Система контроля и управления доступом

PERCo-Web

РУКОВОДСТВО АДМИНИСТРАТОРА

Версия ПО: 2.0.6.30

ОГЛАВЛЕНИЕ

1. Введение

Настоящее **«Руководство администратора СКУД *PERCo-Web*»** (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*, используемых при построении системы.

Руководство должно использоваться совместно с руководствами пользователя на модули 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;
ТРЛ – терминал распознавания лиц;
УРВ – учет рабочего времени;
ЭП – электронная проходная.

Внимание!

В память контроллеров ***PERCo-CL15***, ***PERCo-CR11***, ***PERCo-CT/L14***, ***PERCo-CT13*** встроена специальная версия ПО ***PERCo-Web***, отличающаяся от обычной ограничением некоторых технических характеристик и возможностей (см. раздел **"Основные технические характеристики"**). Модули ПО, предназначенные для встроенной версии ***PERCo-Web***, в своем названии содержат литеру ***E*** ("embedded"): ***PERCo-WBE***, ***PERCo-WSE***, ***PERCo-WME01***, ***PERCo-WME02*** и ***PERCo-WME05***.

2. Назначение

Система контроля и управления доступом *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:

1. 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 и биометрических технологий.
2. 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.

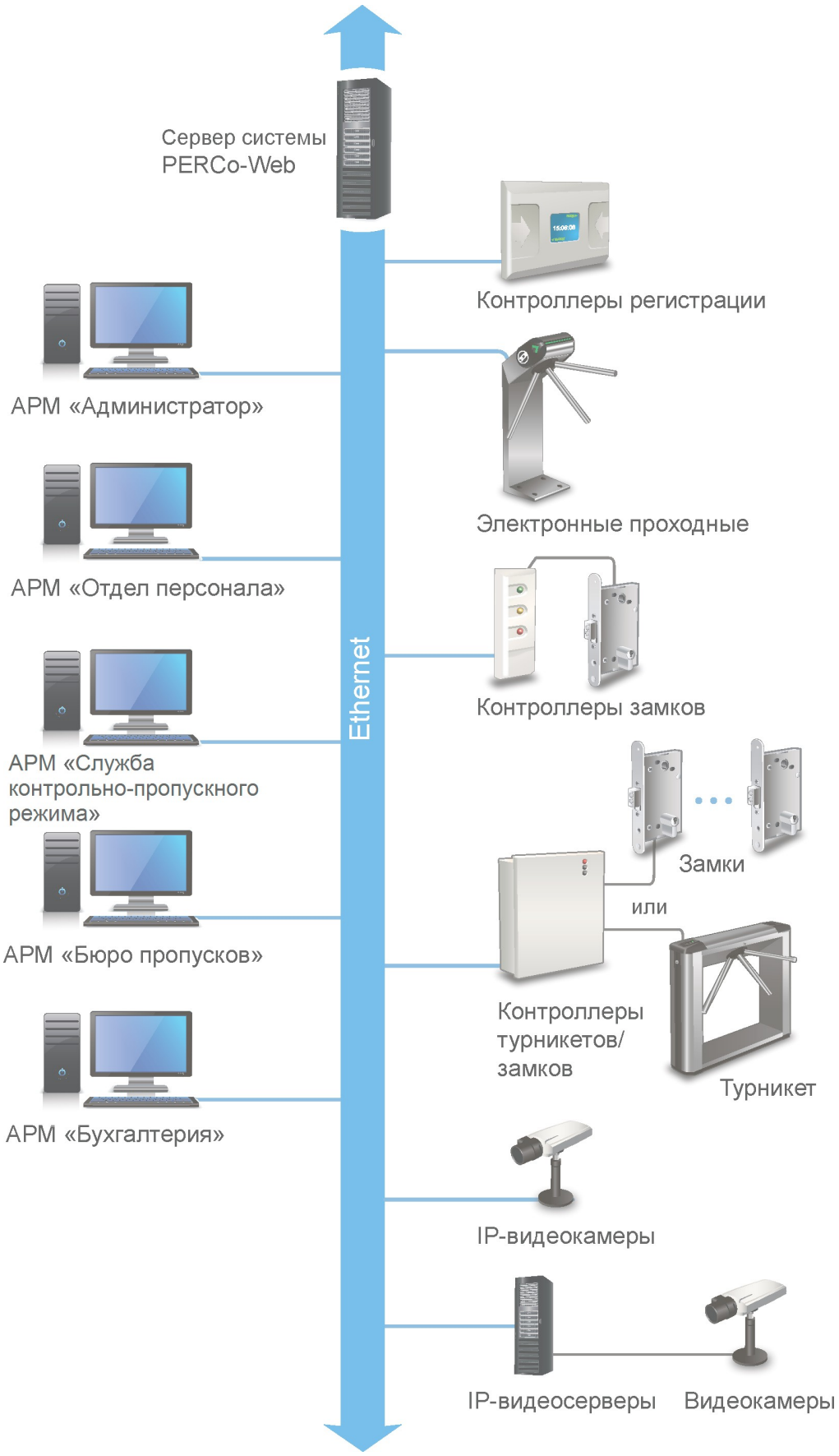
3. Основные особенности системы *PERCo-Web*

- 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.
- Устройства 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.
- Система поддерживает биометрические технологии. Биометрические контроллеры ***PERCo*** снабжены сканерами отпечатков пальцев, помимо этого в системе реализована интеграция со сторонними производителями:
  - оборудование производства ***“Suprema”*** с поддержкой сканирования отпечатков пальцев и распознавания по лицу;
  - оборудование производства ***“ZKTeco”*** с поддержкой сканирования отпечатков пальцев, распознавания по лицу и идентификации по ладони (включает в себя распознавание по форме, отпечатку и рисунку вен ладони).

  Сканирование биометрических данных, при необходимости, дополняет стандартный метод верификации по картам доступа и позволяет увеличить надежность системы контроля и управления доступом на территории предприятия при проходе сотрудников и посетителей, обеспечивая предотвращение случаев прохода по чужой карте доступа.
- Система, кроме стандартов бесконтактных карт *EMM* и *HID*, также поддерживает стандарт *Mifare*. Карты данного типа получили самое широкое распространение по всему миру и позволяют организовать контроль доступа и защиту персональных данных, записанных на карту, на самом высоком уровне.
- В системе предусмотрена возможность использования технологии *NFC* (технология беспроводной передачи данных малого радиуса действия) для эмуляции бесконтактных карт – проход и доступ осуществляется при помощи смартфона с технологией *NFC*.

4. Состав и принципы работы системы

Состав системы представлен на схеме:



Структурная схема системы PERCo-Web

Основные элементы системы:

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 (бесконтактная карта доступа, штрихкод, брелок или смартфон с функцией NFC), с уникальным номером и / или биометрическая информация (отпечатки пальцев, шаблон ладони, шаблон лица). Конфигурирование и управление системой осуществляется через Web-интерфейс сервера системы.

КПП

КПП оборудуются контроллерами, считывателями карт доступа, биометрическими устройствами, 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:

1. Оператором КПП в ручном режиме с помощью ПДУ.
2. 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 (штрихкодам, отпечаткам пальцев, шаблонам ладони, шаблонам лица) используется РКД *«Контроль»*.
3. Автоматически контроллером КПП при проходе по картам доступа (штрихкодам, отпечаткам пальцев, шаблонам ладони, шаблонам лица). При этом в направлении прохода должен быть установлен РКД *«Контроль»*. При проходе через КПП сотрудник (посетитель):
   - в случае идентификации по карте доступа – предъявляет карту считывателю;
   - в случае идентификации по штрихкоду – предъявляет штрихкод устройству с поддержкой сканера штрихкода;
   - в случае идентификации по отпечаткам пальцев – проходит процедуру сканирования отпечатков пальцев;
   - в случае идентификации по карте доступа и отпечаткам пальцев – предъявляет карту считывателю и проходит процедуру сканирования отпечатков пальцев;
   - в случае идентификации по ладони – проходит процедуру сканирования ладони (идентификация по ладони включает в себя распознавание по форме, отпечатку и рисунку вен ладони);
   - при наличии на КПП терминала распознавания лица:
     - в случае идентификации по лицу – распознавание лица происходит автоматически при проходе;
     - в случае идентификации по лицу и карте – после автоматического распознавания лица предъявляет карту считывателю;
     - в случае идентификации по лицу или карте – в случае неудачи распознавания лица предъявляет карту доступа;
     - для идентификации по лицу и ПИН-коду – после автоматического распознавания лица набирает ПИН-код на клавиатуре ТРЛ;
     - для идентификации по лицу, карте и ПИН-коду – после автоматического распознавания лица предъявляет карту доступа и набирает ПИН-код на клавиатуре ТРЛ.

На основании анализа полученной идентификационной информации, а также выданных ее владельцу прав доступа контроллер принимает решение на разрешение или запрет прохода, подавая соответствующую команду ИУ. Каждый факт получения идентификационной информации фиксируется в БД с указанием ее вида, места и времени ее получения, что позволяет системе отслеживать местонахождение, время пребывания и перемещения сотрудника (посетителя) 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»**, описание см. в *Руководствах пользователя* на модули ПО);
- *«Служба контрольно-пропускного режима»* (разделы: «**Контроль доступа»**, **«Заказ пропуска»**, **«Верификация»**, **«Мониторинг»**, описание разделов см. в *Руководствах пользователя* на модули ПО);
- *«Бюро пропусков»* (раздел **«Бюро пропусков»**, описание см. в *Руководствах пользователя* на модули ПО);
- *«Бухгалтерия»* (раздел **«Учет рабочего времени»**, описание раздела см. в *Руководстве пользователя* на модуль ПО ***PERCo-WM01***, ***PERCo-WME01***).

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**.

5.1. 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-Marin* 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-Marin* и блоком индикации со светодиодными индикаторами.
- ***PERCo-CL05.2.*** Позволяет организовать одну одностороннюю точку прохода или, при использовании двух контроллеров данной модели, одну двухстороннюю точку прохода. Контроллер снабжен встроенным считывателем карт доступа формата *HID*, *EM-Marin* и блоком индикации со светодиодными индикаторами. В версии ***PERCo-CL05.2*** контроллера максимальное число хранимых событий журнала регистрации увеличено до 230 000, реализовано использование неограниченного числа комиссионирующих карт, улучшен Web-интерфейс.
- ***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-CT/L04.2.*** Позволяет организовать две двухсторонние точки прохода или четыре односторонние точки прохода, управляя при этом соответственно двумя или четырьмя ИУ. При этом к контроллеру по интерфейсу *RS-485* подключаются дополнительно устанавливаемые выносные считыватели.
- ***Биометрический контроллер PERCo-CL15.*** Предназначен для организации одной односторонней точки прохода, одного направления двухсторонней точки прохода (при использовании двух контроллеров данной модели) или одного направления прохода для шлюза (при использовании четырех контроллеров данной модели).
- ***PERCo-CT/L14.*** Во внутреннюю память контроллера загружена специальная версия ПО ***PERCo-Web***, таким образом, в организуемой на базе данного контроллера системе СКУД нет необходимости иметь сервер на отдельном ПК.
- ***PERCo-CL201.x.*** Подключается в качестве контроллера второго уровня к контроллерам ***PERCo-CT/L04*** и ***PERCo-CT/L04.2*** или встроенному контроллеру ЭП ***PERCo-CT03***, ***PERCo-CT03.2*** по интерфейсу *RS-485* и позволяет организовать одно КПП с контролем проходов в одном направлении. Контроллер снабжен встроенным считывателем карт доступа формата *HID*, *EM-Marin* и блоком индикации со светодиодными индикаторами. Одновременно к контроллеру первого уровня может быть подключено до 8 контроллеров второго уровня.

Примечание:

При работе с контроллерами ***PERCo-CT/L04.2***, ***PERCo-CT03.2*** подключение контроллеров второго уровня ***PERCo-CL201.x*** производится через ***Web-интерфейс*** контроллеров ***PERCo-CT/L04.2***, ***PERCo-CT03.2***, после чего становится доступным управление подключенными контроллерами через интерфейс ***PERCo-Web***.

5.2. 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-CT/L04.2***. Позволяет организовать одну двухстороннюю точку прохода. При этом к контроллеру по интерфейсу *RS-485* подключаются встроенные считыватели турникета, дополнительно устанавливаемые выносные считыватели или ИУ (замки).
- ***PERCo-CT03***, ***PERCo-CT03.2***. Встроенные контроллеры в составе ЭП, позволяют организовать одно КПП с контролем проходов в двух направлениях.
- ***Биометрический контроллер PERCo-CL15***. Предназначен для организации одной односторонней точки прохода, одного направления двухсторонней точки прохода (при использовании двух контроллеров данной модели) или одного направления прохода для шлюза (при использовании четырех контроллеров данной модели).
- ***PERCo-CT/L14***. Во внутреннюю память контроллера загружена специальная версия ПО ***PERCo-Web***, таким образом, в организуемой на базе данного контроллера системе СКУД нет необходимости иметь сервер на отдельном ПК.
- ***PERCo-CT13***. Контроллер встроен в электронные проходные ***KT02.9B***, ***KT02.9Q***.

5.3. Контроллеры регистрации

Контроллеры регистрации предназначены для организации терминала учета рабочего времени и контроля трудовой дисциплины. Не поддерживают возможность управления ИУ.

- ***PERCo-CR01 LICON***. Снабжен двумя встроенными считывателями карт доступа формата *HID*, *EM-Marin* и ЖКИ (дисплеем) с диагональю 2,8''.
- ***PERCo-CR01.2 LICON***. Снабжен двумя встроенными считывателями карт доступа формата *HID*, *EM-Marin* и ЖКИ (дисплеем) с диагональю 2,8''. По сравнению с ***PERCo-CR01 LICON*** число карт доступа пользователей увеличено до 50 000, улучшен Web-интерфейс управления.
- ***Биометрический терминал учета рабочего времени PERCo-CR11***. Снабжен встроенными сканером отпечатков пальцев и двумя считывателями карт доступа форматов *HID*, *EM-Marin* и *Mifare*, имеет цветной ЖКИ с тачскрином и с диагональю 4,8''. Имеет возможность просмотра баланса рабочего времени и ввода оправдательных документов.

5.4. Терминалы распознавания лиц

Терминал распознавания лиц предназначен для организации одной односторонней точки прохода или одного направления двухсторонней точки прохода. Имеет встроенные камеры и датчики для распознавания лиц, ЖК дисплей. В зависимости от модели может быть снабжен встроенным считывателем карт доступа и виртуальной клавиатурой для набора ПИН-кода.

В системе ***PERCo-Web*** предусмотрена полная интеграция следующих типов ТРЛ:

- **Производства *"ZKTeco"***: терминалы ***FaceDepot-7A***, ***FaceDepot-7B***, ***ProFaceX, SpeedFace-V5L-TD*** (с пирометром).
- **Производства *"Suprema"***: терминалы ***FaceStation 2***, ***FaceLight***.

ТРЛ являются полноценными контроллерами с одним выходом для управления ИУ. При необходимости их можно использовать для совместной работы с ЭП или контроллером ***PERCo***. Для этого релейный выход ТРЛ подключается на управляющий вход контроллера ***PERCo*** параллельно ПДУ, при этом конфигурация выхода ТРЛ должна быть нормально разомкнутой.

При проходе через ЭП по распознаванию лица в журнале событий системы будет генерироваться событие *«Проход по идентификатору (лицо)»* от ТРЛ. Для корректной работы учета рабочего времени необходимо в параметрах ТРЛ задать подтверждающий контроллер ***PERCo***. В таком случае от контроллера ***PERCo*** будет ожидаться событие *«Проход по команде от ДУ»*, после чего в журнал событий системы запишется событие прохода, в противном случае – событие *«Отказ от прохода»*.

Если в работе ТРЛ сигнал PASS от ЭП использоваться не будет, то в настройках ТРЛ необходимо активировать параметр *«Регистрация прохода по предъявлению идентификатора»*. Соответственно, в этом случае события отказа от прохода через ЭП по распознаванию лица формироваться не будут.

В системе, имеющей в своем составе ТРЛ, для корректной работы глобального антипасса необходимо из общей схемы маршрутов передвижения исключить ИУ, управляемые ТРЛ.

5.5. Исполнительные устройства

Замки

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

Турникеты

- турникеты-триподы серий ***PERCo-T*** и ***PERCo-TTR***;
- тумбовые турникеты серий ***PERCo-TTD***, ***PERCo-TB*** и ***PERCo-TBC***;
- роторные турникеты серии ***PERCo-RTD***;
- турникеты-скоростные проходы серии ***PERCo-ST***;
- турникеты сторонних производителей.

Калитки

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

Шлагбаумы

- автоматический шлагбаум ***PERCo-GS04***;
- шлагбаумы сторонних производителей.

5.6. 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-AC-02.1***.

- В качестве внешних считывателей карт доступа могут использоваться: считыватели серий ***PERCo-IR***, ***PERCo-MR***, снабженные блоками индикации;
- стойка-считыватель ***PERCo-IRP01***, снабженная ЖК-дисплеем.

Для подключения к USB-разъему ПК используются контрольные считыватели серий:

- ***PERCo-IR 05*** для карт формата *HID*, *EM-Marin;*
- ***PERCo-IR 08***, ***PERCo-MR 08*** для карт формата *Mifare;*

- ***PERCo-IR18*** для карт формата *HID*, *EM-Marin, Mifare* и работы с биометрией.

5.7. 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*. Доступны следующие серии электронных проходных:

- ***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.

5.8. Устройства управления

- ***PERCo-H6/4*** – проводной пульт дистанционного управления (ПДУ) предназначен для автономного управления 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 управления 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***, ***PERCo-CT/L04.2*** или ***PERCo-CT/L14***. 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.

5.9. Контроллеры доступа со сканерами отпечатков пальцев

В целях расширения функциональных возможностей системы ***PERCo-Web*** по поддержке биометрических технологий в общую систему СКУД могут встраиваться следующие контроллеры со сканерами отпечатков пальцев:

1. Контроллеры доступа ***Suprema***

- ***BioEntry Plus*** (платформа ***BioStar 2***) – биометрический контроллер доступа с возможностью подключения по сети *Ethernet* и протоколу TCP/IP.
- ***BioEntry W2*** – биометрический контроллер доступа в прочном металлическом пыле- и влагозащитном корпусе с возможностью подключения по сети *Ethernet* и протоколу TCP/IP.
- ***BioEntry P2*** – биометрический контроллер доступа с подключением по сети *Ethernet* и протоколу TCP/IP.

Примечание:

Для интеграции необходимо, чтобы биометрические контроллеры имели версию внутреннего ПО ("прошивку"), не старее чем:
- для контроллера ***BioEntry W2*** – 1.1.1;
- для контроллера ***BioEntry Plus*** (платформа ***BioStar 2***) – 2.3.1.

Предусмотрено три варианта подключения данных контроллеров к системе:
- в качестве контроллера одностороннего замка. В этом случае ИУ подключается непосредственно к управляющему выходу контроллера ***Suprema***. Связь с контроллером ***Suprema*** в системе осуществляется по интерфейсу *Ethernet*;
- в качестве считывателя отпечатков пальцев при управлении одним из направлений двухстороннего замка (турникета). В этом случае контроллер ***Suprema*** подключается к контроллеру ***PERCo-CT/L04***, ***PERCo-CT/L04.2*** или ***PERCo-CT/L14*** по интерфейсу *Wiegand* через конвертер интерфейса ***PERCo-AC02***;
- для совместной работы с ЭП или контроллером ***PERCo***: релейный выход контроллера ***Suprema*** подключается на управляющий вход контроллера ***PERCo*** параллельно ПДУ, при этом конфигурация выхода ТРЛ должна быть нормально разомкнутой.

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

2. Контроллеры доступа ***ZKTeco***

   В систему ***PERCo-Web*** могут встраиваться контроллеры доступа ***ZKTeco*** с поддержкой гибридной биометрии. Контроллеры указанной линейки поддерживают в том числе сканирование ладоней для бесконтактной верификации доступа.

   Предусмотрено два варианта подключения данных контроллеров к системе:
   - в качестве контроллера одностороннего замка. В этом случае ИУ подключается непосредственно к управляющему выходу контроллера ***ZKTeco***. Связь с контроллером ***ZKTeco*** в системе осуществляется по интерфейсу *Ethernet*;
   - для совместной работы с ЭП или контроллером ***PERCo***: релейный выход контроллера ***ZKTeco*** подключается на управляющий вход контроллера ***PERCo*** параллельно ПДУ, при этом конфигурация выхода ТРЛ должна быть нормально разомкнутой.

