PERCo

Система S–20 «Школа»
Программное обеспечение

PERCo-S-20 «Школа»

РУКОВОДСТВО АДМИНИСТРАТОРА

Версия ПО: 2.9.8.1

СОДЕРЖАНИЕ

1. Введение

Данное руководство системного администратора ПО *«PERCo-S-20 "Школа"»* (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 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;
БД – база данных,
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

Система «PERCo-S-20 "Школа"» (далее – *система*) предназначена для обеспечения безопасности школы, повышения уровня контроля дисциплины, а также автоматизации обеспечения учебных процессов.

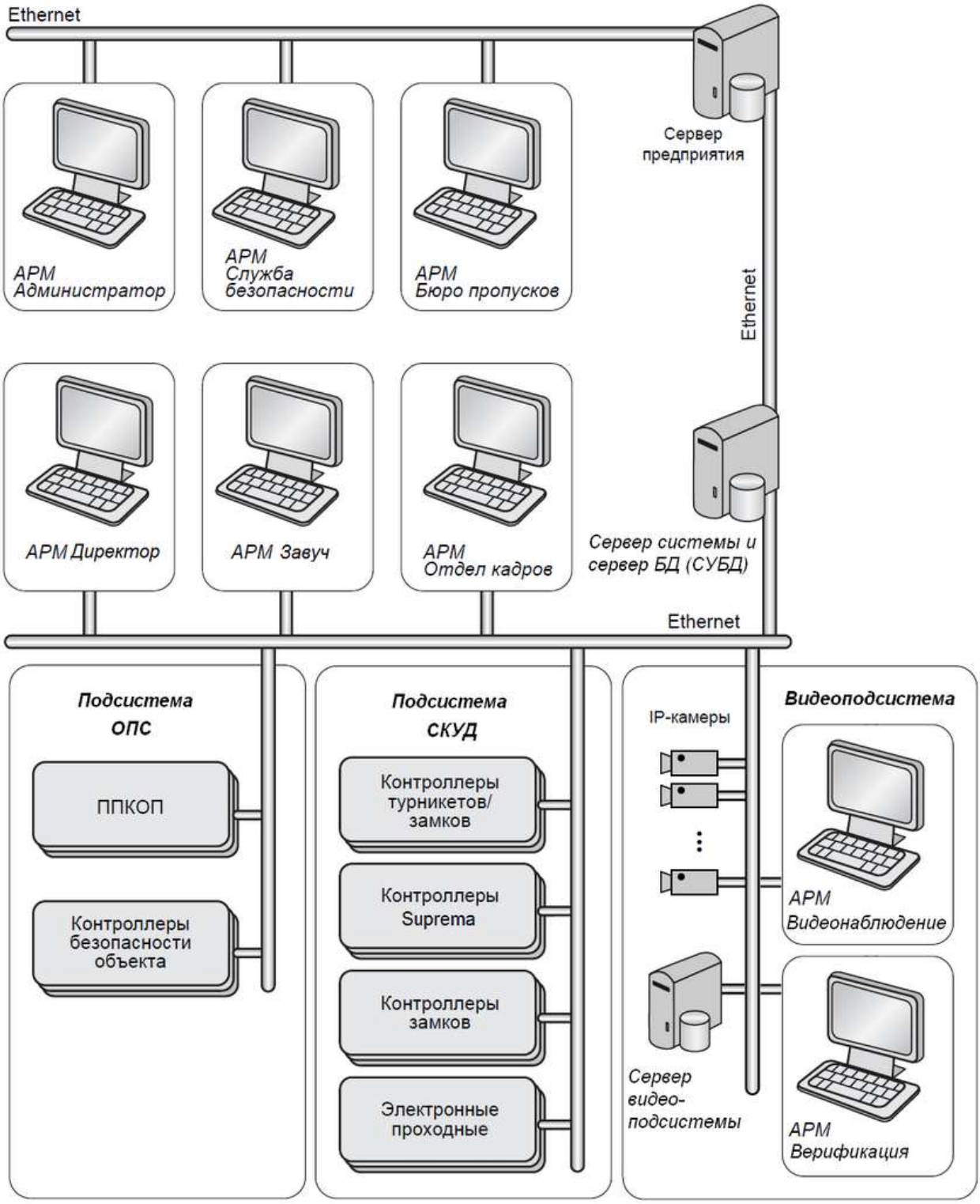
Структурная схема системы показана на рисунке ниже. Все устройства системы работают в единой информационной среде передачи данных, реализованной на основе сети *Ethernet*. Каждое устройство системы (контроллер, ПК), подключаемое к сети, должно иметь фиксированный IP-адрес для связи и обмена данными с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

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»***, создайте список помещений учреждения 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`.

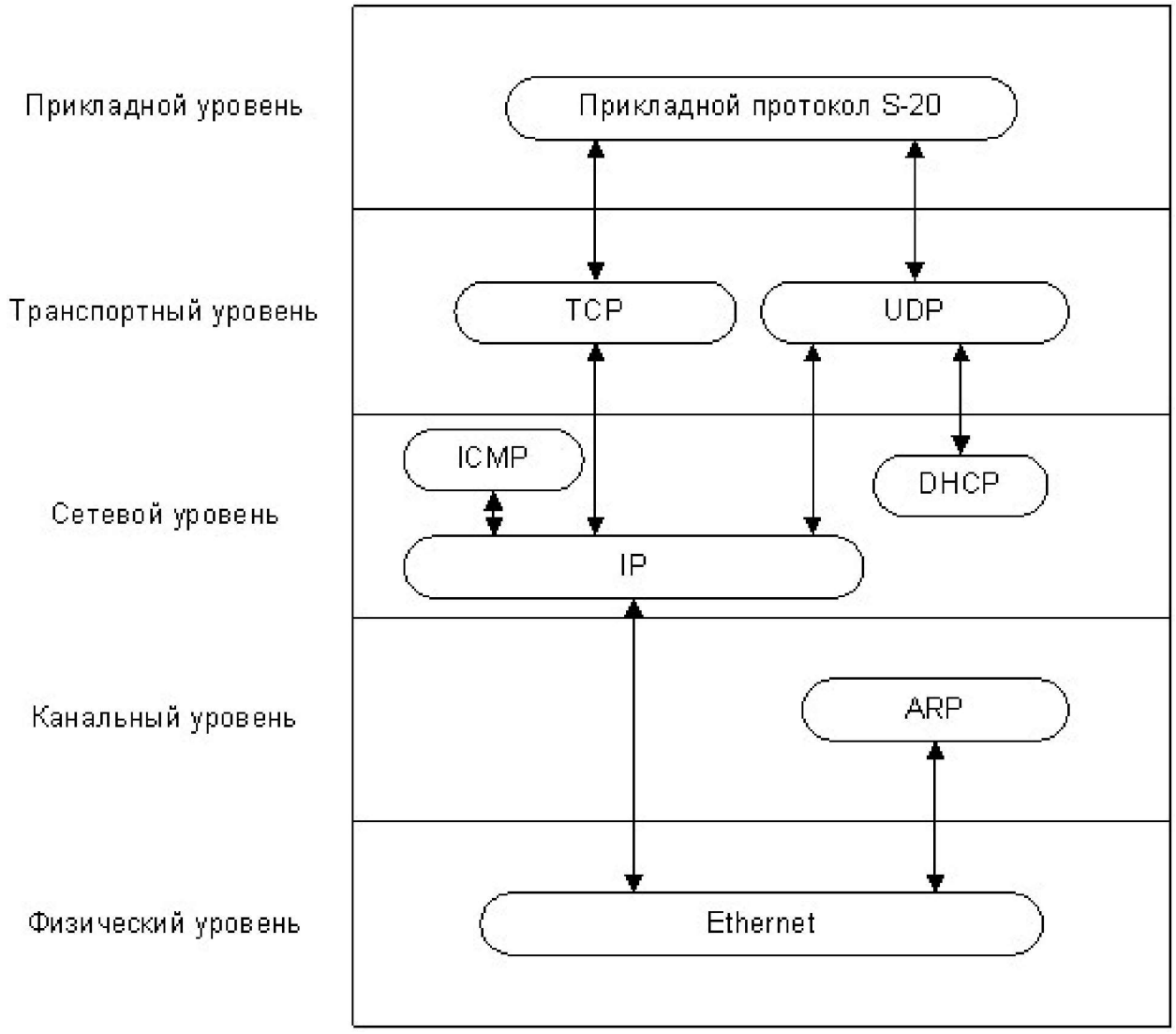
5. Сетевые настройки

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`

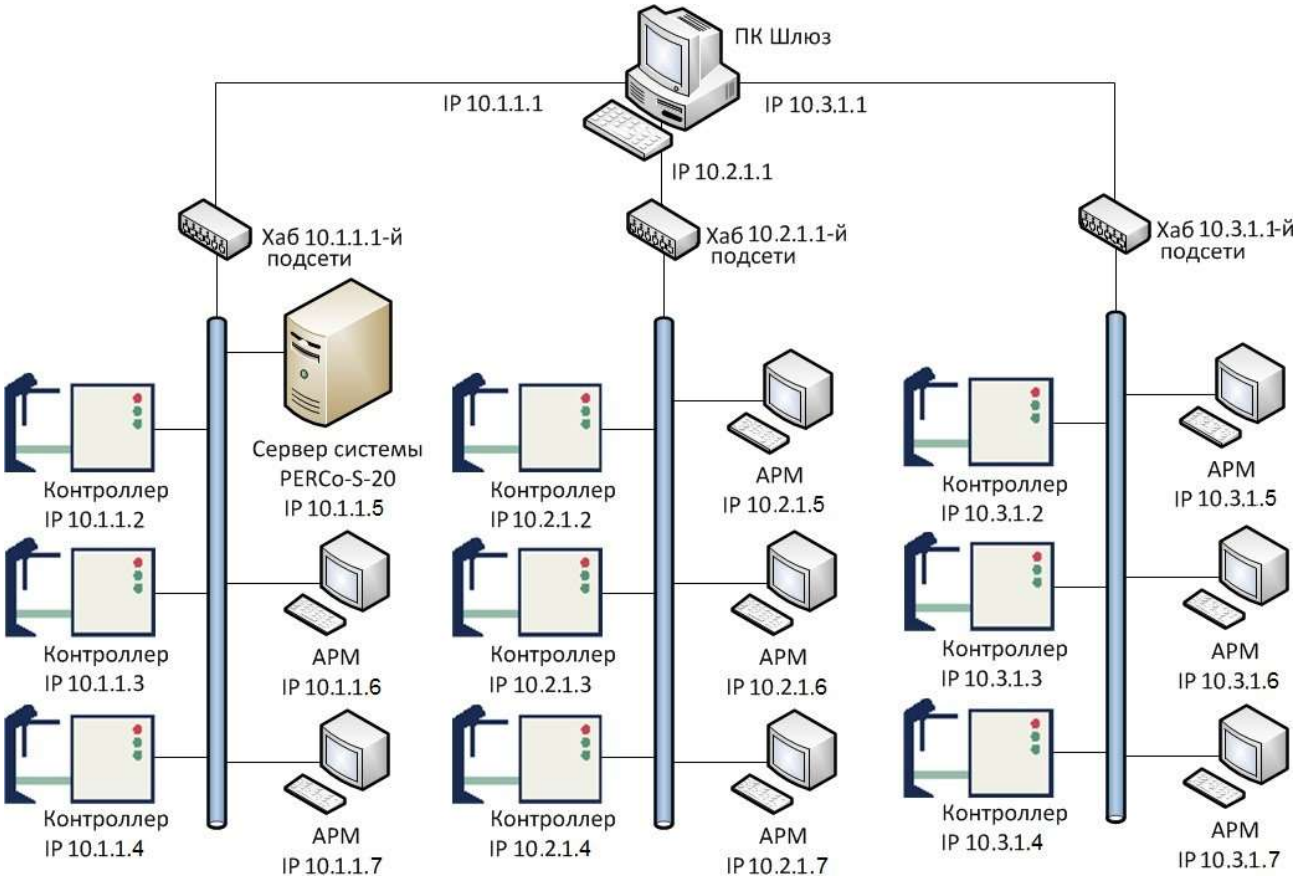
Примечание:

Дополнительная информация о включении маршрутизации пакетов в ОС *Microsoft Windows XP* доступна по ссылке: https://support.microsoft.com/ru-ru/kb/315236.

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

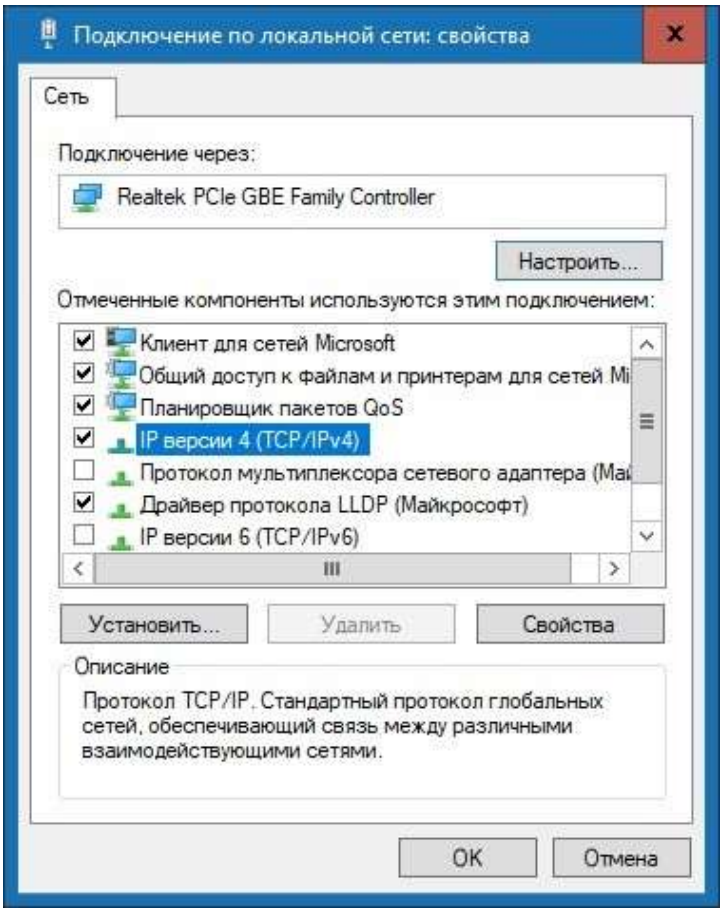


Пример схемы организации широковещательной рассылки

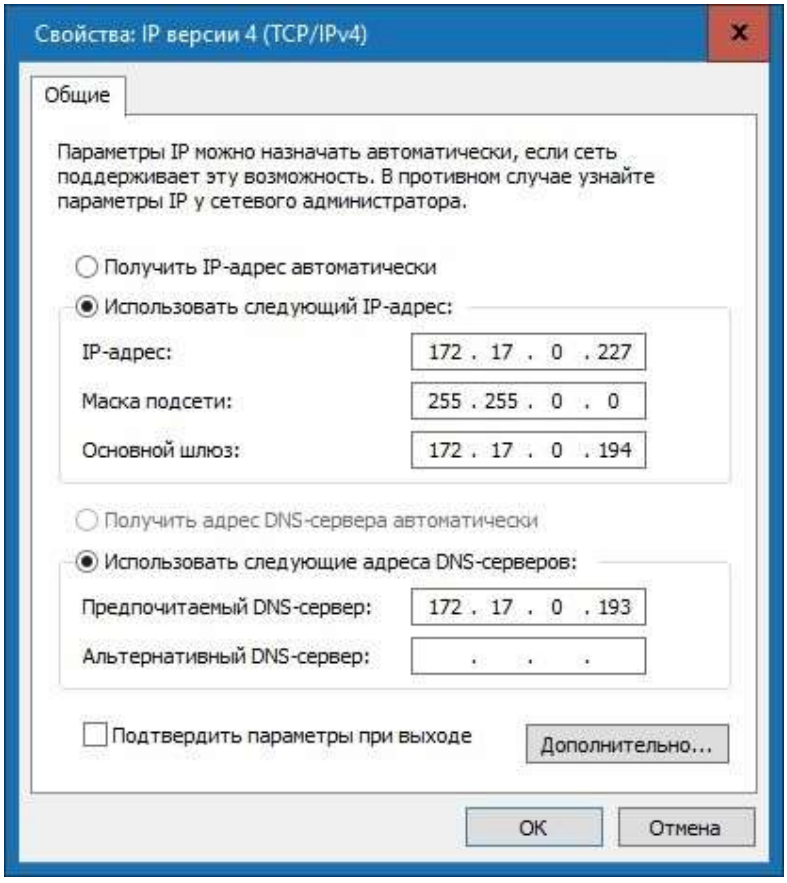
5.3. Добавление сетевого интерфейса ПК

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

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

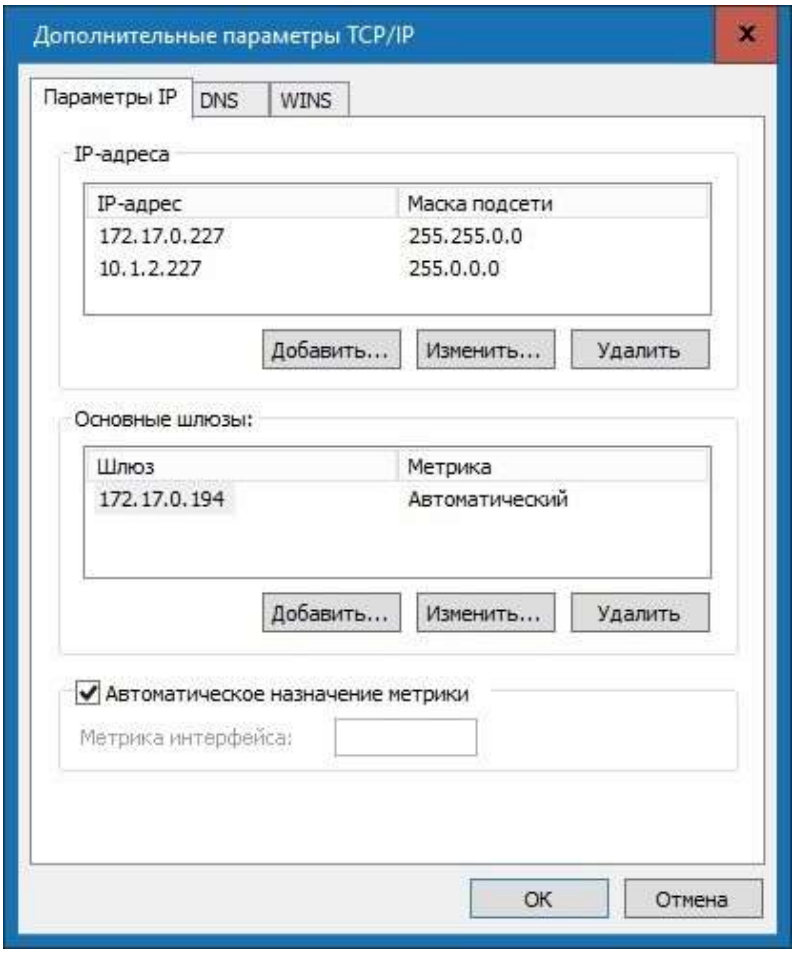


2. Выделите компонент **IP версии 4 (TCP/IPv4)** и нажмите кнопку **Свойства**. Откроется окно **Свойства: IP версии 4 (TCP/IPv4):**

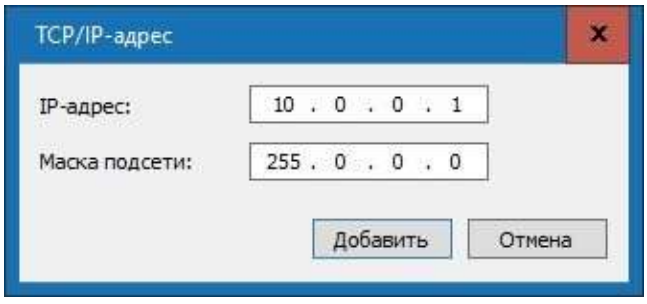


3. В открывшемся окне убедитесь, что переключатель находится в положении

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:

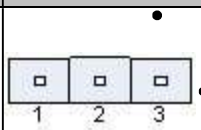
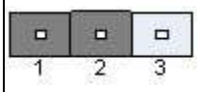
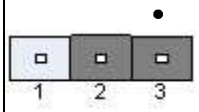
- **IP-адрес:** 10.x.x.x. Значения x указаны в паспорте и на плате устройства,
- **Шлюз:** 0.0.0.0,
- **Маска подсети:** 255.0.0.0,
- **MAC-адрес:** уникальный, неизменяемый в настройке, указан в паспорте и на плате устройства.

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.

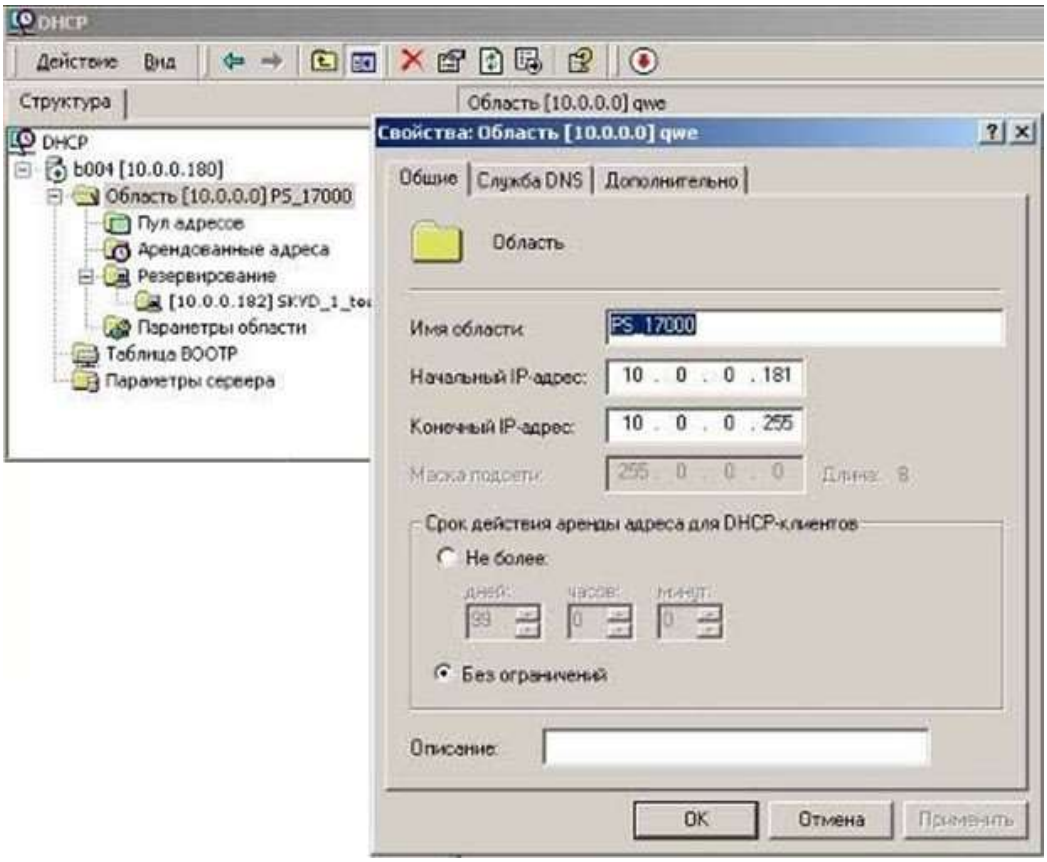
5.5. Настройка DHCP-сервера в ОС Windows

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**.

