

## РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ



# SM01

---

Модуль «Администратор»

# СОДЕРЖАНИЕ

1	Введение .....	4
2	«Консоль управления» .....	5
2.1	Запуск консоли .....	5
2.2	Элементы управления .....	7
2.3	Выбор раздела .....	10
2.4	Закрытие консоли .....	10
3	Раздел «Конфигуратор» .....	12
3.1	Назначение .....	12
3.2	Вкладка «Конфигурация» .....	12
3.2.1	Рабочее окно вкладки .....	12
3.2.2	Автоматическая конфигурация .....	16
3.2.3	Добавление нового устройства .....	19
3.2.4	Настройка системы безопасности .....	22
3.2.5	Состояние связи с контроллерами .....	23
3.2.6	Удаление и восстановление устройства .....	23
3.2.7	Изменение сетевых настроек .....	24
3.2.8	Подвкладка «Параметры» .....	25
3.2.8.1	Конфигурирование картоприемника .....	28
3.2.8.2	Конфигурирование одного алкотестера для одного направления .....	30
3.2.8.3	Конфигурирование двух алкотестеров для двух направлений .....	32
3.2.8.4	Биометрический контроллер Suprema BioEntry W2 .....	36
3.2.9	Подвкладка «Справочник объяснительных» .....	40
3.2.9.1	Создание объяснительной .....	40
3.2.10	Подвкладка «События» .....	41
3.2.10.1	Задание реакции на событие .....	42
3.2.11	Подвкладка «Настройка реакций» .....	44
3.2.11.1	Настройка реакций .....	44
3.2.12	Подвкладка «Камера СКУД» .....	46
3.2.13	Панель ввода дополнительных данных .....	47
3.2.13.1	Список комиссионующих карт .....	47
3.2.13.2	Список карт аварийного доступа .....	49
3.2.13.3	Список карт для постановки шлейфов на охрану .....	50
3.2.13.4	Список PIN-кодов для постановки шлейфов на охрану .....	52
3.2.14	Параметры ресурсов .....	54
3.2.14.1	Ресурсы контроллеров и ЭП PERCo 0.X серии x.1 .....	55
3.2.14.2	Ресурсы контроллеров и ЭП PERCo 0.X серии x.2 .....	56
3.2.14.3	Ресурсы контроллеров и ЭП PERCo 1.X .....	58
3.2.14.4	Контроллер доступа .....	59
3.2.14.5	Контроллер регистрации (LICON) .....	60
3.2.14.6	ППКОП (КБО) .....	62
3.2.14.7	Интеграция ППКОП с ПЦН «АИР» .....	63
3.2.14.8	Считыватель .....	65
3.2.14.9	ИУ (Замок / Турникет / Шлагбаум) .....	68
3.2.14.10	Генератор тревоги .....	71
3.2.14.11	Дополнительные входы .....	72
3.2.14.11.1	Тип входа «Обычный» .....	73
3.2.14.11.2	Тип входа «Специальный» .....	74
3.2.14.11.3	Тип входа «Подтверждение от ВВУ» .....	75
3.2.14.11.4	Тип входа «Запрет от ВВУ» .....	76

3.2.14.12	Дополнительный выход	77
3.2.14.12.1	Тип выхода «Обычный»	78
3.2.14.12.2	Тип выхода «Генератор тревоги»	78
3.2.14.12.3	Тип выхода «ОПС»	78
3.2.14.12.4	Программы управления выходом «ОПС»	79
3.2.14.13	Дополнительный вывод	82
3.2.14.13.1	Тип вывода «Выход обычный»	83
3.2.14.13.2	Тип вывода «Выход генератора тревоги»	83
3.2.14.13.3	Тип вывода «Выход ОПС»	83
3.2.14.13.4	Тип вывода «Вход Fire Alarm»	84
3.2.14.13.5	Тип вывода «Синхронизирующий вход / выход»	84
3.2.14.14	Шлейф сигнализации	85
3.2.14.14.1	Тип шлейфа «Охранный» (ОШС)	85
3.2.14.14.2	Тип шлейфа «Пожарный» (ПШС)	86
3.2.14.15	Зона сигнализации	86
3.2.14.15.1	Тип зоны «Охранная» (ОЗ)	87
3.2.14.15.2	Тип зоны «Пожарная» (ПЗ)	88
3.2.14.16	Приборы ИСО «Орион»	88
3.2.14.17	Интеграция с контроллерами «Suprema»	93
3.2.14.17.1	Контроллер BioEntry Plus	94
3.2.14.17.2	Контроллер BioEntry W2/P2	98
3.2.14.17.3	Замок	102
3.2.14.17.4	Параметры индикации контроллеров «Suprema»	103
3.2.14.18	Биометрические контроллеры PERCo	104
3.2.14.18.1	Контроллер СТ/L14, СТ13	105
3.2.14.18.2	Контроллер CL15	105
3.2.14.18.3	Контроллер регистрации CR11	106
3.2.14.18.4	ИУ	107
3.2.14.18.5	Направление	110
3.2.14.18.6	Считыватель	113
3.2.14.18.7	Вход	113
3.2.14.18.8	Выход	114
3.2.14.19	Видеоподсистема	115
3.2.14.20	Камера	116
3.3	Вкладка «Шлюзы»	117
3.3.1	Рабочее окно вкладки	117
3.3.2	Создание шлюза	118
3.4	Вкладка «Составные объекты»	119
3.4.1	Рабочее окно вкладки	119
3.4.2	Создание составного контроллера	120
4	Раздел «Планировщик заданий»	121
4.1	Назначение	121
4.2	Панели рабочей области	122
4.2.1	Панель «Задания»	122
4.2.2	Панель «Команды»	123
4.2.3	Панель «Расписание»	125
4.2.4	Панель «Отслеживаемые состояния»	125
4.2.5	Панели адресата и ввода текста	126
4.2.5.1	Панели «Телефоны» и «Текст SMS»	126
4.2.5.2	Панели «Контакты Viber» и «Текст сообщения»	127
4.2.6	Панель «Сотрудники»	128

4.2.7	Панель «Считыватели» .....	130
4.3	Задание по предъявлению идентификаторов .....	131
4.4	Задание по времени .....	132
4.5	Задание по времени и достижению состояний .....	133
4.6	Задание по изменению состояний.....	134
4.7	Задание отправки сообщений по неприходу .....	135
4.8	Задание отправки отчета по EMail .....	137
4.9	Журнал выполнения команд .....	140
5	Отчет по отправке сообщений .....	141
5.1	Раздел «Отчет по SMS».....	141
5.1.1	Назначение .....	141
5.1.2	Рабочее окно раздела.....	141
5.2	Раздел «Отчет по сообщениям Viber» .....	144
5.2.1	Назначение .....	144
5.2.2	Рабочее окно раздела.....	145
6	Состав видеоподсистемы .....	148
7	Конфигурирование видеоподсистемы .....	149
7.1	Поиск устройств видеоподсистемы.....	150
8	Подключение камер, поддерживающих стандарт ONVIF .....	153
8.1	Окно «Менеджер поиска и конфигурации камер (стандарт ONVIF)».....	153
8.2	Порядок поиска камер, поддерживающих стандарт ONVIF .....	154
9	«Центр управления видеоподсистемой» .....	156
9.1	Вкладка «Видеоархив».....	156
9.1.1	Рабочее окно вкладки .....	156
9.1.2	Создание и удаление видеоархива .....	157
9.2	Вкладка «Настройки» .....	158
9.2.1	Рабочее окно вкладки .....	158
9.2.2	Настройка IP-фильтра .....	159
9.3	Вкладка «О системе» .....	160
10	Установка драйвера видеочамеры .....	161
11	«Камеры СКУД» .....	162
12	Прозрачное здание – Web-доступ .....	164
12.1	Параметры .....	164
12.2	Инструкция по установке на Apache/PHP .....	166
13	Внешняя программа верификации .....	168
13.1	Регистрация программы.....	168
13.2	Применение программы.....	169
13.3	Реализация программы в виде метода COM-сервера.....	170

## 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 коммиссионированных 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

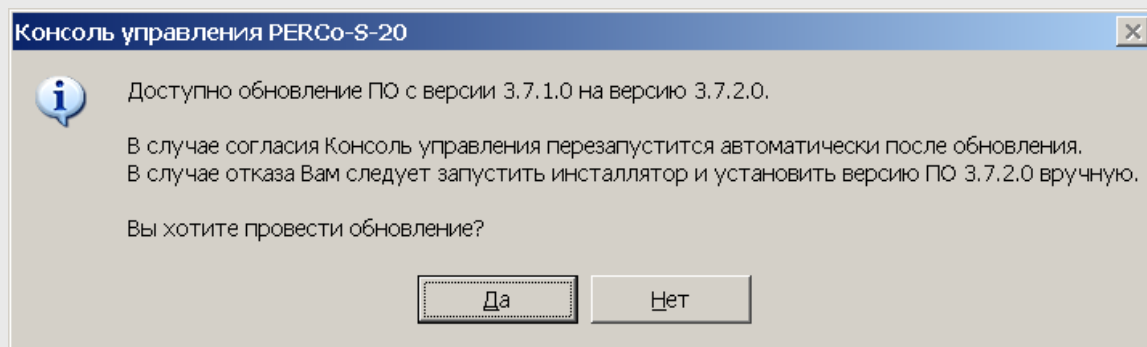
«**Консоль управления**» представляет собой программную оболочку, обеспечивающую доступ и навигацию оператора по установленным на ПК разделам ПО, связь с сервером системы, получение и сохранение информации из БД системы.



#### 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.

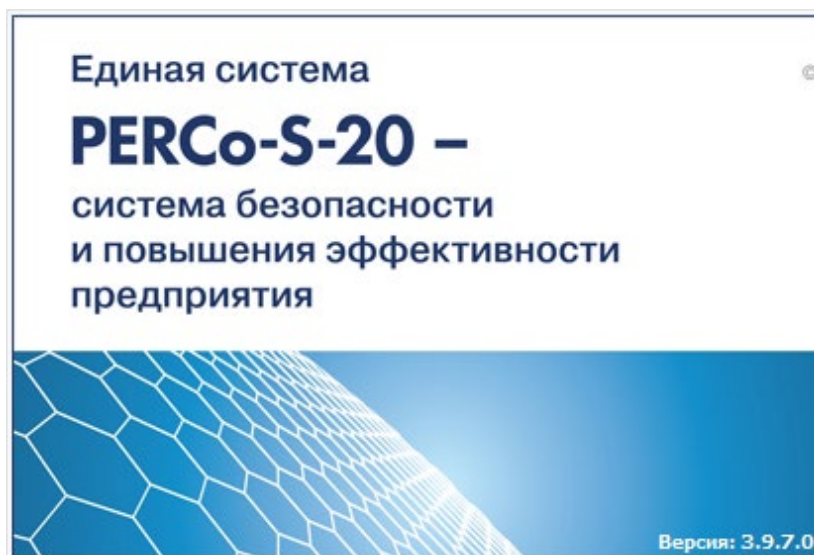
Процедура обновления будет запущена автоматически после подключения к серверу системы, если на сервере системы установлена более поздняя версия ПО. В этом случае при запуске «**Консоли управления**» появится окно с сообщением:



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 последнего оператора, который совершил удачный вход в систему.
- **Пароль** – поле ввода пароля оператора.
- **Сохранить пароль** – при установке флажка после правильного ввода имени и пароля оператора, в случае успешного входа в систему, при последующих запусках **«Консоли управления»** данные запрашиваться не будут. Если флажок снят, то имя пользователя и пароль запрашиваются при каждом входе в систему.

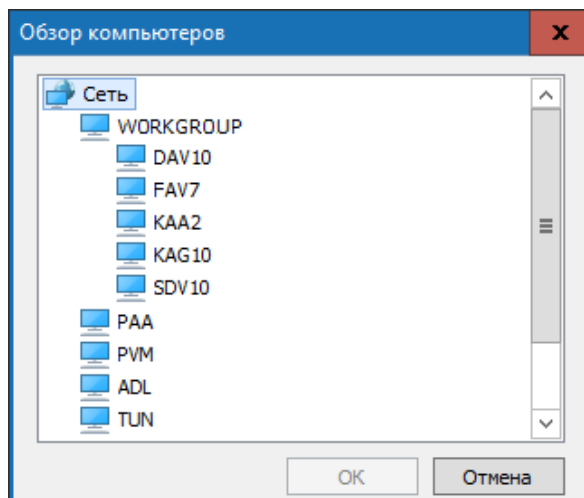


#### **Примечание:**

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 следующем 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.

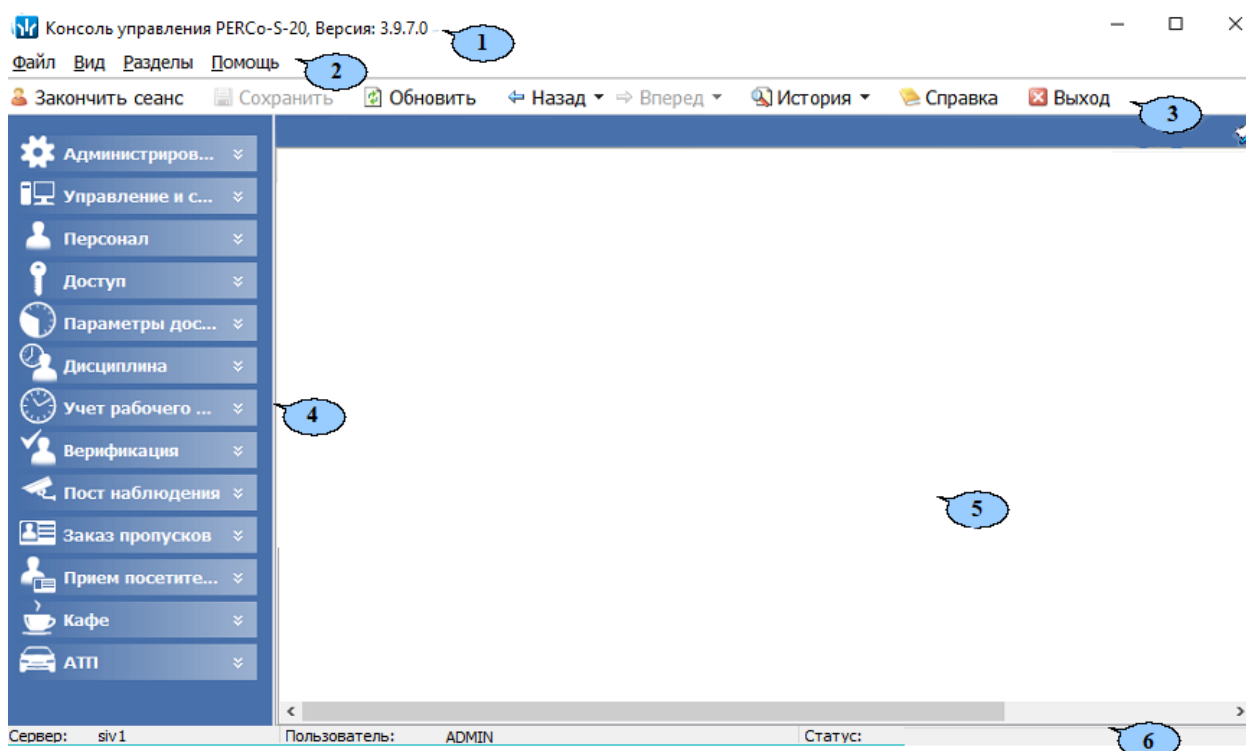
-  – кнопка позволяет открыть окно **Обзор компьютеров** для указания компьютера, на котором установлен сервер системы безопасности в локальной сети. Окно имеет следующий вид:



- **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 строках **Пользователь** и **Пароль** введите имя и пароль, назначенные администратором системы. Пароль должен вводиться латиницей. 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 **«Консоль управления»**.





## 2.2 Элементы управления

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








1. Строка заголовка окна. В строке указана версия запущенной **«Консоли управления»**. 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 **Заккрыть** позволяет завершить работу программы и закрыть окно.

2. Основное меню состоит из следующих компонентов:





- **Файл** – меню данного пункта содержит команду  **Выход F10**, позволяющую завершить работу программы.
- **Вид** – меню данного пункта содержит команды:
  -  **Панель навигатора F11** – команда позволяет скрыть или открыть панель навигатора.
  -  **Панель сообщений** – команда позволяет скрыть или открыть панель **Сообщение** в нижней части рабочей области **«Консоли управления»**.
- **Разделы** – меню данного пункта содержит список групп разделов со списками команд для перехода к одному из установленных на компьютере разделов:

















Администрирование	▶	Конфигуратор
Управление и события	▶	Конфигурация Mifare
Персонал	▶	Помещения и мнемосхема
Доступ	▶	Назначение прав доступа операторов
Параметры доступа	▶	Планировщик заданий
Дисциплина	▶	Отчет по SMS
Учет рабочего времени	▶	
Верификация	▶	
Пост наблюдения	▶	
Заказ пропусков	▶	
Прием посетителей	▶	
Кафе	▶	
АТП	▶	



**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](mailto: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 (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, выберите нужный раздел.



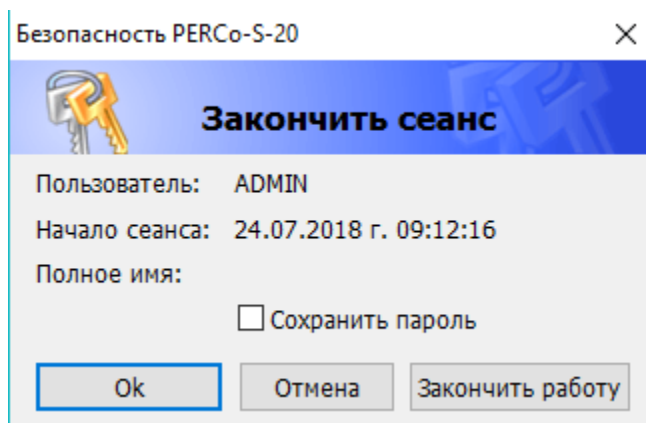
### **Примечание:**

**«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**.

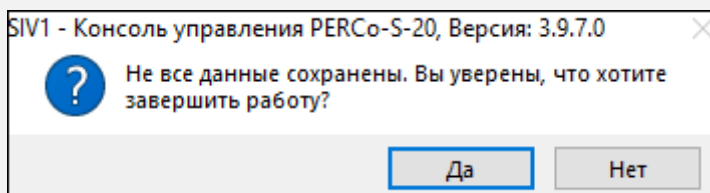


- **ОК** – кнопка позволяет закончить сеанс работы пользователя и открыть окно **Безопасность PERCo-S-20. Начать сеанс** для входа в систему другого пользователя.
- **Отмена** – кнопка позволяет вернуться к работе.
- **Закончить работу** – кнопка позволяет завершить работу программы.
- **Сохранить пароль**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



**Примечание:**

Если какие-либо 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

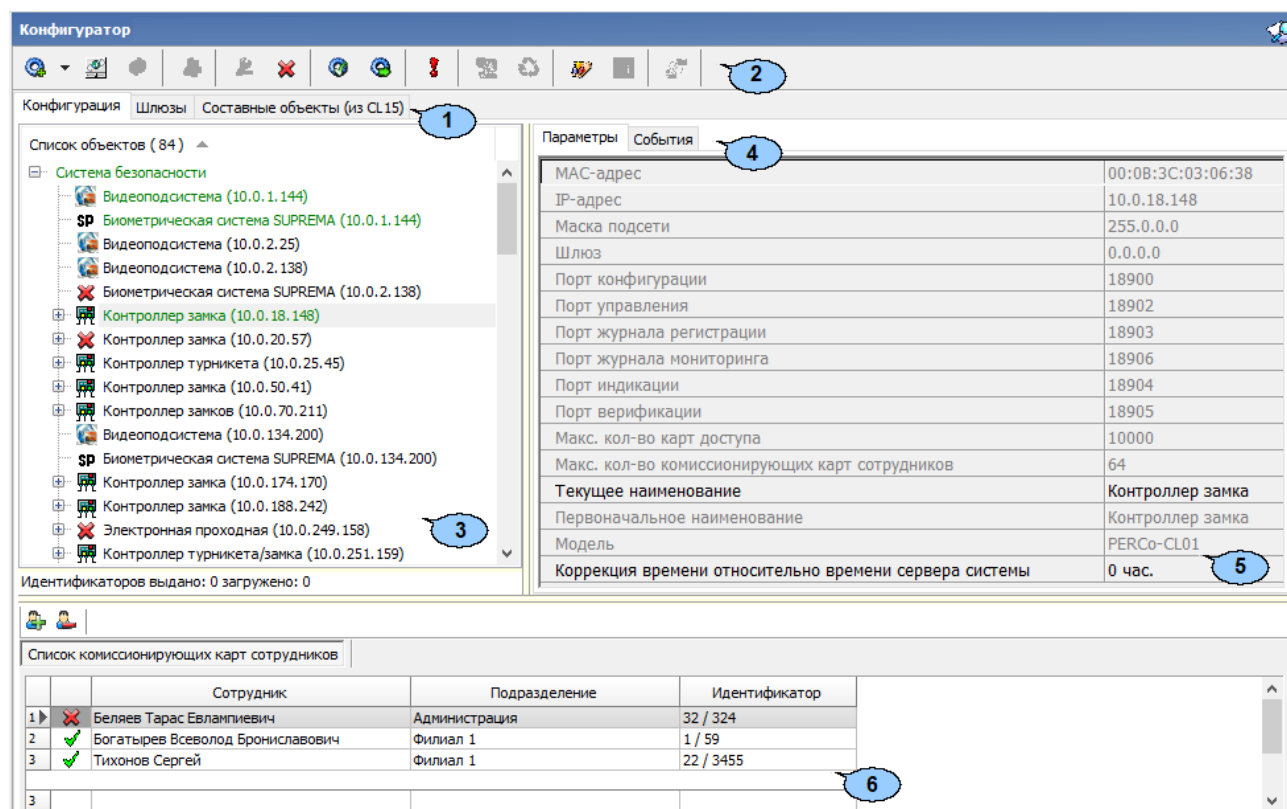
Раздел *«Конфигуратор»* предназначен для конфигурации системы, создания шлюзов и создания составного контроллера.

### 3.2 Вкладка «Конфигурация»

Вкладка *Конфигурация* предназначена для конфигурации системы, добавления в нее новых устройств, настройки параметров их работы, а также задания реакций на события, регистрируемые в системе. Также для контроллеров доступа предусмотрена возможность создания списки комиссионированных карт. Для контроллеров второго уровня списков карт аварийного доступа и для ППКОП списков карт и PIN-кодов постановки и снятия шлейфов сигнализации на охрану.

#### 3.2.1 Рабочее окно вкладки

Рабочее окно вкладки *«Конфигурация»* имеет следующий вид:














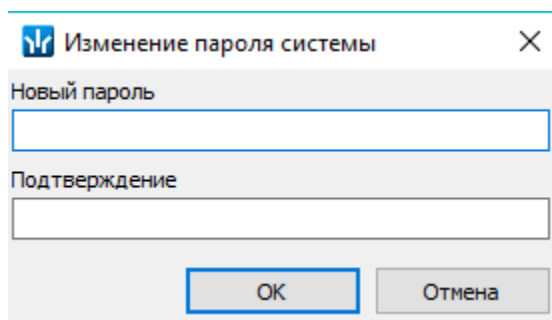
1. Выбор вкладки раздела:

- **Конфигурация;**
- **Шлюзы;**
- **Составные объекты.**

2. 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 переключателей на плате контроллера или после изменения состава подключенных контроллеров второго уровня.
  - для контроллеров **PERCo-CR11, PERCo-CL15, PERCo-CT/L14** получить полную конфигурацию контроллера. Если в конфигурацию контроллера были внесены изменения из других источников, то перед работой с ним необходимо обновить его конфигурацию, либо передать ее из **PERCo-S-20**.
-  **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**. Также 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 ), выделите его 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)** – если кнопка активна, то в рабочей области вкладки «Конфигурация» отображаются 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**.



### Примечание:


Пароль применяется к контроллеру только после успешной передачи параметров. Новый пароль не будет применен, если:


- в момент изменения не было связи с контроллером;
- не удалось авторизоваться.

-  **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**.




Для контроллеров **PERCo-CR11**, **PERCo-CL15**, **PERCo-CT/L14** не требуется исключение из конфигурации, кнопка доступна изначально.

Для контроллеров, работающих по внешнему подключению, можно изменить визуальное отображение сетевых настроек, но нет возможности передать настройки в само устройство.

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


Конфигуратор			
Устройство	IP-адрес	Состояние	Информация
Контроллер CL15	172.17.1.112		Версия прошивки: 1.0.1.W

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 не доступна для встроенного контроллера электронной проходной **PERCo-KT02.x**).
-  **Копирование параметров между шлейфами и реле аппаратуры "Болид"** – кнопка позволяет переносить заданную конфигурацию, заданную на одном шлейфе или реле на другие.

3. 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 контроллером Suprema;
-  – устройство является видеоподсистемой, включенной в конфигурацию системы безопасности;
-  – устройство является камерой, добавленной в видеоподсистему;
- **SP** – устройство является биометрической системой Suprema;
-  – 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:

Сортировка по наименованию	Alt+A
Сортировка по адресу	Alt+Z

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:

Развернуть все	Alt+E
Свернуть все	Alt+C
Скрыть дополнительную информацию	Alt+H

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

4. Выбор вкладки панели настройки:

- **Параметры.** Вкладка позволяет настроить параметры функционирования устройства или ресурса, выделенного в рабочей области раздела.
- **Справочник объяснительных.** На вкладке можно задать список объяснительных, который передается на **CR11**.
- **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.
- **Настройка реакций.** На вкладке можно настроить реакции на события в контроллере.



- **Общий список реакций на события.** На вкладке отображается полный список событий, регистрируемых системой безопасности для всех устройств или ресурсов в рабочей области раздела. Также на вкладке можно задать реакцию системы на любое из событий. Вкладка доступна для ресурса **Система безопасности**.
- **Камера СКУД.** Вкладка доступна для ресурса контроллера **Считыватель** и предназначена для выбора камеры подсистемы **«Камера СКУД»**.

5. Рабочая область вкладки панели настройки.

6. Панель ввода дополнительных данных. Для открытия и скрытия панели используйте контекстное меню рабочей области раздела или сочетание клавиш **Alt+N**. 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.


### 3.2.2 Автоматическая конфигурация



#### Примечание:

Перед добавлением новых устройств убедитесь, что:

- установлена не демонстрационная версия системы **PERCo-S-20**;
- установленная версия **PERCo-S-20** поддерживает работу с требуемыми моделями контроллеров. При необходимости обновите версию.

Для проведения автоматического поиска устройств нажмите  рядом с кнопкой **Провести конфигурацию** на панели инструментов раздела и выберите из выпадающего списка один из вариантов:

- **Конфигурация контроллеров с прямым подключением;**
- **Конфигурация контроллеров с внешним подключением.**

#### Для конфигурации контроллеров с прямым подключением:

1. При выборе **Конфигурации контроллеров с прямым подключением** откроется новое окно **Выбор сетевых интерфейсов**:

Выбор сетевых интерфейсов

Выберите сетевые интерфейсы, по которым будет производиться поиск устройств.

Адрес подсети	Маска подсети
<input type="checkbox"/> 10.0.0.0	255.0.0.0
<input type="checkbox"/> 172.17.0.0	255.255.0.0

Диапазон поиска устройств

IP-адрес начала диапазона

IP-адрес конца диапазона

Поиск только внутри диапазона

Контроллеры доступа и регистрации, КБО, ППКОП

Драйверы шлейфа

Видеоподсистемы

Биометрические системы SUPREMA



OK Отмена

2. В рабочей области 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 искомым устройств.
4. При необходимости адресной отправки запросов на устройства 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:

Конфигуратор

Устройство	IP-адрес	Состояние	Информация
Контроллер СТ/Л 14	172.17.1.108		Найдено новое оборудование.
Контроллер CL15	172.17.1.115		Найдено новое оборудование.
Контроллер CL15	172.17.1.123		Найдено новое оборудование.
Контроллер CL15	172.17.1.125		Найдено новое оборудование.
Контроллер CL15	172.17.1.120		Найдено новое оборудование.
Видеоподсистема	172.17.1.147		Найдено новое оборудование.
Контроллер СТ/Л 14	172.17.1.117		Найдено новое оборудование.
Контроллер CL15	172.17.1.126		Найдено новое оборудование.
Контроллер СТ/Л 14	172.17.1.105		Найдено новое оборудование.
Контроллер CL15	172.17.1.116		Найдено новое оборудование.
Видеоподсистема	172.17.0.45		Найдено новое оборудование.
Видеоподсистема	172.17.0.128		Найдено новое оборудование.

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 устройств 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.

- Выделите в рабочей области раздела корневой элемент (по умолчанию «Система безопасности»). На вкладке **Параметры** произведите настройку [параметров системы](#) в целом.
- 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.

**Для конфигурации контроллеров с внешним подключением:**






**Примечание:**



Для работы с внешними подключениями необходимо предварительно включить эту возможность в центре управления **PERCo-S-20**.

- При выборе **Конфигурация контроллеров с внешним подключением** откроется новое окно **Выбор устройства с внешним подключением:**

Выбор устройств с внешним подключением x

	Устройство	IP-Адрес	MAC-Адрес
1	PERCo-CTL14	172.17.1.118	00:25:0B:11:01:76
2	PERCo-CL15	172.17.1.112	00:25:0B:11:01:70
2			

- В рабочей области окна выберите необходимое устройство (в окне отображаются все активные подключения к серверу, которые еще не были добавлены в **PERCo-S-20**).
- Для обновления списка устройств нажмите кнопку .
- Выберите необходимые устройства из списка и нажмите кнопку **ОК**. Устройства будут добавлены в рабочую область раздела и отмечены значками .
- Если какое-либо из найденных устройств необходимо исключить из конфигурации, выделите его в рабочей области и нажмите кнопку  **Исключить из конфигурации** на панели инструментов раздела. Значок устройства изменится на .
- Для настройки параметров выделите устройство или ресурс в рабочей области раздела и на вкладке **Параметры** панели настройки измените необходимые параметры.
- Для настройки реакций на события выделите устройство или ресурс в рабочей области раздела и на вкладке **События** панели настройки добавьте необходимые реакции.
- Выделите в рабочей области раздела корневой элемент (по умолчанию «Система безопасности»). На вкладке **Параметры** произведите настройку [параметров системы](#) в целом.

9. 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.



**Примечания:**

После добавления контроллера в систему из него вычитывается конфигурация. В случае, если конфигурация не обновилась сразу, следует перечитать конфигурацию с сервера. Для этого нажмите кнопку **Обновить** на панели инструментов вкладки.

### 3.2.3 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.



**Примечание:**

Перед добавлением новых устройств убедитесь, что:

- установлена не демонстрационная версия системы **PERCo-S-20**;
- установленная версия **PERCo-S-20** поддерживает работу с требуемыми моделями контроллеров. При необходимости обновите версию.

Для добавления в конфигурацию системы нового устройства:

1. Нажмите кнопку  **Добавить новое устройство** на панели инструментов раздела. Откроется панель **Поиск по IP-адресу**:

2. Используя раскрывающийся список **Категория**, укажите тип добавляемого устройства:

- **Контроллеры доступа и регистрации, КБО, ППКОП** – для добавления контроллера доступа, регистрации или ППКОП.



