PERCo®

# РУКОВОДСТВО АДМИНИСТРАТОРА


# S-20

Сетевое программное обеспечение

# СОДЕРЖАНИЕ

# 1. Введение

Данное руководство системного администратора сетевого ПО *«Единой системы безопасности и повышения эффективности PERCo-S-20»* (далее – *руководство*) предназначено для администраторов системы, а также для системных администраторов компьютерных сетей и сотрудников служб (подразделений) по поддержке программного и аппаратного обеспечения. В руководство включены следующие описания:

- настройка локальной сети и сетевых параметров контроллеров и ПК системы;
- инсталляция и лицензирование ПО;
- настройка параметров работы ресурсов системы (контроллеров, считывателей, ИУ и др.);
- настройка рассылки сообщений;
- настройка сервера системы и сервера видеоподсистемы, создания и управления БД.

Руководство должно использоваться совместно с руководствами пользователя используемых модулей ПО.

***Примечание:***

Эксплуатационная документация доступна на сайте компании ***PERCo***, расположенном по адресу www.perco.ru, в разделе **Поддержка > Документация**.

Принятые в руководстве сокращения и условные обозначения:

АРМ – автоматизированное рабочее место;
АТП – автотранспортная проходная;
БД – база данных;
ВВУ – внешнее верифицирующее устройство;
ИУ – исполнительное устройство;
ОЗ – охранная зона сигнализации;
ОПС – охранно-пожарная сигнализация;
ОС – операционная система;
ОШС – охранный шлейф сигнализации;
ПЗ – пожарная зона сигнализации;
ПК – персональный компьютер;
ПО – программное обеспечение;
ППКОП – прибор приемно-контрольный охранно-пожарный;
ПШС – пожарный шлейф сигнализации;
РКД – режим контроля доступа;
СБ – служба безопасности;
СКУД – система контроля и управления доступом;
СУБД – система управления базами данных;
ШС – шлейф сигнализации.

# 2. Состав системы

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

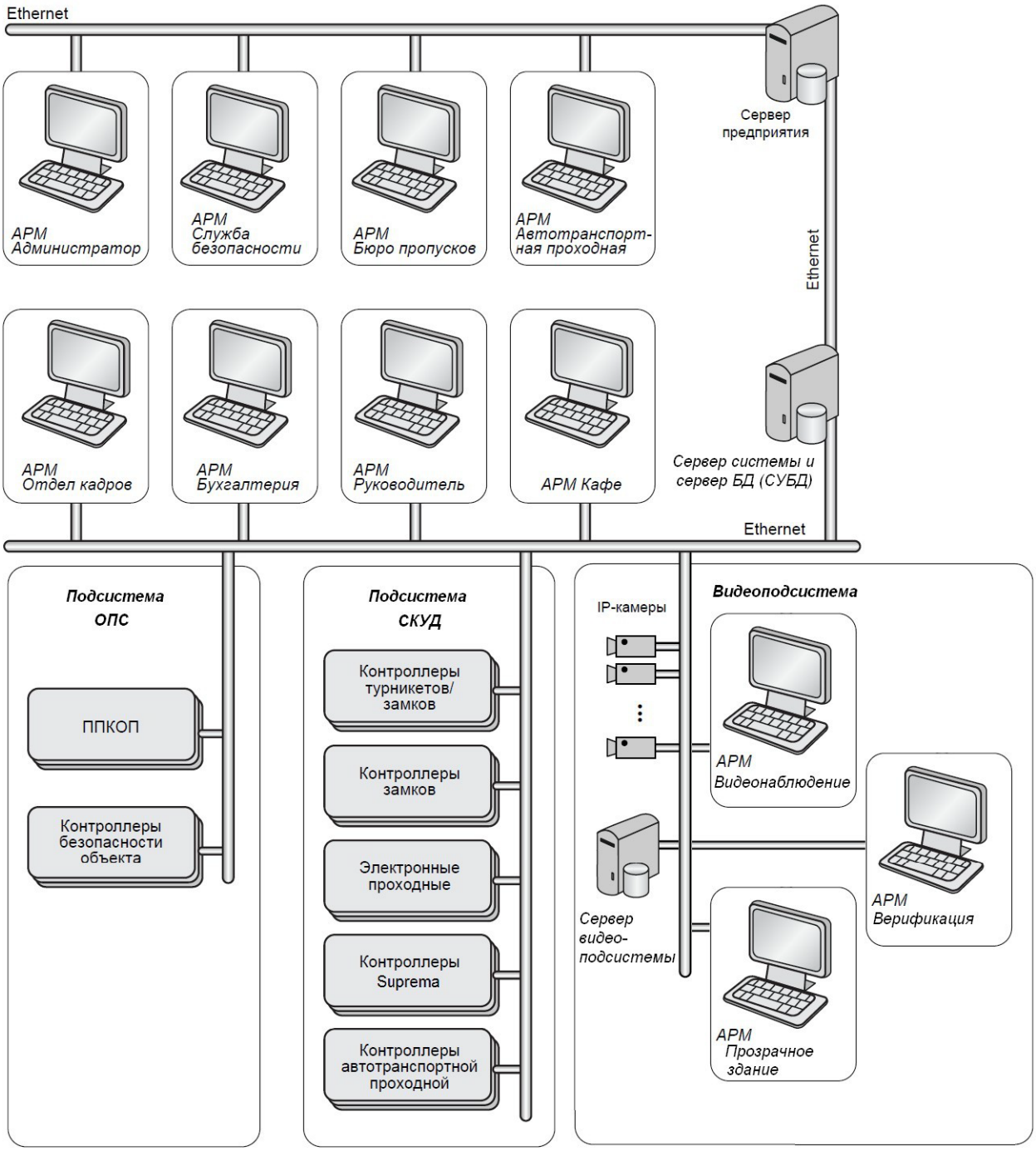
Структурная схема системы показана на рисунке ниже. Все устройства системы работают в единой информационной среде передачи данных, реализованной на основе сети Ethernet. Каждое устройство системы (контроллер, ПК), подключаемое к сети, должно иметь фиксированный IP-адрес для связи и обмена данными с другими устройствами и серверами системы.

***Внимание!***

Для обеспечения информационной безопасности настоятельно рекомендуется разделение существующей или создание отдельной локальной сети Ethernet для контроллеров и серверов системы. При этом ПК с установленными модулями ПО для АРМ могут находиться в сети предприятия.

В состав системы могут входить следующие устройства:

- Контроллеры доступа, регистрации, АТП и электронные проходные для организации необходимого количества точек прохода подсистемы СКУД, а также биометрические контроллеры.
- ППКОП для контроля ОШС и ПШС и организации подсистемы ОПС.
- Один ПК с установленным сервером системы и сервер БД (СУБД) для создания и обслуживания БД системы. Настройка сервера системы и СУБД, а также работа с БД осуществляется с помощью модуля ***«Центр управления»***.
- Необходимое количество ПК с установленным ПО для организации АРМ. Полномочия на доступ к разделам ПО выдаются независимо. Это позволяет организовать АРМ индивидуально для каждого оператора в соответствии с выполняемыми им должностными обязанностями.
- Один или несколько ПК с установленным сервером видеоподсистемы для записи, хранения и просмотра кадров с камер видеоподсистемы. Настройка сервера видеоподсистемы и создание файлов видеоархива осуществляется с помощью ПО ***«Центр управления видеоподсистемой»***.
- IP-камеры (или аналоговые камеры, подключенные к IP-серверам).




**Структурная схема системы PERCo-S-20**

# 3. Требования к персоналу, аппаратным и программным средствам

### Требования к персоналу

Руководство рассчитано на пользователя, обладающего высоким уровнем квалификации в области ИТ и практическими знаниями об установке, настройке и сопровождении приложений в среде ОС семейства *MS Windows*, а также настройке и управлении системами, основанными на архитектуре "клиент-сервер" в сетях на основе протокола TCP / IP.

### Требования к аппаратным средствам

Для работы серверов и АРМ системы необходим ПК, отвечающий следующим минимальным техническим требованиям:

- Процессор: *Intel Core i3* (с частотой не менее 3.6 ГГц). Оперативная память: 4 Гб.
- Объем дискового пространства: 500 Гб.
- Видеокарта и монитор с разрешением не менее 1920x1080 пикселей.
- Устройство чтения DVD-дисков (для установки ПО с дистрибутивного DVD-диска). Клавиатура и манипулятор «мышь».
- Сеть *Ethernet*: *10-BaseT, 100-BaseTX*.

***Примечание:***

Список поддерживаемых системой SMS-провайдеров для отправки SMS-сообщений размещен на сайте компании ***PERCo***, по адресу www.perco.ru, в разделе **Главная > Поддержка > ПО**.

Количество камер (в режиме постоянной записи) на один сервер определяется скоростью записи на жесткий диск и параметрами видео (разрешение, кодек и т. д.). При работе с обычным HDD и при стабильном соединении по LAN рекомендуется использовать не более 15 камер на сервер. При использовании специализированных для записи видео HDD, объединении их в RAID-массивы и детальной настройке качества видео с камер можно добиться увеличения количества камер, поддерживаемых одним сервером видеоподсистемы.

***Важно***: жесткие диски с пометкой "Archive" не предназначены для записи видео с камер.

### Требования к программным средствам

Для работы серверов и АРМ системы на ПК должна быть установлена лицензионная версия ОС семейства *Microsoft Windows*.

- Рекомендована к использованию версия ОС *Windows 7 Pro*.
- Возможно использование *ОС Windows 8.x, Windows 10, Windows Server 2003 SP2, 2008, 2008 R2, 2012, 2012 R2.*
- Возможно, но не рекомендовано использованию ОС Windows: *XP SP3*.

Для серверов системы и видеоподсистемы допустимо использование 64-битных версий ОС.

# 4. Порядок подготовки системы к работе

После завершения монтажных работ придерживайтесь следующей последовательности действий при настройке системы:

1. Ознакомьтесь с разработанной структурной схемой системы, использованной при монтаже. Определите, на какие ПК будет установлен сервер системы и сервер БД, сервер видеоподсистемы и модули ПО для организации АРМ.
2. При необходимости установите и настройте DHCP-сервер. Для установки может использоваться ПК с ОС семейства *Windows* или *Linux*.
3. В соответствии с топологией и маршрутизацией в локальной сети при необходимости измените сетевые настройки ПК и контроллеров.
4. Проверьте связь между ПК сервера системы, контроллерами, ПК АРМ.
5. Установите соответствующие ПО на выбранные ПК.
6. Запустите ***«Центр управления»*** на ПК с установленным сервером системы и создайте новую БД.
7. В срок до 30 дней после начала использования системы приобретите лицензию на используемые модули и введите ключ активации на вкладке **Управление лицензиями**.
8. Запустите ***«Консоль управления»*** под учетной записью главного администратора на одном из ПК.
9. Перейдите в раздел ***«Конфигуратор»*** и произведите добавление устройств системы в конфигурацию.
10. Перейдите в раздел ***«Помещения и мнемосхема»***, создайте список помещений предприятия и расположите добавленные в конфигурацию системы устройства в этих помещениях.
11. Перейдите в раздел ***«Назначение прав доступа операторов»***, создайте учетные записи и выдайте полномочия для операторов каждого АРМ в соответствии с их должностными обязанностями. Задайте пароль для учетной записи `ADMIN`.

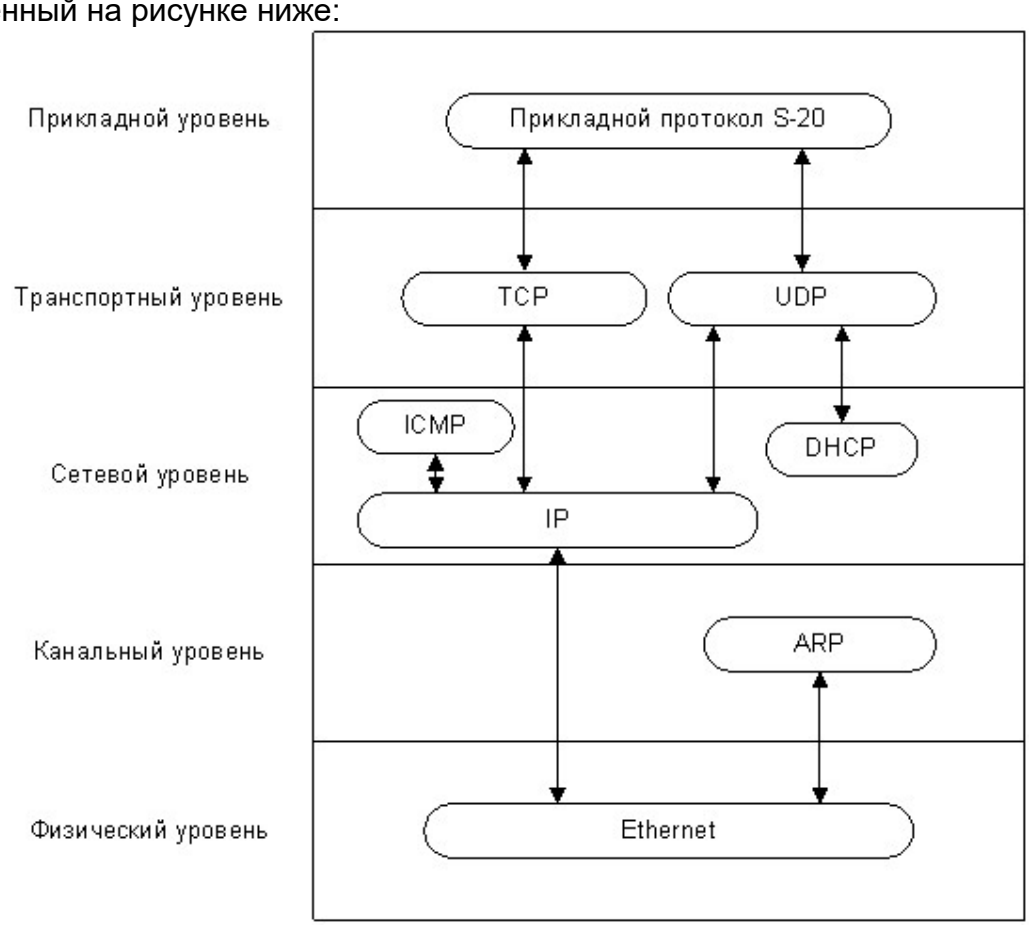
# 5. Сетевые настройки

## 5.1. Используемые сетевые порты и протоколы

***Внимание!***

В ОС семейства *MS Windows* для изменения максимального количества одновременных полуоткрытых исходящих TCP соединений (half-open connections или connection attempts) рекомендуется использовать программу Half-open limit fix. По умолчанию в версии *XP SP 2* и более поздних версиях ОС разрешается иметь не более 10 полуоткрытых исходящих TCP соединений.

Для функционирования системы необходимо обеспечить обмен данными между контроллерами, серверами и АРМ системы по сети *Ethernet*. Для передачи данных прикладным протоколом системы используются как адресная передача пакетов на IP-адреса устройств по протоколу TCP, так и широковещательная рассылка по протоколу *UDP*. Для обмена пакетами в системе используется стек протоколов, приведенный на рисунке ниже:




**Стек протоколов, используемых для обмена в системе**

При передаче пакетов используются сетевые порты, указанные в таблице ниже. Эти порты должны быть свободны и не должны использоваться другими системами и службами в сети предприятия. В системе не поддерживается фрагментация IP-пакетов. Наличие таких серверов или служб, как *DNS* и *WINS*, не требуется.

***Примечание:***

При использовании межсетевого экрана (файервола, брандмауэра), установленного дополнительно или интегрированного в *Windows*, необходимо при конфигурации обеспечить возможность доступа ПО и устройств системы к указанным сетевым портам.

**Используемые в системе сетевые порты**

| Протокол | Порт | Назначение |
|---|---|---|
| UDP | 18900 | конфигурация сетевых параметров контроллера |
| | 18901 | широковещательные кадры (только между контроллерами) внутри подсети |
| TCP | 18902 | порт контроллера для конфигурации, управления и диагностики |
| | 18903 | порт контроллера для приема журнала регистрации |
| | 18904 | порт контроллера для регистрации индицирующего устройства |
| | 18905 | порт контроллера для регистрации верифицирующего устройства |
| | 18906 | порт контроллера для приема и анализа мониторинга |

## 5.2. Организация широковещательной рассылки пакетов

При работе системы в нескольких подсетях для организации широковещательной рассылки пакетов (передачи информации о зональности) произведите следующие настройки:

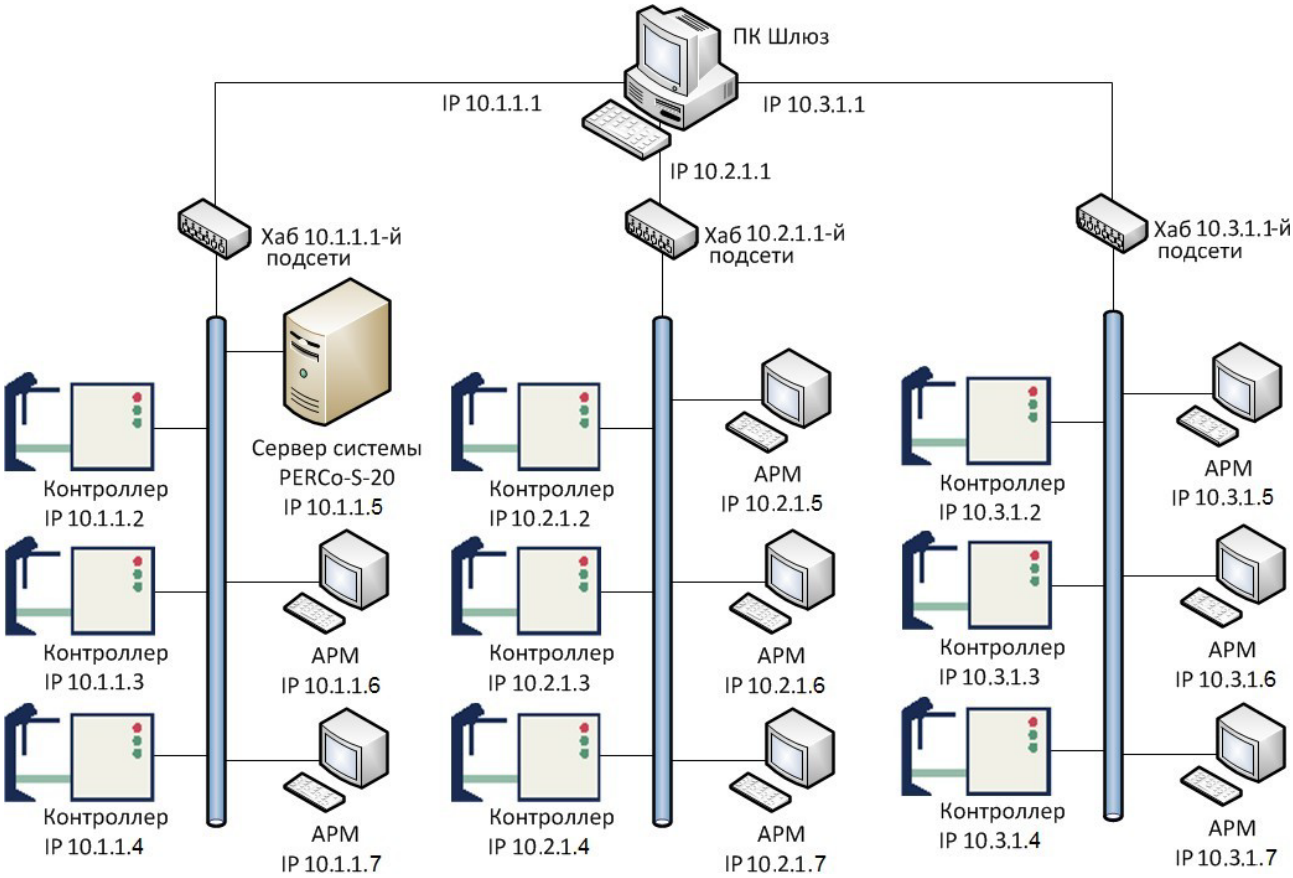
1. Выделить один из ПК системы в качестве шлюза (маршрутизатора). Число сетевых карт, установленных в этом ПК, должно соответствовать числу подключаемых подсетей. Например, если в системе используется три подсети, то на этом ПК должны быть установлены три сетевые карты.
2. Произведите настройку сетевых интерфейсов каждой сетевой карты ПК, выделенного в качестве шлюза.

   Перед настройкой подсетей необходимо проверить, чтобы IP-адрес был свободен и не занят другими устройствами. Например:
   - IP-адрес: 10.1.1.1, Маска подсети: 255.255.0.0
   - IP-адрес: 10.2.1.1, Маска подсети: 255.255.0.0
   - IP-адрес: 10.3.1.1, Маска подсети: 255.255.0.0
3. Включить на ПК, используемом в качестве шлюза, маршрутизацию пакетов TCP/IP. Для этого в ветке реестра ОС *Windows* выполните: `HKEY_LOCAL_MACHINE\SYSTEM\Current Control Set\services\Tcpip\Parameters` установите значение параметра: `IPEnable Router = 1`

***Примечание:***

Дополнительная информация о включении маршрутизации пакетов в ОС *Microsoft Windows XP* доступна по ссылке: https://support.microsoft.com/ru-ru/help/314053/tcp-ip-and-nbt-configuration-parameters-for-windows-xp.

4. Устройствам (контроллерам, ПК) подсети установите соответствующие этой подсети сетевые настройки.
   - Например, для устройств 10.1.1.1-й подсети:
     IP-адрес: 10.1.1.x, где x=2, 3,...
     Маска подсети: 255.0.0.0
     Основной шлюз: 10.1.1.1
   - Например, для устройств 10.2.1.1-й подсети:
     IP-адрес: 10.2.1.x, где x=2, 3,...
     Маска подсети: 255.0.0.0
     Основной шлюз:10.2.1.1
   - Например, для устройств 10.3.1.1-й подсети:
     IP-адрес:10.3.1. x, где x=2, 3,...
     Маска подсети: 255.0.0.0
     Основной шлюз: 10.3.1.1

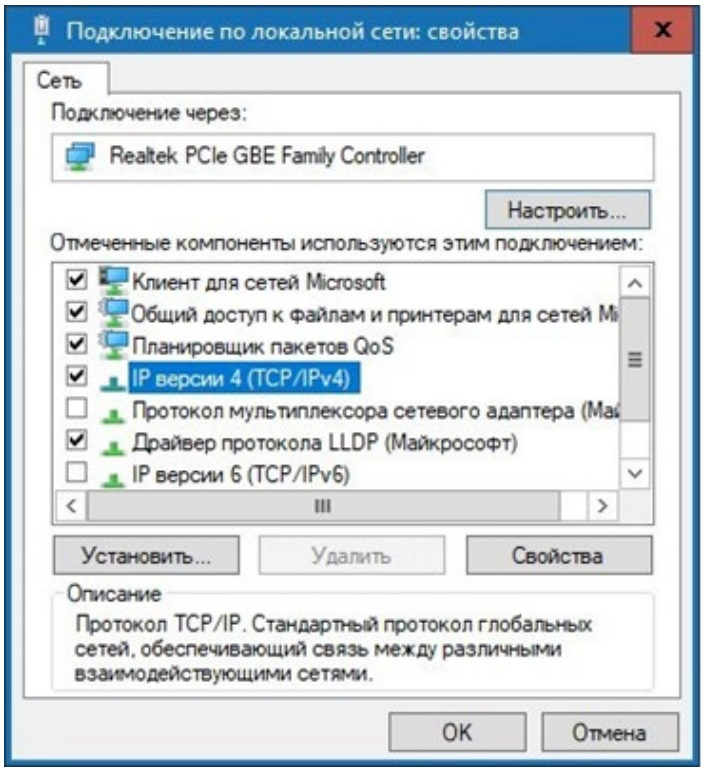



**Пример схемы организации широковещательной рассылки**

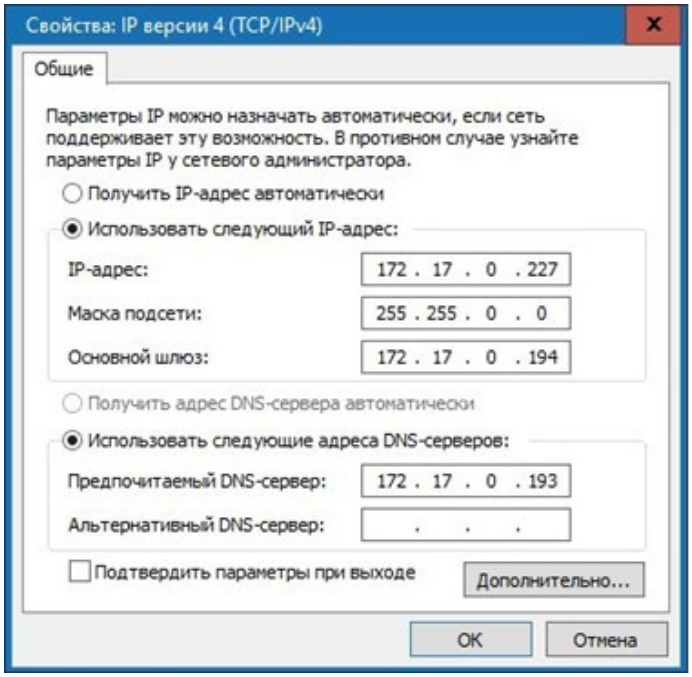
## 5.3. Добавление сетевого интерфейса ПК

Для добавления сетевого интерфейса (IP-адреса и маски подсети) ПК выполните следующие действия:

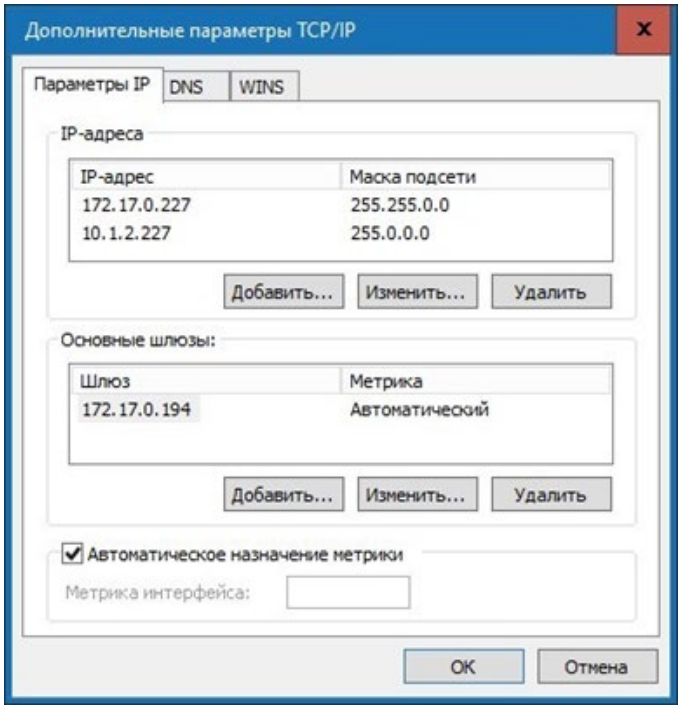
1. Откройте окно свойств **Подключение по локальной сети**:



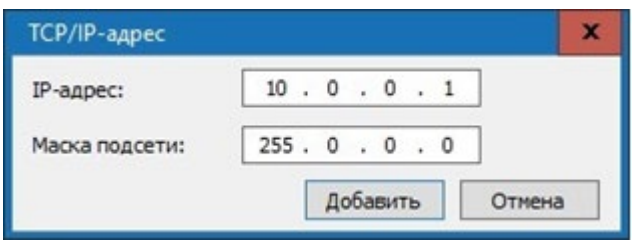
2. Выделите компонент **IP версии 4 (TCP/IPv4)** и нажмите кнопку **Свойства**. Откроется окно **Свойства: IP версии 4 (TCP/IPv4)**:




3. В открывшемся окне убедитесь, что переключатель находится в положении **Использовать следующий IP-адрес**, после этого нажмите кнопку **Дополнительно...**. Откроется окно **Дополнительные параметры TCP/IP**:




4. В области **IP-адреса** нажмите кнопку **Добавить…**. Откроется окно **TCP/IP- адрес**:



5. В поля **IP-адрес** и **Маска подсети** введите, соответственно, значения: 10.x.x.x и 255.0.0.0. Нажмите кнопку **Добавить**. Окно будет закрыто, добавленный IP-адрес появится в области **IP-адреса** окна **Дополнительные параметры TCP/IP**.

## 5.4. Сетевые настройки контроллера

Для обеспечения адресной передачи данных необходимо обеспечения уникальности IP-адресов контроллеров и ПК в используемой подсети и их неизменность при работе системы.

Контроллеры системы могут работать с IP-адресами и сетевыми настройками, заданными при производстве, полученными от DHCP-сервера или заданными вручную.

При производстве контроллерам системы заданы следующие сетевые настройки:

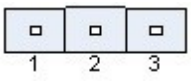
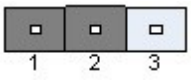
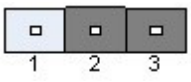
- **IP-адрес:** 10.x.x.x. Значения x указаны в паспорте и на плате устройства,
- **Шлюз:** 0.0.0.0,
- **Маска подсети:** 255.0.0.0,
- **MAC-адрес:** уникальный, неизменяемый в настройке, указан в паспорте и на плате устройства.

Выбор способа получения сетевых настроек контроллером осуществляется установкой перемычки (джампера) на разъем *XP1* платы контроллера. Расположение разъема на плате устройства указывается в его эксплуатационной документации. При производстве перемычка не устанавливается, что соответствует ручному режиму настройки.

***Внимание!***

Установка и снятие перемычки должно производиться только при отключенном источнике питания контроллера.

**Варианты установки перемычки на разъем XP1 контроллера**

| Режим | Разъем | Примечание: |
|---|---|---|
| *«Ручной режим»* (перемычка снята) |  | Если сетевые настройки не были изменены, то контроллер работает с заводскими настройками. При изменении сетевых настроек из ПО или через Web-интерфейс, контроллер начинает работать с новыми настройками без перезапуска |
| *«IP MODE»* (перемычка в положение 1–2) |  | Режим предназначен для работы в сетях с динамическим распределением IP-адресов. Контроллер получает сетевые настройки от DHCP-сервера |
| *«IP DEFAULT»* (перемычка в положение 2–3) |  | Контроллер работает с сетевыми настройками, установленными при производстве. Пароль для доступа к контроллеру сбрасывается. Пользовательские сетевые настройки, если они были заданы ранее, сохраняются. При следующем включении, если перемычка будет снята, контроллер начнет работать с ними |

Изменение сетевых настроек контроллера в *«Ручном режиме»* может производится от ПК, с установленным разделом сетевого ПО ***«Конфигуратор»*** или через *Web*-интерфейс контроллера. При этом необходимо, чтобы контроллер и ПК были подключены к сети *Ethernet* и находились в одной подсети (возможно подключение контроллера непосредственно к разъему сетевой карты ПК). При первом подключении к контроллеру ПК может потребоваться добавить сетевой интерфейс в десятой подсети.

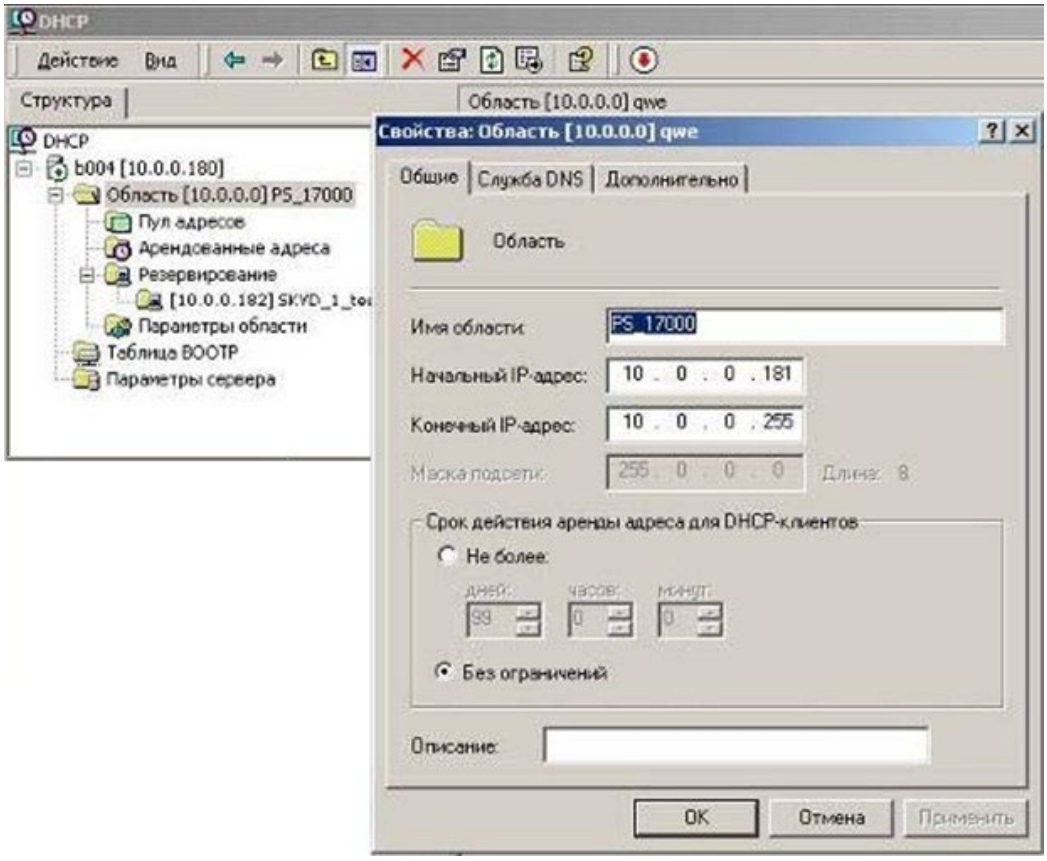
## 5.5. Настройка DHCP-сервера в ОС Windows

Для работы в сетях с динамическим распределением IP-адресов, когда контроллеры получают сетевые настройки от DHCP-сервера, необходимо для всех контроллеров системы с помощью перемычки на плате установить режим *«IP MODE»*.

При настройке DHCP-сервера необходимо зарезервировать диапазон IP-адресов, выделяемых контроллерам системы. После чего привязать MAC-адреса контроллеров к IP-адресам из зарезервированного диапазона.

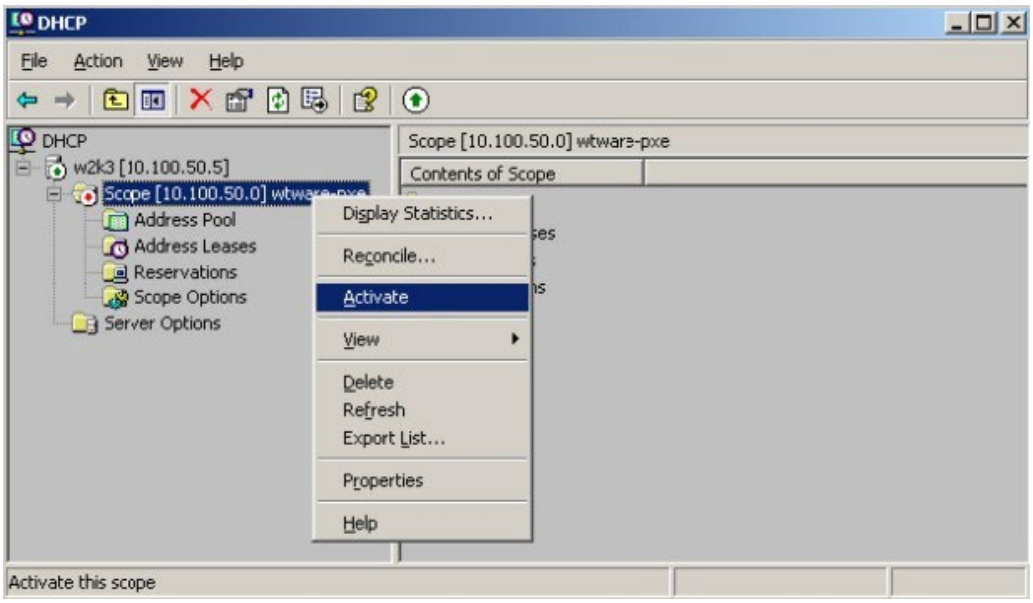
Для этого (на примере настройки DHCP-сервера для системы Windows XP):

1. Запустите DHCP-сервер. Для этого выберите последовательно: **Пуск > > Программы > Администрирование > DHCP**. Откроется окно **DHCP**.



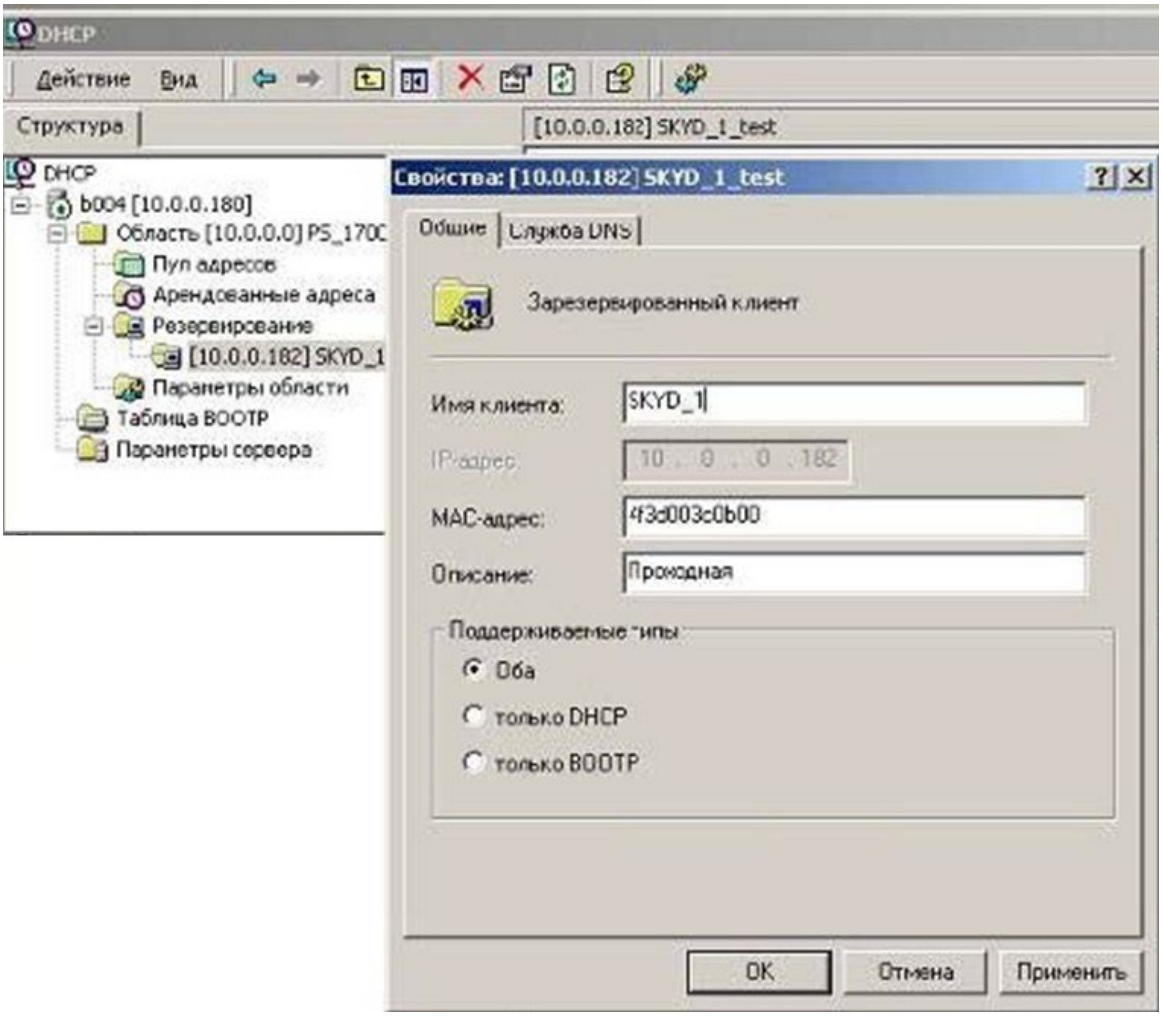

2. Зарезервируйте диапазон IP-адресов для контроллеров системы. Название области и описание могут быть любыми. Это информация необходима для системного администратора, поэтому название должно быть достаточно информативным. Рекомендуется делать область несколько больше, чем число контроллеров, которое планируется использовать. Также задавайте такую область адресов, которая не будет включать в себя уже существующие ПК с фиксированными адресами.

3. Произведите активацию области:




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

4. Проведите резервирование IP-адресов для контроллеров системы. Для этого каждому контроллеру системы в соответствие с MAC-адресом, указанным в его паспорте, выдайте IP-адрес из созданного диапазона. Для удобства добавьте описание, как указано в примере:



5. Выполните операцию для каждого контроллера системы.
6. После включения электропитания и подключения к сети *Ethernet* контроллеры будут отображаться в списке арендованных адресов. Проверьте, чтобы в столбце о времени аренды адреса находилась информация об активном резервировании.

## 5.6. Настройка DHCP-сервера в ОС Linux

Для работы в сетях с динамическим распределением IP-адресов, когда контроллеры получают сетевые настройки от DHCP-сервера, необходимо для всех контроллеров системы с помощью перемычки на плате установить режим *«IP MODE»*.