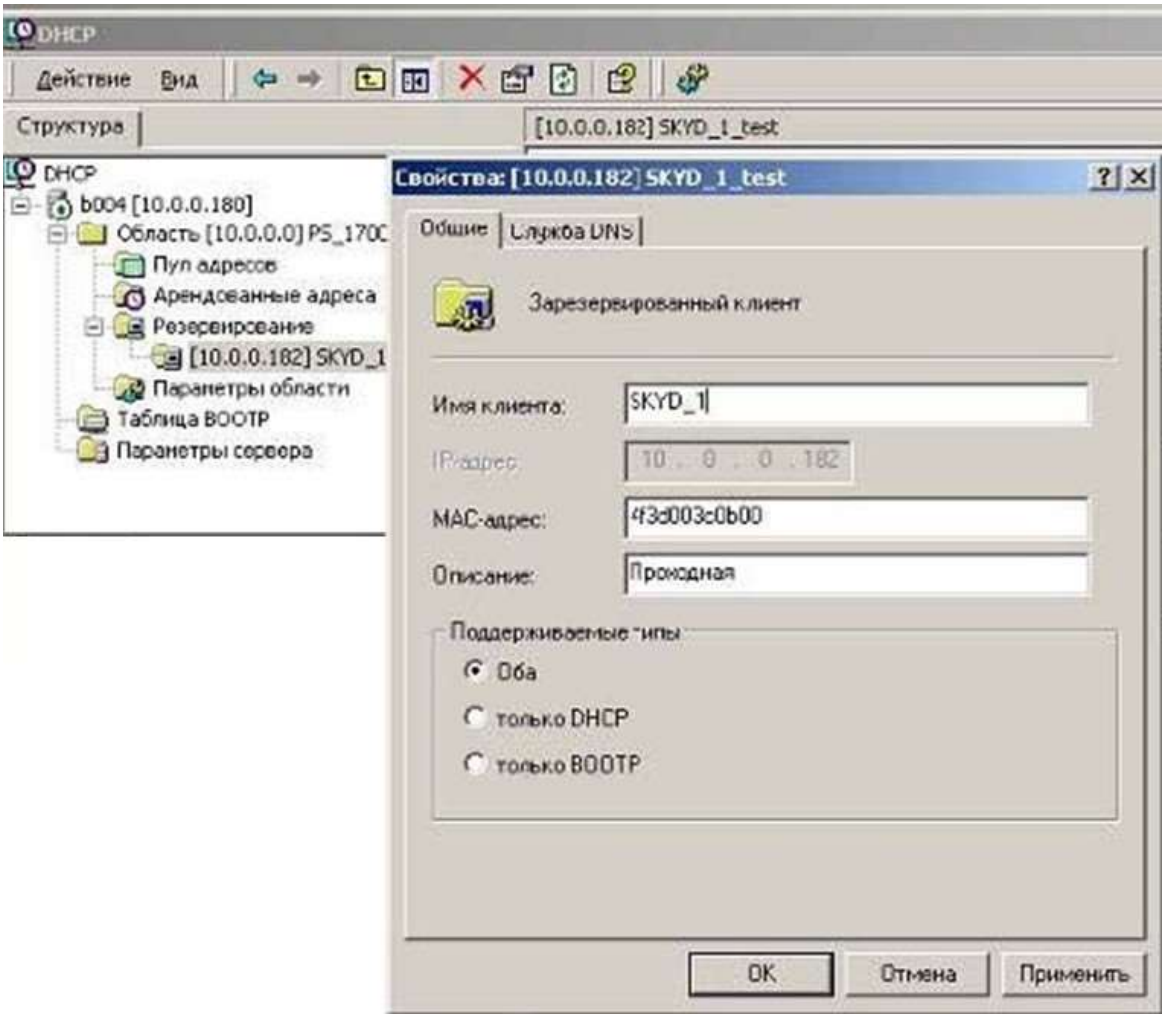


2. Зарезервируйте диапазон IP-адресов для контроллеров системы. Название области и описание могут быть любыми. Это информация необходима для системного администратора, поэтому название должно быть достаточно информативным. Рекомендуется делать область несколько больше, чем число контроллеров, которое 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`.

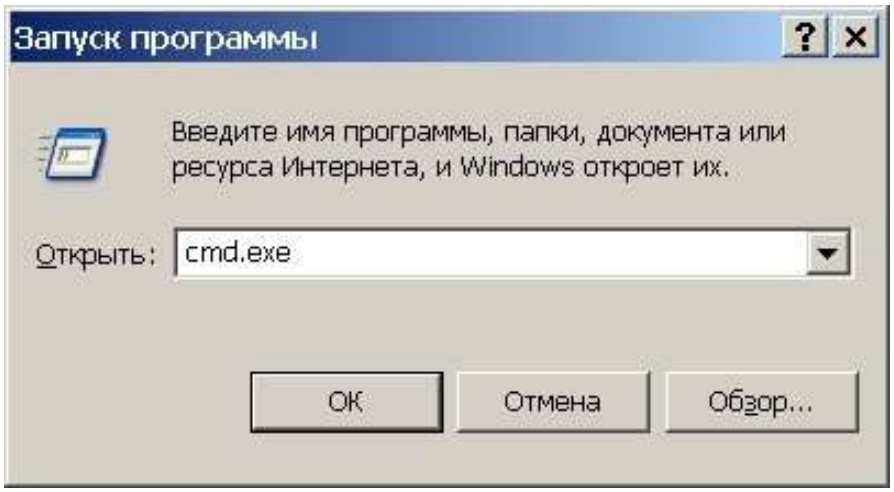
Чтобы внесенные в файл `/etc/dhcp.conf` изменения вступили в силу, необходимо перезапустить сервер. Для этого можно использовать следующие команды:

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

5.7. Проверка связи между ПК и контроллером

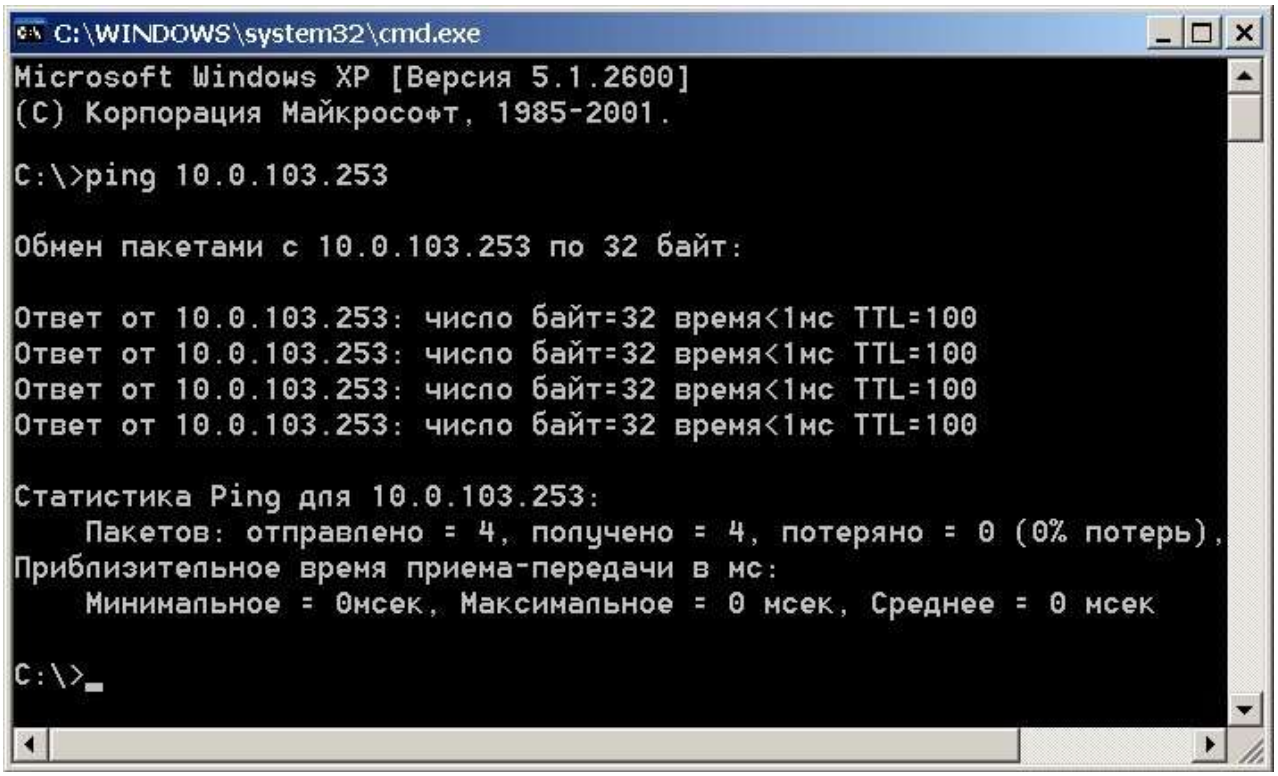
Для корректного функционирования системы необходимо обеспечить устойчивую связь по сети *Ethernet* между сервером системы и всеми контроллерами системы. При необходимости проверки связи между ПК и одним из контроллеров системы произведите следующие действия:

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

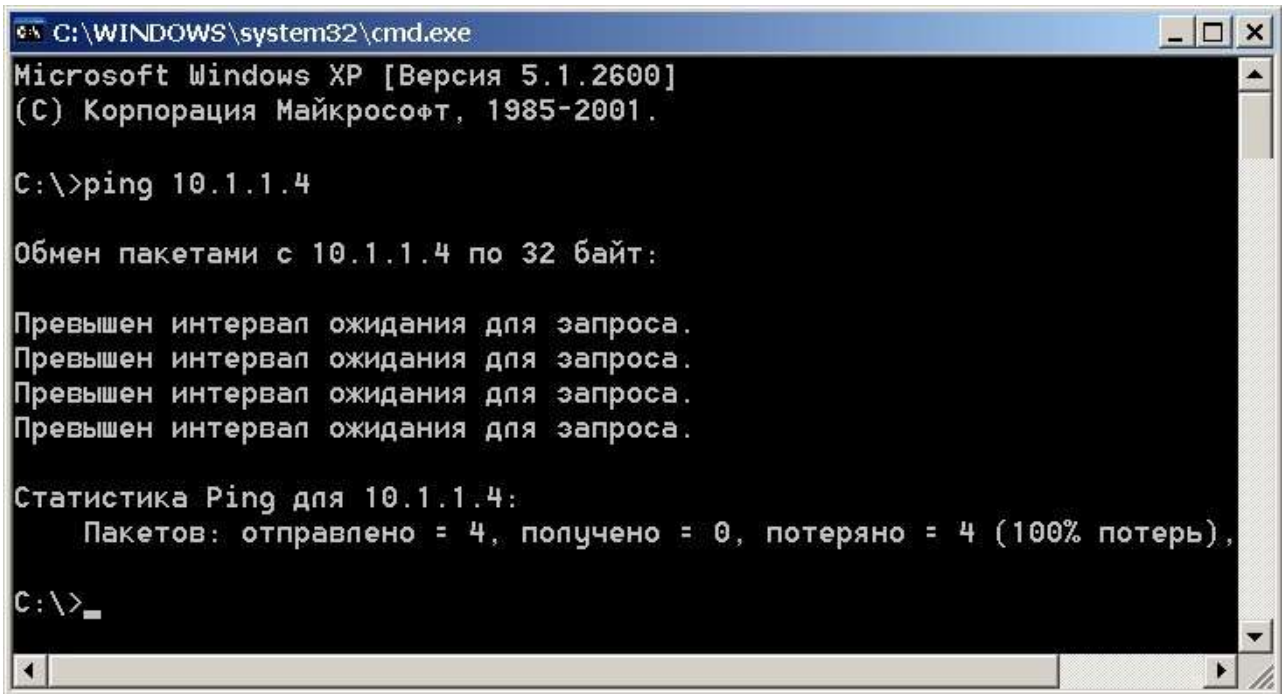


2. В открывшемся окне введите команду: `cmd.exe` и нажмите кнопку **ОК**.
3. Откроется окно интерфейса командной строки с заголовком: **C:\WINDOWS\system32\cmd.exe.**

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, то необходимо проверьте правильность настройки маршрутизации сети.



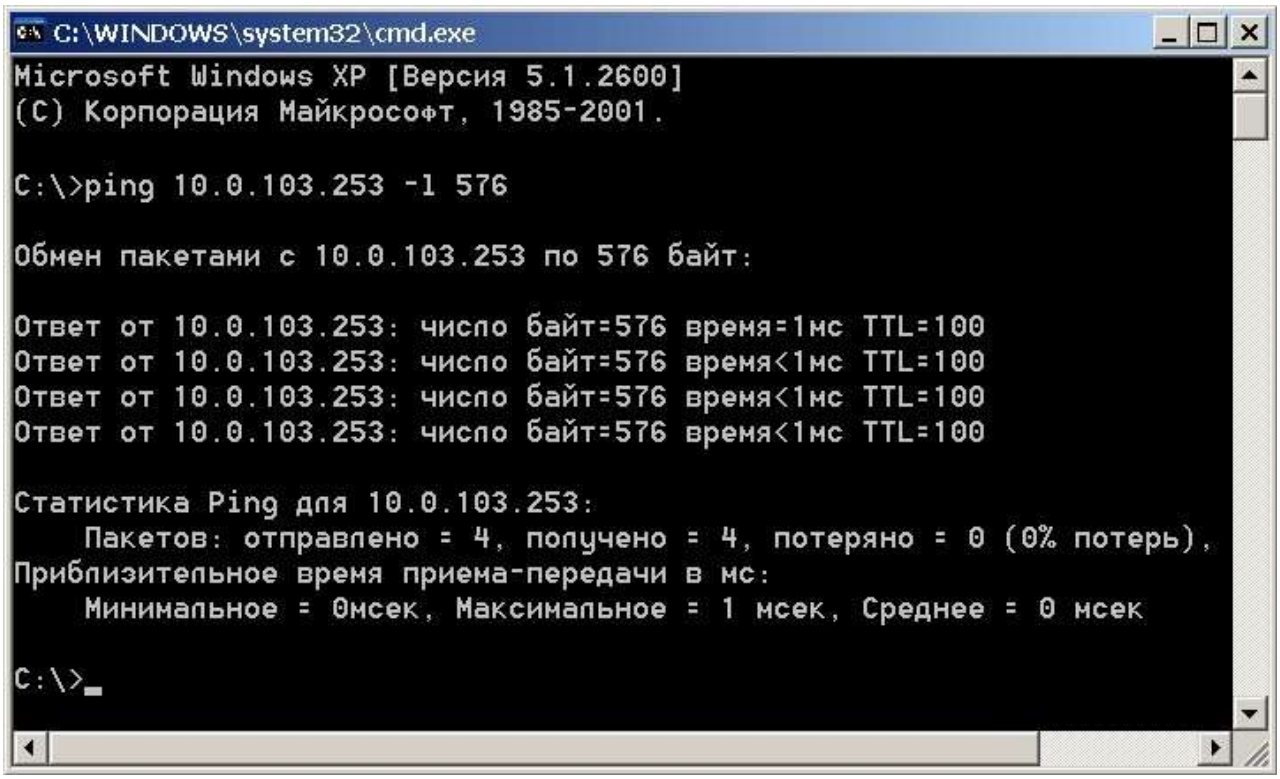
7. Контроллеры системы не поддерживают фрагментацию IP-пакетов. Поэтому необходимо удостовериться, что IP-пакеты на всем протяжении от сервера системы до контроллера не фрагментируются. Для этого введите ту же команду с

ключом `-l` и указанием на размер отправляемого пакета данных, например, 576 байт:

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

8. Если связь есть и размер отправленного пакета совпадает с размером, полученным в ответе, то можно утверждать, что IP-пакеты размером меньшим 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 ключем `-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»***.
- **Сервер видеоподсистемы –** сервер видеоподсистемы и ***«Центр управления видеоподсистемой»*** для работы с видеоархивом.
- **Сервер интеграции –** модуль предназначен для интеграции системы с интернет-ресурсом «Электронный дневник» (1dnevnik.ru) или аналогичным.
- **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.
- **Сервер интеграции с биометрической системой SUPREMA –** модуль обеспечивает интеграцию с биометрическими контроллерами компании ***«Suprema»***.

Внимание!

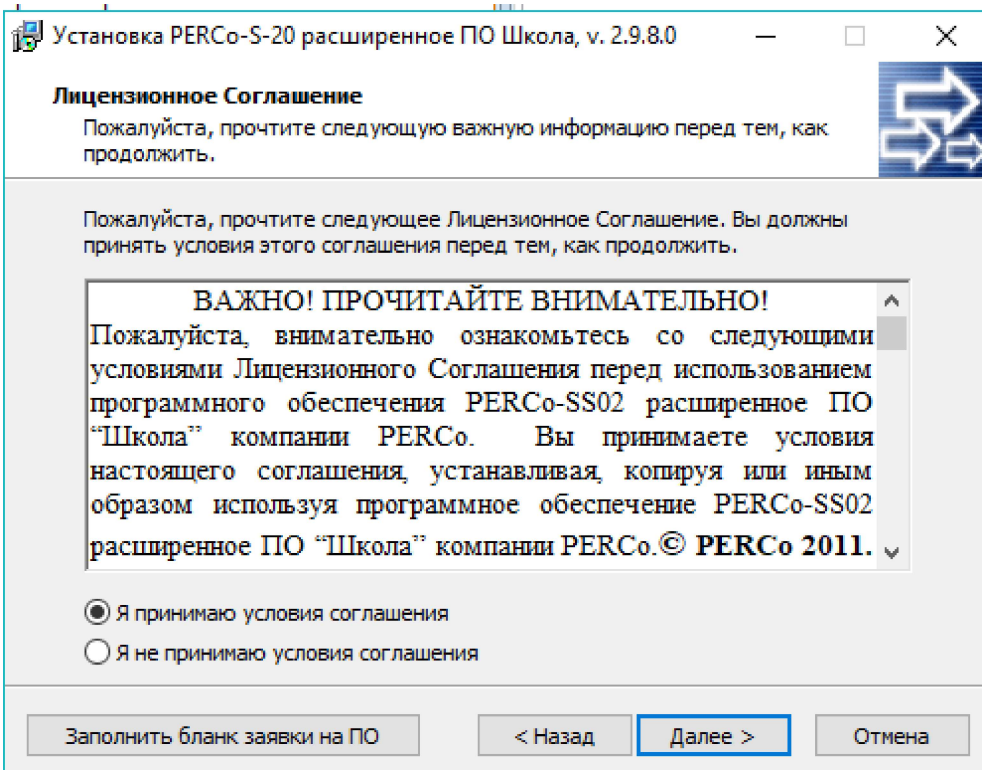
Модуль **Сервер интеграции с биометрической системой SUPREMA** обеспечивает интеграцию с биометрическими контроллерами, имеющими версию внутреннего ПО ("прошивку") не менее чем:

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

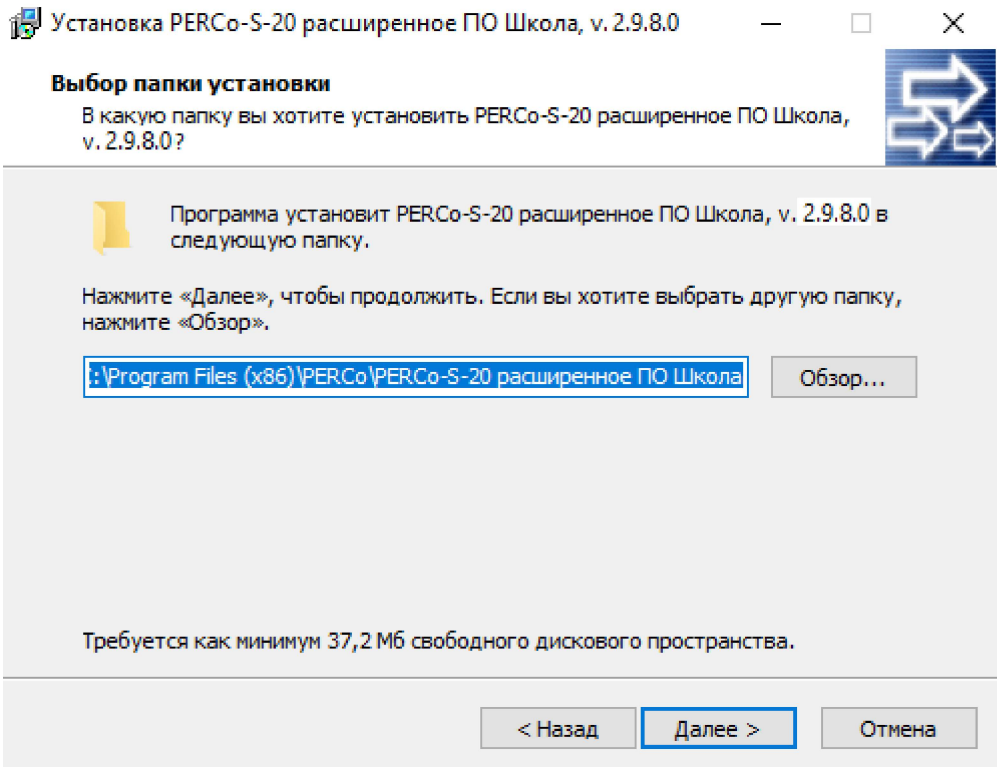
6.2. Установка

При установке ПО придерживайтесь следующей последовательности действий:

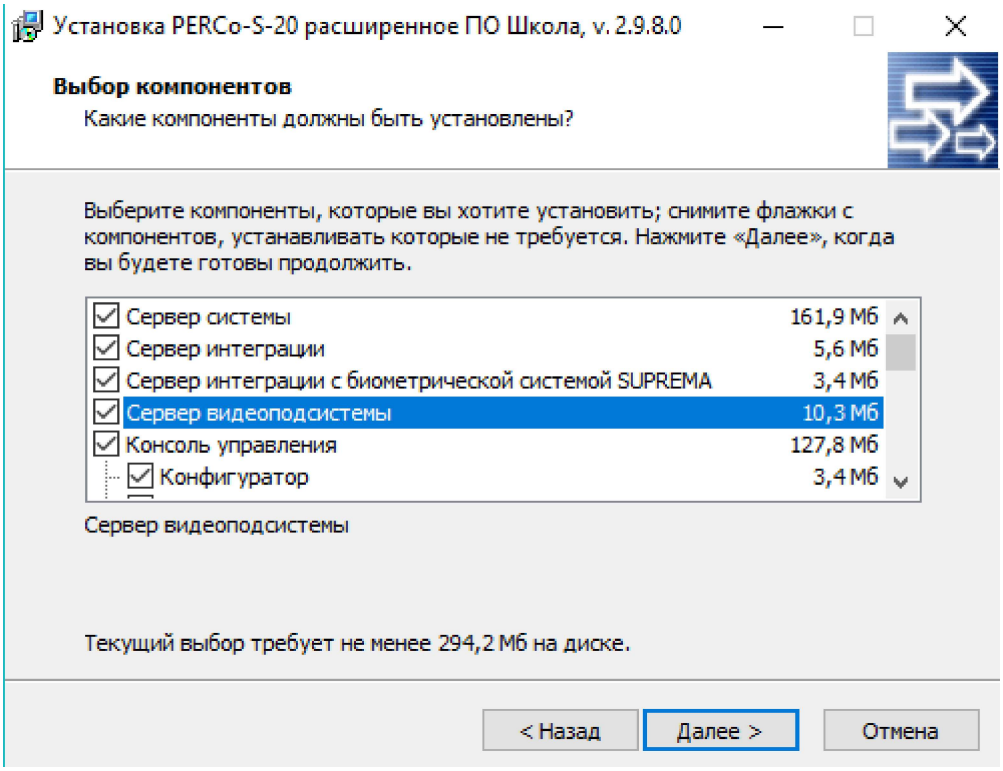
1. Запустите установочный файл `SetupSchoolBase.exe` или `SetupSchoolExtend.exe`. Следуйте указаниям мастера установки. Внимательно ознакомьтесь с предлагаемой информацией и лицензионным соглашением.



