Система S–20 «Школа»
Модуль «Расширенное ПО»

PERCo-SS02

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Версия ПО: 2.9.7.0

СОДЕРЖАНИЕ

1 Введение ... 4
2 «Консоль управления» ... 5
2.1 Запуск консоли ... 5
2.2 Элементы управления ... 8
2.3 Выбор раздела ... 10
2.4 Закрытие консоли ... 11
3 Раздел «Конфигуратор» ... 12
3.1 Назначение ... 12
3.2 Вкладка "Конфигурация" ... 12
3.2.1 Рабочее окно раздела ... 12
3.2.2 Автоматическая конфигурация ... 16
3.2.3 Добавление нового устройства ... 19
3.2.4 Настройка системы безопасности ... 20
3.2.5 Состояние связи с контроллерами ... 21
3.2.6 Удаление и восстановление устройства ... 22
3.2.7 Изменение сетевых настроек ... 23
3.2.8 Подвкладка «Параметры» ... 23
3.2.9 Подвкладка "Справочник объяснительных" ... 29
3.2.10 Подвкладка «События» ... 30
3.2.11 Подвкладка "Настройка реакций" ... 33
3.2.12 Подвкладка «Камера СКУД» ... 36
3.2.13 Панель ввода дополнительных данных ... 37
3.2.14 Параметры ресурсов ... 43
3.3 Вкладка "Шлюзы" ... 98
3.3.1 Рабочее окно вкладки ... 99
3.3.2 Создание шлюза ... 100
3.4 Вкладка "Составные объекты" ... 101
3.4.1 Рабочее окно вкладки ... 101
3.4.2 Создание составного контроллера ... 102
4 Раздел «Видеонаблюдение» ... 103
4.1 Назначение ... 103
4.2 Рабочее окно раздела ... 103
4.3 Создание новой схемы ... 105
4.4 Настройка параметров схемы ... 108
4.4.1 Вкладка «Схема» ... 109
4.4.2 Вкладка «Изображение» ... 110
4.4.3 Вкладка «Камера» ... 111
4.4.4 Вкладка «Действия» ... 112
4.4.5 Вкладка «Разное» ... 112
4.4.6 Вкладка «Вывод» ... 113
5 Раздел «Верификация» ... 114
5.1 Назначение ... 114
5.2 Рабочее окно раздела ... 115
5.3 Конфигурация точки верификации ... 117
5.4 Параметры точки верификации ... 120
5.4.1 Верифицируемые события ... 121
5.4.2 Уведомляющие события ... 123
5.5 Верификация от ПДУ ... 123

6 Раздел «Журнал верификации» ... 127
6.1 Назначение ... 127
6.2 Рабочее окно раздела ... 127
6.3 Формирование отчета ... 132
6.4 Настройки выборки ... 132
7 Раздел «SMS-биллинг» ... 134
7.1 Назначение ... 134
7.2 Используемые термины ... 134
7.3 Рабочее окно раздела ... 136
7.4 Вкладка «Установки» ... 138
7.5 Операции со счетами абонентов ... 140
7.6 Пополнение счетов с помощью импорта из файла MS Office Excel ... 141
7.7 Журнал операций со счетом ... 145

1 Введение

Данное *«Руководство пользователя»* (далее – *руководство*) предназначено для сотрудников службы охраны школ. В руководстве описаны процедуры работы с разделами модуля ***PERCo-SS02 «Расширенное ПО Школа»*** в виде пошаговых инструкций с необходимыми комментариями и примечаниями.

Данное руководство должно использоваться совместно с *«Руководством пользователя»* на модуль ***PERCo-SS01 «Базовое ПО Школа»***

Используемые сокращения и условные обозначения:

АРМ – автоматизированное рабочее место,
БД – база данных,
ОС – операционная система,
ИУ – исполнительное устройство,
ПО – программное обеспечение,
ПК – персональный компьютер,
СУБД – система управления базами данных.

2 «Консоль управления»

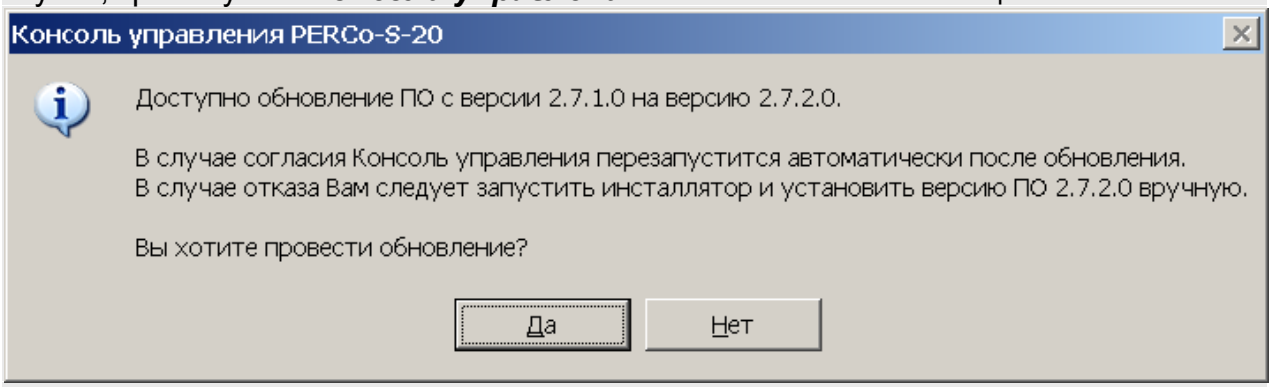
2.1 Запуск консоли

«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 2.6.3.0, в системе реализована функция автоматического обновления. Функция позволяет обновить ПО ***«Консоли управления»*** и всех установленных на ПК сетевых модулей.

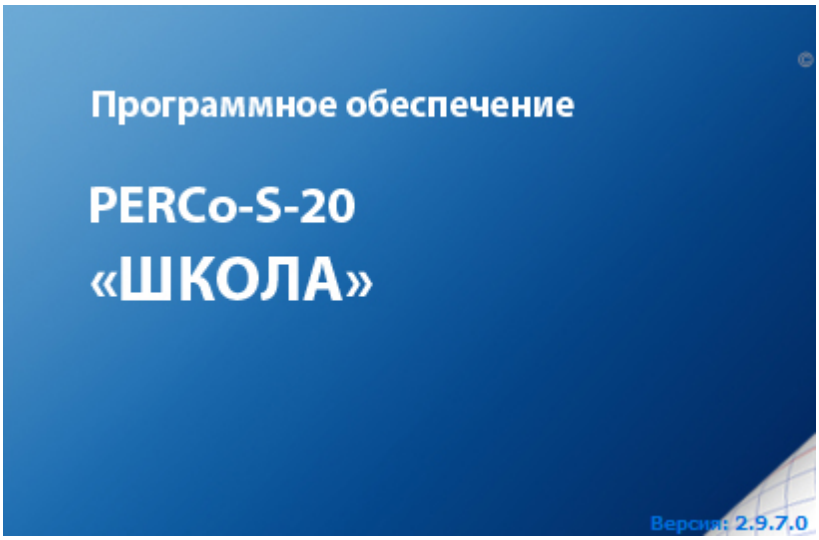
Процедура обновления будет запущена автоматически после подключения к серверу системы, если на сервере системы установлена более поздняя версия ПО. В этом случае, при запуске ***«Консоли управления»*** появится окно с сообщением:



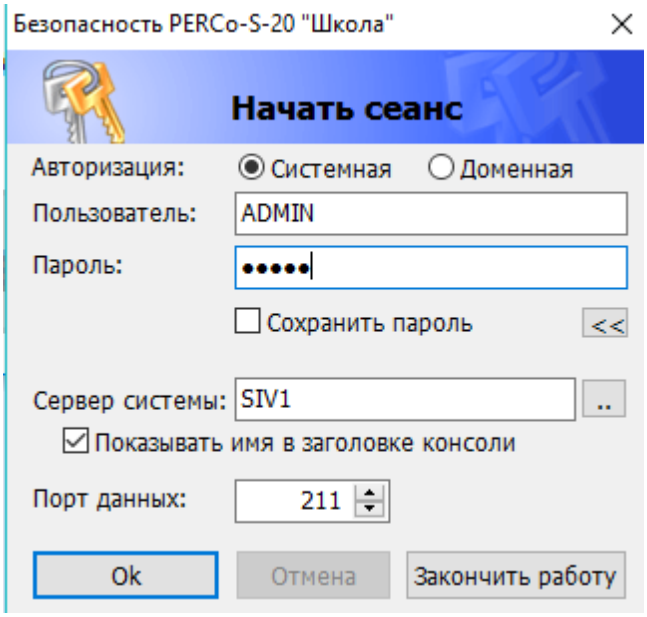
Для начала обновления нажмите кнопку **Да**.

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** – если флажок установлен, то после правильного ввода имени пользователя и пароля и успешного входа в систему при последующих запусках ***«Консоли управления»*** они запрашиваться не будут. Если флажок снят, то имя пользователя и пароль запрашиваются при каждом входе в систему.

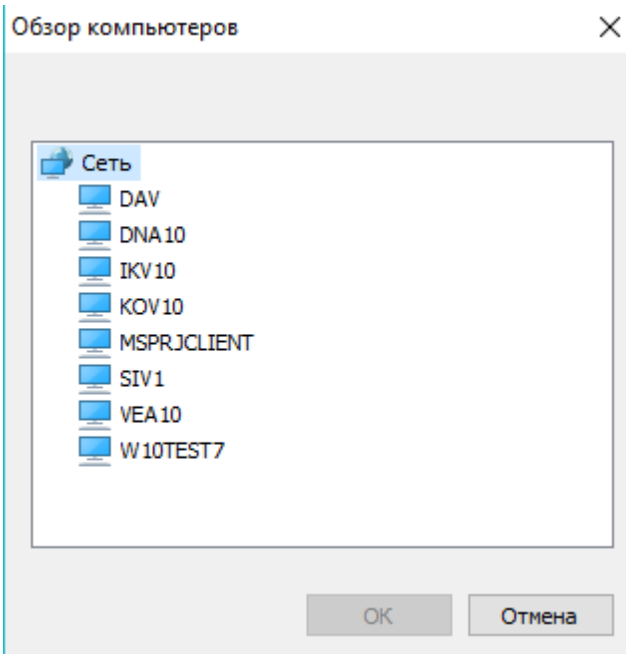
Примечание:

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

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

- << / >> – кнопка позволяет скрыть/открыть дополнительные поля ввода **Сервер системы** и **Порт данных**.
- **Сервер системы** – поле для ввода имени или IP-адреса компьютера, на котором установлен сервер системы. (Если сервер системы установлен на этом же компьютере, введите в строке: `localhost`.)

- **Показывать имя в заголовке консоли** – при установке флажка в строке заголовка ***«Консоли управления»*** будет отображаться имя или IP-адреса компьютера, на котором установлен сервер системы.
- – кнопка позволяет открыть окно **Обзор компьютеров** для указания компьютера, на котором установлен сервер системы в локальной сети:

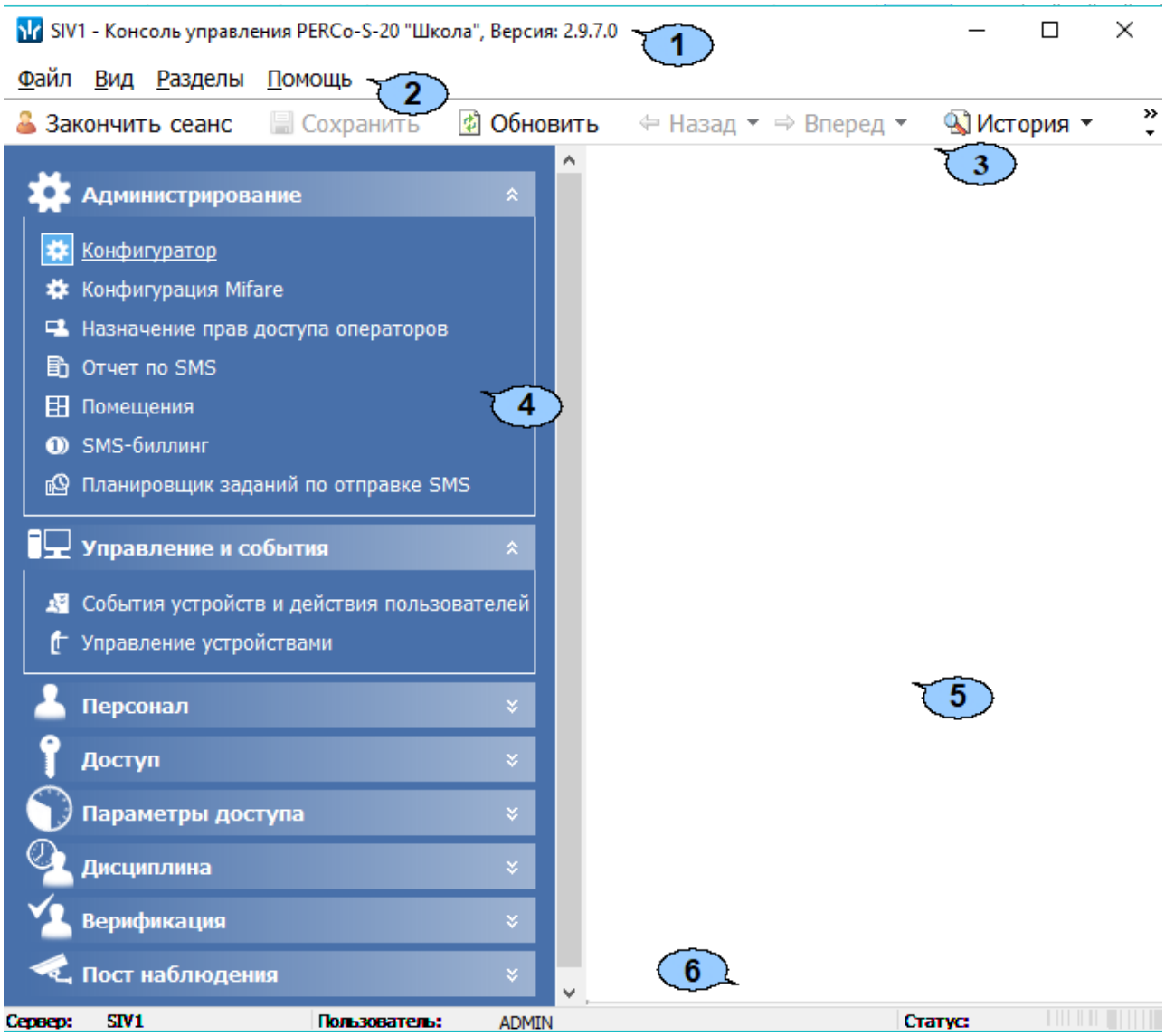


- **Порт данных** – строка позволяет указать порт, по которому будет осуществляться обмен данными с сервером системы. Порт должен совпадать с указанным в ***«Центре управления PERCo-S-20 Школа»*** (см. *«Руководство администратора PERCo-S-20 «Школа»»*). По умолчанию установлен порт `211`.

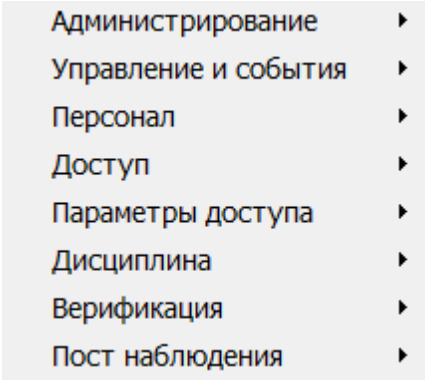
4. В строки **Пользователь** и **Пароль** введите имя и пароль, назначенные администратором системы. Пароль должен вводиться латиницей, проверьте раскладку клавиатуры. После трех неудачных попыток ввода приложение будет закрыто. Для уточнения имени и пароля обратитесь к администратору системы. Если ***«Консоль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

2.2 Элементы управления

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



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



Примечание:

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

- **Помощь** – меню данного пункта содержит следующие команды:

  Справка F1 – команда позволяет вызвать контекстную справку по открытому в рабочей области разделу:

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

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

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

3. Панель инструментов содержит следующие кнопки:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Примечание:

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

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

2.3 Выбор раздела

Для открытия раздела произведите одно из следующих действий:

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

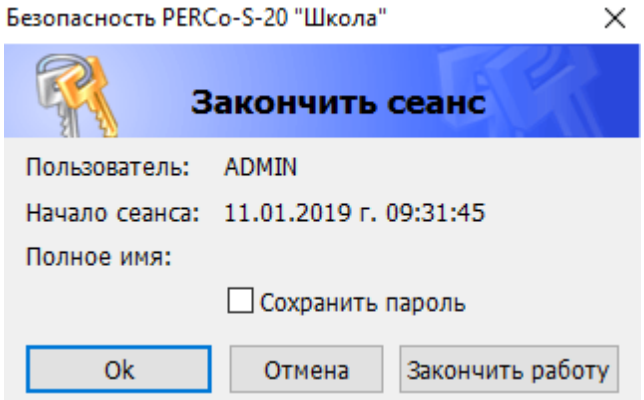
Примечание:

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

2.4 Закрытие консоли

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

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



ОК – кнопка позволяет закончить сеанс работы пользователя и открыть окно **Безопасность PERCo-S-20. Начать сеанс** для входа в систему другого пользователя.

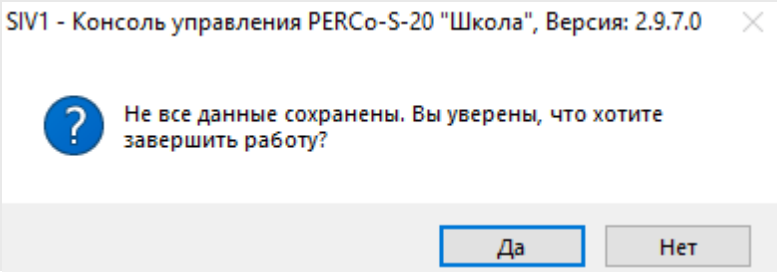
Отмена – кнопка позволяет вернуться к работе.

Закончить работу – кнопка позволяет завершить работу программы.

Сохранить пароль – при установке флажка система не будет запрашивать имя и пароль пользователя при входе в систему. При снятии флажка при входе в систему будет открываться окно **Безопасность PERCo-S-20. Начать сеанс**.

Примечание:

Если какие-либо данные не были сохранены в БД системы, 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

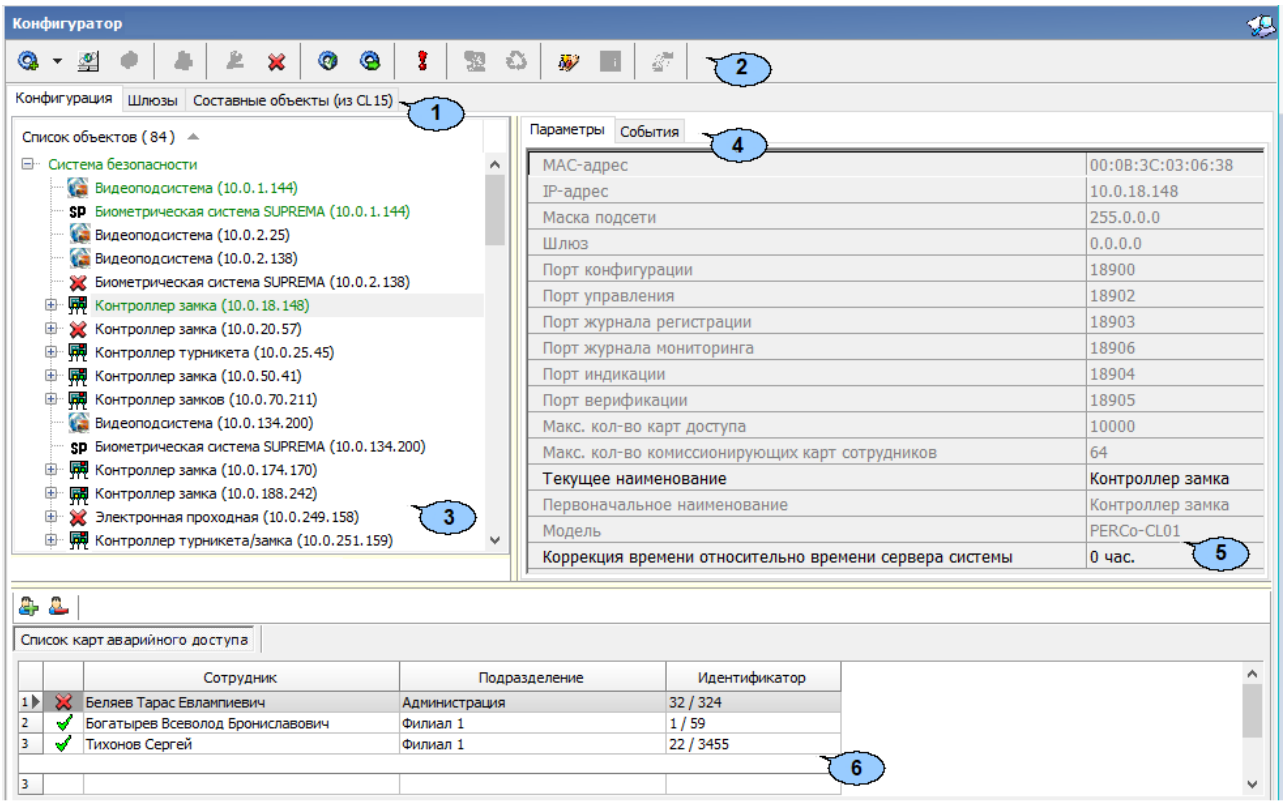
Раздел «***Конфигуратор»*** (Базовая версия) предназначен для конфигурации системы, создания шлюзов и создания составного контроллера.

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 комиссионирующих карт. Для контроллеров второго уровня списков карт аварийного доступа и для ППКОП списков карт и PIN-кодов постановки и снятия шлейфов сигнализации на охрану.

3.2.1 Рабочее окно раздела

Рабочее окно раздела имеет следующий вид:



1. Выбор вкладки раздела:
   - **Конфигурация;**
   - **Шлюзы;**
   - **Составные объекы.**
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 перемычек на плате контроллера или после изменения состава подключенных контроллеров второго уровня.
- для контроллеров серии ***S-30*** 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 группу ресурсов (Ctrl+N) – кнопка позволяет добавить до 7 групп ресурсов. Кнопка доступна при выборе в рабочей области раздела ресурса контроллера **Группа ресурсов**.

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

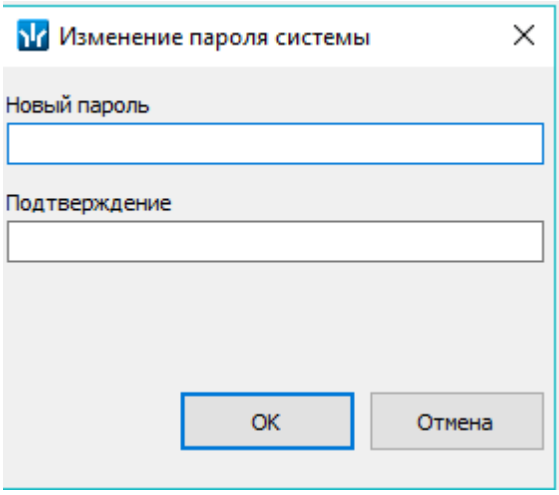
Исключить из конфигурации/ Включить в конфигурацию (Ctrl +O) – кнопка позволяет временно исключить выделенное в рабочей области устройство из конфигурации. Для включения в конфигурацию ранее исключенного устройства (отмеченное в списке объектов значком), выделенное в рабочей области и повторно нажмите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

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

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

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

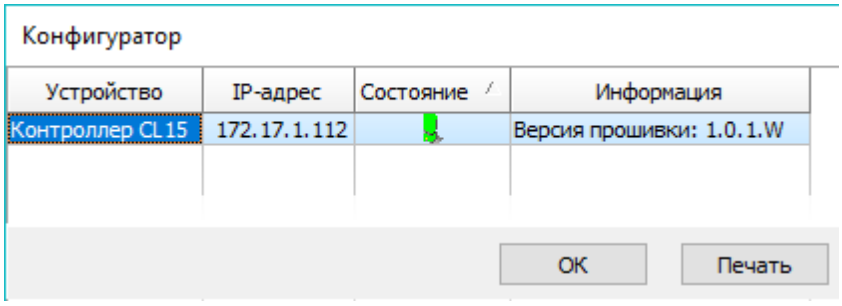
Изменение пароля (Ctrl+P) – кнопка позволяет изменить пароль доступа к контроллерам, добавленным в конфигурацию системы. Кнопка доступна при выборе в рабочей области корневого элемента списка объектов (по умолчанию «*Система безопасности»*). При нажатии кнопки откроется окно **Изменение пароля системы**:



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

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

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



Печать – кнопка 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** (кнопка не доступна для контроллеров электронной проходной ***PERCo-CT03***).

3. Рабочая область раздела **Список объектов** содержит раскрывающийся многоуровневый список устройств (подсистем) добавленных в конфигурацию системы и их ресурсов.

   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;

– устройство включено в конфигурацию системы, 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;
– 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 **Список объектов** 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.

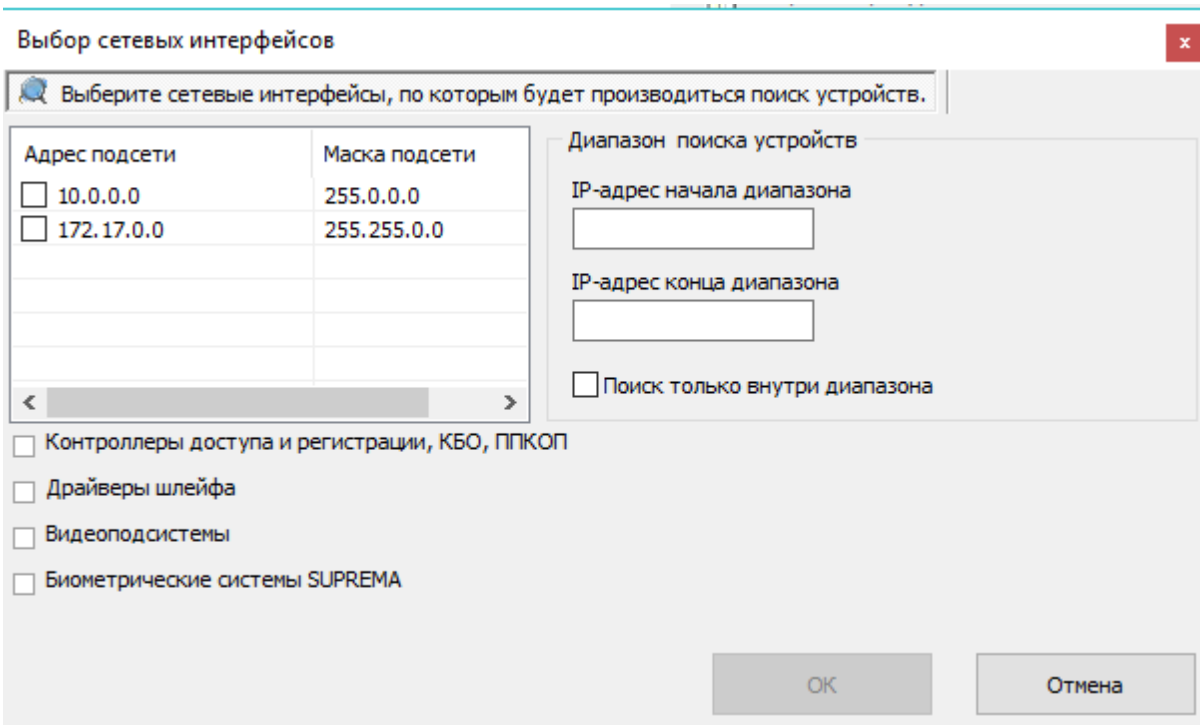
4. Выбор вкладки панели настройки
   - **Параметры**. Вкладка позволяет настроить параметры функционирования устройства или ресурса, выделенного в рабочей области **Список объектов**. Описание параметров приводится в *«Руководстве по эксплуатации»* на устройство.
   - **События**. На вкладке отображается список событий мониторинга, регистрируемых устройством или ресурсом, выделенным в рабочей области **Список объектов**. Также на вкладке можно задать реакцию системы в виде последовательности команд на любое из событий.
   - **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+H**. Значок ✖ в строке с данными сотрудника или PIN-кодом в рабочей области вкладки означает, что данные не были переданы в контроллеры, значок ✔ означает, что данные переданы успешно.

3.2.2 Автоматическая конфигурация

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

Для конфигуряция контроллеров с прямым подключением:

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



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 искомых устройств.
4. При необходимости адресной отправки запросов на устройств внутри диапазона IP-адресов, укажите в соответствующих полях первый и последний IP-адрес диапазона. В этом случае поиск производится широковещательной рассылкой запросов в подсети сетевого интерфейса и адресно в указанном диапазоне IP-адресов.
5. Для проведения только адресной отправки запросов внутри диапазона IP-адресов установите флажок **Поиск только внутри диапазона**.
6. Нажмите кнопку **ОК**. Окно **Выбор сетевых интерфейсов** будет закрыто, начнется поиск устройств.
7. После завершения поиска откроется окно **Конфигуратор** со списком найденных устройств:

Конфигуратор

Устройство	IP-адрес	Состояние	Информация
Контроллер CT/L14	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 CT/L14	172.17.1.117		Найдено новое оборудование.
Контроллер CL15	172.17.1.126		Найдено новое оборудование.
Контроллер CT/L14	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.

ОК Печать

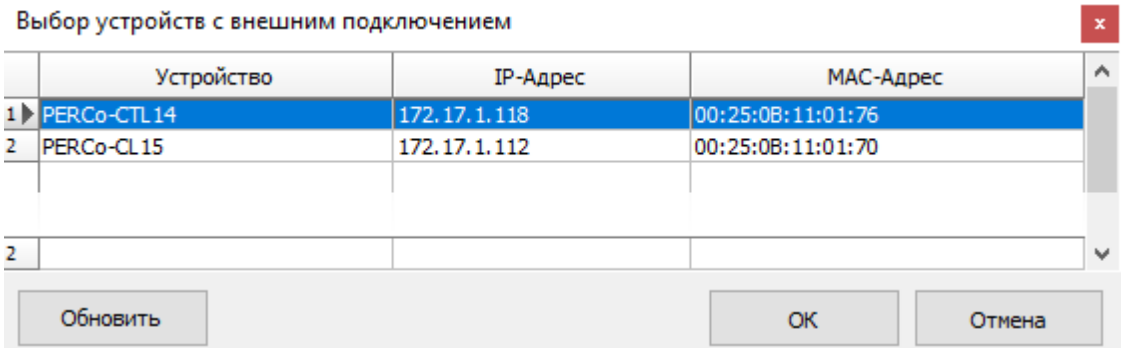
8. Кнопка **Печать** в открывшемся окне позволяет распечатать список найденных устройств.
9. Нажмите кнопку **ОК** (или ☒ в заголовке окна). Все найденные устройства будут добавлены в рабочую область раздела и отмечены значками ❓.
10. Если какое-либо из найденных устройство необходимо исключить из конфигурации,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

Для конфигурация контроллеров с внешним подключением:

Примечание:

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

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



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***).
3. Для обновления списка устройств нажмите кнопку Обновить.
4. Выберите необходимые устройства из списка и нажмите кнопку **ОК**. Устройства будут добавлены в рабочую область раздела и отмечены значками.
5. Если какое-либо из найденных устройство необходимо исключить из конфигурации, выделите его в рабочей области и нажмите кнопку **Исключить из конфигурации** на панели инструментов раздела. Значок устройства изменится на.
6. Для настройки параметров выделите устройство или ресурс в рабочей области раздела и на вкладке **Параметры** панели настройки измените необходимые параметры.
7. Для настройки реакций на события выделите устройство или ресурс в рабочей области раздела и на вкладке **События** панели настройки добавьте необходимые реакции.
8. Выделите в рабочей области раздела 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.

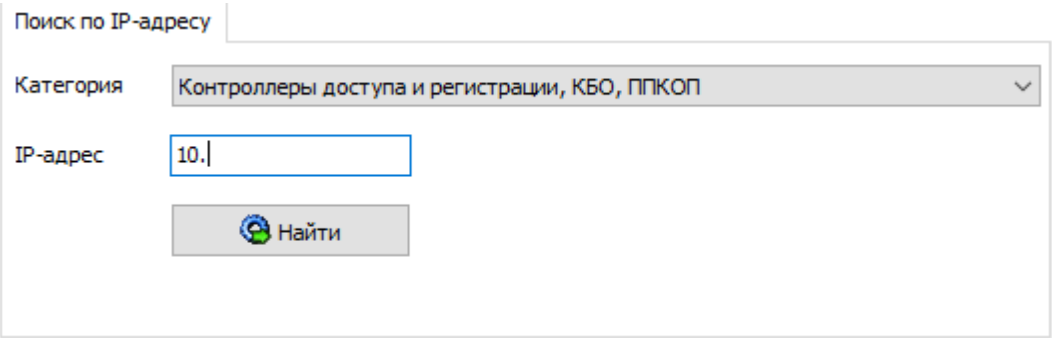
Примечания:

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. Для добавления в конфигурацию системы нового устройства:

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

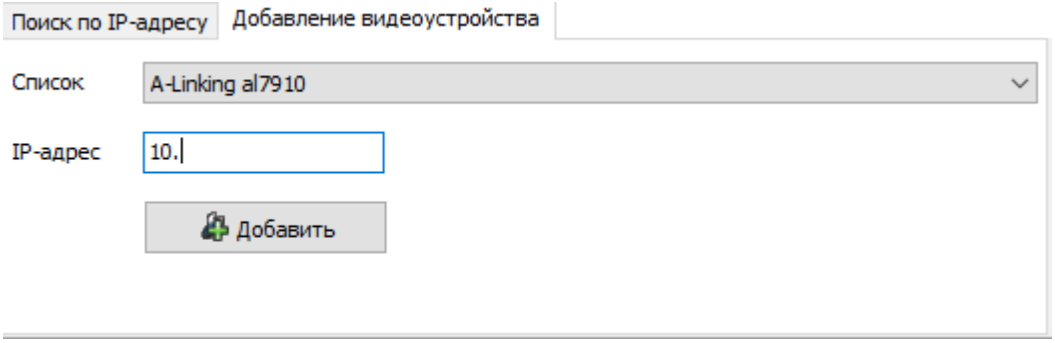


2. Используя раскрывающийся список **Категория**, укажите тип добавляемого устройства:
   - **Контроллеры доступа и регистрации, КБО, ПКОП** – для добавления контроллера доступа, регистрации или ПКОП.
   - **Видеоподсистемы** – для добавления сервера видеоподсистемы с файлами видеоархива.

