Система контроля и управления доступом PERCo-Web

PERCo-WS

«Стандартный пакет ПО»

РУКОВОДСТВО АДМИНИСТРАТОРА

Версия ПО: 1.0.0.409

СОДЕРЖАНИЕ

1 Введение

Настоящее *«Руководство администратора»* (далее – *руководство*) предназначено для ознакомления с функциональными возможностями, основными техническими характеристиками, принципом работы и особенностями настройки системы контроля и управления доступом (далее - *системы*) ***PERCo-Web.***

Руководство предназначено для администраторов системы, а также для системных администраторов компьютерных сетей и сотрудников служб (подразделений) по поддержке программного и аппаратного обеспечения.

В руководство включено описание терминов, используемых при описании системы, приведен перечень оборудования, поддерживаемого системой, указаны требования к ПК и сети *Ethernet*, используемым при построении системы.

Руководство должно использоваться совместно с *«Руководством пользователя»* ПО системы ***PERCo-Web***.

Примечание:
Эксплуатационная документация на оборудование и ПО системы ***PERCo-Web*** доступна в электронном виде на сайте компании ***PERCo***, по адресу: www.perco.ru, в разделе **Поддержка> Документация**.

Принятые сокращения:

АРМ – автоматизированное рабочее место;
БД – база данных;
ИУ – исполнительное устройство;
КПП – контрольно-пропускной пункт;
ПДУ – пульт дистанционного управления;
ПК – персональный компьютер, ноутбук;
ПО – программное обеспечение;
РКД – режим контроля доступа;
СКУД – система контроля и управления доступом;
СУБД – система управления базами данных;
УРВ – учет рабочего времени;
ЭП – электронная проходная.

2 Назначение

Система ***PERCo-Web*** (далее – *система*) предназначена для применения на промышленных предприятиях, в учреждениях, банках, бизнес-центрах, в организациях медицинской, образовательной и других сфер деятельности. Система позволяет решать следующие задачи:

- Автоматизация контроля и управление доступом на территорию предприятия, в том числе:
  - защита от несанкционированного проникновения посторонних лиц на территорию предприятия,
  - разграничение прав доступа сотрудников и посетителей в помещения предприятия,
  - создание АРМ сотрудников службы контрольно-пропускного режима для проведения процедуры верификации прохода сотрудников и посетителей, в том числе с возможностью использования видеокамер.
- Повышение эффективности работы предприятия, в том числе:
  - автоматизированный учет рабочего времени сотрудников,
  - автоматизированный контроль нарушений трудовой дисциплины,
  - организация АРМ различной направленности для служб контрольно-пропускного режима, персонала, бюро пропусков, бухгалтерии.

3 Основные особенности

- Обмен данными между АРМ, БД и оборудованием системы осуществляется по сети *Ethernet*. Это позволяет при развертывании системы использовать уже существующую IT-инфраструктуру предприятия.
- Сервер системы, сервер БД и все необходимое для работы системы ПО устанавливается на одном ПК, подключенном к сети *Ethernet*. Установка дополнительного ПО на АРМ операторов системы не требуется. Доступ осуществляется удаленно, через Web-интерфейс сервера системы.
- Наличие постоянной связи контроллеров системы с сервером не требуется. В энергонезависимую память каждого контроллера передаются все права доступа владельцев карт. Там же сохраняются регистрируемые контроллером события. При восстановлении связи с сервером системы события переносятся в БД системы.
- Контроллеры системы поддерживают возможность обновления встроенного ПО (прошивки) по сети *Ethernet*.
- Система легко масштабируется, то есть возможно увеличение числа контроллеров (КПП) и АРМ с их интеграцией в уже существующую систему.
- При организации дополнительных АРМ достаточно добавить в систему нового оператора и выдать ему полномочия на доступ к соответствующим разделам и подразделам ПО системы.
- ПО системы позволяет гибко настраивать полномочия операторов АРМ. Полномочия выдаются операторам независимо на разделы и подразделы ПО, оборудование, помещения, подразделения и т.д. При этом АРМ связано не с конкретным ПК, а с учетной записью оператора.

4 Состав и принципы работы системы

Система состоит из следующих элементов (см. рис. *«Структурная схема системы PERCo-Web»*):

Сервер системы

На ПК сервера системы устанавливается ПО системы, состоящее из сервера, видеосервера, БД системы и другого вспомогательного ПО. В БД системы каждому сотруднику и посетителю ставится в соответствие пропуск-идентификатор с уникальным номером. В качестве идентификатора выступает бесконтактная карта доступа (брелок). Конфигурирование и управление системой осуществляется через web-интерфейс сервера системы.

КПП

КПП оборудуются контроллерами, считывателями карт доступа, ИУ (турникетами, замками, калитками и т.д.) и другим дополнительным оборудованием (ПДУ, сигнализацией, устройствами аварийного открытия прохода (*FireAlarm*), картоприемниками, IP-видеокамерами и т.д.). Все КПП связаны между собой и с ПК сервера системы по сети *Ethernet*.

Возможны следующие варианты управления ИУ на КПП:

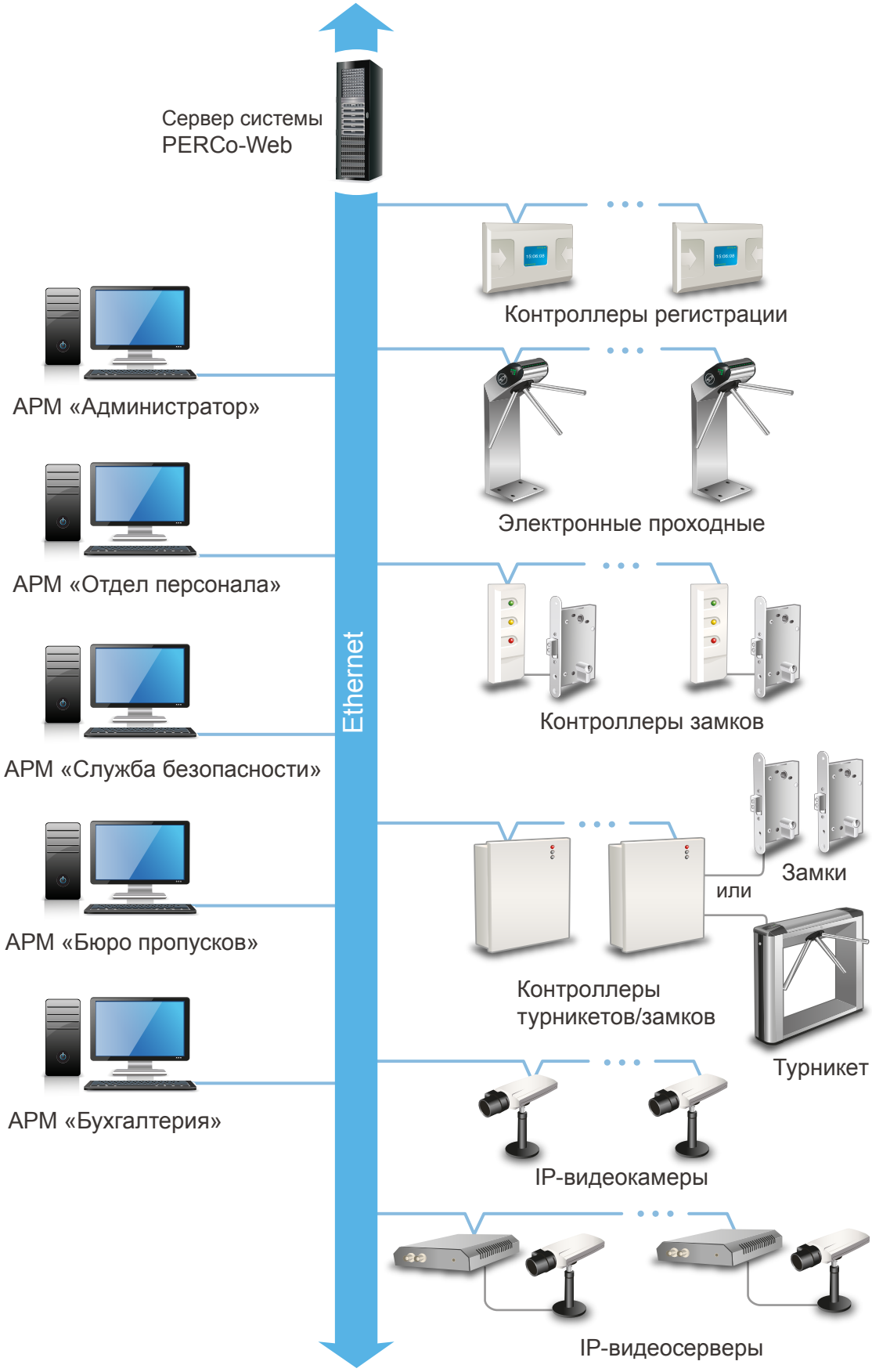
- Оператором КПП в ручном режиме с помощью ПДУ.
- Оператором КПП от ПК заданием для направлений ИУ одного из *режимов контроля доступа* (РКД): *«Открыто»*, *«Закрыто»*, *«Контроль»*. Это позволяет при необходимости обеспечить свободный проход в данном направлении или полностью его перекрыть. Для прохода по картам доступа используется РКД *«Контроль»*.
- Автоматически контроллером КПП при проходе по картам доступа. При этом в направлении прохода должен быть установлен РКД *«Контроль».* При проходе через КПП владелец карты доступа предъявляет ее считывателю. На основании анализа номера карты и выданных ее владельцу прав доступа контроллер принимает решение на разрешение или запрет прохода, подавая соответствующую команду ИУ. Каждый факт предъявления карты фиксируется в БД с указанием места и времени предъявления, что позволяет системе отслеживать местонахождение, время пребывания и перемещения владельца карты по территории и помещениям предприятия.

Усилить контроль доступа на территорию предприятия при проходе сотрудников и посетителей по картам доступа позволяет проведение оператором КПП процедуры верификации. Имеется возможность использования при верификации IP-видеокамер (IP-видеосерверов с видеокамерами), подключенных к системе, для этого в состав ПО системы входит видеосервер.

АРМ

АРМ организуются на удаленных ПК, подключенных к серверу системы. Организация АРМ в системе производится выдачей полномочий операторам на доступ к разделам и подразделам ПО системы. При входе в систему под своей учетной записью оператору доступны только те разделы, на которые ему даны полномочия. На удаленных ПК возможна организация следующих АРМ:

- *«Администратор»* (раздел ***«Администрирование»***),
- *«Отдел персонала»* (раздел ***«Персонал»***),
- *«Служба контрольно-пропускного режима»* (разделы: «***Контроль доступа»***, ***«Заказ пропуска»***, ***«Верификация»***),
- *«Бюро пропусков»* (раздел ***«Бюро пропусков»***),
- *«Бухгалтерия»* (раздел ***«Учет рабочего времени»***).



Структурная схема системы PERCo-Web

5 Поддерживаемое оборудование

Примечание:

Эксплуатационная документация на оборудование системы доступна в электронном виде на сайте компании ***PERCo***, по адресу: www.perco.ru, в разделе **Поддержка> Документация**.

Контроллеры управления дверьми

Для управления дверьми используются контроллеры замка совместно с электромеханическими или электромагнитными замками. Могут использоваться замки (защелки) производства компании ***PERCo*** или стороннего производителя. Компания ***PERCo*** производит следующие модели контроллеров управления дверьми:

PERCo-CL05 Позволяет организовать одно КПП с контролем проходов в одном направлении. Контроллер снабжен встроенным считывателем карт доступа формата *HID*, *EM-Marine* и блоком индикации со светодиодными индикаторами.

PERCo-CL05.1 Позволяет организовать одно КПП с контролем проходов в одном направлении или, при использовании двух контроллеров данной модели, одно КПП с контролем проходов в двух направлениях. Контроллер снабжен встроенным считывателем карт доступа формата *HID*, *EM-Marine* и блоком индикации со светодиодными индикаторами.

PERCo-CT/L04 В варианте конфигурации *«Контроллер управления одной двухсторонней дверью»* позволяет организовать одно КПП с контролем проходов в двух направлениях или в варианте конфигурации *«Контроллер управления двумя односторонними дверьми»* – два КПП с контролем проходов в одном направлении, управляя при этом соответственно одним или двумя ИУ. Выносные считыватели подключаются к контроллеру по интерфейсу *RS-485.*

PERCo-CL201.x Подключается в качестве контроллера второго уровня к контроллерам ***PERCo-CT/L04*** или встроенному контроллеру ЭП ***PERCo-CT03*** по интерфейсу *RS-485* и позволяет организовать одно КПП с контролем проходов в одном направлении. Контроллер снабжен встроенным считывателем карт доступа формата *HID*, *EM-Marine* и блоком индикации со светодиодными индикаторами. Одновременно к контроллеру первого уровня может быть подключено до 8 контроллеров второго уровня.

Контроллеры управления турникетом

Для управления турникетами используются контроллеры турникета совместно с одним турникетом или калиткой производства компании ***PERCo*** или стороннего производителя. Компания ***PERCo*** производит следующие модели контроллеров управления турникетом:

PERCo-CT/L04 В варианте конфигурации *«Контроллер управления турникетом»* позволяет организовать одно КПП с контролем проходов в двух направлениях. По интерфейсу *RS-485* к контроллеру подключаются встроенные считыватели турникета или дополнительно устанавливаемые выносные считыватели.

PERCo-CT03 Встроенный контроллер, поставляется в составе ЭП, позволяет организовать одно КПП с контролем проходов в двух направлениях.

Контроллер регистрации

PERCo-CR01 LICON Контроллер предназначен для организации терминала учета рабочего времени и контроля трудовой дисциплины. Снабжен двумя встроенными считывателями карт доступа формата *HID*, *EM-Marine* и ЖКИ (дисплеем). Контроллер не поддерживает возможность управления ИУ.

ИУ – Замок

- электромеханические замки с контактной группой серий ***PERCo-LB*** и ***PERCo-LBP***;
- электромеханические замки серии ***PERCo-LC***;
- электромеханические и электромагнитные замки сторонних производителей.

ИУ – Турникет

- турникеты-триподы серий ***PERCo-T*** и ***PERCo-TTR***;
- тумбовые турникеты серий ***PERCo-TTD*** и ***PERCo-TB***;
- роторные турникеты серии ***PERCo-RTD***;
- турникеты сторонних производителей.

ИУ – Калитка

- электромеханические полуавтоматические калитки серии ***PERCo-WHD***;
- электромеханические автоматические калитки серии ***PERCo-WMD***;
- калитки сторонних производителей.

Считыватели

Могут быть использованы считыватели карт формата *HID*, *EM-Marin* или *MIFARE*. Внешние считыватели подключаются к контроллерам системы по интерфейсу *RS-485*. Для подключения считывателей с интерфейсом *Wiegand-26, 34, 37, 40, 42* необходимо использовать конвертер интерфейса ***PERCo-AC02***.

В качестве внешних считывателей карт доступа могут использоваться:

- считыватели серии ***PERCo-IR***, снабженные блоками индикации;
- стойка-считыватель ***PERCo-IRP01***, снабженная ЖК-дисплеем.

Для подключения к USB-разъему ПК используются контрольные считыватели ***PERCo-IR05*** для карт формата *HID*, *EM-Marin* и ***PERCo-IR08*** для карт формата *MIFARE*.

Электронные проходные

ЭП представляет собой готовый комплект оборудования для организации КПП с контролем проходов в двух направлениях, то есть ИУ, считыватели карт доступа и встроенный контроллер. В ЭП могут быть установлены считыватели для карт формата *HID*, *EM-Marin* или *MIFARE*.

- ***PERCo-KT02***, ***PERCo-KT08*** – серия ЭП на базе турникета-трипода;
- ***PERCo-KT05*** – серия ЭП на базе тумбового турникета-трипода;
- ***PERCo-KTC01*** – серия ЭП на базе тумбового турникета-трипода со встроенным картоприемником;
- ***PERCo-KR05*** – серия ЭП на базе роторного турникета.

Устройства управления

PERCo-H6/4 – проводной пульт дистанционного управления (ПДУ) предназначен для автономного управлении ИУ. Оператор с помощью ПДУ может подать команду разблокировки ИУ для однократного прохода, установить режим свободного прохода или заблокировать ИУ. Также ПДУ снабжен светодиодной и звуковой индикацией. ПДУ входит в комплект поставки калиток, турникетов и ЭП производства компании ***PERCo***.

Устройство РУ (радиоуправления) – предназначено для автономного управлении ИУ. Комплект состоит из приемника, подключаемого к ИУ, и передатчиков в виде брелоков, с дальностью действия до 40 м. Оператор с помощью устройства РУ может подать команду разблокировки ИУ для однократного прохода, установить режим свободного прохода или заблокировать ИУ.

PERCo-AU01 – ИК-пульт ДУ предназначен для дистанционного управления ИУ. Оператор с помощью ИК-пульта может изменять установленный для направления прохода РКД или подать команду разблокировки ИУ для однократного прохода в этом направлении. ИК-пульт может использоваться с контроллером ***PERCo-CT/L04***. Для приема ИК-сигнала от пульта ДУ необходимо установить и подключить к контроллеру по интерфейсу *RS-485* выносной блок индикации с ИК-приемником ***PERCo-AI01***.

Кнопка ДУ «Выход» – предназначена для ручного управления ИУ при организации КПП с контролем проходов в одном направлении (например, для открытия двери при выходе из помещения). Может использоваться любая кнопка нефиксирующегося типа с нормально разомкнутыми «сухими» контактами.

Дополнительное оборудование

Картоприемники:

- Картоприемники серии ***PERCo-IC02***;
- Картоприемники сторонних производителей.

PERCo-AU05 (ТСВ) – табло системного времени предназначено для отображения времени. ТСВ подключается по интерфейсу *RS-485* к контроллерам ***PERCo-CT/L04*** и ***PERCo-CT03***.

ДКЗП (типа *CLIP-4*) – датчик контроля зоны прохода предназначен для регистрации несанкционированного прохода или проникновения под преграждающими планками.

Сирена – звуковой оповещатель.

Видеокамеры

В системе могут использоваться IP-видеокамеры и аналоговые видеокамеры, подключенные к IP-видеосерверам.

Примечание:

Список поддерживаемых моделей IP-видеокамер содержится на вкладке **Шаблоны камер** подраздела ***«Конфигурация верификации»*** раздела ***«Верификация»***.

6 Основные технические характеристики

Стандарт интерфейса связи	*Ethernet (IEEE 802.3)*
Скорости передачи данных *Ethernet*, *Мбит/с*	10/100
Количество контроллеров СКУД	не более 512
Интенсивность проходов со сменой пространственной зоны, *проходов/секунду*	
для контроллеров на 50000 карт	не более 50
для контроллеров на 10000 карт	не более 200
Формат карт доступа	*HID*, *EM-Marin*, *Mifare*
Общее число карт доступа, *шт.*	
сотрудников	не более 100 000
посетителей	не более 50 000
Число комиссионирующих карт для каждого контроллера, *шт.*	
для ИУ №1	192
для ИУ №2 и следующих	64
Число событий регистрации	
для каждого контроллера	не более 135 000
для ***PERCo-CR01 LICON***	не более 140 000
Количество пространственных зон контроля	не более 1024
Количество критериев доступа по времени типа	
временная зона (до 4-х временных интервалов)	не более 255
недельный график	не более 255
скользящий посуточный график (в пределах 30 суток)	не более 255
скользящих понедельных графиков (в пределах 54 недель)	не более 255
Количество дней с особым статусом, праздников (до 8 типов)	не более 365

Количество карт доступа, хранимых в контроллерах PERCo

Контроллер	Вариант конфигурации	К-во. карт
CL201.x	-	1000
CR01 LICON	-	5000
CL05	-	50000
CT03, CT/L04	Контроллер для управления турникетом	50000
CT03, CT/L04	Контроллер для управления турникетом с подключением до 8 шт. контроллеров замка ***PERCo-CL201.x***	10000
CT/L04	Контроллер для управления двумя односторонними дверьми с подключением до 8 шт. контроллеров замка ***PERCo-CL201.x***	по 1000 на каждый замок
CT/L04	Контроллер для управления одной двухсторонней дверью	50000
CT/L04	Контроллер для управления одной двухсторонней дверью с подключением до 8 шт. контроллеров замка ***PERCo-CL201.x***	10000

Примечания:

- Превышение указанной интенсивности проходов может привести к ошибкам в работе функции Antipass.
- События подключенных контроллеров второго уровня ***PERCo-CL201.x*** хранятся в памяти контроллера первого уровня.

Количество подключаемых:

IP видеокамер	не более 512
IP видеокамер на один видеосервер	не более 64
программных видеосерверов	не более 8
Частота записи видеоинформации, кадров/сек	не более 2
Количество точек верификации в одном шаблоне	не более 4
Количество шаблонов верификации	не более 512

Примечание:

На каждой точке верификации может транслироваться изображение с одной камеры.