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:

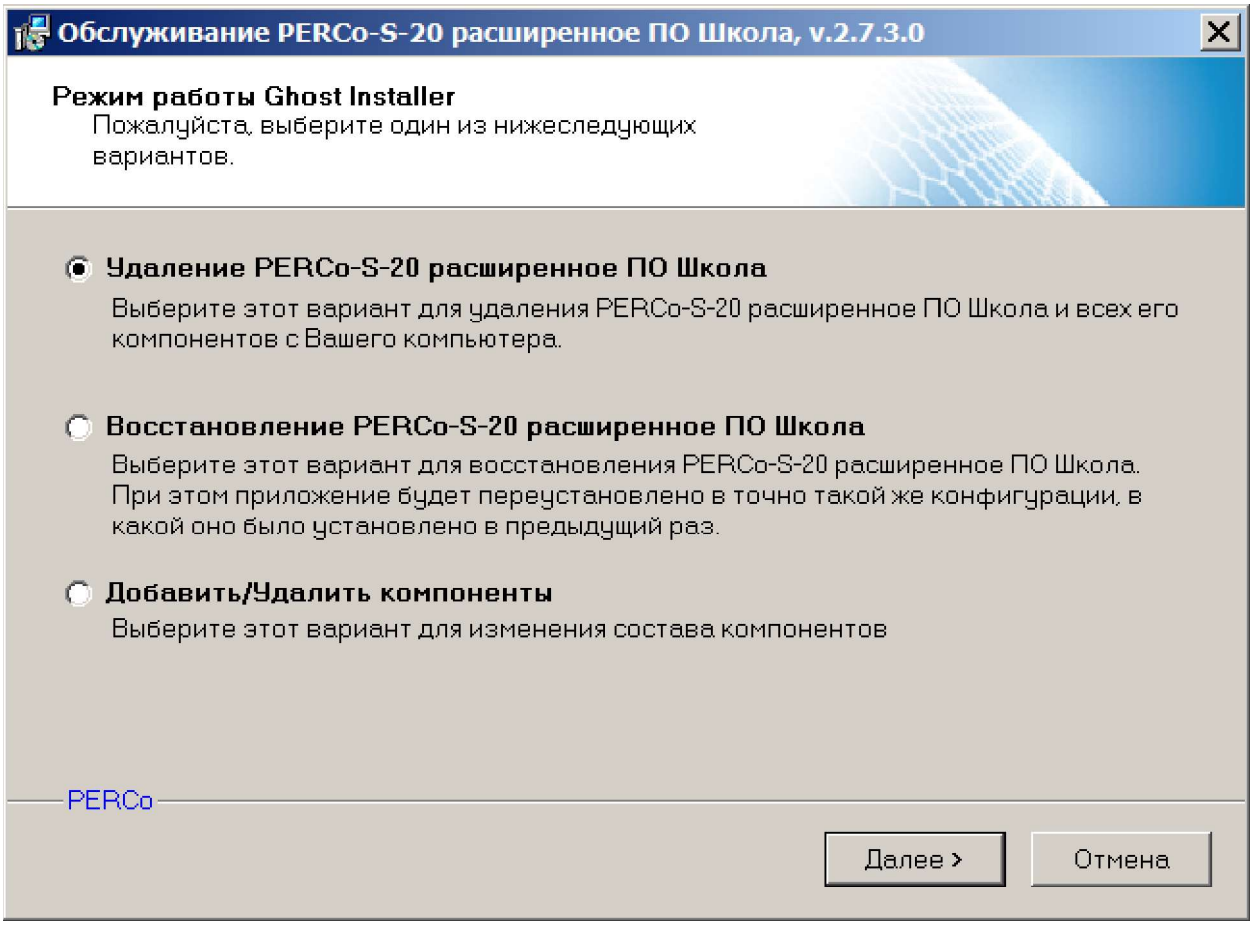
Если был отмечен для установки модуль **Сервер БД**, то перед установкой ПО системы будет запущен стандартный мастер установки SQL сервера *Firebird*.

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

6.3. Установка дополнительных модулей

Для изменения состава модулей сетевого ПО, установленных на ПК, произведите следующие действия:

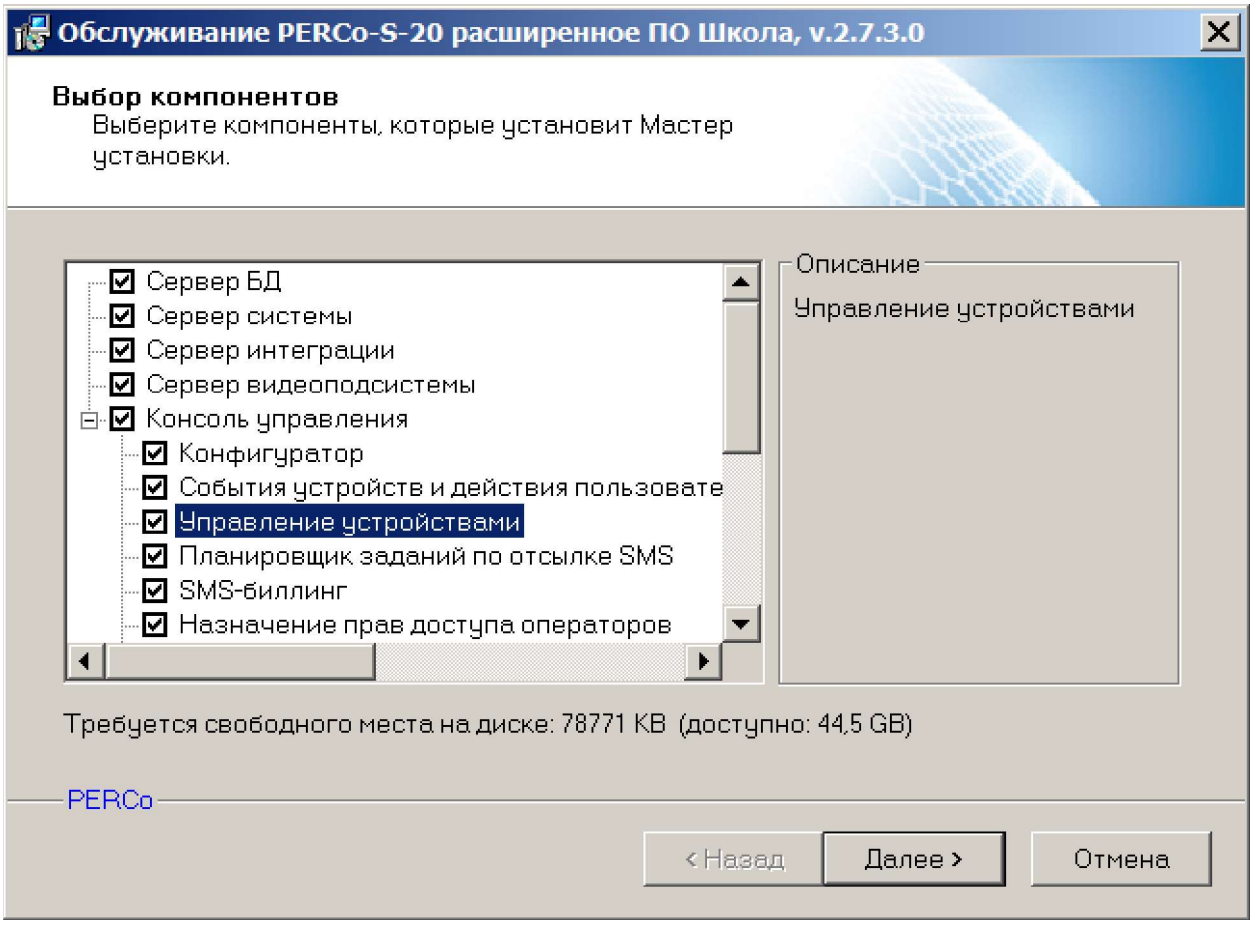
1. Запустите установочный файл `SetupCommon.exe`. Откроется окно **Обслуживание PERCo-S-20 Школа**:



2. В открывшемся окне установите переключатель в положение **Добавить / Удалить компоненты**. Нажмите кнопку **Далее**.

Примечание:

При установке переключателя в положение **Восстановление PERCo-S-20 Школа** все установленные ранее модули сетевого ПО будут переустановлены заново.



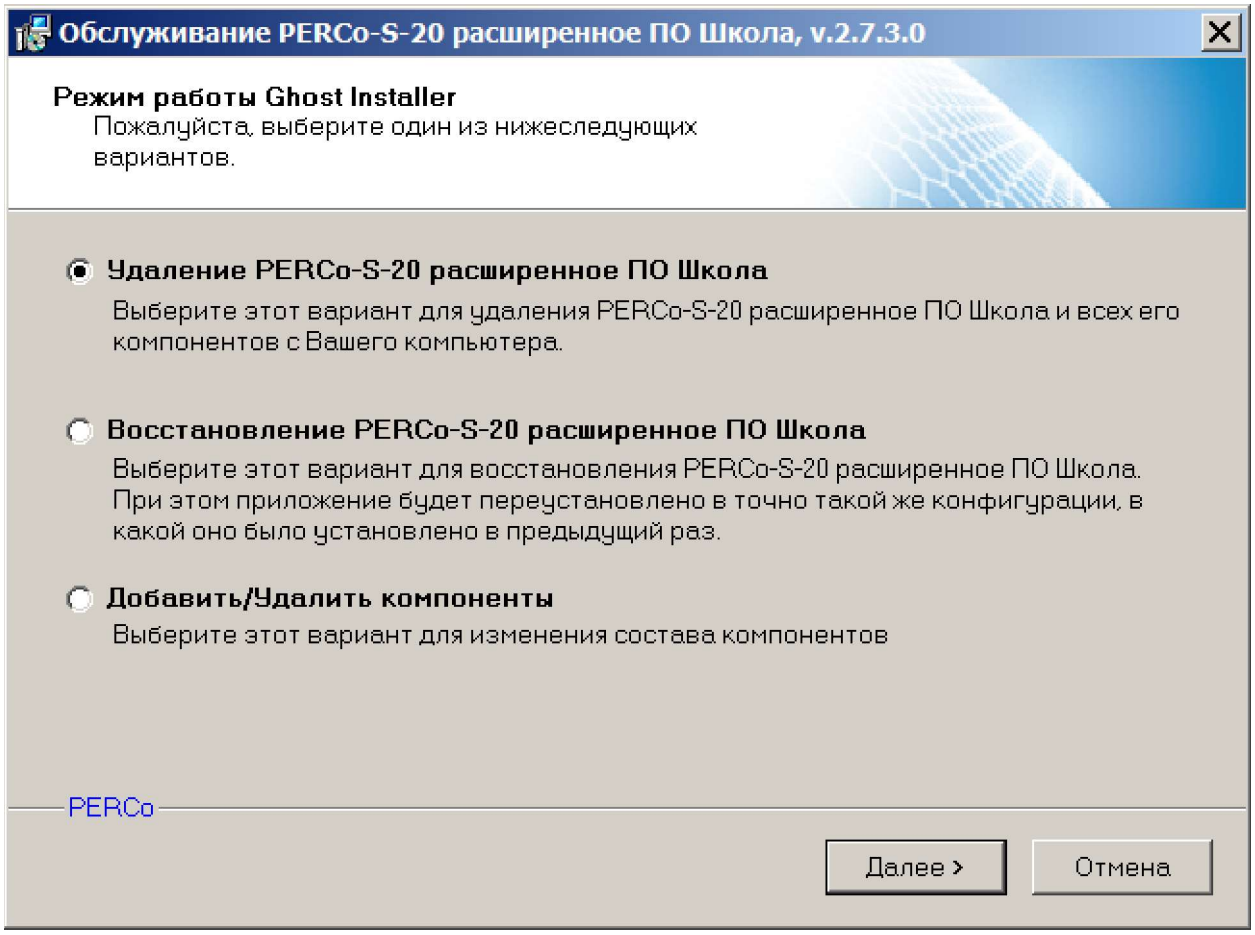
3. В открывшемся окне флажками отмечены установленные на ПК модули. Отметьте флажками модули и разделы ПО, которые должны быть установлены на ПК. При необходимости снимите флажки у тех модулей, которые необходимо удалить с ПК. Нажмите кнопку **Далее**.
4. После завершения установки ПО готово к работе.

6.4. Удаление

Для полного удаления всех модулей сетевого ПО с ПК используйте стандартный компонент *MS Windows «Установка и удаление программ»*. Для запуска компонента выберите последовательно **Пуск > Настройка > Панель управления > Установка и удаление программ**. В открывшемся окне выделите строку *«PERCo-S-20 Школа»* и нажмите кнопку **Удалить**.

Также для полного удаления всех модулей и разделов ПО с ПК можно использовать установочный файл, из которого ПО было установлено, для этого:

1. Запустите установочный файл `SetupSchoolBase.exe` или `SetupSchoolExtend.exe`. Откроется окно **Обслуживание PERCo-S-20 Школа**:



2. В открывшемся окне установите переключатель в положение **Удаление PERCo-S-20 Школа**. Нажмите кнопку **Далее**.
3. Все установленные модули сетевого ПО будут удалены с ПК.

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. Удалите все модули ПО, используя стандартный компонент *MS Windows «Установка и удаление программ»*.
2. Установите новую версию ПО. Для этого запустите установочный файл `SetupSchoolBase.exe` или `SetupSchoolExtend.exe`.

Примечание:

Актуальные версии установочных файлов модулей ***PERCo-SS01*** *«Базовое ПО»* и ***PERCo-SS02*** *«Расширенное ПО»* программного обеспечения ***PERCo-S-20 «Школа»*** можно загрузить с сайта компании ***PERCo***, расположенного по адресу www.perco.ru из раздела **Поддержка > Программное обеспечение**.

3. При необходимости после установки ПО обновите версию БД.

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.

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 модулей и разделов.

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

Примечание:

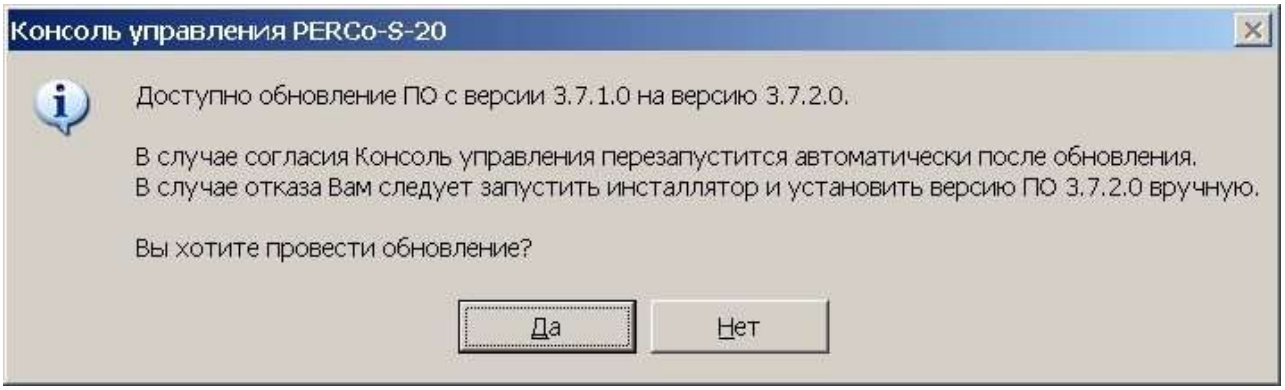
Для работы функции автоматического обновления ПО на ПК должны быть запущены следующие службы:

- *«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:

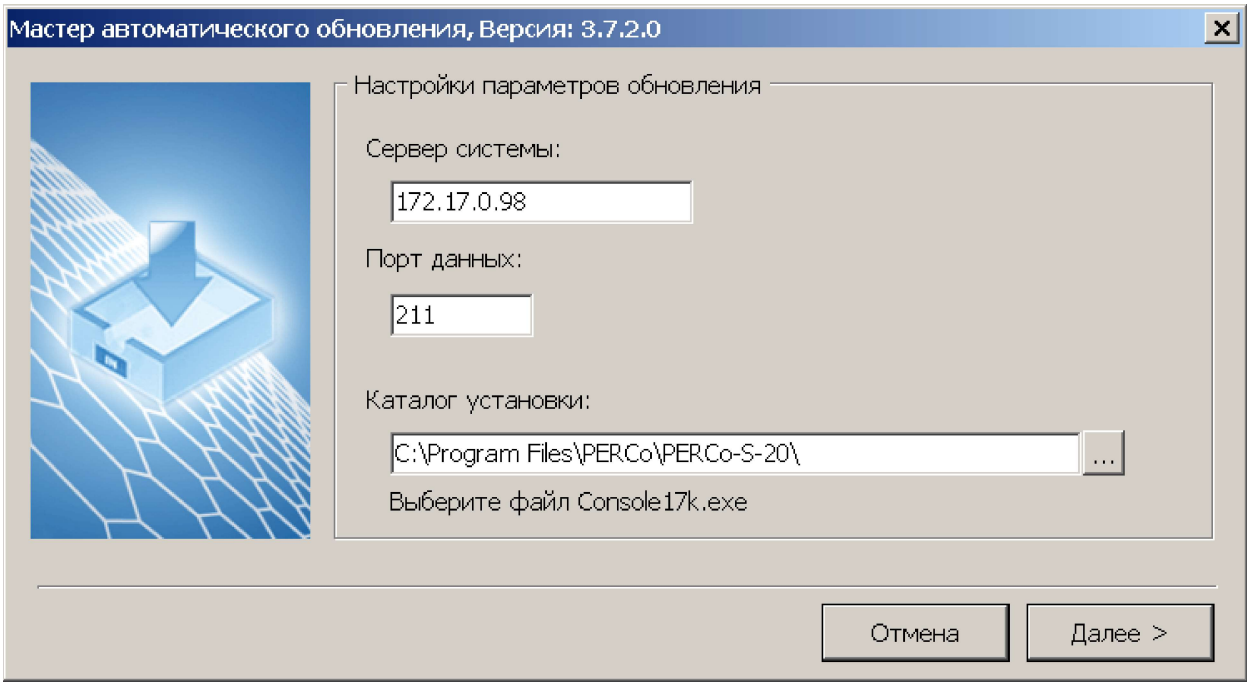
Если файл пакета обновления ПО был загружен ранее или вручную помещен в папку с установленным ПО (по умолчанию `C:\Program Files\PERCo\PERCo-S-20 базовое ПО Школа` или `C:\Program Files\PERCo\PERCo-S-20 расширенное ПО Школа`), то этап получения обновления от сервера системы будет пропущен.

6. При успешном завершении установки обновления появится окно с соответствующим сообщением, после чего будет автоматически запущена ***«Консоль управления»***.

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 базовое ПО Школа` или `C:\Program Files\PERCo\PERCo-S-20 расширенное ПО Школа`. 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.

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,
- управлением лицензиями на сетевые модули системы,
- создания, обслуживания и резервного копирования БД системы,
- настройки параметров рассылки сообщений,

9.1. Управление лицензиями

9.1.1. Приобретение лицензии

Сетевое ПО системы приобретается в составе модулей ***PERCo-SS01 «Базовое ПО»*** и ***PERCo-SS02 «Расширенное ПО»***. При этом каждый модуль состоит из 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:

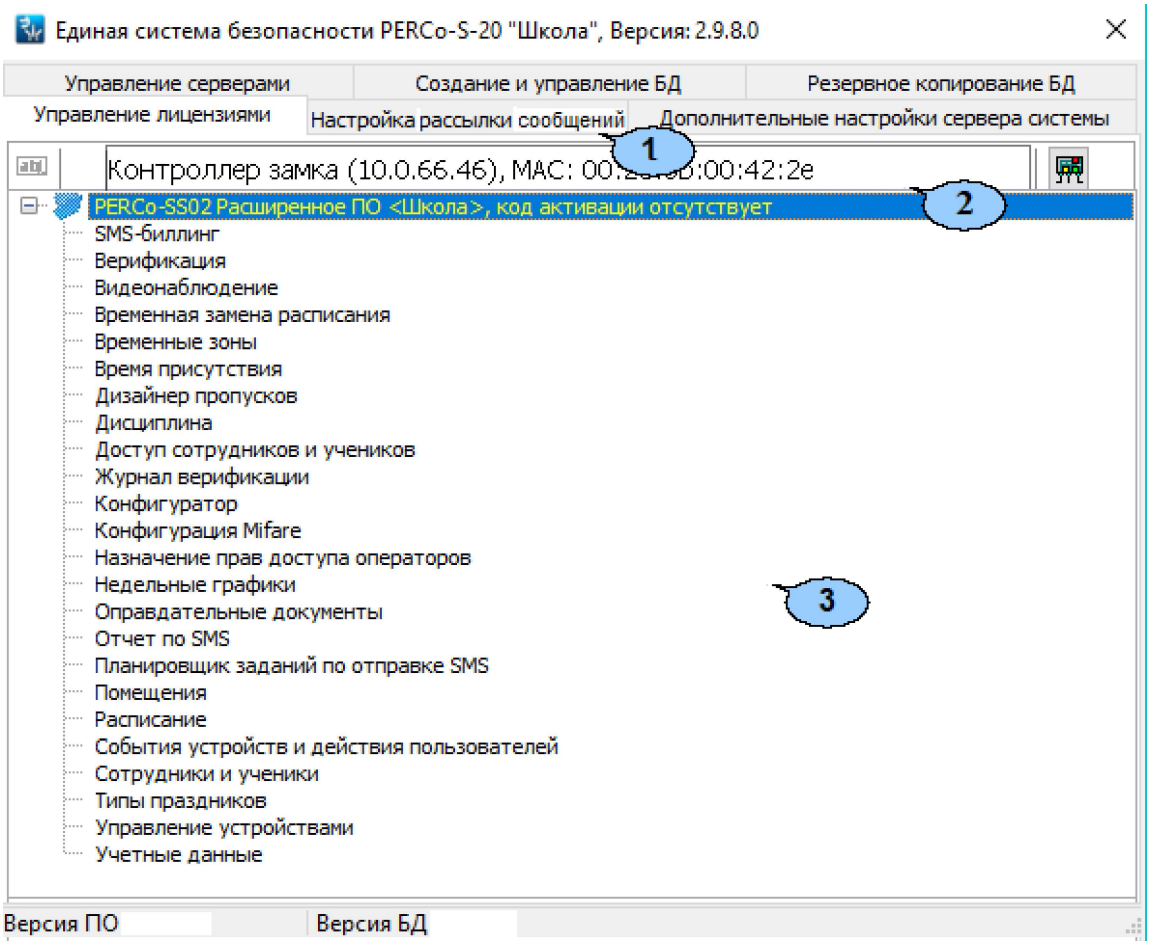
– На сайте компании ***PERCo***, по адресу www.perco.ru в разделе **Поддержка > Программное обеспечение > ПО PERCo-S-20 > Порядок получения права использования ПО PERCo-S-20 и PERCo-S-20 Школа.**

– Используя бланк заявки, сохраненный при установке ПО. Заполненный бланк необходимо отправить в компанию ***PERCo*** по адресу: market@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. Ввод ключа активации

10. Ввод ключей активации модулей сетевого ПО системы осуществляется на вкладке **Управление лицензиями** ПО ***«Центра управления»***. Вкладка имеет следующий вид:

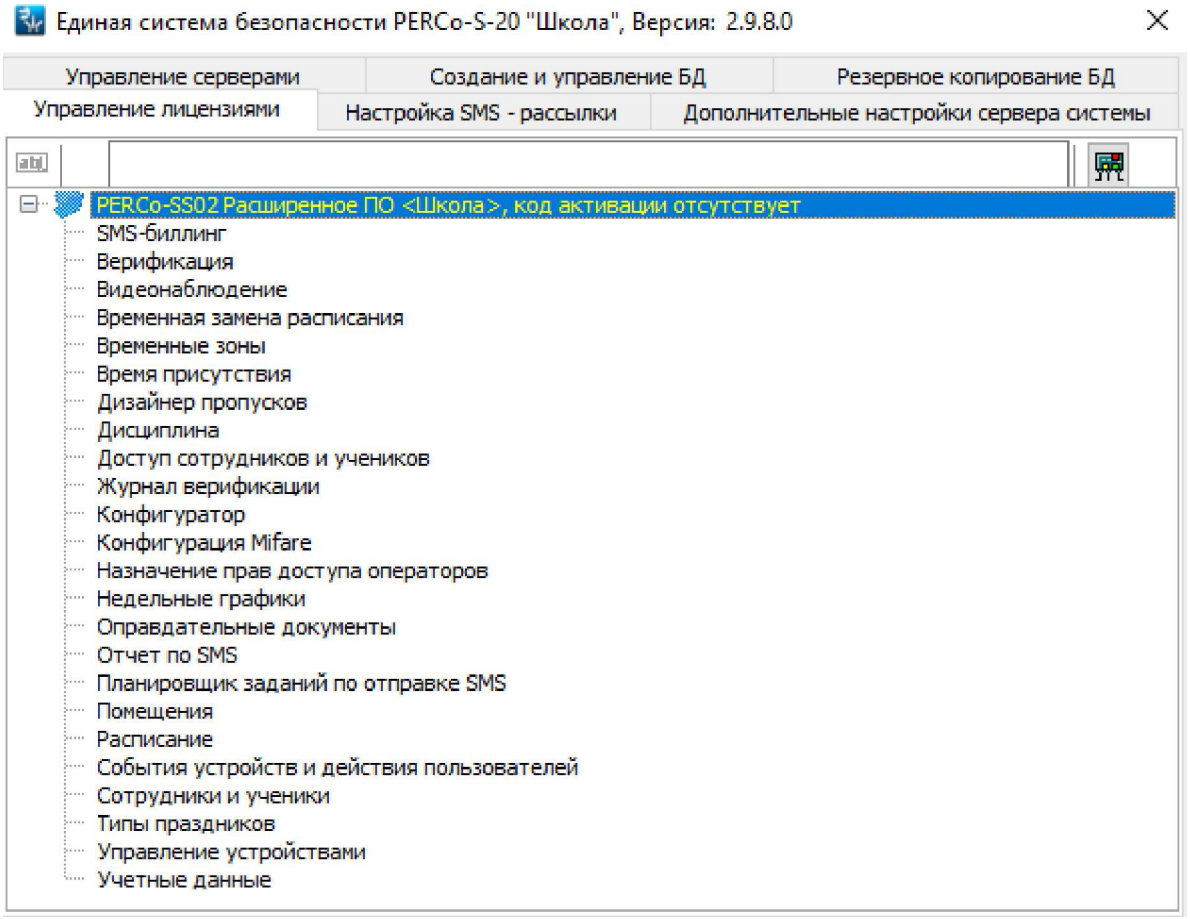


1. Выбор вкладки окна:
   - **Управление серверами**;
   - **Создание и управление БД**;
   - **Резервное копирование БД**;
   - **Управление лицензиями;**
   - **Настройка рассылки сообщений**;
   - **Дополнительные настройки сервера системы.**
2. Панель инструментов вкладки содержит следующие элементы:
   - **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.