Примечания:

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

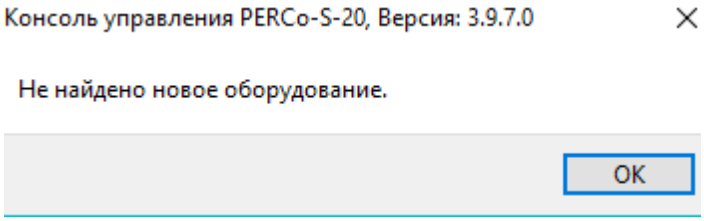
- **Камеры и видеосервера видеоподсистемы** – для добавления камер. При выборе пункта становится доступна вкладка **Добавление видеоустройства**. Для добавления камеры в видеоподсистему в раскрывающемся списке **Список** укажите модель камеры, в поле ввода **IP-адрес** укажите адрес и нажмите кнопку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



- **Камеры стандарта ONVIF видеоподсистемы** – для добавления камер поддерживающих стандарт ONVIF.
- **Биометрические системы SUPREMA.**

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

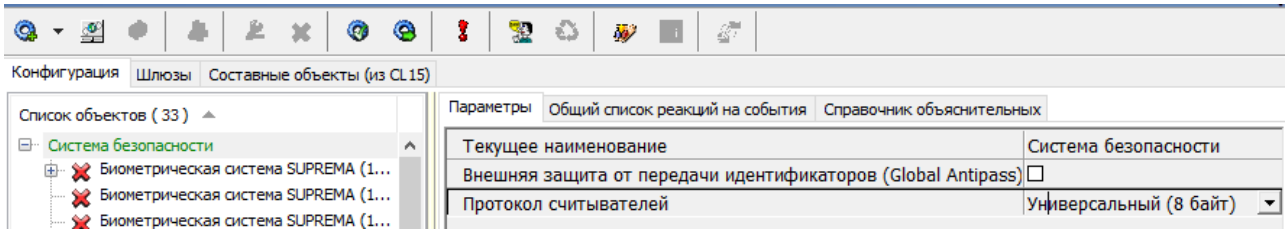
4. В случае успешного поиска откроется окно **Конфигуратор** содержащее в списке искомое устройство и указывающее состояние связи с ним. Для закрытия окна нажмите кнопку **ОК**. Найденное устройство будет добавлено в рабочее окно раздела **Список объектов**, отмеченное значком .
5. Если устройство не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



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

3.2.4 Настройка системы безопасности

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

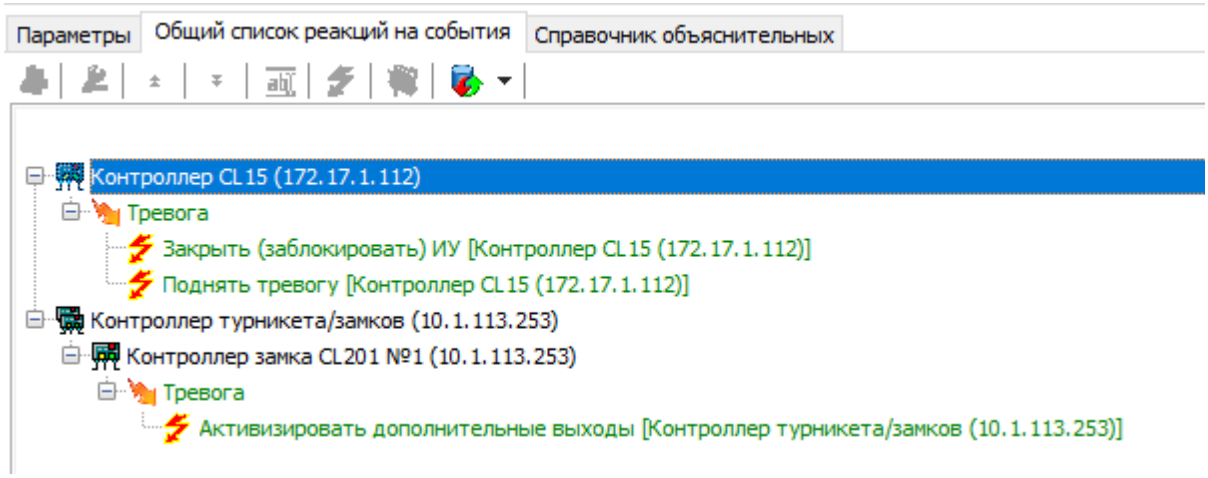


На вкладке **Параметры** доступны следующие параметры системы в целом:

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

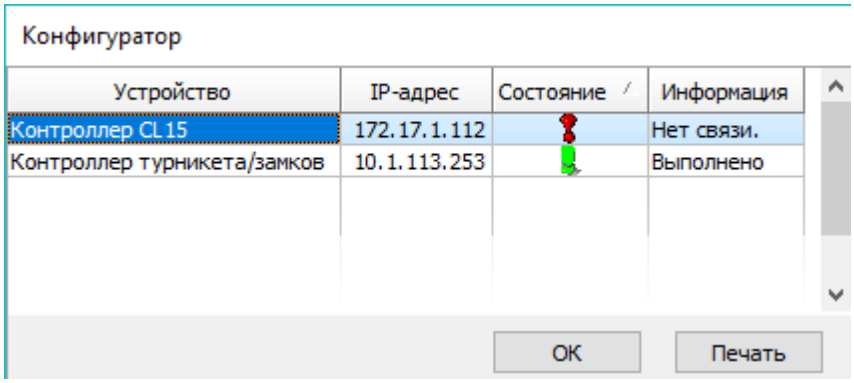
- **Wiegand 26** (3 байта, установлен по умолчанию) Номер карты делится на два числа - серия (1 байт, максимальное значение 255) и номер (2 байта, максимальное значение 65535). В таблицах ПО идентификатору отведено два столбца: **Код семейства** и **Номер**.
- **Универсальный** (8 байт. то есть полностью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

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



3.2.5 Состояние связи с контроллерами

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



Окно содержит следующие элементы:

- **Устройство** – в столбце указан тип устройства.
- **IP-адрес** – в столбце указан адрес устройства в сети.
- **Состояние** – в столбце отображено состояние связи с устройством:
  - – устройство найдено, связь с ним установлена, параметры переданы.
  - – санкционированное отключение связи.

– несанкционированная потеря связи с устройством, либо устройство не найдено, параметры не были переданы в .

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

3.2.6 Удаление и восстановление устройства

Удаления устройства

Внимание!

Прежде чем удалять устройство из конфигурации необходимо убедиться, что оно не связано ни с одним помещением в разделе ***«Помещения»***.
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 **Список объектов**.
2. Исключите устройство из конфигурации, нажав кнопку **Исключить из конфигурации** на панели инструментов раздела. Значок рядом с наименованием устройства примет вид .
3. Нажмите кнопку **Удалить** на панели инструментов раздела. В открывшемся окне **Подтверждение** для подтверждения удаления нажмите кнопку **Да**. Устройство будет удалено из конфигурации системы и исчезнет из рабочей области раздела.
4. Если устройство связано с помещением, появится окно **Подтверждение** с предложением скрыть устройство. Нажмите **Да,** если хотите скрыть устройство. Устройство будет отображаться в рабочей области раздела, выделенное красным цветом, при нажатой кнопке **Отображать скрытые устройства** .

Восстановление устройства

Примечание:

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

Для восстановления скрытого устройства:

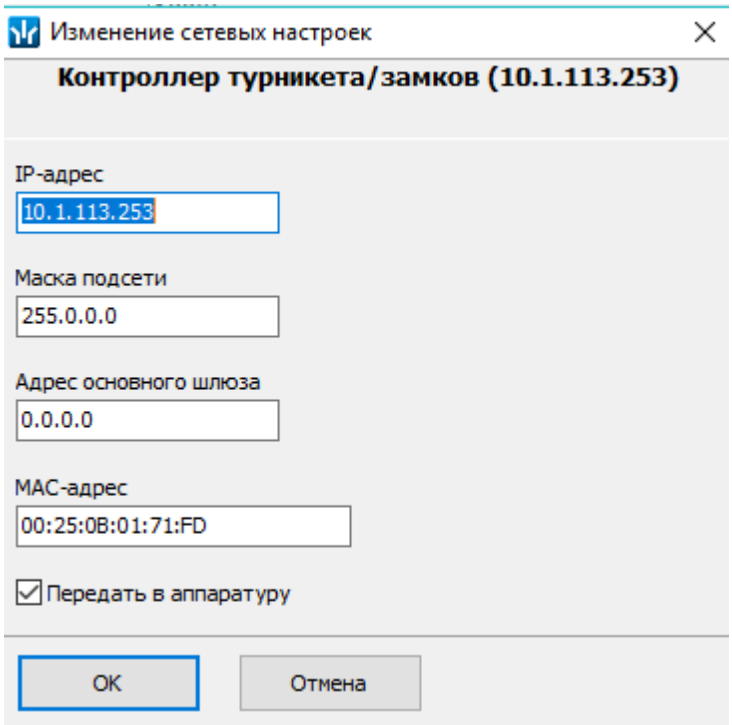
1. Нажмите кнопку **Отображать скрытые устройства** на панели инструментов раздела. В рабочей области раздела станут видны скрытые устройства, они будут выделены красным цветом.
2. Выделите в рабочей области скрытое устройство, которое необходимо восстановить и нажмите кнопку **Восстановить**. В открывшемся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

4. На панели инструментов раздела нажмите кнопку **Передать параметры**. После передачи параметров значок рядом с наименованием устройства примет вид, соответствующий типу устройства.

3.2.7 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 **Список объектов** контроллер, сетевые настройки которого необходимо изменить.
2. Исключите контроллер из конфигурации системы. 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»

На вкладке выводится список параметров и характеристик, доступных для устройства или его ресурса, выделенного в рабочей области раздела. Выделение параметров синим цветом указывает на то, что значения параметров были изменены но внесенные изменения не были переданы в устройства.

Параметры | События

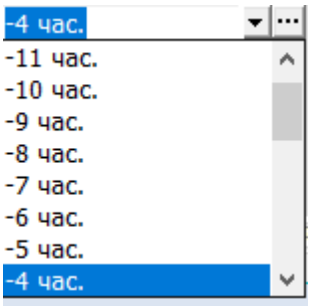
MAC-адрес	00:25:0B:01:71:FD
IP-адрес	10.1.113.253
Маска подсети	255.0.0.0
Шлюз	0.0.0.0
Порт конфигурации	18900
Порт управления	18902
Порт журнала регистрации	18903
Порт журнала мониторинга	18906
Порт журнала отладки	18908
Порт индикации	18904
Порт верификации	18905
Макс. кол-во карт доступа и комиссионирующих карт	50016
Текущее наименование	Контроллер турникета/замков
Первоначальное наименование	Контроллер турникета/замков
Модель	PERCo-CT/L04.2
Разрешить WEB-интерфейс	☐
Коррекция времени относительно времени сервера системы	0 час.

1. Выбор вкладки 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 синим цветом указывает на то, что значение параметра было изменено но внесенные изменения не были переданы в устройство.

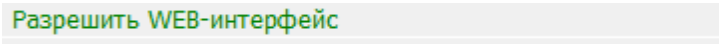
Для настройки параметра устройства или его ресурса, выделенного в рабочей области раздела, нажмите правой кнопкой мыши в правом столбце рабочей области вкладки в строке с наименованием параметра, который необходимо изменить. Используются следующие способы ввода значений параметров:

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

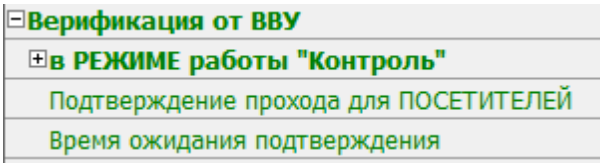
Раскрывающийся список позволяет выбрать одно из предложенных значений параметра. Для раскрытия списка необходимо нажать кнопку справа от установленного ранее значения.



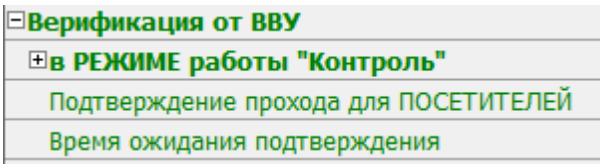
Окошко для флажка позволяет включить или выключить параметр, установив или сняв флажок.

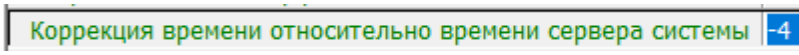


Счетчик позволяет установить числовое значение параметра. Для увеличения/ уменьшения значения параметра используйте кнопки, либо введите значение параметра с помощью клавиатуры.

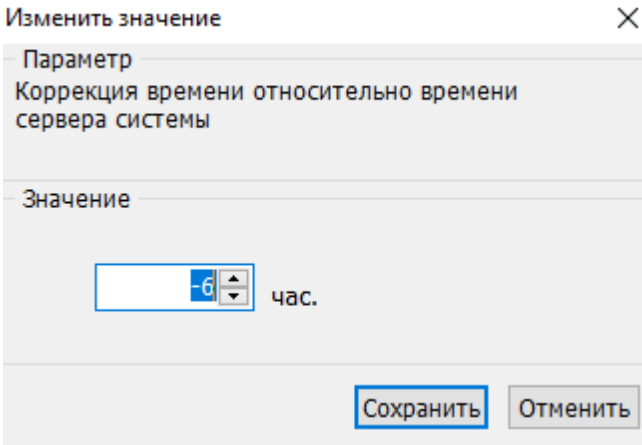


Выпадающий многоуровневый список позволяет получить доступ к группе параметров для их настройки при нажатии на значок ⊞, либо скрыть их, нажав значок ⊟.





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



Биометрический контроллер Suprema BioEntry W2

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

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

1. Запустите ***«Консоль управления»*** и откройте раздел ***«Конфигуратор»***.
2. Выделите в рабочей области раздела ресурс **Биометрическая система SUPREMA**, к которому подключен биометрический контроллер, и раскройте список его собственных ресурсов.
3. Выделите ресурс **Контроллер BioEntry W2.** На вкладке **Параметры**:
   - для параметра **Уровень безопасности** установите требуемый уровень безопасности при использовании верификации по отпечатку пальца;
   - для параметра **Таймаут сканирования пальца** установите время, которое будет выделяться системой на поднесение одного пальца при вводе отпечатков. Параметр задаётся в интервале от 3 до 20 секунд;

- для параметра **Таймаут верификации пальцем** (используется в режиме доступа **Карта и палец**) установите время, в течение которого будет ожидаться поднесение пальца для сканирования отпечатков (отсчёт времени начинается после того, как была предъявлена считывателю карта доступа). Параметр может быть задан в интервале от 1 до 20 секунд;
- для параметра **Таймаут поиска отпечатков** установите время, которое будет отводиться для поиска отпечатка в памяти контроллера. Если за отведенное время отпечаток не будет найден, то аутентификация будет отклонена. Параметр может быть задан в интервале от 1 до 20 секунд;
- для параметра **Чувствительность сканера** установите чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности обеспечивается высокое качество и скорость сканирования, при низком заданном уровне чувствительности уменьшается влияние факторов внешней среды (температуры и влажности воздуха, освещённости помещения, чистоты сканируемой поверхности подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию. Понижение заданного уровня чувствительности сканера осуществляется при необходимости в зависимости от условий эксплуатации. Параметр может быть задан в интервале от 1 до 7, где значение "1" соответствует самой низкой чувствительности, а значение "7" – самой высокой;
- для параметра **Алгоритм поиска отпечатков** установите автоматический алгоритм (рекомендован производителем) поиска отпечатков пальцев;
- для параметра **Режим датчика** установите режим работы считывающего датчика – либо он работает всегда, либо включается автоматически, если обнаруживает палец;
- для параметра **Режим авторизации** установите режим доступа:
  - **частный режим доступа** – в этом случае параметры доступа устанавливаются для отдельного сотрудника/посетителя в рамках СКУД;
  - **общий режим доступа** – в этом случае параметры доступа устанавливаются в рамках биометрического контроллера и будут применяться для всех пользователей, взаимодействующих ним;
- для параметра **Режим доступа** определите режим доступа при общем режиме авторизации (отображается, только если выбран «**Общий**» режим авторизации):
  - **Палец** – для верификации требуется пройти процедуру сканирования отпечатка пальца;
  - **Карта** – для верификации требуется предъявить считывателю карту доступа;
  - **Карта и палец** – для верификации требуется предъявить считывателю карту доступа, после чего пройти процедуру сканирования отпечатка пальца;
  - **Карта или палец** – для верификации требуется предъявить считывателю карту доступа или пройти процедуру сканирования отпечатка пальца;
- для параметра **Схема входных портов** необходимо назначить на входные порты **«Кнопку выхода»** и **«Датчик прохода»** (**«Датчик открытия \закрытия двери»**):
  - **Нет;**
  - **Кнопка выхода – порт 0;**
  - **Кнопка выхода – порт 1;**
  - **Датчик прохода – порт 0;**

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

Примечание:

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

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

Примечание:

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

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

Примечание:

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

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

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

Примечание:

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

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

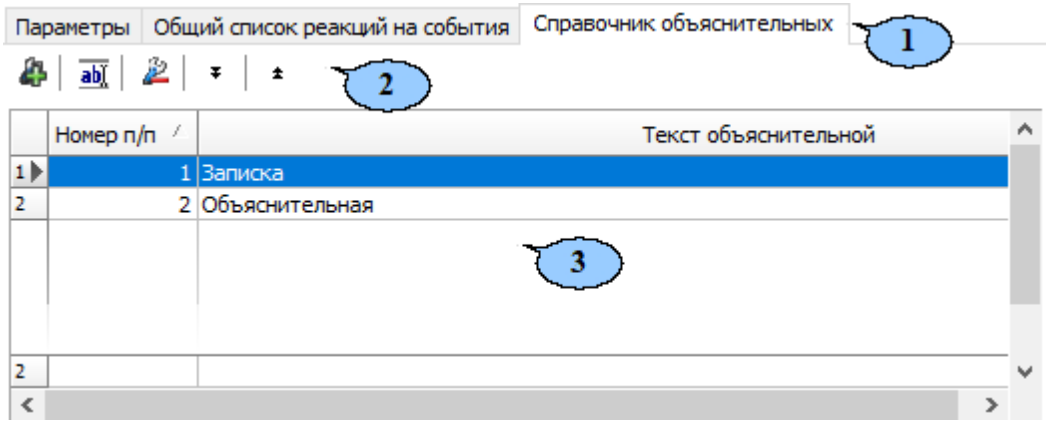
4. Выделите ресурс **Замок.** На вкладке **Параметры**:
   - параметр **Блокировать замок при закрытии двери** – при установке флажка дверь будет заблокирована сразу после закрытия;
   - параметр **Блокировать замок по таймауту, только если дверь закрыта** – при установке флажка замок будет заблокирован по истечении **Времени удержания в разблокированном состоянии** только после закрытия двери. Если флажок не установлен – замок будет заблокирован даже если дверь открыта;
   - для параметра **Время удержания в разблокированном состоянии** установите время, которое должно пройти от разблокировки замка до его блокировки после успешной аутентификации. За это время необходимо открыть дверь – иначе замок заблокируется. Параметр может быть задан в интервале от 1 до 30 секунд или от 1 до 15 минут;
   - для параметра **Предельное время разблокировки** установите максимальное разрешенное время для нахождения двери в открытом состоянии. Если дверь не закрыть за отведенное время – будет сгенерирован сигнал тревоги. Параметр может быть задан в интервале от 1 до 30 секунд или от 1 до 15 минут;
   - параметр **Генерация тревоги по взлому двери** – при установке флажка сигнал тревоги будет автоматически сгенерирован в случае, если был зафиксирован факт открытия двери без команды на открытие от контроллера;
   - параметр **Генерация тревоги по удержанию двери** – при установке флажка сигнал тревоги будет автоматически сгенерирован в случае, если истекло **Предельное время разблокировки** и дверь не была закрыта;

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

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

3.2.9 Подвкладка "Справочник объяснительных"

Рабочее окно подвкладки ***Справочник объяснительных*** доступно при выборе корневого элемента списка объектов (по умолчанию «*Система безопасности*»). Подвкладка предназначена для созадния и редактирования объяснительных. Список объяснительных передается на ***CR11*** и после этого отображается на дисплее в контроллере. Подвкладка имеет следующий вид:



1. Выбор подвкладки 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.

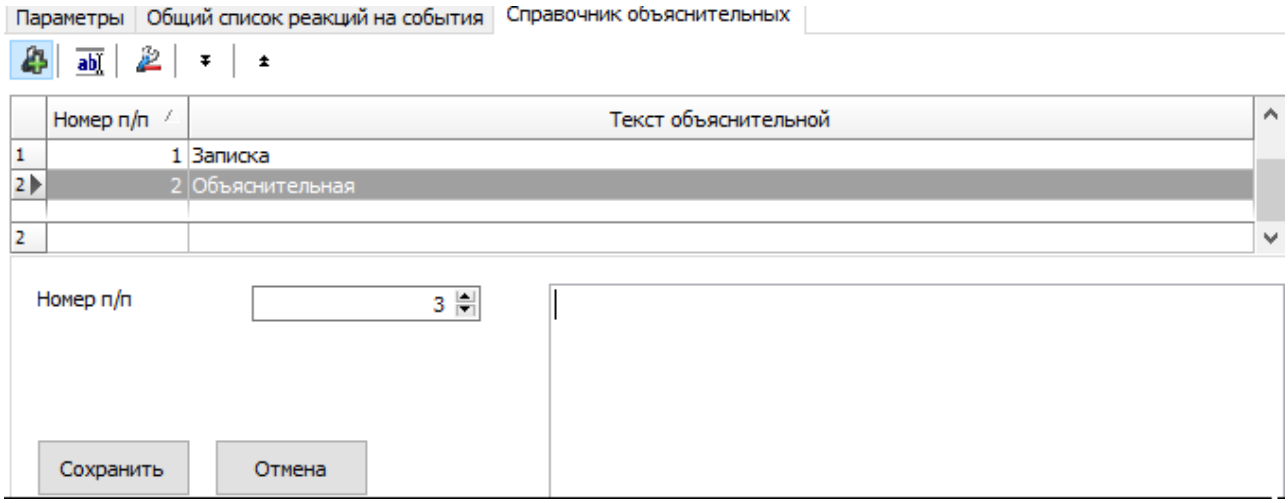
   Удалить – для удаления элемента, выбранного в рабочей области раздела.

   Переместить – для изменения номера п/п элемента, выбранного в рабочей области раздела.
3. Рабочая область подвкладки ***Справочник объяснительных*** содержит список созданных документов.

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 Подвкладка «События»

На вкладке **События** отображается список событий мониторинга, регистрируемых системой для устройства или его ресурса, выделенного в рабочей области раздела.

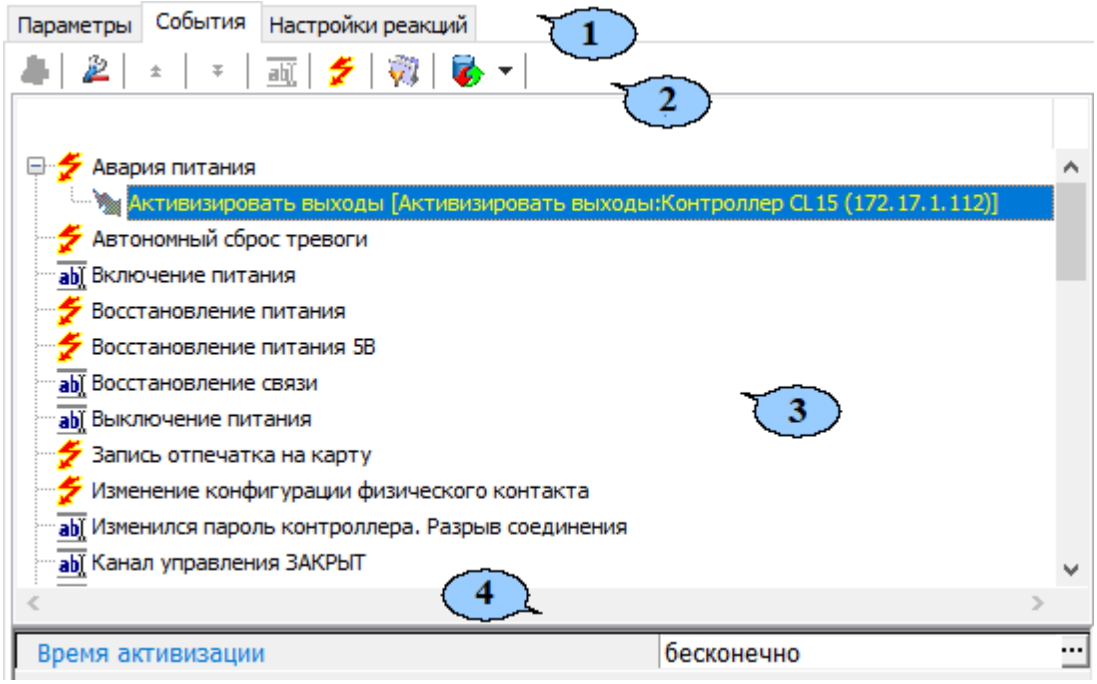
В разделе реализована возможность настроить реакцию системы на любое из этих событий. Реакция системы это предварительно заданная оператором последовательность команд, автоматически выполняемая устройствами системы.

Внимание!

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

Например, может быть задано автоматическое включение записи на камере видеонаблюдения при предъявлении запрещенной карты доступа. Или автоматически открыт замок двери, разблокирован турникеты при переходе ПЗС в режим «*Пожар*».

Подвкладка имеет следующий вид:



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

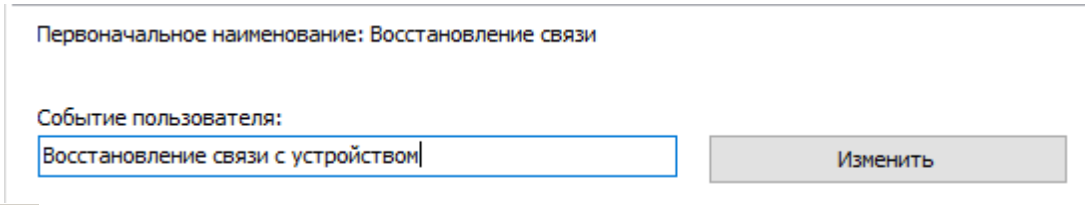
   Добавить реакцию на событие (**Alt+N**) – кнопка позволяет открыть окно **Выбор реакции на событие** для выбранного в рабочей области панели события.

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

   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:

   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. Рабочая область вкладки

– регистрируемое устройством или ресурсом событие.

– событие регистрируемое устройством или ресурсом системы;

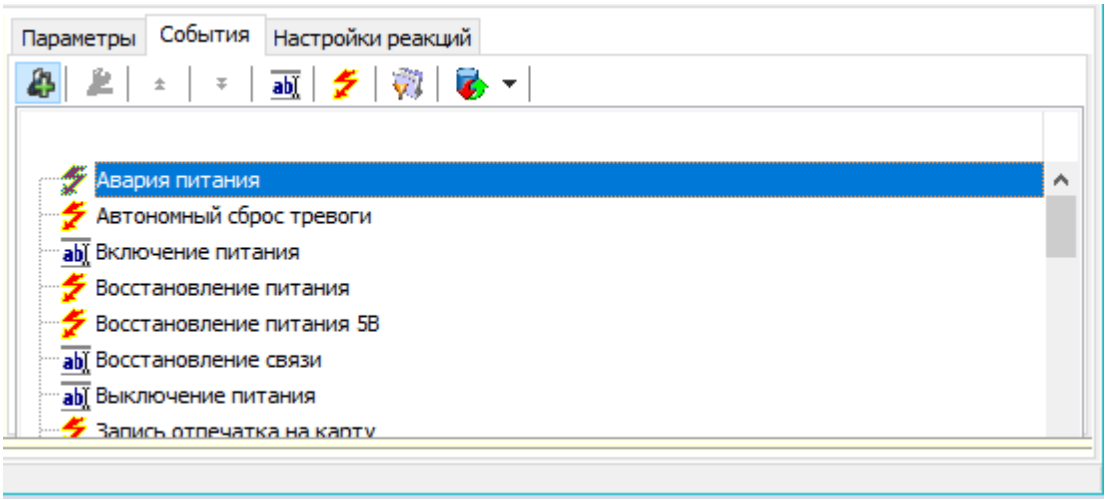
– установленная на событие реакция со стороны системы. Для некоторых реакций доступна панель для задания дополнительных параметров.

4. Панель для настройки дополнительных параметров команд.

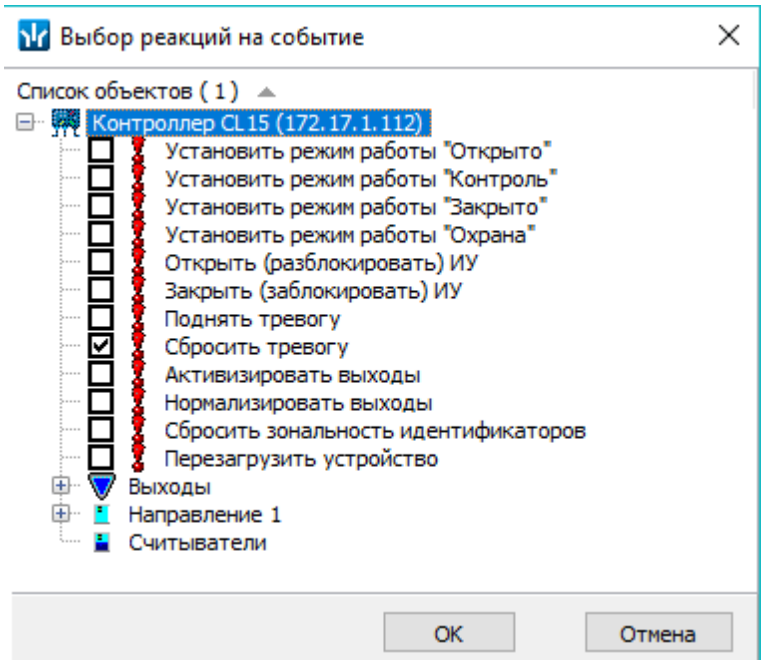
Задание реакции на событие

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

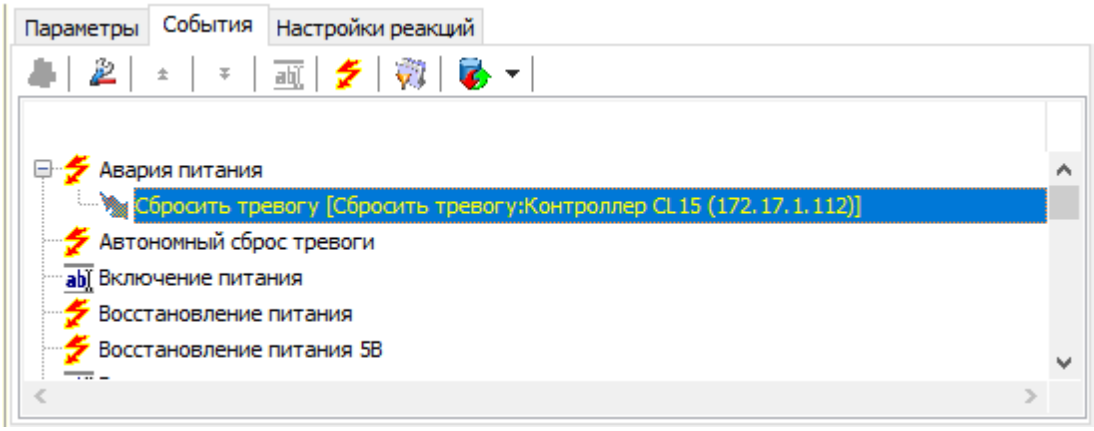
1. Выделите устройство или ресурс, на событие которого необходимо задать реакцию системы в рабочей области раздела **Список объектов**.
2. На панели настройки перейдите на вкладку **События**:



3. Выделите в рабочей области вкладки событие мониторинга, 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:

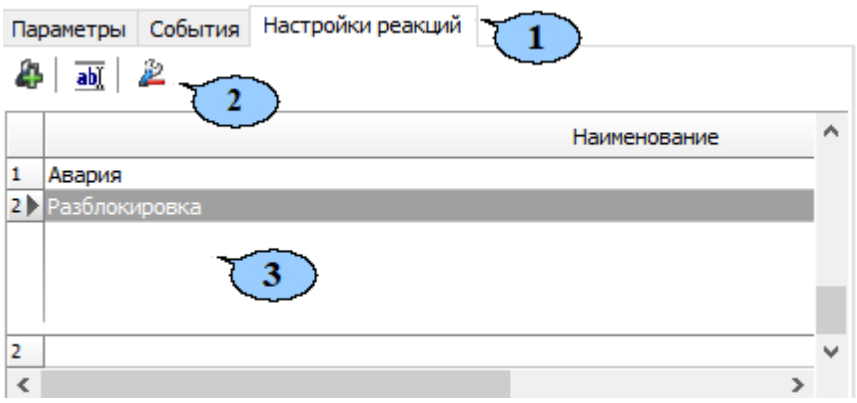


6. Установите последовательность выполнения команд, используя кнопки **Переместить вверх/вниз** ±/ ∓ в инструментах панели.
7. При необходимости установите длительность выполнения команды на панели для ввода дополнительных параметров.
8. Для удаления выделенной в рабочей области реакции на событие нажмите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

3.2.11 Подвкладка "Настройка реакций"

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

Рабочее окно подвкладки имеет следующий вид:

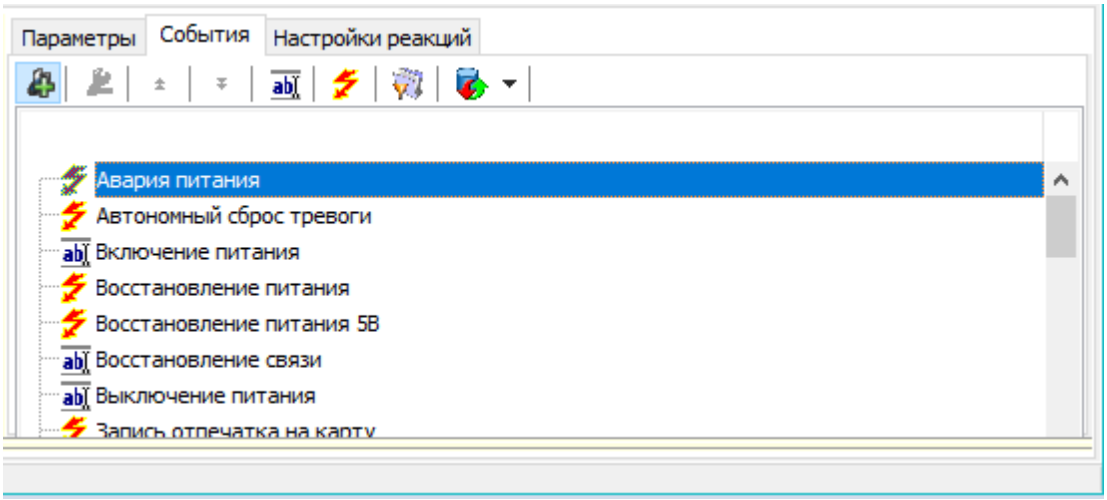


1. Выбор подвкладки панели настройки:
   - **Параметры**;
   - **Справочник объяснительных;**
   - **События;**
   - **Настройка реакции;**
   - **Камера СКУД.**
2. Панель инструментов содержит следующие кнопки:
   Добавить – для создания реакции.
   Изменить название – для изменения названия элемента,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

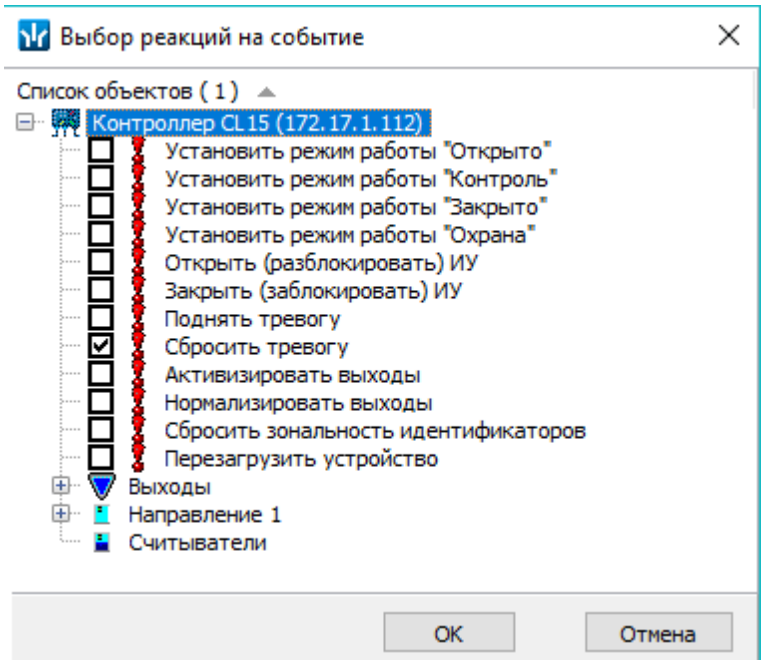
Настройка реакций

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

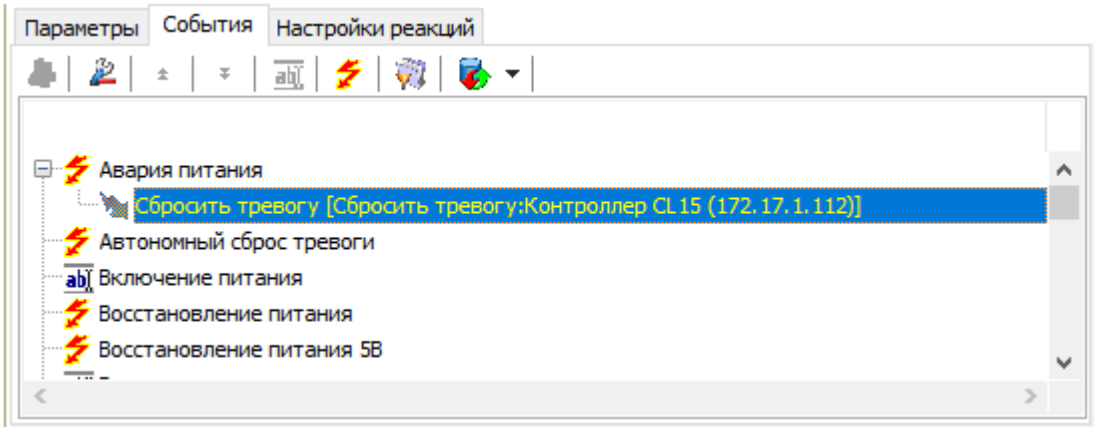
1. Выделите устройство или ресурс, на событие которого необходимо задать реакцию системы в рабочей области раздела **Список объектов**.
2. На панели настройки перейдите на вкладку **События**:



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



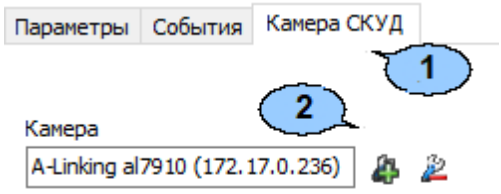
4. В открывшемся окне отметьте в раскрывающемся многоуровневом списке устройств системы флажками нужные команды. Можно задать одновременно несколько команд, как для одного, так и у нескольких устройств и ресурсов. Нажмите кнопку **ОК**.
5. Окно **Выбор реакций на событие** будет закрыто. Отмеченные команды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

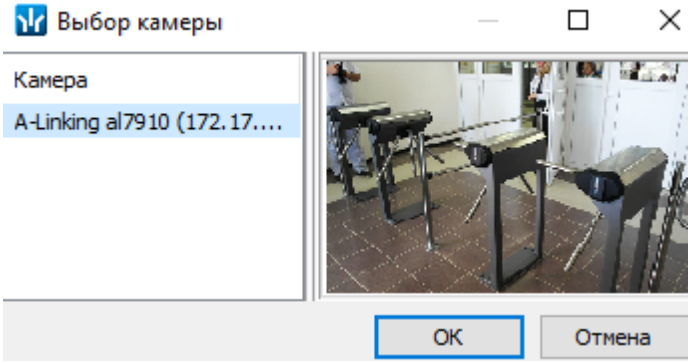
3.2.12 Подвкладка «Камера СКУД»

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



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

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



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

Примечание:

Для отключения камеры от всех считывателей выберете ее в рабочей области **Список объектов**, 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 **Список объектов** раздела:

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

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

- 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 вкладка **Список карт аварийного доступа** (см. *Руководство по эксплуатации* ***PERCo-CL201***).

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

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.

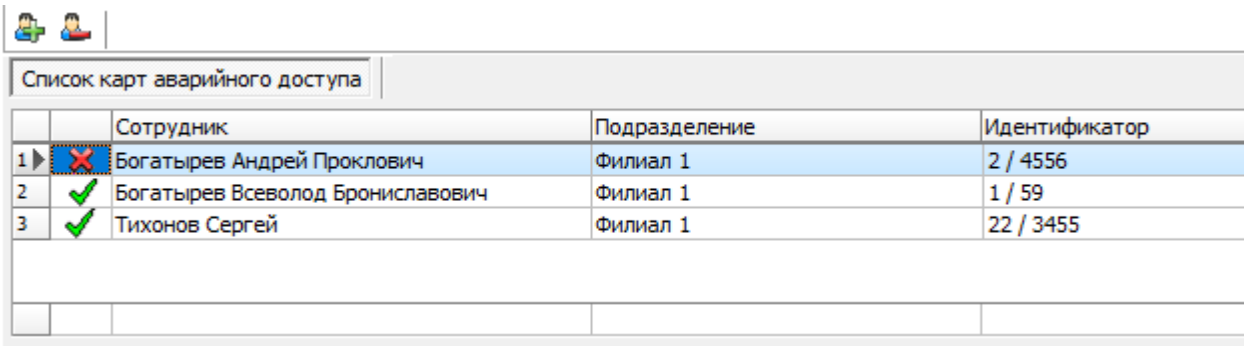
Примечание:

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:

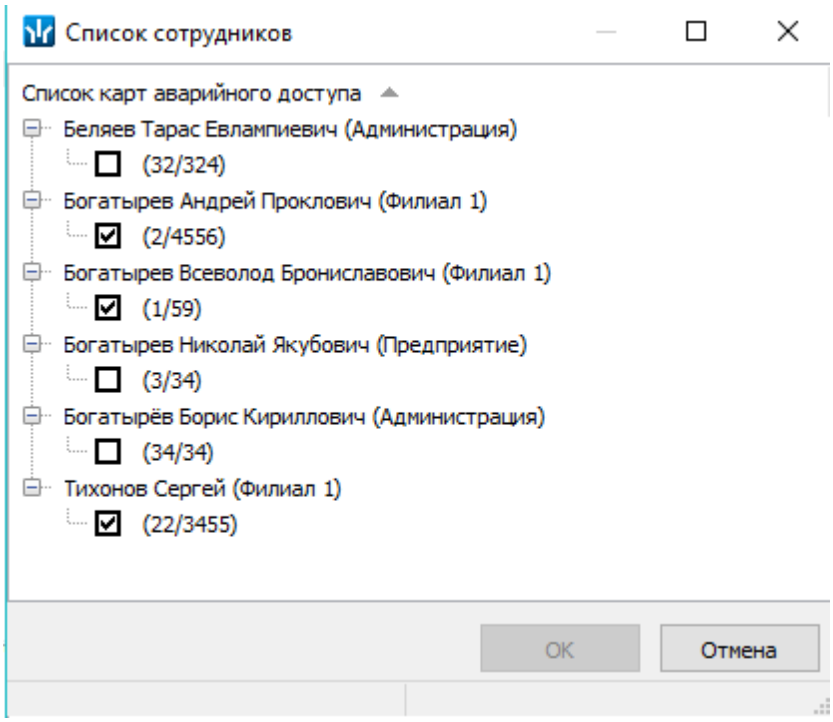
1. В рабочей области раздела **Список объектов** выделите нужный ресурс контроллера **Контроллер замка,** соответствующий контроллеру второго уровня. Откроется панель ввода дополнительных данных.
2. Если панель не открылась, нажмите правую кнопку мыши и в открывшемся контекстном меню выберите пункт **Показать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



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

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

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



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

Список карт для постановки шлейфов на охрану

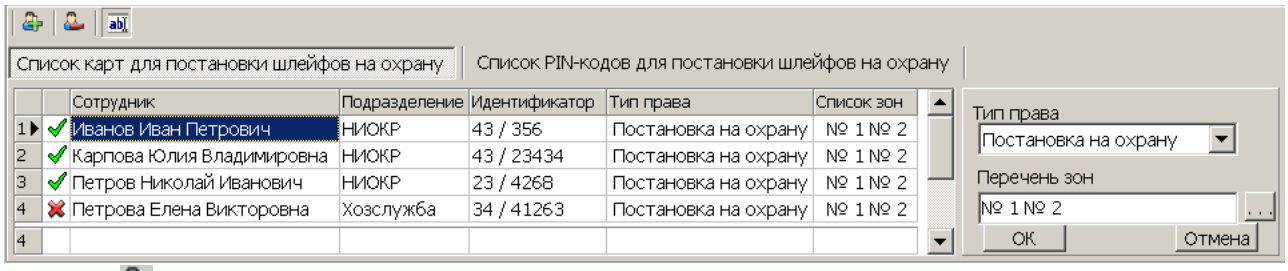
Создание списка карт для постановки и снятия с охраны пожарных и охранных зон сигнализации доступно только для контроллеров ключей постановки и снятия с охраны пожарных и охранных зон сигнализации ППКОП ***PERCo-PU01*** (см. *Руководство по эксплуатации* на ППКОП). Список карт создается независимо для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

Примечание:

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

Для внесения карты сотрудника в список:

1. В рабочей области раздела **Список объектов** 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**:

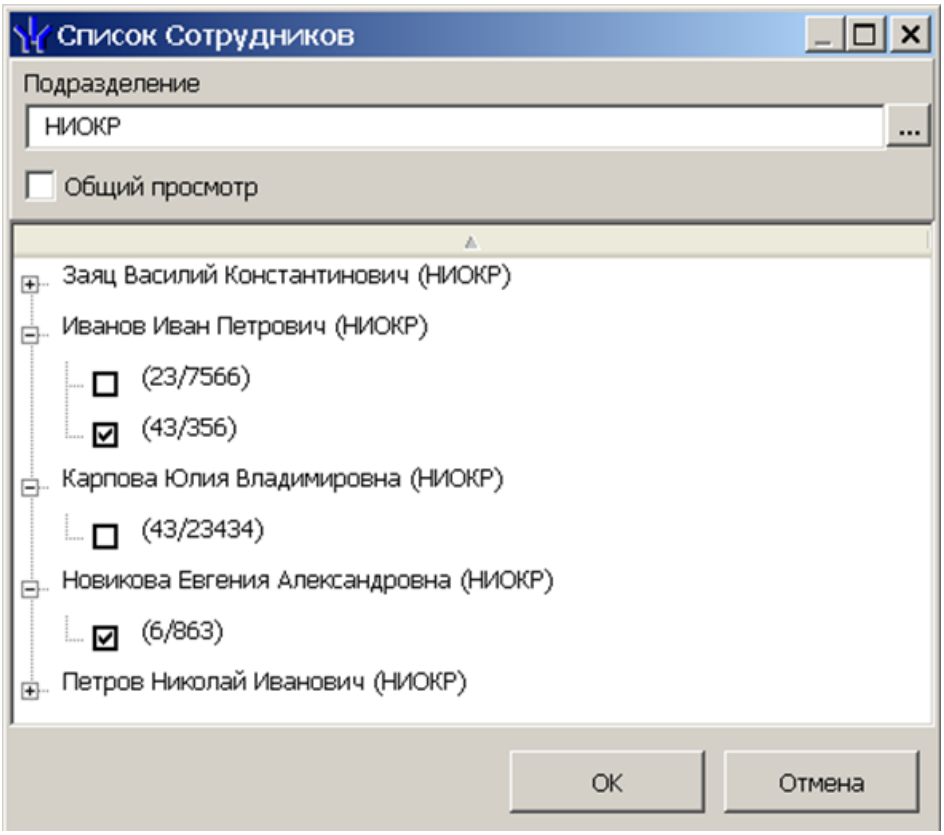


Добавить в список (**Shift+Alt+N**) – кнопка позволяет добавить карту в список карт имеющих право постановки шлейфов, включенных в ОЗ, перечисленные в списке **Перечень зон** на охрану.

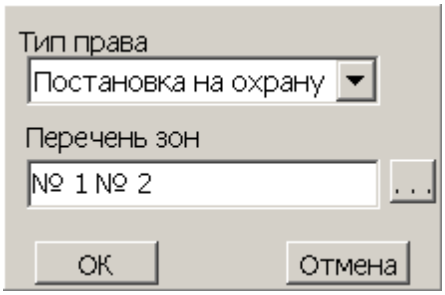
Удалить из списка (**Shift+Alt+D**) – кнопка позволяет удалить выделенную в рабочей области вкладки карту сотрудника (охранника) из списка карт имеющих право постановки на охрану.

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

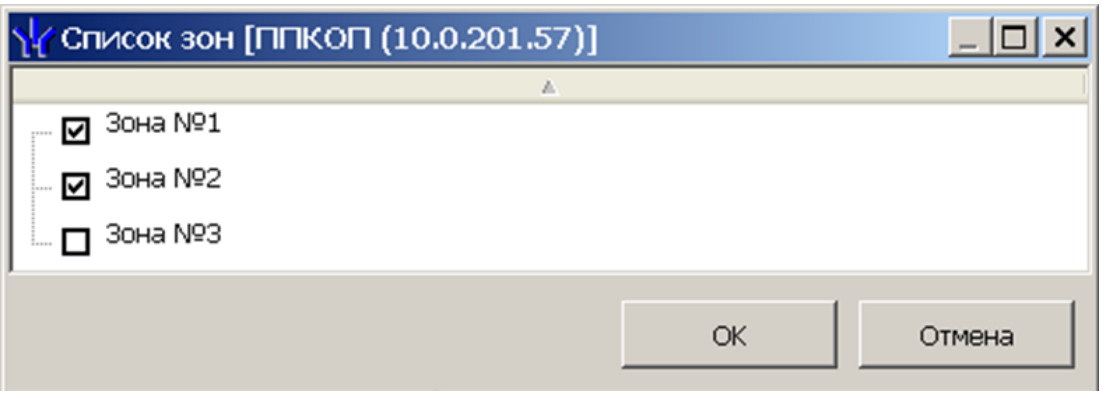
2. Для добавления карт нажмите кнопку **Добавить в список** на открывшейся панели. Откроется окно **Список сотрудников**:



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 установите флажок **Общий просмотр**). Отмеченные сотрудники будут добавлены в рабочую область панели, откроется панель задания прав (если необходимо редактировать права, нажмите кнопку **Изменить** для открытия панели):



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



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

Список PIN-кодов для постановки шлейфов на охрану

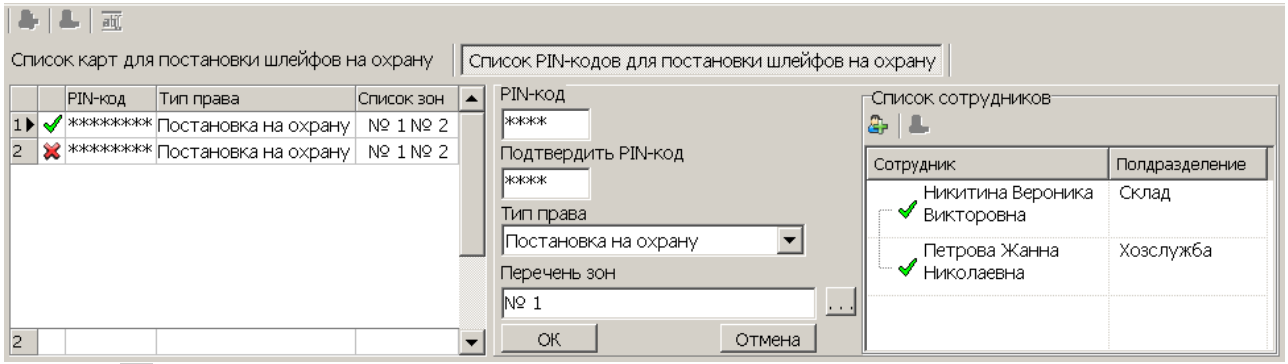
Создание списка PIN-кодов для постановки и снятия с охраны пожарных и охранных зон сигнализации доступно только для контроллеров ППКОП ***PERCo-PU01***. Ввод PIN-кода осуществляется при помощи БУИ ***PERCo-AU02 1-01***, подключенного к контроллеру. Список PIN-кодов создается независимо для каждого контроллера.

Примечание:

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

Для добавления в список нового PIN-кода:

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

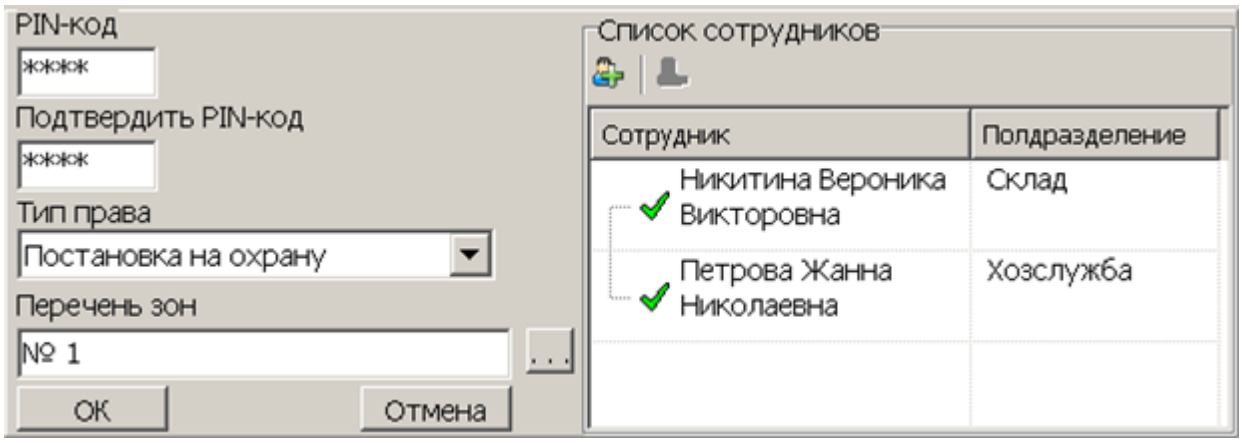


Добавить в список (**Shift+Alt+N**) – кнопка позволяет добавить новый PIN-код.

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

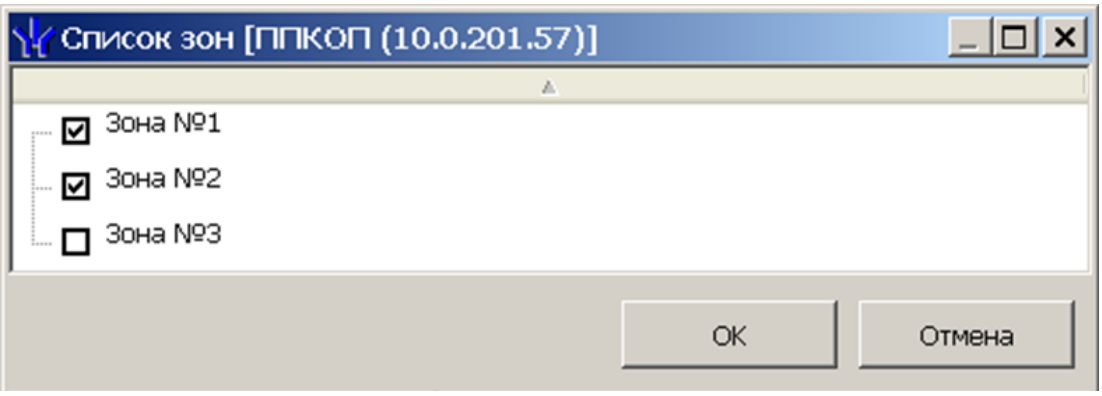
Изменить – кнопка позволяет изменить права PIN-кода, выделенного в рабочей области вкладки.

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

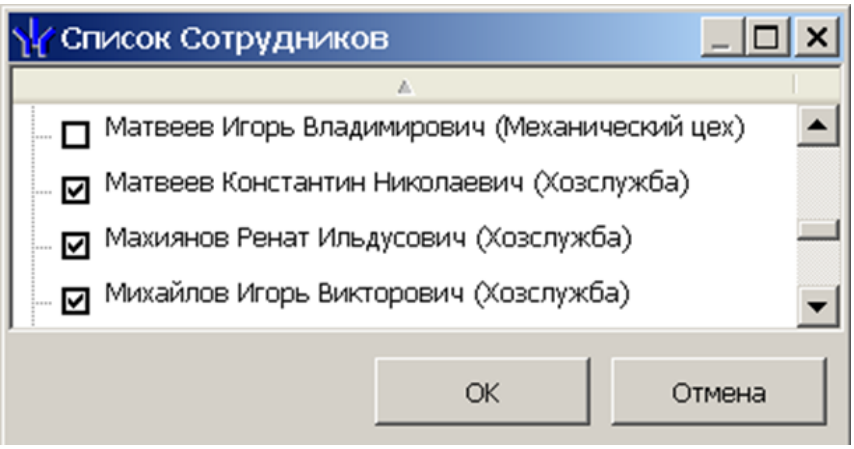


3. В поля **PIN-код** и **Подтвердить PIN-код** введите комбинацию из 4–8 цифр от 1 до 8, которая будет являться PIN-кодом.

4. Для установки прав PIN-кода выберите в раскрывающемся списке **Тип права**:
   - **Постановка на охрану;**
   - **Снятие с охраны;**
   - **Постановка и снятие с охраны.**
5. Для выбора зон сигнализации, управляемых с использованием PIN-кода, нажмите кнопку ··· справа от строки **Перечень зон.** Откроется окно **Список зон ППКОП...**:



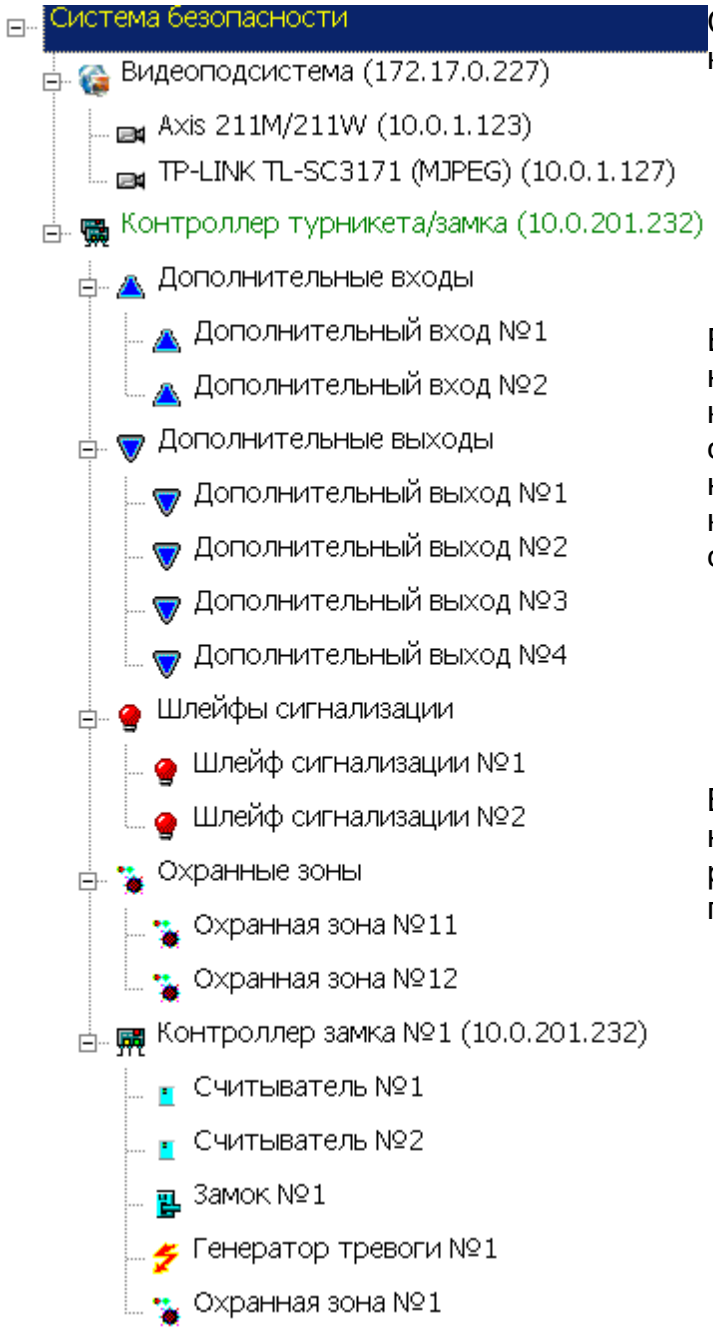
6. В открывшемся окне отметьте флажками зоны, управление которыми будет доступно с использованием PIN-кода. Нажмите кнопку **ОК**.
7. Нажмите кнопку **Добавить в список** в области **Список сотрудников**. Откроется окно **Список сотрудников**:



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

3.2.14 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**;
- **Шлейфы сигнализации**;
- **Зоны** (охранные, пожарные);
- **Контроллер ИУ** (замка, турникета);

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**);
- **Генератор тревоги**;
- **Зона** (**Охранная зона**, **Пожарная зона**).

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

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

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

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

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

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

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

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

Варианты конфигурации ЭП:

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

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

Ресурсы контроллеров и ЭП PERCo серии x.2

Модель	Доп. вход	Доп. выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считы-ватель	ИУ	Ген. тревоги	ОЗ
Контроллеры доступа									

Модель	Доп. вход	Доп. выход	ШС	ОЗ	CL201	Контроллер ИУ			
						Считы-ватель	ИУ	Ген. тревоги	ОЗ
CL201	0	0	0	0	-	1	L	1	1
CT/L04.2 (1)	4	4	0	0	до 8	2	T	1	0
CT/L04.2 (2)	2	3	0	0	до 8	3	T+L	2	1
CT/L04.2 (3)	0	2	0	0	до 8	4	T+L+L	3	2
CT/L04.2 (4)	2	3	0	0	до 8	4	T+2L	2	1
CT/L04.2 (5)	4	4	0	0	до 8	2	T(KR05.2)	1	0
CT/L04.2 (6)	5	4	0	0	до 8	2	G	1	0
CT/L04.2 (7)	3	3	0	0	до 8	3	G+L	2	1
CT/L04.2 (8)	1	2	0	0	до 8	4	G+L+L	3	2
CT/L04.2 (9)	3	3	0	0	до 8	4	G+2L	2	1
CT/L04.2 (10)	5	8	2	2	до 8	1	L	1	1
CT/L04.2 (11)	6	8	1	1	до 8	1	L	1	1
CT/L04.2 (12)	7	8	0	0	до 8	1	L	1	1
CT/L04.2 (13)	3	7	2	2	до 8	2	L+L	2	2
CT/L04.2 (14)	4	7	1	1	до 8	2	L+L	2	2
CT/L04.2 (15)	5	7	0	0	до 8	2	L+L	2	2
CT/L04.2 (16)	2	6	1	1	до 8	3	L+L+L	3	3
CT/L04.2 (17)	3	6	0	0	до 8	3	L+L+L	3	3
CT/L04.2 (18)	0	4	0	0	до 8	4	L+L+L+L	4	4
CT/L04.2 (19)	5	8	2	2	до 8	2	2L	1	1
CT/L04.2 (20)	6	8	1	1	до 8	2	2L	1	1
CT/L04.2 (21)	7	8	0	0	до 8	2	2L	1	1
CT/L04.2 (22)	4	7	1	1	до 8	3	2L+L	2	2
CT/L04.2 (23)	5	7	0	0	до 8	3	2L+L	2	2
CT/L04.2 (24)	3	6	0	0	до 8	4	2L+L+L	3	3
CT/L04.2 (25)	4	7	1	1	до 8	4	2L+2L	2	2
CT/L04.2 (26)	5	7	0	0	до 8	4	2L+2L	2	2
CL05.2	1/1		0	0	-	1	L	1	1
Контроллер регистрации									
CR01.2	-	-	-	-	-	2	-	-	-
Электронные проходные									
CT03 (1)	4	4	0	0	до 8	2	IP-Stile	1	0
CT03 (2)	2	3	0	0	до 8	2	IP-Stile +IC	1	0
CT03 (3)	4	3	0	0	до 8	2	IP-Stile +AP	1	0
CT03 (4)	2	2	0	0	до 8	2	IP-Stile +IC+AP	1	0

Принятые в таблице сокращения:

L – односторонний замок;
2L – двусторонний замок;
T – турникет;
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 возможно подключить до восьми контроллеров замка ***PERCo-CL201***):

1. Контроллер для управления турникетом.
2. Контроллер для управления турникетом и одним односторонним замком.
3. Контроллер для управления турникетом и двумя односторонними замками.

4. Контроллер для управления турникетом и одним двусторонним замком.
5. Контроллер для управления 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 возможно подключить до восьми контроллеров замка ***PERCo-CL201***):

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

Ресурсы контроллеров и ЭП PERCo 1.X

Ресурсы контроллеров и ЭП PERCo 1.X

Модель	Доп. вход	Доп. выход	ИУ	Направления прохода	Считыватель
Контроллеры доступа					
CL15	3	2	1	1	2
CTL14	13	13	до 4	до 2	до 16
Контроллер регистрации					
CR11	-	-	-	2	2
Электронные проходные					
CT13	13	13	до 4	до 2	до 16

Контроллер доступа

Доступны следующие параметры:

Параметры | События

MAC-адрес	00:25:0B: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	☐
Коррекция времени относительно времени сервера системы	0 час.

- **Текущее наименование.** Поле ввода позволяет ввести описательное название контроллера.
- **Разрешить Web-интерфейс**. После установки параметра появляется возможность подключения к web-интерфейсу контроллера. По умолчанию доступ к web-интерфейсу запрещен. Доступ к web-интерфейсу будет возможен после остановки сервера системы или исключения контроллера из конфигурации системы в ПО.
- **Коррекция времени относительно сервера**. Параметр позволяет согласовать работу контроллера и сервера системы, если они находятся в разных часовых поясах.

Контроллер регистрации (LICON)

Доступны следующие параметры:

Параметры | События

MAC-адрес	00:25:0B: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	☐
Коррекция времени относительно времени сервера системы	0 час.
Прямое направление прохода	☑
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 №…».*

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	☐
Режим активизации кнопки "КЛЮЧ"	Одно длинное нажатие

- **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.**

Считыватель

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

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

- **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 (алкометр) или другое оборудование.
  - **Нет.** Подтверждение от верифицирующего устройства не требуется.

Примечание:

Если для параметра **Способ верификации** установлено значение отличное от **Нет**, то в случая 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 (алкометра) или другого оборудования. Имеется возможность настроить запуск процедуры верификации при предъявлении карт доступа независимо для сотрудников и посетителей.
- **При доступности Софт, иначе ПДУ.**
- **ПДУ или Софт.**
- **Сначала ПДУ, затем Софт.**
- **Сначала ВВУ, затем ПДУ.**
- **Сначала ВВУ, затем софт.**
- **При доступности софт, иначе ВВУ.**

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

Внимание!

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

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

- **Нет** – Контроллер не учитывает зональность идентификатора карты для разрешения доступа.
- **Мягкая.** Контроллер разрешит доступ по карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение зональности»,* после совершения прохода регистрируется событие «*Проход по карте с несоответствием текущему местоположению»*.
- **Жесткая.** Контроллер запретит доступ по карте, при этом передается событие мониторинга *«Предъявление карты с нарушением зональности»* и регистрируется событие *«Запрет прохода по причине нарушения зональности».* Если для считывателя установлен параметр **Подтверждение от ДУ** (или верификация от ПО), то будет запущена процедура верификации.

- **Контроль времени для идентификаторов СОТРУДНИКОВ/ ПОСЕТИТЕЛЕЙ.** Параметр позволяет для выбранных РКД определить реакцию контроллера на предъявление карты доступа сотрудника/ посетителя к считывателю в случае нарушения установленного критерия доступа по времени. Для каждого из указанных РКД контроллера можно выбрать один из видов контроля:
  - **Нет.** Контроллер не отслеживает временные критерии прав доступа карты.
  - **Мягкий.** Контроллер разрешит доступ по предъявленной карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение времени»*, после совершения прохода регистрируется событие «*Проход по карте с несоответствием временным критериям доступа»*.
  - **Жесткий.** Контроллер запретит доступ по карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение времени»* и регистрируется событие «*Запрет прохода, несоответствие временным критериям доступа»*. Если для считывателя установлен параметр **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 изымется.
  - **После любого прохода**. Идентификатор изымется 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.