5.10. Картоприемники

- Картоприемник ***PERCo-IC05***, встроенные картоприемники турникетов, скоростных проходов и электронных проходных ***PERCo***.
- Картоприемники сторонних производителей.

5.11. Дополнительное оборудование

- ***PERCo-AU05*** – табло системного времени (ТСВ) предназначено для отображения времени. ТСВ подключается по интерфейсу *RS-485* к контроллерам серий ***PERCo-CT/L04***, ***PERCo-CT/L04.2***, ***PERCo-CT/L14*** и встроенным контроллерам ЭП ***PERCo-CT03***, ***PERCo-CT03.2***, ***PERCo-CT13***.
- ***ДКЗП*** – датчик контроля зоны прохода предназначен для регистрации несанкционированного прохода или проникновения под преграждающими планками.
- ***Сирена*** – звуковой оповещатель.
- ***Сканер штрихкода*** (USB) – устройство для считывания штрихкода и передачи его в систему.

5.12. Видеокамеры

В системе могут использоваться IP-видеокамеры (в т.ч. видеокамеры стандарта ONVIF) и аналоговые видеокамеры, подключенные к IP-видеосерверам.

Примечание:

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

6. Основные технические характеристики

Стандарт интерфейса связи.....*Ethernet (IEEE 802.3)*

Скорости передачи данных *Ethernet*, *Мбит/с* 10/100

Количество контроллеров СКУД ..... не более 1000

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 в системе, *шт.* ..... не ограничено

Максимальное количество сотрудников ..... не более 200 000

Максимальное количество посетителей..... не более 200 000

Число событий регистрации для каждого контроллера..... 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

скользящий понедельный график (в пределах 54 недель)..... не более 255

Количество дней с особым статусом, праздников (до 8 типов)..... не более 365

Объем памяти контроллеров *PERCo*
для хранения идентификаторов и событий журнала регистрации

Контроллер	Вариант конфигурации	К-во карт	К-во событий	К-во отпечатков пальцев
CL201.1	Контроллер замка второго уровня	до 1 000	-	-
CR01 LICON	Контроллер регистрации	до 5 000	до 140 000	-
CL05.1	Контроллер замка	до 50 000	до 135 000	-
CT/L04	Контроллер для управления одной двухсторонней дверью	до 50 000	до 135 000	-
	Контроллер для управления одной двухсторонней дверью с подключением до 8-ми контроллеров замка ***PERCo-CL201***	до 10 000	до 135 000	-
	Контроллер для управления двумя односторонними дверьми с подключением до 8-ми контроллеров замка ***PERCo-CL201***	до 1 000 на каждый замок	до 135 000	-
CT/L04, CT03	Контроллер для управления турникетом	до 50 000	до 135 000	-
	Контроллер для управления турникетом с подключением до 8-ми контроллеров замка ***PERCo-CL201***	до 10 000	до 135 000	-

Контроллер	Вариант конфигурации	К-во карт	К-во событий	К-во отпечатков пальцев
CT/L04	Контроллер АТП	до 50 000	до 135 000	-
	Контроллер АТП с подключением до 8-ми контроллеров замка ***PERCo-CL201***	до 10 000	до 135 000	-
CR01.2 LICON	Контроллер регистрации	до 50 000	до 125 000	-
		до 40 000	до 280 000	-
		до 30 000	до 440 000	-
		до 20 000	до 600 000	-
		до 10 000	до 760 000	-
CL05.2	Контроллер замка	до 50 000	до 230 000	-
		до 40 000	до 390 000	-
		до 30 000	до 550 000	-
		до 20 000	до 710 000	-
		до 10 000	до 870 000	-
CT/L04.2	Универсальный контроллер турникета / замка	до 50 000	до 230 000	-
		до 40 000	до 390 000	-
		до 30 000	до 550 000	-
		до 20 000	до 710 000	-
		до 10 000	до 870 000	-
CT03.2	Встроенный контроллер электронной проходной	до 50 000	до 230 000	-
		до 40 000	до 390 000	-
		до 30 000	до 550 000	-
		до 20 000	до 710 000	-
		до 10 000	до 870 000	-
Биометрический контроллер CL15	Контроллер для управления замком	нет ограничения	нет ограничения	5 000 пользователей по 2 отпечатка пальца
CT/L14, CT13	Контроллер для управления турникетами и / или замками, встроенный контроллер ЭП	нет ограничения	нет ограничения	5 000 пользователей по 2 отпечатка пальца
Биометрический терминал УРВ CR11	Контроллер регистрации	нет ограничения	нет ограничения	5 000 пользователей по 2 отпечатка пальца

Примечания:

- Технические характеристики контроллеров сторонних производителей, имеющих возможность интеграции с системой ***PERCo-Web***, указаны в эксплуатационной документации на эти контроллеры.
- 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.

Внимание!

В специальной версии ПО ***"PERCo-Web"*** (пакеты ПО ***PERCo-WBE***, ***PERCo-WSE***, ***PERCo-WME01***, ***PERCo-WME02***), которая встраивается в память контроллеров ***PERCo-CL15***, ***PERCo-CR11***, ***PERCo-CT/L14***, ***PERCo-CT13***, присутствуют следующие ограничения:

- Устройства (контроллеры) до 10 шт.
- Подразделения до 100 шт.
- Должности до 5000 шт.
- Графики работы до 100 шт.
- Дополнительные текстовые поля до 16 шт.
- Дополнительные графические поля до 10 шт.
- Сотрудники до 500 шт.
- Посетители до 500 шт.
- Шаблоны доступа до 1000 шт.
- Дизайн пропуска до 1000 шт.
- Оправдательные документы до 10 шт.
- Шаблоны верификации до 10 шт.
- Точки верификации до 10 шт.
- Помещения до 100 шт.
- Задания по расписанию до 100 шт.
- Операторы до 100 шт.
- Роли операторов до 100 шт.
- Не поддерживаются работа с камерами и видеосервером, импорт данных.

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 одна из следующих ОС:

- ОС семейства *Microsoft Windows x64*, возможно использование настольных ОС *Windows: 7, 8.1, 10* или *Windows Server 2008 R2, 2012 R2, 2016*.
- Дистрибутивы GNU/Linux с архитектурой amd64:
  - *Ubuntu 16.04, Ubuntu 18.04;*
  - *Fedora 30;*
  - *CentOS 7;*
  - *Alt Linux 8.2;*
  - *Rosa: Enterprise Server 7.3, Cobelt Server 7.3, Enterprise Desktop 7.3, Cobelt Desktop 7.3, Enterprise Desktop RX4.*

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*.

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 объем – 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* или *Apple Mac OS*. Рекомендованы к использованию ОС: *Windows 7, 8.1*, *10; MacOS X* или 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.

Примечание:

IE позволяет работать только с **Менеджером системы *PERCo-Web***, для клиента данный браузер не поддерживается.

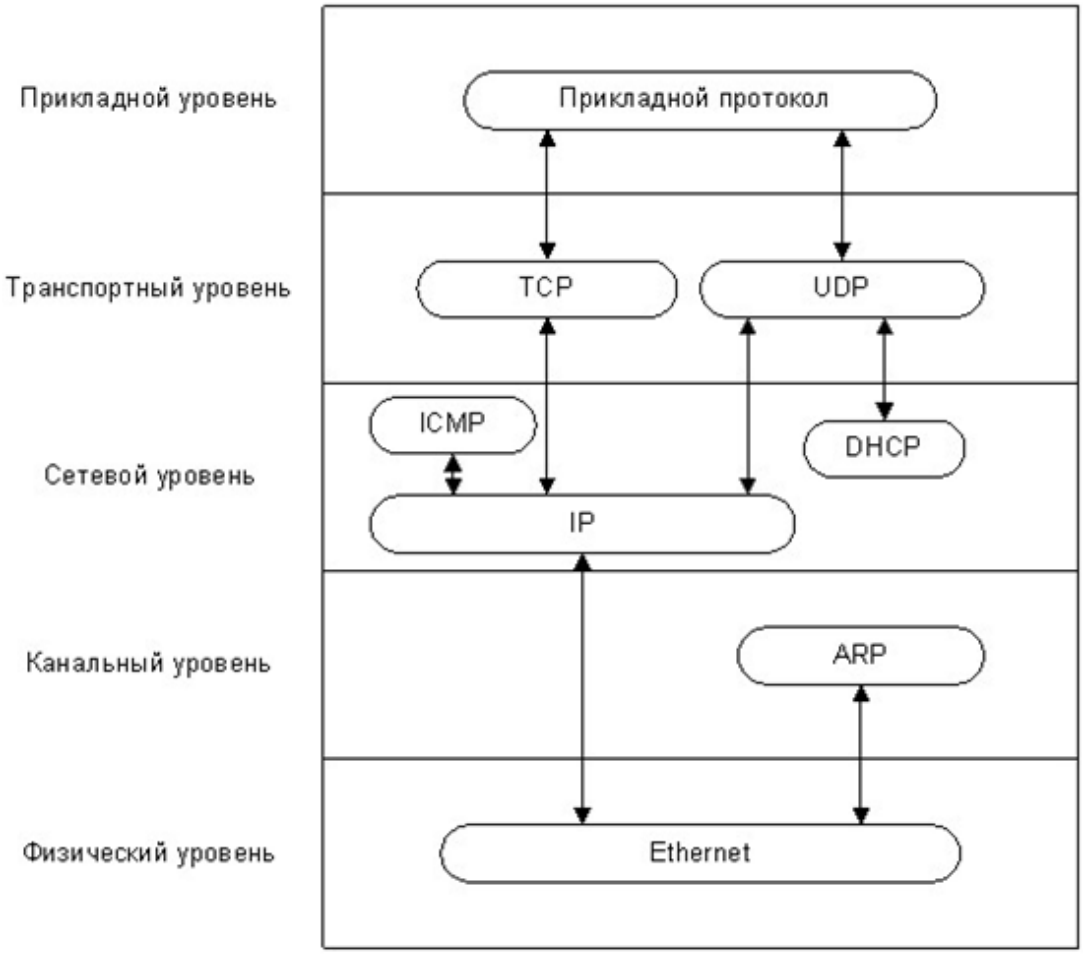
8. Сетевые настройки

8.1. Используемые сетевые порты и протоколы

Внимание!

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

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



Стек протоколов, используемых для обмена в системе

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

Примечание:

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

Используемые в системе сетевые порты

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

8.2. Организация широковещательной рассылки пакетов

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

1. Выделите один из ПК системы в качестве шлюза (маршрутизатора). Число сетевых карт, установленных в этом ПК, должно соответствовать числу подключаемых подсетей. Например, если в системе используется три подсети, то на этом ПК должны быть установлены три сетевые карты.
2. Произведите настройку сетевых интерфейсов каждой сетевой карты ПК, выделенного в качестве шлюза. Перед настройкой подсетей необходимо проверить, чтобы IP-адрес был свободен и не занят другими устройствами.

   Например,
   - IP-адрес: `10.1.1.1` Маска подсети: `255.255.0.0`
   - IP-адрес: `10.2.1.1` Маска подсети: `255.255.0.0`
   - IP-адрес: `10.3.1.1` Маска подсети: `255.255.0.0`
3. Включите на ПК, используемом в качестве шлюза, маршрутизацию пакетов TCP/IP. Для этого в ветке реестра ОС *Windows*:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters`

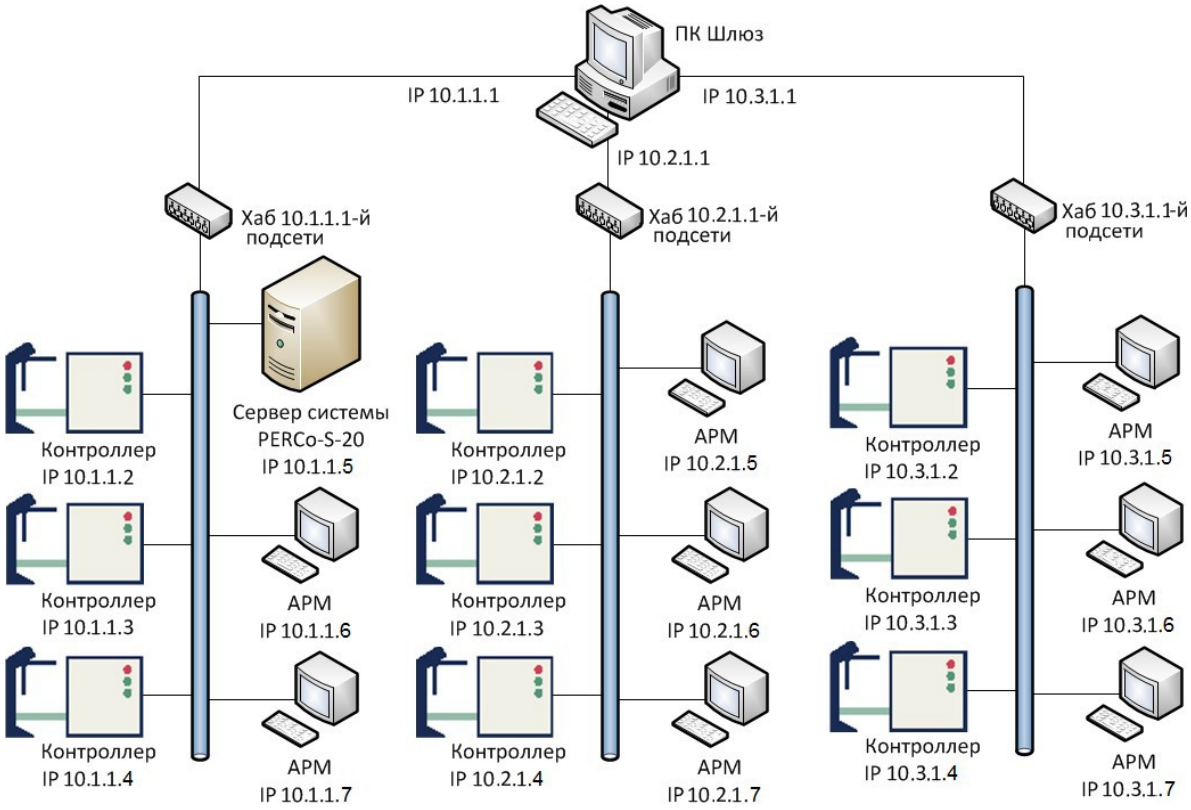
   установите значение параметра: `IPEnableRouter=1`

Примечание:

Дополнительная информация о включении маршрутизации пакетов в ОС *Microsoft Windows* доступна на сайте производителя по адресу: https://support.microsoft.com/

4. Устройствам (контроллерам, ПК) подсети установите соответствующие этой подсети сетевые настройки.

   Например,
   - для устройств *10.1.1.1*-й подсети:
     - IP-адрес: `10.1.1.x`, где `x`= 2, 3, ... ;
     - Маска подсети: `255.0.0.0`;
     - Основной шлюз: `10.1.1.1`.
   - для устройств *10.2.1.1*-й подсети:
     - IP-адрес: `10.2.1.x`, где `x`= 2, 3, ... ;
     - Маска подсети: `255.0.0.0`;
     - Основной шлюз:`10.2.1.1`.
   - для устройств *10.3.1.1*-й подсети:
     - IP-адрес: `10.3.1.x`, где `x`= 2, 3, ... ;
     - Маска подсети: `255.0.0.0`;
     - Основной шлюз: `10.3.1.1`.

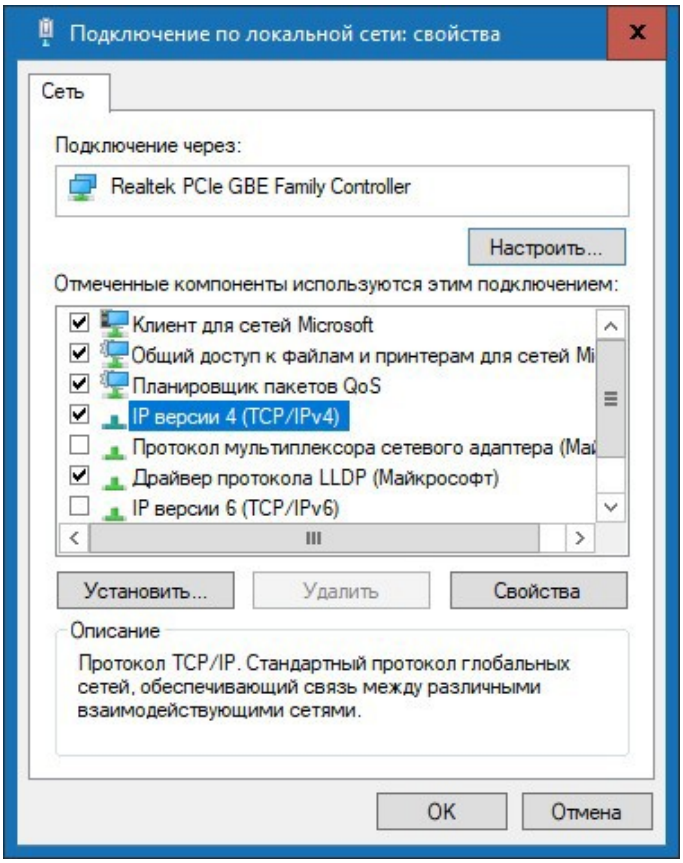


Пример схемы организации широковещательной рассылки

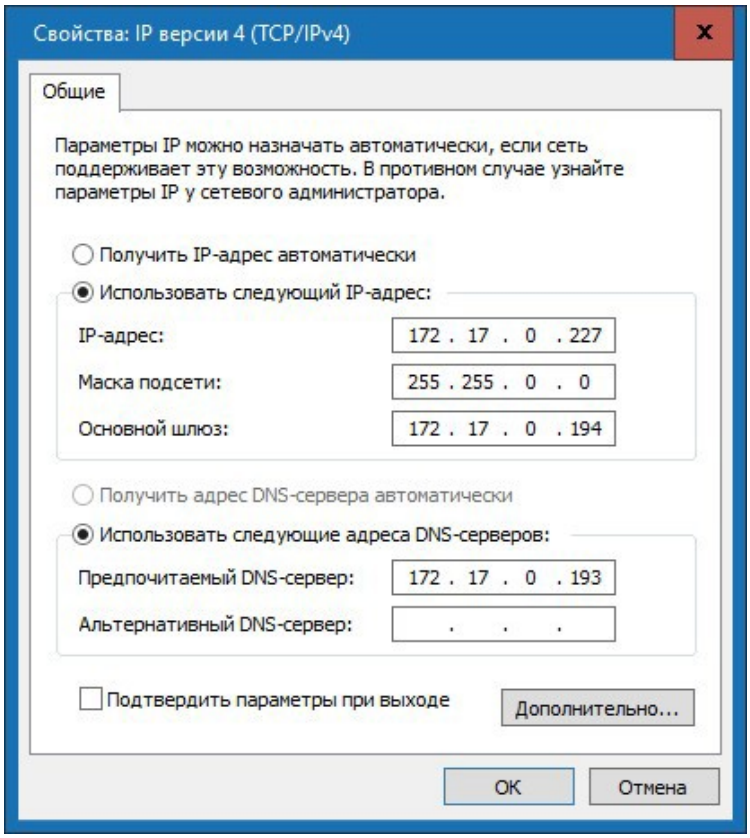
8.3. Добавление сетевого интерфейса ПК

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

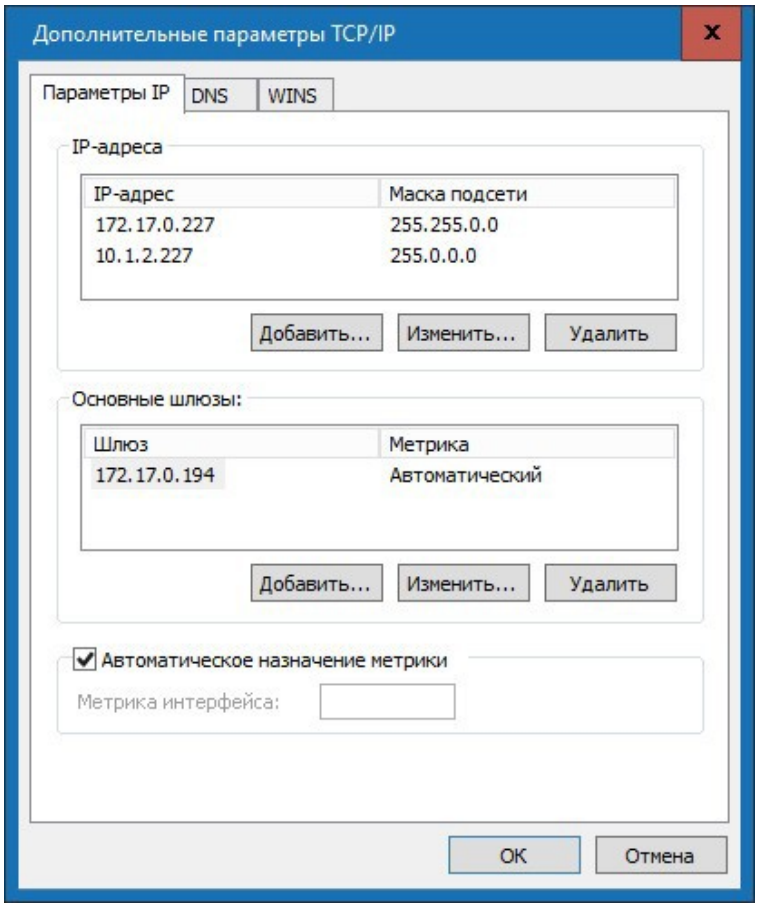
1. Откройте окно свойств **Подключение по локальной сети**.
2. Нажмите кнопку **Свойства**. Откроется новое окно:



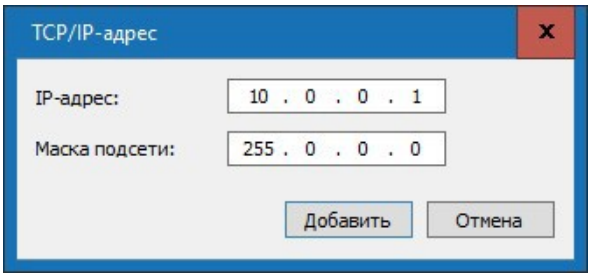
3. Выделите компонент **IP версии 4 (TCP/IPv4)** и нажмите кнопку **Свойства**. Откроется окно **Свойства: IP версии 4 (TCP/IPv4)**:



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



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



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

8.4. Сетевые настройки контроллера

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

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

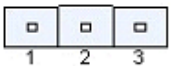
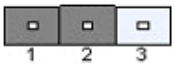
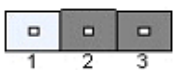
При производстве контроллерам системы заданы следующие сетевые настройки:
- **MAC-адрес:** уникальный, неизменяемый (указан в паспорте и на плате устройства);
- **IP-адрес:** `10.x.x.x` (указан в паспорте и на плате устройства);
- **Шлюз:** `0.0.0.0`;
- **Маска подсети:** `255.0.0.0`.