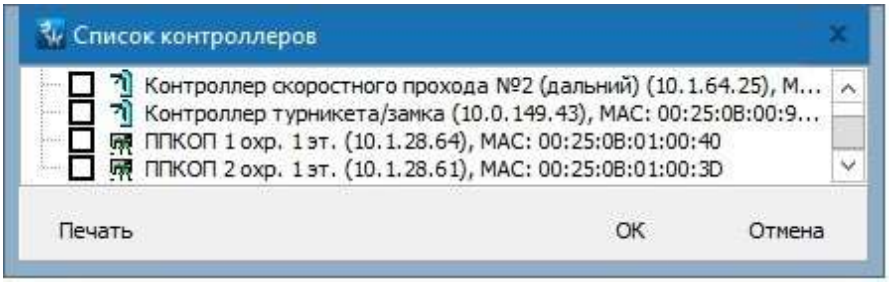
Ввод ключа активации

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 Школа.** После этого перейдите на вкладку **Управление лицензиями**:



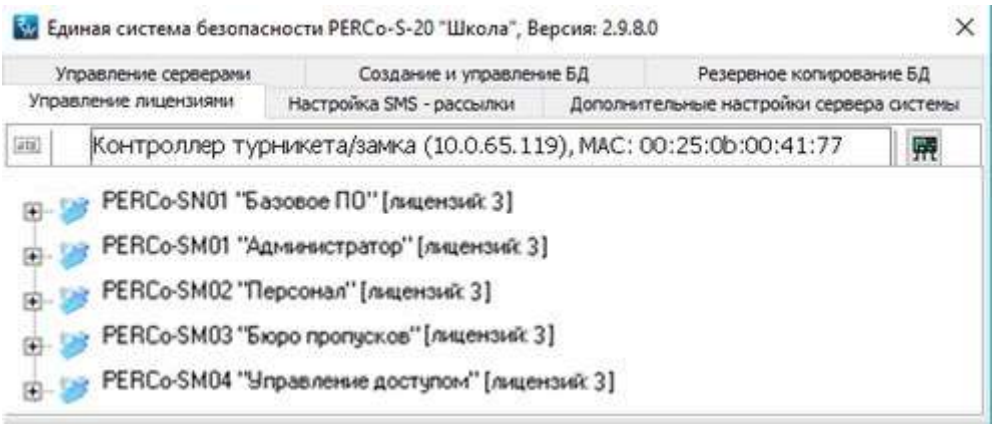
3. В верхней части окна нажмите кнопку  **Выбор контроллера, содержащего лицензию.** Откроется окно **Список контроллеров**:



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.

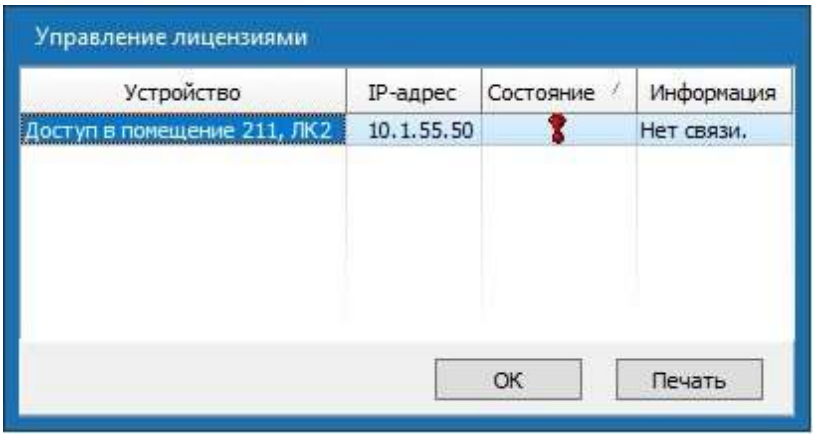
6. Нажмите кнопку **Изменить код активации** в верхней части окна. Откроется панель **Лицензионное соглашение** для ввода ключа активации выделенного модуля:

7. Введите ключ активации, указанный для выделенного модуля в лицензионном соглашении, без пробелов и разделителей. Нажмите кнопку **ОК**. Сервер системы осуществит проверку введенного ключа. При правильном вводе рядом с названием выделенного модуля появится информация о количестве приобретенных лицензий на АРМ с возможностью использования модуля, как показано в примере:



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:

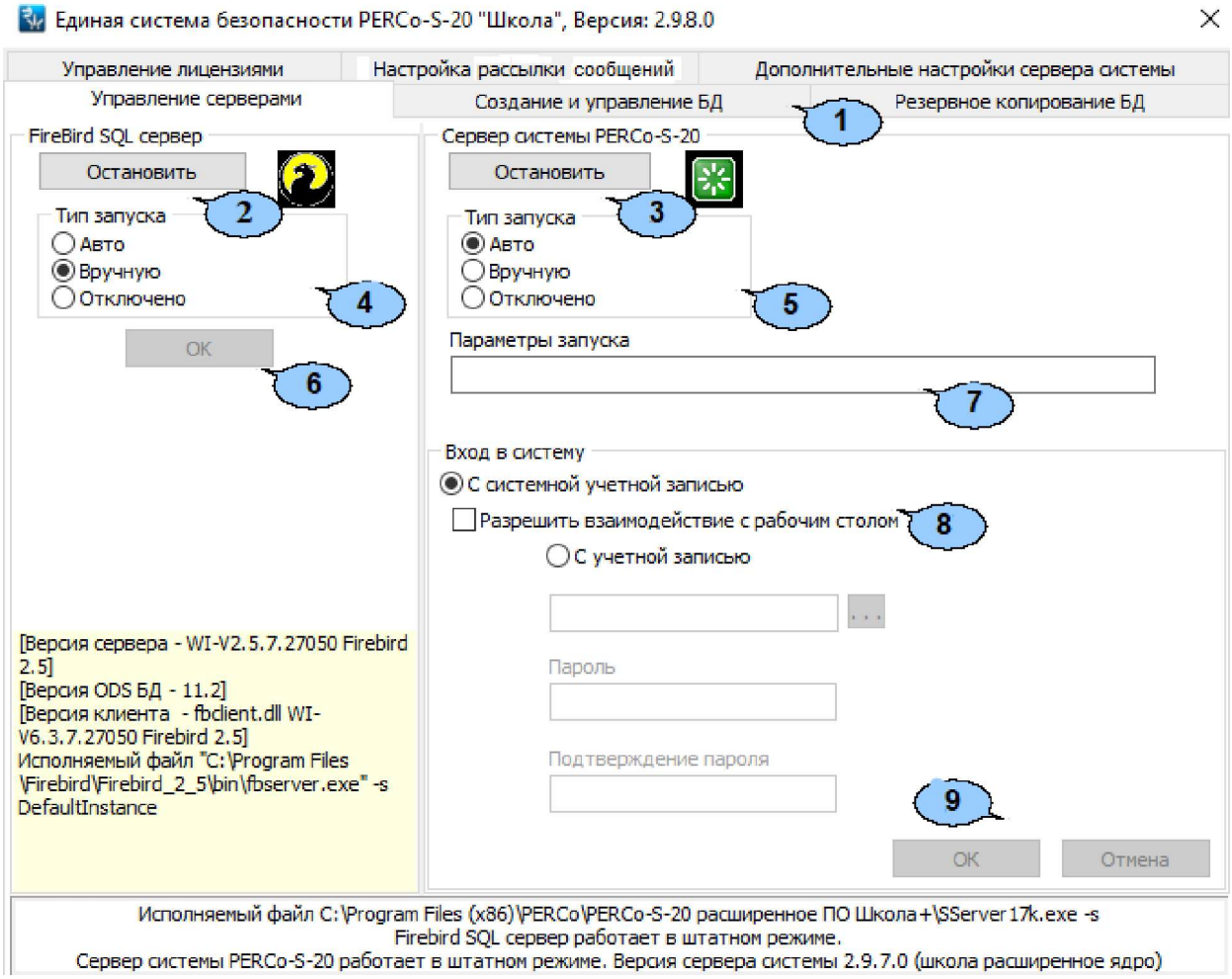


10. В открывшемся окне нажмите кнопку **ОК**. Проверьте наличие связи между сервером системы и контроллером, указанным в лицензионном соглашении. Повторно введите ключ активации, указанный в лицензионном соглашении для выделенного в рабочей области окна модуля.

10.1. Создание и управление БД

10.1.1. Запуск и остановка СУБД и сервера системы

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

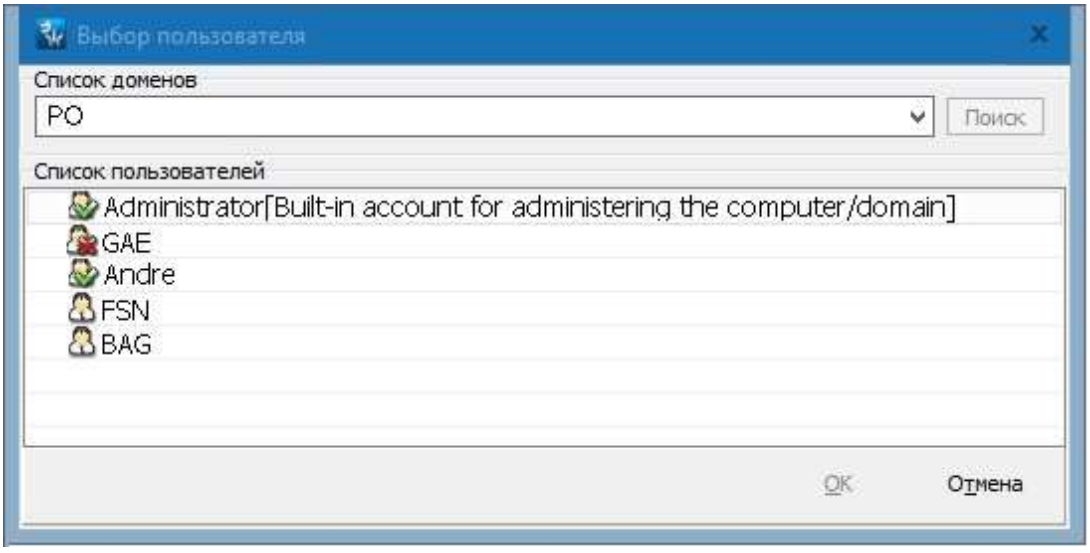


1. Выбор вкладки окна:
   - **Управление серверами;**
   - **Создание и управление БД;**
   - **Резервное копирование БД;**
   - **Управление лицензиями;**
   - **Настройка рассылки сообщений;**
   - **Дополнительные настройки сервера системы.**
2. Кнопка **Остановить / Запустить Firebird SQL сервер** 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.

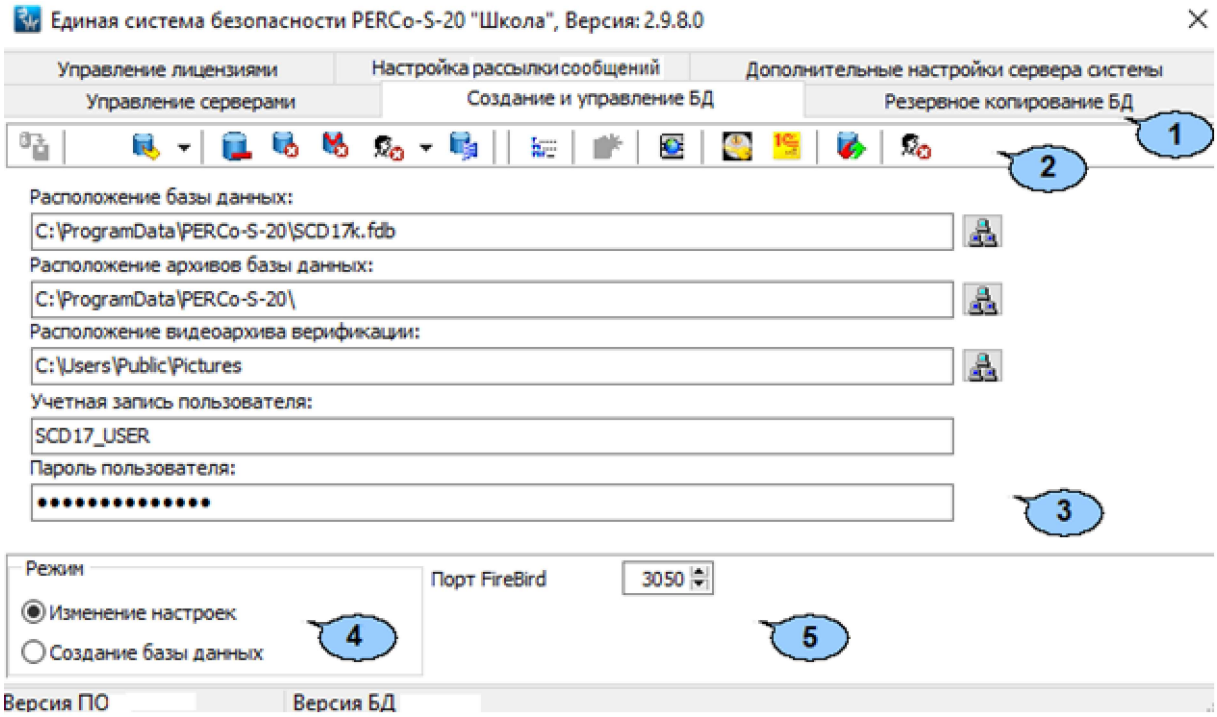
4. Переключатели **Тип запуска** позволяют установить способ запуска СУБД сервера. После изменения положения переключателей необходимо нажать кнопку **ОК**:
   - **Авто** – сервер будет запущен автоматически при запуске ОС.
   - **Вручную** – сервер запускается вручную с помощью кнопки **Запустить**.
   - **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 пользователя**:



9. Кнопки:
   - **ОК** – предназначена для сохранения внесенных на панели изменений,
   - **Отмена** – предназначена для отмены внесенных на панели изменений.

10.1.2. Описание вкладки «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.**
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 счёт 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 / учеников** – кнопка позволяет удалить из БД системы учетные данные удаленных сотрудников (учеников) за указанный период.

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.
- **Проверка целостности базы данных** (**Alt+B**) – кнопка позволяет проверить файл БД на наличие ошибок.

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 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 **Выбрать папку для архивов** 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 **Выбрать папку видеоархива верификации** справа от поля ввода.

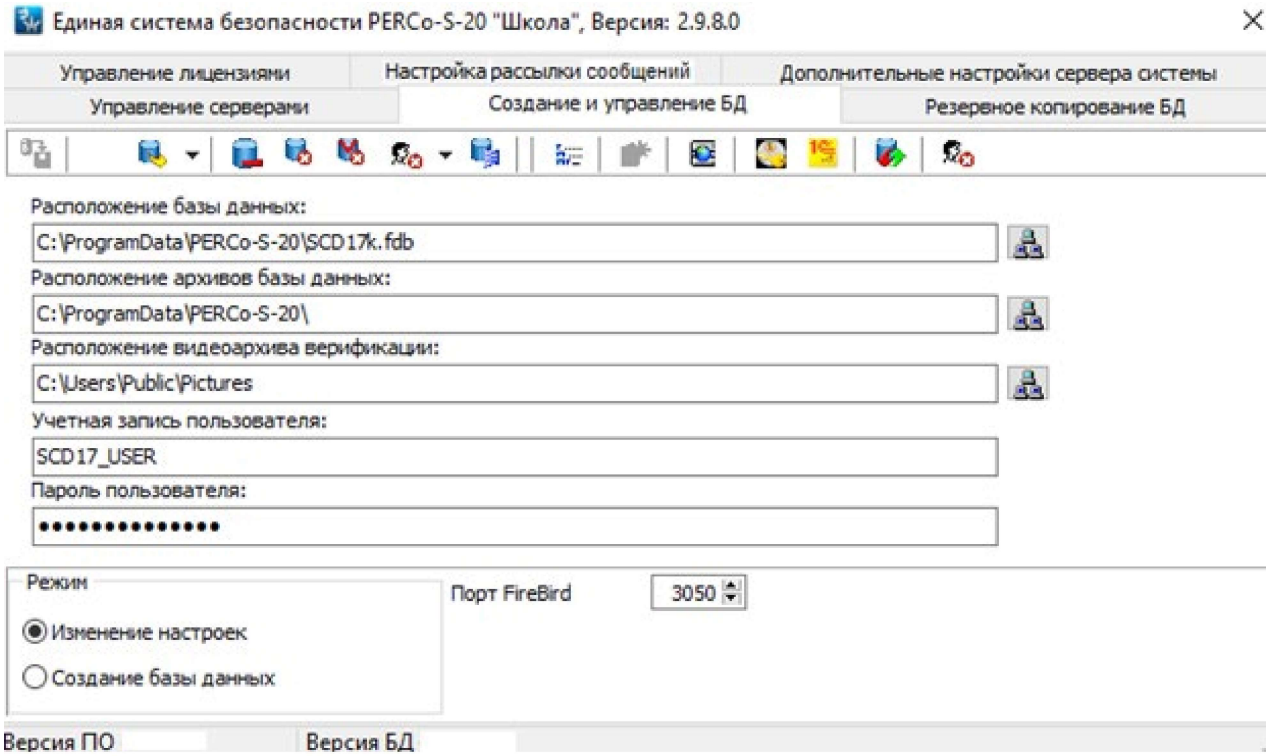
- **Учетная запись пользователя** – поле позволяет указать имя пользователя БД. Учетная запись пользователя задается при создании БД и указывается в случае смены используемой БД. Учетная запись по умолчанию: `SCD17_USER`.
- **Пароль пользователя** – поле позволяет указать пароль для доступа к БД. Пароль 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`.

10.1.3. 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 Школа** запущены.
3. Перейдите на вкладку **Создание и управление БД**.
4. На панели **Режим** установите переключатель в положение **Создание базы данных**. Вкладка примет следующий вид:

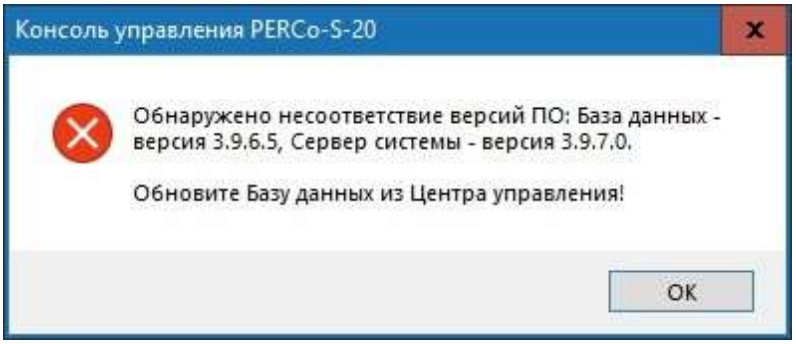


5. В поле **Расположение базы данных** укажите папку, в которой будет создан файл БД. Путь к папке может быть введен вручную или указан в окне **Обзор папок**. Для открытия окна нажмите кнопку  **Укажите файл БД**, справа от поля ввода. Для повышения безопасности не рекомендуется предоставлять общий 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 **Выбрать папку для архивов** справа от поля ввода и укажите папку в открывшемся окне **Обзор папок**.
7. В поле **Расположение видеоархивов 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 **Выбрать папку 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**.