7 Требования к аппаратным и программным средствам

Требования к аппаратным средствам сервера системы

Для работы ПО необходимы ПК, отвечающие следующим минимальным техническим требованиям:

- Процессор: *Intel Core i5* (с частотой не менее 3.2 ГГц),
- Оперативная память: 4 Гб,
- Объем дискового пространства: 10 Гб.
- Видеокарта и монитор с разрешением 1280x1024 пикселей.
- Сеть: *Ethernet* (IEEE 802.3) 10-BaseT, 100-BaseTX.

Требования к программным средствам сервера системы

Для работы системы на ПК должна быть установлена лицензионная версия ОС семейства *Microsoft Windows*. Допустимо использование 64-битных версий ОС.

- Рекомендованы к использованию версии *ОС Windows Server: 2008 R2, 2012 R2.*
- Возможно использование ОС *Windows: 7, 8.1*, *10*.

Для работы с системой необходим один из следующих web-браузеров:

- Mic*rosoft IE* версии 10 или выше;
- *Google Chrome* версии 32 или выше;
- *Mozilla Firefox* версии 32 или выше;
- *Opera* версии 30 или выше;
- *Microsoft Edge*.

Требования к аппаратным средствам АРМ

Для работы ПО необходимы ПК, отвечающие следующим минимальным техническим требованиям:

- Процессор:
  - минимальный: *Intel Celeron* (2 CPUs с частотой не менее 1.8 ГГц),
  - рекомендуемый: *Intel Core i3* (2 CPUs с частотой не менее 1.8 ГГц).
- Оперативная память:
  - минимальный: 2 Гб,
  - рекомендуемый: 4 Гб.
- Видеокарта и монитор с разрешением 1280x1024 пикселей.
- Сеть: *Ethernet* (IEEE 802.3) 10-BaseT, 100-BaseTX.

Требования к программным средствам АРМ

Для работы системы на ПК должна быть установлена лицензионная версия ОС семейства *Microsoft Windows* (*Windows 7, 8.1, 10*) или *Apple MacOS X* и выше, для работы на планшетах и смартфонах рекомендованы ОС: *Android 5,0* и выше, либо *iOS 8.0* и выше, либо *Ubuntu 14* и выше.

Для работы с системой необходим один из следующих web-браузеров:

- *Microsoft IE* версии 10 или выше;
- *Google Chrome* версии 32 или выше;
- *Mozilla Firefox* версии 32 или выше;

- *Opera* версии 30 или выше;
- *Microsoft Edge*;
- *Apple Safari 9* или выше.

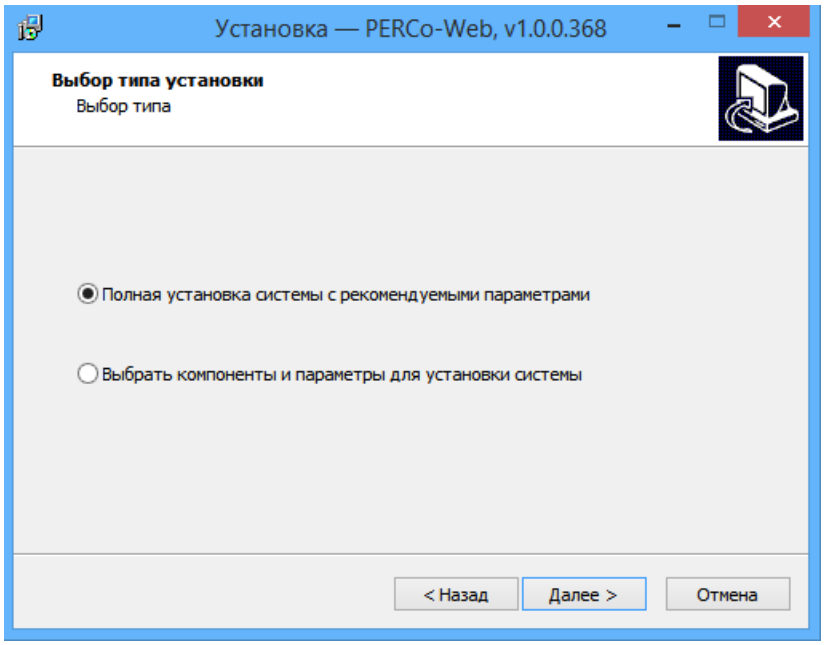
8 Установка системы

Внимание!

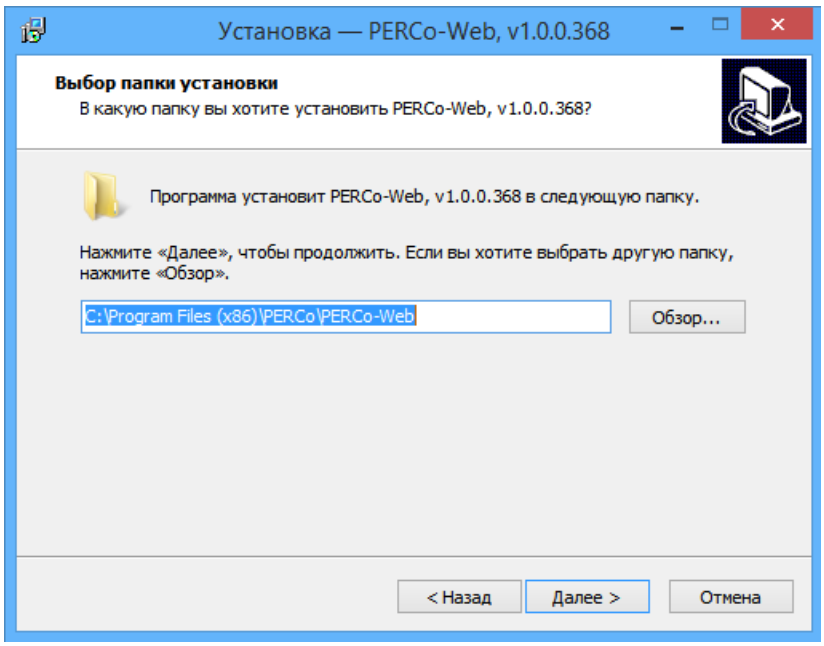
Для корректной работы сервера системы может потребоваться дополнительная настройка брандмауэра *Windows*.

При установке системы придерживайтесь следующей последовательности действий:

1. Запустите установочный файл `Setup.exe`. Следуйте указаниям мастера установки. Актуальная версия установочного файла системы *«PERCo-Web»* доступна на сайте компании ***PERCo***, расположенном по адресу www.perco.ru в разделе **Поддержка> Программное обеспечение**.
2. Выберите тип установки. Если нет необходимости выбора компонентов для установки и настройки сетевых параметров серверов системы, то выбирайте тип **Полная установка системы с рекомендованными параметрами**, в противном случае - **Выбор компонентов и параметры для установки системы**. Нажмите кнопку **Далее**.



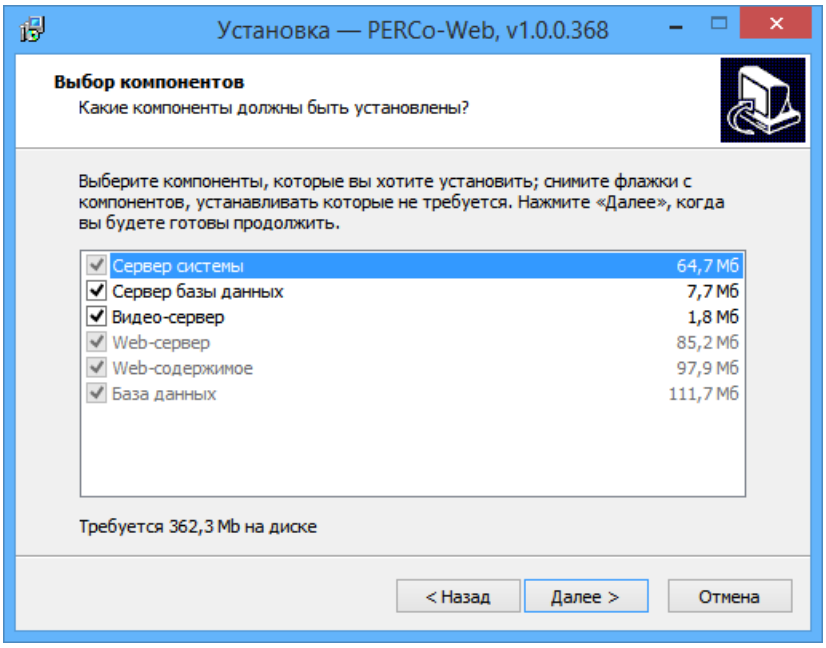
3. Укажите папку для установки системы. Нажмите кнопку **Далее**.



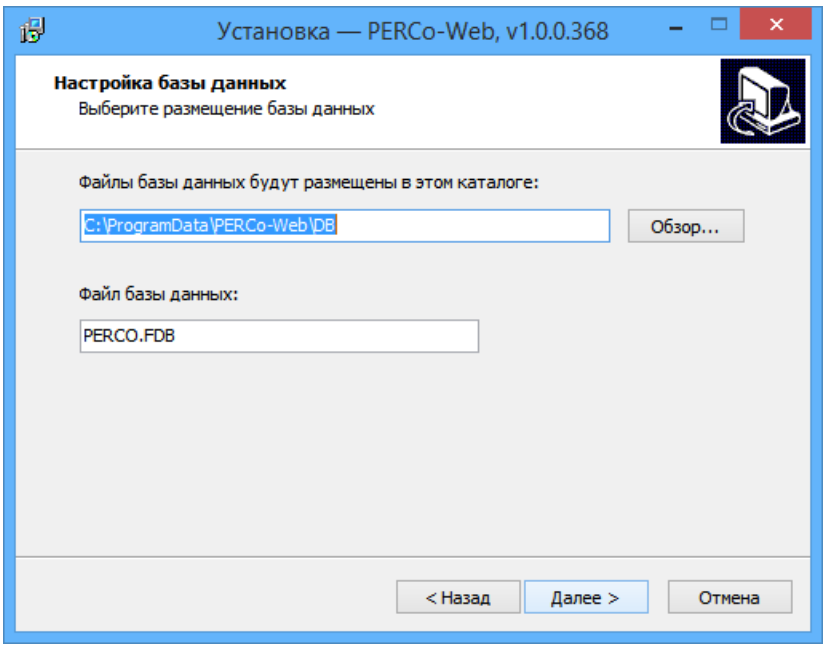
4. Отметьте флажками компоненты системы, которые необходимо установить на ПК. Нажмите кнопку **Далее**.

Примечание:

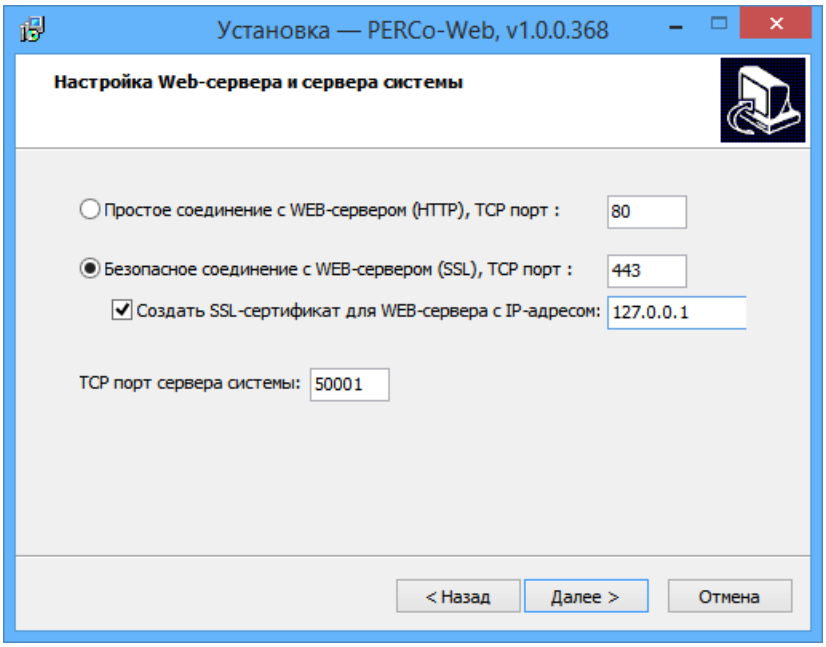
Если для установки был отмечен компонент **Сервер базы данных**, то перед установкой ПО системы будет запущен стандартный мастер установки SQL сервера *Firebird* и *FireBird ODBC Driver*.



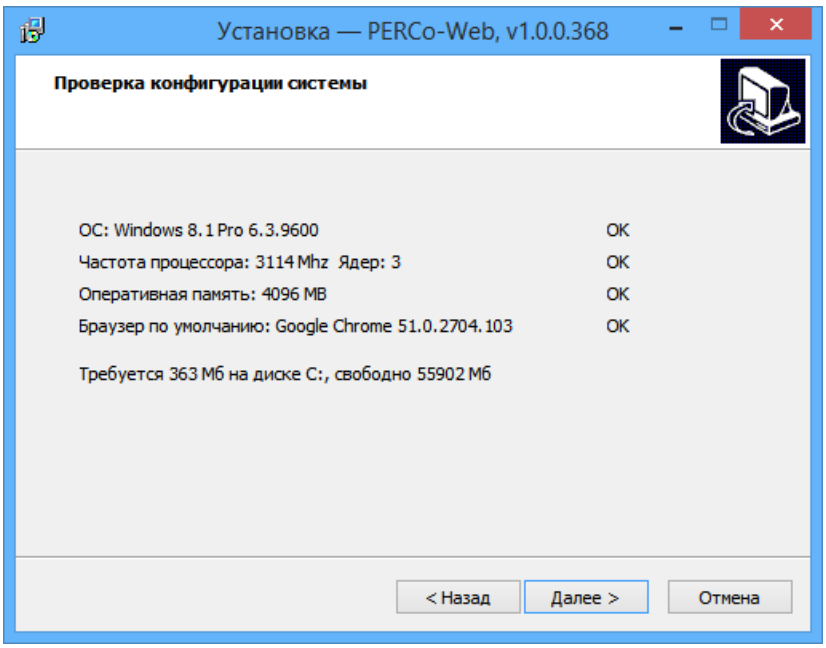
5. Укажите папку расположения БД системы. Нажмите кнопку **Далее**.



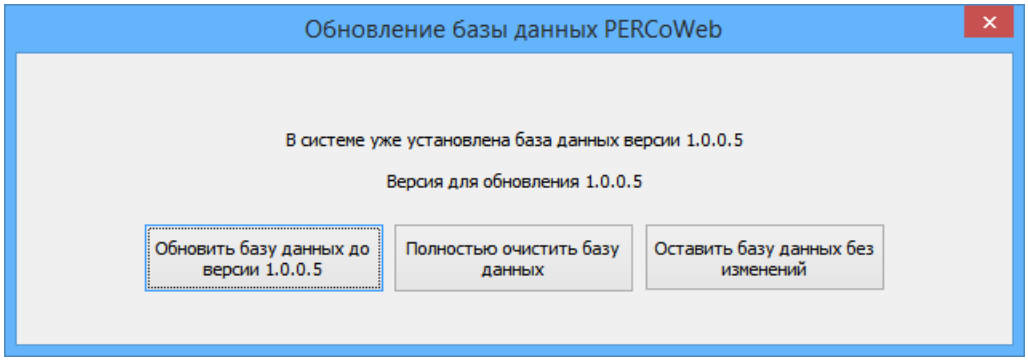
6. Произведите настройку сетевых параметров серверов системы. Нажмите кнопку **Далее**.



7. Будет проведена проверка конфигурации системы. По окончании проверки нажмите кнопку **Далее**.



8. Будет произведена установка системы на ПК. После завершения установки в указанной папке автоматически будет создана новая БД системы. Если в папке расположения БД находится созданная ранее БД, то откроется окно **Обновление базы данных**:



9. В открывшемся окне нажмите одну из кнопок:
   - **Обновить базу данных**
   - **Полностью очистить базу данных**
   - **Оставить базу данных без изменений**
10. При необходимости приобретите лицензию на ПО системы.

Примечание:

Для полного удаления всех модулей системы 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 *«PERCoWeb»* и нажмите кнопку **Удалить**.

9 Управление лицензиями

ПО системы состоит из модуля ***«Стандартный пакет ПО»*** и дополнительных модулей ПО для расширения функциональных возможностей системы. ПО может приобретаться как в составе комплекта из нескольких модулей, так и отдельными модулями. Функционирование дополнительных модулей возможно только совместно с модулем ***«Стандартный пакет ПО»***. Для приобретения доступны:

- ***PERCo-WS «Стандартный пакет ПО»*** – позволяет организовать полноценную СКУД с поддержкой всех основных функций обеспечения безопасности, в том числе: контроль доступа по времени, контроль зональности (antipass), доступ с комиссионированием.
- ***PERCo-WM-01 Модуль «Учет рабочего времени»*** – позволяет вести учет рабочего времени сотрудников и составлять отчеты о дисциплине труда.
- ***PERCo-WM-02 Модуль «Верификация»*** – позволяет усилить контроль доступа на территорию предприятия за счет проведения оператором КПП процедуры верификации.

Для упрощения процедуры приобретения лицензии на ПО системы, а также для знакомства с его возможностями, в течение 60 дней с момента первого запуска ПО работает в ознакомительном режиме. При этом сохраняются все функциональные возможности всех модулей ПО.

После окончания ознакомительного периода доступ к дополнительным модулям ПО, для которых не введен код активации, будет запрещен. Если не была приобретена лицензия на ***«Стандартный пакет ПО»***, то ПО автоматически перейдет на состав бесплатного модуля ***PERCo-WB «Базовый пакет ПО»*** со следующими ограничениями:

- количество карт доступа в системе будет ограничено первыми выданными 100 картами;
- возможность ввода данных и выдачи карт доступа посетителям будет недоступна.

При этом вся введенная ранее информация о картах доступа и посетителях будет сохранена в БД системы и доступ к ней будет восстановлен после приобретения модуля ***«Стандартный пакет ПО»***.

В качестве *электронного ключа защиты* ПО системы от несанкционированного использования применяется один из контроллеров системы. Выполнение функции ключа не влияет на функционирование контроллера. Для использования в качестве ключа контроллер должен быть добавлен в конфигурацию системы в подразделе ***«Конфигурация»*** раздела ***«Администрирование»***.

После ввода *кода активации* в случае отсутствия связи между контроллером-ключом и сервером системы все лицензированные модули ПО продолжают функционировать без каких-либо ограничений в течение 30 дней. Если в течение этого периода связь не восстановлена, то блокируется доступ ко всем разделам ПО, кроме раздела ***«Администрирование»*** (для ввода ключа активации). При этом вся введенная ранее в системе информация сохраняется в БД системы и доступ к ней будет разрешен после восстановления связи с контроллером-ключом.

Состав модулей ПО PERCo-Web

Модуль ПО	Входящие в модуль разделы
PERCo-WB «Базовый пакет ПО»	***«Администрирование»*** ***«Персонал»*** ***«Бюро пропусков»***, подразделы: • ***«Сотрудники»*** • ***«Шаблоны доступа»*** ***«Контроль доступа»***, подразделы: • ***«Управление устройствами»*** • ***«Отчет по доступу в помещения»***
PERCo-WS «Стандартный пакет ПО»	Все разделы, входящие в ***«Бесплатное ПО»***, а также: ***«Бюро пропусков»*** • ***«Посетители»*** • ***«Дизайн пропуска»*** • ***«Отчет по посетителям»*** ***«Контроль доступа»***, подраздел: • ***«Отчет о проходах»*** ***«Заказ пропуска»***
PERCo-WM-01 «Учет рабочего времени»	***«Учет рабочего времени»*** ***«Контроль доступа»***, подраздел: • ***«Местонахождение»***
PERCo-WM-02 «Верификация»	***«Верификация»*** ***«Контроль доступа»***, подраздел: • ***«Журнал верификации»***

Порядок приобретения лицензии на ПО

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 системы.
2. Заполните заявку для приобретения лицензии на ПО системы. Заявку можно заполнить на сайте компании **PERCo**, по адресу www.perco.ru в разделе **Продукция> Системы контроля доступа> СКУД PERCo-Web> Программное обеспечение> Порядок лицензирования**. В заявке необходимо указать:

- MAC-адрес выбранного контроллера,
- перечень приобретаемых модулей.

3. После получения лицензионного соглашения, содержащего коды активации модулей системы, необходимо ввести их в подразделе ***«Лицензии»*** раздела ***«Администрирование»***.

10 Менеджер системы PERCo-Web

Окно *«Менеджера системы PERCo-Web»* (далее – *«Менеджер PERCo-Web»*) открывается нажатием на иконку на рабочем столе или в области уведомлений. В окне *«Менеджера PERCo-Web»* доступны две вкладки:

Вкладка **Состояние** предназначена для:
- запуска и остановки серверов системы;
- просмотра списка контроллеров, подключенных к серверу системы.