ИУ (Замок/ Турникет)

Доступны следующие параметры:

Параметры | События

Адрес	1
Текущее наименование	Замок
Первоначальное наименование	Замок
Прямое направление прохода	☑
Нормальное (т.е заблокированное) состояние контакта (вход ИУ)	Нормально замкнут
Нормальное состояние "Закрыто" выхода ИУ	Не запитан
Нормализация выхода ИУ	После "Открытия"
Режим работы выхода управления ИУ	Потенциальный
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа идентификатора)	4 сек.
Регистрация прохода по предъявлению идентификатора	☐
Внутренняя защита от передачи идентификаторов (Local Antipass)	☐
Дополнительные выходы, реагирующие через группу ресурсов	

- **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 перемычки *«номер считывателя» (XP2)* на плате считывателя.
  - Если параметр отключен, то тот считыватель, который в соответствии с его перемычкой должен иметь номер 1, в контроллере будет опознан как считыватель номер 2, и соответственно наоборот, считыватель номер 2 в контроллере будет опознан как считыватель номер 1.
- **Нормальное (т.е. заблокированное) состояние контакта (вход ИУ)** (*Нормально разомкнут* / *Нормально замкнут*). Состояние датчика двери / выхода PASS турникета при заблокированном состоянии данного ИУ.
- **Нормальное состояние «Закрыто» выхода ИУ** (*Не запитан*/ *Запитан*) (Не доступен в конфигурации *«Контроллер АТП»*). Параметр указывает, активизирован ли выход управления ИУ (подано управляющее напряжение на реле или транзистор) при заблокированном ИУ.
- **Нормализация выхода ИУ** (*После «Открытия»*/ *После «Закрытия»*). Параметр определяет, в какой момент нормализуется состояние выхода управления ИУ.
- **Режим работы выхода управления ИУ** (доступен только в конфигурации *«Контроллер управления дверьми»*). Описывает логику управления подключенным ИУ.
  - **Потенциальный.**
  - **Импульсный** – режим управления применяется только для замков, поддерживающих этот режим. Рекомендуется использовать для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки «CISA»).
- **Время управляющего импульса.** Параметр доступен при выборе импульсного режима работы выхода ИУ и определяет длительность импульса управления ИУ.

- **Предельное время разблокировки**. Параметр позволяет указать время, по истечении которого контроллер сформирует сообщение *«ИУ не закрыто после прохода по идентификатору»* по причине того, что ИУ не заблокировано.
- **Время удержания в разблокированном состоянии** (**время анализа идентификатора**). Время, на которое открывается ИУ.
- **Регистрация прохода по предъявлению идентификатора** (не доступен в конфигурации *«Контроллер АТП»*). При установке параметра контроллер будет считать проход совершившимся сразу после предъявления карты доступа, независимо от того, будет ли реально совершен проход через ИУ или нет.

Внимание!

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

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

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

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

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

Настройка параметров ресурсов
Параметры ресурсов
Ресурсы контроллеров и ЭП PERCo серии x.1
Ресурсы контроллеров и ЭП PERCo серии x.2
Параметры контроллера доступа
Параметры контроллера регистрации (LICON)
Параметры ППКОП (КБО)
Параметры считывателя
Параметры генератора тревоги
Параметры ШС
Параметры зон сигнализации
Параметры дополнительных входов
Параметры дополнительных выходов
Интеграция с контроллерами «Suprema»
Параметры видеоподсистемы
Параметры камер

Генератор тревоги

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

Параметры | События

Текущее наименование	Генератор тревоги
Первоначальное наименование	Генератор тревоги
Генерация тревоги при предъявлении идентификатора	
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
Генерация тревоги при несанкционированной разблокировке ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Закрыто"	Нет
Генерация тревоги по недопустимо долгому открытию ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
Генерация тревоги по датчику вскрытия корпуса	Нет
Дополнительные входы, активизирующие генерацию тревоги	
Тип тревоги	Тихая
Дополнительный вход №1	☐
Дополнительный вход №2	☐

- **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.

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).

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
⊟**Охранный**	
Контроль вскрытия корпуса извещетелей	☐
Поддержка перезапроса	☐
Длительность нарушения	70 мс.
Задержка взятия на охрану	0 мс.
Задержка восстановления нарушенного шлейф	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.

- В противном случае в режиме *«СНЯТ»* продолжается отслеживание состояния ШС.

Если ШС перейдет в состояние *«нарушение»*, то регистрируется событие *«Неисправность снятого ОШС»*. Состояние выходов ОПС не изменяется.

Если после этого ШС возвращается в состояние *«норма»* и продержится этом состоянии время, указанное в этом параметре, то регистрируется событие *«Нормализация снятого ОШС»*. Состояние выходов ОПС не изменяется.

Для настройки ресурса 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	☐
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).

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.

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

Для настройки ресурса доступны следующие параметры:

Адрес	1
Текущее наименование	Зона №1
Первоначальное наименование	Зона №1
⊟Тип	Охранная
⊟Охранная	
Повторное включение сирены	☐
Режим работы при невзятии	Тревога
⊟Не менять при тревоге по Охранным шлейфам сигнализации	
Выходы, работающие по программе "Сирена" или "Лампа"	☐
⊟Шлейфы, активизирующие зону	
Шлейф сигнализации №1	☑
Шлейф сигнализации №2	☑
Шлейф сигнализации №8	☐

- **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 «Школа»*** 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.

Для настройки ресурса 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	☑
Шлейф сигнализации №4	☑
Шлейф сигнализации №7	☐

- **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.

Дополнительный вход

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

Для настройки ресурса доступны следующие параметры:

Тип. Раскрывающийся список позволяет выбрать один из следующих типов:

- **Нет.** К данному входу не подключено никакое внешнее оборудование.
- **Обычный.** К данному входу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
- **Специальный**. Предназначен для автономного сброса тревоги, выключения сирены.

- **FireAlarm**. Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ *Fire Alarm*. Тип входа **FireAlarm** не может быть изменён для входов контроллеров и ЭП ***PERCo*** серии x.2, для которых он установлен по умолчанию. В этом случае дополнительный вход обозначается как **Вход FireAlarm.**
- **Подтверждение от ВВУ.** Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае разрешения прохода.
- **Запрет от ВВУ.** Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае запрета прохода.

В зависимости от выбранного типа остальные параметры выхода могут различаться.

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

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

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

Для настройки ресурса доступны следующие параметры:

Параметры | События

Адрес	1
Текущее наименование	Дополнительный вход №1
Первоначальное наименование	Дополнительный вход №1
Нормальное состояние контакта	Разомкнут
⊟Тип	Обычный
⊟**Обычный**	
⊟**Дополнительные входы, маскируемые при активизации**	
⊟Критерий маскирования	На указанное время
⊟**На указанное время**	
Время	0 мс.
Дополнительный вход №2	☐
⊟**Дополнительные выходы, активизируемые при активизации**	
⊟Критерий активизации	На указанное время
⊟**На указанное время**	
Время	0 мс.
Дополнительный выход №1	☐
Дополнительный выход №2	☐
Дополнительный выход №3	☐
Дополнительный выход №4	☐
⊟**Дополнительные выходы, нормализируемые при активизации**	
⊟Критерий нормализации	На указанное время
⊟**На указанное время**	
Время	0 мс.
Дополнительный выход №1	☐
Дополнительный выход №2	☐
Дополнительный выход №3	☐
Дополнительный выход №4	☐

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

- **Дополнительные выходы, нормализируемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть нормализированы. Укажите временной критерий нормализации.
- Временной **Критерий маскирования/активизации/нормализации**:
  - **На указанное время.** Выбранные дополнительные входы будут маскированы на указанное время.
  - **На время срабатывания.** Выбранные дополнительные входы будут маскированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
  - **На время срабатывания и после срабатывания.** Выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал, плюс указанное время.

Для настройки ресурса доступны следующие параметры:

Параметры | События

Адрес	2
Текущее наименование	Дополнительный вход №2
Первоначальное наименование	Дополнительный вход №2
Нормальное состояние контакта	Разомкнут
⊟Тип	Специальный
⊟**Специальный**	
Сброс тревоги (Генератор тревоги)	☐
Сброс сирены (Выход "С" ОПС)	☐

- **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*.

Доступны следующие параметры:

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

- **Нормальное состояние контакта** (*Разомкнут/ Замкнут*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.
- **Контроллер.** Параметр позволяет определить устройство, от которого будет ожидаться сигнал 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 нормализированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть нормализированы. Укажите временной критерий нормализации.
- Временной **Критерий маскирования/активизации/нормализации**:
  - **На указанное время.** Выбранные дополнительные входы будут маскированы на указанное время.
  - **На время срабатывания.** Выбранные дополнительные входы будут маскированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
  - **На время срабатывания и после срабатывания.** Выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал, плюс указанное время.

Доступны следующие параметры:

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

- **Нормальное состояние контакта** (*Разомкнут/ Замкнут*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.
- **Контроллер.** Параметр позволяет определить устройство, от которого будет ожидаться сигнал запрета прохода. В этом качестве могут выступать 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, нормализируемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть нормализированы. Укажите временной критерий нормализации.
- Временной **Критерий маскирования/активизации/нормализации**:
  - **На указанное время.** Выбранные дополнительные входы будут маскированы на указанное время.
  - **На время срабатывания.** Выбранные дополнительные входы будут маскированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
  - **На время срабатывания и после срабатывания.** Выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал, плюс указанное время.

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 оределяется 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.

В окне доступны следующие параметры:

Параметры | События

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**.

Для настройки ресурса доступны следующие параметры:

Параметры | События

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 нормализированного на противоположное.

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 нормализированного 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
⊟**ОПС**	
Нормальное состояние	Не запитан
Задержка перед запуском	0 мс.
Время активизации	1 сек.
Программа управления	Не управлять
⊟**Зоны, активизирующие выход**	
Охранная зона №3	☐
Охранная зона №4	☐
Охранная зона №5	☐
Охранная зона №6	☐
Охранная зона №7	☐
Охранная зона №8	☐
Охранная зона №9	☐
Охранная зона №10	☐

- **Нормализованное состояние** (*Не запитан/ Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода. Для выходов №1 и № 2 нормализованное состояние: **Не запитан**.
- **Задержка перед запуском.** Промежуток времени между изменением режима ОЗ и запуском программы управления выходом.
- **Время активизации.** Время, на которое выход, при наличии активизирующего управляющего воздействия, меняет свое состояние из нормализированного на противоположное.

Примечание:

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

- **Программа управления**. 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»).

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

- **Включить при тревоге.** В случае перехода хотя бы одной из ОЗ в режим *«ТРЕВОГА»* выход будет активизирован на **Время активизации**.
- **Мигать при тревоге.** В случае перехода хотя бы одной из ОЗ в режим *«ТРЕВОГА»* выход будет активизироваться с частотой 1Гц.
- **Лампа 1**. Программа управления световым оповещателем тревожной ситуации. Для смены режима требуется, чтобы все ОЗ изменили свое состояние.
- **Лампа 2.** Программа управления световым оповещателем тревожной ситуации. Для смены режима требуется, чтобы хотя бы одна ОЗ изменила свое состояние.
- **ПЦН 1.** Программа для передачи тревожных извещений на пост центрального наблюдения (ПЦН). В случае перехода всех ОЗ в режим *«ОХРАНА»* выход будет активизирован. Передача тревожных извещений на ПЦН
- **ПЦН 2.** Программа для передачи тревожных извещений на пост центрального наблюдения (ПЦН). В случае перехода всех ОЗ в режим *«ОХРАНА»* или в режим *«СНЯТА»* выход будет активизирован.
- **Сирена.** Программа управления звуковым оповещателей тревожной ситуации. В случае перехода хотя бы одной из ОЗ в режим *«ТРЕВОГА»* выход будет активизирован на **Время активизации**.
- **Вкл. перед взятием для ИУ в 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, активирующие выход** изменила свое состояние.

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

В таблице указаны следующие режимы работы выхода:

0 – выход нормализован.

N – состояние выхода не изменяется.

∞ – выход активизирован постоянно.

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

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

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

Программы управления выходами для контроллеров доступа

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

Программы управления выходами для ППКОП

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

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.

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
Параметры кнопки выхода	
Нормальное состояние	Нормально открыто
Параметры датчика прохода	
Нормальное состояние	Нормально открыто
Порядок байтов идентификатора карты	От старшего байта к младшему
Настройки Wiegand	
Режим	Вход
Коррекция времени относительно времени сервера системы	0 час.

- **IP-адрес**.
- **Маска подсети**.
- **Шлюз**.
- **Макс. кол-во сотрудников/посетителей** – определяет максимально допустимое количество сотрудников/посетителей, информация о которых может храниться в контроллере.
- **Макс. кол-во отпечатков пальцев** – определяет максимально допустимое количество отпечатков пальцев, информация о которых может храниться в контроллере.
- **Порт** – порт контроллера, который необходимо использовать для подключения.

- **Модель** – отображает официальное наименование модели устройства.
- **Серийный номер** – серийный номер устройства.
- **Уровень безопасности** – уровень безопасности при использовании верификации по отпечатку пальца:
  - Нормальный;
  - Безопасный;
  - Наиболее безопасный.

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

- **Таймаут сканирования пальца** – время, которое выделяется системой на поднесение одного пальца при вводе отпечатков. Параметр может быть задан в интервале от 3 до 20 секунд.
- **Таймаут верификации пальцем** (используется в режиме доступа **карта и палец**) – интервал времени, в течение которого ожидается поднесение пальца для сканирования отпечатков, при этом отсчёт времени интервала начинается после того, как была предъявлена считывателю карта доступа. Параметр может быть задан в интервале от 1 до 20 секунд.
- **Таймаут поиска отпечатков** – время поиска отпечатка в памяти контроллера. Если за отведенное время отпечаток не будет найден, то аутентификация будет отклонена. Параметр может быть задан в интервале от 1 до 20 секунд.
- **Чувствительность сканера** – определяет чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности – обеспечивается высокое качество и скорость сканирования, при низком заданном уровне чувствительности – уменьшается влияние факторов внешней среды (температуры и влажности воздуха, освещённости помещения, чистоты сканируемой поверхности подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию. Понижение заданного уровня чувствительности сканера осуществляется при необходимости в зависимости от условий эксплуатации. Параметр может быть задан в интервале от 1 до 7, где значение 1 – соответствует самой низкой чувствительности, а значение 7 – самой высокой.
- **Алгоритм поиска отпечатков** – позволяет выбрать алгоритм поиска отпечатков пальца. Выбор алгоритма влияет на скорость верификации по отпечатку пальца:
  - **Автоматический (рекомендован производителем);**
  - **Нормальный;**
  - **Быстрый;**

- **Очень быстрый.**

Выбор **алгоритма поиска отпечатков** определяет тот объём памяти контроллера, который будет выделяться для поиска совпадения отсканированного отпечатка с отпечатком в базе данных. Если в базе данных контроллера большое количество разных отпечатков, то для быстрого поиска совпадений потребуется больший объём памяти контроллера. Однако, выделение большего объёма памяти контроллера для поиска совпадений может замедлить остальные параллельно 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 ним.
- **Режим доступа** – определяет режим доступа при общем режиме авторизации (отображается
- только если режим авторизации выставлен как **«Общий»**):
  - **Палец** – для верификации требуется пройти процедуру сканирования отпечатка пальца;
  - **Карта** – для верификации требуется предъявить считывателю карту доступа;
  - **Карта и палец** – для верификации требуется предъявить считывателю карту доступа, после чего пройти процедуру сканирования отпечатка пальца;
  - **Карта или палец** – для верификации требуется предъявить считывателю карту доступа или пройти процедуру сканирования отпечатка пальца.

Примечание:

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

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

Примечание:

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

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

Примечание:

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

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

Примечание:

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

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

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

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

Примечание:

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

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

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
Параметры кнопки выхода	
Нормальное состояние	Нормально открыто
Параметры датчика прохода	
Нормальное состояние	Нормально открыто
Порядок байтов идентификатора карты	От старшего байта к младшему
Настройки Wiegand	
Режим	Вход
Коррекция времени относительно времени сервера системы	0 час.

- **IP-адрес**.
- **Маска подсети**.
- **Шлюз**.
- **Макс. кол-во сотрудников/посетителей** – определяет максимально допустимое количество сотрудников/посетителей, информация о которых может храниться в контроллере.
- **Макс. кол-во отпечатков пальцев** – определяет максимально допустимое количество отпечатков пальцев, информация о которых может храниться в контроллере.
- **Порт** – порт контроллера, который необходимо использовать для подключения.
- **Модель** – отображает официальное наименование модели устройства.
- **Серийный номер** – серийный номер устройства.
- **Уровень безопасности** – уровень безопасности 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, загрязнённости сканируемой поверхности пальцев и т.д. В этом случае для успешной верификации потребуется повторно пройти процедуру сканирования отпечатков.

- **Таймаут сканирования пальца** – время, которое выделяется системой на поднесение одного пальца при вводе отпечатков. Параметр может быть задан в интервале от 3 до 20 секунд.
- **Таймаут верификации пальцем** (используется в режиме доступа ***карта и палец***) – интервал времени, в течение которого ожидается поднесение пальца для сканирования отпечатков, при этом отсчёт времени интервала начинается после того, как была предъявлена считывателю карта доступа***.*** Параметр может быть задан в интервале от 1 до 20 секунд.
- **Таймаут поиска отпечатков** – время поиска отпечатка в памяти контроллера. Если за отведенное время отпечаток не будет найден, то аутентификация будет отклонена. Параметр может быть задан в интервале от 1 до 20 секунд.
- **Чувствительность сканера** – определяет чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности – обеспечивается высокое качество и скорость сканирования, при низком заданном уровне чувствительности – уменьшается влияние факторов внешней среды (температуры и влажности воздуха, освещённости помещения, чистоты сканируемой поверхности подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию. Понижение заданного уровня чувствительности сканера осуществляется при необходимости в зависимости от условий эксплуатации. Параметр может быть задан в интервале от 1 до 7, где значение "1" – соответствует самой низкой чувствительности, а значение "7" – самой высокой.
- **Алгоритм поиска отпечатков** – выбор алгоритма влияет на скорость верификации по отпечатку пальца:
  - **Автоматический (рекомендован производителем);**
  - **Нормальный;**
  - **Быстрый;**
  - **Очень быстрый.**

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

- **Режим датчика** – параметр определяет режим работы считывающего датчика, либо он работает всегда, либо включается автоматически, если обнаруживает палец;
- **Режим авторизации** – параметр определяет режим авторизации:
  - **частный режим доступа** – в этом случае параметры доступа устанавливаются для отдельного сотрудника/посетителя в рамках СКУД;
  - **общий режим доступа** – в этом случае параметры доступа устанавливаются в рамках биометрического контроллера и будут применяться для всех пользователей, взаимодействующих ним.
- **Режим доступа** – определяет режим доступа при общем режиме авторизации (отображается, только если режим авторизации выставлен как **«Общий»**):
  - **Палец** – для верификации требуется пройти процедуру сканирования отпечатка пальца;
  - **Карта** – для верификации требуется предъявить считывателю карту доступа;
  - **Карта и палец** – для верификации требуется предъявить считывателю карту доступа, после чего пройти процедуру сканирования отпечатка пальца;
  - **Карта или палец** – для верификации требуется предъявить считывателю карту доступа или пройти процедуру сканирования отпечатка пальца.

Примечание:

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

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

Примечание:

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

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

Примечание:

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

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

Примечание:

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

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

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

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

Примечание:

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

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

Для настройки доступны следующие параметры:

Параметры | События

Текущее наименование	Замок
Первоначальное наименование	Замок
Блокировать замок при закрытии двери	☐
Блокировать замок по таймауту, только если дверь закрыта	☑
Время удержания в разблокированном состоянии	5 сек.
Предельное время разблокировки	10 сек.
Генерация тревоги по взлому двери	☑
Генерация тревоги по удержанию двери	☑
Регистрация прохода по предъявлению идентификатора/пальца	☐

- **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.

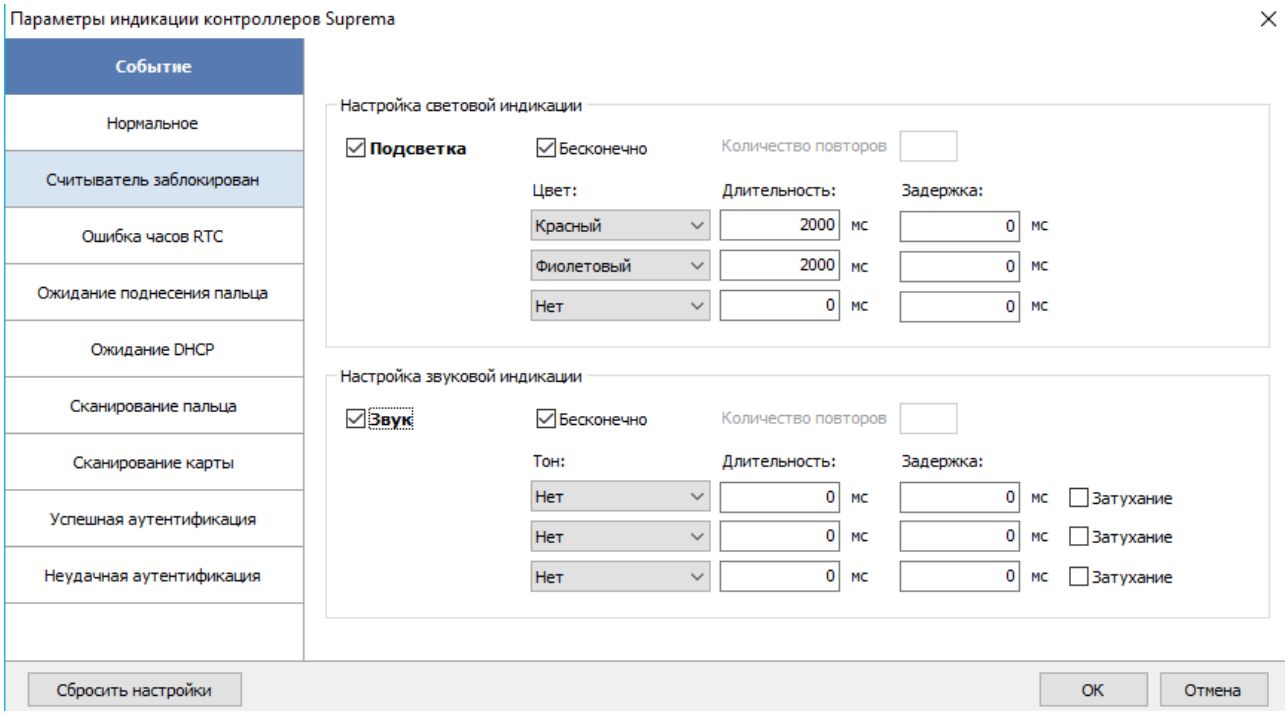
- **Время удержания в разблокированном состоянии** – устанавливает время, которое должно пройти от разблокировки замка до его блокировки после успешной аутентификации. За это время необходимо открыть дверь – иначе замок заблокируется. Параметр может быть задан в интервале от 1 до 30 секунд или от 1 до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

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:**



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

- **Нормальное** – событие возникает в случае нормальной работы контроллера (режим работы "Контроль");
- **Считыватель заблокирован** – событие возникает в случае блокировки контроллера (режим работы "Закрыто");
- **Ошибка часов RTC (Real Time Clock)** – событие возникает в случае несовпадения внутреннего времени контроллера со временем сети;

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

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

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

Примечание:

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

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

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

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

Примечание:

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

- **Тон** – параметр позволяет выбрать тон звучания;
- **Длительность** – параметр позволяет задать длительность звучания индикации тем или иным тоном;
- **Задержка** – параметр позволяет задать задержку перед началом звучания индикации тем или иным тоном от начала цикла индикации.

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

Для сохранения изменений индикации нажмите кнопку **ОК**, для выхода без сохранения нажмите кнопку **Отмена**.

Биометрические контроллеры PERCo

Биометрические контроллеры, разработанные компанией ***PERCo***, позволяют усилить контроль территории и повысить уровень безопасности за счёт 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 CT/L14, CT13;**
- **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.

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 | События | Настройки реакций

MAC-адрес	00:25:0B: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 комиссионирующих карт	1000000
Текущее наименование	Контроллер CT/L14
Внешнее подключение	☐

- **MAC-адрес.**
- **IP-адрес.**
- **Маска подсети.**
- **Шлюз.**
- **Порт конфигурации.**
- **Порт управления.**

- **Макс. кол-во карт доступа и комиссионирующих карт.**
- **Внешнее подключение.** Отображение флажка у параметра означает, что контроллер был добавлен по внешнему подключению (контроллер сам подключается к серверу системы S-20).

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 | События | Настройки реакций

MAC-адрес	00:25:0B: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 комиссионирующих карт	1000000
Текущее наименование	Контроллер CL15
Внешнее подключение	☐
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 комиссионирующих 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.

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 комиссионирующих карт	1000000
Текущее наименование	Контроллер регистрации CR11
Внешнее подключение	☐
Первоначальное наименование	Контроллер регистрации CR11
Модель	PERCo-CR11
Время анализа идентификатора	7 сек.
Внутренняя защита от передачи идентификаторов (Local Antipass)	☐
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 комиссионирующих 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 позволят выбрать критерий доступа по времени, созданный в разделе **«Временные зоны»,** для входа.
- **Временная зона выхода.** Параметр позволят выбрать критерий доступа по времени, созданный в разделе **«Временные зоны»,** для выхода
- **Часовой пояс.** Параметр предназначен для выбора часового пояса.

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	☐
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 МУ
Время идентификации постановки/снятия РКД "Охрана"	10 сек.
Внутренняя защита от передачи идентификаторов (Local Antipass)	☑
Генерация тревоги	
Генерация тревоги при предъявлении идентификатора	
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	
в РЕЖИМЕ РАБОТЫ "Контроль"	☑
в РЕЖИМЕ РАБОТЫ "Закрыто"	☑
Генерация тревоги по недопустимо долгому открытию ИУ	☑
Генерация тревоги при предъявлении "тревожного" пальца	☐

- **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 разблокируемом 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 МУ;**
  - **Блокировать МУ.**
- **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.

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.
Защита от передачи идентификаторов СОТРУДНИКОВ (Antipass)	
в РЕЖИМЕ РАБОТЫ "Открыто"	Да
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Охрана"	Жесткая
Защита от передачи идентификаторов ПОСЕТИТЕЛЕЙ (Antipass)	
в РЕЖИМЕ РАБОТЫ "Контроль"	Жесткая
Контроль времени для СОТРУДНИКОВ	
в РЕЖИМЕ РАБОТЫ "Открыто"	Нет
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Охрана"	Жесткий
Контроль времени для ПОСЕТИТЕЛЕЙ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Мягкий
Настройки верификации	
Уровни верификации	
Уровень 1	
Счетчик проходов	☐
Софт	☑
Софт, если подключен	☐
ПДУ	☑
ВВУ	☐
Уровень 2	
Уровень 3	
Уровень 4	
Настройки верификации ПДУ	
Настройки верификации ВВУ	
Настройки верификации софта	
Время ожидания подтверждения	35 сек.
Настройки верификации счетчика проходов	
Время ожидания подтверждения	1 сек.
Изымать идентификаторы ПОСЕТИТЕЛЕЙ	Нет

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

- **Время идентификации комиссионирования.** Параметр позволяет задать максимальное время, за которое определяется, имеет ли комиссионирующий 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.

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.

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
⊟Тип	Сигнал прохода
⊟**Сигнал прохода**	
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 сбороса тревоги.**
- **Нормальное состояние** (*Не запитан/ Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода.
- **Направление.** Параметр задаёт направление, к которому привязывается считыватель.
- **Антидребезг.** Значение должно быть от 0 до 950 миллисекунд с шагом 50; от 1 секунды до 4 минут; бесконечно.

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	Выход 1
Первоначальное наименование	Выход 1
⊟Тип	Выход управления ИУ
⊟**Выход управления ИУ**	
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 задаёт 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.

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.

Для настройки доступны следующие параметры видеоподсистемы:

Текущее название – поле для ввода описательное название видеоподсистемы.

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

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"	☐
Использовать как камеру СКУД	☑
Время предзаписи для камеры СКУД	3 сек.
Порт	80
Порт стоп-кадра	80
Логин пользователя	
Пароль пользователя	
Детектор движения	
Порт	80
Продолжительность записи	2 мин. 0 сек.
Аудио-режимы	
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 видеоинформации с камеры до и после регистрации события, связанного с проходом через ИУ в направлении считывателя. Значение установленное по умолчанию 3 секунды. При этом в видеоархиве будет сохранена видеоинформация за 3 секунды до регистрации события и 3 секунды после.
- **Порт, Порт стоп-кадра** – параметры, указывающие номера сетевых портов, используемых для связи с камерой.
- **Логин пользователя, Пароль пользователя** – поля для ввода имени и пароль пользователя для доступа к камере.

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

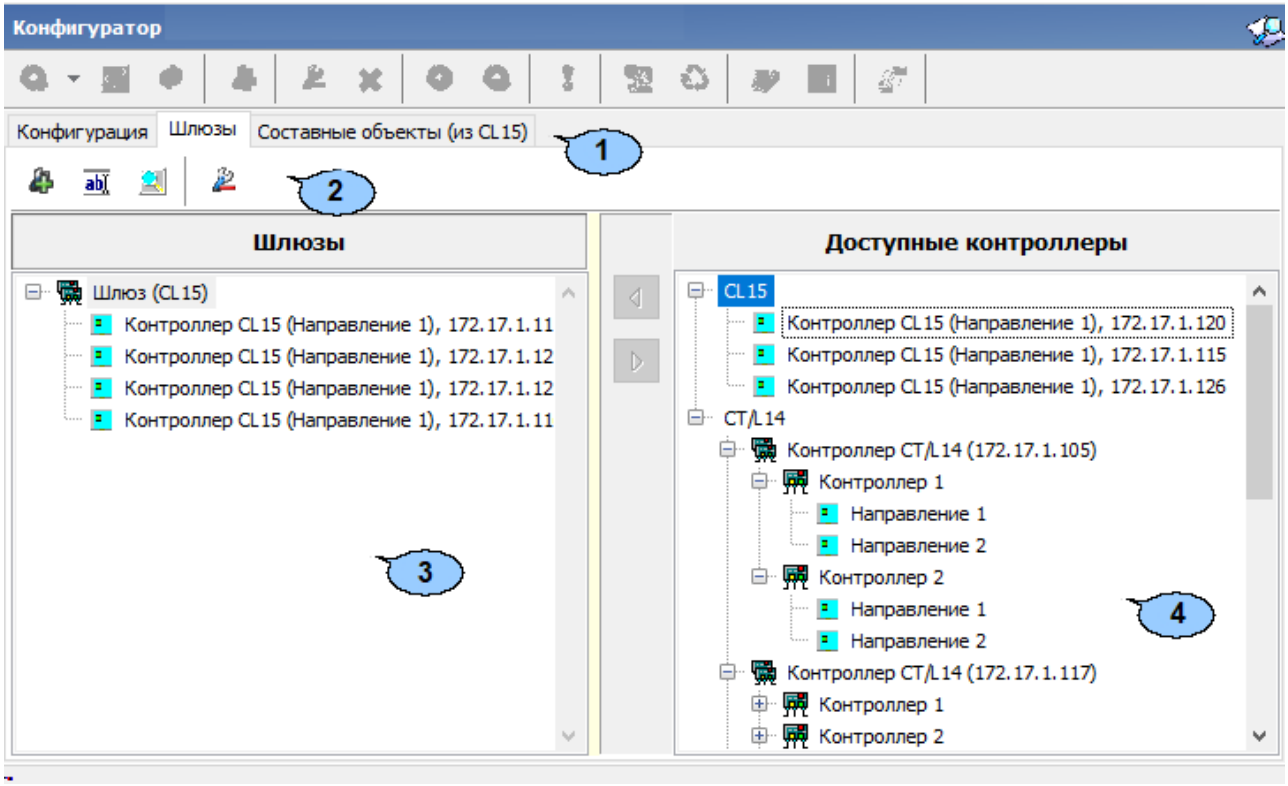
  Режим Downstream:
  - **Да** – аудио-сигнал со встроенного микрофона камеры транслируется в разделы ПО и может быть сохранен в видеоархиве. Необходимо дополнительно указать сетевой порт для передачи аудио-сигнала.
  - **Нет** – передача аудио-сигнала с камеры отключена.
- **Видео-режим** – параметр позволяет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



1. Выбор вкладки раздела:
   - **Конфигурация;**
   - **Шлюзы;**
   - **Составные объекы**.
2. Панель инструментов содержит следующие кнопки:

   Добавить – для создания нового шлюза.

   Изменить название – для изменения названия выбранного в рабочей области раздела элемента.

   Пареметры 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

Закрыть

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

   Удалить – для удаления выбранного в рабочей области раздела элемента.