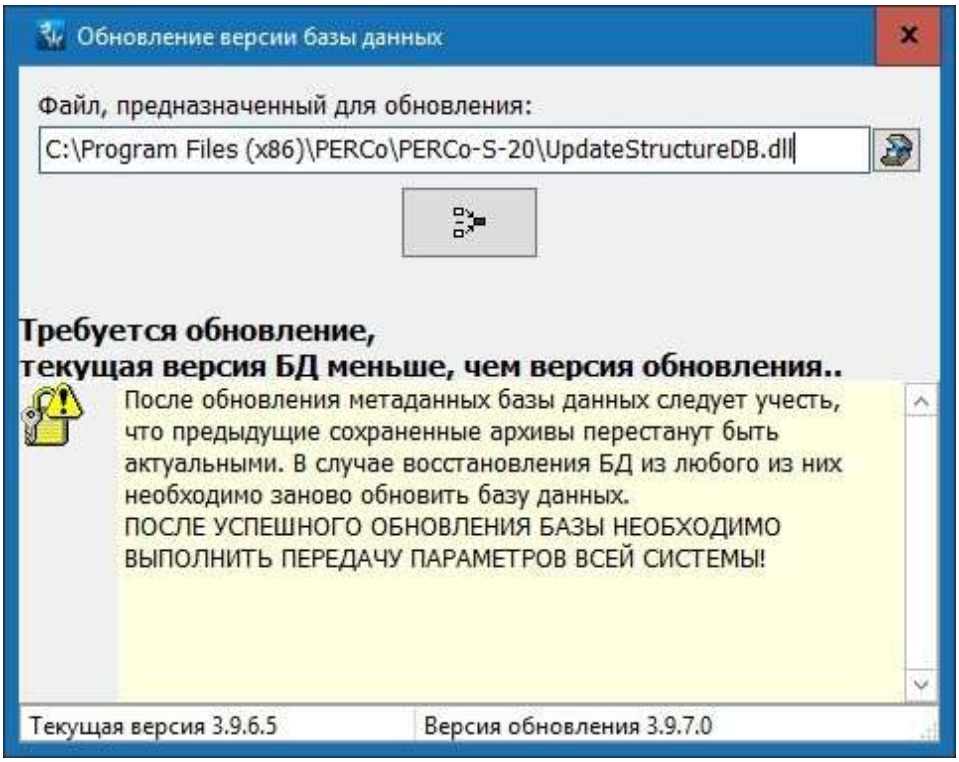
10.1.4. Обновление версии БД

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:



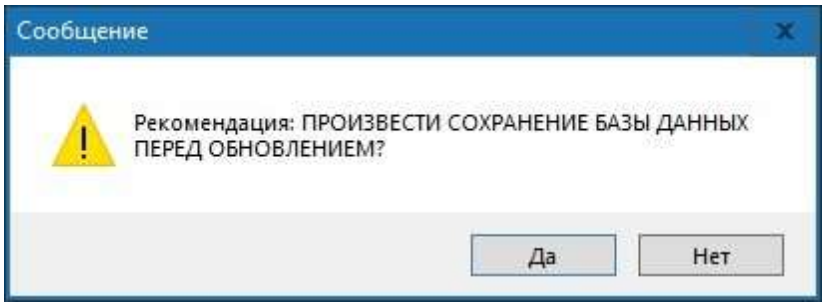
Для обновления версии БД выполните следующие действия:

1. Запустите ***«Центр управления»*** и перейдите на вкладку **Создание и управление БД**.
2. На панели инструментов вкладки нажмите кнопку **Обновление версии базы данных**. Откроется окно **Обновление версии базы данных**:



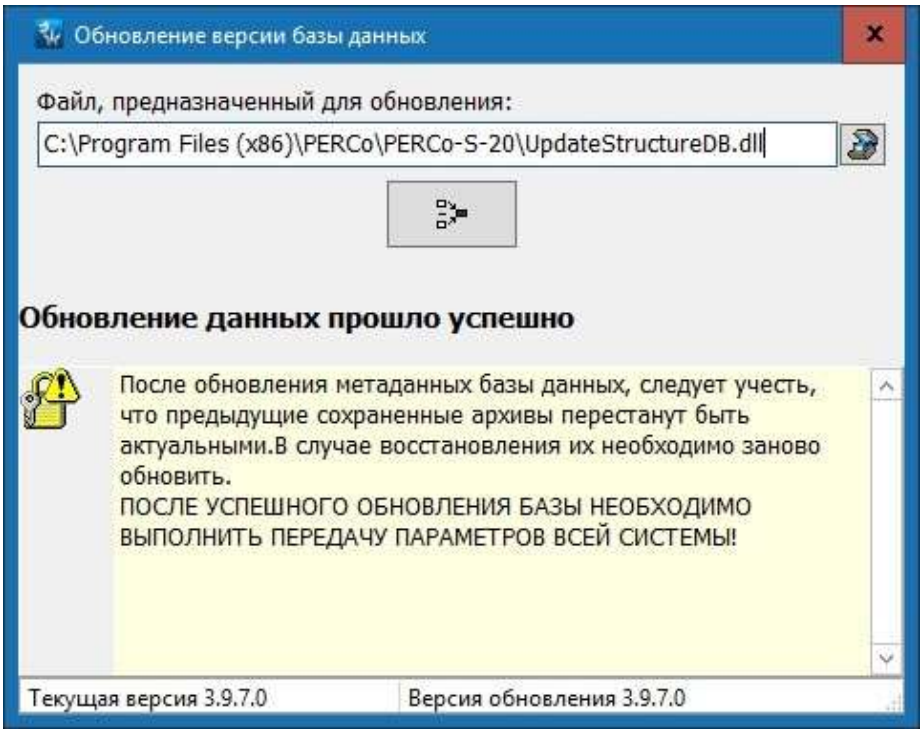
3. В открывшемся окне для изменения пути к файлу `UpdateStructureDB.dll` нажмите кнопку  .

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



5. 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**.

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



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

10.1.5. 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.

10.1.6. 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.

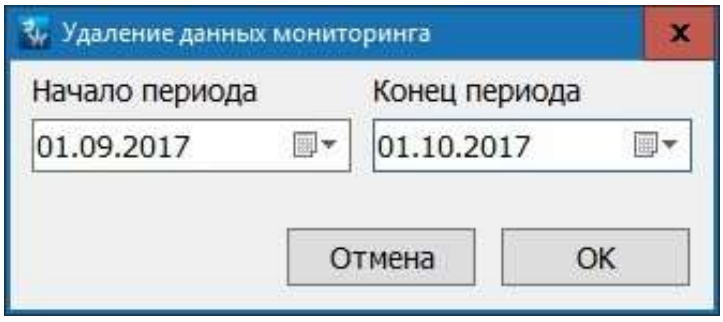
Таким образом, при нормальной работе в папке, указанной в поле **Расположение базы данных**, могут существовать два файла БД: рабочая и предыдущая копия, а также резервная копия БД в папке, указанной в поле **Расположение архивов базы данных**.

10.1.7. 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**:



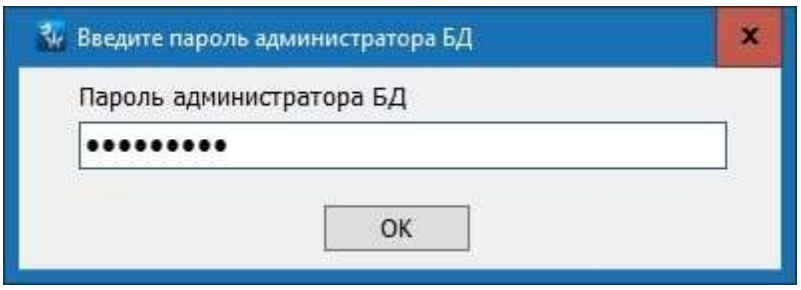
3. В открывшемся окне установите с помощью полей ввода дат **Начало периода** и **Конец периода** временной промежуток, за который будут удалены события. Нажмите кнопку **ОК**. События из журнала мониторинга будут удалены.
4. Для удаления событий регистрации на панели инструментов вкладки нажмите кнопку **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.

10.1.8. Настройки сервера БД

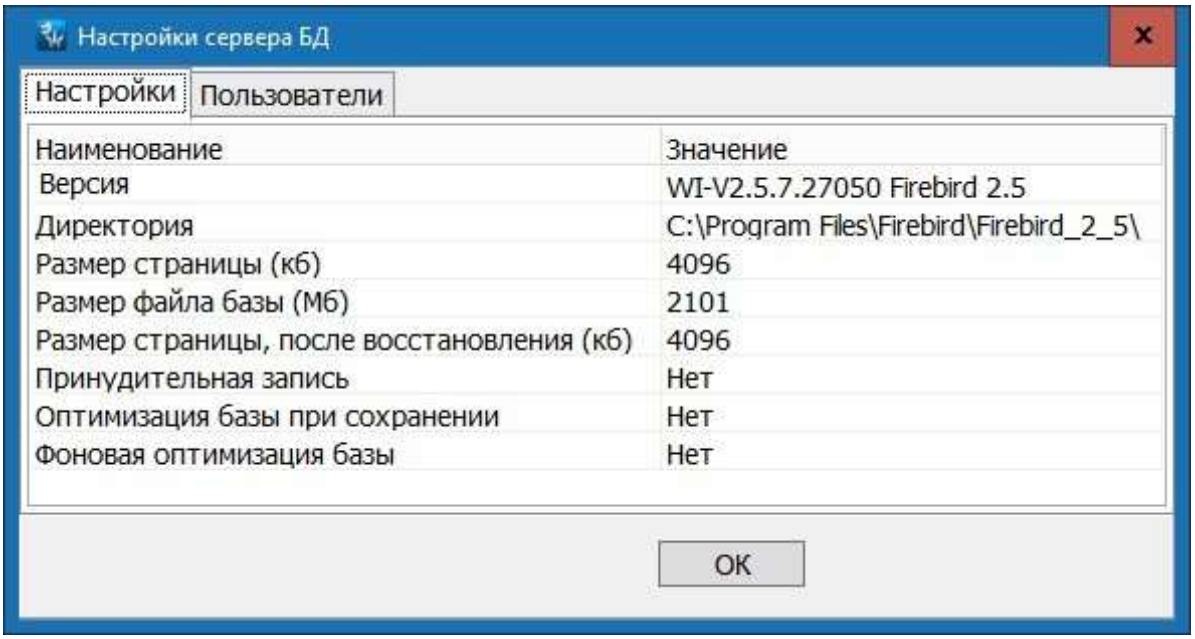
Для доступа к настройкам сервера БД:

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:

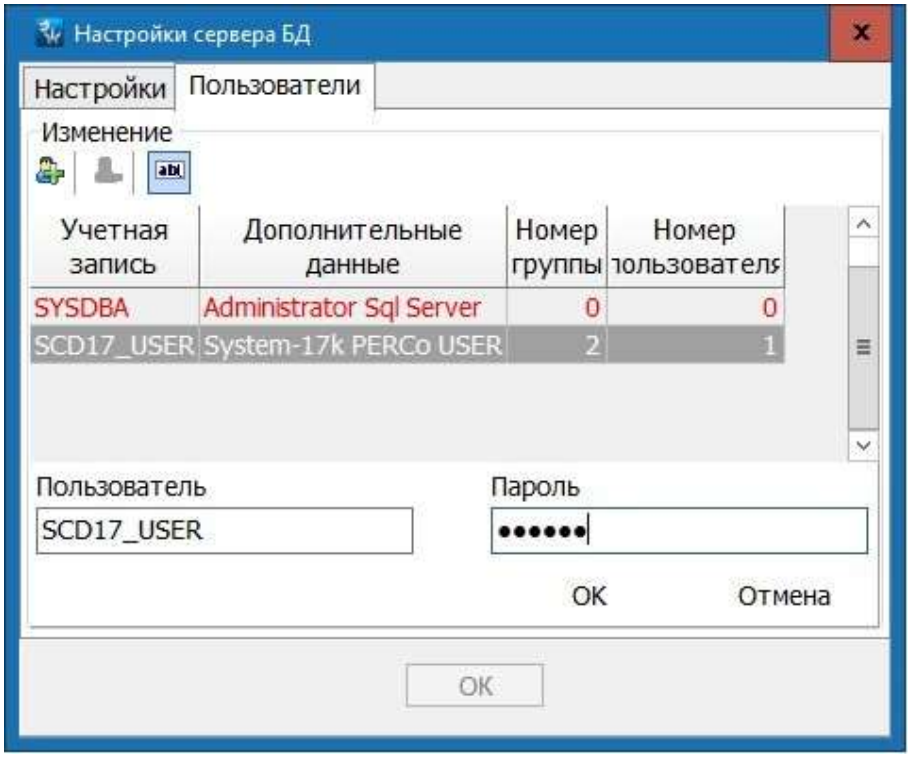


Рабочая область вкладки **Настройки** содержит следующие поля с данными и параметры сервера СУБД:

- **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.

10.1.9. Восстановление предыдущего пароля устройств

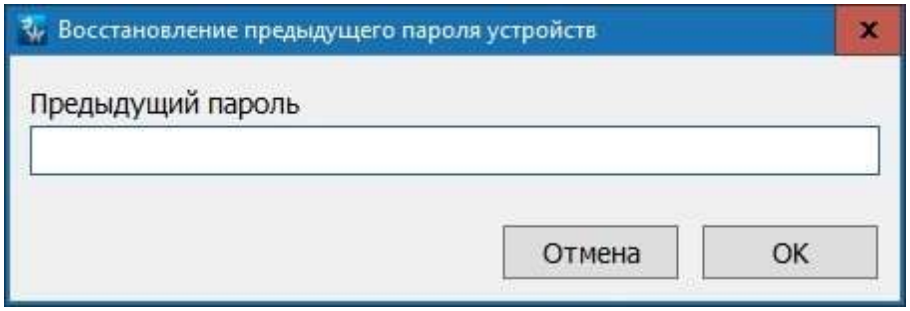
Восстановление предыдущего пароля доступа к устройствам системы может потребоваться после восстановления БД из резервной копии, в случае если после создания резервной копии пароль был изменен. То есть если пароль, сохраненный в устройствах, отличается от пароля, используемого в БД.

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**:



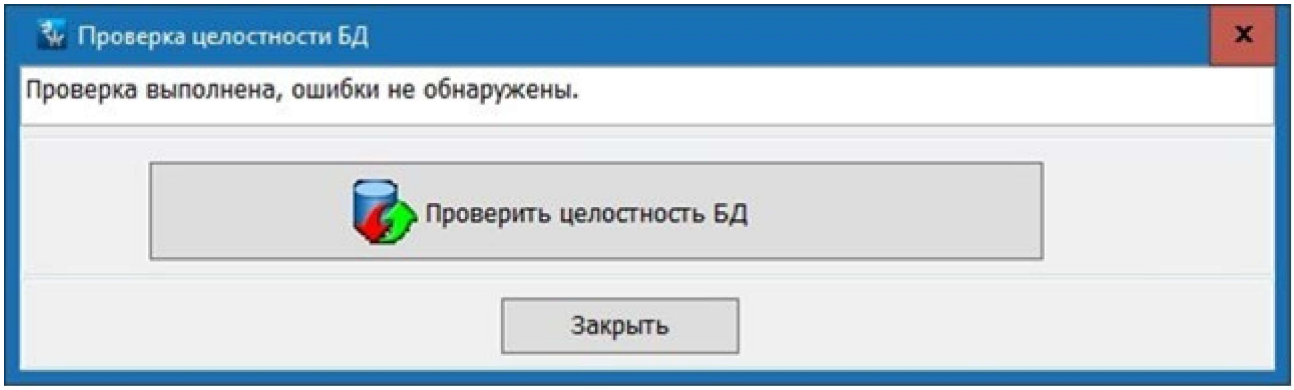
3. В открывшемся окне в поле **Предыдущий пароль** введите пароль, сохраненный в устройствах системы, то есть используемый до восстановления БД. Нажмите на кнопку **ОК**.
4. В открывшемся окне подтверждения изменения пароля нажмите кнопку **Да**. После проведения процедуры восстановления в системе будет 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**.

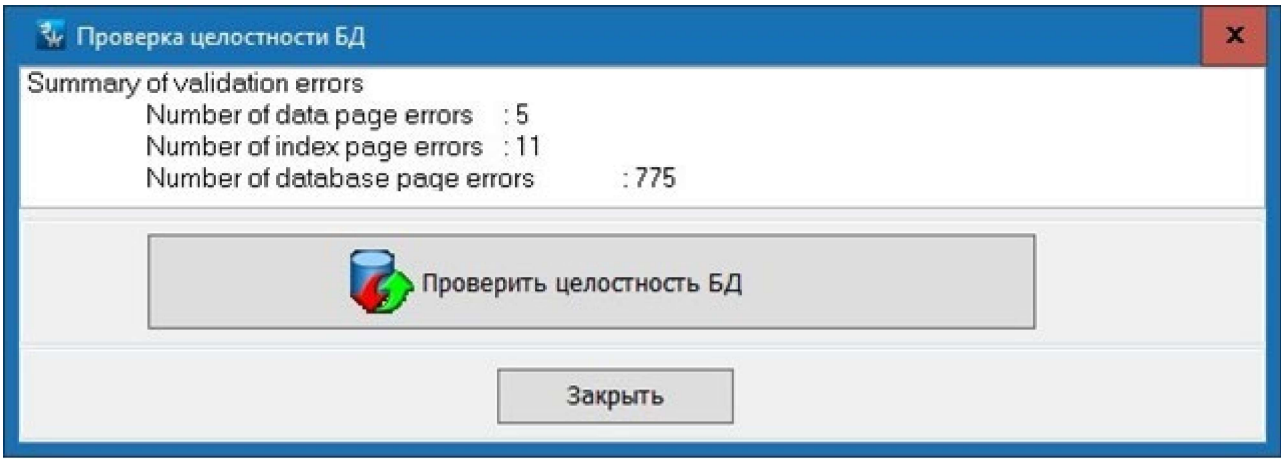
10.1.10. Проверка целостности БД

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.

10.2. Планировщик резервного копирования БД

10.2.1. Описание вкладки «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.

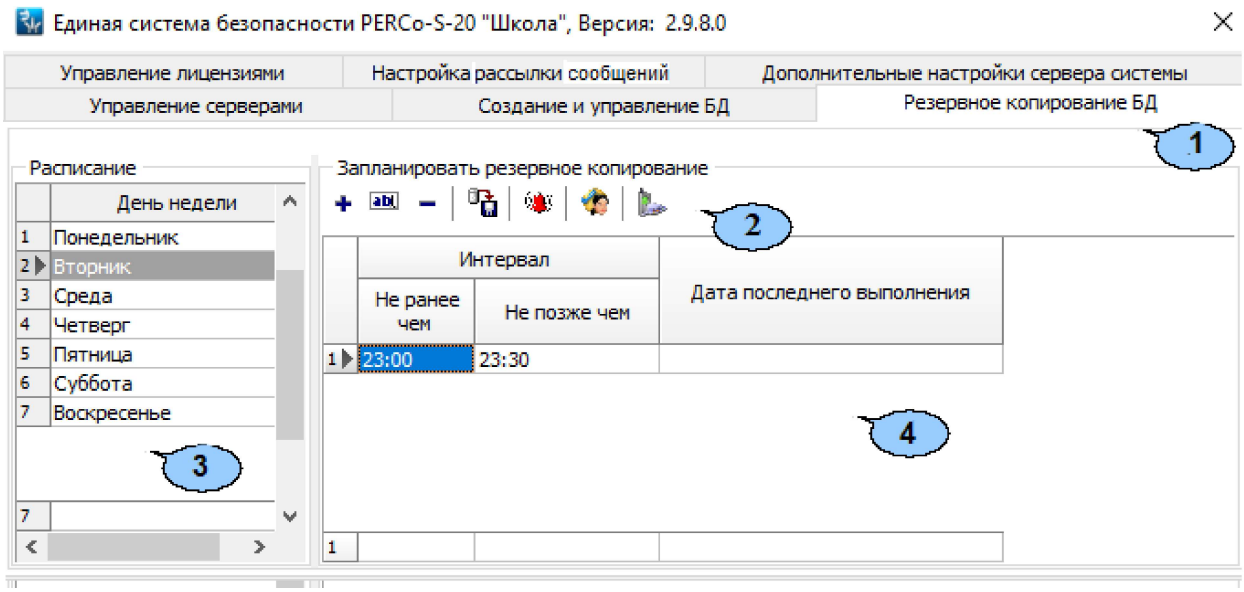
Для немедленного создания резервной копии БД перейдите на вкладку **Создание и управление БД** и нажмите кнопку **Сохранение базы данных** на панели инструментов вкладки.

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.**

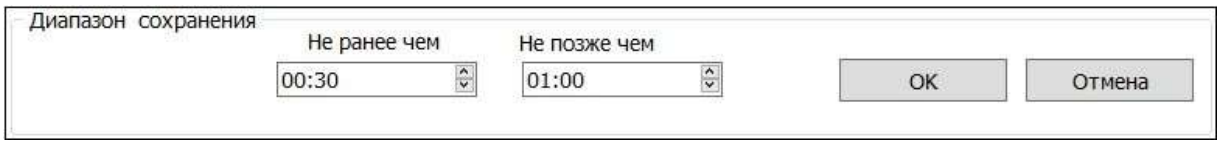
2. Панель инструментов вкладки:
   - **Добавление** (**Ctrl+N**) – кнопка позволяет установить время создания резервной копии БД для дня недели, выбранного на панели **Расписание**.
   - **Редактирование** (**Ctrl+E**) – кнопка позволяет изменить время резервного копирования БД, выделенное в рабочей 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.

10.2.2. 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.

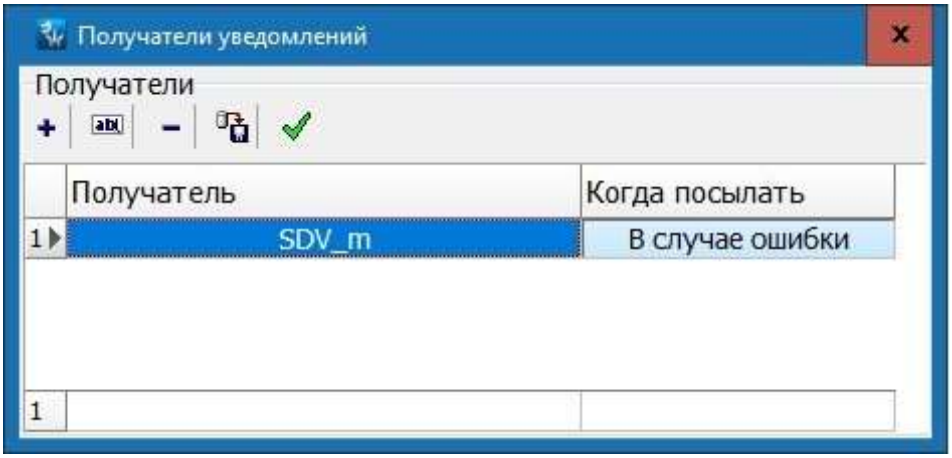
5. При необходимости добавьте дополнительные интервалы времени резервного копирования.
6. Для изменения временного интервала выделите его в рабочей области вкладки и нажмите на панели инструментов вкладки кнопку **Редактирование**. На открывшейся панели **Диапазон сохранения** произведите необходимые 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.

10.2.3. 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.

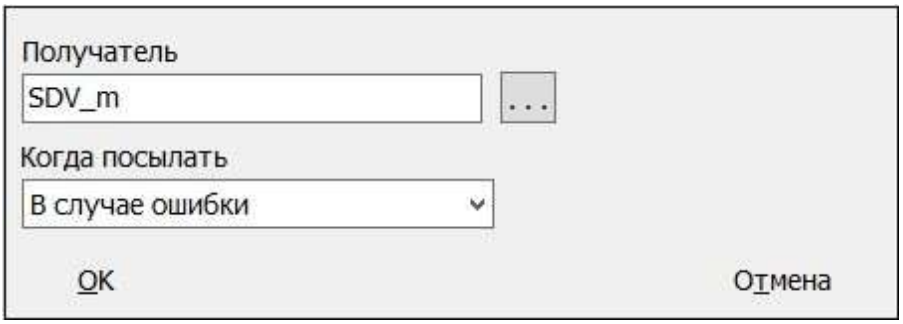
Инструменты панели **Получатели**:

- **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.

