то выделите его в рабочей области и нажмите на панели инструментов раздела кнопку **Исключить из конфигурации** . Выделенное устройство будет исключено из конфигурации и отмечено значком .

Поиск видеоподсистемы по IP-адресу

8. Если видеоподсистема не была найдена при автоматическом поиске, то произведите ее поиск по IP-адресу ПК, на котором установлен модуль **Сервер видеоподсистемы**. Для этого на панели инструментов раздела нажмите кнопку **Добавить новое устройство** – . В нижней части окна откроется панель **Поиск нового устройства**:



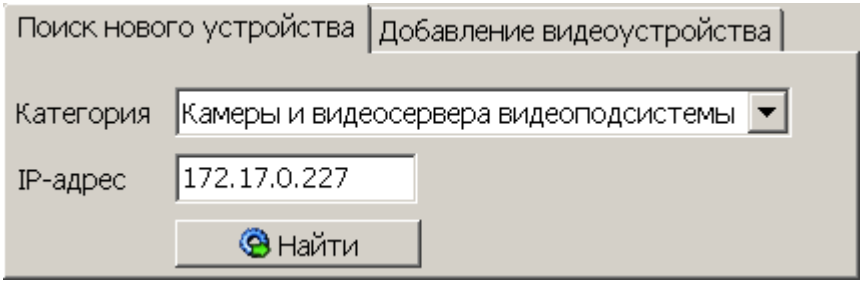
9. На открывшейся панели, в раскрывающемся списке **Категория**, выберите пункт: **Видеоподсистемы**.
10. В поле **IP-адрес** введите IP-адрес ПК, на котором установлен модуль **Сервер видеоподсистемы**. Нажмите на панели ставшую при этом активной кнопку **Поиск**.
11. По окончании поиска откроется окно **Конфигуратор** со списком найденных устройств. В открывшемся окне нажмите кнопку **ОК**. Найденная видеоподсистема будет добавлена в рабочую область раздела и отмечена значком .

Поиск камеры поддерживающих стандарт ONVIF

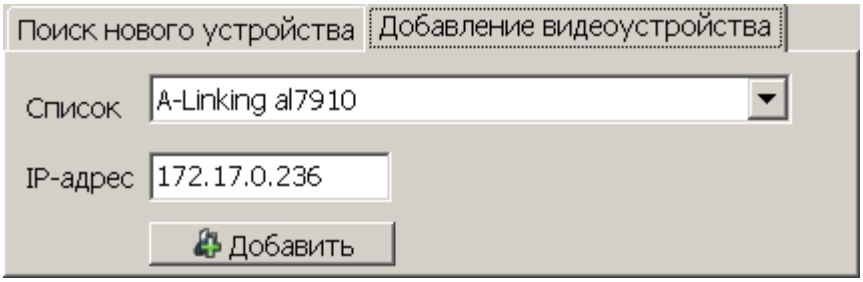
12. Если подключенные камеры поддерживают стандарт ONVIF, то произведите поиск камер поддерживающих стандарт ONVIF.

Поиск камеры по IP-адресу

13. Если камера не была найдена при автоматическом поиске, то произведите ее поиск по IP-адресу. Для этого в рабочей области раздела выделите видеоподсистему, в которую необходимо добавить камеру.
14. На панели **Поиск нового устройства** в раскрывающемся списке **Категория** выберите пункт: **Камеры и видеосервера видеоподсистемы**. Убедитесь, что в поле **IP-адрес** указан IP-адрес ПК, на котором установлен модуль **Сервер видеоподсистемы**. На панели станет доступна вкладка **Добавление видеоустройства**:



15. Перейдите на вкладку **Добавление видеоустройства**. В раскрывающемся списке **Список** выберите модель искомой видеокамеры, в поле **IP-адрес** введите ее IP-адрес. Нажмите ставшую при этом активной кнопку **Добавить**.



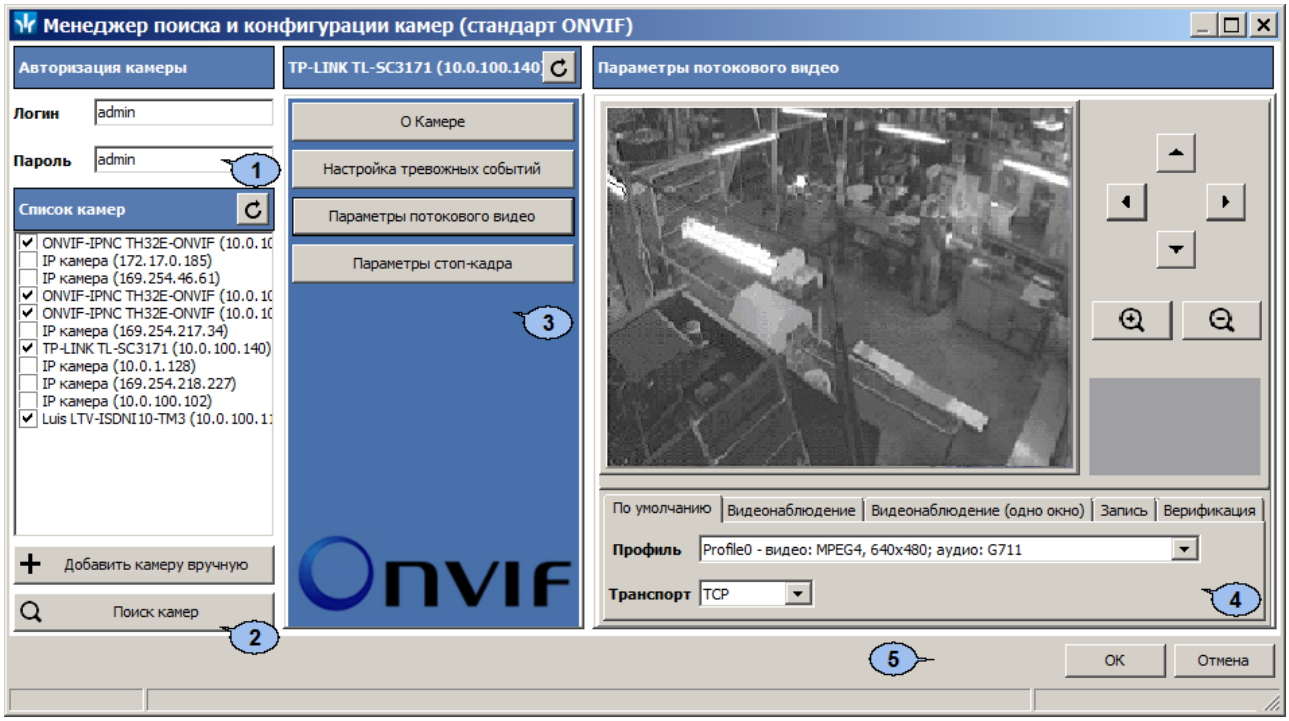
16. По окончании поиска откроется окно **Конфигуратор**. В открывшемся окне нажмите кнопку **ОК**. Найденная камера будет добавлена в рабочую область раздела и отмечена значком .

Настройка параметров видеоподсистемы

17. Произведите настройку параметров видеоподсистемы и камер. Для этого выделите устройство в рабочей области раздела и на вкладке **Параметры** панели настройки произведите необходимые изменения.
18. Для добавления найденных устройств в конфигурацию системы выделите в рабочей области раздела видеоподсистему и нажмите кнопку **Передать параметры** на панели инструментов раздела. В устройства будут переданы заданные параметры конфигурации. В случае успешной передачи параметров в устройства значки в списке объектов заменятся на значки, и соответственно для видеоподсистемы и камер.
19. При необходимости произведите настройку подсистемы ***«Камеры СКУД»***.

8 Подключение камер, поддерживающих стандарт ONVIF

Описание элементов окна «Менеджер поиска и конфигурации камер (стандарт ONVIF)»



1. Панель **Авторизация камеры** содержит поля для ввода единых логина и пароля доступа к камерам.
2. Панель **Список камер** содержит список найденных камер.

   – кнопка в заголовке панели позволяет произвести повторное подключение к найденным камерам.

   Добавить камеру вручную – кнопка позволяет произвести поиск камеры по ее IP-адресу.

   Поиск камер – кнопка позволяет заново произвести поиск камер.
3. Панель содержит следующие кнопки для выбора отображаемой в рабочей области окна информации о камере, выделенной на панели **Список камер**

   – кнопка в заголовке панели позволяет повторно подключиться к камере.

   - **О камере** – для отображения общей информации о камере
   - **Настройка тревожных событий** – для выбора событий, передаваемых камерой, регистрация которых соответствует регистрации события *«Тревога»* в системе.
   - **Параметры потокового видео** – для настройки потокового видео с камеры. Доступны следующие инструменты:
     - Видеоокно для просмотра видеоизображения с камеры в режиме реального времени;
     - **Профиль** – раскрывающийся список для выбора алгоритма сжатия (видеокодека) и размера изображения потокового видео с камеры;
     - **Транспорт** – раскрывающийся список выбора протокола передачи потокового видео;

- Для PTZ-камер, поддерживающих удаленное управление, доступны кнопки управления ориентацией и зумом камеры, а так же поле для выбора направления камеры.