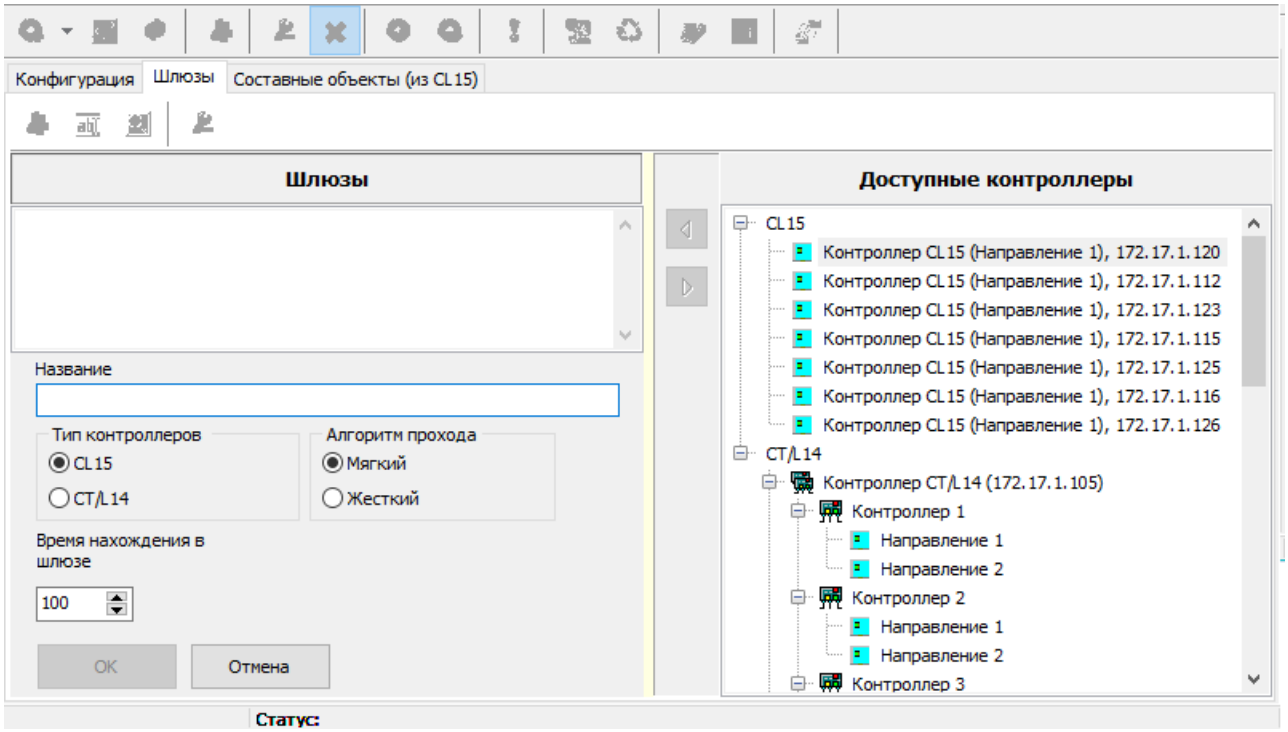
3. Рабочая область вкладки ***Шлюзы*** содержит список созданных шлюзов.

4. Список доступных контроллеров ***CL15*** и ***CT/L14***.

3.3.2 Создание шлюза

Для создания шлюза:

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



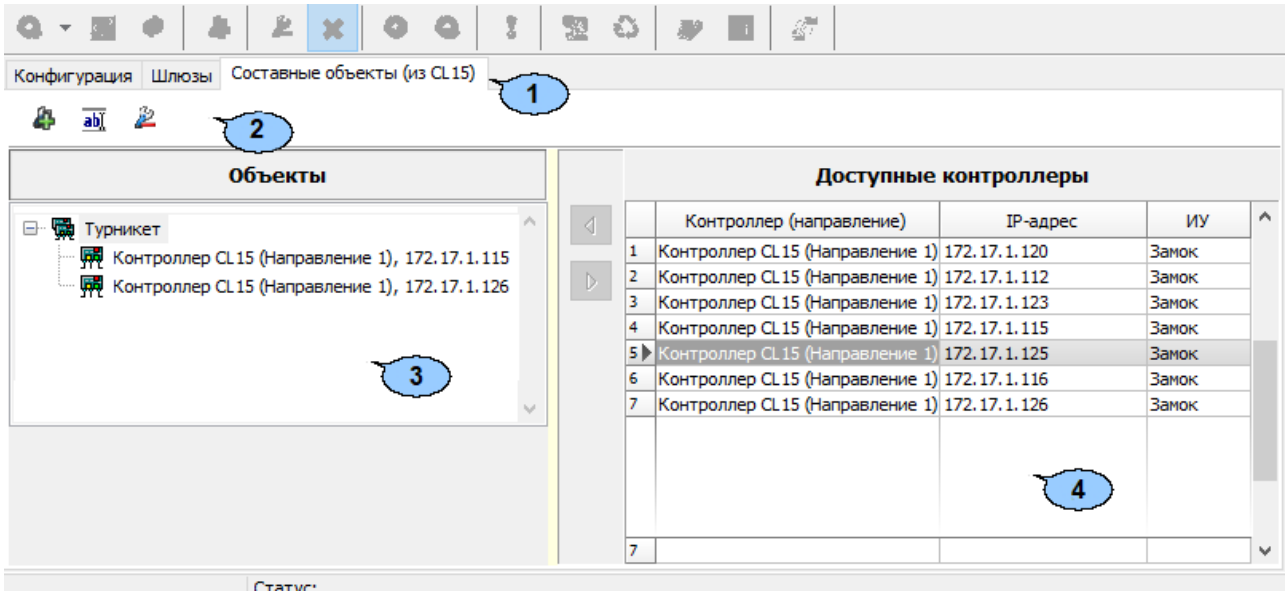
2. В открывшемся окне в поле **Название** введите имя для нового шлюза.
3. Выберите необходимый тип контроллера.
4. Выберите алгоритм прохода:
   - Тип **Мягкий.** При использоваии данного режима, если человек находится внутри шлюза, то возможен проход вперед и выход назад.
   - Тип **Жесткий.** При использоваии 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 отобразиться 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 **Конфигураци** 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:

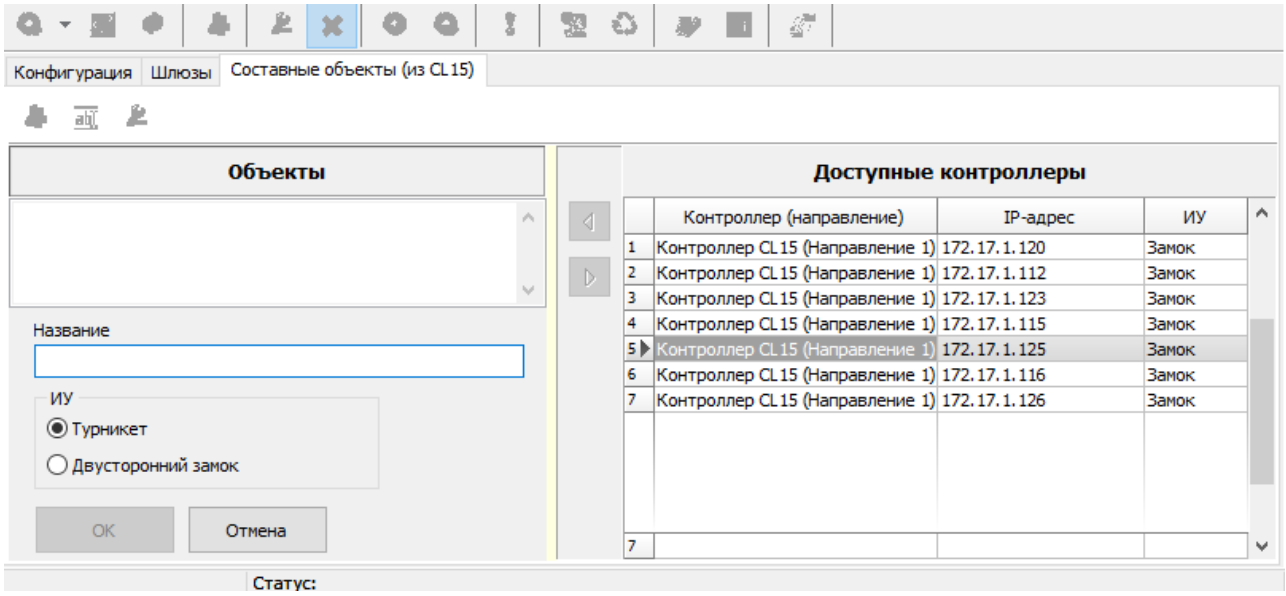


1. Выбор вкладки раздела:
   - **Конфигурация;**
   - **Шлюзы**;
   - **Составные объекты.**
2. Панель инструментов содержит следующие кнопки:
   Добавить – для создания составного контроллера.
   Изменить название – для изменения названия выбранного в рабочей области раздела элемента.
   Удалить – для удаления выбранного в рабочей области раздела элемента.
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 **Конфигураци** и нажмите на панели инструментов раздела кнопку **Передать измененные параметры**.

4 Раздел «Видеонаблюдение»

4.1 Назначение

Раздел ***«Видеонаблюдение»*** предназначен для отображения и записи в режиме реального времени видеоинформации, получаемой с камер видеоподсистемы системы безопасности. В разделе предусмотрена возможность просмотра записанного ранее видеоархива .

Для работы раздела необходим **Сервер видеоподсистемы**. В разделе доступны все камеры, подключенные к видеоподсистеме системы безопасности в разделе ***«Конфигуратор»***. В штатном режиме при запущенном сервере видеоподсистемы (сервер запускается автоматически при загрузке ОС) запись кадров с камер производится непрерывно. Объем хранимого на сервере видеоподсистемы видеоархива (глубина записи) зависит от размера созданного файла видеоархива.

Примечание

При необходимости остановка записи с камер производится из раздела ***«Управление устройствами»***.

4.2 Рабочее окно раздела

При описании раздела используются следующие термины:

Видеоокно – панель рабочей области раздела, на которой выводятся кадры с одной (или нескольких) заранее указанных при создании или настройки схемы видеокамер.

Схема – совокупность видеоокон, одновременно отображаемых в рабочей области раздела. В разделе может быть создано несколько схем с возможностью быстрого переключения между схемами.

Если ранее была создана хотя бы одна схема расположения видеоокон, то рабочее окно раздела имеет следующий вид:

1. Панель инструментов раздела:

   Создать новую схему – кнопка позволяет создать в рабочей области раздела новую схему расположения видеоокон. Каждое видеоокно связанно с одной (или несколькими) из камер системы безопасности.

Примечание

Открыть видеоокно одной из камер видеоподсистемы можно так же не создавая схемы. Для этого нажмите стрелку справа от кнопки **Создать новую схему** и в открывшемся меню выберите нужную камеру. Видеоокно выбранной камеры будет открыто на новой вкладке с названием, соответствующим названию камеры.

   Удалить схему – кнопка позволяет удалить открытую схему.

2. Рабочая область раздела содержит видеоокна для вывода изображений, получаемых с камер. Расположение и размер видеоокон зависит от настроек выбранной схемы. Для раскрытия рабочей области раздела на весь экран монитора (перехода в полноэкранный режим) нажмите на клавиатуре сочетание клавиш **Ctrl +Enter**. Для выхода из полноэкранного режима нажмите **Esc** (действие доступно при установке флажка у соответствующего параметра на вкладке **Разное** окна **Параметры отображения**).

Примечание

Для каждого видеоокна также доступны следующие действия:

При наведении указателя мыши на видеоокно в левом верхнем углу отображается название камеры, с которой получается изображение, выводимое в видеоокне: ACTi ACM4001.

Размер видеоокна может быть изменен вручную. Для этого подведите указатель мыши к его границе, при этом указатель примет вид **-** или ¦. Нажмите левую кнопку мыши и, удерживая ее, переместите границу видеоокна в нужное положение. Это действие доступно после установке флажка у параметра **Разрешить изменение размеров мышью** на вкладке **Схема** окна **Параметры отображения**.

При нажатии правой кнопкой мыши в видеоокне камеры откроется контекстное меню, содержащее следующие пункты:

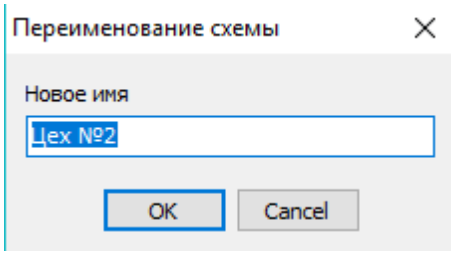
- **Открыть веб-страницу устройства** – команда позволяет открыть в браузере (например, *Internet Explorer*) веб-интерфейс камеры, с которой получается изображение, выводимое на панели.
- **Параметры отображения**– команда позволяет открыть окно **Параметры отображения** для изменения параметров панели или схемы.

3. Элементы управления видеоокна отображаются в левом нижнем углу при наведении указателя мыши на видеоокно. Элементы управления доступны после установки флажков у соответствующих им параметров на вкладке **Действия** окна **Параметры отображения**.

   Открыть в полном окне – кнопка позволяет открыть видеоокно камеры на дополнительной вкладке, название которой соответствует выбранной камере (например, **ACTi ACM4001**). Открыть дополнительную вкладку так же можно дважды нажав левой кнопкой мыши в видеоокне камеры. Для закрытия вкладки нажмите ☒ рядом с ее заголовком.

Воспроизвести – кнопка позволяет открыть дополнительную вкладку **Проигрыватель** для воспроизведения записанных с камеры кадров. Глубина записи зависит от установленного при конфигурации видеоподсистемы размера файла видеоархива. Настройка производится в разделе ***«Центр управления видеоподсистемой»***. Для закрытия вкладки **Проигрыватель** нажмите ☒ рядом с ее заголовком.

4. Вкладки для выбора одной из созданных ранее схем расположения видеоокон камер. При нажатии правой кнопкой мыши на заголовке вкладки (схемы) откроется контекстное меню, содержащее следующие команды:
   - **Создать новую схему**– команда (аналогична соответствующей кнопки панели инструментов раздела) позволяет создать новую схему расположения видеоокон камер в рабочей области раздела.
   - **Переименовать схему** – команда позволяет открыть окно **Переименование схемы**. После изменения названия нажмите кнопку **ОК**.



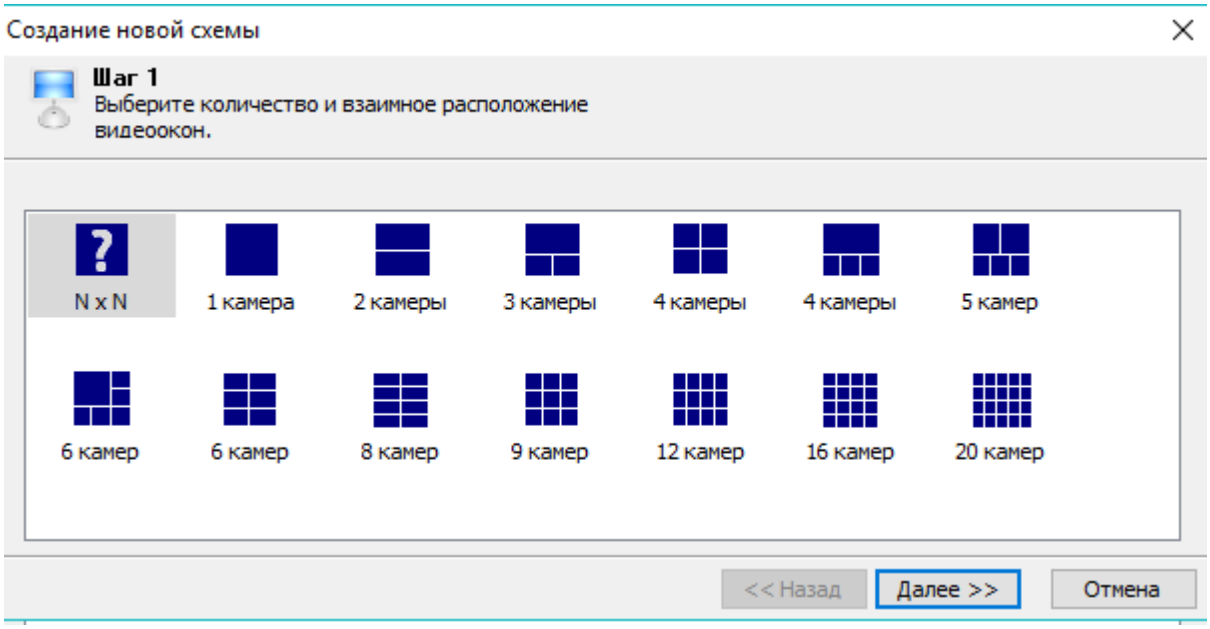
   - **Удалить схему** – команда (аналогична соответствующей кнопки панели инструментов раздела) позволяет удалить схему.

5. Регулятор громкости.

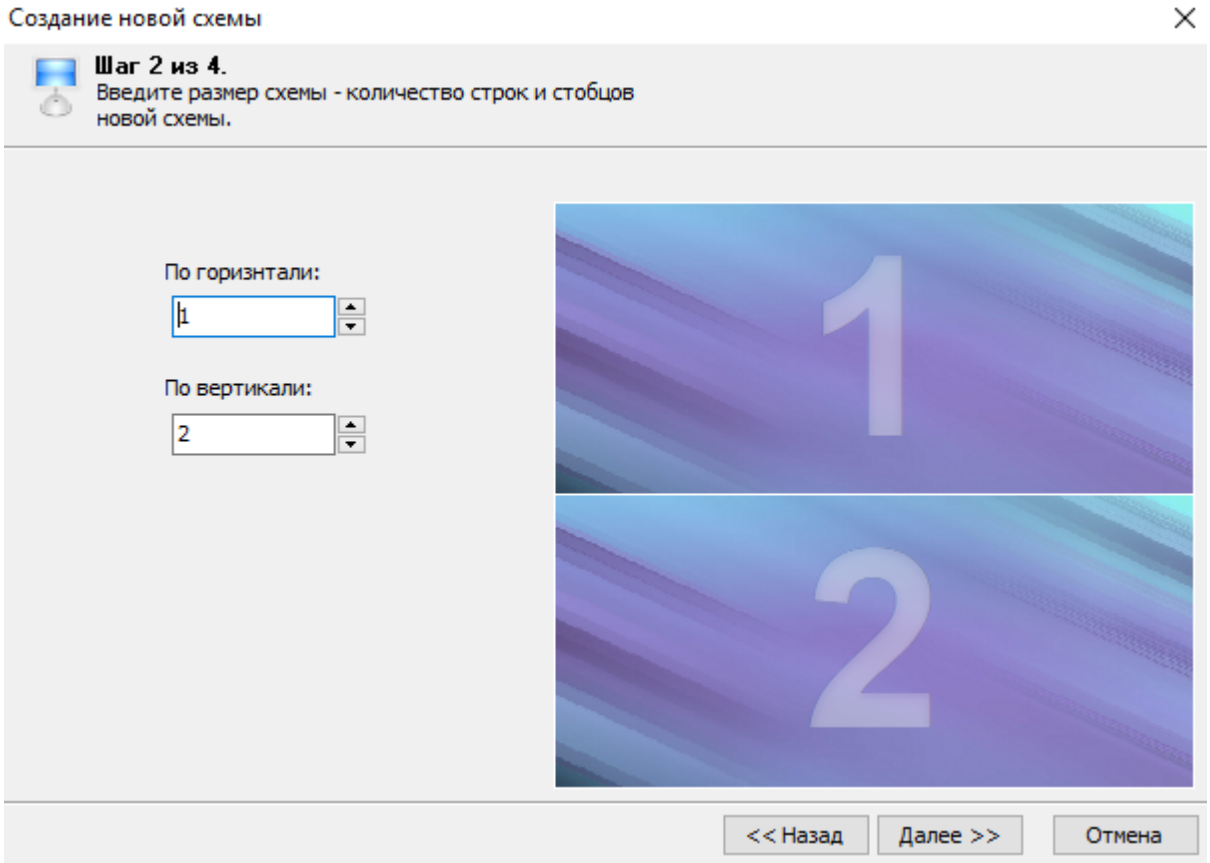
4.3 Создание новой схемы

Одновременно в разделе может быть создано несколько схем расположения видеоокон. Переход между схемами осуществляется выбором соответствующей вкладки в рабочей области раздела. Настройки схемы сохраняются локально на ПК оператора. Для создания новой схемы:

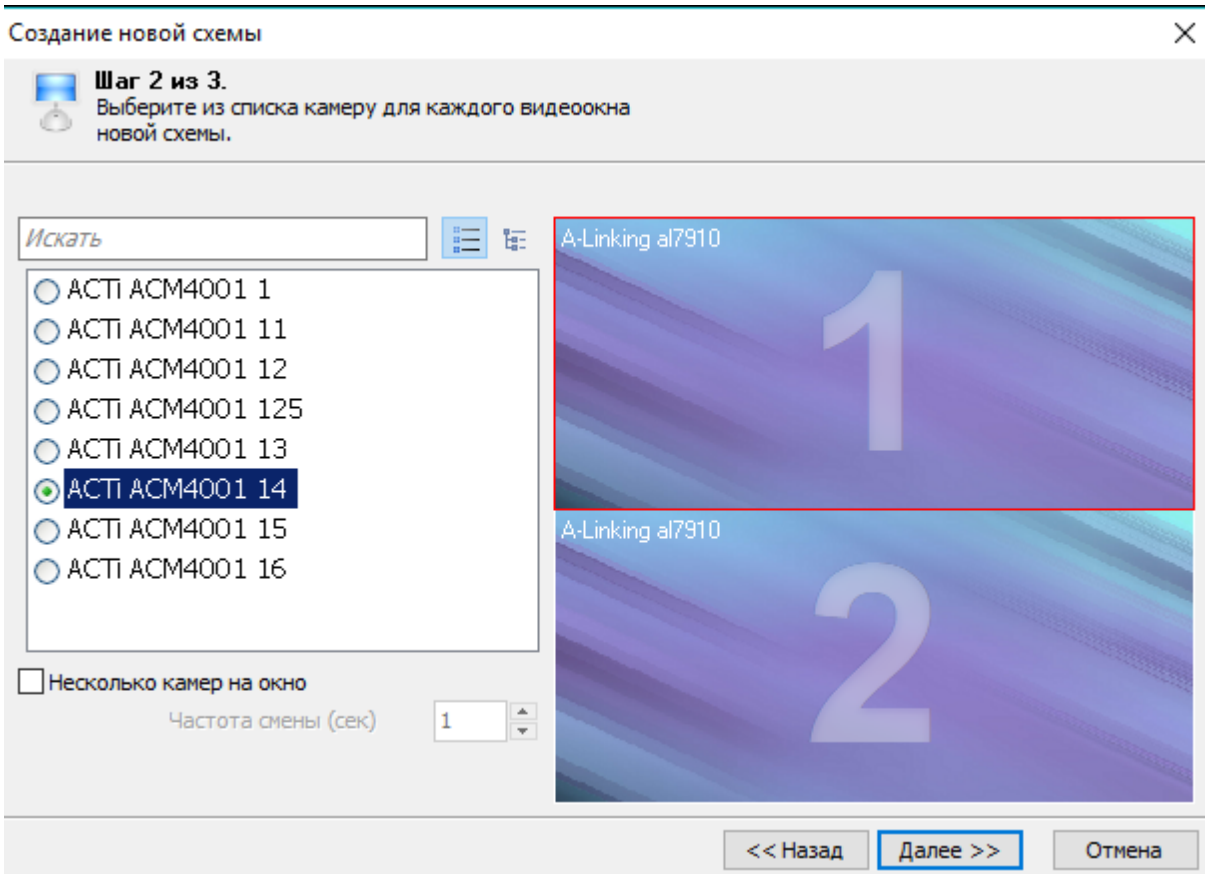
1. Нажмите кнопку **Создать новую схему** – на панели инструментов раздела. Откроется окно **Создание новой схемы**:



2. В открывшемся окне выберите один из вариантов расположения видеоокон камер. Количество видеоокон зависит от количества камер, с которых предполагается выводить изображения в рабочую область раздела. Нажмите кнопку **Далее**.
3. Если ни один из вариантов расположения видеоокон не подходит, выделите иконку N x N и нажмите кнопку **Далее**.

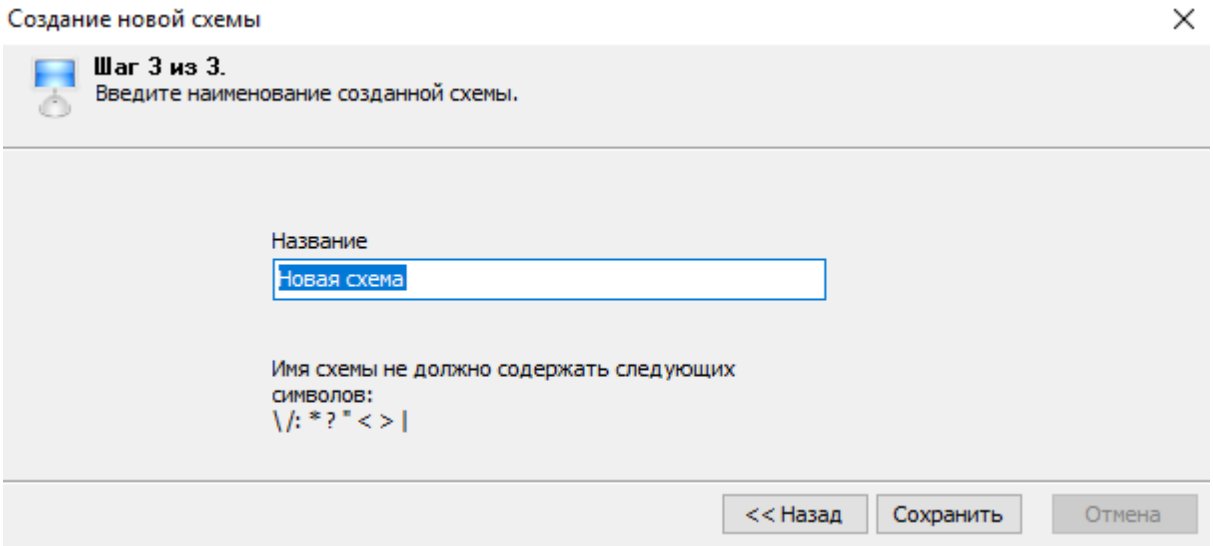


4. В открывшемся окне укажите с помощью счетчика **По горизонтали:** необходимое количество столбцов, а с помощью счетчика **По вертикали:** необходимое количество рядов видеоокон для вывода изображений с необходимого количества камер. При этом в правой части окна будет отображаться установленный вариант расположения в рабочей области раздела. Нажмите кнопку **Далее**.
5. Откроется окно для выбора камер:



В левой части окна выводится список доступных камер. При этом если нажата кнопка , камеры в списке расположены в алфавитном порядке в соответствии с их названиями, если нажата кнопка , то камеры связаны с помещениями, в которых они расположены. В правой части окна отображается выбранный вариант расположения видеоокон в рабочей области раздела.

6. В каждом видеоокне укажите камеры, изображения с которых будет транслироваться в этом видеоокне. Для этого выделите в правой части окна одно из видеооокон (при этом оно будет отмечено рамкой), затем в левой части отметьте флажком одну из камер, которая будет связана с данным видеоокном. При поиске видеокамеры используйте поле ввода **Искать** для ввода шаблона поиска по названию камеры. Соответствующие шаблону камеры будут выделены в списке красным. При установке флажка **Несколько камер на окно** в одном видеоокне будут отображаться изображения с нескольких выбранных для него в списке камер, при этом переключение между камерами будет производиться через интервал времени, установленный при помощи счетчика **Частота смены (сек)**. Таким образом определите камеры для каждого видеоокна, после чего нажмите кнопку **Далее**. Откроется новое окно:



7. В открывшемся окне задайте название схемы. Это название будет указываться в заголовке вкладки схемы. Нажмите кнопку **Сохранить**. В рабочей области раздела появится вкладка с названием новой схемы.
8. При необходимости создания нескольких схем повторите описанные выше действия.
9. Для изменения названия схемы нажмите правой кнопкой мыши на заголовке соответствующей ей вкладки. В открывшемся меню выберите команду **Переименовать схему**. В открывшемся окне **Переименование схемы** введите новое название и нажмите кнопку **ОК**. Название схемы будет изменено.
10. Для удаления схемы откройте ее в рабочей области раздела и нажмите кнопку **Удалить схему** на панели инструментов раздела.

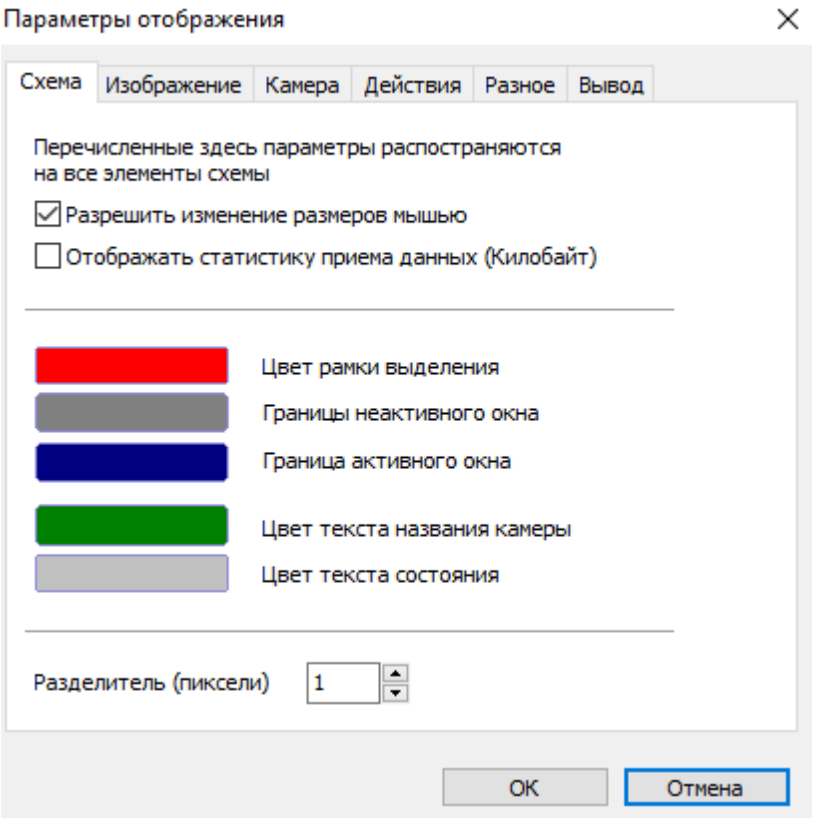
4.4 Настройка параметров схемы

Для изменения параметров созданной схемы или одного из видеоокон:

1. Нажмите правой кнопкой мыши в одном из видеоокон схемы. В открывшемся меню выберите пункт **Параметры отображения**. Откроется окно **Параметры отображения**. В окне доступны следующие вкладки:
   - **Схема**;
   - **Изображение**;
   - **Камера**;
   - **Действия**;
   - **Разное**;
   - **Вывод**.
2. В открывшемся окне измените необходимые параметры на соответствующих вкладках, после чего нажмите кнопку **ОК**.
3. Окно **Параметры отображения** будет закрыто, измененные параметры будут применены к схеме.

4.4.1 Вкладка «Схема»

Вкладка **Схема** предназначена для настройки внешнего вида схемы и выглядит следующим образом:



Разрешить изменение размеров мышью – при установке флажка будет доступно изменение размеров видеоокон схемы вручную.

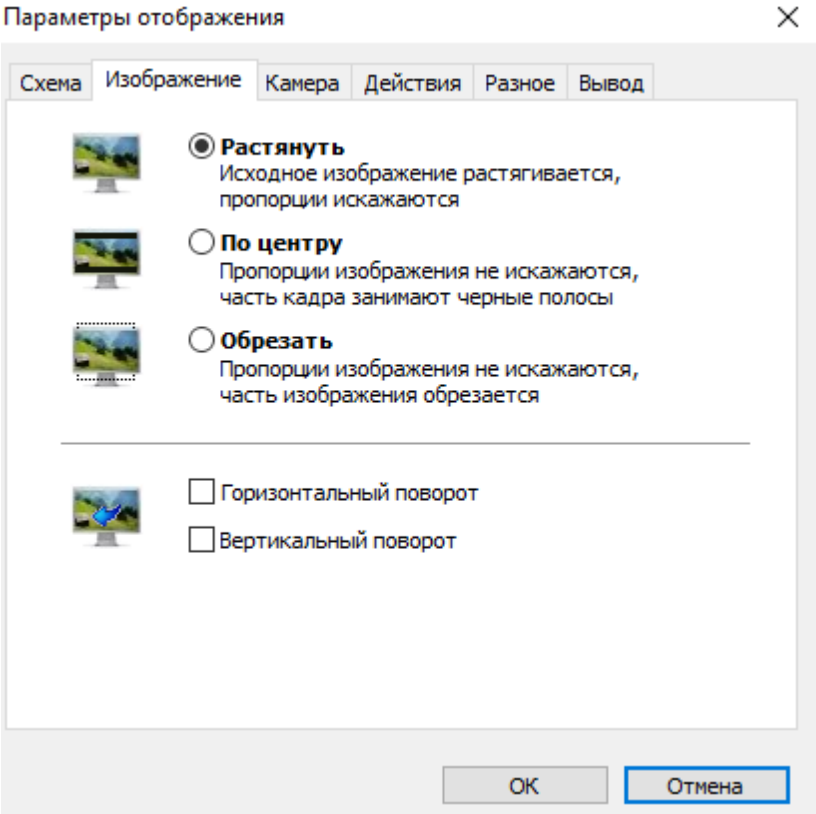
Отображать статистику приема данных (Килобайт) – при установке флажка в правом верхнем углу каждого видеоокна будет отображаться объем полученных данных.

В центральной части вкладки расположены кнопки, окрашенные в цвета соответствующих элементов схемы. При нажатии каждой кнопки открывается окно **Цвет** для изменения цвета элемента, указанного справа от кнопки.

Разделители (пиксели) – счетчик позволяет установить толщину границ (рамок) между видеоокнами.