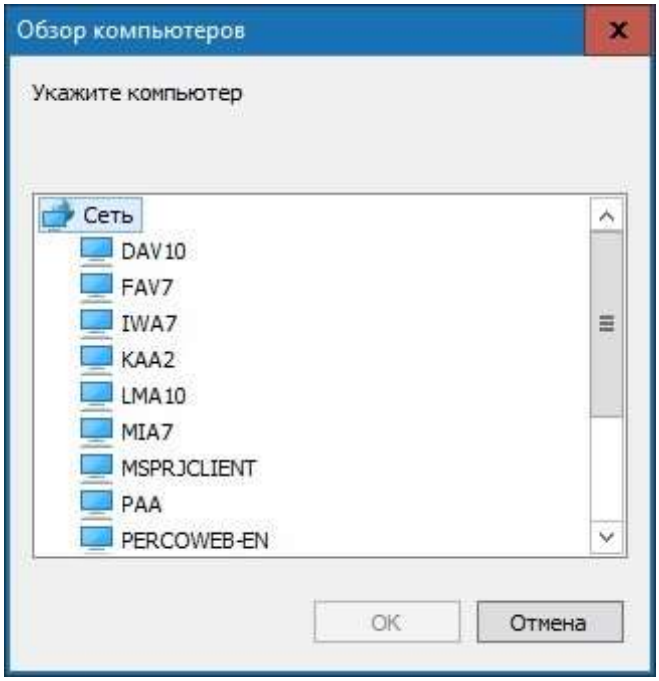
- **Удалить получателя** (**Ctrl+D**) – кнопка позволяет удалить выделенный в рабочей области окна ПК из списка получателей уведомлений.
- **Сохранить данные** (**Ctrl+S**) – кнопка позволяет сохранить изменения в списке получателей.
- **Тестирование уведомлений** (**Ctrl+T**) – кнопка позволяет протестировать 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. Откроется окно **Обзор компьютеров**:



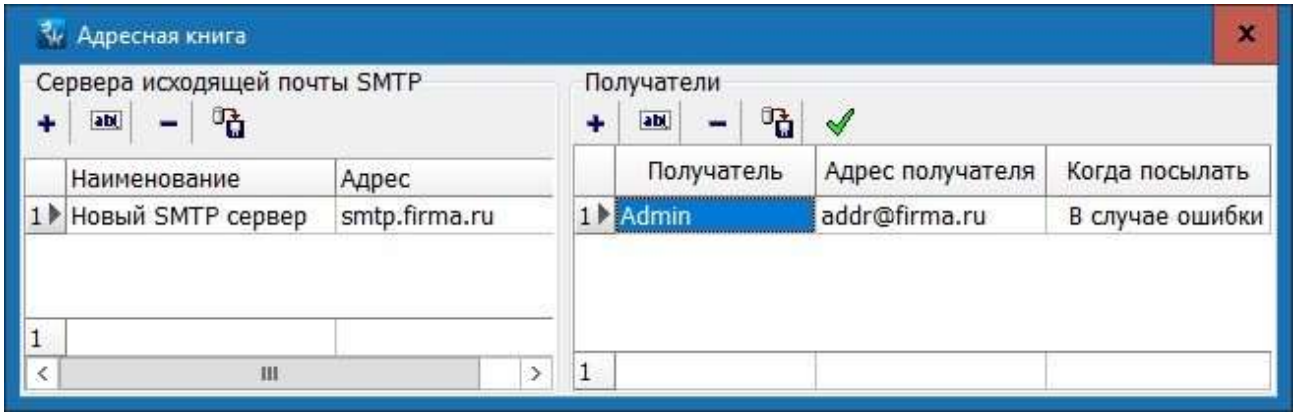
5. В открывшемся окне выделите сетевое имя необходимого ПК и нажмите кнопку **ОК**.

Окно будет закрыто. Имя ПК будет отображено в поле **Получатель**.

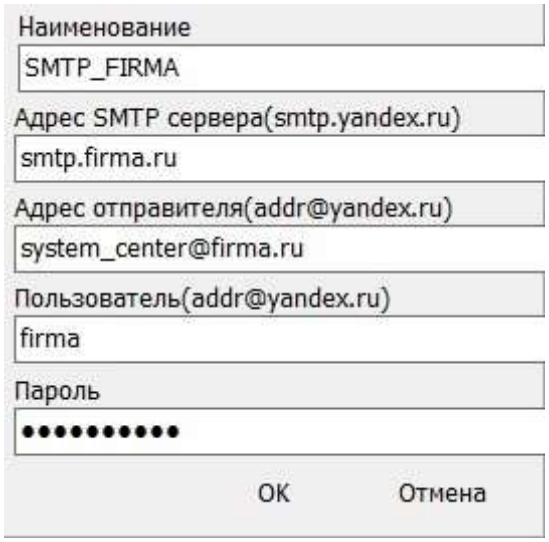
6. Нажмите кнопку **ОК** на панели ввода и редактирования данных. Панель будет закрыта. Имя выбранного ПК будет добавлено в список в окне **Получатели уведомлений** с указанием условия отправки уведомлений.
7. Нажмите кнопку **Сохранение данные** для сохранения внесенных в список изменений.
8. Для тестирования 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.

10.2.4. 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:



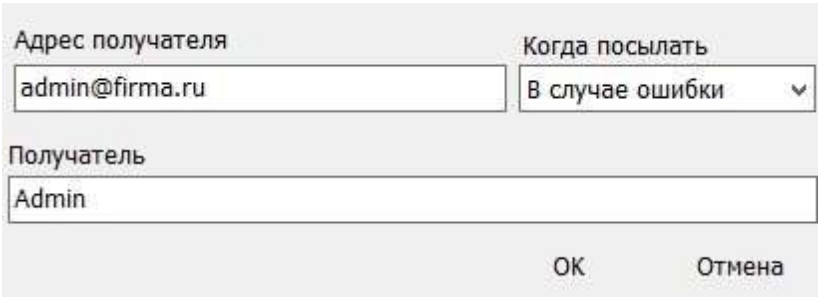
- **Наименование –** название отправителя.
- **Адрес SMTP сервера –** адрес SMTP сервера, используемого отправителем для отправки уведомлений.
- **Адрес отправителя –** адрес электронной почты отправителя, с которого рассылаются уведомления.
- **Пользователь –** имя отправителя, указываемое в уведомлении.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

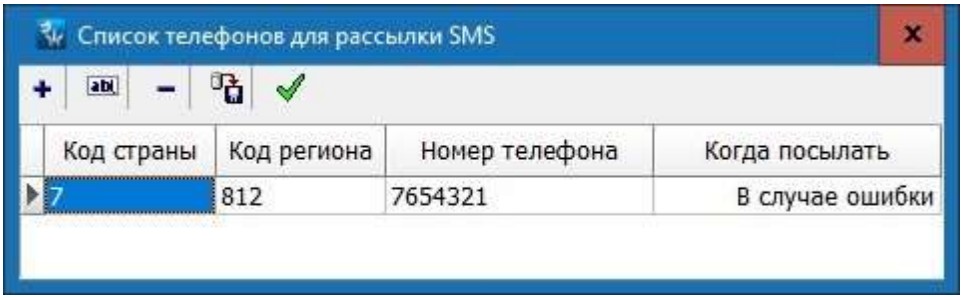
1. Нажмите кнопку **Настроить почтовую рассылку уведомлений** на панели инструментов вкладки **Резервное копирование БД**. Откроется окно **Адресная книга**.
2. Для отправки сообщений по электронной почте необходимо указать на панели **Сервера исходящей почты SMTP** хотя бы одного отправителя, с электронной 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.

10.2.5. Настройка SMS-рассылки уведомлений

Внимание!

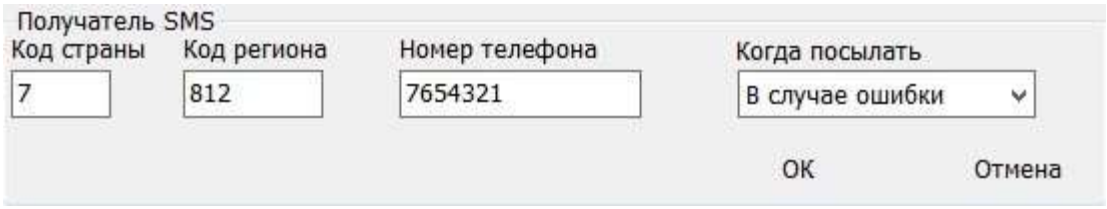
Для отправки уведомлений по SMS должна быть настроена рассылка SMS-сообщений на вкладке Настройка SMS-рассылки.

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.

10.3. SMS-рассылка

В системе предусмотрена возможность отправки SMS-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 и ученики»***.

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

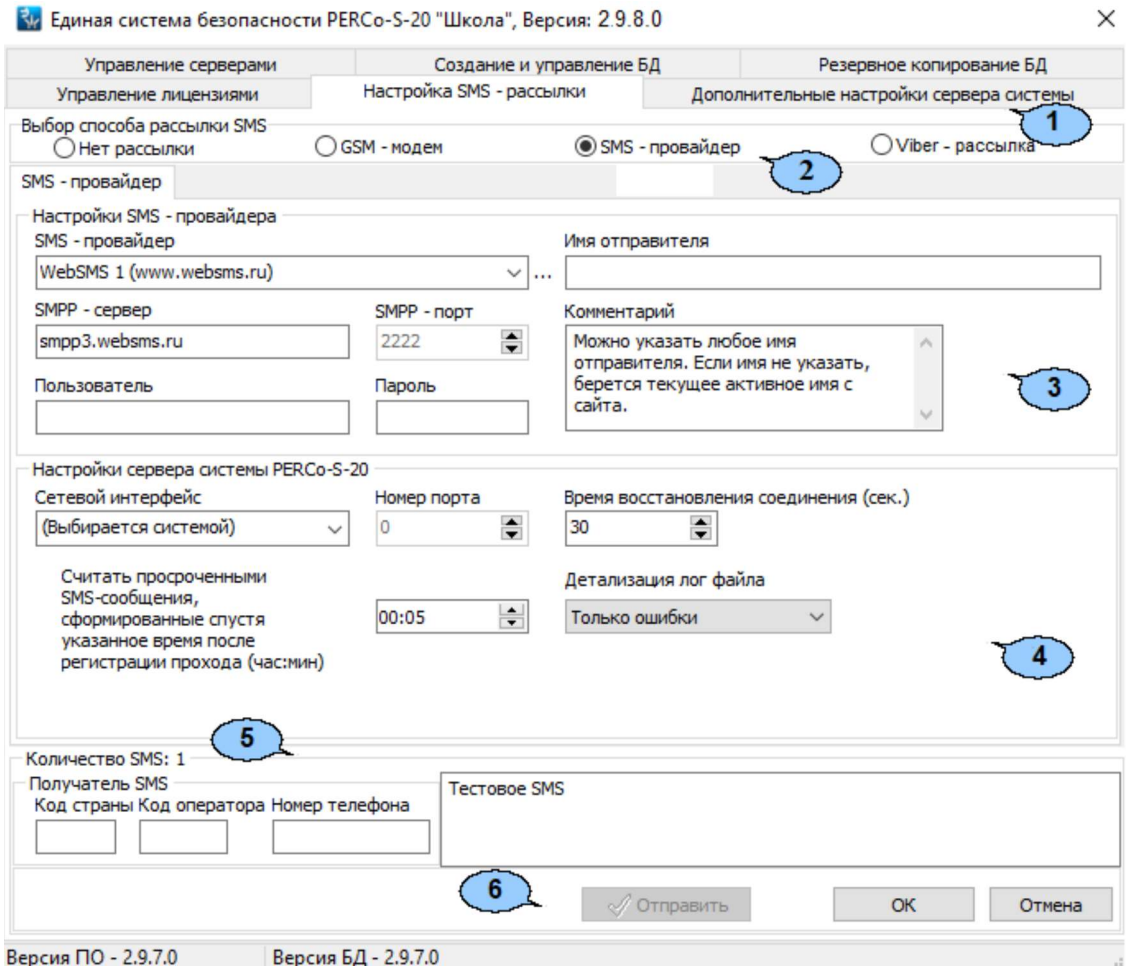
Для выбора способа отправки SMS-сообщений сервером системы: запустите ***«Центр управления»***, перейдите на вкладку **Настройка SMS-рассылки** и установите переключатель **Выбор способа рассылки SMS** в одно из положений:

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

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 SMS-рассылки** при положении переключателя **Выбор способа рассылки SMS: 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**.
2. Переключатель **Выбор способа рассылки SMS** позволяет выбрать способ отправки SMS-сообщений:
   - **Нет рассылки;**
   - **GSM-модем;**
   - **SMS-провайдер**.
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.

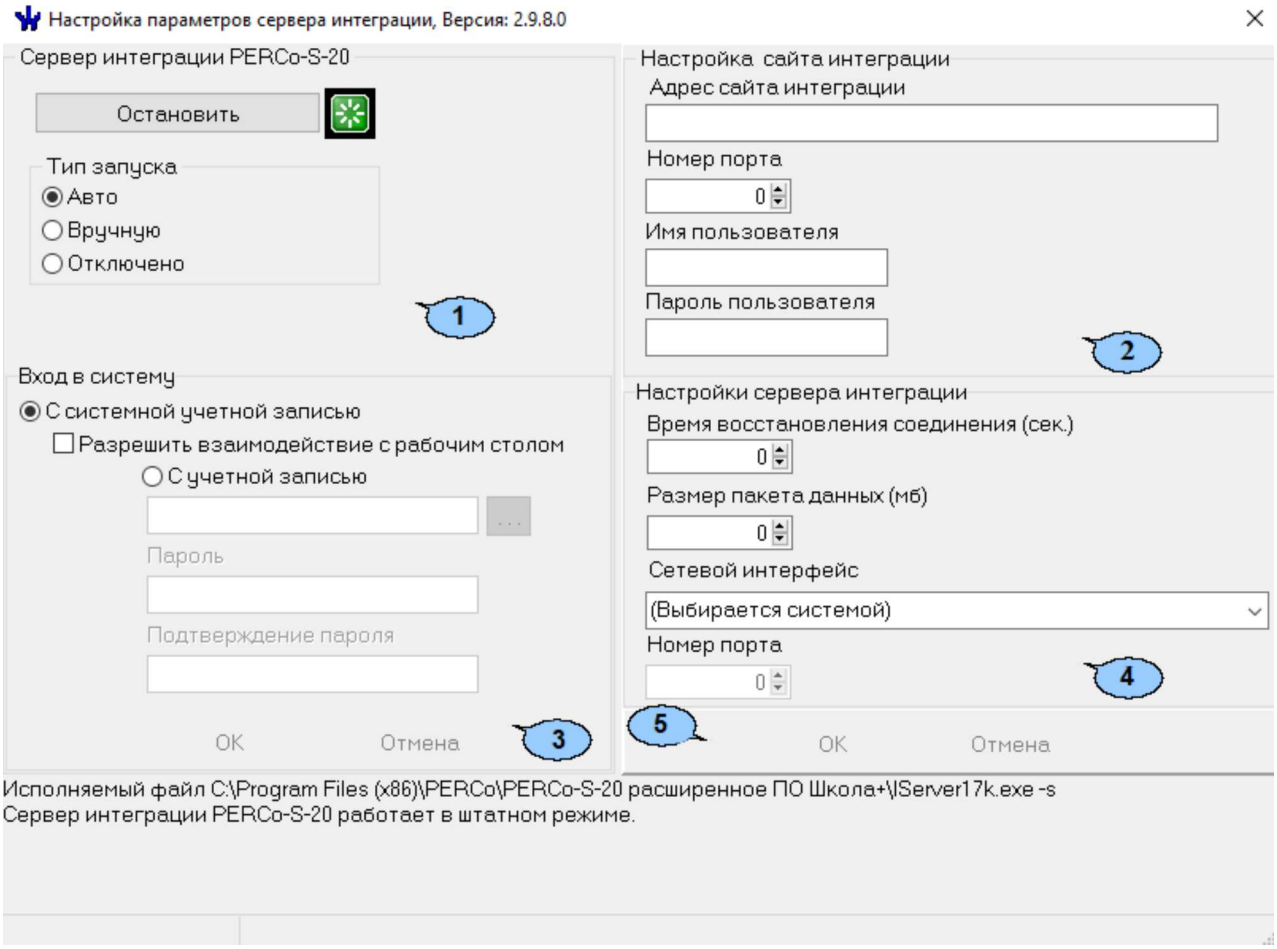
Порядок настройки SMS-рассылки через SMS-провайдера:

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

10.4. Настройка параметров сервера интеграции

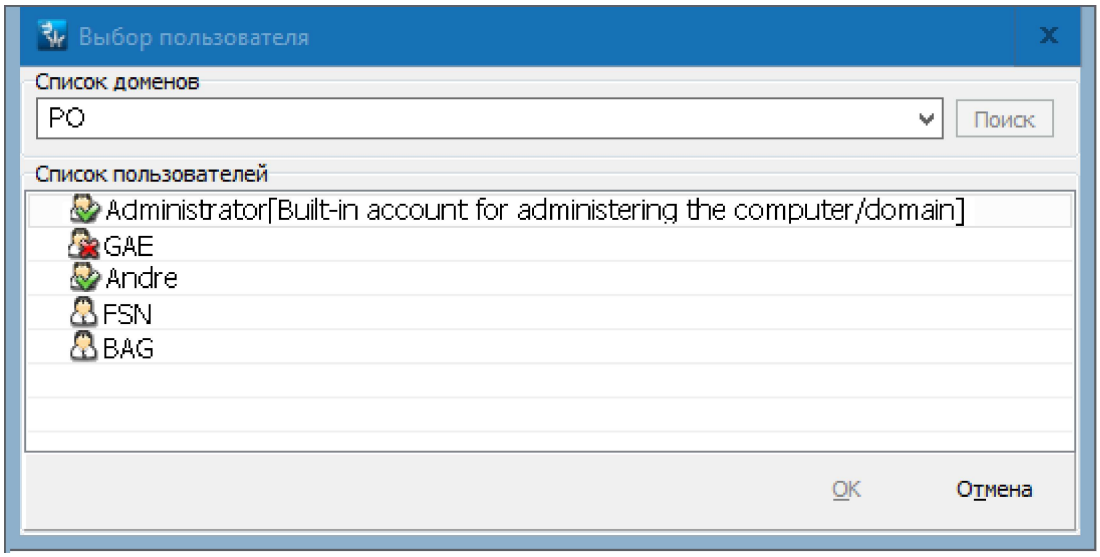
Модуль **Сервер интеграции** предназначен для интеграции системы с интернет-ресурсом «Электронный дневник» (1dnevnik.ru) или аналогичным. Интеграция дает возможность родителям просматривать на сайте не только оценки своих детей, но и данные о времени прихода и ухода ребенка из школы. Данные о проходах в автоматическом режиме передаются из БД системы в БД интернет-ресурса.

Для настройки параметров интеграции запустите модуль ***«Центр управления сервера интеграции PERCo-S-20 Школа»***. Откроется окно **Настройка параметров сервера интеграции**:



1. Панель **Сервер интеграции PERCo-S-20** содержит:
   - **Остановить/Запустить** – кнопка позволяет остановить/запустить сервер интеграции. Состояния серверов отображается с помощью индикатора справа от кнопки: / – **сервер системы запущен / остановлен.**
   - **Тип запуска** – переключатель позволяет установить способ запуска сервера интеграции:
     - **Авто** – сервер будет запущен автоматически при запуске ОС.
     - **Вручную** – сервер запускается вручную с помощью кнопки **Запустить**.
     - **Отключено** – запуск сервера невозможен.
2. Панель **Настройка сайта интеграции** содержит:
   - **Адрес сайта интеграции** – поле для ввода адреса интернет-ресурса, с которым осуществляется интеграция.
   - **Номер порта** – счетчик позволяет указать сетевой порт сервера интеграции, через который будет осуществляться связь с интернет-ресурсом.
   - **Имя пользователя** – поле для ввода названия учетной записи (логина) доступа к интернет-ресурсу.
   - **Пароль пользователя** – поле для ввода пароля доступа к интернет-ресурсу.
3. Переключатель **Вход в систему** позволяет выбрать учетную запись пользователя ОС, от имени которого будет запускаться сервер интеграции. Для корректной работы сервера 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 пользователя**:



4. Панель **Настройка сервера интеграции** содержит:
   - **Время восстановления соединения (сек)** – счетчик позволяет установить минимальный временной интервал между моментом разрыва связи сервера интеграции с интернет ресурсом и попыткой ее восстановления.
   - **Размер пакета данных (мб)** – счетчик позволяет установить максимальный размер пакета данных.
   - **Сетевой интерфейс** – раскрывающийся список позволяет указать сетевой интерфейс сервера интеграции, с которого будет осуществляться подключение к интернет ресурсу.
   - **Номер порта** – счетчик позволяет указать сетевой порт сервера интеграции, через который осуществляется соединения с интернет-ресурсом.
5. Кнопки:
   - **ОК** – предназначена для сохранения внесенных в окне изменений,
   - **Отмена** – предназначена для отмены внесенных в окне изменений.

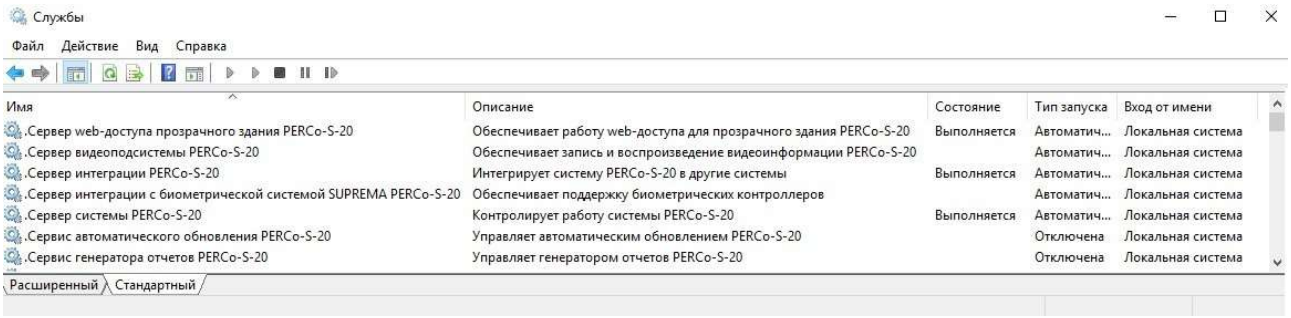
11. Службы системы

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:

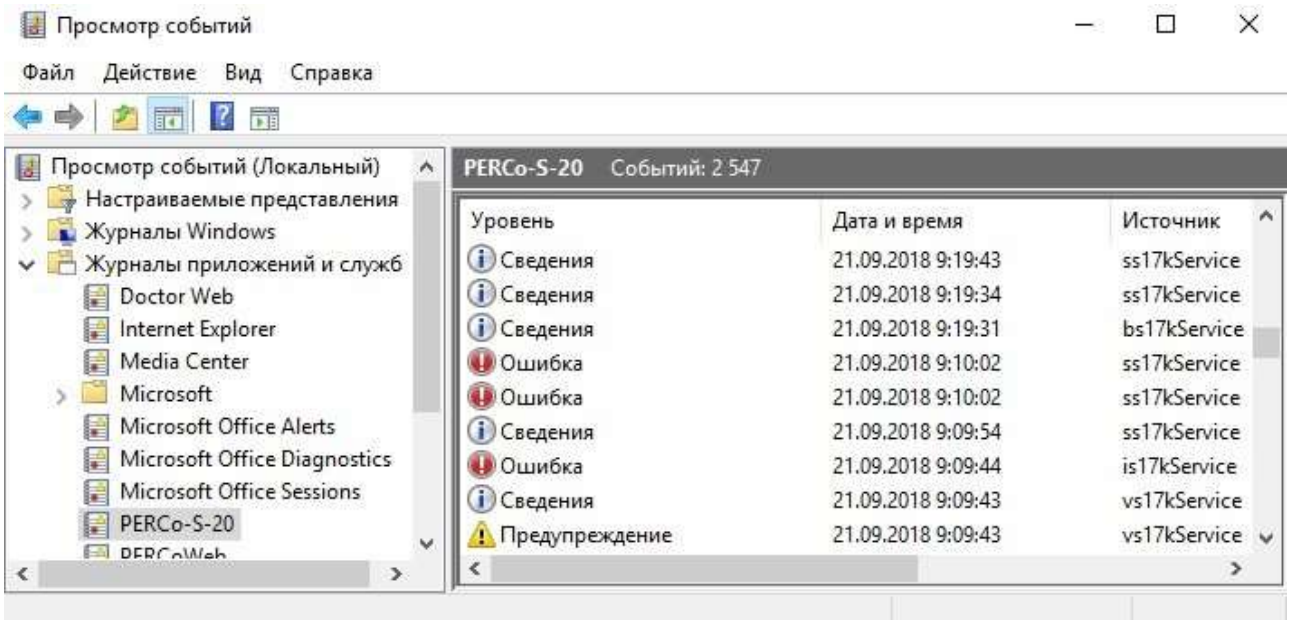
- *«Сервер системы PERCo-S-20»* – служба обеспечивает работу сервера системы. Устанавливается с модулем **Сервер системы**.
- *«Сервис автоматического обновления PERCo-S-20»* – служба обеспечивает возможность автоматического обновления консоли управления и сервера видеоподсистемы. Устанавливается с модулем **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 интеграции PERCo-S-20»* – служба обеспечивает работу сервера интеграции.
- *«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*.