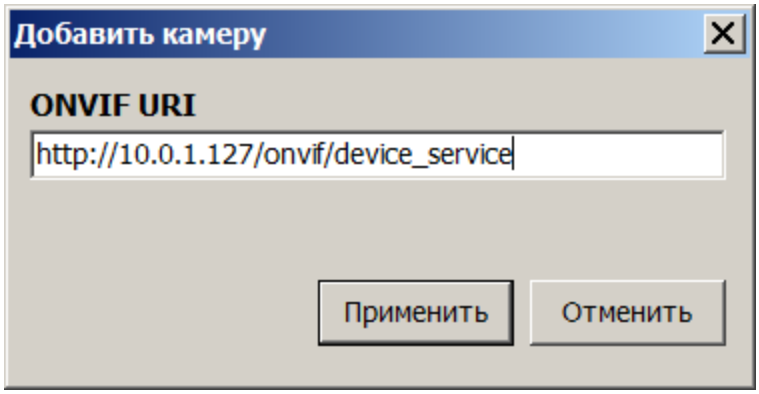
- **Параметры стоп-кадра** – для настройки профиля стоп кадр.

4. Рабочая область окна.
5. Кнопки **ОК** и **Отмена** позволяют закрыть окно. При нажатии кнопки **ОК** отмеченные камеры будут добавлены в конфигурацию подсистемы.

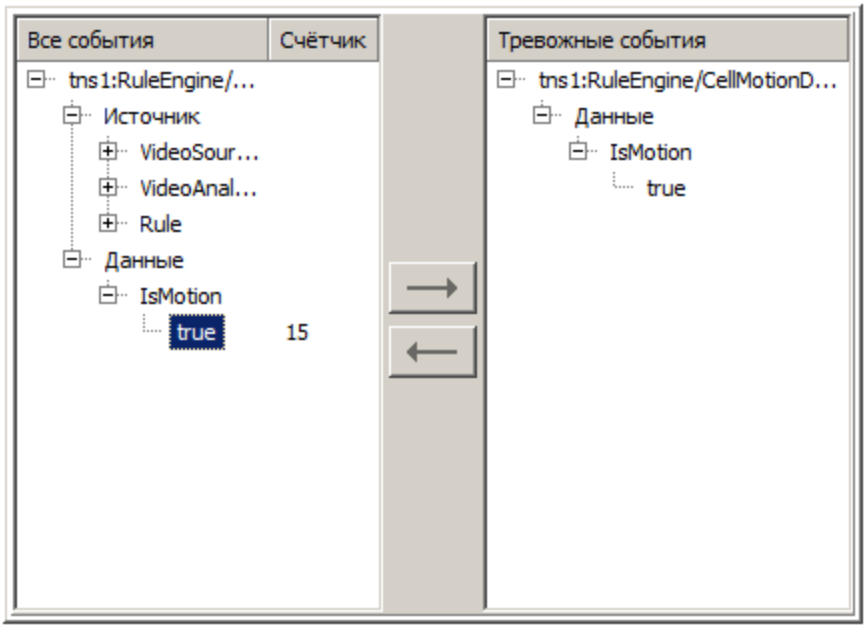
Порядок поиска камер поддерживающих стандарт ONVIF

Для поиска камер, поддерживающих стандарт ONVIF:

1. Запустите ***«Консоль управления»*** и перейдите в раздел ***«Конфигуратор»***.
2. На панели инструментов раздела нажмите кнопку **Добавить новое устройство** –  . В нижней части окна откроется панель **Поиск нового устройства**
3. На открывшейся панели в раскрывающемся списке **Категория** выберите пункт **Камеры стандарта ONVIF видеоподсистемы**. Убедитесь, что в поле **IP-адрес** указан IP-адрес ПК, на котором установлен модуль **Сервер видеоподсистемы**. Нажмите кнопку **Поиск**. Откроется окно **Менеджер поиска и конфигурации камер (стандарт ONVIF)**:
4. Автоматически будет запущен процесс поиска камер, по окончании которого в открывшемся окне на панели **Список камер** появится список найденных камер. Обратите внимание, что камеры, добавленные ранее в конфигурацию видеоподсистемы в списке не отображаются. Камеры для которых подходит логин и пароль доступа, указанные на панели **Авторизация камеры**, отмечаются флажками, то есть происходит автоматическая авторизация.
5. Если камера была найдена, но автоматическая авторизация не произошла, то выделите эту камеру на панели **Список камер**; на панели **Авторизация камеры** введите верные логин и пароль доступа к камере, после чего нажмите кнопку  в заголовке панели **Список камер**.
6. Если камера не была найдена автоматически, то для поиска по IP-адресу нажмите кнопку **Добавить камеру вручную**. Откроется окно **Добавить камеру**:



7. В открывшемся окне укажите IP-адрес искомой камеры и нажмите кнопку **Применить**. Окно **Добавить камеру** будет закрыто, начнется процесс поиска камеры. Найденная камера будет добавлена в список на панели **Список камер**.
8. При необходимости для выбора тревожных событий нажмите кнопку **Настройка тревожных событий**. Рабочая область окна примет следующий вид:



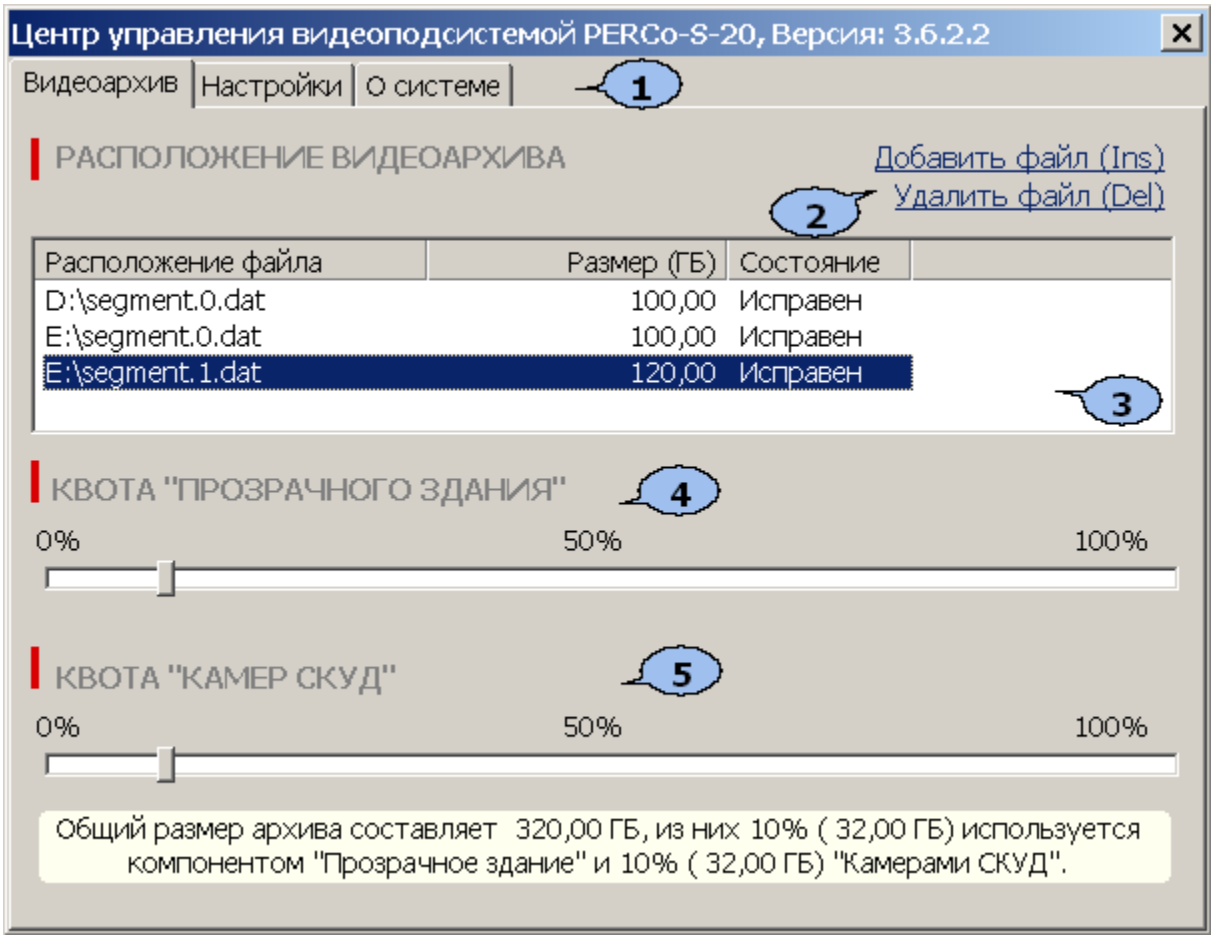
9. В левой части рабочей области отображается список событий регистрируемых камерой. Наличие, перечень и описание событий зависит от модели камеры. Используя кнопу  добавьте необходимые события камеры в тревожные события. Для удаления события используйте кнопку  .
10. Для настройки параметров потокового видео нажмите кнопку **Параметры потокового видео**, после чего с помощью соответствующего раскрывающегося списка выбери профиль и протокол.
11. Для настройки параметров стоп-кадра нажмите кнопку **Параметры стоп-кадра**, после чего с помощью соответствующего раскрывающегося списка выбери профиль.
12. Для добавления камер, отмеченных флажками на панели **Список камер**, в конфигурацию видеоподсистемы нажмите кнопку **ОК** в нижней части окна. Окно **Менеджер поиска и конфигурации камер (стандарт ONVIF)** будет закрыто.
13. Откроется окно **Конфигуратор** со списком найденных камер. В открывшемся окне нажмите кнопку **ОК**. Найденные камеры будут добавлены конфигурацию видеоподсистемы в рабочей области раздела и отмечены значком  .
14. Произведите настройку параметров камер. Для этого выделите одну из найденных камер в рабочей области раздела после чего на вкладке **Параметры** панели настройки произведите необходимые изменения.
15. Для добавления камер в конфигурацию системы выделите в рабочей области раздела видеоподсистему в которую добавлены камеры и нажмите на панели инструментов раздела кнопку **Передать параметры** –  . В камеры будут переданы новые параметры конфигурации. В случае успешной передачи параметров значки  в списке объектов заменятся на значки  камер.