Для настройки DHCP-сервера ***ISC DHCPD*** в среде ОС семейства *Linux* необходимо внести изменения в файл конфигурации сервера: `/etc/dhcp.conf`. Пример варианта файла конфигурации показан ниже:

```
# Подсеть 10.100.0.0, маска сети 255.255.255.0
subnet 10.100.0.0 netmask 255.255.255.0 { # маска подсети
255.255.255.0
option subnet-mask 255.255.255.0;
…
# диапазон адресов для контроллеров # 10.100.0.10-10.100.0.254
range 10.100.0.10 10.100.0.254;
…
#описание контроллеров (proxod_1, …, office_room_101) #обратите
внимание на то, что необходимо использовать #IP-адрес из
выделенного диапазона

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

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

Чтобы внесенные в файл `/etc/dhcp.conf` изменения вступили в силу, необходимо перезапустить сервер. Для этого можно использовать следующие команды:

`/ etc/ rc. d/ init. d/ dhcpd stop` – для остановки,

`/ etc/ rc. d/ init. d/ dhcpd start` – для его запуска.

## 5.7. Внешнее подключение контроллера к серверу PERCo-S-20

В случаях, когда IP-адрес контроллера должен скрываться по соображениям безопасности, возможен вариант подключения контроллера к серверу по внешнему IP-адресу сервера. При таком подключении сервер запоминает MAC-адрес контроллера, при этом IP-адрес контроллера может быть любым, меняться динамически, а также контроллер может находиться во внешней сети.

***Внимание!***

Данная функция возможна только для контроллеров ***CL15*** (***.1***, ***.3***, ***.7***), ***CR11*** (***.1***), ***CR02.9, CT/L14*** (***.1***) и для встроенного контроллера ***CT13*** (***.1***) электронных проходных ***KT02.9*** (***.B***, ***.Q***), ***KT05.9A***, ***KTC01.9A***.

С помощью контроллера, подключенного к серверу системы по внешнему IP-адресу сервера, невозможно выдать идентификатор доступа.

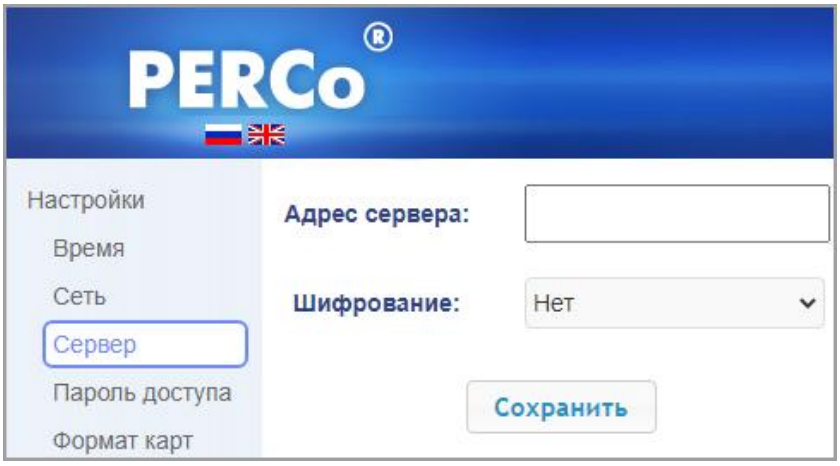
Для подключения контроллера к серверу системы ***PERCo-S-20*** по внешнему IP-адресу сервера:

1. Убедитесь, что контроллер и ПК подключены к сети *Ethernet* и находятся в одной подсети (возможно подключение контроллера непосредственно к разъему сетевой карты ПК). При первом подключении к контроллеру ПК может потребоваться добавить сетевой интерфейс в десятой подсети. Также может потребоваться отключить прокси-сервер в сетевых настройках используемого браузера. Наличие таких серверов или служб, как DNS и WINS, не требуется.
2. Подключитесь к Web-интерфейсу контроллера. Для этого введите в адресную строку браузера IP-адрес контроллера (указан в паспорте и на плате контроллера), после чего нажмите кнопку **Enter** на клавиатуре. При необходимости введите пароль доступа к контроллеру. По умолчанию пароль отсутствует.

***Примечание:***

Полное руководство по работе с Web-интерфейсом смотрите в руководствах по эксплуатации на контроллеры ***CL15*** (***.1***, ***.3***, ***.7***), ***CR11*** (***.1***), ***CR02.9, CT/L14*** (***.1***) и электронные проходные ***KT02.9*** (***.B***, ***.Q***), ***KT05.9A***, ***KTC01.9A***.

3. Перейдите в подраздел **Сервер** раздела **Настройки** в меню Web-интерфейса. Откроется страница с рабочей областью следующего вида:

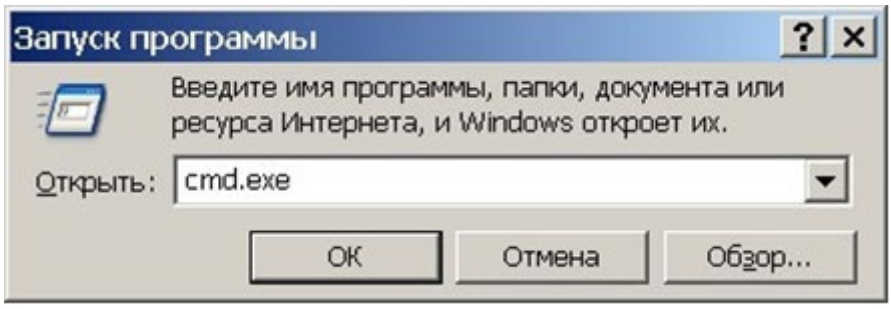



4. В открывшемся окне произведите необходимые изменения:
   - в поле **Адрес сервера** введите IP-адрес сервера, на котором установлена система ***PERCo-S-20***;
   - в параметре **Шифрование** задайте требуемый способ шифрования.
5. Нажмите кнопку **Сохранить**. Внесенные изменения будут сохранены.

## 5.8. Проверка связи между ПК и контроллером

Для корректного функционирования системы необходимо обеспечить устойчивую связь по сети *Ethernet* между сервером системы и всеми контроллерами системы. При необходимости проверки связи между ПК и одним из контроллеров системы произведите следующие действия:

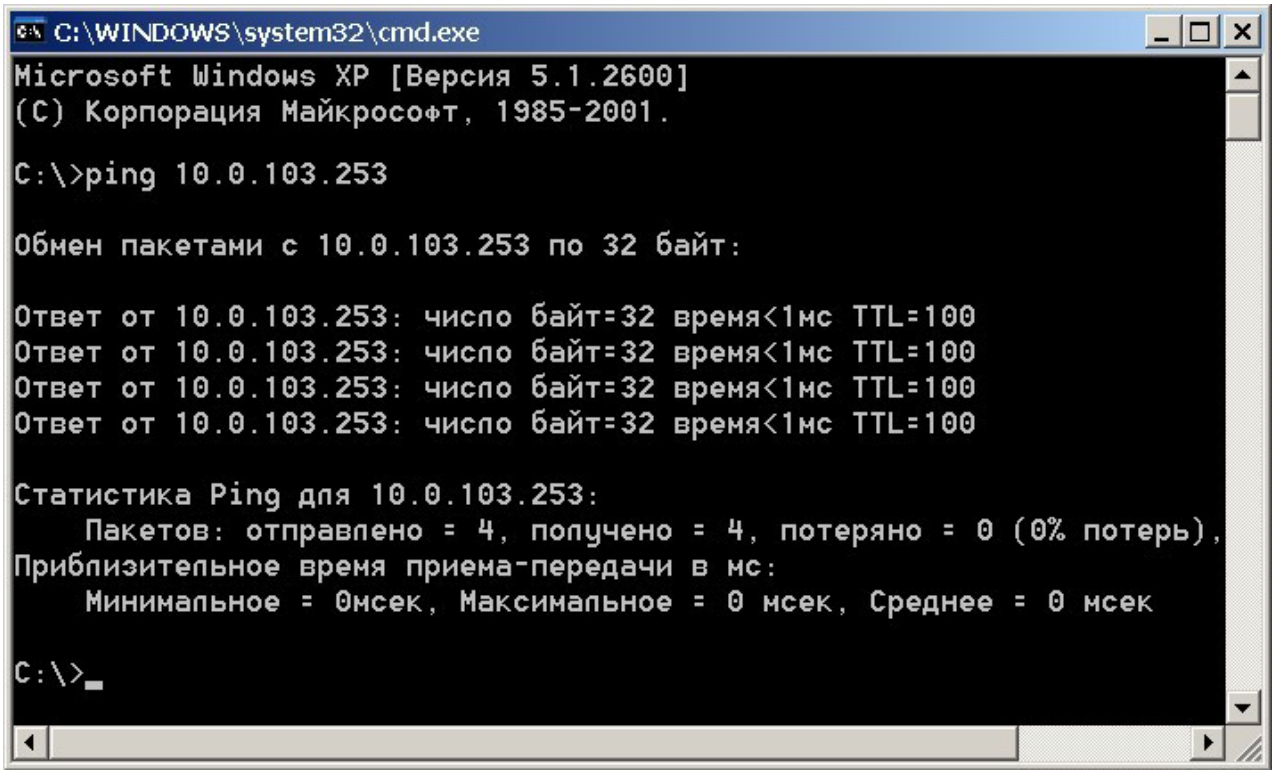
1. Выберите последовательно на ПК: **Пуск > Выполнить**. Откроется окно **Запуск программы**:



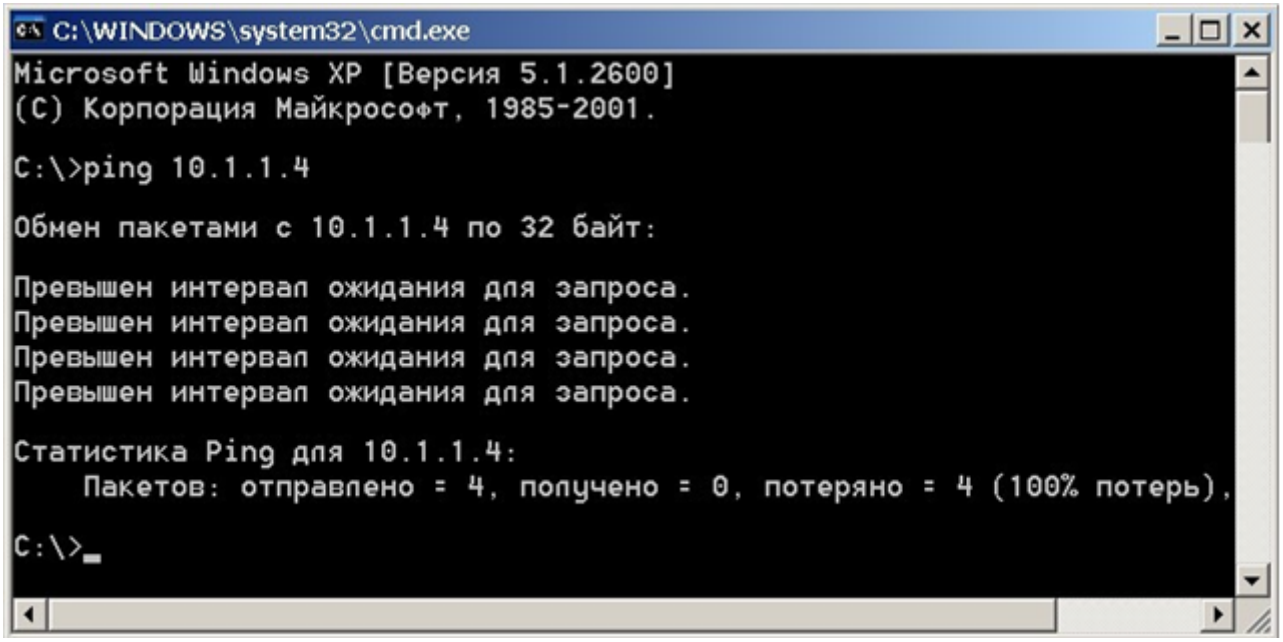

2. В открывшемся окне введите команду: `cmd.exe` и нажмите кнопку **ОК**.
3. Откроется окно интерфейса командной строки с заголовком:

   C:\WINDOWS\system32\cmd.exe.

4. В открывшемся окне введите команду:
   `ping XX.XX.XX.XX`, где `XX.XX.XX.XX` – IP-адрес контроллера, с которым необходимо проверить связь (например `10.0.103.253`).
5. Если связь будет установлена, то появится ответ следующего вида:
   `Ответ от XX.XX.XX.XX: число байт=32 время<10мс TTL=128`.



6. Если связь не установлена, то есть ответ от IP-адреса не получен, проверьте правильность настройки маршрутизации сети.

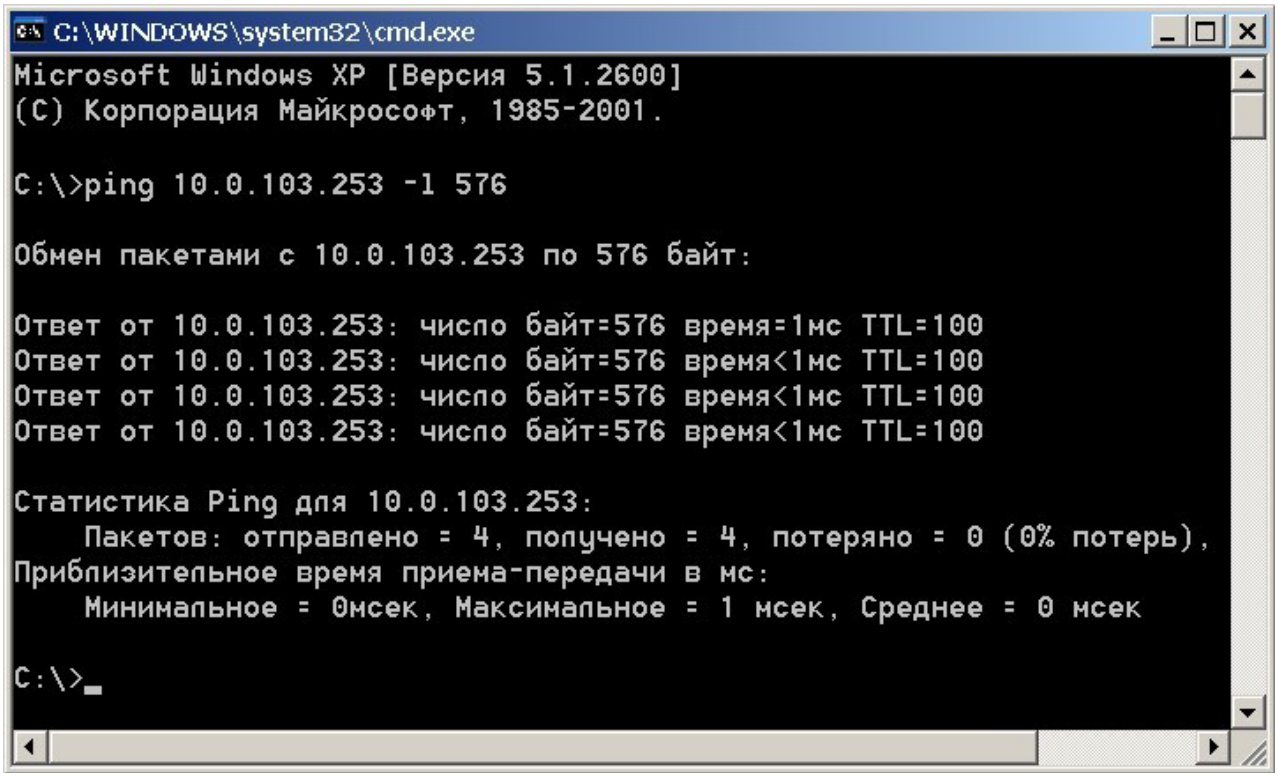



7. Контроллеры системы не поддерживают фрагментацию IP-пакетов. Поэтому необходимо удостовериться, что IP-пакеты на всем протяжении от сервера системы до контроллера не фрагментируются. Для этого введите ту же команду с ключом `-l` и указанием на размер отправляемого пакета данных, например, 576 байт:

   `ping XX.XX.XX.XX -l 576`.

8. Если связь есть, а размер отправленного пакета совпадает с размером, полученным в ответе, можно утверждать, что IP-пакеты размером меньше 576 байт не фрагментируются:

   `Ответ от 193.124.71.56: число байт=576 время<10мс TTL=128`.



9. Если положительный ответ получить не удается, то вероятнее всего на пути следования IP-пакетов находится сетевое коммутирующее оборудование (роутер, концентратор и сетевые модемы), делящее IP-пакеты на фрагменты размером меньше 576 байт. Проверьте настройки этого оборудования и по возможности увеличьте максимальный размер блока данных одного пакета MTU (maximum transmission unit). Обычно этот параметр обозначается как **MaxMTU** или **IPMTU**.
10. Если в сети возможны несколько вариантов коммутации, то наберите команду с ключом `–t`:

    ```
    ping XX.XX.XX.XX -l 576 –t.
    ```

11. Коммутируя разными способами, смотрите на время ответа, выбирая соединение, дающее максимально быстрый ответ. Для вывода статистики нажмите: **Ctrl**+**Break** (**Pause**).
12. Для остановки нажмите **Ctrl**+**C**.

# 6. Установка и удаление ПО

## 6.1. Структура сетевого ПО

***Примечание:***

Актуальную версию установочного файла ПО *«Сетевое программное обеспечение S-20»* можно загрузить с сайта компании ***PERCo***, расположенного по адресу www.perco.ru из раздела **Поддержка > Программное обеспечение**.

В структуру сетевого ПО входят:

- **Сервер БД** – СУБД на базе SQL-сервера *Firebird*.
- **Сервер системы** – модуль содержит сервер системы для работы с БД системы и раздел ***«Центр управления»***.
- **Консоль управления**. Раскрывающийся список содержит перечень модулей сетевого ПО. При выборе хотя бы одного модуля автоматически будет установлена программная оболочка ***«Консоль управления»*** для запуска разделов ПО.
- **SM19 Модуль интеграции с 1С** – модуль обмена данными между сервером системы с сервером БД 1С разработанный компанией ***PERCo***.
- **Поддержка интеграции с 1С для Формула Ай-Ти** – модуль, обеспечивающий интеграцию с ПО ***ФОРМУЛА: Модуль «Учет рабочего времени» Интеграция PERCo-S-20 и 1С:Предприятия 8.2***.

***Внимание!***

Модуль **Поддержка интеграции с 1С для Формула Ай-Ти** должен быть установлен на все ПК, с установленным модулем ***ФОРМУЛА: Модуль «Учет рабочего времени» Интеграция PERCo-S-20 и 1С:Предприятия 8.2***.

- **Сервер видеоподсистемы** – сервер видеоподсистемы и ***«Центр управления видеоподсистемой»*** для работы с видеоархивом.
- **WEB-доступ прозрачного здания** – Web-интерфейс раздела сетевого ПО ***«Прозрачное здание»***.
- **Конвертор БД из PERCo-SYS-15000**.
- **Сервер интеграции с биометрической системой SUPREMA** – модуль обеспечивает интеграцию с биометрическими контроллерами компании ***«Suprema»***.

***Внимание!***

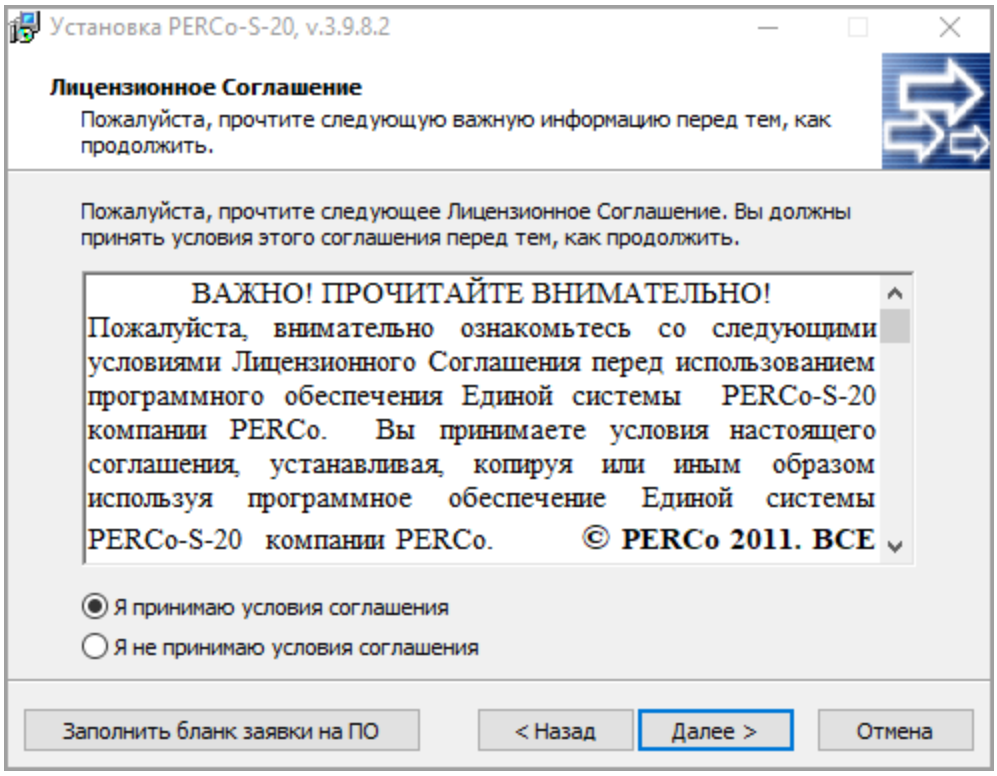
Модуль **Сервер интеграции с биометрической системой SUPREMA** обеспечивает интеграцию с биометрическими контроллерами, имеющими версию внутреннего ПО ("прошивку") не менее чем:

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

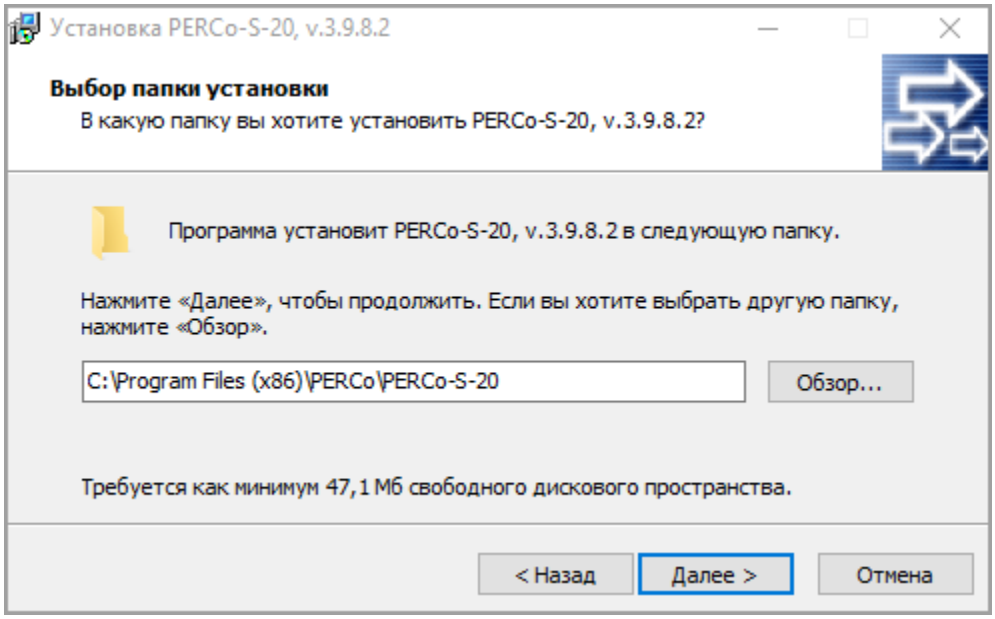
## 6.2. Установка

При установке сетевого ПО придерживайтесь следующей последовательности действий:

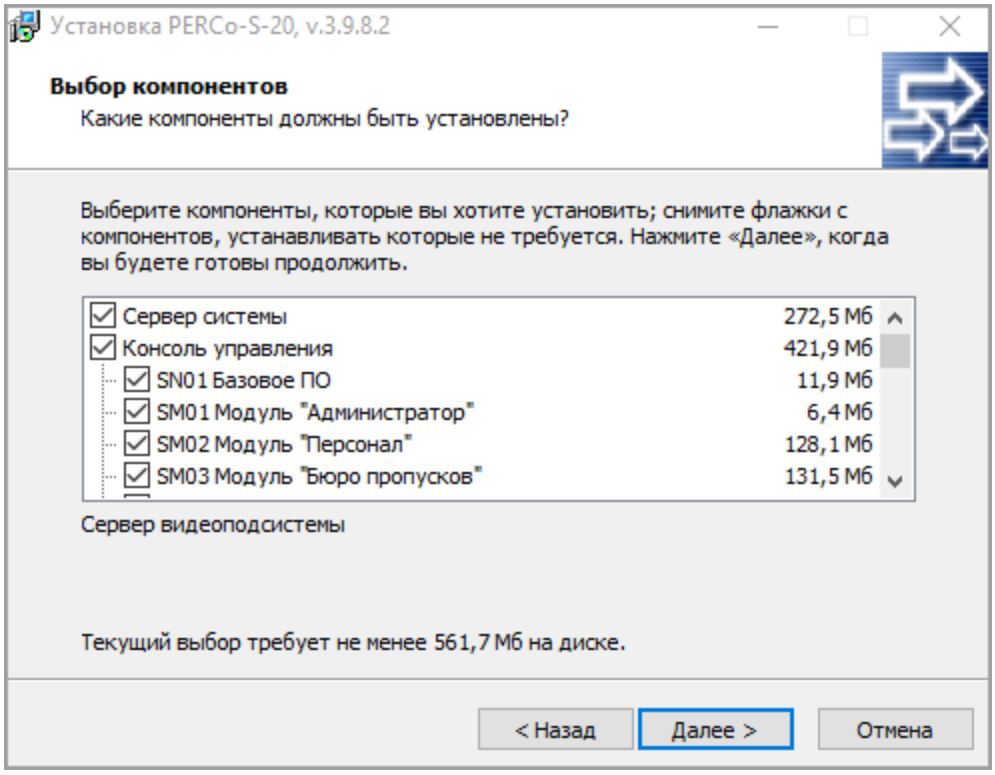
1. Запустите установочный файл `SetupCommon.exe`. Следуйте указаниям мастера установки. Внимательно ознакомьтесь с предлагаемой информацией и лицензионным соглашением:




2. Для принятия лицензионного соглашения установите флажок **Я принимаю условия соглашения**. В случае необходимости нажмите кнопку **Заполнить бланк заявки на ПО**. При этом в программе *MS Office Word* будет открыт бланк заявки на приобретение лицензии на ПО. Нажмите кнопку **Далее**.




3. При необходимости измените название и расположение папки, в которую будет произведена установка ПО. Нажмите кнопку **Далее**.




4. Отметьте флажками модули сетевого ПО, которые необходимо установить на ПК в соответствии с разработанной структурной схемой системы. Нажмите кнопку **Далее**.

***Примечание:***

Если был отмечен для установки модуль **Сервер БД**, то перед установкой ПО системы будет запущен стандартный мастер установки SQL сервера *Firebird*.

5. Следуйте указаниям мастера установки. После завершения установки ПО готово к работе.

***Примечание:***

Если система уже установлена, но требуется установить дополнительные модули, запустите установочный файл `SetupCommon.exe` и в окне **Выбор компонентов** отметьте флажками требуемые модули, после чего следуйте указаниям мастера установки.

## 6.3. Удаление

Для полного удаления всех модулей сетевого ПО с ПК используйте стандартный компонент *MS Windows «Установка и удаление программ»*. В открывшемся окне выделите строку *«PERCo-S-20»* и нажмите кнопку **Удалить**.

# 7. Обновление версии ПО

## 7.1. Обновление ПО серверов

***Внимание!***

При обновлении ПО модуля **Сервера системы** связь устройств системы с сервером будет нарушена и обмен информацией с БД будет невозможен.

**Обновление ПО сервера системы**

Для обновления ПО на ПК, используемом в качестве сервера системы, выполните следующие действия:

1. Убедитесь, что встроенное ПО (прошивки) контроллеров обновлено до последней версии.
   При необходимости выполните обновление встроенного ПО (прошивок) контроллеров.

***Примечание:***

Актуальные версии встроенного ПО (прошивок) контроллеров доступны на сайте компании ***PERCo*** по ссылке https://www.perco.ru/partneram/programmnoe-obespechenie.php, вкладка **Прошивки оборудования**. Инструкция по обновлению включена в архив с файлом соответствующего ПО.

2. Проверьте целостность БД и исправьте обнаруженные ошибки.
3. Удалите все сетевые модули ПО PERCo S-20.
4. Установите новую версию ПО.

***Примечание:***

Актуальную версию установочного файла ПО *«Сетевое программное обеспечение S-20»* можно загрузить с сайта компании ***PERCo*** по ссылке https://www.perco.ru/partneram/programmnoe-obespechenie.php, вкладка **ПО PERCo-S-20**.

5. Скопируйте с заменой все файлы из архива `Update.rar` в папку с установленным сетевым ПО (по умолчанию: `C:\Program Files\PERCo\PERCo-S-20`).

***Примечание:***

Архив `Update.rar` доступен для скачивания по ссылке https://www.perco.ru/download/support/download/Update.rar.

6. После установки ПО обновите версию БД, даже если текущая версия БД актуальна.

**Обновление ПО сервера видеоподсистемы**

Автоматическое обновление модуля ПО **Сервер видеоподсистемы** возможно если на том же ПК установлен один из модулей сетевого ПО, то есть может быть запущена ***«Консоль управления»***. В ином случае модуль необходимо полностью удалить, а затем установить из установочного файла `SetupCommon.exe`.

## 7.2. Обновление ПО АРМ

Функция автоматического обновления доступна для версий ПО ***«Консоль управления»***, выпущенных позднее версии 3.6.3.0.

Функция предусматривает возможность обновления модуля **Консоль управления** и всех установленных на ПК сетевых модулей.

Функция запускается после обновления ПО модуля **Сервер системы** при подключении ***«Консоли управления»*** к серверу системы.

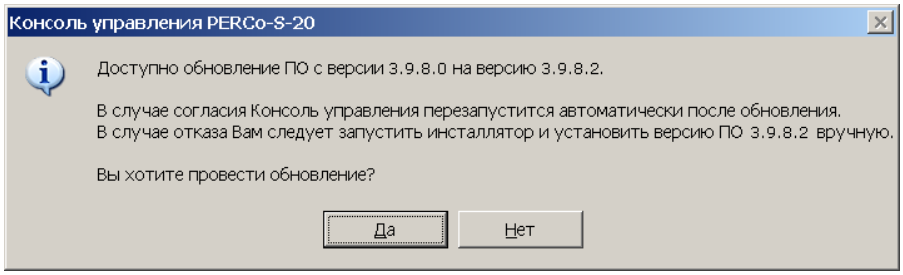
***Примечание:***

Для работы функции автоматического обновления ПО на ПК должны быть запущены следующие службы:

- *«Сервис автоматического обновления PERCo-S-20»;*
- *«Службы терминалов» MS Windows*.

Для обновления ПО на АРМ выполните следующие действия:

1. Обновите ПО сервера системы согласно подразделу **«Обновление ПО серверов»**.
2. Запустите ***«Консоль управления»***.
3. При подключении консоли к серверу системы, на котором была обновлена версия ПО, откроется окно с сообщением:




4. Если необходимо запустить процедуру автоматического обновления, нажмите кнопку **Да**. Откроется окно **Мастер автоматического обновления**.
5. Процедура обновления производится автоматически и состоит из следующих этапов:
   - Ожидание выгрузки приложений.
   - Получение пакета обновления от сервера системы.
   - Установка пакета обновления.
   - Регистрация пакета обновления.

   При этом процедура обновления может быть прервана на любом этапе и будет возобновлена при следующем запуске ***«Консоли управления»***.

***Примечание:***

Если файл пакета обновления ПО был загружен ранее или вручную помещен в папку с установленным ПО (по умолчанию `C:\Program Files\PERCo\PERCo-S-20`), то этап получения обновления от сервера системы будет пропущен.

6. При успешном завершении установки обновления появится окно с соответствующим сообщением, после чего будет автоматически запущена ***«Консоль управления»***.
7. Скопируйте с заменой все файлы с расширением `.bpl` из архива `Update.rar` в папку с установленным сетевым ПО (по умолчанию: `C:\Program Files\PERCo\PERCo-S-20`).

***Примечание:***

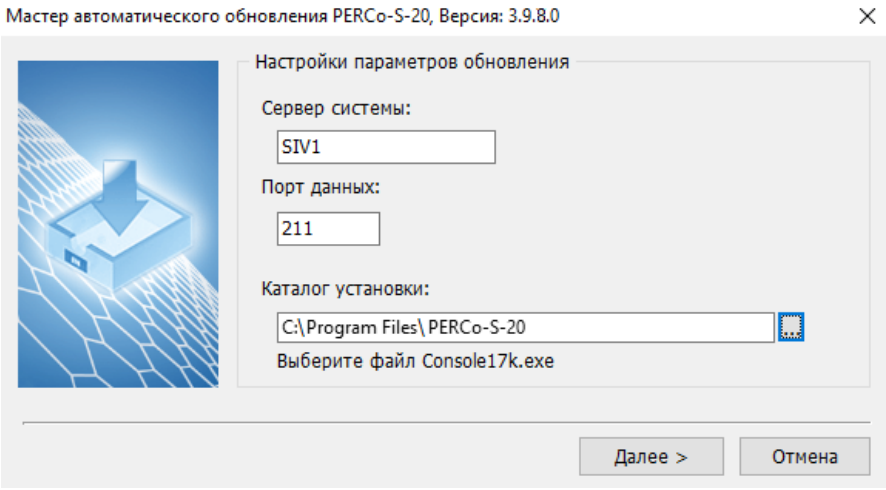
Архив `Update.rar` доступен для скачивания по ссылке https://www.perco.ru/download/support/download/Update.rar.

8. Перезапустите ***«Консоль управления»***.

### Ручной запуск обновления ПО на АРМ

При необходимости процедуру обновления можно запустить вручную, при условии, что на ПК установлена ***«Консоль управления»***. Для этого:

1. Запустите от имени администратора файл `AUClient17k.exe`, расположенный в папке с установленным сетевым ПО. По умолчанию: `C:\Program Files\PERCo\PERCo-S-20`. Откроется окно **Мастер автоматического обновления**:




2. В открывшемся окне укажите IP-адрес сервера системы, с которого будет загружено обновление и порт обмена данными с сервером.
3. Если в поле **Каталог установки** текст выделен красным цветом, то необходимо указать папку, в которой расположен файл запуска ***«Консоли управления»***.

   Для этого нажмите кнопку ... справа от поля. В открывшемся окне выберите файл `Console17k.exe` и нажмите кнопку **Открыть**.
4. В окне **Мастер автоматического обновления** нажмите кнопку **Далее**.

   Будет запущена стандартная процедура обновления ПО на АРМ, описанная выше.
9. Скопируйте с заменой все файлы с расширением `.bpl` из архива `Update.rar` в папку с установленным сетевым ПО (по умолчанию: `C:\Program Files\PERCo\PERCo-S-20`).

***Примечание:***

Архив `Update.rar` доступен для скачивания по ссылке https://www.perco.ru/download/support/download/Update.rar.

5. Перезапустите ***«Консоль управления»***.

# 8. Учетные записи системы

В системе предусмотрены следующие типы учетных записей для доступа к разделам «***Консоли управления***»:

- Уникальная учетная запись главного администратора. Права не ограничены. По умолчанию для `ADMIN` пароль не задан. Пароль учетной записи может быть изменен в разделе ***«Назначение прав доступа операторов»***.
- Учетная запись администратора. Права не ограничены. По умолчанию не задана. Создается и изменяется в разделе ***«Назначение прав доступа операторов»***.
- Учетная запись оператора. Права каждого оператора ограничены выданными полномочиями. По умолчанию не задана. Создается и изменяется в разделе ***«Назначение прав доступа операторов»***.

В системе предусмотрены следующие типы учетных записей для доступа к БД в ***«Центре управления»***:

- Уникальная учетная запись администратора БД (*Administrator Sql Server*). Необходима для создания новой БД и доступа к окну **Настройка сервера БД**. По умолчанию задана учетная запись `SYSDBA` с паролем `masterkey`. Пароль учетной записи может быть изменен в окне **Настройка сервера БД**.
- Учетные записи пользователей БД. Добавляются при создании новой БД на вкладке **Создание и управление БД**. Необходимы для доступа и изменения этой базы. По умолчанию `scd17_user` с паролем `scd17_password`. После создания БД пароль учетной записи может быть изменен в окне **Настройка сервера БД**.

# 9. «Центр управления»

Модуль ***«Центр управления»*** предназначен для:

- управления и настройки СУБД и сервера системы;
- управления лицензиями на сетевые модули системы;
- создания, обслуживания и резервного копирования БД системы;
- настройки параметров рассылки сообщений;
- настройки параметров отправки отчетов по e-mail;
- настройки модуля интеграции с ИСО «Орион».

## 9.1. Управление лицензиями

### 9.1.1. Порядок приобретения лицензии и ключей активации

Сетевое ПО системы приобретается в составе модулей, позволяющих расширять функциональные возможности системы в целом или отдельных ее подсистем. При этом каждый модуль состоит из одного или нескольких разделов. Запуск разделов осуществляется из ***«Консоли управления»***. Для упрощения процедуры приобретения лицензии на сетевое ПО, а также для знакомства с его возможностями, в течение 30 дней с момента первого запуска ПО работает в ознакомительном режиме.

В ознакомительном режиме работы сохраняются все функциональные возможности ПО, но в строке заголовка окна ***«Консоли управления»*** отображается количество дней, оставшихся до окончания ознакомительного периода. По прошествии 30 дней доступ к модулям сетевого ПО, для которых не введен ключ активации, будет запрещен.

В качестве электронного ключа защиты ПО от несанкционированного использования применяется один из контроллеров системы. Выполнение функции электронного ключа защиты не влияет на функциональные возможности контроллера.

Для использования контроллера в качестве электронного ключа защиты ПО от несанкционированного использования:

- контроллер должен быть добавлен в конфигурацию системы в разделе ***«Конфигуратор»***;
- должна поддерживаться постоянная связь между контроллером и сервером системы.

В случае отсутствия связи между контроллером и сервером системы все введенные ключи активации не смогут пройти проверку, и модули будут запущены в ознакомительном режиме.

Для приобретения лицензии и получения ключей активации модулей ПО:

1. Выберите один из приобретенных ранее контроллеров ***PERCo***, который будет использоваться в качестве электронного ключа защиты ПО.
2. Заполнить заявку для приобретения лицензии на сетевое ПО. В заявке укажите MAC-адрес выбранного контроллера, перечень приобретаемых модулей и количество АРМ, на которых каждый модуль планируется использовать.

***Примечание:***

Заявку для приобретения лицензии на сетевое ПО можно заполнить следующими способами:

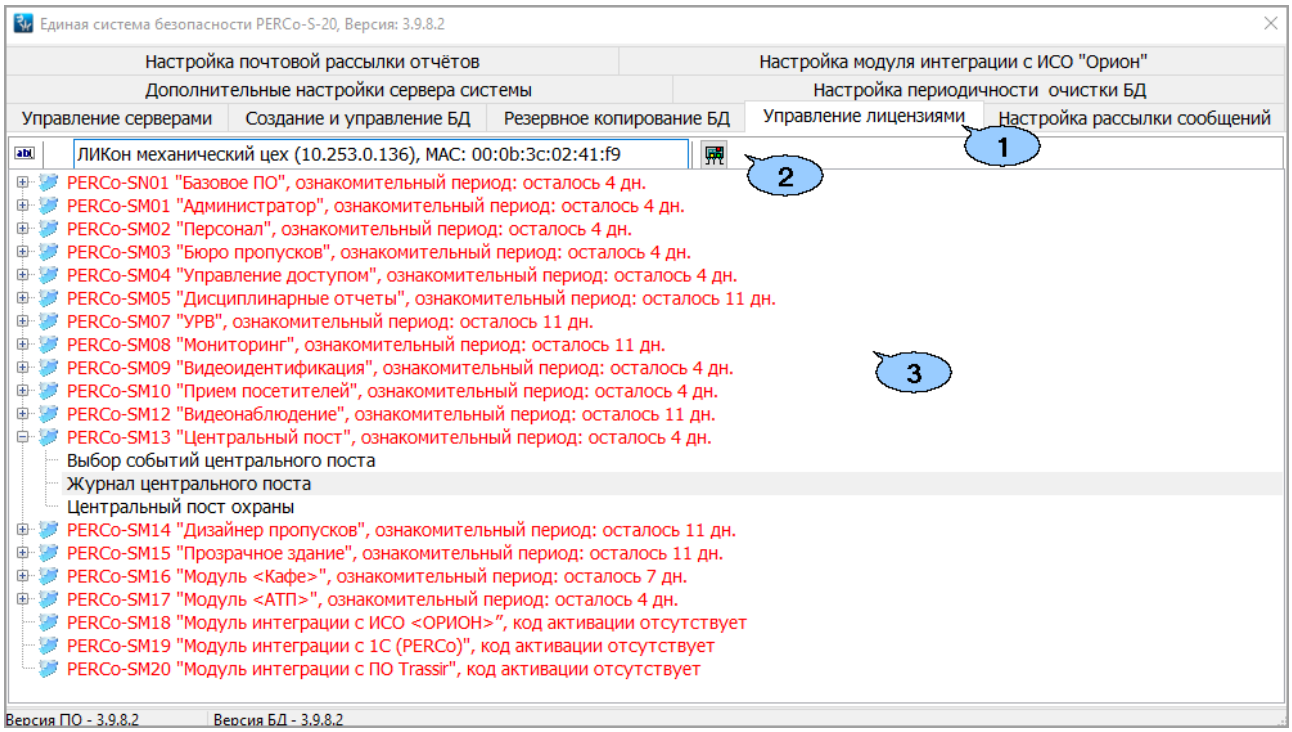
– На сайте компании ***PERCo***, по адресу www.perco.ru в разделе **Поддержка > > Программное обеспечение > ПО PERCo-S-20 > Порядок получения права использования ПО PERCo-S-20 и PERCo-S-20 Школа**.

– Используя бланк заявки, сохраненный при установке ПО. Заполненный бланк необходимо отправить в компанию ***PERCo*** по адресу: mail@perco.ru.

3. После получения лицензионного соглашения, содержащего ключи активации модулей ПО, необходимо ввести их в ***«Центре управления»*** на вкладке **Управление лицензиями**.

### 9.1.2. Вкладка «Управление лицензиями»

Вкладка **Управление лицензиями** ПО ***«Центр управления»*** имеет следующий вид:

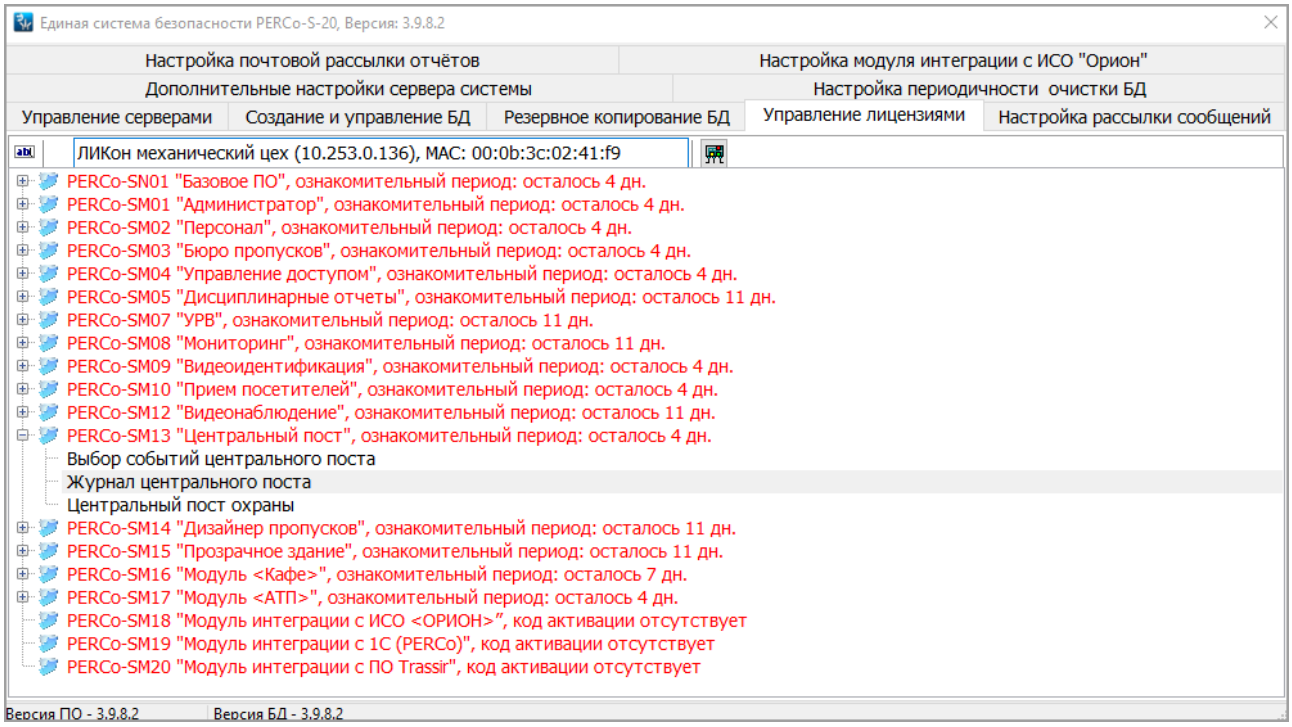



1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями**;
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы**;
   - **Настройка периодичности очистки БД**;
   - **Настройка почтовой рассылки отчетов**;
   - **Настройка модуля интеграции с ИСО "Орион"**.
2. Панель инструментов вкладки содержит следующие элементы:
   - **Изменить код активации** (**Ctrl+E**) – кнопка позволяет ввести ключ активации для модуля, выделенного в рабочей области вкладки.
   - **Выбор контроллера, содержащего лицензию** (**Ctrl+N**) – кнопка позволяет указать контроллер, который будет использоваться в качестве электронного ключа защиты ПО от несанкционированного использования. Выбранный контроллер отображается в поле слева от кнопки.
3. Рабочая область вкладки содержит список модулей сетевого ПО с указанием количества приобретенных по лицензии АРМ.

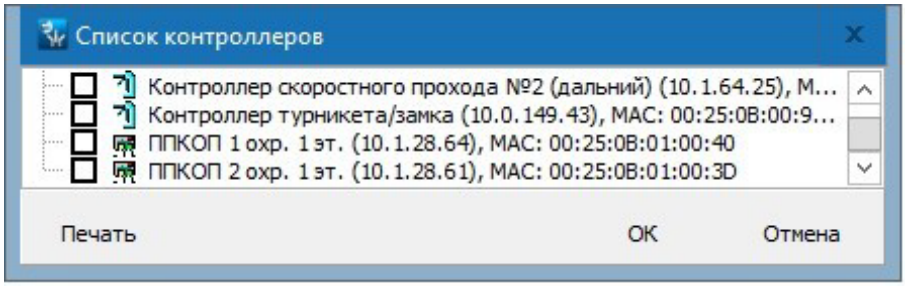
### 9.1.3. Ввод ключа активации

Для ввода ключей активации модулей сетевого ПО выполните следующие действия:

1. Запустите ***«Центр управления»***.
2. В открывшемся окне на вкладке **Управление серверами** убедитесь, что запущены **FireBird SQL сервер** и **Сервер системы PERCo-S-20**. После этого перейдите на вкладку **Управление лицензиями**:




3. В верхней части окна нажмите кнопку  **Выбор контроллера, содержащего лицензию**. Откроется окно **Список контроллеров**:

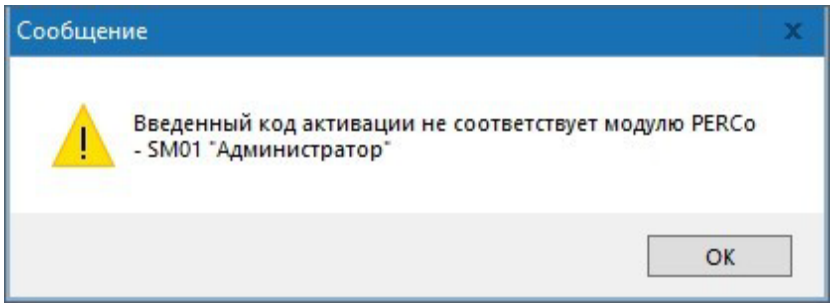



4. В открывшемся окне отметьте флажком контроллер, MAC-адрес которого был указан в заявке для приобретения лицензии на сетевое ПО. Нажмите кнопку **OK**. Окно **Список контроллеров** будет закрыто. Наименование выбранного контроллера появится в верхней части окна. Этот контроллер будет в дальнейшем использоваться в качестве электронного ключа защиты ПО.
5. Выделите в рабочей области окна название модуля, для которого необходимо ввести ключ активации.

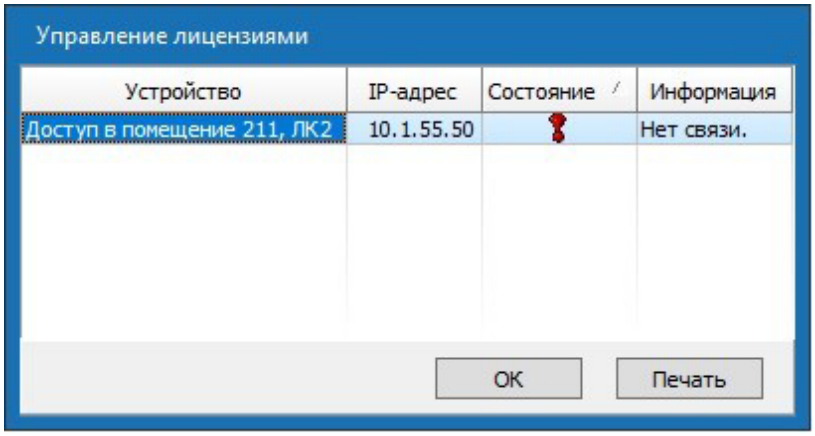
6. Нажмите кнопку **Изменить код активации** в верхней части окна. Откроется панель **Лицензионное соглашение** для ввода ключа активации выделенного модуля:


7. Введите ключ активации, указанный для выделенного модуля в лицензионном соглашении, без пробелов и разделителей. Нажмите кнопку **ОК**. Сервер системы осуществит проверку введенного ключа.

8. В случае ошибки при вводе ключа активации (несоответствии ключа выбранному модулю или контроллеру) откроется окно с соответствующим сообщением:




9. В случае нарушения связи между сервером системы и контроллером, используемым в качестве электронного ключа защиты, откроется окно:

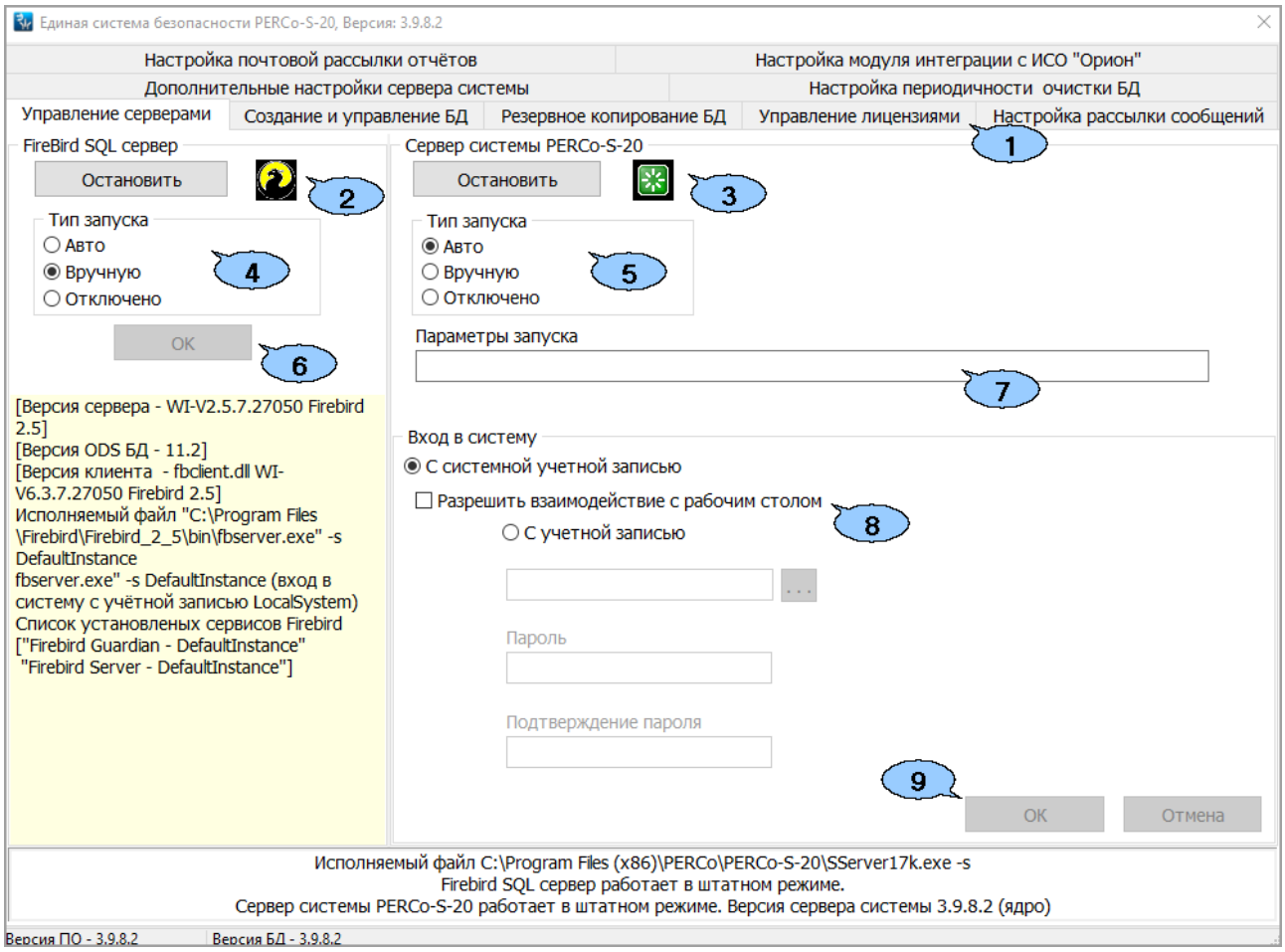



10. В открывшемся окне нажмите кнопку **ОК**. Проверьте наличие связи между сервером системы и контроллером, указанным в лицензионном соглашении. Повторно введите ключ активации, указанный в лицензионном соглашении для выделенного в рабочей области окна модуля.

## 9.2. Создание и управление БД

### 9.2.1. Запуск и остановка СУБД и сервера системы

Запуск и остановка сервера СУБД и сервера системы осуществляется на вкладке **Управление серверами** ПО ***«Центра управления»***:

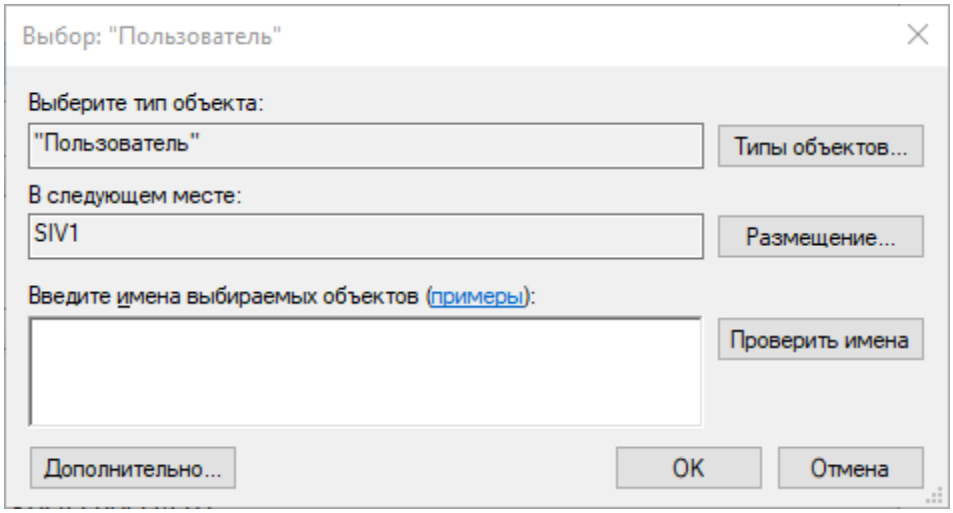



1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями**;
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы**;
   - **Настройка периодичности очистки БД**;
   - **Настройка почтовой рассылки отчетов**;
   - **Настройка модуля интеграции с ИСО «Орион»**.
2. Кнопка **Остановить** / **Запустить Firebird SQL сервер** позволяет остановить / запустить сервер СУБД. Состояние сервера отображается с помощью индикатора, расположенного справа от кнопки:

    – сервер СУБД запущен / остановлен.
3. Кнопка **Остановить** / **Запустить Сервер системы PERCo-S-20** позволяют остановить / запустить сервер системы. Состояние сервера отображается с помощью индикатора, расположенного справа от кнопки:

 /  – сервер системы запущен / остановлен.

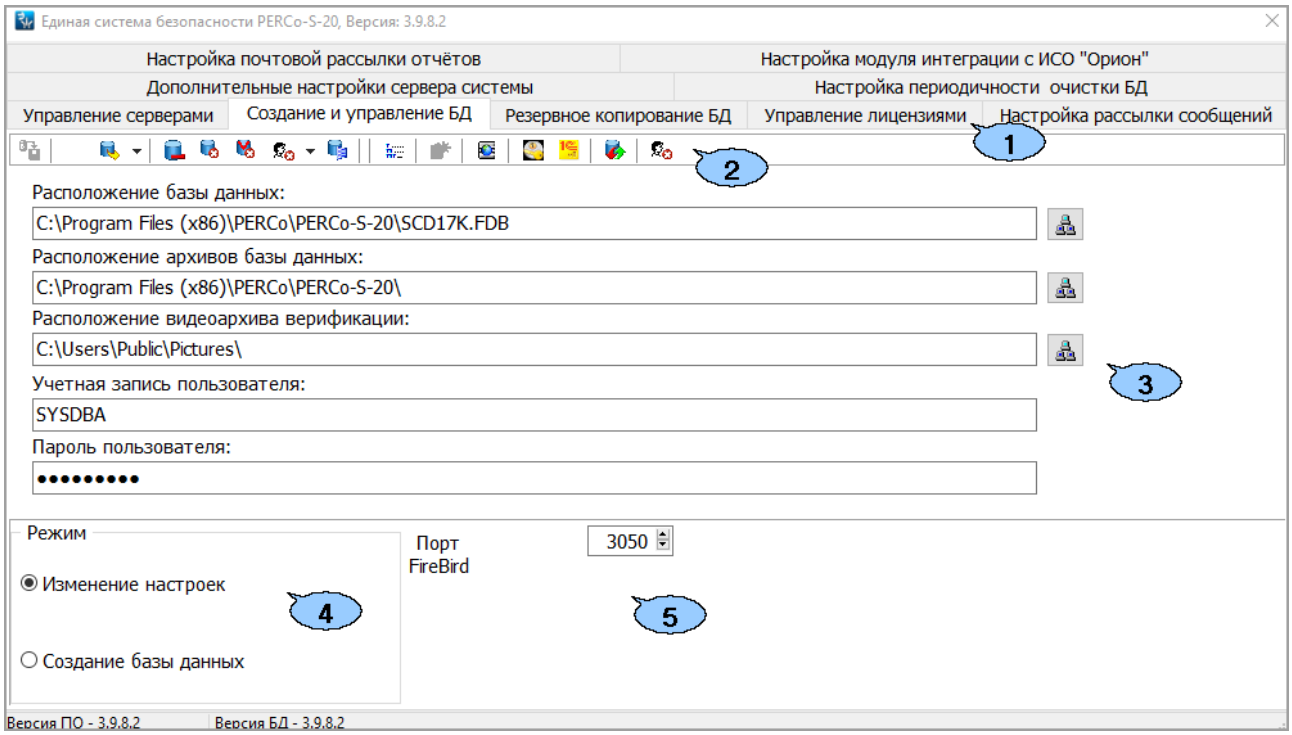
4. Переключатели **Тип запуска** позволяют установить способ запуска СУБД сервера. После изменения положения переключателей необходимо нажать кнопку **ОК**:
   - **Авто** – сервер будет запущен автоматически при запуске ОС.
   - **Вручную** – сервер запускается вручную с помощью кнопки **Запустить**.
   - **Отключено** – запуск сервера невозможен.
5. Переключатели **Тип запуска** позволяют установить способ запуска сервера системы.
   - **Авто** – сервер будет запущен автоматически при запуске ОС.
   - **Вручную** – сервер запускается вручную с помощью кнопки **Запустить**.
   - **Отключено** – запуск сервера невозможен.
6. **ОК** – кнопка сохранения изменений после изменения способа запуска сервера системы или СУБД.
7. **Параметры запуска** – поле для ввода дополнительных параметров при запуске сервера системы.
8. **Вход в систему** – переключатель позволяет выбрать учетную запись пользователя ОС, от имени которого будут запускаться серверы. Для корректной работы серверов (создания почтовой и SMS-рассылок) необходимо, чтобы пользователю были предоставлены полные права администратора ПК.
   - **С системной учетной записью** – запуск серверов осуществляется от имени встроенной учетной записи администратора ПК.
   - **С учетной записью** – запуск серверов осуществляется от имени указанной учетной записи. Для выбора учетной записи нажмите кнопку  . Откроется окно **Выбор: "Пользователь"**:




9. Кнопки:
   - **ОК** – предназначена для сохранения внесенных изменений;
   - **Отмена** – предназначена для отмены внесенных изменений.

### 9.2.2. Вкладка «Создание и управление БД»

Вкладка предназначена для управления настройками БД и имеет следующий вид:



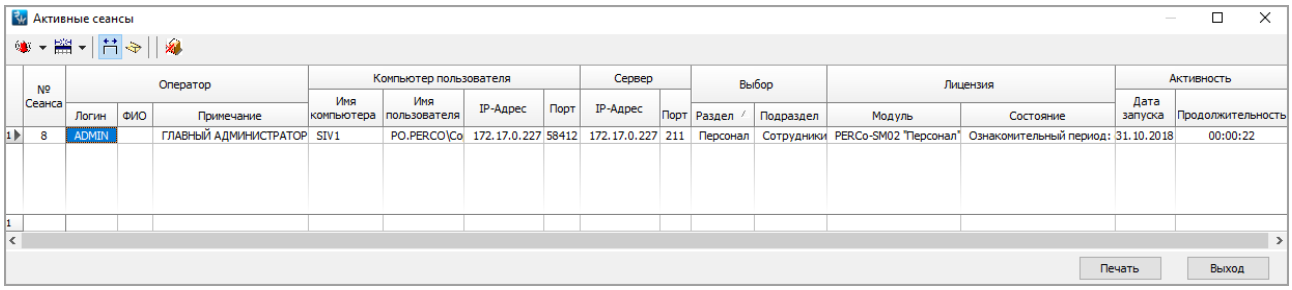

1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями**;
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы**;
   - **Настройка периодичности очистки БД**;
   - **Настройка почтовой рассылки отчетов**;
   - **Настройка модуля интеграции с ИСО «Орион»**.
2. Панель инструментов вкладки:
   - **Сохранение настроек базы данных** (**Ctrl+S**) – кнопка позволяет сохранить изменения, внесенные в параметры БД.
   - **Сохранение базы данных, оптимизация и проверка целостности** (**Ctrl+B**) – кнопка позволяет сохранить резервную копию БД в папке, указанной в поле **Расположение архивов базы данных**. Название файла резервной копии: `Backup1.fbk`. При нажатии стрелки справа от кнопки откроется меню, позволяющее выбрать **Восстановление БД** и **Сохранение БД с последующим восстановлением:**
     – **Восстановление БД** (**Ctrl+R**) – кнопка позволяет восстановить БД из созданной ранее резервной копии, сохраненной в папке, указанной в поле **Расположение архивов базы данных**.
     – **Сохранение БД с последующим восстановлением** (**Ctrl+A**) – кнопка позволяет сохранить резервную копию БД, а затем восстановить БД из резервной копии, что позволяет за счет очистки БД от удаленных ранее событий мониторинга, регистрации, верификации или учетных данных уменьшить размер БД.

- **Удаление данных мониторинга** (**Ctrl+D**) – кнопка позволяет удалить сохраненные в БД события мониторинга за указанный период.
- **Удаление данных по событиям** (**Ctrl+E**) – кнопка позволяет удалить сохраненные в БД события регистрации за указанный период.
- **Удаление данных верификации** (**Ctrl+O**) – кнопка позволяет удалить из папки, указанной в поле **Расположение видеоархива верификации** кадры, записанные с камер наблюдения при проведении процедуры верификации, за указанный период.
- **Очистка БД от удаленных сотрудников / посетителей** – кнопка позволяет удалить из БД системы учетные данные удаленных сотрудников или посетителей за указанный период. При нажатии стрелки справа от кнопки откроется меню, позволяющее выбрать категорию пользователей.

***Примечание:***

Для уменьшения размера БД после удаления событий мониторинга, регистрации, верификации или учетных данных с помощью кнопок , необходимо оптимизировать БД. Для этого сохраните резервную копию БД, используя кнопку **Сохранение базы данных**, **оптимизация и проверка целостности**, а затем восстановите из резервной копии, используя кнопку **Восстановление БД**.

- **Настройки сервера БД** (**Alt+N**) – кнопка позволяет изменить настройки сервера БД, изменить пароль администратора, создать дополнительные учетные записи администратора.
- **Оптимизация индексов** (**Ctrl+I**) – кнопка позволяет оптимизировать работу ПО с БД. Рекомендуется проводить раз в неделю.
- **Создание базы данных** (**Ctrl+N**) – кнопка позволяет создать новую БД. Кнопка доступна при установке переключателя **Режим** в положение **Создание базы данных**.
- **Обновление версии базы данных** (**Ctrl+U**) – кнопка позволяет привести в соответствие версию БД с версией ПО после его обновления.
- **Восстановление предыдущего пароля устройств** (**Alt+R**) – кнопка позволяет восстановить пароль доступа к устройствам системы. Процедура необходима в случае несоответствия пароля, заданного в устройствах системы, паролю, сохраненному в восстановленной БД.
- **Настройка работы со сторонним ПО** (**Ctrl+1**) – кнопка позволяет открыть окно **Настройка работы с 1С (сторонним ПО)** для доступа к дополнительным инструментам подготовки БД к интеграции с системой программ ***1С:Предприятие***.
- **Проверка целостности базы данных** (**Alt+B**) – кнопка позволяет проверить файл БД на наличие ошибок.
- **Показать активные сеансы** – кнопка позволяет открыть окно **Активные сеансы**, содержащее информацию об операторах, подключенных к серверу системы:



На панели инструментов окна доступны следующие элементы:

-  **Настройка обновления информации** – при нажатии стрелки справа от кнопки откроется меню, позволяющее настроить частоту обновления информации о подключенных операторах или провести принудительное обновление.
-  **Отображение столбцов** – при нажатии стрелки справа от кнопки откроется меню, позволяющее выбрать столбцы с данными, отображаемыми в рабочей области вкладки.
-  **Автоматическая настройка ширины колонок включена / Ручная настройка ширины колонок включена** – кнопка позволяет выбрать режим подбора ширины столбцов в рабочей области окна.