12. 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**.

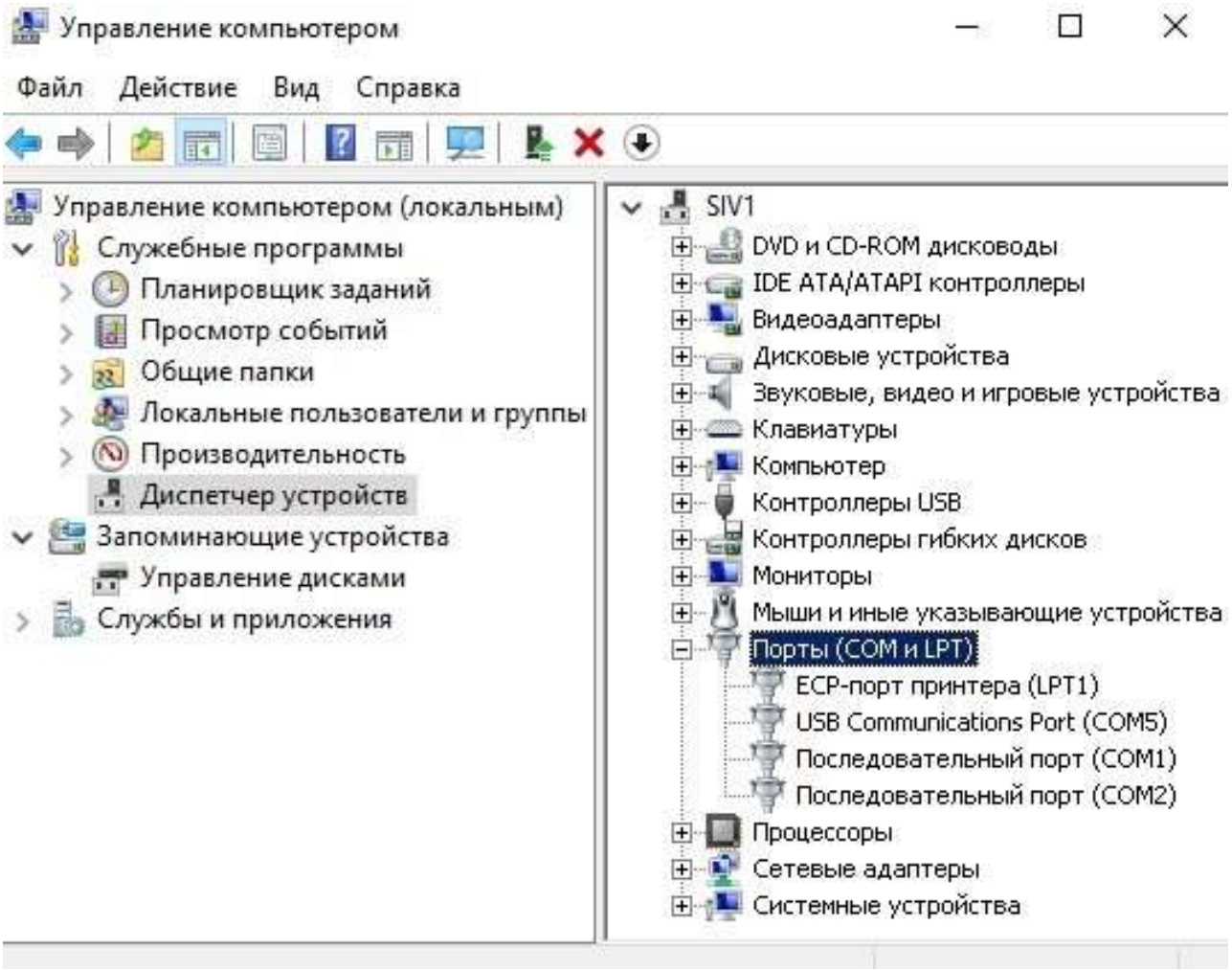
13. Установка драйвера контрольного считывателя

Примечание:

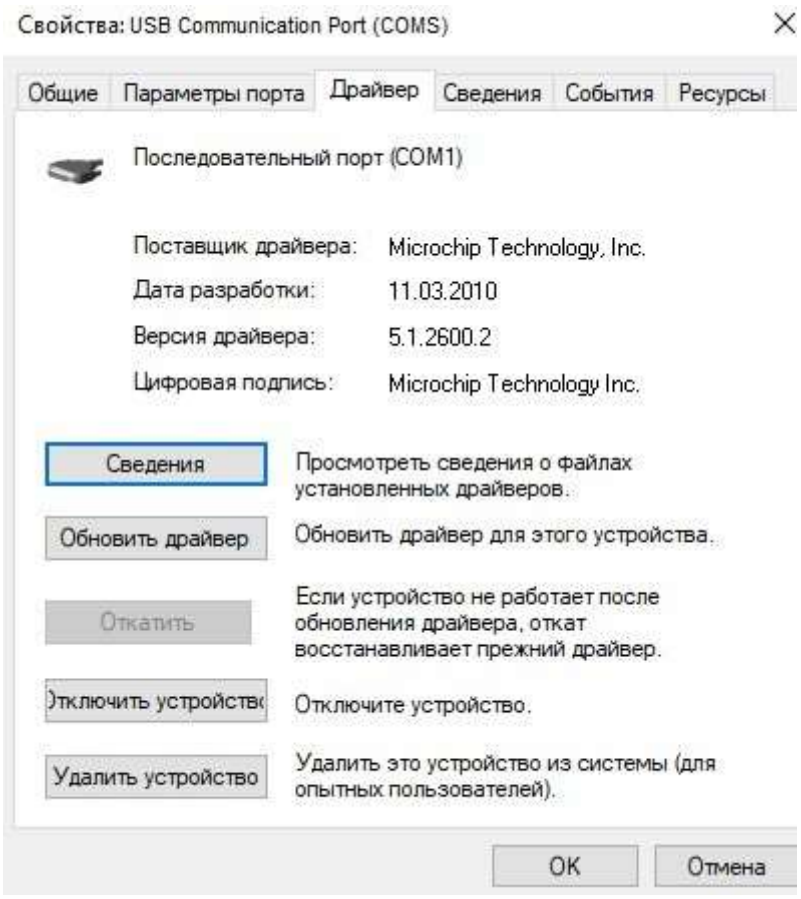
При подключении контрольных считывателей карт доступа серий ***PERCo-IR05.x***, ***PERCo-IR08.x*** к USB-порту ПК может потребоваться установить дополнительный драйвер. Файл архива с драйвером можно загрузить с сайта компании ***PERCo***, расположенного по адресу www.perco.ru, из разделе **Главная >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

Для установки драйвера:

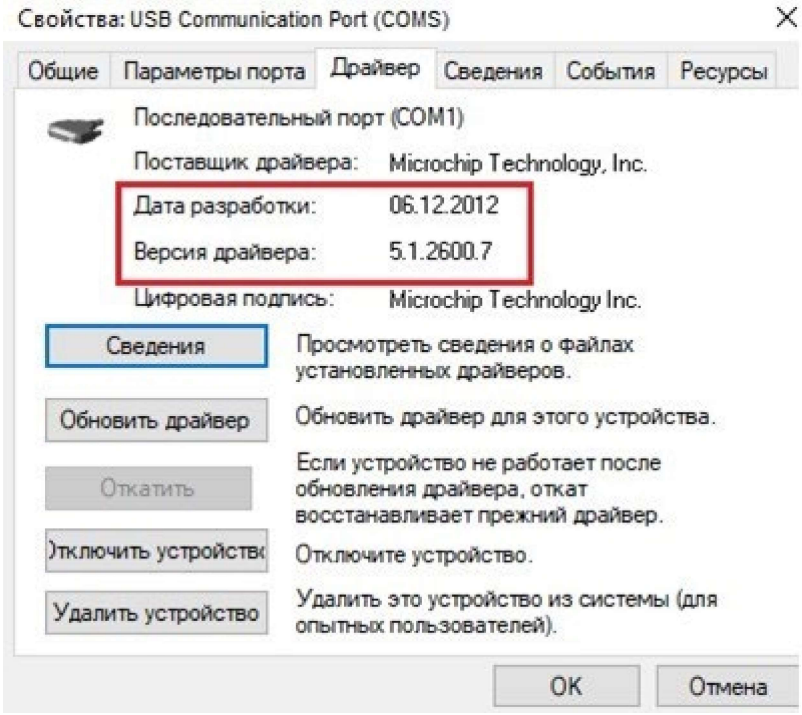
1. Выберите последовательно: **Пуск > Настройка > Панель управления > Администрирование > Управление компьютером**. Откроется окно **Управление компьютером**:



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:



14. Состав видеоподсистемы

Видеоподсистема состоит из камер наблюдения, АРМ операторов и одного или нескольких программных серверов видеонаблюдения.

В системе могут использоваться IP-видеокамеры и аналоговые видеокамеры, подключенные к IP-видеосерверам. Поддерживается работа камер в качестве детекторов движения.

Для записи видеоархива данных, получаемых с IP-видеокамеры и IP-видеосерверов, необходимо установить сервер видеоподсистемы. Сервер видеоподсистемы по сети *Ethernet* производит запись с камер видеоподсистемы. Запись начинается по команде оператора или ПО. В системе может быть установлено несколько серверов. Управление сервером видеоподсистемы и создание файлов видеоархивов производится из модуля ***«Центр управления видеоподсистемой»***.

Подключение камеры к тому или иному серверу, а также настройка параметров камеры, производится в расширенной версии раздела ***«Конфигуратор»***.

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. Видеоинформация с камер передается непосредственно в модуль. Запись в формате потокового видео ведется по команде оператора или ПО.
- ***«Камера СКУД»*** – компонент видеоподсистемы, позволяющий при предъявлении карты доступа считывателю производить автоматическую запись с камеры, связанной с этим считывателем. Камера устанавливается в точке прохода таким образом, что в ее поле зрения попадает место предъявления карт доступа считывателю. Компонентом могут быть использованы только те камеры, для которых установлен параметр **Использовать, как камеру СКУД**. Длительность записи определяется параметром **Время предзаписи для камер СКУД**.
- ***«Верификация»*** – модули ПО, предназначены для организации АРМ оператора службы безопасности. Модули позволяют усилить контроль доступа через точки прохода, за счет проведения оператором процедуры верификации. При организации точек верификации доступна возможность использования камер видеоподсистемы. Видеоинформация с камер передается непосредственно в модуль.

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.

15. 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.

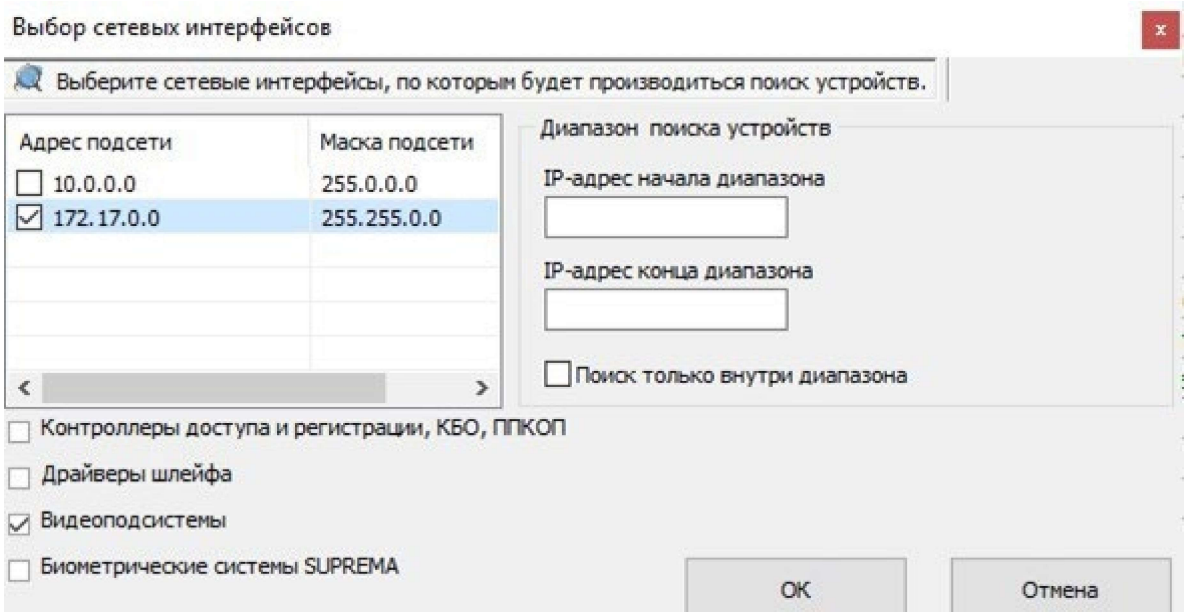
При настройке видеоподсистемы придерживайтесь следующей последовательности действий:

1. Убедитесь, что установлен модуль **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».***

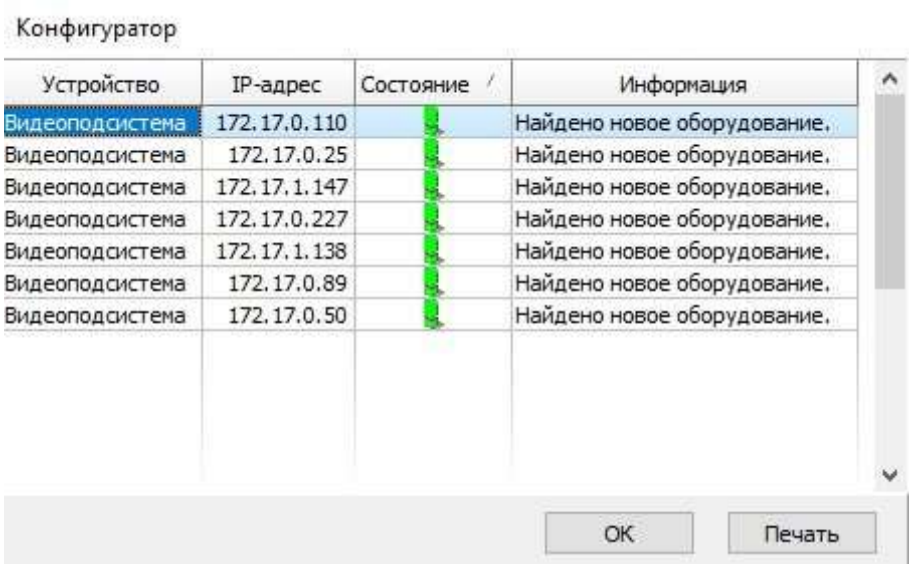
15.1. Поиск устройств видеоподсистемы

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:



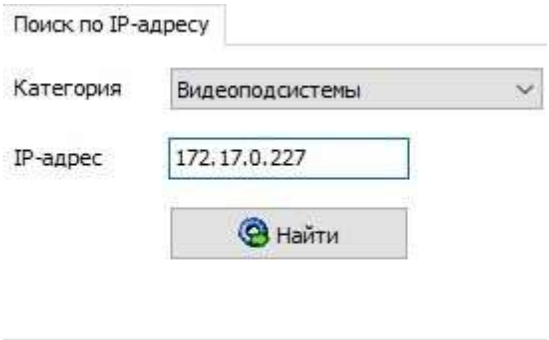
В открывшемся окне нажмите кнопку **ОК**. Все найденные устройства будут добавлены в рабочую область раздела и отмечены значками .

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 .

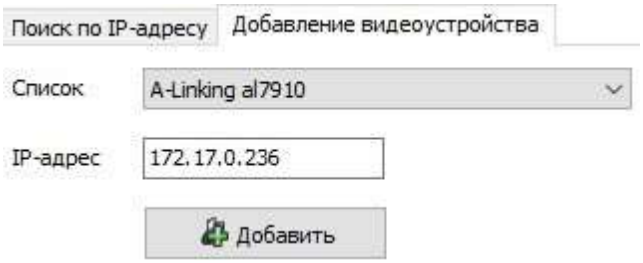
Поиск камеры поддерживающих стандарт ONVIF

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:

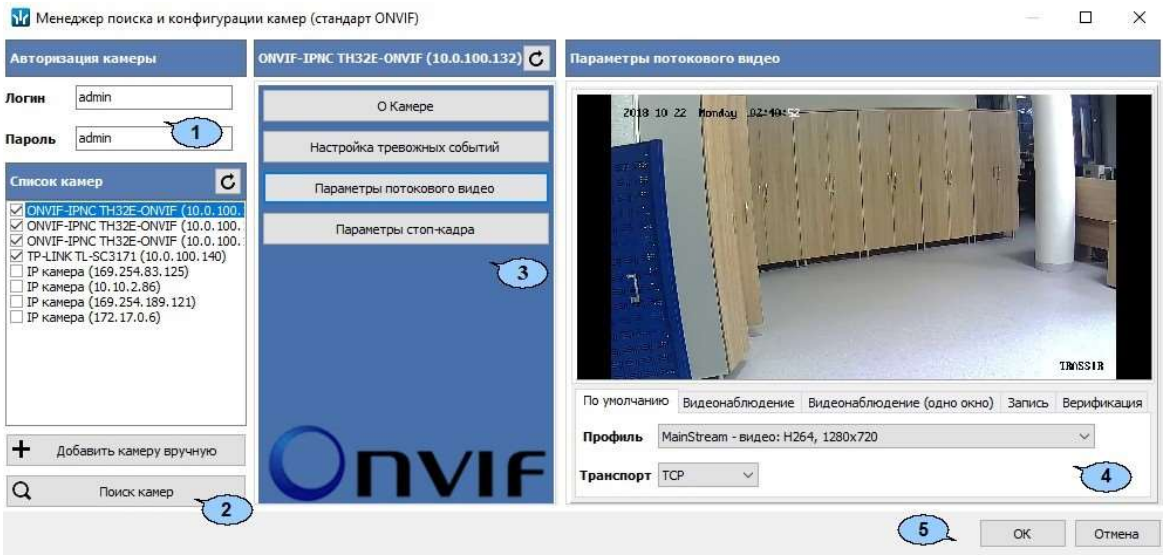
1. В рабочей области раздела выделите видеоподсистему, в которую необходимо добавить камеру и нажмите кнопку **Добавить новое устройство**.
2. На панели **Поиск по IP-адресу** в выпадающем списке **Категория** выберите пункт: **Камеры и видеосервера видеоподсистемы**. Убедитесь, что в поле **IP-адрес** 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 .

16. Подключение камер, поддерживающих стандарт ONVIF

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

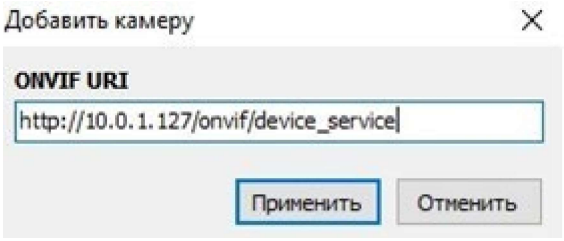


1. Панель **Авторизация камеры** содержит поля для ввода единых логина и пароля доступа к камерам.
2. Панель **Список камер** содержит список найденных камер.
   - – кнопка в заголовке панели позволяет произвести повторное подключение к найденным камерам.
   - **Добавить камеру вручную** – кнопка позволяет 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.

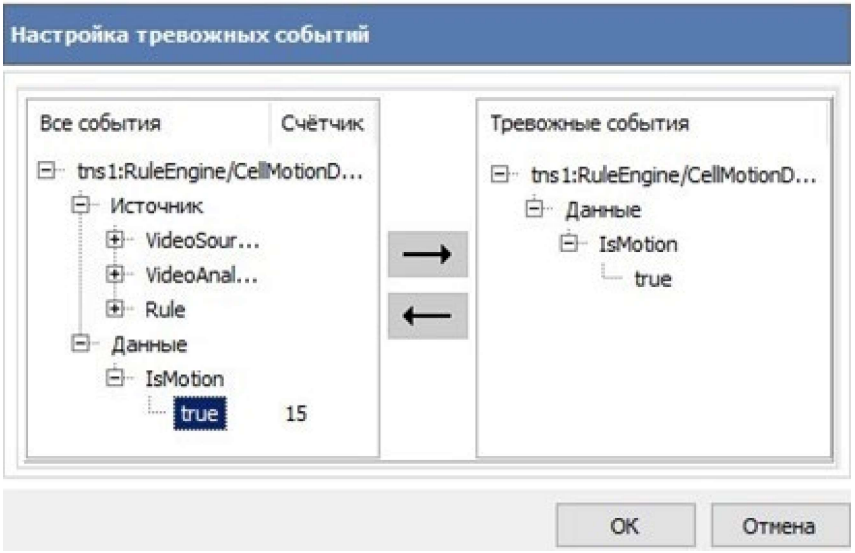
Порядок поиска камер, поддерживающих стандарт ONVIF

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.

17. «Центр управления видеоподсистемой»

17.1. Вкладка «Видеоархив»

17.1.1. 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.

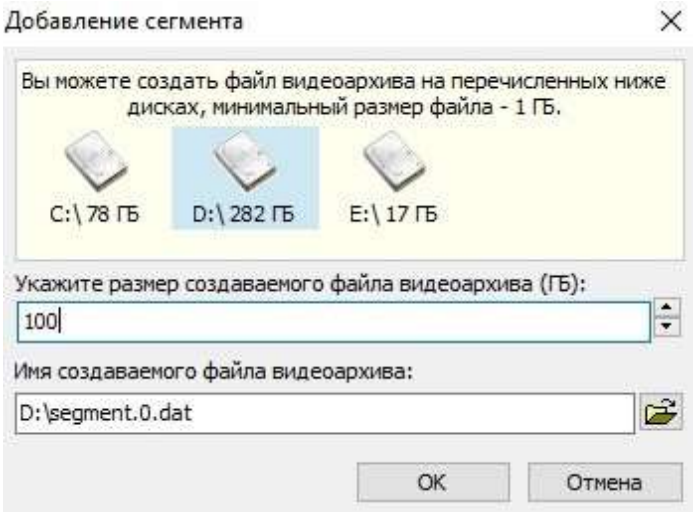
Внимание!

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

17.1.2. 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**.