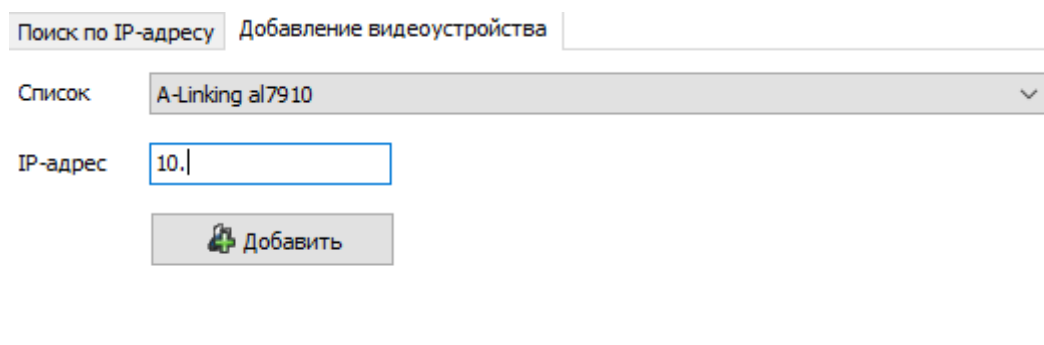
**Примечания:**

• Порядок конфигурирования видеоподсистемы описан в руководстве администратора системы.

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

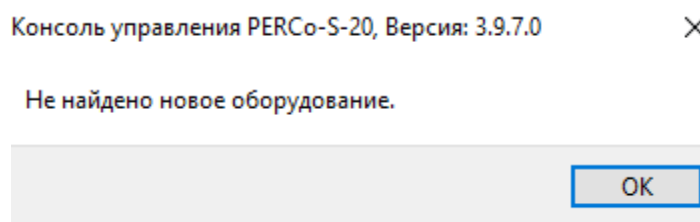
- **Видеоподсистемы** – для добавления сервера видеоподсистемы с файлами видеоархива.

- **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.
  - **Драйверы шлейфа.**
  - **Панели приемно-контрольные.**
  - **Панели индикации выносные.**
  - **Модули управления ИСО "Орион"** – для интеграции 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.
  - **Биометрические системы SUPREMA.**
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**, в котором будет отображаться искомое устройство и состояние связи с ним. Для закрытия окна нажмите кнопку **ОК**. Найденное устройство будет добавлено в рабочую область раздела и отмечено значком .
  5. Если устройство не было найдено, откроется окно с сообщением:

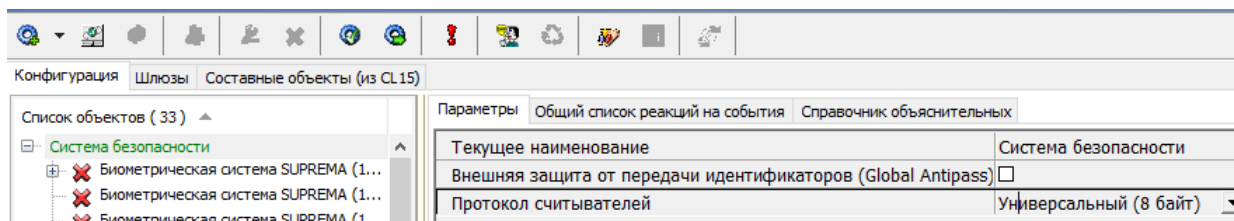


6. Закройте окно, нажав кнопку **ОК**, затем проверьте состояние устройства его подключение к сети *Ethernet*, устраните найденные неполадки, после чего повторите поиск, нажав кнопку **Найти**.
7. Для настройки параметров выделите устройство или его ресурс в рабочей области раздела, затем на вкладке **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.

### 3.2.4 Настройка системы безопасности

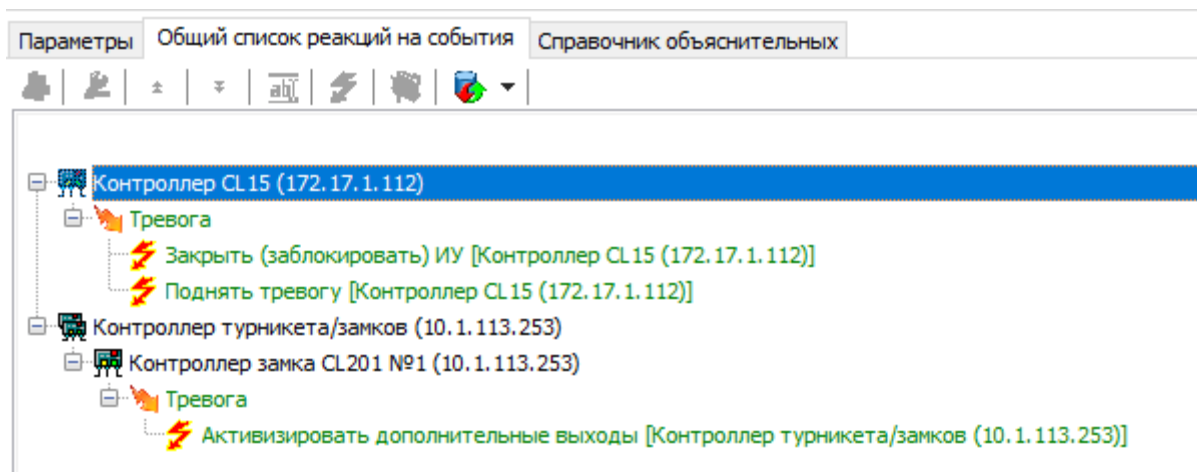
Настройки системы безопасности доступны при выборе в рабочей области корневого элемента списка объектов (по умолчанию «Система безопасности»):





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



- Строка **Текущее наименование** позволяет изменить 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 EM-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, которым в системе установлены какие-либо реакции. При двойном нажатии левой кнопкой мыши на устройстве в рабочей области вкладки отобразится полный список событий этого устройства:



### 3.2.5 Состояние связи с контроллерами

При проведении автоматической конфигурации системы, добавлении или восстановлении устройств, а также после неудачной передачи 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 выглядит следующим образом и содержит элементы:

Устройство	IP-адрес	Состояние /	Информация
Контроллер CL 15	172.17.1.112		Нет связи.
Контроллер турникета/замков	10.1.113.253		Выполнено

- **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.
- **OK** – кнопка позволяет закрыть окно.
- **Печать** – кнопка позволяет сформировать документ для предварительного просмотра и печати.

### 3.2.6 Удаление и восстановление устройства

#### Удаление 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 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 красным цветом, если активна кнопка  **Отображать скрытые устройства**.

### **Восстановление устройства**



#### **Примечание:**



Восстановить можно только скрытое устройство. Удаленное ранее устройство необходимо заново [добавлять в конфигурацию](#).

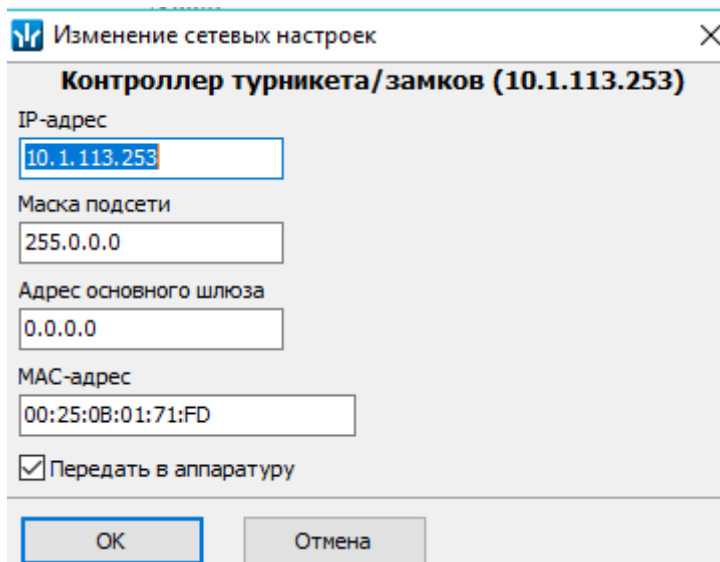
Для восстановления скрытого устройства:

1. Нажмите кнопку  **Отображать скрытые устройства** на панели инструментов раздела. В рабочей области раздела станут видны скрытые устройства, которые 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.

### **3.2.7 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 **OK** для применения измененных настроек или кнопку **Отмена** для выхода без сохранения.
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.

### 3.2.8 Подвкладка «Параметры»

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

Параметры <span style="float: right;">События</span>	
MAC-адрес	00:25:0B:01:71:FD
IP-адрес	10.1.113.253
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 журнала отладки	18908
Порт индикации	18904
Порт верификации	18905
Макс. кол-во карт доступа и коммиссионированных карт	50016
Текущее наименование	Контроллер турникета/замков
Первоначальное наименование	Контроллер турникета/замков
Модель	PERCo-CT/L04.2
Разрешить WEB-интерфейс	<input type="checkbox"/>
Коррекция времени относительно времени сервера системы	0 час.

1. Выбор подвкладки панели настройки:
  - **Параметры**;

- [Справочник объяснительных](#);
- [События](#);
- [Настройка реакций](#);
- [Камера СКУД](#).

2. Рабочая область вкладки содержит список параметров и характеристик, доступных для устройства ресурса, выделенного в рабочей области раздела. Выделение параметра зеленым цветом указывает на то, что значение параметра было изменено, но внесенные изменения не были переданы в устройство.

Для настройки параметра устройства или его ресурса:

1. Выделите в рабочей области раздела необходимый элемент.
2. В строке с наименованием параметра, который необходимо изменить, нажмите правой кнопкой мыши в правом столбце рабочей области вкладки.

Используются следующие способы ввода значений параметров:

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

Текущее наименование	Контроллер турникета/замков
----------------------	-----------------------------

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

-4 час. ▾ ⋮

-11 час.  
 -10 час.  
 -9 час.  
 -8 час.  
 -7 час.  
 -6 час.  
 -5 час.  
 -4 час.

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

Разрешить WEB-интерфейс

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

0
▲ ▼

Выпадающий многоуровневый список позволяет получить доступ к группе параметров для их настройки при нажатии на значок ⊕, либо скрыть их, нажав значок ⊖.

⊖ Верификация от ВВУ

⊕ в РЕЖИМЕ работы "Контроль"

Подтверждение прохода для ПОСЕТИТЕЛЕЙ

Время ожидания подтверждения

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

Коррекция времени относительно времени сервера системы

Изменить значение
✕

Параметр  
Коррекция времени относительно времени сервера системы

Значение

-6

▲ ▼

час.

Сохранить

Отменить

### 3.2.8.1 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 типа "дополнительный выход" и переименуйте его в **Выход "Изъять карту"**. Выход 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**;

Параметры		События	
Адрес		3	
Текущее наименование		Выход "Изъять карту"	
Первоначальное наименование		Дополнительный выход №3	
<input type="checkbox"/> Тип		Обычный	
<input type="checkbox"/> <b>Обычный</b>			
	Нормальное состояние		Не запитан

4. При необходимости настройте реакцию системы на сигнал от картоприемника **«Авария»**. Для этого выделите ресурс типа "дополнительный вход" и переименуйте его во **Вход "Картоприемник переполнен"**. Вход 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:

Параметры		События	
Адрес		4	
Текущее наименование		Вход "Картоприемник переполнен"	
Первоначальное наименование		Дополнительный вход №4	
<input type="checkbox"/> Тип		Обычный	
<input type="checkbox"/> <b>Обычный</b>			
	Нормальное состояние контакта		Разомкнут
<input type="checkbox"/> <b>Дополнительные входы, маскируемые при активизации</b>			
<input type="checkbox"/> <b>Дополнительные выходы, активизируемые при активизации</b>			
<input type="checkbox"/> <b>Дополнительные выходы, нормализуемые при активизации</b>			

5. Выделите ресурс типа "дополнительный вход" и переименуйте его во **Вход "Карта изъята"**. Вход 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**;
  - для параметров **Контроллер**, **Считыватель** выберите контроллер и считыватель, для которых будет подтвержден проход от картоприемника:

Параметры	
Адрес	3
Текущее наименование	Вход "Карта изъята"
Первоначальное наименование	Дополнительный вход №3
[-] Тип	Подтверждение от ВВУ
[-] <b>Подтверждение от ВВУ</b>	
Нормальное состояние контакта	Разомкнут
Контроллер	Стойка турникета №1
Считыватель	Считыватель на выход
[+] <b>Дополнительные входы, маскируемые при активизации</b>	
[+] <b>Дополнительные выходы, активизируемые при активизации</b>	
[+] <b>Дополнительные выходы, нормализируемые при активизации</b>	




**Примечание:**

Для контроллеров с версией прошивки x.0.0.19 и ниже недоступно значение параметра **Тип: Подтверждение от ВВУ** для ресурса типа **"Дополнительный вход"**. В этом случае выход картоприемника «Карта изъята» подключается ко 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 типа "считыватель" и переименуйте его во **Считыватель на выход**. Номер считывателя должен соответствовать выходному считывателю, в направлении которого установлен картоприемник. На панели **Параметры**:
- для параметра **Способ верификации** установите значение **ВВУ**.
  - 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 **Выход "Изъять карту"**.

- Для параметра **Изымать идентификаторы ПОСЕТИТЕЛЕЙ** установите требуемое значение. Идентификаторы посетителей будут изыматься при условии, что:
  - Выбраны значения параметра **После любого прохода** или **После прохода в последний день действия идентификатора**.
  - В разделе **«Доступ» > «Доступ посетителей»** установлен параметр **Удалять после прохода** для указанных посетителей.

Параметры		События	Камера СКУД
Адрес	2		
Текущее наименование	Считыватель на выход		
Первоначальное наименование	Считыватель №2		
Модель	PERCo-IRxx		
Способ верификации	ВВУ		
[-] <b>Верификация от ВВУ</b>			
[-] <b>в РЕЖИМЕ работы "Контроль"</b>			
при проходе СОТРУДНИКОВ	<input type="checkbox"/>		
при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ	<input type="checkbox"/>		
при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ	<input type="checkbox"/>		
при проходе ПОСЕТИТЕЛЕЙ	<input checked="" type="checkbox"/>		
при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ	<input type="checkbox"/>		
при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	<input type="checkbox"/>		
Подтверждение прохода для ПОСЕТИТЕЛЕЙ	Постоянно		
Время ожидания подтверждения	6 сек.		
По истечении времени ожидания подтверждения генерировать событие	Запрет прохода от ВВУ		
[+] <b>Верификация от ПДУ</b>			
[+] <b>Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)</b>			
[-] <b>Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)</b>			
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет		
[+] <b>Контроль времени для идентификаторов СОТРУДНИКОВ</b>			
[-] <b>Контроль времени для идентификаторов ПОСЕТИТЕЛЕЙ</b>			
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет		
[+] <b>Дополнительные входы, маскируемые при разблокировке ИУ</b>			
[+] <b>Дополнительные выходы, активизируемые при разблокировке ИУ</b>			
[+] <b>Дополнительные выходы, нормализируемые при разблокировке ИУ</b>			
[+] <b>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ</b>			
[-] <b>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ</b>			
Критерий активизации	На время срабатывания		
Выход "Изъять карту"	<input checked="" type="checkbox"/>		
Изымать идентификаторы ПОСЕТИТЕЛЕЙ	После прохода в последний день действия идентификатора		

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

### 3.2.8.2 Конфигурирование одного алкотестера для одного направления

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

После монтажа и подключения алкотестера 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 алкотестер. Раскройте список его ресурсов.
3. Выделите ресурс типа "дополнительный вход" и переименуйте его во **Вход "Подтверждение от алкотестера"** на вход. На панели **Параметры**:
  - для параметра **Тип** установите значение **Подтверждение от ВВУ**;

- для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели);
- для параметров **Контроллер**, **Считыватель** выберите контроллер и считыватель, для которых будет подтвержден проход от алкотестера:

Параметры		События
Адрес	3	
Текущее наименование	Вход "Подтверждение от алкотестера" на вход	
Первоначальное наименование	Дополнительный вход №3	
<input type="checkbox"/> Тип	Подтверждение от ВВУ	
<input type="checkbox"/> <b>Подтверждение от ВВУ</b>		
Нормальное состояние контакта	Разомкнут	
Контроллер	Стойка турникета №1	
Считыватель	Считыватель на вход	
<input type="checkbox"/> <b>Дополнительные входы, маскируемые при активизации</b>		
<input type="checkbox"/> <b>Дополнительные выходы, активизируемые при активизации</b>		
<input type="checkbox"/> <b>Дополнительные выходы, нормализируемые при активизации</b>		



**Примечание:**

Если к контроллеру подключен только один выход алкотестера, то **Вход "Подтверждение от алкотестера" на вход** конфигурируется в зависимости от типа управляющего сигнала. При этом **Вход "Запрет от алкотестера" на вход** не используется.

4. Выделите ресурс типа "дополнительный вход" и переименуйте его во **Вход "Запрет от алкотестера" на вход**. На панели **Параметры**:
  - для параметра **Тип** установите значение **Запрет от ВВУ**;
  - для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели);
  - для параметров **Контроллер**, **Считыватель** выберите контроллер и считыватель, для которых будет отклонен проход от алкотестера:


Параметры		События
Адрес	4	
Текущее наименование	Вход "Запрет от алкотестера" на вход	
Первоначальное наименование	Дополнительный вход №4	
<input type="checkbox"/> Тип	Запрет от ВВУ	
<input type="checkbox"/> <b>Запрет от ВВУ</b>		
Нормальное состояние контакта	Разомкнут	
Контроллер	Стойка турникета №1	
Считыватель	Считыватель на вход	
<input type="checkbox"/> <b>Дополнительные входы, маскируемые при активизации</b>		
<input type="checkbox"/> <b>Дополнительные выходы, активизируемые при активизации</b>		
<input type="checkbox"/> <b>Дополнительные выходы, нормализируемые при активизации</b>		

5. Выделите ресурс типа "считыватель" и переименуйте его в **Считыватель на вход**. Номер считывателя должен соответствовать считывателю, в направлении которого установлен алкотестер. 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 алкотестера;
- для параметра **По истечении времени ожидания подтверждения генерировать событие** установите значение **Запрет прохода от ВВУ**, если к контроллеру подключены два выхода алкотестера (для управляющих сигналов разрешения и запрета прохода). **Отказ от прохода, нет ответа от ВВУ**, если подключен только один выход разрешения прохода алкотестера.

Параметры	
Адрес	1
Текущее наименование	Считыватель на вход
Первоначальное наименование	Считыватель №1
Модель	PERCo-IRxx
Способ верификации	ВВУ
<b>[-] Верификация от ВВУ</b>	
<b>[-] в РЕЖИМЕ работы "Контроль"</b>	
при проходе СОТРУДНИКОВ	<input checked="" type="checkbox"/>
при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ	<input type="checkbox"/>
при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ	<input type="checkbox"/>
при проходе ПОСЕТИТЕЛЕЙ	<input type="checkbox"/>
при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ	<input type="checkbox"/>
при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	<input type="checkbox"/>
Подтверждение прохода для ПОСЕТИТЕЛЕЙ	Постоянно
Время ожидания подтверждения	30 сек.
По истечении времени ожидания подтверждения генерировать событие	Запрет прохода от ВВУ
<b>[+] Верификация от ПДУ</b>	
<b>[+] Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)</b>	
<b>[+] Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)</b>	
<b>[+] Контроль времени для идентификаторов СОТРУДНИКОВ</b>	
<b>[+] Контроль времени для идентификаторов ПОСЕТИТЕЛЕЙ</b>	
<b>[+] Дополнительные входы, маскируемые при разблокировке ИУ</b>	
<b>[+] Дополнительные выходы, активизируемые при разблокировке ИУ</b>	
<b>[+] Дополнительные выходы, нормализуемые при разблокировке ИУ</b>	
<b>[+] Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ</b>	
<b>[+] Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ</b>	
Изымать идентификаторы ПОСЕТИТЕЛЕЙ	Нет

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

### 3.2.8.3 Конфигурирование двух алкотестеров для двух направлений

Два алкотестера (или другие ВВУ) могут использоваться для подтверждения или запрета возможности прохода в обоих направлениях.

После монтажа и подключения алкотестеров необходимо произвести их конфигурирование в сетевом ПО системы, для этого:

1. Запустите **«Консоль управления»** и откройте раздел **«Конфигуратор»**.
2. Выделите в рабочей области раздела контроллер, к которому подключены алкотестеры. Раскройте список его ресурсов.

3. Выделите ресурс типа "дополнительный вход" и переименуйте его во **Вход "Подтверждение от алкотестера" на вход**. На панели **Параметры**:
- для параметра **Тип** установите значение **Подтверждение от ВВУ**;
  - для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели);
  - для параметров **Контроллер**, **Считыватель** выберите контроллер и считыватель, для которых будет подтвержден проход от алкотестера на вход:

Параметры	
Адрес	3
Текущее наименование	Вход "Подтверждение от алкотестера" на вход
Первоначальное наименование	Дополнительный вход №3
☐Тип	Подтверждение от ВВУ
☐ <b>Подтверждение от ВВУ</b>	
Нормальное состояние контакта	Разомкнут
Контроллер	Стойка турникета №1
Считыватель	Считыватель на вход
☑ <b>Дополнительные входы, маскируемые при активизации</b>	
☑ <b>Дополнительные выходы, активизируемые при активизации</b>	
☑ <b>Дополнительные выходы, нормализируемые при активизации</b>	



**Примечание:**

Если к контроллеру подключен только один выход алкотестера на вход, то **Вход "Подтверждение от алкотестера" на вход** конфигурируется в зависимости от типа управляющего сигнала. При этом **Вход "Запрет от алкотестера" на вход** не используется.

4. Выделите ресурс типа "дополнительный вход" и переименуйте его в **Вход "Запрет от алкотестера" на вход**. На панели **Параметры**:
- для параметра **Тип** установите значение **Запрет от ВВУ**;
  - для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели);
  - для параметров **Контроллер**, **Считыватель** выберите контроллер и считыватель, для которых будет отклонен проход от алкотестера на вход:

Параметры	
Адрес	4
Текущее наименование	Вход "Запрет от алкотестера" на вход
Первоначальное наименование	Дополнительный вход №4
☐Тип	Запрет от ВВУ
☐ <b>Запрет от ВВУ</b>	
Нормальное состояние контакта	Разомкнут
Контроллер	Стойка турникета №1
Считыватель	Считыватель на вход
☑ <b>Дополнительные входы, маскируемые при активизации</b>	
☑ <b>Дополнительные выходы, активизируемые при активизации</b>	
☑ <b>Дополнительные выходы, нормализируемые при активизации</b>	

5. Выделите ресурс типа "считыватель" и переименуйте его в **Считыватель на вход**. На панели **Параметры**:
  - для параметра **Способ верификации** установите значение **ВВУ**;
  - в раскрывшемся списке отметьте флажками параметры: **при проходе СОТРУДНИКОВ**;
  - для параметра **Время ожидания подтверждения** установите требуемое значение времени, в течение которого контроллер должен ожидать управляющий сигнал от алкотестера на вход;
  - для параметра **По истечении времени ожидания подтверждения генерировать событие** установите значение **Запрет прохода от ВВУ**, если к контроллеру подключены два выхода алкотестера на вход (для управляющего сигнала разрешения и запрета прохода). В ином случае - **Отказ от прохода, нет ответа от ВВУ**.

Параметры		События	Камера СКУД
Адрес	1		
Текущее наименование	Считыватель на вход		
Первоначальное наименование	Считыватель №1		
Модель	PERCo-IRxx		
Способ верификации	ВВУ		
<input type="checkbox"/> <b>Верификация от ВВУ</b>			
<input type="checkbox"/> <b>в РЕЖИМЕ работы "Контроль"</b>			
при проходе СОТРУДНИКОВ			<input checked="" type="checkbox"/>
при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ			<input type="checkbox"/>
при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ			<input type="checkbox"/>
при проходе ПОСЕТИТЕЛЕЙ			<input type="checkbox"/>
при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ			<input type="checkbox"/>
при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ			<input type="checkbox"/>
Подтверждение прохода для ПОСЕТИТЕЛЕЙ			Постоянно
Время ожидания подтверждения			30 сек.
По истечении времени ожидания подтверждения генерировать событие			Запрет прохода от ВВУ
<input type="checkbox"/> <b>Верификация от ПДУ</b>			
<input type="checkbox"/> <b>Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)</b>			
<input type="checkbox"/> <b>Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)</b>			
<input type="checkbox"/> <b>Контроль времени для идентификаторов СОТРУДНИКОВ</b>			
<input type="checkbox"/> <b>Контроль времени для идентификаторов ПОСЕТИТЕЛЕЙ</b>			
<input type="checkbox"/> <b>Дополнительные входы, маскируемые при разблокировке ИУ</b>			
<input type="checkbox"/> <b>Дополнительные выходы, активизируемые при разблокировке ИУ</b>			
<input type="checkbox"/> <b>Дополнительные выходы, нормализируемые при разблокировке ИУ</b>			
<input type="checkbox"/> <b>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ</b>			
<input type="checkbox"/> <b>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ</b>			
Изымать идентификаторы ПОСЕТИТЕЛЕЙ			Нет

6. Конфигурация первого алкотестера на вход завершена. Перейдем к конфигурации второго алкотестера на выход.
7. Выделите ресурс типа "дополнительный вход" и переименуйте его в **Вход "Подтверждение от алкотестера" на выход**. На панели **Параметры**:
  - для параметра **Тип** установите значение **Подтверждение от ВВУ**;
  - для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели);

- для параметров **Контроллер**, **Считыватель** выберите контроллер и считыватель, для которых будет подтвержден проход от алкотестера на выход:

Параметры	
Адрес	5
Текущее наименование	Вход "Подтверждение от алкотестера" на выход
Первоначальное наименование	Дополнительный вход №5
Тип	Подтверждение от ВВУ
Подтверждение от ВВУ	
Нормальное состояние контакта	Разомкнут
Контроллер	Стойка турникета №1
Считыватель	Считыватель на выход
+ Дополнительные входы, маскируемые при активизации	
+ Дополнительные выходы, активизируемые при активизации	
+ Дополнительные выходы, нормализируемые при активизации	



**Примечание:**

Если к контроллеру подключен только один выход алкотестера на выход, то **Вход "Подтверждение от алкотестера" на выход** конфигурируется в зависимости от типа управляющего сигнала. При этом **Вход "Запрет от алкотестера" на выход** при этом не используется.


8. Выделите ресурс типа "дополнительный вход" и переименуйте его в **Вход "Запрет от алкотестера" на выход**. На панели **Параметры**:
  - для параметра **Тип** установите значение **Запрет от ВВУ**;
  - для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели);
  - для параметров **Контроллер**, **Считыватель** выберите контроллер и считыватель, для которых будет отклонен проход от алкотестера на выход:

Параметры	
Адрес	6
Текущее наименование	Вход "Запрет от алкотестера" на выход
Первоначальное наименование	Дополнительный вход №6
Тип	Запрет от ВВУ
Запрет от ВВУ	
Нормальное состояние контакта	Разомкнут
Контроллер	Стойка турникета №1
Считыватель	Считыватель на выход
+ Дополнительные входы, маскируемые при активизации	
+ Дополнительные выходы, активизируемые при активизации	
+ Дополнительные выходы, нормализируемые при активизации	

9. Выделите ресурс типа "считыватель" и переименуйте его в **Считыватель на выход**. На панели **Параметры**:
  - для параметра **Способ верификации** установите значение **ВВУ**;
  - в раскрывшемся списке отметьте флажками параметры: **при проходе СОТРУДНИКОВ**;
  - для параметра **Время ожидания подтверждения** установите требуемое значение времени, в течение которого контроллер должен ожидать управляющий сигнал от алкотестера на выход;

- для параметра **По истечении времени ожидания подтверждения генерировать событие** установите значение **Запрет прохода от ВВУ**, если к контроллеру подключены два выхода алкотестера на выход (для управляющего сигнала разрешения и запрета прохода). В ином случае - **Отказ от прохода, нет ответа от ВВУ**.

Параметры	
Адрес	2
Текущее наименование	Считыватель на выход
Первоначальное наименование	Считыватель №2
Модель	PERCo-IRxx
Способ верификации	ВВУ
[-] <b>Верификация от ВВУ</b>	
[-] <b>в РЕЖИМЕ работы "Контроль"</b>	
при проходе СОТРУДНИКОВ	<input checked="" type="checkbox"/>
при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ	<input type="checkbox"/>
при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ	<input type="checkbox"/>
при проходе ПОСЕТИТЕЛЕЙ	<input type="checkbox"/>
при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ	<input type="checkbox"/>
при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	<input type="checkbox"/>
Подтверждение прохода для ПОСЕТИТЕЛЕЙ	Постоянно
Время ожидания подтверждения	30 сек.
По истечении времени ожидания подтверждения генерировать событие	Запрет прохода от ВВУ
[+] <b>Верификация от ПДУ</b>	
[+] <b>Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)</b>	
[+] <b>Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)</b>	
[+] <b>Контроль времени для идентификаторов СОТРУДНИКОВ</b>	
[+] <b>Контроль времени для идентификаторов ПОСЕТИТЕЛЕЙ</b>	
[+] <b>Дополнительные входы, маскируемые при разблокировке ИУ</b>	
[+] <b>Дополнительные выходы, активизируемые при разблокировке ИУ</b>	
[+] <b>Дополнительные выходы, нормализируемые при разблокировке ИУ</b>	
[+] <b>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ</b>	
[+] <b>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ</b>	
Изымать идентификаторы ПОСЕТИТЕЛЕЙ	Нет

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

### 3.2.8.4 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 задается 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 (отсчет 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, освещенности 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 с 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 подключенным 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 зеленая 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 производиться 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 **Настройках 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**:

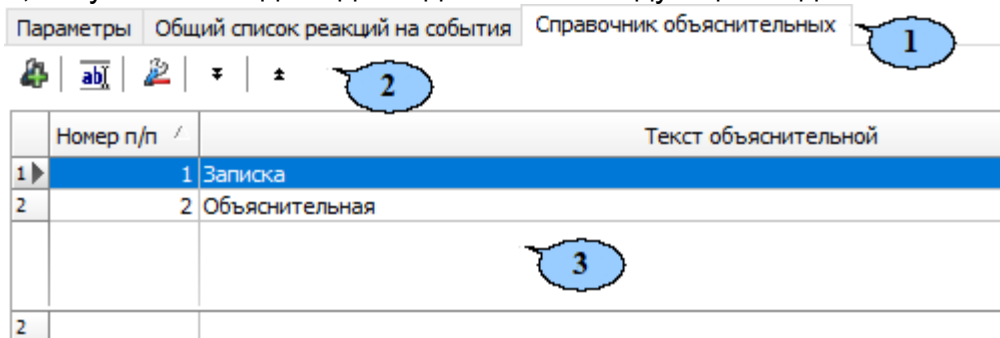
- параметр **Блокировать замок при закрытии двери** – при установке флажка дверь будет заблокирована сразу после закрытия;
- параметр **Блокировать замок по таймауту, только если дверь закрыта** – при установке флажка замок будет заблокирован по истечении **Времени удержания в разблокированном состоянии** 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**.



### 3.2.9 Подкладка «Справочник объяснительных»

Рабочее окно подкладки **Справочник объяснительных** доступно при выборе корневого элемента списка объектов (по умолчанию «Система безопасности»). Подкладка предназначена для создания и редактирования объяснительных, которые передаются в контроллер **CR11**. В интерфейсе контроллера из созданного ранее списка объяснительных есть возможность выбрать причину (объяснительную) опоздания, отсутствия и т.д. Подкладка имеет следующий вид:



1. Выбор подкладки панели настройки:

- [Параметры](#);
- [Справочник объяснительных](#);
- [События](#);
- [Настройка реакций](#);
- [Камера СКУД](#).