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

Внимание!

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

Варианты установки перемычки на разъем XP1 контроллера *PERCo*

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

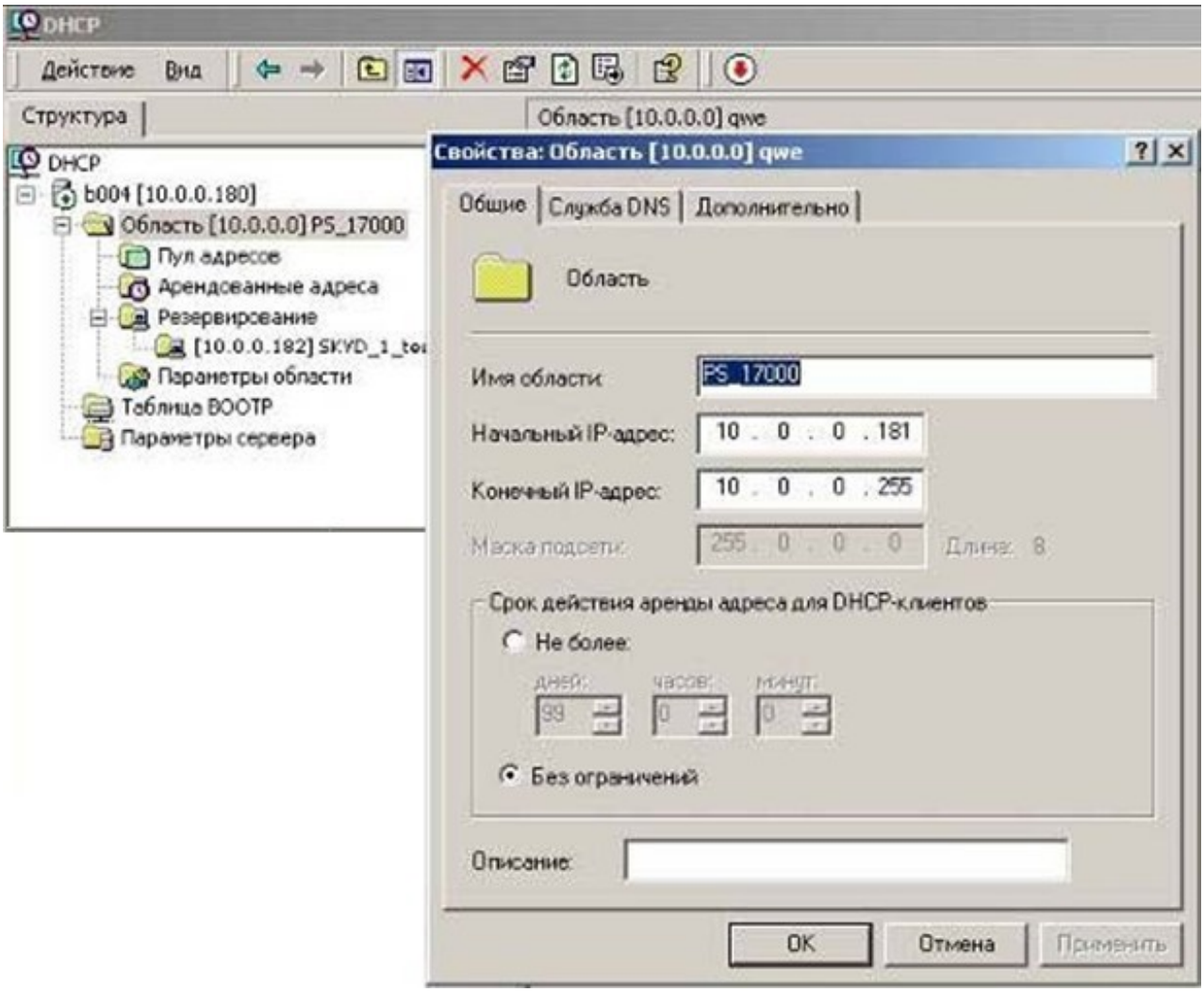
Изменение сетевых настроек контроллера в *«Ручном режиме»* может производиться от ПК с установленным ПО ***PERCo-Web*** или через Web-интерфейс контроллера. При этом необходимо, чтобы контроллер и ПК были подключены к сети *Ethernet* и находились в одной подсети (возможно подключение контроллера непосредственно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

8.5. Настройка DHCP-сервера в ОС Windows

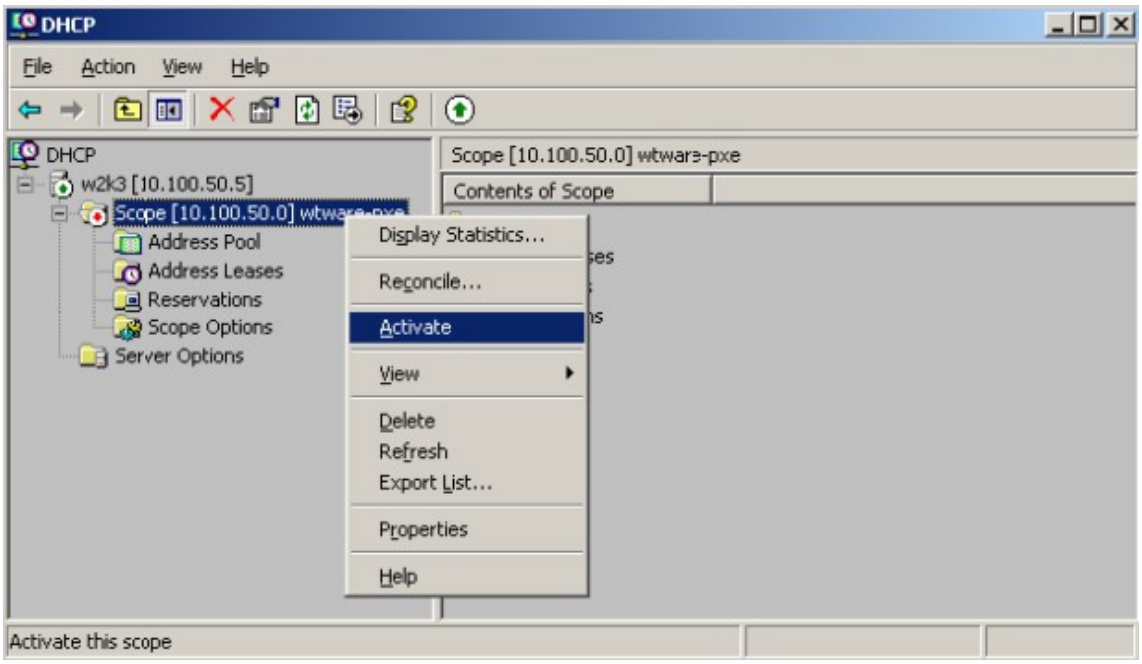
Для работы в сетях с динамическим распределением IP-адресов, когда контроллеры получают сетевые настройки от DHCP-сервера, необходимо для всех контроллеров системы с помощью перемычки на плате установить режим *«IP MODE»*.

При настройке DHCP-сервера необходимо зарезервировать диапазон IP-адресов, выделяемых контроллерам системы. После чего привязать MAC-адреса контроллеров к IP-адресам из зарезервированного диапазона. Для этого (далее приведен пример настройки DHCP-сервера для системы *Windows XP*):

1. Запустите DHCP-сервер. Для этого выберите последовательно: **Пуск> Программы> Администрирование> DHCP**. Откроется окно **DHCP**.
2. Зарезервируйте диапазон IP-адресов для контроллеров системы. Название области и описание могут быть любыми. Эта информация необходима для системного администратора, поэтому название должно быть достаточно информативным. Рекомендуется делать область несколько больше, чем число контроллеров, которое планируется использовать. Также задавайте такую область адресов, которая не будет включать в себя уже существующие ПК с фиксированными адресами:

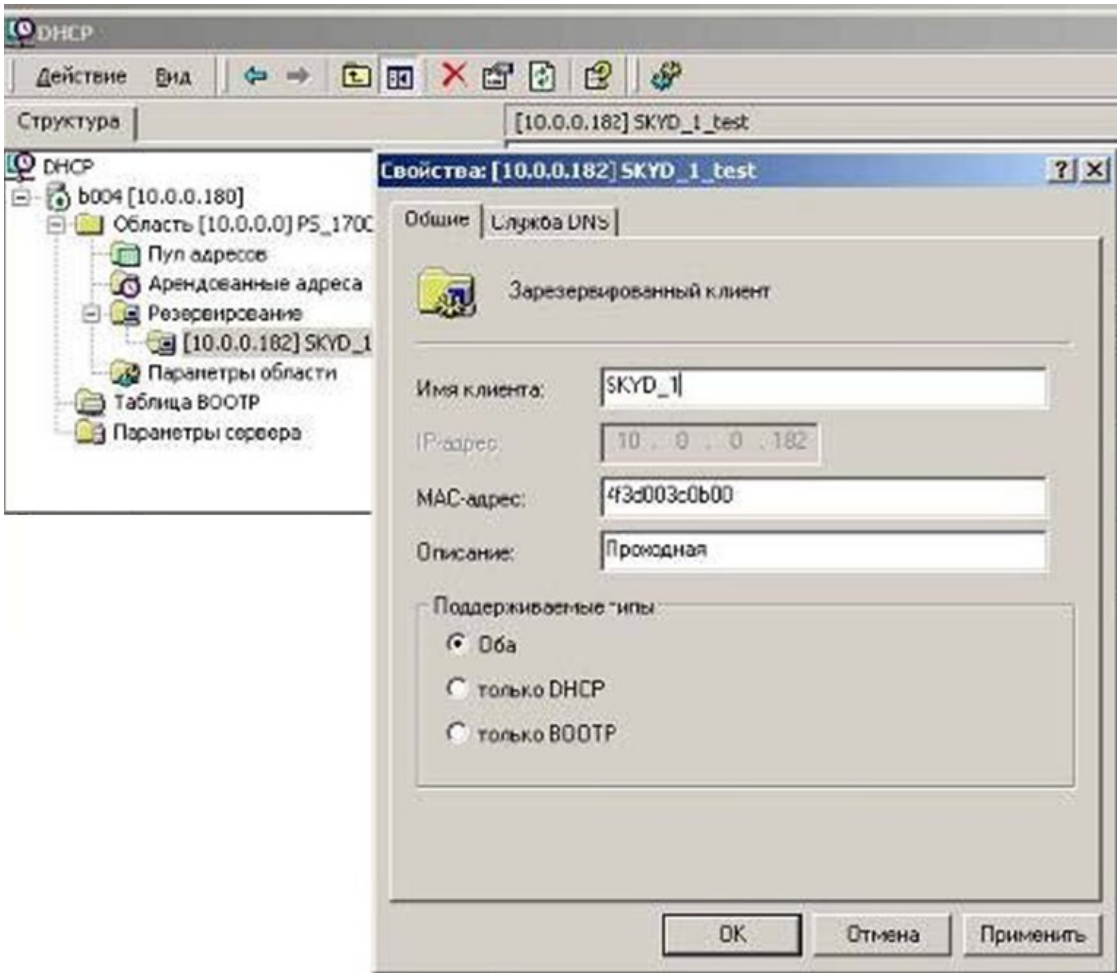


3. Произведите активацию области:



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

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



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

8.6. Настройка DHCP-сервера в ОС Linux

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

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

Пример варианта файла конфигурации:

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

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

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

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

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

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

8.7. Внешнее подключение контроллера к серверу *PERCo-Web*

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

Внимание!

Данная функция возможна только для контроллеров ***PERCo-CL15***, ***PERCo-CR11***, ***PERCo-CT/L14*** и для встроенного контроллера ***CT13*** электронных проходных ***PERCo-KT02.9B***, ***PERCo-KT02.9Q***.

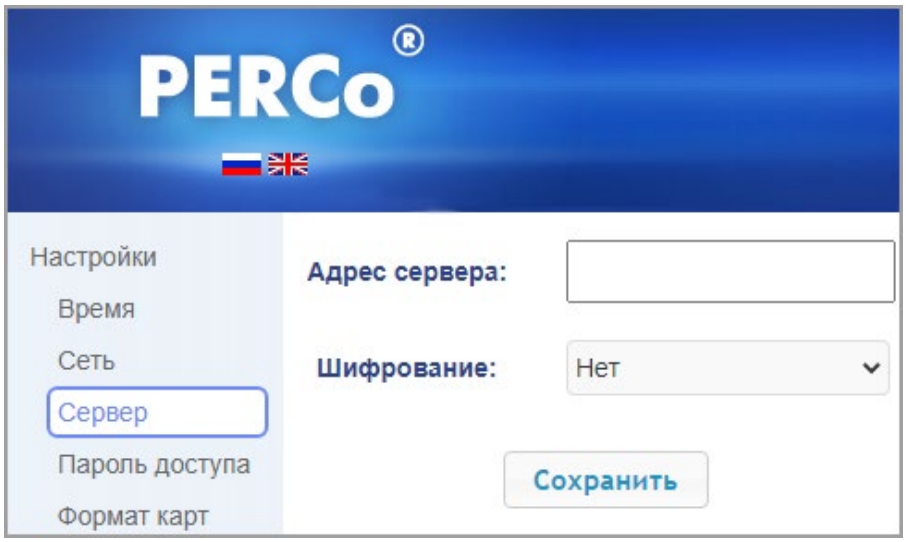
Для подключения контроллера к серверу ***PERCo-Web*** по внешнему IP-адресу сервера:

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

Примечание:

Полное руководство по работе с Web-интерфейсом смотрите в руководствах по эксплуатации на контроллеры ***PERCo-CL15***, ***PERCo-CR11***, ***PERCo-CT/L14*** и на электронные проходные ***PERCo-KT02.9B***, ***PERCo-KT02.9Q***.

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

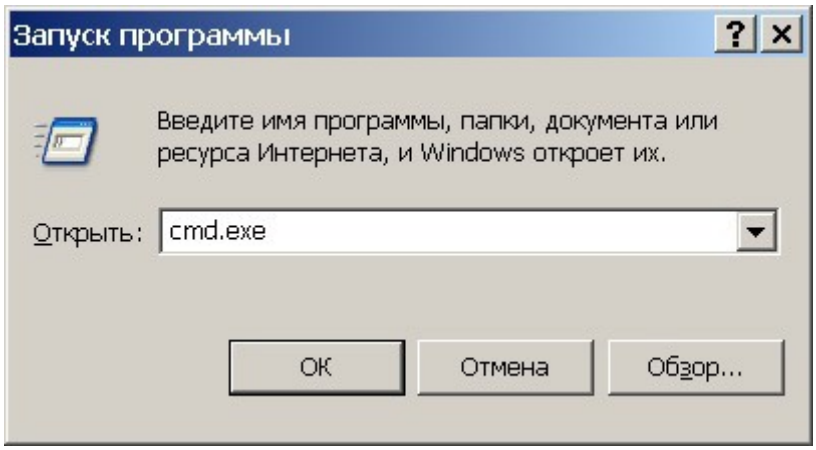


4. В открывшемся окне произведите необходимые изменения:
   - в поле **Адрес сервера** введите IP-адрес сервера, на котором установлена система ***PERCo-Web***;
   - в параметре **Шифрование** задайте требуемый способ шифрования.
5. Нажмите кнопку **Сохранить**. Внесенные изменения будут сохранены.