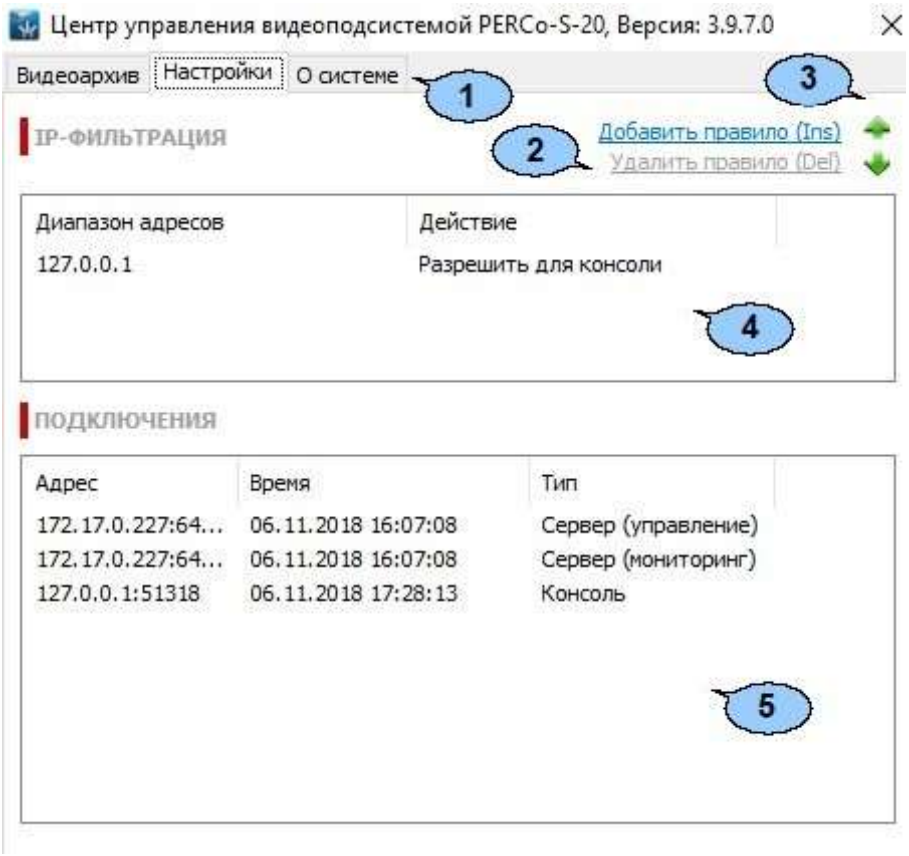
Для удаления файла видеоархива выделите его в рабочей области вкладки **Видеоархив** и нажмите кнопку **Удалить файл**. В появившемся диалоговом окне подтвердите удаление.

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

17.2. Вкладка «Настройки»

17.2.1. 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.

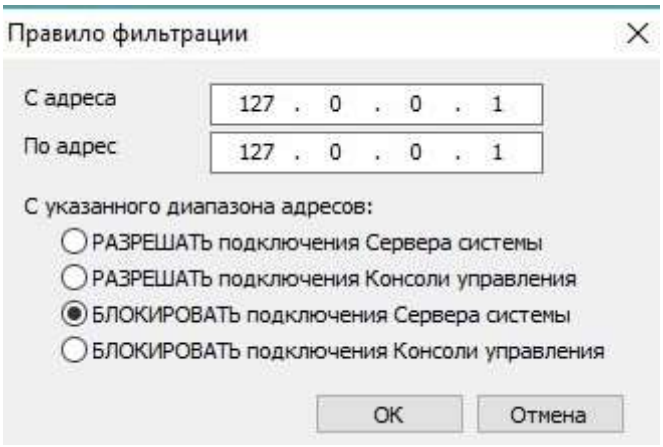
17.2.2. Настройка IP-фильтра

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.

Для удаления созданного ранее фильтра выделите его в рабочей области вкладки и нажмите кнопку **Удалить правило** на панели инструментов вкладки.

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

17.3. 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:

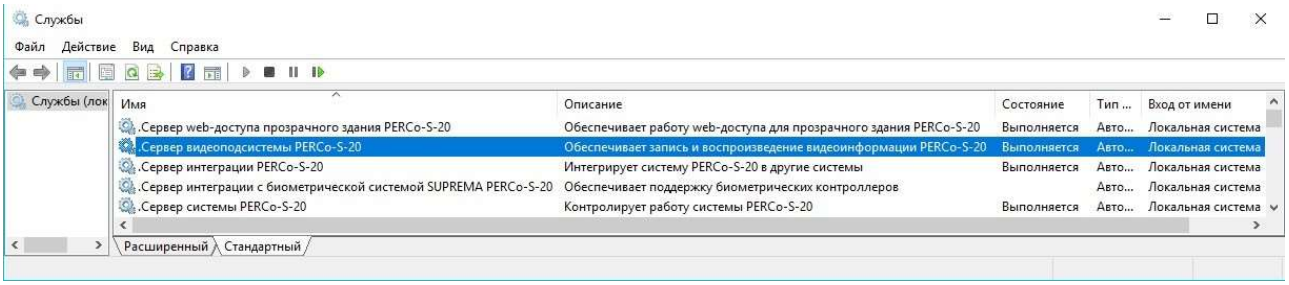
1. Выбор вкладки окна:
   - **Видеоархив**;
   - **Настройки**;
   - **О системе.**
2. Рабочая область вкладки с описанием характеристик системы.

18. 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.

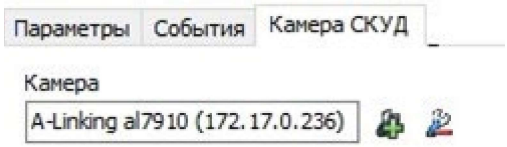
19. «Камеры СКУД»

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.

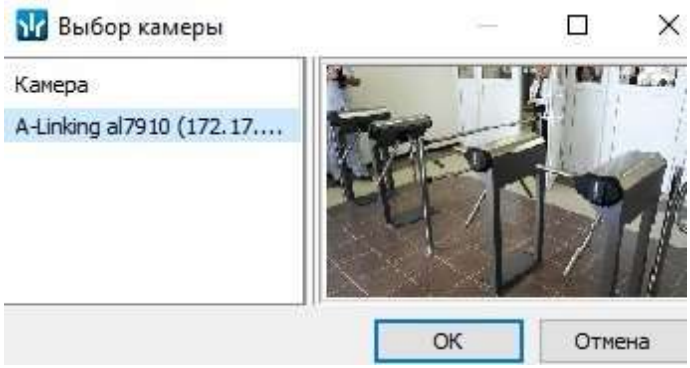
С любым считывателем, подключенным к одному из контроллеров системы, можно связать одну из камер видеоподсистемы. При этом одна камера одновременно может быть связана с несколькими считывателями.

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**.

20. Конфигурирование считывателей Mifare

20.1. 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**).

20.2. 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, при этом не имея фактического доступа к ключам и паролям.

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.

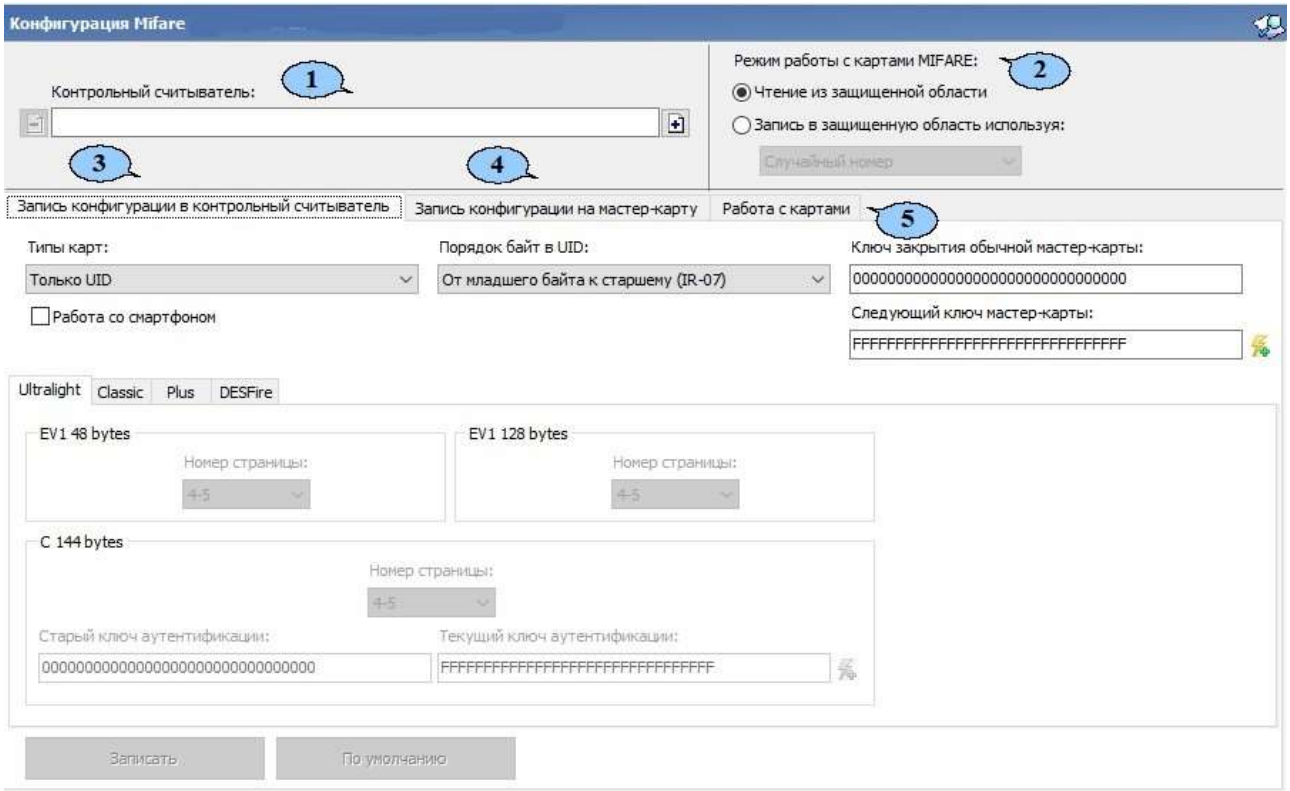
Чтобы карты доступа **MIFARE** работали в СКУД в защищенном режиме, необходимо:

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.

20.3. 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 защищённой области –** режим, при котором происходит только чтение номера карты защищённой области;
   - **Запись в защищённую область используя –** режим, при котором происходит

чтение существующего номера карты из защищённой 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, 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.

20.4. Вкладка "Запись конфигурации в контрольный считыватель"

Вкладка **Запись конфигурации в контрольный считыватель** позволяет выбрать один или несколько типов карт **MIFARE**, которые будут использоваться в СКУД, и задать параметры для выбранных типов карт (т.е. конфигурацию для карт **MIFARE**).

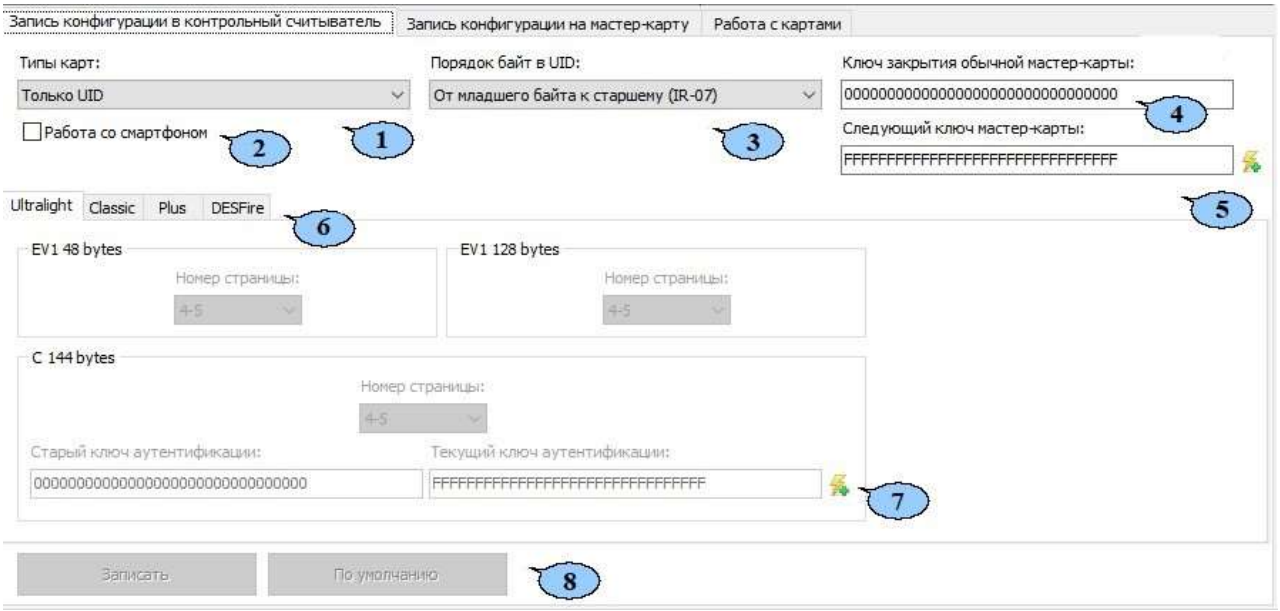
Общие термины и определения:

- ***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 неё информации.
- ***Номер сектора –*** номер части внутренней защищённой 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 защищённой 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. Строка **Типы карт** – позволяет с помощью установки флажка выбрать один или несколько типов карт **MIFARE**, которые будут использоваться в СКУД.
2. Поле **Порядок байтов 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. Параметр **Работа со смартфоном –** 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.

6. Подвкладки **Ultralight, Classic, Plus, DESFire** – позволяют перейти к настройкам конфигурации различных типов карт **MIFARE.**
7. Кнопка **Генерация случайной последовательности** – позволяет задать для поля **Следующий ключ мастер-карты** новый ключ при помощи генератора случайных чисел.

8. Кнопка **Записать** – позволяет записать заданную для карт конфигурацию в энергонезависимую память контрольного считывателя.
9. Кнопка **По умолчанию** – для сброса измененных настроек.

20.4.1. Подвкладки Ultralight, Classic, Plus, DESFire

Подвкладки **Ultralight, Classic, Plus, DESFire** позволяют задать рабочие параметры криптозащиты для соответствующих типов карт, отмеченных флажками в выпадающем списке строки **Типы карт** вкладки **Запись конфигурации в контрольный 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 **Ultralight, Classic, Plus, DESFire.**

Предусмотрены следующие области подвкладок:

- **Ultralight: EV1 48 bytes, EV1 128 bytes, C 144 bytes;**
- **Classic: ID 64, 1KB, 4KB;**
- **Plus: 2KB, 4KB, SE1KB;**
- **DESFire.**

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).

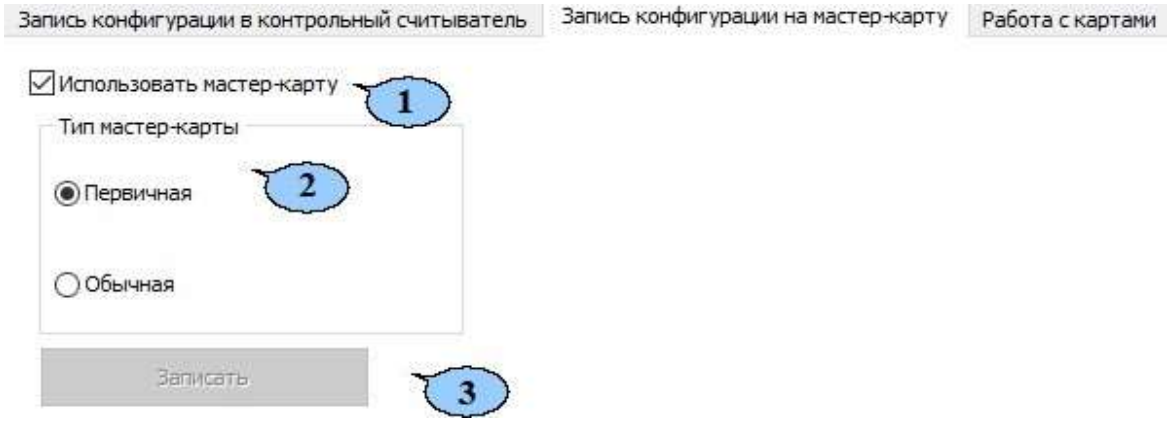
Внимание!

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.

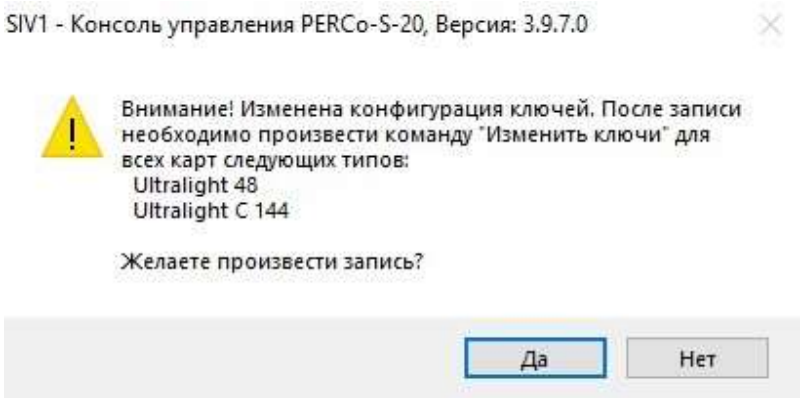
20.5. Вкладка "Запись конфигурации на мастер-карту"

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 её в состояние простой карты пользователя **невозможна**! (Т.е. карта, однажды записанная как мастер-карта, может использоваться далее только в этом качестве.)

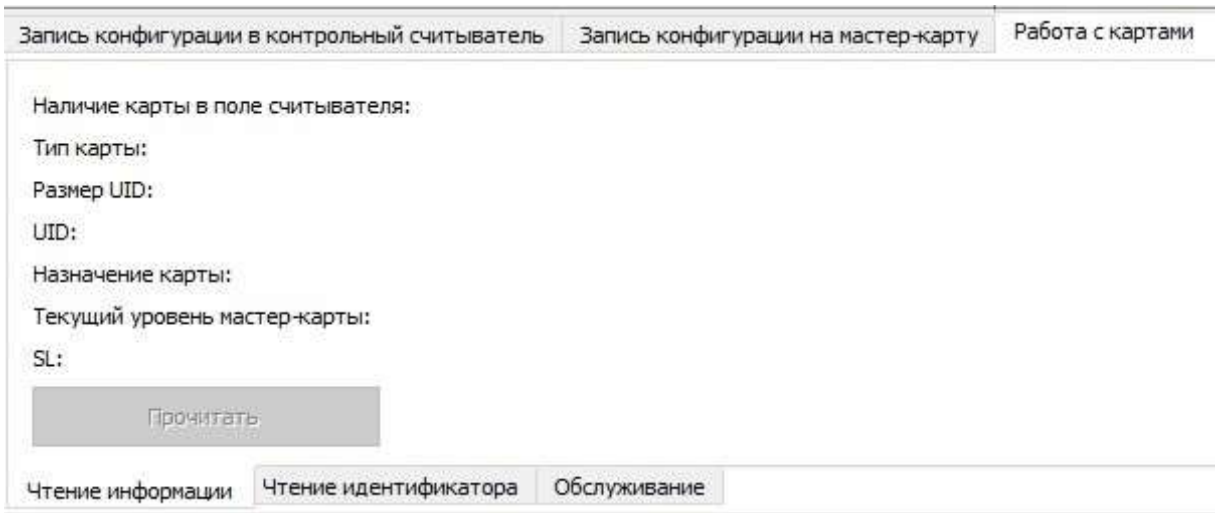
20.6. Вкладка "Работа с картами"

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).

20.6.1. Подвкладка "Чтение информации"

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



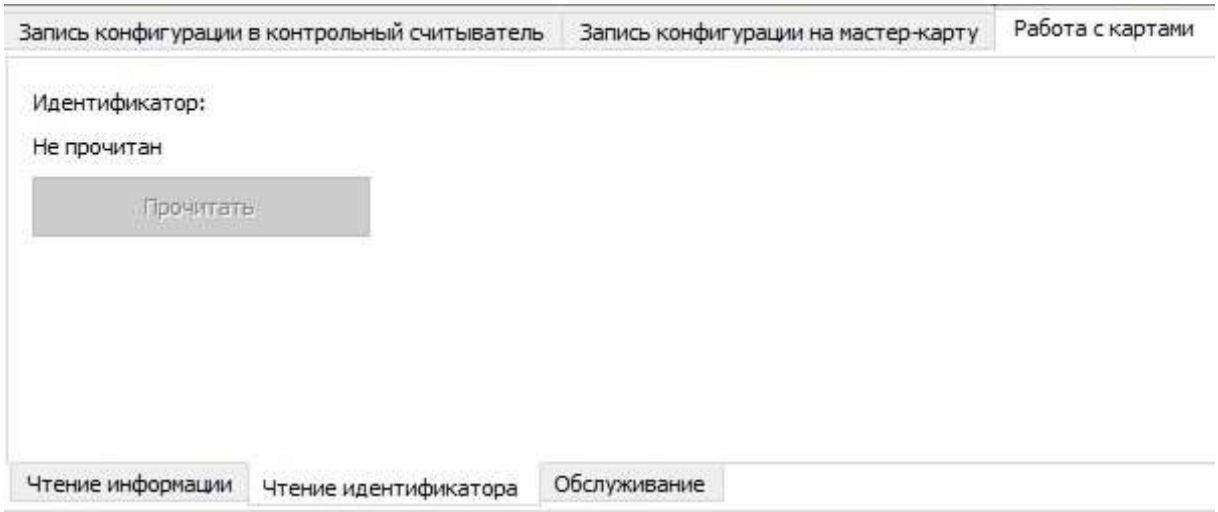
- Рабочая область подвкладки отображает следующую информацию:
  - **Наличие карты в поле считывателя –** отображает наличие или отсутствие

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.

20.6.2. Подвкладка "Чтение идентификатора"

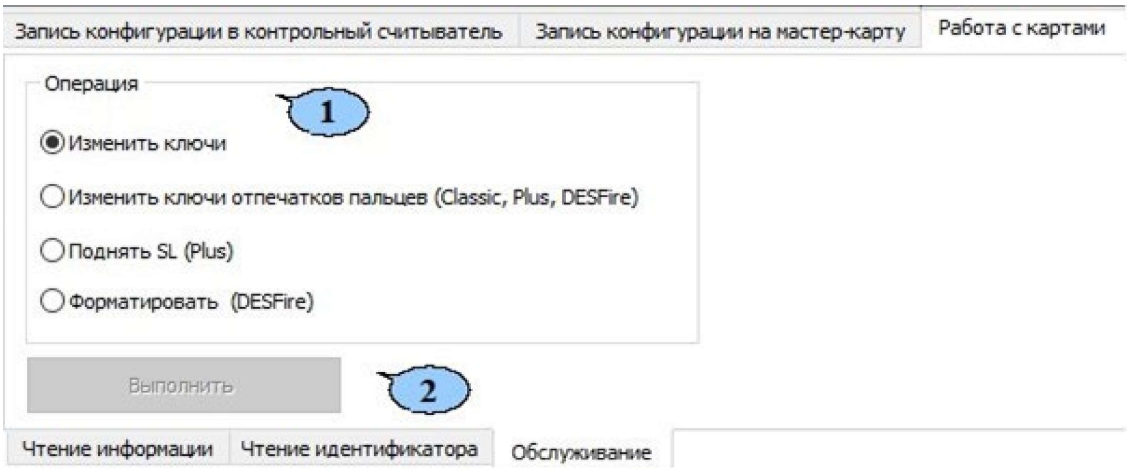
Подвкладка **Чтение идентификатора** позволяет прочесть и отобразить идентификатор из внутренней области памяти карты **Mifare:**



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

20.6.3. 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, её 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, её 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.

20.7. 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 неё 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 её 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. 30.07.2020

www.perco.ru

тел: 8 (800) 333-52-53