-  **Послать сообщение операторам в выбранные сеансы** – кнопка позволяет отправить мгновенное сообщение
- выбранным в рабочей области окна операторам. Сообщение появится в нижней части консоли управления каждого оператора.
-  **Закрыть выбранные сеансы** – кнопка позволяет отключить от БД системы выбранных в рабочей области окна операторов.

3. Рабочая область вкладки:
   - **Расположение базы данных** – поле позволяет ввести название файла БД и указать его расположение. Путь может быть введен вручную или указан в окне **Обзор файлов и папок**. Для открытия окна нажмите кнопку  **Укажите файл БД**, справа от поля ввода. Файл БД должен располагаться на ПК с установленными СУБД и сервером системы. Название файла БД по умолчанию: `C:\SCD17K.FDB`.
   - **Расположение архивов базы данных** – поле позволяет указать путь к папке для сохранения и последующего восстановления файла с резервной копией БД. Одновременно в папке может храниться только одна копия БД. Путь к локальной папке может быть введен вручную. Для указания папки, расположенной на удаленном ПК, нажмите кнопку  **Выбор папки для архивов БД** справа от поля ввода и укажите папку в открывшемся окне **Обзор папок**. Обратите внимание, что к папке в этом случае должен быть предоставлен общий доступ.
   - **Расположение видеоархива верификации** – поле позволяет указать папку для хранения кадров с камер наблюдения, записанных при проведении процедуры верификации. Путь может быть введен вручную или указан в окне **Обзор папок**. Для открытия окна нажмите кнопку  **Выбор папки видеоархива верификации** справа от поля ввода.
   - **Учетная запись пользователя** – поле позволяет указать имя пользователя БД. Учетная запись пользователя задается при создании БД и указывается в случае смены используемой БД. Учетная запись по умолчанию: `SCD17_USER`.
   - **Пароль пользователя** – поле позволяет указать пароль для доступа к БД. Пароль доступа задается при создании БД и указывается в случае смены используемой БД. Пароль по умолчанию: `scd17_password`.

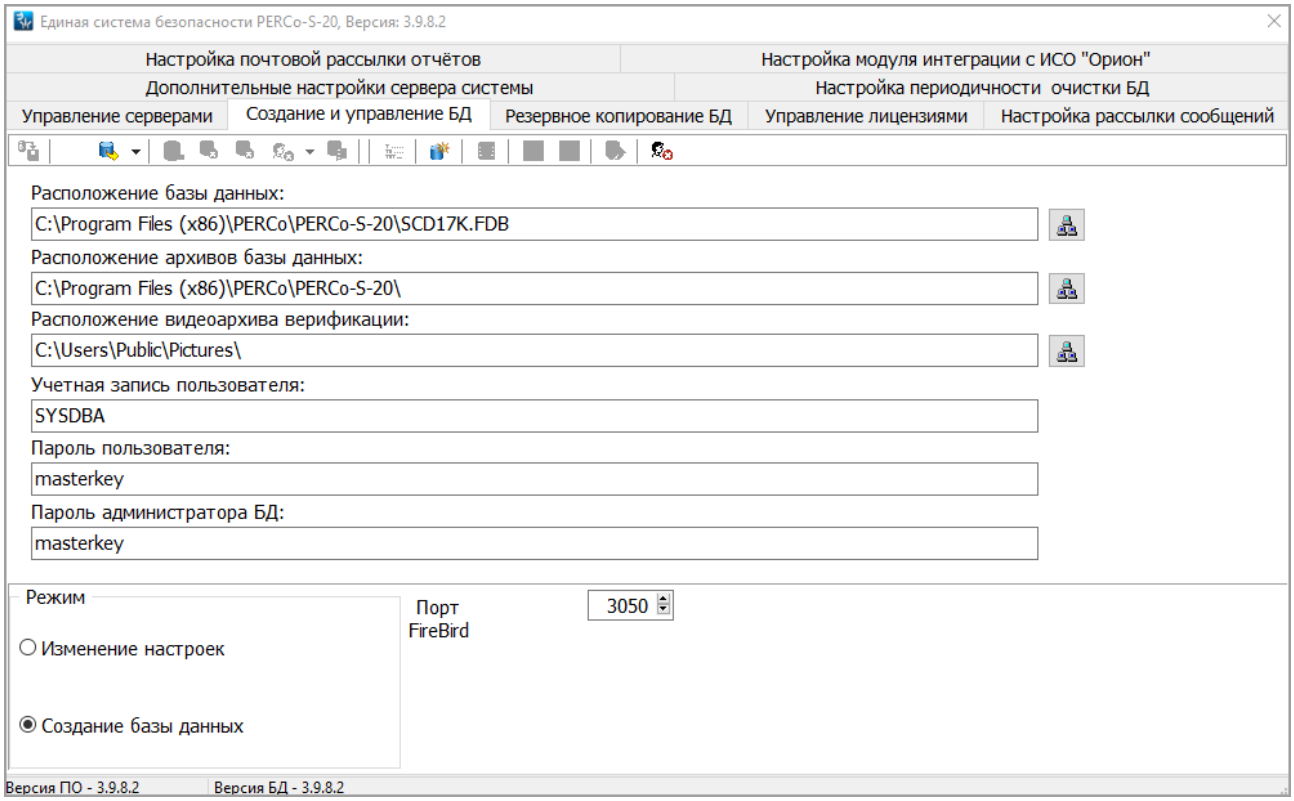
4. Переключатель **Режим** позволяет выбрать режим работы вкладки:
   - **Изменение настроек** – для работы с файлом БД, созданным ранее.
   - **Создание базы данных** – для создания новой БД.

5. **Порт FireBird: по умолчанию** – счетчик позволяет при необходимости изменить сетевой порт обмена данными между запущенной на АРМ ***«Консолью управления»*** и сервером системы (СУБД) **FireBird**. По умолчанию задано значение 3050.

### 9.2.3. Создание БД

Для создания нового файла БД:

1. Запустите ***«Центр управления»***.
2. На вкладке **Управление серверами** убедитесь, что **Firebird SQL Server** и **Сервер системы PERCo-S-20** запущены.
3. Перейдите на вкладку **Создание и управление БД**.
4. На панели **Режим** установите переключатель в положение **Создание базы данных**. Вкладка примет следующий вид:



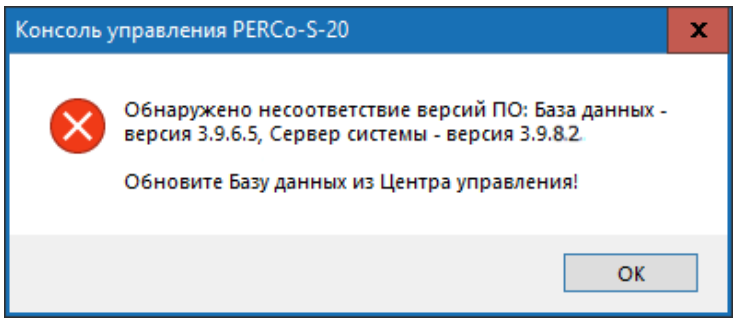

5. В поле **Расположение базы данных** укажите папку, в которой будет создан файл БД. Путь к папке может быть введен вручную или указан в окне **Обзор папок**. Для открытия окна нажмите кнопку  **Укажите файл БД**, справа от поля ввода. Для повышения безопасности не рекомендуется предоставлять общий доступ к этой папке.
6. В поле **Расположение архивов базы данных** укажите путь к папке для сохранения и последующего восстановления файла с резервной копией БД. Рекомендуется хранить файл с резервной копией БД отдельно от основного файла БД на другом жестком диске или другом ПК. Путь к локальной папке может быть введен вручную. Для указания папки, расположенной на удаленном ПК, нажмите кнопку  **Выбор папки для архивов БД** справа от поля ввода и укажите папку в открывшемся окне **Обзор папок**.
7. В поле **Расположение видеоархива верификации** укажите папку, в которой

будут сохраняться кадры с камер наблюдения при проведении процедуры верификации. Путь к папке может быть введен вручную или указан в окне **Обзор папок**. Для открытия окна нажмите кнопку  **Выбор папки видеоархива верификации** справа от поля ввода.

8. В полях **Учетная запись пользователя** и **Пароль пользователя** задайте имя пользователя, пароль для доступа к БД. Эти данные будут необходимы при проведении любых операций с БД.
9. В строке **Пароль администратора БД** введите пароль администратора БД (администратора сервера СУБД). Пароль по умолчанию: `masterkey`.
10. На панели инструментов вкладки нажмите кнопку  **Сохранение настроек базы данных**.
11. На панели инструментов вкладки нажмите кнопку  **Создать базу данных**.
12. Новая БД будет создана. В открывшемся при завершении операции окне с сообщением нажмите кнопку **ОК**.

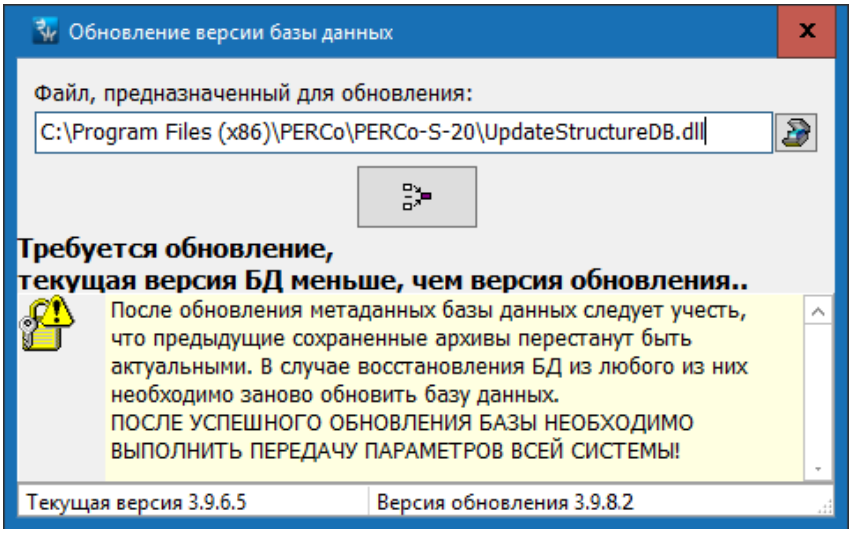
### 9.2.4. Обновление версии БД

Обновление версии БД производится только в случае обновления версии ПО сервера системы. В этом случае при запуске ***«Консоли управления»*** и подключении к серверу системы появится окно с сообщением:



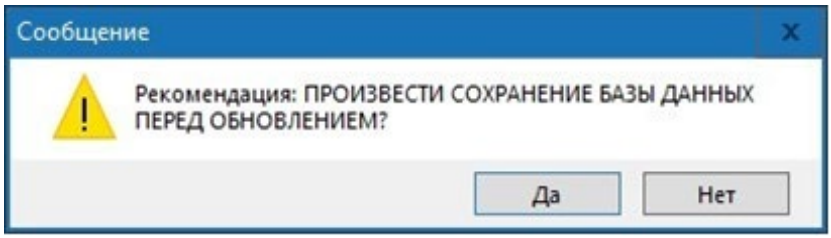

Для обновления версии БД выполните следующие действия:

1. При использовании 64-разрядной операционной системы:
   - Запустите ***«Центр управления»*** и перейдите на вкладку **Управление серверами**.
   - Остановите сервер СУБД с помощью кнопки **Остановить Firebird SQL сервер**.
   - Найдите файл `security2.fdb` в папке, где была установлена старая версия ПО (по умолчанию: `C:\Program Files (x86)\Firebird\Firebird_2_5`).
   - Скопируйте с заменой файл `security2.fdb` в папку с новой версией ПО (по умолчанию: `C:\Program Files\Firebird\Firebird_2_5`).
2. Удалите *Firebird*, используя стандартный компонент *MS Windows «Установка и удаление программ»*. В открывшемся окне выделите строку *«Firebird [версия]»* и нажмите кнопку **Удалить**.
3. Запустите ***«Центр управления»*** и перейдите на вкладку **Создание и управление БД**.
4. На панели инструментов вкладки нажмите кнопку  **Обновление версии базы данных**. Откроется окно **Обновление версии базы данных**:



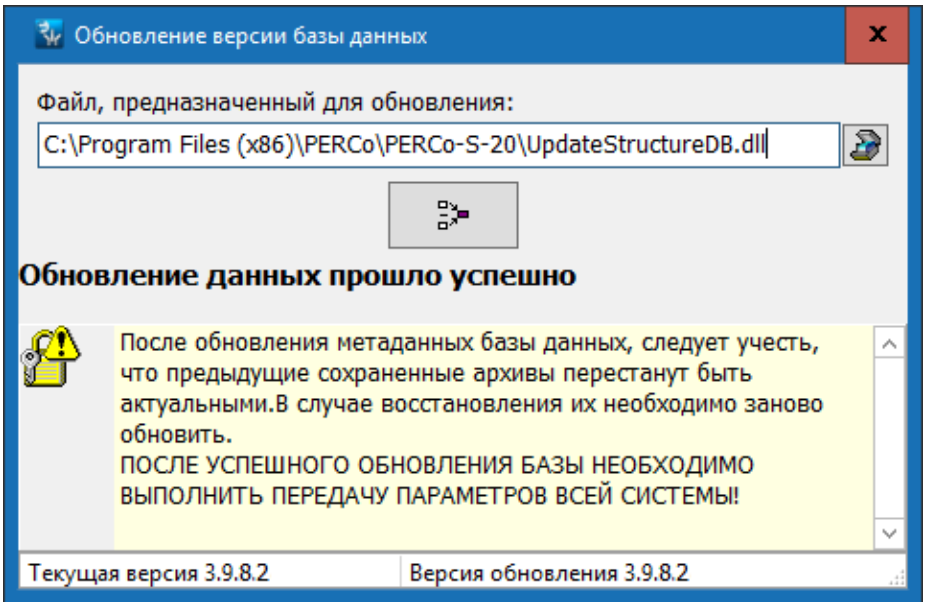

5. В открывшемся окне для изменения пути к файлу `UpdateStructureDB.dll` нажмите кнопку  .

6. Для запуска процедуры обновления БД нажмите кнопку  **Приступить к обновлению**.




7. Для сохранения резервной копии БД в открывшемся диалоговом окне нажмите кнопку **Да**. Исходная версия БД будет сохранена в файле `Backup1.fbk` в папке, указанной в поле **Расположение архивов базы данных**.

8. После окончания процедуры обновления в окне **Обновление версии базы данных** появится сообщение *«Обновление данных прошло успешно»:*




9. Нажмите кнопку  в строке заголовка окна для его закрытия.

### 9.2.5. Создание резервной копии БД

Резервная копия БД необходима для восстановления данных системы в случае потери основного файла БД.

***Примечание:***
В системе предусмотрена возможность регулярного автоматического резервного копирования БД по заранее установленному расписанию. Для настройки расписания перейдите на вкладку **Резервное копирование БД**.

Для сохранения резервной копии БД выполните следующие действия:

1. Запустите ***«Центр управления»*** и перейдите на вкладку **Создание и управление БД**.
2. На панели инструментов вкладки нажмите стрелку справа от кнопки  и в выпадающем списке выберите пункт **Сохранение базы данных, оптимизация и проверка целостности** (**Ctrl+B**). БД будет сохранена в папке, указанной в строке **Расположение архивов базы данных**, в файле с названием `Backup1.fbk`. В указанной папке может сохраняться только одна резервная копия БД.

### 9.2.6. Восстановление БД из резервной копии

Если основной файл БД утерян, то перед восстановлением БД из резервной копии необходимо предварительно создать новую БД, указав в поле **Расположение архивов базы данных** место расположения файла резервной копии `Backup1.fbk`. Для восстановления БД из резервной копии выполните следующие действия:

1. Запустите ***«Центр управления»*** и перейдите на вкладку **Создание и управление БД**.
2. На панели инструментов вкладки нажмите стрелку справа от кнопки  и в выпадающем списке выберите пункт **Восстановление БД**. Будет запущена процедура восстановления БД из файла `Backup1.fbk`, расположенного в папке, указанной в поле **Расположение архивов базы данных**.
3. Файл с восстановленной БД будет помещен в папку с основной БД и иметь то же название, но с добавлением символа `#`. В случае повторного восстановленная, файл будет сохранен без символа `#` в названии. Для имени файла БД по умолчанию: `SCD17K.FDB` имя файла с восстановленной БД будет: `SCD17K#.FDB`.
4. Для начала работы сервера с восстановленной БД перейдите на вкладку **Управление серверами** и перезапустите сервер системы и сервер СУБД.

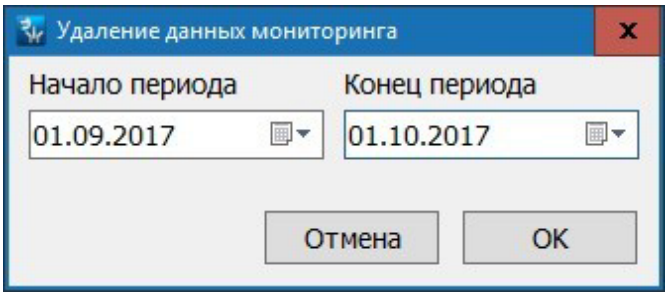
Таким образом, при нормальной работе в папке, указанной в поле **Расположение базы данных**, могут существовать два файла БД: рабочая и предыдущая копия, а также резервная копия БД в папке, указанной в поле **Расположение архивов базы данных**.

### 9.2.7. Очистка БД

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

Для очистки БД произведите следующие действия:

1. Запустите ***«Центр управления»*** и перейдите на вкладку **Создание и управление БД**.
2. Для удаления данных событий мониторинга на панели инструментов вкладки нажмите кнопку **Удаление данных мониторинга**. Откроется окно **Удаление данных мониторинга**:

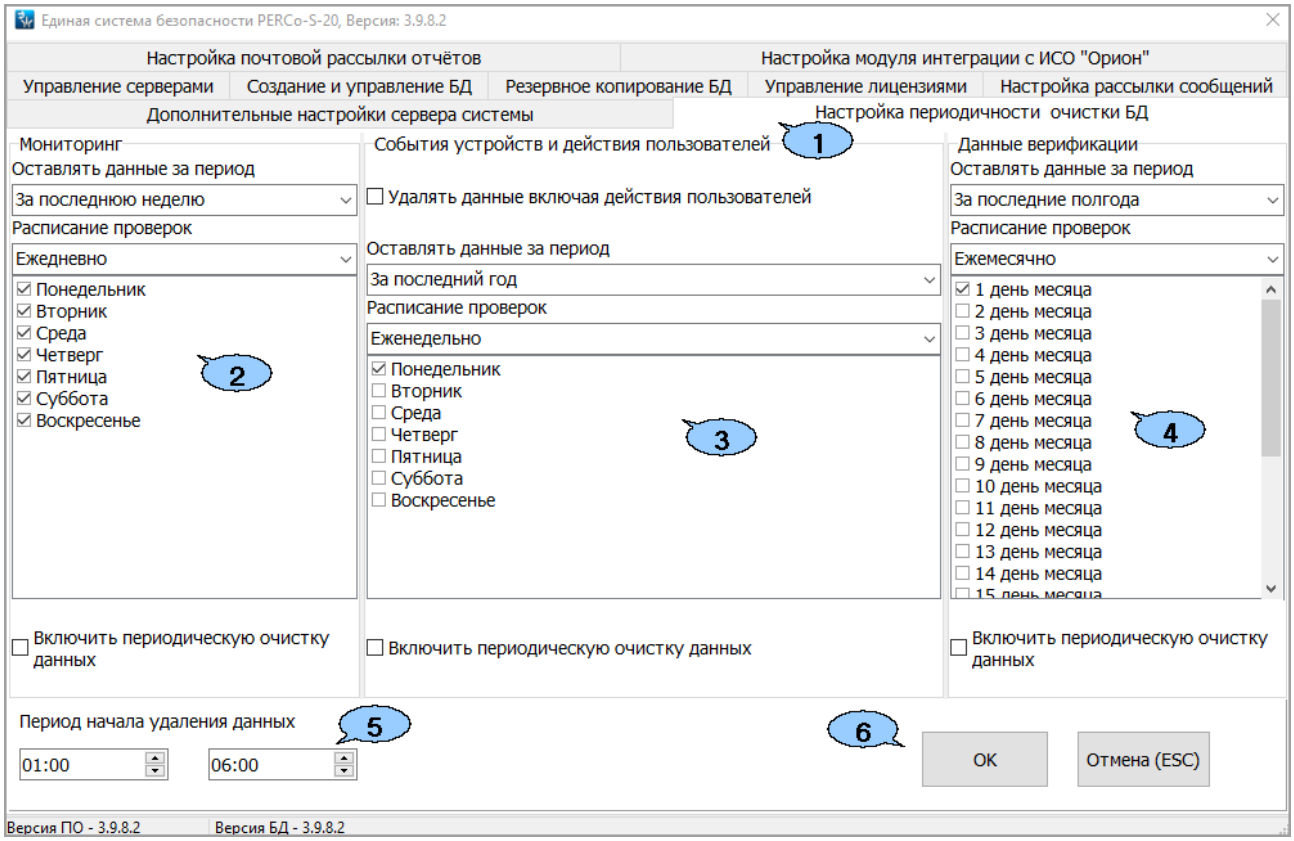



3. В открывшемся окне установите с помощью полей ввода дат **Начало периода** и **Конец периода** временной промежуток, за который будут удалены события. Нажмите кнопку **ОК**. События из журнала мониторинга будут удалены.
4. Для удаления событий регистрации на панели инструментов вкладки нажмите кнопку **Удаление данных по событиям**.
5. В открывшемся окне **Удаление данных по событиям** установите с помощью полей ввода дат **Начало периода** и **Конец периода** временной промежуток, за который будут удалены события. Нажмите кнопку **ОК**. События из журнала регистрации будут удалены.
6. Для удаления сохраненных при проведении процедуры верификации кадров с камер на панели инструментов вкладки нажмите кнопку **Удаление данных верификации**.
7. В открывшемся окне **Удаление данных верификации** установите с помощью полей ввода дат **Начало периода** и **Конец периода** временной промежуток, за который будут удалены кадры. Нажмите кнопку **ОК**. Кадры верификации будут удалены.
8. Для оптимизации БД после очистки и уменьшения размера файла необходимо на панели инструментов вкладки нажать стрелку справа от кнопки и в выпадающем списке выбрать пункт **Сохранение базы данных, оптимизация и проверка целостности**. Резервная копия БД будет сохранена в папке, указанной в строке **Расположение архивов базы данных**.
9. После этого необходимо обновить БД из сохраненной резервной копии. Для этого на панели инструментов вкладки нажмите стрелку справа от кнопки и в выпадающем списке выберите пункт **Восстановление БД**. Будет запущена процедура восстановления БД из резервной копии.

При необходимости можно настроить автоматическую очистку БД на вкладке **Настройка периодичности очистки БД**.

## 9.2.8. Настройка периодичности очистки БД

Вкладка предназначена для задания периодичности автоматической очистки БД и имеет следующий вид:




1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями**;
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы**;
   - **Настройка периодичности очистки БД**;
   - **Настройка почтовой рассылки отчетов**;
   - **Настройка модуля интеграции с ИСО "Орион"**.
2. Панель **Мониторинг** позволяет настроить периодичность очистки данных мониторинга и содержит следующие функции:
   - **Оставлять данные за период** – с помощью выпадающего списка можно установить, данные за какой период будут храниться в системе:
     - за последнюю неделю;
     - за последний месяц;
     - за последние полгода;
     - за последний год.
   - **Расписание проверок** – с помощью выпадающего списка можно выбрать, как часто будет проходить проверка БД на удаление данных:
     - ежедневно;
     - еженедельно;
     - ежемесячно.

- **Включить периодическую очистку данных** – установите флажок для включения функции периодической очистки данных.

3. Панель **События устройств и действия пользователей** позволяет настроить периодичность очистки событий устройств и действий пользователей и содержит следующие функции:
   - **Удалять данные включая действия пользователей** – при установке флажка будут удаляться все данные, включая все действия пользователей. Если флажок не устанавливать, будут удалены только события устройств.

***Примечание:***
Установка флажка на параметр **Удалять данные включая действия пользователей** не рекомендуется по соображениям безопасности, так как это может привести к потере важных сведений, к примеру, информации об увольнении или принятии на работу сотрудников.

   - **Оставлять данные за период** – с помощью выпадающего списка можно установить, данные за какой период будут храниться в системе:
     – за последнюю неделю;
     – за последний месяц;
     – за последние полгода;
     – за последний год.
   - **Расписание проверок** – с помощью выпадающего списка можно выбрать, как часто будет проходить проверка БД на удаление данных:
     – ежедневно;
     – еженедельно;
     – ежемесячно.
   - **Включить периодическую очистку данных** – установите флажок для включения функции периодической очистки данных.

4. Панель **Данные верификации** позволяет настроить периодичность очистки данных верификации и содержит следующие функции:
   - **Оставлять данные за период** – с помощью выпадающего списка можно установить, данные за какой период будут храниться в системе:
     – за последнюю неделю;
     – за последний месяц;
     – за последние полгода;
     – за последний год.
   - **Расписание проверок** – с помощью выпадающего списка можно выбрать, как часто будет проходить проверка БД на удаление данных:
     – ежедневно;
     – еженедельно;
     – ежемесячно.
   - **Включить периодическую очистку данных** – установите флажок для включения функции периодической очистки данных.

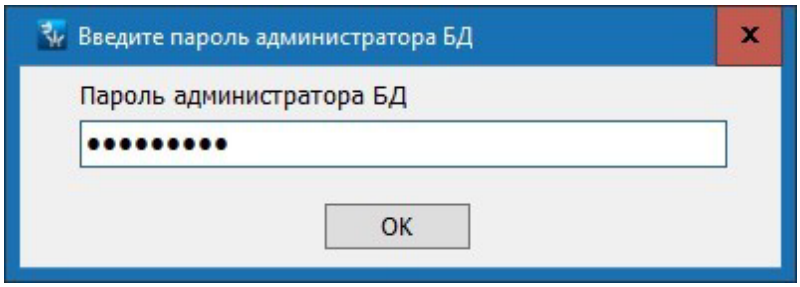
5. Панель **Период начала удаления данных** позволяет задать временной промежуток, в который будет начинаться очистка БД. Например, при установке *14:00-18:00* очистка БД может начаться в любой момент с 14:00 до 18:00.

6. Кнопки:
   - **ОК** – предназначена для сохранения внесенных изменений;
   - **Отмена (ESC)** – предназначена для отмены внесенных изменений.

### 9.2.9. Настройки сервера БД

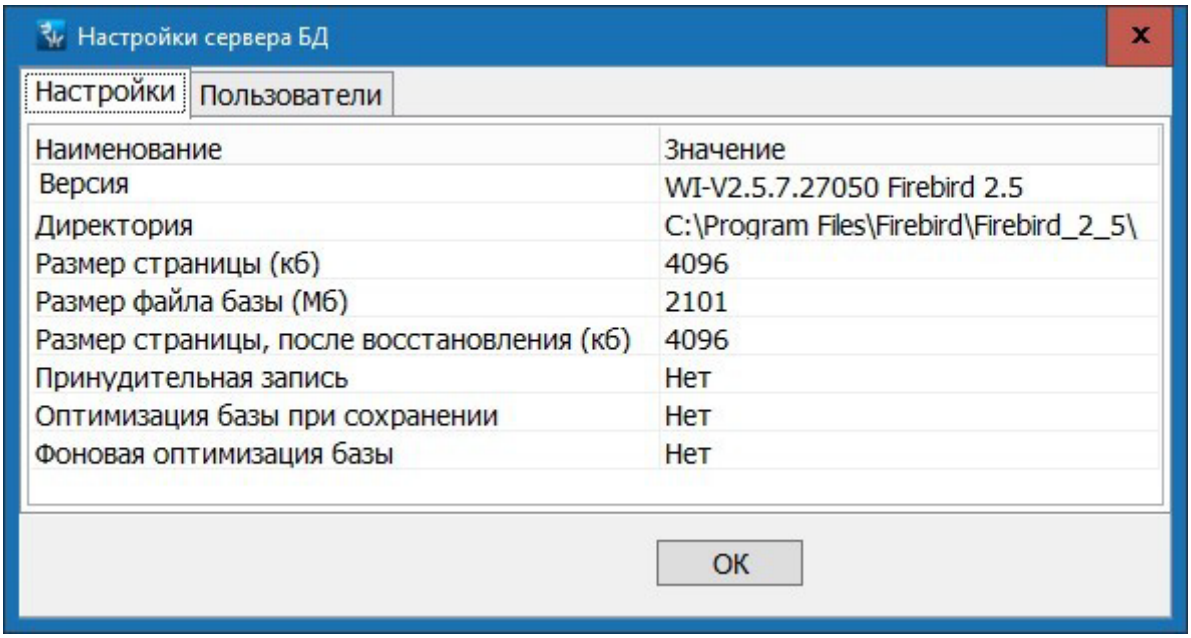
Для доступа к настройкам сервера БД:

1. Запустите ***«Центр управления»*** и перейдите на вкладку **Создание и управление БД**.
2. На панели инструментов вкладки нажмите кнопку **Настройки сервера БД**. Откроется окно **Введите пароль администратора**:




3. В открывшемся окне введите пароль администратора БД и нажмите кнопку **ОК** (пароль по умолчанию: `masterkey`). Откроется окно **Настройки сервера БД**, содержащее две вкладки:
   - **Настройки;**
   - **Пользователи**.

**Вкладка «Настройки»** выглядит следующим образом:




Рабочая область вкладки **Настройки** содержит следующие поля с данными и параметры сервера СУБД:

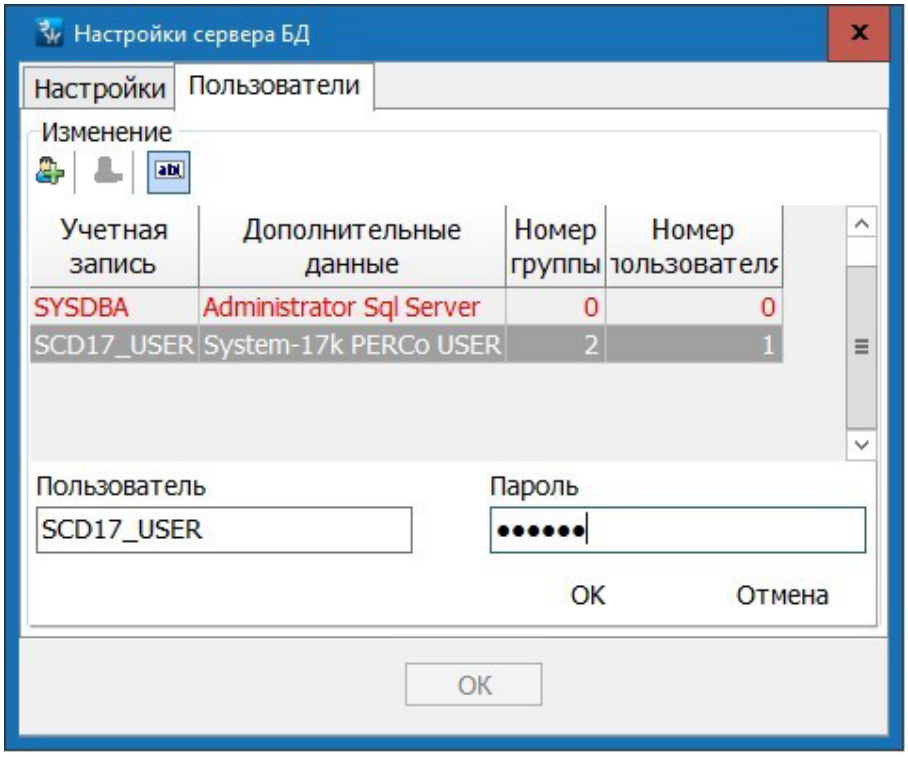
- **Версия** – версия запущенного сервера.
- **Директория** – папки установки сервера СУБД.
- **Количество баз** – количество подключенных к серверу БД.
- **Количество соединений** – количество подключенных к серверу клиентов.
- **Размер страницы (кб)** – установленный размер страницы файла БД.
- **Размер файла базы (Мб)** – текущий размер файла БД, подключенной к серверу.
- **Размер страницы, после восстановления (кб)** – раскрывающийся список позволяет изменить размер страницы файла БД. Для оптимизации работы с БД рекомендуется установить значение параметра кратным размеру кластера

жесткого диска, на котором работает БД. По умолчанию установлено значение 4096 байт. После изменения значения параметра необходимо сохранить резервную копию БД, после чего использовать ее в качестве основной.

- **Принудительная запись:**
  - **Да** – позволяет повысить надежность сохранения данных, уменьшив при этом скорость работы с БД.
  - **Нет** – позволяет увеличить скорость операций с БД за счет использования системного кэша в памяти ПК. В случае сбоя в питании ПК данные, находящиеся в кэше, могут быть потеряны.
- **Оптимизация базы при сохранении**
  - **Да** – при сохранении резервной копии БД производиться ее оптимизация.
  - **Нет** – оптимизация резервной копии БД не производится.
- **Фоновая оптимизация базы**
  - **Да** – оптимизация БД производится в процессе работы, при этом работа с файлом БД может быть замедлена.
  - **Нет** – фоновая оптимизация не производится.

Для закрытия окна с сохранением внесенных изменений нажмите кнопку **ОК**.

**Вкладка «Пользователи»** выглядит следующим образом:




В рабочей области вкладки содержится список учетных записей администратора и пользователей БД. Красным выделены учетные записи, которые не могут быть удалены. Это записи администратора БД: `sysdba` и запись пользователя подключенной БД: по умолчанию `scd17_user`.

Панель инструментов вкладки:

- **Добавить пользователя** – кнопка позволяет открыть панель ввода данных для добавления новых пользователей БД. Добавление пользователя может потребоваться в случае подключения БД к другому серверу, то есть не к тому, на котором БД была создана.
- **Удалить пользователя** – кнопка позволяет удалить выделенную в рабочей области вкладки учетную запись пользователя.

- **Изменение пароля** – кнопка позволяет открыть панель ввода данных для изменения пароля, выделенного в рабочей области вкладки пользователя или администратора. Обратите внимание, что пароли регистрозависимы.

***Внимание!***

Рекомендуется изменить пароль `masterkey` администратора БД, заданный по умолчанию, на пароль известный только администратору системы.

## 9.2.10. Восстановление предыдущего пароля устройств

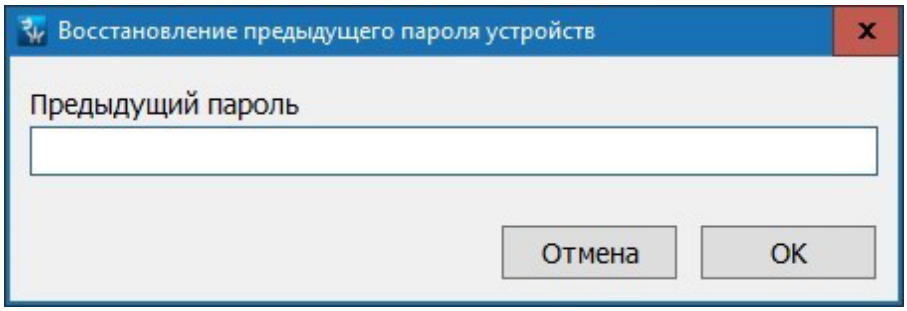
Восстановление предыдущего пароля доступа к устройствам системы может потребоваться после восстановления БД из резервной копии, в случае если после создания резервной копии пароль был изменен. То есть если пароль, сохраненный в устройствах, отличается от пароля, используемого в БД.

***Примечание:***

При проведении процедуры восстановления пароля все «***Консоли управления»*** должны быть закрыты.

Для восстановления предыдущего пароля, после восстановления БД из резервной копии:

1. Запустите ***«Центр управления»*** и перейдите на вкладку **Создание и управление БД**.
2. Нажмите кнопку **Восстановление предыдущего пароля устройств** на панели инструментов вкладки. Откроется окно **Восстановление предыдущего пароля устройств**:




3. В открывшемся окне в поле **Предыдущий пароль** введите пароль, сохраненный в устройствах системы, то есть используемый до восстановления БД. Нажмите на кнопку **ОК**.
4. В открывшемся окне подтверждения изменения пароля нажмите кнопку **Да**. После проведения процедуры восстановления в системе будет использоваться пароль из резервной копии БД.
5. Закройте окно **Единая система безопасности**, нажав кнопку в строке заголовка окна.
6. Запустите ***«Консоль управления»*** и перейти в раздел ***«Конфигуратор»***.
7. Передайте восстановленный пароль в устройства системы. Для этого в рабочей области раздела выберите корневой элемент списка устройств (по умолчанию **Система безопасности**) и нажмите на панели инструментов раздела кнопку **Передать параметры**.

## 9.2.11. Интеграция с 1С:Предприятие 8

В результате интеграции функция учета рабочего времени сотрудников передается системе программ ***1С: Предприятие***. Расчет производится на основании событий входа-выхода, регистрируемых контроллерами системы. При интеграции производится синхронизация следующих данных:

- Список структурных подразделений предприятия;
- Должности сотрудников;
- Графики работы и праздничные дни;
- Список сотрудников и их учетные данные.

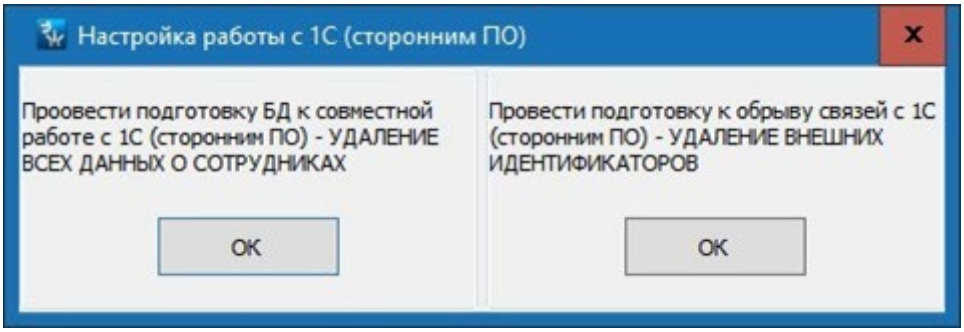
После проведения синхронизации редактирование этих данных будет возможно только в системе программ ***1С:Предприятие***. Провести интеграцию с ***1С:Предприятие*** можно следующими способами:

1. С помощью ***PERCo-SM19 «Модуль интеграции с 1С»,*** разработанного компанией ***PERCo***.

***Примечание:***
Дополнительная информация о работе системы с модулем ***PERCo-SM19 «Модуль интеграции с 1С»*** доступна на сайте компании ***PERCo*** по адресу www.perco.ru в разделе **Поддержка > Документация**.

Для проведения интеграции системы с системой программ ***1С:Предприятие 8:***

- Установите модуль ***PERCo-SM19 «Модуль интеграции с 1С»***, входящий в установочный файл ***«Сетевое программное обеспечение S-20»***.
- Запустите ***«Центр управления»*** и перейдите на вкладку **Создание и управление БД**.
- Нажмите кнопку **Настройка работы со сторонним ПО** на панели инструментов вкладки. Откроется окно **Настройка работы с 1С (сторонним ПО)**:




  - **Проведение подготовки БД к совместной работе с 1С** . Из БД системы ***PERCo-S-20*** будут удалены все синхронизируемые данные. То есть при синхронизации все данные для учета рабочего времени будут получены из БД системы программ ***1С:Предприятие***.
  - **Проведение подготовки к обрыву связей с 1С.** Будет прекращена синхронизация БД системы ***PERCo-S-20*** и БД системы программ ***1С:Предприятие***. При этом вся добавленная при синхронизации информация будет сохранена. Все функции ***«Консоли управления»*** по работе с данными будут восстановлены.
- Для подготовки БД к работе со сторонним ПО нажмите кнопку **ОК** в левой части открывшегося окна.
- Закройте окно **Единая система безопасности**, нажав кнопку в строке заголовка окна.

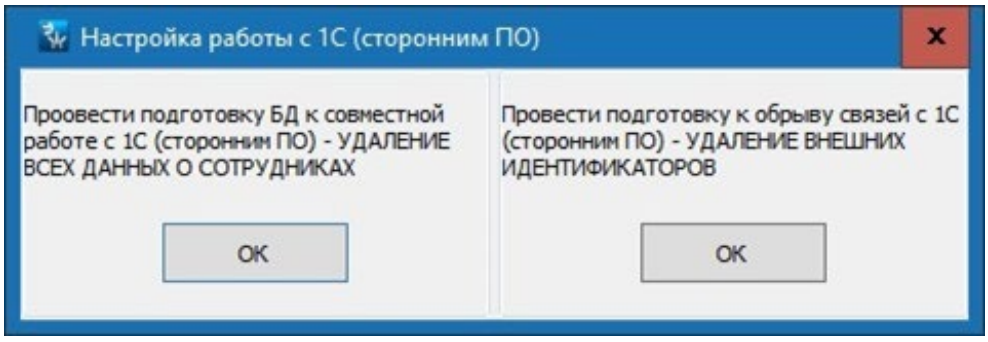
- Запустите ***1С:Предприятие*** и откройте файл внешней обработки ***SM19_1C_Integration_ZUP_xxxxxx.epf*** (где ***xxxxxx*** – версия обработки) модуля ***PERCo-SM19 «Модуль интеграции с 1С»*.** По умолчанию обработка находится в папке с установленным ПО системы ***PERCo-S-20.*** Следуйте рекомендациям руководства пользователя модуля.

2. С помощью модуля **Поддержка интеграции с 1С для Формула Ай-Ти,** разработанного компанией ***PERCo,*** и ПО ***ФОРМУЛА: Модуль «Учет рабочего времени» Интеграция PERCo-S-20 и 1С: Предприятия 8.2*,** разработанного компанией **Формула Ай-Ти**.

***Примечание:***
Дополнительная информация о работе системы с модулем ***ФОРМУЛА: Модуль «Учет рабочего времени» Интеграция PERCo-S-20 и 1С:Предприятие 8.2*** доступна на сайте компании ***PERCo***, по адресу www.perco.ru в разделе **Поддержка > Документация**.

Для проведения интеграции системы с системой программ ***1С:Предприятие 8***:

- Установите приобретаемый отдельно модуль ПО ***ФОРМУЛА: Модуль «Учет рабочего времени» Интеграция PERCo-S-20 и 1С:Предприятия 8.2***.
- На тот же ПК установите модуль **Поддержка интеграции с 1С для Формула Ай-Ти**, входящий в установочный файл ***«Сетевое программное обеспечение S-20»***.
- Запустите ***«Центр управления»*** и перейдите на вкладку **Создание и управление БД**.
- Нажмите кнопку **Настройка работы со сторонним ПО** на панели инструментов вкладки. Откроется окно **Настройка работы с 1С (сторонним ПО)**:

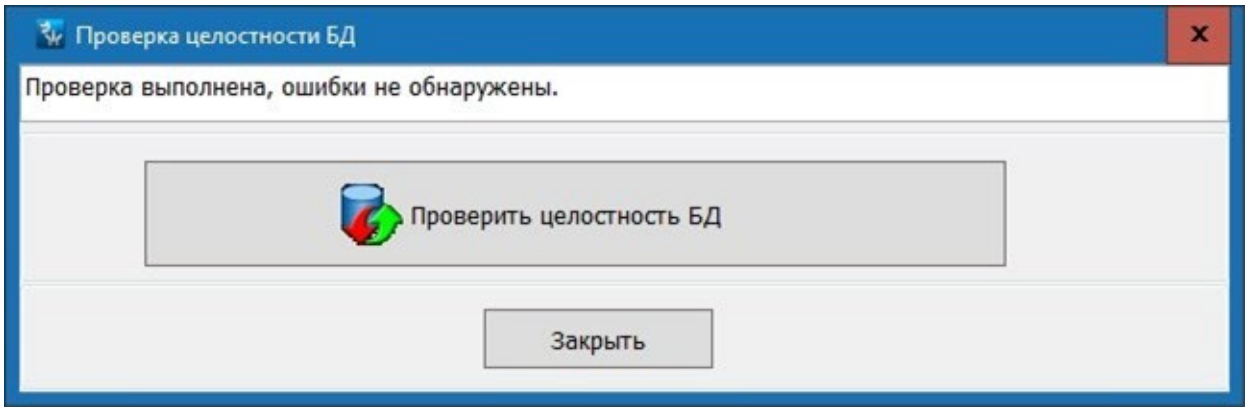



  - **Проведение подготовки БД к совместной работе с 1С**. Из БД системы ***PERCo-S-20*** будут удалены все синхронизируемые данные. То есть при синхронизации все данные для учета рабочего времени будут получены из БД системы программ ***1С:Предприятие***.
  - **Проведение подготовки к обрыву связей с 1С.** Будет прекращена синхронизация БД системы ***PERCo-S-20*** и БД системы программ ***1С:Предприятие***. При этом вся добавленная при синхронизации информация будет сохранена. Все функции ***«Консоли управления»*** по работе с данными будут восстановлены.
- Для подготовки БД к работе со сторонним ПО нажмите кнопку **ОК** в левой части открывшегося окна.
- Закройте окно **Единая система безопасности**, нажав кнопку в строке заголовка окна.
- Запустите модуль ***ФОРМУЛА: Модуль «Учет рабочего времени» Интеграция PERCo-S-20 и 1С: Предприятия 8.2***. Следуйте рекомендациям руководства пользователя модуля.

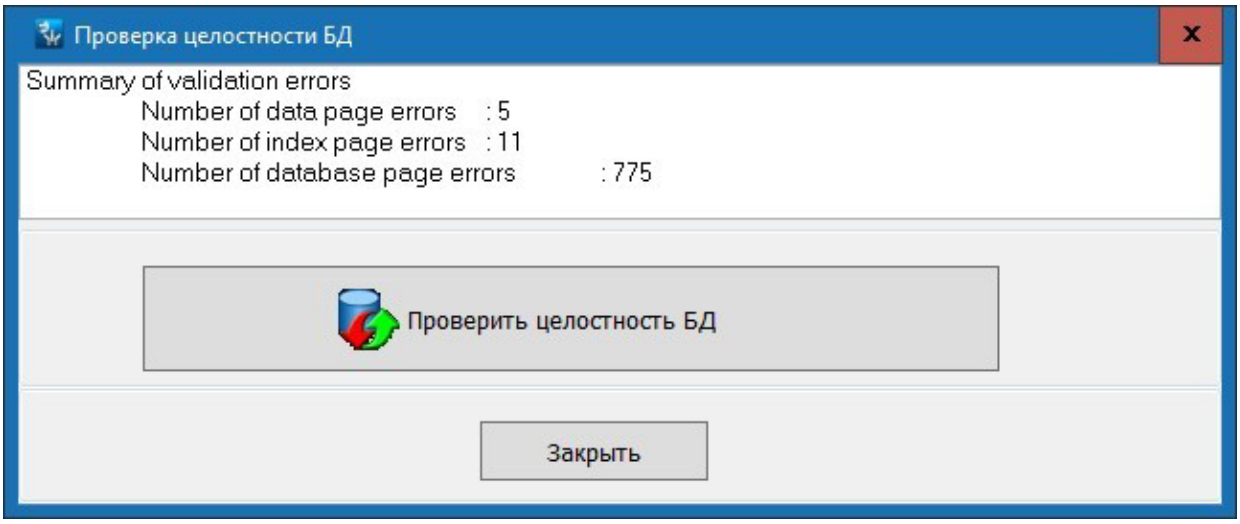
## 9.2.12. Проверка целостности БД

Для проверки БД системы на наличие ошибок:

1. Запустите ***«Центр управления»*** и перейдите на вкладку **Создание и управление БД**.
2. Нажмите кнопку **Проверка целостности БД** на панели инструментов вкладки. Откроется окно **Проверка целостности БД**.
3. В открывшемся окне нажмите кнопку **Проверка целостности БД**. Начнется проверка БД.
4. Если при проверке ошибки не обнаружены, то в рабочей области окна появится сообщение: *«Проверка выполнена, ошибки не обнаружены»*:




5. В случае обнаружения ошибок в рабочей области окна появится отчет об их характере и количестве:




6. При обнаружении ошибок нажмите кнопку **Попытка восстановления целостности БД**.
7. В случае успешного исправления обнаруженных ошибок файл БД будет заменен восстановленным файлом, а файл с ошибками будет сохранен с расширением `.bad`. В появившемся окне с сообщением нажмите кнопку **ОК**.

В случае невозможности исправления обнаруженных ошибок произведите восстановление БД из резервной копии.

## 9.3. Планировщик резервного копирования БД

### 9.3.1. Вкладка «Резервное копирование БД»

Создание резервной копии БД необходимо, чтобы исключить возможность потери данных в случае выхода из строя ПК сервера системы. В системе предусмотрены возможности ручного и автоматического сохранения резервных копий используемой БД.

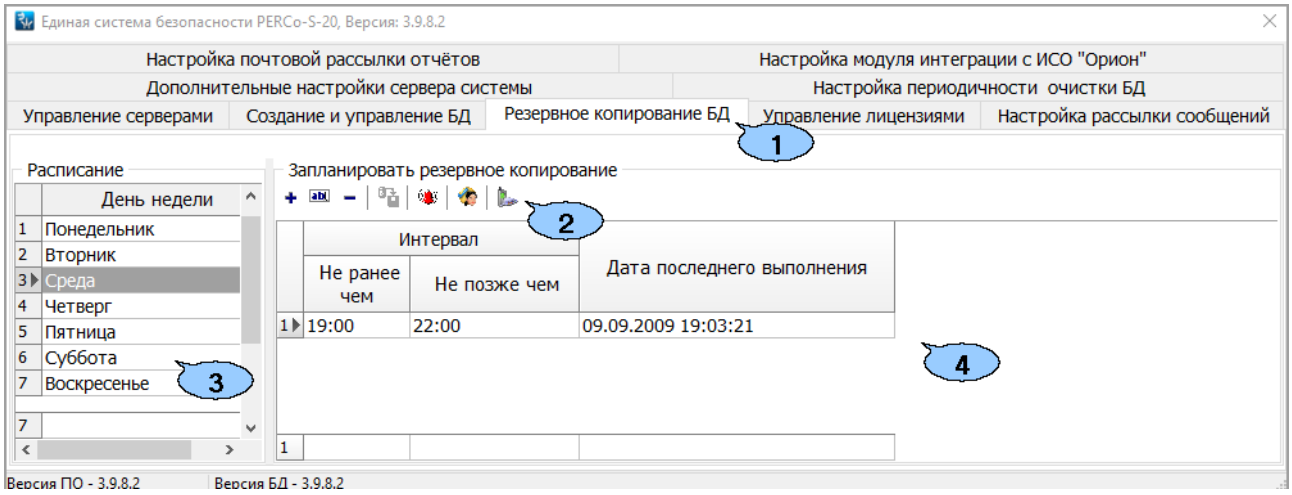
Для немедленного создания резервной копии БД перейдите на вкладку **Создание и управление БД** и нажмите кнопку **Сохранение базы данных** на панели инструментов вкладки.

Настройка расписания автоматического резервного копирования производится на вкладке **Резервное копирование БД** ПО ***«Центр управления»***. Резервная копия БД будет сохранена в каталоге, указанном в строке **Расположение архивов базы данных** вкладки **Создание и управление БД**. При этом в каталоге всегда хранится только одна, последняя резервная копия БД.

При создании резервной копии БД существует возможность отправки уведомлений через службу сообщений Windows, по электронной почте или SMS-сообщением. Доступны два условия отправки уведомлений:

- **Всегда** – уведомление отправляется при каждой попытке создания резервной копии БД.
- **В случае ошибки** – уведомление отправляется только в случае, если ПО не сможет создать резервную копию БД.

Вкладка **Резервное копирование БД** имеет следующий вид:




1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями**;
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы**;
   - **Настройка периодичности очистки БД**;
   - **Настройка почтовой рассылки отчетов**;
   - **Настройка модуля интеграции с ИСО "Орион"**.

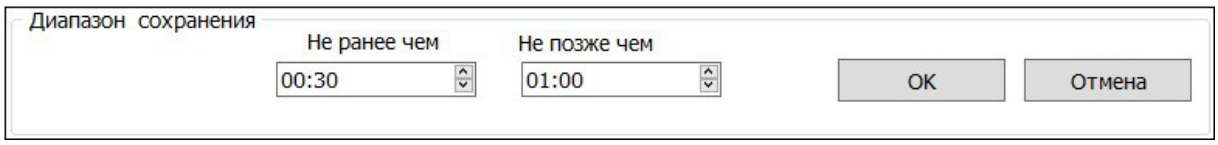
2. Панель инструментов вкладки:
   - **Добавление** (**Ctrl+N**) – кнопка позволяет установить время создания резервной копии БД для дня недели, выбранного на панели **Расписание**.
   - **Редактирование** (**Ctrl+E**) – кнопка позволяет изменить время резервного копирования БД, выделенное в рабочей области вкладки.
   - **Удаление** (**Ctrl+D**) – кнопка позволяет удалить время резервного копирования, выделенное в рабочей области вкладки.
   - **Сохранение расписания** (**Ctrl+S**) – кнопка позволяет сохранить изменения в расписании резервного копирования БД.
   - **Настроить сетевую рассылку уведомлений** (**Alt+S**) – кнопка позволяет настроить рассылку уведомлений на ПК с помощью *Службы сообщений MS Windows*.
   - **Настроить почтовую рассылку уведомлений** (**Ctrl+M**) – кнопка позволяет настроить рассылку уведомлений на ящики электронной почты.
   - **Настройка SMS-рассылки** – кнопка позволяет настроить рассылку уведомлений на телефоны с помощью SMS-сообщений.
3. Панель **Расписание** позволяет выбрать день недели для настройки расписания резервного копирования.
4. Рабочая область **Запланировать резервное копирование** вкладки содержит установленное время создания резервной копии БД для выбранного на панели **Расписание** дня недели.

### 9.3.2. Создания расписания резервного копирования БД

***Примечание:***
Рекомендуется производить резервное копирование БД ежедневно в часы наименьшей нагрузки на систему. При работе сервера системы в круглосуточном режиме производите резервное копирование в ночное время.

Для создания расписания резервного копирования:

1. Запустите ***«Центр управления»*** и перейдите на вкладку **Резервное копирование БД**.
2. На панели **Расписание** выберите день недели, для которого необходимо добавить время создания резервной копии БД.
3. Нажмите на панели инструментов вкладки кнопку **Добавление**. В нижней части окна откроется панель **Диапазон сохранения**:




4. На открывшейся панели с помощью полей ввода времени **Не ранее чем** и **Не позже чем** установите интервал времени, в течение которого сервер системы произведет резервное копирование БД. Нажмите на кнопку **ОК**. Панель **Диапазон сохранения** будет закрыта. Созданный интервал будет добавлен в рабочую область вкладки.

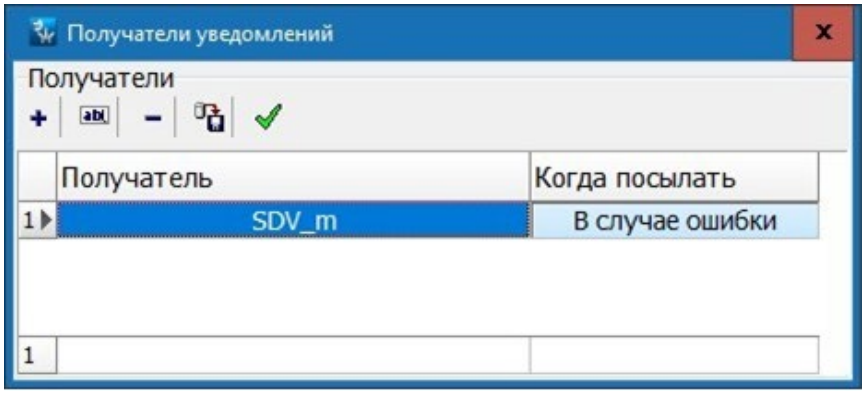
5. При необходимости добавьте дополнительные интервалы времени резервного копирования.
6. Для изменения временного интервала выделите его в рабочей области вкладки и нажмите на панели инструментов вкладки кнопку **Редактирование**. На открывшейся панели **Диапазон сохранения** произведите необходимые изменения и нажмите кнопку **ОК**.
7. Для удаления временного интервала выделите его на панели **Запланировать резервное копирование** и нажмите кнопку **Удаление**. В открывшемся окне подтверждения нажмите **Да**.