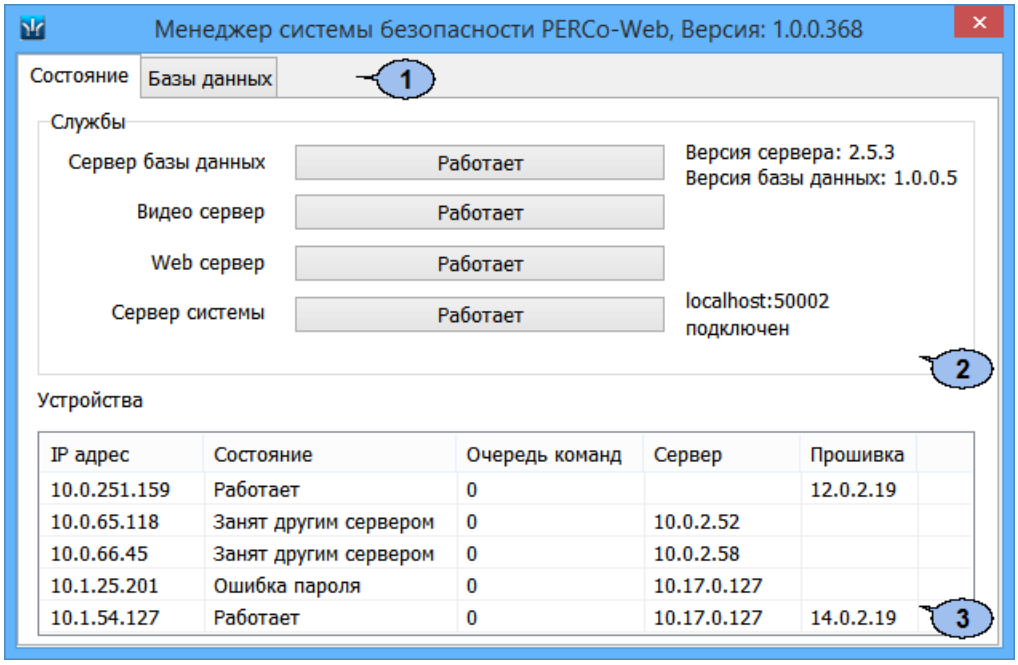
Вкладка **Базы данных** предназначена для:
- указания путей расположения файлов БД и резервной копии БД системы;
- создания резервной копии БД системы;

  Примечание:
  В системе предусмотрена возможность автоматического создания резервной копии БД по расписанию. Создание расписания производится в подразделе ***«Задания»*** раздела ***«Администрирование»***.

- восстановления БД из созданного ранее файла резервной копии;
- импорт БД из файла более ранних версий БД системы.

10.1 Управление серверами системы

Запуск и остановка серверов системы осуществляется на вкладке **Состояние** окна *«Менеджера PERCo-Web»*. Вкладка имеет следующий вид:



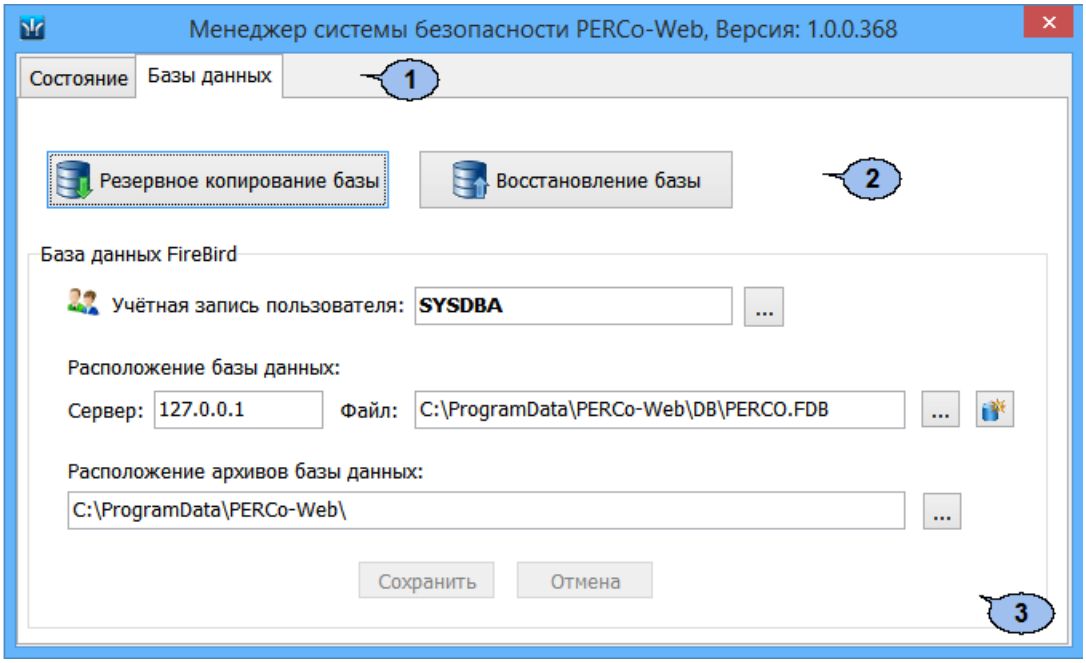
1. Выбор вкладки окна:
   - **Состояние**
   - **Базы данных**

2. Панель **Службы** содержит кнопки для запуска и остановки серверов системы.

3. Рабочая область вкладки содержит список контроллеров, подключенных к серверу системы.

10.2 Управление БД

Управление БД системы осуществляется на вкладке **Базы данных** окна *«Менеджера PERCo-Web»*. Вкладка имеет следующий вид:



1. Выбор вкладки окна:
   - **Состояние**
   - **Базы данных**

2. Кнопки управления БД:
   Резервное копирование базы – кнопка позволяет создать резервную копию БД.
   Восстановление базы – кнопка позволяет восстановить БД из созданной ранее резервной копии.

3. Панель **База данных FireBird** содержит следующие элементы:
   Учетная запись пользователя: – при нажатии кнопки … справа от поля открывается окно для создания новой учетной записи пользователя БД или выбора одной из созданных ранее.
   Расположение базы данных:
   Сервер: – поле для ввода IP-адреса ПК, на котором установлена СУБД.
   Файл – при нажатии кнопки … справа от поля откроется окно проводника для выбора папки расположения БД.
   Создать новую базу данных – кнопка позволяет создать новую БД в указанной папке.
   Расположение архивов базы данных: – при нажатии кнопки …

справа от поля откроется окно проводника для выбора папки расположения резервной копии БД.

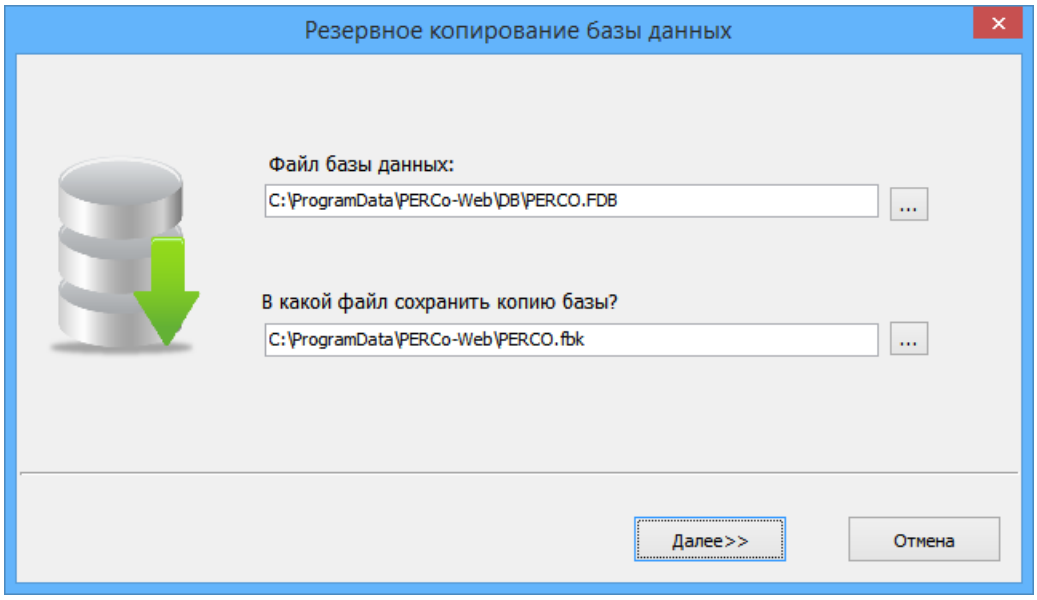
Сохранить – кнопка позволяет сохранить внесенные на панели изменения.

Отмена – кнопка позволяет отменить внесенные на панели изменения.

10.2.1 Резервное копирование БД

Для создания резервной копии БД:

1. Запустите *«Менеджер PERCo-Web»*.
2. Перейдите на вкладку **Базы данных**.
3. Нажмите кнопку **Резервное копирование базы**. Откроется окно **Резервное копирование базы данных**:

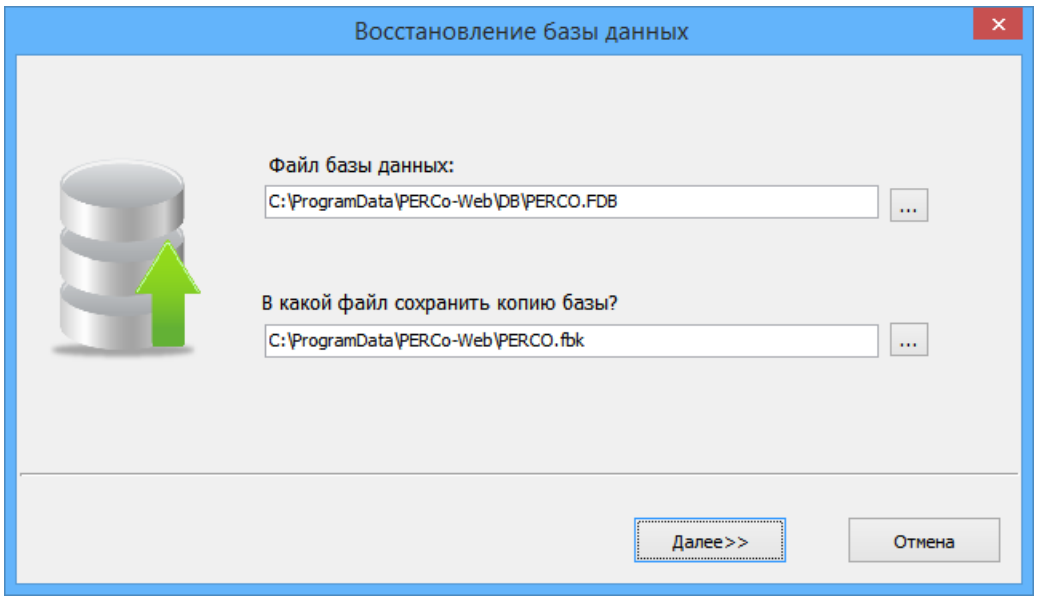


4. В открывшемся окне нажмите кнопку ... справа от поля **Файл базы данных**. В открывшемся окне проводника выберите папку расположения БД.
5. Нажмите кнопку ... справа от поля **В какой файл сохранить копию базы?**. В открывшемся окне проводника выберите папку, в которой необходимо сохранить резервную копию БД. Нажмите кнопку **Далее**.
6. Будет запущен процесс сохранения резервной копии БД. По окончании процесса нажмите кнопку **ОК**. Окно **Резервное копирование базы данных** будет закрыто.

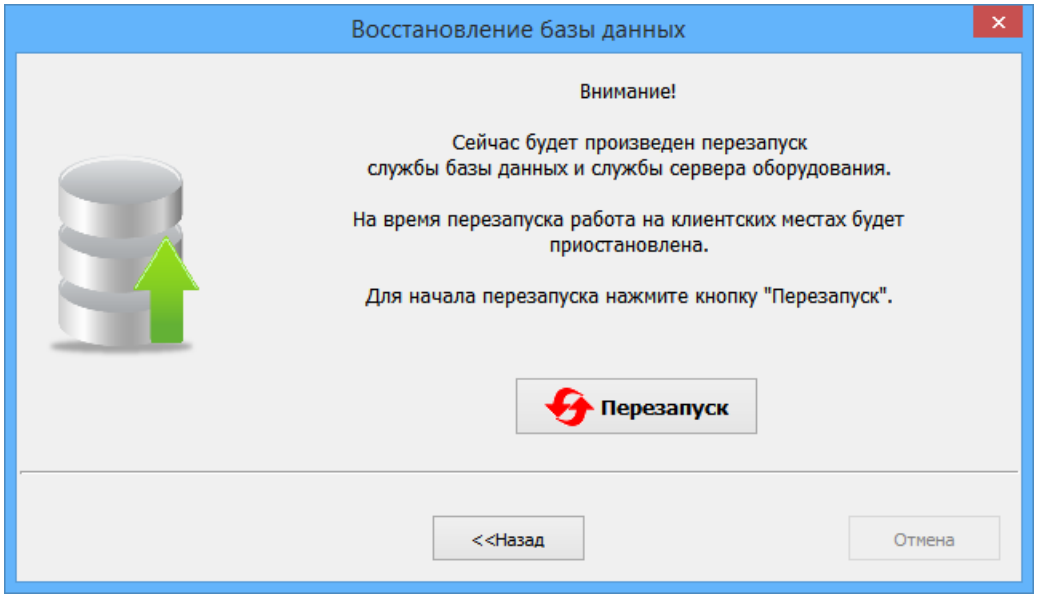
10.2.2 Восстановление БД из резервной копии

Для создания резервной копии БД:

1. Запустите *«Менеджер PERCo-Web»*.
2. Перейдите на вкладку **Базы данных**.
3. Нажмите кнопку **Восстановление базы**. Откроется окно **Восстановление базы данных**:



4. В открывшемся окне нажмите кнопку ... справа от поля **Выберите файл базы данных из архива**. В открывшемся окне проводника выберите папку расположения резервной копии БД.
5. Нажмите кнопку ... справа от поля **В какой файл восстановить базу?**. В открывшемся окне проводника выберите папку, в которой необходимо сохранить восстановленную БД. Нажмите кнопку **Далее**.
6. Будет запущен процесс восстановления БД. По окончании процесса нажмите кнопку **Далее**. В рабочей области окна появится сообщение о необходимости перезапуска серверов системы и кнопка **Перезапуск**.



7. Нажмите кнопку **Перезапуск**. По окончании процесса перезапуска серверов системы нажмите кнопку ОК . Окно **Восстановление базы данных** будет закрыто. Сервер системы начнет работу с восстановленной БД.

11 Предварительная настройка

При подготовке системы к работе придерживайтесь следующей последовательности действий:

1. Осуществите вход в систему, используя web-браузер. Для этого в адресной строке браузера введите IP-адрес ПК, на котором установлен сервер системы. При первом входе в систему необходимо задать пароль для неизменяемой учетной записи `admin`.

2. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
   - Откройте подраздел ***«Конфигурация»***.
     - выберите язык и формат отображения дат в системе;
     - создайте список помещений предприятия;
     - произведите поиск и добавление контроллеров в конфигурацию системы;
     - Разместите контроллеры на схеме помещений.
   - Откройте подраздел ***«Роли и права операторов»***, создайте необходимые роли операторов и установите для них полномочия.
   - Откройте подраздел ***«Операторы»***, создайте учетные записи для операторов системы, назначьте им созданные ранее роли и выдайте права на разделы.

3. Используя панель навигации, перейдите в раздел ***«Бюро пропусков»***. Откройте подраздел ***«Шаблоны доступа»***.
   - Создайте шаблоны доступа для сотрудников предприятия и посетителей. При создании шаблона для каждого помещения устанавливаются индивидуальные права доступа и критерии доступа по времени.
   - При необходимости отредактируйте календарь праздничных дней, доступ в которые будет ограничен или запрещен.

4. Используя панель навигации, перейдите в раздел ***«Персонал»***.
   - Откройте подраздел ***«Должности»*** и создайте список должностей предприятия.
   - Откройте подраздел ***«Дополнительные данные»*** и при необходимости создайте поля для ввода дополнительных текстовых и графических данных.
   - Откройте подраздел ***«График работы»***:
     - создайте графики работы для сотрудников предприятия. Укажите для каждого графика регистрирующие помещения и параметры составления отчетов по дисциплине труда;
     - При необходимости отредактируйте календарь праздничных дней (календарь используется при составлении отчетов в разделе ***«Учет рабочего времени»***).
   - Откройте подраздел ***«Подразделения»*** и создайте список структурных подразделений предприятия. Для каждого подразделения укажите данные, которые будут автоматически устанавливаться сотрудникам и посетителям подразделения.

5. Используя панель навигации, перейдите в раздел  ***«Бюро пропусков»***. Откройте подраздел ***«Дизайн пропуска»*** и создайте шаблоны дизайна пропусков сотрудников и посетителей для подразделений предприятия.
6. Используя панель навигации, перейдите в раздел  ***«Персонал»***. Откройте подраздел ***«Сотрудники»*** и создайте список сотрудников предприятия. Для каждого сотрудника:
   - Заполните учетную карточку (укажите ФИО, подразделений, должность, график работы и т.д.).
   - Добавьте фотографию.
   - Выдайте карту доступа и установите шаблон доступа.
   - Распечатайте пропуск (наклейку на карту доступа).
7. Используя панель навигации, перейдите в раздел  ***«Администрирование»***. Откройте подраздел ***«Конфигурация»*** и при необходимости укажите для контроллеров сотрудников, карты доступа которых будут являться комиссионирующими.
8. Настройте функции контроля персональных параметров доступа карт в системе.

12 Функции Antipass и Global Antipass

В системе предусмотрена возможность включения и отключения функций контроля персональных параметров карт доступа.

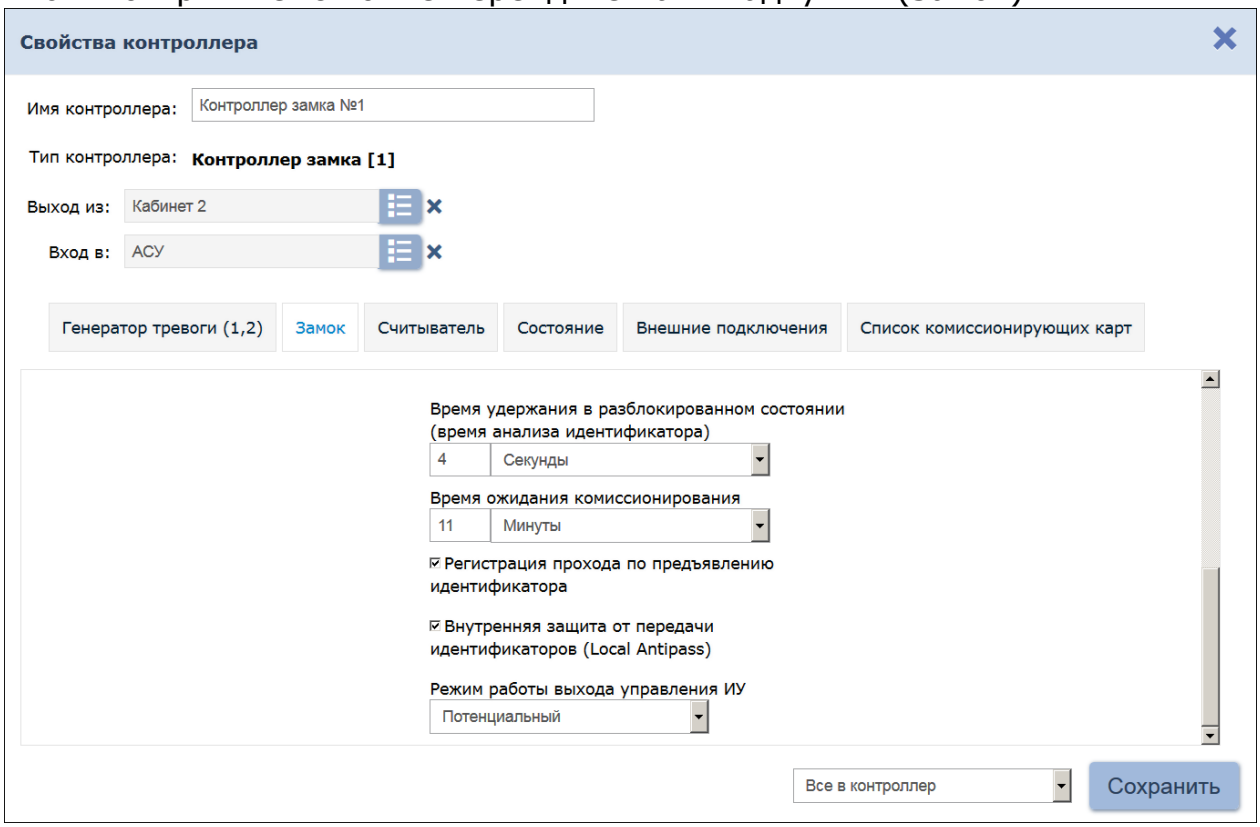
Функция Antipass

Примечание:

Для использования функции antipass в шаблоне доступа карты необходимо указать помещения, при доступе в которые должен производиться контроль. Настройка шаблона проводится в подразделе ***«Шаблон доступа»*** раздела ***«Бюро пропусков»***.