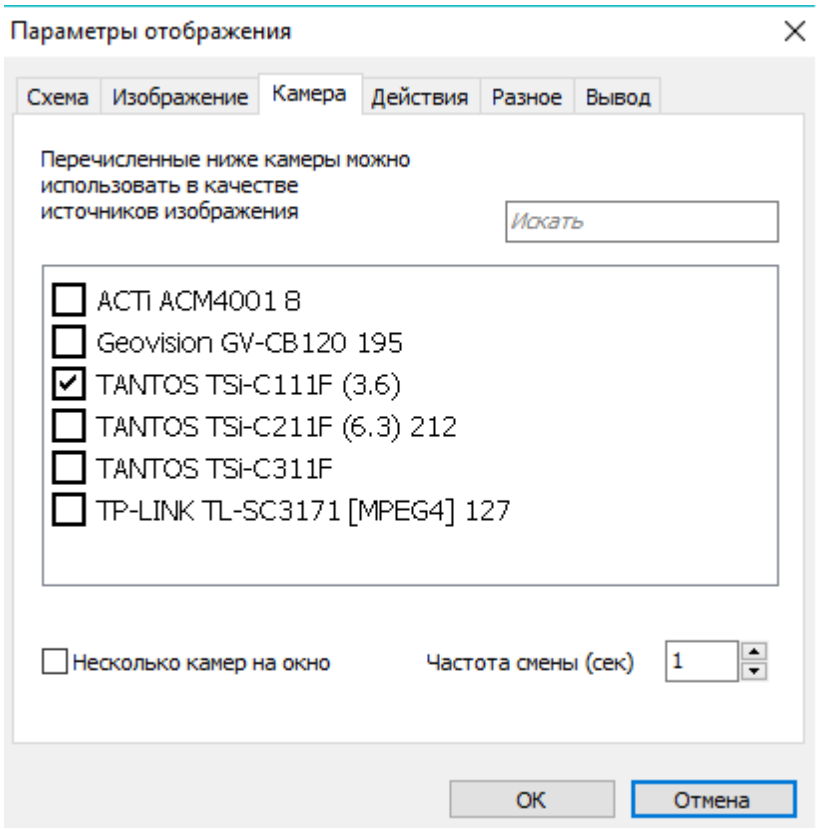
4.4.2 Вкладка «Изображение»

Вкладка **Изображение** предназначена для изменения расположения изображения с камеры в выбранном видеоокне. Вкладка имеет вид:



4.4.3 Вкладка «Камера»

Вкладка **Камера** содержит список доступных камер и предназначена для изменения камеры, изображение с которой будет отображаться в выбранном видеоокне. Вкладка имеет вид:



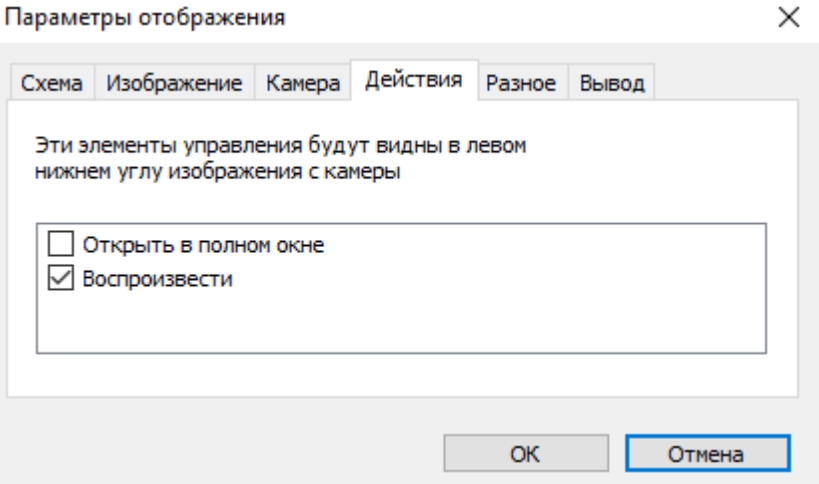
Искать – поле ввода позволяет ввести образец для поиска в списке камеры по ее названию. Все соответствующие образцу камеры в списке будут выделены красным цветом.

Несколько камер на окно – при установке флажка в видеоокне поочередно будет отображаться изображение с нескольких камер выбранных в списке.

Частота смены (сек) – счетчик позволяет установить время, в течение которого будет отображаться изображение с каждой из выбранных в списке камер.

4.4.4 Вкладка «Действия»

Вкладка **Действия** предназначена для выбора элементов управления, которые будут отображаться в левом нижнем углу каждого видеоокна схемы. Вкладка имеет вид:

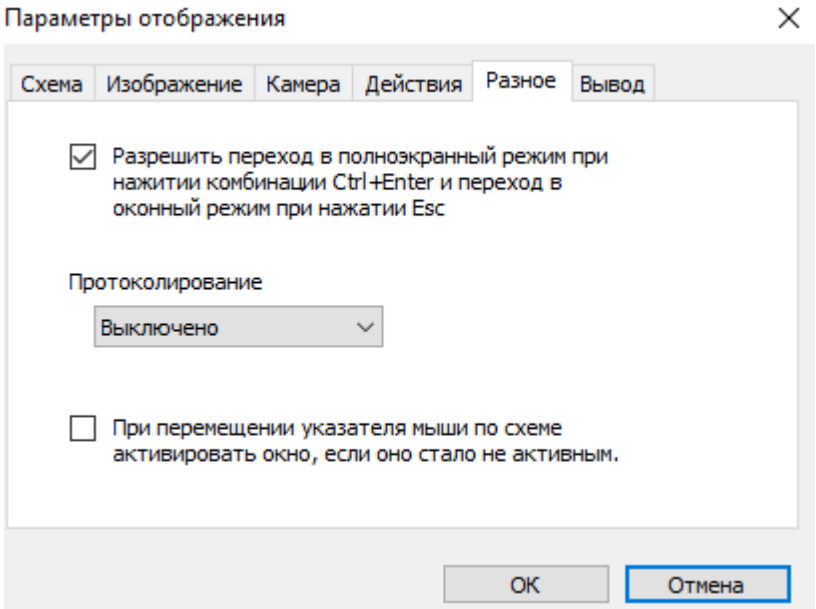


Открыть в полном окне – при установке флажка в каждом видеоокне схемы будет отображаться кнопка , позволяющая открыть видеоокна на дополнительной вкладке.

Воспроизвести – при установке флажка в каждом видеоокне схемы будет отображаться кнопка , позволяющая открыть дополнительную вкладку **Проигрыватель** для воспроизведения записанных кадров с камеры, которой соответствует видеоокно.

4.4.5 Вкладка «Разное»

Вкладка **Разное** содержит дополнительные параметры настройки схемы. Вкладка имеет вид:



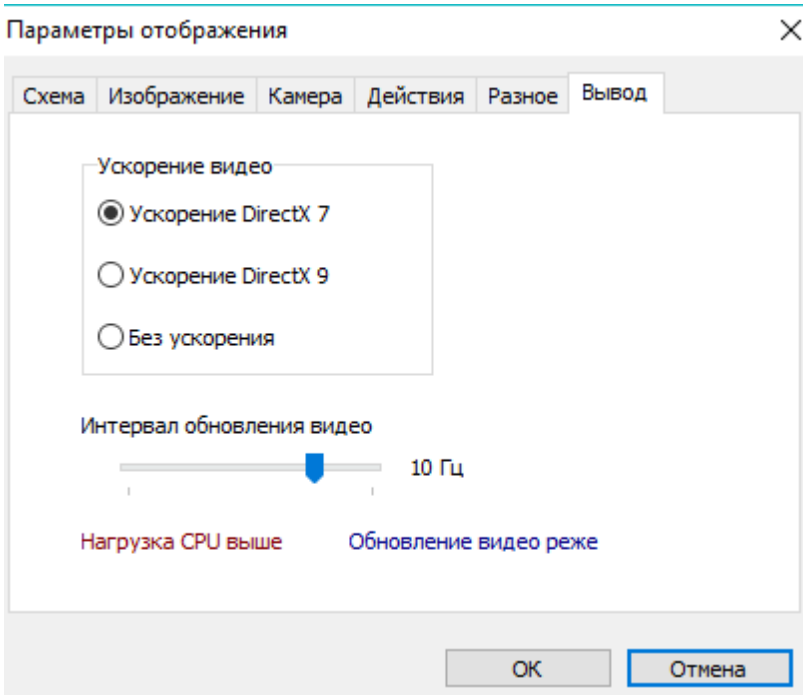
Разрешить переход в полноэкранный режим при нажатии комбинации Ctrl+Enter и переход в оконный режим при нажатии Esc – при установке флажка для схемы будет доступен переход в полноэкранный режим.

Протоколирование – функция используется службой сервиса и разработчиками.

При перемещении указателя мыши по схеме активировать окно, если оно стало не активным – используется при работе с несколькими мониторами.

4.4.6 Вкладка «Вывод»

Вкладка **Вывод** предназначена настройки параметров отображения изображения с камер в видеоокнах схемы. Вкладка имеет вид:



Ускорение видео – переключатель позволяет выбрать вариант используемого аппаратного ускорения.

Интервал обновления видео – ползунок позволяет установить частоту обновления рабочей области раздела от 8 до 50 кадров в секунду.

5 Раздел «Верификация»

5.1 Назначение

При описании раздела используются следующие понятия:

Верификация – процедура подтверждения оператором системы безопасности с помощью комиссионирующего устройства (ПДУ, кнопки ДУ, команды ПО) прав предъявленного идентификатора. Принятие решения оператором происходит на основании сравнения изображения, получаемого с камер наблюдения видеоподсистемы системы безопасности, и данных о владельце идентификатора (в том числе фотографий), хранящихся в базе данных системы безопасности.

Индикация – процедура, при которой в режиме реального времени оператор системы безопасности информируется о событиях, связанных с предъявлением идентификаторов. Для каждого события оператору предоставляются кадры с камер наблюдения видеоподсистемы системы безопасности и данные владельцев предъявленных идентификаторах, хранящихся в базе данных системы безопасности.

Точка верификации – это один из считывателей и связанная с этим считывателем камера.

Раздел ***«Верификация»*** позволяет сотруднику службы охраны производить идентификацию владельца карты доступа, сравнивая внешность проходящего сотрудника (ученика) или изображение с видеокамеры и фото владельца карты, хранящееся в БД системы, и на основании этого принимать решение о подтверждении его права на проход. Решение может приниматься как вручную оператором, так и в автоматическом режиме.

Все действия оператора, информация о фактах предъявления карт доступа и кадры с видеокамер автоматически записываются разделом и доступны для последующего просмотра и анализа в разделе ***«Журнал верификации»***.

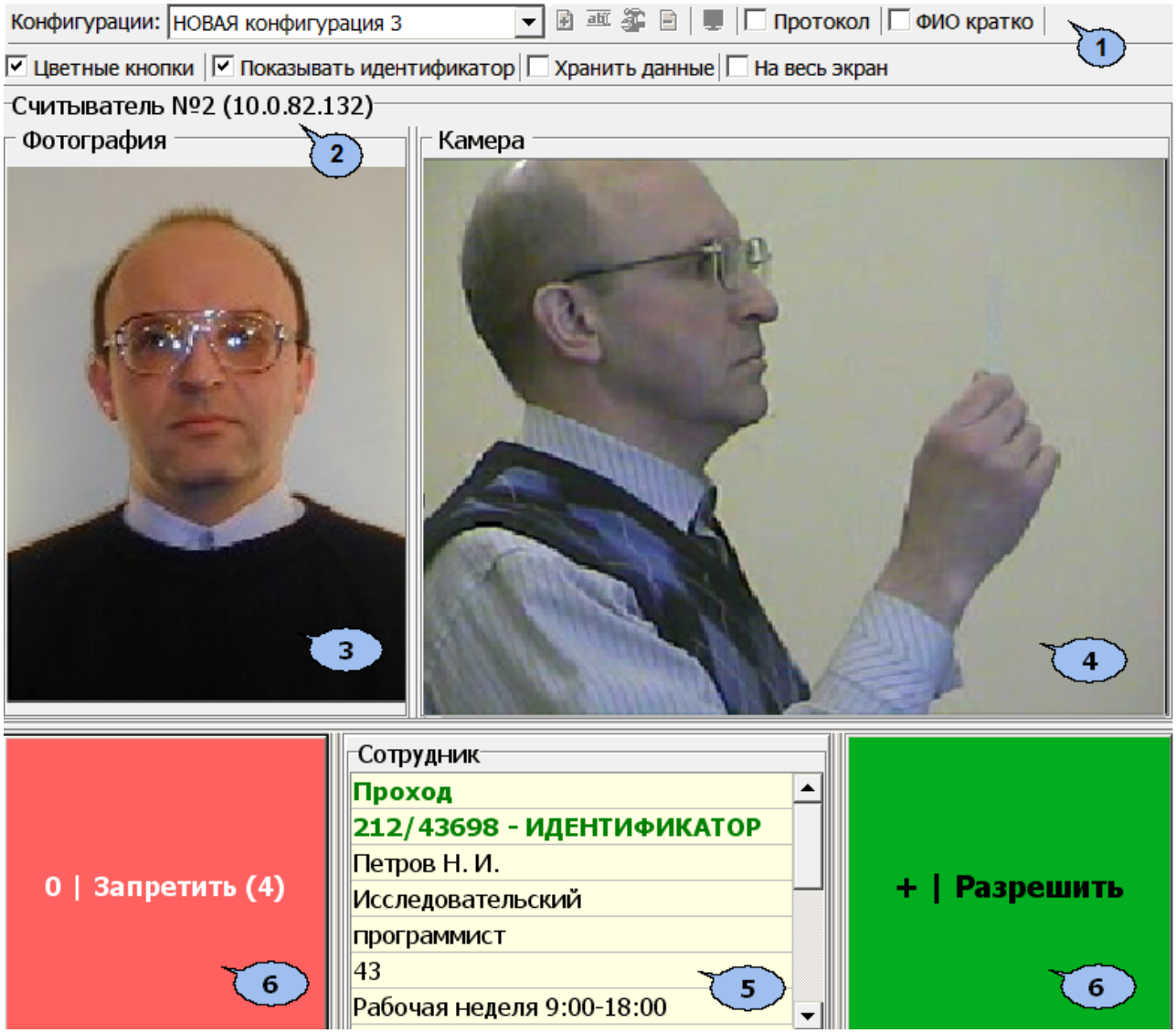
Раздел позволяет одновременно контролировать до 4-х точек верификации (и 4-х связанных с ними камер наблюдения).

Перед началом работы с разделом необходимо создать хотя бы одну конфигурацию точек верификации. В процессе конфигурации создаются точки верификации, то есть выбираются считыватели и связанные с ними камеры, определяется для каждой точки верификации, какие запросы и события будут обрабатываться разделом, и какая информация о сотруднике (ученике) будет предоставляться оператору.

Имеется возможность настроить и сохранить несколько вариантов конфигурации точек верификации и при необходимости переходить между ними при помощи раскрывающегося списка **Конфигурации верификации**.

5.2 Рабочее окно раздела

Если конфигурация точек верификации уже создана, то рабочее окно раздела для одной точки верификации состоит из следующих элементов:

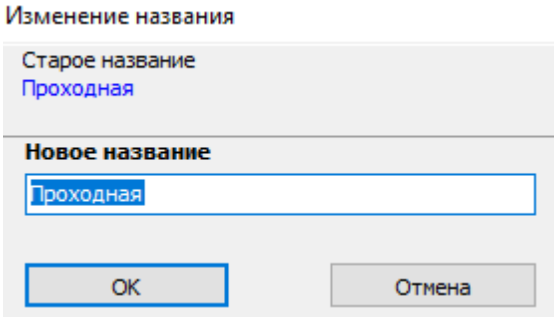


1. Панель инструментов раздела:

   Конфигурация верификации – раскрывающийся список позволяет выбирать конфигурацию точек верификации. В списке отображается название выбранной конфигурации.

   Добавить конфигурацию (**Ctrl+N**) – кнопка позволяет создать новую конфигурацию верификации.

   Изменить название (**Ctrl+E**) – кнопка позволяет изменить название конфигурации точек верификации, выбранной в раскрывающемся списке на панели инструментов. При нажатии кнопки откроется окно **Изменение названия**:



После ввода нового названия нажмите кнопку **OK**.

Изменить состав (**Ctrl+T**) – кнопка позволяет изменить параметры конфигурации точек верификации, выбранной в раскрывающемся списке на панели инструментов.

Удалить (**Ctrl+D**) – кнопка позволяет удалить конфигурацию точек верификации, выбранную в раскрывающемся списке на панели инструментов.

На весь экран (Ctrl+Enter) – кнопка позволяет перейти в полноэкранный режим. Для выхода из полноэкранного режима нажмите кнопку **Esc**.

Протокол. При установке флажка в текстовые log-файлы записывается отладочная информацию о работе раздела. Данная функция предназначена для разработчиков. При работе с разделом рекомендуется снять флажок.

ФИО кратко. При установке флажка на панели **Сотрудник (ученик)** вместо имени и отчества владельца карты доступа отображаются его инициалы.

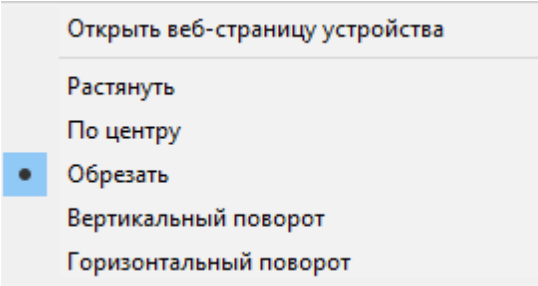
Цветные кнопки. При установке флажка кнопки **Запретит**, **Разрешить** будут выделены соответственно красным и зеленым цветом.

Показывать идентификатор. При установке флажка на панели **Сотрудник (ученик)** будет отображаться идентификатор предъявленной карты доступа.

Хранить данные. При установке флажка будет происходить локальное кэширование данных о сотрудниках.

На весь экран. При установке флажка во время перехода на вкладку верификация будет автоматически производиться переход в полноэкранный режим. Для выхода из полноэкранного режима нажмите кнопку **Esc**.

2. В строке отображается название считывателя, с которым связана точка верификации и IP-адрес контроллера, к которому он подключен.
3. **Фотография.** При предъявлении карты доступа на панели отображается фотография сотрудника (ученика) из БД системы. В качестве фотографии может быть сохранен кадр, полученный с камеры. Для этого после предъявления идентификатора и получения информации о его владельце нажмите правой кнопкой мыши на панели **Фотография** и затем нажмите на появившуюся кнопку Кадр --> Фотография "Фролов В. П.". Кадр с камеры будет сохранен в базе данных в качестве фотографии владельца предъявленной карты.
4. Панель **Камера для** отображения кадров камеры. При нажатии правой кнопкой мыши в блоке отображения кадров видеокамер на экран выводится контекстное меню, позволяющее перейти в веб-интерфейс видеокамеры или установить параметры отображения:

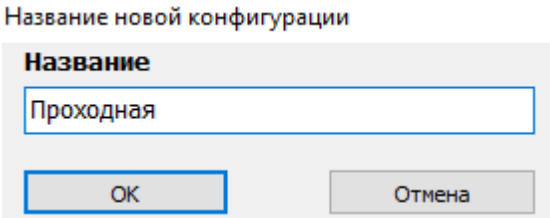


5. Панель **Сотрудник (ученик)** При предъявлении карты доступа в таблице отображается: название запроса (события), номер идентификатора и учетные данные о владельце идентификатора, выбранные при конфигурации точек верификации.
6. Кнопки **Запретить** и **Разрешить** предназначены для принятия решения оператором. Кнопки становятся активными при поступлении верифицируемого запроса, требующего принятия решения оператором. Если в параметрах точки верификации ни одно из событий (предъявлений идентификатора) не определено как верифицируемое, то кнопки не будет доступны. На кнопках отображены наименование *горячих* клавиш на цифровом блоке клавиатуры (кнопки работают при включенном режиме ввода цифр *Num Lock*).

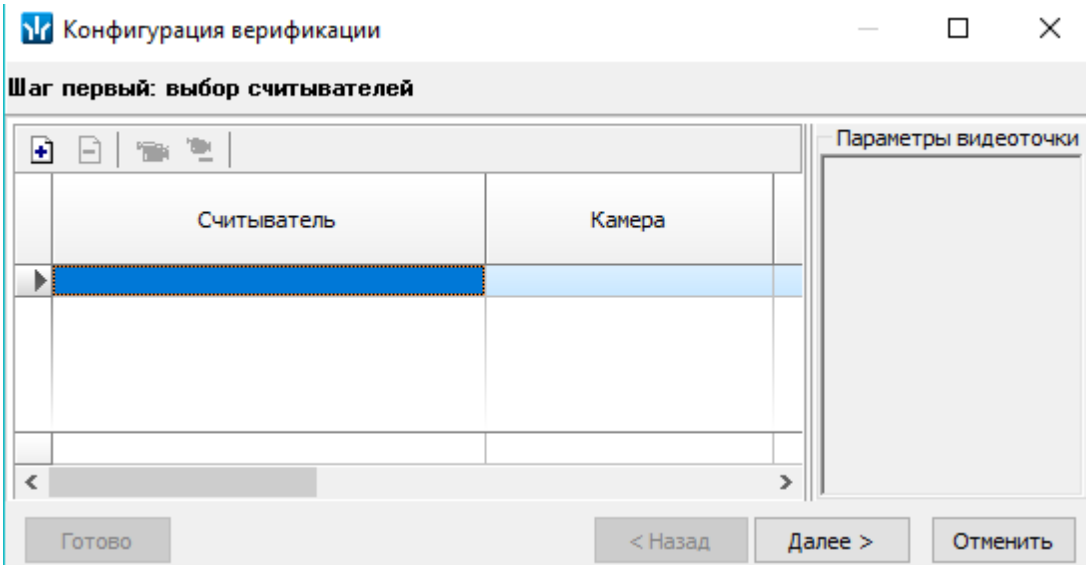
5.3 Конфигурация точки верификации

Для создания новой конфигурации точек верификации:

1. Нажмите на кнопке **Добавить** на панели инструментов раздела. Откроется окно **Название новой конфигурации**:



2. Введите название конфигурации. Это название будет отображаться в раскрывающемся списке **Конфигурация верификации**. Нажмите кнопку **OK**. Откроется окно **Конфигурация верификации. Шаг первый: выбор считывателей:**



На панели инструментов окна **Конфигурация верификации** могут быть доступны следующие кнопки:

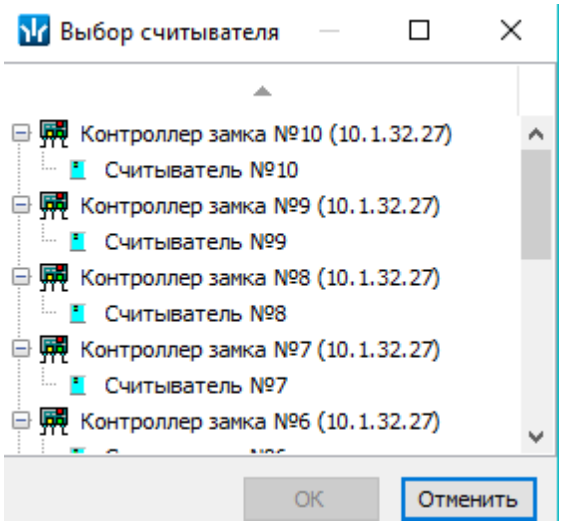
Добавить считыватель (**Ctrl+N**) – кнопка позволяет добавить точку верификации.

Удалить считыватель (**Ctrl+D**) – кнопка позволяет удалить точку верификации.

Показать кадр камеры (**Ctrl+V**) – при нажатии кнопки откроется область окна с изображением кадров с выделенной камеры.

Удалить камеру (**Ctrl+Alt+D**) – кнопка позволяет удалить выбранную камеру.

3. Нажмите кнопку **Добавить считыватель** . Откроется окно **Выбор считывателя**. В окне будет отображаться список контроллеров с подключенными к ним считывателями:



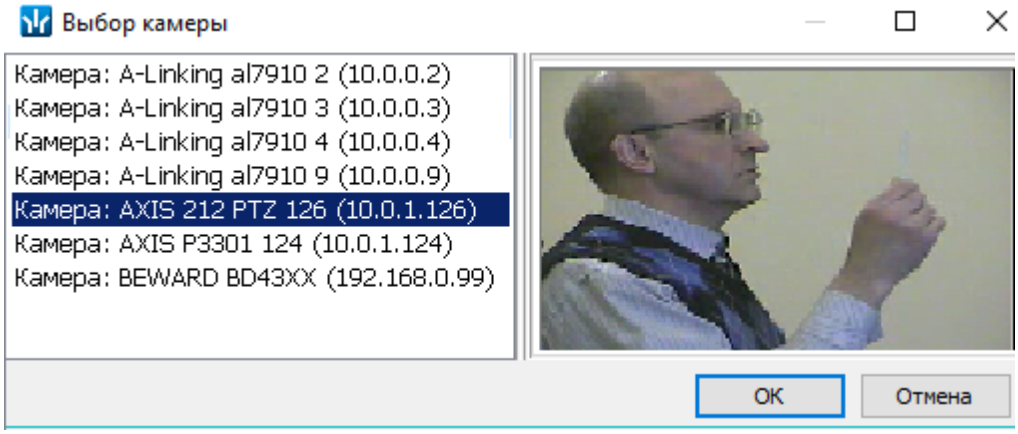
4. В открывшемся окне выделите считыватель, для которого необходимо создать точку верификации. Нажмите кнопку **OK**. (Если считыватель уже присутствует в конфигурации, то кнопка **OK** будет недоступна.) Окно **Выбор считывателя** будет закрыто, выбранный считыватель будет добавлен в список в окне **Конфигурация верификации**. (При необходимости считыватель можно удалить с помощью кнопки **Удалить считыватель** .)

Внимание!

Контроль за предъявлением карт доступа в режиме верификации для выбранного считывателя может осуществляться только из одного раздела ***«Верификация»***. Невозможно организовать несколько рабочих мест операторов раздела ***«Верификации»***, контролирующих одновременно одну точку верификации.

5. Для выбранного считывателя станет доступна область **Параметры видеоточки**. Укажите, какие именно события подлежат верификации со стороны оператора. Если для этих событий необходимо сохранять кадры с камер, поставьте флажок у параметра **Запись кадров видеокамеры** для выбранных событий. Описание параметров точки верификации.

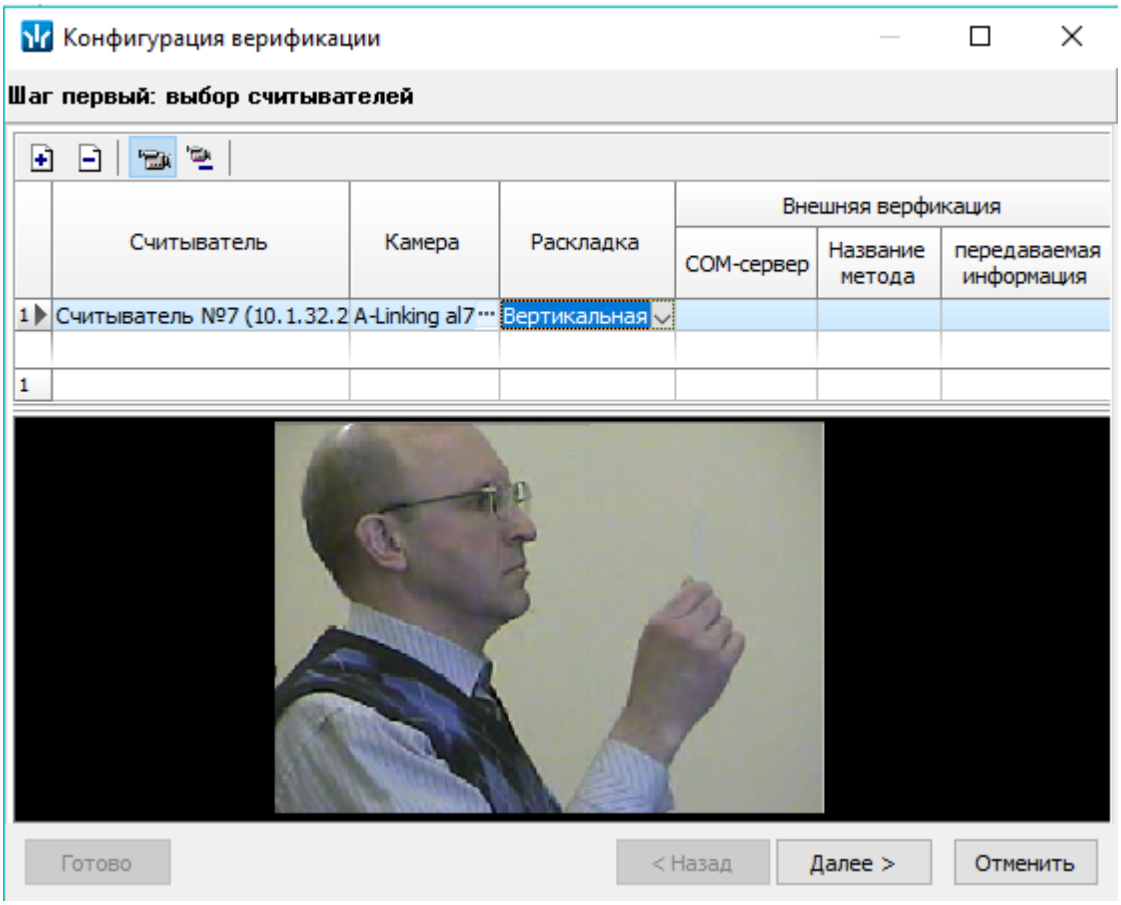
6. С помощью кнопок ... в столбцах **Камера** укажите камеру, которая будет связана с выбранным считывателем. Камера позволит оператору дистанционно контролировать ситуацию в месте прохода. При нажатии кнопки ... откроется окно **Выбор камеры**:



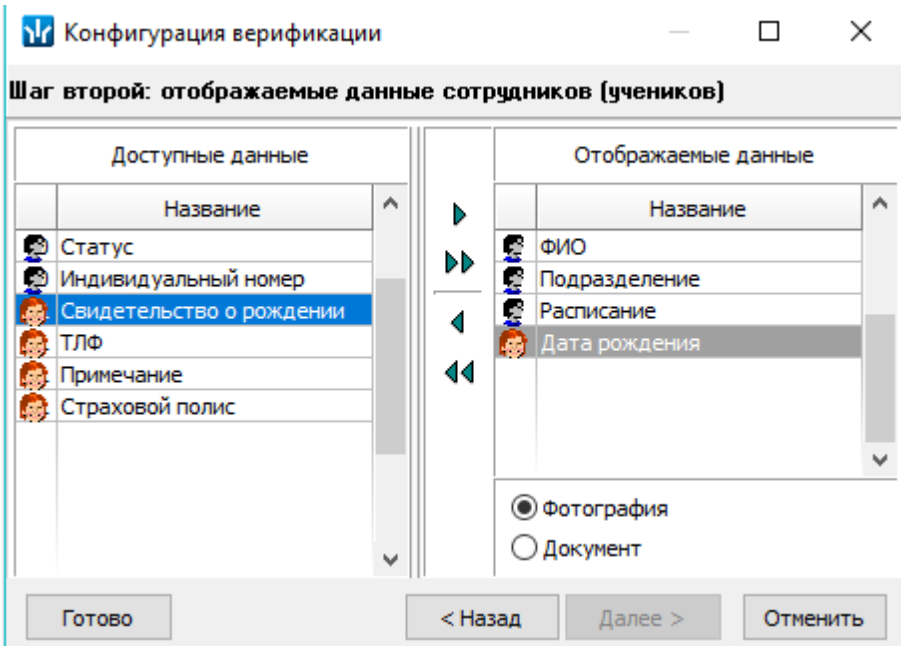
Примечание:

Для подключения к системе камер видеонаблюдения необходима установить модуль **Сервер видеоподсистемы** и добавить видеоподсистему в конфигурацию системы.

7. В открывшемся окне отобразится список всех камер, входящих в конфигурацию системы безопасности. Выделите в списке камеру, при этом в правой части окна будет транслироваться изображение с выбранной камеры. Нажмите кнопку **OK**. Окно **Выбор камеры** будет закрыто, выбранная камера будет добавлена в столбец **Камера**. (При необходимости камеру можно удалить с помощью кнопки **Удалить камеру** .
8. После добавления камеры станет доступна кнопка **Показать кадр с камеры** , при нажатии которой в нижней части окна будет транслироваться изображение с камеры, связанной с выделенным в списке считывателем:



9. В столбце **Раскладка** с помощью раскрывающегося списка выберите взаимное расположение панелей рабочего окна точки верификации **Вертикальное** или **Горизонтальное.**
10. При необходимости добавьте еще один считыватель. Максимально в одной конфигурации может быть добавлено четыре считывателя, то есть оператор можетодновременно отслеживать до четырех точек верификации. После выбора считывателей, настройки их параметров и добавления камер нажмите кнопку **Далее**. Откроется окно **Конфигурация верификации. Шаг второй: отображаемые данные сотрудников (учеников)**:



11. Определите, какие данные должны отображаться в таблице данных рабочего окна раздела при верификации карты доступа сотрудника (ученика). Для выбора данных выделите их в столбце **Доступные данные** и при помощи стрелок, расположенных в центральной части окна, перенесите в столбец **Отображаемые данные**. Значком в списке обозначаются основные доступные данные, значком - дополнительные данные. Установите флажок у параметра **Фотография** или **Документ** для отображения фотографии посетителя или скана его документа. Нажмите кнопку **Готово**.

Примечание:

Категории дополнительных данных для сотрудников (учеников) задаются в разделе ***«Учетные данные»***.

12. Окно **Конфигурация верификации** будет закрыто. Параметры конфигурации будут применены.

5.4 Параметры точки верификации

Параметры точки верификации устанавливаются независимо для каждого считывателя. Это можно сделать в процессе создания конфигурации верификации либо при нажатии кнопки **Изменить состав** на панели инструментов раздела, для изменения параметров конфигурации, выбранной в строке **Конфигурация верификации**.

Параметры точки верификации:

Параметры видеоточки	
Количество видеокадров предзаписи	0
Количество записываемых видеокадров	5
Частота записи видеокадров (кадр/сек.)	2
⊟Режим отображения информации	Не более чем
⊟**Не более чем**	
Значение	5 сек.
Таймаут верификации	5 сек.

Количество видеокадров предзаписи – параметр, определяет количество кадров, записаных с выбранной камеры перед предъявлением карты доступа к выбранному считывателю, сохраняемое в журнале.

Количество записываемых видеокадров – параметр, определяет количество кадров, записаных с выбранной видеокамеры после предъявлении карты доступа к выбранному считывателю, сохраняемое в журнале.

Частота записи видеокадров (кадр/сек.) – параметр, определяет частоту записи видеокадров.

Режим отображения информации – параметр, указывающий, в течение какого времени после команды в рабочем окне будет отображаться информация о карте доступа. Доступны два варианта значения параметра:

- **Постоянный** – в этом случае отображение информации не ограничено временем.
- **Не более чем** – в этом случае данные идентификатора отображаются после команды в течение времени, указанного в параметре **Значение**.

Таймаут верификации – время, в течение которого контроллер, отправивший запрос на верификацию, будет ожидать ответа оператора.

5.4.1 Верифицируемые события

Укажите, какие именно события подлежат верификации со стороны оператора. Для этого раскройте параметр **События** и укажите, какие события, связанные с предъявлением карт доступа, необходимо отслеживать:

Параметры видеоточки	
⊟**События**	
⊟**Сотрудников**	
⊟Проход	Отслеживать
⊟**Отслеживать**	
Запись кадров видеокамеры	☐
Верификация	Нет
⊞Проход с нарушением ВРЕМЕНИ	Отслеживать
⊞Проход с нарушением ЗОНАЛЬНОСТИ	Отслеживать
⊞Постановка на охрану	Отслеживать
⊞Снятие с охраны	Отслеживать
⊟**Посетителей**	
⊟Проход	Отслеживать
⊟**Отслеживать**	
Запись кадров видеокамеры	☐
Верификация	Нет
⊞Проход с нарушением ВРЕМЕНИ	Отслеживать
⊞Проход с нарушением ЗОНАЛЬНОСТИ	Отслеживать
⊞**Уведомляющие события**	

Проход – событие, возникающее при предъявлении карты доступа, имеющей право на проход через ИУ, управляемое считывателем.