9 «Центр управления видеоподсистемой»

9.1 Вкладка «Видеоархив»

9.1.1 Рабочее окно вкладки

Вкладка **Видеоархив** предназначена для создания и удаления файлов видеоархива. Одновременно может быть создано несколько файлов видеоархива, расположенных на одном или разных логических дисках ПК. Вкладка имеет следующий вид:



1. Выбор вкладки окна:
   - **Видеоархив**
   - **Настройки**
   - **О системе**
2. Панель инструментов вкладки:
   Добавить файл (**Ins**) – кнопка позволяет добавить новый файл видеоархива.
   Удалить файл (**Del**) – позволяет удалить выделенный в рабочей области вкладки файл видеоархива.

Примечание:

Объем файла видеоархива выделяется для записи с камер видеонаблюдения. Запись ведется только по команде оператора или ПО. Из этого объема выделяется квота на запись камер СКУД и квота на запись камер прозрачного здания.

3. Рабочая область вкладки содержит список созданных ранее файлов видеоархивов с указанием их расположения, размера и состояния.

4. Ползунок **Квота «Прозрачного здания»** предназначен для указания части файла видеоархива, которая будет зарезервирована для записи кадров с камер ***«Прозрачное здание»***.
5. Ползунок **Квота «Камер СКУД»** предназначен для указания части видеоархива, которая будет зарезервирована для записи видеоинформации с камеры СКУД.

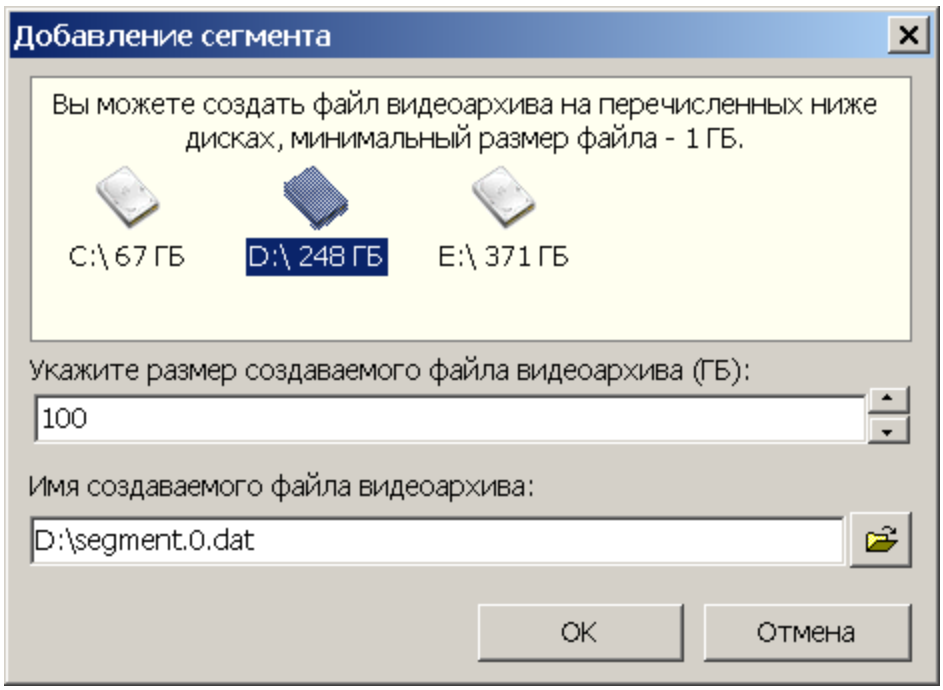
Внимание!

Видеоархив имеет циклическую структуру. При заполнении выделенного объема старая информация стирается и автоматически заменяться новой!

9.1.2 Создание видеоархива

Для создания нового файла видеоархива:

1. Запустите ***«Центр управления видеоподсистемой»*** и перейдите на вкладку **Видеоархив**.
2. Нажмите кнопку **Добавить файл** на панели инструментов вкладки. Откроется окно **Добавление сегмента**:

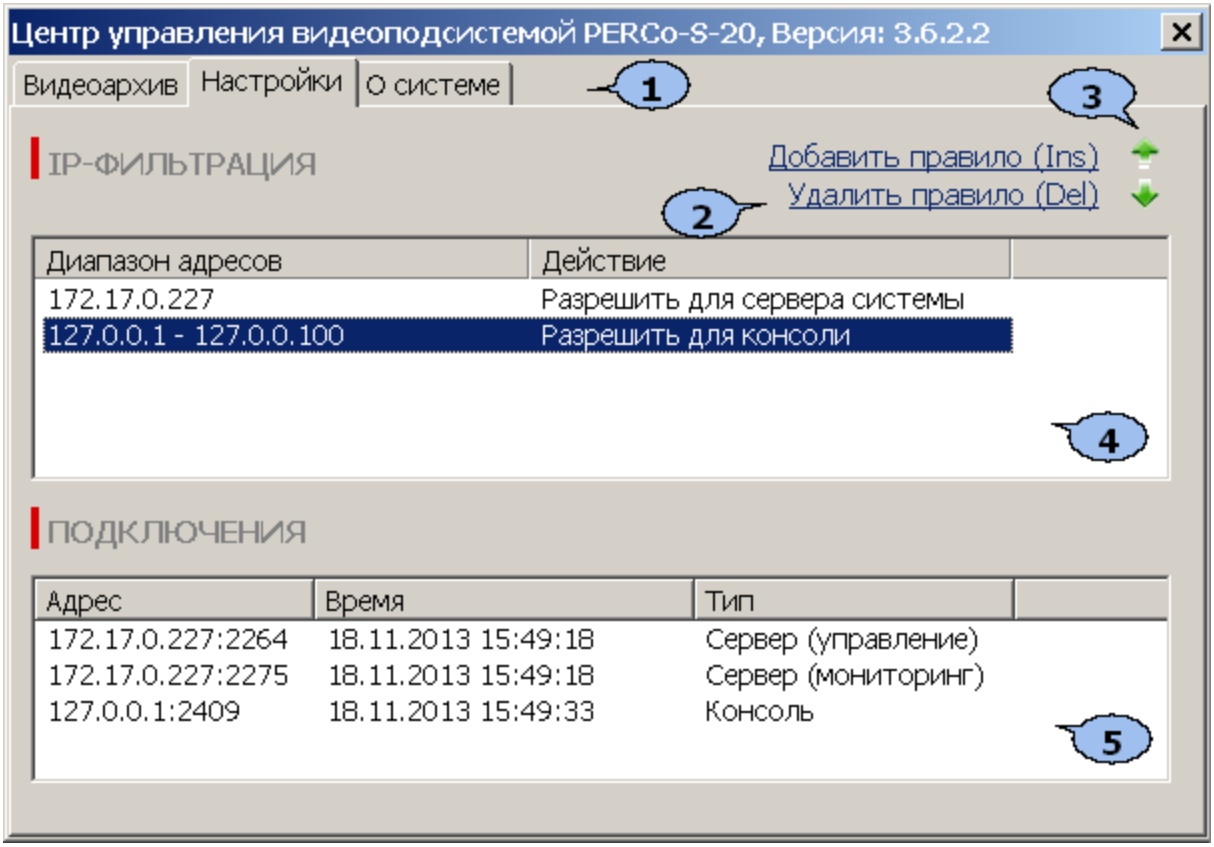


3. В открывшемся окне выделите название логического диска ПК, на котором будет создан файл видеоархива.
4. С помощью соответствующего счетчика укажите размер создаваемого файла видеоархива.
5. При необходимости измените имя файла видеоархива и его расположение (по умолчанию файл видеоархива `segment0.dat` располагается в корневом каталоге указанного диска).
6. Нажмите кнопку **ОК**. Окно **Добавление сегмента** будет закрыто. Файл видеоархива будет добавлен в список в рабочей области вкладки **Видеоархив**.
7. Для удаления файла видеоархива выделите его в рабочей области вкладки **Видеоархив**, и нажмите кнопку **Удалить файл**. В появившемся диалоговом окне подтвердите удаление.
8. Закройте ***«Центр управления видеоподсистемой»***, нажав кнопку **Закрыть** в строке заголовка окна.