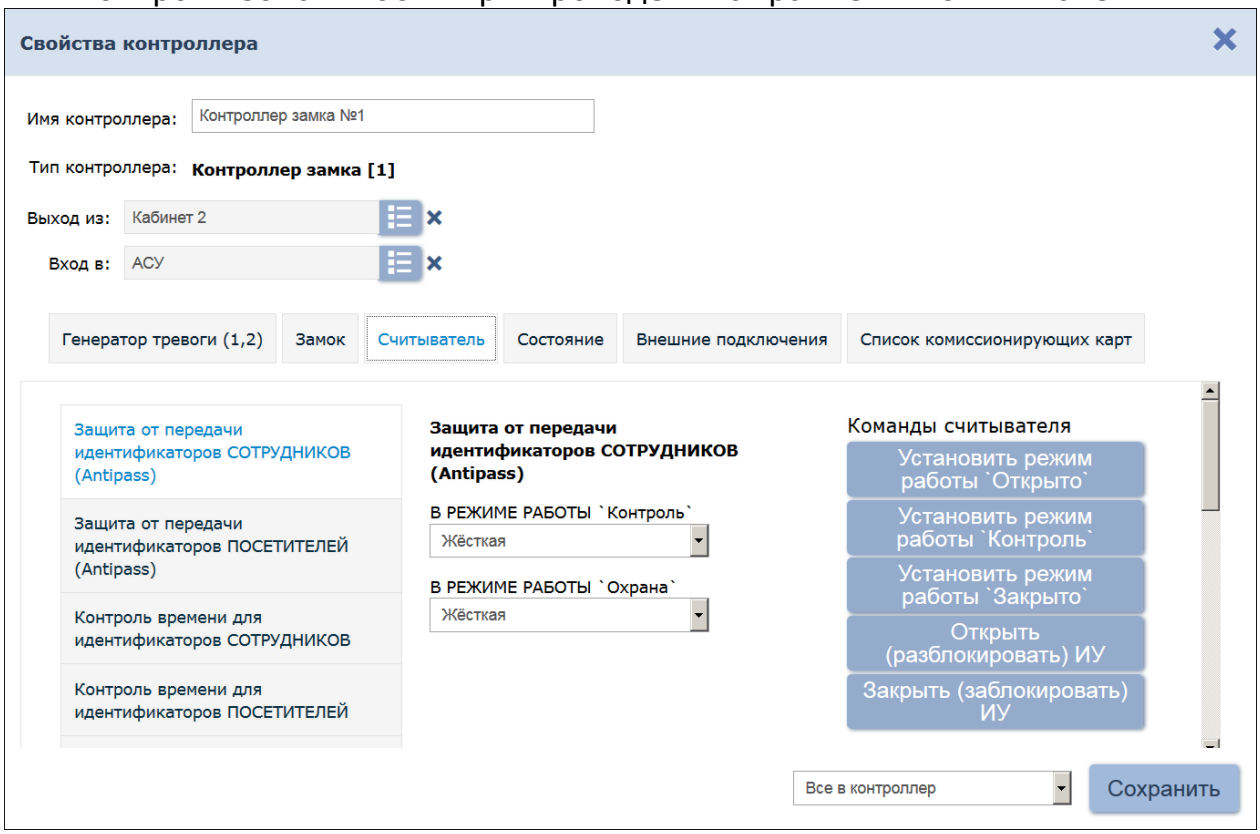
Для включения/ отключения функции контроля зональности:

1. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
2. Откройте подраздел ***«Конфигурация»***.
3. Перейдите на вкладку **Контроллеры**.
4. В рабочей области страницы выберите контроллер, для которого необходимо включить функцию контроля зональности.
5. Нажмите кнопку **Редактировать** на панели инструментов страницы. Откроется окно **Свойства контроллера**.
6. В открывшемся окне перейдите на вкладку **ИУ** (Замок).



7. В рабочей области окна для включения/ отключения функции контроля зональности на выбранном ИУ установите/ снимите флажок у параметра **Внутренняя защита от передачи идентификаторов (Local Antipass)**.
8. Перейдите на вкладку **Считыватель** для настройки параметров

контроля зональности при проходе в направлении считывателя.

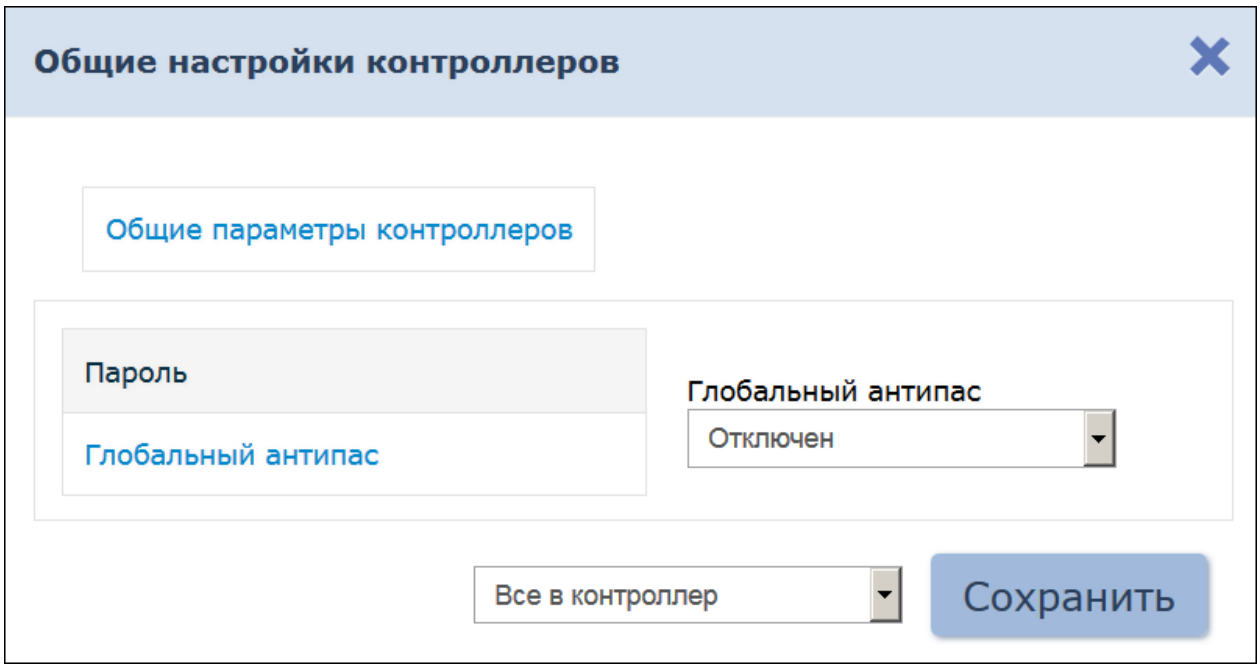


9. В рабочей области окна независимо для сотрудников и посетителей установите жесткий или мягкий режим контроля зональности при различных РКД.
10. Нажмите кнопку **Сохранить**. Окно **Свойства контроллера** будет закрыто, измененные параметры будут переданы в контроллер.

Функция Global Antipass

Для включения/ отключения функции глобального контроля зональности:

1. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
2. Откройте подраздел ***«Конфигурация»***.
3. Перейдите на вкладку **Контроллеры**.
4. В рабочей области страницы выберите корневой элемент списка **Общие параметры контроллеров**.
5. Нажмите кнопку **Редактировать** на панели инструментов страницы. Откроется окно **Общие настройки контроллеров**.
6. В левой части окна нажмите кнопку **Глобальный антипас**. Рабочая область окна примет следующий вид:



7. Для включения/ отключения функции глобального контроля зональности в раскрывающемся списке **Глобальный антипас** выберите **Включен**/ **Отключен**.
8. Нажмите кнопку **Сохранить**. Окно **Общие настройки контроллеров** будет закрыто, измененные параметры будут переданы в контроллеры системы.

13 Раздел «Администрирование»

Раздел предназначен для организации АРМ сотрудника предприятия, занимающегося настройкой и администрированием системы. Раздела позволяет произвести первичное конфигурирование оборудования системы, добавление операторов системы и ее лицензирование. Использование раздела позволяет контролировать работу системы, составляя отчеты о регистрируемых событиях.

13.1 Подраздел «Конфигурация»

В подразделе доступны следующие вкладки:

Вкладка **Помещения** предназначена для создания списка помещений предприятия.

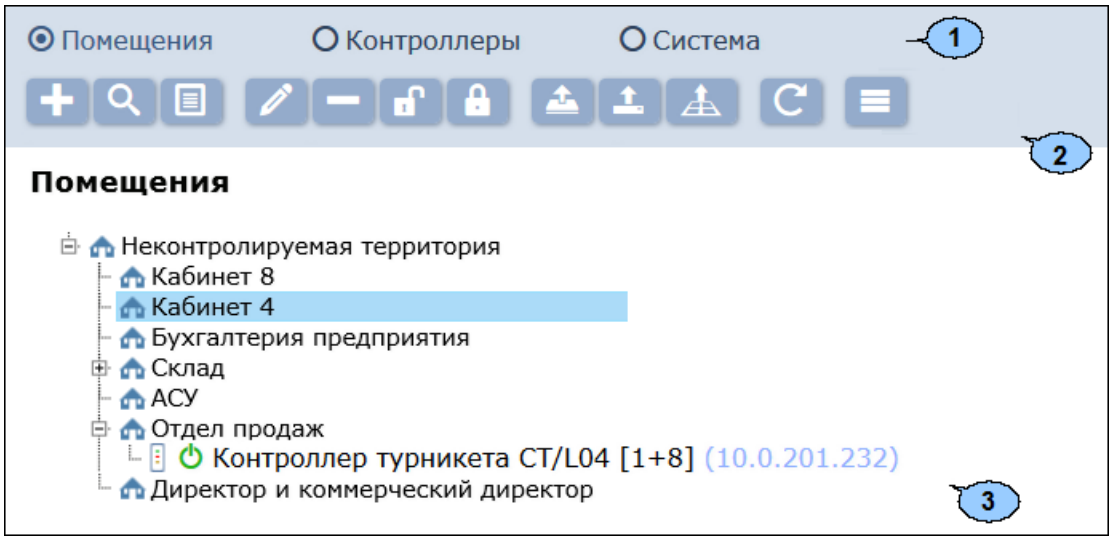
Вкладка **Контроллеры** предназначена для:

- поиска контроллеров в локальной сети и добавления в конфигурацию системы;
- настройки параметров контроллеров и их ресурсов;
- подачи команд управления;
- временного исключения контроллера из конфигурации;
- создания списка комиссионирующих карт.

Вкладка **Система** предназначена для выбора языка интерфейса системы.

13.1.1 Вкладка «Помещения»

Страница вкладки имеет следующий вид:



1. Переключатель выбора вкладки подраздела:
   - **Помещения**
   - **Контроллеры**
   - **Система**
2. Панель инструментов страницы:

   Добавить помещение – кнопка позволяет добавить вложенное помещение в помещение, выделенное в рабочей области страницы.

 **Поиск контроллеров** – кнопка позволяет произвести поиск контроллеров (которые ранее не были добавлены в конфигурацию системы) в локальной сети и разместить их в выделенном в рабочей области страницы помещении.

 **Установить контроллер** – кнопка позволяет разместить контроллеры, добавленные ранее в конфигурацию системы, в выделенном в рабочей области страницы помещении.

 **Редактировать** – кнопка позволяет изменить название выделенного в рабочей области панели помещен или настроить параметры выделенного в рабочей области контроллера.

 **Удалить помещение/ Отвязать контроллер** – кнопка позволяет удалить выделенное в рабочей области страницы помещение или контроллер из помещения.

 **Активировать** – кнопка позволяет включить в конфигурацию системы ранее исключенный или найденный контроллер.

 **Деактивировать** – кнопка позволяет временно исключить из конфигурации системы контроллер, выделенный в рабочей области страницы. При этом наименование исключенного контроллера затеняется.

 **Передать изменения конфигурации в контроллеры** – кнопка позволяет передать измененные параметры в контроллеры системы.

 **Передать всю конфигурацию в контроллеры** – кнопка позволяет передать все параметры в контроллеры системы.

 **Передать зоны безопасности считывателей** – кнопка позволяет передать в контроллеры системы информацию о расположении считывателей относительно пространственных зон безопасности.

 **Обновить помещения и контроллеры** – кнопка позволяет обновить информацию о состоянии контроллеров системы.

 **Дополнительно** – кнопка позволяет открыть меню команд для выбора дополнительных действий:

- **Печать таблицы** – позволяет распечатать список помещений с указанием расположенных в них контроллеров.
- **Экспорт в XLS** – позволяет сохранить список помещений с указанием расположенных в них контроллеров в файл электронных таблиц *MS Office Excel* с расширением `.xls`.
- **Экспорт в CSV** – позволяет сохранить список помещений с указанием расположенных в них контроллеров в файл электронных таблиц *OpenOffice Calc* с расширением `.csv`.

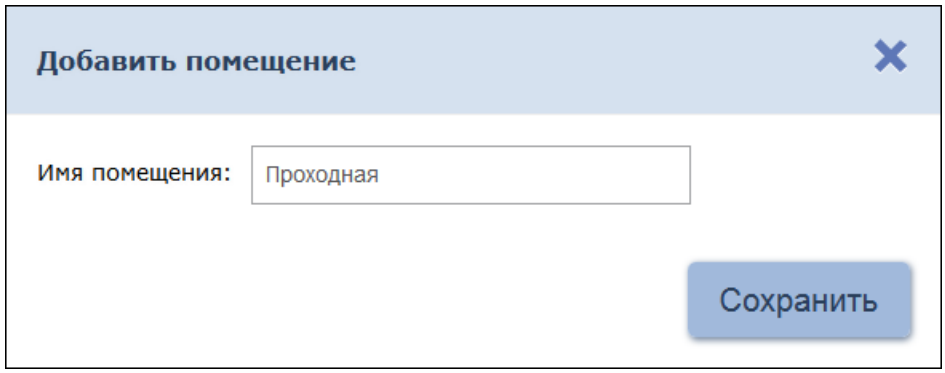
3. Рабочая область страницы содержит многоуровневый раскрывающийся список помещений с указанием расположенных в них контроллеров. По умолчанию в рабочей области находится неудаляемое помещение *«Неконтролируемая территория».*

Примечание:
В рабочей области панели реализована функция Drag-and-drop, позволяющая изменять расположение помещений в списке с помощью мыши.

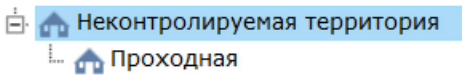
Создание списка помещений

Для создания списка помещений:

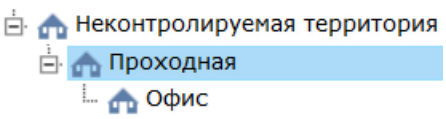
1. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
2. Откройте подраздел ***«Конфигурация»***.
3. Перейдите на вкладку **Помещения**.
4. Выделите в рабочей области страницы помещение *«Неконтролируемая территория»*.
5. Нажмите на панели инструментов страницы кнопку **Добавить помещение** . Откроется окно **Добавить помещение**:



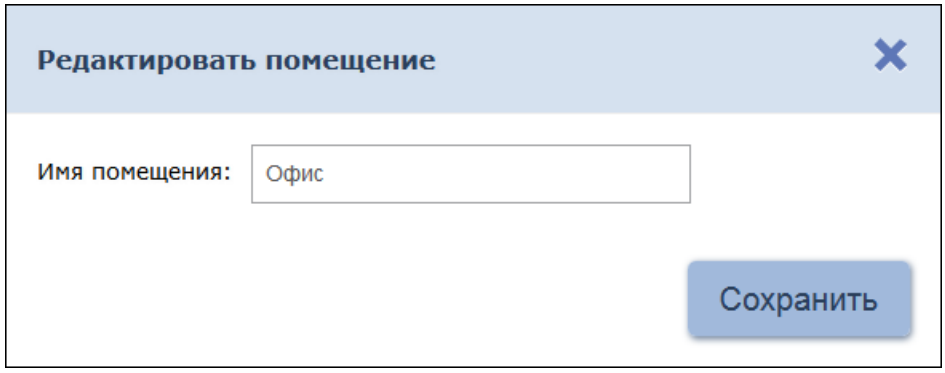
6. В открывшемся окне введите название нового помещения и нажмите кнопку **Сохранить**. Окно будет закрыто, помещение будет добавлено в раскрывающийся список в рабочей области страницы, как вложенное в помещение *«Неконтролируемая территория»*:



7. Для добавления вложенного помещения выделите в рабочей области страницы то помещение, в которое необходимо добавить вложенное, и нажмите кнопку **Добавить помещение** . Откроется окно **Добавить помещение**.
8. В открывшемся окне введите название нового помещения и нажмите кнопку **Сохранить**. Окно будет закрыто, помещение будет добавлено в выделенное в рабочей области страницы:



9. Для изменения названия добавленного ранее помещения выделите его в рабочей области страницы и нажмите на панели инструментов страницы кнопку **Редактировать** . Откроется окно **Редактировать помещение**:

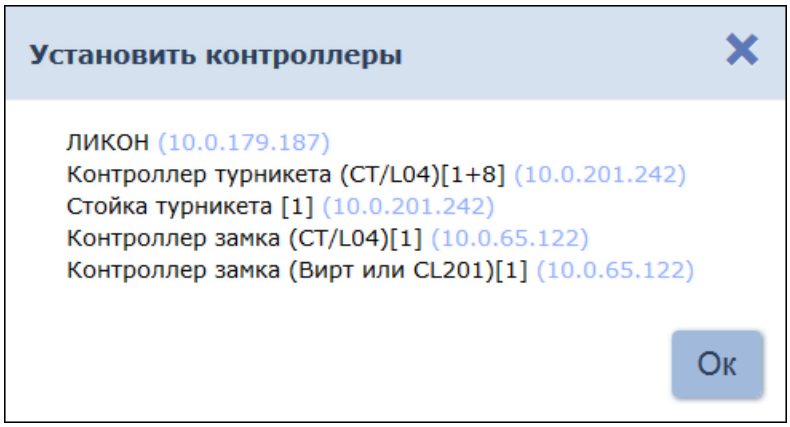


10. В открывшемся окне произведите необходимые изменения и нажмите кнопку **Сохранить**.
11. Для удаления добавленного ранее помещения выделите его в рабочей области страницы и нажмите кнопку **Удалить помещение/ Отвязать контроллер** на панели инструментов страницы. В открывшемся окне подтверждения нажмите кнопку **ОК**. Помещение будет удалено из списка.

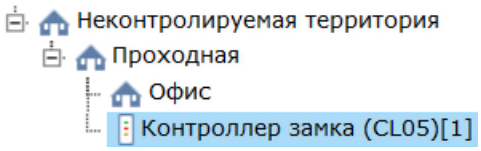
Размещение контроллеров в помещениях

После создания списка помещений необходимо расположить в них контроллеры, входящие в систему ***PERCo-Web*** . Для размещения контроллеров в помещениях:

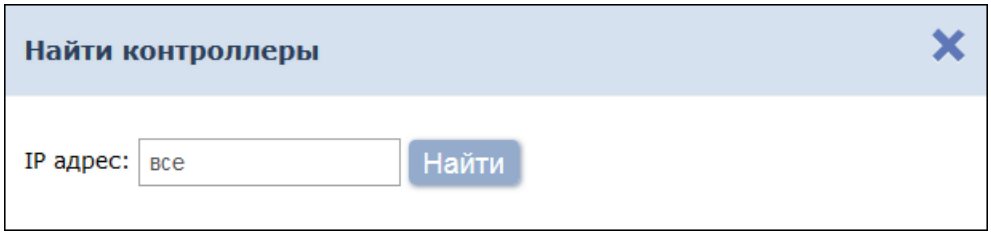
1. Для размещения контроллера в одно из помещений выделите это помещение в рабочей области страницы и нажмите на панели инструментов кнопку **Установить контроллер** . Откроется окно **Установить контроллеры**, содержащее список контроллеров, добавленных ранее в конфигурацию системы:



2. В открывшемся окне выделите контроллер и нажмите кнопку **Ок**. Наименование контроллера появится в выделенном помещении:



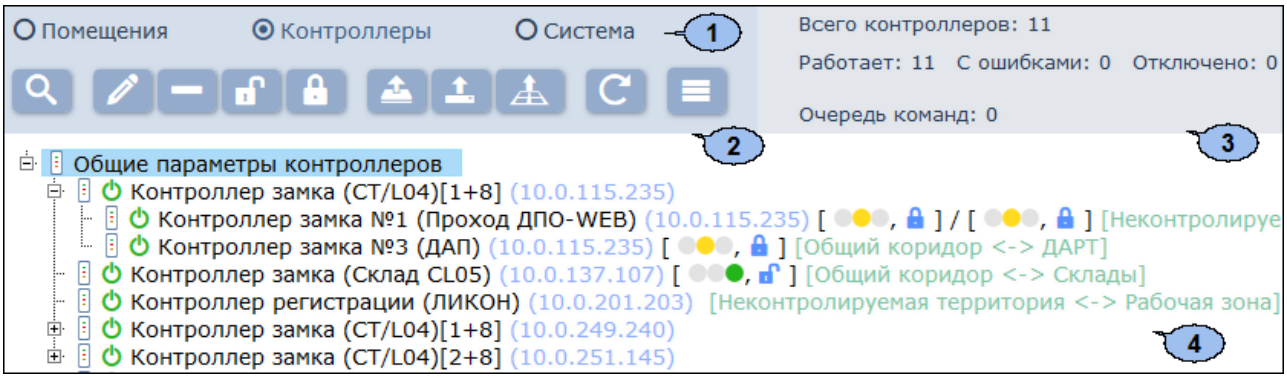
3. При необходимости в помещении можно расположить контроллер, который ранее не был добавлен в конфигурацию системы. Для этого выделите помещение и нажмите кнопку **Поиск контроллеров** . Откроется окно **Найти контроллеры**:



4. В открывшемся окне введите IP-адрес искомого контроллера и нажмите кнопку **Найти**. Найденный контроллер будет размещен в помещении и автоматически добавлен в конфигурацию системы.
5. При необходимости произведите настройку параметров работы контроллера. Для этого выделите контроллер в рабочей области страницы и нажмите на панели инструментов страницы кнопку **Редактировать** . В открывшемся окне **Свойства контроллера** произведите необходимые изменения и нажмите кнопку **Сохранить и закрыть**.
6. Для контроллеров электромеханических замков модели ***PERCo-CL05.1***, открывающихся при подаче напряжения, возможна совместная работа двух контроллеров при организации КПП с контролем проходов в двух направлениях. Для поддержки смены зональности при проходе через такое КПП, необходимо установить флажок у параметра **Смена зоны при проходе** соответствующего контроллеру ИУ ресурса в окне **Свойства контроллера**.
7. Для удаления добавленного ранее в помещение контроллера выделите его в рабочей области страницы и нажмите кнопку **Удалить помещение/ Отвязать контроллер** на панели инструментов. В открывшемся окне подтверждения нажмите кнопку **ОК**. Помещение будет удалено из списка.
8. Нажмите на панели инструментов страницы кнопку **Передать всю конфигурацию в контроллеры** .