Проход с нарушением времени – событие, возникающее при предъявлении карты доступа, имеющей право на проход через ИУ, управляемое считывателем. При этом время предъявления карты не соответствует временному критерию доступа данной карты.

Проход с нарушением зональности – событие, возникающее при предъявлении карты доступа, имеющей право на проход через ИУ, управляемое считывателем. При этом владелец карты нарушил последовательность или направление прохождения точек прохода (нарушение функций системы безопасности *Antipass* или *Global Antipass*).

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

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

Для каждого события можно установить:

- **Не отслеживать** – в этом случае контроллер не сообщает о предъявлении карты доступа, принимает решение самостоятельно.
- **Отслеживать** – в этом случае контроллер при предъявлении карты будет посылать запрос на принятие решения оператором.

Запись кадров видеокамеры – при установке флажка для этого параметра раздел будет записывать кадры видеокамер в количестве и с частотой, указанными в параметрах точки верификации.

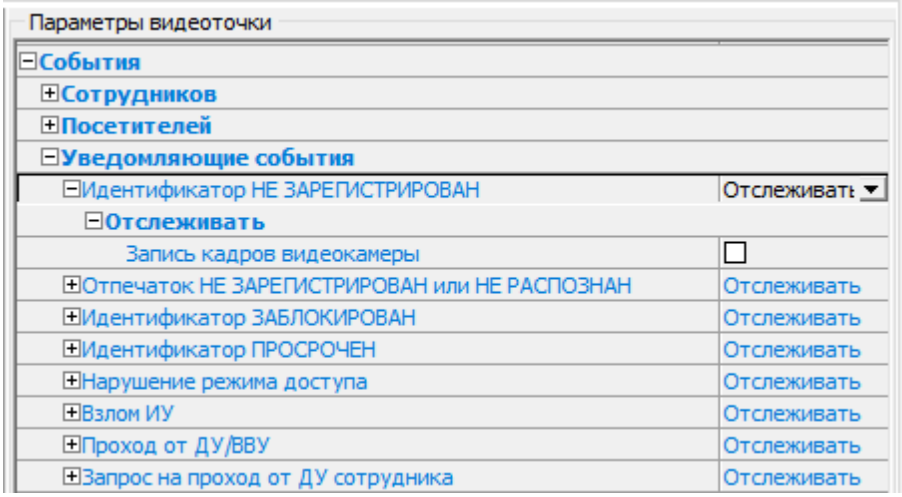
Верификация – параметр позволяет установить способ принятия решения для верифицируемых событий**:**

- **Нет** – при установке этого значения в разделе будет отображаться только информация о владельце предъявленной карты доступа, контроллер принимает решение самостоятельно.
- **Да** – при установке этого значения в разделе будет отображаться информация о владельце предъявленной карты доступа и контроллер перейдет в режим ожидания команды о разрешении/запрещении прохода: оператор должен принять решение, используя кнопки **Разрешить**/**Запретить**.

Разрешить – при установке флажка по истечении таймаута верификации (минус 2 секунды, которые зарезервированы на доставку команды контроллеру) раздел автоматически разрешит проход без вмешательства оператора. При этом оператор в течение этого времени может самостоятельно принять нужное для него решение, используя соответствующие кнопки.

5.4.2 Уведомляющие события

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



Идентификатор НЕ ЗАРЕГИСТРИРОВАН – событие, происходящее при предъявлении карты доступа, которой нет в список карт контроллера.

Отпечаток НЕ ЗАРЕГИСТРИРОВАН или НЕ РАСПОЗНАН – событие, происходящее при предъявлении отпечатка пальца, которого нет в системе или же он не распозан.

Идентификатор ЗАБЛОКИРОВАН – происходит в случае предъявления карты доступа, которая была заблокирована.

Идентификатор ПРОСРОЧЕН – событие, происходящее при предъявлении карты доступа с истекшим сроком действия.

Нарушение режима доступа – событие, происходящее при предъявлении карты доступа в режиме *«Закрыто»*.

Взлом ИУ – событие, возникающее при несанкционированном проходе через ИУ, регистрируется по факту срабатыванием датчика прохода.

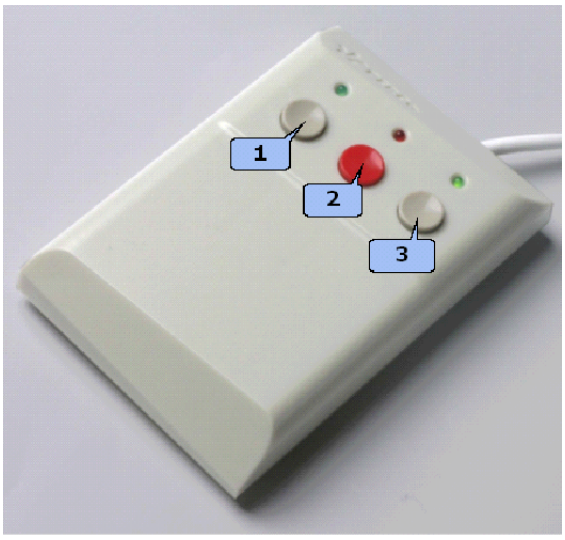
Проход от ДУ/ВВУ – событие, возникающее при проходе через ИУ после подтверждения от ПДУ или ВВУ, приводящего к разблокировке ИУ.

Запрос на проход от ДУ сотрудника (ученика) – событие, возникающее при предъявлении карты доступа сотрудника (ученика), и контроллер ожидает подтверждения прохода с помощью ПДУ. Будет отображена вся требуемая информация о владельце карты, что позволит оператору выполнить нужную команду с помощью ПДУ.

5.5 Верификация от ПДУ

В качестве верифицирующего устройства при работе с разделом может использоваться ПДУ. С помощью одного ПДУ можно осуществлять верификацию на двух точках верификации, но при этом оба считывателя и ПДУ должны быть подключены к одному и тому же контроллеру.

При верификации от ПДУ кнопки **Разрешить** и **Запретить** в рабочей области раздела недоступны и решение о подтверждении или отклонении запроса, поступающего при предъявлении карты доступа, будет приниматься оператором с помощью кнопок на ПДУ.



При поступлении запроса ПДУ издает звуковой сигнал и начинает мигать световой индикатор над одной из кнопок. На экране монитора отображается информация о владельце предъявленной карты (в том числе фотография) из базы данных системы, а также кадры с камеры, указанной при конфигурации точки верификации.

- Для подтверждения запроса оператор должен нажать на ПДУ кнопку **Разрешение прохода** соответствующую направлению прохода, от которого поступил запрос.
- Для отклонения запроса оператор должен нажать на ПДУ кнопку **Запрету прохода**, расположенную в центре.

Для настройки верификации от ПДУ:

1. Перейдите в раздел ***«Конфигуратор»***. Для считывателя, указанного при конфигурации точки верификации, установите для параметра **Подтверждение от ДУ > в режиме «Контроль»** значение **Да**:

Параметры | События | Камера СКУД

Адрес	1
Текущее наименование	Считыватель
Первоначальное наименование	Считыватель
Модель	PERCo-IRxx
⊞ **Запрещение ДУ**	
⊟ **Подтверждение от ДУ**	
⊟ в РЕЖИМЕ РАБОТЫ "Контроль"	Да
⊟ **Да**	
⊟ **Верифицировать идентификаторы СОТРУДНИКОВ**	
при проходе	☑
при проходе с НАРУШЕНИЕМ ВРЕМЕНИ	☑
при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	☑
⊟ **Верифицировать идентификаторы ПОСЕТИТЕЛЕЙ**	
при проходе	☑
при проходе с НАРУШЕНИЕМ ВРЕМЕНИ	☑
при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	☑
Время ожидания подтверждения при верифицикации	5 сек.

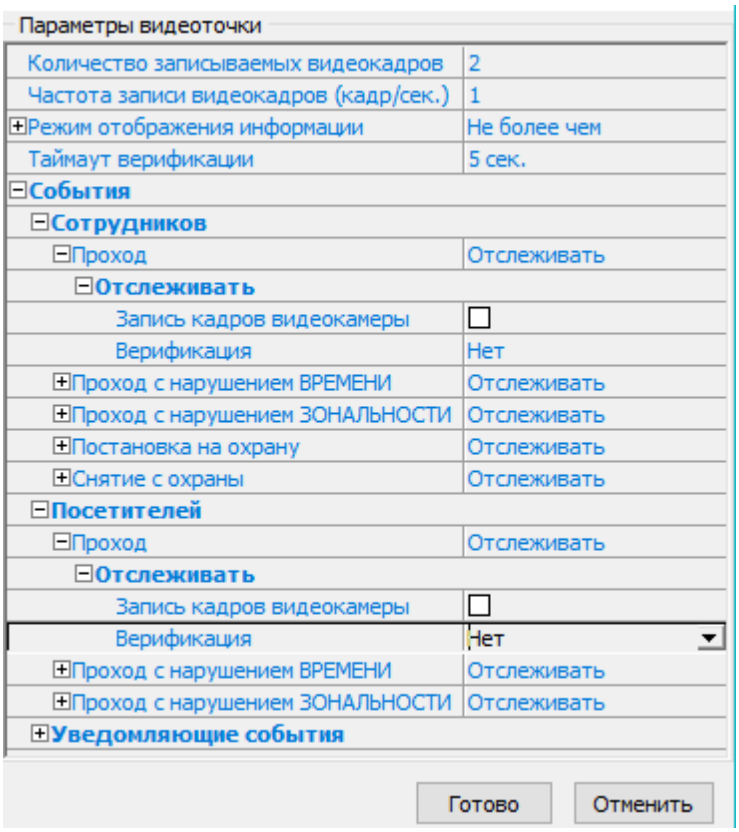
2. Отметьте флажками события, связанные с предъявлением идентификаторов сотрудниками (учениками), для которых требуется подтверждение от ПДУ.

3. Установите требуемое значение параметра **Время ожидания подтверждения при верификации** от ПДУ. По истечении этого времени запрос будет автоматически отклонен.
4. Нажмите кнопку **Передать измененные параметры** на панели инструментов раздела. Измененные параметры будут переданы в контроллер, к которому подключен считыватель.

Примечание:

При установке значения **Да** для параметра считывателя **Подтверждение от ДУ> в режиме «Контроль»** подтверждение прохода от ПДУ для отмеченных событий будет требоваться независимо от того, открыт раздел ***«Верификация»*** или нет.

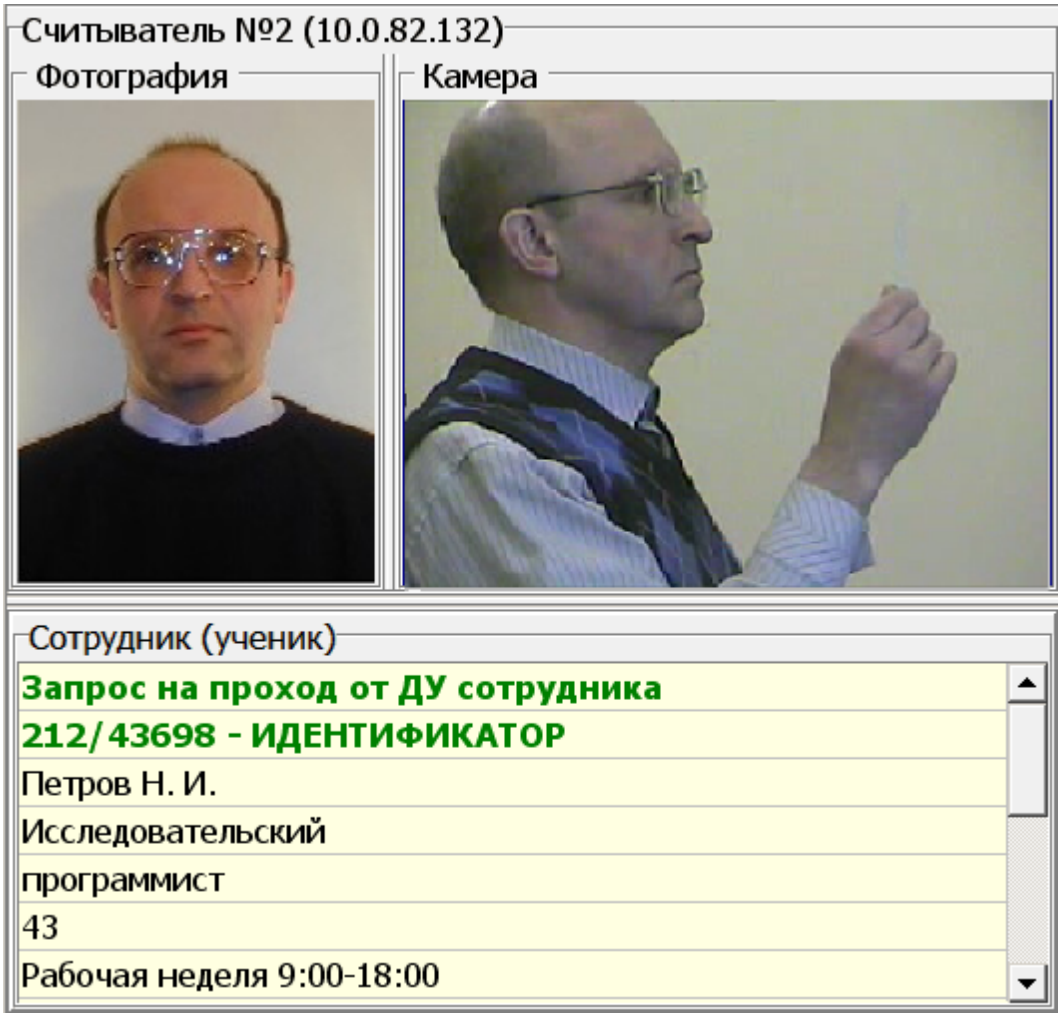
5. Перейдите в раздел ***«Верификация»***. Нажмите кнопку **Изменить состав** на панели инструментов раздела. Откроется окно **Конфигурация верификация** (вкладка **Считыватели**).
6. Выделите в рабочей области окна считыватель точки верификации, при предъявлении карты которому требуется подтверждение от ПДУ.
7. На панели **Параметры видеоточки** для всех видов отслеживаемых событий в раскрывающихся многоуровневых списках **События> Сотрудников** установите для параметра **Верификация** значения **Нет**:



Примечание:

Контроль за предъявлением карт доступа в режиме верификации для выбранного считывателя может осуществляться только из одного раздела ***«Верификация»***. Невозможно организовать несколько рабочих мест операторов раздела ***«Верификации»***, контролирующих одновременно одну точку верификации.

8. Нажмите кнопку **ОК**. Окно **Конфигурация верификации** будет закрыто. Кнопки **Разрешить, Запретить** будут скрыты. Панель точки верификации в рабочей области окна раздела примет следующий вид:



9. При необходимости произведите аналогичные действия для второй точки верификации, связанной со вторым считывателем, подключенным к тому же контроллеру.

6 Раздел «Журнал верификации»

6.1 Назначение

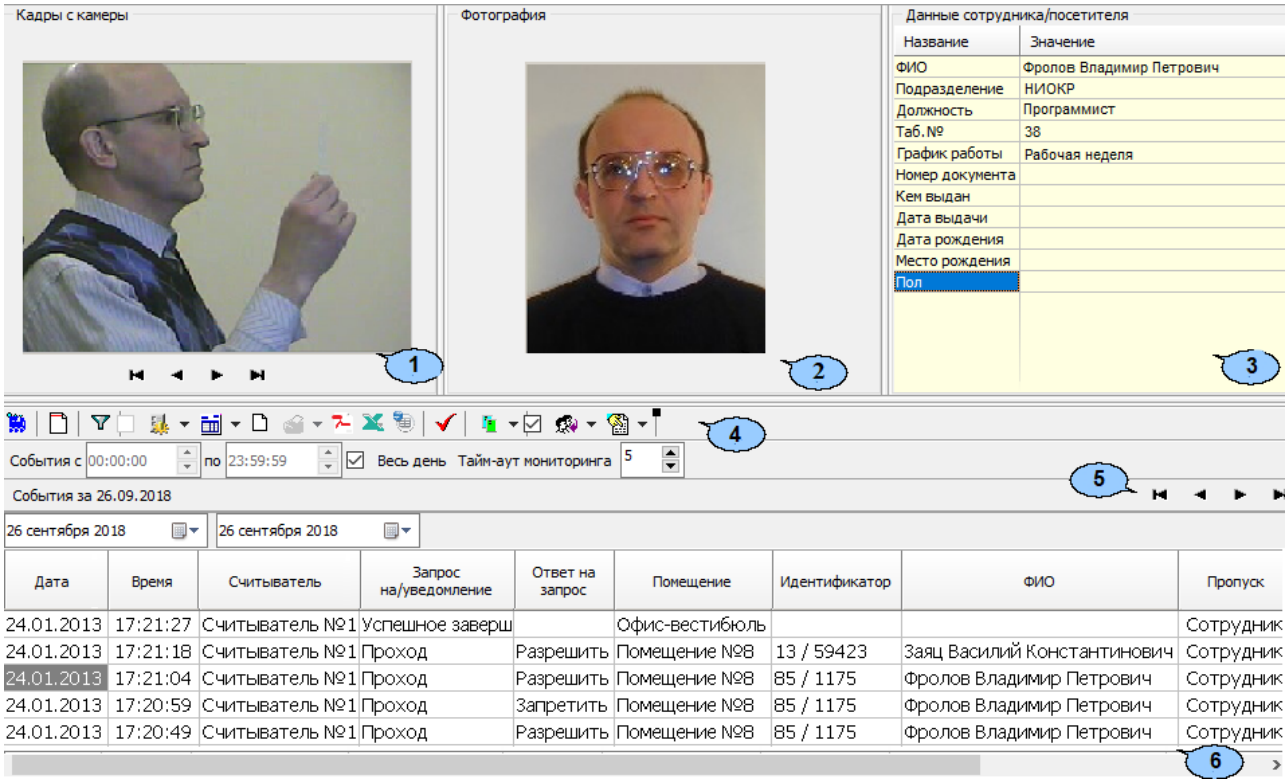
Раздел ***«Журнал верификация»*** предназначен для составления отчетов о событиях, зарегистрированных при работе раздела ***«Верификация»*** и действиях операторов. К отчету могут быть приложены кадры с камеры и фотографии владельцев предъявленных карт доступа.

Внимание!

В разделе ***«Журнал верификация»*** события сохраняются только при работе с разделом ***«Верификация»***. То есть раздел должен быть открыт.

6.2 Рабочее окно раздела

Рабочее окно раздела имеет следующий вид следующих элементов:

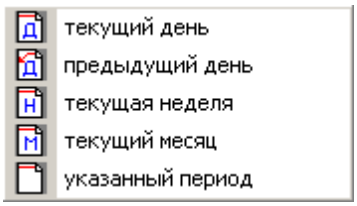


1. Панель **Кадры с камеры** предназначена для отображения кадров записанных для события, выделенного в рабочей области раздела. Рядом с наименованием панели отображается информация о времени записи кадра и его порядковом номере. В нижней части панели расположены кнопки перехода между кадрами:
   - – первый кадр,
   - – предыдущий кадр,
   - – следующий кадр,
   - – последний кадр.
2. Панель **Фотография** предназначена для отображения фотографии из базы данных системы для сотрудника (ученика) предъявившего карту доступа.
3. Панель **Данные сотрудника/ученика** предназначена для отображения учетных данных.

4. Панель инструментов раздела:

/ **Запустить/ Остановить мониторинг** – кнопка позволяет включить/ отключить автоматическое обновление списка событий в рабочей области раздела. При включенном автоматическом обновлении показ кадров с камер не производится

Период– при нажатии кнопки открывается контекстное меню, позволяющее выбрать периода времени, события за который будут отображены в рабочей области раздела:



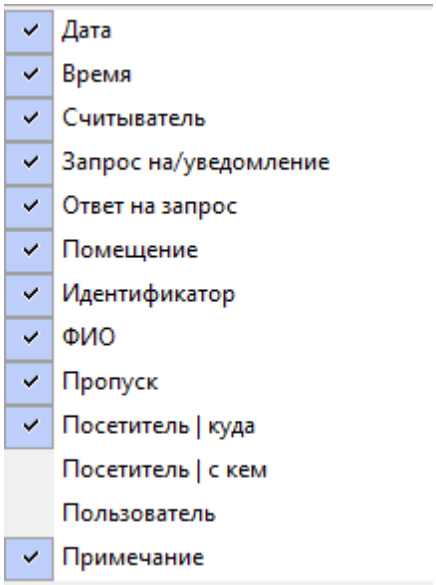
Дополнительные условия выборки – кнопка позволяет построить выборку (фильтровать) из событий отображенных в рабочей области раздела. Для отмены построенной выборки необходимо снять флажок справа от кнопки.

Выборка по событиям – при нажатии стрелки справа от кнопки откроется контекстное меню со списком типов событий. В рабочей области отображаются события отмеченные флажками.

- ✓ Проход
- ✓ Проход с нарушением ВРЕМЕНИ
- ✓ Проход с нарушением ЗОНАЛЬНОСТИ
- ✓ Проход с нарушением ВРЕМЕНИ и ЗОНАЛЬНОСТИ
- ✓ Постановка на охрану
- ✓ Снятие с охраны
- ✓ Постановка на охрану с нарушением ВРЕМЕНИ
- ✓ Постановка на охрану с нарушением ЗОНАЛЬНОСТИ
- ✓ Постановка на охрану с нарушением ВРЕМЕНИ и ЗОНАЛЬНОСТИ
- ✓ Проход разрешен
- ✓ Нарушение ВРЕМЕНИ
- ✓ Нарушение ЗОНАЛЬНОСТИ
- ✓ Нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ
- ✓ Попытка постановки на охрану с нарушением ВРЕМЕНИ
- ✓ Попытка постановки на охрану с нарушением ЗОНАЛЬНОСТИ
- ✓ Попытка постановки на охрану с нарушением ВРЕМЕНИ и ЗОНАЛЬНОСТИ
- ✓ Попытка снятия с охраны с нарушением ВРЕМЕНИ
- ✓ Попытка снятия с охраны с нарушением ЗОНАЛЬНОСТИ
- ✓ Попытка снятия с охраны с нарушением ВРЕМЕНИ и ЗОНАЛЬНОСТИ
- ✓ Идентификатор НЕ ЗАРЕГИСТРИРОВАН
- ✓ Идентификатор ЗАБЛОКИРОВАН
- ✓ Идентификатор ПРОСРОЧЕН
- ✓ Нарушение режима доступа
- ✓ Не удалось подключиться к контроллеру
- ✓ Не удалось выполнить команду установки режима верификации контроллера
- ✓ Не удалось зарегистрировать верификацию (занято другим ПК)
- ✓ Успешный запуск верификации/индикации
- ✓ Успешное завершение сеанса верификации/индикации
- ✓ Контроллер прервал подключение
- ✓ Восстановление подключения
- ✓ Отказ в верификации: нет прав на работу с контроллером
- ✓ Отказ в верификации: контроллер отключен в разделе КОНФИГУРАТОР
- ✓ Взлом ИУ
- ✓ Проход от ДУ
- ✓ Запрос прохода от ДУ
- ✓ Ожидание комиссионирования прохода
- ✓ Нарушение комиссионирования (запрет прохода)
- ✓ ВНИМАНИЕ: на диске видеоархива менее 1Гб. При достижении 500Мб запись будет прекращена.
- ✓ На диске видеоархива менее 500Мб. Запись прекращена.
- ✓ Расположение видеоархива в "Единая система безопасности PERCo-S-20" не задано.
- ✓ Запись кадров невозможна, т.к. запись на диск видеоархива запрещена в Windows.
- ✓ Отпечаток НЕ ЗАРЕГИСТРИРОВАН или НЕ РАСПОЗНАН
- ✓ Снятие с охраны с нарушением ВРЕМЕНИ
- ✓ Снятие с охраны с нарушением ЗОНАЛЬНОСТИ
- ✓ Снятие с охраны с нарушением ВРЕМЕНИ и ЗОНАЛЬНОСТИ

Отключить все

Настройка столбцов таблицы – при нажатии на стрелку справа от кнопки откроется контекстное меню, содержащее список заголовков столбцов рабочей области раздела. Столбцы, заголовки которых отмечены флажками отображаются в рабочей области:



Посмотреть область листа для печати – при нажатой кнопки будет показана приблизительная область печати с помощью мигающих значков для книжной и альбомной ориентации страниц в столбцах, которые ограничивают область печати.

Печать отчетов – при нажатии на стрелку справа от кнопки откроется контекстное меню, позволяющее выбрать тип печатаемого отчета:

- **Отчет о событиях** – список всех событиях, отображенных в рабочей области раздела.
- **Отчет о событии** – подробный отчет об одном событии, выделенном в рабочей области раздела. Отчет включает фотографию сотрудника (ученика), если они доступны для выбранного события.

После выбора типа отчета откроется окно предварительного просмотра и печати.

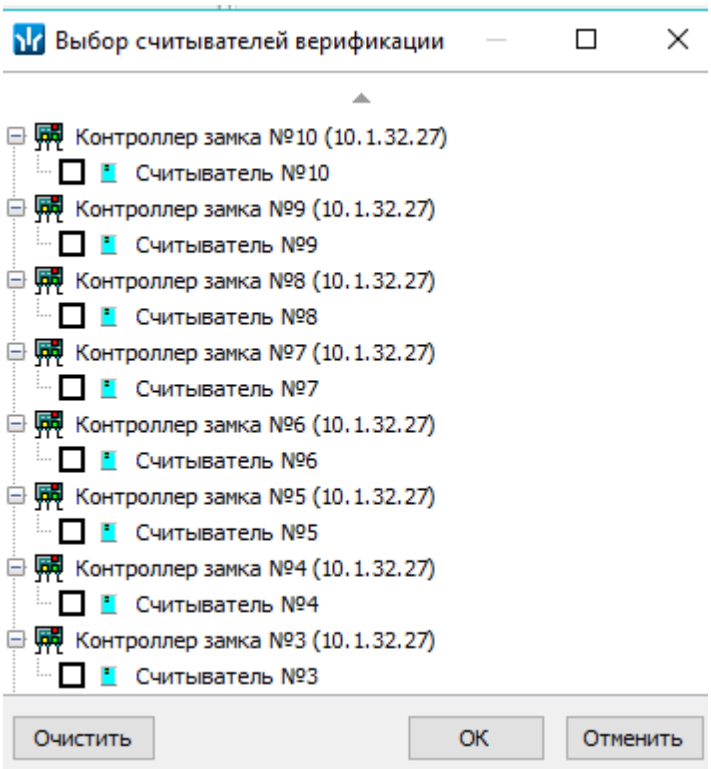
Экспорт отчета о событии в формат PDF – кнопка позволяет сохранить данные о событии, выделенном в рабочей области раздела, включая кадры с камер и фотографию владельца предъявленной карты в файле с расширением `pdf`.

Экспорт в Excel (**Ctrl+Y**) – кнопка позволяет сохранить список событий верификации, отображаемый в рабочее области, в файле с расширением `.xls`.

Экспорт в OpenOffice Calc – кнопка позволяет сохранить список событий верификации, отображаемый в рабочей области, в файле с расширением `.ods`.

Обновить (**Ctrl+R**) – кнопка позволяет обновить список событий в рабочей области раздела после изменения периода отчета, времени в течении суток или для актуализации отчета.

Выбор считывателей – при нажатии кнопки откроется окно **Выбор считывателей верификации**. В окне будет отображаться список контроллеров с подключенными к ним считывателями:



Отметьте флажками считыватели события, связанные с которыми должны отображаться в рабочей области раздела.

Выбор считывателей – при нажатии стрелки справа от кнопки открывается меню, позволяющее включить/исключить считыватели, отмеченные в окне **Выбор считывателей верификации,** из условий выборки.

Применить/отменить фильтр по считывателям – при помощи флажка справа от кнопки **Выбор считывателей** применяются/отменяются заданные условия выборки событий по считывателям.

Выборка по пользователям – при нажатии на стрелку справа от кнопки откроется контекстное меню, содержащее список операторов раздела. В рабочей области раздела отображаются события, зарегистрированные в период активности отмеченных флажками операторов.

События с 00:00:00 по 23:59:59 – поля ввода времени начала и окончания периода времени, за который отображаются события в рабочей области. Поля не доступны при установленном флажке **Весь день**.

Весь день – при установке флажка в рабочей области будут отображаться события независимо от времени.

Тайм-аут мониторинга – счетчик позволяет указать частоту автоматического обновления списка событий в рабочей области раздела.

5. Кнопки перемещения по списку событий:
   – переход к первому событью списка,
   – переход к предыдущему событью в списке,
   – переход к следующему событью в списке,
   – переход к последнему событью списка.
6. Рабочая область раздела содержит список событий зарегистрированных при работе раздела ***«Верификация»***.

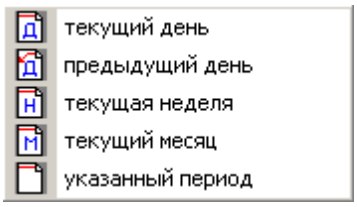
Примечание:

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

6.3 Формирование отчета

Для составления отчета о зарегистрированных событиях:

1. Укажите период, за который необходимо составить отчет. Для этого на панели инструментов раздела нажмите кнопку **Период**. Откроется меню для выбора периода:



2. В открывшемся меню выберите нужный период.
3. При выборе пункта **Указанный период** откроется дополнительная панель с полями ввода даты начала и окончания периода:

4. При необходимости сужения интервала времени в течение суток снимите флажок **Весь день** и укажите промежуток времени с помощью полей ввода времени **События с... по...**.
5. При необходимости используйте другие инструменты фильтрации событий.
6. Нажмите кнопку **Обновить** на панели инструментов раздела. В рабочей области раздела список событий будет обновлен.
7. При необходимости распечатайте список событий или экспортируйте в файл.

6.4 Настройки выборки

Дополнительные условия выборки

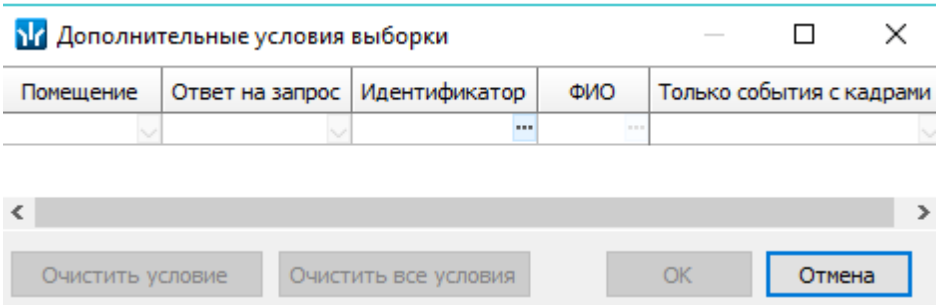
Доступны следующие условия выборки:

- **Помещение** – поиск событий, связанных с проходом в выбранное с помощью раскрывающегося списка помещение. Список помещений задается в разделе «***Помещения***».
- **Ответ на запрос** (Разрешить/ Запретить/ Без подтверждения) – поиск событий, связанных с конкретным ответом верификации на запрос от считывателя.
- **Идентификатор** – поиск событий, связанных с проходом по определенной карте доступа.
- **ФИО** – поиск событий, связанных с конкретным сотрудником (учеником). Удаленные на момент построения выборки сотрудники (ученики) выделяются в списке красным цветом:
- **Только события с кадрами** (Да/Нет) – поиск событий, которые были зафиксированы кадрами с видеокамер.

Порядок построения выборки

Для настройки дополнительных условий выборки:

1. Нажмите кнопку **Дополнительные условия выборки** в панели инструментов раздела. Откроется окно **Дополнительные условия выборки**:



2. Настройте условия выборки, используя кнопки или . Для удаления выделенного условия используйте кнопку **Очистить условие**, для удаления всех установленных условий используйте кнопку **Очистить все условия**.
3. Для применения условий выборки нажмите кнопку **OK**. Окно будет закрыто. События, соответствующие условиям выборки, будут отображены в рабочей области раздела. Для закрытия окна без применения выборки нажмите кнопку **Отмена**.
4. Для отмены применения выборки снимите флажок справа от кнопки **Дополнительные условия выборки.**

7 Раздел «SMS-биллинг»

7.1 Назначение

Раздел ***«SMS-биллинг»*** предназначен для создания биллинговой системы (автоматизированной системы расчетов) поддержки услуги *«SMS-уведомление родителей»* в рамках системы безопасности ***PERCo-S-20 «Школа»***.

Раздел ***«SMS-биллинг»*** предоставляет оператору следующие возможности:

- производить пополнение или списание средств со счетов абонентов вручную;
- производить пополнение средств на счетах абонентов, используя импорта данных из файла *MS Office Excel*;
- задавать индивидуально для каждого счета дату списания абонентной платы;
- установить период времени для автоматической отправки служебных SMS-сообщений абоненту с уведомлением о недостатке средств на его счету для списания абонентной платы, а также содержание таких сообщений;
- установить максимальное количество SMS-сообщений, которое может быть отправлено в течение одного месяца;
- задать текст служебного SMS-сообщения, которое будет автоматически отправлено абоненту в случае достижения им установленного максимального количества SMS-сообщений за текущий месяц;
- установить дату, после которой в случае пополнения счета не будет происходить автоматического списания средств до начала следующего учетного периода.

Примечание:

Служебные SMS-сообщения, а также сообщения, отправленные из раздела ***«Сотрудники и ученики»***, в SMS-биллинге не учитываются.

7.2 Используемые термины

В разделе используются следующие понятия:

Абонент – пользователь услуги *«SMS-уведомление родителей»,* на чей телефонный номер отправляется SMS-сообщение с уведомлением.

Услуга ***SMS-уведомление родителей*** – заключается в отправке SMS–сообщений с уведомлением о входе и выходе ученика из школы, о неприбытии ученика или о каких-либо планируемых в школе мероприятиях. С каждым учеником можно связать один или несколько телефонов, по которым будут отправляться SMS-уведомления.

Примечание:

Для пользования услугой необходимо, чтобы в разделе ***«Сотрудники и ученики»*** для ученика был задан хотя бы один телефонный номер и этот номер был отмечен как активный. Кроме этого, в разделе ***«Планировщик заданий по отправке SMS»*** ученик должен быть добавлен хотя бы в одно активное задание по отправке SMS-сообщений.