2. Панель инструментов содержит следующие кнопки:

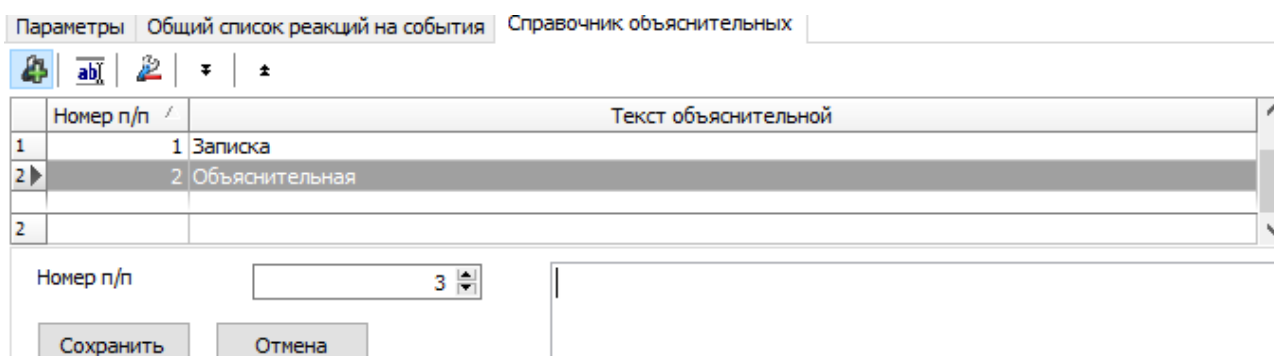
- **Добавить** – для создания новой объяснительной.
- **Изменить** – для изменения названия элемента, выбранного в рабочей области раздела.
- **Удалить** – для удаления элемента, выбранного в рабочей области раздела.
- **Переместить** – для последовательного выбора элемента в рабочей области раздела.



3. Рабочая область подкладки **Справочник объяснительных** содержит список созданных документов.

#### 3.2.9.1 Создание объяснительной

Для создания объяснительной:

1. Нажмите кнопку **Добавить** на панели инструментов вкладки. Откроется новое окно:



2. В поле **Номер п/п** укажите номер объяснительной с помощью клавиатуры или используйте счетчик .
3. В пустое поле введите текст для объяснительной.
4. Для сохранения изменений нажмите **ОК**. Для выхода без сохранения нажмите **Отмена**.
5. Для передачи измененных параметров нажмите на панели инструментов раздела кнопку  **Передать измененные параметры**.

### 3.2.10 Подкладка «События»

На подкладке **События** перечислен список событий мониторинга, регистрируемых устройством, выделенным в рабочей области раздела. В разделе реализована возможность [настроить реакцию системы](#) на любое из этих событий.

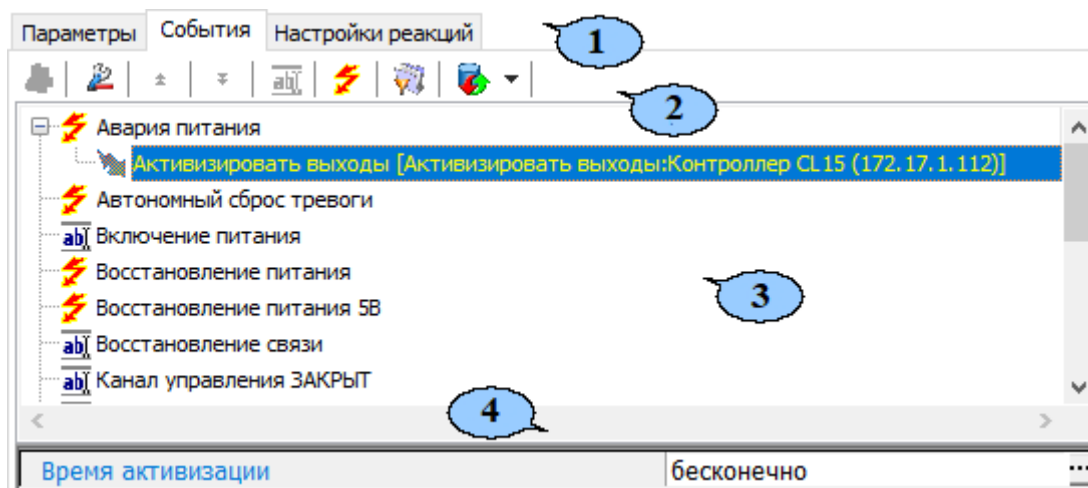
Реакция системы это предварительно заданная оператором последовательность команд, автоматически выполняемая устройствами системы.








#### **Внимание!**

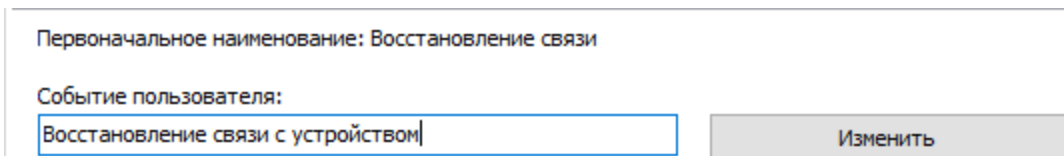
Команды, определенные как реакция на событие, будут выполняться только при запущенном сервере системы безопасности и наличии связи с соответствующими устройствами.

Подкладка имеет следующий вид:



1. Выбор подкладки панели настройки:
  - [Параметры](#);
  - [Справочник объяснительных](#);
  - **События**;
  - [Настройка реакций](#);
  - [Камера СКУД](#).
2. На подкладке 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.
  -  **Переместить вверх** (**Ctrl+Up**) – кнопка позволяет переместить выбранную в рабочей области реакцию на событие вверх в порядке следования реакций.

-  **Переместить вниз (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:






Первоначальное наименование: Восстановление связи




Событие пользователя:

Восстановление связи с устройством

Изменить

-  **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:

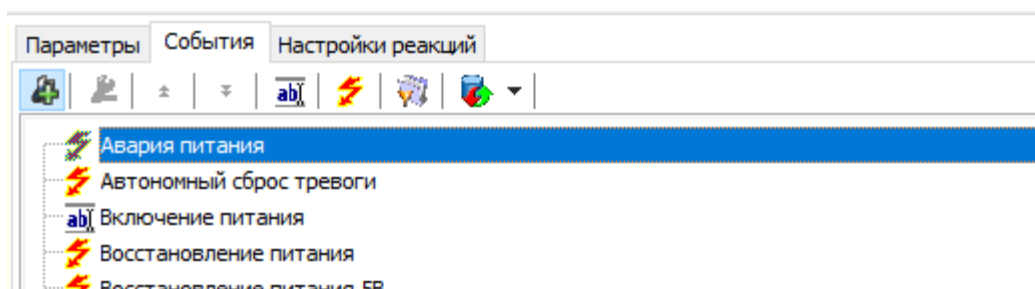
-  – событие (мониторинга), регистрируемое устройством или ресурсом, поддерживающее возможность задания реакции системы;
-  – событие, регистрируемое устройством или ресурсом системы;
-  – установленная для события команда.


4. Панель для настройки дополнительных параметров команд.

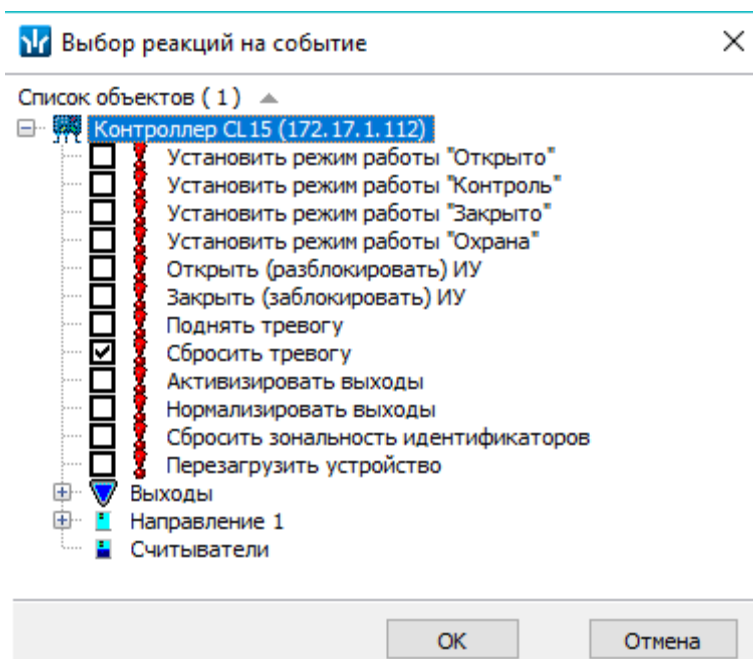
### 3.2.10.1 Задание реакции на событие

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

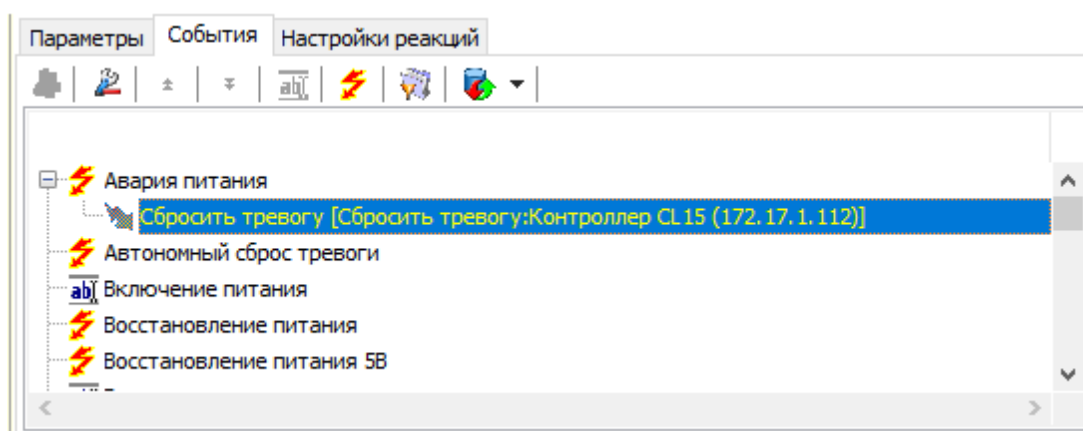
1. Выделите устройство или ресурс, на событие которого необходимо задать реакцию системы в рабочей области раздела.
2. На панели настройки перейдите на вкладку **События**:






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:

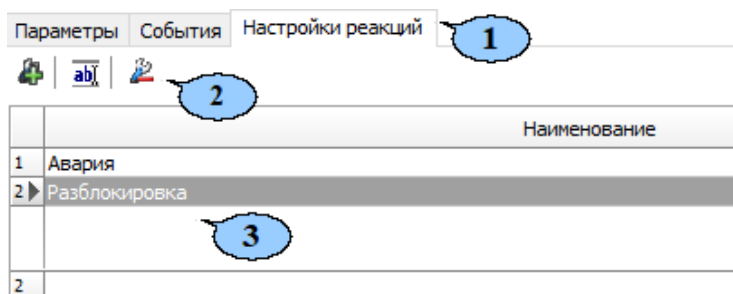


6. Установите последовательность выполнения команд, используя кнопки  /  **Переместить вверх / вниз** в инструментах панели.
7. При необходимости установите длительность выполнения команды на панели для ввода дополнительных параметров.
8. Для удаления выделенной в рабочей области реакции на событие нажмите кнопку  **Удалить реакцию на событие**. В открывшемся окне подтверждения нажмите **Да**.
9. Нажмите кнопку **Сохранить** на панели инструментов **«Консоли управления»**.

### 3.2.11 Подкладка «Настройка реакций»

Подкладка **Настройка реакций** позволяет настроить реакции на события в контроллере.

Рабочее окно подкладки имеет следующий вид:

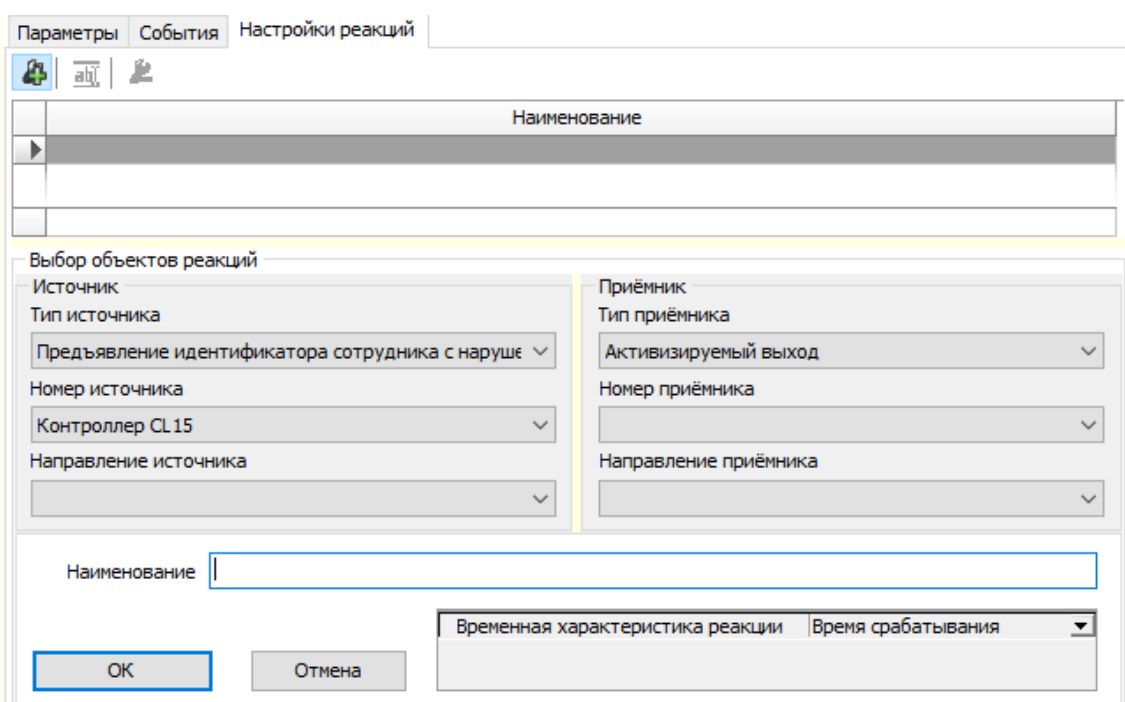


- Выбор подкладки панели настройки:
  - [Параметры](#);
  - [Справочник объяснительных](#);
  - [События](#);
  - **Настройка реакции**;
  - [Камера СКУД](#).
- Панель инструментов содержит следующие кнопки:
  - **Добавить** – для создания реакции.
  - **Изменить название** – для изменения названия элемента, выбранного в рабочей области раздела.
  - **Удалить** – для удаления элемента, выбранного в рабочей области раздела.
- Список созданных реакций.


#### 3.2.11.1 Настройка реакций

Для настройки реакции в устройстве:

- Нажмите кнопку **Добавить** на панели инструментов вкладки. Откроется новое окно:

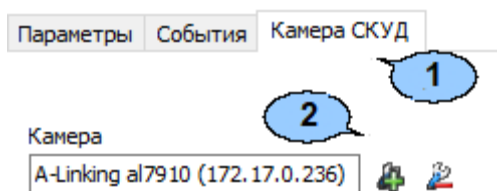



1. В окне **Источник** с помощью выпадающего списка выберите **Тип источника**:
  - **Активизация входа FIRE ALARM;**
  - **Активизация датчика вскрытия корпуса;**
  - **Блокировка ИУ (нормализация выхода управления ИУ);**
  - **Закрывание ИУ (нормализация входа PASS);**
  - **ИУ перешло в режим «Охрана»;**
  - **ИУ перешло в режим «Тревога»;**
  - **ИУ снято с охраны;**
  - **Команда от сервера;**
  - **Недопустимо долгое открытие ИУ в РКД "КОНТРОЛЬ";**
  - **Несанкционированная разблокировка ИУ в РКД "КОНТРОЛЬ";**
  - **акция входа FIRE ALARM;**
  - **Открывание ИУ (активизация входа PASS);**
  - **Предъявление идентификатора, отсутствующего в списке;**
  - **Предъявление идентификатора посетителя;**
  - **Предъявление идентификатора посетителя с нарушением времени;**
  - **Предъявление идентификатора посетителя с нарушением комиссионирования;**
  - **Предъявление идентификатора посетителя с нарушением местоположения;**
  - **Предъявление идентификатора посетителя с нарушением режима доступа;**
  - **Предъявление идентификатора с истекшим сроком действия;**
  - **Предъявление идентификатора сотрудника;**
  - **Предъявление идентификатора сотрудника с нарушением времени;**
  - **Предъявление идентификатора сотрудника с нарушением комиссионирования;**
  - **Предъявление идентификатора сотрудника с нарушением местоположения;**
  - **Предъявление идентификатора сотрудника с нарушением режима доступа;**
  - **Предъявление идентификатора, который заблокирован;**
  - **Разблокировка ИУ (активизация выхода управления ИУ);**
  - **Разблокировка ИУ в РКД "ЗАКРЫТО";**
  - **Активизация входа (тип обычный).**
2. Выберите с помощью выпадающего списка **Номер источника** и **Направление источника**.
3. В окне **Приемник** выберите из выпадающего списка **Тип приемника**:
  - **Активизируемый выход;**
  - **Маскируемый вход (тип обычный);**
  - **Нормализуемый выход.**
4. Выберите с помощью выпадающего списка **Номер приемника** и **Направление приемника**.
5. В поле **Наименование** введите название для реакции.
6. В поле **Временная характеристика реакции** выберите из выпадающего списка:
  - **Время срабатывания.**

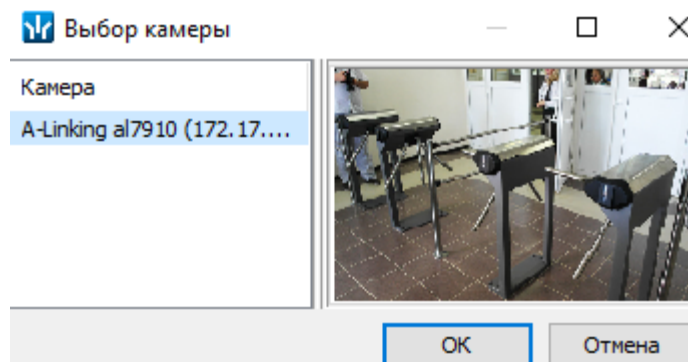
- **Время абсолютное.** Для этого выберите из выпадающего списка параметр **Время абсолютное**. В поле **Время реакции** нажмите кнопку . Откроется новое окно **Изменить значение**. Выберите необходимое время или установите флажок около параметра **Бесконечно**. Для сохранения изменений нажмите **Сохранить**, для закрытия окна без сохранений нажмите **Отменить**.
  - **Время после срабатывания.** Для этого выберите из выпадающего списка параметр **Время после срабатывания**. В поле **Время реакции** нажмите кнопку . Откроется новое окно **Изменить значение**. Выберите необходимое время или установите флажок около параметра **Бесконечно**. Для сохранения изменений нажмите **Сохранить**, для закрытия окна без сохранений нажмите **Отменить**.
7. Для сохранения реакции нажмите **Сохранить**, для выхода без сохранения нажмите **Отменить**.
  8. Для передачи измененных параметров нажмите на панели инструментов раздела кнопку  **Передать измененные параметры**.

### 3.2.12 Подкладка «Камера СКУД»


Подкладка 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 видеочамера может использоваться при работе с несколькими считывателями.



1. Выбор подкладки панели настройки:
  - [Параметры](#);
  - [Справочник объяснительных](#);
  - [События](#);
  - [Настройка реакций](#);
  - **Камера СКУД**.
2. На подкладке доступны следующие инструменты:
  -  **Добавить камеру** – кнопка позволяет открыть окно **Выбор камеры**:



Для выбора камеры, которая будет использоваться, как камера СКУД для считывателя, выделите нужную камеру в рабочей области. Для удобства выбора 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**.

### 3.2.13 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:

Развернуть все	Alt+E
Свернуть все	Alt+C
Скрыть дополнительную информацию	Alt+H



**Примечание:**

Для контроллеров **PERCo-CT/L04.2** панель дополнительных данных не доступна. Настройка комиссионированных 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 комиссионированных 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 комиссионированных карт сотрудников](#) и [Список карт аварийного доступа](#) (см. *Руководство по эксплуатации PERCo-CL201*).

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

#### 3.2.13.1 Список комиссионированных карт

**Комиссионирование** - процедура подтверждения прав предъявленной карты посредством предъявления второй, комиссионированной карты.

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



**Примечание:**

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

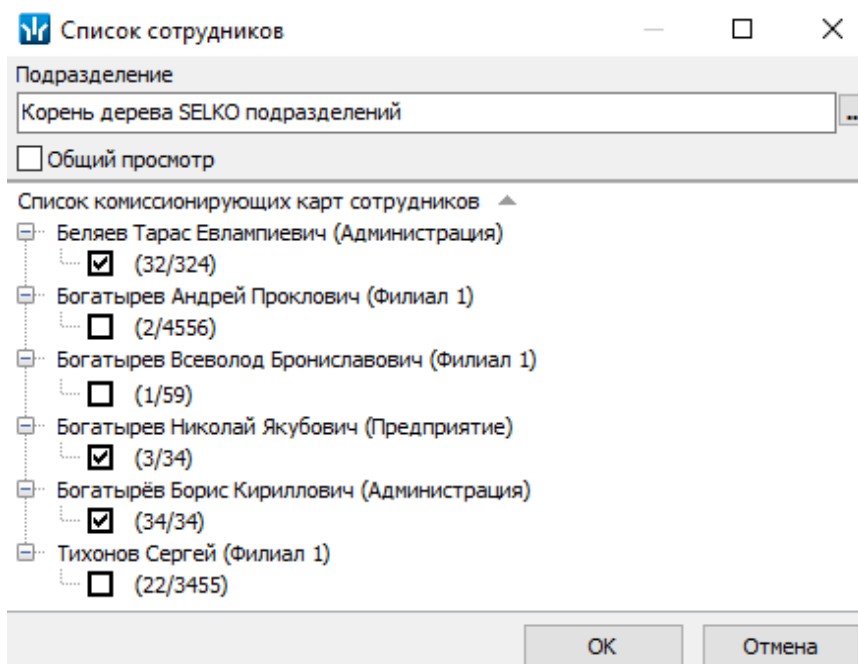
Для контроллера **PERCo-CT/L04** в конфигурации «Контроллер АТП» процедура подтверждения прав предъявленной карты может осуществляться картой охранника, имеющей право на досмотр, то есть внесенной в **Список карт, имеющих право на досмотр**.




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

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

		Сотрудник	Подразделение	Идентификатор
1	✘	Беляев Тарас Евлампиевич	Администрация	32 / 324
2	✔	Богатырев Николай Якубович	Предприятие	3 / 34
3	✔	Богатырёв Борис Кириллович	Администрация	34 / 34

- **Добавить в список (Shift+Alt+N)** – кнопка позволяет добавить карту сотрудника (охранника) в список коммиссионированных (имеющих право на досмотр) карт.
  - **Удалить из списка (Shift+Alt+D)** – кнопка позволяет удалить выделенную в рабочей области вкладки карту сотрудника (охранника) из списка коммиссионированных (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 коммисионирующих 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 кнопку **Да**.
6. Для сохранения списка 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.

### 3.2.13.2 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.

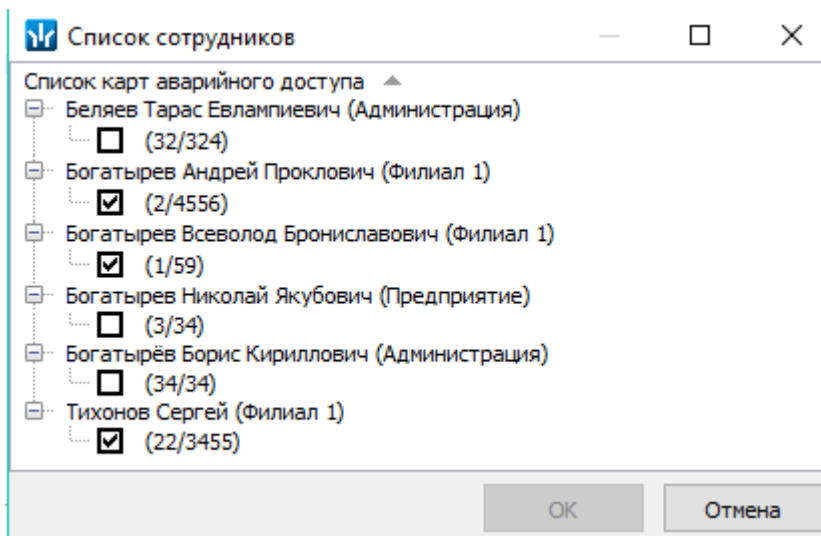
Для внесения карты сотрудника в список карт аварийного доступа:



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**:

		Сотрудник	Подразделение	Идентификатор
1		Богатырев Андрей Проклович	Филиал 1	2 / 4556
2		Богатырев Всеволод Брониславович	Филиал 1	1 / 59
3		Тихонов Сергей	Филиал 1	22 / 3455

-  **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.

- 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:



- 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**.
- Для сохранения списка в БД системы нажмите кнопку **Сохранить** на панели инструментов **«Консоли управления»**.
- Для передачи прав карт в контроллер нажмите кнопку  **Передать измененные параметры** на панели инструментов раздела.

### 3.2.13.3 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.

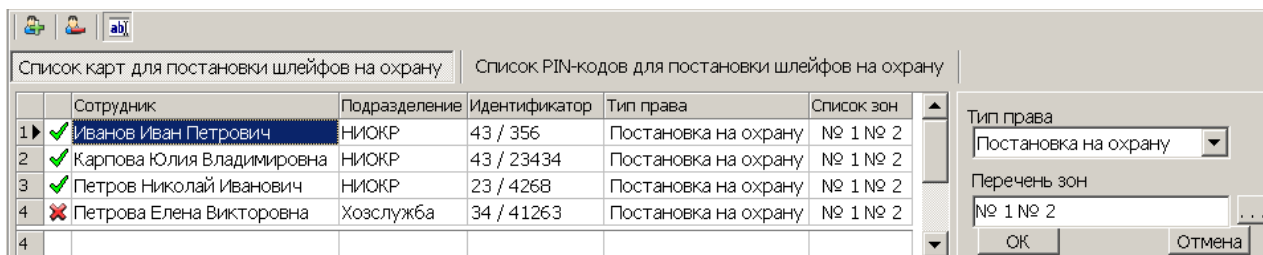





#### **Примечание:**


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.

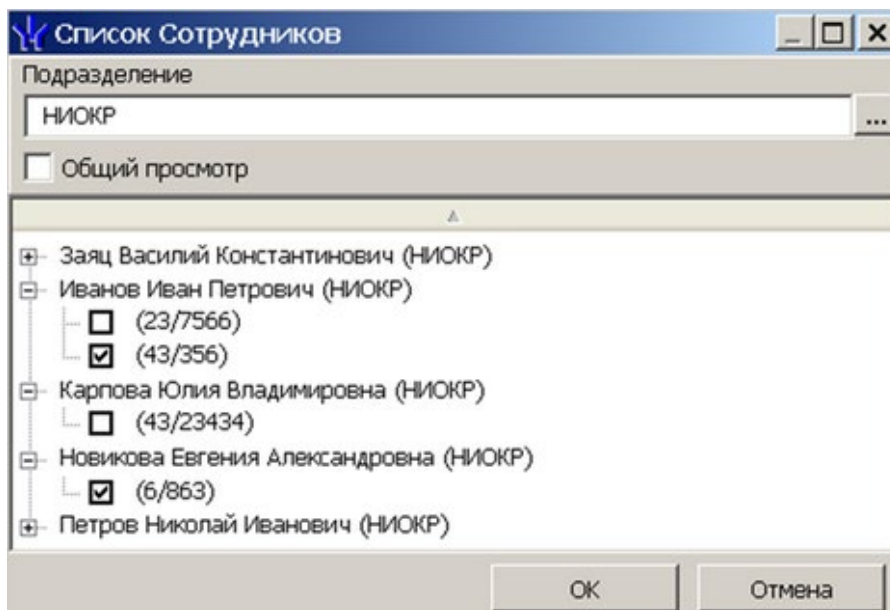
Для внесения карты сотрудника в список:



- 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**:

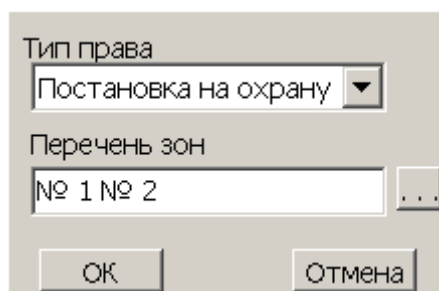


-  **Добавить в список (Shift+Alt+N)** – кнопка позволяет добавить карту в список карт имеющих право постановки шлейфов, включенных в ОЗ, перечисленные в списке **Перечень зон** на охрану.
-  **Удалить из списка (Shift+Alt+D)** – кнопка позволяет удалить выделенную в рабочей области вкладки карту сотрудника (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 для задания прав (если необходимо отредактировать права, нажмите кнопку  **Изменить**):





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.**

- 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....**:



- В открывшемся окне отметьте флажками зоны, управление которыми будут доступно по карте. Нажмите кнопку **ОК**.
- Нажмите кнопку **ОК** на панели задания прав, панель будет закрыта.
- 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**.
- Для сохранения списка в БД системы нажмите кнопку **Сохранить** на панели инструментов **«Консоли управления»**.
- Для передачи прав карт в контроллер нажмите кнопку  **Передать измененные параметры** на панели инструментов раздела.

### 3.2.13.4 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.

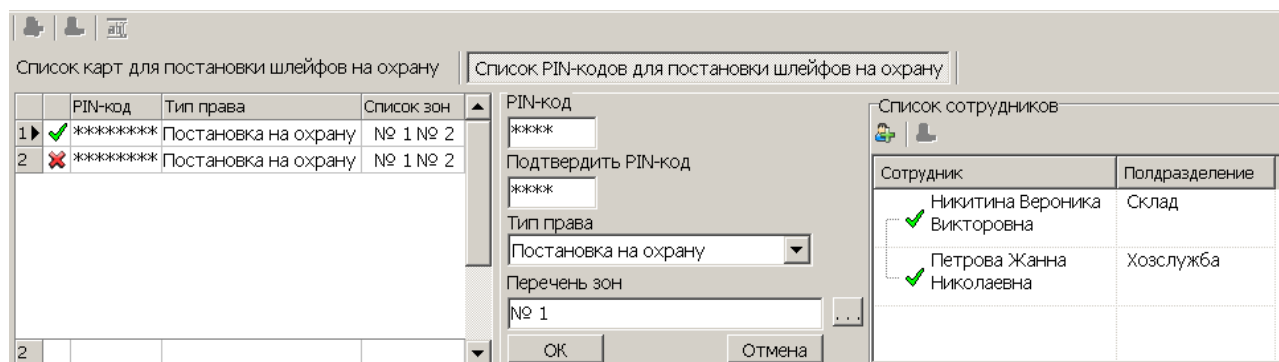



#### Примечания:





- 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.