9.2 Вкладка «Настройки»

9.2.1 Рабочее окно вкладки

Вкладка **Настройка** предназначена для настройки фильтра подключений к серверу видеоподсистемы и отслеживания текущих подключений. Вкладка имеет следующий вид:



1. Выбор вкладки окна:
   - **Видеоархив**
   - **Настройки**
   - **О системе**
2. Панель инструментов вкладки
   Добавить правило (**Ins**) – кнопка позволяет добавить фильтр IP-адресов.
   Удалить правило (**Del**) – кнопка позволяет удалить выделенный в рабочей области вкладки фильтр IP-адресов.
3. Кнопки предназначены для перемещения выделенного в рабочей области вкладки фильтра IP-адресов вверх и вниз в списке. Фильтры применяются последовательно сверху-вниз.
4. Рабочая область вкладки содержит список созданных ранее фильтров IP-адресов. Для изменения настроек фильтра дважды нажмите на него левой кнопкой мыши и в открывшемся окне **Правило фильтрации** измените необходимые настройки.
5. Панель **Подключения** содержит список поддерживаемых сервером видеоподсистемы подключений в настоящий момент времени.

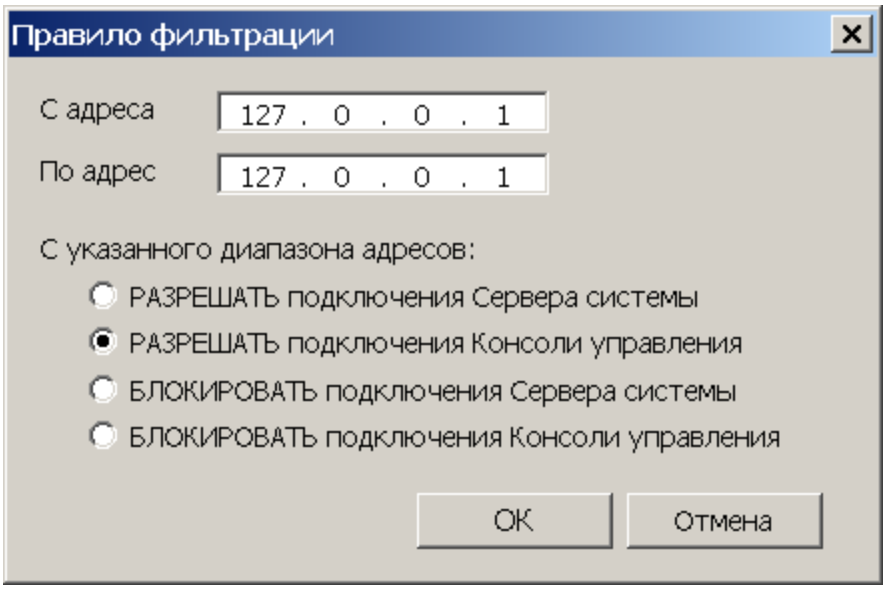
9.2.2 Настройка IP-фильтра

Возможно создание фильтров, используя следующие правила фильтрации:

- **РАЗРЕШАТЬ подключения Сервера системы**
- **РАЗРЕШАТЬ подключения Консоли управления**
- **БЛОКИРОВАТЬ подключения Сервера системы**
- **БЛОКИРОВАТЬ подключения Консоли управления**

Для добавления фильтра IP-адресов:

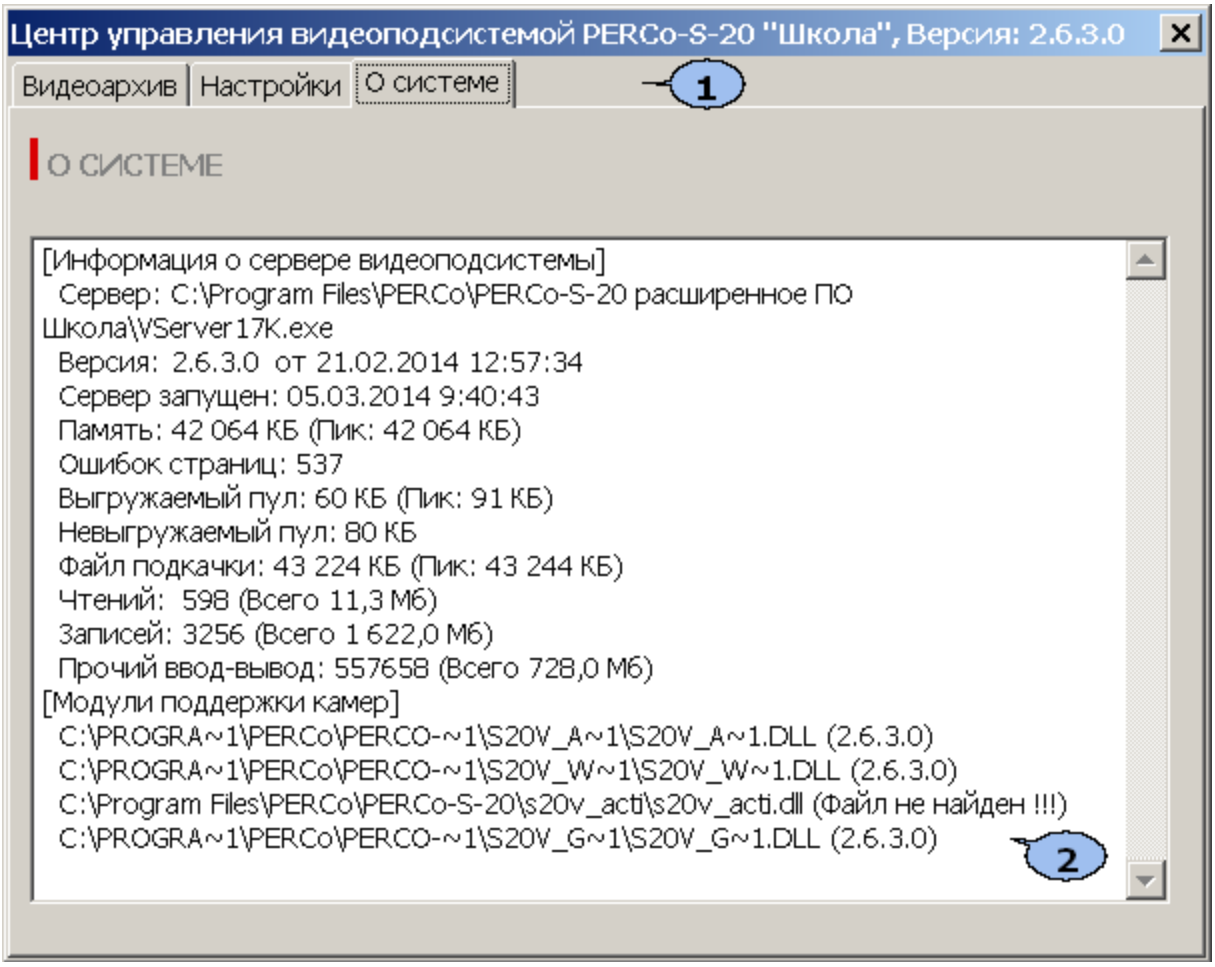
1. Запустите ***«Центр управления видеоподсистемой»*** и перейдите на вкладку **Настройки**.
2. Нажмите кнопку **Добавить правило** на панели инструментов вкладки. Откроется окно **Правило фильтрации**:



3. В открывшемся окне с помощью переключателя выберите одно из правил фильтрации.
4. С помощью полей **С адреса… По адрес** укажите диапазон PI-адресов (или один адрес) к которым выбранное правило фильтрации будет применяться.
5. Нажмите кнопку **ОК**. Окно **Правило фильтрации** будет закрыто. Новый фильтр будет добавлен в рабочую область вкладки **Настройки**.
6. При необходимости добавьте другие фильтры.
7. С помощью кнопок вверх и вниз на панели инструментов вкладки установите порядок применения фильтров.
8. Для изменения созданного ранее фильтра дважды нажмите на него левой кнопкой мыши в рабочей области вкладки. В открывшемся окне **Правило фильтрации** произведите необходимые изменения и нажмите кнопку **ОК**. Окно будет закрыто.
9. Для удаления созданного ранее фильтра выделите его в рабочей области вкладки и нажмите кнопку **Удалить правило** на панели инструментов вкладки.
10. Закройте ***«Центр управления видеоподсистемой»***, нажав кнопку **Закрыть** в строке заголовка окна.