13.1.2 Вкладка «Контроллеры»

Страница вкладки имеет следующий вид:



1. Переключатель выбора вкладки подраздела:
   - **Помещения**
   - **Контроллеры**
   - **Система**
2. Панель инструментов страницы:

   Поиск контроллеров – кнопка позволяет произвести поиск контроллеров, которые ранее не были добавлены в конфигурацию системы, в локальной сети.

   Редактировать – кнопка позволяет открыть окно **Свойства контроллера** для изменения параметров выделенного в рабочей области панели контроллера и его ресурсов. Если в рабочей области страницы выделен корневой элемент *«Общие параметры контроллеров»*, то открывается окно **Общие настройки контроллеров**.

   Удалить – кнопка позволяет удалить выделенный в рабочей области панели контроллер из конфигурации системы.

   Активировать – кнопка позволяет включит в конфигурацию системы ранее исключенный или найденный контроллер.

   Деактивировать – кнопка позволяет временно исключить из конфигурации системы контроллер, выделенный в рабочей области страницы. При этом наименование контроллера затеняется.

   Передать изменения конфигурации в контроллеры – кнопка позволяет передать измененные параметры в контроллеры системы.

   Передать всю конфигурацию в контроллеры – кнопка позволяет передать все параметры в контроллеры системы.

   Передать зоны безопасности считывателей – кнопка позволяет передать в контроллеры системы информацию о расположении считывателей относительно пространственных зон безопасности.

   Обновить помещения и контроллеры – кнопка позволяет

обновить информацию о состоянии контроллеров системы.

Дополнительно – кнопка позволяет открыть меню команд для выбора дополнительных действий:

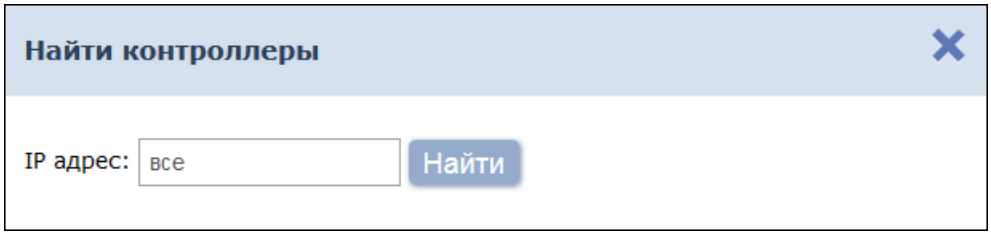
- **Печать таблицы** – позволяет распечатать список помещений с указанием расположенных в них контроллеров.
- **Экспорт в XLS** – позволяет сохранить список помещений с указанием расположенных в них контроллеров в файл электронных таблиц *MS Office Excel* с расширением `.xls`.
- **Экспорт в CSV** – позволяет сохранить список помещений с указанием расположенных в них контроллеров в файл электронных таблиц *OpenOffice Calc* с расширением `.csv`.
- **Выделить все контроллеры (Ctrl+A)** – позволяет выделить все контроллеры.

3. Панель информации о состоянии контроллеров системы.
4. Рабочая область страницы содержит список контроллеров, добавленных в конфигурацию системы. Значок **Валидность** слева от наименования указывает на то, что в контроллер не были переданы измененные параметры. Справа от наименования контроллера расположены значки, указывающие на установленный РКД и состояние ИУ:
   - – РКД *«Открыто»*,
   - – РКД *«Контроль»*,
   - – РКД *«Закрыто»*,
   - – ИУ заблокировано,
   - – ИУ разблокировано,
   - – взлом ИУ.

Поиск контроллеров

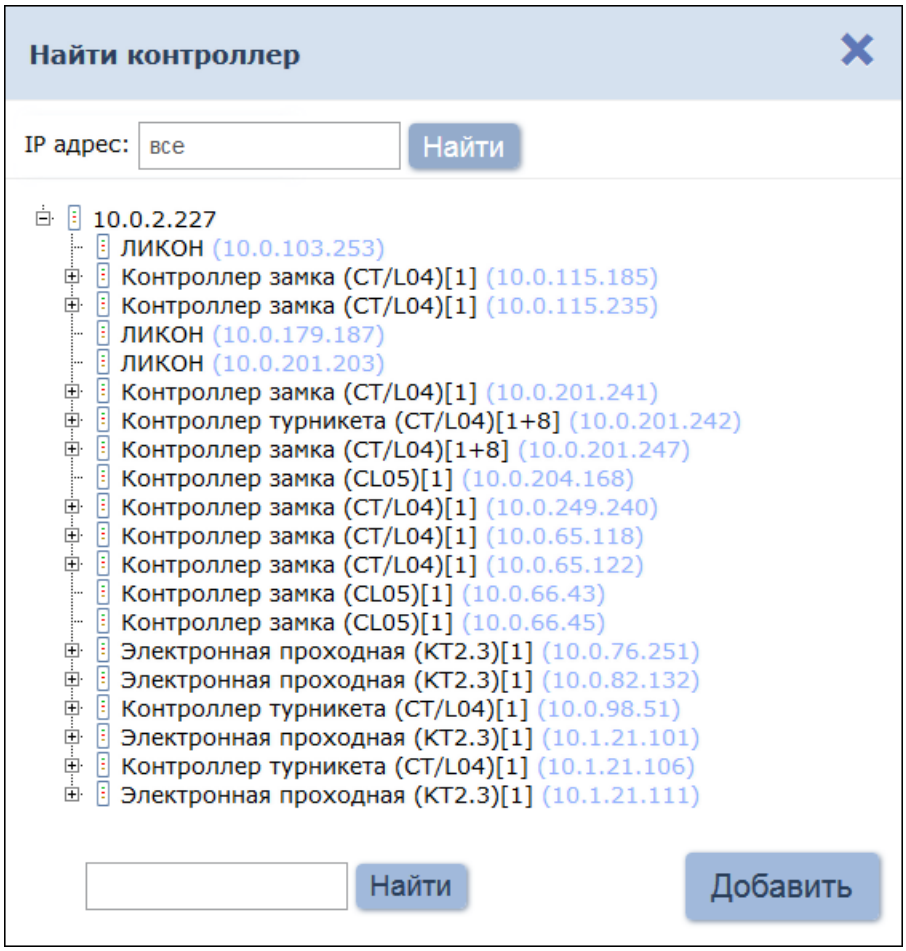
Для проведения автоматической конфигурации:

1. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
2. Откройте подраздел ***«Конфигурация»***.
3. Перейдите на вкладку **Контроллеры**.
4. Нажмите на панели инструментов страницы кнопку **Поиск контроллеров** . Откроется окно **Найти контроллер:**



5. Если необходимо произвести поиск контроллера по IP-адресу, то введите его в поле **IP адрес** и нажмите кнопку **Найти**.
6. Если необходимо произвести поиск всех контроллеров в сети, то нажмите кнопку **Найти**.

7. По окончании поиска список найденных контроллеров появится в рабочей области окна:



8. Для поиска контроллера в списке введите его IP-адрес в поле, расположенное в нижней части окна, и нажмите кнопку **Найти**. Название контроллера будет выделено в списке желтым.
9. Выделите в списке контроллер (или несколько контроллеров), который необходимо добавить в конфигурацию системы. Нажмите кнопку **Добавить**. Окно будет закрыто, отмеченные контроллеры появятся в рабочей области страницы.
10. Активируйте добавленный контроллер. Для этого выделите его в рабочей области страницы и нажмите кнопку **Активировать** .
11. Произведите настройку параметров добавленного контроллера. Для этого выделите контроллер или его ресурс в рабочей области страницы и нажмите на панели инструментов кнопку **Редактировать** . Откроется окно **Свойства контроллера**.
12. В открывшемся окне при необходимости в поле **Имя контроллера** измените описательное название контроллера.
13. Укажите (или, при необходимости, измените) помещения, доступ между которыми обеспечивается контроллером. Для этого нажмите кнопку **Выбрать из списка** справа от поля **Выход из**. В открывшемся окне **Помещения** выделите помещение, в которое осуществляется доступ через считыватель №1, и нажмите кнопку **Ок**.

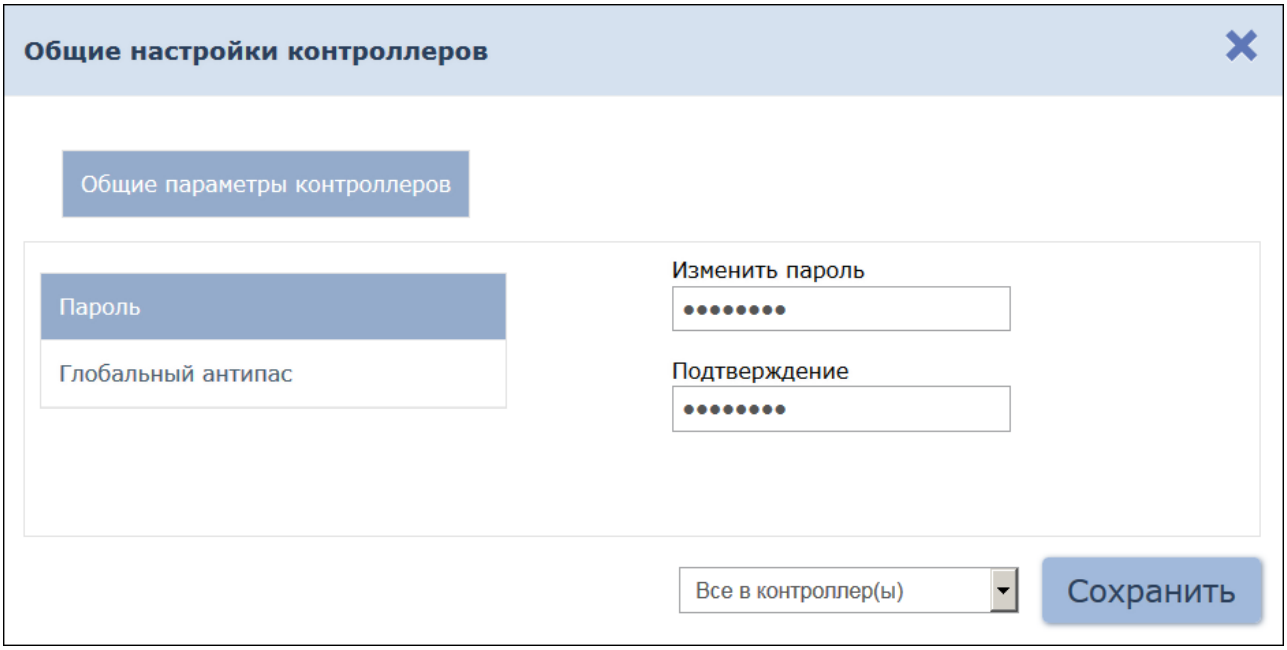
Тем же образом в поле **Вход в** укажите помещение, в которое осуществляется доступ через считыватель №2.

14. Для настройки параметров ресурсов контроллера перейдите на вкладку, соответствующую наименованию ресурса, и произведите необходимые изменения. Список доступных параметров зависит от типа контроллера и выбранного ресурса.
15. С помощью раскрывающегося списка в нижней части окна **Свойства контроллера** выберите способ сохранения параметров и нажмите кнопку **Сохранить и закрыть**. Окно **Свойства контроллера** будет закрыто.
16. Передайте конфигурацию в контроллеры. Для этого на панели инструментов страницы нажмите кнопку **Передать изменения конфигурации в контроллеры** или **Передать всю конфигурацию в контроллеры**.

Общие параметры контроллеров

Для настройки общих параметров контроллеров:

1. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
2. Откройте подраздел ***«Конфигурация»***.
3. Перейдите на вкладку **Контроллеры**.
4. Выделите в рабочей области страницы корневой элемент **Общие параметры контроллеров**.
5. Нажмите на панели инструментов страницы кнопку **Редактировать**. Откроется окно **Общие настройки контроллеров**:

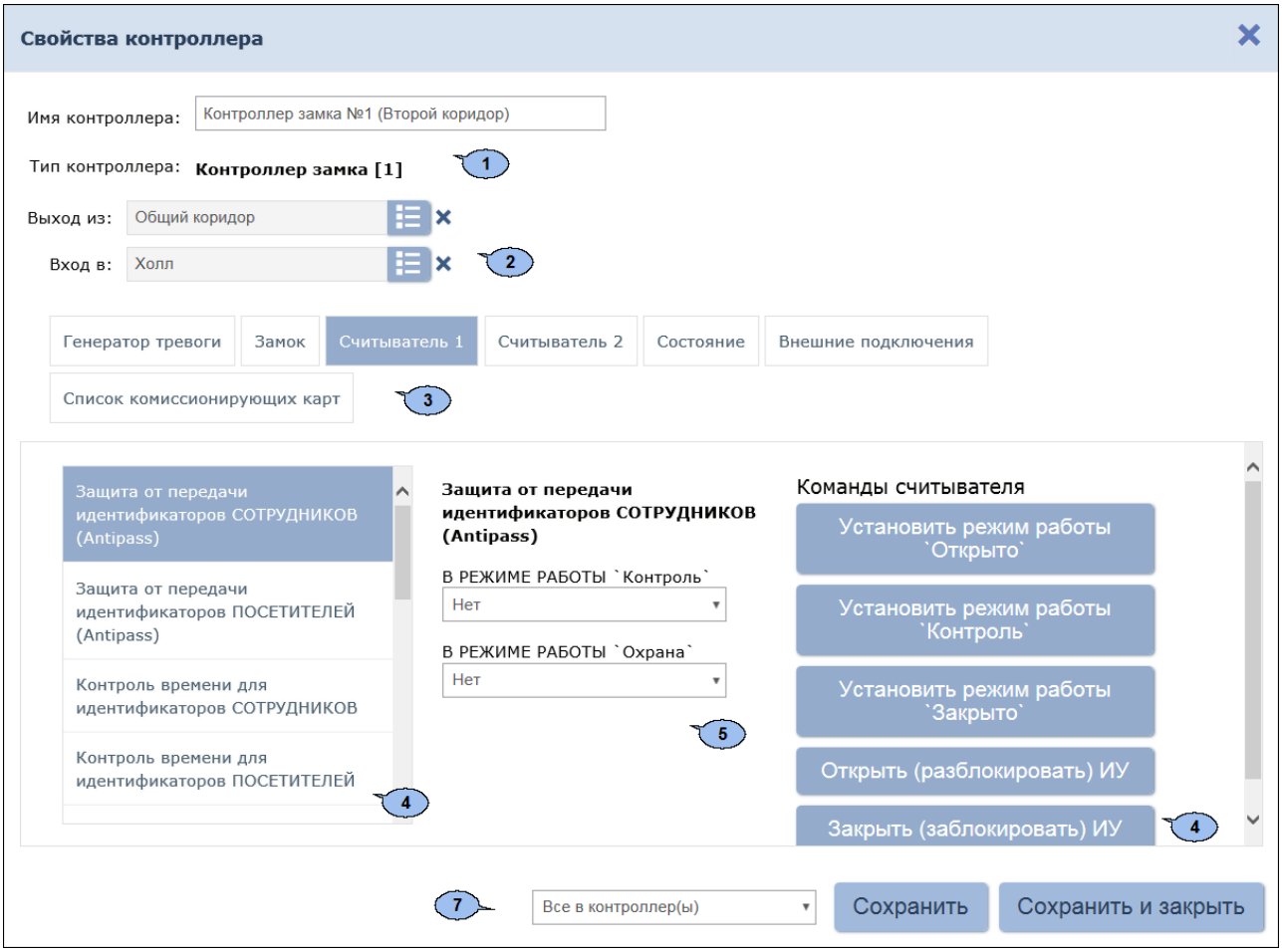


6. В открывшемся окне при необходимости измените общий пароль для доступа к контроллерам и настройте работу функции глобального контроля зональности (глобального антипаса).
7. С помощью раскрывающегося списка в нижней части окна выберите

способ сохранения параметров и нажмите кнопку **Сохранить**. Окно **Общие настройки контроллеров** будет закрыто.

Окно «Свойства контроллера»

Окно **Свойства контроллера** имеет следующий вид:



1. **Имя контроллера** – поле для ввода описательного названия контроллера.
2. Инструменты для указания или изменения помещений, доступ между которыми обеспечивается контроллером.

   Выбрать из списка – кнопка справа от поля **Выход из** позволяет выбрать помещение, доступ в которое осуществляется через считыватель №1. Кнопка **Сбросить** позволяет удалить из поля выбранное ранее помещение.

   Выбрать из списка – кнопка справа от поля **Вход в** позволяет выбрать помещение, доступ в которое осуществляется через считыватель №2. Кнопка **Сбросить** позволяет удалить из поля выбранное ранее помещение.
3. Выбор вкладки ресурса. В зависимости от типа контроллера список ресурсов и соответствующих им вкладок может отличаться. Доступны следующие вкладки:
   - **Внешние подключения** – вкладка с информацией о внешних

подключениях контроллера;
- **Генератор тревоги**;
- **Дополнительные входы**;
- **Дополнительные выходы**;
- **Дополнительный вывод**;
- **Замок CL-05.1**;
- **ИУ** (Замок, Турникет);
- **Общие**;
- **Свойства ЛИКОНА и Строки**;
- **Состояние** – вкладка с информацией о состоянии контроллера;
- **Список комиссионирующих карт**;
- **Считыватель**.

4. Параметры, доступные для выбранного ресурса.
5. Возможные значение и варианты настройки выделенного параметра ресурса.
6. Кнопки команд управления, доступных для выбранного ресурса. Для оперативного управления устройствами предназначен подраздел ***«Управление устройствами»*** раздела ***«Контроль доступа»***.
7. Кнопка **Сохранить**, **Сохранить и закрыть** и раскрывающийся список способа сохранения изменений при нажатии:
   - **Только в базу данных** – параметры сохраняются только в БД системы и впоследствии должны быть переданы в контроллер(ы).
   - **Все в контроллер(ы)** – в контроллер(ы) передаются все параметры.
   - **Измененные в контроллер(ы)** – в контроллер(ы) передаются только измененные параметры.