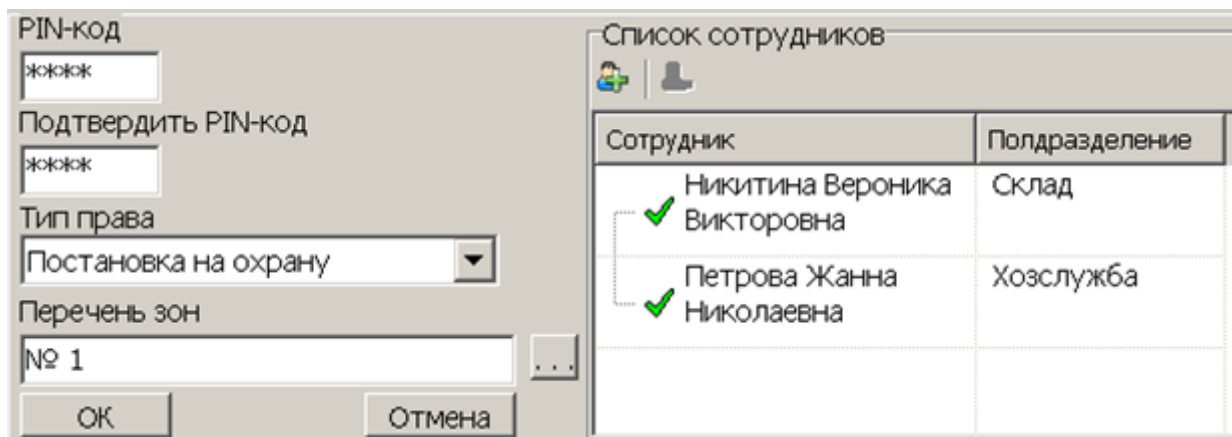
Для добавления в список нового PIN-кода:

- 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**:




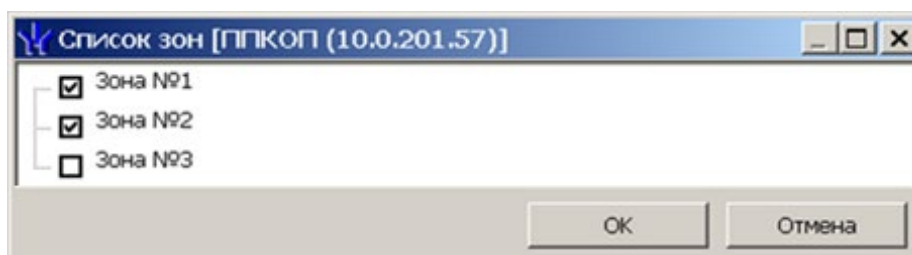
-  **Добавить в список (Shift+Alt+N)** – кнопка позволяет добавить новый PIN-код.


-  **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):

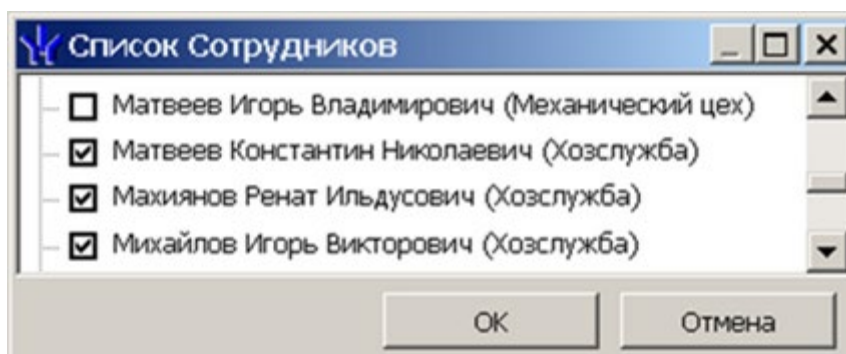




Сотрудник	Подразделение
<input checked="" type="checkbox"/> Никитина Вероника Викторовна	Склад
<input checked="" type="checkbox"/> Петрова Жанна Николаевна	Хозслужба

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...**:




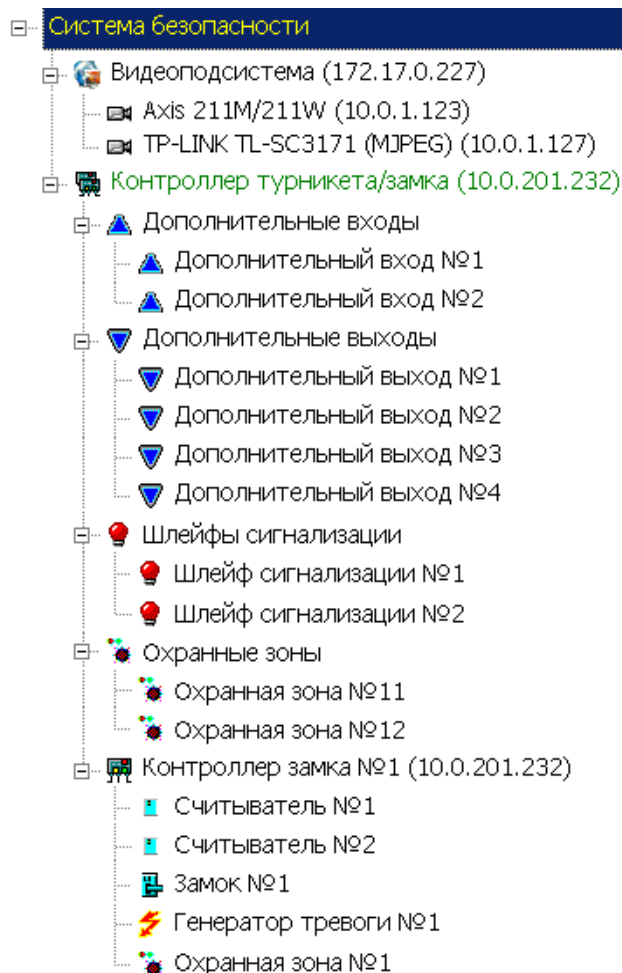
6. В открывшемся окне отметьте флажками зоны, управление которыми будет доступно с использованием PIN-кода. Нажмите кнопку **ОК**.
7. Нажмите кнопку  **Добавить в список** в области **Список сотрудников**. Откроется окно **Список сотрудников**:



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 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.

### 3.2.14 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](#);
- [Дополнительный вывод](#);
- [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.

### 3.2.14.1 Ресурсы контроллеров и ЭП PERCo 0.X серии x.1

Модель*	Доп. вход	Доп.выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считыватель	ИУ	Ген. тревоги	ЗС
<b>Контроллеры PERCo</b>									
CL201	0	0	0	0	-	1	замок	1	1
СТ/L04 (1)	2	4	2	2	0	2	замок	1	1
СТ/L04 (2)	2	4	2	2	8	2	замок	1	1
СТ/L04 (3)	2	4	2	2	8	2	2 замка	2	2
СТ/L04 (4)	2	2	0	0	0	2	турникет	1	0
СТ/L04 (5)	2	2	0	0	8	2	турникет	1	0
СТ/L04 (6)	2	2	0	0	0	2	шлагбаум	1	0
СТ/L04 (7)	2	2	0	0	8	2	шлагбаум	1	0
CL05	0	1	0	0	0	1	замок	1	1
<b>Контроллер ЭП PERCo</b>									
СТ03(1)	2	2	0	0	0	2	турникет	1	0
СТ03(2)	2	2	0	0	8	2	турникет	1	0
<b>Контроллер регистрации PERCo</b>									
CR01	-	-	-	-	-	2	-	-	-
<b>Контроллеры ППКОП PERCo</b>									
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**.



## 3.2.14.2 Ресурсы контроллеров и ЭП PERCo 0.X серии x.2

Модель	Доп. вход	Доп. выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считыватель	ИУ	Ген. тревоги	ОЗ
<b>Контроллеры доступа</b>									
CL201	0	0	0	0	-	1	L	1	1
СТ/L04.2 (1)	4	4	0	0	до 8	2	T	1	0
СТ/L04.2 (2)	2	3	0	0	до 8	3	T+L	2	1
СТ/L04.2 (3)	0	2	0	0	до 8	4	T+L+L	3	2
СТ/L04.2 (4)	2	3	0	0	до 8	4	T+2L	2	1
СТ/L04.2 (5)	4	4	0	0	до 8	2	T(KR05.2)	1	0
СТ/L04.2 (6)	5	4	0	0	до 8	2	G	1	0
СТ/L04.2 (7)	3	3	0	0	до 8	3	G+L	2	1
СТ/L04.2 (8)	1	2	0	0	до 8	4	G+L+L	3	2
СТ/L04.2 (9)	3	3	0	0	до 8	4	G+2L	2	1
СТ/L04.2 (10)	5	8	2	2	до 8	1	L	1	1
СТ/L04.2 (11)	6	8	1	1	до 8	1	L	1	1
СТ/L04.2 (12)	7	8	0	0	до 8	1	L	1	1
СТ/L04.2 (13)	3	7	2	2	до 8	2	L+L	2	2
СТ/L04.2 (14)	4	7	1	1	до 8	2	L+L	2	2
СТ/L04.2 (15)	5	7	0	0	до 8	2	L+L	2	2
СТ/L04.2 (16)	2	6	1	1	до 8	3	L+L+L	3	3
СТ/L04.2 (17)	3	6	0	0	до 8	3	L+L+L	3	3
СТ/L04.2 (18)	0	4	0	0	до 8	4	L+L+L+L	4	4
СТ/L04.2 (19)	5	8	2	2	до 8	2	2L	1	1
СТ/L04.2 (20)	6	8	1	1	до 8	2	2L	1	1
СТ/L04.2 (21)	7	8	0	0	до 8	2	2L	1	1
СТ/L04.2 (22)	4	7	1	1	до 8	3	2L+L	2	2
СТ/L04.2 (23)	5	7	0	0	до 8	3	2L+L	2	2
СТ/L04.2 (24)	3	6	0	0	до 8	4	2L+L+L	3	3
СТ/L04.2 (25)	4	7	1	1	до 8	4	2L+2L	2	2
СТ/L04.2 (26)	5	7	0	0	до 8	4	2L+2L	2	2
CL05.2	1/1		0	0	-	1	L	1	1
<b>Контроллер регистрации</b>									
CR01.2\ CR01.9	-	-	-	-	-	2	-	-	-
<b>Электронные проходные</b>									
СТ03 (1)	4	4	0	0	до 8	2	IP-Stile	1	0
СТ03 (2)	2	3	0	0	до 8	2	IP-Stile+IC	1	0
СТ03 (3)	4	3	0	0	до 8	2	IP-Stile+AP	1	0
СТ03 (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;
- **T(KR05.2)** – ЭП (**KR05.2**);
- **G** – шлагбаум;
- **IP-Stile** – электронная проходная;
- **IC** – встроенный картоприемник;
- **AP** – встроенное устройство «Антипаника».

**Варианты шаблонов конфигурации контроллера PERCo-CT/L04.2 (к любой конфигурации можно 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 электронной проходной KR05.2.
6. Контроллер для управления автотранспортной проходной (АТП).
7. Контроллер для управления АТП и одним односторонним замком.
8. Контроллер для управления АТП и двумя односторонними замками.
9. Контроллер для управления АТП и одним двусторонним замком.
10. Контроллер для управления одним односторонним замком с двумя ШС.
11. Контроллер для управления одним односторонним замком с одним ШС.
12. Контроллер для управления одним односторонним замком.
13. Контроллер для управления двумя односторонними замками с двумя ШС.
14. Контроллер для управления двумя односторонними замками с одним ШС.
15. Контроллер для управления двумя односторонними замками.
16. Контроллер для управления тремя односторонними замками с одним ШС.
17. Контроллер для управления тремя односторонними замками.
18. Контроллер для управления четырьмя односторонними замками.
19. Контроллер для управления одним двусторонним замком с двумя ШС.
20. Контроллер для управления одним двусторонним замком с одним ШС.
21. Контроллер для управления одним двусторонним замком.
22. Контроллер для управления одним двусторонним и одним односторонним замками с одним ШС.
23. Контроллер для управления одним двусторонним и одним односторонним замками.
24. Контроллер для управления одним двусторонним и двумя односторонним замками.
25. Контроллер для управления двумя двусторонними замками с одним ШС.
26. Контроллер для управления двумя двусторонними замками.

**Варианты шаблонов конфигурации ЭП PERCo-CT03 (к любой конфигурации можно 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».

## 3.2.14.3 Ресурсы контроллеров и ЭП PERCo 1.X

Модель (номер шаблона)	Доп. вход	Доп. выход	CL201/ CL211	Контроллер ИУ	
				Считыватель (+сканнер)	ИУ
<b>Контроллеры доступа</b>					
CL201/CL211	0	0	-	1	L
CT/L14\CT/L14.1 (1)	10	6	до 8	2 (+2)	G
CT/L14\CT/L14.1 (2)	6	4	до 8	4 (+2)	G +L+L
CT/L14\CT/L14.1 (3)	5	4	до 8	4 (+2)	G +T
CT/L14\CT/L14.1 (4)	5	3	до 8	4 (+2)	L+L+L+L
CT/L14\CT/L14.1 (5)	4	3	до 8	4 (+2)	T+L+L
CT/L14\CT/L14.1 (6)	3	3	до 8	4 (+2)	T+T
CT/L14\CT/L14.1 (7)	9	5	до 8	4 (+2)	Шлюз (L+L)
CT/L14\CT/L14.1 (8)	8	5	до 8	4 (+2)	Шлюз (T)
CT/L14\CT/L14.1 (9)	6	4	до 8	4 (+2)	Шлюз (T+L)
CT/L14\CT/L14.1(10)	3	3	до 8	4 (+2)	Шлюз (T+T)
CT/L14\CT/L14.1(11)	7	5	до 8	4 (+2)	Шлюз (G+G)
CL15, CL15.1, CL15.3, CL15.7	1	1	-	1	L
<b>Контроллер регистрации</b>					
CR11, CR11.1	-	-	-	1 на 2 направления	-
<b>Электронные проходные</b>					
CT13\CT13.1 (1)	8	5	до 8	2 (+2)	IP-Stile
CT13\CT13.1 (2)	7	4	до 8	2 (+2)	IP-Stile+IC
CT13\CT13.1 (3)	8	4	до 8	2 (+2)	IP-Stile+AP
CT13\CT13.1 (4)	7	3	до 8	2 (+2)	IP-Stile+IC+AP

Принятые в таблице сокращения:

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

**Варианты шаблонов конфигурации контроллера PERCo-CT/L14, PERCo-CT/L14.1:**

1. АТП;
2. АТП и замки;
3. АТП и турникет;
4. Замки;
5. Турникет и замки;
6. Турникеты;
7. Шлюз из замков;
8. Шлюз из роторного турникета;
9. Шлюз из турникета и замка;
10. Шлюз из турникетов;
11. Шлюз из шлагбаумов.

**Варианты шаблонов конфигурации контроллера ЭП PERCo-CT13 / PERCo-CT13.1):**

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».

### 3.2.14.4 Контроллер доступа

В окне доступны следующие параметры:

Параметры		События
MAC-адрес	00:25:08:00:FB:92	
IP-адрес	172.17.17.133	
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 журнала отладки	18908	
Порт индикации	18904	
Порт верификации	18905	
Текущее наименование	Контроллер турникета/замка	
Первоначальное наименование	Контроллер турникета/замка	
Модель	PERCo-CT/L04	
Разрешить WEB-интерфейс	<input type="checkbox"/>	
Коррекция времени относительно времени сервера системы	0 час.	

- **Текущее наименование.** Поле ввода позволяет изменить 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.

### 3.2.14.5 Контроллер регистрации (LICON)

В окне доступны следующие параметры:

Параметры		События	
MAC-адрес		00:25:08:01:69:A3	
IP-адрес		10.1.105.163	
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 журнала отладки		18908	
Порт индикации		18904	
Порт персонализации		18907	
Макс. кол-во карт доступа		50016	
Текущее наименование		Контроллер регистрации	
Первоначальное наименование		Контроллер регистрации	
Модель		PERCo-CR01.2 LICON	
Разрешить WEB-интерфейс		<input type="checkbox"/>	
Коррекция времени относительно времени сервера системы		0 час.	
Прямое направление прохода		<input checked="" type="checkbox"/>	
Защита от передачи идентификаторов (Antipass)		Нет	
Время ожидания персонализации		5 сек.	
Время отображения персонализации		5 сек.	
+ Локализация отображаемых строк:			

- **Текущее наименование** Поле ввода позволяет изменить 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.** Выпадающий список позволяет изменить содержание сообщений, отображаемых на ЖКИ контроллера.

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

### 3.2.14.6 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:

Параметры	События
MAC-адрес	00:25:0B:00:00:39
IP-адрес	10.0.201.57
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
Максимальное количество ключей	200
Текущее наименование	ППКОП
Первоначальное наименование	ППКОП
Модель	PERCo-PU01
Коррекция времени относительно времени сервера системы	0 час.
Использовать встроенный звуковой извещатель	<input type="checkbox"/>
Режим активизации кнопки "КЛЮЧ"	Одно длинное нажатие
Включить интеграцию с ПЦН "АИР"	<input type="checkbox"/>

- **Текущее наименование.** Поле ввода позволяет изменить 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 активизации кнопки "КЛЮЧ".** Выпадающий 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»**.

### 3.2.14.7 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 шесть ресурсов УОО:

Текущее наименование	Объект интеграции с ПЦН "АИР"
Первоначальное наименование	Объект интеграции с ПЦН "АИР"
<b>Сетевые параметры концентратора</b>	
IP-адрес	10.0.201.254
Маска подсети	255.0.0.0

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

- **Сетевые параметры концентратора:**
  - IP-адрес;
  - Маска подсети.

Для каждого УОО доступны следующие параметры:

Текущее наименование	УОО №1
Адрес	1
Первоначальное наименование	УОО №1
Номер в концентраторе	29
<b>Зоны</b>	
Зона №1	<input checked="" type="checkbox"/>
Зона №2	<input type="checkbox"/>
Зона №3	<input type="checkbox"/>

- **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»

В окне доступны следующие параметры:

Адрес	5
Текущее наименование	Шлейф сигнализации №5
Первоначальное наименование	Шлейф сигнализации №5
Тип	КТС
КТС	
Длительность нарушения	70 мс.

- **Текущее наименование.** Поле ввода позволяет изменить название ресурса.
- **Длительность нарушения** – параметр определяет время интегрирования ШС.

### Тип зоны «КТС»

В окне доступны следующие параметры:

Адрес	3
Текущее наименование	Зона №3
Первоначальное наименование	Зона №3
Тип	КТС
КТС	
Шлейфы, активизирующие зону	
Шлейф сигнализации №5	<input checked="" type="checkbox"/>
Шлейф сигнализации №6	<input type="checkbox"/>

- **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.

### 3.2.14.8 Считыватель

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

Адрес	4
Текущее наименование	Считыватель №4
Первоначальное наименование	Считыватель №4
Модель	PERCo-IRxx
Способ верификации	Нет
[-] <b>Верификация от ВВУ</b>	
[+] <b>в РЕЖИМЕ работы "Контроль"</b>	
Подтверждение прохода для ПОСЕТИТЕЛЕЙ	Постоянно
Время ожидания подтверждения	5 сек.
По истечении времени ожидания подтверждения генерировать событие	Запрет прохода от ВВУ
[-] <b>Верификация от ПДУ</b>	
[+] <b>в РЕЖИМЕ работы "Контроль"</b>	
Подтверждение прохода для ПОСЕТИТЕЛЕЙ	Постоянно
Время ожидания подтверждения	5 сек.
[+] <b>Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)</b>	
[+] <b>Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)</b>	
[+] <b>Контроль времени для идентификаторов СОТРУДНИКОВ</b>	
[+] <b>Контроль времени для идентификаторов ПОСЕТИТЕЛЕЙ</b>	
[+] <b>Дополнительные входы, маскируемые при разблокировке ИУ</b>	
[+] <b>Дополнительные выходы, активизируемые при разблокировке ИУ</b>	
[+] <b>Дополнительные выходы, нормализируемые при разблокировке ИУ</b>	
[+] <b>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ</b>	
[+] <b>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ</b>	
Изымать идентификаторы ПОСЕТИТЕЛЕЙ	Нет <span style="float: right;">▼</span>

- **Текущее наименование.** Поле ввода позволяет изменить 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 или другое оборудование.
  - **Нет.** Подтверждение от верифицирующего устройства не требуется.



#### **Примечание:**

Если для параметра **Способ верификации** 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.

- **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**.
- **ВВУ.** Для верификации от алкотестера 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.**



### **Внимание!**

Возможность верификации от ВВУ доступна для контроллеров с версий прошивки x.0.0.20 и старше. Обратите внимание, что при обновлении прошивки изменяется конфигурация контроллера. Потребуется повторно добавить контроллер в конфигурацию системы.

- **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.** Рекомендуются в случае подключения ВВУ имеющего только один выход разрешения прохода.
  - **Отказ от прохода, нет ответа от ВВУ.** Рекомендуются 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 **Подтверждение от 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 сроком 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 идентификаторы ПОСЕТИТЕЛЕЙ.** Функция доступна только при наличии связи контроллера с сервером системы. Параметр позволяет выбрать условие, при котором идентификатор предъявленной карты доступа посетителя может быть автоматически изъят.
  - **Нет.** Идентификатор не изымается.
  - **После любого прохода.** Идентификатор изымается из доступа при первом предъявлении.
  - **После прохода в последний день действия идентификатора.** Идентификатор изымается из доступа, если дата предъявления совпадает с датой окончания срока действия карты.

### 3.2.14.9 ИУ (Замок / Турникет / Шлагбаум)

В окне доступны следующие параметры:

Параметры	
Адрес	1
Текущее наименование	Замок
Первоначальное наименование	Замок
Прямое направление прохода	<input checked="" type="checkbox"/>
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.
Регистрация прохода по предъявлению идентификатора	<input type="checkbox"/>
Внутренняя защита от передачи идентификаторов (Local Antipass)	<input type="checkbox"/>
<b>Дополнительные выходы, реагирующие через группу ресурсов</b>	

- **Текущее наименование.** Поле ввода позволяет изменить 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 переключки *«номер считывателя» (XP2)* на плате считывателя.
  - Если параметр отключен, то тот считыватель, который в соответствии с его переключкой 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 запрошен / Запрошен*) (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 комиссионированием / досмотром / подтверждением 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).

Также 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 параметре 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 производиться при взятой на охрану ОЗ. При снятом параметре (по умолчанию) в РКД «*Охрана*» сигналы на входах **Тип: Fire Alarm** игнорируются.

### 3.2.14.10 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**). В окне доступны следующие параметры:

Параметры	
Текущее наименование	Генератор тревоги
Первоначальное наименование	Генератор тревоги
<b>Генерация тревоги при предъявлении идентификатора</b>	
если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН	Нет
если ИДЕНТИФИКАТОР ЗАПРЕЩЕН	Нет
если ИСТЕК СРОК ДЕЙСТВИЯ	Нет
если НАРУШЕНО ВРЕМЯ	Нет
если НАРУШЕНА ЗОНАЛЬНОСТЬ	Нет
если НАРУШЕН РЕЖИМ РАБОТЫ	Нет
если НАРУШЕНО КОМИССИОНИРОВАНИЕ	Нет
<b>Генерация тревоги при несанкционированной разблокировке ИУ</b>	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Закрыто"	Нет
<b>Генерация тревоги по недопустимо долгому открытию ИУ</b>	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
Генерация тревоги по датчику вскрытия корпуса	Нет
<b>Дополнительные входы, активизирующие генерацию тревоги</b>	
Тип тревоги	Тихая
Дополнительный вход №1	<input type="checkbox"/>
Дополнительный вход №2	<input type="checkbox"/>

- **Текущее наименование.** Поле ввода позволяет изменить 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.** Тревога не генерируется.
  - **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.



### 3.2.14.11 Дополнительные входы

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.** Выпадающий 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 sireны.
  - **FireAlarm.** Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ *Fire Alarm*. Тип входа **FireAlarm** не может быть изменен для входов контроллеров и ЭП **PERCo** серии х.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 задает номер ИУ, к которому привязывается считыватель.
  - **Направление.** Параметр задает направление ИУ, к которому привязывается считыватель.

### 3.2.14.11.1 Тип входа «Обычный»

В окне доступны следующие параметры:

Параметры	
Адрес	1
Текущее наименование	Дополнительный вход №1
Первоначальное наименование	Дополнительный вход №1
Нормальное состояние контакта	Разомкнут
<input type="checkbox"/> Тип	Обычный
<input type="checkbox"/> <b>Обычный</b>	
<input type="checkbox"/> <b>Дополнительные входы, маскируемые при активизации</b>	
<input type="checkbox"/> Критерий маскирования	На указанное время
<input type="checkbox"/> <b>На указанное время</b>	
Время	0 мс.
Дополнительный вход №2	<input type="checkbox"/>
<input type="checkbox"/> <b>Дополнительные выходы, активизируемые при активизации</b>	
<input type="checkbox"/> Критерий активизации	На указанное время
<input type="checkbox"/> <b>На указанное время</b>	
Время	0 мс.
Дополнительный выход №1	<input type="checkbox"/>
Дополнительный выход №2	<input type="checkbox"/>
Дополнительный выход №3	<input type="checkbox"/>
Дополнительный выход №4	<input type="checkbox"/>
<input type="checkbox"/> <b>Дополнительные выходы, нормализируемые при активизации</b>	
<input type="checkbox"/> Критерий нормализации	На указанное время
<input type="checkbox"/> <b>На указанное время</b>	
Время	0 мс.
Дополнительный выход №1	<input type="checkbox"/>
Дополнительный выход №2	<input type="checkbox"/>
Дополнительный выход №3	<input type="checkbox"/>
Дополнительный выход №4	<input type="checkbox"/>

- **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, нормализуемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализованы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть нормализованы. 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.

### 3.2.14.11.2 Тип входа «Специальный»

В окне доступны следующие параметры:

Параметры		События	
Адрес		2	
Текущее наименование		Дополнительный вход №2	
Первоначальное наименование		Дополнительный вход №2	
Нормальное состояние контакта		Разомкнут	
<input type="checkbox"/> Тип		Специальный	
<input type="checkbox"/> Специальный			
Сброс тревоги (Генератор тревоги)		<input type="checkbox"/>	
Сброс сирены (Выход "С" ОПС)		<input type="checkbox"/>	

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



#### **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*.

### 3.2.14.11.3 Тип входа «Подтверждение от ВВУ»

Доступны следующие параметры:

Адрес	2
Текущее наименование	Дополнительный вход №2
Первоначальное наименование	Дополнительный вход №2
<input type="checkbox"/> Тип	Подтверждение от ВВУ
<input type="checkbox"/> <b>Подтверждение от ВВУ</b>	
Нормальное состояние контакта	Разомкнут
Контроллер	Контроллер замка CL201 №1
Считыватель	Считыватель CL201 №1
<input type="checkbox"/> <b>Дополнительные входы, маскируемые при активизации</b>	
<input type="checkbox"/> Критерий маскирования	На указанное время
<input type="checkbox"/> <b>На указанное время</b>	
Время	0 мс.
<input type="checkbox"/> <b>Дополнительные выходы, активизируемые при активизации</b>	
<input type="checkbox"/> Критерий активизации	На указанное время
<input type="checkbox"/> <b>На указанное время</b>	
Время	0 мс.
<input type="checkbox"/> <b>Дополнительные выходы, нормализируемые при активизации</b>	
<input type="checkbox"/> Критерий нормализации	На указанное время
<input type="checkbox"/> <b>На указанное время</b>	
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 ожидать сигнал подтверждения прохода. В этом качестве могут выступать также 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.
- **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 нормализованы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть нормализованы. 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.

#### 3.2.14.11.4 Тип входа «Запрет от ВВУ»

Доступны следующие параметры:

Адрес	2
Текущее наименование	Дополнительный вход №2
Первоначальное наименование	Дополнительный вход №2
<input type="checkbox"/> Тип	Запрет от ВВУ
<input type="checkbox"/> <b>Запрет от ВВУ</b>	
Нормальное состояние контакта	Разомкнут
Контроллер	Контроллер замка CL201 №1
Считыватель	Считыватель CL201 №1
<input type="checkbox"/> <b>Дополнительные входы, маскируемые при активизации</b>	
<input type="checkbox"/> Критерий маскирования	На указанное время
<input type="checkbox"/> <b>На указанное время</b>	
Время	0 мс.
<input type="checkbox"/> <b>Дополнительные выходы, активизируемые при активизации</b>	
<input type="checkbox"/> Критерий активизации	На указанное время
<input type="checkbox"/> <b>На указанное время</b>	
Время	0 мс.
<input type="checkbox"/> <b>Дополнительные выходы, нормализуемые при активизации</b>	
<input type="checkbox"/> Критерий нормализации	На указанное время
<input type="checkbox"/> <b>На указанное время</b>	
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 ожидать сигнал запрета прохода. В этом качестве могут выступать также 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, нормализуемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализованы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть нормализованы. 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.

### 3.2.14.12 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 изменить 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 определяется 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.

### 3.2.14.12.1 Тип выхода «Обычный»

В окне доступны следующие параметры:

Параметры	
Адрес	1
Текущее наименование	Выход 1
Первоначальное наименование	Выход 1
Тип	Обычный
Нормальное состояние	Не запитан

- **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**.

### 3.2.14.12.2 Тип выхода «Генератор тревоги»

В окне доступны следующие параметры:

Параметры	
Адрес	1
Текущее наименование	Дополнительный выход №1
Первоначальное наименование	Дополнительный выход №1
Тип	Генератора тревоги
Генератора тревоги	
Нормальное состояние	Не запитан
Время активизации	0 мс.

- **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 нормализованного на противоположное.

### 3.2.14.12.3 Тип выхода «ОПС»

Программа управления задает логику работы контроллера по управлению данным 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 нормализованного на противоположное. Нормализация выхода происходит либо по истечении времени, указанному в параметре **Время активизации** (если оно не бесконечное), либо по сбросу панели, либо после выключения ее питания.

В окне доступны следующие параметры:

Параметры	События
Адрес	3
Текущее наименование	Дополнительный выход №3
Первоначальное наименование	Дополнительный выход №3
☐ Тип	ОПС
☐ <b>ОПС</b>	
Нормальное состояние	Не запитан
Задержка перед запуском	0 мс.
Время активизации	1 сек.
Программа управления	Не управлять
☐ <b>Зоны, активизирующие выход</b>	
Охранная зона №3	<input type="checkbox"/>
Охранная зона №4	<input type="checkbox"/>
Охранная зона №5	<input type="checkbox"/>
Охранная зона №6	<input type="checkbox"/>
Охранная зона №7	<input type="checkbox"/>
Охранная зона №8	<input type="checkbox"/>
Охранная зона №9	<input type="checkbox"/>
Охранная зона №10	<input type="checkbox"/>

- **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 нормализованного на противоположное.



**Примечание:**

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

- **Программа управления**. Выпадающий 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, активизирующие выход** (логическое «И»). Во всех остальных случаях для активизации выхода достаточно поступления сигнала об изменении режима любой из ОЗ, указанных в параметре (логическое «ИЛИ»).

### 3.2.14.12.4 Программы управления выходом «ОПС»

При управлении выходом отслеживается режим работы ОЗ, отмеченных в списке **Зоны, активизирующие 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 оповещателем 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 импульсном режиме 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 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, активизирующие выход**, изменила свое состояние.
- AND – для смены режима необходимо, чтобы все ОЗ или ПЗ, отмеченные в списке **Зоны, активизирующие 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
<i>Включить при тревоге</i>	OR	0	0	такт
<i>Мигать при тревоге</i>	OR	0	0	1Гц
<i>Лампа 1</i>	AND	0	∞	1Гц
<i>Лампа 2</i>	OR	0	∞	1Гц
<i>ПЦН 1</i>	AND	0	∞	0
<i>ПЦН 2</i>	AND	∞	∞	0
<i>Сирена</i>	OR	0	0	такт
<i>Вкл. перед взятием для ИУ в импульсном режиме управления</i>	OR	0	tзад	0
<i>Вкл. при взятии</i>	OR	0	такт	0
<i>Вкл. при снятии</i>	OR	такт	0	0
<i>Вкл. при автоперевзятии</i>	Не используется			

### Программы управления выходами для ППКОП

Название программы	Зоны	Режим зоны								Неисправность ППКОП
		Снята	Взята	Автоперевзятие	Охрана	Тревога	Внимание	Пожар	Неисправность	
<i>Включить при неисправности</i>	OR	0	N	N	N	N	N	N	такт	такт
<i>Мигать при неисправности</i>	OR	0	N	N	N	N	N	N	1Гц	1Гц
<i>Включить при пожаре</i>	OR	N	N	N	0	N	N	такт	N	N
<i>Мигать при пожаре</i>	OR	N	N	N	0	N	N	1Гц	N	N
<i>Включить при внимании и пожаре</i>	OR	0	N	N	0	N	такт	такт	N	N
<i>Мигать при внимании и пожаре</i>	OR	0	N	N	0	N	1Гц	1Гц	N	N

Название программы	Зоны	Режим зоны								Неисправность ППКОП
		Снята	Взята	Автоперевзятие	Охрана	Тревога	Внимание	Пожар	Неисправность	
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

### 3.2.14.13 Дополнительный вывод

Контроллер может иметь один дополнительный вывод (коричневый провод), который в зависимости от конфигурации может использоваться как вход *Fire Alarm*, как дополнительный выход или как канал синхронизации при совместной работе двух контроллеров. Для настройки ресурса доступны следующие параметры:

- **Текущее наименование.** Поле ввода позволяет изменить название вывода.
- **Тип.** Раскрывающийся список позволяет выбрать следующие типы вывода:
  - **Нет.** К данному выводу не подключено никакое внешнее оборудование.
  - **Выход обычный.** К выводу подключено дополнительное оборудование, логика управления которым определяется через описание других устройств системы (за исключением ресурса **Генератор тревоги**).
  - **Выход генератора тревоги.** Решение об активизации дополнительного вывода принимается в соответствии с параметрами, заданными для ресурса **Генератор тревоги**.
  - **Выход ОПС.** Вывод предназначен для управления световым или звуковым оповещателем, а также для передачи тревожных извещений на пульт центрального наблюдения (ПЦН) при изменении режима ОЗ.
  - **Вход Fire Alarm.** Дополнительный вывод используется для подключения устройства аварийной разблокировки («*Fire Alarm*»).
  - **Синхронизирующий вход / выход.** Шина синхронизации совместной работы двух контроллеров.