8.8. Проверка связи между ПК и контроллером

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

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

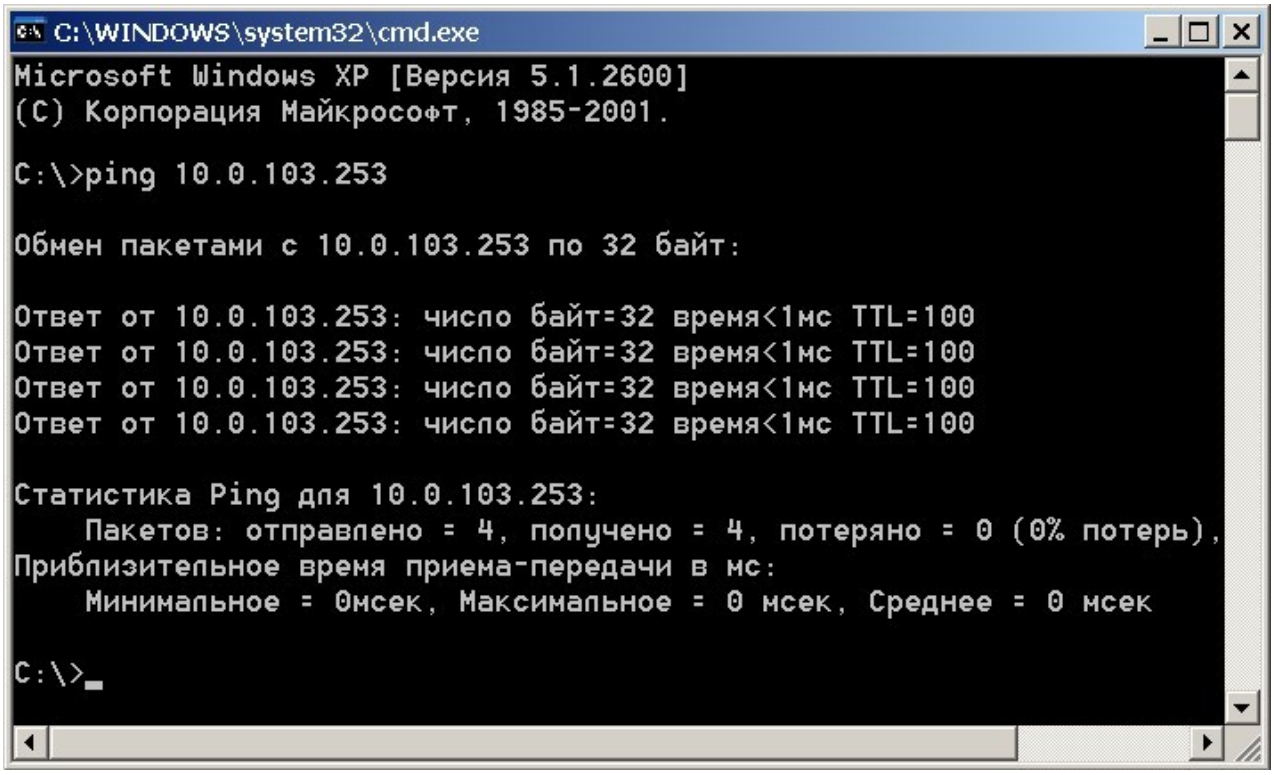


2. В открывшемся окне введите команду: **cmd.exe** и нажмите кнопку **ОК**.
3. Откроется окно интерфейса командной строки с заголовком:

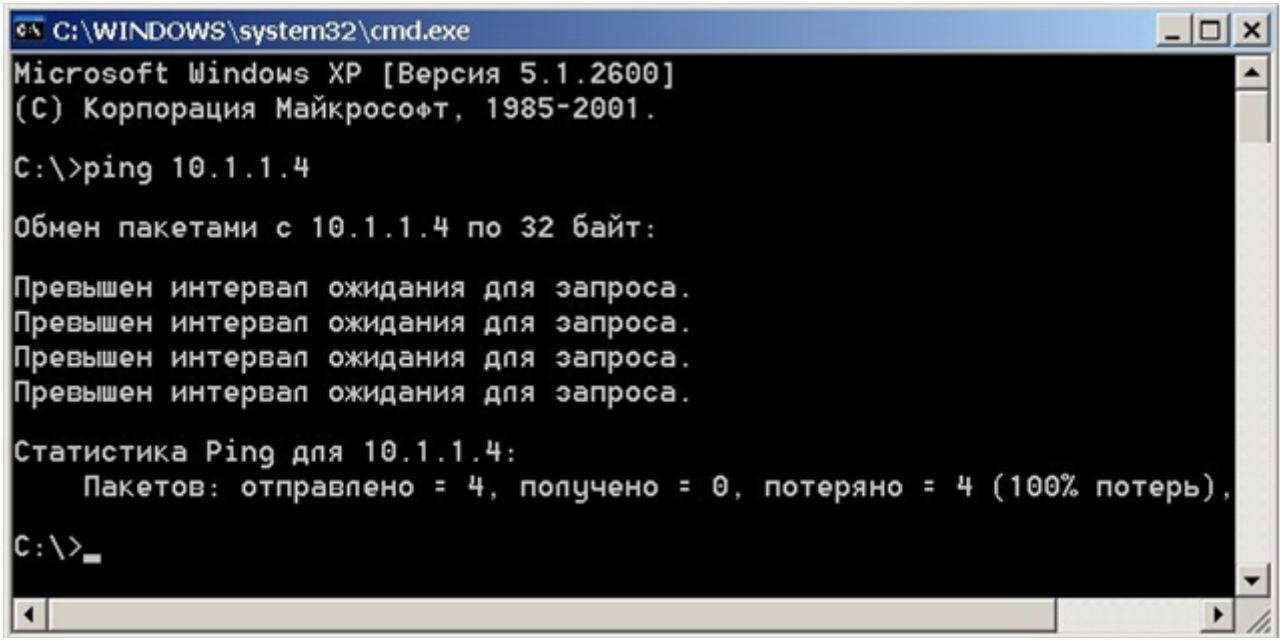
   C:\WINDOWS\system32\cmd.exe.
4. В открывшемся окне введите команду:

   `ping XX.XX.XX.XX`, где `XX.XX.XX.XX` – IP-адрес контроллера, с которым необходимо проверить связь (например 10.0.103.253).
5. Если связь будет установлена, то появится ответ следующего вида:

   `Ответ от XX.XX.XX.XX: число байт=32 время<10мс TTL=128.`



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

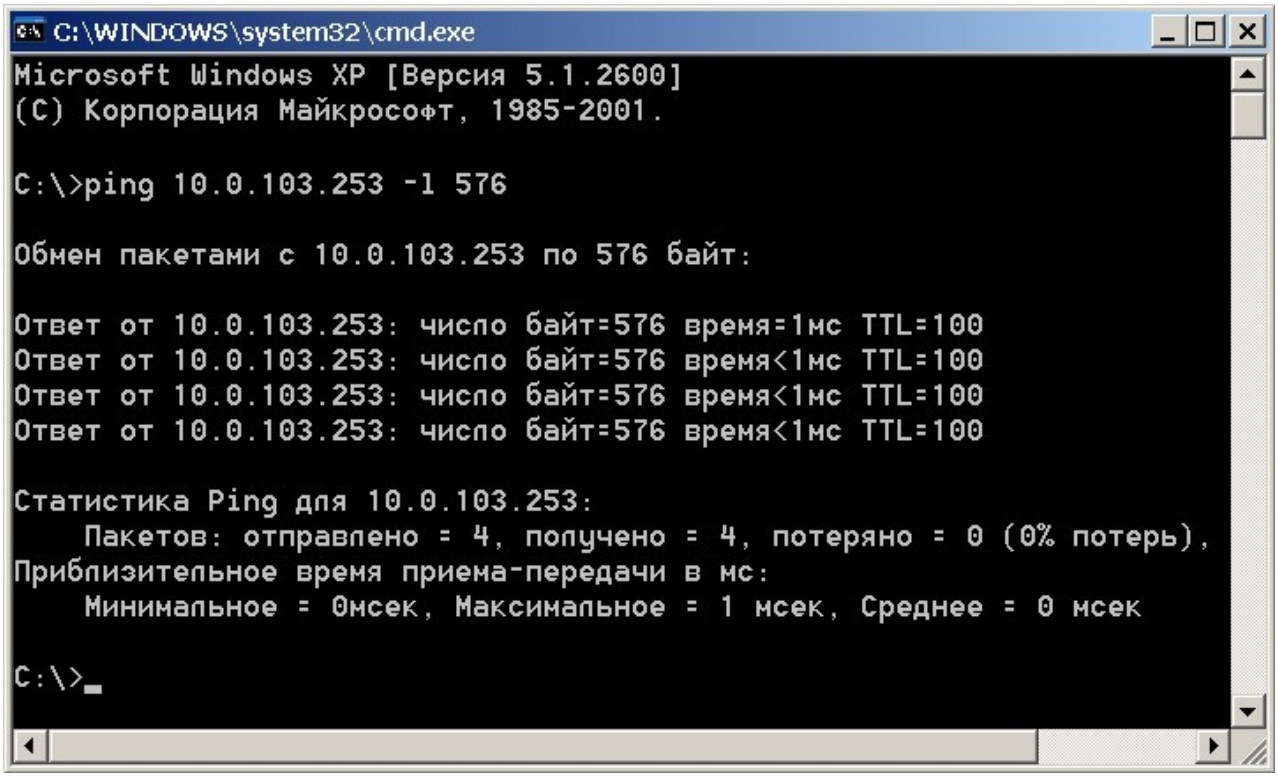


7. Контроллеры системы не поддерживают фрагментацию IP-пакетов. Поэтому необходимо удостовериться, что IP-пакеты на всем протяжении от сервера системы до контроллера не фрагментируются. Для этого введите ту же команду с ключом `-l` и указанием на размер отправляемого пакета данных, например, 576 байт:

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

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

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



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

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

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

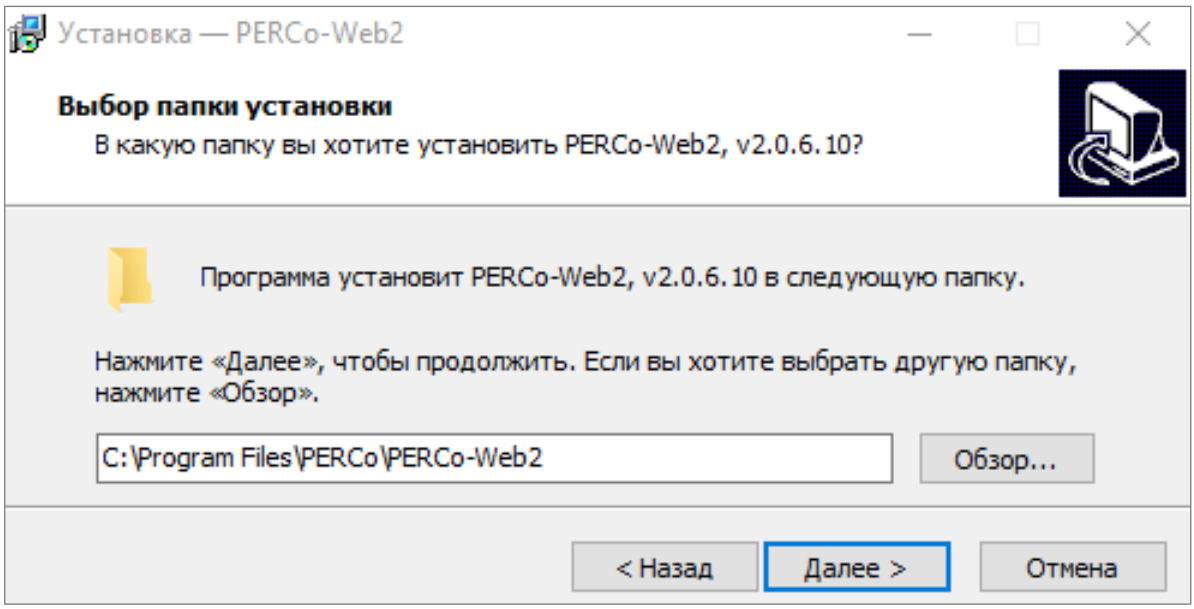
9. Установка системы

Внимание!

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

При установке системы придерживайтесь следующей последовательности действий:

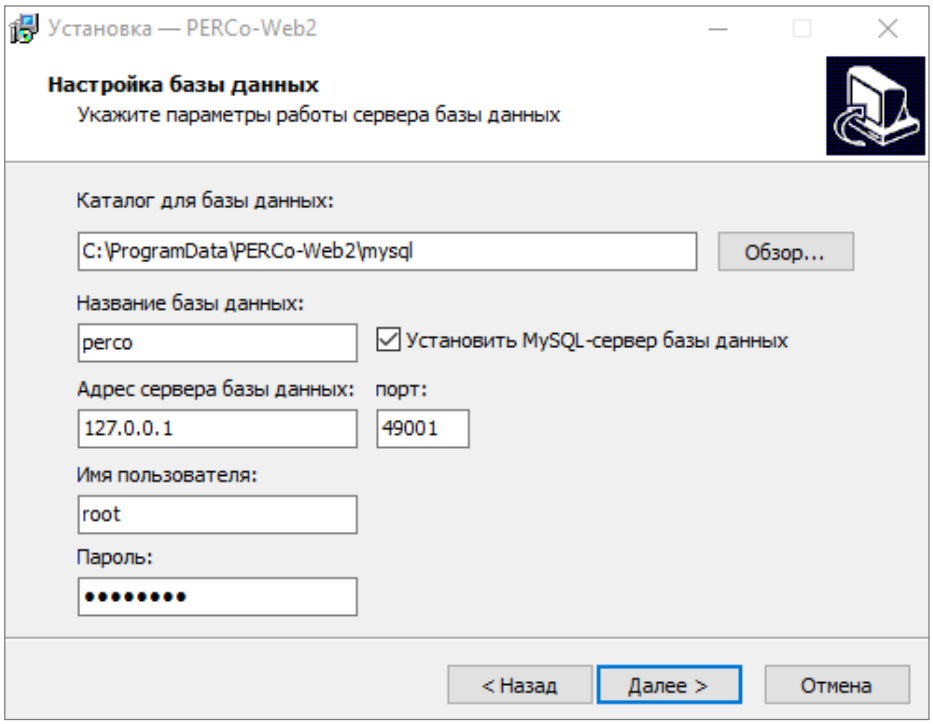
1. Запустите установочный файл Setup.exe. Следуйте указаниям мастера установки. Актуальная версия установочного файла системы ***PERCo-Web*** доступна на сайте компании ***PERCo***, расположенном по адресу: www.perco.ru, в разделе **Поддержка> Программное обеспечение**.
2. Выберите язык установки.
3. Выберите тип установки. Если нет необходимости выбора компонентов для установки и настройки сетевых параметров серверов системы, то выбирайте тип **Полная установка системы с рекомендуемыми параметрами**, в противном случае – **Выбрать компоненты и параметры для установки системы**. Нажмите кнопку **Далее**.
4. Открывшееся диалоговое окно содержит лицензионное соглашение на использование системы. После его прочтения необходимо установить переключатель в положение **Я принимаю условия соглашения** и нажать кнопку **Далее** для продолжения установки. При установке переключателя в положение **Я не принимаю условия соглашения**, кнопка **Далее** будет неактивна (нельзя будет продолжить установку системы).
5. В открывшемся диалоговом окне необходимо выбрать папку, в которую будут установлены файлы системы:



Для установки рекомендуется использовать папку, установленную по умолчанию. По умолчанию это *C:\Program Files\PERCo\PERCo-Web*. Если необходимо, укажите другую папку или выберите ее, нажав кнопку **Обзор**. Для продолжения установки нажмите кнопку **Далее**.

6. Если был выбран тип установки **Выбрать компоненты и параметры для установки системы**, то откроется окно со списком для выбора компонентов для дальнейшей установки. В открывшемся окне отметьте флажками компоненты системы, которые необходимо установить на ПК, и нажмите кнопку **Далее**.

Откроется новое окно:

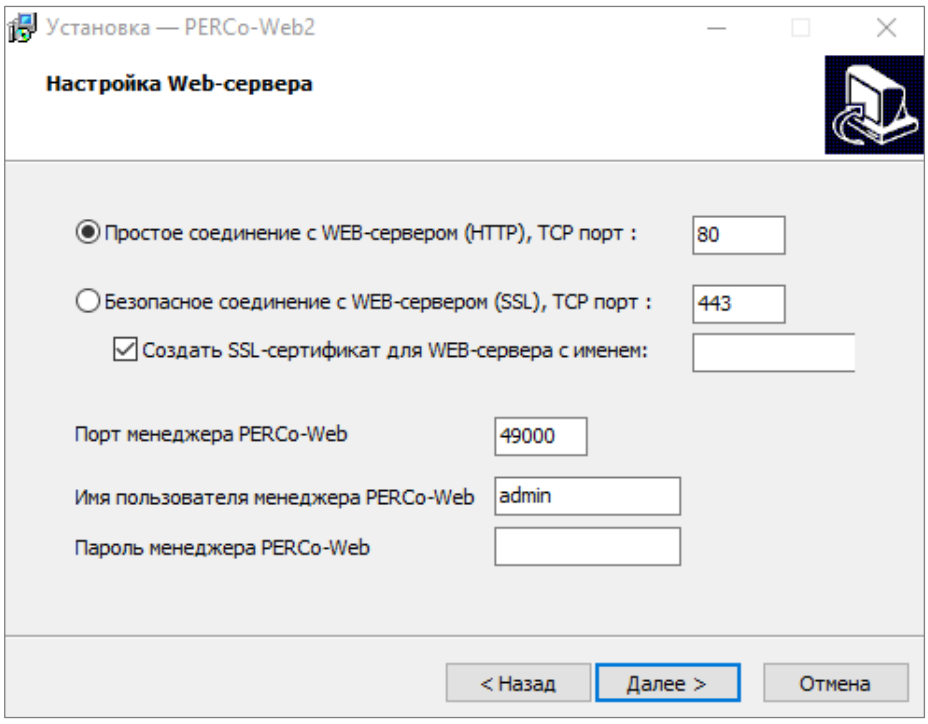


7. Для установки сервера базы данных MySQL установите флажок у параметра **Установить MySQL-сервер базы данных**. В поле **Каталог для базы данных** укажите папку расположения БД системы. По умолчанию это *C:\ProgramData\PERCo-Web\mysql*. Если необходимо, укажите другую папку или выберите ее, нажав кнопку **Обзор**. В поле **Название базы данных** укажите название базы данных. По умолчанию это *perco.* При необходимости измените значения в полях **Адрес сервера базы данных** и **порт**. В полях **Имя пользователя** и **Пароль** необходимо указать данные учетной записи пользователя.

Примечание:

Если сервер MySQL уже был установлен, то необходимо снять флажок у параметра **Установить MySQL-сервер** и указать учетные данные от необходимого сервера в соответствующих полях окна.

8. Для продолжения установки нажмите кнопку **Далее**. Откроется новое окно:



9. Произведите настройку сетевых параметров серверов системы. Для этого установите флажок **Простое соединение с WEB-сервером (HTTP), TCP** или **Безопасное соединение с WEB-сервером (SSL), TCP** и укажите свободный порт. Если указанный порт уже используется в системе, появится диалоговое окно. В окне нажмите кнопку **ОК** и выберите свободный порт.

Внимание!

Версия ***PERCo-Web*** (2.x.x.x) не может быть установлена поверх версии ***PERCo-Web*** (1.x.x.x). Поэтому при таком обновлении ПО при установке ***PERCo-Web*** версии 2.x.x.x необходимо будет задать порт, отличный от используемого ранее установленной версией (по умолчанию используется порт 80, измените на другой свободный), а затем мигрировать данные из первой версии ПО с помощью утилиты миграции.

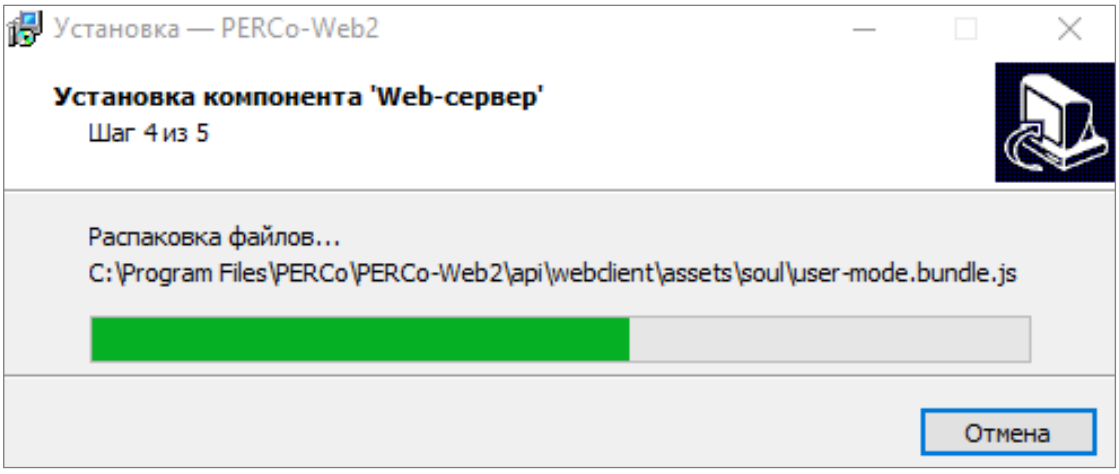
10. При необходимости установите флажок **Создать SSL-сертификат для WEB-сервера** и укажите имя для SSL-сертификата.

Внимание!

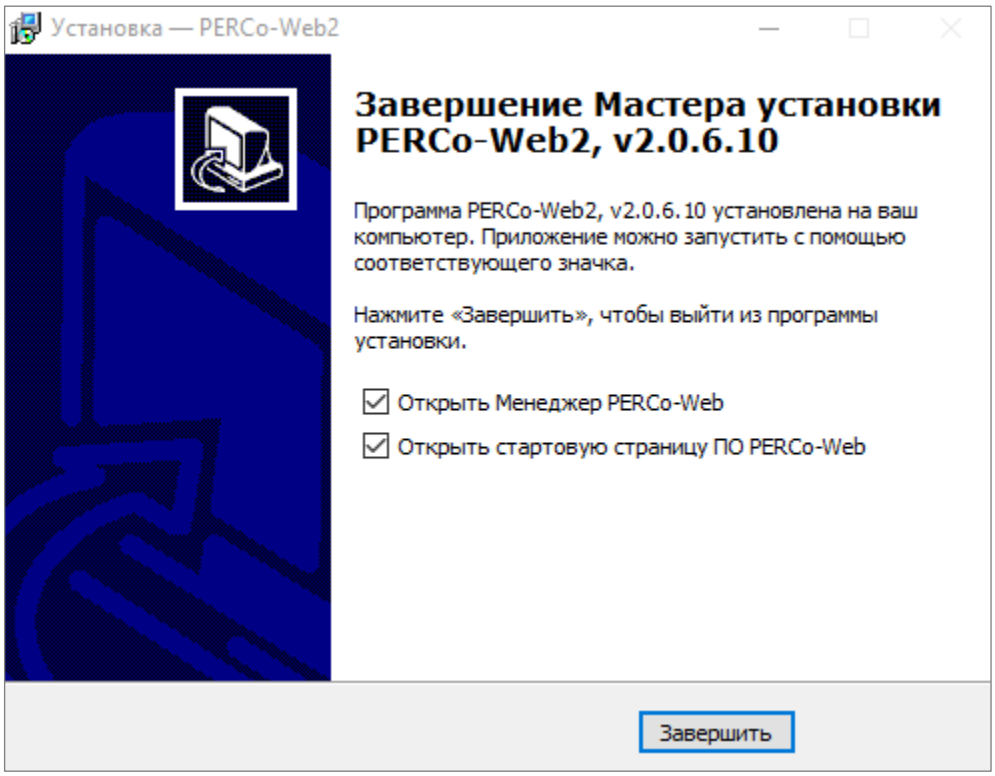
Для поддержки шифрования в целях повышения безопасности рекомендовано выбрать параметр **Безопасное соединение с WEB-сервером (SSL), TCP**.