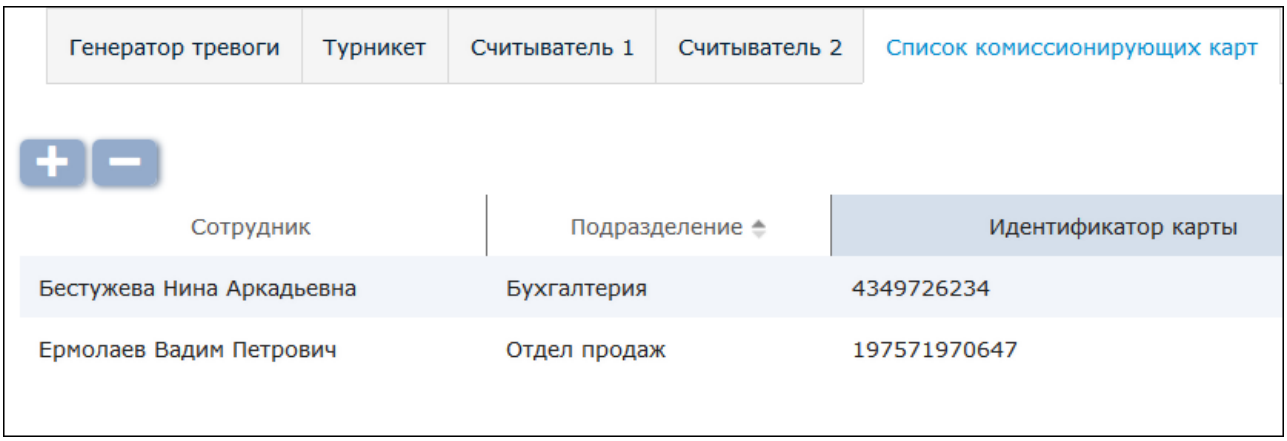
Создание списка комиссионирующих карт

Примечание:

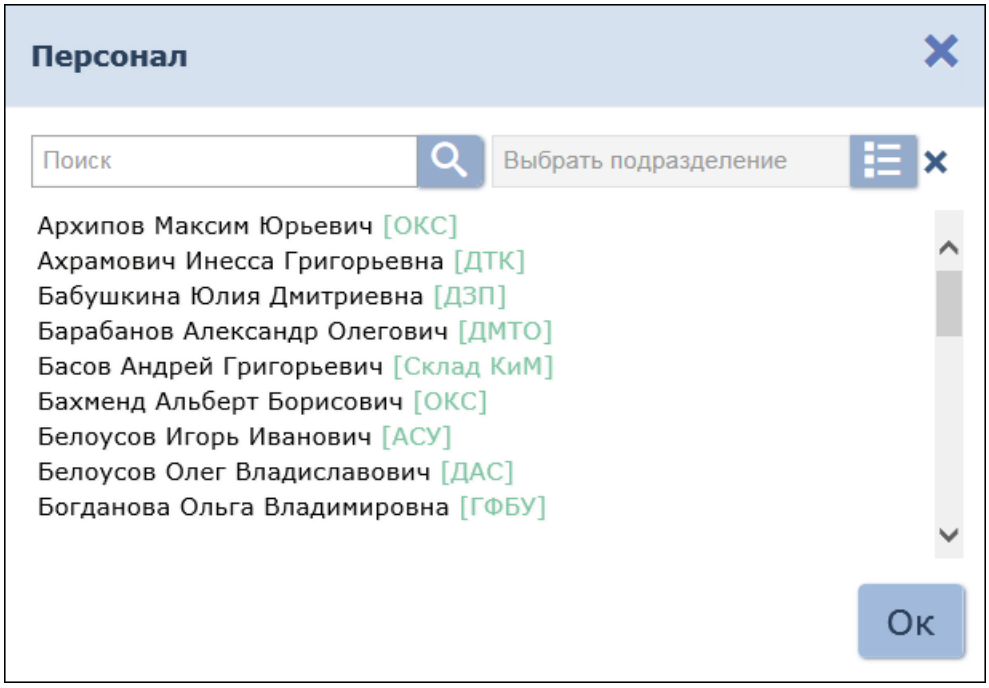
Для использования функции комиссионирования в шаблоне доступа карты необходимо указать помещения, доступ в которые будет осуществляться с комиссионированием. Для помещений необходимо установить тип права **...с комиссионированием**. Настройка шаблона проводится в подразделе ***«Шаблон доступа»*** раздела ***«Бюро пропусков»***.

Для создания списка комиссионирующих карт контроллера:

1. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
2. Откройте подраздел ***«Конфигурация»***.
3. Перейдите на вкладку **Контроллеры**.
4. Выделите контроллер в рабочей области страницы.
5. Нажмите кнопку **Редактировать** на панели **Контроллеры**. Откроется окно **Свойства контроллера**.
6. В открывшемся окне перейдите на вкладку **Список комиссионирующих карт**.



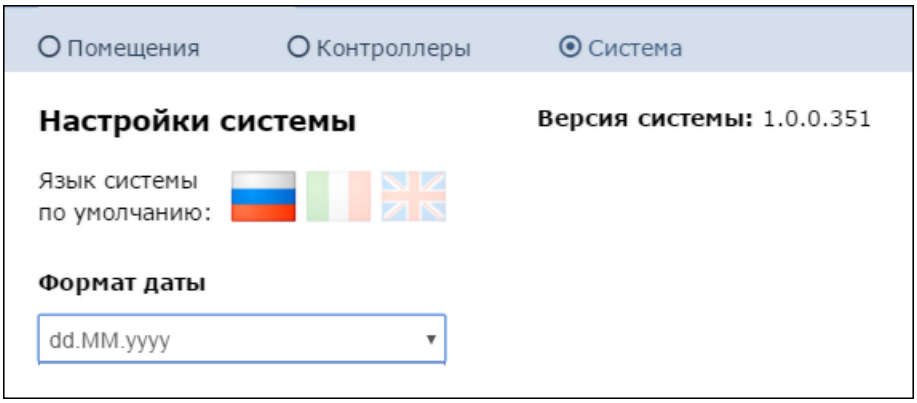
7. Нажмите кнопку **Добавить**  . Откроется окно **Персонал**:



8. В открывшемся окне, используя стандартные средства **Поиск** и **Выбрать подразделение**, выделите одного или несколько сотрудников карты доступа, выданные которым, будут являться комиссионирующими для данного контроллера.
9. Нажмите кнопку **Ок**. Окно **Персонал** будет закрыто, номера карт отмеченных сотрудников будут добавлены в рабочую область вкладки.
10. С помощью раскрывающегося списка в нижней части окна выберите способ сохранения параметров и нажмите кнопку **Сохранить**. Окно **Свойства контроллера** будет закрыто.

13.1.3 Вкладка «Система»

Вкладка **Система** предназначена для выбора языка интерфейса и формата даты. Также на вкладке отображается версия ПО системы.

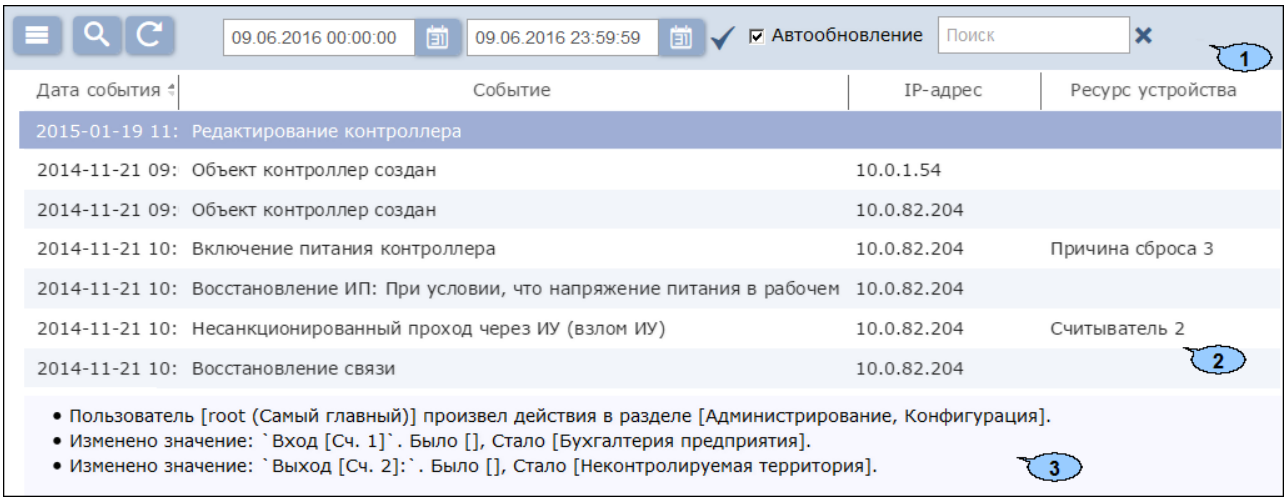


13.2 Подраздел «События системы»

Подраздел предназначен для:

- оставления отчетов о событиях, регистрируемых устройствами системы, и действиях, совершаемых операторами системы;
- просмотра событий, регистрируемых в системе в режиме реального времени.

Страница подраздела имеет следующий вид:



1. Панели инструментов подраздела содержит:

   Дополнительно – кнопка позволяет открыть меню команд для выбора дополнительных действий:

   - **Экспорт в XLS** – позволяет сохранить список событий в файл электронных таблиц *MS Office Excel* с расширением `.xls`.
   - **Экспорт в CSV** – позволяет сохранить список событий в файл электронных таблиц *OpenOffice Calc* с расширением `.csv`.
   - **Сбросить фильтры** – позволяет сбросить все фильтры рабочей области (в том числе выбранное подразделение).
   - **Параметры отображения таблицы** – позволяет открыть дополнительное окно для выбора столбцов, отображаемых в

рабочей области страницы.

 **Расширенный поиск** – кнопка позволяет настроить фильтр данных, отображаемых в рабочей области страницы.

 **Обновить данные** – кнопка позволяет обновить данные в рабочей области в соответствии с установленным фильтром.

 – кнопки позволяют открыть панель календаря для ввода даты и времени начала и конца периода, за который будут отображаться события в рабочей области. Установленные дата и время отображаются в поле слева от соответствующей кнопки.

 **Применить** – кнопка позволяет сформировать список событий за указанный период.

Автообновление – при установке флажка регистрируемые в системе события отображаются в рабочей области в режиме реального времени.

Поиск – поле позволяет ввести образец для поиска в рабочей области страницы. Кнопка **Сбросить**  позволяет очистить поле.

2. Рабочая область подраздела содержит события, зарегистрированные устройствами системы за указанный на панели инструментов период.

Примечания:

- В рабочей области реализованы функции сортировки по элементам одного из столбцов, изменения ширины и и последовательности столбцов.
- В нижней части рабочей области расположены инструменты для перемещения по страницам данных.

3. Панель дополнительных данных содержит дополнительную информацию о событии, выделенном в рабочей области подраздела.

13.3 Подраздел «Задания»

Вкладка предназначена для создания заданий, автоматически выполняемых сервером системы. Доступны задания следующих типов:

- *«Резервное копирование базы данных»* – для создания резервной копии БД. По умолчанию БД сохраняется в папке `C:\ProgramData\PERCo-Web`, в файле с расширением `.fbk`.
- *«Учет рабочего времени за предыдущий день»* – для автоматического расчета отработанного сотрудниками времени за предыдущий день. Позволяет ускорить вывод отчетов в разделе ***«Учет рабочего времени»***.

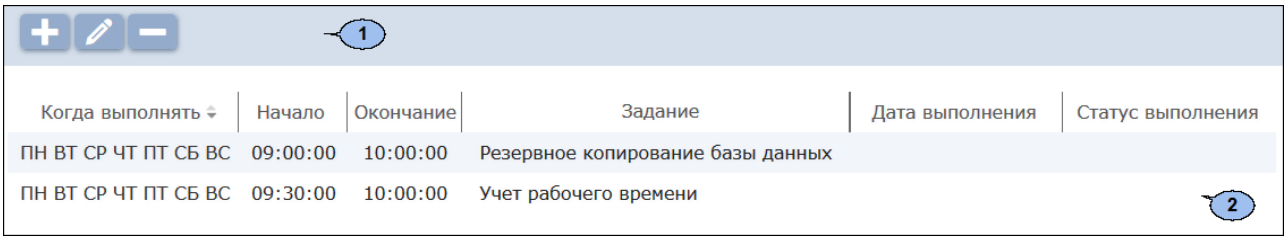
Внимание!

По умолчанию в подразделе созданы по одному ежедневному заданию каждого типа. При необходимости возможно изменение параметров этих заданий. Удаление задания без добавления задания такого же типа приведет соответственно:

- к отключению резервного копирования базы данных,

- к увеличению продолжительности расчета отчетов по учету рабочего времени.

Страница подраздела имеет следующий вид:



1. Панель инструментов страницы содержит:

   Добавить – кнопка позволяет добавить новое задание.

   Редактировать – кнопка позволяет изменить параметры выделенного в рабочей области страницы задания.

   Удалить – кнопка позволяет удалить выделенное в рабочей области страницы задание.

2. Рабочая область вкладки содержит список заданий сервера системы. При первом запуске подраздела в рабочей области страницы доступны по одному заданию каждого типа.

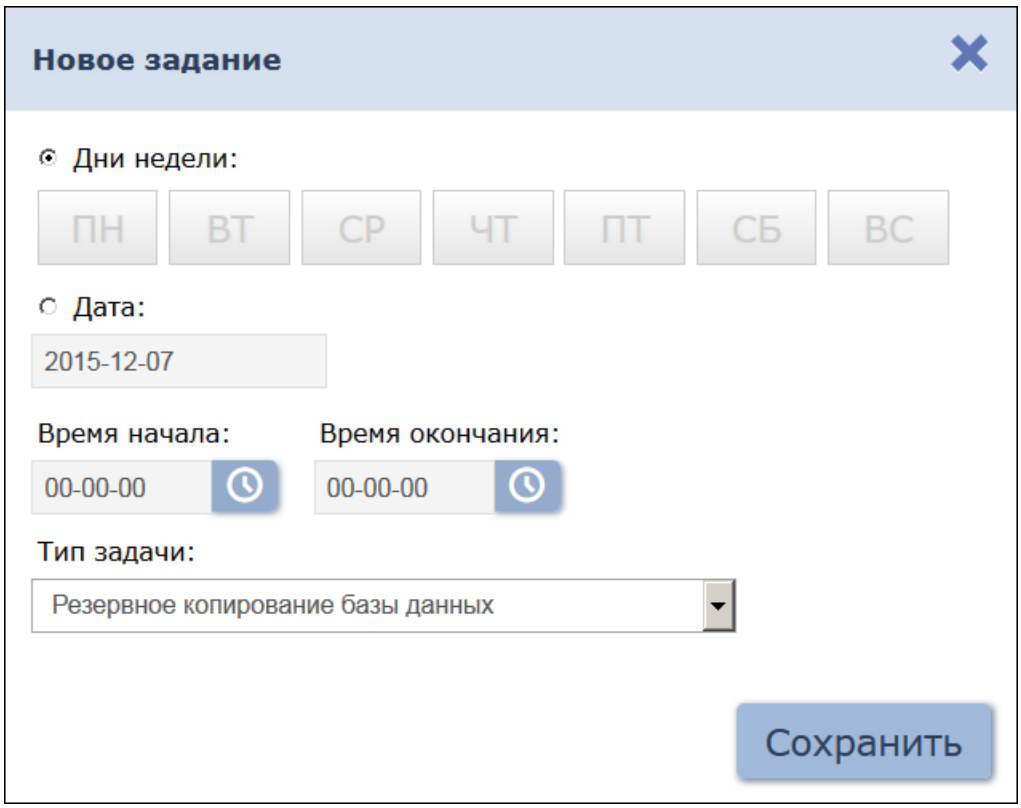
   Примечание:

   В рабочей области реализованы функции сортировки по элементам одного из столбцов и изменения ширины столбцов.

13.3.1 Создание нового задания

Для создания нового задания сервера системы:

1. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
2. Откройте подраздел ***«Задания»***.
3. Нажмите на панели инструментов страницы кнопку **Добавить**. Откроется окно **Новое задание**:



4. С помощью раскрывающегося списка **Тип задания** выберите тип нового задания:
   - **Резервное копирование базы данных**
   - **Учет рабочего времени за предыдущий день**
5. В открывшемся окне с помощью переключателя выберите периодичность выполнения задания:
   - **Дни недели** – если задание необходимо выполнять еженедельно. С помощью соответствующих кнопок укажите дни недели, в которые будет запускаться задание.
   - **Дата** – если задание необходимо выполнить один раз. С помощью календаря укажите дату запуска задания.

   Примечание:
   Для выполнения заданий рекомендуется выбирать период времени, когда совершается минимальное количество проходов проходов и минимальное количество операторов подключено к серверу системы.
6. С помощью полей ввода **Время начала** и **Время окончания** укажите период времени в течение суток, в который задание необходимо запустить.
7. После указания всех параметров задания нажмите кнопку **ОК**. Окно **Задание** будет закрыто. Новое задание появится в рабочей области страницы.

13.4 Подраздел «Операторы»

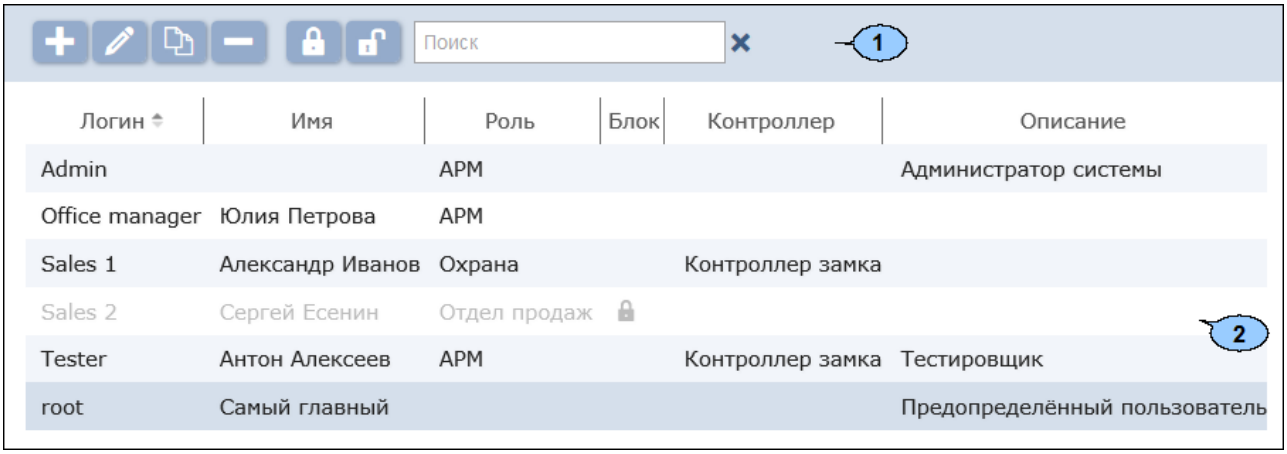
Примечание:

Перед началом работы с разделом создайте роли операторов и выдайте им полномочия в подразделе ***«Роли и права операторов»*** раздела ***«Администрирование»***.

Подраздел предназначен для:

- создания списка операторов системы с указанием доступных разделов и выдачи им полномочий на основе ролей,
- временного блокирования/ разблокирования возможности доступа оператора в систему,
- редактирования данных и удаления добавленных ранее операторов.

Страница подраздела имеет следующий вид:



1. Панель инструментов страницы:

   Добавить – кнопка позволяет добавить нового оператора.

   Редактировать – кнопка позволяет изменить данные оператора, выделенного в рабочей области страницы.

   Удалить – кнопка позволяет удалить выделенного в рабочей области страницы оператора.

   Заблокировать – кнопка позволяет временно блокировать возможность доступа в систему оператора, выделенного в рабочей области страницы.

   Разблокировать – кнопка позволяет разблокировать ранее блокированную возможность доступа в систему для оператора, выделенного в рабочей области страницы.

   Поиск – поле позволяет ввести образец для поиска в рабочей области страницы. Кнопка **Сбросить** позволяет очистить поле.

2. Рабочая область страницы содержит список операторов системы. Значок в строке с данными оператора указывает на то, что доступ оператора в систему заблокирован.

Примечание:

В рабочей области реализованы функции сортировки по элементам одного из столбцов и изменения ширины столбцов.