### 3.2.14.13.1 Тип вывода «Выход обычный»

В окне доступны следующие параметры:

Параметры	
Текущее наименование	Дополнительный вывод
Первоначальное наименование	Дополнительный вывод
☐ Тип	Выход обычный
☐ <b>Выход обычный</b>	
Нормальное состояние	Не запитан

- **Нормальное состояние** (*Не запитан / Запитан*). Параметр определяет, подано ли управляющее напряжение на реле вывода при нормальном состоянии вывода.

### 3.2.14.13.2 Тип вывода «Выход генератора тревоги»

В окне доступны следующие параметры:

Параметры	
Текущее наименование	Дополнительный вывод
Первоначальное наименование	Дополнительный вывод
☐ Тип	Выход генератора тревоги
☐ <b>Выход генератора тревоги</b>	
Нормальное состояние	Не запитан
Время активизации	1 сек.

- **Нормальное состояние** (*Не запитан / Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормальном состоянии вывода.
- **Время активизации**. Время, на которое вывод, при наличии активизирующего управляющего воздействия, меняет свое состояние из нормального на противоположное.

### 3.2.14.13.3 Тип вывода «Выход ОПС»

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

В окне доступны следующие параметры:

Параметры	
Текущее наименование	Дополнительный вывод
Первоначальное наименование	Дополнительный вывод
Тип	Выход ОПС
Выход ОПС	
Нормальное состояние	Не запитан
Задержка перед запуском	0 мс.
Время активизации	1 сек.
Программа управления	Не управлять
Зоны, активизирующие выход	
Охранная зона	<input type="checkbox"/>

- **Нормальное состояние** (*Не запитан / Запитан*). Параметр определяет, подано ли управляющее напряжение на реле вывода при нормальном состоянии выхода.
- **Задержка перед запуском**. Промежуток времени между изменением режима ОЗ и запуском программы управления выводом.
- **Время активизации**. Время, на которое вывод, при наличии активизирующего управляющего воздействия, меняет свое состояние из нормализованного 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 вывода после его активизации.
- **Зоны, активизирующие выход**. Параметр позволяет выбрать ОЗ, нарушение которых приведет к активизации вывода (запуску выбранной для него программы управления). Для программ «Лампа 1», «ПЦН 1» и «ПЦН 2» активизация вывода произойдет только при переходе в данный режим всех ОЗ, указанных в параметре **Зоны, активизирующие выход** (логическое «И»). Во всех остальных случаях для активизации вывода достаточно поступления сигнала об изменении режима любой из ОЗ, указанных в параметре (логическое «ИЛИ»).

#### 3.2.14.13.4 Тип вывода «Вход Fire Alarm»

В режиме «Вход Fire Alarm» дополнительный вывод используется для подключения устройства аварийной разблокировки («Fire Alarm»). Управляющим элементом могут быть нормально замкнутый контакт реле или схема с открытым коллекторным выходом. При подаче на вывод управляющего сигнала от устройства аварийной разблокировки («Fire Alarm»), подключенного к контроллеру, ИУ разблокируется и остается разблокированным до снятия сигнала. На блоке индикации горит зеленый индикатор разрешения прохода. Игнорируются все команды управления.

#### 3.2.14.13.5 Тип вывода «Синхронизирующий вход / выход»

В режиме «Синхронизация» вывод используется для синхронизации совместной работы двух контроллеров при организации двухсторонней точки прохода. В этом режиме выводы контроллеров соединяются друг с другом. Это позволяет избежать регистрации события **Взлом ИУ** при проходе в направлении противоположном направлению, в котором установлен контроллер. Подключение другого оборудования к дополнительным выводам контроллеров в этом случае не допускается.

### 3.2.14.14 Шлейф сигнализации

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

- **Текущее наименование.** Поле ввода позволяет изменить название ШС.
- **Тип.** Раскрывающийся список позволяет выбрать тип ШС:
  - **Нет** – ШС отключен.
  - **Охранный** – подключен охранный ШС.
  - **Пожарный** – подключен пожарный ШС (только для ППКОП).
  - **КТС** – подключен пожарный КТС (только для ППКОП).

#### 3.2.14.14.1 Тип шлейфа «Охранный» (ОШС)

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

Параметры		События	
Адрес		1	
Текущее наименование		Шлейф сигнализации №1	
Первоначальное наименование		Шлейф сигнализации №1	
☐ Тип		Охранный	
☐ <b>Охранный</b>			
Контроль вскрытия корпуса извещателей		<input type="checkbox"/>	
Поддержка перезапроса		<input type="checkbox"/>	
Длительность нарушения		70 мс.	
Задержка взятия на охрану		0 мс.	
Задержка восстановления нарушенного шлейфа		0 мс.	

- **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 истечении 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.
  - Если для параметра установлено значение, отличное от **0**, то 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.

### 3.2.14.14.2 Тип шлейфа «Пожарный» (ПШС)

В окне доступны следующие параметры:

Адрес	3
Текущее наименование	Шлейф сигнализации №3
Первоначальное наименование	Шлейф сигнализации №3
[-] Тип	Пожарный
[-] Пожарный	
[-] Нормальное состояние контакта извещателей	Нормально разомкнут
[-] Нормально разомкнут	
Поддержка перезапроса	<input type="checkbox"/>
Задержка при включении	0 мс.
Задержка сброса	0 мс.

- **Текущее наименование.** Поле ввода позволяет изменить название ресурса.
- **Нормальное состояние контактов извещателей** (*Нормально разомкнут / Нормально замкнут*) – параметр, определяющий нормализованное состояние контакта извещателей, подключенных к ШС.
- **Поддержка перезапроса** – параметр, определяющий необходимо ли 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).

### 3.2.14.15 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 изменить 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.

### 3.2.14.15.1 Тип зоны «Охранная» (ОЗ)

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

В окне доступны следующие параметры:

Адрес	1
Текущее наименование	Зона №1
Первоначальное наименование	Зона №1
Тип	Охранная ▼
Охранная	
Повторное включение сирены	<input type="checkbox"/>
Режим работы при невзятии	Тревога
Не менять при тревоге по Охранным шлейфам сигнализации	
Выходы, работающие по программе "Сирена" или "Лампа"	<input type="checkbox"/>
Шлейфы, активизирующие зону	
Шлейф сигнализации №1	<input checked="" type="checkbox"/>
Шлейф сигнализации №2	<input checked="" type="checkbox"/>
Шлейф сигнализации №8	<input type="checkbox"/>

- **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. Доступны 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, активизирующие зону.** 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.



### 3.2.14.15.2 Тип зоны «Пожарная» (ПЗ)

В окне доступны следующие параметры:

Адрес	2
Текущее наименование	Зона №2
Первоначальное наименование	Зона №2
[-] Тип	Пожарная
[-] Пожарная	
Количество сработавших извещателей для перехода в режим "ПОЖАР"	2
[-] Шлейфы, активизирующие зону	
Шлейф сигнализации №3	<input checked="" type="checkbox"/>
Шлейф сигнализации №4	<input checked="" type="checkbox"/>
Шлейф сигнализации №7	<input type="checkbox"/>

- **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.

### 3.2.14.16 Приборы ИСО «Орион»

Для приборов ИСО «Орион» доступны следующие общие параметры:

- **Текущее наименование** – 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"**

В окне доступны следующие параметры:

Параметры	События
IP-адрес	10.0.12.145
Порт управления	8080
Порт журнала мониторинга и регистрации	8090
Текущее наименование	Модуль управления ИСО "Орион"
Первоначальное наименование	Модуль управления ИСО "Орион"
Модель	PERCo-ORION01
Пользователь	ADMINISTRATOR
Пароль	*****
Примечание	

- **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 указанными 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, ...**

В окне доступны следующие параметры:

Параметры	События
Адрес	1
Текущее наименование	COM1
Первоначальное наименование	COM
Использовать	<input checked="" type="checkbox"/>
Тип преобразователя интерфейса	C2000
Тип протокола	Орион-Про
Приоритет опроса	Самый высокий
Скорость обмена (бод.)	9600
Примечание	

- **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 *C2000M (C2000)*, работающий в режиме ПИ, подключен по COM-порту. В этом режиме ядро опроса будет посылать дополнительные команды управления приемом-передачей.
  - **C2000-ПИ** – значение необходимо выбрать в случае подключения оборудования ИСО «Орион» через *C2000 USB*-конвертер.
  - **C2000** – значение необходимо выбрать в случае подключения через пульт *C2000M (C2000)* в режиме компьютер.



**Примечание:**

Для параметра **Тип преобразователя** интерфейса:

- Значения **C2000-ПИ** и **C2000** выбираются при использовании преобразователей интерфейсов с автоматическим переключением приема / передачи сигнала. В этом случае дополнительные команды не генерируются.
  - При подключении *C2000M (C2000)* через *C2000USB*, необходимо выбрать пункт **ПИ-ГР** или **C2000**, 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 обмена данными между устройствами ИСО «Орион» и XML-RPC-сервером.

**Пульт**

В окне доступны следующие параметры:

Параметры	События
Адрес по RS-232	1
Адрес по RS-485	1
Текущее наименование	Пульт
Первоначальное наименование	Пульт
Модель	0/200
Примечание	

- **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**

В окне доступны следующие параметры:

Параметры	События
Адрес	1
Текущее наименование	ШС №1 (Охранный)
Первоначальное наименование	ШС №1
Тип	Охранный
Примечание	
Заблокировать	<input type="checkbox"/>

- **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](http://www.bolid.ru).

- **Тип** – выпадающий 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 приемок;
  - Дренчерная завеса;
  - Закрытие электрораздвижки;
  - Запуск второго рабочего насоса;
  - Запуск жокей-насоса;
  - Запуск первого рабочего насоса;
  - Запуск резервного насоса;
  - Зоны УОП;
  - Источник 26 В;
  - Источник ОП;
  - Источник питания 27 В;
  - Контроль состояния прибора;
  - Контроль ШС;
  - Масса;
  - Основной ввод АВР;
  - Основной резервуар;
  - Открытие электрораздвижки;
  - Питание второго рабочего насоса;
  - Питание жокей-насоса;
  - Питание первого рабочего насоса;
  - Питание резервного насоса;
  - Питание электрораздвижки;
  - 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;
  - Состояние КЦ4;

- Источник РП;
- Контроль дистанционного запуска РО (речевого оповещения);
- Контроль ЗУ;
- Контроль источника ОП (220В);
- Контроль источника РП (АКБ);
- Контроль неисправности АУП («М\Д»);
- 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)**. В окне доступны следующие параметры:

Параметры	События
Адрес	1
Текущее наименование	Зона №1 (Охранный)
Первоначальное наименование	Зона №1
Тип зоны	Адресный релейный модуль ▾
Примечание	
Заблокировать	<input type="checkbox"/>

- **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

В окне доступны следующие параметры:

Параметры	События
Адрес	1
Текущее наименование	Реле №1 (Реле)
Первоначальное наименование	Реле №1
Тип	Реле
Примечание	



#### **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](http://www.bolid.ru).

- **Тип** – выпадающий 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).

### 3.2.14.17 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.



#### **Внимание!**

Для интеграции необходимо, чтобы биометрические контроллеры имели версию внутреннего ПО ("прошивку") не менее чем:

- для контроллера *BioEntry W2* – 1.1.1;
- для контроллера *BioEntry Plus* (платформа *BioStar 2*) – 2.3.1.

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](#);
- Контроллер [BioEntry W2](#);
- [Замок](#);
- Биометрический считыватель.

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

- **Текущее наименование** – название прибора, которое может быть изменено пользователем;
- **Первоначальное наименование** – наименование прибора в системе по умолчанию.

### 3.2.14.17.1 Контроллер BioEntry Plus

В окне доступны следующие параметры:

Параметры	События
IP-адрес	172.17.111.221
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	539316581
Уровень безопасности	Средний
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
<input type="checkbox"/> <b>Параметры кнопки выхода</b>	
Нормальное состояние	Нормально открыто
<input type="checkbox"/> <b>Параметры датчика прохода</b>	
Нормальное состояние	Нормально открыто
Порядок байтов идентификатора карты	От старшего байта к младшему
<input type="checkbox"/> <b>Настройки Wiegand</b>	
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 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, загрязненности 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 отсчет 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, освещенности 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 объем 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 объем памяти контроллера. Однако, выделение большего объема памяти контроллера для поиска совпадений может замедлить остальные параллельно проходящие 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 с 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 подключенным 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 зеленая 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 производиться 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.

## 3.2.14.17.2 Контроллер BioEntry W2/P2

В окне доступны следующие параметры:

Параметры	События
IP-адрес	172.17.100.230
Маска подсети	255.255.0.0
Шлюз	172.17.0.50
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	Средний
Таймаут сканирования пальца	10 сек.
Таймаут верификации пальцем	5 сек.
Таймаут поиска отпечатка	5 сек.
Чувствительность сканера	3
Алгоритм поиска отпечатков	Автоматический
Режим датчика	Включен всегда
Режим авторизации	Частный
Схема входных портов	Кнопка выхода - порт 0; Датчик прохода - порт 1
[-] <b>Параметры кнопки выхода</b>	
Нормальное состояние	Нормально открыто
[-] <b>Параметры датчика прохода</b>	
Нормальное состояние	Нормально открыто
Порядок байтов идентификатора карты	От старшего байта к младшему
[-] <b>Настройки Wiegand</b>	
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 при использовании верификации по отпечатку пальца:
  - **Средний;**
  - **Высокий;**
  - **Очень высокий.**

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, загрязненности 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 отсчет 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, освещенности 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 объем 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 большой объем памяти контроллера. Однако, выделение большего объема 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 с 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 подключенным 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 зеленая 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 производиться 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 **Настройках 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.


### 3.2.14.17.3 Замок

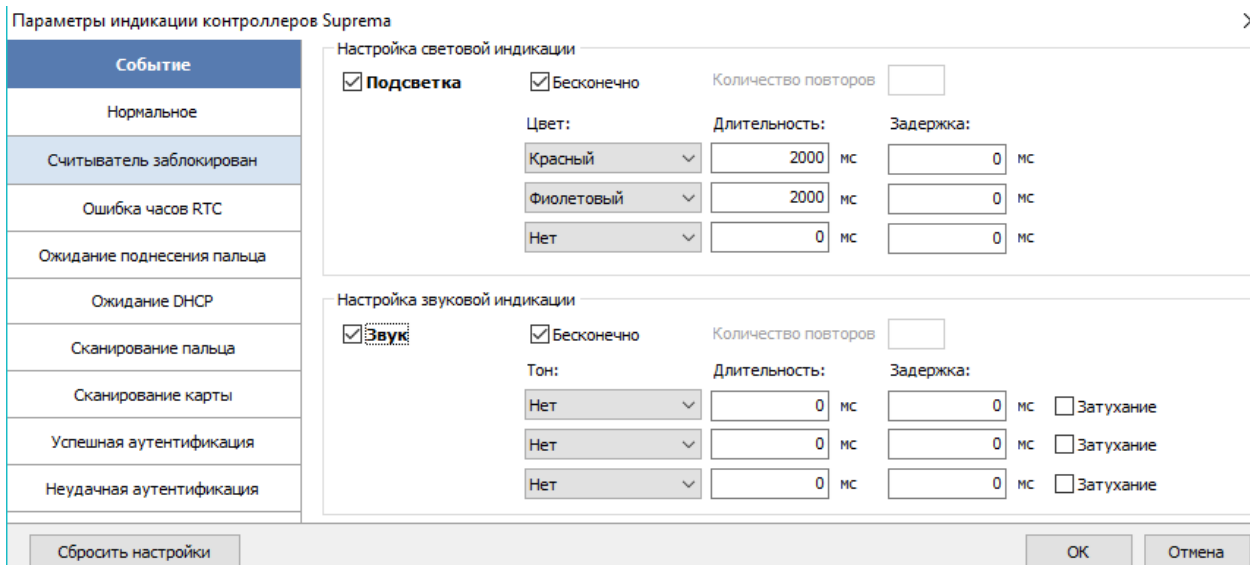
Для настройки доступны следующие параметры:

Параметры		События
Текущее наименование		Замок
Первоначальное наименование		Замок
Блокировать замок при закрытии двери		<input type="checkbox"/>
Блокировать замок по таймауту, только если дверь закрыта		<input checked="" type="checkbox"/>
Время удержания в разблокированном состоянии		5 сек.
Предельное время разблокировки		10 сек.
Генерация тревоги по взлому двери		<input checked="" type="checkbox"/>
Генерация тревоги по удержанию двери		<input checked="" type="checkbox"/>
Регистрация прохода по предъявлению идентификатора/пальца		<input type="checkbox"/>

- **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.

### 3.2.14.17.4 Параметры индикации контроллеров «Suprema»

Для настройки 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**:



Параметры индикации контроллеров Suprema

Событие	Настройка световой индикации	Настройка звуковой индикации
Нормальное	<input checked="" type="checkbox"/> Подсветка	<input checked="" type="checkbox"/> Звук
Считыватель заблокирован	<input checked="" type="checkbox"/> Бесконечно	<input checked="" type="checkbox"/> Бесконечно
Ошибка часов RTC	Цвет: Красный	Тон: Нет
Ожидание поднесения пальца	Длительность: 2000 мс	Длительность: 0 мс
Ожидание DHCP	Задержка: 0 мс	Задержка: 0 мс
Сканирование пальца	Цвет: Фиолетовый	Тон: Нет
Сканирование карты	Длительность: 2000 мс	Длительность: 0 мс
Успешная аутентификация	Задержка: 0 мс	Задержка: 0 мс
Неудачная аутентификация	Цвет: Нет	Тон: Нет
	Длительность: 0 мс	Длительность: 0 мс
	Задержка: 0 мс	Задержка: 0 мс

Сбросить настройки

OK Отмена

- 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 "Закрты");
  - **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 трех);
- **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 кнопку **Сбросить настройки**.
- Для сохранения изменений индикации нажмите кнопку **ОК**, для выхода без сохранения нажмите кнопку **Отмена**.

### 3.2.14.18 Биометрические контроллеры PERCo

Биометрические контроллеры, разработанные компанией **PERCo**, позволяют усилить контроль территории и повысить уровень безопасности за счет использования биометрических технологий при верификации. Биометрические контроллеры доступа имеют возможность подключения по сети Ethernet с использованием стека протоколов TCP/IP. Их использование позволяет дополнить стандартный метод верификации с использованием карт доступа, при этом биометрические идентификаторы значительно сложнее подделать и невозможно потерять.

Для настройки параметров работы в СКУД доступны следующие устройства:

- Контроллер **СТ/L14, СТ13**;
- Контроллер **CL15**;
- Контроллер регистрации **CR11**.

Для настройки ресурсов доступны следующие параметры:

- **Текущее наименование** – название прибора, которое может быть изменено пользователем;
- **Первоначальное наименование** – наименование прибора в системе по умолчанию.

### 3.2.14.18.1 Контроллер СТ/L14, СТ13

Для настройки параметров контроллера перейдите в раздел **«Конфигуратор»** на вкладку **«Конфигурация»** и выделите в рабочей области раздела универсальный биометрический контроллер. На панели настроек перейдите на вкладку **Параметры**.

Доступны следующие параметры:

Параметры	
MAC-адрес	00:25:08:11:01:6C
IP-адрес	172.17.1.108
Маска подсети	255.255.0.0
Шлюз	
Порт конфигурации	12345
Порт управления	443
Макс. кол-во карт доступа и коммиссионированных карт	1000000
Текущее наименование	Контроллер СТ/L14
Внешнее подключение	<input type="checkbox"/>

- **MAC-адрес.**
- **IP-адрес.**
- **Маска подсети.**
- **Шлюз.**
- **Порт конфигурации.**
- **Порт управления.**
- **Макс. кол-во карт доступа и коммиссионированных карт.**
- **Внешнее подключение.** Отображение флажка у параметра означает, что контроллер был добавлен по внешнему подключению (контроллер сам подключается к серверу системы S-20).

### 3.2.14.18.2 Контроллер CL15

Для настройки параметров контроллера перейдите в раздел **«Конфигуратор»** на вкладку **«Конфигурация»** и выделите в рабочей области раздела односторонний биометрический контроллер. На панели настроек перейдите на вкладку **Параметры**.

Доступны следующие параметры:

Параметры	
MAC-адрес	00:25:08:11:01:73
IP-адрес	172.17.1.115
Маска подсети	255.255.0.0
Шлюз	
Порт конфигурации	12345
Порт управления	443
Макс. кол-во карт доступа и коммиссионированных карт	1000000
Текущее наименование	Контроллер CL15
Внешнее подключение	<input type="checkbox"/>
Первоначальное наименование	Контроллер замка CL15
Модель	PERCo-CL15
Часовой пояс	UTC+03:00

- **MAC-адрес.**
- **IP-адрес.**

- **Маска подсети.**
- **Шлюз.**
- **Порт конфигурации.**
- **Порт управления.**
- **Макс. кол-во карт доступа и коммиссионированных карт.**
- **Внешнее подключение.** Отображение флажка у параметра означает, что контроллер был добавлен по внешнему подключению (контроллер сам подключается к серверу системы S-20).
- **Модель.** Параметр отображает официальное наименование модели устройства.
- **Часовой пояс.** Параметр предназначен для выбора часового пояса.

### 3.2.14.18.3 Контроллер регистрации CR11

Для настройки параметров контроллера перейдите в раздел **«Конфигуратор»** на вкладку **«Конфигурация»** и выделите в рабочей области раздела биометрический контроллер регистрации. На панели настроек перейдите на вкладку **Параметры**.

Доступны следующие параметры:

MAC-адрес	02:97:02:17:01:6A
IP-адрес	172.17.1.106
Маска подсети	255.255.0.0
Шлюз	
Порт конфигурации	12345
Порт управления	443
Макс. кол-во карт доступа и коммиссионированных карт	1000000
Текущее наименование	Контроллер регистрации CR11
Внешнее подключение	<input type="checkbox"/>
Первоначальное наименование	Контроллер регистрации CR11
Модель	PERCo-CR11
Время анализа идентификатора	7 сек.
Внутренняя защита от передачи идентификаторов (Local Antipass)	<input type="checkbox"/>
Время ожидания персонализации от сервера	2 сек.
Время отображения информации на дисплее	3 сек.
Язык дисплея	Русский
Временная зона входа	Всегда
Временная зона выхода	Никогда
Часовой пояс	UTC+03:00

- **MAC-адрес.**
- **IP-адрес.**
- **Маска подсети.**
- **Шлюз.**
- **Порт конфигурации.**
- **Порт управления.**
- **Макс. кол-во карт доступа и коммиссионированных карт.**
- **Внешнее подключение.** Отображение флажка у параметра означает, что контроллер был добавлен по внешнему подключению (контроллер сам подключается к серверу системы S-20).
- **Модель.** Параметр отображает официальное наименование модели устройства.
- **Время анализа идентификатора.** Параметр предназначен для выбора времени для поиска информации об идентификаторе в системе.

- **Внутренняя защита от передачи идентификаторов (Local Antipass).** При установленном параметре контроллер отслеживает случаи повторного предъявления одной и той же карты доступа / биоидентификатора к тому же считывателю.
- **Время ожидания персонализации от сервера.** 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 информации на дисплее.** Поле ввода позволяет задать время, в течение которого на ЖКИ контроллера отображается персональная информация, связанная с предъявленной картой доступа.
- **Язык дисплея.** Параметр предназначен для выбора языка.
- **Временная зона входа.** Параметр позволяет выбрать критерий доступа по времени, созданный в разделе «**Временные зоны**», для входа.
- **Временная зона выхода.** Параметр позволяет выбрать критерий доступа по времени, созданный в разделе «**Временные зоны**», для выхода
- **Часовой пояс.** Параметр предназначен для выбора часового пояса.

### 3.2.14.18.4 ИУ

Для настройки параметров перейдите в раздел «**Конфигуратор**» на вкладку «**Конфигурация**» и выделите в рабочей области раздела универсальное ИУ. На панели настроек перейдите на вкладку **Параметры**.

Доступны следующие параметры:

Параметры		События	
Адрес		1	
Текущее наименование		Универсальное ИУ 1	
Первоначальное наименование		Односторонний замок	
Алгоритм		Турникет	
Регистрация прохода по предъявлению идентификатора		<input type="checkbox"/>	
Время удержания в разблокируемом состоянии (время анализа идентификатора)		550 мс.	
Предельное время разблокировки		50 мс.	
Режим работы выхода управления ИУ		Потенциальный	
Нормализация выхода ИУ		После "Закрытия"	
Реакция на FireAlarm в режиме работы "Охрана"		Разблокировать ИУ	
Время идентификации постановки/снятия РКД "Охрана"		10 сек.	
Внутренняя защита от передачи идентификаторов (Local Antipass)		<input checked="" type="checkbox"/>	
<b>Генерация тревоги</b>			
<b>Генерация тревоги при предъявлении идентификатора</b>			
если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН		<input checked="" type="checkbox"/>	
если ИДЕНТИФИКАТОР ЗАПРЕЩЕН		<input checked="" type="checkbox"/>	
если ИСТЕК СРОК ДЕЙСТВИЯ		<input type="checkbox"/>	
если НАРУШЕНО ВРЕМЯ		<input checked="" type="checkbox"/>	
если НАРУШЕНА ЗОНАЛЬНОСТЬ		<input checked="" type="checkbox"/>	
если НАРУШЕН РЕЖИМ РАБОТЫ		<input type="checkbox"/>	
если НАРУШЕНО КОМИССИОНИРОВАНИЕ		<input checked="" type="checkbox"/>	
<b>Генерация тревоги при несанкционированной разблокировке ИУ</b>			
в РЕЖИМЕ РАБОТЫ "Контроль"		<input checked="" type="checkbox"/>	
в РЕЖИМЕ РАБОТЫ "Закрыто"		<input checked="" type="checkbox"/>	
Генерация тревоги по недопустимо долгому открытию ИУ		<input checked="" type="checkbox"/>	
Генерация тревоги при предъявлении "тревожного" пальца		<input type="checkbox"/>	

- **Алгоритм** – определяет алгоритм работы универсального ИУ:
  - **Замок;**
  - **Турникет;**
  - **Автотранспортная проходная;**
  - **Шлюз;**
  - **ЛИКОН.**
- **Регистрация прохода по предъявлению идентификатора** – если флажок установлен, то событие совершения прохода регистрируется сразу после поднесения карты доступа / сканирования пальца без ожидания сигнала от датчика прохода. Если флажок не установлен, то событие совершения прохода регистрируется после поднесения карты доступа / сканирования пальца и срабатывания датчика прохода.
- **Время удержания в разблокированном состоянии (время анализа идентификатора)** – устанавливает время, которое должно пройти от разблокировки ИУ до его блокировки после успешной аутентификации. За это время необходимо совершить проход – иначе ИУ заблокируется. Параметр может быть задан в интервале: от 250 до 750 миллисекунд с шагом 250 миллисекунд; от 1 секунды до 4 минут; бесконечно.
- **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. Параметр может быть задан в интервале: от 250 до 750 миллисекунд с шагом 250 миллисекунд; от 1 секунды до 4 минут; бесконечно.
  - **Режим работы выхода управления ИУ** – 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»).
- **Нормализация выхода ИУ** – параметр определяет, в какой момент нормализуется состояние выхода управления ИУ:
  - **После «Открытия»;**
  - **После «Закрытия».**
- **Реакция на FireAlarm в режиме работы "Охрана"** – определяет реакцию на команду от устройства Fire Alarm, находящегося в составе ОЗ, которая будет производится при взятой на охрану ОЗ.
  - **Разблокировать ИУ;**
  - **Блокировать ИУ.**
- **Время идентификации постановки / снятия РКД "Охрана"**
- **Внутренняя защита от передачи идентификаторов (Local Antipass)** – при установленном параметре контроллер отслеживает случаи повторного предъявления одной и той же карты доступа / биоидентификатора к тому же считывателю.
- **Генерация тревоги при предъявлении идентификатора** – параметр позволяет указать события, связанные с предъявлением карт доступа, при регистрации которых произойдет генерация тревоги:
  - **если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН;**
  - **если ИДЕНТИФИКАТОР ЗАПРЕЩЕН;**
  - **если ИСТЕК СРОК ДЕЙСТВИЯ;**
  - **если НАРУШЕНО ВРЕМЯ;**

- если **НАРУШЕНА ЗОНАЛЬНОСТЬ**;
- если **НАРУШЕН РЕЖИМ РАБОТЫ**;
- если **НАРУШЕНО КОМИССИОНИРОВАНИЕ**.
- **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:
  - в **РЕЖИМЕ РАБОТЫ "Контроль"**;
  - в **РЕЖИМЕ РАБОТЫ "Закрыто"**.
- **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 при предъявлении "тревожного" пальца** – параметр позволяет для РКД «*Контроль*» указать, будет ли генерироваться тревога в случае, если был считан "тревожный" отпечаток пальца.

### 3.2.14.18.5 Направление

Для настройки параметров перейдите в раздел **«Конфигуратор»** на вкладку **«Конфигурация»** и выделите в рабочей области раздела необходимый элемент. На панели настроек перейдите на вкладку **Параметры**.