8. Нажмите кнопку **Сохранение расписания** для сохранения внесенных в расписание изменений.
9. При необходимости выделите на панели **Расписание** другой день недели и создайте для него временной интервал резервного копирования.
10. Настройте рассылку уведомлений о результатах резервного копирования БД на ПК, ящики электронной почты или телефоны.

### 9.3.3. Настройка сетевой рассылки уведомлений

***Внимание!***

Для работы рассылки на ПК с установленным сервером системы и ПК получателей уведомлений должна быть запущена «*Служба сообщений MS Windows*».

Окно настройки сетевой рассылки уведомлений **Получатели уведомлений** имеет следующий вид:




В рабочей области окна отображается список сетевых имен ПК для отправки уведомлений и условия их отправки.

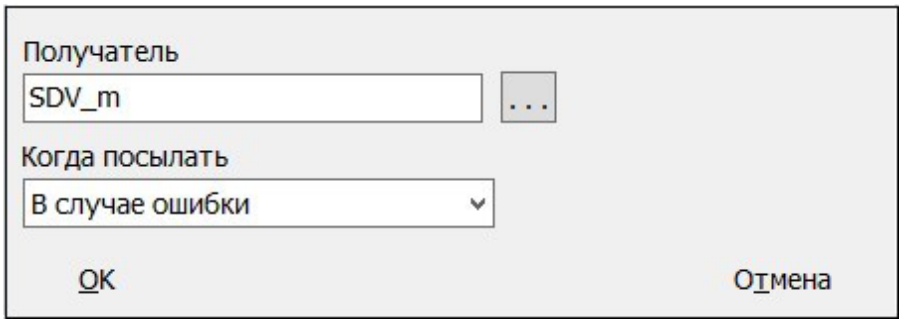
Инструменты панели **Получатели**:

- **Добавить нового получателя** (**Ctrl+N**) – кнопка позволяет добавить имя ПК, на который будут отправляться уведомления.
- **Изменить получателя** (**Ctrl+E**) – кнопка позволяет для выделенного в списке ПК открыть панель ввода и редактирования данных. На панели можно изменить получателя или условие отправки.
- **Удалить получателя** (**Ctrl+D**) – кнопка позволяет удалить выделенный в рабочей области окна ПК из списка получателей уведомлений.
- **Сохранить данные** (**Ctrl+S**) – кнопка позволяет сохранить изменения в списке получателей.

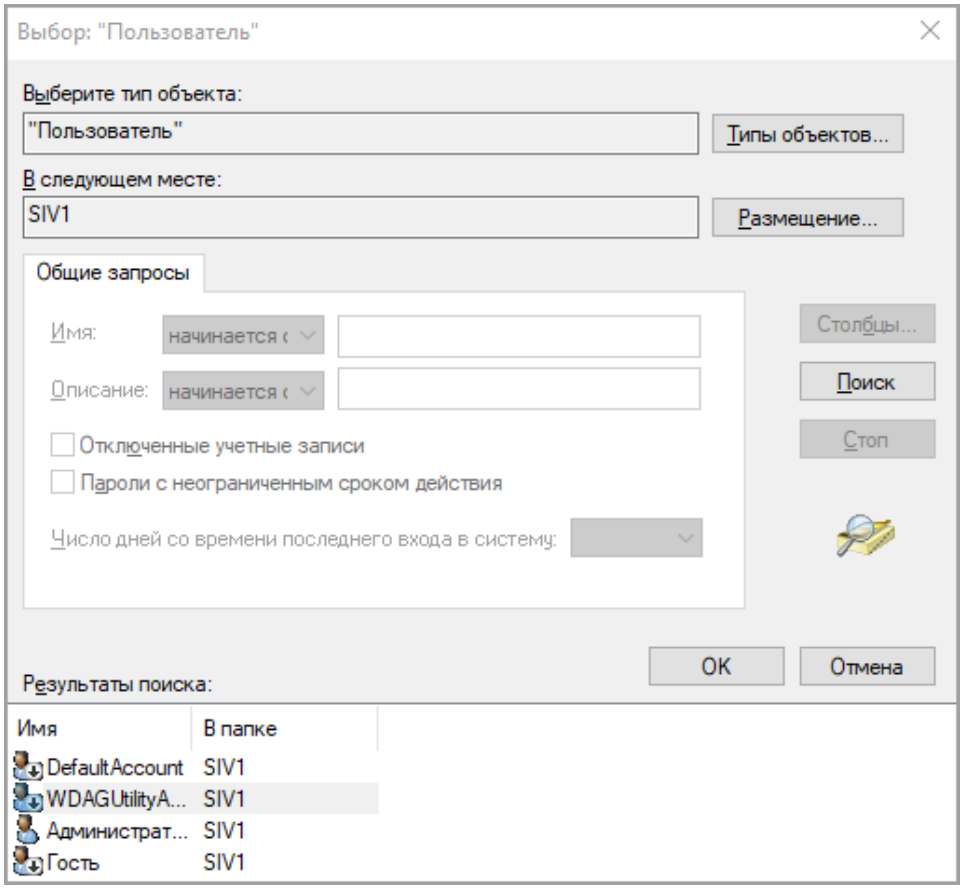
- **Тестирование уведомлений** (**Ctrl+T**) – кнопка позволяет протестировать отправку уведомлений. При нажатии кнопки на выделенный в списке ПК будет отправлено тестовое уведомление.

**Для настройки рассылки уведомлений на ПК:**

1. Нажмите кнопку **Настроить сетевую рассылку уведомлений** на панели инструментов вкладки **Резервное копирование БД**. Откроется окно **Получатели уведомлений**.
2. Для добавления ПК, на который будет отправляться уведомление нажмите кнопку **Добавить нового получателя** на панели инструментов окна. Откроется панель ввода и редактирования данных:



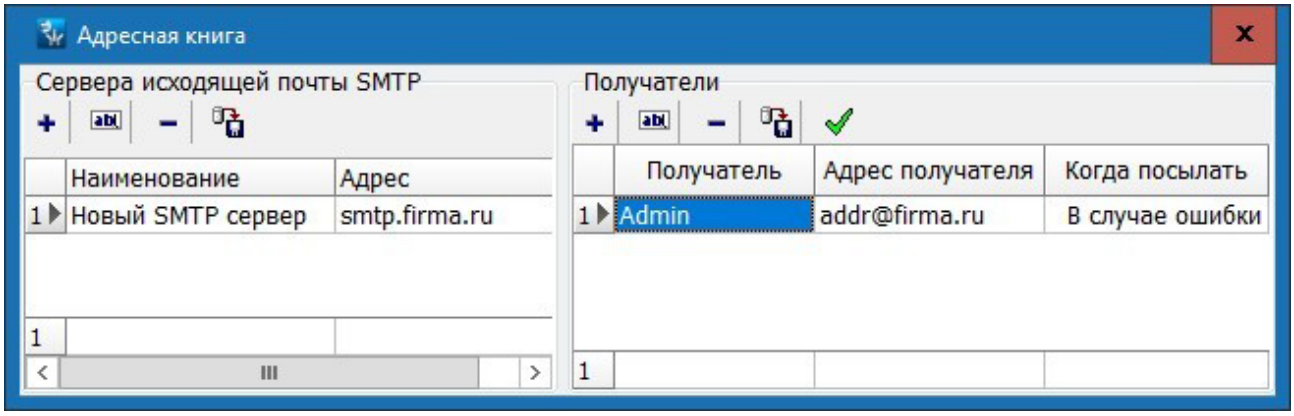

3. С помощью раскрывающегося списка **Когда посылать** укажите условие отправки уведомления.
4. В поле **Получатель** укажите ПК, на который будут отправляться уведомления. Для этого нажмите кнопку ... справа от поля, затем в открывшемся окне нажмите кнопку **Дополнительно**. Откроется новое окно **Выбор: "Пользователь"**:



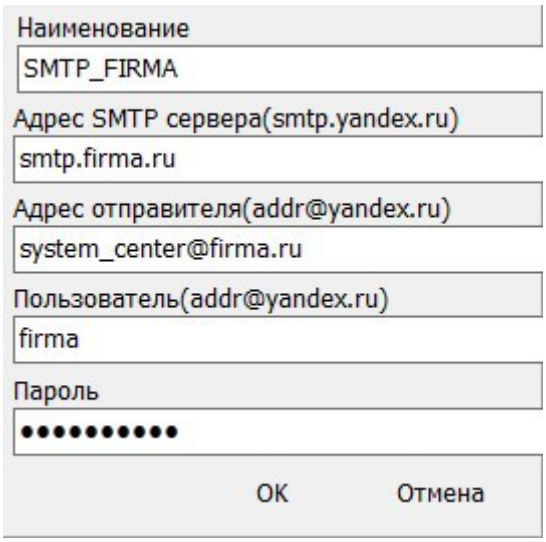
5. Нажмите кнопку **Поиск** – в поле **Результаты поиска** появится список компьютеров. В списке выделите необходимый ПК и нажмите кнопку **ОК**.
6. Нажмите кнопку **ОК** на панели ввода и редактирования данных. Панель будет закрыта. Имя выбранного ПК будет добавлено в список в окне **Получатели уведомлений** с указанием условия отправки уведомлений.
7. Нажмите кнопку **Сохранение данные** для сохранения внесенных в список изменений.
8. Для тестирования службы отправки уведомлений выделите в списке один из ПК и нажмите кнопку **Тестирование уведомлений**. На этот ПК будет отправлено тестовое сообщение *«Тестирование»*.
9. Для закрытия окна **Получатели уведомлений** нажмите кнопку **Закрыть** в строке заголовка окна.

### 9.3.4. Настройка почтовой рассылки уведомлений

Окно настройки почтовой рассылки уведомлений **Адресная книга** имеет следующий вид:




1. Рабочая область панели **Сервера исходящей почты SMTP** содержит список адресов электронной почты отправителей.
2. Инструменты панели **Сервера исходящей почты SMTP**:
   - **Добавить** (**Alt+N**) – кнопка позволяет добавить нового отправителя. При нажатии кнопки откроется панель ввода и редактирования данных:



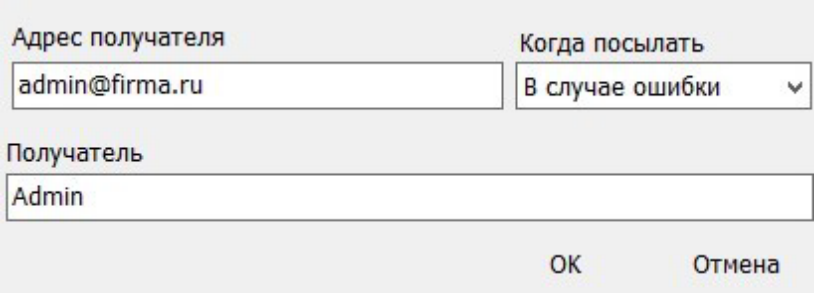
- **Наименование** – название отправителя.
- **Адрес SMTP сервера** – адрес SMTP сервера, используемого отправителем для отправки уведомлений.
- **Адрес отправителя** – адрес электронной почты отправителя, с которого рассылаются уведомления.
- **Пользователь** – имя отправителя, указываемое в уведомлении.
- **Пароль** – пароль доступа к электронной почте отправителя.

- **Изменить** (**Alt**+**E**) – кнопка позволяет изменить запись отправителя, выделенную в рабочей области панели **Сервера исходящей почты SMTP**.
- **Удалить** (**Alt**+**D)** – кнопка позволяет удалить отправителя, выделенного в рабочей области панели **Сервера исходящей почты SMTP**.
- **Сохранить** (**Alt**+**S**) – кнопка позволяет сохранить внесенные изменения.

3. Рабочая область панели **Получатели** содержит список адресов электронной почты, на которые отправляются уведомления о создании резервной копии БД и условия их отправки.

4. Инструменты панели **Получатели**:

- **Добавить** (**Ctrl**+**N)** – кнопка позволяет добавить адрес электронной почты, на который будут отправляться уведомления. При нажатии на кнопку откроется новая панель:




  - **Адрес получателя** – адрес электронной почты, на который отправляются уведомления.
  - **Получатель** – имя получателя в уведомлении.
  - **Когда посылать** – выпадающий список позволяет указать условие отправки уведомлений.

- **Изменить** (**Ctrl**+**E**) – кнопка позволяет для выделенного в рабочей области панели **Получатели** адреса открыть панель ввода и редактирования данных. На панели можно изменить адрес и имя получателя или условие отправки.
- **Удалить** (**Ctrl**+**D**) – кнопка позволяет удалить выделенный в рабочей области панели **Получатели** адрес электронной почты из списка получателей уведомлений.
- **Сохранить** (**Ctrl**+**S**) – кнопка позволяет сохранить внесенные изменения.
- **Проверить отправку почтового сообщения** (**Ctrl**+**T**) – кнопка позволяет протестировать отправку уведомлений. При нажатии кнопки на выделенный в списке адрес будет отправлено тестовое уведомление.

**Для настройки рассылки уведомлений по электронной почте:**

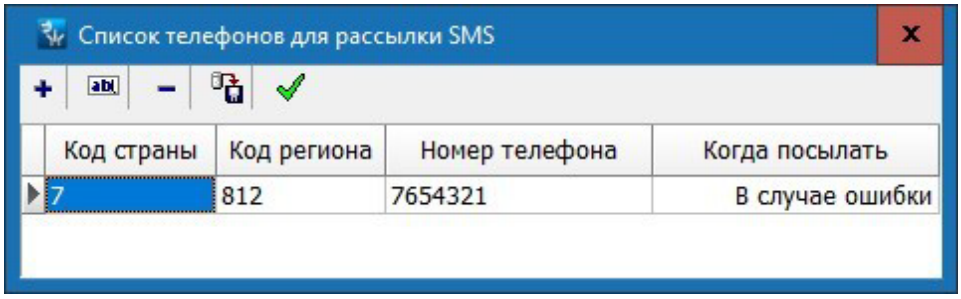
1. Нажмите кнопку **Настроить почтовую рассылку уведомлений** на панели инструментов вкладки Резервное копирование БД. Откроется окно **Адресная книга**.
2. Для отправки сообщений по электронной почте необходимо указать на панели **Сервера исходящей почты SMTP** хотя бы одного отправителя, с электронной почты которого будут отправляться уведомления. Для этого нажмите кнопку **Добавить** в инструментах панели. Откроется панель ввода и редактирования данных.
3. На открывшейся панели укажите адрес электронной почты отправителя и SMTP сервер. Нажмите кнопку **ОК**. Панель будет закрыта, отправитель будет добавлен в список на панели **Сервера исходящей почты SMTP**.
4. Нажмите кнопку **Сохранить** в инструментах панели **Сервера исходящей почты SMTP** для сохранения внесенных изменений.
5. Для добавления адреса электронной почты, на который будут отправляться уведомления при создании БД, нажмите кнопку **Добавить** на панели **Получатели**. Откроется панель ввода и редактирования данных.
6. В открывшейся панели укажите адрес электронный почты, условие отправки и имя получателя. Нажмите кнопку **ОК**. Панель будет закрыта. Получатель будет добавлен в список на панели **Получатели**.
7. Нажмите кнопку **Сохранить** в инструментах панели **Получатели** для сохранения внесенных изменений.
8. Для тестирования отправки уведомлений выделите получателя в списке на панели **Получатели** и нажмите кнопку **Проверить отправку почтового сообщения** в инструментах панели. На адрес получателя будет отправлено тестовое уведомление.
9. Для закрытия окна **Адресная книга** нажмите кнопку **Закрыть** в строке заголовка окна.

### 9.3.5. Настройка SMS-рассылки уведомлений

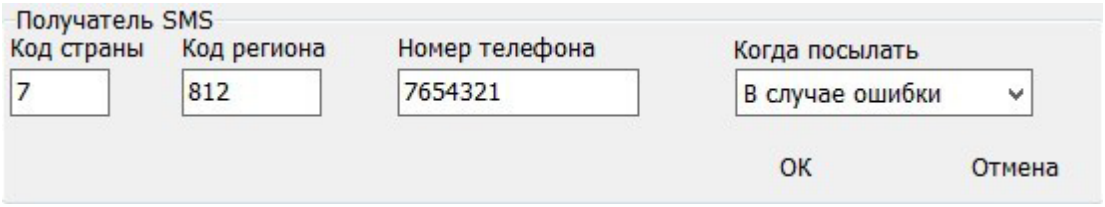
***Внимание!***

Для отправки уведомлений по SMS должна быть настроена рассылка SMS-сообщений на вкладке Настройка рассылки сообщений.

Окно настройки SMS-рассылки уведомлений **Список телефонов для рассылки SMS** имеет следующий вид:



1. В рабочей области окна отображается список номеров телефонов, на которые отсылаются уведомления и условия их отправки.
2. Инструменты окна **Список телефонов для рассылки SMS**:
   - **Добавить** (**Ctrl+N)** – кнопка позволяет добавить номер телефона, на который будут отправляться уведомления:




     – **Код страны**, **Код региона**, **Номер телефона** – поля для ввода телефона получателя.
     – **Когда посылать** – выпадающий список позволяет указать условие отправки уведомлений.
   - **Изменить** (**Ctrl+E**) – кнопка позволяет для выделенного в рабочей области окна открыть панель ввода и редактирования данных. На панели можно изменить номер телефона и условие отправки.
   - **Удалить** (**Ctrl+D)** – кнопка позволяет удалить выделенный в рабочей области окна телефон из списка получателей уведомлений.
   - **Сохранить** (**Ctrl+S**) – кнопка позволяет сохранить внесенные изменения.
   - **Проверить отправку СМС сообщения** (**Ctrl+T**) – кнопка позволяет протестировать отправку уведомлений. При нажатии кнопки на выделенный в списке телефон будет отправлено тестовое уведомление.

**Для создания SMS-рассылки уведомлений:**

1. Нажмите кнопку **Настройка SMS-рассылки** на панели инструментов вкладки Резервное копирование БД. Откроется окно **Список телефонов для рассылки SMS**.
2. Для добавления номера телефона, на который будет осуществляться отправка уведомлений нажмите кнопку **Добавить** на панели инструментов окна. Откроется панель ввода и редактирования данных.
3. На открывшейся панели укажите номер телефона и условие отправки SMS-сообщения. Нажмите кнопку **ОК**. Панель будет закрыта. Телефон будет добавлен в список телефонов в рабочей области окна **Список телефонов для рассылки SMS**.
4. Нажмите кнопку **Сохранить** на панели инструментов окна для сохранения внесенных изменений.
5. Для тестирования отправки SMS-сообщений выделите в списке один из телефонов и нажмите кнопку **Проверить отправку SMS-сообщения** на панели инструментов окна. На этот телефон будет отправлено тестовое уведомление.
6. Для закрытия окна **Список телефонов для рассылки SMS** нажмите кнопку **Закрыть** в строке заголовка окна.

## 9.4. Настройка рассылки сообщений

В системе предусмотрена возможность отправки сообщений сервером системы в следующих случаях:

- При автоматическом создании резервной копии БД. Рассылка настраивается в ***«Центре управления»*** на вкладке **Резервное копирование БД**.
- В ходе выполнения заданий, созданных в разделе ***«Планировщик заданий»***.
- При рассылке сообщений из раздела ***«Сотрудники»***.

Отчет о созданных, отправленных и не отправленных SMS-сообщениях доступен в разделе ***«Отчет по SMS»***.

Для выбора способа отправки SMS-сообщений сервером системы: запустите ***«Центр управления»***, перейдите на вкладку **Настройка рассылки сообщений** и установите переключатель **Выбор способа рассылки** в одно из положений:

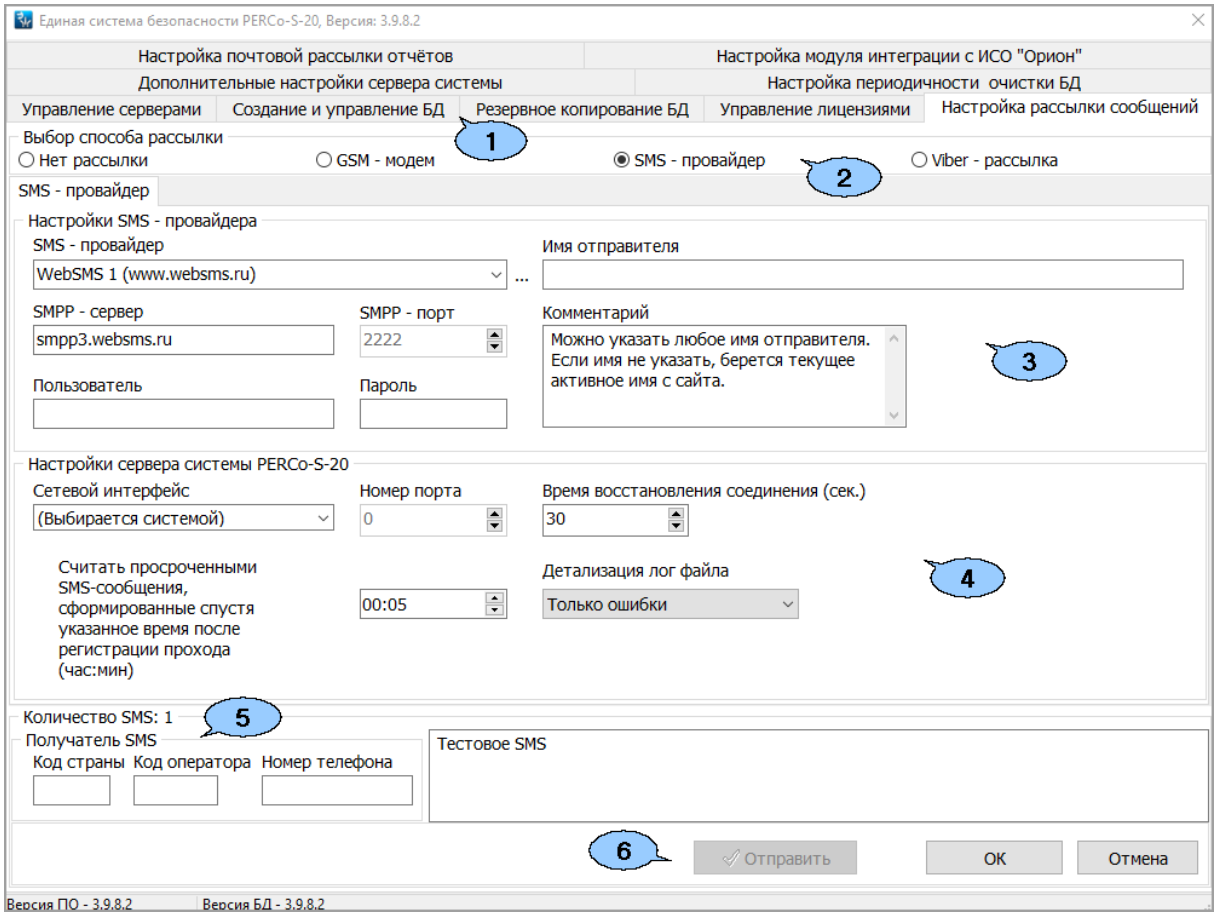
- **Нет рассылки** – рассылка отключена.
- **SMS-провайдер** – рассылка осуществляется SMS-провайдером. Для связи сервера системы с SMS-провайдером требуется наличие постоянного доступа в *Internet*.
- **Viber-рассылка** – рассылка осуществляется с помощью мессенджера *Viber*.

### 9.4.1. Настройка SMS-провайдера

***Примечание:***

Список поддерживаемых системой SMS-провайдеров для отправки SMS-сообщений находится на сайте компании ***PERCo***, по адресу www.perco.ru, в разделе **Главная > Поддержка > ПО**.

Вкладка **Настройка рассылки сообщений** при положении переключателя **Выбор способа рассылки: SMS-провайдер** имеет следующий вид:




1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями**;
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы**;
   - **Настройка периодичности очистки БД**;
   - **Настройка почтовой рассылки отчетов**;
   - **Настройка модуля интеграции с ИСО "Орион"**.
2. Переключатель **Выбор способа рассылки** позволяет выбрать способ отправки SMS-сообщений:
   - **Нет рассылки**;
   - **GSM-модем**;
   - **SMS-провайдер**;
   - **Viber-рассылка**.

3. Панель **Настройки SMS-провайдера** содержит следующие элементы:
   - **SMS-провайдер** – выпадающий список позволяет выбрать одного из поддерживаемых системой SMS-провайдеров.
   -  **Открыть сайт провайдера** – кнопка справа от списка **SMS-провайдер** позволяет перейти на сайт выбранного провайдера.
   - **SMPP-сервер** – заполняется автоматически при выборе провайдера.
   - **SMPP-порт** – заполняется автоматически при выборе провайдера.
   - **Пользователь** – имя учетной записи (логин) зарегистрированное у провайдера.
   - **Пароль** – пароль доступа к учетной записи.
   - **Имя отправителя** – имя отправителя, указанное в сообщении.
   - **Комментарий** – поле с дополнительной информацией о выбранном провайдере. Заполняется автоматически при выборе провайдера.
4. Панель **Настройки сервера системы PERCo-S-20** содержит дополнительные параметры настройки взаимодействия сервера системы с SMS-провайдером:
   - **Сетевой интерфейс** – выпадающий список позволяет выбрать сетевой интерфейс (IP-адрес), через который сервер системы будет осуществляться связь с SMS-провайдером.
   - **Номер порта** – счетчик позволяет указать сетевой порт сервера системы, через который осуществляться связь с SMS-провайдером.
   - **Время восстановления соединения (сек.)** – счетчик позволяет установить минимальный временной интервал между моментом разрыва связи сервера системы с SMS-провайдером и попыткой ее восстановления.
   - **Считать просроченными SMS-сообщения, сформированные спустя указанное время после регистрации прохода (час: мин)** – счетчик позволяет указать максимальный интервал времени между регистрацией события, ведущего к отправке SMS, и отправкой сообщения сервером системы. В случае превышения этого времени SMS-сообщение будет считаться просроченным.
   - **Детализация лог-файла** – выпадающий список позволяет указать, какие сведения о работе сервера системы с SMS-провайдером сохраняются в лог-файл:
     - **Только ошибки**;
     - **Ошибки и предупреждения**;
     - **Служебная информация**;
     - **Трассировка**.
5. **Получатель SMS** – панель содержит поля для ввода номера телефона и тестового SMS-сообщения.
6. Кнопки:
   - **Отправить** – кнопка доступна после завершения настройки SMS-рассылки и предназначена для отправки тестового SMS-сообщения на номер телефона, указанный на панели **Получатель SMS**.
   - **ОК** – предназначена для сохранения внесенных на панели изменений.
   - **Отмена** – предназначена для отмены внесенных на панели изменений.

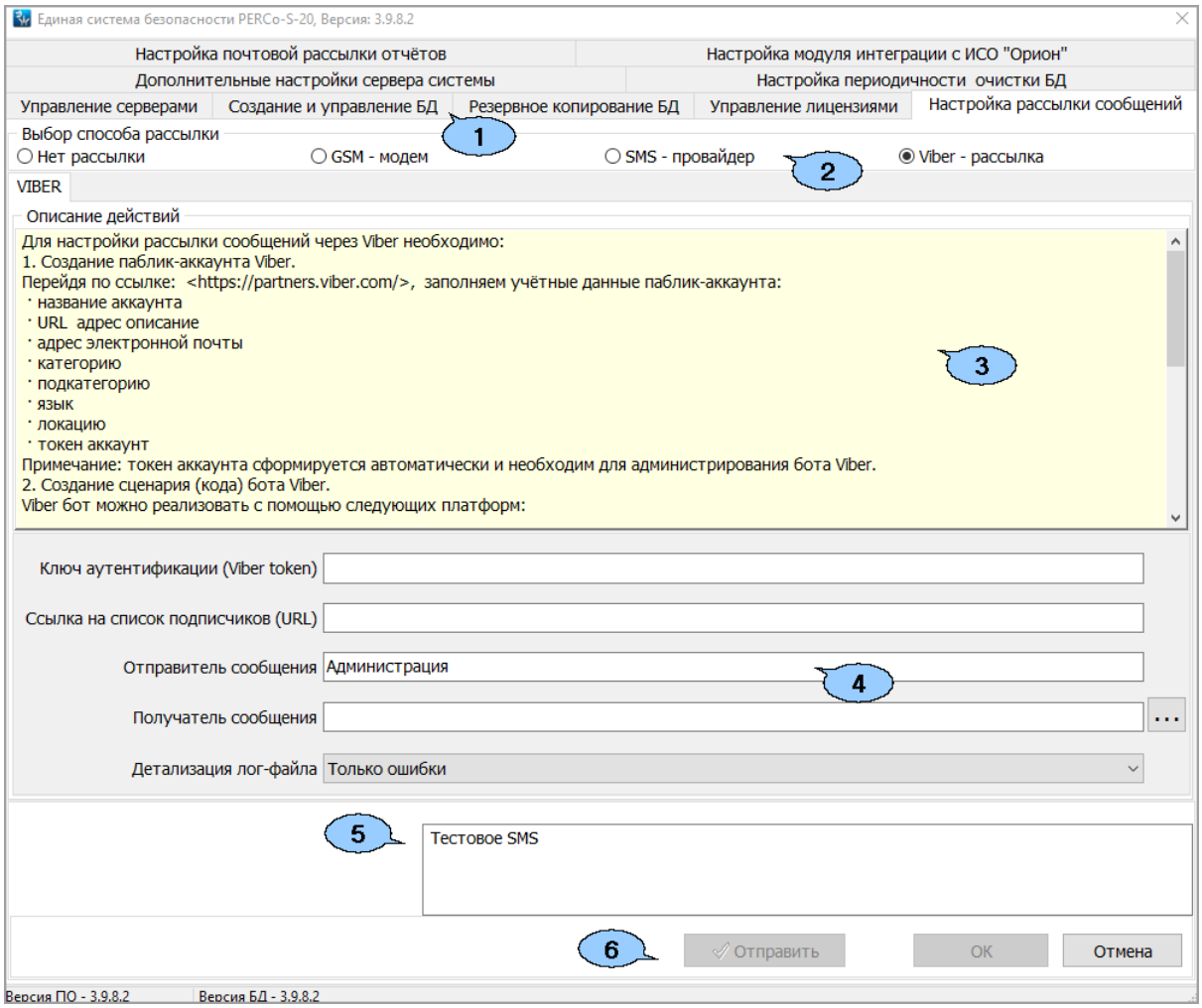
**Порядок настройки рассылки сообщений через SMS-провайдера:**

1. Запустите ***«Центр управления»*** и перейдите на вкладку **Настройка рассылки сообщений**.
2. Установите переключатель **Выбор способа рассылки** в положение **SMS-провайдер**.

3. На панели **Настройки SMS-провайдера** с помощью выпадающего списка **SMS-провайдер** выберите провайдера, услуги которого используются для отправки SMS-сообщений.
4. В полях **Пользователь** и **Пароль** укажите имя и пароль доступа к учетной записи, полученные при регистрации от провайдера. В поле **Имя отправителя** введите имя, которое будет указано в SMS-сообщениях.
5. При необходимости измените дополнительные параметры настройки взаимодействия сервера системы с SMS-провайдером на панели **Настройки сервера системы PERCo-S-20**.
6. Для проверки правильности настроек SMS-рассылки на панели **Получатель SMS** введите номер телефона, на который будет отправлено тестовое SMS-сообщение.
7. Для сохранения внесенных изменений нажмите кнопку **ОК**.
8. Нажмите кнопку **Отправить**. При корректной настройке SMS-рассылки на указанный на панели **Получатель SMS** номер телефона будет доставлено тестовое сообщение.

### 9.4.2. Настройка Viber-рассылки

Вкладка **Настройка рассылки сообщений** при положении переключателя **Viber-рассылка** имеет следующий вид:

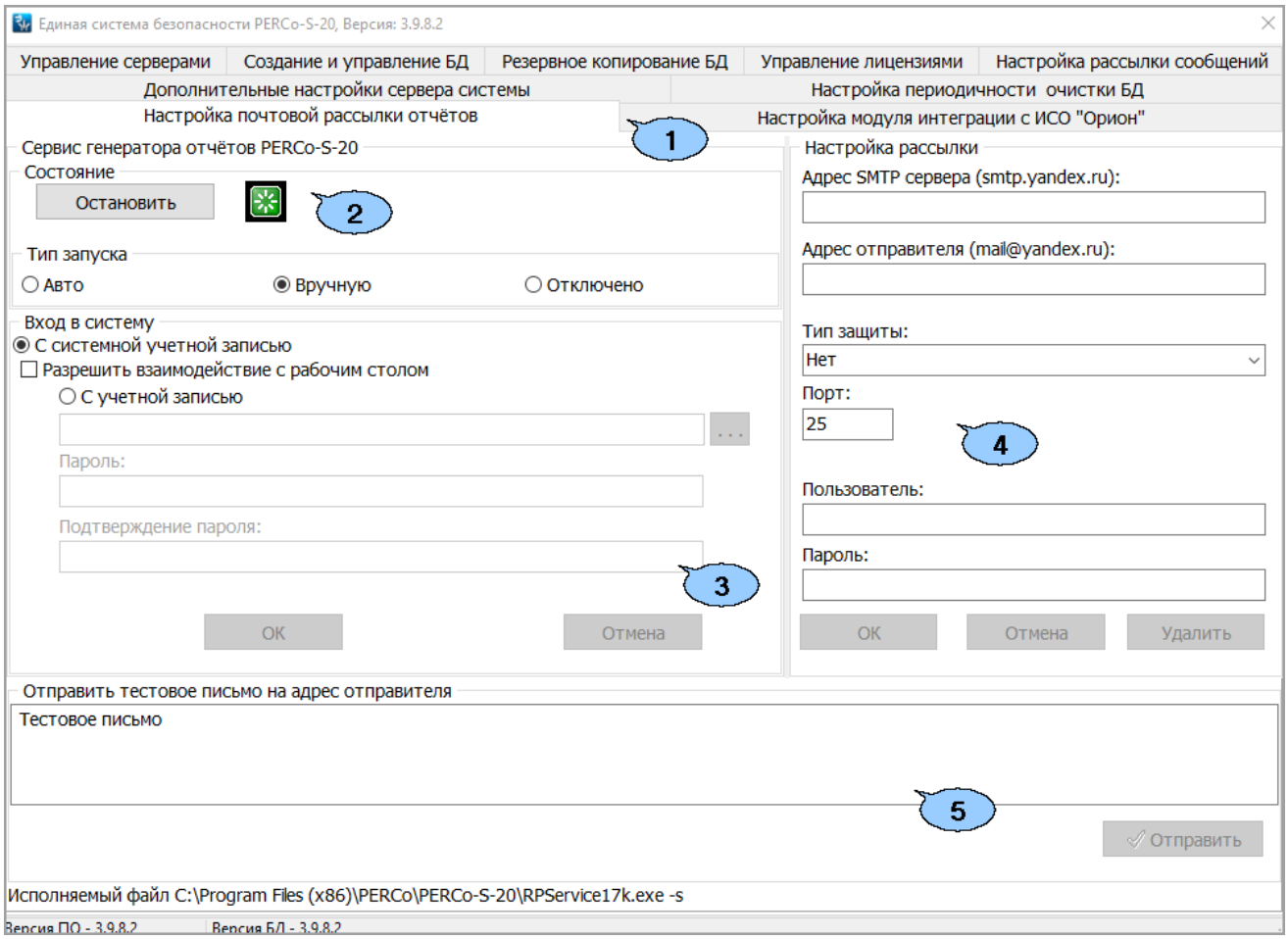


1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями**;
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы**;
   - **Настройка периодичности очистки БД**;
   - **Настройка почтовой рассылки отчетов**;
   - **Настройка модуля интеграции с ИСО "Орион"**.
2. Переключатель **Выбор способа рассылки** позволяет выбрать способ отправки SMS-сообщений:
   - **Нет рассылки**;
   - **GSM-модем**;
   - **SMS-провайдер**;
   - **Viber-рассылка**.
3. **Описание действий** – поле содержит информацию по подробной настройке рассылки сообщений посредством мессенджера Viber.
4. Панель имеет поля для ввода следующих данных:
   - **Ключ аутентификации (Viber token)** – служит для ввода токена, полученного при регистрации паблик аккаунта Viber.
   - **Ссылка на список подписчиков (URL)** – служит для ввода ссылки на базу подписчиков, зарегистрированных в системе.
   - **Отправитель сообщения** – служит для указания отправителя сообщений.
   - **Получатель сообщения** – служит для указания получателя/получателей сообщений. Кнопка **Получить список контактов** позволяет открыть окно со списком контактов, доступных для добавления.
   - **Детализация лог-файла** – выпадающий список позволяет выбрать следующие варианты:
     - Ошибки;
     - Ошибки и предупреждения;
     - Служебная информация;
     - Трассировка.
5. Поле служит для ввода тестового сообщения.
6. На панели расположены кнопки:
   - **Отправить** – кнопка доступна после завершения настройки Viber-рассылки и предназначена для отправки тестового сообщения получателю, указанному в поле **Получатель сообщения**.
   - **ОК** – предназначена для сохранения внесенных на панели изменений.
   - **Отмена** – предназначена для отмены внесенных на панели изменений.

## 9.5. Настройка почтовой рассылки отчетов

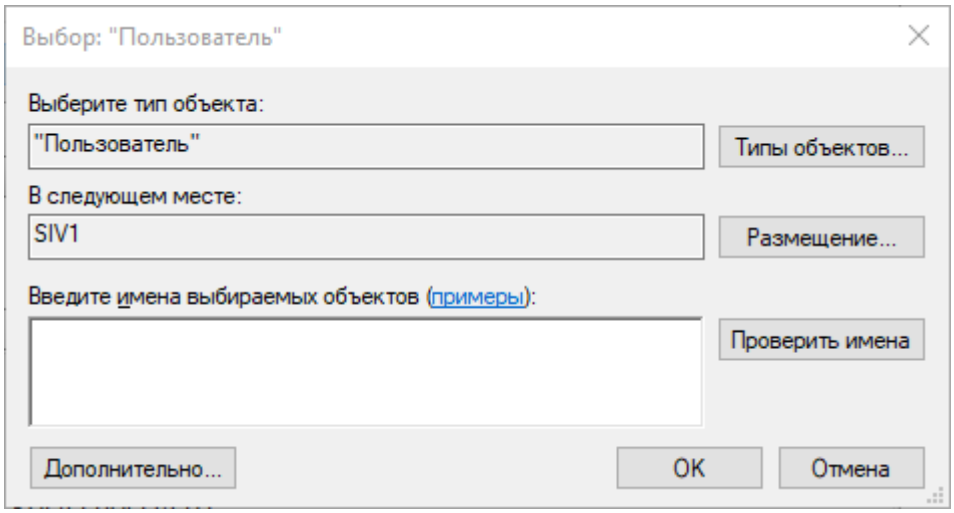
В системе предусмотрена возможность автоматической отправки отчетов по электронной почте в ходе выполнения заданий раздела ***«Планировщик заданий»***.

Вкладка имеет следующий вид:




1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями**;
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы**;
   - **Настройка периодичности очистки БД**;
   - **Настройка почтовой рассылки отчетов**;
   - **Настройка модуля интеграции с ИСО "Орион"**.
2. Панель **Сервис генератора отчетов PERCo-S-20** содержит:
   - Кнопку **Остановить / Запустить**, которая позволяет управлять работой сервиса генератора отчетов **PERCo-S-20.**
   - Индикатор состояния сервиса генератора отчетов **PERCo-S-20**:
      – сервис запущена / остановлена.
   - Переключатели **Тип запуска** позволяют установить способ запуска сервиса генератора отчетов **PERCo-S-20**:
     - **Авто** – сервис запускается автоматически при запуске ОС.
     - **Вручную** – сервис запускается вручную.
     - **Отключено** – сервис отключен.

3. **Вход в систему** переключатель позволяет выбрать учетную запись пользователя ОС, от имени которого будут запускаться серверы. Для корректной работы серверов (создания почтовой и SMS рассылок) необходимо, чтобы пользователю были выданы полные права администратора ПК.
   - **С системной учетной записью** – запуск серверов осуществляется от имени встроенной учетной записи администратора ПК.
   - **С учетной записью** – запуск серверов осуществляется от имени указанной учетной записи. Для выбора учетной записи нажмите кнопку . Откроется окно **Выбор: "Пользователь"**:




4. Панель **Настройка рассылки** содержит параметры настройки SMTP-сервера, используемого для отправки почты. Параметры настраиваются согласно рекомендациям провайдера, предоставляющего услуги SMTP-сервера исходящей почты. Доступны следующие параметры:
   - **Адрес SMTP сервера** – электронный адрес исходящей почты используемого почтового сервера.
   - **Адрес отправителя** – электронный адрес, с которого производится рассылка отчетов.
   - **Тип защиты** (**Нет / SSL / TSL**) – раскрывающийся список позволяет выбрать один из криптографических протоколов шифрования сообщений.
   - **Порт** – используемый порт.
   - **Пользователь** – учетная запись (login).
   - **Пароль** – пароль учетной записи.
5. **Отправить тестовое письмо** – поле для ввода текста.
   - **Отправить** – кнопка для отправки тестового письма.

## 9.6. Интеграция с ИСО «Орион»

В системе предусмотрена возможность интеграции с оборудованием ИСО (интегрированной системы охраны) «Орион» производства ЗАО НВП «Болид». После проведения интеграции в системе появляется возможность отслеживать состояния подключенных устройств ИСО «Орион», получать регистрируемые ими события и подавать команды управления.

Интеграция системы с оборудованием ИСО «Орион» возможно только при подключении оборудования к ПК через пульты управления **С 2000** или **С 2000-М** производства ЗАО НВП «Болид».

**Поддерживаемые приборы ИСО «Орион»**

| Категория прибора | Прибор |
|---|---|
| Пульты управления | ***С2000***<br>***С2000-М*** |
| Блоки индикации и управления клавиатуры | ***С2000-К***<br>***С2000-КС***<br>***С2000-БКИ***<br>***С2000-БКИ (вер. 2.20)***<br>***С2000-БИ***<br>***С2000-БИ (вер. 2.23)***<br>***С2000-БИ исп. 01*** |
| ППКОП с радиальными ШС | ***С2000-4***<br>***С2000-4 (вер. 3.00)***<br>***Сигнал-20***<br>***Сигнал-20П***<br>***Сигнал-20П (вер. 2.04)***<br>***Сигнал-20 сер. 02***<br>***Сигнал-20М*** |
| Контроллеры доступа | ***С2000-2*** |
| Адресно-аналоговые подсистемы (КДЛ) | ***С2000-КДЛ***<br>***С2000-КДЛ-2И***<br>***С2000-КДЛС*** |
| Адресно-пороговые подсистемы | ***Сигнал-10*** |
| Адресно-канальные подсистемы | ***С2000-Adem*** |
| Приборы речевого оповещения | ***Рупор***<br>***Рупор (вер. 2.00)***<br>***Рупор-200***<br>***Рупор исп. 01*** |
| Приборы управления пожаротушением | ***С2000-АСПТ***<br>***С2000-АСПТ (вер. 2.00)***<br>***С2000-АСПТ (вер. 3.00)***<br>***С2000-ПТ***<br>***Поток-3Н***<br>***Поток-3Н (вер. 1.03)***<br>***Поток-БКИ*** |
| Релейные блоки | ***С2000-КПБ***<br>***С2000-КПБ (вер. 2.01)***<br>***С2000-СП1*** |
| Приборы передачи извещений | ***С2000-ИТ***<br>***С2000-PGE***<br>***УО-4С*** |
| Резервированные источники питания | ***РИП-12 RS***<br>***РИП-12-2А RS***<br>***РИП-24-2А RS*** |
| Преобразователи протоколов | ***С2000-ПП*** |

Для интеграции необходимы следующие программные средства:

- ***«Модуль управления ИСО Орион»***, разработанный ЗАО НВП «Болид». Для использования модуля необходимо приобрести электронный ключ защиты. В состав модуля входит XML-RPC-сервер, обеспечивающий обмен данными между системой и оборудования ИСО «Орион».
- ПО ***PPROG*** и ***UPROG*** разработанные ЗАО НВП «Болид» для конфигурации приборов ИСО «Орион».

***Примечание:***

Дополнительная информация о продуктах ЗАО НВП «Болид» доступна на сайте: www.bolid.ru.

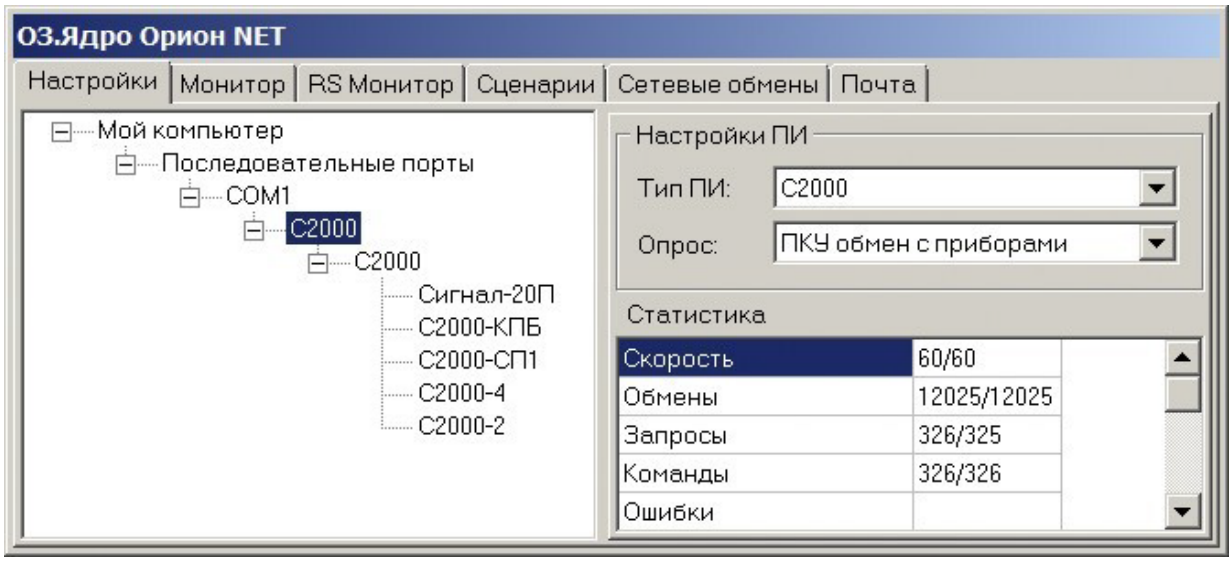
### 9.6.1. Порядок интеграции с ИСО «Орион»

***Внимание!***

Интеграция системы с оборудования ИСО «Орион» производится с помощью компонента ***PERCo-SM18 «Модуль интеграции с ИСО "Орион"»***. Модуль не требует установки и может использоваться в течение ознакомительного периода. В течение этого времени на модуль необходимо приобрести лицензию и ввести ключ активации. В противном случае возможность работы системы с оборудования ИСО «Орион» блокируется.

Для проведения интеграции:

1. Произведите монтаж и настройку оборудования ИСО «Орион» согласно эксплуатационной документации на устройства.
2. Произведите конфигурирование устройств ИСО «Орион». Конфигурирование производится от ПК с использованием ПО ***PPROG*** и ***UPROG*** согласно эксплуатационной документации на ПО.
3. Установите ПО ***«Модуль управления ИСО Орион»*** на ПК, к которому подключено оборудования ИСО «Орион».
4. Запустить ***«Модуль управления ИСО Орион»*** при этом на ПК автоматически будет запущен XML-RPC-сервер. В области уведомлений (рядом с часами) появится значок **RS Ядро Орион Про**  .
5. Дважды нажмите на значок **RS Ядро Орион Про**  . Откроется окно **ОЗ.Ядро Орион NET**. При корректной настройке оборудования на вкладке **Настройки** будет отображена созданная конфигурация подключенного оборудования ИСО «Орион»:

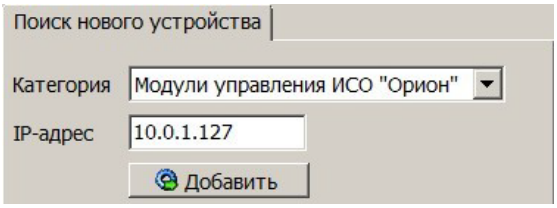


6. Запустите модуль ***«Центр управления PERCo-S-20»*** и перейдите на вкладку **Настройка модуля интеграции с ИСО "Орион"**. С помощью выпадающего списка **Сетевой интерфейс** укажите сетевой интерфейс, с которого сервер системы будет осуществлять подключение к XML-RPC-серверу. При необходимости произведите настройку других параметров.
7. Запустите ***«Консоль управления»*** и перейдите в раздел ***«Конфигуратор»***. Добавьте в конфигурацию системы конфигурацию оборудование ИСО «Орион». Конфигурация приборов и их ресурсов должна повторять конфигурацию, созданную с использованием ПО ***PPROG*** или ***UPROG***.

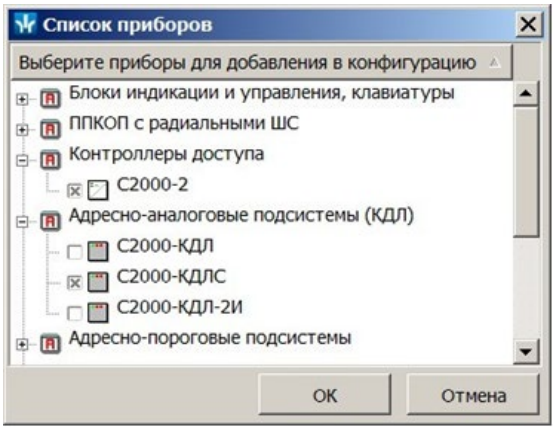
***Внимание!***

Обратите внимание, что конфигурация приборов ИСО «Орион», созданная в раздел ***«Конфигуратор»***, не синхронизируется с конфигурацией, заданной в программах ***UPROG*** и ***PPROG***. Поэтому при изменении конфигурацию системы ИСО «Орион» (добавлении или удалении приборов, изменении настроек ресурсов) эти изменения требуется вручную внести и в разделе ***«Конфигуратор»***.

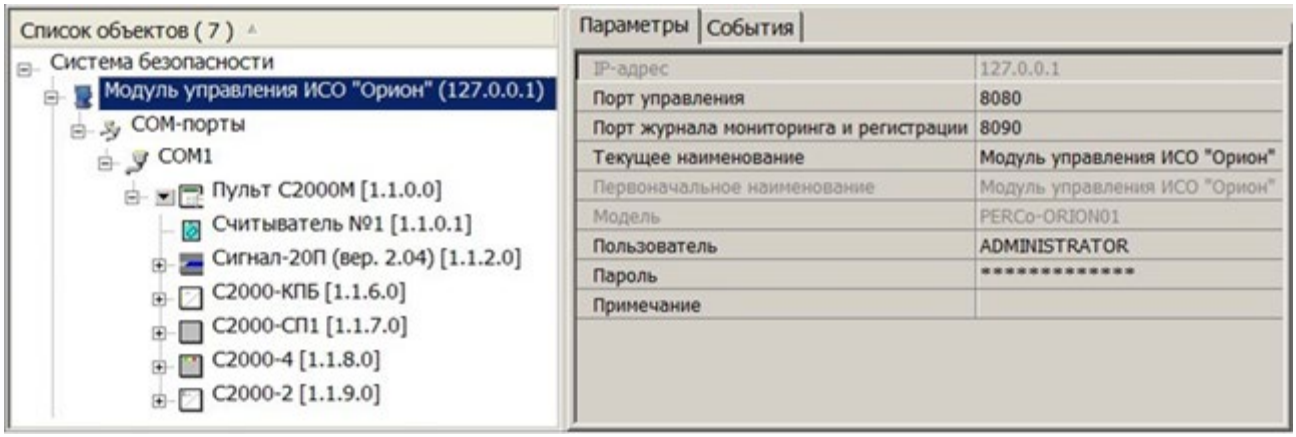
- Для создания конфигурации нажмите на панели инструментов раздела кнопку **Добавить новое устройство**. На открывшейся панели **Поиск нового устройства** с помощью выпадающего списка **Категория** выберите **Модули управления ИСО Орион**. В поле **IP-адрес** укажите IP-адрес ПК, на котором установлен ***«Модуль управления ИСО Орион»:***




- Нажмите кнопку **Добавить**. Панель **Поиск нового устройства** будет закрыта. В рабочей области раздела будет добавлено устройство *«Модуль управления ИСО "Орион"»*.
- Выделите группу ресурсов добавленного устройства *«COM-порты»* и нажмите на панели инструментов раздела кнопку **Добавить COM-порты**. В рабочей области раздела будет добавлена группа ресурсов *«COM1»*. При необходимости тем же образом добавьте группу ресурсов *«COM2»*, *«COM3»* и т.д. Количество аппаратно поддерживаемых COM-портов определяется вариантом исполнения ПО ***«Модуль управления ИСО Орион»***.
- Выделите группу ресурсов *«COM1»* и на панели **Параметры** укажите номер COM-порта ПК, к которому физически подключено оборудование ИСО «Орион».
- Для группы ресурсов *«COM1»* доступны ресурсы *«Пульт»* и *«Считыватель №1»*. Нажмите в стрелку слева от группы ресурсов *«Пульт»*. Откроется окно **Список приборов**, содержащее перечень поддерживаемых приборов ИСО «Орион», сгруппированных по категориям:




- В открывшемся окне поставьте отметки у приборов, которые необходимо добавить в конфигурацию системы и нажмите кнопку **ОК**. Окно будет закрыто. Указанные приборы будут добавлены в рабочее окно раздела, отмеченные значками .
- Произведите настройку параметров приборов ИСО «Орион» и их ресурсов (шлейфов, реле). Параметры будут доступны на вкладке **Параметры** при выделении устройства или его ресурса в рабочей области раздела:




***Примечание:***

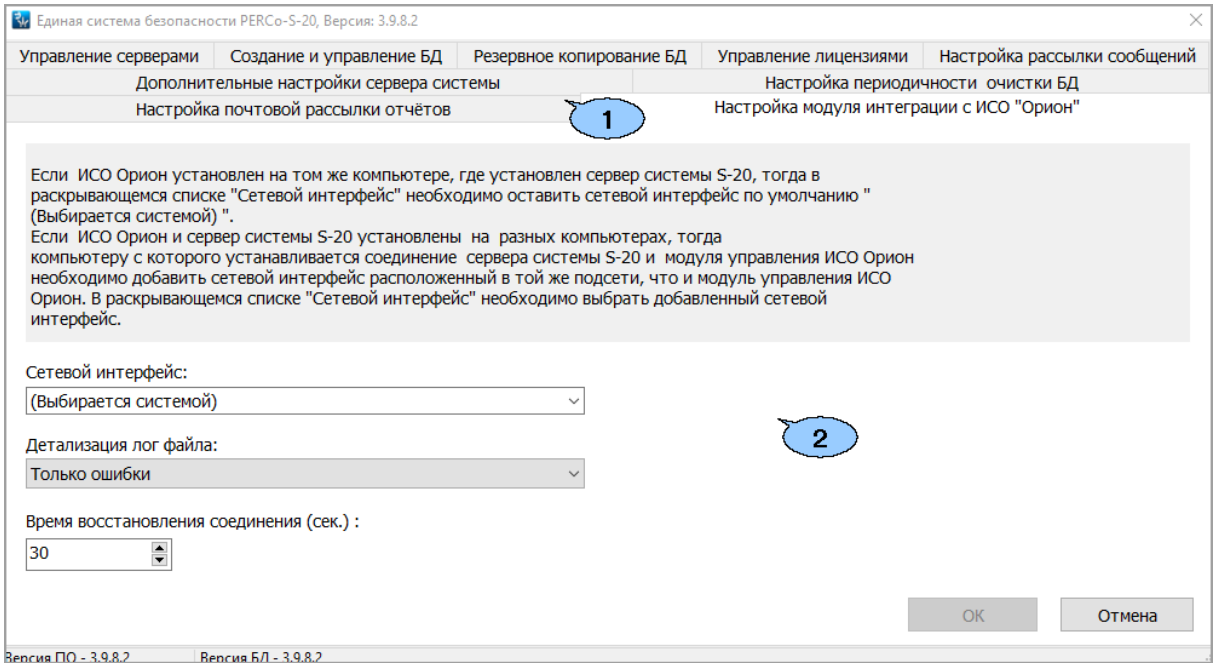
Значок в рабочей области раздела ***«Конфигуратор»*** слева от компонентов интеграции оборудования ИСО «Орион» указывает на то, что возможность работы с этим оборудованием заблокирована. Это возможно после окончания ознакомительного периода использования компонента ***SM18 «Модуль интеграции с ИСО "Орион"»*** в следующих случаях:

- За этот период не была приобретена лицензия и не введен ключ активации для компонента ***SM18 «Модуль интеграции с ИСО "Орион"»***
- Ключ активации введен, но нарушена связь с контроллером, выбранным в качестве электронного ключа защиты ПО.

8. Установите связь с приборами, добавленными в конфигурацию. Для этого нажмите кнопку **Передать параметры** на панели инструментов раздела.
9. При необходимости на вкладке **События** произведите настройку реакции системы на события мониторинга, регистрируемые приборами ИСО «Орион».

### 9.6.2. Вкладка «Настройка модуля интеграции с ИСО Орион»

Вкладка предназначена для настройки интеграции системы с оборудованием ИСО «Орион» производства ЗАО НВП «Болид». Вкладка имеет следующий вид:




1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями**;
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы**;
   - **Настройка периодичности очистки БД**;
   - **Настройка почтовой рассылки отчетов**;
   - **Настройка модуля интеграции с ИСО «Орион»**.
2. Рабочая область вкладки содержит следующие элементы:
   - **Сетевой интерфейс** – раскрывающийся список позволяет выбрать сетевой интерфейс, через который сервер системы будет осуществлять связь к ПК с установленным модулем ***«Модуль управления ИСО Орион»***.
   - **(Выбирается системой)** – вариант установлен по умолчанию и используется в случае, если ***«Модуль управления ИСО Орион»*** установлен на том же ПК, что и сервер системы.

     Если ***«Модуль управления ИСО Орион»*** и сервер системы установлены на разных ПК, то необходимо указать сетевой интерфейс сервера системы, с которого осуществляется подключение.

***Внимание!***

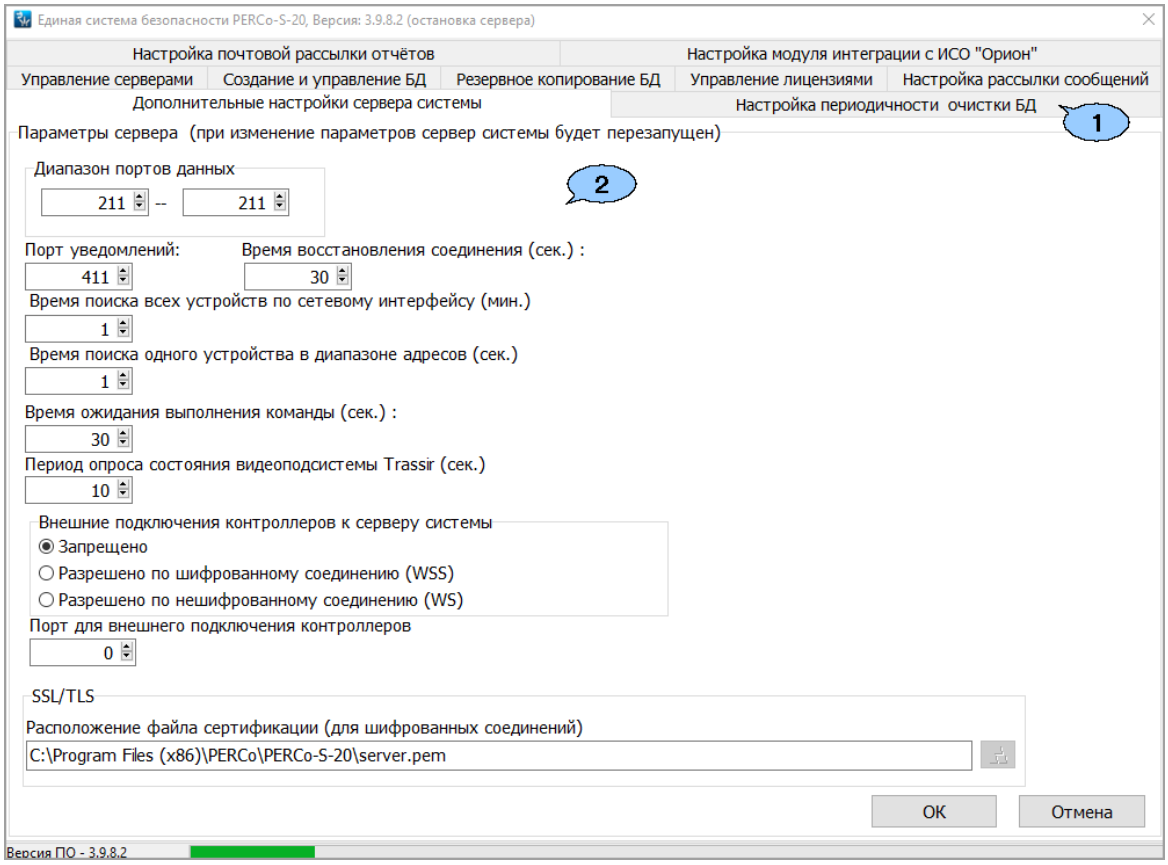
ПК, на котором установлен сервер системы, и ПК, на котором установлен ***«Модуль управления ИСО Орион»,*** должны находиться в одной подсети. Для этого одному из ПК может быть добавлен дополнительный сетевой интерфейс.

   - **Детализация лог файла** – раскрывающийся список позволяет выбрать степень детализации лог-файла.
     - **Только ошибки;**

  - **Ошибки и предупреждения;**
  - **Служебная информация;**
  - **Трассировка.**
- **Время восстановления соединения (сек.)** – счетчик позволяет установить минимальный временной интервал между моментом разрыва связи сервера системы с ПК, на котором установлен ***«Модуль управления ИСО Орион»,*** и попыткой ее восстановления.
- Кнопки:
  - **ОК** – предназначена для сохранения внесенных на панели изменений.
  - **Отмена** – предназначена для отмены внесенных на панели изменений.

## 9.7. Дополнительные настройки сервера системы

Вкладка предназначена для управления дополнительными настройками сервера системы и имеет следующий вид:




1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями**;
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы**;
   - **Настройка периодичности очистки БД**;
   - **Настройка почтовой рассылки отчетов**;
   - **Настройка модуля интеграции с ИСО "Орион"**.
2. Параметры сервера:
   - **Диапазон портов данных** – счетчик позволяет при необходимости изменить сетевой порт обмена данными между запущенной на АРМ

- ***«Консолью управления»*** и сервером системы (СУБД) **FireBird**. По умолчанию задано значение `211`.
- **Порт уведомлений** – счетчик позволяет при необходимости изменить сетевой порт обмена уведомлениями между запущенной на АРМ ***«Консолью управления»*** и сервером системы (СУБД) **FireBird**. По умолчанию задано значение `411`.
- **Время восстановления соединения (сек.)** – счетчик позволяет изменить время, через которое сервер системы попытается восстановить связь с контроллером системы в случае ее неожиданной потери. Заданное по умолчанию время – 30 сек.
- **Время поиска всех устройств по сетевому интерфейсу (мин.)** – счетчик позволяет при необходимости увеличить максимальное время, отведенное серверу системы на поиск всех устройств по сетевому интерфейсу. Заданное по умолчанию время – 1 мин.
- **Время поиска одного устройства в диапазоне адресов (сек.)** – счетчик позволяет при необходимости увеличить максимальное время, отведенное серверу системы на поиск одного устройства в диапазоне адресов. Заданное по умолчанию время – 1 сек.
- **Время ожидания выполнения команды (сек.)** – счетчик позволяет задать время ожидания выполнения команды. Заданное по умолчанию время – 30 секунд.
- **Период опроса состояния видеоподсистемы Trassir (сек.)** – счетчик позволяет задать период опроса для видеоподсистемы. Заданное по умолчанию значение – 10 секунд.
- **Внешние подключения контроллеров к серверу системы** – параметр определяет, может ли сам контроллер выступать инициатором подключения к серверу системы.

***Примечание:***

В случае, когда сервер системы и контроллеры находятся в пределах одной сети, система по команде осуществляет поиск контроллеров внутри сети, установка параметра не требуется.

В случае, когда контроллер находится за пределами сети сервера системы, а также когда необходимо подключить контроллер, находящийся, например, за преобразователем сетевых адресов *NAT* (от англ. *Network Address Translation*), необходимо разрешить реверсные подключения контроллеров к серверу системы. В таком случае контроллер сможет самостоятельно инициализировать подключение, что упрощает его подключение к системе.

  - **Запрещено;**
  - **Разрешено по шифрованному соединению (WSS);**
  - **Разрешено по нешифрованному соединению (WS).**
- **Порт для внешнего подключения контроллеров** – счетчик позволяет при необходимости указать сетевой порт подключения контроллеров по протоколу **Websocket** (протокол предназначен для обмена сообщениями между браузером и веб-сервером в режиме реального времени поверх TCP-соединения).
- **SSL/TLS** (настройки доступны, если для параметра **Внешние подключения контроллеров к серверу системы** определено значение **Разрешено по шифрованному соединению (WSS)**)**:**
  - **Расположение файла сертификации (для шифрованных соединений)** – указывает на расположение файла сертификации. Для выбора нового расположения нажмите кнопку  **Выбрать файл сертификации**.

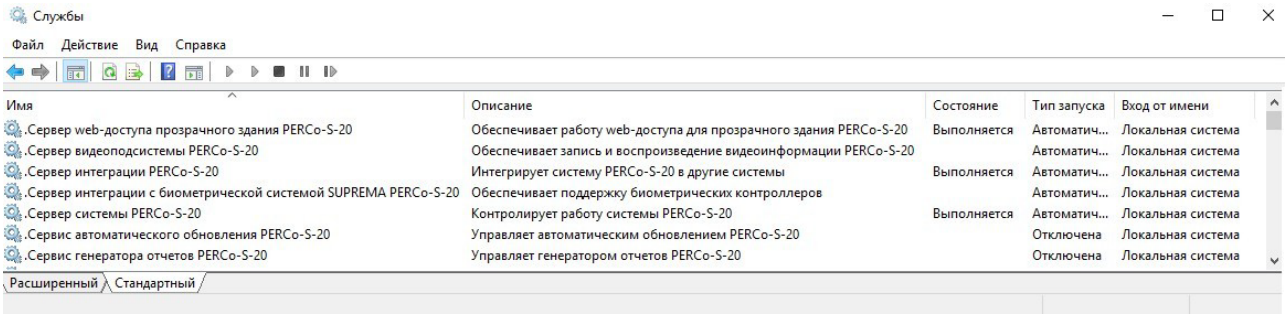
# 10. Службы системы

После установки на ПК модулей системы для обеспечения их работы, при загрузке ОС должны автоматически запускаться соответствующие службы.

***Внимание!***

Запуск, остановка и настройка автоматического запуска служб возможна только при наличии прав администратора ПК.

Для просмотра запущенных служб нажмите последовательно: **Пуск > Настройка > > Панель управления**, затем **Администрирование > Службы**. Откроется окно **Службы**:




С модулями системы устанавливаются следующие службы:

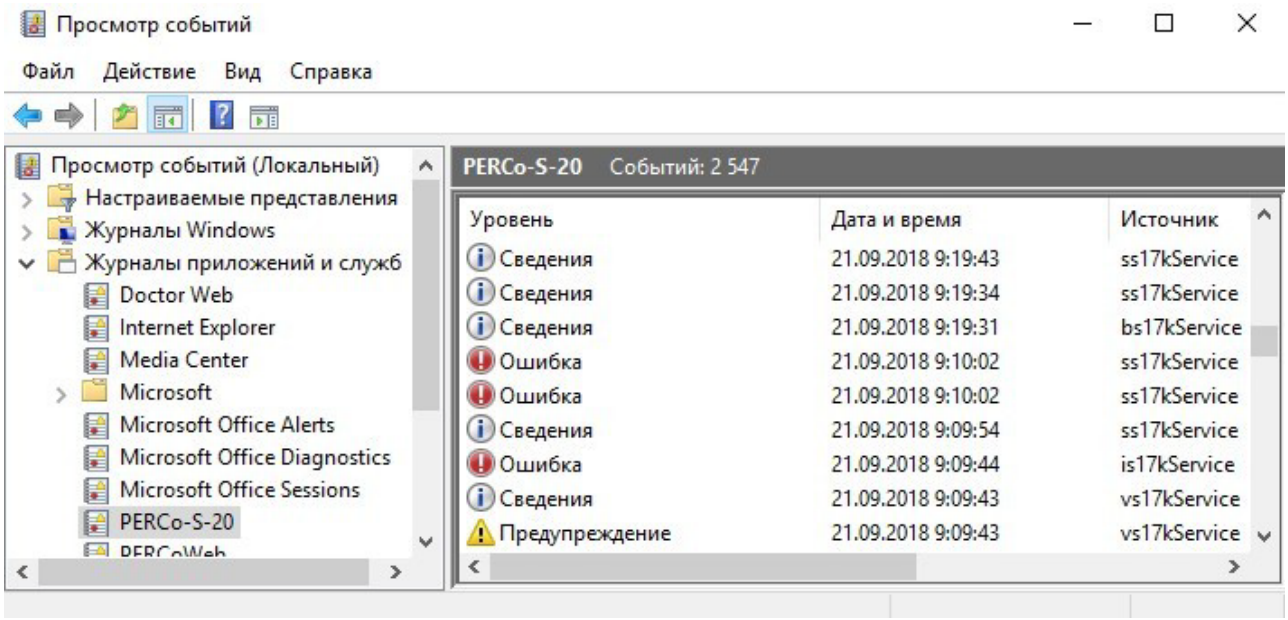
- *«Сервер системы PERCo-S-20»* – служба обеспечивает работу сервера системы. Устанавливается с модулем **Сервер системы**.
- *«Сервис автоматического обновления PERCo-S-20»* – служба обеспечивает возможность автоматического обновления консоли управления и сервера видеоподсистемы. Устанавливается с модулем **Консоль управления**. Для работы службы необходим стандартный компонент *MS Windows «Службы терминалов»*.
- *«Сервер видеоподсистемы PERCo-S-20»* – служба обеспечивает работу сервера видеоподсистемы. Устанавливается с модулем **Сервер видеоподсистемы**.
- *«Сервер Web-доступа прозрачного здания PERCo-S-20»* – служба обеспечивает работу Web-сервер необходимого для доступа к Web-интерфейсу модуля ***«Прозрачное здание»***. Устанавливается с модулем **Web-доступ прозрачного здания**.
- *«Сервер генератора отчетов PERCo-S-20»* – служба обеспечивает возможность выполнения заданий раздела ***«Планировщик заданий»***, связанных с отправкой отчетов по электронной почте. Управление запуском службы осуществляется на вкладке **Настройка почтовой рассылки отчетов** раздела ***«Центр управления».***
- *«Сервер интеграции PERCo-S-20»* – служба интегрирует систему ***PERCo-S-20*** в другие системы.
- *«Сервер интеграции с биометрической системой SUPREMA PERCo-S-20»* – служба обеспечивает поддержку биометрических контроллеров.

Кроме этого, на ПК с установленным сервером системы для обеспечения работы с БД должны быть запущены службы СУБД на базе SQL сервера *Firebird*. Службы доступны после установки модуля **Сервер БД**:

- *«Firebird Server - DefaultInstance»* – служба SQL сервера *Firebird*.
- *«Firebird Guardian - DefaultInstance»* – служба поддержки SQL сервера *Firebird*.

# 11. Журнал событий Windows

Информация о работе служб системы доступна в журнале событий Windows. Для просмотра событий необходимо открыть панель управления *Windows* **Пуск > Настройка > Панель управления**, затем **Администрирование > Просмотр событий**. Откроется окно **Просмотр событий**:




Для просмотра событий служб системы выберите в левой части окна журнал **PERCo-S-20**. В рабочей области окна будет доступен список сообщений соответствующей службы. В столбце **Источник** указано наименование службы:

- `ss7kService` – *«Сервер системы PERCo-S-20».*
- `au17kService` – *«Сервис автоматического обновления PERCo-S-20».*
- `vs17kService` – *«Сервер видеоподсистемы PERCo-S-20».*
- `ws17kService` – *«Сервер web-доступа прозрачного здания PERCo-S-20».*
- `rp17kService` – *«Сервер генератора отчетов PERCo-S-20».*

События служб сервера *Firebird* доступны в журнале **Приложение**.

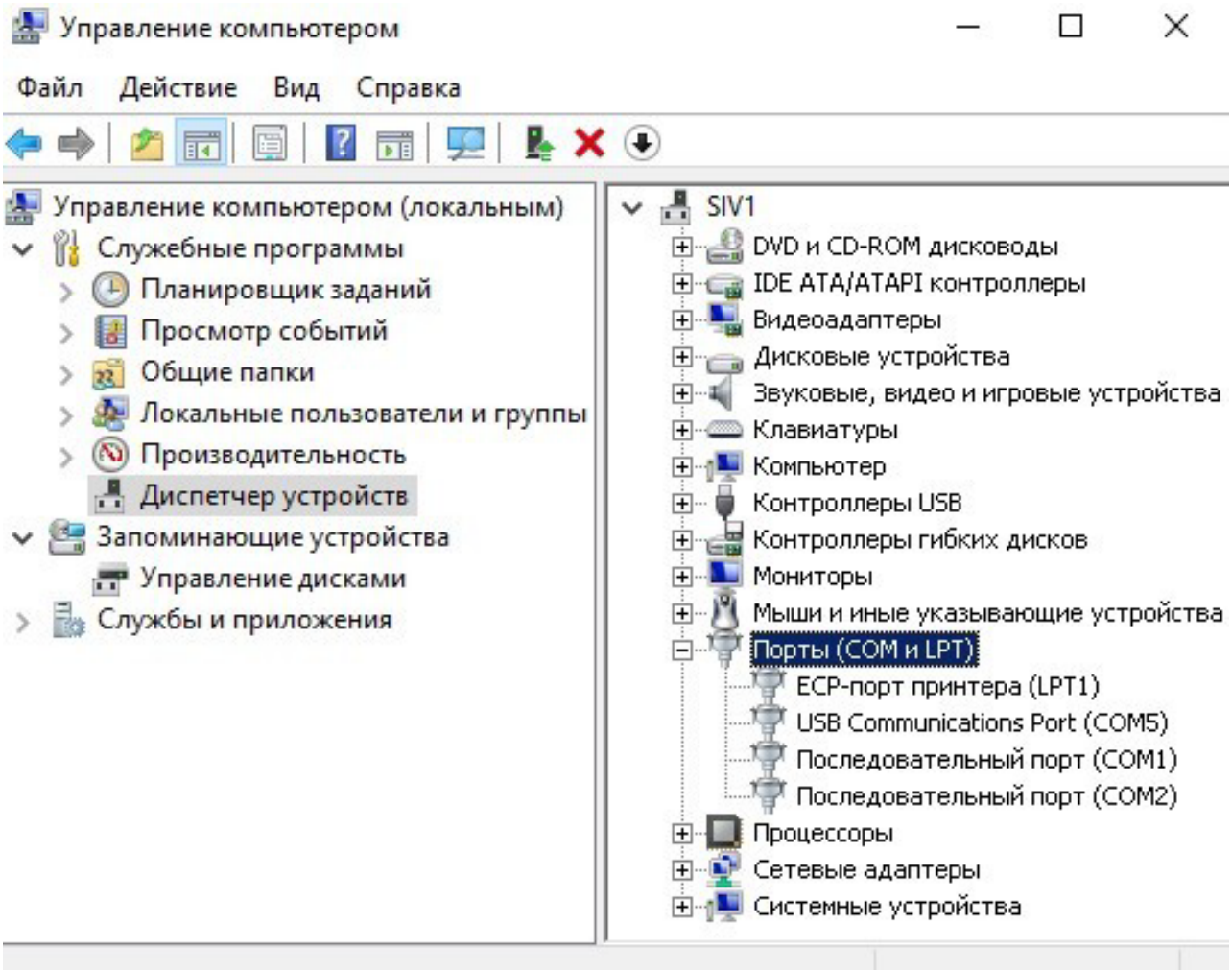
# 12. Установка драйвера контрольного считывателя

***Примечание:***

При подключении контрольных считывателей карт доступа серий ***PERCo-IR05.x***, ***PERCo-IR08.x*** к USB-порту ПК может потребоваться установить дополнительный драйвер. Файл архива с драйвером можно загрузить с сайта компании ***PERCo***, расположенного по адресу www.perco.ru, из разделе **Главная > Поддержка > Программное обеспечение**. После скачивания файл архива необходимо распаковать.

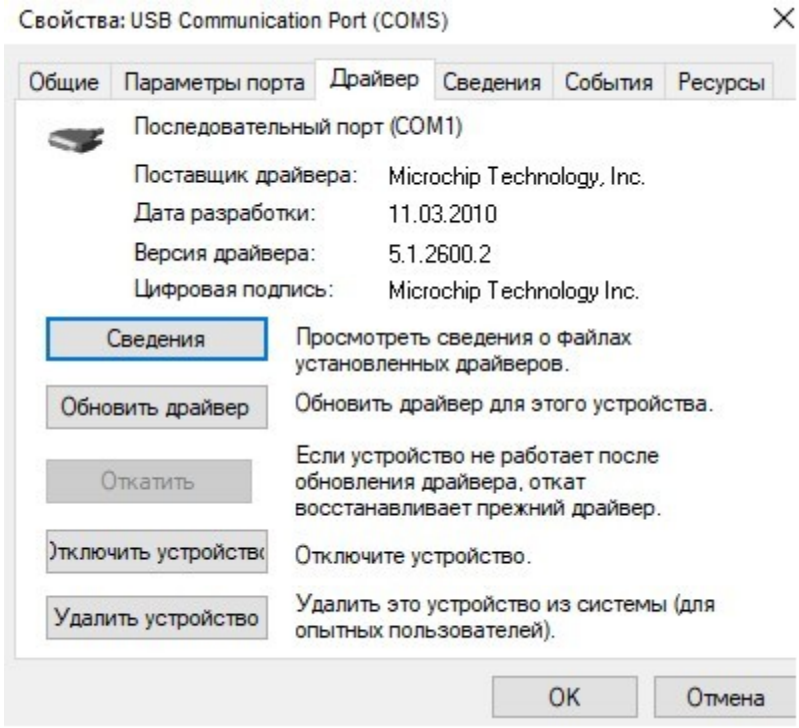
Для установки драйвера:

1. Выберите последовательно: **Пуск > Настройка > Панель управления > > Администрирование > Управление компьютером**. Откроется окно **Управление компьютером**:

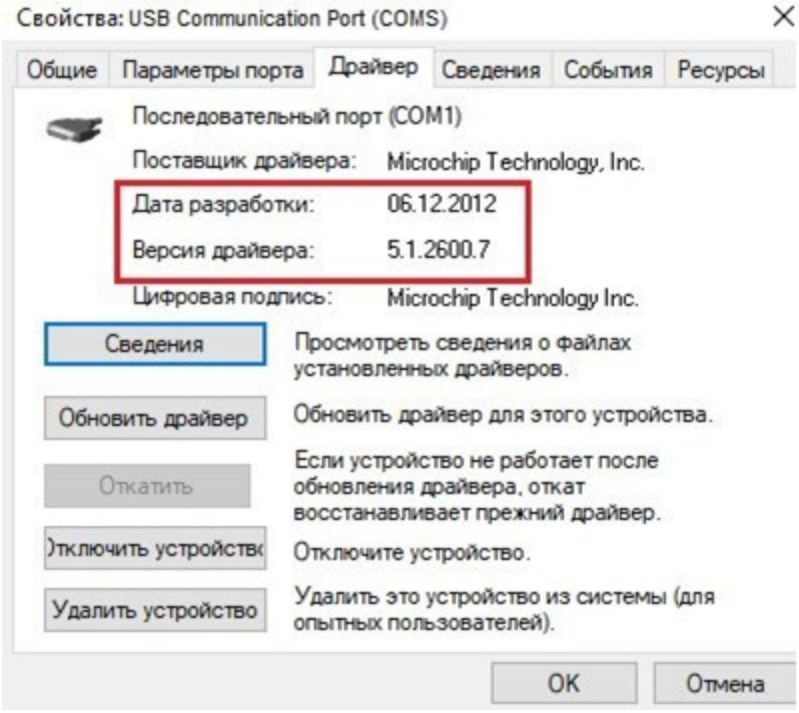



2. В левой части открывшегося окна выберите пункт **Диспетчер устройств**. В рабочей области окна появится список устройств ПК.
3. Найдите в списке **Порты (COM и LPT)** и дважды нажмите левой кнопкой мыши на устройстве **USB Communication Port**. Откроется окно **Свойства: USB Communication Port**.

4. В открывшемся окне перейдите на вкладку **Драйвер**:




5. На вкладке **Драйвер** нажмите кнопку **Обновить**. Будет запущен *Мастер обновления оборудования*, вид которого зависит от версии установленной ОС.
6. Следуя указаниям мастера обновления укажите место расположения драйвера на диске компьютера и установите драйвер.
7. В случае успешной установки драйвера данные на вкладке **Драйвер** окна **Свойства: USB Communication Port** будут изменены. В строках **Дата разработки** и **Версия драйвера** появится информация об установленном драйвере:



# 13. Примеры конфигурирования оборудования

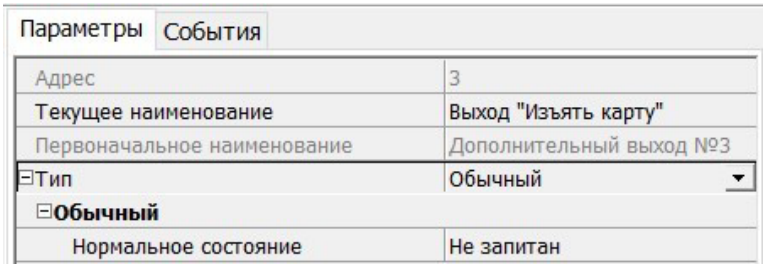
***Внимание!***

Для поддержки возможности подключения внешнего верифицирующего устройства (ВВУ), то есть устройства подтверждения или запрета прохода, необходимо обновить встроенное ПО контроллеров ***PERCo-CT/L04*** и ***PERCo-CT03*** до версии прошивки x.0.0.20.

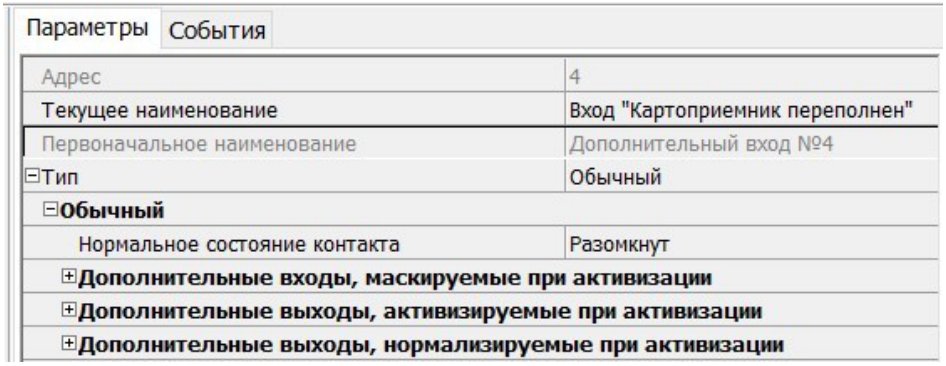
## 13.1. Картоприемник

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

1. Запустите ***«Консоль управления»*** и откройте раздел ***«Конфигуратор»***.
2. Выделите в рабочей области раздела контроллер, к которому подключен картоприемник. Раскройте список его ресурсов.
3. Выделите ресурс типа "дополнительный выход" и переименуйте его в **Выход "Изъять карту"**. Выход должен соответствовать выходу контроллера, к которому физически подключен вход *«Изъять карту»* картоприемника. На панели **Параметры**:
   - для параметра **Тип** установите значение **Обычный**;




   - для параметра **Нормальное состояние** оставьте значение **Не запитан**:
4. При необходимости настройте реакцию системы на сигнал от картоприемника *«Авария»*. Для этого выделите ресурс типа "дополнительный вход" и переименуйте его во **Вход "Картоприемник переполнен"**. Вход должен соответствовать входу контроллера, к которому физически подключен выход *«Авария»* картоприемника. На панели **Параметры**:
   - для параметра **Тип** выберите **Обычный**;
   - для параметра **Нормальное состояние контакта** установите значение **Разомкнут**;
   - настройте нужную реакцию, используя параметры активизации или нормализации выходов:



5. Выделите ресурс типа "дополнительный вход" и переименуйте его в **Вход "Карта изъята"**. Вход должен соответствовать входу контроллера, к которому физически подключен выход *«Карта изъята»* картоприемника. На панели **Параметры**:
   - для параметра **Тип** выберите **Подтверждение от ВВУ**;
   - для параметра **Нормальное состояние контакта** – значение **Разомкнут**;


   - для параметров **Контроллер, Считыватель** выберите контроллер и считыватель, для которых будет подтвержден проход от картоприемника.

***Примечание:***

Для контроллеров с версией прошивки x.0.0.19 и ниже недоступно значение параметра **Тип: Подтверждение от ВВУ** для ресурса типа **"Дополнительный вход"**. В этом случае выход картоприемника *«Карта изъята»* подключается ко входу управления контроллера *DU A* или *DU B* и дополнительно не конфигурируется в ПО. Тот же метод подключения может использоваться в том случае, если все дополнительные входы контроллера заняты.

6. Выделите ресурс типа "считыватель" и переименуйте его в **Считыватель на выход.** Номер считывателя должен соответствовать выходному считывателю, в направлении которого установлен картоприемник. На панели **Параметры**:
   - Для параметра **Способ верификации** установите значение **ВВУ**.
   - В выпадающем списке отметьте флажками параметры: **при проходе ПОСЕТИТЕЛЕЙ**; **при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ**; **при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**. В этом случае подтверждением для контроллера доступа будет сигнал от картоприемника *«Карта изъята»*.
   - Для параметра **Подтверждение прохода для ПОСЕТИТЕЛЕЙ** установите требуемое значение.
   - Для параметра **Время ожидания подтверждения** установите требуемое значение времени, в течение которого контроллер должен ожидать сигнал *«Карта изъята»*.
   - Для параметра **Дополнительные выходы активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ** установите **Критерий активизации** в положение **На время срабатывания**; затем установите флажок **Выход "Изъять карту"**.
   - Для параметра **Изымать идентификаторы ПОСЕТИТЕЛЕЙ** установите требуемое значение. Идентификаторы посетителей будут изыматься при условии, что:
     - выбраны значения параметра **После любого прохода** или **После прохода в последний день действия идентификатора**.

Параметры | События | Камера СКУД

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

- в разделе ***«Доступ»*** **> «Доступ посетителей»** установлен параметр **Удалять после прохода** для указанных посетителей.

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

## 13.2. Конфигурирование одного алкотестера для одного направления

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

После монтажа и подключения алкотестера необходимо произвести его конфигурирование в сетевом ПО системы, для этого выполните следующие действия:

1. Запустите ***«Консоль управления»*** и откройте раздел ***«Конфигуратор»***.
2. Выделите в рабочей области раздела контроллер, к которому подключен алкотестер. Раскройте список его ресурсов.
3. Выделите ресурс типа "дополнительный вход" и переименуйте его во **Вход "Подтверждение от алкотестера" на вход**. На панели **Параметры**:
   - для параметра **Тип** установите значение **Подтверждение от ВВУ**;
   - для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели);


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

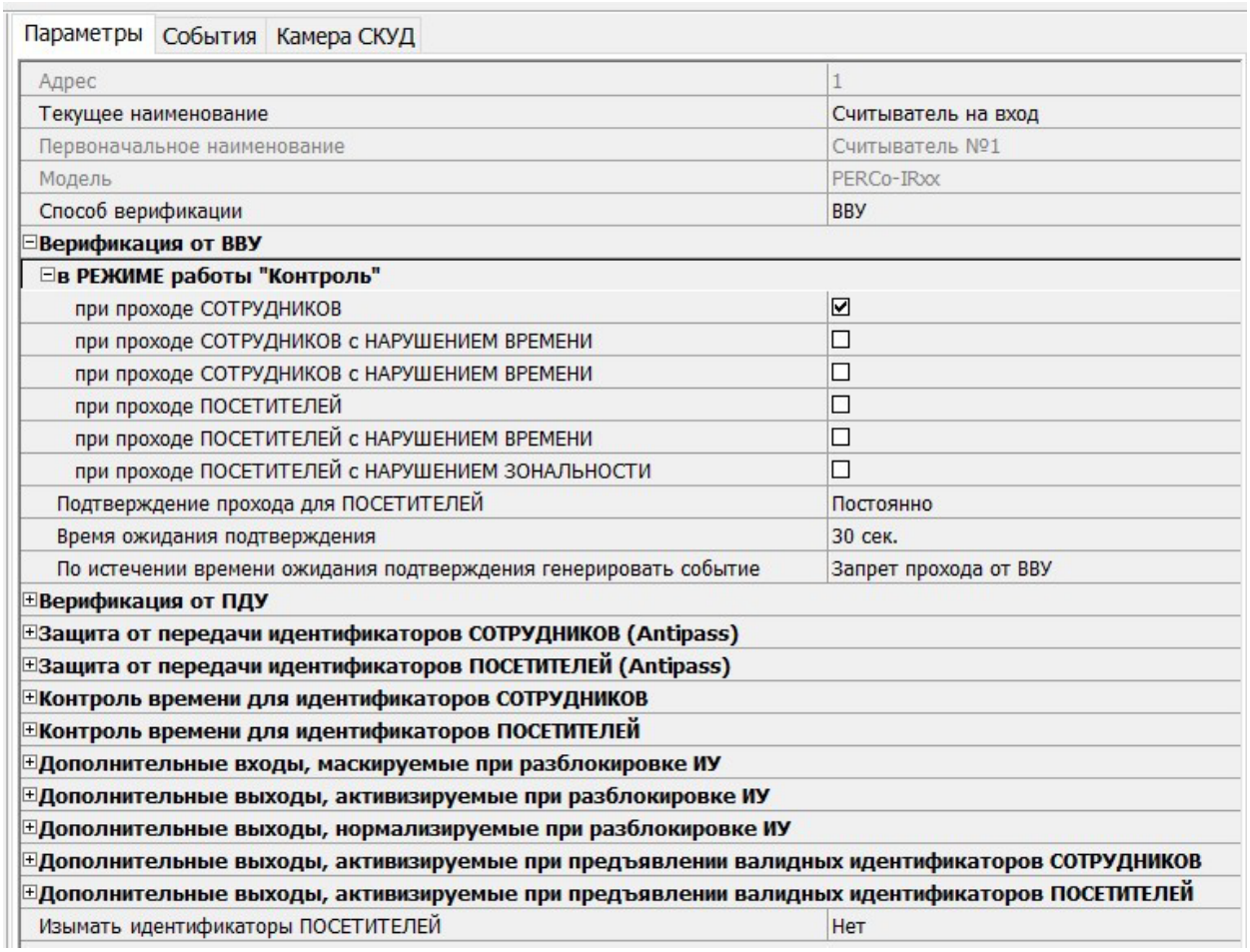
***Примечание:***

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

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


5. Выделите ресурс типа "считыватель" и переименуйте его в **Считыватель на вход.** Номер считывателя должен соответствовать считывателю, в направлении которого установлен алкотестер. На панели **Параметры**:
   - для параметра **Способ верификации** установите значение **ВВУ**;
   - в раскрывшемся списке отметьте флажками параметры: **при проходе СОТРУДНИКОВ** и при необходимости **при проходе ПОСЕТИТЕЛЕЙ**; для параметра **Подтверждение прохода для ПОСЕТИТЕЛЕЙ** установите требуемое значение;

- для параметра **Время ожидания подтверждения** установите требуемое значение времени, в течение которого контроллер должен ожидать управляющий сигнал от алкотестера;
- для параметра **По истечении времени ожидания подтверждения генерировать событие** установите значение **Запрет прохода от ВВУ**, если к контроллеру подключены два выхода алкотестера (для управляющих сигналов разрешения и запрета прохода). **Отказ от прохода, нет ответа от ВВУ**, если подключен только один выход разрешения прохода алкотестера.




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

## 13.3. Конфигурирование двух алкотестеров для двух направлений

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

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

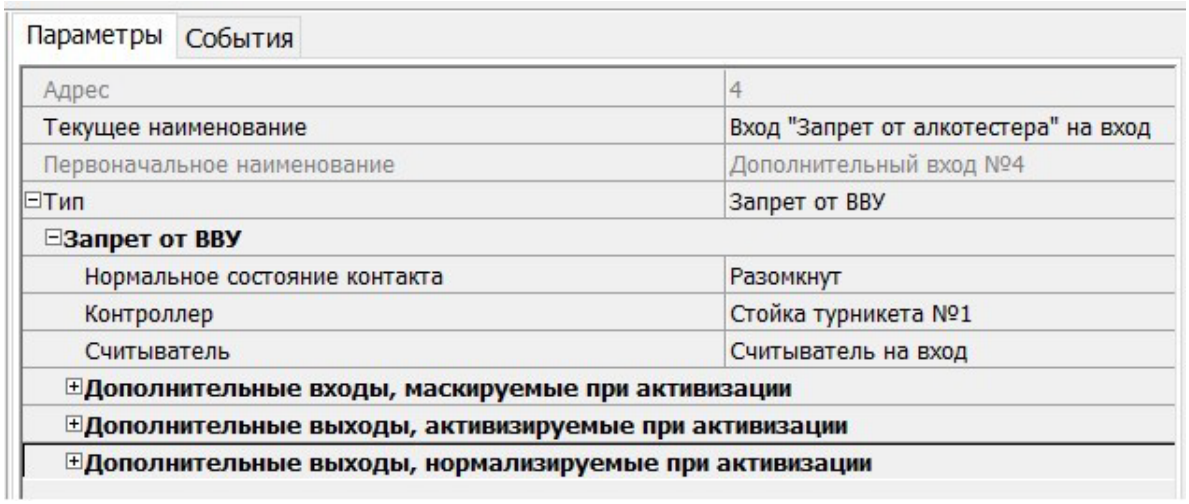
1. Запустите ***«Консоль управления»*** и откройте раздел ***«Конфигуратор»***.
2. Выделите в рабочей области раздела контроллер, к которому подключены алкотестеры. Раскройте список его ресурсов.
3. Выделите ресурс типа "дополнительный вход" и переименуйте его во **Вход "Подтверждение от алкотестера" на вход**. На панели **Параметры**:
   - для параметра **Тип** установите значение **Подтверждение от ВВУ**;

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


***Примечание:***

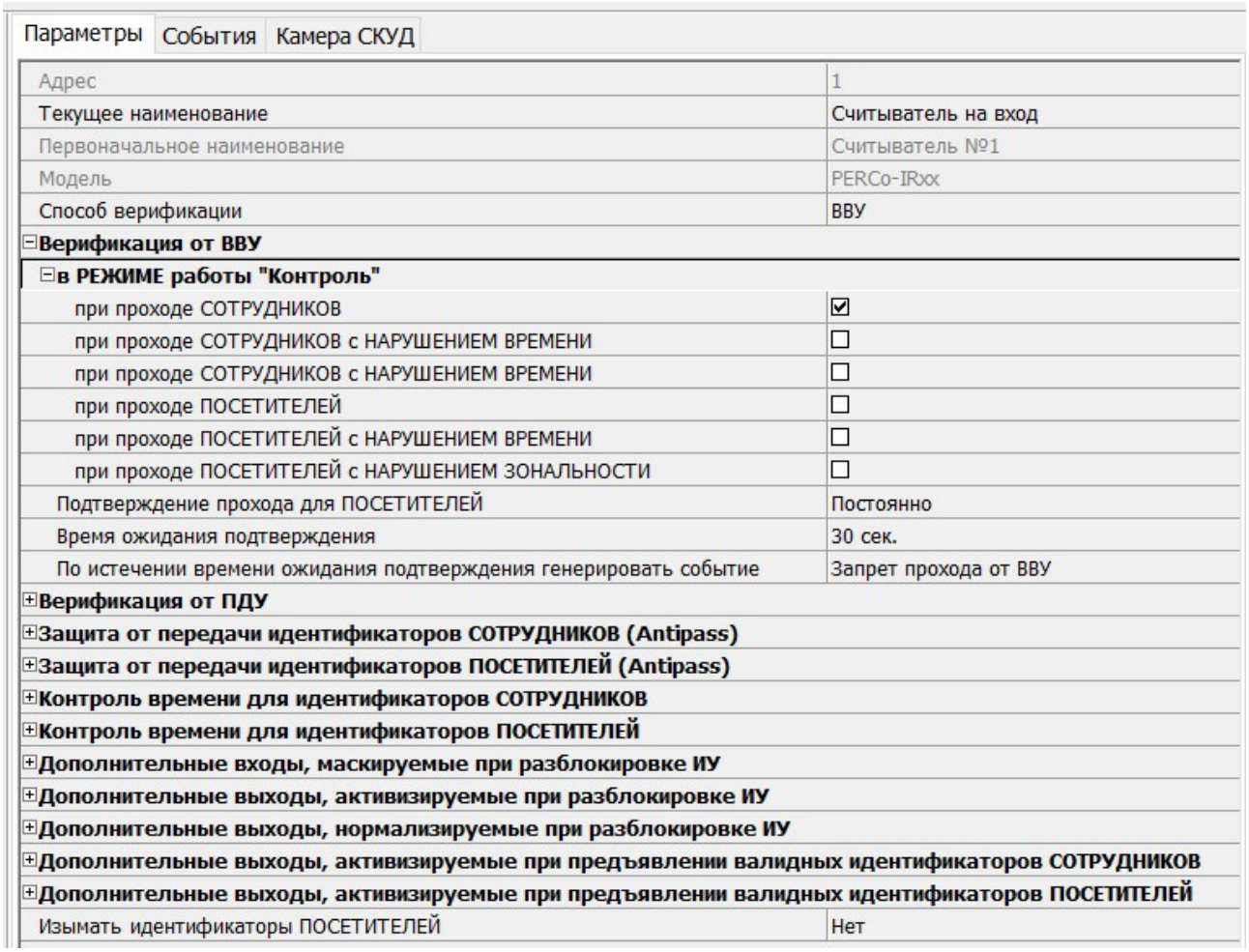
Если к контроллеру подключен только один выход алкотестера на вход, то **Вход "Подтверждение от алкотестера" на вход** конфигурируется в зависимости от типа управляющего сигнала. **Вход "Запрет от алкотестера" на вход** при этом не используется.

4. Выделите ресурс типа "дополнительный вход" и переименуйте его во **Вход "Запрет от алкотестера" на вход**. На панели **Параметры**:
   - для параметра **Тип** установите значение **Запрет от ВВУ**;
   - для параметра **Нормальное состояние** установите значение **Разомкнут** (зависит от используемой модели);




   - для параметров **Контроллер, Считыватель** выберите контроллер и считыватель, для которых будет отклонен проход от алкотестера на вход.
5. Выделите ресурс типа "считыватель" и переименуйте его в **Считыватель на вход**. На панели **Параметры**:
   - для параметра **Способ верификации** установите значение **ВВУ**;
   - в раскрывшемся списке отметьте флажками параметры: **при проходе СОТРУДНИКОВ**;

- для параметра **Время ожидания подтверждения** установите требуемое значение времени, в течение которого контроллер должен ожидать управляющий сигнал от алкотестера на вход;




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

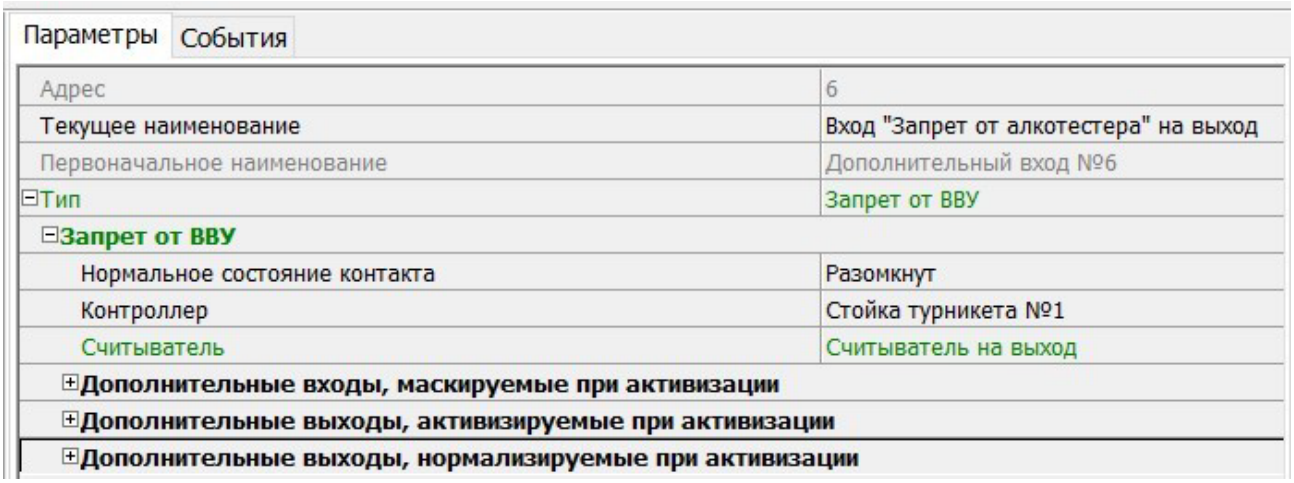
6. Конфигурация первого алкотестера на вход завершена. Перейдем к конфигурации второго алкотестера на выход.

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

***Примечание:***

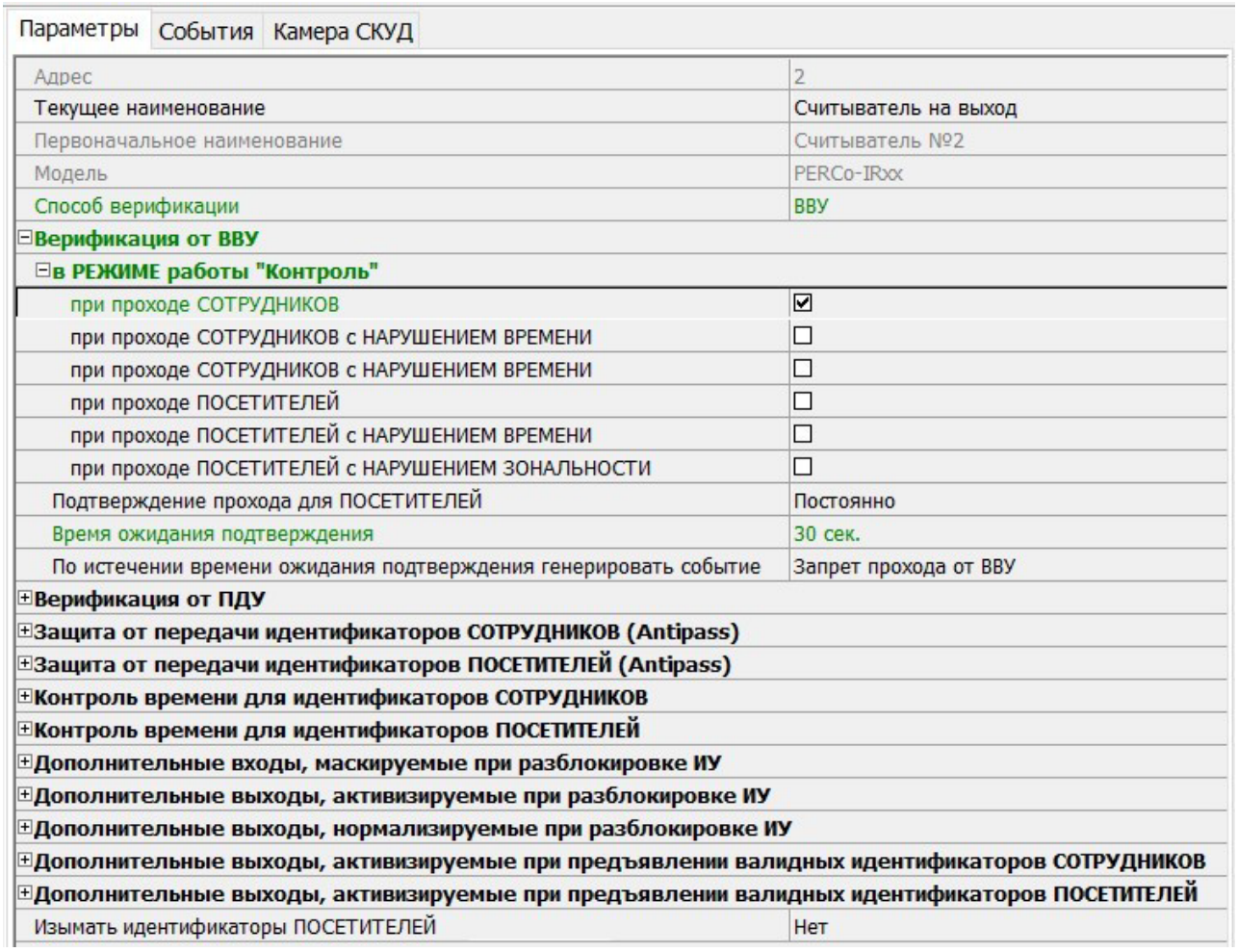
Если к контроллеру подключен только один выход алкотестера на выход, то **Вход "Подтверждение от алкотестера" на выход** конфигурируется в зависимости от типа управляющего сигнала. **Вход "Запрет от алкотестера" на выход** при этом не используется.


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




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

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




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

## 13.4. Биометрический контроллер Suprema BioEntry W2

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

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

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

- для параметра **Таймаут верификации пальцем** (используется в режиме доступа **карта и палец**) установите время, в течение которого будет ожидаться поднесение пальца для сканирования отпечатков (отсчет времени начинается после того, как была предъявлена считывателю карта доступа). Параметр может быть задан в интервале от 1 до 20 секунд;
- для параметра **Таймаут поиска отпечатков** установите время, которое будет отводиться для поиска отпечатка в памяти контроллера. Если за отведенное время отпечаток не будет найден, то аутентификация будет отклонена. Параметр может быть задан в интервале от 1 до 20 секунд;
- для параметра **Чувствительность сканера** установите чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности обеспечивается высокое качество и скорость сканирования, при низком заданном уровне чувствительности – уменьшается влияние факторов внешней среды (температуры и влажности воздуха, освещенности помещения, чистоты сканируемой поверхности подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию. Понижение заданного уровня чувствительности сканера осуществляется при необходимости в зависимости от условий эксплуатации. Параметр может быть задан в интервале от 1 до 7, где значение «1» – соответствует самой низкой чувствительности, а значение «7» – самой высокой;
- для параметра **Алгоритм поиска отпечатков** установите автоматический алгоритм (рекомендован производителем) поиска отпечатков пальцев;
- для параметра **Режим датчика** установите режим работы считывающего датчика – либо он работает всегда, либо включается автоматически, если обнаруживает палец;
- для параметра **Режим авторизации** установите режим доступа:
  - **частный режим доступа** – в этом случае параметры доступа устанавливаются для отдельного сотрудника / посетителя в рамках СКУД;
  - **общий режим доступа** – в этом случае параметры доступа устанавливаются в рамках биометрического контроллера и будут применяться для всех пользователей, взаимодействующих 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 выпадающего списка выбрать **Нормально закрыто**.

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

***Примечание:***

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

- параметр **Настройки Wiegand (Режим)** – позволяет задать режим работы интерфейса *Wiegand* контроллера ***Suprema***:
  - **Вход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как вход. В этом режиме контроллер ***Suprema*** работает как обычный контроллер доступа, ожидая поступления данных по интерфейсу *Wiegand.*
  - **Выход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как выход. В этом режиме контроллер ***Suprema*** работает совместно с контроллером ***PERCo*** в составе СКУД (может производить аутентификацию и управление подключенным по интерфейсу *Wiegand* оборудованием (замком и т.д.)).
- параметр **Использовать аутентификацию** – при установке флажка контроллером ***Suprema*** при предъявлении карты / пальца будет производиться предварительная аутентификация. В случае успешной предварительной аутентификации данные будут переданы в контроллер ***PERCo*** для повторной аутентификации (загорится зеленая индикация). В случае ошибки предварительной аутентификации данные в контроллер ***PERCo*** передаваться не будут – необходимо провести повторную успешную аутентификацию. Если флажок не выставлен, то процедура аутентификации будет 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**.

# 14. Модуль ABBYY распознавания данных документа

## 14.1. Дополнительные системные требования

Для распознавания данных документов, удостоверяющих личность, в системе используется инструмент *ABBYY PassportReader SDK*. С его помощью можно извлечь данные, например, из таких документов, как паспорт гражданина Российской Федерации, заграничный паспорт, водительское удостоверение.

***Примечание:***

По умолчанию в ***PERCo-S-20*** поддерживается *ABBYY PassportReader SDK* версии 1.5. Для перехода на версию 1.5.2 обновите ПО в соответствии с инструкцией.

Дополнительные требования:

- 100% TWAIN-совместимый сканер для сканирования.
- Пользователь должен иметь права доступа к следующим разделам системного реестра:
  - "HKEY_LOCAL_MACHINE\Software\ABBYY\PassportReader SDK\1.5" – полный контроль только для установки:
  - "HKEY_LOCAL_MACHINE\Software\ABBYY\FREngine\9.0\LicenseManager" – полный контроль.
- Следующие папки должны быть доступны:
  - Папка с бинарными файлами *ABBYY PassportReader SDK* – доступ на чтение,
  - Папка %TEMP% – полный доступ.
- Версия *Microsoft .NET Framework* должна быть не ниже 3.5. Вы можете установить *.NET Framework 3.5,* запустив файл dotnetfx35setup.exe с установочного компакт-диска *ABBYY PassportReader* SDK.

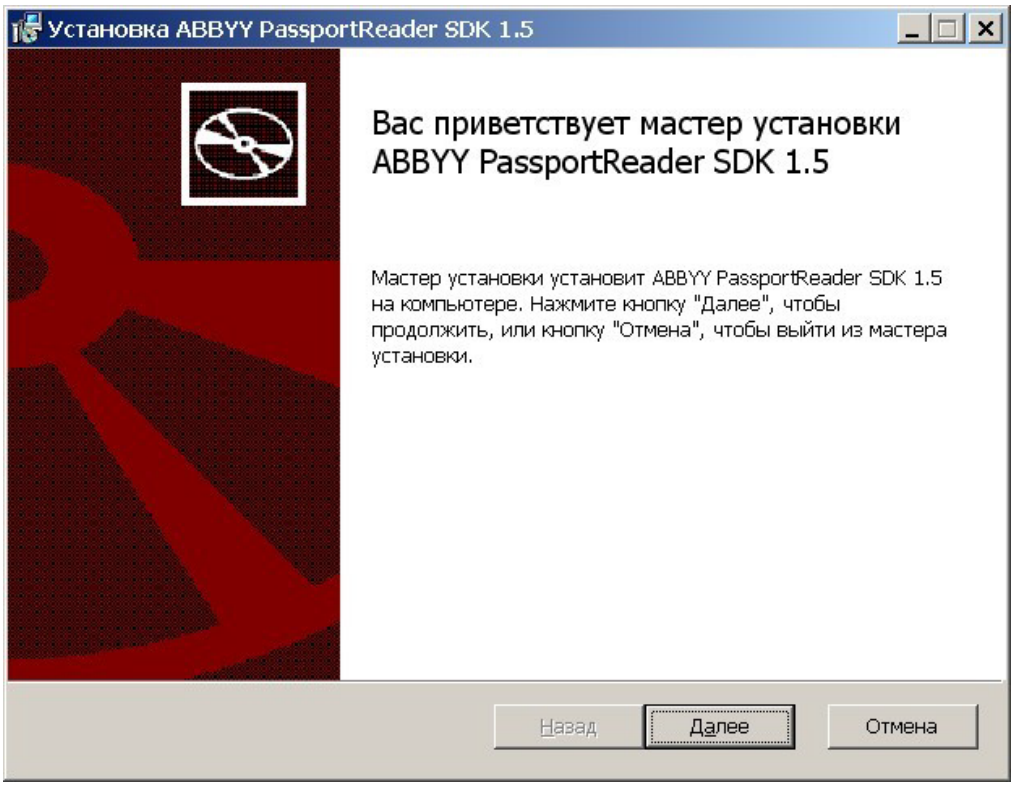
***Примечание:***

Если на ПК установлена ОС *Windows 8*, то на ней предустановлена версия *.NET Framework 4.0*. В этом случае вы можете включить компонент .NET Framework 3.5 в *Компонентах Windows*.

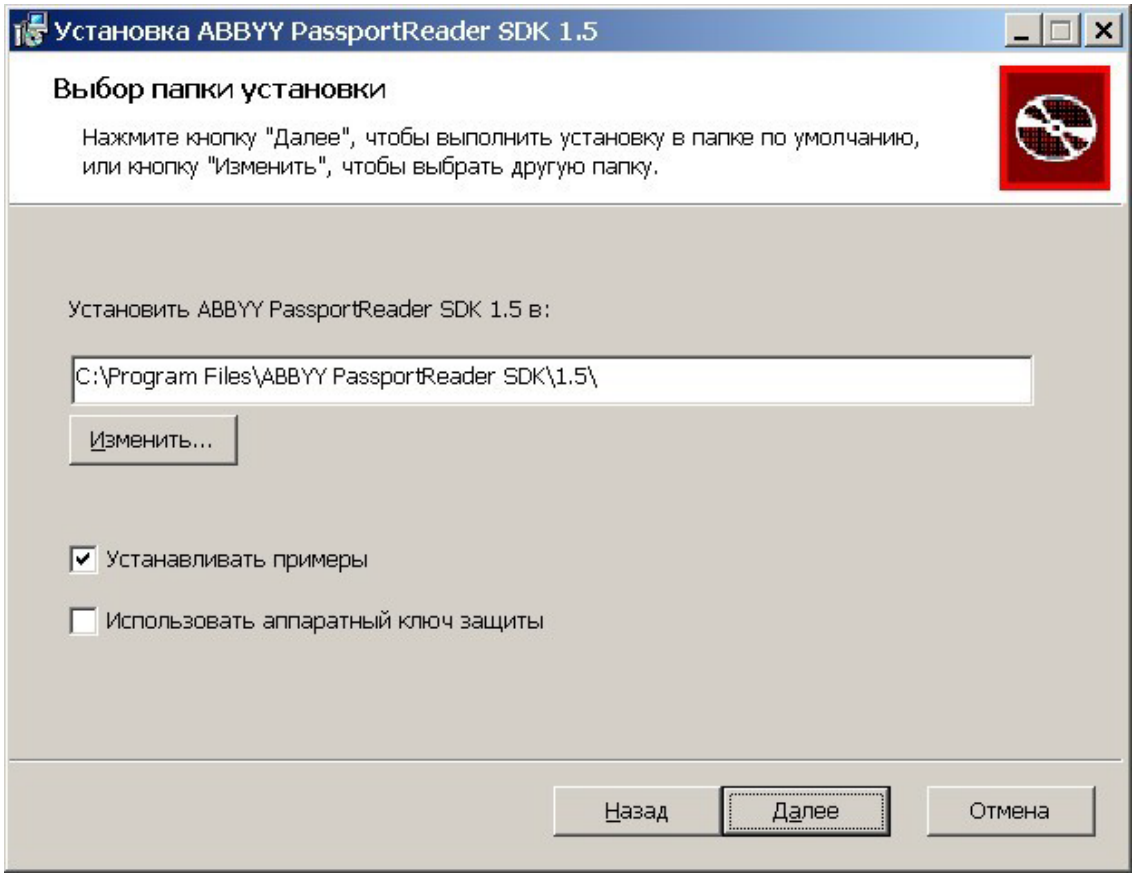
## 14.2. Установка ABBYY PassportReader SDK

Чтобы установить *ABBYY PassportReader SDK*:

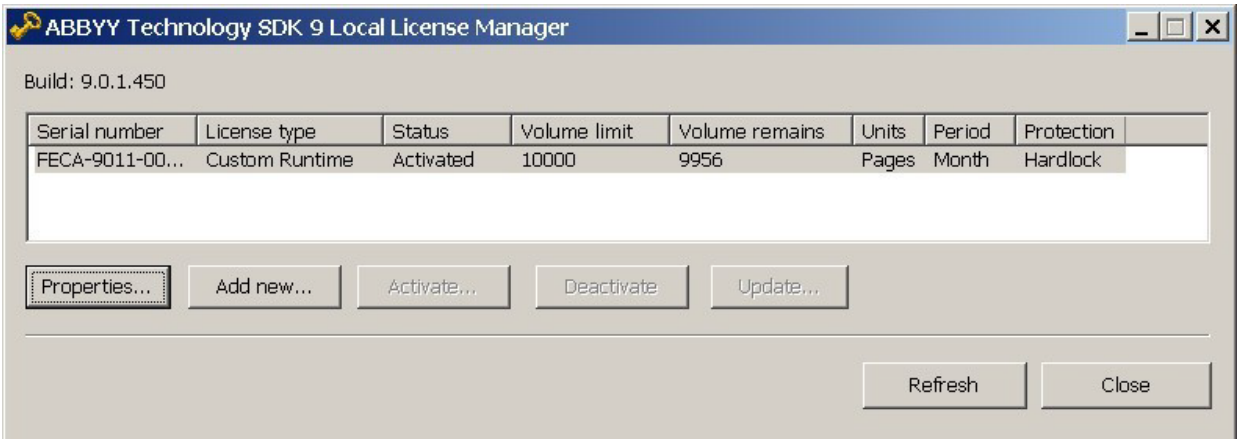
1. Запустите файл `ABBYY PassportReader SDK.msi` с компакт-диска *ABBYY PassportReader SDK* и следуйте инструкциям ***Мастера установки***:




2. При необходимости измените путь к папке установки:



3. Установите флажок **Устанавливать примеры**, если установка производится с целью разработки нового приложения или для просмотра готовых примеров использования API.
4. Установите флажок **Использование аппаратного ключа защиты**, если лицензионный ключ вашей копии программы сохранен в USB-ключе.




После завершения установки запускается ***Менеджер лицензий***. Если этого не произошло, выберите последовательно: **Пуск > Программы > ABBYY PassportReader SDK 1.5 > Менеджер лицензий**.

***Примечание:***

В случае использования аппаратного ключа защиты активация лицензии не требуется, достаточно установить драйверы аппаратного ключа защиты и подключить USB-ключ к ПК. Чтобы установить драйверы аппаратного ключа защиты, запустите файл `IKEYDRVR.EXE` из папки *USB Drivers* установочного компакт-диска.

5. С помощью ***Менеджера лицензий*** можно активировать лицензию *ABBYY PassportReader SDK* и посмотреть ее свойства. Нажмите кнопку **Add new…**, добавьте лицензию вашей копии программы в список и активируйте ее через интернет или по электронной почте, следуя инструкциям ***Мастера активации***.
6. После завершения активации библиотека *ABBYY PassportReader SDK* готова к использованию. Подробную информацию о продукте можно узнать из *Руководства пользователя ABBYY PassportReader SDK*. Для просмотра руководства нажмите последовательно: **Пуск > Программы > ABBYY PassportReader SDK 1.5 > Руководство пользователя**.

## 14.3. Установка в автоматическом режиме

Библиотека *ABBYY PassportReader SDK* может быть установлена в автоматическом режиме через командную строку. При установке могут быть использованы следующие параметры командной строки:

`INSTALL_SAMPLES` – установка примеров кода.

Значение 1 – устанавливать примеры кода.

По умолчанию примеры кода устанавливаются.

`.USE_HW_KEY` – использование аппаратного ключа защиты.

Значение 1 – использовать аппаратный ключ защиты. В этом случае программа будет настроена на использование аппаратного ключа защиты.

После завершения установки необходимо установить драйверы аппаратного ключа защиты. Для этого запустите файл `IKEYDRVR.EXE` из папки *USB Drivers* установочного компакт-диска.

По умолчанию аппаратный ключ не используется.

Также можно воспользоваться стандартными параметрами утилиты `msiexec`. Ниже приведены примеры командных строк для основных сценариев установки:

- Установка библиотеки *ABBYY PassportReader SDK* и примеров кода. Для работы с продуктом будет использоваться программный ключ защиты (лицензионный ключ, хранящийся в файле, который должен быть получен при активации лицензии). В конце установки запускается менеджер лицензий, позволяющий активировать лицензию:
  ```
  msiexec /qn /l* <log file> /I "ABBYY PassportReader SDK.msi"
  ```
- Установка библиотеки *ABBYY PassportReader SDK*. Примеры кода не устанавливаются. После установки продукт готов работать с аппаратным ключом защиты. Обратите внимание, что необходимо установить драйверы аппаратного ключа защиты. Активировать лицензию не требуется, достаточно подключить USB-ключ к ПК. Свойства лицензии можно посмотреть при помощи менеджера лицензий:
  ```
  msiexec /qn /l* <log file> /I "ABBYY PassportReader SDK.msi"
  INSTALL_SAMPLES="" USE_HW_KEY="1"
  ```

## 14.4. Обновление модуля «Распознавание документов»

В системе ***PERCo-S-20*** предусмотрена возможность обновления интеграции систем ***PERCo-S-20*** и *ABBYY PassportReader SDK*, в частности, переход на версию *ABBYY PassportReader SDK* 1.5.2.

**Дополнительные требования к программным средствам**

- Операционная система: *Windows* 7 и выше.
- К использованию рекомендуется 32-битная версия *ABBYY PassportReader SDK* 1.5.2.
- Пользователь *Windows* должен иметь права администратора, так как при обновлении требуется добавление параметра в реестр *Windows*.

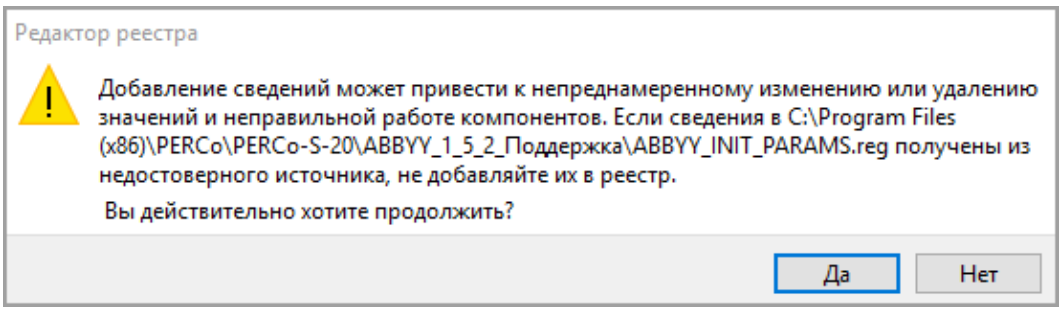
**Порядок обновления ПО ABBYY PassportReader SDK до версии 1.5.2**

***Примечание:***

При использовании ***PERCo-S-20*** версии 3.9.8.1 скачайте архив с файлами обновления по ссылке: https://www.perco.ru/products/modul-po-raspoznavanie-dokumentov.php.

В ***PERCo-S-20*** версии 3.9.8.2 архив с файлами обновления поставляется вместе с дистрибутивом ***PERCo-S-20***.

1. Удалите старую версию ПО *ABBYY PassportReader SDK*.
2. Распакуйте архив и скопируйте его содержимое с файлами обновления в каталог ПО ***PERCo-S-20*** (с полной заменой файлов).
3. Запустите файл `ABBYY_INIT_PARAMS.reg`. В окне **Редактор реестра** выберите **Да**:




4. Процесс обновления завершен.

# 15. Параметры ресурсов

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


Список доступных ресурсов контроллера сгруппирован по типам:

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

Если к контроллеру подключены несколько ИУ или замковые контроллеры ***PERCo-CL201*** (***PERCo-CL211***), то в списке ресурсов будет отображаться несколько контроллеров ИУ. Каждый контроллер ИУ также обладает своим списком ресурсов:

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

В зависимости от типа контроллера наличие и количество ресурсов может различаться. Ниже в таблицах представлен перечень ресурсов контроллеров.

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

| Модель* (номер шаблона) | Доп. вход | Доп. выход | ШС | ОЗ | CL201/ CL211 | Контроллер ИУ | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Считы-ватель | ИУ | Ген. тревоги | ЗС |
| **Контроллеры PERCo** | | | | | | | | | |
| **CL201/CL211** | 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 контроллера ЭП ***PERCo-CT03***:

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

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

| Модель (номер шаблона) | Доп. вход | Доп. выход | ШС | ОЗ | CL201/ CL211 | Контроллер ИУ | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Считы-ватель | ИУ | Ген. тревоги | ОЗ |
| **Контроллеры доступа** | | | | | | | | | |
| **CL201/CL211** | 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\CR01.9** | - | - | - | - | - | 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(KR 05.2)** – ЭП ***PERCo-KR 05.2***;
**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*** или ***PERCo-CL211***):

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 с контроллером ***PERCo-CT03.2*** (к любой конфигурации возможно подключить до восьми контроллеров замка ***PERCo-CL201*** или ***PERCo-CL211***):

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».

## 15.3. Ресурсы контроллеров и ЭП PERCo 1.X

| Модель (номер шаблона) | Доп. вход | Доп. выход | CL201/ CL211 | Контроллер ИУ | |
|---|---|---|---|---|---|
| | | | | Считыватель (+сканер) | ИУ |
| **Контроллеры доступа** | | | | | |
| **CL201/CL211** | 0 | 0 | - | 1 | L |
| **CT/L14\CT/L14.1 (1)** | 10 | 6 | до 8 | 2 (+2) | G |
| **CT/L14\CT/L14.1 (2)** | 6 | 4 | до 8 | 4 (+2) | G+L+L |
| **CT/L14\CT/L14.1 (3)** | 5 | 4 | до 8 | 4 (+2) | G+T |
| **CT/L14\CT/L14.1 (4)** | 5 | 3 | до 8 | 4 (+2) | L+L+L+L |
| **CT/L14\CT/L14.1 (5)** | 4 | 3 | до 8 | 4 (+2) | T+L+L |