11. В поле **Порт менеджера PERCo-Web** укажите свободный порт для работы с **Менеджером системы безопасности PERCo-Web**. По умолчанию это порт: 49000. В полях **Имя пользователя менеджера PERCo-Web** и **Пароль менеджера PERCo-Web** необходимо указать данные учетной записи пользователя. Для продолжения установки нажмите кнопку **Далее**.
12. В открывшемся окне укажите папку расположения файлов БД видеосервера системы. По умолчанию это *C:\ProgramData\PERCo-Web\video*. Если необходимо, укажите другую папку или выберите ее, нажав кнопку **Обзор**. Для продолжения установки нажмите кнопку **Далее**.
13. В открывшемся окне при необходимости установите флажок **Создать значки на Рабочем столе**. По окончании установки на рабочем столе автоматически отобразятся значки **PERCo-Web** и **Менеджер PERCo-Web**. Для продолжения установки нажмите кнопку **Далее**.
14. Будет проведена проверка конфигурации системы. Для продолжения установки нажмите кнопку **Далее**.
15. В открывшемся окне в виде списка отображены все выбранные параметры для установки системы. Для продолжения установки нажмите кнопку **Установить**.

    Начнется процесс установки и откроется новое диалоговое окно. В диалоговом окне установки отображается информация о результатах установки системы:



16. По завершению установки для автоматического запуска ***Менеджера PERCo-Web*** необходимо установить флажок **Открыть Менеджер PERCo-Web**; для автоматического запуска стартовой страницы ПО ***PERCo-Web*** необходимо установить флажок **Открыть стартовую страницу ПО PERCo-Web**:



17. Для закрытия окна мастера установки нажмите кнопку **Завершить**. Система ***PERCo-Web*** установлена на компьютер.
18. При необходимости приобретите лицензию на ПО системы.
19. Откройте **Менеджер PERCo-Web**, перейдите на вкладку **Опасная зона** и нажмите кнопку Скачать секретный ключ. На компьютер автоматически загрузится файл с генерированным секретным ключом для возможности восстановления доступа к зашифрованным данным системы ***PERCo-Web***. В случае полной переустановки системы необходимо будет зайти в **Менеджер PERCo-Web**, загрузить ранее сохраненный секретный ключ и перезагрузить все сервисы (Web-сервер и Сервер 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 > Параметры > Приложения**. В открывшемся окне выделите строку *«PERCo-Web2»* и нажмите кнопку **Удалить**.

10. 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*** (***PERCo-WSE***) ***«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-WM01*** (***PERCo-WME01***) ***Модуль «Учет рабочего времени»*** – позволяет вести учет рабочего времени сотрудников и составлять отчеты о дисциплине труда. Лицензируется только совместно с ***PERCo-WS*** (***PERCo-WSE***).
- ***PERCo-WM02*** (***PERCo-WME02***) ***Модуль «Верификация»*** – позволяет усилить контроль доступа на территорию предприятия за счет проведения оператором КПП процедуры верификации. Лицензируется только совместно с ***PERCo-WS*** (***PERCo-WSE***).
- ***PERCo-WM03 «Интеграция с 1С»*** – позволяет синхронизировать базы данных ***PERCo-Web*** и ***1С: Предприятие***. Модуль интеграции представляет собой приложение в виде файла внешней обработки для программного продукта ***«1С: Предприятие 8»***. Лицензируется только совместно с ***PERCo-WS*** (***PERCo-WSE***) и ***PERCo-WM01 (PERCo-WME01***).
- ***PERCo-WM04 «Интеграция с внешними системами»*** – позволяет включить отображение документации по адресу: /dev для возможности работы с API. Лицензируется только совместно с ***PERCo-WS***.
- ***PERCo-WM05*** (***PERCo-WME05***) ***Модуль «Мониторинг»*** – позволяет организовать наблюдение за подконтрольным системе предприятием, управлять устройствами системы в ручном режиме, а также создавать и редактировать план предприятия. Лицензируется только совместно с ***PERCo-WS*** (***PERCo-WSE***).
- ***PERCo-WM06 «Интеграция с TRASSIR»*** – позволяет провести интеграцию системы ***PERCo-Web*** с видеоподсистемой ***Trassir***, что расширяет функциональные возможности ***PERCo-Web*** за счет использования ресурсов видеоподсистемы ***Trassir***. Лицензируется только совместно с ***PERCo-WS***.

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 для дальнейшей работы с ПО необходимо получить и ввести код активации на бесплатный модуль ***PERCo-WB*** (***PERCo-WBE***) ***«Базовый пакет ПО»*** со следующими ограничениями:

- количество карт доступа (идентификаторов) в системе будет ограничено первыми выданными 100 картами (идентификаторами);
- возможность ввода данных и выдачи карт доступа (идентификаторов) посетителям будет недоступна;
- работа с дополнительными модулями ПО ***PERCo-WM*** будет недоступна;
- интеграция с контроллерами сторонних производителей (биометрические контроллеры и терминалы распознавания лиц ***ZKTeco***, ***Suprema***) будет недоступна.

При этом вся введенная ранее информация о картах доступа (идентификаторах) 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 производства ***PERCo***. 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, 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 ***PERCo-WBE*** ***«Базовый пакет ПО»***	Количество карт ограничено – ***до 100 шт***. Разделы: **«Персонал»** с подразделами: • **«Сотрудники»**, • **«Подразделения»**, • **«Должности»**; **«Бюро пропусков»** с подразделами: • **«Сотрудники»**, • **«Шаблоны доступа»**; **«Контроль доступа»** с подразделом: • **«Управление устройствами»**; **«Администрирование»** с подразделами: • **«Конфигурация»**, • **«События системы»**, • **«Задания»**, • **«Операторы»**, • **«Роли и права операторов»**, • **«Лицензии»**
PERCo-WS ***PERCo-WSE*** ***«Стандартный пакет ПО»***	Все разделы, входящие в ***«Базовый пакет ПО»***, а также добавляется: раздел **«Заказ пропуска»**, в раздел **«Персонал»** добавляется подраздел: • **«Дополнительные данные»**; в раздел **«Бюро пропусков»** добавляются подразделы: • **«Посетители»**, • **«Дизайн пропуска»**, • **«Отчет по посетителям»**; в раздел **«Контроль доступа»** добавляются подразделы: • **«Отчет о проходах»**, • **«Отчет по доступу в помещения»**
PERCo-WM01 ***PERCo-WME01*** ***«Учет рабочего времени»***	Все разделы, входящие в ***«Стандартный пакет ПО»***, а также добавляется: раздел **«Учет рабочего времени»**, с подразделами: • **«Журнал отработанного времени»**, • **«Оправдательные документы»**, • **«Формирование табеля»**, • **«Отчеты по дисциплине»**; в раздел **«Персонал»** добавляется подраздел: • **«Графики работы»**; в раздел **«Контроль доступа»** добавляется подраздел: • **«Местонахождение»**
PERCo-WM02 ***PERCo-WME02*** ***«Верификация»***	Все разделы, входящие в ***«Стандартный пакет ПО»***, а также добавляется: Раздел **«Верификация»** с подразделами:

Модуль ПО	Входящие в модуль разделы
	• **«Верификация»**, • **«Конфигурация верификации»**; в раздел **«Контроль доступа»** добавляется подраздел: • **«Журнал верификации»**
PERCo-WM03 «Интеграция с 1С»	Модуль синхронизирует базы данных ***PERCo-Web*** и ***1С: Предприятие***
PERCo-WM04 «Интеграция с внешними системами»	Модуль включает отображение документации по адресу: /dev для возможности работы с API
PERCo-WM05 PERCo-WME05 «Мониторинг»	Все разделы, входящие в ***«Стандартный пакет ПО»***, а также добавляется: Раздел **«Мониторинг»** с подразделами: • **«Режим интерактивного плана»**; • **«Режим редактирования»**
PERCo-WM06 «Интеграция с TRASSIR»	Модуль позволяет провести интеграцию системы ***PERCo-Web*** с видеоподсистемой ***Trassir***, что дает возможность использовать оборудование ***TRASSIR*** для видеонаблюдения и для распознавания пользователей по лицу

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 **Поддержка > Программное обеспечение > ПО *PERCo-Web* > Порядок получения лицензионного соглашения ПО *PERCo-Web*** или **Каталог> Система контроля доступа *PERCo-Web* > Программное обеспечение > ПО *PERCo-Web* > Порядок получения лицензионного соглашения ПО *PERCo-Web***.

   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»**.

Внимание!

Использование в системе ***PERCo-Web*** контроллеров только сторонних производителей (биометрические контроллеры и терминалы распознавания лиц ***ZKTeco***, ***Suprema***) возможно только в течение ознакомительного периода. По его окончании необходимо будет приобрести хотя бы один контроллер ***PERCo*** в качестве электронного ключа и лицензию на стандартный пакет ПО.

11. Менеджер системы безопасности PERCo-Web

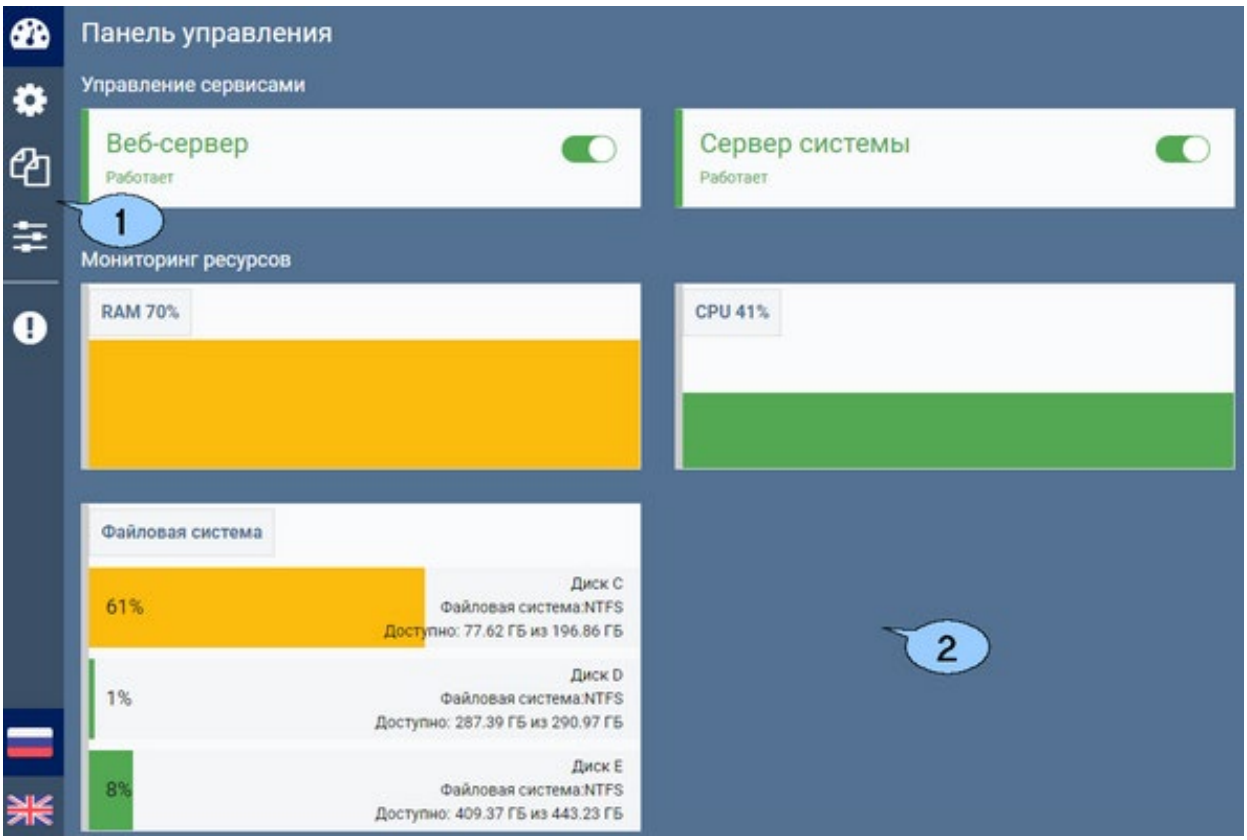
Окно **Менеджер PERCo-Web** открывается нажатием на иконку **Менеджер PERCo-Web** на рабочем столе или по IP-адресу в адресной строке браузера (например, http://127.x.x.x:49000/, где 127.x.x.x – IP-адрес компьютера с установленным сервером системы, :49000 – порт **Менеджера PERCo-Web**, указанный при установке системы ***PERCo-Web***).

На экране появится окно для авторизации входа пользователя. В окне в соответствующих полях введите имя пользователя и пароль (по умолчанию это *admin* / *admin*), после чего будет выполнен вход в **Менеджер**.

Менеджер PERCo-Web предназначен для:

- запуска и остановки серверов системы;
- импорта БД из файла более ранних версий БД системы;
- создания и восстановления резервной копии БД;
- просмотра логов **Менеджера PERCo-Web**;
- сброса учетной записи администратора.

Окно **Менеджер PERCo-Web** выглядит следующим образом:



1. Панель содержит следующие вкладки:
   - **Мониторинг**;
   - **Настройки**;
   - **Резервные копии и логи**;
   - **Настройки менеджера**;
   - **Опасная зона**.

   Иконки в левом нижнем углу позволяют сменить язык интерфейса.
2. Рабочая область окна зависит от выбранной вкладки.

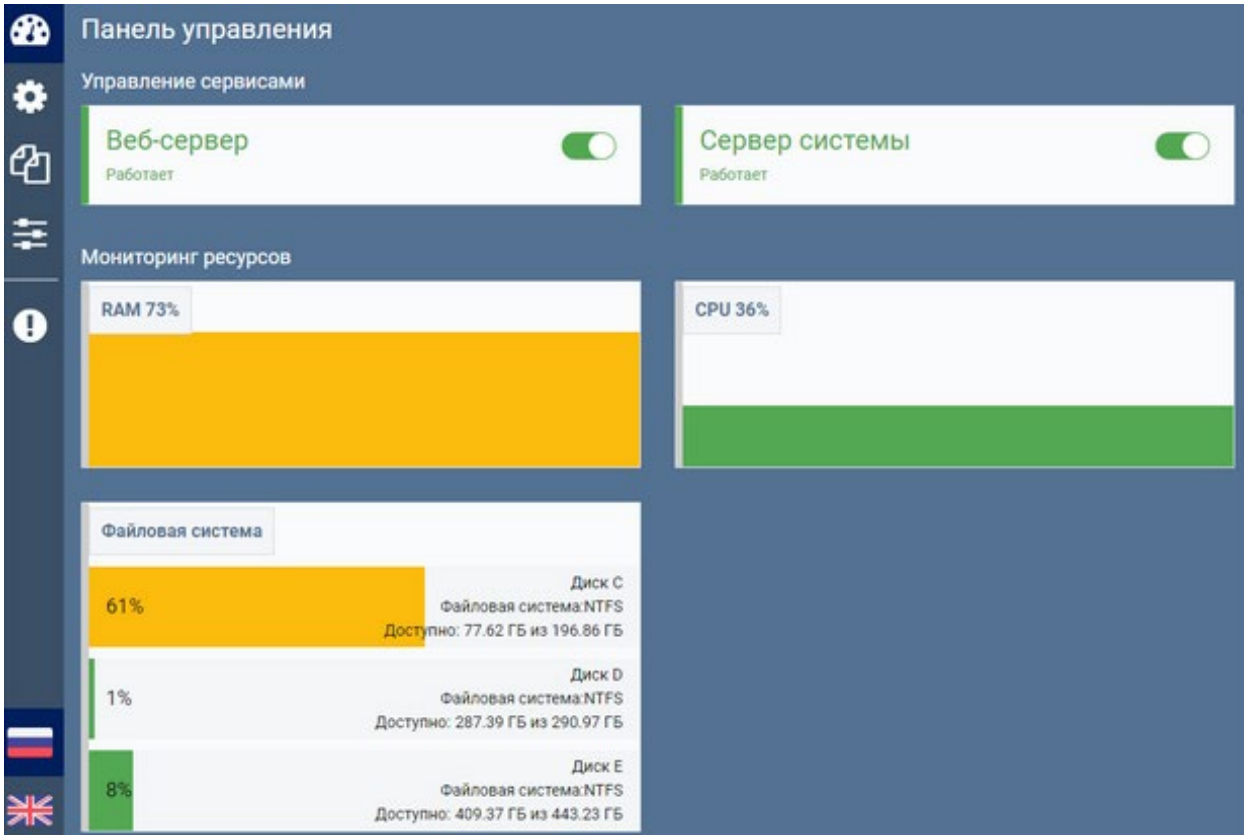
Примечание:

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

11.1. Вкладка «Мониторинг»

Вкладка **Мониторинг** (не путать с разделом **«Мониторинг»** системы ***PERCo-Web***, он описывается в ***Руководстве пользователя модуля PERCo-WM05, WME05 «Мониторинг»***) предназначена для запуска и остановки серверов системы.

Вид вкладки:



Рабочая область вкладки содержит следующие элементы:

- **Управление сервисами** – панель содержит информацию о состоянии серверов и переключатель для их запуска или остановки. Для изменения состояния сервера используйте переключатель .
- **Мониторинг ресурсов** – панель визуально отображает состояние сервера на текущий момент времени.

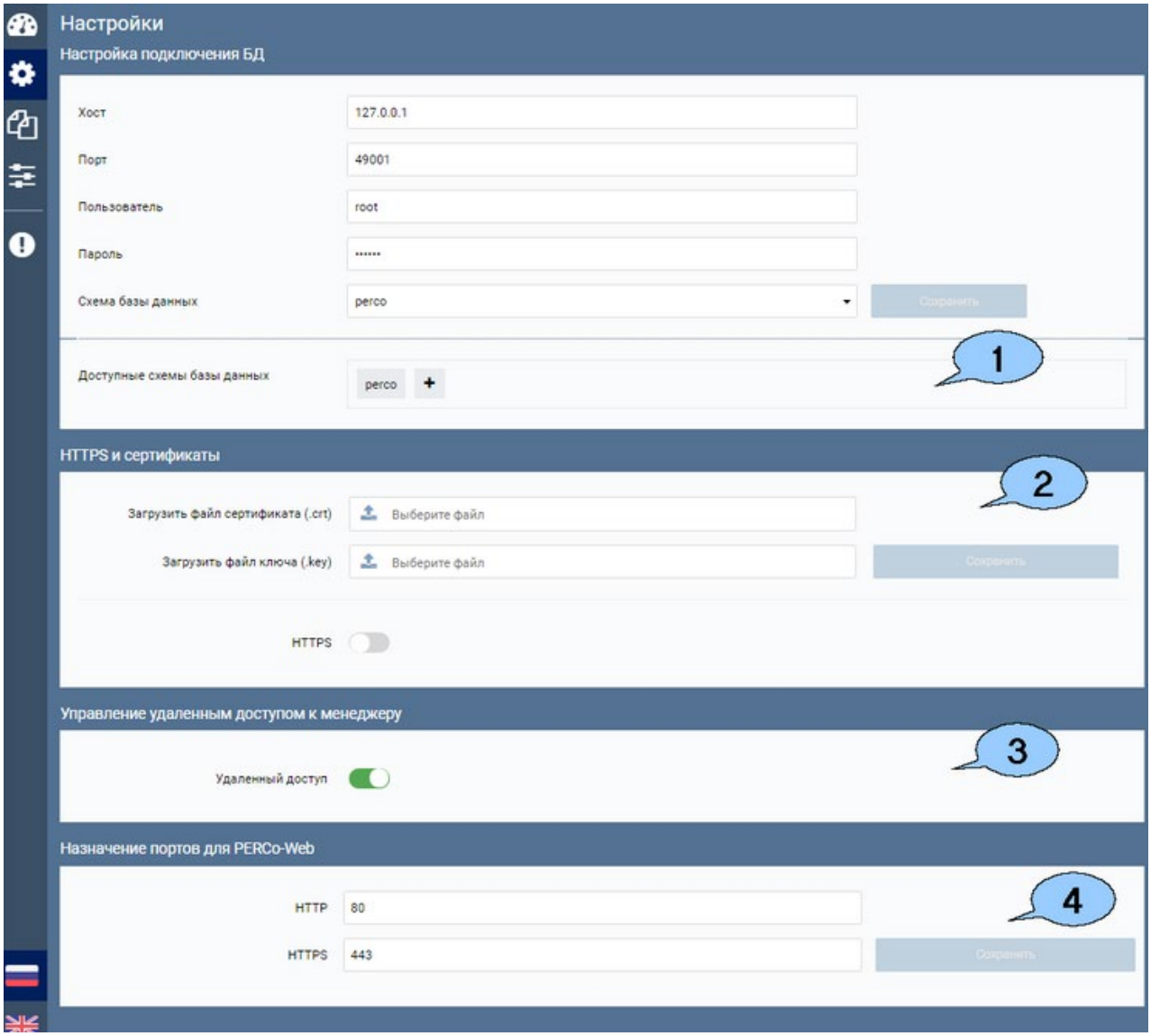
Примечание:

Состояние сервера отражает состояние памяти сервера и загрузки процессора всеми текущими процессами, то есть не только процессами ***PERCo-Web***.