9.3 Вкладка «О системе»

Вкладка **О системе** содержит информацию о сервере видеоподсистемы и установленных модулях поддержки (драйверах) камер. Сервер видеоподсистемы запускается автоматически при загрузке ОС. При работе сервера запускается служба *«.Сервер видеоподсистемы PERCo-S-20»*. Вкладка имеет следующий вид:



1. Выбор вкладки окна:
   - **Видеоархив**
   - **Настройки**
   - **О системе**
2. Рабочая область вкладки

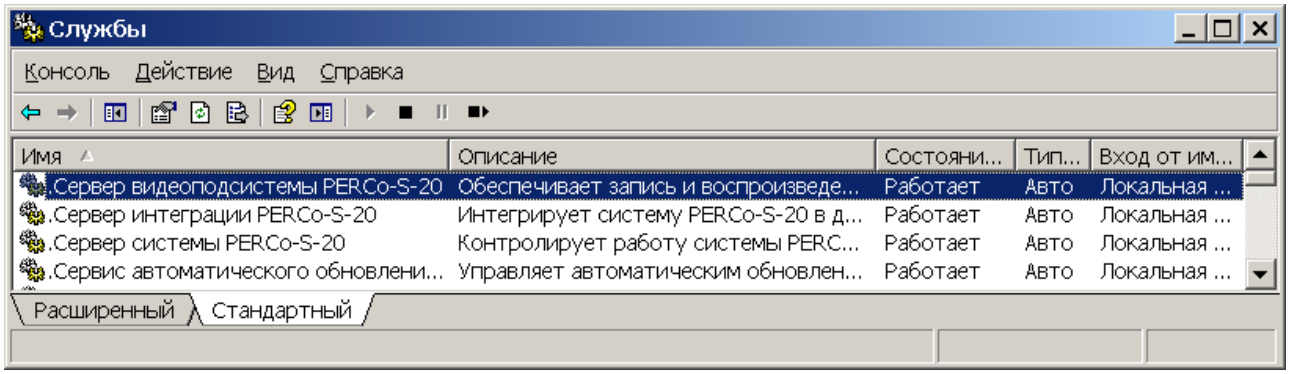
10 Установка драйвера видеокамеры

Внимание!

Список поддерживаемых видеоподсистемой камер наблюдения представлен на сайте компании ***PERCo***, по адресу www.perco.ru, в разделе **Главная> Продукция> Комплексные системы безопасности> Видеокамеры**. Для поддержки некоторых моделей камер требуется установка дополнительных драйверов.

Для установки драйвера видеокамеры:

1. Перед установкой драйвера камеры необходимо остановить сервер видеоподсистемы. Для этого нажмите последовательно: **Пуск> Настройка> Панель управления**, затем **Администрирование> Службы**. Откроется окно **Службы**:



2. В открывшемся окне выделите строку: *«.Сервер видеоподсистемы PERCo-S-20».*
3. Нажмите в выделенной строке правой кнопкой мыши и в открывшемся меню выберите пункт **Стоп**. Или нажмите кнопку **Остановить службу** ■ на панели инструментов окна.
4. Сервер видеоподсистемы будет остановлен. Статус **Работает** в столбце **Состояние** исчезнет.
5. Установите драйвер для используемой модели камеры. Для этого распакуйте архив, загруженный с сайта компании ***PERCo,*** и запустите исполняемый файл. Следуйте указаниям мастера установки.
6. После окончания установки заново запустите сервер видеоподсистемы. Для этого в окне **Службы** выделите строку, *«.Сервер видеоподсистемы PERCo-S-20»* и нажмите на него правой кнопкой мыши и в открывшемся меню выберите пункт **Пуск**. Или нажмите кнопку **Запуск службы** ▶ на панели инструментов окна.
7. Сервер видеоподсистемы будет запущен. В столбце **Состояние** появится статус **Работает**.
8. Запустите ***«Консоль управления»***, перейдите в раздел ***«Конфигуратор»*** и добавьте камеру в видеоподсистему.

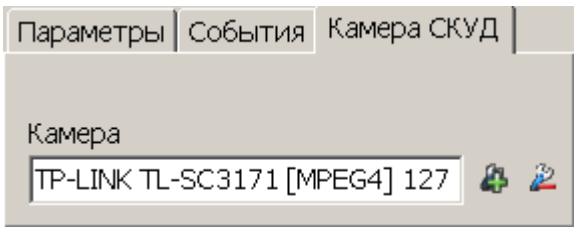
11 «Камеры СКУД»

Камера СКУД – камера, установленная в точке прохода таким образом, что в поле зрения камеры попадает место предъявления карт доступа считывателю. Запись кадров с камеры производится автоматически при регистрации события, связанного с проходом (или запретом прохода) через ИУ в направлении контролируемом считывателем.

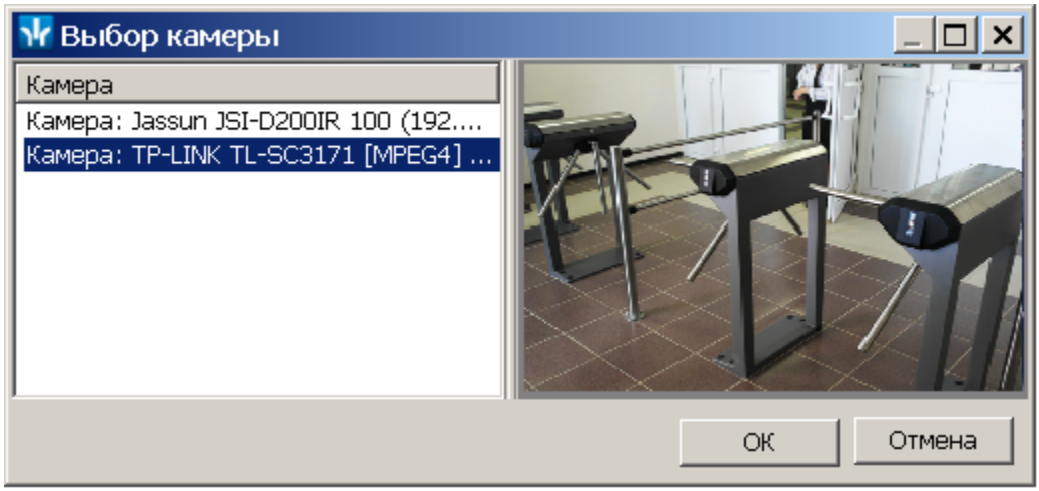
С любым считывателем, подключенным к одному из контроллеров, системы можно связать одну из камер видеоподсистемы. При этом одна камера одновременно может быть связана с несколькими считывателями.

Настройка камеры СКУД:

1. Запустите ***«Центр управления видеоподсистемой»*** и перейдите на вкладку **Видеоархив**.
2. Убедитесь, что создан хотя бы один файл видеоархива. Укажите с помощью ползунка **Квота «Камер СКУД»**, какая часть файла видеоархива будет зарезервирована для записи кадров с камеры СКУД.
3. Запустите ***«Консоль управления»*** и перейдите в раздел ***«Конфигуратор»***.
4. Выделите в рабочей области раздела один из считывателей системы, на котором будут регистрироваться события, приводящие к началу записи.
5. На панели настроек в правой части окна перейдите на вкладку **Камера СКУД**.



6. Нажмите на панели настроек кнопку **Добавить камеру**. Откроется окно **Выбор камеры**.



7. Выделите в рабочей области открывшегося окна камеру, с которой будет производиться запись при регистрации событий прохода, связанных с данным считывателем. При этом в правой части окна будут отображаться кадры с камеры. Нажмите кнопку **ОК**. Окно будет закрыто. В поле **Камера** на панели настроек появится название выбранной камеры.
8. При необходимости выберите камеры для других считывателей системы.
9. Выделите в рабочей области раздела используемую видеоподсистему и перейдите на панели настроек в правой части окна на вкладку **Параметры**.

10. Установите необходимое значение параметра **Частота кадров при записи для «Камер СКУД»** (рекомендованное значение 240 кадров в минуту).
11. Выделите в рабочей области раздела, камеру видеоподсистемы, используемую как камера СКУД.
12. На панели настроек в правой части окна убедитесь, что для камеры установлен флажок у параметра **Использовать, как камеру СКУД**.
13. Установите необходимое значение параметра **Время предзаписи для камеры СКУД**. Параметр указывает время записи до и после регистрации события (значение по умолчанию 3 секунды, то есть в видеоархиве будут сохранены кадры с камеры за 3 секунды до регистрации события и 3 секунды после).
14. Нажмите кнопку **Передать измененные параметры** на панели инструментов раздела.
15. Для просмотра записанного видеоархива, связанного с зарегистрированным событием перейдите в раздел ***«События устройств и действия пользователей»***.
16. Выделите в рабочей области раздела событие и нажмите на панели инструментов кнопку **Просмотр видеоархива**. Откроется окно **Видеоархив**.

12 Прозрачное здание - Web-доступ

12.1 Параметры

Примечание:

Для работы web-доступа ***«Прозрачное здание»*** в системе должны быть установлены:

- модуль **Web-доступ прозрачного здания** или настроен внешний web-сервер,
- **Сервер видеоподсистемы**,
- модуль ***PERCo-SM01 «Администратор»***.

Для работы web-доступа ***«Прозрачное здание»*** необходим web-сервер с интерпретатором *PHP* и поддержкой *SSL*. Так же необходимо обеспечить связь web-сервера с сервером системы.