Доступны следующие параметры:

Параметры	События	Камера СКУД
Адрес		1
Текущее наименование		Направление 1
Первоначальное наименование		Направление 1
Время идентификации доступа		17 сек.
Время ожидания комиссионирования		9 сек.
Время идентификации комиссионирования		6 сек.
<b>[-] Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)</b>		
в РЕЖИМЕ РАБОТЫ "Открыто"		Да
в РЕЖИМЕ РАБОТЫ "Контроль"		Нет
в РЕЖИМЕ РАБОТЫ "Охрана"		Жесткая
<b>[-] Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)</b>		
в РЕЖИМЕ РАБОТЫ "Контроль"		Жесткая
<b>[-] Контроль времени для СОТРУДНИКОВ</b>		
в РЕЖИМЕ РАБОТЫ "Открыто"		Нет
в РЕЖИМЕ РАБОТЫ "Контроль"		Нет
в РЕЖИМЕ РАБОТЫ "Охрана"		Жесткий
<b>[-] Контроль времени для ПОСЕТИТЕЛЕЙ</b>		
в РЕЖИМЕ РАБОТЫ "Контроль"		Мягкий
<b>[-] Настройки верификации</b>		
<b>[-] Уровни верификации</b>		
<b>[-] Уровень 1</b>		
Счетчик проходов		<input type="checkbox"/>
Софт		<input checked="" type="checkbox"/>
Софт, если подключен		<input type="checkbox"/>
ПДУ		<input checked="" type="checkbox"/>
ВВУ		<input type="checkbox"/>
<b>[+] Уровень 2</b>		
<b>[+] Уровень 3</b>		
<b>[+] Уровень 4</b>		
<b>[+] Настройки верификации ПДУ</b>		
<b>[+] Настройки верификации ВВУ</b>		
<b>[-] Настройки верификации софта</b>		
Время ожидания подтверждения		35 сек.
<b>[-] Настройки верификации счетчика проходов</b>		
Время ожидания подтверждения		1 сек.
Изымать идентификаторы ПОСЕТИТЕЛЕЙ		Нет

- **Время идентификации доступа.** Время, на которое открывается ИУ.
- **Время ожидания коммиссионирования / Время досмотра / Время ожидания подтверждения проезда картой водителя (сотрудника).** Параметр позволяет ограничить интервал времени между предъявлением карт пользователя (сотрудника / посетителя / служебного ТС) и коммиссионирующей карты (сотрудника / охранника / водителя) в случае, если в правах карты пользователя установлен доступ с коммиссионированием / доступ с досмотром / подтверждение проезда картой водителя.
- **Время идентификации коммиссионирования.** Параметр позволяет задать максимальное время, за которое определяется, имеет ли коммиссионированный необходимые права.
- **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 **Подтверждение от ДУ** (или верификация от ПО), то будет запущена процедура верификации.
- **Уровни верификации.** Параметр позволяет задать способ и очередность верификации. Доступны следующие уровни:
  - **Счетчик проходов;**
  - **Софт;**
  - **Софт, если подключен;**
  - **ПДУ;**
  - **ВВУ.**



- **Настройки верификации ПДУ, ВВУ, софта, счетчика проходов.**
- **Подтверждение прохода:**
  - при проходе **СОТРУДНИКОВ**;
  - при проходе **СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ**;
  - при проходе **СОТРУДНИКОВ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**;
  - при проходе **ПОСЕТИТЕЛЕЙ**;
  - при проходе **ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ**;
  - при проходе **ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**.
- **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**.

- **Изымать идентификаторы ПОСЕТИТЕЛЕЙ.** Функция доступна только при наличии связи контроллера с сервером системы. Параметр позволяет выбрать условие, при котором идентификатор предъявленной карты доступа посетителя автоматически удаляется.
  - **Нет.** Идентификатор не удаляется автоматически.
  - **После любого прохода.** Идентификатор удаляется при первом предъявлении.
  - **После прохода в последний день действия идентификатора.** Идентификатор удаляется если дата предъявления совпадает с датой окончания срока действия карты.

### 3.2.14.18.6 Считыватель

Для настройки параметров считывателя перейдите в раздел **«Конфигуратор»** на вкладку **«Конфигурация»** и выделите в рабочей области раздела необходимый считыватель. На панели настроек перейдите на вкладку **Параметры**.

Доступны следующие параметры:

Параметры	События
Адрес	1
Текущее наименование	Считыватель 1
Первоначальное наименование	Считыватель 1
Тип	RS485
Номер направления	Направление 1
Порт	1

- **Тип** – определяет тип подключения считывателя:
  - RS485;
  - RS232;
  - Morpho;
  - Mifare;
  - Barcode terminator / Barcode-USB terminator;
  - Barcode / Barcode-USB;
  - Barcode-USB keyboard.
- **Номер направления.** Номер направления, к которому привязывается считыватель.
- **Порт.** Порт на плате, к которому подключается считыватель.

### 3.2.14.18.7 Вход

Для настройки параметров перейдите в раздел **«Конфигуратор»** на вкладку **«Конфигурация»** и выделите в рабочей области раздела необходимый элемент. На панели настроек перейдите на вкладку **Параметры**.

Доступны следующие параметры:

Параметры	События
Адрес	1
Текущее наименование	Вход 1
Первоначальное наименование	Вход 1
<input type="checkbox"/> Тип	Сигнал прохода
<input checked="" type="checkbox"/> <b>Сигнал прохода</b>	
Контроллер	Контроллер CL15
Направление	Направление 1
Нормальное состояние	Разомкнут
Антидребезг	20 мс.

- **Тип.** Выпадающий список позволяет выбрать один из следующих типов:
  - **Обычный.** К данному входу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
  - **Кнопка ПДУ / Кнопка выхода.**

- **Кнопка ПДУ / (СТОП).**
- **Сигнал прохода.**
- **Вход FireAlarm.** Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ *Fire Alarm*.
- **Нет.** К данному входу не подключено никакое внешнее оборудование.
- **Подтверждение от ВВУ.** Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае разрешения прохода.
- **Вход запрета от ВВУ.** Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае запрета прохода.
- **Вход сброса тревоги.**
- **Нормальное состояние** (*Не запитан / Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода.
- **Направление.** Параметр задает направление, к которому привязывается считыватель.
- **Антидребезг.** Значение должно быть от 0 до 950 миллисекунд с шагом 50; от 1 секунды до 4 минут; бесконечно.

### 3.2.14.18.8 Выход

Для настройки параметров перейдите в раздел **«Конфигуратор»** на вкладку **«Конфигурация»** и выделите в рабочей области раздела необходимый элемент. На панели настроек перейдите на вкладку **Параметры**.

Доступны следующие параметры:

Параметры	
Адрес	1
Текущее наименование	Выход 1
Первоначальное наименование	Выход 1
<input type="checkbox"/> Тип	Выход управления ИУ
<input type="checkbox"/> <b>Выход управления ИУ</b>	
Контроллер	Контроллер CL15
Направление	Направление 1
Нормальное состояние	Не запитан

- **Тип.** Выпадающий список позволяет выбрать один из следующих типов:
  - **Обычный.** К данному выходу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
  - **Выход управления ИУ.** Предназначен для подключения к ИУ для передачи управляющих сигналов *Блокировать / Разблокировать*.
  - **Выход индикации ПДУ.** Предназначен для подключения к ПДУ для передачи управляющих сигналов смены индикации.
- **Нормальное состояние** (*Не запитан / Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода.
- **Контроллер.**
- **Направление.** Параметр задает направление ИУ, к которому привязывается считыватель.
- **Антидребезг.** Значение должно быть от 0 до 950 миллисекунд с шагом 50; от 1 секунды до 4 минут; бесконечно.

### 3.2.14.19 Видеоподсистема


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

Параметры		События
MAC-адрес	48:5B:39:6D:80:96	
IP-адрес	172.17.1.138	
Маска подсети	255.255.0.0	
Порт конфигурации	20900	
Порт управления	20902	
Порт журнала мониторинга и регистрации	20903	
Текущее наименование	Видеоподсистема	
Первоначальное наименование	Видеоподсистема	
Модель	PERCo-VS01	
Частота кадров при записи для "Прозрачного здания"	60 кадр/мин.	
Частота кадров при записи для камер СКУД	240 кадр/мин.	

Доступны следующие параметры:

- **Текущее название** – поле для ввода названия видеоподсистемы.
- **Частота кадров при записи для «Прозрачного здания»** – параметр предназначен для камер видеоподсистемы, для которых установлен флажок у параметра **Использовать в "Прозрачном здании"**. Параметр устанавливает частоту записи кадров с камеры. По умолчанию 60 кадров в минуту.
- **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.


### 3.2.14.20 Камера

Для настройки параметров камеры перейдите в раздел **«Конфигуратор»** на вкладку **«Конфигурация»** 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:

Параметры	События
IP-адрес	172.17.0.236
Текущее наименование	A-Linking al7910
Первоначальное наименование	A-Linking al7910
Использовать в "Прозрачном здании"	<input type="checkbox"/>
Использовать как камеру СКУД	<input checked="" type="checkbox"/>
Время предзаписи для камеры СКУД	3 сек.
Порт	80
Порт стоп-кадра	80
Логин пользователя	
Пароль пользователя	
[-] <b>Детектор движения</b>	
Порт	80
Продолжительность записи	2 мин. 0 сек.
[-] <b>Аудио-режимы</b>	
Режим "Downstream"	Нет
Видео-режим	Режим "Http"

Доступны следующие параметры камеры (в зависимости от типа камеры список параметров может изменяться):

- **Текущее наименование** – поле для ввода 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 видеoinформации 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 видеoinформация 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.**

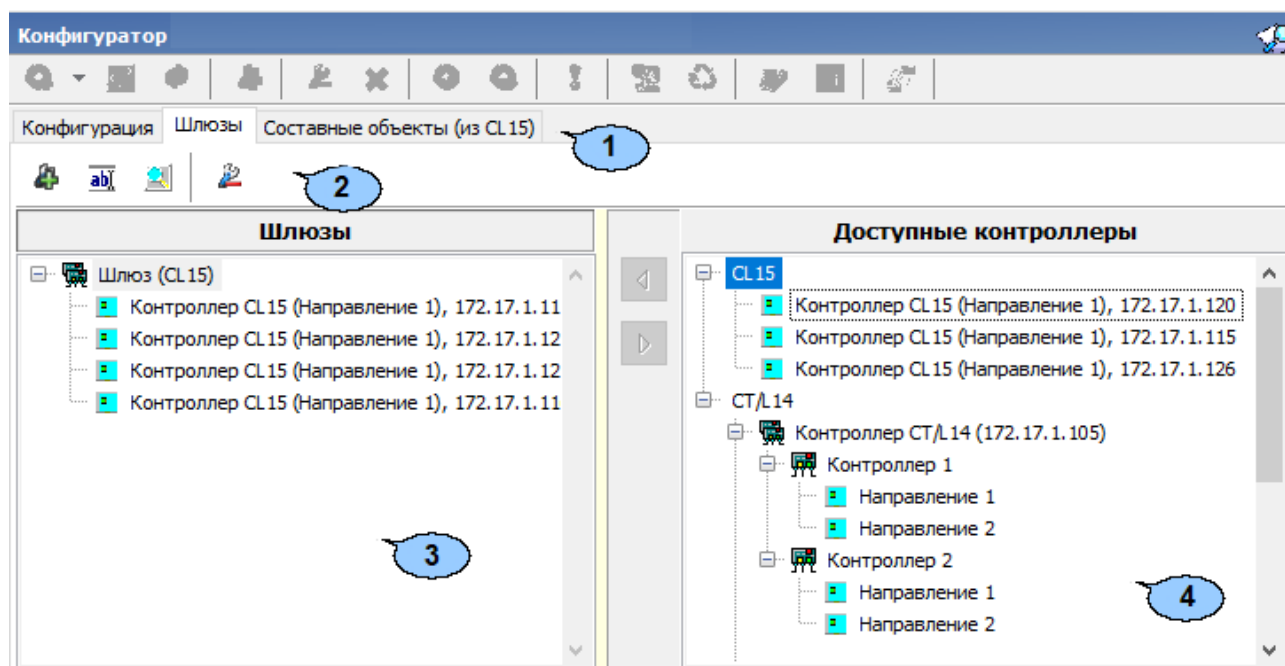
- **Режим Downstream:**
  - **Да** – аудио-сигнал со встроенного микрофона камеры транслируется в разделы ПО и может быть сохранен в видеоархиве. Необходимо дополнительно указать сетевой порт для передачи аудио-сигнала.
  - **Нет** – передача аудио-сигнала с камеры отключена.
- **Видео-режим** – параметр 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 ограничено.
  - **Tunnelled** – режим туннелирования RTSP через HTTP. Используется при невозможности подключения через Unicast. Количество подключений ограничено.
- **Дополнительные параметры** – параметр доступен только для камер, поддерживающих стандарт ONVIF. При выделении строки появится кнопка , позволяющая открыть окно **Менеджер поиска и конфигурации камер (стандарт ONVIF)**.




### 3.3 Вкладка «Шлюзы»

Вкладка **Шлюзы** предназначен для создания шлюза из нескольких направлений контроллера **CT/L14** или из нескольких контроллеров **CL15**.

#### 3.3.1 Рабочее окно вкладки


Рабочее окно вкладки **Шлюзы** имеет следующий вид:



- Выбор вкладки раздела:
  - [Конфигурация](#);
  - [Шлюзы](#);
  - [Составные объекты](#).
- Панель инструментов содержит следующие кнопки:
  -  **Добавить** – для создания нового шлюза.
  -  **Изменить название** – для изменения названия выбранного в рабочей области раздела элемента.
  -  **Параметры точек доступа** – кнопка позволяет настроить параметры для точек доступа:


Точка доступа	Режим доступа
Контроллер 1 (Направление 1)	По считывателю или ДУ
Контроллер 1 (Направление 2)	По ДУ
Контроллер 2 (Направление 1)	По считывателю
Контроллер 2 (Направление 2)	По считывателю или ДУ

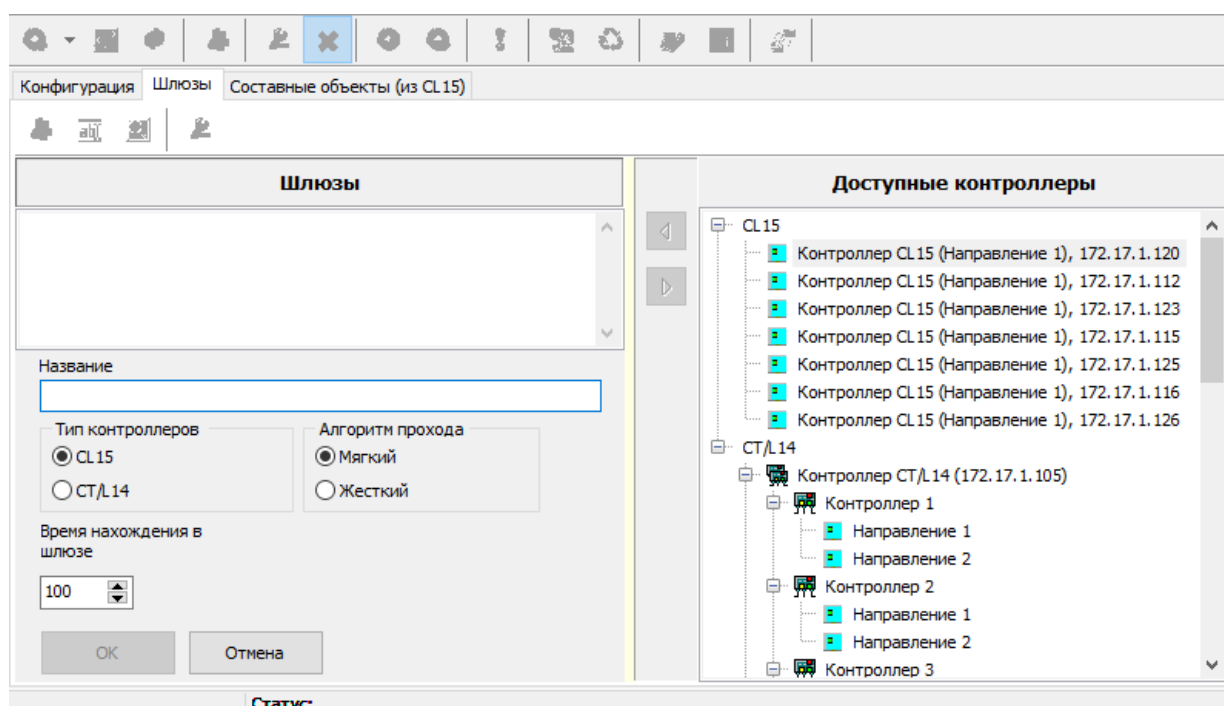
Выберите режим доступа для каждого контроллера в окне **Режим доступа**, используя выпадающий список.

-  **Удалить** – для удаления элемента, выбранного в рабочей области раздела.
- Рабочая область вкладки **Шлюзы** содержит список созданных шлюзов.
  - Список доступных контроллеров **CL15** и **СТ/L14**.



### 3.3.2 Создание шлюза


Для создания шлюза:

- Нажмите кнопку  **Добавить** на панели инструментов вкладки. Откроется новое окно:



2. В открывшемся окне в поле **Название** введите имя для нового шлюза.
3. Выберите необходимый тип контроллера.
4. Выберите алгоритм прохода:
  - Тип **Мягкий**. При использовании данного режима, если человек находится внутри шлюза, то возможен проход вперед и выход назад.
  - Тип **Жесткий**. При использовании данного режима, если человек находится внутри шлюза, то возможен только проход вперед.
5. Установите значение для параметра **Время нахождения в шлюзе**.
6. Нажмите кнопку **ОК** для сохранения названия нового шлюза. Для выхода без сохранения нажмите кнопку **Отмена**.
7. Добавьте необходимые контроллеры из списка окна **Доступные контроллеры**.

Для этого выберите контроллер и нажмите . Контроллер отобразится в списке окна **Шлюзы** (для удаления контроллера из шлюза выберите контроллер нажмите ).

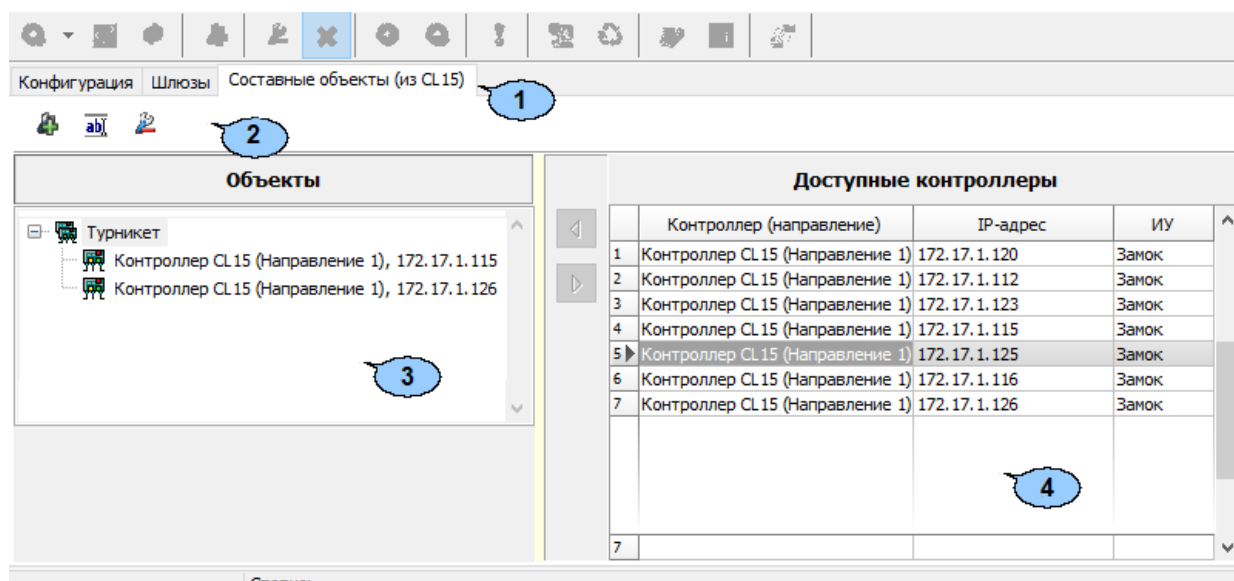
8. Для сохранения изменений нажмите кнопку **ОК**. Для выхода без сохранения нажмите кнопку **Отмена**.
9. Для передачи измененных параметров перейдите на вкладку **Конфигурация** и нажмите на панели инструментов раздела кнопку  **Передать измененные параметры**.

### 3.4 Вкладка «Составные объекты»

Вкладка **Составные объекты** предназначена для создания составного контроллера из двух контроллеров **CL15**.




#### 3.4.1 Рабочее окно вкладки

Рабочее окно вкладки **Составные объекты** имеет следующий вид:




1. Выбор вкладки раздела:
  - [Конфигурация](#);
  - [Шлюзы](#);
  - **Составные объекты**.

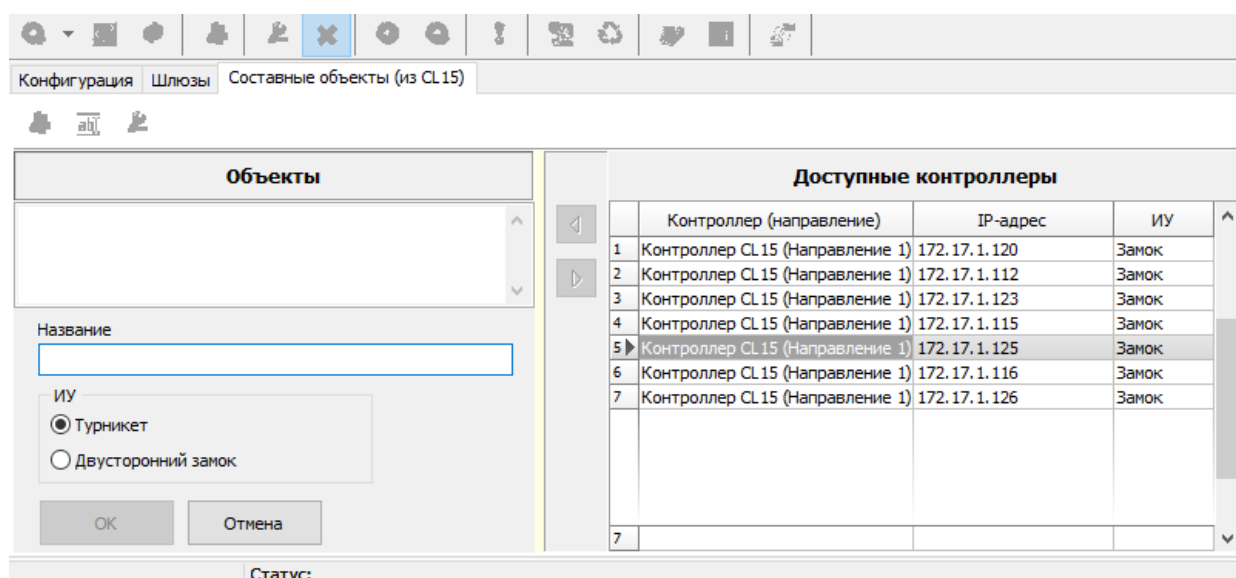




2. Панель инструментов содержит следующие кнопки:
  -  **Добавить** – для создания составного контроллера.
  -  **Изменить название** – для изменения названия выбранного в рабочей области раздела элемента.
  -  **Удалить** – для удаления элемента, выбранного в рабочей области раздела.
3. Рабочая область вкладки **Составные объекты** содержит список созданных составных контроллеров.
4. Список доступных контроллеров **CL15**.

### 3.4.2 Создание составного контроллера

Для создания составного контроллера из двух контроллеров CL15:

1. Нажмите кнопку  **Добавить** на панели инструментов вкладки. Откроется новое окно:



2. В открывшемся окне в поле **Название** введите имя для нового объекта
3. Выберите тип **ИУ**:
  - **Турникет**;
  - **Двусторонний замок**.
4. Нажмите кнопку **ОК** для сохранения названия нового составного объекта. Для выхода без сохранения нажмите кнопку **Отмена**.
5. Добавьте необходимые контроллеры из списка **Доступные контроллеры**. Для этого выберите контроллер и нажмите  .
6. Для сохранения изменений нажмите **ОК**. Для выхода без сохранения нажмите **Отмена**.
7. Для передачи измененных параметров перейдите на вкладку **Конфигурация** и нажмите на панели инструментов раздела кнопку  **Передать измененные параметры**.

## 4 Раздел «Планировщик заданий»

### 4.1 Назначение









#### **Внимание!**

- Для создания задания по отправке отчета «Т13» необходимо приобрести лицензию на модуль **PERCo-SM07 «УРВ»**.
- Для создания задания по отправке дисциплинарных отчетов необходимо приобрести лицензию на модуль **PERCo-SM05 «Дисциплинарные отчеты»**.

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 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**, сотруднику будет отправлено сообщение с текстом, введенным на панели **Текст сообщения** 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. Сотрудникам будут отправлены сообщения с текстом, введенным на панели **Текст сообщения**, 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 достижению:**) в установленный на панели **Расписание** промежуток времени сотрудникам будут отправлены сообщения с текстом, введенным на панели **Текст сообщения**, 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 достижению:**) (однократно, при установке флажка **Выполнять только один раз**, или каждый раз) в установленный на панели **Расписание** промежуток времени сотрудникам будут отправлены сообщения с текстом, введенным на панели **Текст сообщения**, и выполнены команды в установленном на панели **Команды** порядке.
-  **Отправка сообщений по неприходу** – При опоздании сотрудника из числа перечисленных на время, превышающее указанное в поле ввода времени **Допустимое опоздание**, ему будет отправлено сообщение с текстом, введенным на панели **Текст сообщения**.
-  **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»**.

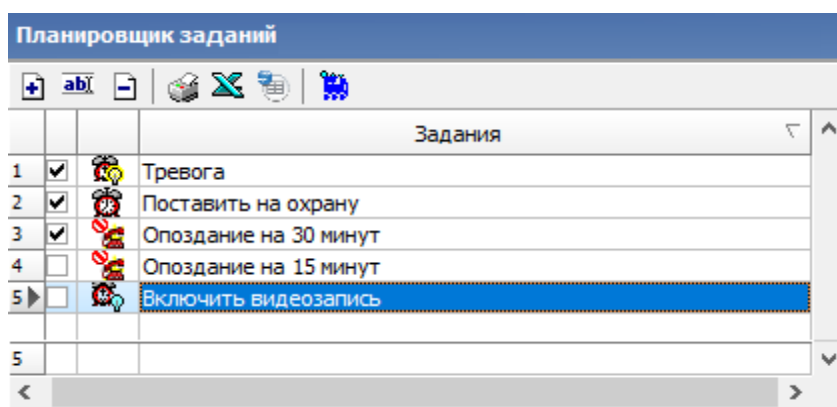
**Примечание:**

В зависимости от выбора способа рассылки в **«Центре управления»** на вкладке **Настройка рассылки сообщений** панели адресата и ввода текста сообщения будут иметь соответствующие название и вид.

## 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**:

Новое задание

Название

Тип задания

по предъявлению идентификаторов

по времени

по времени и достижению состояний

по изменению состояний





отправка сообщений по неприходу

отчет по EMail

ОК Отмена

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







- Изменить (Ctrl+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 сообщений 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.

Команда	Устройство	IP-адрес
Установить режим работы "Закрыто"	 Контроллер замка	10.0.8.102
Поставить на охрану/контроль	 Зона №1 (ППКОП)	10.0.201.57
Поставить на охрану/контроль	 Зона №5 (ППКОП)	10.0.201.57
Активизировать	 Дополнительный выход №3	10.0.201.241
Установить режим работы "Закрыто"	 Контроллер шлагбаума	10.0.201.241


  

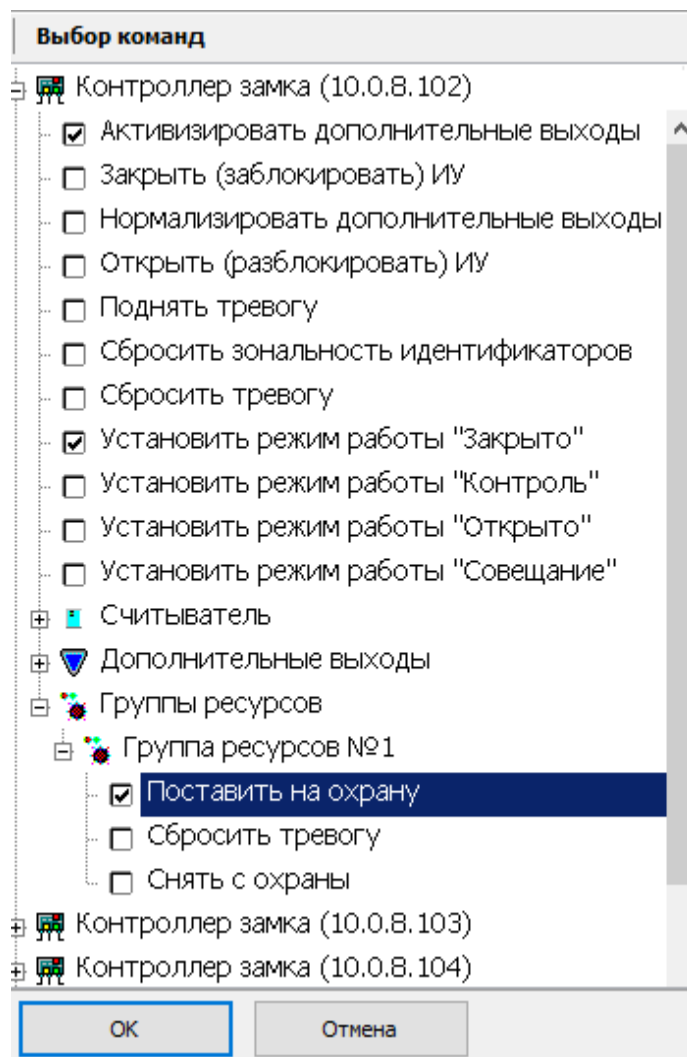
60 сек  Время активизации

Выполнение команд по достижении:  ВСЕХ состояний

Повторять выполнение при неуспехе       Выполнять только один раз

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 [Панель «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.

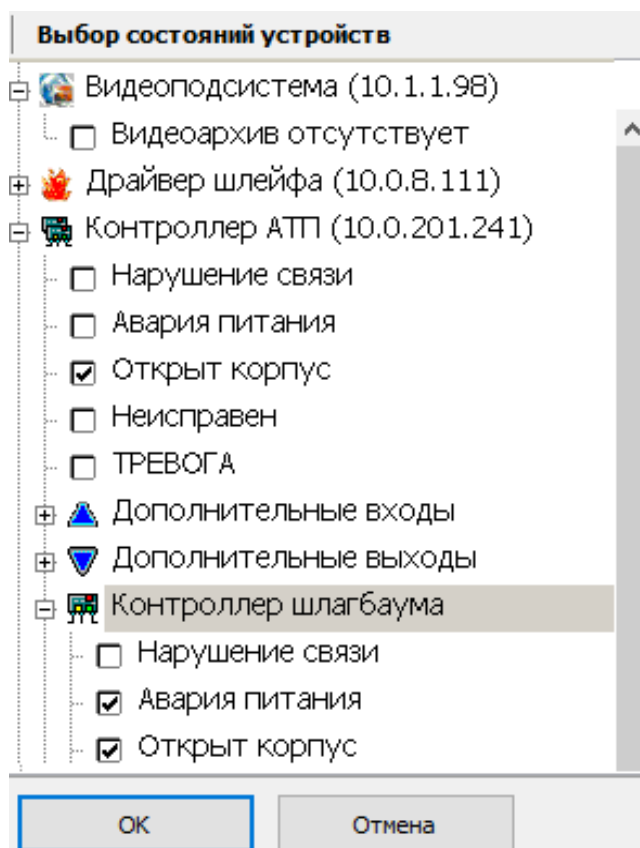
### 4.2.4 Панель «Отслеживаемые состояния»

Панель имеет следующий вид:


Отслеживаемые состояния	
Устройство	Состояния
Замок (10.0.8.103)	Взлом по считывателю №1 Взлом по считывателю №2
Контроллер шлагбаума (10.0.201.241)	Авария питания Открыт корпус Неисправен ТРЕВОГА
ППКОП (10.0.201.57)	Неисправен
Выполнение команд по достижении: <span style="border: 1px dashed gray; padding: 2px;">хотя бы ОДНОГО состояния</span>	

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 достижению:** – 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 адресата и ввода текста

Панели адресата будут иметь различный вид в зависимости от выбора способа рассылки сообщений во вкладке *Настройка рассылки сообщений «Центра управления»* системы.