11.2. Вкладка «Настройки»

Вкладка **Настройки** предназначена для управления БД системы, удаленным доступом, HTTPS и сертификатами.

Вид вкладки:



1. Панель **Настройка подключения БД** содержит следующие элементы:
   - **Хост** – в поле необходимо указать адрес сервера для созданной базы данных.
   - **Порт** – в поле необходимо указать порт для созданной базы данных.
   - **Пользователь** – в поле необходимо ввести имя пользователя для подключения к базе данных.
   - **Пароль** – в поле необходимо ввести пароль для указанного пользователя для подключения к базе данных.
   - **Схема базы данных** – в поле необходимо ввести название созданной базы данных. При вводе имени несозданной базы данных она будет создана автоматически.
   - **Сохранить** – кнопка позволяет сохранить внесенные на панели изменения.
   - **Доступные схемы базы данных** – панель позволяет добавить БД.
2. Панель **HTTPS и сертификаты** содержит следующие элементы:
   - **Загрузить файл сертификата (.crt)** – панель позволяет загрузить публичный ключ. После загрузки файл будет храниться на сервере **Менеджера PERCo-Web**.
   - **Загрузить файл ключа (.key)** – панель позволяет загрузить секретный ключ сервера. После загрузки файл будет храниться на сервере **Менеджера PERCo-Web**.

- **HTTPS** – переключатель позволяет включить / выключить шифрование данных. Чтобы включить SSL-шифрование, необходимо загрузить файл сертификата и файл ключа. При загрузке некорректных файлов ключа или сертификата при запуске **Менеджера PERCo-Web** отобразится ошибка:

  Не удалось корректно прочитать SSl-сертификат, менеджер работает по протоколу http.

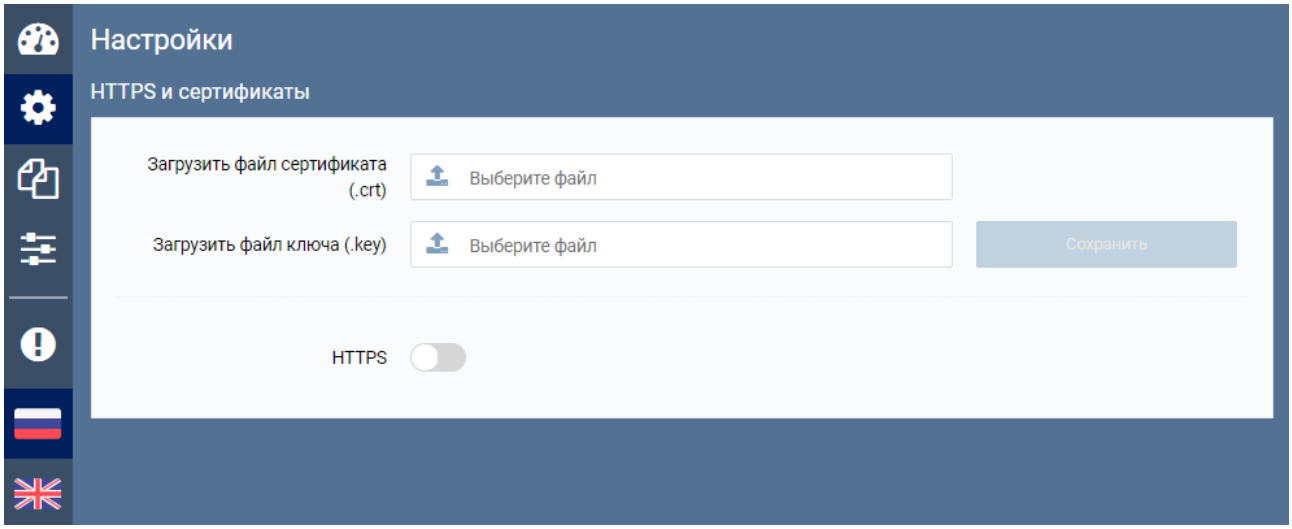
- Кнопка **Сохранить** сохраняет внесенные изменения.

3. Панель **Управление удаленным доступом к менеджеру** позволяет включить / выключить разрешение на подключение к **Менеджеру PERCo-Web** по удаленному доступу.
4. Панель **Назначение портов для PERCo-Web** позволяет указать, какой порт будет использоваться для обычного соединения (HTTP), а какой – для зашифрованного (HTTPS).

11.2.1. Вкладка «Настройки» Менеджера PERCo-Web, встраиваемой в память контроллеров PERCo

Вкладка **Настройки** Менеджера ***PERCo-Web***, встраиваемой в память контроллеров ***PERCo***, отличается от стандартной и предназначена для управления HTTPS и сертификатами.

Вид вкладки:



Панель **HTTPS и сертификаты** содержит следующие элементы:

- **Загрузить файл сертификата (.crt)** – панель позволяет загрузить публичный ключ. После загрузки файл будет храниться на сервере ***Менеджера PERCo-Web***.
- **Загрузить файл ключа (.key)** – панель позволяет загрузить секретный ключ сервера. После загрузки файл будет храниться на сервере ***Менеджера PERCo-Web***.
- **HTTPS** – переключатель позволяет включить/выключить шифрование данных. Чтобы включить SSL-шифрование, необходимо загрузить файл сертификата и файл ключа. При загрузке некорректных файлов ключа или сертификата при запуске ***Менеджера PERCo-Web*** отобразится ошибка:

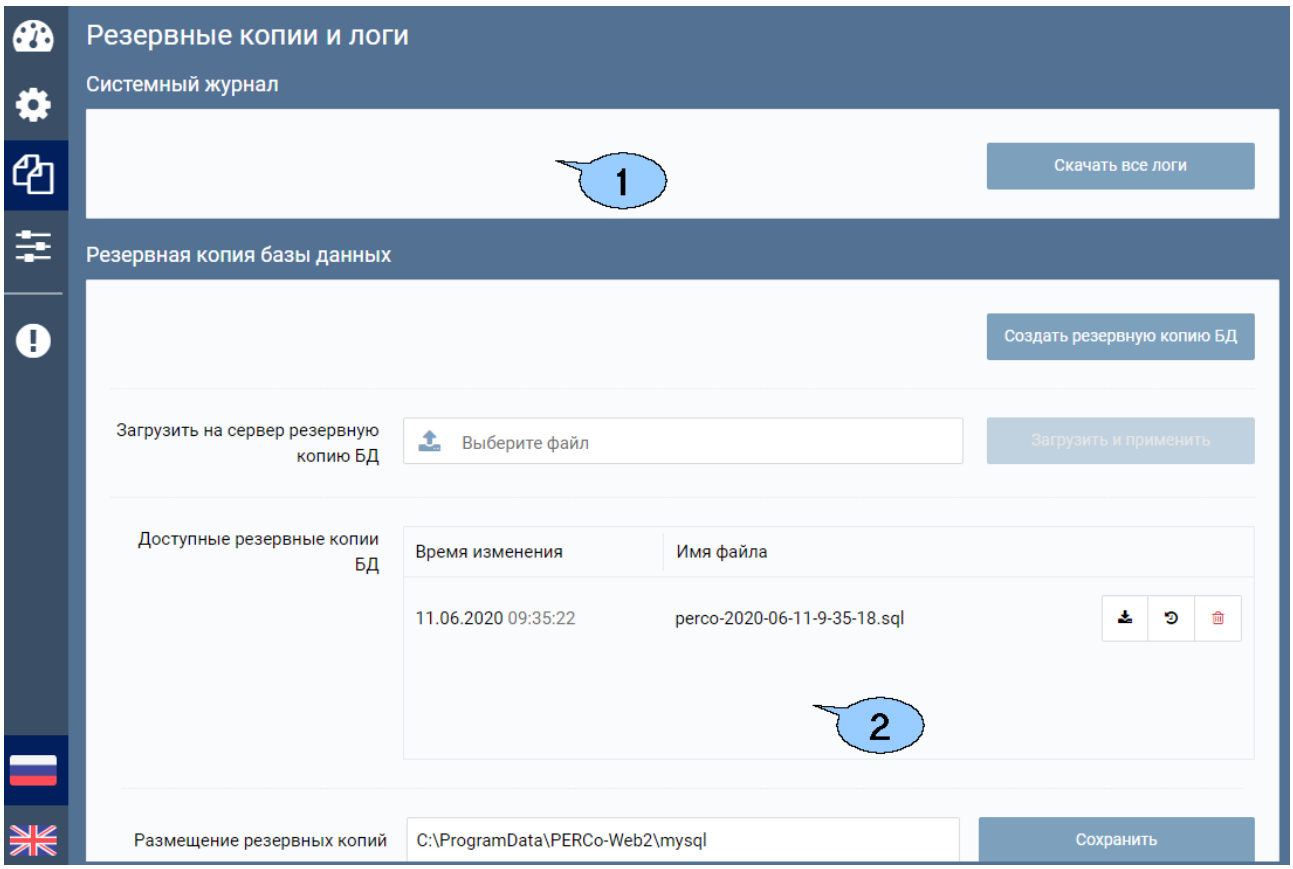
  Не удалось корректно прочитать SSl-сертификат, менеджер работает по протоколу http.

- Кнопка **Сохранить** сохраняет внесенные изменения.

11.3. Вкладка «Резервные копии и логи»

Вкладка **Резервные копии и логи** предназначена для просмотра логов системы и для управления резервными копиями БД.

Вид вкладки:

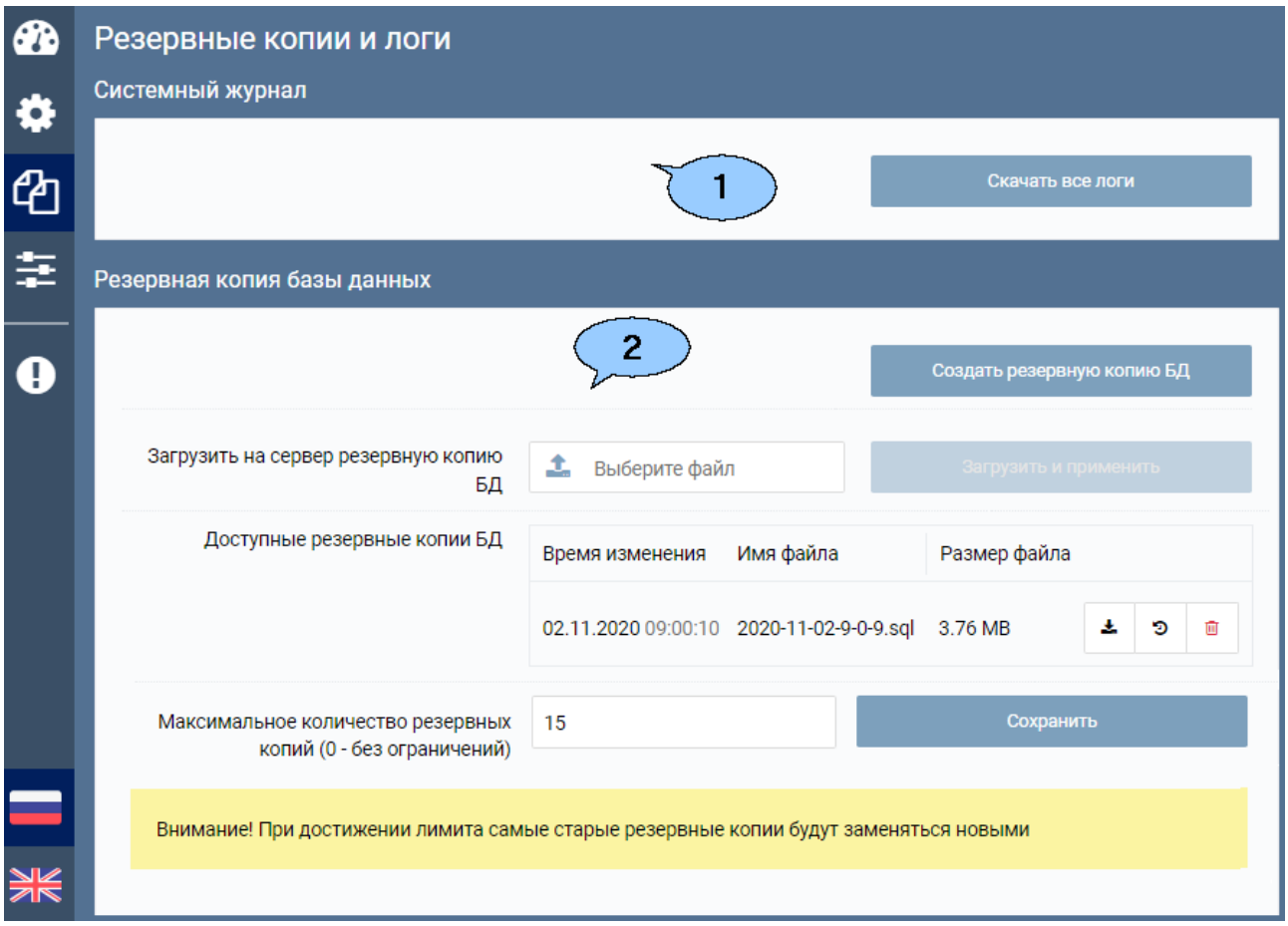


Рабочая область вкладки содержит следующие элементы:

1. **Системный журнал** – панель содержит кнопку **Скачать все логи**, которая позволяет скачать архив с текстовыми файлами, содержащими системную информацию о действиях, произошедших на сервере.
2. Панель **Резервная копия базы данных** содержит следующие элементы:
   - Кнопка **Создать резервную копию БД** позволяет создать резервную копию БД.
   - Поле **Загрузить на сервер резервную копию БД** позволяет выбрать файл с компьютера.
   - Панель **Доступные резервные копии БД** содержит список сохраненных резервных копий.
   - Поле **Размещение резервных копий** позволяет указать путь для размещения резервных копий.
   - **Скачать резервную копию** – кнопка позволяет скачать выбранную резервную копию.
   - **Восстановить резервную копию** – кнопка позволяет восстановить БД из созданной ранее резервной копии.
   - **Удалить резервную копию** – кнопка позволяет удалить из списка выбранную резервную копию.

11.3.1. Вкладка «Резервные копии и логи» Менеджера PERCo-Web, встраиваемой в память контроллеров PERCo

Вкладка **Резервные копии и логи** Менеджера ***PERCo-Web***, встраиваемой в память контроллеров ***PERCo***, отличается от стандартной и имеет следующий вид:



Рабочая область вкладки содержит следующие элементы:

1. **Системный журнал** – панель содержит кнопку **Скачать все логи**, которая позволяет скачать архив с текстовыми файлами, содержащими системную информацию о действиях, произошедших на сервере.
2. Панель **Резервная копия базы данных** содержит следующие элементы:
   - Кнопка **Создать резервную копию БД** позволяет создать резервную копию БД.
   - Поле **Загрузить на сервер резервную копию БД** позволяет выбрать файл с компьютера.
   - Панель **Доступные резервные копии БД** содержит список сохраненных резервных копий.
   - **Скачать резервную копию** – кнопка позволяет скачать выбранную резервную копию.
   - **Восстановить резервную копию** – кнопка позволяет восстановить БД из созданной ранее резервной копии.
   - **Удалить резервную копию** – кнопка позволяет удалить из списка выбранную резервную копию.
   - **Максимальное количество резервных копий (0 – без ограничений)** – поле позволяет ввести значение максимального количества хранимых резервных копий.

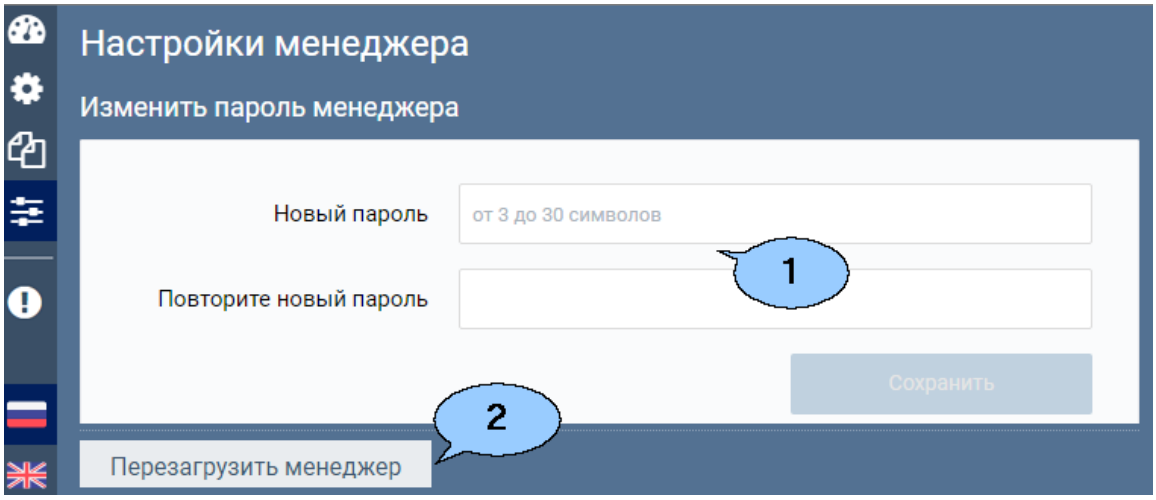
Внимание!

При достижении лимита самые старые резервные копии будут заменяться новыми.

11.4. Вкладка «Настройки менеджера»

Вкладка **Настройки менеджера** предназначена для изменения пароля.

Вид вкладки:

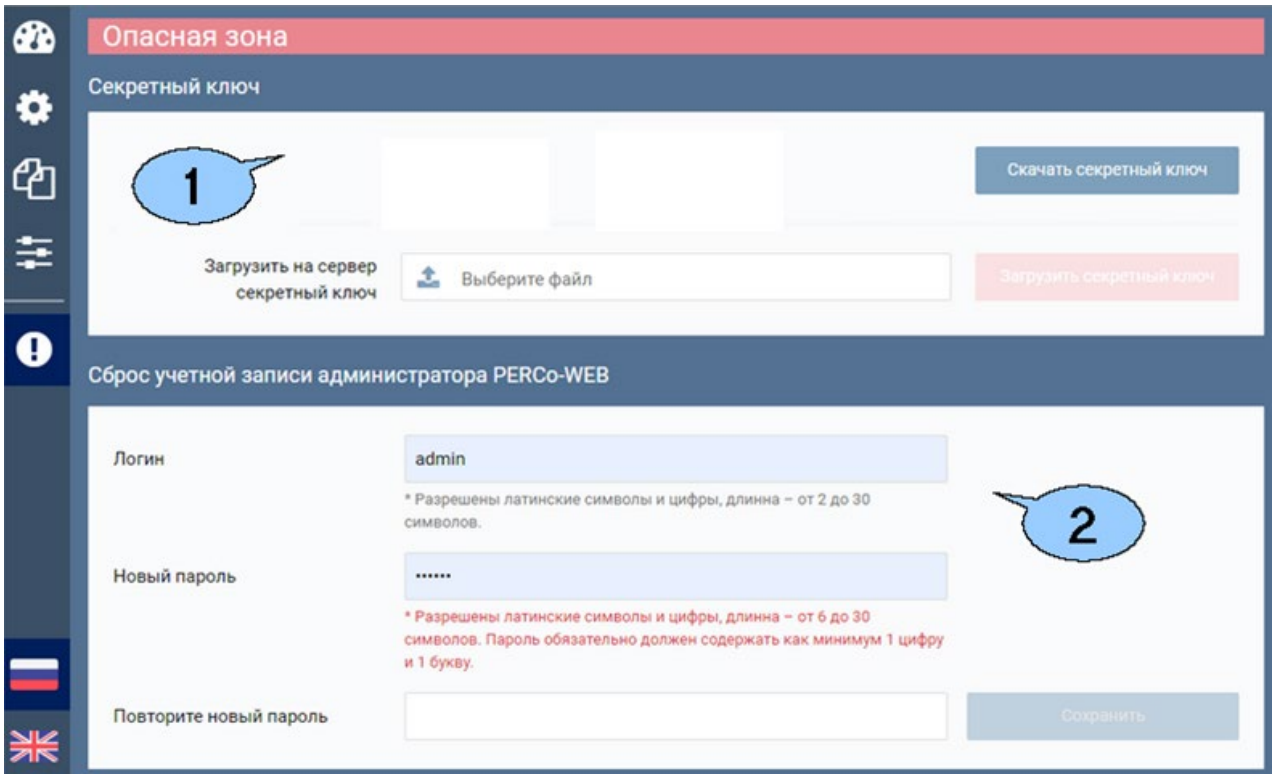


1. Панель **Изменить пароль менеджера** позволяет указать новый пароль для **Менеджера системы PERCo-Web**.
2. Кнопка Перезагрузить менеджер позволяет перезапустить **Менеджер системы PERCo-Web**.