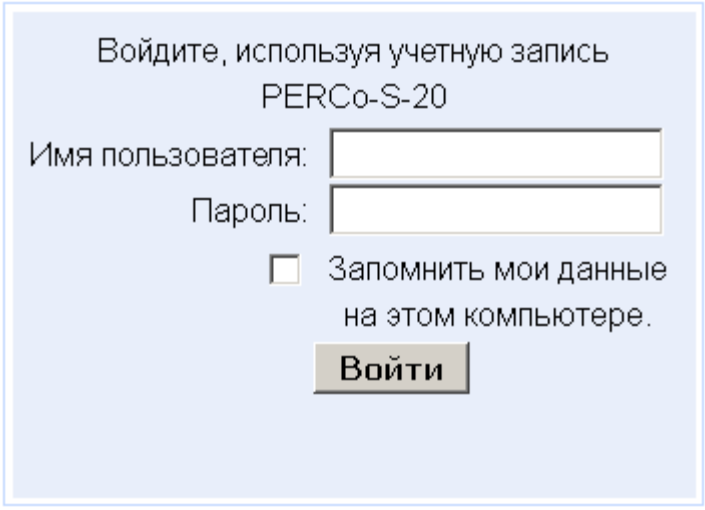
- Web-сервер может быть интегрированный установлен на одном из ПК, входящих в систему. Сервер в этом случае устанавливается вместе с модулем **Web-доступ прозрачногоздания** из установочного файла сетевого ПО системы и запускается автоматически при загрузке ОС.
- Может использоваться внешний web-сервер установленный на ПК не входящем в систему. Работа web-доступа в этом случае реализуется с помощью скриптов PHP размещенных на этом сервере. Процедура установки web-сервера *Apache* с поддержкой *PHP* и размещение на нем скриптов web-доступа описана ниже.

Для перехода на страницу настройки параметров web-доступа ***«Прозрачное здание»:***

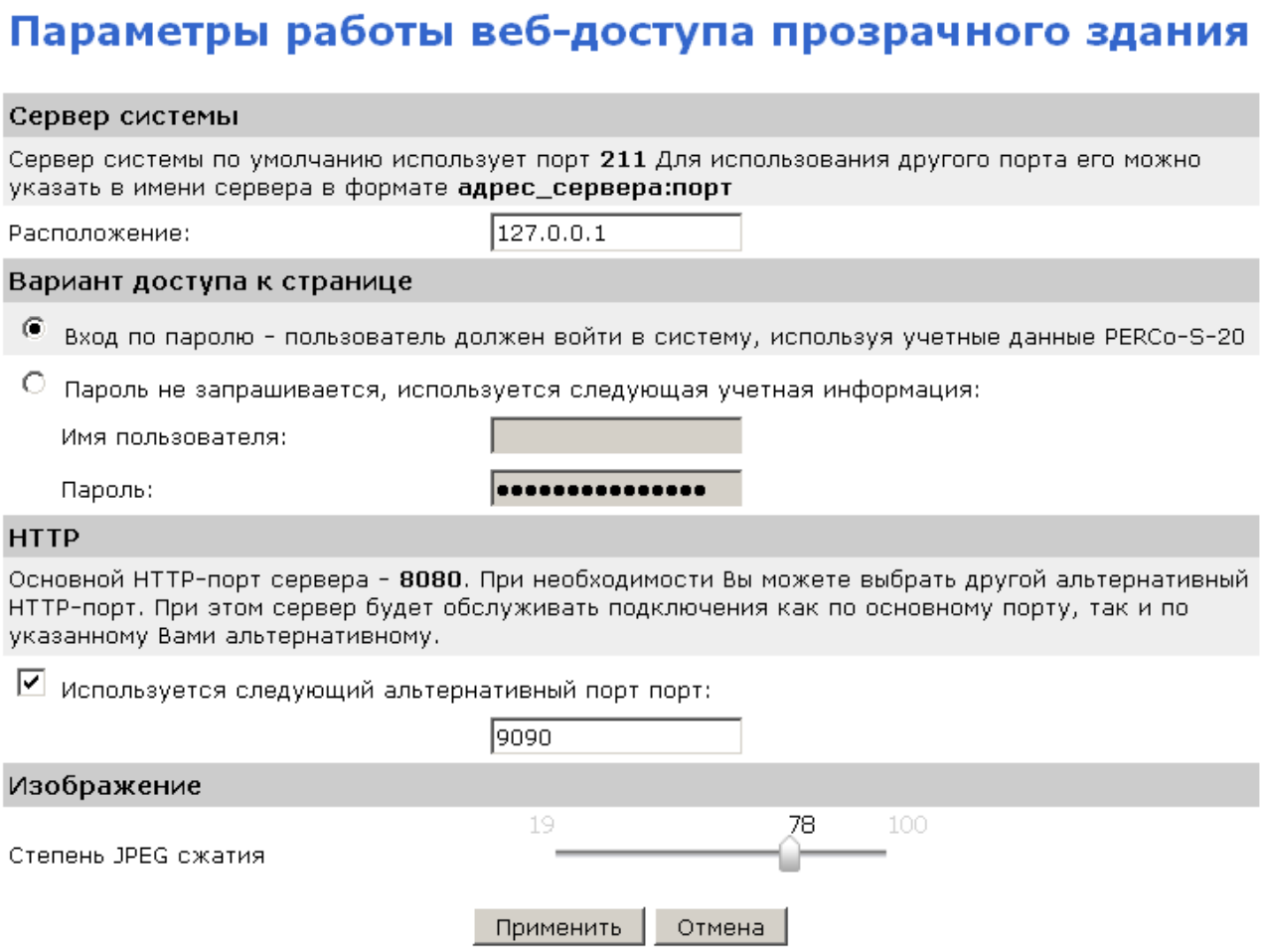
Введите в адресной строке браузера (например *Internet Explorer*) адрес: `http://x.x.x.x:8080/admin.html`, где `x.x.x.x` IP-адрес web-сервера.

Если web-сервер установлен на том же ПК, с которого осуществляется доступ, то выполните одно из следующих действий:

- Выберите последовательно: **Пуск > Программы > PERCo > PERCo-S-20 > PERCo > Настройка WEB-доступа для прозрачного здания**.
- Введите в адресной строке браузера (например *Internet Explorer*): `http://localhost:8080/admin.html`.



Откроется страница **Параметры работы веб-доступа прозрачного здания**:



На странице доступны следующие вкладки:

- **Установка** – содержит рекомендации по установке и настройке web-доступа ***«Прозрачное здание»***. На вкладке размещены ссылка на инструкцию по установке web-сервера *Apache* с поддержкой *PHP* и размещение на нем скриптов web-доступа а так же ссылка на архив со скриптами *php*.
- **Параметры** – содержит параметры настройки web-сервера и web-доступа ***«Прозрачное здание»***.
- **Статистика** – содержит статистику работы web-доступа ***«Прозрачное здание»*** через web-интерфейс.

12.2 Инструкция по установке на Apache/PHP

Примечание:

Ссылки на архив скриптов для web-доступа и инструкцию по установке и настройке так же доступны на вкладке **Установка**. После загрузки необходимо вручную распаковать содержимое этого архива в папку хранения интернет файлов web-сервера.

Инструкция по установке на Apache/PHP

Для работы web-доступа ***«Прозрачное здание»*** необходим web-сервер с интерпретатором PHP и поддержкой SSL (Apache IIS). Тестирование работы производилось на web-сервере Apache 2.2.11 с openSSL - 0.9.8 php 5.2.6.

1. Установите сервер.
2. Установите поддержку PHP.
3. Создайте сертификат для SSL.

4. Скопируйте файлы веб-доступа в папку хранения интернет файлов вебсервера (для Apache - `htdocs`)
5. Пропишите в файл `config.cfg` - адрес сервера системы PERCo-S-20. Адрес необходимо вводить без пробелов и отступов.
6. Перезапустите сервер.

Использование нестандартный порта для SSL или HTTP

Если вы используете нестандартный порт для SSL или HTTP, то вам необходимо явно указывать порт для редиректа между страницами.

Например (если порт SSL: 447) В файле `index.html` необходимо заменить строку:

```
self.location.href="https://" + document.location.host +
"/html/enter.html";
```

на

```
self.location.href="https://" + document.location.host +
":447/html/enter.html";
```

и в файле `main.html`

```
self.location.href="https://"+ document.location.host+ "/
html/enter.html";
```

на

```
self.location.href="https://" + document.location.host +
":447/html/enter.html";
```

Для обратного перехода (если порт для HTTP: 80) в файле `enter.html` необходимо заменить строку:

```
self.location.href="http://" + document.location.host +
"/html/main.html";
```

на

```
self.location.href="http://" + document.location.host +
":80/html/main.html";
```

Даже если у вас какой то один из портов нестандартный править нужно во всех местах , поскольку *Apache* не редиректит на порт по умолчанию . Если же порты стандартные - ничего трогать не надо.

Защита сервера при помощи SSL

Создание сертификата (эта информация взята из инструкции по установке *TortoiseSVN*, поэтому, если ваш администратор может сам настроить SSL, можно это не читать . Или если у вас возникли проблемы с настройкой SSL обращайтесь либо к своему системному администратору, либо приглашайте специалиста по настройке веб сервера)

Хотя в *Apache 2.2.x* и есть поддержка *OpenSSL*, по умолчанию она отключена. Вам необходимо включить её вручную.