Абонентная плата – плата, вносимая абонентом за право пользования услугой *«SMS-уведомление родителей»*. Величина абонентной платы может быть установлена независимо для каждого абонента. Абонентная плата списывается со счета абонента автоматически один раз в течение одного учетного периода (месяца):

- в первый день учетного периода (если на счету достаточно средств);
- в течение учетного периода (при поступлении достаточного количества средств на счет);
- при включении услуги *«SMS-уведомление родителей».*

Примечание:

Система позволяет задать определенное количество дней до конца учетного периода, в течение которых при поступлении достаточного количества средств на счет абонента автоматического списания абонентной платы производиться не будет.

Счет – учетная запись, связанная с телефонным номером абонента. Если в разделе ***«Сотрудники и ученики»*** для ученика введено несколько телефонных номеров, то для каждого телефонного номера (каждого абонента) будет создан отдельный счет. Также, если для нескольких учеников будет указан один и тот же телефонный номер для отправки SMS, то для каждого ученика тоже будет создан отдельный счет. С каждым счетом связаны следующие параметры:

- размер абонентной платы;
- дата начала учетного периода;
- дата последнего списания абонентной платы;
- остаток средств, доступных для списания абонентной платы;
- количество SMS-сообщений, отправленных за текущий учетный период;
- максимальное количество SMS-сообщений, которое может быть отправлено в течение одного учетного периода, максимальное количество может быть не ограничено;
- даты отправки служебных SMS-сообщений с уведомлением о недостатке средств на счету для списания абонентной платы за следующий учетный период.
- даты отправки служебных SMS-сообщений с уведомлением о достижении максимального количества SMS-сообщений за учетный период;
- дата окончания отправки SMS-сообщений в кредит.

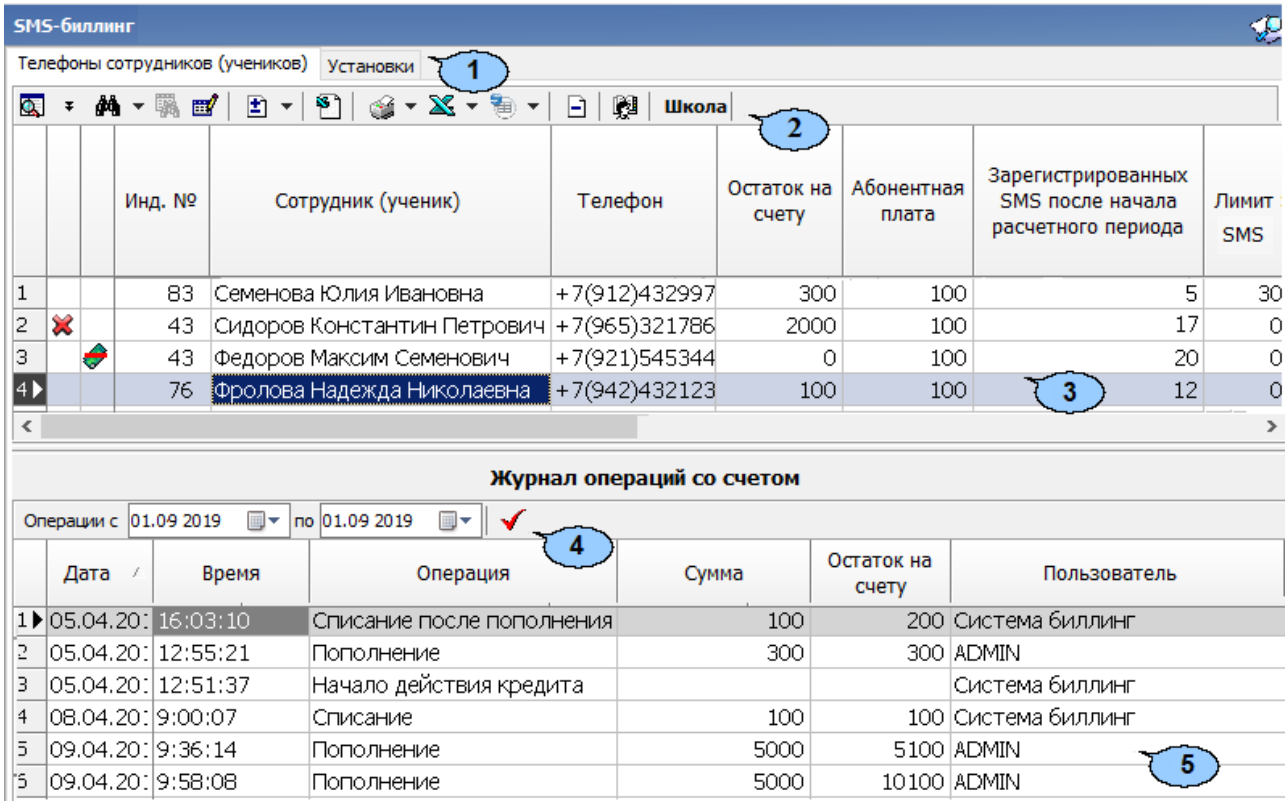
Отправка SMS-сообщений в кредит – отправка SMS-сообщений на номер абонента не прекращается в течение установленного (отличного от нуля) количества дней после неудачной попытки автоматического списания абонентной платы при недостатке средств на счету абонента. Кредит автоматически предоставляется в следующих случаях:

- в начале учетного периода;
- при добавлении нового абонента (создании счета для нового активного телефона);
- при активизации телефона;
- при добавлении ученика в новое задание по отправке SMS-сообщений или активизации задания.

Журнал операций со счетами – история списаний и пополнений средств на счетах абонентов с указанием того, были эти операции произведены автоматически биллинговой системой или оператором.

7.3 Рабочее окно раздела

Вкладка предназначена для отслеживания состояния счетов абонентов и просмотра журнала операций со счетами. Рабочее окно раздела имеет следующий вид:



1. Выбор вкладки раздела:
   - **Телефоны сотрудников (учеников);**
   - **Установки**.
2. Функциональные кнопки раздела:

   Общий поиск сотрудника (ученика) (**Shift+Ctrl+F**) – кнопка позволяет произвести поиск сотрудника (ученика) по всем подразделениям.

   / **Показать/Скрыть результаты общего поиска** – кнопки позволяют открыть или скрыть панель с результатами общего поиска.

   Поиск – при нажатии стрелки справа от кнопки открывается меню позволяющее выбрать тип поиска в выбранном подразделении:
   - **быстрый поиск**;
   - **поиск с выбором**.

   Применить/Отменить выборку (**Shift+Ctrl+O**) – кнопка позволяет показать/скрыть результат применения выборки в рабочей области вкладки.

   Настроить выборку (**Ctrl+O**) – кнопка позволяет настроить фильтр данных, отображаемых в рабочей области вкладки.

   Изменить параметры, счета телефонов – при нажатии стрелки справа от кнопки открывается меню, позволяющее указать абонентов, для которых будут изменены параметры счетов.

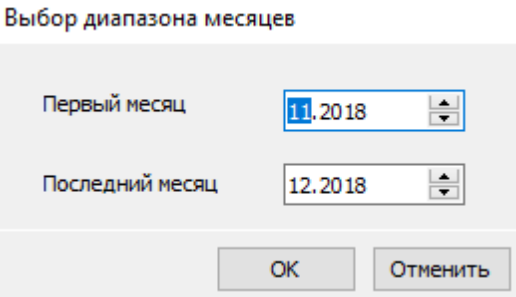
   Пополнение счетов с помощью импорта из файла MS Excel – кнопка позволяет произвести пополнение счетов с помощью импорта данных о суммах пополнения из заранее подготовленного файла *MS Excel*.

Печать информации системы биллинга – при нажатии стрелки справа от кнопки открывается меню, позволяющее указать, какие данные необходимо распечатать. После выбора нужного пункта будет открыто окно предварительного просмотра данных для печати.

Экспорт в MS Excel – при нажатии стрелки справа от кнопки открывается меню, позволяющее указать, какие данные необходимо экспортировать в файл *MS Office Excel*.

Экспорт в OpenOffice Calc – при нажатии стрелки справа от кнопки открывается меню, позволяющее указать, какие данные необходимо экспортировать в файл *OpenOffice Calc*.

Удалить операции из журнала – кнопка позволяет удалить записи **Журнала операций со счетом** за указанный период в открывающемся окне **Выбор диапазона месяцев**:



Удаление операций текущего месяца запрещено.

Выбор подразделения (**Ctrl+B**) – кнопка позволяет выбрать подразделение, ученики (сотрудники) которого будут отображаться в рабочей области раздела. Справа от кнопки отображается название выбранного в данный момент подразделения.

3. Рабочая область вкладки **Список телефонов учеников сотрудников (учеников)** выбранного на панели управления подразделения. Список абонентов создается автоматически из учеников (сотрудников), для которых заданы один или несколько телефонных номеров и создано хотя бы одно задание по отправке SMS-сообщений.

   Значок во втором столбце рабочей области означает, что на счету абонента недостаточно средств для списания абонентной платы.

   Значок в первом столбце рабочей области означает, что отправка SMS-сообщений абоненту невозможна. При наведении курсора на значок будет отображена одна из следующих причин:

   - **Телефон неактивен** – в разделе ***«Сотрудники и ученики»*** телефон данного абонента не отмечен как активный.
   - **Телефона нет в активных заданиях** – в разделе ***«Планировщик заданий по отправке SMS»*** ученик (сотрудник) не добавлен ни в одно задание по отправке SMS-сообщений, либо эти задания неактивны.
   - **Нет списания в текущем месяце и нет кредита** – абонент не внес на счет в текущем месяце абонентную плату и при этом срок рассылки SMS-сообщений в кредит не был предоставлен.
   - **Нет списания в текущем месяце, кредит окончен** – абонент не внес на счет в текущем месяце абонентную плату и при этом срок рассылки SMS-сообщений в кредит истек.

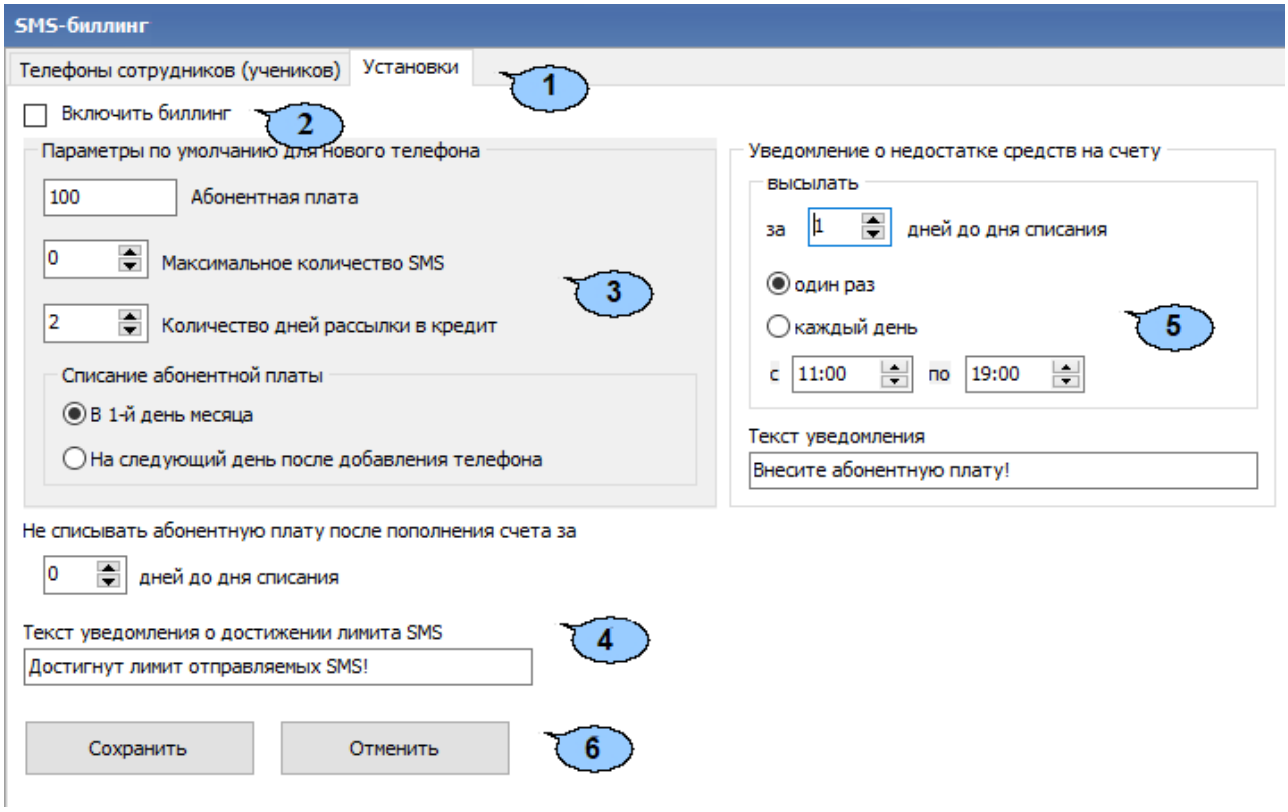
Примечание:

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

4. Панель инструментов журнала операций со счетом.
   Операции с... по... – Поля ввода дат позволяют установить период, за который будут отображаться записи **Журнала операций со счетом**.
   Получить – кнопка позволяет обновить записи **Журнала операций со счетом** в соответствии с указанным периодом.
5. **Журнал операций со счетом** выбранного в рабочей области абонента за указанный на панели инструментов журнала период.

7.4 Вкладка «Установки»

Вкладка предназначена для изменения общих параметров биллинговой системы и параметров счетов абонентов назначаемых по умолчанию. Рабочее окно вкладки имеет следующий вид:



1. Выбор вкладки раздела:
   - **Телефоны сотрудников (учеников)**;
   - **Установки.**
2. Флажок **Включить биллинг**. При установленном флажке биллинговая система включена. Любое SMS-сообщение, сгенерированное в разделе ***«Планировщик заданий по отправке SMS»***, может быть отправлено на телефон абонента только если выполнены следующие условия:
   - В текущем месяце была списана абонентная плата. Или абонентная плата не была списана, но не истекло установленное количество дней рассылки SMS-сообщений в кредит.

- Количество SMS-сообщений, которое может быть отправлено на телефонный номер абонента в течение месяца, не достигло установленного максимального значения (лимита).

При снятом флажке биллинговая система отключена. Отправка SMS-сообщений осуществляется без проверки параметров счетов абонентов.

3. Область **Параметры по умолчанию для нового телефона** содержит параметры счетов, задаваемые по умолчанию для новых абонентов.

   Абонентная плата за месяц – плата, ежемесячно снимаемая со счета абонента.

   Максимальное количество SMS в месяц – при достижении максимального количества отправка SMS-сообщений прекращается. При установке значения параметра «**0**», количество отправленных SMS-сообщений не контролируется.

   Количество дней рассылки в кредит – количество дней первой неуспешной попытки списания абонентной платы, в течение которых SMS-сообщения будут отправляться абоненту.

   Списание абонентной платы – переключатель позволяет выбрать день списания абонентной платы:
   - **в 1-й день месяца** – абонентная плата списывается в первый день каждого месяца.
   - **На следующий день после добавления телефона** – абонентная плата списывается на следующий день после добавления задания по отправки SMS.

4. **Не списывать абонентную плату после пополнения счета за ... дней до конца месяца** – счетчик позволяет установить количество дней в конце месяца, в течение которых абонентная плата за текущий месяц при ее несвоевременном внесении со счета списана не будет. Внесенные в этот период средства будут сняты в качестве абонентной платы в начале следующего месяца.

   Текст уведомления о достижении лимита SMS в месяц – поле ввода позволяет задать текст служебного SMS-сообщения с уведомлением о достижении максимального количества сообщений, которое может быть отправлено в течение месяца.

5. Область **Уведомление о недостатке средств на счету высылать** содержит параметры отправки служебных SMS-сообщений с уведомлением в случае недостатка средств на счету для списания абонентной платы за следующий месяц.

   за...дней до конца месяца – счетчик позволяет задать количество дней до конца месяца, за которое необходимо отправить служебное SMS-сообщение.

   один раз/ каждый день – переключатель позволяет указать, будет ли SMS-сообщение с уведомлением о недостатке средств на счету отправлено однажды или будет отправляться каждый день до конца текущего месяца.

   с... по... – поля ввода времени позволяют указать временной интервал, в течение которого может быть отправлено служебное SMS-сообщение с уведомлением о недостатке средств на счету.

   Текст уведомления – поле ввода позволяет задать текст уведомления служебного SMS-сообщение о недостатке средств на счету.

6. Кнопки **Сохранить** и **Отменить** становятся активными после изменения любого параметра. При нажатии кнопки **Сохранить** измененные параметры будут сохранены. При нажатии кнопки **Отменить** будут возвращены параметры, установленные ранее.

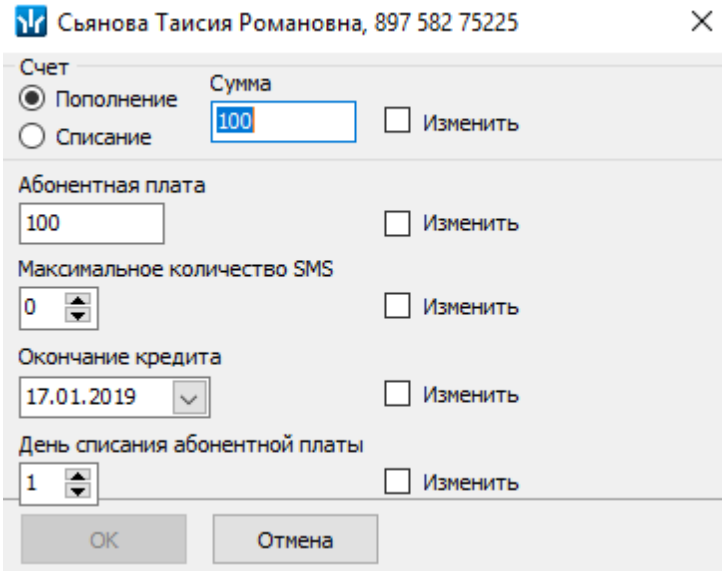
7.5 Операции со счетами абонентов

Оператор имеет возможность вручную производить пополнение и списание средств со счетов, а также изменять заданные по умолчанию параметры счетов для одного или нескольких абонентов. Для этого:

1. Выделите в рабочей области один или несколько счетов (телефонов), используя кнопки **Ctrl**, **Shift** на клавиатуре или поиск с выбором.
2. На панели инструментов раздела нажмите стрелку справа от кнопки **Изменить параметры, счета телефонов** . В открывшемся меню выберите:
   - **Выделенного** – если необходимо внести изменения в счет одного абонента. Если выделено несколько абонентов, изменения будут внесены только в счет того, кто был выделен последним.
   - **Выбранных** – если необходимо внести изменения в счета всех выделенных абонентов.
   - **Всех** – если необходимо внести изменения в счета всех абонентов выбранного подразделения.
3. Откроется окно **Изменение счетов, параметров рассылки** (если выбран один абонент, в заголовке окна будет указано его ФИО):

Примечания:

- В окне **Изменение счетов, параметров рассылки** отображаются параметры выделенного счета. Если выделено несколько счетов, то в окне отображаются параметры, заданные на вкладке **Установки**.
- В поле ввода **Сумма** автоматически заносится размер абонентной платы.



Счет – используя переключатель **Пополнение**/**Списание** и поле ввода **Сумма** блока **Счет** оператор может внести/снять с выделенных счетов необходимую сумму.

Абонентная плата – поле ввода позволяет изменить абонентную плату для выбранных счетов.

Максимальное количество SMS – счетчик позволяет изменить максимальное число отправляемых в месяц SMS-сообщений, для выбранных счетов. При установке значения параметра «**0**» количество отправленных SMS-сообщений не контролируется.

Окончания кредита – счетчик позволяет изменить количество дней после начала календарного месяца, в течение которых SMS-сообщения на номер абонента будут отправляться даже если на его счету недостаточно средств для списания абонентной платы.

День списания абонентной платы – счетчик позволяет установить день месяца, в который автоматически списывается абонентная плата.

Примечание:

При изменении значения параметра **День списания абонентной платы** возможно списание абонентной платы за неполный месяц.

4. В открывшемся окне внесите необходимые изменения. При изменении любого параметра соответствующий флажок **Изменить** будет установлен. Или вручную установите флажки у тех параметров, которые необходимо сохранить. Нажмите кнопку **ОК**, которая станет доступна после установки хотя бы одного флажка. Окно **Изменение счетов, параметров рассылки** будет закрыто, внесенные изменения будут сохранены для выделенных абонентов.

7.6 Пополнение счетов с помощью импорта из файла MS Office Excel

Система позволяет произвести пополнение счетов с помощью импорта из заранее подготовленного файла *MS Excel*.

Создание списка телефонов

Предварительно нужно сформировать список телефонов (счетов) и указать в этом списке, какие суммы необходимо внести на счета абонентов. Для этого:

1. Нажмите стрелку справа от кнопки **Экспорта в MS Excel** и выберите пункт **Список телефонов для пополнения счетов**. Откроется окно **Экспорт данных в файл Excel**.
2. В открывшемся окне укажите место на диске, куда необходимо сохранить файл, и при необходимости измените имя файла. После этого нажмите кнопку **Сохранить**. Окно **Экспорт данных в файл Excel** будет закрыто.
3. В открывшемся окне с сообщением об успешном завершении экспорта нажмите кнопку **ОК.** Список телефонов будет сохранен в указанном месте:

	A	B	C	D
1	**Фамилия**	**Имя**	**Телефон**	**Сумма**
2	Сьянова	Таисия	79758275225	0
3	Алиева	Яна	79583236363	0
4	Яковченко	Алексей	79638521525	0
5	Лавров	Борислав	73652365858	0

4. В созданном файле в столбце **Сумма** укажите суммы, которые необходимо внести на счета соответствующих абонентов. Сохраните внесенные в файл изменения.

Внимание!

Добавление новых учеников (сотрудников) или изменение телефонов непосредственно в созданном файле недопустимо. Все изменения должны производиться в соответствующем разделе ПО.

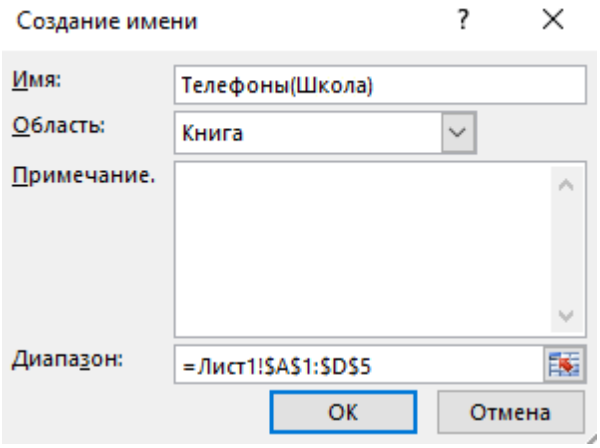
Подготовка файла к импорту

После ввода сумм пополнения счетов необходимо произвести подготовку файла для импорта**.**

1. Откройте ранее созданный файл со списком телефонов и указанием вносимых сумм в приложении *MS Office Excel*. Первая строка данных таблицы должна содержать имена столбцов переносимых данных, как в ранее подготовленном файле.
2. Выделите область импортируемых данных:

	A	B	C	D
1	**Фамилия**	**Имя**	**Телефон**	**Сумма**
2	Сьянова	Таисия	7975827522	150
3	Алиева	Яна	79583236363	200
4	Яковченко	Алексей	79638521525	200
5	Лавров	Борислав	73652365858	100
6				

3. Присвойте наименование выделенному диапазону ячеек. Для этого выберите в главном меню программы пункт **Формулы**. На открывшейся панели инструментов нажмите кнопку **Диспетчер имен**. Откроется окно **Диспетчер имен.**
4. В открывшемся окне нажмите кнопку **Создать**…. Откроется окно **Создание имени**:



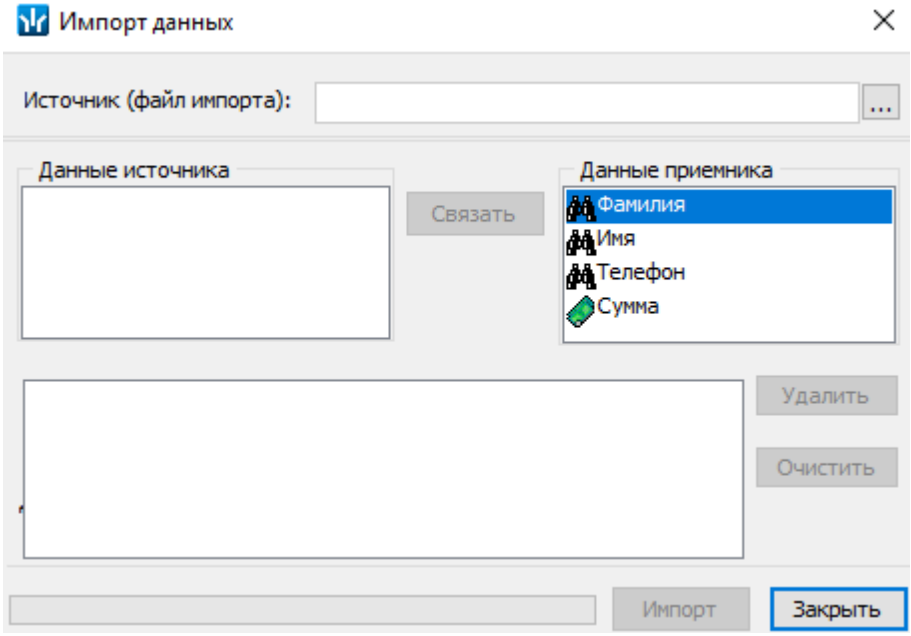
5. В окне **Создание имени** введите наименование диапазону ячеек в поле **Имя**. Имя может быть произвольным, например *«Телефоны(Школа)».*
6. Нажмите кнопку **OK**. Окно **Создание имени** будет закрыто. В рабочей области окна **Диспетчер имен** появится строка с указанным названием.
7. Нажмите кнопку **Закрыть**, окно будет закрыто.
8. Сохраните файл и закройте его. Файл готов для импорта данных.

Примечание:

Если в книге *MS Office Excel* имеется несколько сохраненных областей, то при импорте система потребует оставить только одну из них, а остальные удалить. Для удаления сохраненной области в окне **Присвоение имени** выделите имя области, которую необходимо удалить и нажмите кнопку **Удалить**.

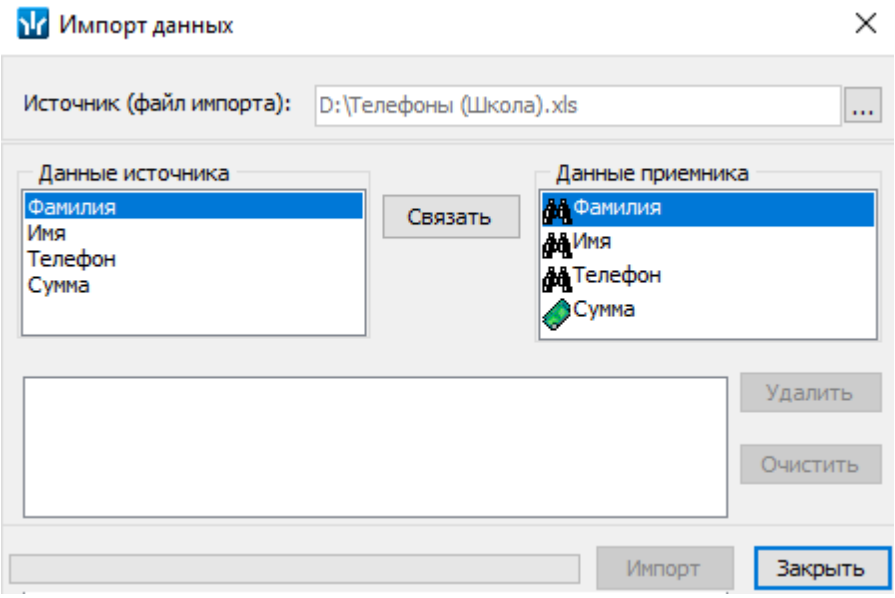
Импорт списка телефонов

1. Нажмите кнопку **Пополнение счетов с помощью импорта из Excel-файла** на панели инструментов раздела. Откроется окно **Импорт данных**:

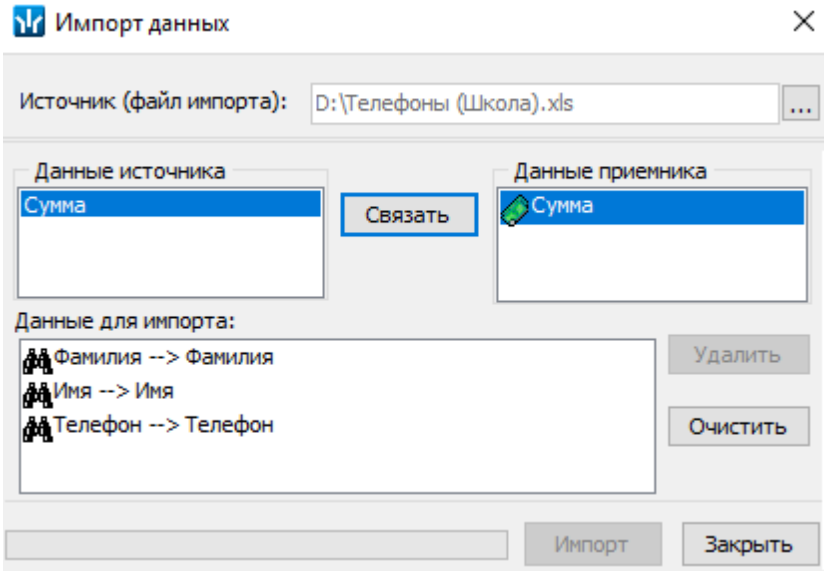


Список **Данные приемника** содержит обязательные для импорта поля с заголовками импортируемых данных: **Фамилия**, **Имя**, **Телефон** и **Сумма**.

2. В открывшемся окне нажмите кнопку ... . Откроется окно **Файл импорта данных**.
3. Укажите в открывшемся окне место расположения сохраненного файла *MS Office Excel* с суммами пополнения счетов и нажмите кнопку **Открыть**. Список **Данные источника** окна **Импорт данных** заполнится заголовками столбцов с данными, импортируемыми из сохраненной области файла *MS Office Excel*:



4. Выберите последовательно в списках **Данные источника** и **Данные приемника** соответствующие друг другу названия столбцов и нажмите кнопку **Связать.** В области **Данные для импорта** при этом будет добавляться пара связанных друг с другом элементов обоих списков.



Примечание:

Кнопка **Удалить** служит для построчного удаления элементов списка **Данные для импорта**, кнопка **Очистить** – для очистки всего списка.

5. Нажмите кнопку **Импорт** для начала импорта данных. Кнопка становится активной после заполнения окна **Данные для иморта** парами связанных друг с другом элементов. При успешном завершении импорта откроется окно с сообщением об успешном завершении импорта. Нажмите **ОК**.
6. Для выхода из окна **Импорт данных** нажмите кнопку **Закрыть.**

7.7 Журнал операций со счетом

В **Журнале операций со счетом** отображаются операции со счетом выбранного в рабочей области раздела абонента, за установленный на панели инструментов журнала период. Рабочая область страницы выглядит следующим образом:

Журнал операций со счетом

Операции с 01.09 2019 по 01.09 2019

	Дата	Время	Операция	Сумма	Остаток на счету	Пользователь
1	05.04.20	16:03:10	Списание после пополнения	100	200	Система биллинг
2	05.04.20	12:55:21	Пополнение	300	300	ADMIN
3	05.04.20	12:51:37	Начало действия кредита			Система биллинг
4	08.04.20	9:00:07	Списание	100	100	Система биллинг
5	09.04.20	9:36:14	Пополнение	5000	5100	ADMIN
6	09.04.20	9:58:08	Пополнение	5000	10100	ADMIN

Для обновления данных журнала после изменения периода используйте кнопку **Получить**.

В столбце **Пользователь** отображается информация о том, кто произвел операцию со счетом:

- Если операция произведена автоматически, то в столбце отображается – **Система биллинга**.
- Если операция произведена оператором, то в столбце отображается имя оператора, под которым он вошел в систему ***PERCo-S-20 «Школа»***.

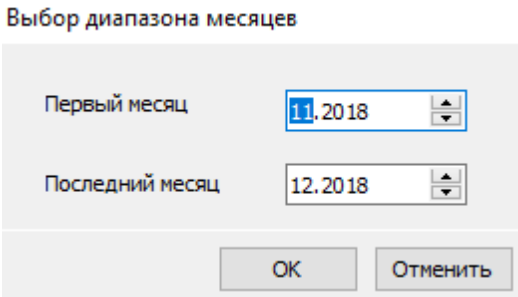
В журнал сохраняется информация о следующих операциях со счетом:

- **Пополнение**. Оператор вручную или с помощью импорта из файла *MS Office Excel* произвел пополнение счета.
- **Списание**. Оператор вручную произвел списание указанной суммы со счета (например, при вводе неправильных данных о пополнении). Или произошло автоматическое списание абонентной платы биллинговой системой в начале месяца.
- **Списание после пополнения**. Произошло автоматическое списание абонентной платы биллинговой системой после пополнения счета, если в начале месяца списание не было произведено.
- **Списание после добавления в задание**: Произошло автоматическое списание абонентной платы биллинговой системой после добавления нового абонента (создания нового счета).
- **Списание после активизации.** Произошло автоматическое списание абонентной платы биллинговой системой после активизации телефона.
- **Начало действия кредита**. Биллинговой системой установлена дата начала отправки SMS-сообщений в кредит.
- **Продление срока действия кредита**. Оператор вручную продлил срок действия кредита.

Удаление данных журнала

Для удаления данных журнала:

1. Нажмите кнопку **Удалить операции из журнала** панели инструментов раздела. После нажатия кнопки откроется окно **Выбор диапазона месяцев** для установки периода:



Удаление операций текущего месяца запрещено.

2. Установите необходимый диапазон и нажатие кнопку **ОК**.

3. В открывшемся окне подтверждения нажмите **Да**.

ООО «ПЭРКо»

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

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

Техническая поддержка:
Call-центр: 8-800-775-37-05 (бесплатно)
Тел.: (812) 247-04-55

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

turnstile@perco.ru - по вопросам обслуживания турникетов и ограждений

locks@perco.ru - по вопросам обслуживания замков

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

www.perco.ru

Кор. 01.08.2019

www.perco.ru

тел: 8 (800) 333-52-53