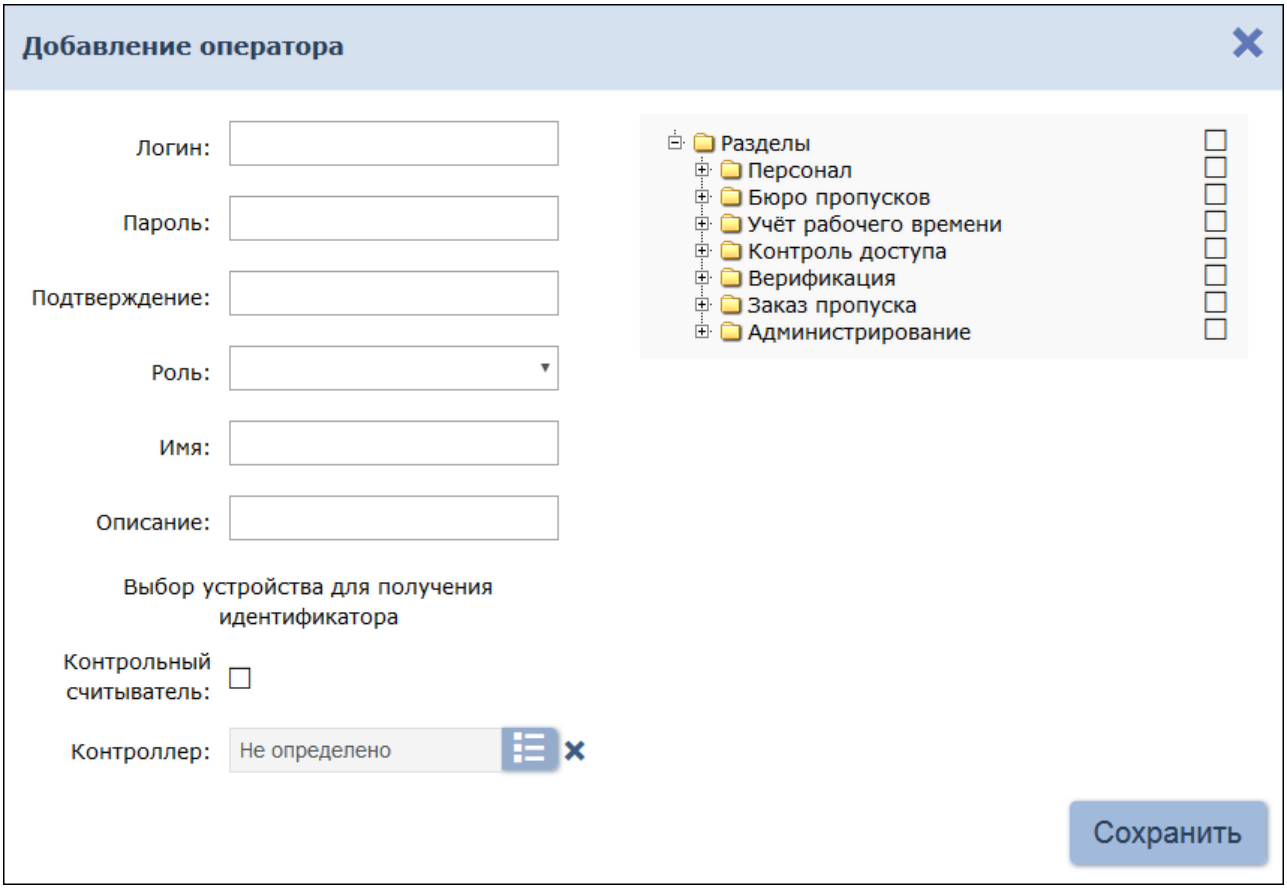
13.4.1 Добавление оператора системы

Примечание:

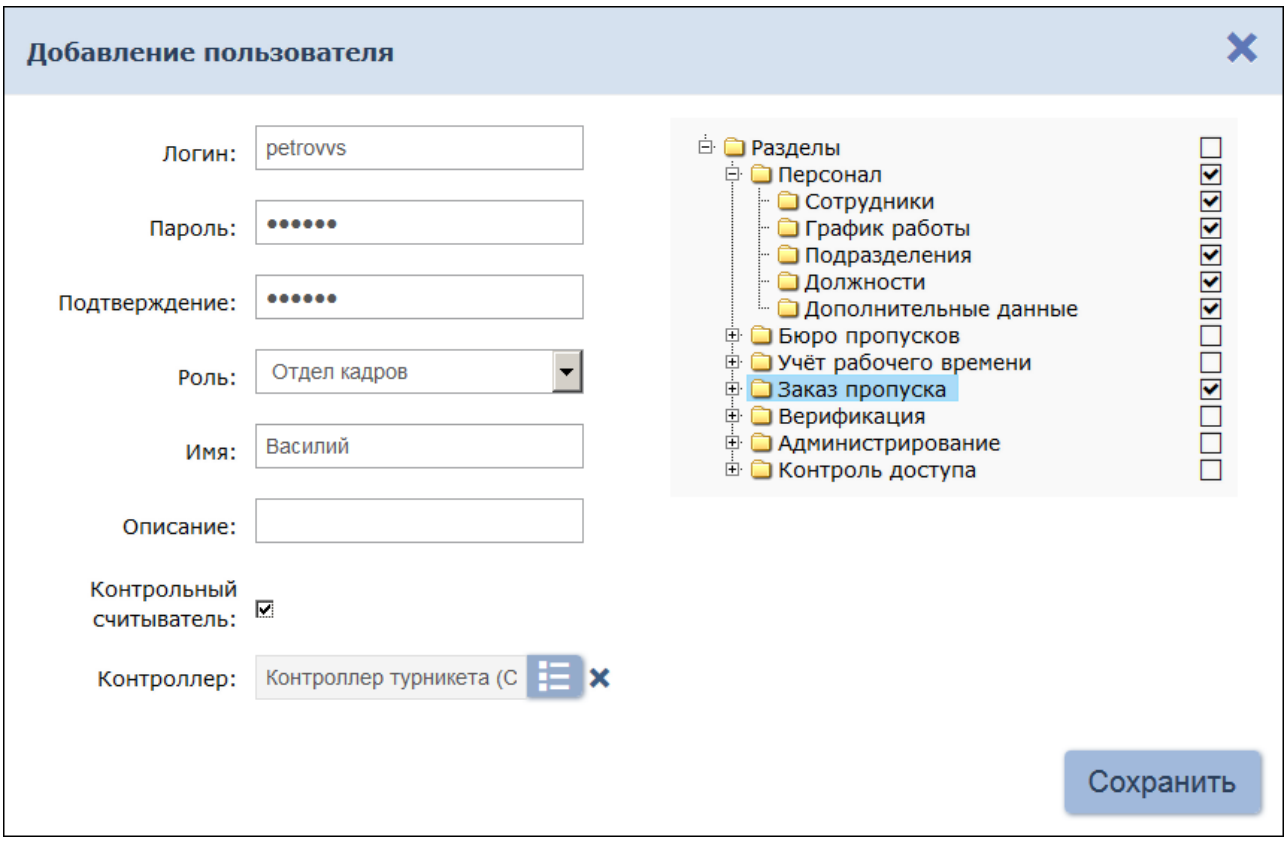
Перед добавлением операторов создайте в подразделе ***«Права операторов»*** раздела ***«Администрирование»*** необходимые роли операторов и выдайте им полномочия.

Для добавления нового оператора:

1. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
2. Откройте подраздел ***«Операторы»***.
3. Нажмите на панели инструментов вкладки кнопку **Добавить**. Откроется окно **Добавление оператора**:



4. В соответствующих полях укажите для оператора его логин и пароль.
5. С помощью раскрывающегося списка **Роль** укажите для оператора его полномочия. Роли операторов создаются в разделе ***«Права операторов»***.
6. При необходимости укажите для оператора **Имя** и **Описание**.



7. Для использования оператором контрольного считывателя для считывания номеров карт доступа, подключаемого к USB-разъему ПК, установите флажок **Контрольный считыватель**.
8. Если контрольный считыватель не используется, то выберите контроллер, подключенные к которому считыватели будут использоваться оператором для ввода номеров карт доступа. Для этого нажмите кнопку **Выбрать из списка** справа от поля **Контроллер**. В открывшемся окне выберите нужный контроллер.
9. На панели **Доступ к разделам** установите флажки у разделов, подразделов и вкладок подразделов, доступ к которым будет разрешен оператору.

Внимание!

- При выдачи оператору полномочий на подраздел ***«Конфигурация»*** раздела ***«Администрирование»*** ему предоставляется полный доступ ко всем контроллерам системы, вне зависимости от полномочий его роли на контроллеры. Это может привести к несанкционированному доступу в помещения.
- При выдачи оператору полномочий на подраздел ***«Роли и права операторов»*** раздела ***«Администрирование»*** ему предоставляется возможность создавать новые роли операторов и изменять права созданных ранее ролей. Это может привести к несанкционированному изменению полномочий ролей.

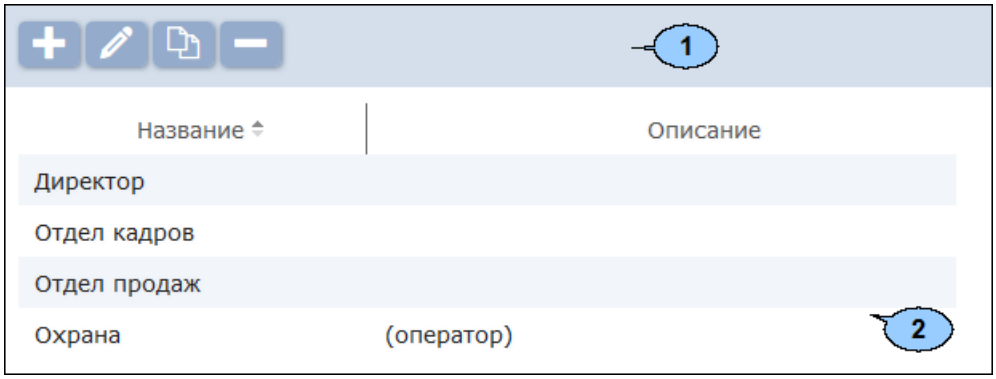
10. Нажмите кнопку **Сохранить**. Окно **Добавление оператора** будет закрыто. Новый оператор будет добавлен в список в рабочей области страницы.

13.5 Подраздел «Роли и права операторов»

Подраздел предназначен для:

- создания ролей операторов и выдачи полномочий,
- редактирования и удаления добавленных ранее ролей операторов.

Страница подраздела имеет следующий вид:



1. Панель инструментов страницы:

   Добавить – кнопка позволяет добавить новую роль оператора.

   Редактировать – кнопка позволяет изменить название, описание и полномочия роли, выделенной в рабочей области страницы.

   Копировать – кнопка позволяет добавить новую роль оператора на основе созданной ранее.

   Удалить – кнопка позволяет удалить роль, выделенную в рабочей области страницы.

2. Рабочая область страницы содержит список созданных ранее ролей операторов.

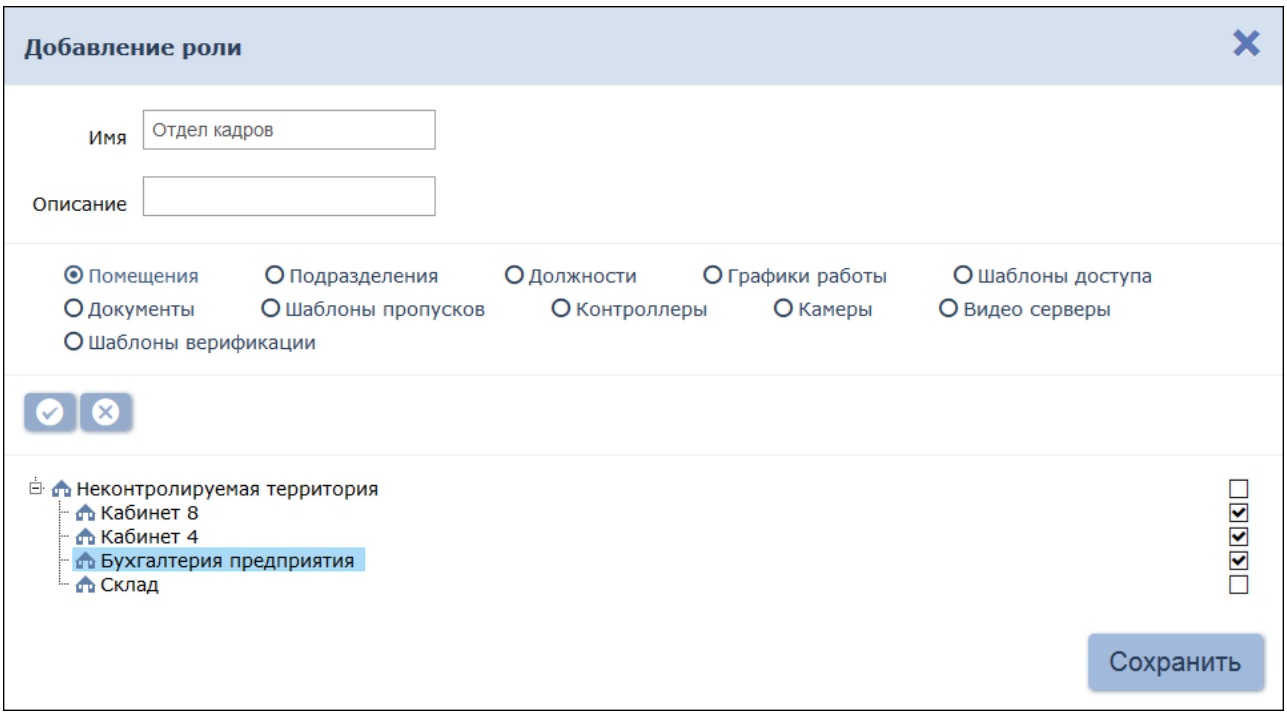
   Примечание:

   В рабочей области реализованы функции сортировки по элементам одного из столбцов и изменения ширины столбцов.

13.5.1 Добавление роли оператора (набора полномочий)

Для добавления новой роли оператора:

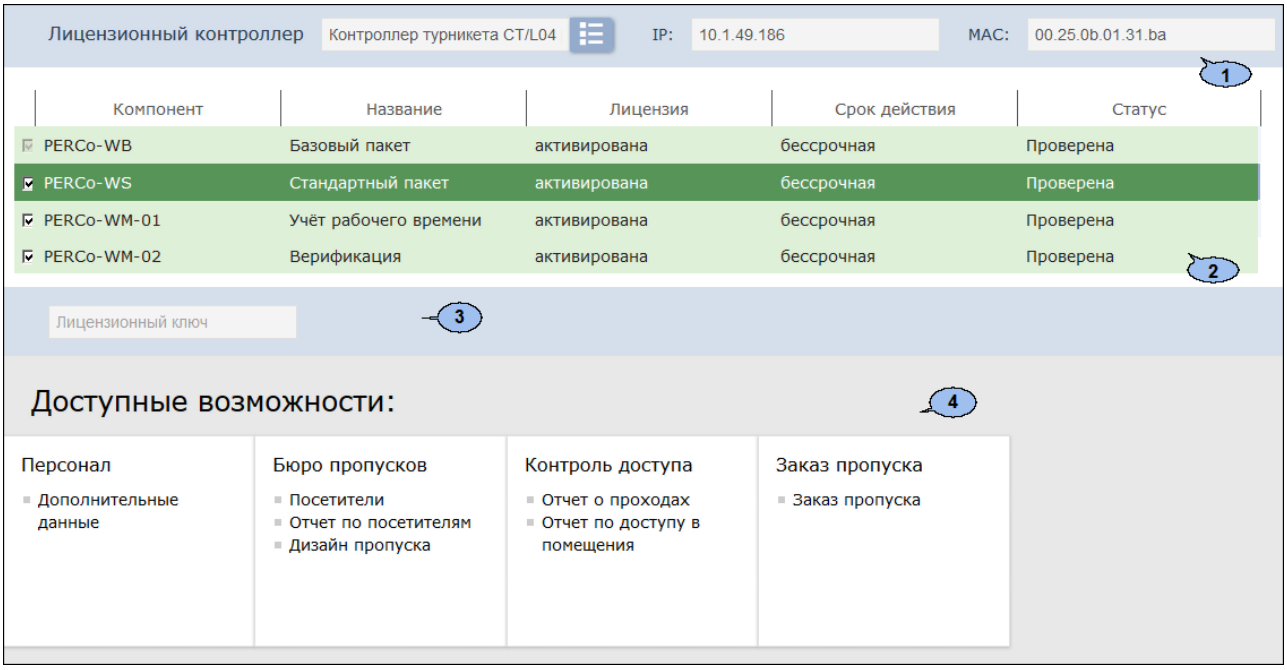
1. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
2. Откройте подраздел ***«Роли и права операторов»***.
3. Нажмите на панели инструментов вкладки кнопку **Добавить**. Откроется окно **Добавление роли**:



4. В открывшемся окне в поле **Имя** введите название роли, в поле **Описание** при необходимости введите дополнительную информацию о роли.
5. Выдайте полномочия созданной роли. Для этого с помощью переключателя выберите тип полномочий. При этом в рабочей области страницы появится список объектов данного типа, доступных в системе. Доступны следующие типы полномочий:
   - **Помещения**
   - **Подразделения**
   - **Должности**
   - **Графики работы**
   - **Шаблоны доступа**
   - **Шаблоны верификации**
   - **Шаблоны пропусков**
   - **Контроллеры**
   - **Камеры**
   - **Видеосерверы**
6. Установите флажки у тех объектов, полномочия на которые должны быть доступны для созданной роли оператора. При необходимости используйте кнопки **Выделить все** и **Снять выделение** .
7. С помощью переключателя выберите другой тип объектов и выдайте на них полномочия.
8. Нажмите кнопку **Сохранить**. Окно **Добавление роли** будет закрыто. Новая роль будет добавлена в список в рабочей области страницы.
9. Для добавления нового оператора системы откройте подраздел ***«Операторы»***.

13.6 Подраздел «Лицензии»

Подраздел предназначен для ввода кодов активации установленных модулей ПО системы. Страница подраздела имеет следующий вид:



1. Панель **Лицензионный контроллер** содержит кнопку **Выбрать контроллер**  , позволяющую выбрать контроллер, который будет использоваться в качестве электронного ключа защиты ПО системы, и поля для отображения IP- и MAC-адресов выбранного контроллера.
2. Рабочая область вкладки содержит список установленных модулей.

   Примечание:

   В рабочей области реализованы функции сортировки по элементам одного из столбцов и изменения ширины столбцов.
3. Поле **Лицензионный ключ** для ввода кода активации. Панель открывается после выбора в рабочей области страницы одного из модулей.
4. Панель **Доступные возможности** содержит список разделов и подразделов системы, доступных для выбранного в рабочей области страницы модуля.

13.6.1 Ввод кода активации

Для ввода кодов активации модулей ПО системы:

1. Используя панель навигации, перейдите в раздел  ***«Администрирование»***.
2. Откройте подраздел ***«Лицензии»***.

   Примечание:

   Контроллер, использующийся в качестве электронного ключа защиты ПО системы, должен быть добавлен в конфигурацию системы на вкладке ***«Контроллеры»*** подраздела ***«Конфигурация»***.

3. На панели **Лицензионный контроллер** нажмите кнопку **Выбрать контроллер**  . Откроется окно **Выберите лицензионный контроллер**:

4. В открывшемся окне выделите контроллер, выбранный в качестве электронного ключа защиты ПО системы. Нажмите кнопку **Выбрать**.
5. Окно **Выберите лицензионный контроллер** будет закрыто. На панели **Лицензионный контроллер** появятся IP-, MAC-адреса и наименование выбранного контроллера.
6. В рабочей области вкладки выделите название модуля, для которого необходимо ввести код активации.
7. В поле **Лицензионный ключ** введите код активации, указанный для выделенного модуля в лицензионном соглашении. Код вводится без пробелов и разделителей. Нажмите кнопку **Отправить** справа от поля.
8. Сервер системы осуществит проверку введенного кода. При правильном вводе рядом с названием выделенного модуля в столбце **Тип лицензии** появится слово *«активирована»*.
9. В случае ошибки при вводе кода активации, несоответствии кода выбранному модулю или контроллеру, нарушении связи с контроллером откроется окно с соответствующим предупреждением.

14 Параметры контроллера

В зависимости от типа контроллера список ресурсов и соответствующих им вкладок может отличаться. Доступны следующие вкладки:

- **Внешние подключения** – вкладка с информацией о внешних подключениях контроллера;
- **Генератор тревоги**;
- **Дополнительные входы**;
- **Дополнительные выходы**;
- **Дополнительный вывод**;
- **Замок CL-05.1**;
- **ИУ** (Замок, Турникет);
- **Общие**;
- **Свойства ЛИКОНА и Строки**;
- **Состояние** – вкладка с информацией о состоянии контроллера;
- **Список комиссионирующих карт**;
- **Считыватель**.

14.1 Вкладка «Общие»

«Сеть»

На вкладке доступны сетевые настройки, IP- и Mac-адреса контроллера.

«Разное»

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

Версия прошивки – в поле указана версия встроенного ПО контроллера

14.2 Вкладка ИУ («Замок», «Турникет»)

Прямое направление прохода. Параметр позволяет изменить нумерацию считывателей по отношению к направлению прохода.

- По умолчанию параметр установлен, и нумерация считывателей соответствует положению перемычки «номер считывателя» (XP2) на плате считывателя (в турникетах ***PERCo*** правый считыватель - №1, левый - №2).
- Если параметр отключен, то тот считыватель, который в соответствии с его перемычкой должен иметь №1 (или нечетный номер), в контроллере будет опознан как считыватель №2 (четный номер), и соответственно наоборот, считыватель №2 в контроллере будет опознан как считыватель №1.

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

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

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

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

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

Время ожидания комиссионирования. Параметр позволяет ограничить интервал времени между предъявлением карты доступа и комиссионирующей карты в случае, если в правах карты установлен доступ с комиссионированием/ доступ с досмотром/ подтверждение проезда картой водителя.

Регистрация прохода по предъявлению идентификатора. При установке параметра контроллер будет считать проход совершившимся сразу после предъявления карты доступа, независимо от того, будет ли реально совершен проход через ИУ или нет.

Внимание!