11.5. Вкладка «Опасная зона»

Вкладка **Опасная зона** предназначена для восстановления доступа к зашифрованным данным системы ***PERCo-Web*** и сброса учетной записи администратора.

Вид вкладки:



Рабочая область вкладки содержит следующие элементы:

1. Панель **Секретный ключ**. Это ключ шифрования приватных данных, он генерируется при первом запуске системы ***PERCo-Web*** и больше никогда не меняется. При утере ключа все пароли и зашифрованные данные становятся недоступными. После установки

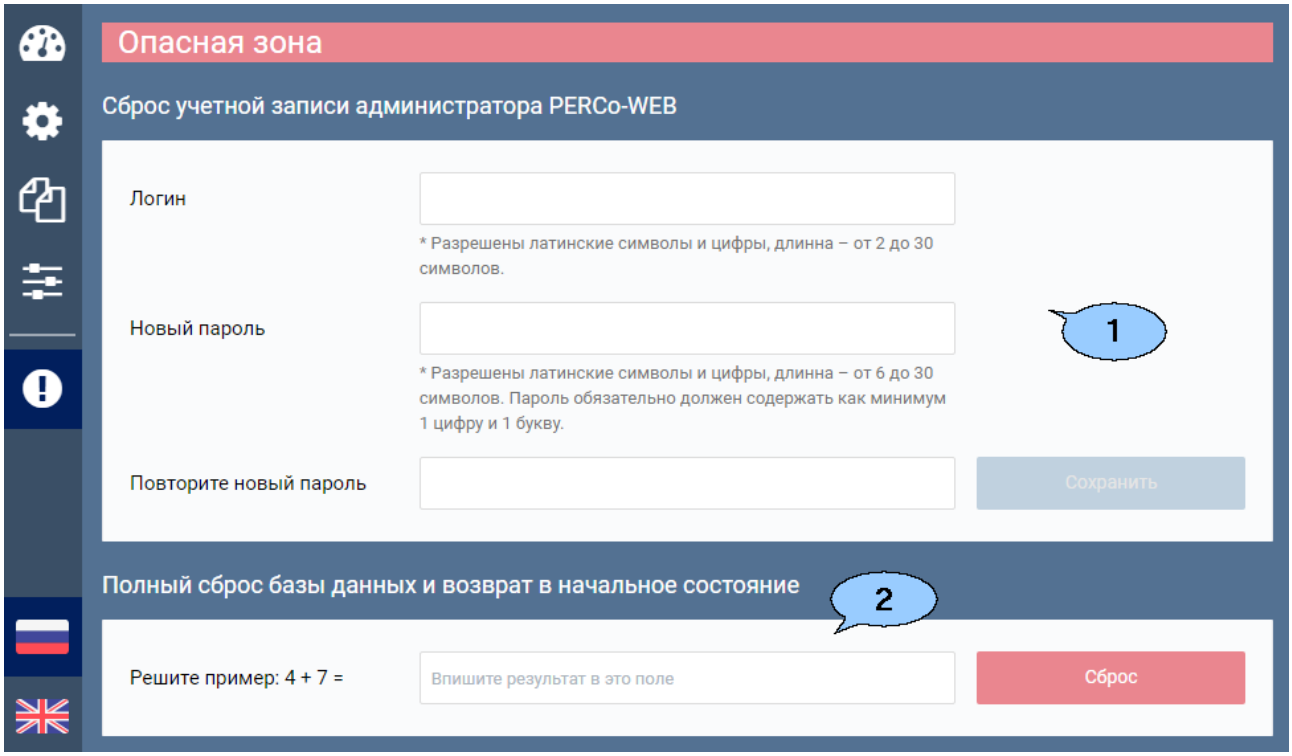
системы ***PERCo-Web*** ключ необходимо скачать и сохранить в недоступном месте.

- Кнопка **Скачать секретный ключ** позволяет скачать файл с секретным ключом для восстановления доступа к зашифрованным данным системы ***PERCo-Web***.
- Кнопка **Загрузить секретный ключ** позволяет загрузить файл с ранее сгенерированным секретным ключом.

2. Панель **Сброс учетной записи администратора PERCo-Web** позволяет указать новый логин и пароль для учетной записи администратора ***Менеджера системы PERCo-Web***, кнопка **Сохранить** позволяет сохранить внесенные изменения.

11.5.1. Вкладка «Опасная зона» Менеджера PERCo-Web, встраиваемой в память контроллеров PERCo

Вкладка **Опасная зона** Менеджера ***PERCo-Web***, встраиваемой в память контроллеров ***PERCo***, отличается от стандартной и выглядит следующим образом:



Рабочая область вкладки содержит следующие элементы:

1. Панель **Сброс учетной записи администратора PERCo-Web** – позволяет указать новый логин и пароль для учетной записи администратора ***Менеджера системы PERCo-Web***, кнопка **Сохранить** позволяет сохранить внесенные изменения.
2. Панель **Полный сброс базы данных и возврат в начальное состояние** – позволяет сбросить базу данных до начального состояния. Для этого решите пример и нажмите кнопку **Сброс**. Новые примеры генерируются при каждом входе в ***Менеджер системы PERCo-Web***.

12. Интеграция с 1С: Предприятие 8

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

- список структурных подразделений предприятия;
- список организаций;
- должности сотрудников;
- графики работы и праздничные дни;
- события;
- список сотрудников и их учетные данные;
- классификаторы.

После активации лицензии на модуль ***PERCo-WM03 «Интеграция с 1С»***, редактирование этих данных в системе ***PERCo-Web*** будет заблокировано.

Провести интеграцию с ***1С: Предприятие*** можно с помощью модуля ***PERCo-WM03 «Модуль интеграции с 1С»***, разработанного компанией **PERCo**.

Для проведения интеграции:

1. Установите модуль ***PERCo-WM03 «Модуль интеграции с 1С»***.
2. Запустите ***1С: Предприятие*** и откройте файл внешней обработки ***Perco_СинхронизацияДанныхЗУП_1С_xx.epf*** (где xx – версия файла обработки) модуля ***PERCo-WM03 «Модуль интеграции с 1С»***. Файл можно скачать в разделе **«Администрирование» > «Лицензии» > *PERCo-WM03***. Следуйте рекомендациям руководства пользователя модуля.

Примечание:

Дополнительная информация о работе системы с модулем ***PERCo-WM03 «Модуль интеграции с 1С»*** доступна на сайте компании ***PERCo*** по адресу: www.perco.ru, в разделе **Поддержка> Документация**.

13. Интеграция с видеоподсистемой Trassir

Система ***PERCo-Web*** поддерживает интеграцию с видеоподсистемой ***Trassir***. Камеры данной видеоподсистемы можно использовать как для видеонаблюдения, так и для распознавания сотрудников / посетителей по лицу.

Провести интеграцию с видеоподсистемой ***Trassir*** можно с помощью модуля ***PERCo-WM06 «Интеграция с TRASSIR»***, разработанного компанией **PERCo** (лицензируется только совместно с ***PERCo-WS***). Порядок приобретения лицензии на модуль указан в разделе ***«Управление лицензиями»***.

Внимание!

Для работы модуля интеграции необходимо иметь лицензию на ***TRASSIR-Server*** или приобрести ее, выбрав при первичном запуске один из вариантов активации. В ознакомительных целях доступна demo-версия ПО.

Инструкция по активации лицензии и другая эксплуатационная документация на ПО ***TRASSIR*** доступна в электронном виде на сайте компании ООО ***«ДССЛ-Первый»***, по адресу: *www.dssl.ru*, в разделе **Техподдержка > Техническая документация**.

13.1. Функциональные возможности

Интеграция системы ***PERCo-Web*** с видеоподсистемой ***Trassir*** предоставляет следующие возможности:

1. Вывод «живого видео» с камер видеоподсистемы ***Trassir*** и управление камерами в режиме «online».
2. Использование системы автоматического распознавания лиц ***TRASSIR Face Recognition***. В этом случае в качестве идентификаторов доступа в системе ***PERCo-Web*** используются шаблоны лиц сотрудников / посетителей, загруженные в базу данных системы ***PERCo-Web*** и в базу лиц **Trassir**.

Примечание:

Для использования видеокамер ***TRASSIR*** в качестве камер для идентификации по лицу требуется иметь лицензию на модуль распознавания и поиска лиц по базе ***«TRASSIR Face Recognition»*** или приобрести ее на сайте производителя по адресу: *www.dssl.ru*.

3. Использование камер видеоподсистемы ***Trassir*** при организации точек верификации доступа (см. *Руководство пользователя* ***PERCo-WM02***).

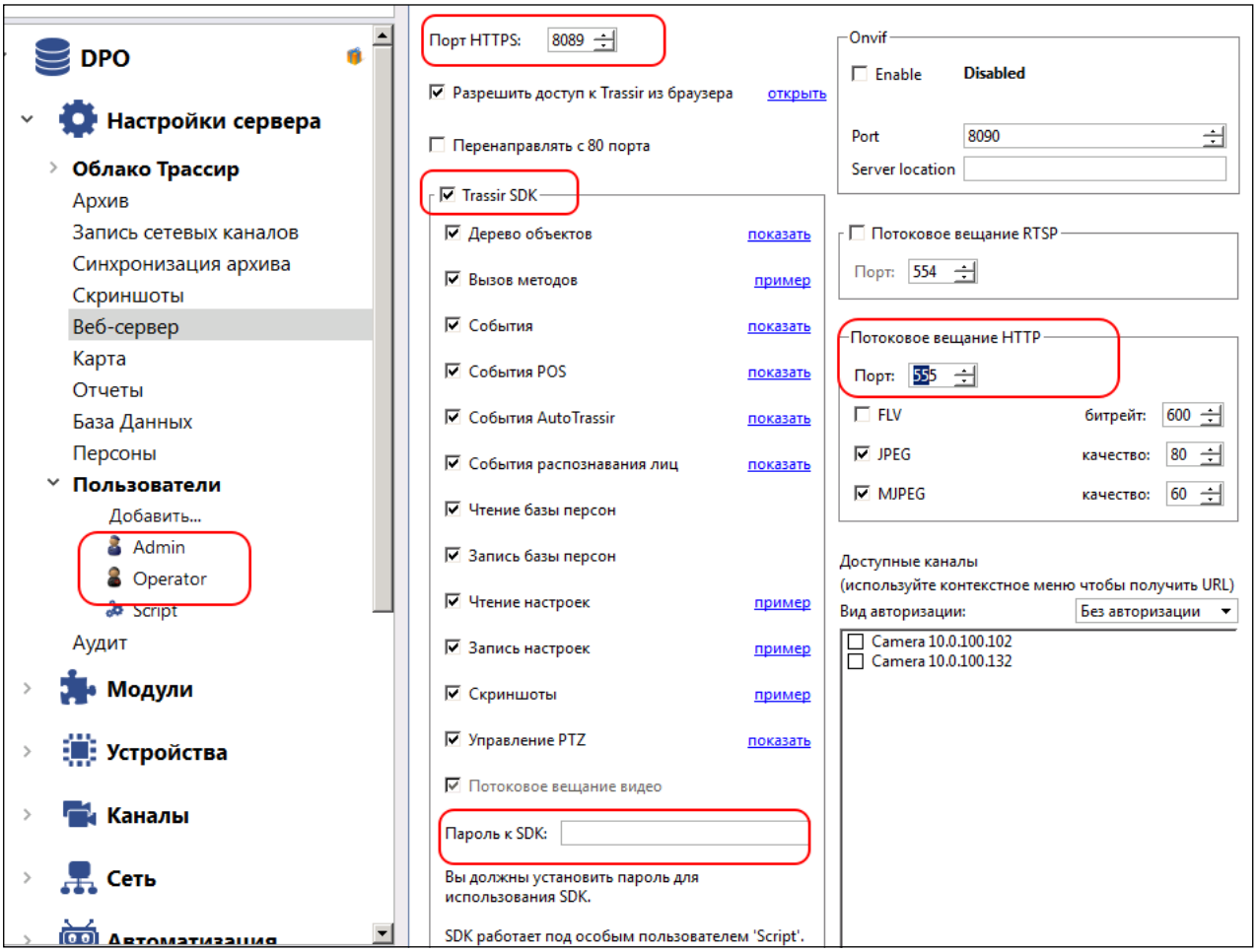
13.2. Порядок интеграции с видеоподсистемой Trassir

13.2.1. Настройка сервера TRASSIR

Для проведения интеграции системы ***PERCo-Web*** с видеоподсистемой ***Trassir***:

1. Установите модуль ***PERCo-WM06 «Интеграция с TRASSIR»***.
2. Скачайте последнюю актуальную версию ПО **TRASSIR-Server**, доступную по ссылке: *https://www.dssl.ru/support/tech/soft/trassir_index.php*.
3. Установите (обновите) ПО и произведите его дальнейшую настройку, следуя инструкции, доступной на сайте *www.dssl.ru* в разделе **Техподдержка > Техническая документация > ПО TRASSIR**.
4. В разделе ***«Пользователи»*** сервера ***TRASSIR*** создайте пользователей и выдайте им права на требуемые виды операций.
5. В подразделе ***«Веб-сервер»*** сервера ***TRASSIR*** обратите внимание на параметры, которые потребуются для настройки сервера ***TRASSIR*** в системе ***PERCo-Web***:
   - **Порт HTTPS** – порт задан по умолчанию.
   - **Trassir SDK** – поставьте флажок на параметр **Trassir SDK**. Подробная информация по настройке SDK доступна в руководстве пользователя ПО ***TRASSIR***, в разделе ***«TRASSIR SDK»***.
   - **Пароль к SDK** – задайте пароль к SDK.

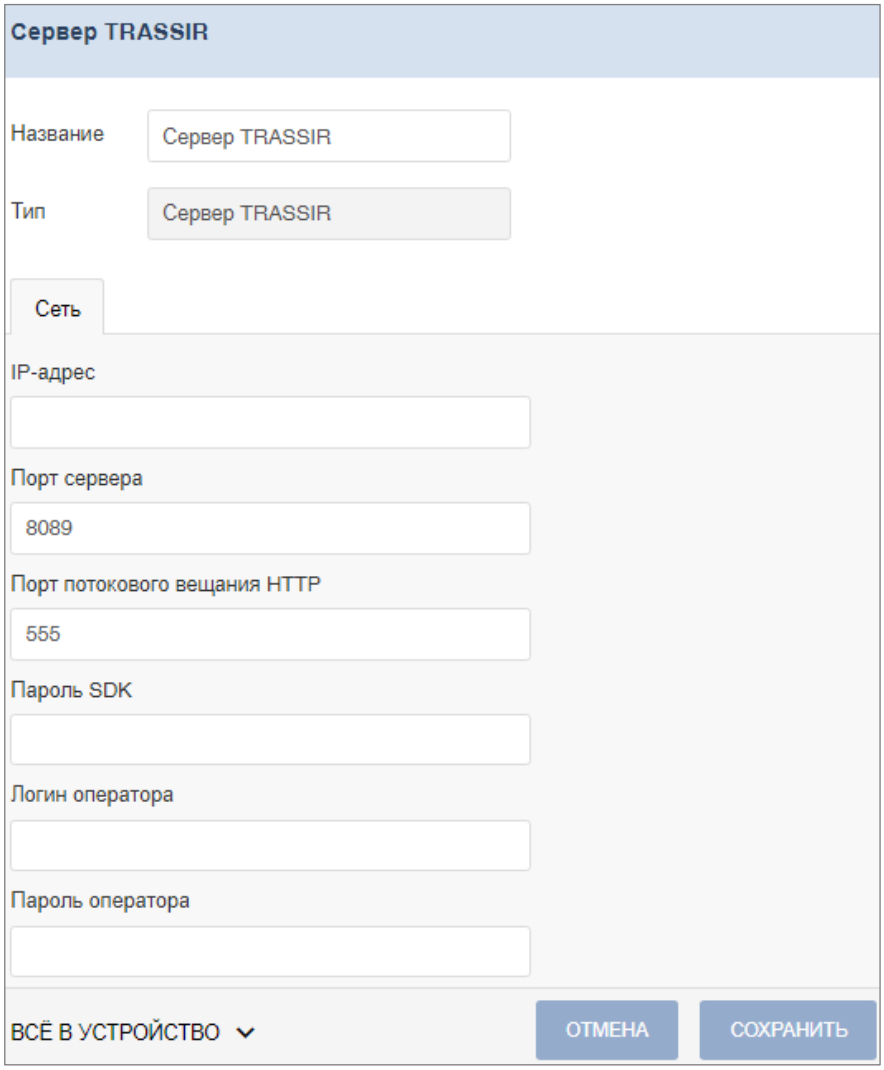
- **Потоковое вещание HTTP** – порт задан по умолчанию.



13.2.2. Конфигурация сервера TRASSIR в системе PERCo-Web

Для добавления сервера ***TRASSIR*** в конфигурацию системы ***PERCo-Web***:

1. Используя панель навигации, перейдите в раздел  ***«Администрирование»***.
2. Откройте подраздел ***«Конфигурация»***.
3. Перейдите на вкладку **Устройства**.
4. Нажмите на панели инструментов страницы кнопку  **Добавить**. Из выпадающего списка выберите **Добавить сервер TRASSIR**. Откроется следующее окно:



5. В открывшемся окне при необходимости в поле **Название** измените название сервера.
6. Поле **Тип** неизменно.
7. На вкладке **Сеть** заполните значения следующих параметров:
   - В поле **IP-адрес** введите IP-адрес компьютера, на котором установлен сервер ***TRASSIR***.
   - Поле **Порт сервера** заполняется автоматически при наличии настроенного сервера ***TRASSIR***.
   - Поле **Порт потокового вещания HTTP** заполняется автоматически при наличии настроенного сервера ***TRASSIR***.
   - В поле **Пароль SDK** введите пароль к SDK, заданный при настройке сервера ***TRASSIR***.
   - В поле **Логин оператора** введите логин пользователя, заданный при настройке сервера ***TRASSIR***.
   - В поле **Пароль оператора** введите пароль пользователя, заданный при настройке сервера ***TRASSIR***.
8. Используя выпадающий список внизу окна, выберите один из способов сохранения изменений:
   - **Только в базу данных** – параметры сохраняются только в БД системы и впоследствии должны быть переданы в устройство.
   - **Все в устройство** – в устройство передаются все параметры.
   - **Измененные в устройство** – в устройство передаются только измененные параметры.
9. Нажмите кнопку **Сохранить**. Окно будет закрыто, сервер ***TRASSIR*** будет добавлен в рабочую область страницы.

10. Активируйте добавленный сервер. Для этого выделите его в рабочей области страницы и нажмите кнопку **Активировать** на панели инструментов.
11. Используя меню **Поиск устройств**, вызовите окно **Найти устройства**. Добавьте и активируйте видеокамеры ***TRASSIR***, подключенные к добавленному серверу. Добавление камер ***TRASSIR*** аналогично добавлению других устройств. Подробнее.