| **CT/L14\CT/L14.1 (6)** | 3 | 3 | до 8 | 4 (+2) | T+T |
| **CT/L14\CT/L14.1 (7)** | 9 | 5 | до 8 | 4 (+2) | Шлюз (L+L) |
| **CT/L14\CT/L14.1 (8)** | 8 | 5 | до 8 | 4 (+2) | Шлюз (T) |
| **CT/L14\CT/L14.1 (9)** | 6 | 4 | до 8 | 4 (+2) | Шлюз (T+L) |
| **CT/L14\CT/L14.1(10)** | 3 | 3 | до 8 | 4 (+2) | Шлюз (T+T) |
| **CT/L14\CT/L14.1(11)** | 7 | 5 | до 8 | 4 (+2) | Шлюз (G+G) |
| **CL15, CL15.1, CL15.3, CL15.7** | 1 | 1 | - | 1 | L |
| **Контроллер регистрации** | | | | | |
| **CR11, CR11.1** | - | - | - | 1 на 2 направления | - |
| **CR02.9** | - | - | - | 2 | - |
| **Электронные проходные** | | | | | |
| **CT13\CT13.1 (1)** | 8 | 5 | до 8 | 2 (+2) | IP-Stile |
| **CT13\CT13.1 (2)** | 7 | 4 | до 8 | 2 (+2) | IP-Stile+IC |
| **CT13\CT13.1 (3)** | 8 | 4 | до 8 | 2 (+2) | IP-Stile+AP |
| **CT13\CT13.1 (4)** | 7 | 3 | до 8 | 2 (+2) | IP-Stile+IC+AP |

Принятые в таблице сокращения:

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

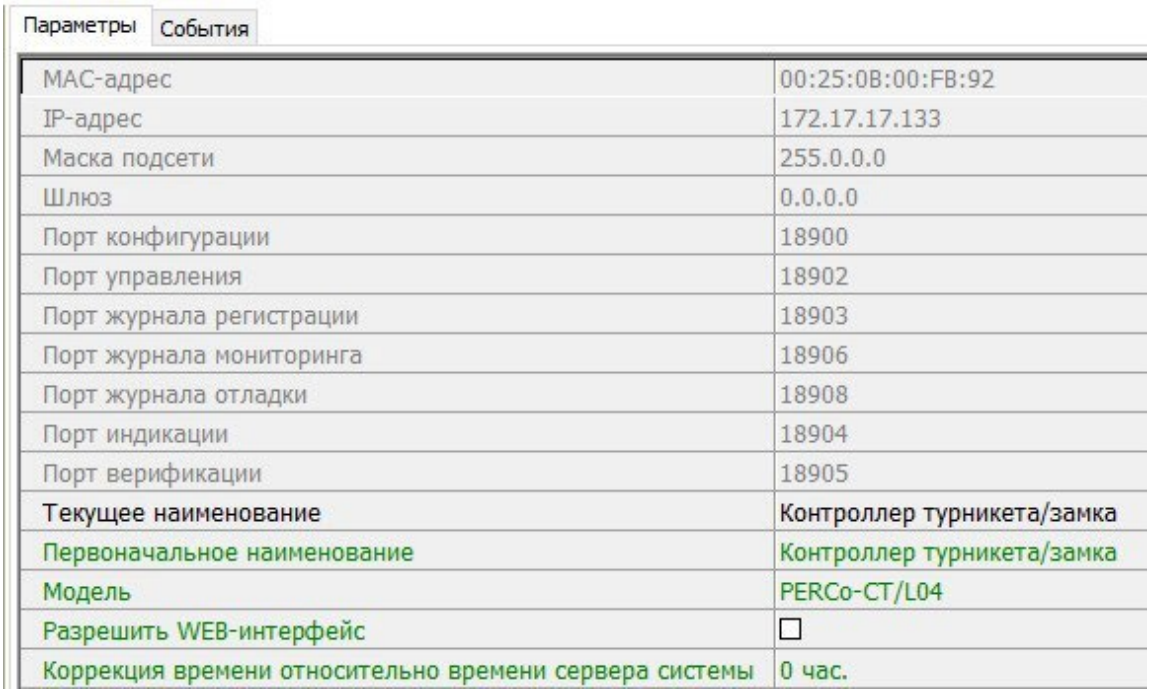
Варианты шаблонов конфигурации контроллера ***PERCo-CT/L14*** или ***PERCo-CT/L14.1***:

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

Варианты шаблонов конфигурации ЭП с контроллером ***PERCo-CT13 / PERCo-CT13.1***:

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

## 15.4. Контроллер доступа

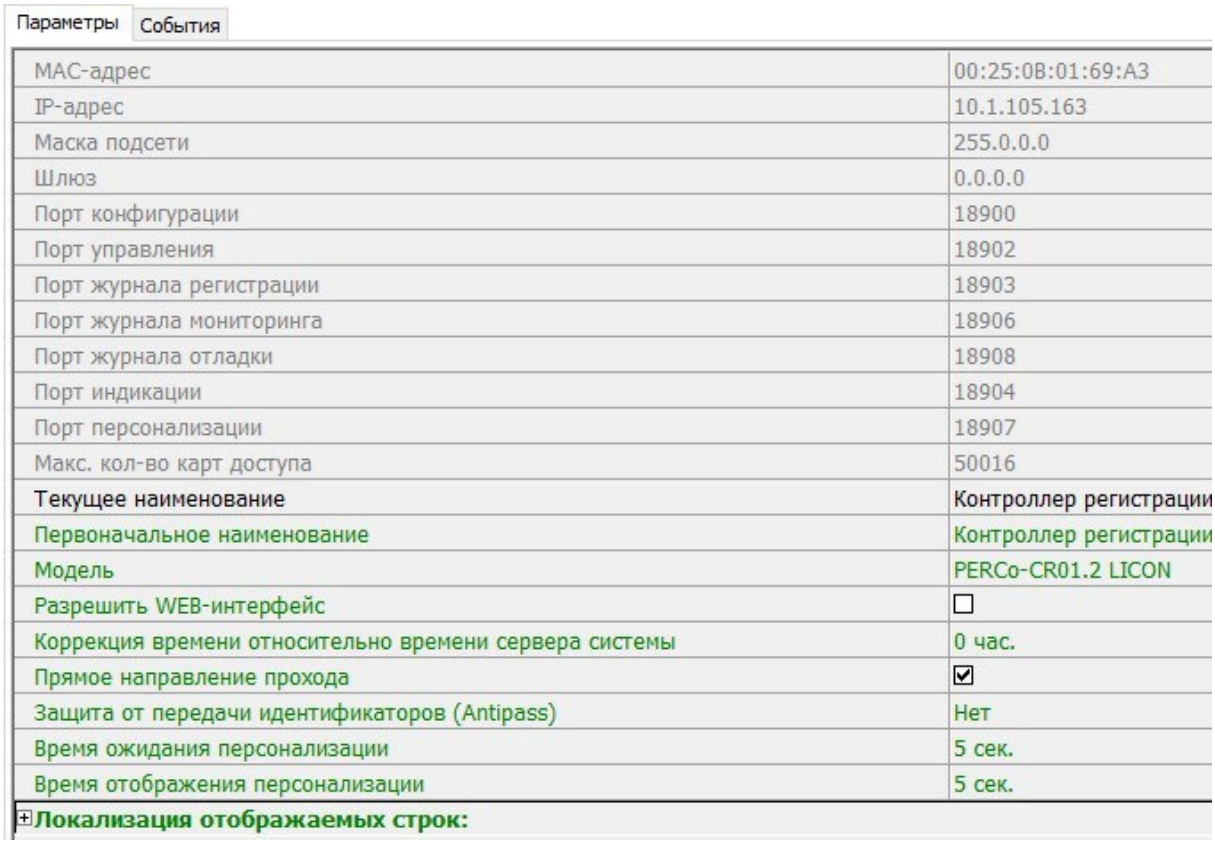



В окне доступны следующие параметры:

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

## 15.5. Контроллер регистрации (LICON)

Доступны следующие параметры:




- **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:***

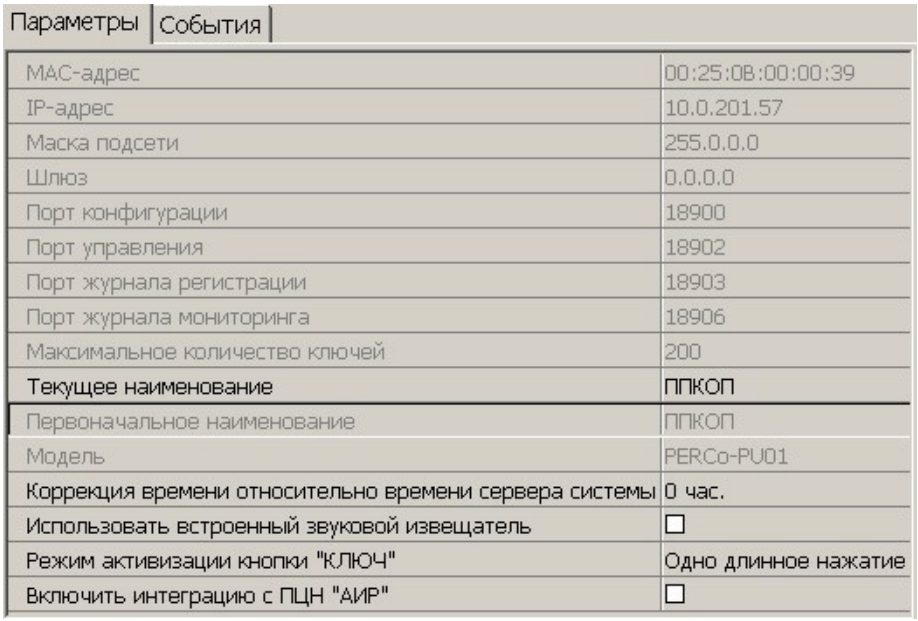
Флажок **Контроль повторного предъявления идентификаторов** автоматически устанавливается при активизации функции системы безопасности **Внешняя защита от передачи идентификаторов (Global Antipass)**.

- **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 №…».*

## 15.6. ППКОП (КБО)

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




- **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".** Раскрывающийся список позволяет выбрать способ разблокирования кнопок БУИ. Доступны следующие варианты:
  - **Одно нажатие**;
  - **Одно длинное нажатие**;
  - **Два длинных нажатия**;
  - **Три коротких нажатия**.
- **Включить интеграцию с ПЦН «АИР»** (для ППКОП). При установке флажка появляется возможность передавать тревожные сообщения на внешний пульт центрального наблюдения (ПЦН) и добавляется ресурс **Объект интеграции с ПЦН «АИР»**.

## 15.7. Интеграция ППКОП с ПЦН "АИР"

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

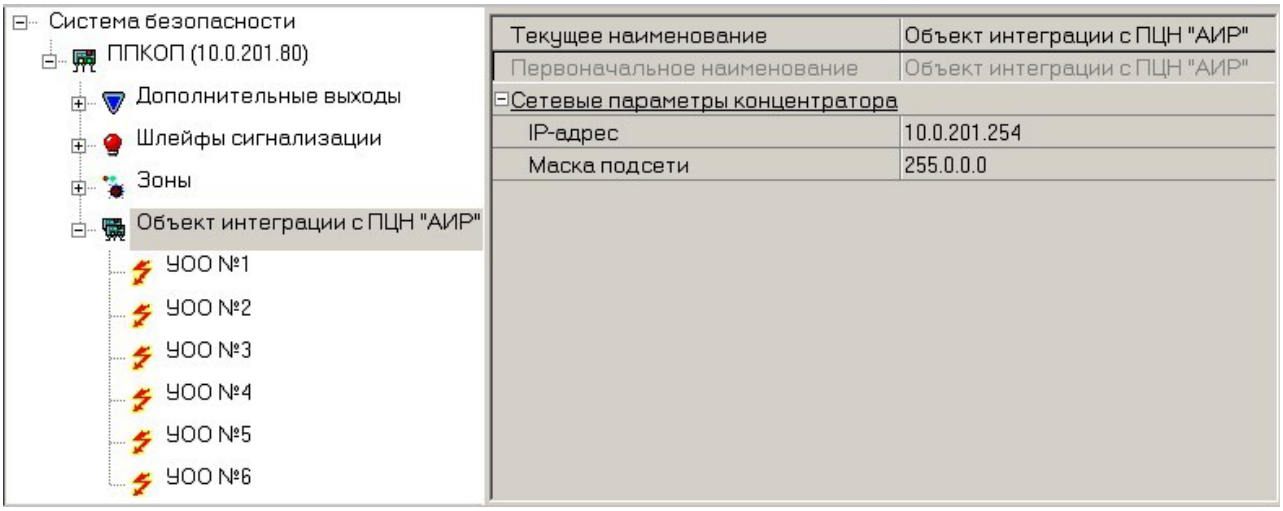
В разделе использованы следующие сокращения:

- УОО – устройство охранное объектовое.
- КТС – кнопка тревожной сигнализации.

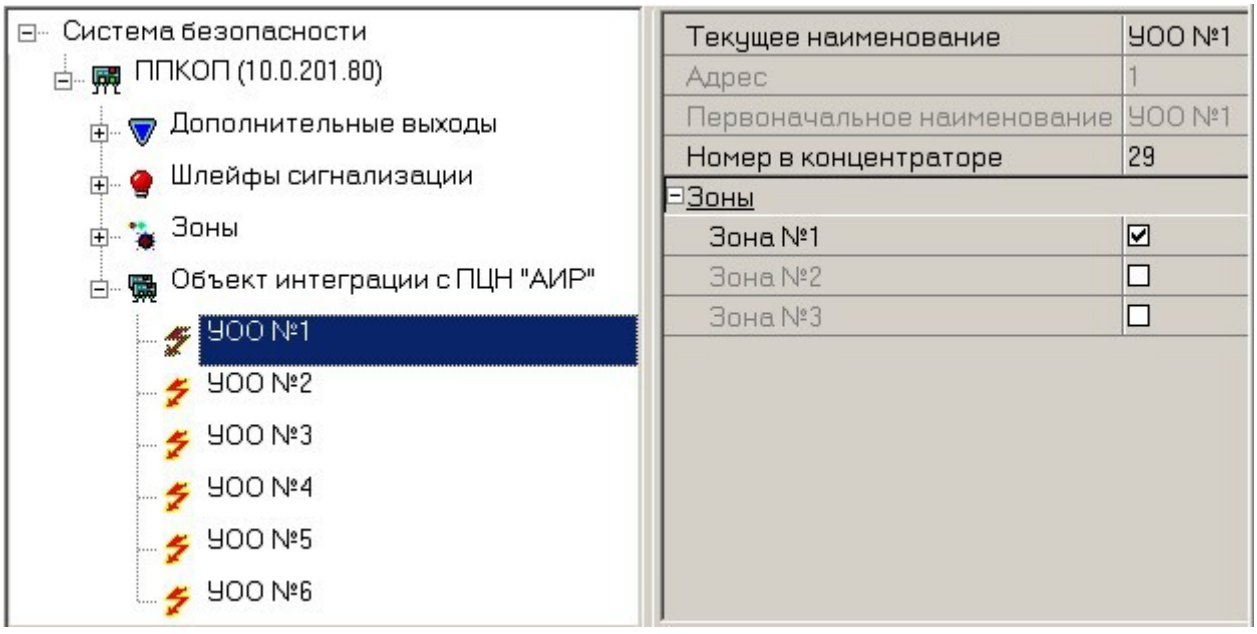
Для включения интеграции следует установить флажок у параметра ППКОП **Включить интеграцию с ПЦН «АИР»**. После этого для ППКОП будет добавлена группа ресурсов **Объект интеграции с ПЦН " АИР"** содержащая шестью ресурсов УОО.

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

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




Для каждого УОО доступны следующие параметры:




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

## 15.8. Считыватель

| | |
|---|---|
| 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 |

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:

- **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»***.
- **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 изымается.
  - **После любого прохода**. Идентификатор изымается из доступа при первом предъявлении.
  - **После прохода в последний день действия идентификатора**. Идентификатор изымается из доступа, если дата предъявления совпадает с датой окончания срока действия карты.

## 15.9. ИУ (Замок / Турникет / Шлагбаум)

Доступны следующие параметры:

- **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.
- **Время ожидания комиссионирования** / **Время досмотра** / **Время ожидания подтверждения проезда картой водителя (сотрудника)**. Параметр позволяет ограничить интервал времени между предъявлением карт пользователя (сотрудника / посетителя / служебного ТС) и комиссионирующей карты (сотрудника / охранника / водителя) в случае, если в правах карты пользователя установлен доступ с комиссионированием / доступ с досмотром / подтверждение проезда картой водителя.
- **Регистрация прохода по предъявлению идентификатора** (не доступен в конфигурации *«Контроллер АТП»*). При установке параметра контроллер будет считать проход совершившимся сразу после предъявления карты доступа, независимо от того, будет ли реально совершен проход через ИУ или нет.

***Внимание!***

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

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

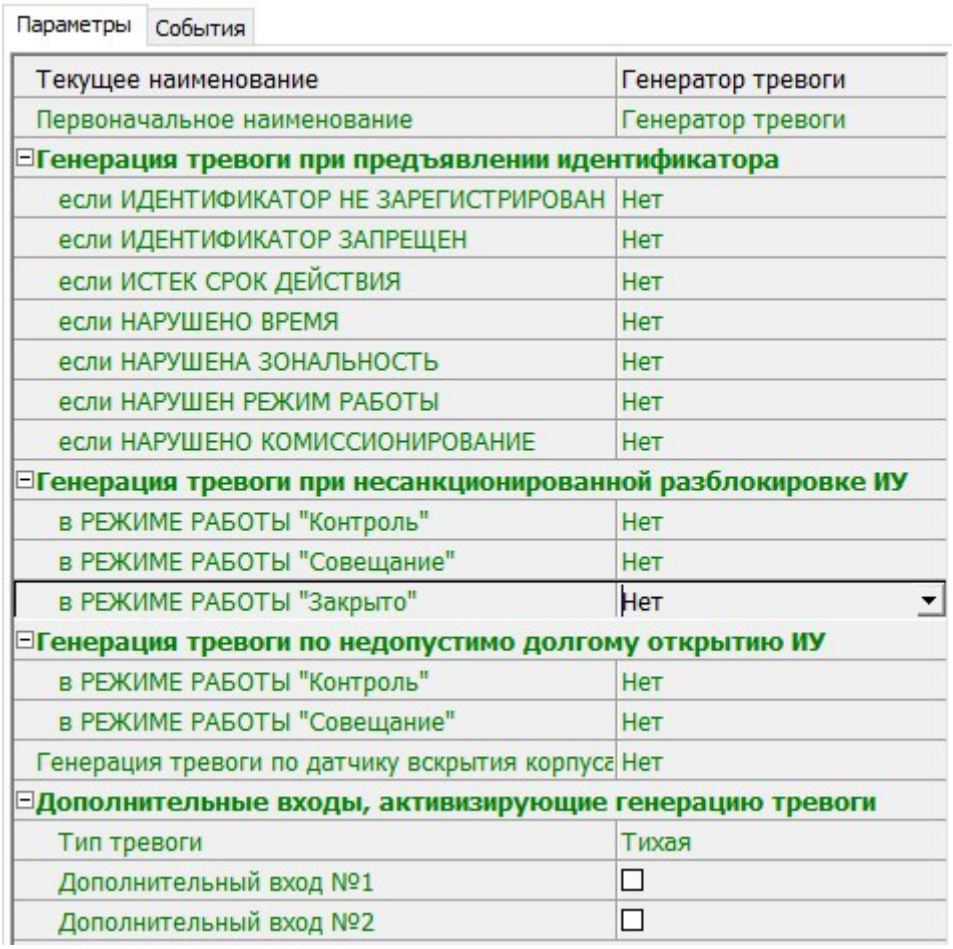
Обратное может привести к некорректной работе функции контроля зональности (Antipass).

Также при установке этого параметра не рекомендуется устанавливать для параметра **Защита от передачи идентификаторов** значение **Жесткая**

- **Отсутствие датчиков проезда** (Доступен только в конфигурации *«Контроллер АТП»*). При установке параметра контроллер будет считать проезд совершившимся сразу после предъявления карты доступа, независимо от того, будет ли реально совершен проход через ИУ или нет. ИУ будет открыто на Время удержания в разблокированном состоянии.
- **Задержка восстановления датчиков проезда** (Доступен только в конфигурации *«Контроллер АТП»*) Параметр определяет промежуток времени между моментом нормализации датчика проезда и подачей команды на закрытие ИУ. Рекомендуемое время 0,5-3 сек.
- **Внутренняя защита от передачи идентификаторов (Local Antipass)**. При установленном параметре контроллер отслеживает случаи повторного прохождения (регистрации) через одно КПП в том же направлении. Для контроллеров ***PERCo CT/L14***, ***CT/L14.1***, ***CL15***, ***CL15.1***, ***CL15.3***, ***CL15.7***, ***CR11***, ***CR11.1***, ***CR02.9***, ***CT13***, ***CT13.1,*** ***CL211.3***, ***CL211.9*** отслеживается повторное предъявление карты доступа / идентификатора одного и того же сотрудника. Для контроллеров ***PERCo CT03.2***, ***CT/L04.2***, ***CR01.2***, ***CR01.9*** отслеживается повторное предъявление одной и той же карты доступа / идентификатора, вне зависимости от закрепленного за ней сотрудника.
- **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.

## 15.10. Генератор тревоги

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




- **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.

## 15.11. Дополнительный вход

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

Доступны следующие параметры:

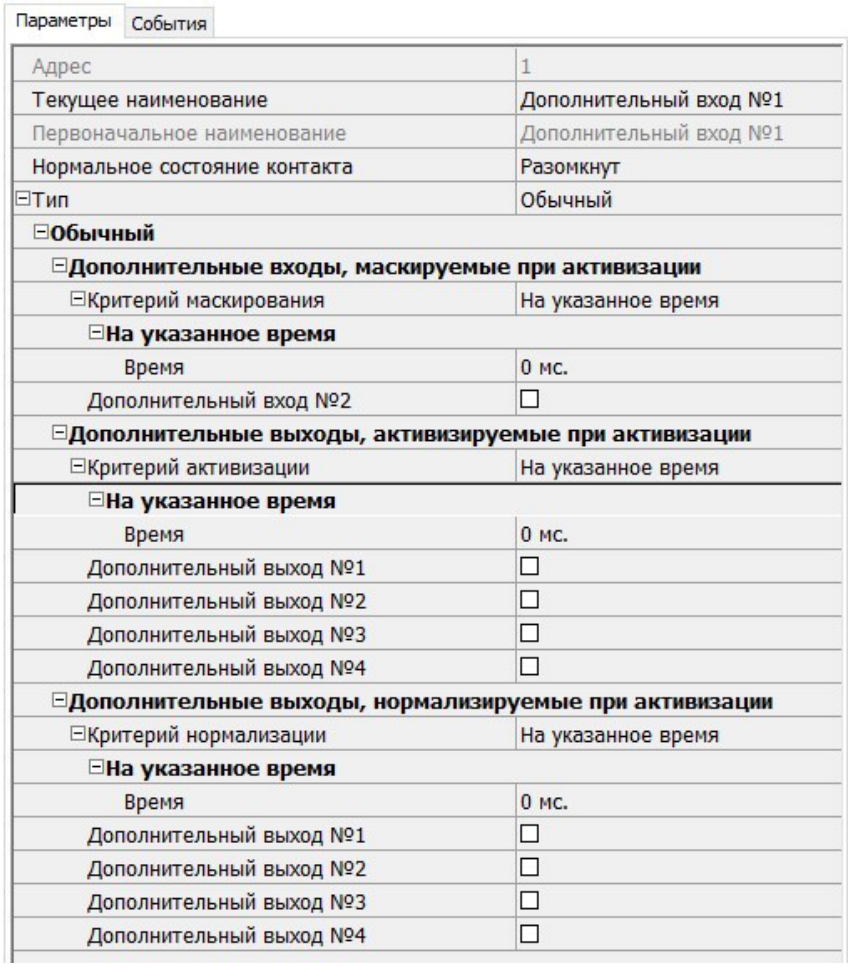
- **Тип.** Выпадающий список позволяет выбрать один из следующих типов:
  - **Нет**. К данному входу не подключено никакое внешнее оборудование.
  - **Обычный**. К данному входу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
  - **Специальный**. Предназначен для автономного сброса тревоги, выключения сирены.
  - **FireAlarm**. Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ *Fire Alarm*. Тип входа **FireAlarm** не может быть изменен для входов контроллеров и ЭП ***PERCo*** серии 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 задает номер ИУ, к которому привязывается считыватель.
  - **Направление**. Параметр задает направление ИУ, к которому привязывается считыватель.

### 15.11.1. Тип входа "Обычный"




Доступны следующие параметры:

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

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

### 15.11.2. Тип входа "Специальный"


Доступны следующие параметры:

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

### 15.11.3. Тип входа "Подтверждение от ВВУ"

| | |
|---|---|
| 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. |

Доступны следующие параметры:

- **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.
- **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.

## 15.11.4. Тип входа "Запрет от ВВУ"

| | |
|---|---|
| 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. |

Доступны следующие параметры:

- **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.

- **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.

## 15.12. Дополнительный выход

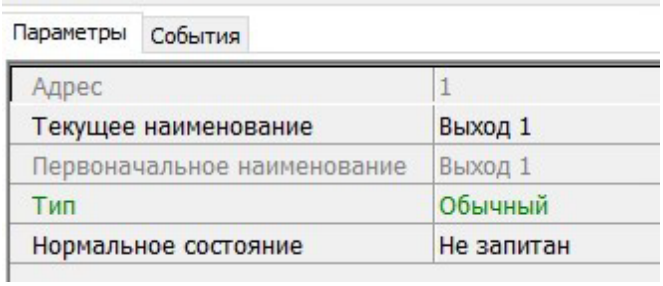
Дополнительные выходы могут быть использованы для управления любым дополнительным оборудованием в рамках системы. Для настройки ресурса доступны следующие параметры:

- **Текущее наименование**. Поле ввода позволяет изменить название выхода.
- **Тип.** Раскрывающийся список позволяет выбрать следующие типы выхода:
  - **Нет**. К данному выходу не подключено никакое внешнее оборудование.
  - **Обычный**. К выходу подключено дополнительное оборудование, логика управления которым определяется через описание других устройств системы (за исключением ресурса **Генератор тревоги**).
  - **Генератор тревоги**. Решение об активизации дополнительного выхода принимается в соответствии с параметрами, заданными для ресурса **Генератор тревоги**.
  - **ОПС**. Выход предназначен для управления световым или звуковым оповещателем, а также для передачи тревожных извещений на пульт центрального наблюдения (ПЦН) при изменении режима ОЗ.

***Примечание:***

После включения питания все выходы нормализуются.

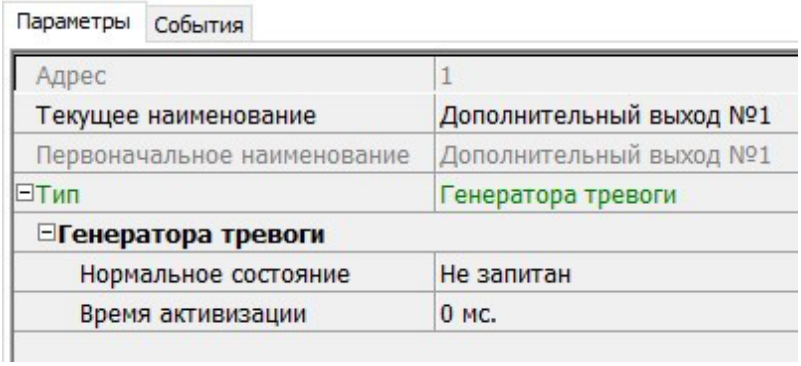
### 15.12.1. Тип выхода "Обычный"




Доступны следующие параметры:

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

### 15.12.2. Тип выхода "Генератор тревоги"

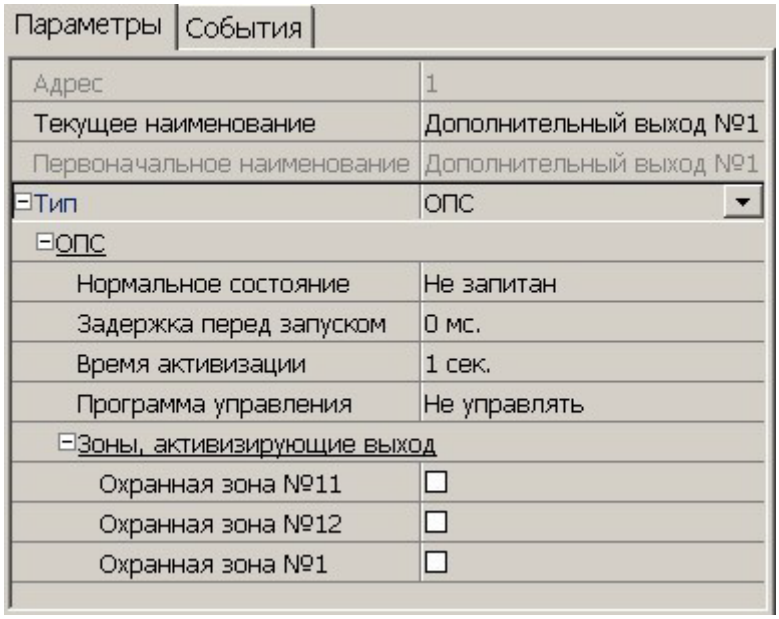



Доступны следующие параметры:

- **Нормализованное состояние** (*Не запитан / Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода. Для выходов №1 и № 2 нормализованное состояние: **Не запитан**.
- **Время активизации**. Время, на которое выход, при наличии активизирующего управляющего воздействия, меняет свое состояние из нормализированного на противоположное.

### 15.12.3. Тип выхода "ОПС"

Программа управления задает логику работы контроллера по управлению данным дополнительным выходом. Инициатором активизации выхода является изменение режима ОЗ, отмеченных как **Зоны, активизирующие выход**. После возникновения события, инициирующего активизацию выхода, он активизируется. В зависимости от параметра **Программа управления** выход может быть *запитан* / *не запитан* постоянно (пока ресурс панели находится в текущем режиме), либо изменять свое физическое состояние (мигать) из 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:

- **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»).

### 15.12.4. Программы управления выходом "ОПС"

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

- **Включить при тревоге**. В случае перехода хотя бы одной из ОЗ в режим *«ТРЕВОГА»* выход будет активизирован на **Время активизации**.
- **Мигать при тревоге**. В случае перехода хотя бы одной из ОЗ в режим *«ТРЕВОГА»* выход будет активизироваться с частотой 1Гц.

- **Лампа 1**. Программа управления световым оповещателем тревожной ситуации. Для смены режима требуется, чтобы все ОЗ изменили свое состояние.
- **Лампа 2**. Программа управления световым оповещателем тревожной ситуации. Для смены режима требуется, чтобы хотя бы одна ОЗ изменила свое состояние.
- **ПЦН 1**. Программа для передачи тревожных извещений на пост центрального наблюдения (ПЦН). В случае перехода всех ОЗ в режим *«ОХРАНА»* выход будет активизирован. Передача тревожных извещений на ПЦН
- **ПЦН 2**. Программа для передачи тревожных извещений на пост центрального наблюдения (ПЦН). В случае перехода всех ОЗ в режим *«ОХРАНА»* или в режим *«СНЯТА»* выход будет активизирован.
- **Сирена**. Программа управления звуковым оповещателей тревожной ситуации. В случае перехода хотя бы одной из ОЗ в режим *«ТРЕВОГА»* выход будет активизирован на **Время активизации**.
- **Вкл. перед взятием для ИУ в 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 | Авто-перевзятие | Охрана | Тревога | Внимание | Пожар | Неисправ-ность | |
| *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 |

| Название программы | Зоны | Режим зоны | | | | | | | | Неисправность ППКОП |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Снята | Взятие | Авто-перевзятие | Охрана | Тревога | Внимание | Пожар | Неисправ-ность | |
| *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 |

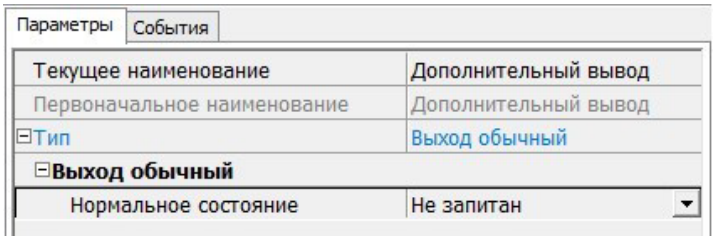
## 15.13. Дополнительный вывод

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

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

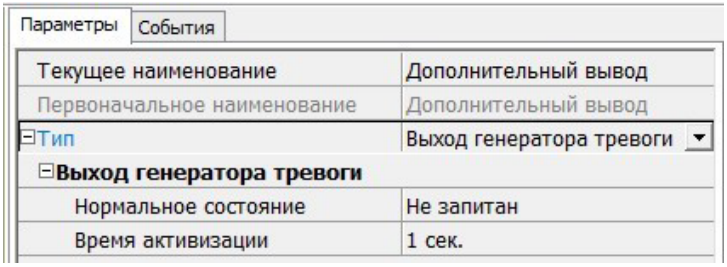
### 15.13.1. Тип вывода "Выход обычный"

В окне доступны следующие параметры:




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

### 15.13.2. Тип вывода "Выход генератора тревоги"



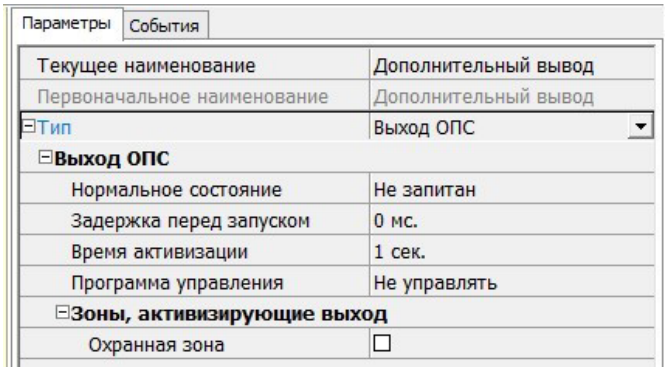

В окне доступны следующие параметры:

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

### 15.13.3. Тип вывода "Выход ОПС"

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

В окне доступны следующие параметры:



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

### 15.13.4. Тип вывода "Вход Fire Alarm"

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

### 15.13.5. Тип вывода "Синхронизирующий вход / выход"

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

## 15.14. Шлейф сигнализации

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

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

### 15.14.1. Тип шлейфа "Охранный" (ОШС)

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


- **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.

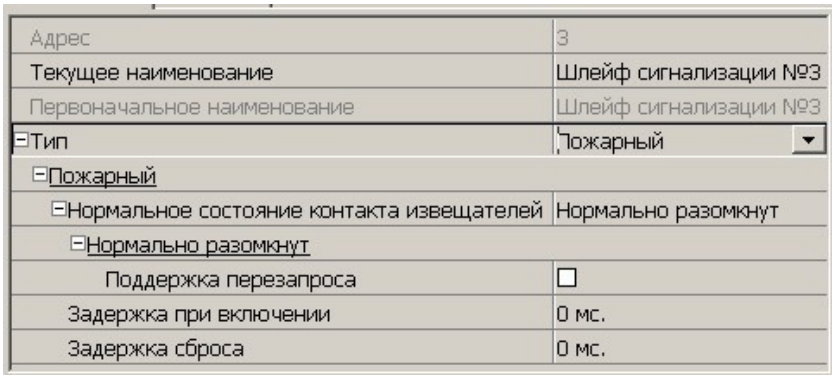
***Внимание!***

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.

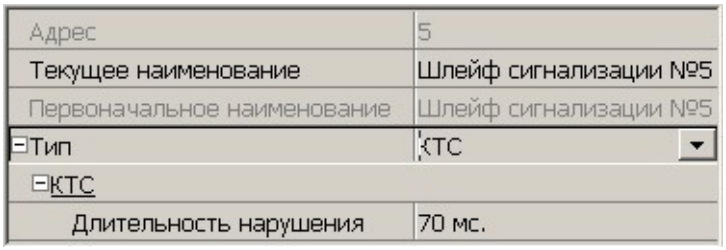
### 15.14.2. Тип шлейфа "Пожарный" (ПШС)

Доступны следующие параметры:




- **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).

### 15.14.3. Тип шлейфа "КТС"




Доступны следующие параметры:

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

## 15.15. Зона сигнализации

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

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

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

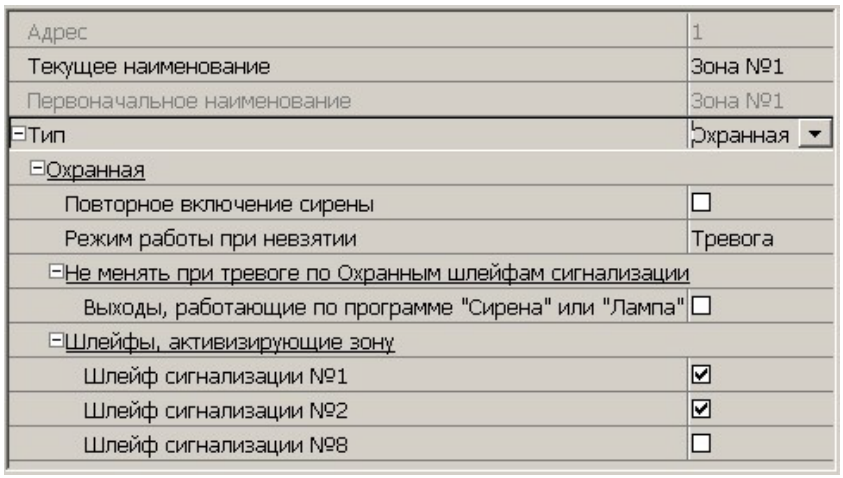
Для настройки зон сигнализации доступны следующие параметры:

- **Текущее наименование**. Поле ввода позволяет изменить название зоны.
- **Тип**. Раскрывающийся список позволяет выбрать тип зоны сигнализации:
  - **Нет** – зона не сконфигурирована.
  - **Охранная** – зона сконфигурирована как ОЗ.
  - **Пожарная** – (только для ППКОП) зона сконфигурирована как ПЗ.
  - **КТС** – (только для ППКОП) зона сконфигурирована для шлейфов КТС.

### 15.15.1. Тип зоны "Охранная" (ОЗ)

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

Доступны следующие параметры:




- **Включить ИУ в зону**. При установке параметра ИУ, подключенное к контроллеру будет включено в ОЗ. В РКД *«Охрана»* при регистрации события *«Взлом ИУ»* ОЗ перейдет в режим *«ТРЕВОГА»*.
- **Повторное включение сирены**. При установке параметра активизация дополнительного выхода, для которого установлен **Тип: ОПС** и выбрана программа управления *«Сирена»,* происходит при каждом переходе ИУ или одного из ШС в состояние *«нарушение»*, даже если ОЗ уже находится в режиме *«ТРЕВОГА»*.
- **Режим работы при невзятии**. Параметр указывает действие, которое будет происходить при невозможности взятия ОЗ на охрану. Доступны следующие значения:
  - **Тревога**. ОЗ будет переведена в режим *«ТРЕВОГА»*.
  - **Автоматическое перевзятие**. Производится повторная попытка взятия на охрану до тех пор, пока постановка на охрану не произойдет.
  - **Возврат в «Снята»**. ОЗ перейдет в режим *«СНЯТА»*.

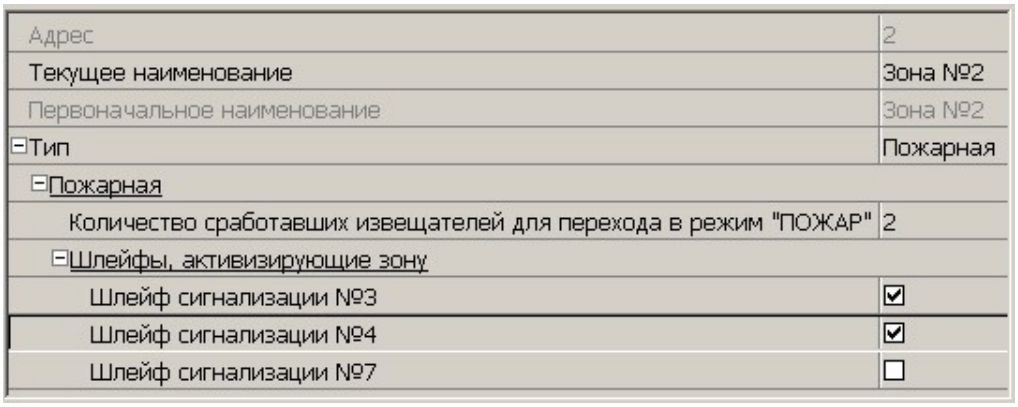
***Внимание!***

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

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

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

### 15.15.2. Тип зоны "Пожарная" (ПЗ)

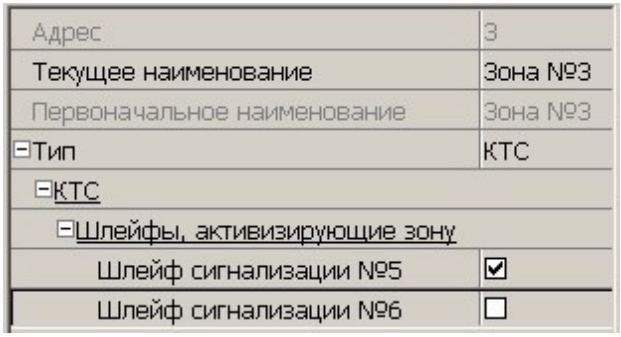



Доступны следующие параметры:

- **Количество сработавших извещателей для перехода в режим "ПОЖАР"** (*«1» / «2»*) – параметр, задающий минимальное количество извещателей, срабатывание которых переводит данную ПЗ в режим *«Пожар»*.
- **Переводить ИУ в режим «Открыто» (только для КБО)** – параметр, задающий условия перевода ИУ в РКД «*Открыто»*. Можно установить следующие значения:
  - **Никогда –** изменения режимов работы ПЗ не влияют на состояние ИУ.
  - **При переходе ПЗ в режим "ПОЖАР", но ОЗ не в режиме "Охрана**".
  - **При переходе ПЗ в режим "ПОЖАР", ОЗ в любом режиме**.
  - **При переходе ПЗ в режим "ПОЖАР" или "ВНИМАНИЕ", но ОЗ не в режиме "Охрана"**.
  - **При переходе ПЗ в режим "ПОЖАР" или "ВНИМАНИЕ", ОЗ в любом режиме**.
  - **При переходе ПЗ в режим "ПОЖАР" (ОЗ в любом режиме) или "ВНИМАНИЕ" (ОЗ не в режиме "Охрана")**.
- **Шлейфы, включенные в зону**. Параметр позволяет отметить флажками ПШС, которые будут входить в ПЗ и состояние которых будет отслеживаться контроллером при постановке ПЗ на контроль (переводе в режим *«Норма»*). В ОЗ могут входить ШС, для которых выбран **Тип: Пожарный**. При этом каждый ШС может входить только в одну ОЗ.

### 15.15.3. Тип зоны "КТС"

Доступны следующие параметры:



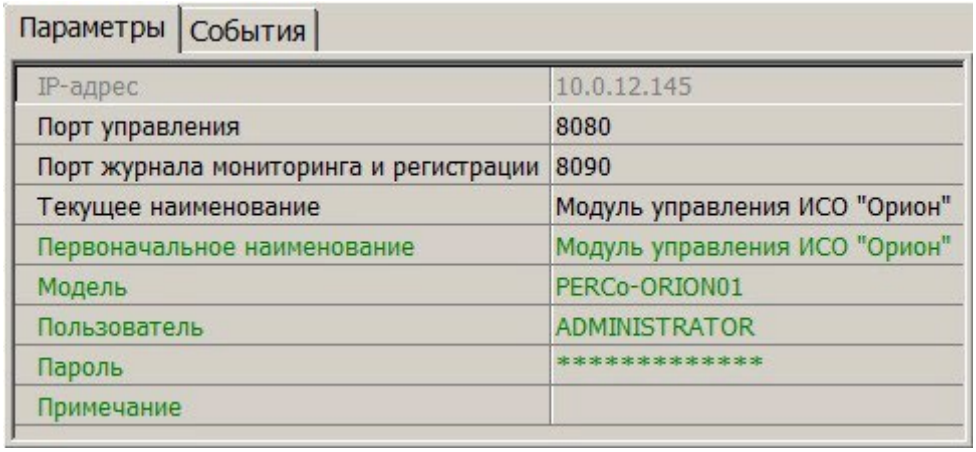
- **Шлейфы, активизирующие зону**. Параметр позволяет отметить флажками ШС, которые будут входить в зону КТС и состояние которых будет отслеживаться контроллером при переводе зоны КТС в режим *«Охрана»*. В ОЗ могут входить ШС, для которых выбран **Тип: КТС**. При этом каждый ШС может входить только в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

## 15.16. Приборы ИСО "Орион"

Для приборов ИСО «Орион» доступны следующие общие параметры:

- **Текущее наименование** – название прибора, которое может быть изменено пользователем.
- **Первоначальное наименование** – наименование прибора в системе по умолчанию.
- **Модель** – модель прибора.
- **Примечание:** – дополнительная информация о приборе, которая может быть добавлена пользователем.

**Модуль управления ИСО "Орион"**




В окне доступны следующие параметры:

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

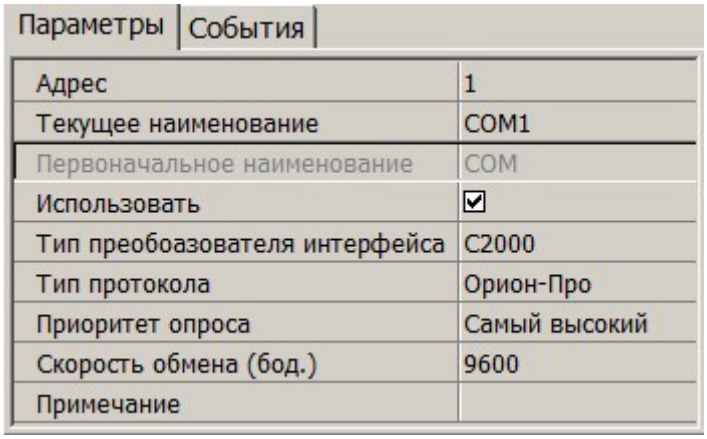
***Примечание:***

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

- **Порт управления** (по умолчанию 8080) – номер IP–порта XML-RPC- сервера для обмена данными с сервером системы.
- **Порт журнала мониторинга и регистрации** (по умолчанию 8090) – номер IP-порта сервера системы для приема событий, регистрируемых приборами ИСО «Орион» от XML-RPC-сервера.
- **Пользователь** – имя пользователя для доступа к XML-RPC-серверу.
- **Пароль** – пароль для доступа к XML-RPC-серверу.

**COM1, COM2, ...**

В окне доступны следующие параметры:




- **Адрес** – номер COM-порта ПК, к которому физически подключено оборудование ИСО «Орион».
- **Использовать** – при снятии флажка будет остановлен обмен данными с устройствами ИСО «Орион», входящими в группу ресурсов.
- **Тип преобразователя интерфейса** – параметр позволяет указать тип преобразователя интерфейса, соответствующий установленному оборудованию:
  - **ПИ-ГР** – значение необходимо выбрать в случае, если пульт *С2000М* (*С2000*), работающий в режиме ПИ, подключен по COM-порту. В этом режиме ядро опроса будет посылать дополнительные команды управления приемом-передачей.
  - **С2000-ПИ** – значение необходимо выбрать в случае подключения оборудования ИСО «Орион» через *С2000* USB-конвертер.
  - **С2000** – значение необходимо выбрать в случае подключения через пульт *С2000М* (*С2000*) в режиме компьютер.

***Примечание:***

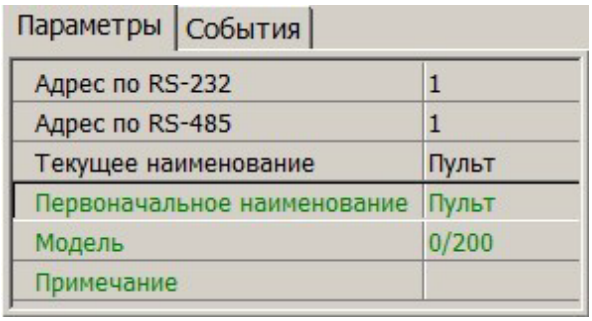
***Для параметра Тип преобразователя интерфейса:***

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

**Пульт**

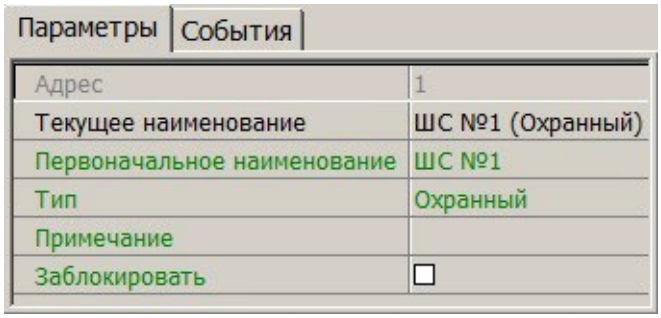
- **Тип протокола** (*Орион-Про* / *Орион*) – протокол обмена данными между устройствами ИСО «Орион» и XML-RPC-сервером по COM-порту.
- **Приоритет опроса** – параметр позволяет выбрать значение приоритета опроса модулем ИСО «Орион» оборудования, которое подключено к этому порту.
- **Скорость обмена (бод.)** (*9600* / *19200*) – скорость обмена данными между устройствами ИСО «Орион» и XML-RPC-сервером.

В окне доступны следующие параметры:




- **Адрес по RS-232** – адрес прибора при передаче данных по интерфейсу RS- 232.
- **Адрес по RS-485** – адрес прибора при передаче данных по интерфейсу RS- 485.

**ШС**




В окне доступны следующие параметры:

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

***Примечание:***

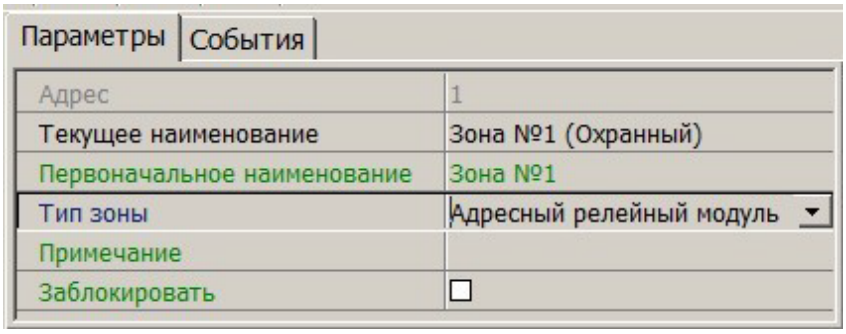
Описание режима работы ШС в зависимости от выбранного типа конфигурации и используемого прибора приводится в эксплуатационной документации конкретного прибора. Документация доступна на сайте производителя: www.bolid.ru.

- **Тип** – выпадающий список позволяет выбрать вариант конфигурации ШС в зависимости от типа подключенного оборудования:
  - **Охранный**;
  - **Пожарный**;
  - **Ademco (Приемник)**;
  - **Ademco (Радиоповторитель)**;
  - **Автоматическое управление второго рабочего насоса**;
  - **Автоматическое управление жокей-насоса**;
  - **Автоматическое управление первого рабочего насоса**;
  - **Автоматическое управление резервного насоса**;
  - **Агрегат 1**;
  - **Агрегат 2**;
  - **Агрегат 3**;
  - **Контроль состояния прибора**;
  - **Контроль ШС**;
  - **Масса**;
  - **Основной ввод АВР**;
  - **Основной резервуар**;
  - **Открытие электрозадвижки;**
  - **Питание второго рабочего насоса**;
  - **Питание жокей-насоса**;
  - **Питание первого рабочего насоса**;
  - **Питание резервного насоса**;
  - **Питание электрозадвижки**;
  - **Агрегат 4**;
  - **Адресно-аналоговый дымовой**;
  - **Адресно-аналоговый тепловой**;
  - **Влагоизмерительный**;
  - **Входной**;
  - **Выход Р1**;

- **Выход Р2**;
- **Выход Р3**;
- **Выход Р4**;
- **Выходное напряжение**;
- **Выходной ток**;
- **Давление**;
- **Давление в системе**;
- **ДД запуска**;
- **Дистанционный пуск**;
- **Дистанционный пуск потока**;
- **Дренажный приямок**;
- **Дренчерная завеса**;
- **Закрытие электрозадвижки**;
- **Запуск второго рабочего насоса**;
- **Запуск жокей-насоса**;
- **Запуск первого рабочего насоса**;
- **Запуск резервного насоса**;
- **Зоны УОП**;
- **Источник 26 В**;
- **Источник ОП**;
- **Источник питания 27 В**;
- **Источник РП**;
- **Контроль дистанционного запуска РО (речевого оповещения)**;
- **Контроль ЗУ**;
- **Контроль источника ОП (220В)**;
- **Контроль источника РП (АКБ)**;
- **Контроль неисправности АУП («М\Д»)**;
- **Пожарный адресно- пороговый**;
- **Проверка 220В**;
- **Проверка АКБ**;
- **Проверка ЗУ**;
- **Программируемый технологический**;
- **Режим автоматического запуска**;
- **Режим запуска**;
- **Режим прибора**;
- **Резервный ввод АВР**;
- **Резервный резервуар**;
- **Ручной пуск**;
- **Ручной пуск (АСПТ)**;
- **Ручной пуск (Поток)**;
- **Ручной пуск (Рупор)**;
- **СДУ**;
- **Состояние КЦ1**;
- **Состояние КЦ10**;
- **Состояние КЦ11**;
- **Состояние КЦ12**;
- **Состояние КЦ13**;
- **Состояние КЦ14**;
- **Состояние КЦ15**;
- **Состояние КЦ16**;
- **Состояние КЦ17**;
- **Состояние КЦ18**;
- **Состояние КЦ2**;
- **Состояние КЦ3**;
- **Состояние КЦ4**;
- **Состояние КЦ5**;
- **Состояние КЦ6**;
- **Состояние КЦ7**;
- **Состояние КЦ8**;
- **Состояние КЦ9**;
- **Состояние устройства**;
- **Технологический**;
- **Тревожная кнопка**;
- **Цепь ДС дверей**.

**Зона**

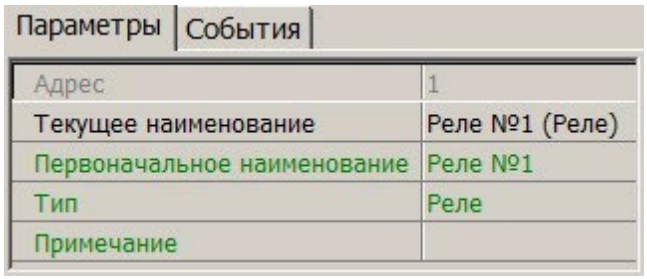
Ресурс доступен для категории приборов **Адресно-аналоговые подсистемы (КДЛ).** В окне доступны следующие параметры:




- **Тип зоны** – раскрывающийся список позволяет выбрать тип зоны:
  - **Шлейф** (варианты конфигурации ШС указаны выше);
  - **Адресный релейный модуль**.

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

**Реле**




В окне доступны следующие параметры:

***Примечание:***

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

- **Тип** – выпадающий список позволяет выбрать вариант конфигурации реле в зависимости от типа подключенного оборудования:
  - **Адресный релейный модуль**;
  - **Выход КПБ (АСПТ)**;
  - **ЗО (Сирена)**;
  - **Контролируемый выход**;
  - **Пуск 1**;
  - **Пуск 2**;
  - **Пуск 3**;
  - **Пуск 4**;
  - **Пусковая цепь**;
  - **Реле**;
  - **Речевое оповещение**;
  - **СО1 (УХОДИ)**;
  - **СО2 (НЕ ВХОДИ)**;
  - **СО3 (Автоматика отключена)**.

## 15.17. Интеграция с контроллерами "Suprema"

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

***Внимание!***

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

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

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

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

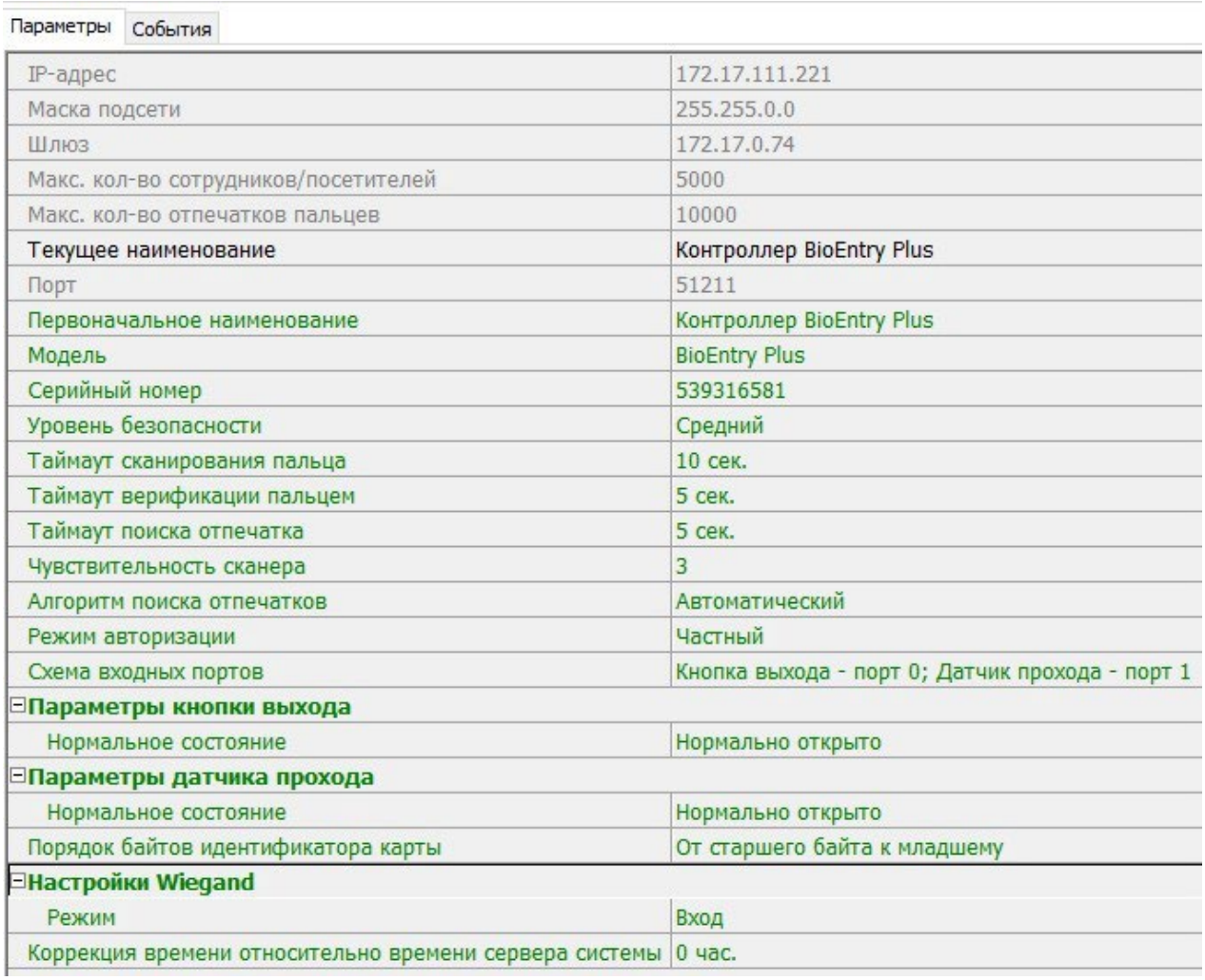
- **Контроллер BioEntry Plus**;
- **Контроллер BioEntry W2**;
- **Замок**;
- **Биометрический считыватель**.

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

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

### 15.17.1. Контроллер BioEntry Plus

В окне доступны следующие параметры:


Параметры | События

| | |
|---|---|
| IP-адрес | 172.17.111.221 |
| Маска подсети | 255.255.0.0 |
| Шлюз | 172.17.0.74 |
| Макс. кол-во сотрудников/посетителей | 5000 |
| Макс. кол-во отпечатков пальцев | 10000 |
| Текущее наименование | Контроллер BioEntry Plus |
| Порт | 51211 |
| Первоначальное наименование | Контроллер BioEntry Plus |
| Модель | BioEntry Plus |
| Серийный номер | 539316581 |
| Уровень безопасности | Средний |
| Таймаут сканирования пальца | 10 сек. |
| Таймаут верификации пальцем | 5 сек. |
| Таймаут поиска отпечатка | 5 сек. |
| Чувствительность сканера | 3 |
| Алгоритм поиска отпечатков | Автоматический |
| Режим авторизации | Частный |
| Схема входных портов | Кнопка выхода - порт 0; Датчик прохода - порт 1 |
| **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, загрязненности сканируемой поверхности пальцев и т.д. В этом случае для успешной верификации потребуется повторно пройти процедуру сканирования отпечатков.
- **Таймаут сканирования пальца** – время, которое выделяется системой на поднесение одного пальца при вводе отпечатков. Параметр может быть задан в интервале от 3 до 20 секунд.
- **Таймаут верификации пальцем** (используется в режиме доступа **карта и палец**) – интервал времени, в течение которого ожидается поднесение пальца для сканирования отпечатков, при этом отсчет времени интервала начинается после того, как была предъявлена считывателю карта доступа*.* Параметр может быть задан в интервале от 1 до 20 секунд.
- **Таймаут поиска отпечатков** – время поиска отпечатка в памяти контроллера. Если за отведенное время отпечаток не будет найден, то аутентификация будет отклонена. Параметр может быть задан в интервале от 1 до 20 секунд.
- **Чувствительность сканера** – определяет чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности обеспечивается высокое качество и скорость сканирования, при низком заданном уровне чувствительности – уменьшается влияние факторов внешней среды (температуры и влажности воздуха, освещенности помещения, чистоты сканируемой поверхности подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию. Понижение заданного уровня чувствительности сканера осуществляется при необходимости в зависимости от условий эксплуатации. Параметр может быть задан в интервале от 1 до 7, где значение 1 – соответствует самой низкой чувствительности, а значение 7 – самой высокой.

- **Алгоритм поиска отпечатков** – позволяет выбрать алгоритм поиска отпечатков пальца. Выбор алгоритма влияет на скорость верификации по отпечатку пальца:
  - **Автоматический (рекомендован производителем)**;
  - **Нормальный**;
  - **Быстрый**;
  - **Очень быстрый**.

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

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

- **Режим доступа** – определяет режим доступа при общем режиме авторизации (отображается только если режим авторизации выставлен как **«Общий»**):
  - **Палец** – для верификации требуется пройти процедуру сканирования отпечатка пальца;
  - **Карта** – для верификации требуется предъявить считывателю карту доступа;
  - **Карта и палец** – для верификации требуется предъявить считывателю карту доступа, после чего пройти процедуру сканирования отпечатка пальца;
  - **Карта или палец** – для верификации требуется предъявить считывателю карту доступа или пройти процедуру сканирования отпечатка пальца.

***Примечание:***

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

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

***Примечание:***

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

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

***Примечание:***

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

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

***Примечание:***

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

- **Настройки Wiegand (Режим)** – позволяет задать режим работы интерфейса *Wiegand* контроллера ***Suprema***:
  – **Вход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как вход. В этом режиме контроллер ***Suprema*** работает как обычный контроллер доступа, ожидая поступления данных по интерфейсу *Wiegand*;
  – **Выход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как выход. В этом режиме контроллер ***Suprema*** работает совместно с контроллером ***PERCo*** в составе СКУД (может производить аутентификацию и управление подключенным по интерфейсу *Wiegand* оборудованием (замком и т.д.)).