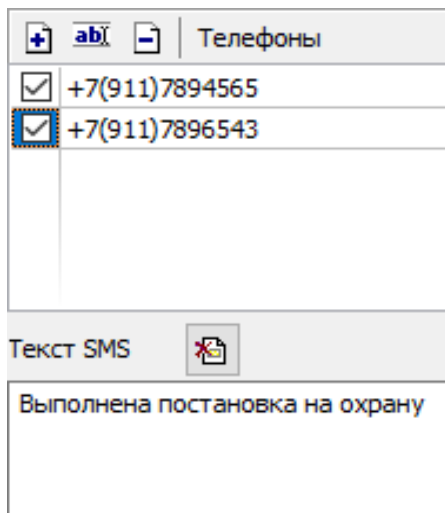
### 4.2.5.1 Панели «Телефоны» и «Текст SMS»

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



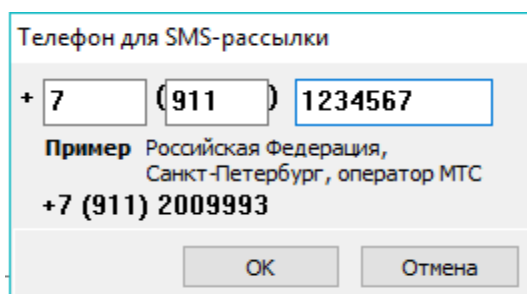
**Примечание:**

Для отправки SMS-сообщений необходимо чтобы в «**Центре управления**» на вкладке **Настройка рассылки сообщений** 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 **OK**.

- **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.

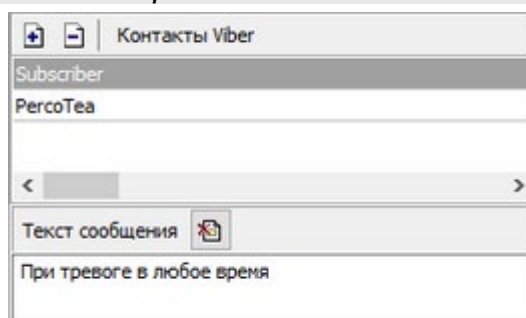
**4.2.5.2 Панели «Контакты Viber» и «Текст сообщения»**

Панель **Контакты Viber** позволяет выбрать контакты получателей, а панель **Текст сообщения** – ввести текст сообщения для рассылки при выполнении задания.



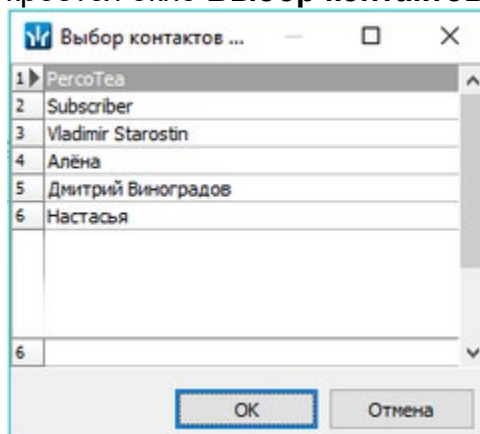
**Примечание:**

Для отправки сообщений *Viber* необходимо, чтобы в «**Центре управления**» на вкладке **Настройка рассылки сообщений** был выбран и настроен способ отправки сообщений *Viber-рассылка*.



Инструменты панелей:

- **Добавить** – кнопка позволяет добавить контакт Viber для отправки сообщения. При нажатии кнопки откроется окно **Выбор контактов**:



Выберите необходимый контакт, а затем нажмите кнопку **OK**.

- **Удалить** – кнопка позволяет удалить выбранный в рабочей области контакт.
- **Удалить текст SMS** – кнопка позволяет очистить рабочую область панели **Текст SMS**.




#### 4.2.6 Панель «Сотрудники»

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

	Сотрудник	Подразделение	Должность
1	Беляев Тарас Евлампиевич	Администрация	Помошник
2	Богатырев Андрей Проклович	Филиал 1	Сотрудник
3	Богатырев Всеволод Брониславович	Филиал 1	Аналитик
4	Богатырев Николай Якубович	Предприятие	Помошник
5	Богатырёв Борис Кириллович	Администрация	Руководитель отдел
6	Каширина Регина Андрияновна	Администрация	Директор
7	Тихонов Сергей	Филиал 1	Аналитик
7			

Допустимое опоздание (часы : минуты) 00:05

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 выделение 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:

Предприятие			
	Сотрудник	Подразделение	Должность
1	Беляев Тарас Евлампиевич	Администрация	Помошник
2	Богатырёв Борис Кириллович	Администрация	Руководитель отдела
3	Богатырев Николай Якубович	Предприятие	Помошник
4	Каширина Регина Андрияновна	Администрация	Директор
4			

OK      Отмена

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

Подразделения


- ✓ (не определено)
- ✓ **НИОКР**
- ✓ Предприятие
  - ✓ Администрация
  - ✓ Бухгалтерия
  - ✓ Отдел кадров
  - ✓ Отдел рекламы
  - ✓ Отдел сервисного обслуживания
- ✓ Филиал 1
- ✓ Филиал 2

Показывать скрытые       Автоматическая сортировка

Строка для поиска

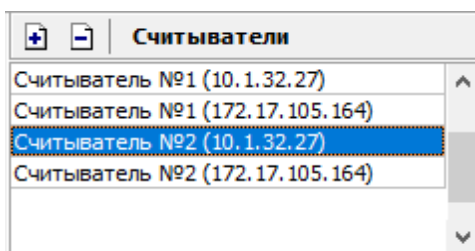
Поиск | F3       Искать с начала названия

OK      Отмена


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.

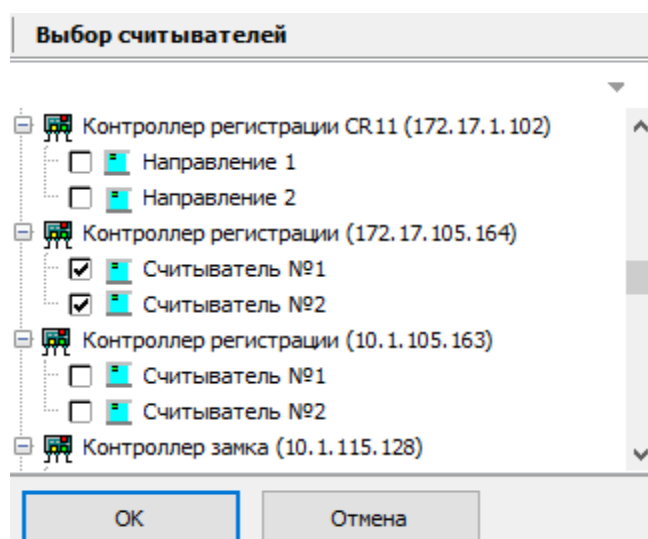
#### 4.2.7 Панель «Считыватели»

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**:

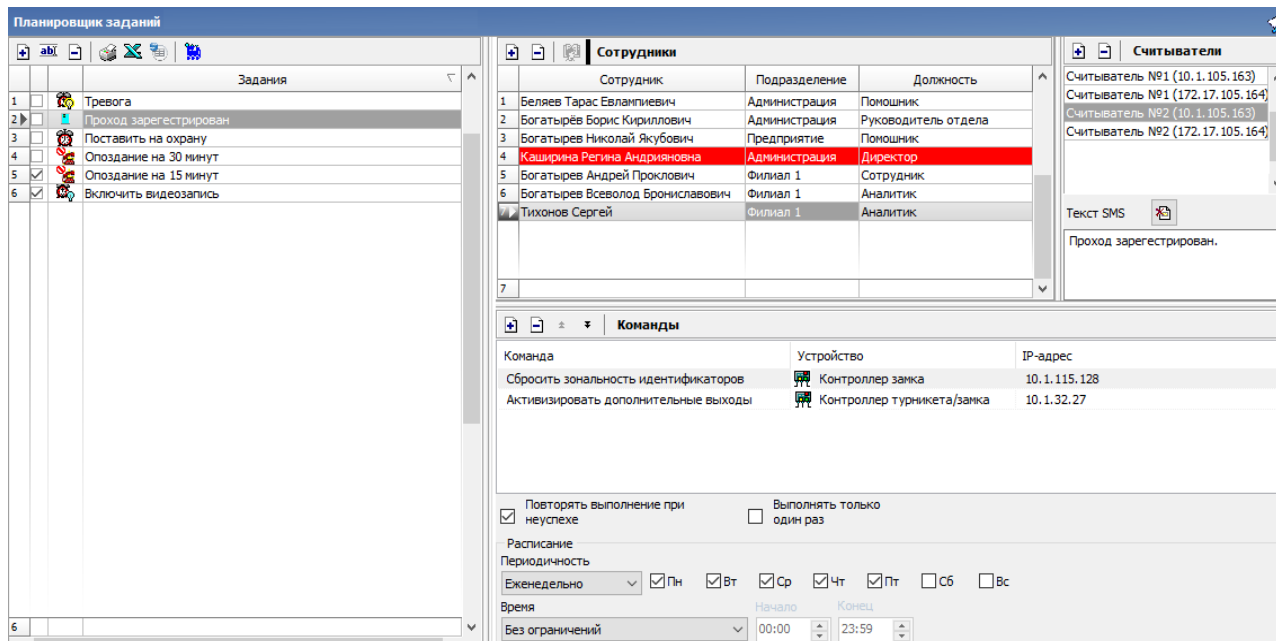


На открывшейся панели в раскрывающемся многоуровневом списке контроллеров системы безопасности отметьте флажками необходимые считыватели, затем нажмите кнопку **ОК**.

-  **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:

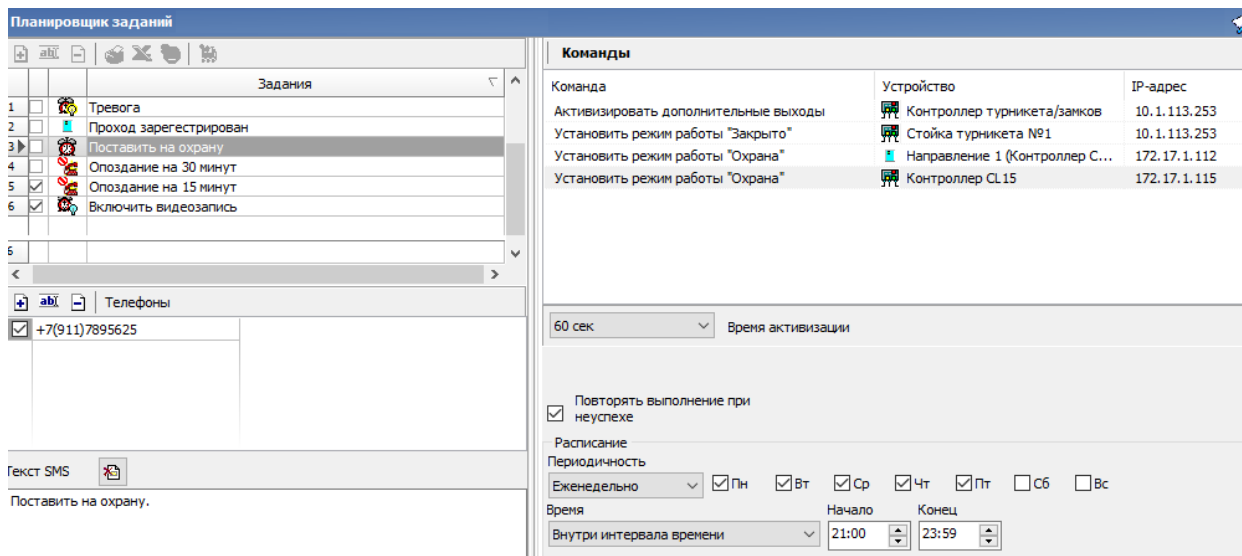


Порядок настройки задания:

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:



### Внимание!

В случае, если в «**Центре управления**» на вкладке **Настройка рассылки сообщений** был выбран и настроен способ отправки сообщений *Viber-рассылка*, панели адресата и ввода текста сообщения будут иметь соответствующий вид.

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:

The screenshot shows the 'Планировщик заданий' (Task Scheduler) interface. It is divided into several panels:

- Задания (Tasks):** A list of tasks with checkboxes and icons. Tasks include: Тревога (Alarm), Проход зарегистрирован (Access granted), Поставить на охрану (Set to guard), Опоздание на 30 минут (30 min delay), Опоздание на 15 минут (15 min delay), and Включить видеозапись (Enable video recording).
- Телефоны (Phones):** A list of phone numbers, with +7(911)1235689 selected.
- Текст SMS (SMS Text):** A text input field containing 'Тревога!' (Alarm!).
- Отслеживаемые состояния (Monitored States):** A table showing monitored states:
 

Устройство (Device)	Состояния (States)
Замок №1 (10.0.201.232)	ТРЕВОГА
Зона №1 (10.0.201.57)	ТРЕВОГА
Зона №2 (10.0.201.57)	ТРЕВОГА
- Команды (Commands):** A table showing commands:
 

Команда (Command)	Устройство (Device)	IP-адрес (IP Address)
Начать запись (Start recording)	A-Linking al7910 9	10.0.0.9
Начать запись (Start recording)	A-Linking al7910 3	10.0.0.3
Активизировать (Activate)	Дополнительный выход №1 (Контроллер замка)	10.0.8.103
Активизировать (Activate)	Дополнительный выход №2 (Контроллер замка)	10.0.8.103
- Additional Settings:**
  - Activation time: 30 сек (30 sec)
  - Execution on achievement: хотя бы ОДНОГО состояния (at least one state)
  - Repeat on failure:  Повторять выполнение при неуспехе
  - Schedule:
    - Periodicity: Ежедневно (Daily)
    - Days:  Пн  Вт  Ср  Чт  Пт  Сб  Вс
    - Time: Внутри интервала времени (Within time interval), Start: 00:00, End: 23:59



### Внимание!

В случае, если в «**Центре управления**» на вкладке **Настройка рассылки сообщений** был выбран и настроен способ отправки сообщений *Viber-рассылка*, панели адресата и ввода текста сообщения будут иметь соответствующий вид.

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:

The screenshot shows the 'Планировщик заданий' (Task Scheduler) interface. The main window is titled 'Планировщик заданий' and contains several panels:

- Задания (Tasks):** A list of tasks with checkboxes. The task 'Проезд перекрыт' is selected and highlighted in blue.
- Отслеживаемые состояния (Monitored States):** A table showing monitored states for the selected task.
 

Устройство	Состояния
Считыватель (10.0.8.102)	Режим "Открыто"
Считыватель №1 (10.0.201.232)	Режим "Открыто"
Считыватель №2 (10.0.201.232)	Режим "Открыто"
- Команды (Commands):** A table showing commands to be executed when the task starts.
 

Команда	Устройство	IP-адрес
Активизировать	Дополнительный выход №3...	10.0.201.241
Установить режим работы "Закртыо"	Контроллер шлагбаума	10.0.65.118
Установить режим работы "Закртыо"	Контроллер замка	10.0.8.103
- Время активизации (Activation Time):** A dropdown menu set to '60 сек'.
- Выполнение команд по достижении (Command Execution on Achievement):** A dropdown menu set to 'хотя бы ОДНОГО состояния'.
- Повторять выполнение при неуспехе (Repeat on Failure):** A checked checkbox.
- Выполнять только один раз (Execute only once):** An unchecked checkbox.
- Расписание (Schedule):** A section for setting the task's schedule.
  - Периодичность (Frequency):** A dropdown menu set to 'Еженедельно'.
  - Дни недели (Days of the Week):** Checkboxes for Пн, Вт, Ср, Чт, Пт, Сб, Вс. Пн, Вт, Ср, and Чт are checked.
  - Время (Time):** A dropdown menu set to 'Внутри интервала времени'.
  - Начало (Start Time):** A time picker set to 08:30.
  - Конец (End Time):** A time picker set to 19:00.
- Телефоны (Phones):** A list of phone numbers. The number '+7(911)5269636' is selected.
- Текст SMS (SMS Text):** A text input field containing 'Поезд перекрыт'.



### Внимание!

В случае, если в «*Центре управления*» на вкладке **Настройка рассылки сообщений** был выбран и настроен способ отправки сообщений *Viber-рассылка*, панели адресата и ввода текста сообщения будут иметь соответствующий вид.

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 сообщений 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:

Планировщик заданий

Задания

1	<input type="checkbox"/>		Тревога
2	<input type="checkbox"/>		Проход зарегистрирован
3	<input type="checkbox"/>		Проезд перекрыт
4	<input type="checkbox"/>		Поставить на охрану
5	<input type="checkbox"/>		Опоздание на 30 минут
6	<input checked="" type="checkbox"/>		Опоздание на 15 минут
7	<input checked="" type="checkbox"/>		Включить видеозапись

Подразделения  Показать скрытые подразделения

(не определено)

- Предприятие
  - Администрация
  - Бухгалтерия
  - Отдел кадров
  - Отдел рекламы
  - Отдел сервисного обслуживания
- Филиал 1
- Филиал 2

Весь список

Сотрудник	Подразделение	Должность	
1	Беляев Тарас Евангелиевич	Администрация	Помошник
2	Богатырев Андрей Проклович	Филиал 1	Сотрудник
3	Богатырев Всеволод Брониславович	Филиал 1	Аналитик
4	Богатырев Николай Якубович	Предприятие	Помошник
5	Богатырев Борис Кириллович	Администрация	Руководитель отдела
6	Каширина Регина Андрияновна	Администрация	Директор
7	Тихонов Сергей	Филиал 1	Аналитик

Текст SMS

Опоздание на 15 минут.

Допустимое опоздание (часы : минуты) 00:15



### Внимание!

В случае, если в **«Центре управления»** на вкладке **Настройка рассылки сообщений** был выбран и настроен способ отправки сообщений **Viber-рассылка**, панели адресата и ввода текста сообщения будут иметь соответствующий вид.

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:

The screenshot shows a configuration window for report settings. It is divided into several sections:

- Выбор отчета (Report Selection):** Contains radio buttons for different report types. Callout 1 points to the 'Отчет Т13' option, which is selected.
- Параметры отчета (Report Parameters):**
  - Формат (Format):** Checkboxes for PDF, MS Excel (форма 1), and MS Excel (форма 2).
  - Период отчета (Report Period):** A dropdown menu set to 'Предыдущий месяц'.
  - Подразделение (Department):** A text field with '(не определено)' and a search icon.
  - Сортировка, её порядок (Sorting):** A list with 'ФИО' selected.
  - Отображение данных (Data Display):** Radio buttons for 'Часы : минуты' (selected) and 'Доли часа'.
  - Тип расчета (для смен с переходом через 0) (Calculation Type):** Radio buttons for 'Посуточный' (selected) and 'Посменный'.
- Периодичность формирования (Formation Periodicity):**
  - Ежемесячно (Monthly):** A dropdown menu.
  - 1 -й день месяца (1st day of the month):** A numeric input field.
  - Время (Time):** A time picker set to 09:00. Callout 3 points to this field.
- E-Mail-адреса (E-Mail addresses):** A list box for entering email addresses. Callout 4 points to this area.
- Buttons:** 'OK' and 'Отмена' (Cancel) buttons. Callout 5 points to the 'Отмена' button.




### Внимание!


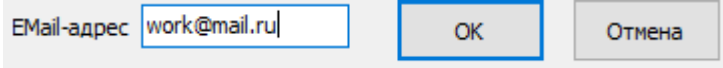


Наличие тех или иных параметров на панели зависит от выбранного типа отчета.

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 которым 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 T13:
  - **часы : минуты;**
  - **доли часа.**
- **Тип расчета (для смен с переходом через 0)** – переключатель позволяет выбрать способ расчета времени в отчете T13:
  - **посуточный;**
  - **посменный.**
- **Отображаемые столбцы** – на панели с помощью флажков можно отметить столбцы с данными, отображаемые в отчете «*Время прихода, время присутствия*»:
  - **время прихода;**
  - **время ухода;**
  - **время присутствия.**
- **Виды нарушений** – на панели с 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 **E-Mail-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 **OK** и **Отмена** позволяют сохранить измененные параметры задания или отменить внесенные в задание изменения.

### **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 **E-Mail-адреса** нажмите кнопку  **Добавить**. На открывшейся панели введите электронный адрес, на который будет отправляться отчет, после чего нажмите кнопку **OK**. 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:

Планировщик заданий

Журнал с 21.02.2018 по 06.11.2018 1



Устройство	Команда	Результат	Дата	Время
Группа ресурсов №1 (10.0.1.68)	Снять с охраны	Выполнена	21.09.2018	16:05:33
Группа ресурсов №1 (10.0.1.60)	Снять с охраны	Выполнена	21.09.2018	16:05:33
Группа ресурсов №1 (10.0.0.34)	Снять с охраны	Выполнена	21.09.2018	16:05:33
Электронная проходная (10.0.0.75)	Закрыть (заблокировать) ИУ	Ошибка	28.09.2018	15:10:21
Электронная проходная (10.0.0.75)	Установить режим работы "Открыто"	Выполнена	28.09.2018	15:05:21

2

---

Устройство	Состояния
A-Linking al7910 20 (192.168.1.20)	ТРЕВОГА
A-Linking al7910 25 (192.168.1.25)	ТРЕВОГА <span style="border: 1px solid blue; border-radius: 50%; padding: 2px;">3</span>
A-Linking al7910 26 (192.168.1.26)	ТРЕВОГА



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:

Ввод диапазона дат

Начальная дата	21.08.2018
Конечная дата	19.09.2018
<input type="button" value="OK"/> <input type="button" value="Отменить"/>	

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

-  **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 Отчет по отправке сообщений

В зависимости от выбора способа рассылки сообщений в «*Центре управления*» в системе будет отображен один из нескольких разделов:

- [Отчет по SMS](#);
- [Отчет по сообщениям Viber](#).

### 5.1 Раздел «Отчет по SMS»

#### 5.1.1 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.)

#### 5.1.2 Рабочее окно раздела








Рабочее окно раздела имеет следующий вид:

Отчет по SMS				
Отчет с	21.02.2018	по	06.11.2018	НИОКР
Сообщения из заданий без идентификаторов				
Подразделения, сотрудники	Всего	Доставленных	Недоставленных	Запрещенных
НИОКР	25	24		1
Егоров Игорь Степанович (ведущий инженер, НИОКР)	12	12		
Иванов Константин Николаевич (инженер, НИОКР)	13	12		1
01.03.2018				
02.03.2018				
03.03.2018				
04.03.2018				
05.03.2018				

	Дата начала обработки	Время начала обработки	Дата завершения обработки	Время завершения обработки	Владелец идентификатора / отсутствующий	Статус завершения обработки	Телефон	Текст SMS
1	10.04.2018	17:00:57	10.04.2018	17:01:03	Иванов Константин Николаевич	Доставлено	7911994	Состоится собрание в 18.00 12
2	09.04.2018	15:27:00	09.04.2018	15:27:04	Иванов Константин Николаевич	Доставлено	7911994	Иванов К. Н. 09.04 15:26 Вход в
3	09.04.2018	15:12:34	09.04.2013	15:12:3В	Иванов Константин Николаевич	Доставлено	7911994	Иванов К. Н. 09.04 15:12 Внесит
4	09.04.2018	15:12:09	09.04.2018	15:12:17	Иванов Константин Николаевич	Доставлено	7911994	Иванов К. Н. 09.04 15:12 Выход
5	09.04.2018	15:12:08	09.04.2013	15:12:13	Иванов Константин Николаевич	Доставлено	7911994	Иванов К. Н. 09.04 15:12 Вход в
6	10.04.2018	13:32:58	10.04.2018	13:33:04	Иванов Константин Николаевич	Доставлено	7911994	Состоится собрание в 15.00 12
7	09.04.2018	12:36:25	09.04.2018	12:36:30	Иванов Константин Николаевич	Доставлено	7911994	Иванов К. Н. 09.04 12:36 Дости

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;
  - **Подразделения и 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 сообщений** – 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 сообщений** – отчет для выделенного в рабочей области сотрудника или подразделения.
-  **НИОКР Выбор подразделения (Ctrl+B)** – кнопка и название выбранного подразделения.
- **Сообщения 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 о доставленных, недоставленных и запрещенных 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:

<input checked="" type="checkbox"/>	Дата начала обработки
<input checked="" type="checkbox"/>	Время начала обработки
<input checked="" type="checkbox"/>	Дата завершения обработки
<input checked="" type="checkbox"/>	Время завершения обработки
<input checked="" type="checkbox"/>	Владелец идентификатора / отсутствующий
<input type="checkbox"/>	Контакт Viber
<input checked="" type="checkbox"/>	Статус завершения обработки
<input checked="" type="checkbox"/>	Текст сообщения
<input checked="" type="checkbox"/>	Подразделение
<input checked="" type="checkbox"/>	Должность
<input checked="" type="checkbox"/>	Задание
<input checked="" type="checkbox"/>	Считыватель
<input checked="" type="checkbox"/>	SMS-провайдер
<input checked="" type="checkbox"/>	Комментарий
<input type="checkbox"/>	Сообщение Viber
<input checked="" type="checkbox"/>	Тип SMS

- 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:

SMS-сообщение	
<input type="text" value="24.04.2012, 09:42:05"/>	Дата/время прохода (выполнения задания)
<input type="text" value="24.04.2012, 09:42:05"/>	Создано
<input type="text" value="24.04.2012, 11:41:30"/>	Отправлено
<input type="text" value="24.04.2012, 11:41:30"/>	Зарегистрировано
<input type="text"/>	Доставлено
<input type="text" value="24.04.2012, 11:43:00"/>	Неотправлено или недоставлено
<input type="text" value="22"/>	Количество повторов

- **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 сообщений по неприходу**.
- **«Сообщение общей рассылки»** – сообщение создано в разделе **«Сотрудники и ученики»**
- **«Тестовое сообщение»** – сообщение, отправленное 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.

## 5.2 Раздел «Отчет по сообщениям Viber»

### 5.2.1 Назначение

Раздел **«Отчет по сообщениям Viber»** предназначен для просмотра и печати отчетов об отправке сообщений с помощью мессенджера Viber в процессе выполнения заданий, созданных в разделе **«Планировщик заданий»**.

В процессе отправки сообщение может получить один из следующих статусов:

- **Отправленное;**
- **Неотправленное;**
- **Запрещенное.**

## 5.2.2 Рабочее окно раздела

Рабочее окно раздела имеет следующий вид:

Отчет по сообщениям Viber									
Отчет с		01.01.2020	по		21.01.2020	НИОКР <input checked="" type="checkbox"/> Сообщения из заданий без идентификаторов			
Подразделения, сотрудники					Всего	Отправленных	Неотправленных	Запрещенных	
НИОКР					9	9			
Разумовский Николай (НИОКР)					9	9			


  

	Дата начала обработки	Время начала обработки	Дата завершения обработки	Время завершения обработки	Владелец идентификатора / отсутствующий	Статус завершения обработки	Задание	Контакт Viber	Сообщение Viber
1	21.01.2020	12:07:56	21.01.2020	12:07:56	Разумовский Николай	Отправлено	По неприходу	Subscriber	
2	20.01.2020	16:39:01	20.01.2020	16:39:01	Разумовский Николай	Отправлено	Общая рассылка	Subscriber	
3	20.01.2020	16:34:01	20.01.2020	16:34:02	Разумовский Николай	Отправлено	По неприходу	Subscriber	
4	18.01.2020	23:57:55	18.01.2020	23:57:55	Разумовский Николай	Отправлено	По неприходу	Subscriber	

### 1. Панель инструментов раздела:

- **Отчет с ... по...** – поля ввода даты 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;
  - **Подразделения и 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 сообщений Viber 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 сообщений** – 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 сообщений Viber 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 сообщений** – отчет для выделенного в рабочей области сотрудника или подразделения.

-  **НИОКР Выбор подразделения (Ctrl+B)** – кнопка и название выбранного подразделения.
- **Сообщения из заданий без идентификаторов** – при установке флажка в рабочей области будут отображаться данные об отправке сообщений Viber заданиями, не связанными с предъявлением идентификаторов сотрудников.

2. Рабочая область. В рабочей области в виде многоуровневого раскрывающегося списка отображаются данные об отправленных, неотправленных и запрещенных сообщениях Viber 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 контакт для отправки сообщений Viber.
- Зеленым цветом выделены сотрудники, уволенные на момент построения отчета.

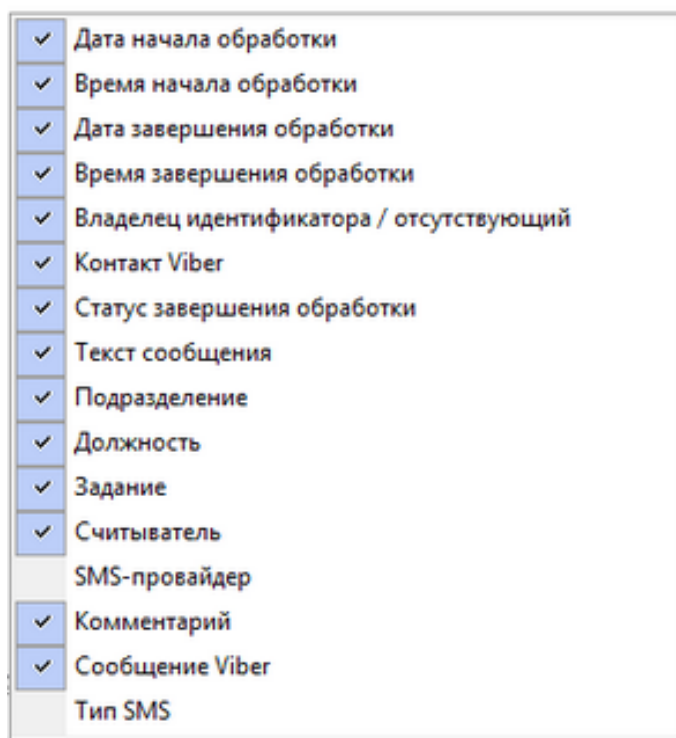



**Примечание:**

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 **Сообщение Viber** с подробной информацией об этапах обработки выбранного на панели дополнительных данных сообщения Viber:

21.01.2020, 12:07:56	Дата/время прохода (выполнения задания)
21.01.2020, 12:07:56	Создано
21.01.2020, 12:07:56	Отправлено
21.01.2020, 12:07:56	Финальный статус: <b>Отправлено</b>

Количество повторов: 0

- **Дата/время прохода (выполнения задания)** – дата и время события, послужившего причиной создания сообщения Viber.
- **Создано** – дата и время создания сообщения Viber.
- **Отправлено** - дата и время отправки сообщения Viber.
- **Финальный статус** - финальный статус отправленного сообщения (*Отправлено/ Не отправлено*).
- **Количество повторов** - отображение количества повторов отправки сообщения при неудачной попытке.



**Примечание:**

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

4. Рабочая область панели дополнительных данных. На панели отображается информация о созданных сообщениях Viber для выбранного в рабочей области сотрудника или подразделения. Значок в первом столбце указывает на раздел, в котором было создано сообщение Viber. 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 **Уведомление по неприходу**.
- «Сообщение общей рассылки» – сообщение создано в разделе **«Сотрудники»**.
- «Тестовое сообщение» – сообщение отправлено при тестовой рассылке из **«Центра управления»**.



**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](http://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»** и произведите [поиск необходимого устройства](#).
4. Произведите настройку параметров видеоподсистемы и камер. Для этого выделите устройство в рабочей области раздела и на вкладке **Параметры** панели настройки произведите необходимые изменения.
5. 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.
6. При необходимости произведите настройку подсистемы [«Камеры СКУД»](#).

## 7.1 Поиск устройств видеоподсистемы

### Автоматический поиск устройств видеоподсистемы

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

Выбор сетевых интерфейсов x

Выберите сетевые интерфейсы, по которым будет производиться поиск устройств.