1. В файле конфигурации Apache разкомментируйте строки:

   ```
   #LoadModule ssl_module modules/mod_ssl.so
   ```

   и в конце

   ```
   #Include conf/extra/httpd-ssl.conf
   ```

   после чего измените строку

   ```
   SSLMutex "file:C:/Program Files/Apache Software
   Foundation/\Apache2.2/logs/ssl_mutex"
   ```

   на

   ```
   SSLMutex default
   ```

2. Далее вам надо создать сертификат SSL. Для этого откройте командную строку (окно эмуляции DOS) и перейдите в папку Apache (например, `C:\program files\apache group\apache2`) и введите следующую команду:

   ```
   bin\openssl req -config bin\openssl.cnf -new -out my-server.csr
   ```

   (эта строка у меня не срабатывала - я переходил сразу к следующей /прим. автора/)

   У вас будет запрошена парольная фраза. Пожалуйста, не используйте просто слова, используйте целые предложения, например, часть стихотворения. Чем длиннее фраза, тем лучше. Ещё вам надо будет ввести URL вашего сервера. Все другие вопросы необязательны, но я рекомендую ответить и на них. Обычно файл `privkey.pem` создаётся автоматически, но если этого не произошло, вам надо ввести эту команду для его генерации:

   ```
   bin\openssl genrsa -out conf\privkey.pem 2048
   ```

   Потом введите команды:

   ```
   bin\openssl rsa -in conf\privkey.pem -out conf\server.key
   ```

   и (одной строкой):

   ```
   bin\openssl req -new -key conf\server.key -out conf\server.csr -config conf\openssl.cnf потом (одной строкой)
   bin\openssl x509 -in conf\server.csr -out conf\server.crt -req -signkey conf\server.key -days 4000
   ```

   Это создаст сертификат со сроком действия в 4000 дней. И, наконец, введите (одной строкой):

   ```
   bin\openssl x509 -in conf\server.cert -out conf\server.der.crt -outform DER
   ```

   Эти команды создали несколько файлов в папке conf Apache (`server.der.crt`, `server.csr`, `server.key`, `.rnd`, `privkey.pem`, `server.cert`).

3. Перезапустите службу *Apache*.

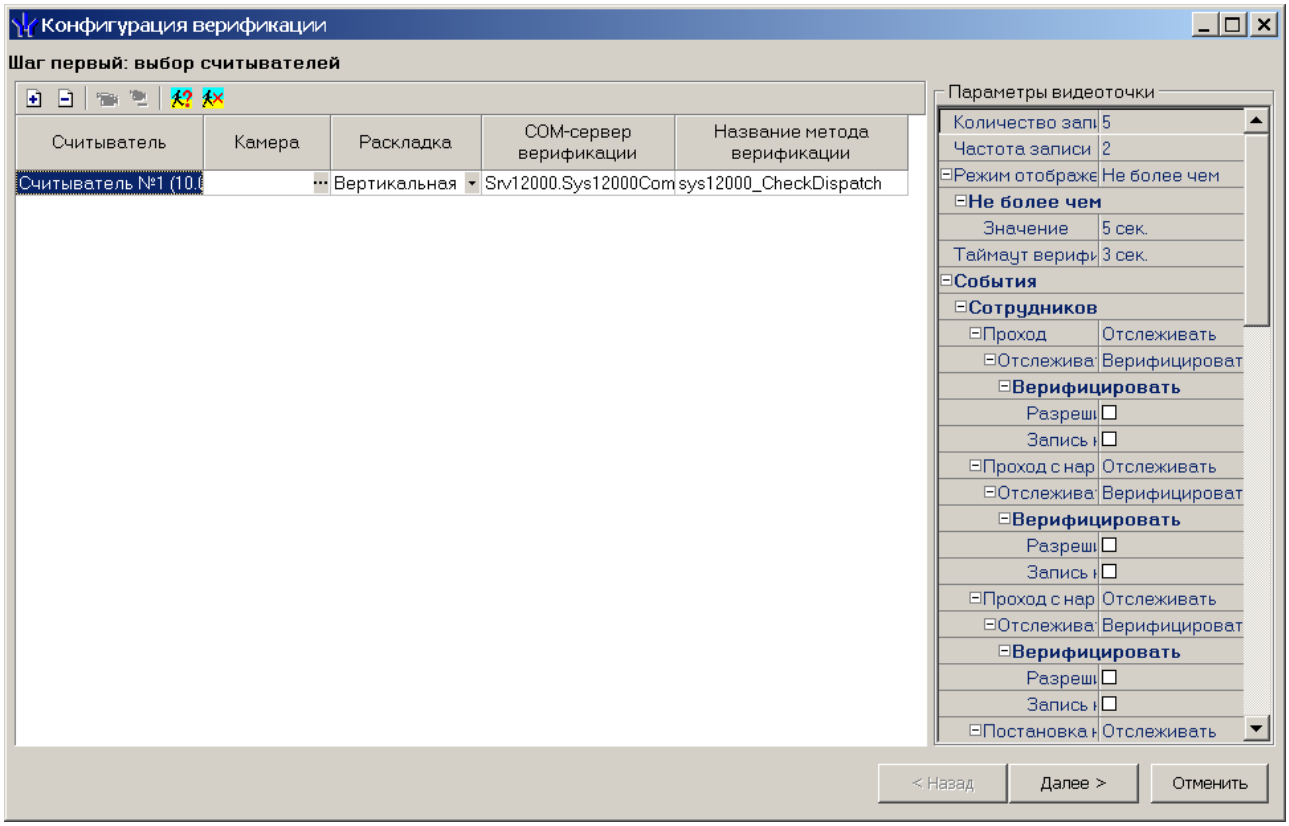
13 Внешняя программа верификации

13.1 Регистрация программы

В разделе ***«Верификация»*** модуля ***PERCo-SM09 «Верификация»*** реализована возможность использование внешней программы верификации (далее – ВПВ). При использовании ВПВ оператору ***PERCo-S-20*** недоступны штатные средства реагирования на запрос (кнопки *РАЗРЕШИТЬ/ЗАПРЕТИТЬ*). Регистрация ВПВ производится на уровне точки верификации в процессе ее конфигурации.

Регистрация ВПВ

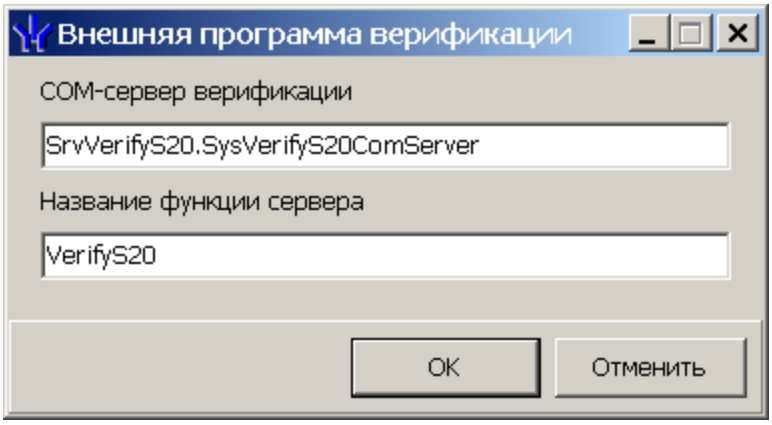
Регистрации и дерегистрация ВПВ производится при конфигурации точки верификацией в окне **Конфигурация верификации**:



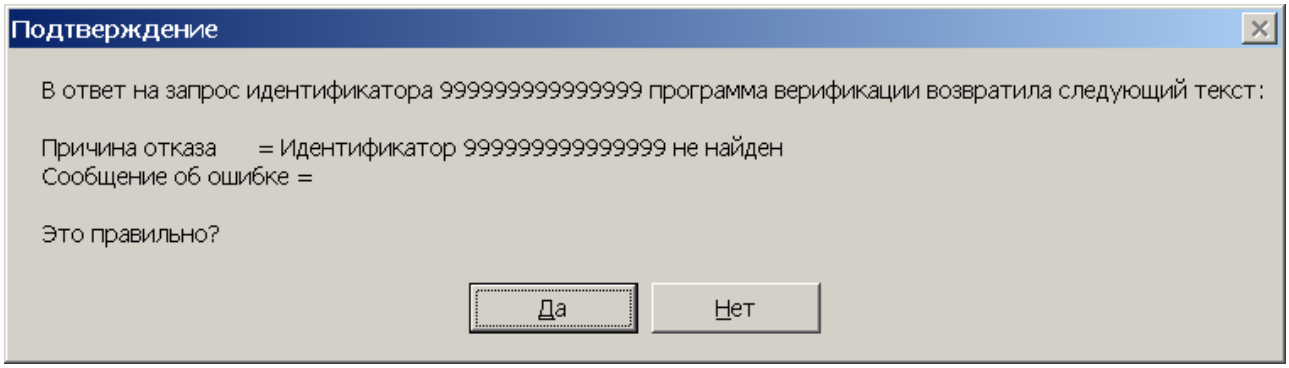
Регистрация внешней программы верификации – кнопка позволяет передать право принятия решения при проведении процедуры верификации для выбранной точки верификации внешней программе.

Дерегистрация программы верификации – кнопка позволяет отключить для выбранной точки внешнюю программу верификации.