- **Использовать аутентификацию** – при установке флажка контроллером ***Suprema*** при предъявлении карты / пальца будет производиться предварительная аутентификация. В случае успешной предварительной аутентификации данные будут переданы в контроллер ***PERCo*** для повторной аутентификации (загорится зеленая индикация). В случае ошибки предварительной аутентификации данные в контроллер ***PERCo*** передаваться не будут – необходимо провести повторную успешную аутентификацию. Если флажок не выставлен, то процедура аутентификации будет 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.

### 15.17.2. Контроллер BioEntry W2/P2

В окне доступны следующие параметры:

Параметры | События

| | |
|---|---|
| IP-адрес | 172.17.100.230 |
| Маска подсети | 255.255.0.0 |
| Шлюз | 172.17.0.50 |
| Макс. кол-во сотрудников/посетителей | 100000 |
| Макс. кол-во отпечатков пальцев | 200000 |
| Текущее наименование | Контроллер BioEntry W2 |
| Порт | 51211 |
| Первоначальное наименование | Контроллер BioEntry W2 |
| Модель | BioEntry W2 |
| Серийный номер | 544108028 |
| Уровень безопасности | Средний |
| Таймаут сканирования пальца | 10 сек. |
| Таймаут верификации пальцем | 5 сек. |
| Таймаут поиска отпечатка | 5 сек. |
| Чувствительность сканера | 3 |
| Алгоритм поиска отпечатков | Автоматический |
| Режим датчика | Включен всегда |
| Режим авторизации | Частный |
| Схема входных портов | Кнопка выхода - порт 0; Датчик прохода - порт 1 |
| **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, загрязненности сканируемой поверхности пальцев и т.д. В этом случае для успешной верификации потребуется повторно пройти процедуру сканирования отпечатков.
- **Таймаут сканирования пальца** – время, которое выделяется системой на поднесение одного пальца при вводе отпечатков. Параметр может быть задан в интервале от 3 до 20 секунд.
- **Таймаут верификации пальцем** (используется в режиме доступа ***карта и палец***) – интервал времени, в течение которого ожидается поднесение пальца для сканирования отпечатков, при этом отсчет времени интервала начинается после того, как была предъявлена считывателю карта доступа***.*** Параметр может быть задан в интервале от 1 до 20 секунд.
- **Таймаут поиска отпечатков** – время поиска отпечатка в памяти контроллера. Если за отведенное время отпечаток не будет найден, то аутентификация будет отклонена. Параметр может быть задан в интервале от 1 до 20 секунд.
- **Чувствительность сканера** – определяет чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности обеспечивается высокое качество и скорость сканирования, при низком заданном уровне чувствительности – уменьшается влияние факторов внешней среды (температуры и влажности воздуха, освещенности помещения, чистоты сканируемой поверхности подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию. Понижение заданного уровня чувствительности сканера осуществляется при необходимости в зависимости от условий эксплуатации. Параметр может быть задан в интервале от 1 до 7, где значение "1" – соответствует самой низкой чувствительности, а значение "7" – самой высокой.
- **Алгоритм поиска отпечатков** – выбор алгоритма влияет на скорость верификации по отпечатку пальца:
  – **Автоматический (рекомендован производителем**);
  – **Нормальный**;
  – **Быстрый**;
  – **Очень быстрый**.

  Выбор **алгоритма поиска отпечатков** определяет тот объем памяти контроллера, который будет выделяться для поиска совпадения отсканированного отпечатка с отпечатком в базе данных. Если в базе данных контроллера большое количество разных отпечатков, то для быстрого поиска совпадений потребуется больший объем памяти контроллера. Однако, выделение большего объема памяти контроллера для поиска совпадений может

замедлить остальные параллельно происходящие процессы поиска совпадений, например, если к контроллеру подключены несколько считывателей, на которых в этот же момент времени происходит верификация по отпечаткам пальцев.

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

***Примечание:***

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

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

***Примечание:***

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

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

***Примечание:***

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

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

***Примечание:***

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

- **Настройки Wiegand (Режим)** – позволяет задать режим работы интерфейса *Wiegand* контроллера ***Suprema***:
  - **Вход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как вход. В этом режиме контроллер ***Suprema*** работает как обычный контроллер доступа, ожидая поступления данных по интерфейсу *Wiegand*;
  - **Выход** – интерфейс *Wiegand* контроллера ***Suprema*** настроен как выход. В этом режиме контроллер ***Suprema*** работает совместно с контроллером ***PERCo*** в составе СКУД (может производить аутентификацию и управление подключенным по интерфейсу *Wiegand* оборудованием (замком и т.д.)).
- **Использовать аутентификацию** – при установке флажка контроллером ***Suprema*** при предъявлении карты / пальца будет производиться предварительная аутентификация. В случае успешной предварительной аутентификации данные будут переданы в контроллер ***PERCo*** для повторной аутентификации (загорится зеленая индикация). В случае ошибки предварительной аутентификации данные в контроллер ***PERCo*** передаваться не будут – необходимо провести повторную успешную аутентификацию. Если флажок не выставлен, то процедура аутентификации будет 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**.

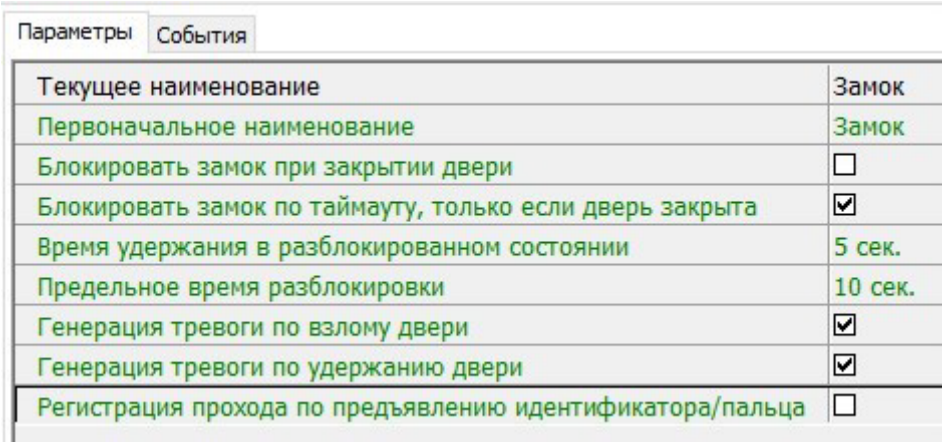
***Примечание:***

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.

### 15.17.3. Замок

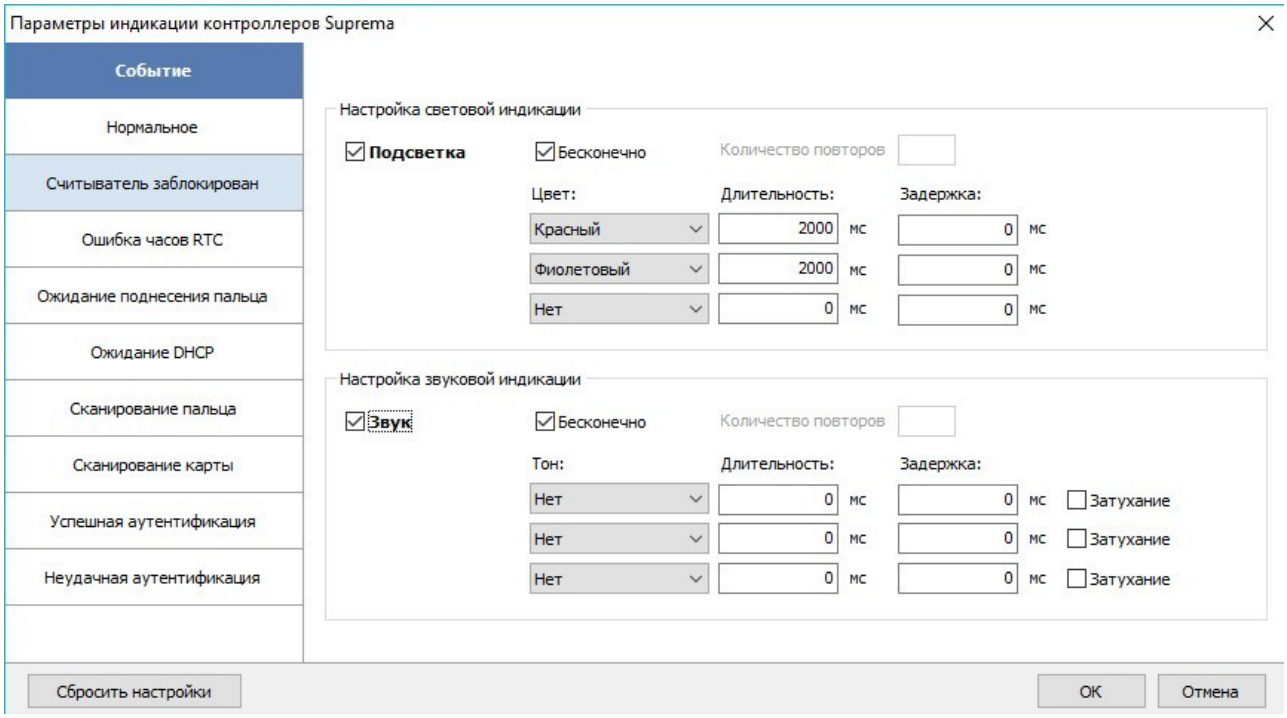
В окне доступны следующие параметры:




- **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.

### 15.17.4. Параметры индикации контроллеров "Suprema"

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




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

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

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

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

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

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

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

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

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

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

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

## 15.18. Биометрические контроллеры PERCo

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

Для настройки параметров работы в СКУД доступны следующие устройства:

- **Контроллер CT/L14, CT13**;
- **Контроллер CL15**;
- **Контроллер регистрации CR11**.

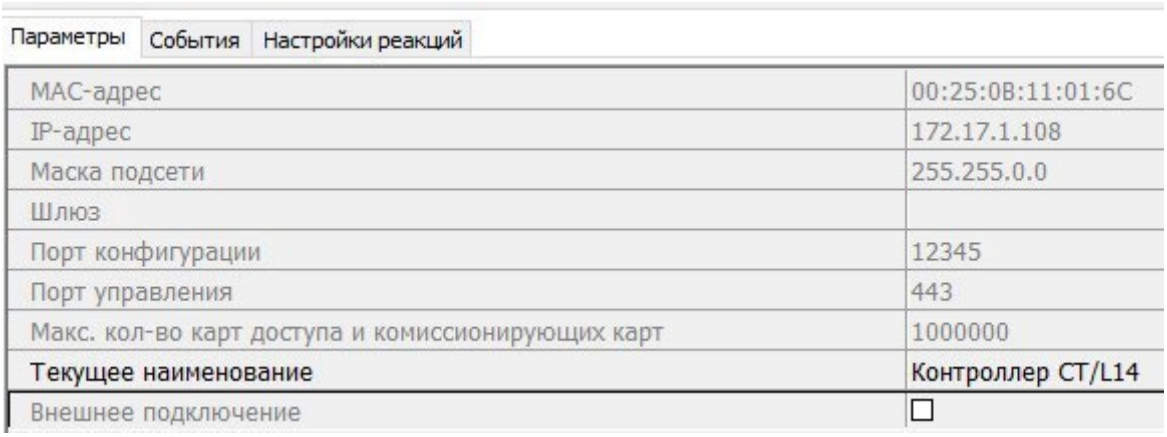
Для настройки ресурсов доступны следующие параметры:

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

### 15.18.1. Контроллер CT/L14, CT13

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:

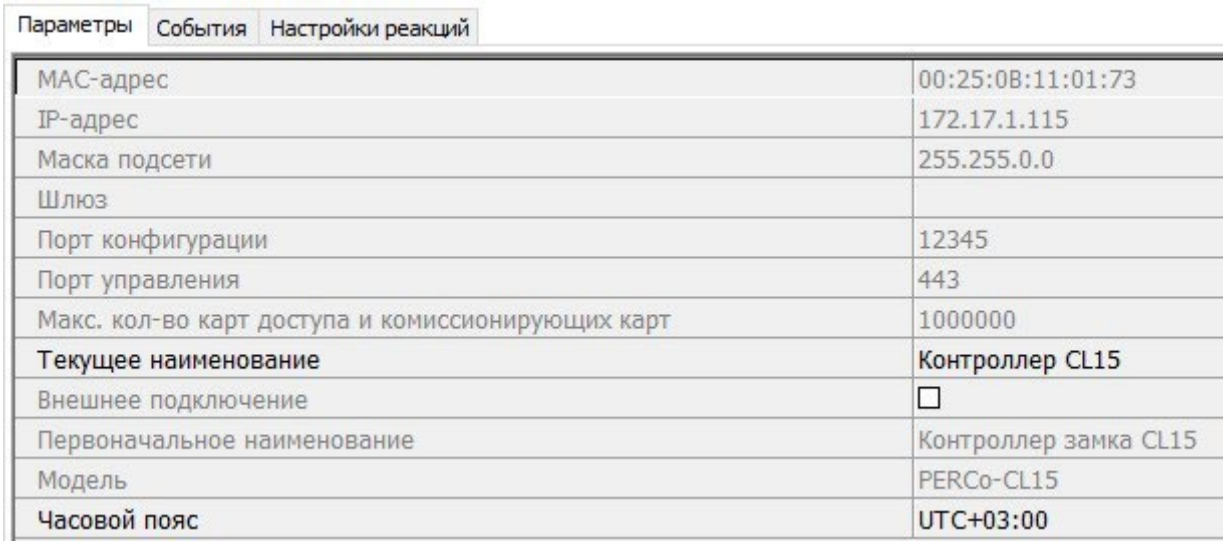



- **MAC-адрес**.
- **IP-адрес**.
- **Маска подсети**.
- **Шлюз**.
- **Порт конфигурации**.
- **Порт управления**.
- **Макс. кол-во карт доступа и комиссионирующих карт**.
- **Внешнее подключение**. Отображение флажка у параметра означает, что контроллер был добавлен по внешнему подключению (контроллер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

## 15.18.2. Контроллер CL15

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

Доступны следующие параметры:




- **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.

### 15.18.3. Контроллер регистрации CR11

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

Доступны следующие параметры:

| | |
|---|---|
| MAC-адрес | 02:97:02:17:01:6A |
| IP-адрес | 172.17.1.106 |
| Маска подсети | 255.255.0.0 |
| Шлюз | |
| Порт конфигурации | 12345 |
| Порт управления | 443 |
| Макс. кол-во карт доступа и 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.

### 15.18.4. ИУ

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

Доступны следующие параметры:

Параметры | События

| | |
|---|---|
| Адрес | 1 |
| Текущее наименование | Универсальное ИУ 1 |
| Первоначальное наименование | Односторонний замок |
| Алгоритм | Турникет |
| Регистрация прохода по предъявлению идентификатора | ☐ |
| Время удержания в разблокируемом состоянии (время анализа идентификатора) | 550 мс. |
| Предельное время разблокировки | 50 мс. |
| Режим работы выхода управления ИУ | Потенциальный |
| Нормализация выхода ИУ | После "Закрытия" |
| Реакция на FireAlarm в режиме работы "Охрана" | Разблокировать ИУ |
| Время идентификации постановки/снятия РКД "Охрана" | 10 сек. |
| Внутренняя защита от передачи идентификаторов (Local Antipass) | ☑ |
| **⊟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**.

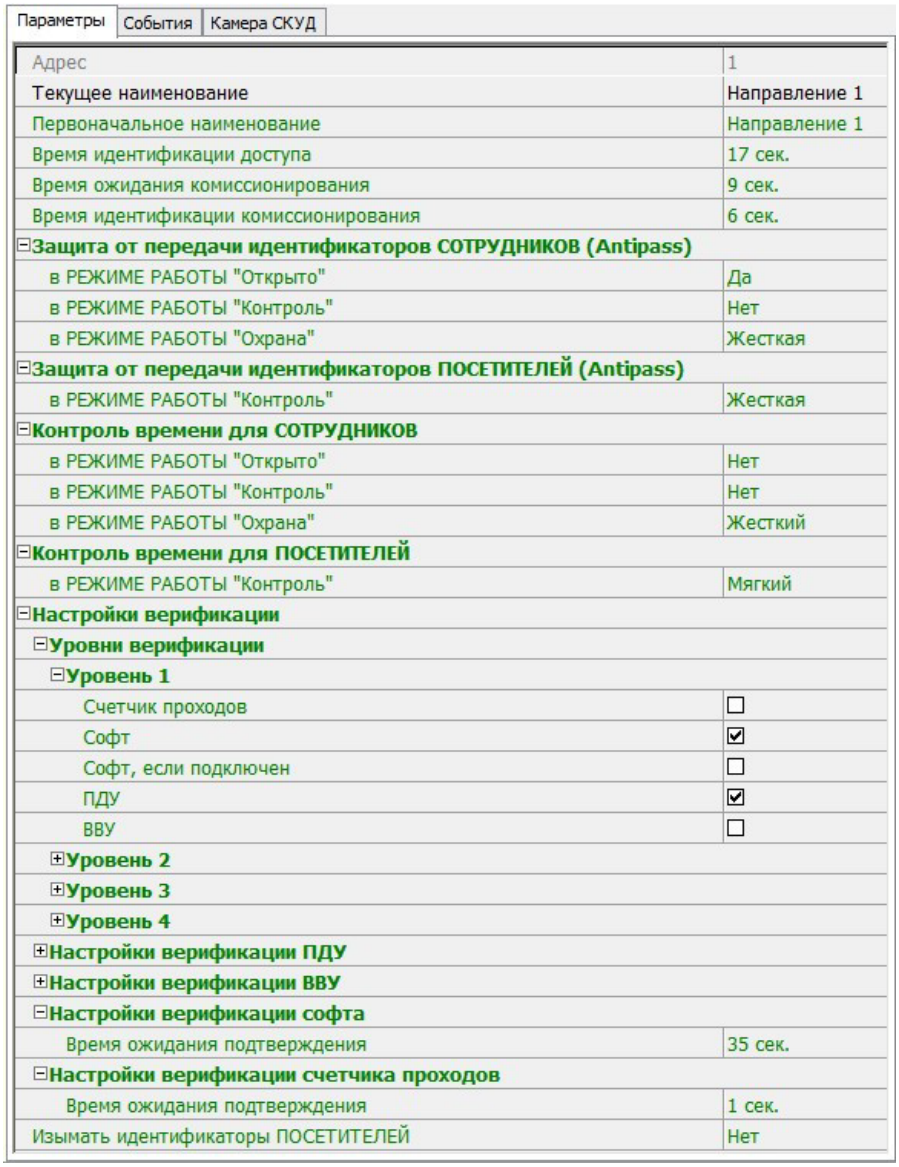
- **Регистрация прохода по предъявлению идентификатора** – если флажок установлен, то событие совершения прохода регистрируется сразу после поднесения карты доступа / сканирования пальца без ожидания сигнала от датчика прохода. Если флажок не установлен, то событие совершения прохода регистрируется после 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 ИУ**;
  – **Блокировать ИУ**.
- **Время идентификации постановки / снятия РКД "Охрана"**
- **Внутренняя защита от передачи идентификаторов (Local Antipass)** – при установленном параметре контроллер отслеживает случаи повторного предъявления одной и той же карты доступа / биоидентификатора к тому же считывателю.
- **Генерация тревоги при предъявлении идентификатора** – параметр позволяет указать события, связанные с предъявлением карт доступа, при регистрации которых произойдет генерация тревоги:
  – **если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН**;
  – **если ИДЕНТИФИКАТОР ЗАПРЕЩЕН**;
  – **если ИСТЕК СРОК ДЕЙСТВИЯ**;
  – **если НАРУШЕНО ВРЕМЯ**;
  – **если НАРУШЕНА ЗОНАЛЬНОСТЬ**;
  – **если НАРУШЕН РЕЖИМ РАБОТЫ**;
  – **если НАРУШЕНО КОМИССИОНИРОВАНИЕ**.

- **Генерация тревоги при несанкционированной разблокировке ИУ** – параметр позволяет для РКД *«Контроль»* и «Закрыто» указать, будет ли генерироваться тревога в случае механической разблокировки ИУ при помощи ключа, то есть без команды от контроллера:
  – **в РЕЖИМЕ РАБОТЫ "Контроль"**;
  – **в РЕЖИМЕ РАБОТЫ "Закрыто"**.
- **Генерация тревоги по недопустимо долгому открытию ИУ** – параметр позволяет для РКД «*Контроль*» указать, будет ли генерироваться тревога в случае, если после открытия ИУ оно не было нормализовано в течение **Предельного времени разблокировки**, заданного в параметрах этого ИУ.
- **Генерация тревоги при предъявлении "тревожного" пальца** – параметр позволяет для РКД «*Контроль*» указать, будет ли генерироваться тревога в случае, если был считан "тревожный" отпечаток пальца.

### 15.18.5. Направление

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

Доступны следующие параметры:



- **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!***

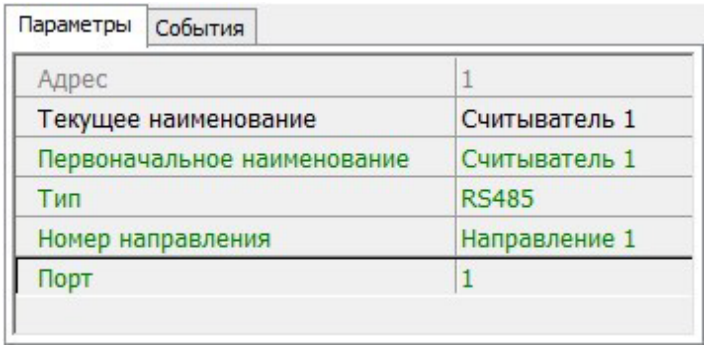
Для **ПДУ** по истечении **времени ожидания подтверждения** автоматически будет генерироваться событие **Запрет прохода от ПДУ**.

- **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.

### 15.18.6. Считыватель

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

Доступны следующие параметры:




- **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.

### 15.18.7. Вход

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

Доступны следующие параметры:


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

- **Кнопка ПДУ / Кнопка выхода**.
- **Кнопка ПДУ / (СТОП**).
- **Сигнал прохода**.
- **Вход FireAlarm**. Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ *Fire Alarm*.
- **Нет.** К данному входу не подключено никакое внешнее оборудование.
- **Подтверждение от ВВУ**. Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае разрешения прохода.
- **Вход запрета от ВВУ**. Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае запрета прохода.
- **Вход сброса тревоги**.

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

### 15.18.8. Выход

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

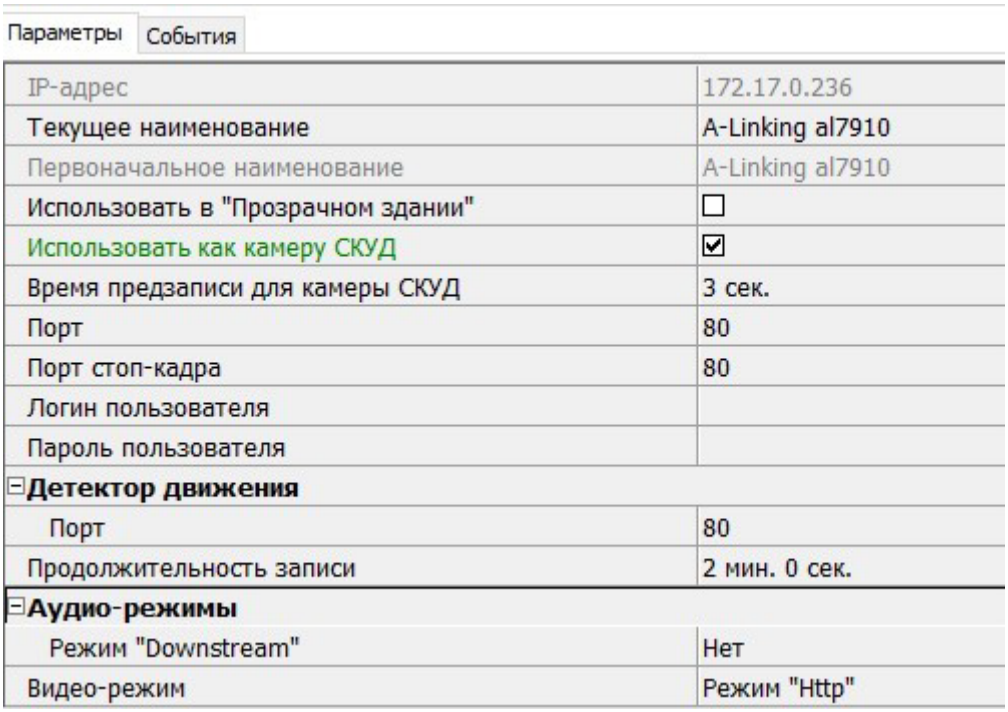
Доступны следующие параметры:


- **Тип**. Выпадающий список позволяет выбрать один из следующих типов:
  - **Обычный**. К данному выходу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
  - **Выход управления ИУ.** Предназначен для подключения к ИУ для передачи управляющих сигналов *Блокировать* / *Разблокировать*.
  - **Выход индикации ПДУ**. Предназначен для подключения к ПДУ для передачи управляющих сигналов смены индикации.
- **Нормальное состояние** (*Не запитан / Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода.
- **Контроллер**.

- **Направление**. Параметр задает направление ИУ, к которому привязывается считыватель.
- **Антидребезг.** Значение должно быть от 0 до 950 миллисекунд с шагом 50; от 1 секунды до 4 минут; бесконечно.

## 15.19. 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:




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)**.

## 15.20. 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:


Доступны следующие параметры:

- **Текущее название** – поле для ввода названия видеоподсистемы.
- **Частота кадров при записи для «Прозрачного здания»** – параметр предназначен для камер видеоподсистемы, для которых установлен флажок у параметра **Использовать в "Прозрачном здании"**. Параметр устанавливает частоту записи кадров с камеры. По умолчанию 60 кадров в минуту.
- **Частота кадров при записи для «Камер СКУД»** – параметр предназначен для камер видеоподсистемы, используемых в качестве камер СКУД, то есть для которых установлен флажок у параметра **Использовать как камеру СКУД**. Параметр устанавливает частоту записи кадров с камеры. По умолчанию 240 кадров в минуту.

# 16. Состав видеоподсистемы

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

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

***Внимание!***

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

# 17. Конфигурирование видеоподсистемы

***Внимание!***

Перед проведением конфигурации:

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

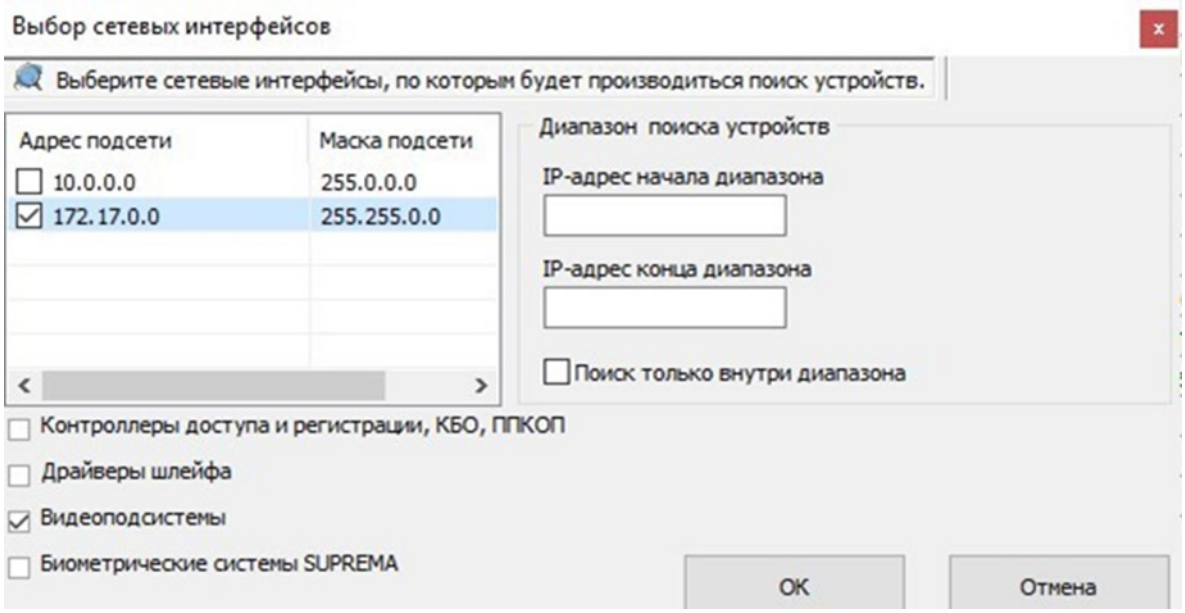
При настройке видеоподсистемы придерживайтесь следующей последовательности действий:

1. Убедитесь, что установлен модуль сетевого ПО: **Сервер видеоподсистемы** и запущена соответствующая служба.
2. Запустите ***«Центр управления видеоподсистемой»***, перейдите на вкладку **Видеоархив** и создайте хотя бы один файл видеоархива.
3. Запустите ***«Консоль управления»*** и перейдите в раздел ***«Конфигуратор»*** и произведите поиск необходимого устройства.
4. Произведите настройку параметров видеоподсистемы и камер. Для этого выделите устройство в рабочей области раздела и на вкладке **Параметры** панели настройки произведите необходимые изменения.
5. Для добавления найденных устройств в конфигурацию системы выделите в рабочей области раздела видеоподсистему и нажмите кнопку **Передать параметры** на панели инструментов раздела. В устройства будут переданы заданные параметры конфигурации. В случае успешной передачи параметров в устройства значки в списке объектов заменятся на значки и, соответственно, для видеоподсистемы и камер.
6. При необходимости произведите настройку подсистемы ***«Камеры СКУД»***.

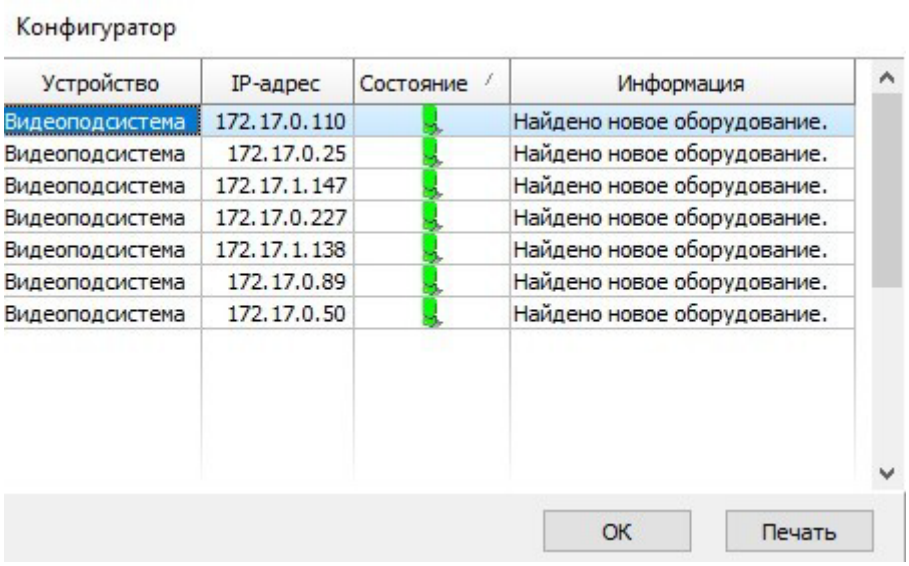
## 17.1. Поиск устройств видеоподсистемы

**Автоматический поиск устройств видеоподсистемы**

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



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



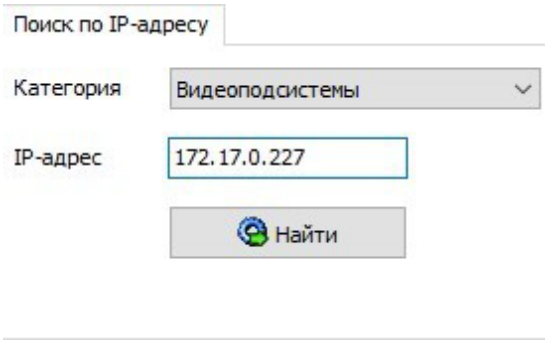

В открывшемся окне нажмите кнопку **ОК**. Все найденные устройства будут добавлены в рабочую область раздела и отмечены значками .

3. Если какое-либо из найденных устройств необходимо исключить из конфигурации, то выделите его в рабочей области и нажмите на панели инструментов раздела кнопку **Исключить из конфигурации**. Выделенное устройство будет исключено из конфигурации и отмечено значком .

**Поиск видеоподсистемы по IP-адресу**

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

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




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

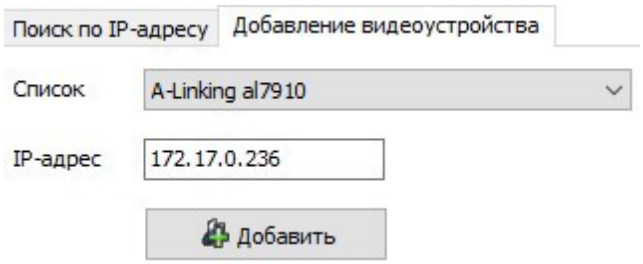
**Поиск камеры поддерживающих стандарт ONVIF**

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

**Поиск камеры по IP-адресу**

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

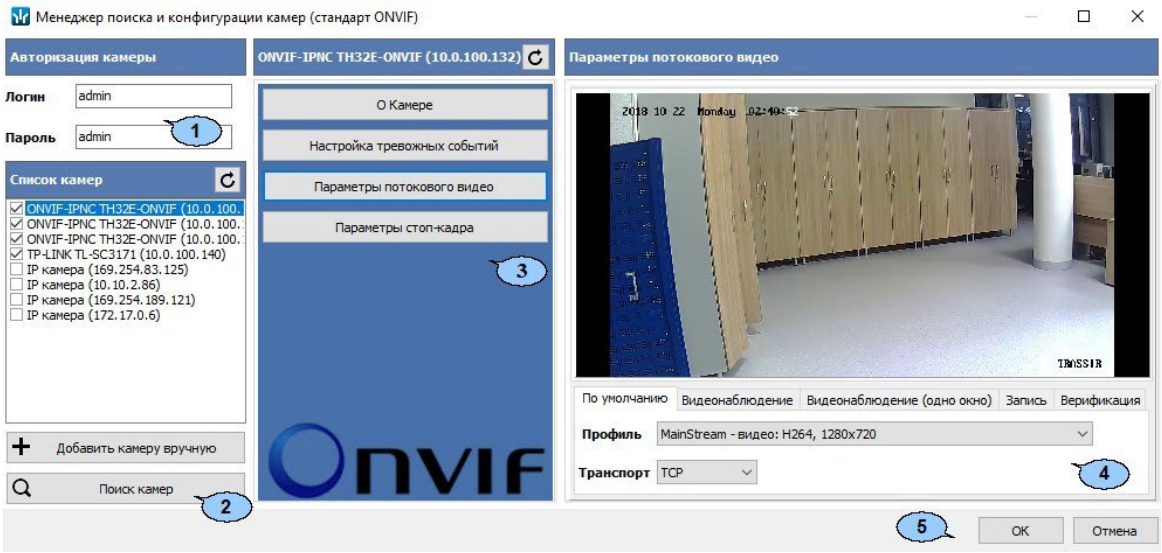
1. В рабочей области раздела выделите видеоподсистему, в которую необходимо добавить камеру и нажмите кнопку **Добавить новое устройство**.
2. На панели **Поиск по IP-адресу** в выпадающем списке **Категория** выберите пункт: **Камеры и видеосервера видеоподсистемы**. Убедитесь, что в поле **IP-адрес** указан IP-адрес ПК, на котором установлен модуль **Сервер видеоподсистемы**. На панели станет доступна вкладка **Добавление видеоустройства**.
3. Перейдите на вкладку **Добавление видеоустройства**:




4. В выпадающем списке **Список** выберите модель искомой видеокамеры, в поле **IP-адрес** введите ее IP-адрес. Нажмите ставшую при этом активной кнопку **Добавить**.
5. По окончании поиска откроется окно **Конфигуратор**. В открывшемся окне нажмите кнопку **ОК**. Найденная камера будет добавлена в рабочую область раздела и отмечена значком .

# 18. Подключение камер, поддерживающих стандарт ONVIF

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

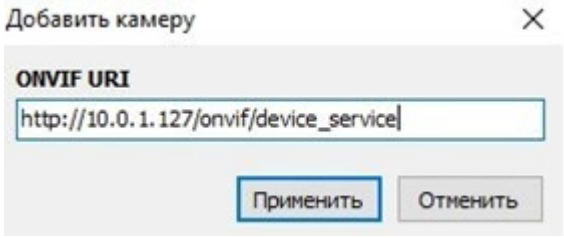



1. Панель **Авторизация камеры** содержит поля для ввода единых логина и пароля доступа к камерам.
2. Панель **Список камер** содержит список найденных камер.
   - – кнопка в заголовке панели позволяет произвести повторное подключение к найденным камерам.
   - **Добавить камеру вручную** – кнопка позволяет произвести поиск камеры по ее IP-адресу.
   - **Поиск камер** – кнопка позволяет заново произвести поиск камер.
3. Панель содержит следующие кнопки для выбора отображаемой в рабочей области окна информации о камере, выделенной на панели **Список камер.**
   - – кнопка в заголовке панели позволяет повторно подключиться к камере.
   - **О камере** – для отображения общей информации о камере.
   - **Настройка тревожных событий** – для выбора событий, передаваемых камерой, регистрация которых соответствует регистрации события *«Тревога»* в системе.
   - **Параметры потокового видео** – для настройки потокового видео с камеры. Доступны следующие инструменты:
     – Видеоокно для просмотра видеоизображения с камеры в режиме реального времени;
     – **Профиль** – выпадающий список для выбора алгоритма сжатия (видеокодека) и размера изображения потокового видео с камеры;
     – **Транспорт** – выпадающий список выбора протокола передачи потокового видео;
     – Для PTZ-камер, поддерживающих удаленное управление, доступны кнопки управления ориентацией и зумом камеры, а также поле для выбора направления камеры.
   - **Параметры стоп-кадра** – для настройки профиля стоп-кадр.
4. Рабочая область окна.
5. Кнопки **ОК** и **Отмена** позволяют закрыть окно. При нажатии кнопки **ОК** отмеченные камеры будут добавлены в конфигурацию подсистемы.

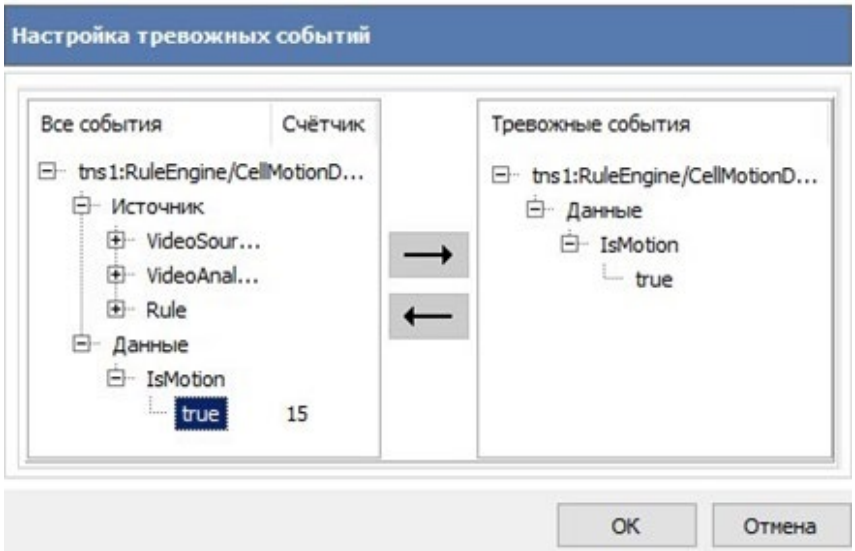
**Порядок поиска камер, поддерживающих стандарт ONVIF**

Для поиска камер, поддерживающих стандарт ONVIF:

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




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



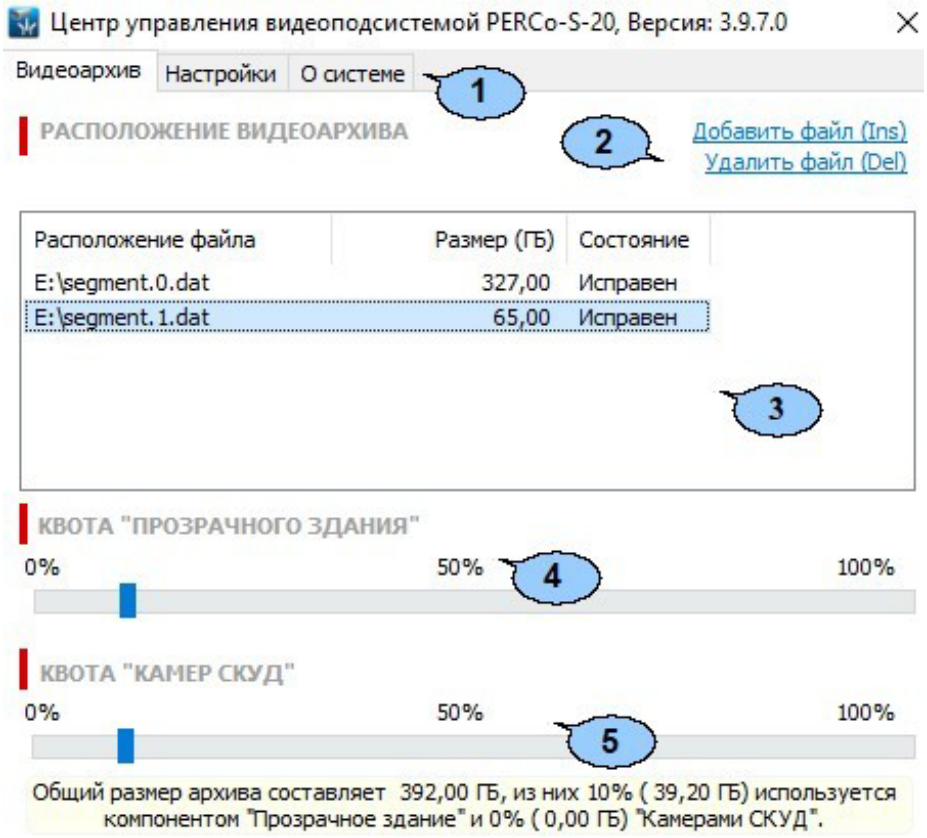
9. В левой части рабочей области отображается список событий, регистрируемых камерой. Наличие, перечень и описание событий зависит от модели камеры. Используя кнопу  добавьте необходимые события камеры в тревожные события. Для удаления события используйте кнопку  .
10. Для настройки параметров потокового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

# 19. «Центр управления видеоподсистемой»

## 19.1. Вкладка «Видеоархив»

### 19.1.1. Рабочее окно вкладки

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




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

***Примечание:***

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

3. Рабочая область вкладки содержит список созданных ранее файлов видеоархивов с указанием их расположения, размера и состояния.
4. Ползунок **Квота «Прозрачного здания»** предназначен для указания части файла видеоархива, которая будет зарезервирована для записи кадров с камер ***«Прозрачное здание»***.

5. Ползунок **Квота «Камер СКУД»** предназначен для указания части видеоархива, которая будет зарезервирована для записи видеоинформации с камеры СКУД.

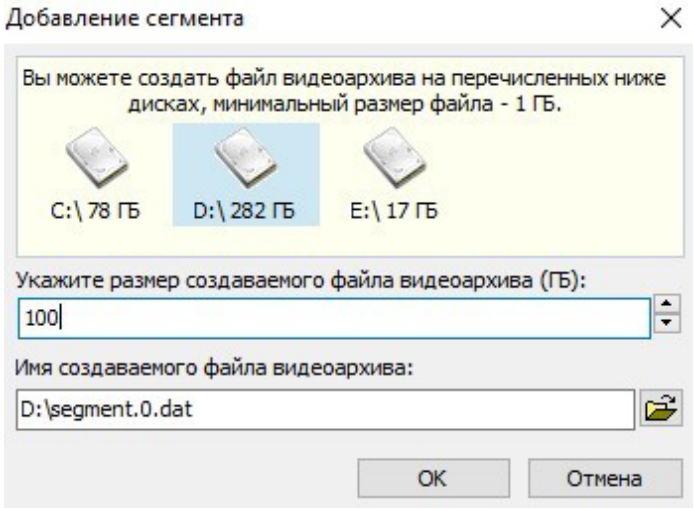
***Внимание!***

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

### 19.1.2. Создание и удаление видеоархива

Для создания нового файла видеоархива:

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




3. В открывшемся окне выделите название диска ПК, на котором будет создан файл видеоархива.
4. С помощью соответствующего счетчика укажите размер создаваемого файла видеоархива или введите значение с клавиатуры.
5. При необходимости измените имя файла видеоархива и его расположение (по умолчанию файл видеоархива `segment0.dat` располагается в корневом каталоге указанного диска). Для изменения расположения нажмите кнопку рядом с полем **Имя создаваемого файла видеоархива**.
6. Нажмите кнопку **ОК**. Окно **Добавление сегмента** будет закрыто. Файл видеоархива будет добавлен в список в рабочей области вкладки **Видеоархив**.

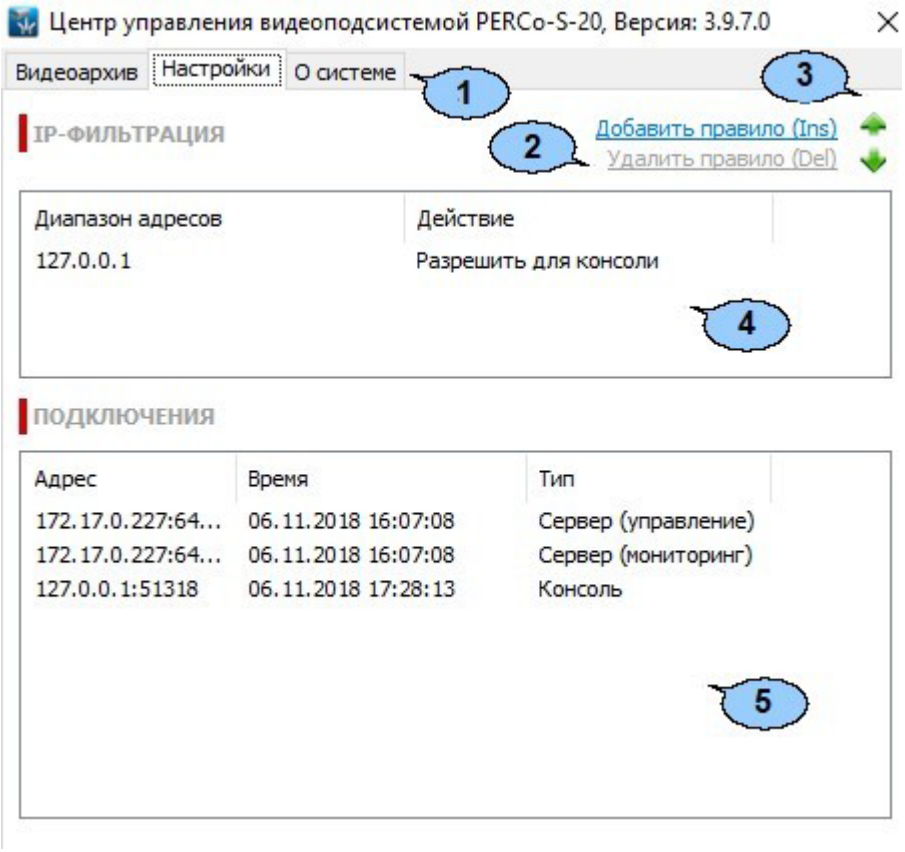
Для удаления файла видеоархива выделите его в рабочей области вкладки **Видеоархив** и нажмите кнопку **Удалить файл**. В появившемся диалоговом окне подтвердите удаление.

Закройте ***«Центр управления видеоподсистемой»***, нажав кнопку **Закрыть** в строке заголовка окна.

## 19.2. Вкладка «Настройки»

### 19.2.1. Рабочее окно вкладки

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




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

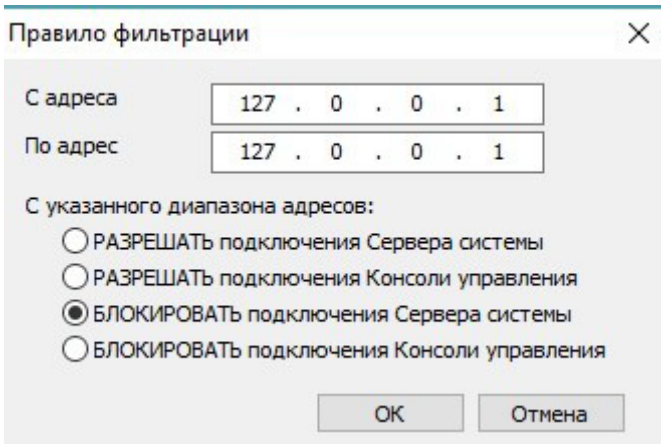
### 19.2.2. Настройка IP-фильтра

Возможно создание фильтров с использованием следующих правил:

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

Для добавления фильтра IP-адресов:

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




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

## 19.3. Вкладка «О системе»

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

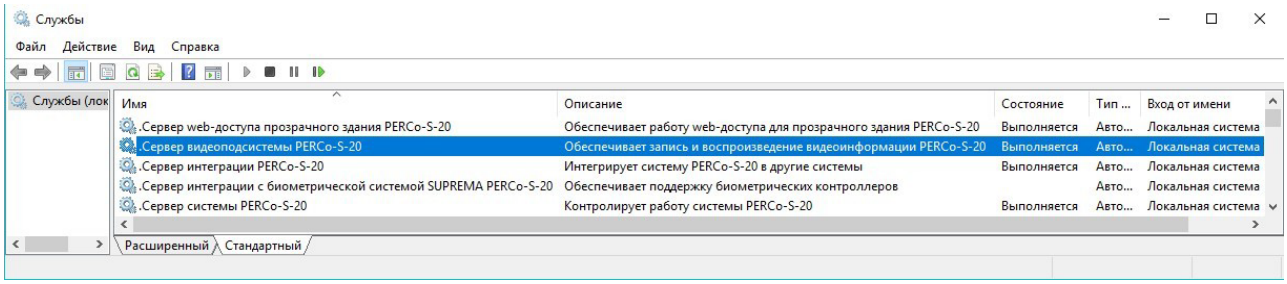

1. Выбор вкладки окна:
   - **Видеоархив**;
   - **Настройки**;
   - **О системе**.
2. Рабочая область вкладки с описанием характеристик системы.

# 20. Установка драйвера видеокамеры

***Внимание!***

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

Для установки драйвера видеокамеры:




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

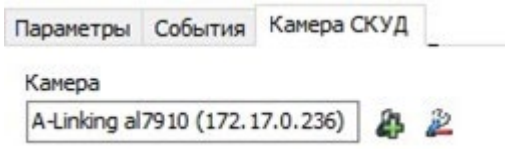
# 21. "Камеры СКУД"

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

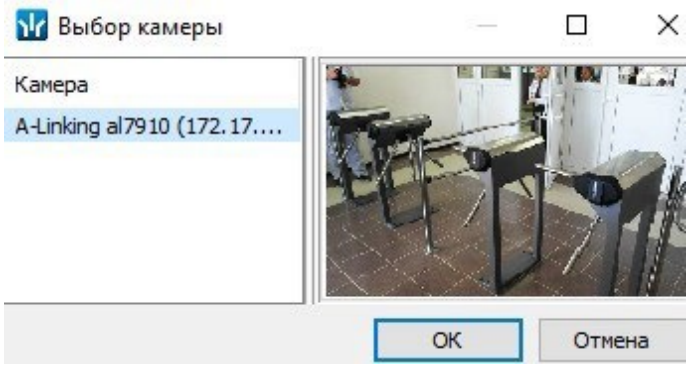
С любым считывателем, подключенным к одному из контроллеров системы, можно связать одну из камер видеоподсистемы. При этом одна камера одновременно может быть связана с несколькими считывателями.

Настройка камеры СКУД:

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




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




7. Выделите в рабочей области открывшегося окна камеру, с которой будет производиться запись при регистрации событий прохода, связанных с данным считывателем. При этом в правой части окна будут отображаться кадры с камеры. Нажмите кнопку **ОК**. Окно будет закрыто. В поле **Камера** на панели настроек появится название выбранной камеры.
8. При необходимости выберите камеры для других считывателей системы.
9. Выделите в рабочей области раздела используемую видеоподсистему и перейдите на панели настроек в правой части окна на вкладку **Параметры**.
10. Установите необходимое значение параметра **Частота кадров при записи для «Камер СКУД»** (рекомендованное значение 240 кадров в минуту).

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

# 22. Прозрачное здание – Web-доступ

## 22.1. Параметры

***Примечание:***

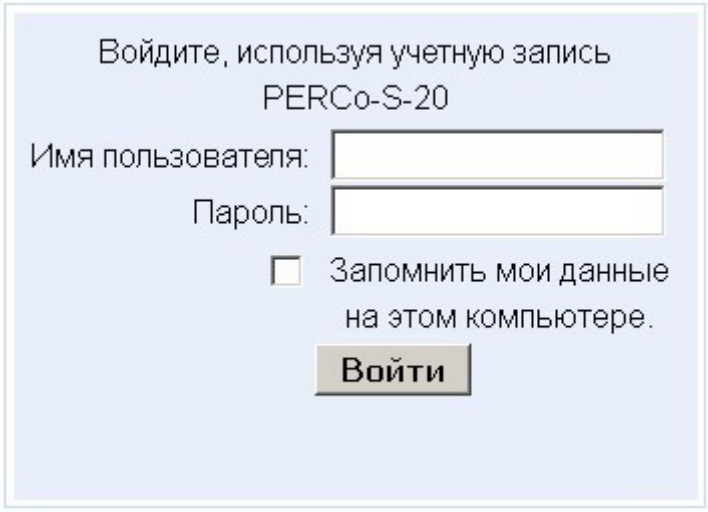
Для работы Web-доступа ***«Прозрачное здание»*** в системе должны быть установлены:
- модуль **Web-доступ прозрачного здания** или настроен внешний Web-сервер,
- **Сервер видеоподсистемы**,
- модуль ***PERCo-SM01 «Администратор»***

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

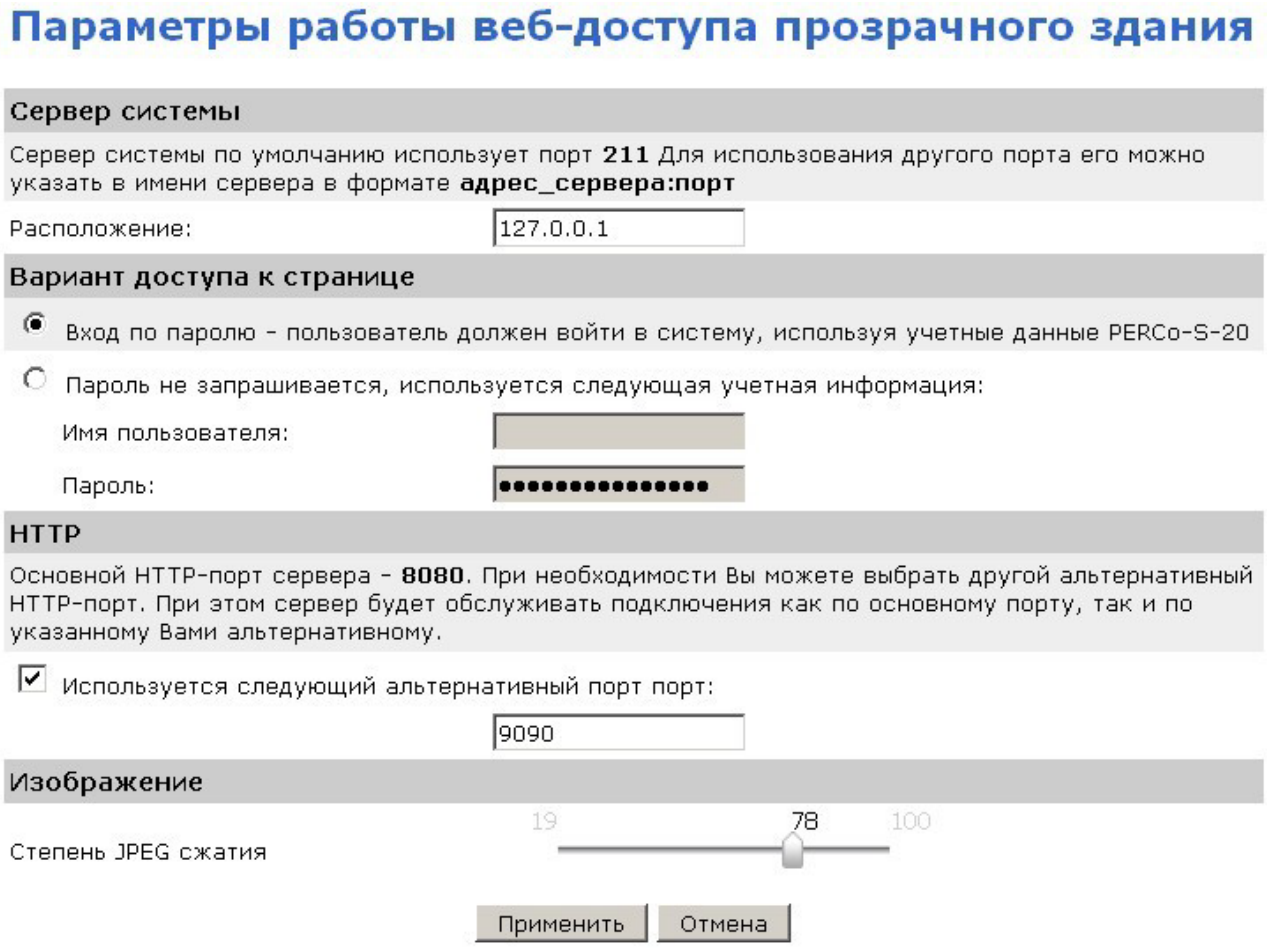
- Web-сервер может быть интегрированный установлен на одном из ПК, входящих в систему. Сервер в этом случае устанавливается вместе с модулем **Web-доступ прозрачного здания** из установочного файла сетевого ПО системы и запускается автоматически при загрузке ОС.
- Может использоваться внешний Web-сервер,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

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

- Введите в адресной строке браузера (например, *Internet Explorer*) адрес: `http://x.x.x.x:8080/admin.html`, где `x.x.x.x` IP-адрес Web-сервера.
- Если Web-сервер установлен на том же ПК, с которого осуществляется доступ, то выполните одно из следующих действий:
  - Выберите последовательно: **Пуск > Программы > PERCo > PERCo-S-20 > > PERCo > Настройка WEB-доступа для прозрачного здания**.
  - Введите в адресной строке браузера (например, *Internet Explorer*): `http://localhost:8080/admin.html`.



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




На странице доступны следующие вкладки:

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

## 22.2. Инструкция по установке на Apache/PHP

***Примечание:***

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

**Инструкция по установке на Apache/PHP**

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

Выполните следующие действия:

1. Установите сервер.
2. Установите поддержку PHP.
3. Создайте сертификат для SSL.
4. Скопируйте файлы веб-доступа в папку хранения интернет файлов вебсервера (для Apache – `htdocs`)
5. Пропишите в файл `config. cfg` – адрес сервера системы ***PERCo-S-20***. Адрес необходимо вводить без пробелов и отступов.
6. Перезапустите сервер.

**Использование нестандартного порта для SSL или HTTP**

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

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

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

на

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

и в файле `main. html`

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

на

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

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

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

на

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

Даже если какой-то один из портов нестандартный, то править необходимо во всех местах, поскольку *Apache* не редиректит на порт по умолчанию. Если же порты стандартные, то нет необходимости вносить изменения.

**Защита сервера при помощи SSL**

Создание сертификата

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

1. В файле конфигурации Apache разкомментируйте строки:

   ```
   # Load Module ssl_ module modules/ mod_ ssl. so
   ```

   и в конце

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

   после чего измените строку

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

   на

   ```
   SSLMutex default
   ```

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

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

   Обычно файл `privkey. pem` создается автоматически, но если этого не произошло, введите для его генерации:

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

   Потом введите команды:

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

   и (одной строкой):

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

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

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

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

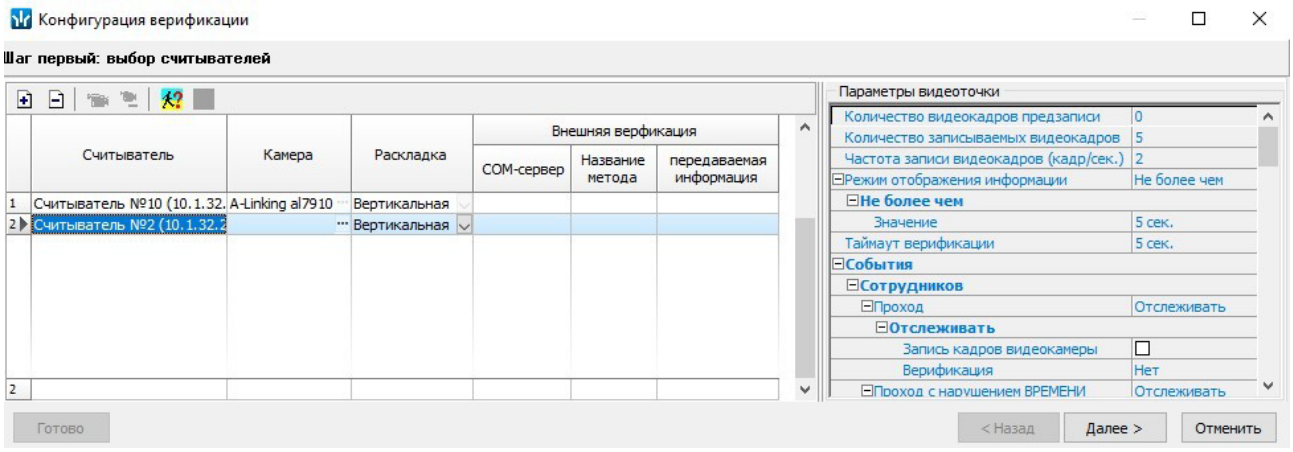
3. Перезапустите службу *Apache*.

# 23. Внешняя программа верификации

## 23.1. Регистрация программы

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

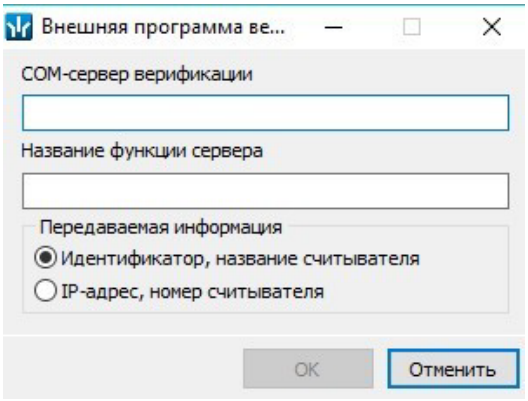
**Регистрация ВПВ**




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

- Кнопка **Регистрация внешней программы верификации** – позволяет передать право принятия решения при проведении процедуры верификации для выбранной точки верификации внешней программе.
- Кнопка **Дерегистрация программы верификации** – позволяет отключить для выбранной точки внешнюю программу верификации.

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



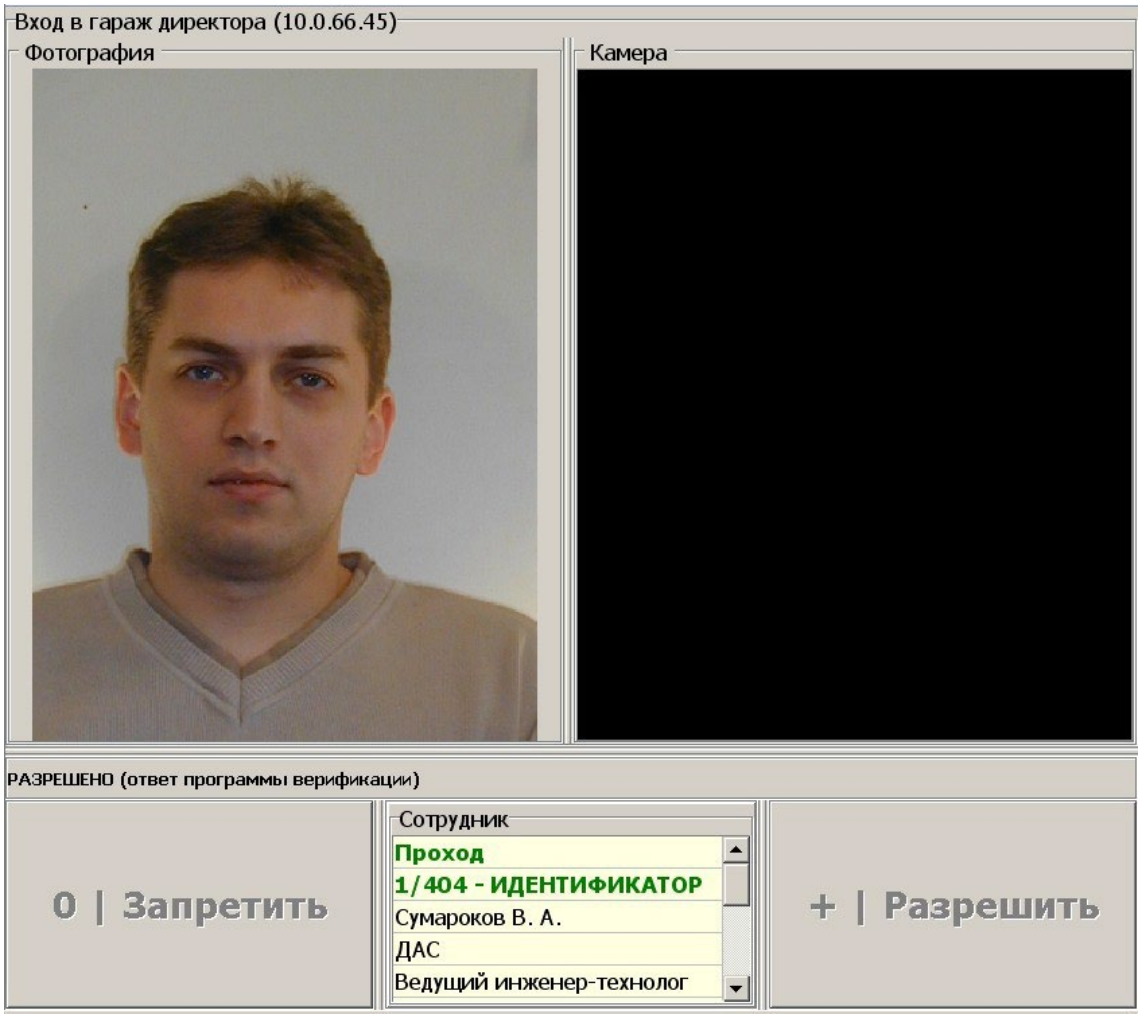

В поле **COM-сервер верификации** необходимо ввести название сервера, в поле **Название функции сервера** – название функции верификации (эти данные сообщают программисты-создатели ВПВ). Выберите тип передаваемой информации. Нажмите кнопку **ОК,** система проверяет возможность связи с ВПВ, и при благополучном вызове ВПВ ей будет послан тестовый запрос на обработку идентификатора 999999999999999. После получения ответа на этот запрос откроется окно подтверждения.

Для подтверждения операции нажмите кнопку **Да.** Окно **Внешняя программа верификации** будет закрыто, описание ВПВ будет сохранено для последующего использования.

## 23.2. Применение программы

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

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




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

## 23.3. Реализация программы в виде метода COM-сервера

**(Для программистов, реализующих ВПВ в виде метода COM-сервера)**

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

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