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

- устанавливать для параметра **Подтверждение разрешения** значение отличное от **Нет**, то есть запрещено проведение процедуры верификации от ПДУ;
- проводить процедуру верификации из ПО.

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

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

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

Режим работы выхода управления ИУ. Параметр позволяет выбрать режим управления подключенным ИУ.

- **Потенциальный**
- **Импульсный** – режим управления применяется только для замков, поддерживающих этот режим. Рекомендуется использовать для

электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки «CISA»).

FireAlarm в режиме «Охрана». При установленном флажке аварийная разблокировка (открытие прохода ИУ) в случае поступления управляющего сигнала от устройства Fire Alarm произойдет также при взятой на охрану ОЗ, включающей данное ИУ. При снятом параметре (по умолчанию) в РКД «Охрана» сигналы на входах **Тип: Fire Alarm** игнорируются.

14.3 Вкладка «Замок CL05.1»

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

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

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

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

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

Время ожидания комиссионирования. Параметр позволяет ограничить интервал времени между предъявлением карты доступа и комиссионирующей карты в случае, если в правах карты установлен доступ с комиссионированием/ доступ с досмотром/ подтверждение проезда картой водителя.

Регистрация прохода по предъявлению идентификатора. При установке параметра контроллер будет считать проход совершившимся сразу после предъявления карты доступа, независимо от того, будет ли реально совершен проход через ИУ или нет.

Внимание!

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

- устанавливать для параметра **Подтверждение разрешения** значение отличное от **Нет**, то есть запрещено проведение процедуры верификации от ПДУ;
- проводить процедуру верификации из ПО.

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

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

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

Режим работы выхода управления ИУ. Параметр позволяет выбрать режим управления подключенным ИУ.

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

Смена зоны при проходе. При установленном флажке в случае прохода через ИУ регистрируется переход из одной пространственной зоны контроля в другую.

FireAlarm в режиме «Охрана». При установленном флажке аварийная разблокировка (открытие прохода ИУ) в случае поступления управляющего сигнала от устройства Fire Alarm произойдет также при взятой на охрану ОЗ, включающей данное ИУ. При снятом параметре (по умолчанию) в РКД «Охрана» сигналы на входах **Тип: Fire Alarm** игнорируются.

14.4 Вкладки «Свойства ЛИКОНА» и «Строки»

На вкладке **Свойства ЛИКОНА** расположены параметры настройки для контроллера регистрации ***PERCo-CR01 LICON***. Вкладка **Строки** позволяет изменить содержание сообщений, отображаемых на ЖКИ контроллера.

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

Примечание:

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

Индикация баланса рабочего времени. При установке флажка на ЖКИ помимо времени регистрации прохода отображается персональная информация о нарушениях и балансе рабочего времени, связанная с предъявленной картой доступа.

Время ожидания ответа на запрос от сервера системы (по умолчанию 2 сек). Поле ввода позволяет задать время, в течение которого контроллер ожидает получения от сервера системы персональной информации (ФИО), связанной с предъявленной картой доступа. В случае невозможности получения информации на ЖКИ отображается номер карты.

Время показа информации о сотруднике (по умолчанию 2 сек). Поле ввода позволяет задать время, в течение которого на ЖКИ контроллера отображается персональная информация, связанная с предъявленной картой доступа.

14.5 Вкладка «Дополнительные входы»

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

Тип. Раскрывающийся список позволяет выбрать один из следующих типов:

- **Нет**. К данному входу не подключено никакое внешнее оборудование.
- **Обычный**. К данному входу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
- **Специальный**. Предназначен для автономного сброса тревоги, выключения сирены.
- **FireAlarm**. Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ Fire Alarm.

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

Примечание:

Для входа **Тип**: **FireAlarm** параметр **Нормальное состояние контакта** недоступен. Установлено постоянное значение **Замкнут**.

В зависимости от выбранного типа остальные параметры выхода могут различаться.

Обычный

Временной Критерий маскирования/активизации/ нормализации:

- **На указанное время**. Выбранные дополнительные входы будут маскированы/ активизированы/ нормализованы на указанное время.
- **На время срабатывания**. Выбранные дополнительные входы будут маскированы/ активизированы/ нормализованы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать

управляющий сигнал.

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

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

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

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

Специальный

Сброс тревоги (Генератор тревоги). При установке параметра получение управляющего сигнала на данном дополнительном входе приведет к сбросу тревоги.

14.6 Вкладка «Дополнительные выходы»

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

Примечание:

После включения питания все выходы нормализуются.

Тип. Раскрывающийся список позволяет выбрать следующие типы выхода:

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

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

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

14.7 Вкладка «Дополнительный вывод»

Тип. Раскрывающийся список позволяет выбрать один из следующих типов:

- **Нет**. К данному входу не подключено никакое внешнее оборудование.
- **Обычный**. К данному входу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
- **Генератор тревоги**. Решение об активизации дополнительного выхода принимается в соответствии с параметрами, заданными для ресурса **Генератор тревоги**.
- **FireAlarm**. Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ Fire Alarm.
- **Синхронизирующий вход/выход**. Вывод используется для синхронизации совместной работы двух контроллеров при организации КПП с контролем проходов в двух направлениях. В этом режиме выводы контроллеров соединяются друг с другом.

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

14.8 Вкладка «Генератор тревоги»

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

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

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

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

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

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

14.9 Вкладка «Считыватель»

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

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

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

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

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

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

Временной критерий маскирования:

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

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

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

Временной критерий активизации/нормализации:

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

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

Подтверждение от ДУ. Параметр позволяет указать, будет ли при предъявлении карты доступа считывателю в РКД «Контроль» формироваться запрос на верифицирующее устройство. В качестве верифицирующих устройств могут использоваться: ПДУ, картоприемник или другое оборудование.

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

  Примечание:

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

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

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

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

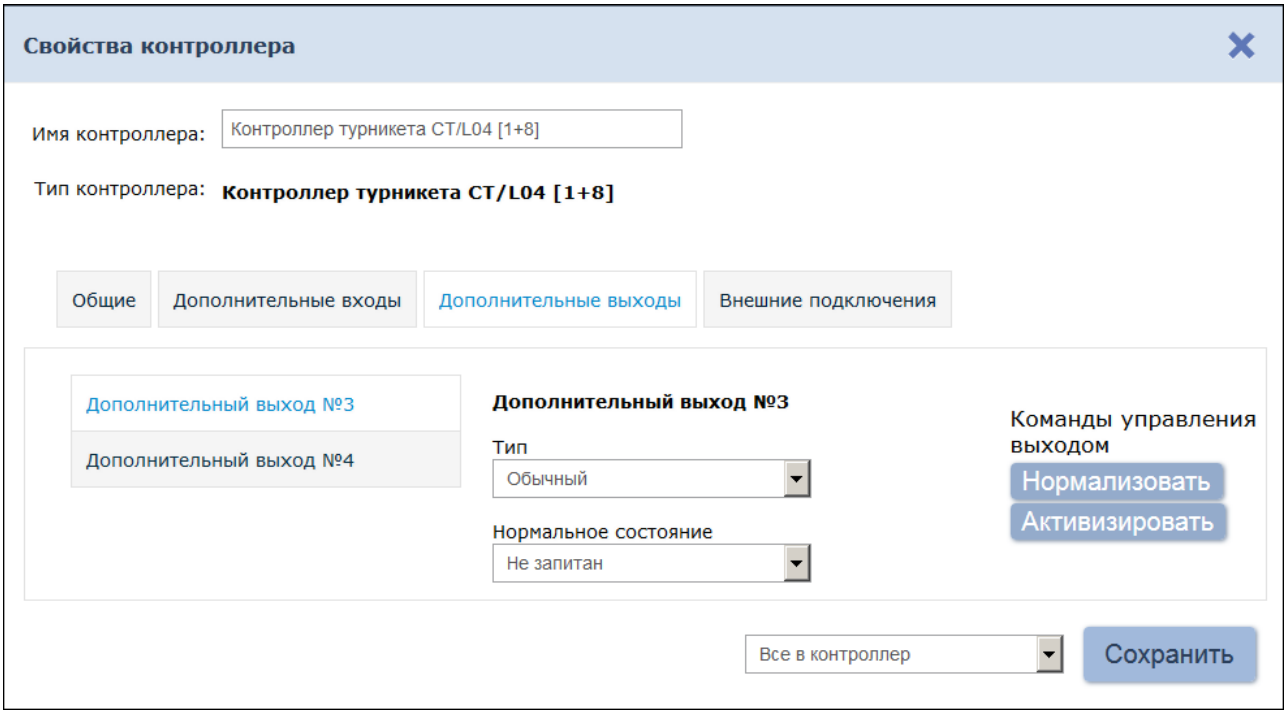
Разрешение ДУ. При установке флажка использование ПДУ при РКД *«Контроль»* в направлении данного считывателя будет разрешено.

Изымать идентификаторы ПОСЕТИТЕЛЕЙ после прохода. При установке флажка предъявленная карта доступа после прохода изымается из учетных данных посетителя, данные посетителя отправляются в архив. Функция доступна только при наличии связи контроллера с сервером системы.

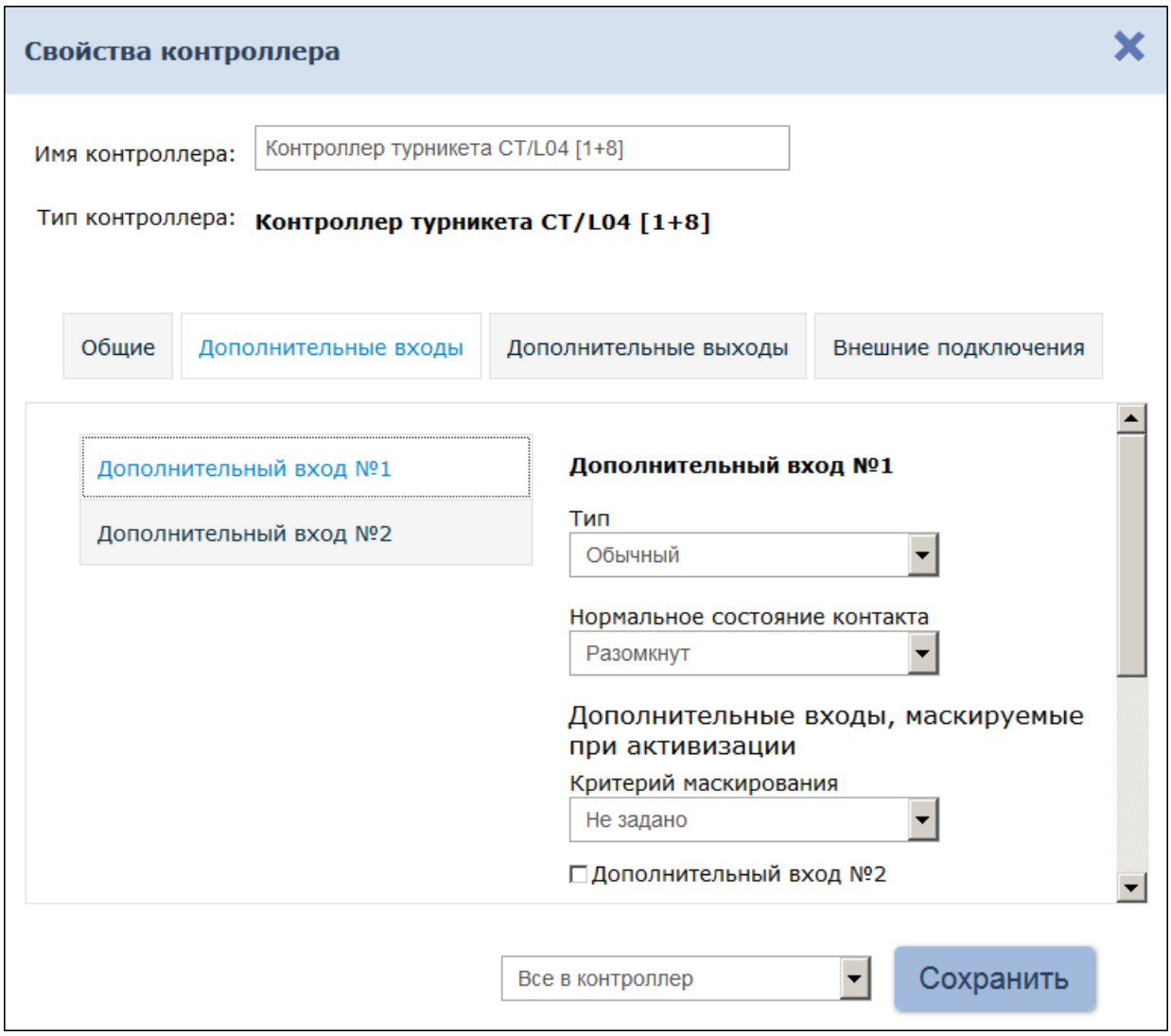
15 Пример конфигурирования картоприемника

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

1. Используя панель навигации, перейдите в раздел ***«Администрирование»***.
2. Откройте подраздел ***«Конфигурация»***.
3. В рабочей области страницы выделите контроллер, к которому физически подключен картоприемник.
4. Нажмите кнопку **Редактировать** на панели инструментов страницы. Откроется окно **Свойства контроллера**.
5. В открывшемся окне перейдите на вкладку **Дополнительные выходы**.



6. В рабочей области окна выберите **Дополнительный выход №3**. Номер выхода должен соответствовать выходу контроллера, к которому физически подключен вход *«Изъять карту»* картоприемника.
7. Установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
   - для параметра **Тип** значение **Обычный**;
   - для параметра **Нормальное состояние** значение **Не запитан**.
8. При необходимости настройте реакцию системы на сигнал от картоприемника *«Авария»*. Для этого перейдите на вкладку **Дополнительные входы**.



9. В рабочей области окна выберите **Дополнительный вход №1**. Номер входа должен соответствовать входу контроллера, к которому физически подключен выход *«Авария»* картоприемника.
10. Установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
    - для параметра **Тип** значение **Обычный**,
    - для параметра **Нормальное состояние контакта** значение **Разомкнут**,
    - используя параметры активизации или нормализации выходов, настройте требуемую реакцию контроллера.
11. Нажмите кнопку **Сохранить и закрыть**. Окно **Свойства контроллера** будет закрыто.
12. В рабочей области страницы выделите контроллер ИУ того же контроллера.
13. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется окно **Свойства контроллера**.
14. Перейдите на вкладку ресурса **Считыватель №2**. Номер считывателя должен соответствовать выходному считывателю, в направлении которого установлен картоприемник.
15. Подтверждением изъятия карты для контроллера доступа является

сигнал от картоприемника «Карта изъята». Для настройки подтверждения в левой части рабочей области окна выберите параметр **Подтверждение от ДУ** (выход картоприемника *«Карта изъята»* должен быть подключен ко входу контроллера от ПДУ, управляющим открытием данного направления прохода).

16. Установите с помощью раскрывающегося списка в рабочей области окна для параметра **В режиме "Контроль"** значение **Да**.
17. Установите в рабочей области окна флажки:
    - **при проходе ПОСЕТИТЕЛЕЙ**;
    - **при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ**;
    - **при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**.
18. Установите в рабочей области окна требуемое значение параметра **Время ожидания подтверждения**, указывающего время, в течение которого контроллер должен ожидать сигнал *«Карта изъята»*.
19. В левой части рабочей области окна выберите параметр **Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ**.
20. Установите с помощью раскрывающегося списка в рабочей области окна для параметра **Критерий активизации** значение **На время срабатывания**.
21. Установите в рабочей области окна флажок **Дополнительный выход №3** (номер выхода, к которому подключен вход *«Изъять карту»* картоприемника).
22. В левой части рабочей области окна выберите параметр **Изымать идентификаторы посетителей после прохода**.
23. Установите в рабочей области окна флажок у параметра **Изымать идентификаторы посетителей после прохода**.
24. Нажмите кнопку **Сохранить**. Окно **Свойства контроллера** будет закрыто.

16 Термины и определения

Antipass – функция системы безопасности, заключающаяся в контроле повторного прохождения (регистрации) через одно КПП в том же направлении с использованием одного и того же идентификатора.

Global Antipass – функция системы безопасности, заключающаяся в контроле зональности идентификатора, то есть функция контроля нарушений последовательности прохождения (регистрации) через КПП с учетом направления прохода. Последовательность прохождения КПП определяется взаимным расположением пространственных зон с учетом их вложенности (как пример, нельзя войти в помещение, не войдя в здание).

Автоматизированное рабочее место (АРМ) – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида. Состоит из рабочего места оператора (на удаленном ПК), которому администратором системы выданы полномочия на доступ к разделам и подразделам ПО системы.

База данных (БД) – организованная структура совместно используемых данных системы. В БД системы хранятся: номера карт доступа, персональные данные пользователей, права доступа карт, регистрируемые устройствами системы события и т.д. БД расположена на сервере системы. Работа с БД осуществляется из *«Менеджера PERCo-Web»*.

Блок индикации – представляет собой совокупность светодиодных или пиктографических индикаторов для отображения состояние ИУ и/ или установленного РКД в направлении одного из считывателей. Блок индикации может быть встроенным в считыватель, контроллер, стойку турникета, ЭП или выносным.

Верификация – процедура подтверждения прав предъявленной карты с помощью верифицирующего устройства. Подтверждение может производиться автоматически (контроллером, картоприемником) или вручную оператором (с ПДУ, кнопки ДУ, команды ПО). Верификация оператором производится на основе визуального сравнения внешности пользователя карты с фотографией, хранящейся в БД системы и выводимой на монитор при предъявлении карты.

Видеоокно – панель рабочей области раздела, на которой в режиме реального времени отображаются кадры с подключенных к системе IP-видеокамер, заранее указанных при конфигурации точки верификации.

Идентификатор – некоторое устройство или признак, по которому определяется пользователь. Каждый идентификатор характеризуется определенным уникальным кодом. В качестве идентификатора в системе используются бесконтактные карты форматов EM-Marine, HID и MIFARE.

Исполнительное устройство (ИУ) – устройство, ограничивающее доступ, например: турникет, калитка, дверной замок и т.п.

Карта доступа – бесконтактная пластиковая электронная карта (электронный ключ), с помощью которой осуществляется идентификация пользователя. Имеет размеры кредитной карты (может иметь и другие исполнения, к примеру, в виде брелоков и др.). В карте доступа заключен чип с уникальным числовым кодом. Не требует встроенного источника питания, что делает срок службы карты практически неограниченным. В системе используются карты форматов HID, EM-Marin, MIFARE.

Комиссионирование доступа – процедура подтверждения прав предъявленной карты посредством предъявления второй, комиссионирующей карты.

Контроллер (системы) – устройство, управляющее системой безопасности или ее элементами. На базе контроллера организуется КПП.

Обновление встроенного ПО – для обновления встроенного ПО и форматирования памяти контроллеров системы используется программа *«Прошиватель»*. Программа вместе с файлами прошивок входит в состав *«Программного обеспечения для смены прошивок в контроллерах системы S-20»*. Актуальную версию программы можно загрузить с сайте компании www.perco.ru из раздела **Поддержка> Программное обеспечение**.

Полномочия оператора – права на доступ к разделам и подразделам ПО системы, выданные оператору АРМ администратором системы. Используя роли оператора, выдаются полномочия на: помещения, подразделения, должности, графики работы, шаблоны доступа, шаблоны пропусков, контроллеры, камеры, видеосерверы, шаблоны верификации.

Пространственная зона – часть территории объекта, пересечение границ которой осуществляется только через специально оборудованные КПП с предъявлением карт доступа.

Режим контроля доступа (РКД) – режим функционирования системы или отдельной ее части (контроллера, считывателя), например РКД «Открыто», «Закрыто», «Контроль» и т.д.

Система контроля и управления доступом (СКУД) – совокупность программно-аппаратных средств, обеспечивающих ограничение и учет доступа людей (транспорта) на заданной территории.

Считыватель – устройство, предназначенное для считывания номера карты доступа и передачи этого номера в контроллер с целью идентификации пользователей в системе.

Электронная проходная (ЭП) – серийное изделие, представляющее собой совокупность программных и аппаратных средств для организации одного КПП с контролем проходов в двух направлениях. В ЭП входят: ИУ (турникет) со встроенным контроллером СКУД, двумя считывателями и ПО.

ООО «Завод ПЭРКо»

По вопросам выбора и приобретения
оборудования и систем безопасности:

Call-центр: 8-800-333-52-53
Тел.: (812) 329-89-24, 329-89-25

Юридический адрес:

180006, г. Псков, ул. Леона Поземского, 123 В

Техническая поддержка:

Call-центр: 8-800-775-37-05
Тел.: (812) 292-36-05

system@perco.ru
по вопросам обслуживания электроники систем безопасности

turnstile@perco.ru
по вопросам обслуживания турникетов, калиток, ограждений

locks@perco.ru
по вопросам обслуживания электромеханических замков

soft@perco.ru
по вопросам технической поддержки программного обеспечения

Утв. 22.06.2016
Кор. 30.08.2016
Отп. 30.08.2016

www.perco.ru

тел: 8 (800) 333-52-53