После ее нажатия кнопки **Регистрация внешней программы верификации** откроется окно **Внешняя программа верификации**:



В поле **COM-сервер верификации** необходимо ввести название сервера, в поле **Название функции сервера** – название функции верификации (эти данные сообщают программисты-создатели ВПВ). После заполнения этих полей и нажатия кнопки **ОК** система проверяет возможность связи с ВПВ, и при благополучном вызове ВПВ ей будет послан тестовый запрос на обработку идентификатора 999999999999999. После получения ответа на этот запрос откроется окно подтверждения следующего вида (полученная от конкретной ВПВ информация будет отличаться от отображенной в окне примера – это зависит от самой ВПВ):

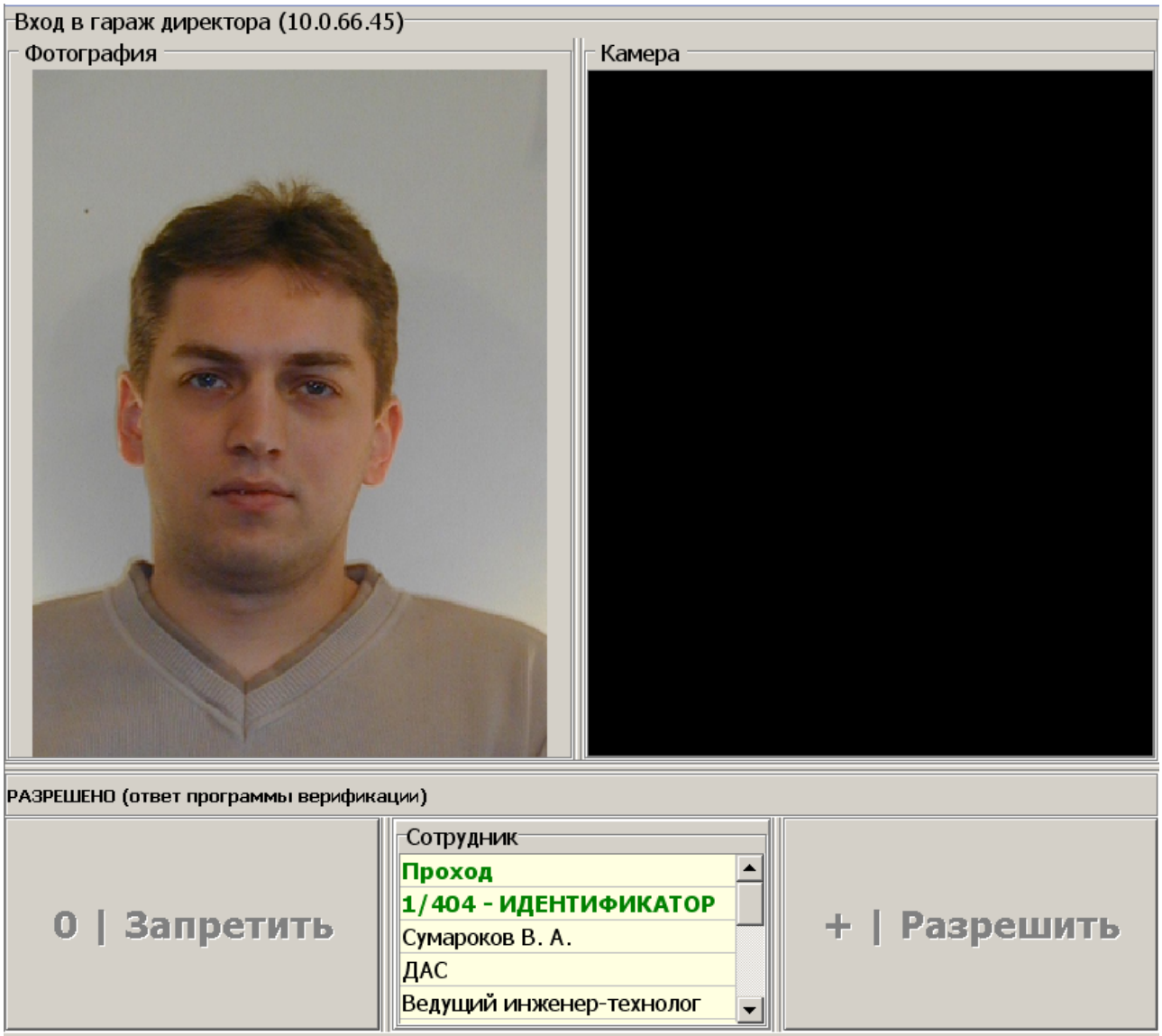


Если будет нажата кнопка **Да**, то окно **Внешняя программа верификации** будет закрыто, описание ВПВ будет сохранено для последующего использования.

13.2 Применение программы

После регистрации ВПВ становятся недоступными кнопки ответа на запрос (***РАЗРЕШИТЬ/ЗАПРЕТИТЬ***). При получении запроса от контроллера ПО ***PERCo-S-20*** посылает запрос в ВПВ. В ВПВ будут посланы только те запросы, которые связаны с отслеживаемыми и верифицируемыми событиями сотрудников и посетителей (см. параметры видеоточки окна конфигурации верификации). Если по истечении таймаута верификации (см. параметр **Время ожидания подтверждения при верификации** соответствующего считывателя в разделе ***«Конфигуратор»*** – для изменения таймаута, или параметр **Таймаут верификации** в окне **Конфигурация верификация** раздела ***«Верификация»*** – для ознакомлением с его значением) ответ на запрос от ВПВ получен не будет, то будет выполнена команда автоподтверждения, выбранная для данного типа события).

Если ответ на запрос положителен, то в контроллер будет послана команда, по которой исполнительный механизм контроллера будет разблокирован, а под панелью фотографии будет выведено информационное сообщение о разрешении запроса:



Если же ответ на запрос отрицателен, то в контроллер будет послана команда запрета запроса, а на этой же панели будет выведена причина отказа, полученный от ВПВ.

13.3 Реализация программы в виде метода COM-сервера

Информация для программистов, реализующих ВПВ в виде метода COM-сервера

COM-сервер должен реализовать интерфейс ***IDispatch*** и быть зарегистрирован в Windows на ПК, где работает консоль управления ***PERCo-S-20***. Название функции (метода) – на Ваше усмотрение. Для регистрации ВПВ администратору ***PERCo-S-20*** будет необходимо вручную ввести символьное представление ***Class ID (CLSID)*** сервера и название функции сервера, используемой как ВПВ.

При регистрации ВПВ ПО ***PERCo-S-20*** использует функции *Windows API* (для получения ссылки на интерфейс ***IDispatch***):

```
CLSIDFromProgID,
CoCreateInstance (ClassID, nil, CLSCTX_INPROC_SERVER or
CLSCTX_LOCAL_SERVER, IDispatch, Result)),
```

а также методы интерфейса ***IDispatch*** (для вызова функции сервера):

```
GetIDsOfNames
Invoke.
```

Описание функции на IDL

```
HRESULT _stdcall <Название функции>
   ([in] BSTR AIdentifier,
   [in] long ATimeOut,
   [in] BSTR AReaderName,
   [in] long ATypeInquery,
   [in, out] BSTR * ADenyReason,
   [in, out] BSTR * AErrorMessage,
   [out, retval] long * Value )
```

Описание функции на Delphi Object Pascal

```
function <Название функции>
   (const AIdentifier: WideString;
   ATimeOut: Integer;
   const AReaderName: WideString;
   ATypeInquery: Integer;
   var ADenyReason, AErrorMessage: WideString): Integer.
```

Описание функции на C#

```
int <Название функции>
   (string AIdentifier,
   int ATimeOut,
   string AReaderName,
   int ATypeInquery,
   ref string ADenyReason,
   ref string AErrorMessage)
```

Функция возвращает 0 (нет ошибки при работе функции) или 1 (произошла ошибка при работе функции, ее текст в ***AErrorMessage***). Эта информация – для программистов, но, тем не менее, будет отображена в окне точки верификации.

AIdentifier – символьное представление идентификатора (число от 1-18446744073709551614);
ATimeOut – время ожидания ответа на запрос контроллером (секунд);
AReaderName – название считывателя, от которого пришел запрос;
ATypeInquery – код запроса:
0 – прохода без нарушения времени и зональности,
1 – проход с нарушением времени,
2 – проход с нарушением зональности,
3 – проход с нарушением времени и зональности,
4 – постановка на охрану,
5 – снятие с охраны;
ADenyReason – текст причины отказа. Отказано или нет в запросе, определяется по наличию в возвращенной строке ***ADenyReason*** хотя бы одного не пробельного символа.

Примечание

При некорректных результатах работы раздела верификации полезной может оказаться информация из файла `Console17k.log` (по меньшей мере, Window'ские тексты исключений).

ООО «ПЭРКо»

Call-центр: 8-800-333-52-53 (бесплатно)
Тел.: (812) 247-04-57

Почтовый адрес:
194021, Россия, Санкт-Петербург,
Политехническая улица, дом 4, корпус 2

Техническая поддержка:

Call-центр: 8-800-775-37-05 (бесплатно)

Тел.: (812) 247-04-55

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

turnstile@perco.ru - по вопросам обслуживания турникетов и ограждений

locks@perco.ru - по вопросам обслуживания замков

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

www.perco.ru

Кор. 05.06.2018

www.perco.ru

тел: 8 (800) 333-52-53