```
CLSIDFrom Prog ID,
Co Create Instance (Class ID, nil, CLSCTX_ INPROC_ SERVER or
CLSCTX_ LOCAL_ SERVER, IDispatch, Result)),
```

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

```
Get IDs Of Names, Invoke.
```

**Описание функции на IDL**

```
HRESULT _ stdcall < Название функции> ([ in] BSTR AIdentifier,
[ in]  long  ATime Out, [ in] BSTR AReader Name, [ in] long
AType Inquery,
[ in, out] BSTR * ADeny Reason, [ in, out] BSTR * AError
Message, [ out, retval] long * Value)
```

**Описание функции на Delphi Object Pascal**

```
function   < Название функции> (const AIdentifier: Wide
String; ATime Out: Integer;
const AReader Name: Wide String; AType Inquery: Integer;
var ADeny Reason, AError Message: Wide String): Integer.
```

**Описание функции на C#**

```
int < Название функции> (string AIdentifier, int ATime Out,
string AReader Name, int AType Inquery,
ref string ADeny Reason, ref string AError Message)
```

Функция возвращает 0 (нет ошибки при работе функции) или 1 (произошла ошибка при работе функции, ее текст в ***AErrorMessage***).

***AIdentifier*** – символьное представление идентификатора (число от 1 до 18446744073709551614);

***ATimeOut*** – время ожидания ответа на запрос контроллером (секунд);

***AReaderName*** – название считывателя, от которого пришел запрос;

***ATypeInquery*** – код запроса:

0 – прохода без нарушения времени и зональности,
1 – проход с нарушением времени,
2 – проход с нарушением зональности,
3 – проход с нарушением времени и зональности, 4 – постановка на охрану,
5 – снятие с охраны;

***ADenyReason*** – текст причины отказа. Отказано или нет в запросе, определяется по наличию в возвращенной строке ***ADenyReason*** хотя бы одного не пустого символа.

***Примечание:***

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

# 24. Конфигурирование считывателей Mifare

## 24.1. Назначение

**Общие термины и определения:**

- **UID** – открытый неизменяемый уникальный код карты (длиной 4 или 7 байтов), который записывается в незащищенной области памяти. В случае настройки системы для работы с крипто-защищенными ID карт в системе не используется.
- **ID** – персонифицированная идентификационная информация пользователя карты, записанная в защищенной области памяти карты.
- **NFC** – технология беспроводной передачи данных малого радиуса действия, поддерживается современными продвинутыми смартфонами. В СКУД PERCo может быть использована для эмуляции бесконтактной карты на смартфоне, т.е. смартфон с NFC используется как обычная бесконтактная карта формата Mifare (без поддержки шифрования).

***Примечание:***

В руководстве приведено полное описание средств довольно сложной криптозащиты, предусмотренной в стандарте **MIFARE**. При использовании стандарта в рамках обычной СКУД предприятия для поддержания высокой степени защиты карт от копирования достаточно применения всего одного-двух параметров криптозащиты, (к примеру, для карт **MIFARE Plus** вполне достаточно параметров уровня безопасности **SL1**).

## 24.2. Рекомендации по работе с картами Mifare

Для того, чтобы построить систему контроля и управления доступом и быть уверенным, что карты доступа защищены от копирования, необходимо использовать карты доступа с защитой от копирования. Такими картами являются карты формата **MIFARE: Classic, Plus, DESFire.**

***Примечание:***

Карты **MIFARE Ultralight** (кроме **MIFARE Ultralight C**) не имеют защиты от копирования, и по своим возможностям сопоставимы с традиционными Proximity-картами.

Карты **MIFARE** поступают с завода-изготовителя в незащищенном виде. При работе с такими картами считыватель будет использовать только открытый UID карты, который копируется так же легко, как и ID традиционных Proximity-карт (HID, EM-Marine).

***Внимание!***

Заказчик / собственник объекта должен ответственно подойти к вопросу криптозащиты – не доверять создание и запись на карты ключей криптозащиты ни поставщику карт и считывателей, ни монтажнику СКУД, ни кому-либо еще, т.к. если ключи криптозащиты известны постороннему, то тот легко может копировать карты доступа.

От владельца объекта СКУД требуется самому или через доверенное лицо придумать значения паролей и ключей и записать их в карты и считыватели. Для программирования считывателей создается мастер-карта, на которой будет храниться вся ключевая информация. Далее оператор с помощью мастер-карты сможет «прошивать» считыватели, не имея при этом фактического доступа к ключам и паролям.

***Примечание:***
Для встроенных считывателей *Mifare* контроллеров ***CL15***, ***CL15.1***, ***CL15.7*** возможность конфигурации мастер-картой отсутствует.
Для настройки необходимо записать конфигурацию в контрольный считыватель и передать изменения в контроллер, для этого:

- После настройки параметров на вкладке **Запись конфигурации в контрольный считыватель** подраздела ***«Конфигурация Mifare»*** раздела ***«Администрирование»*** нажмите кнопку **Записать**;
- На вкладке ***«Конфигурация»*** раздела ***«Конфигуратор»*** выделите контроллер, в который будет передаваться конфигурация, и нажмите на панели инструментов кнопку **Передать параметры**.

**Основные характеристики разных чипов MIFARE**

| Тип карты | MIFARE Ultralight | MIFARE Classic ID 64 / 1KB / 4KB | MIFARE DESFire E V1 2K / 4K / 8K | MIFARE Plus (S and X) 2K / 4K |
|---|---|---|---|---|
| Крипто-алгоритм | Нет | CRYPTO1 | DES & 3DES/AES | CRYPTO1/AES |
| Длина серийного номера, байт | 7 | 4/7 | 7 | 7 |
| EEPROM, байт | 64 | 1024/4096/4096 | 2048/4096/8192, гибкая файловая структура | 2048/4096 |
| Количество циклов перезаписи | 10 000 | 100 000 | 500 000 | 200 000 |
| Организация памяти | 16 стр./ 4 байт | 16 сект./ 64 байт, 32 сект./ 64 байт, 8 сект./ 256 байт | Определяется программно | 32 сект./4 блока, 8 сект./1 блок |

Криптозащита, встроенная в чип **MIFARE Classic**, в настоящее время признается недостаточно высокой. Чтобы надежно защитить карты доступа от копирования и подделки, разработана линейка карт **MIFARE Plus**, где используется криптография AES, вскрытие которой в настоящее время считается гарантировано невозможным.

Бесконтактные карты **MIFARE Plus** поддерживают 3 уровня безопасности и могут быть в любой момент переведены с одного уровня на более высокий:

- **Уровень безопасности SL1.** На этом уровне карты **MIFARE Plus** имеют 100%-ную совместимость с **MIFARE Classic 1KB (4KB)**.
- **Уровень безопасности SL2.** Аутентификация по AES является обязательной. Для защиты данных используется CRYPTO1.
- **Уровень безопасности SL3.** Аутентификация, обмен данными, работа с памятью только по AES.

Карты формата **MIFARE DESFire EV1** имеют самую высокую степень защиты и гибкую файловую структуру памяти.

Чтобы защитить карту доступа **MIFARE Classic 1KB (4KB)**, достаточно записать в один из блоков памяти идентификатор (например, ID длиной 3 байта для передачи по Wiegand-26) и закрыть доступ к этому блоку криптоключом. А считыватель вместо

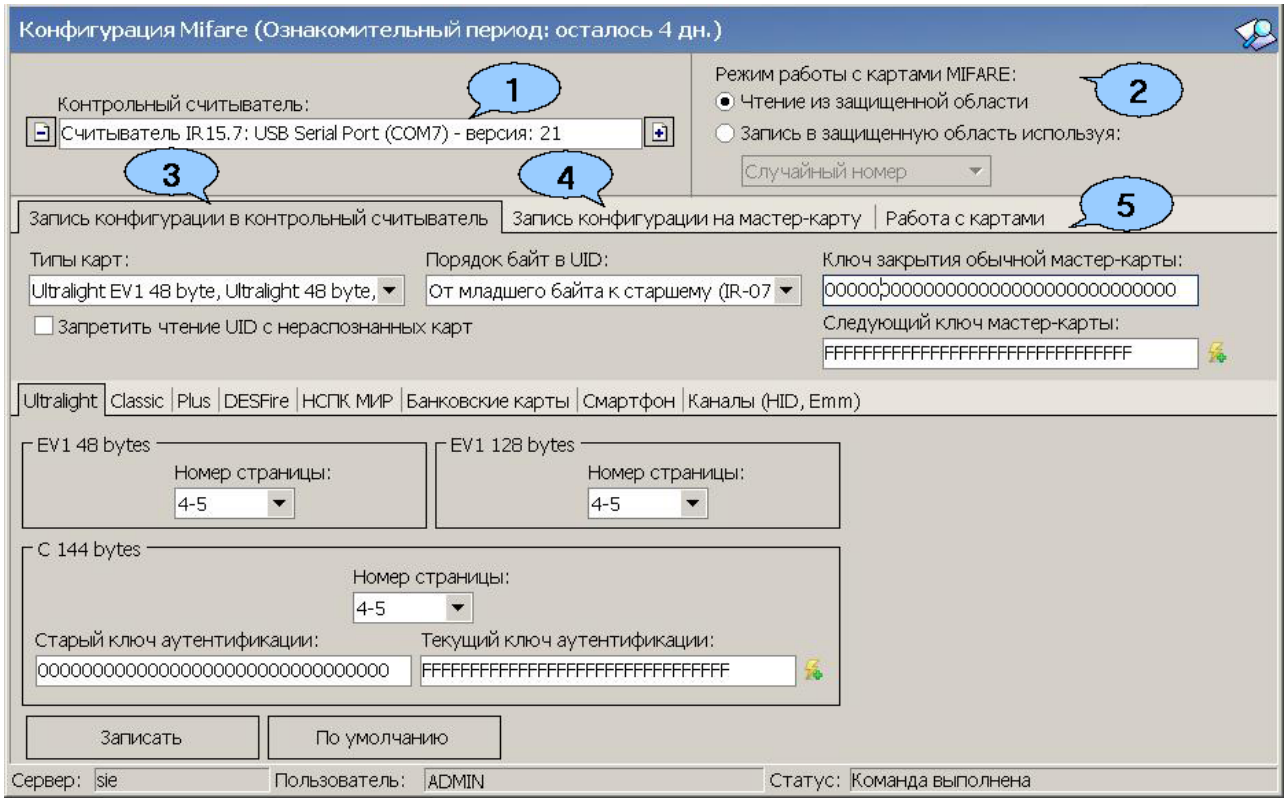
чтения UID-номера настроить на чтение ID-идентификатора из указанного блока памяти **MIFARE Classic** с помощью такого же криптоключа, которым закрыта память карты.

Чтобы карты доступа **MIFARE** работали в СКУД в защищенном режиме, необходимо:

1. Провести организационные мероприятия по предотвращению дискредитации ключевой информации.
2. Для карт **MIFARE Plus** – выбрать уровень безопасности, на котором будут работать карты в данной СКУД: SL1, SL2 или SL3. Тот или иной уровень должен быть выбран, исходя из специфики объекта и требований защищенности. Уровень SL3 – самый высокий с точки зрения защиты.
3. Провести подготовку считывателей. Каждый считыватель, подключаемый к контроллеру СКУД, должен быть запрограммирован на чтение данных из того же блока памяти и по тому же ключу AES, что и карта **MIFARE**. При использовании считывателей ***PERCo*** необходимо через ПО настроить контрольный считыватель, записать мастер-карту и с ее помощью сконфигурировать все считыватели СКУД.
4. Эмиссия простых карт пользователей **MIFARE** при помощи контрольного считывателя с интерфейсом USB **PERCo-MR08**. Это запись идентификатора в соответствии с конфигурацией в выбранный сектор памяти **MIFARE**, фактический перевод карт на выбранный уровень безопасности (SL1, SL2 или SL3 для **MIFARE Plus**), закрытие выбранного сектора памяти секретным ключом с криптографией (AES или CRYPTO1). Этот идентификатор будет связан с конкретным работником и будет считываться в защищенном режиме.

## 24.3. Рабочее окно раздела

Раздел **Конфигурация Mifare** содержит вкладки **Запись конфигурации в контрольный считыватель, Запись конфигурации на мастер-карту, Работа с картами** и предназначена для выбора контрольного считывателя, который будет использоваться для последующей конфигурации карт, а также режима работы с картами **Mifare**.




1. Поле **Контрольный считыватель** – позволяет добавить или удалить контрольный считыватель, который будет использоваться для работы с картами **Mifare** с помощью кнопок:
   - **Добавить контрольный считыватель**;
   - **Удалить контрольный считыватель**.
2. Область **Режим работы с картами Mifare** – позволяет переключаться между следующими режимами работы:
   - **Чтение из защищенной области** – режим, при котором происходит только чтение номера карты защищенной области;
   - **Запись в защищенную область используя** – режим, при котором происходит чтение существующего номера карты из защищенной области с последующей перезаписью номера карты на новый, который может быть сгенерирован следующими способами:
     - **Случайный номер** – в этом случае случайный номер карты генерируется автоматически;
     - **Возрастающий номер** – в этом случае номер карты будет сгенерирован программой согласно внутреннему алгоритму.
3. Подвкладка **Запись конфигурации в контрольный считыватель** – позволяет выбрать типы карт Mifare (смартфон, банковские карты), которые будут использоваться в СКУД, и задать им необходимые параметры.
4. Подвкладка **Запись конфигурации на мастер-карту** – позволяет выбрать тип (первичная или обычная) и записать мастер-карту.
5. Подвкладка **Работа с картами** – позволяет прочитать параметры карты с помощью считывателя.

## 24.4. Вкладка «Запись конфигурации в контрольный считыватель»

Вкладка **Запись конфигурации в контрольный считыватель** позволяет выбрать

один или несколько типов карт **MIFARE** (смартфон, банковские карты), которые будут использоваться в СКУД, и задать параметры для выбранных типов карт (т.е. конфигурацию для карт **MIFARE**).

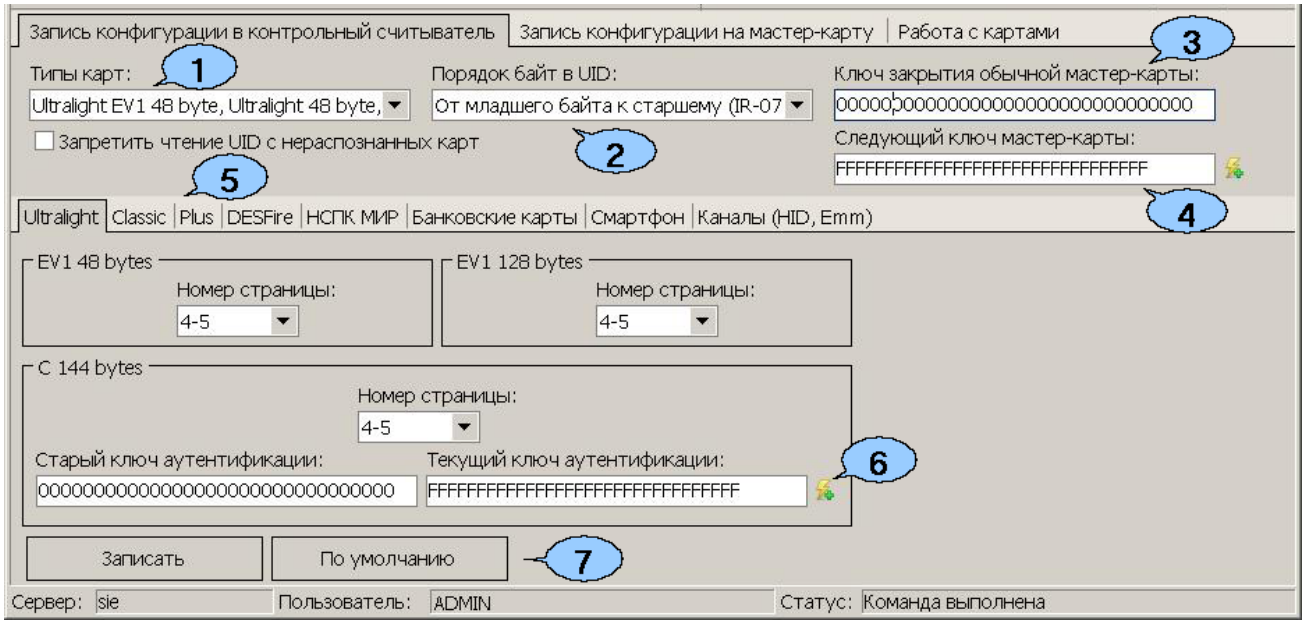
**Общие термины и определения:**

- ***Страница*** – защищенная память карты разбита на пронумерованные части – страницы (кол-во частей зависит от объема памяти).
- ***Номер страницы –*** номер страницы памяти карты, позволяющий обратиться к этой странице с целью записи в нее информации.
- ***Номер сектора*** – номер части внутренней защищенной области памяти карты, которая содержит в себе несколько блоков данных для хранения информации.
- ***Номер блока*** – номер минимальной части памяти карты. Блоки данных доступны для чтения / записи при условии успешной авторизации по ключу.
- ***Номер приложения*** – номер файла памяти, расположенного во внутренней защищенной области памяти карты, в который записывается информация.
- ***SL (secure level)*** – уровень безопасности (только для карт **MIFARE Plus**):
  - Уровень безопасности 0, или начальный уровень. На этом уровне карты **MIFARE Plus** находятся до ввода в эксплуатацию. С SL0 карта переводится на требуемый уровень безопасности;
  - Уровень безопасности 1. На этом уровне карты **MIFARE Plus** имеют полную совместимость с картами **MIFARE Classic 1KB, MIFARE Classic 4KB** и могут работать в рамках одной СКУД;
  - Уровень безопасности 2. Аутентификация по крипто-алгоритму AES становится обязательной. Для защиты данных начинает использоваться крипто-алгоритм CRYPTO1;
  - Уровень безопасности 3. Для аутентификации, обмена и шифрования данных, для работы с памятью начинает использоваться крипто-алгоритм AES.

***Примечание:***

Карты **MIFARE Plus** могут быть в любой момент переведены с низкого уровня безопасности на более высокий. Перевод с более высокого уровня безопасности на более низкий невозможен.

Вкладка содержит:




1. Выпадающий список **Типы карт** – позволяет с помощью установки флажка выбрать один или несколько типов карт **MIFARE**, которые будут использоваться в СКУД.
2. Поле **Порядок байт в UID** – определяет порядок следования байтов открытого **UID** карты при его считывании (в случае, если в системе будет использоваться идентификация пользователей по открытому **UID)**:
   - **От младшего байта к старшему (IR-07)**;
   - **От старшего байта к младшему**.
3. **Ключ закрытия обычной мастер-карты** – поле отображает текущий ключ закрытия мастер-карты.
4. **Следующий ключ мастер-карты** – поле отображает ключ, который будет записан в конфигурацию как следующий ключ закрытия мастер-карты;
5. Подвкладки **Ultralight, Classic, Plus, DESFire, НСПК МИР, Банковские карты, Смартфон, Каналы (HID, Emm)** – позволяют перейти к настройкам конфигурации различных типов карт **MIFARE** (смартфона, банковских карт).
6. Кнопка  **Генерация случайной последовательности** – позволяет задать для поля **Следующий ключ мастер-карты** новый ключ при помощи генератора случайных чисел.
7. Кнопка **Записать** – позволяет записать заданную для карт конфигурацию в энергонезависимую память контрольного считывателя. Кнопка **По умолчанию** – для сброса измененных настроек.

### 24.4.1. Подвкладки Ultralight, Classic, Plus, DESFire, НСПК МИР, Банковские карты, Смартфон, Каналы (HID, Emm)

1. Подвкладки **Ultralight, Classic, Plus, DESFire** позволяют задать рабочие параметры криптозащиты для соответствующих типов карт, выбранных в выпадающем списке строки **Типы карт** вкладки **Запись конфигурации в онтрольный считыватель**. Эти параметры будут задаваться простым картам пользователей при их эмиссии и персонализации с помощью контрольного считывателя, также эти параметры будут перенесены в конфигурацию считывателей на точках прохода с помощью мастер-карты.

***Примечание:***

Допустимые значения параметров отображаются в выпадающих списках при нажатии на стрелку в конце строки с данным параметром. Применять в конфигурации можно любой из активных (неактивные выделяются серым цветом) параметров и любое из его допустимых значений.

Области подвкладок предназначены для конфигурирования параметров соответствующих типов карт.

Подвкладки и области различных типов карт содержат следующие параметры криптозащиты:

- **Номер страницы, номер сектора, номер блока** – адрес в памяти карты для хранения ID пользователя карты, используемый в СКУД.
- **Ключ аутентификации** – пароль, которым закрыт доступ к ID карты, отображается в формате Hex.
- **Старые параметры**, **Старый ключ аутентификации** – поля для отображения пароля доступа к ID и его характеристик, которые действуют до предстоящей переконфигурации параметров (при предыдущей конфигурации параметров они были отображены в полях **Текущие параметры**, **Текущий ключ аутентификации**).
- **Текущие параметры**, **Текущий ключ аутентификации** – поля для отображения пароля доступа к ID и его характеристик, которые будут действовать после переконфигурации параметров (при следующей переконфигурации они будут отображены в полях **Старые параметры, Старый ключ аутентификации**).
- На подвкладке **Plus**, кроме того, имеется область персонификации с параметрами, определяющими уровень безопасности (SL1, SL2, SL3).

***Внимание!***

Данные параметры предназначены для обеспечения самых высоких уровней защиты (например, карт платежных систем). В рамках обычных СКУД не рекомендуется использовать данные параметры, чтобы при утере их значений не пришлось менять все персонифицированные в системе карты.

- Кнопка  **Генерация случайной последовательности** – позволяет заполнить поле параметра значением, задаваемым генератором случайных чисел.

2. Подвкладка **НСПК МИР** предназначена для внесения следующих данных:
   - **ID приложения**;
   - **ключ приложения**.
3. Подвкладка **Банковские карты** позволяет выбрать тип идентификатора для банковских карт:
   - **в качестве ID используется UID карты**;
   - **в качестве ID используется PAN карты**;
   - **в качестве ID используется ID из эмулируемой области (приложения) Mifare Classic**;
   - **в качестве ID используется ID из приложения НСПК МИР**.

***Примечание:***

В качестве приложения может выступать, например, транспортное приложение универсальной карты.

4. Подвкладка **Смартфон** предназначена для возможности прохода по смартфонам с технологией NFC.

***Примечание:***

При работе со смартфоном на ОС Android, поддерживающим технологию NFC, в качестве идентификатора сотрудника (посетителя) используется уникальный идентификатор, генерируемый приложением **«PERCo.Доступ»** (требуется установка и запуск приложения, бесплатно на *Google Play*).

При работе со смартфоном Apple, поддерживающим технологию NFC, в качестве идентификатора сотрудника (посетителя) используется уникальный идентификатор (*Token*), привязанный к банковской карте (при привязке нескольких банковских карт осуществляется считывание *Token* той карты, которая активна в данный момент).

Уникальный идентификатор добавляется в систему аналогично другим картам.

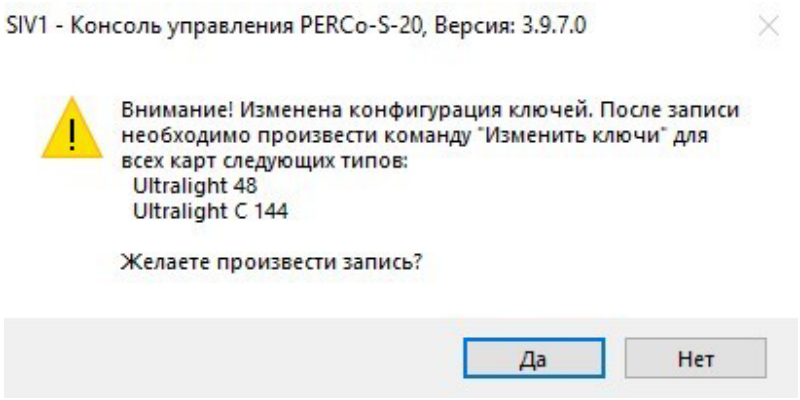
5. Подвкладка **Каналы (HID, Emm)** позволяет включить/отключить возможность работы со стандартами бесконтактных карт *HID* и *EM-Marine*. Если флажки не установлены, считыватель ***PERCo-IR19*** и контроллер замка ***PERCo-CL211.9*** будут поддерживать только работу со стандартом *Mifare*.

## 24.5. Вкладка «Запись конфигурации на мастер-карту»

Вкладка **Запись конфигурации на мастер-карту** предназначена для записи конфигурации из контрольного считывателя на мастер-карту, с помощью которой конфигурация переносится ее на считыватели **PERCo-MR07** системы. Вкладка содержит:


1. **Использовать мастер-карту** – удалите флажок, если предполагается работа только с контроллерами ***CL15*** и ***CR11***. При снятом флажке появляется возможность редактировать вручную информацию на подвкладках **Ultralight, Classic, Plus, DESFire.** По завершению редактирования и после нажатия кнопки **Записать** появится диалоговое окно. Для подтверждения нажмите **Да.**

Пример диалогового окна:



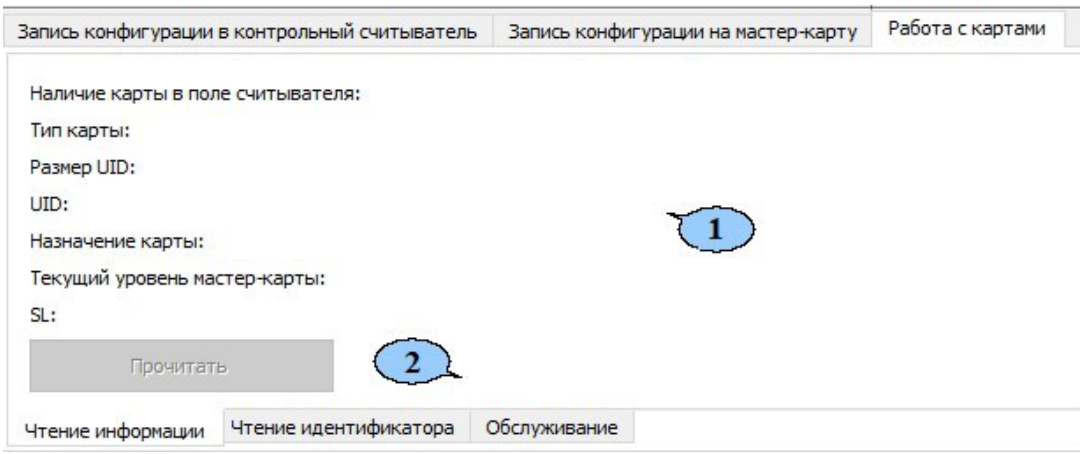

2. Область **Тип мастер-карты** – позволяет выбрать тип мастер-карты для записи:
   - **Первичная** – мастер-карта, которая предназначена для первоначальной конфигурации считывателей. Уровень первичной мастер-карты – 1,
   - **Обычная** – мастер-карта, которая предназначена для программирования считывателей с целью переноса в них вновь заданной конфигурации;
3. Кнопка **Записать** – позволяет записать конфигурацию системы из контрольного считывателя на мастер-карту. После нажатия на кнопку необходимо записываемую мастер-карту поднести к контрольному считывателю.

***Примечание:***

Чистая карта типа **DESFire** может быть записана в качестве дополнительной мастер-карты для СКУД. Перезапись мастер-карты с целью перевода ее в состояние простой карты пользователя **невозможна**! (Т.е. карта, однажды записанная как мастер-карта, может использоваться далее только в этом качестве.)

## 24.6. Вкладка «Работа с картами»

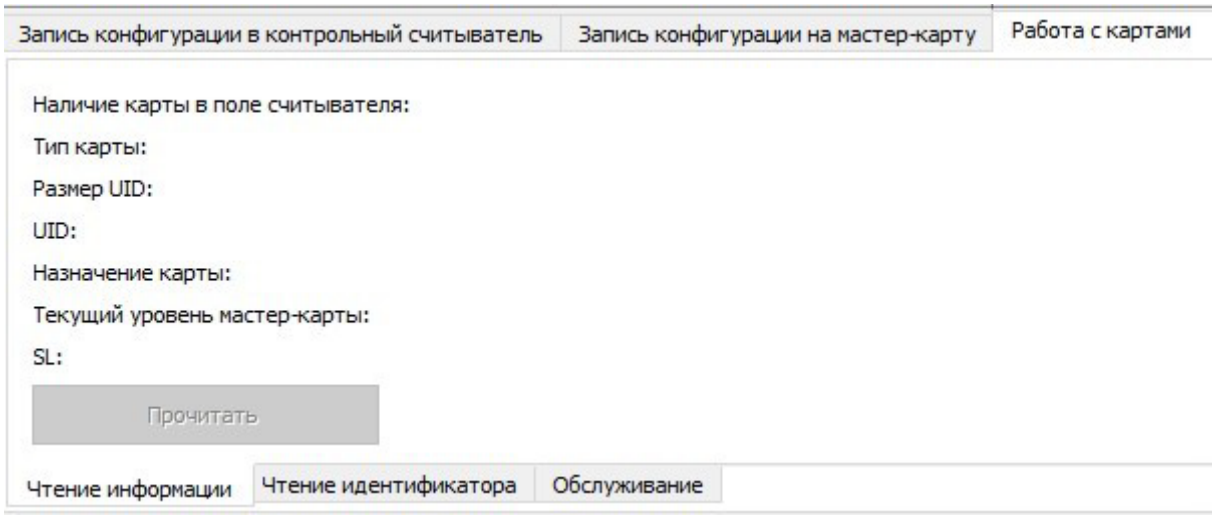
Подвкладка **Работа с картами** содержит следующие дополнительные подвкладки:




1. Рабочая область вкладки (вид области зависит от выбранной подвкладки).
2. Подвкладки для работы с картами **MIFARE**:
   - **Чтение информации** – позволяет прочесть и отобразить информацию с карты **MIFARE**;
   - **Чтение идентификатора** – позволяет прочесть и отобразить идентификатор из защищенной области памяти карты **MIFARE**;
   - **Обслуживание** – позволяет производить обслуживание карт **MIFARE** (изменять ключи и уровень безопасности, форматировать карты).

### 24.6.1. Подвкладка «Чтение информации»

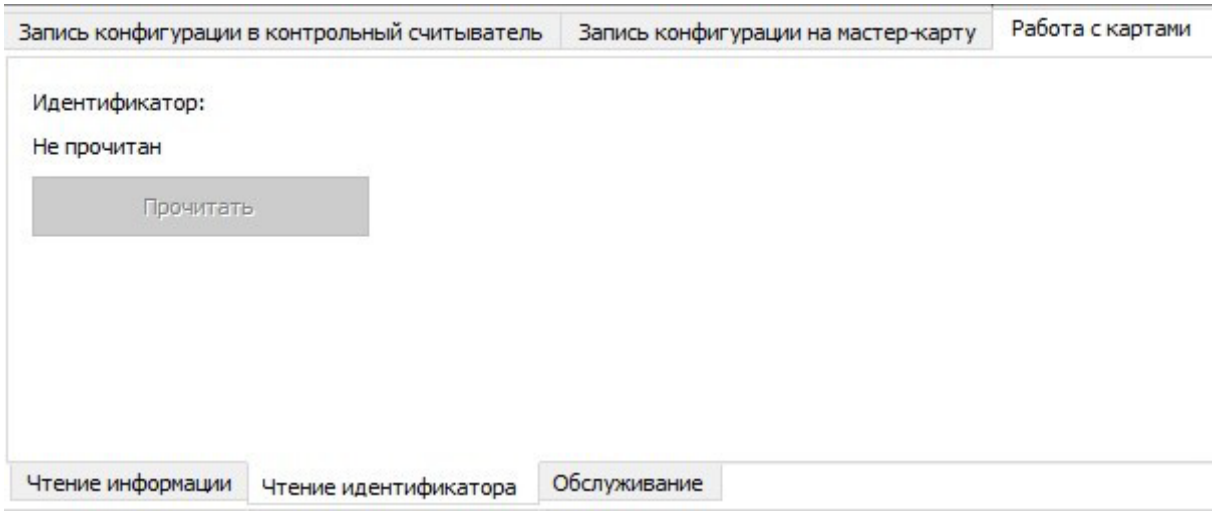
Подвкладка **Чтение информации** позволяет прочесть и отобразить информацию, которая доступна для прочтения с карты **Mifare**.




- Рабочая область подвкладки отображает следующую информацию:
  - **Наличие карты в поле считывателя** – отображает наличие или отсутствие карты в поле считывателя.
  - **Тип карты** – отображает тип карты в поле считывателя.
  - **Размер UID** – отображает размер идентификатора пользователя, который записан на карту.
  - **UID** – отображает идентификатор пользователя, который записан на карту; **Назначение карты** – отображает назначение карты (т.е. – мастер-карта, простая карта).
  - **Текущий уровень мастер-карты** – отображает текущий уровень мастер-карты (если была прочитана простая карта – отображается значение 0).
  - **SL** – отображает уровень безопасности для карт **Mifare Plus** (если была прочитана карта другого типа – отображается значение 0).
- Кнопка **Прочитать** – позволяет прочитать информацию с помощью контрольного считывателя.

### 24.6.2. Подвкладка «Чтение идентификатора»

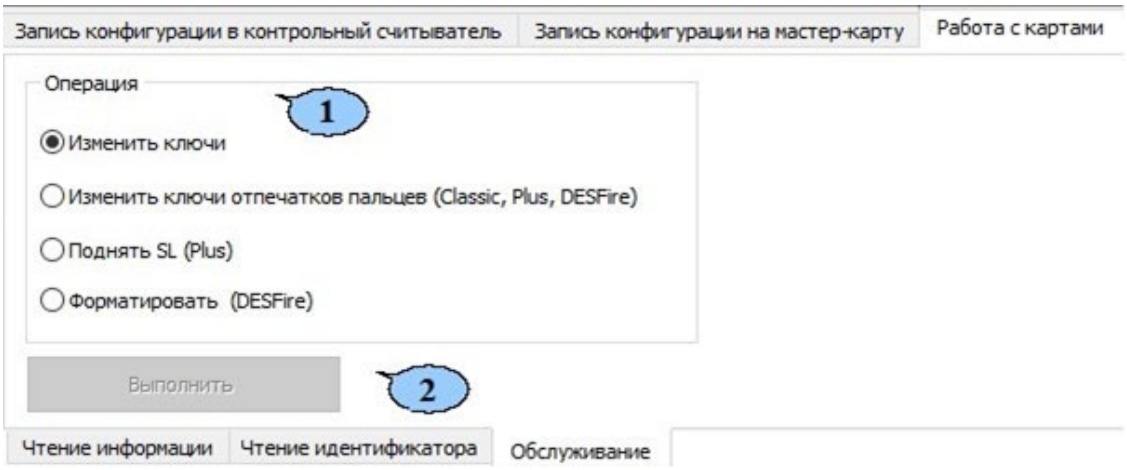
Подвкладка **Чтение идентификатора** позволяет прочесть и отобразить идентификатор из внутренней области памяти карты **Mifare:**




- Рабочая область подвкладки отображает следующую информацию:
  - **Идентификатор** – отображает идентификатор, считанный из внутренней области памяти карты.
- Кнопка **Прочитать** – позволяет прочитать информацию с помощью контрольного считывателя.

### 24.6.3. Подвкладка «Обслуживание»

Подвкладка **Обслуживание** позволяет производить обслуживание карт **Mifare**.




1. Область **Операция** содержит следующие возможности по обслуживанию карт:
   - **Изменить ключи** – по команде считыватель определяет наличие карты в поле считывателя, ее тип, и меняет значение ключа согласно параметрам, заданным в конфигурации контрольного считывателя для данного типа карт;
   - **Поднять SL (Plus)** – по команде считыватель определяет наличие карты в поле считывателя, ее тип (операция предназначена для карт **Mifare Plus**), и поднимает значение SL до указанного в параметрах, заданных в конфигурации контрольного считывателя;
   - **Форматировать (DESFire Ev1)** – по команде будет произведено форматирование карты (операция предназначена для простых карт **Mifare DESFire Ev1** (**не мастер-карт**)) в том случае, если на карте записано несколько приложений и нет свободного места для создания нового приложения;
2. Кнопка **Выполнить** – позволяет выполнить выбранную операцию.

## 24.7. Алгоритм работы с картами Mifare

Далее для примера приведен алгоритм действий по настройке СКУД для работы с защищенной областью памяти карт пользователей формата **MIFARE Classic 4KB**.

Для начала необходимо записать конфигурацию в контрольный считыватель. Для этого:

1. Перейдите в раздел **Администрирование** на вкладку **Конфигурация Mifare**.
2. На вкладке **Запись конфигурации в контрольный считыватель** с помощью раскрывающегося меню **Типы карт** установите флажок напротив **Classic 4KB**.
3. В поле **Ключ закрытия обычной мастер-карты** отображается пароль идентификации карты, как мастер-карты для текущей конфигурации считывателей **PERCo-MR 07** (это то значение, которое было записано в поле **Следующий ключ мастер-карты** при предыдущей конфигурации считывателей **PERCo-MR07**). При создании первичной мастер-карты (для конфигурации считывателей, поставленных с завода-изготовителя) данное поле заполнено нулями (не заполнено).
4. В поле **Следующий ключ мастер-карты** с помощью кнопки  сгенерируйте новый ключ закрытия мастер-карты, который будет использоваться в конфигурации как пароль идентификации для следующей мастер-карты (мастер-карты, которой будет осуществляться переконфигурация считывателей в следующий раз). Данный ключ запоминается в системе и при следующей переконфигурации контрольного считывателя автоматически пропишется в поле Ключ закрытия обычной мастер-карты.

***Внимание!***

Данный пароль сохраняется в системе только до следующей переконфигурации, после чего из памяти системы удаляется и восстановлению не подлежит.

5. На вкладке **Classic** определите параметры карты – адрес места в памяти карты, куда будет записываться идентификатор пользователя ID, и пароли доступа к нему (т.е. задайте конфигурацию карт пользователя) в поле **4KB** (поле предназначено для работы с картами **MIFARE Classic 4KB**):
   - Определите **Номер сектора**. Он представляет собой часть памяти карты, в которую будет записан идентификатор, и из которой он будет
   - считываться при взаимодействии пользователя со СКУД. **Номер сектора** выбирается произвольно.
   - Определите **Номер блока**. Он представляет собой часть сектора памяти, в которую будет записан идентификатор, и с которой он будет считываться при взаимодействии пользователя со СКУД. **Номер блока** выбирается произвольно.
   - В поле **Старые параметры** отображаются параметры **Тип ключа аутентификации** и **Ключ аутентификации**, которые были записаны при предыдущей конфигурации в поле **Текущие параметры** и в данный момент (т.е. до переконфигурации считывателей и карт пользователей) являются действующими в СКУД.
   - В поле **Текущие параметры** определите параметры **Тип ключа аутентификации** и **Ключ аутентификации**, которые будут записаны на карты в данный момент, и будут являться действующими в СКУД.

***Примечание:***

Важно, чтобы значения параметров **Тип ключа аутентификации** и **Ключ аутентификации** в поле **Старые параметры** совпадали с типом ключа аутентификации и ключом аутентификации, которые записаны на простые карты пользователей в данный момент, иначе перезаписать в них новые ключи (т.е. перейти на работу с новой конфигурацией системы) будет невозможно. В случае, если простая карта пользователя ранее не использовалась, то значения параметров в области **Старые параметры** не влияют на запись.

6. Нажмите кнопку **Записать** для записи конфигурации в контрольный считыватель.
7. Далее необходимо записать конфигурацию из контрольного считывателя на мастер-карту. Для этого:
   - На вкладке **Запись конфигурации на мастер-карту** укажите тип карты:
     - **Первичная** – мастер-карта, которая предназначена для первоначального программирования считывателей, поставленных с завода-изготовителя. Уровень первичной мастер-карты – 1.
     - **Обычная** – мастер-карта, которая предназначена для нового перепрограммирования считывателей с целью переноса в них новой конфигурации.
   - Приложите мастер-карту к контрольному считывателю и нажмите кнопку **Записать** для записи в нее конфигурации.

***Примечание:***

В качестве мастер-карты в СКУД **PERCo-S-20** используется мастер-карта **DESFire**. Чистая (т.е. без записей в защищенной области) карта типа **DESFire** также может быть записана в качестве дополнительной мастер-карты для СКУД. Перезапись мастер-карты с целью перевода ее в состояние карты пользователя или чистой карты невозможна! (Т.е. карта, однажды записанная как мастер-карта, может использоваться далее только в этом качестве.).

8. С помощью записанной мастер-карты необходимо запрограммировать все считыватели. Для этого достаточно два раза в течение 10 сек. поднести мастер-карту к перепрограммируемому считывателю – новая конфигурация автоматически запишется в память считывателя.

Теперь ваша СКУД готова работать с новыми параметрами. Осталось перепрограммировать простые карты пользователей.

- Если простые карты пользователей, которые необходимо перепрограммировать, использовались в системе ранее, то необходимо перейти на вкладку **Работа с картами > Обслуживание**. Далее выберите в поле **Операция** параметр **Изменить ключи**. Поднесите простую карту пользователя к контрольному считывателю и нажмите кнопку **Выполнить**. На простую карту пользователя запишется новая конфигурация.
- Если простые карты пользователей, которые необходимо перепрограммировать, не использовались ранее, то необходимо их персонифицировать, т.е. – выдать им идентификатор и закрепить за пользователем. Это можно сделать в разделе **Доступ > Доступ сотрудников (Доступ посетителей)** с помощью кнопки **Выдать карту** на вкладке **Сотрудники (Посетители)**.

При необходимости изменения конфигурации необходимо повторить все действия, начиная с п.1, при этом учитывая, что:

– Если в текущую конфигурацию СКУД добавляются новые типы карт

пользователей, то ранее выданные карты будут работать.

- Если в конфигурации изменяются какие-либо параметры для уже выданных карт пользователей (номера страниц / секторов / блоков, типы и/или значения ключей, уровни безопасности SL), то ранее выданные карты пользователей не будут работать и их необходимо перепрограммировать с учетом новой конфигурации.
- Особенности работы с мастер-картами и рекомендации по паролям для них приведены в руководстве по эксплуатации на контрольный считыватель ***PERCo-MR08***.

**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. 31.01.2025

www.perco.ru