Адрес подсети	Маска подсети
<input type="checkbox"/> 10.0.0.0	255.0.0.0
<input checked="" type="checkbox"/> 172.17.0.0	255.255.0.0

Диапазон поиска устройств

IP-адрес начала диапазона

IP-адрес конца диапазона

Поиск только внутри диапазона

Контроллеры доступа и регистрации, КБО, ППКОП








Драйверы шлейфа




Видеоподсистемы

Биометрические системы SUPREMA

- В открывшемся окне отметьте подсети, в которых будет произведен поиск устройств или воспользуйтесь панелью **Диапазон поиска устройств**. Установите флажок **Видеоподсистемы**. Нажмите кнопку **OK**. По окончании поиска откроется окно **Конфигуратор** со списком найденных устройств:


Конфигуратор

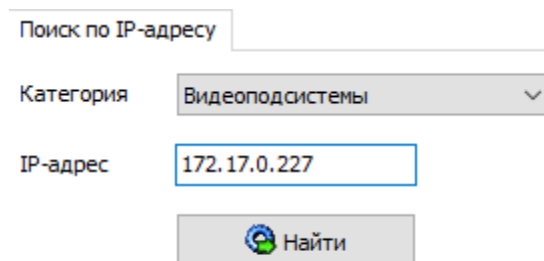
Устройство	IP-адрес	Состояние	Информация
Видеоподсистема	172.17.0.110		Найдено новое оборудование.
Видеоподсистема	172.17.0.25		Найдено новое оборудование.
Видеоподсистема	172.17.1.147		Найдено новое оборудование.
Видеоподсистема	172.17.0.227		Найдено новое оборудование.
Видеоподсистема	172.17.1.138		Найдено новое оборудование.
Видеоподсистема	172.17.0.89		Найдено новое оборудование.
Видеоподсистема	172.17.0.50		Найдено новое оборудование.


- В открывшемся окне нажмите кнопку **OK**. Все найденные устройства будут добавлены в рабочую область раздела и отмечены значками .
- 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

Если видеоподсистема не была найдена при автоматическом поиске, то произведите ее поиск по IP-адресу ПК, на котором установлен модуль **Сервер видеоподсистемы**.

1. Для этого на панели инструментов раздела нажмите кнопку  **Добавить новое устройство**. В нижней части окна откроется панель **Поиск по IP-адресу**:




2. На открывшейся панели в выпадающем списке **Категория** выберите пункт: **Видеоподсистемы**.
3. В поле **IP-адрес** введите IP-адрес ПК, на котором установлен модуль **Сервер видеоподсистемы**. Нажмите на панели ставшую при этом активной кнопку **Найти**.
4. 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 .

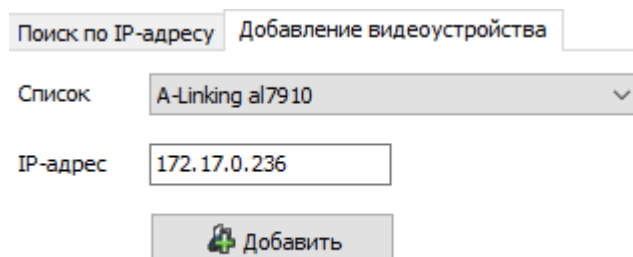
### Поиск камер, поддерживающих стандарт ONVIF

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

### Поиск камеры по IP-адресу


Если камера не была найдена при автоматическом поиске, то произведите ее поиск по IP-адресу. Для этого:

1. В рабочей области раздела выделите видеоподсистему, в которую необходимо добавить камеру и нажмите кнопку  **Добавить новое устройство**.
2. На панели **Поиск по IP-адресу** в выпадающем 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**.
3. Перейдите на вкладку **Добавление видеоустройства**:









4. В выпадающем списке **Список** выберите модель искомой видеокамеры, в поле **IP-адрес** введите ее IP-адрес. Нажмите ставшую при этом активной кнопку **Добавить**.

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

Произведите настройку параметров видеоподсистемы и камер. Для этого выделите устройство в рабочей области раздела и на вкладке **Параметры** панели настройки произведите необходимые изменения.

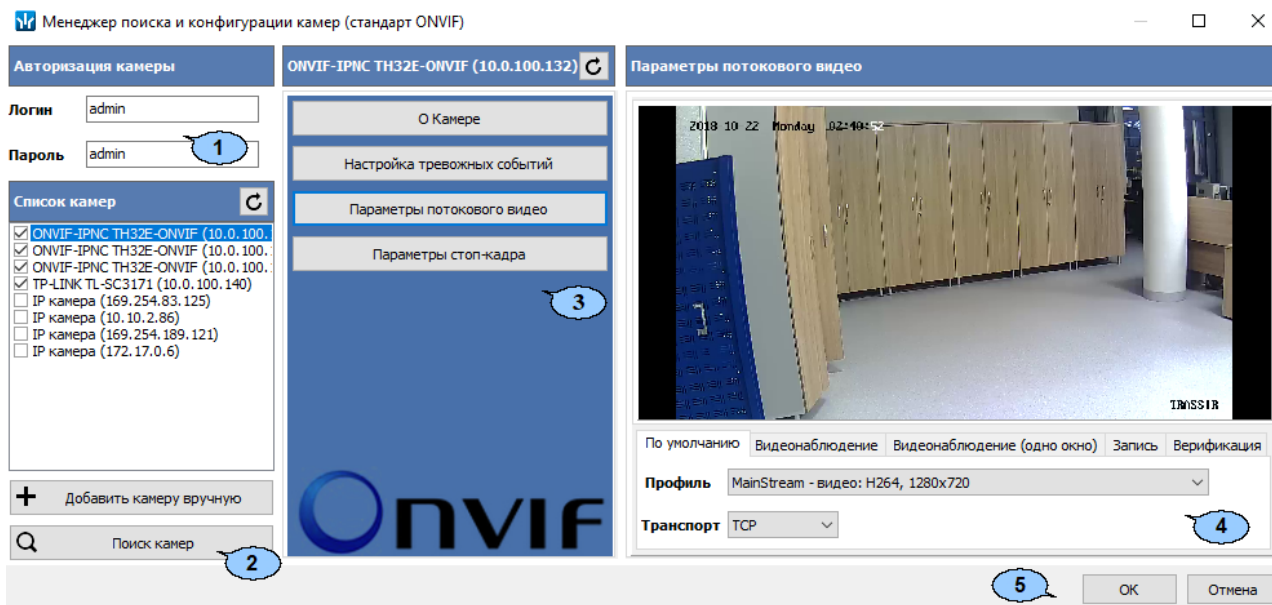
Для добавления найденных устройств в конфигурацию системы выделите в рабочей области раздела видеоподсистему и нажмите кнопку  **Передать параметры** на панели инструментов раздела. В устройства будут переданы заданные параметры конфигурации. В случае успешной передачи параметров в устройства значки  в списке объектов заменятся на значки  и , соответственно, для видеоподсистемы и камер.

При необходимости произведите настройку подсистемы [«Камеры СКУД»](#).

## 8 Подключение камер, поддерживающих стандарт ONVIF

### 8.1 Окно «Менеджер поиска и конфигурации камер (стандарт ONVIF)»

Окно **Менеджер поиска и конфигурации камер (стандарт ONVIF)** выглядит следующим образом и содержит элементы:





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** – выпадающий список для выбора алгоритма сжатия (видеокодека) и размера изображения потокового видео с камеры;
    - **Транспорт** – выпадающий список выбора протокола передачи потокового видео;
    - Для PTZ-камер, поддерживающих удаленное управление, доступны кнопки управления ориентацией и зумом камеры, а также поле для выбора направления камеры.

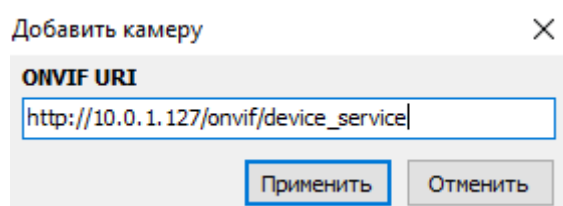
- **Параметры стоп-кадра** – для настройки профиля стоп-кадр.

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

## 8.2 Порядок поиска камер, поддерживающих стандарт ONVIF

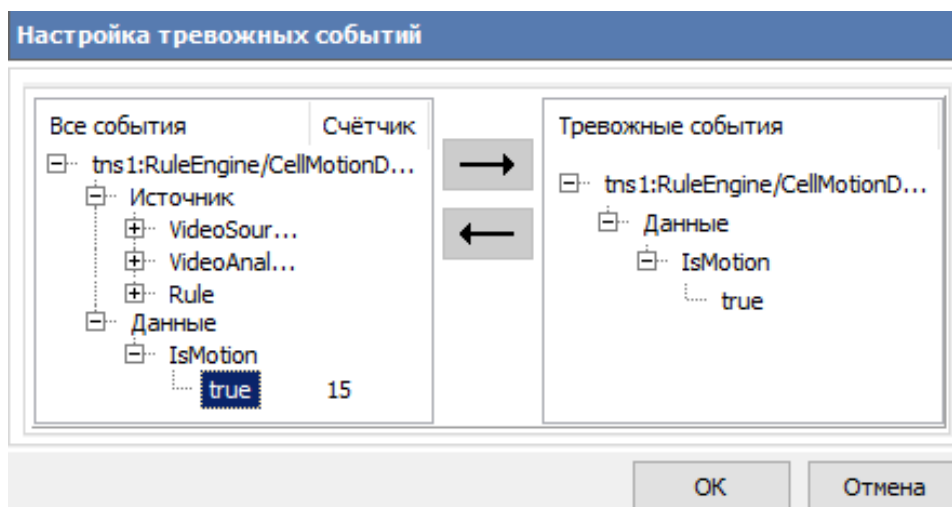
Для поиска камер, поддерживающих стандарт ONVIF, выполните следующие действия:







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 выпадающем 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:



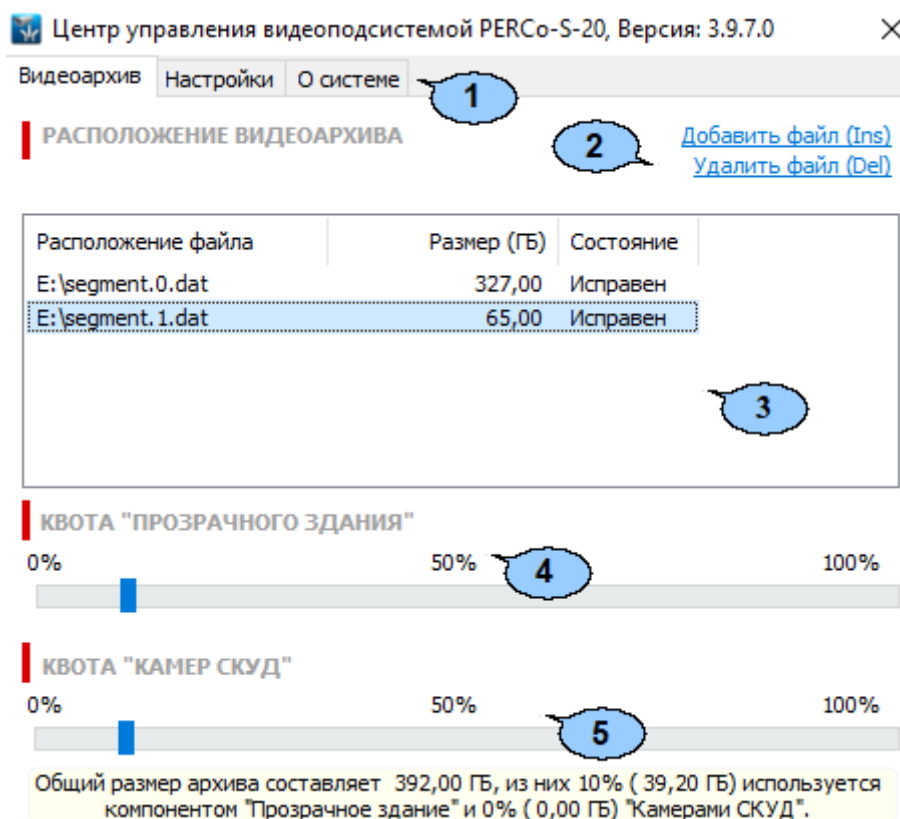
9. В левой части рабочей области отображается список событий, регистрируемых камерой. Наличие, перечень и описание событий зависит от модели камеры. Используя кнопку  добавьте необходимые события камеры в тревожные события. Для удаления события используйте кнопку .
10. Для настройки параметров потокового 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 этого 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:



- Выбор вкладки окна:
  - **Видеоархив**;
  - [Настройки](#);
  - [О системе](#).
- 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.

- Рабочая область вкладки содержит список созданных ранее файлов видеоархивов с указанием их расположения, размера и состояния.
- 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 видеoinформации с камеры СКУД.



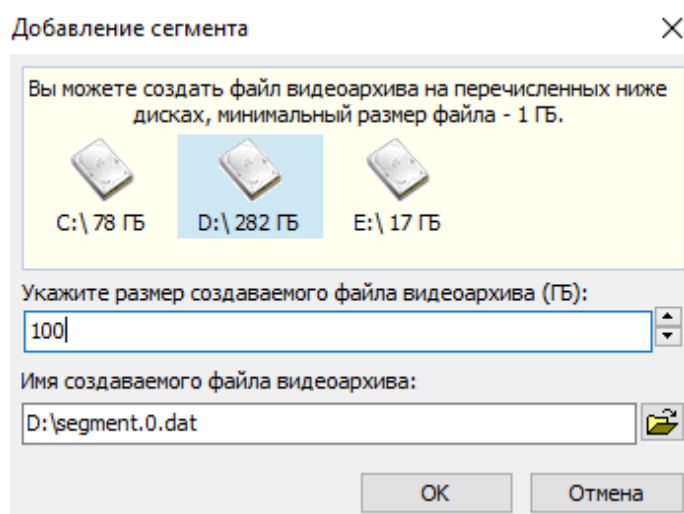
### **Внимание!**


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

## 9.1.2 Создание и удаление 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**:

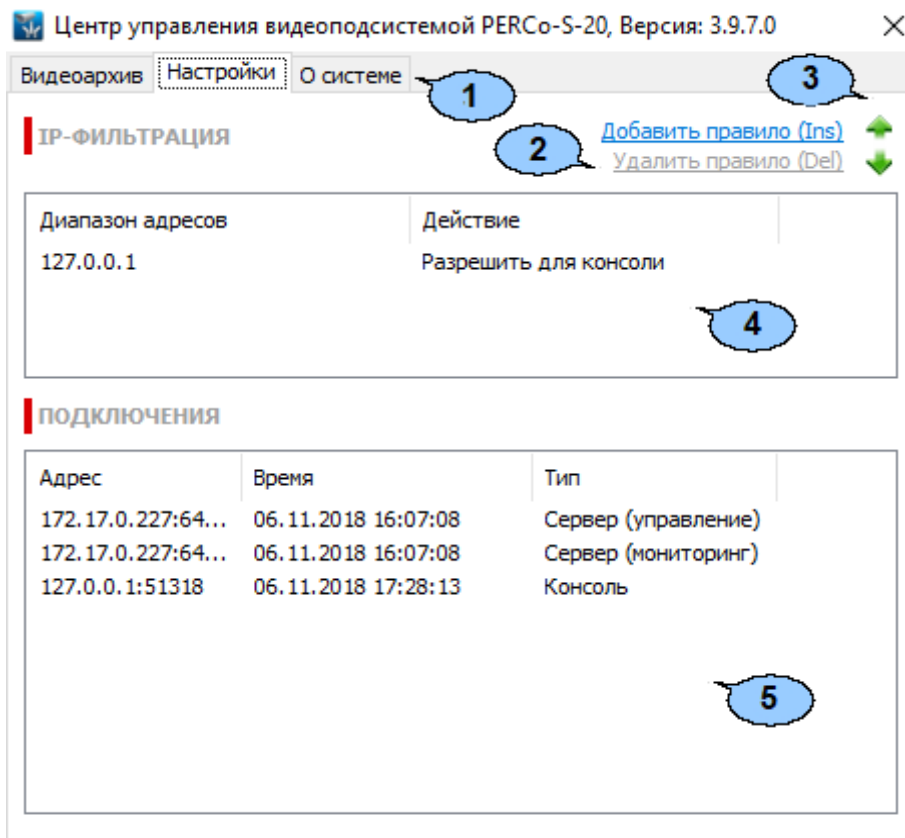




3. В открывшемся окне выделите название диска ПК, на котором будет создан файл видеоархива.
4. С помощью соответствующего счетчика укажите размер создаваемого файла видеоархива или введите значение с клавиатуры.
5. При необходимости измените имя файла видеоархива и его расположение (по умолчанию файл видеоархива `segment0.dat` располагается в корневом каталоге указанного диска). Для изменения расположения нажмите кнопку  рядом с полем **Имя создаваемого файла видеоархива**.
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  **Закреть** 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 содержит:
  - **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 с использованием следующих правил:

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

Для добавления фильтра IP-адресов:

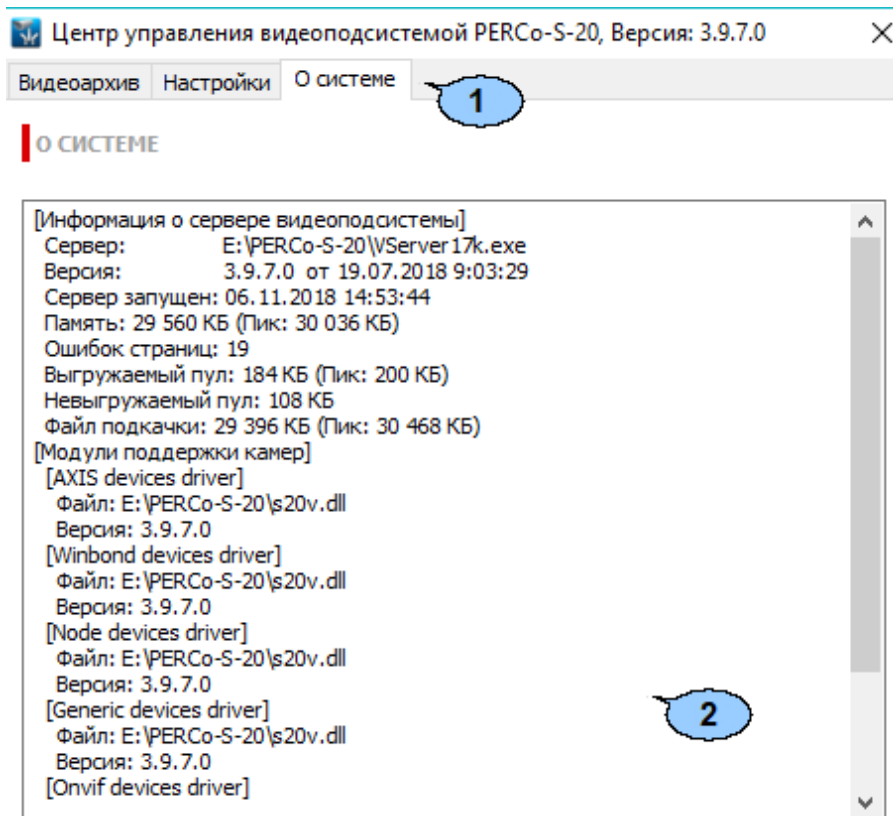
1. Запустите **«Центр управления видеоподсистемой»** и перейдите на вкладку **Настройки**.
2. Нажмите кнопку **Добавить правило** на панели инструментов вкладки. Откроется окно **Правило фильтрации**:

3. В открывшемся окне с помощью переключателя выберите одно из правил фильтрации.
4. С помощью полей **С адреса** и **По адрес** укажите диапазон IP-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  **Закреть** 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 с описанием характеристик системы.

## 10 Установка драйвера видеокамеры

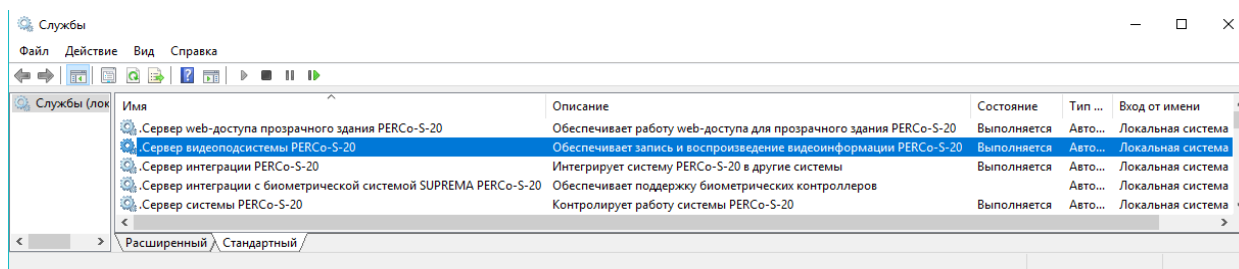


### Внимание!

Список поддерживаемых видеоподсистемой камер наблюдения представлен на сайте компании **PERCo**, по адресу [www.perco.ru](http://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 **Выполняется** 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 правой кнопкой мыши. 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 **Выполняется**.
8. Запустите «**Консоль управления**», перейдите в раздел «**Конфигуратор**» и добавьте камеру в видеоподсистему.

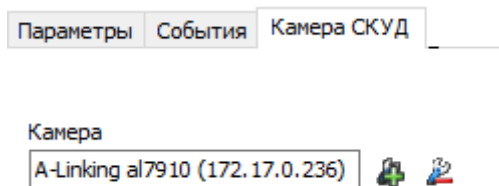
## 11 «Камеры СКУД»

**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.

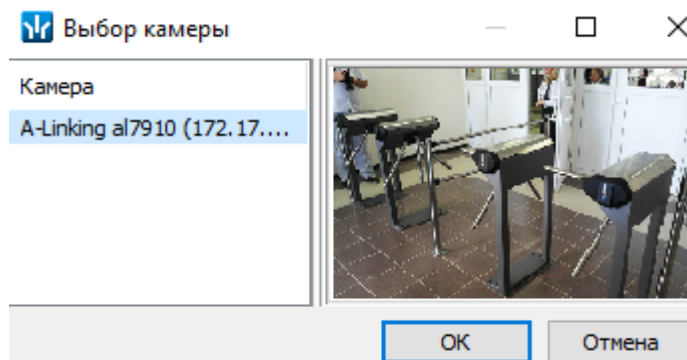
С любым считывателем, подключенным к одному из контроллеров, системы можно связать одну из камер видеоподсистемы. При этом одна камера одновременно может быть связана с несколькими считывателями.

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*. Также 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 прозрачного здания** 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`.

Войдите, используя учетную запись  
PERCo-S-20

Имя пользователя:

Пароль:

Запомнить мои данные  
на этом компьютере.

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

## Параметры работы веб-доступа прозрачного здания

### Сервер системы

Сервер системы по умолчанию использует порт **211**. Для использования другого порта его можно указать в имени сервера в формате **адрес\_сервера:порт**

Расположение:

### Вариант доступа к странице

Вход по паролю - пользователь должен войти в систему, используя учетные данные PERCo-S-20

Пароль не запрашивается, используется следующая учетная информация:

Имя пользователя:

Пароль:

### HTTP

Основной HTTP-порт сервера - **8080**. При необходимости Вы можете выбрать другой альтернативный HTTP-порт. При этом сервер будет обслуживать подключения как по основному порту, так и по указанному Вами альтернативному.

Используется следующий альтернативный порт:

### Изображение

Степень JPEG сжатия 19  100

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 также 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 также доступны на вкладке **Установка**. После загрузки необходимо вручную распаковать содержимое этого архива в папку хранения интернет файлов Web-сервера.

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. Выполните следующие действия:

1. Установите сервер.
2. Установите поддержку PHP.
3. Создайте сертификат для SSL.
4. Скопируйте файлы веб-доступа в папку хранения интернет файлов Web-сервера (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 используется нестандартный порт для SSL или HTTP, то 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 какой-то один из портов нестандартный, то править необходимо во всех местах, поскольку *Apache* не редиректит на порт по умолчанию. Если же порты стандартные, то нет необходимости вносить изменения.

## Защита сервера при помощи SSL

### Создание сертификата

Хотя в *Apache 2.2.x* и есть поддержка *OpenSSL*, по умолчанию она отключена. Необходимо подключить вручную. Для этого:

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 необходимо 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
```

Обычно файл `privkey.pem` создается автоматически, но если этого не произошло, введите 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*.

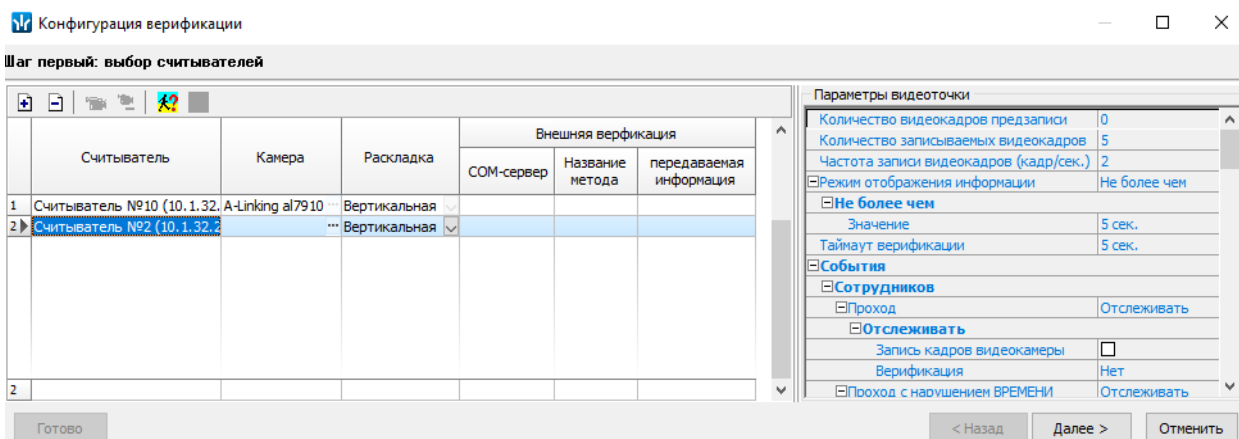




## 13 Внешняя программа верификации


### 13.1 Регистрация программы

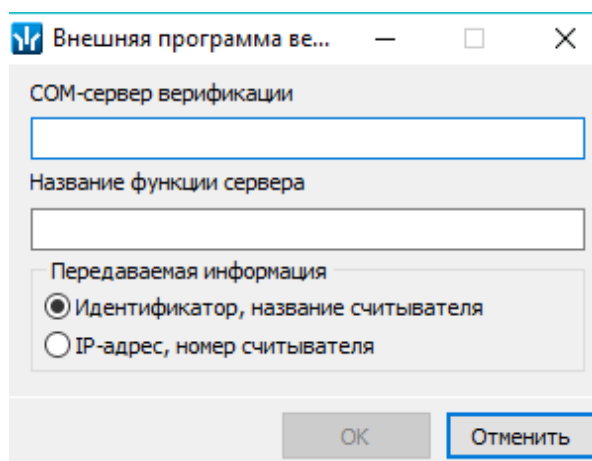
В разделе **«Верификация»** модуля **PERCo-SM09 «Верификация»** реализована возможность использование внешней программы верификации (далее – ВПВ). При использовании ВПВ оператору **PERCo-S-20** недоступны штатные средства реагирования на запрос (кнопки **РАЗРЕШИТЬ / ЗАПРЕТИТЬ**). Регистрация ВПВ производится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

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**:



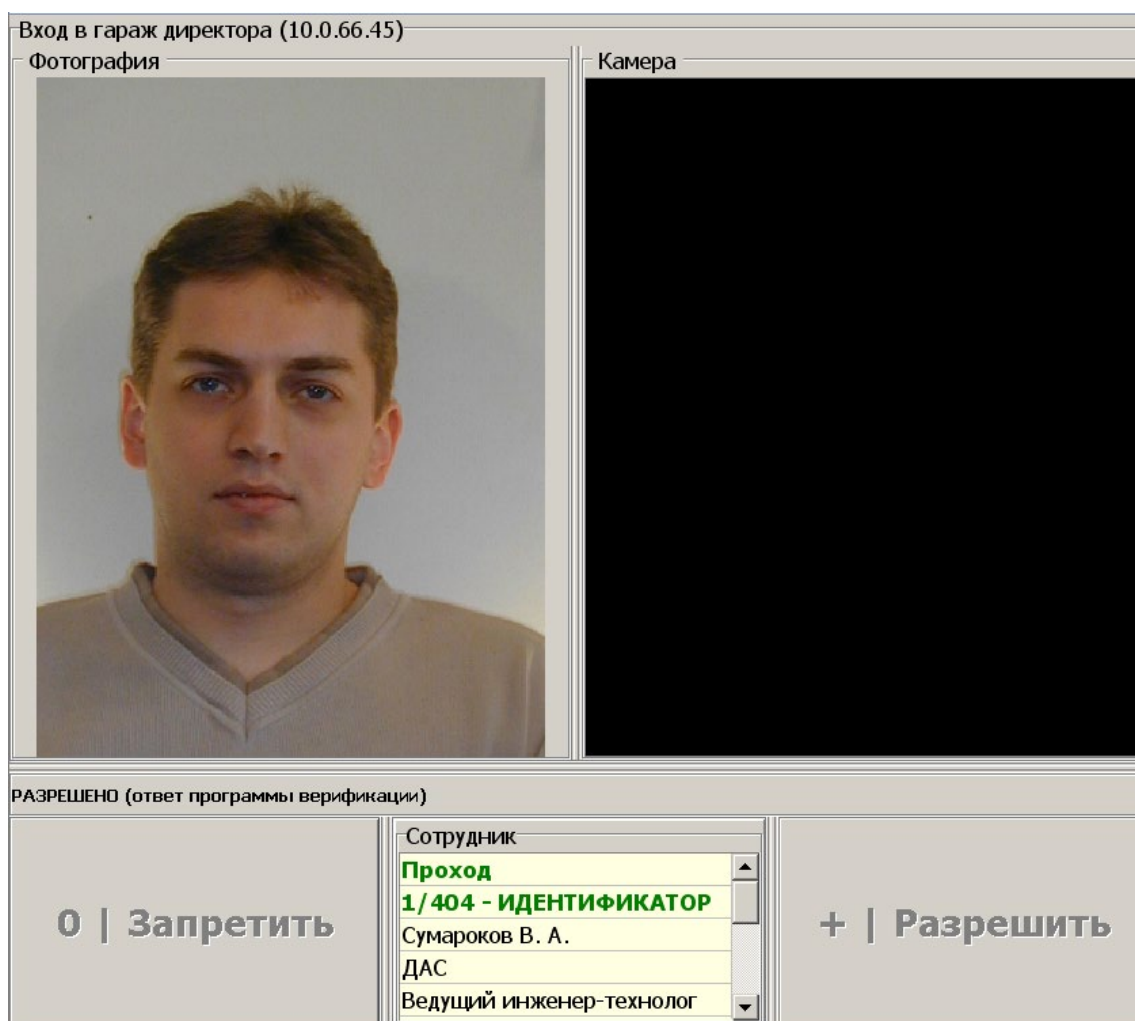
В поле **COM-сервер верификации** необходимо ввести название сервера, в поле **Название функции сервера** – название функции верификации (эти данные сообщают программисты-создатели ВПВ). Выберите тип передаваемой информации. Нажмите кнопку **ОК**, система проверяет возможность связи с ВПВ, и при благополучном вызове ВПВ ей будет послан тестовый запрос на обработку идентификатора 9999999999999999. После получения ответа на этот запрос откроется окно подтверждения.

Для подтверждения операции нажмите кнопку **Да**. 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 ознакомления 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) заполняется пользователем. 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 ATypeInquiry,
[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;
ATypeInquiry: Integer;
var ADenyReason, AErrorMessage: WideString): Integer.
```

#### Описание функции на C#

```
int <Название функции>
(string AIdentifier,
int ATimeout,
string AReaderName,
int ATypeInquiry,
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*).

**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 пустого символа.



**Примечание:**

При некорректных результатах работы раздела верификации можно посмотреть информацию файла `Console17k.log`.

## **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](http://www.perco.ru)**

Кор. 23.10.2023



[www.perco.ru](http://www.perco.ru)