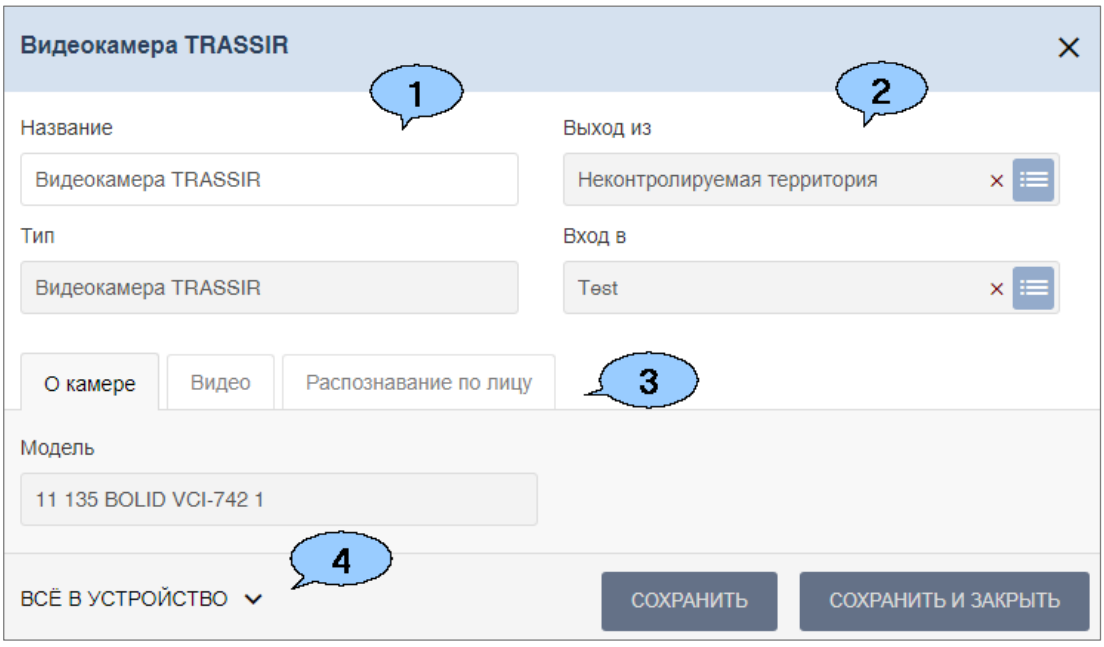
Внимание!
Видеокамеры ***TRASSIR*** отображаются в окне **Найти устройства** только после подключения сервера ***TRASSIR***.

12. Перейдите на вкладку **Помещения** и разместите видеокамеры ***TRASSIR*** в необходимых помещениях. Размещение камер ***TRASSIR*** аналогично размещению других устройств. Подробнее.
13. При желании поменяйте название камеры. Для этого выберите ее в рабочей области страницы и нажмите на панели инструментов кнопку **Редактировать**. В открывшемся окне **Редактировать устройство** в поле **Название** измените название видеокамеры, после чего нажмите кнопку **Сохранить и закрыть**.
14. Нажмите на панели инструментов страницы кнопку **Передать всю конфигурацию в устройства**.
15. При необходимости задайте реакции для контроллеров и ресурсов системы ***PERCo-Web*** на события, регистрируемые видеоподсистемой ***Trassir***, в подразделе ***«Реакции на события»*** раздела ***«Администрирование»***. Подробнее.

13.3. Параметры видеокамер TRASSIR

Для настройки параметров видеокамеры ***TRASSIR***:

- Используя панель навигации, перейдите в раздел ***«Администрирование»***.
- Откройте подраздел ***«Конфигурация»***.
- Перейдите на вкладку **Устройства**.
- Выделите в рабочей области страницы настраиваемую видеокамеру.
- Нажмите на панели инструментов страницы кнопку **Редактировать** или дважды кликните на строке с видеокамерой, после чего откроется следующее окно:

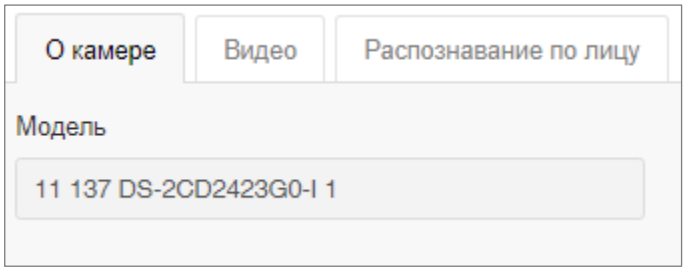


1. Поле **Название** предназначено для ввода описательного названия устройства. Поле **Тип** неизменно.
2. Инструменты для указания или изменения помещений, доступ между которыми обеспечивается видеокамерой (доступно при наличии модуля ***«TRASSIR Face Recognition»***):

   Поля **Выход из** и **Вход в** – кнопка справа от поля позволяет выбрать помещение, доступ в которое будет осуществляться с помощью системы автоматического распознавания лиц ***TRASSIR Face Recognition***. Кнопка **Сбросить** позволяет удалить из поля выбранное ранее помещение.
3. Выбор вкладок окна:
   - **О камере**;
   - **Видео**;
   - **Распознавание по лицу**.

Вкладка «О камере»

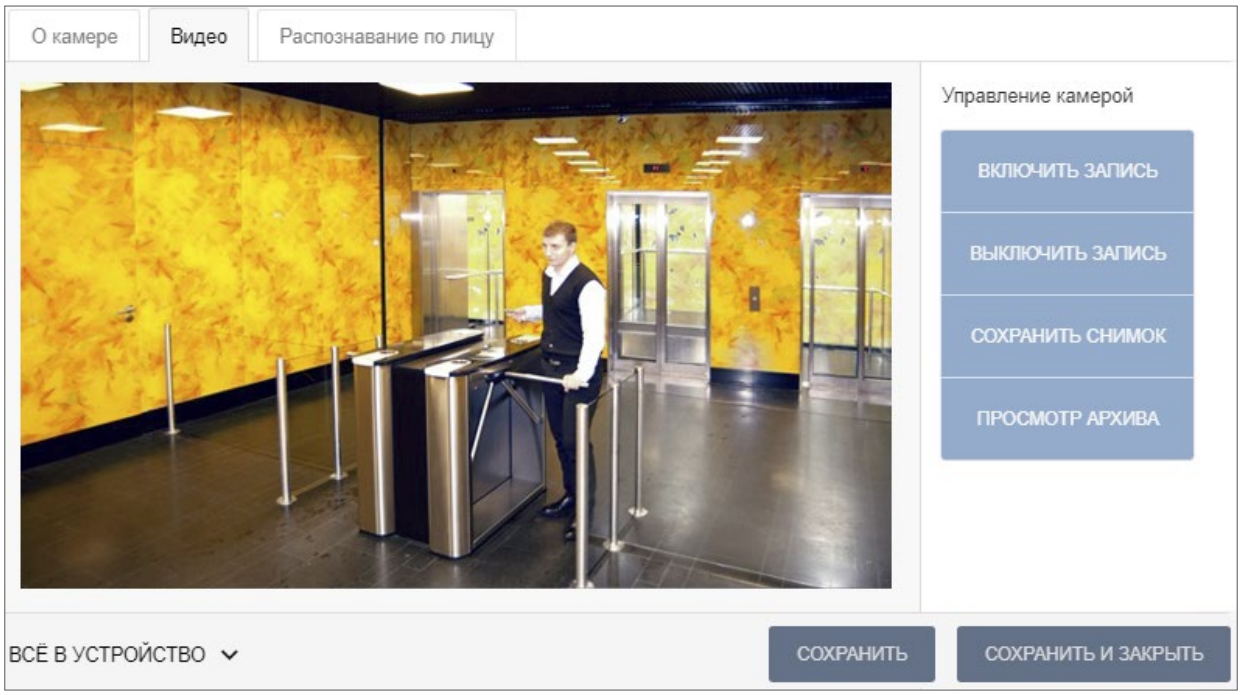
Вкладка **О камере** содержит информацию о модели камеры и имеет следующий вид:



Вкладка «Видео»

На вкладке **Видео** отображается видеосъемка с выбранной камеры в режиме реального времени. Для того, чтобы перейти в полноэкранный режим, кликните левой кнопкой мыши по иконке в правом верхнем углу изображения с камеры. Для выхода из полноэкранного режима кликните левой кнопкой мыши по иконке в правом верхнем углу изображения с камеры.

Вид вкладки:



Поддерживаются следующие команды:

– **Включить запись** – позволяет вручную включить запись на канале записи сервера ***TRASSIR***. В таком случае в рабочей области страницы подраздела ***«Конфигурация»*** появится надпись *«Идет запись»*.

Внимание!

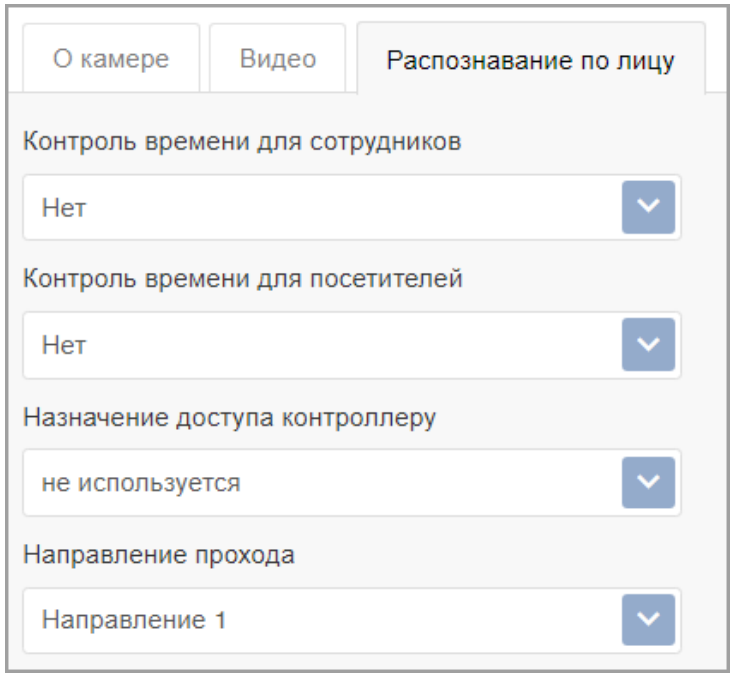
Запись видео может производиться сервером ***TRASSIR*** автоматически по настроенным алгоритмам, то есть надпись *«Идет запись»* может появляться без включения записи вручную.

– **Выключить запись** – позволяет выключить текущую запись.
– **Сохранить снимок** – позволяет сохранить скриншот «живого видео». Сохранение скриншота осуществляется в архив видеоподсистемы ***Trassir***.
– **Просмотр архива** – позволяет найти определенную видеозапись, выбрав дату и время начала записи. Полный архив хранится на сервера ***TRASSIR*** в подразделе ***«Веб-сервер»***.

Вкладка «Распознавание по лицу»

Вкладка **Распознавание по лицу** позволяет настроить параметры функции контроля по времени и назначить доступ контроллеру.

Вид вкладки:



На вкладке расположены поля для настройки следующих параметров:

- **Контроль времени для СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ** – позволяет определить реакцию системы на сканирование лица сотрудника / посетителя в случае нарушения установленного критерия доступа по времени. Можно выбрать один из видов контроля:
  – **Нет** – система не отслеживает временные критерии прав доступа.
  – **Мягкий** – система разрешит доступ. При этом регистрируется событие мониторинга *«Предъявление идентификатора, нарушение времени»*, после совершения прохода регистрируется событие *«Проход с несоответствием временным критериям доступа»*.
  – **Жесткий** – система запретит доступ, при этом регистрируется событие мониторинга *«Предъявление идентификатора, нарушение времени»* и регистрируется событие *«Запрет прохода, несоответствие временным критериям доступа»*.
- **Назначение доступа контроллеру** – раскрывающийся список позволяет выбрать контроллер, которому будет передана команда разблокировки для выбранного направления прохода в случае успешного распознавания по лицу видеокамерой ***TRASSIR***.

- **Направление прохода** – раскрывающийся список позволяет задать направление прохода (1 – в одну сторону, 2 – в противоположную).

4. Раскрывающийся список позволяет выбрать способ сохранения изменений:
   - **Только в базу данных** – параметры сохраняются только в БД системы и впоследствии должны быть переданы в устройство.
   - **Все в устройство** – в устройство передаются все параметры.
   - **Измененные в устройство** – в устройство передаются только измененные параметры.

13.4. Функция «Живое видео» и управление видеокамерами TRASSIR

Интеграция с видеоподсистемой ***Trassir*** позволяет осуществлять контроль над объектом в интерфейсе системы ***PERCo-Web*** посредством вывода «живого видео» с камер видеоподсистемы.

Функция «Живое видео» и управление видеокамерами ***TRASSIR*** доступны в следующих разделах системы ***PERCo-Web***:

- раздел **«Администрирование»> «Конфигурация»> «Устройства»>** параметры видеокамеры ***TRASSIR*** **>** вкладка **«Видео»**;
- подраздел ***«Управление устройствами»*** раздела ***«Контроль доступа»*** (см. *Руководство пользователя* ***PERCo-WS***);
- раздел ***«Мониторинг»*** (см. *Руководство пользователя* ***PERCo-WM05***).

Команды управления видеокамерами приведены в описании вкладки **«Видео»** и в разделе **«Команды управления устройствами»** данного руководства.

13.5. Распознавание по лицу с помощью системы TRASSIR Face Recognition

«TRASSIR Face Recognition» – модуль в составе ПО ***TRASSIR***, позволяющий автоматически распознавать лица пользователей и искать их по заранее настроенной базе. Фотография лица пользователя, загруженная в базу ***Trassir***, может быть использована в качестве идентификатора доступа в системе ***PERCo-Web***.

Примечание:

Для качественной работы функции распознавания по лицу ознакомьтесь с рекомендациями на сайте производителя:

Рекомендации к фотографиям, используемым для распознавания:

https://www.dssl.ru/files/trassir/manual/ru/setup-face-d-b.html

Рекомендации по установке и настройке камеры:
https://www.dssl.ru/files/trassir/manual/ru/setup-face-recognizer-description.html

13.5.1. Порядок работы с функцией распознавания по лицу

Примечание:

В данном подразделе приведена краткая инструкция по настройке модуля распознавания и поиска лиц по базе ***«TRASSIR Face Recognition»***, подробное руководство доступно в электронном виде на сайте компании ООО ***«ДССЛ-Первый»***, по адресу: *www.dssl.ru*.

1. Активируйте лицензию на распознавание лиц в настройках сервера ***TRASSIR***.
2. В разделе **Модули** сервера ***TRASSIR*** перейдите в модуль **Распознавание лиц**.
3. Выполните необходимые настройки и включите опцию распознавания лиц у нужных камер.
4. В системе ***PERCo-Web*** откройте параметры видеокамеры ***TRASSIR*** и укажите помещение, доступ в которое будет осуществляться с помощью системы автоматического распознавания лиц ***TRASSIR Face Recognition***, после чего на вкладке **«Распознавание по лицу»** настройте параметры функции контроля по времени.

5. Настройте параметры доступа сервера ***TRASSIR*** в подразделе ***«Шаблоны доступа»*** раздела ***«Бюро пропусков»*** (см. *Руководство пользователя* ***PERCo-WS***).

Внимание!

Видеокамеры ***TRASSIR*** должны быть связаны с помещениями в конфигурации системы ***PERCo-Web***.

6. В разделах ***«Персонал»*** и ***«Бюро пропусков»*** произведите сканирование лиц сотрудников и посетителей с использованием сервера ***TRASSIR*** (см. *Руководство пользователя* ***PERCo-WS***).
7. При необходимости организуйте точки верификации доступа с использованием функции распознавания по лицам (см. *Руководство пользователя* ***PERCo-WM02***).

Примечание:

База лиц хранится на сервере ***TRASSIR*** в подразделе ***«Персоны»***.

14. Утилита миграции БД с более ранней версии ПО

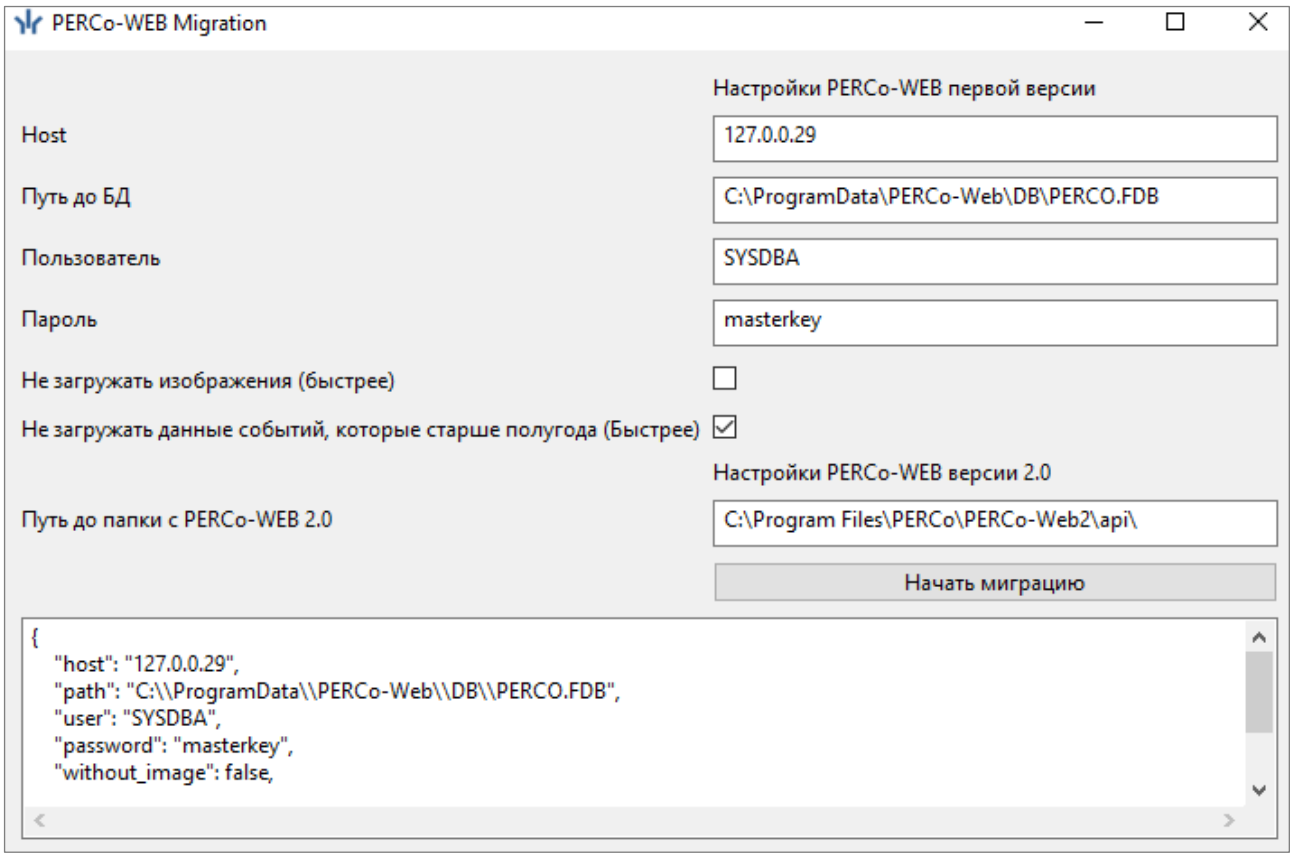
Внимание!

Утилиту миграции необходимо запускать от имени администратора. Перед началом работы убедитесь, что на ПК, с которого импортируются данные, установлен и запущен сервер баз данных *«Firebird»*. Также рекомендуется сделать резервную копию базы данных ***PERCo-Web*** первой версии. Перед началом миграции необходимо остановить Web-серверы и серверы системы в обеих версиях ***Менеджера PERCo-Web***.

Утилита **Миграции** предназначена для переноса информации из базы данных системы безопасности предыдущих (1.x.x.x) версий ***PERCo-Web***.

Для запуска утилиты необходимо запустить файл ***pw_migration***, который находится в папке с установленными файлами системы ***PERCo-Web*** (по умолчанию это *C:\Program Files\PERCo\PERCo-Web2\migration)*.

Окно выглядит следующим образом:



Окно утилиты миграции содержит следующие элементы:

- **Host** – поле предназначено для ввода IP-адреса машины, на которой была установлена система безопасности ***PERCo-Web*** первой версии.
- **Путь до БД –** поле предназначено для указания пути, по которому находится база данных первой версии ***PERCo-Web***.
- **Пользователь** – поле предназначено для ввода имени пользователя, заданного в настройках *Firebird*.
- **Пароль –** поле предназначено для ввода пароля пользователя, заданного в настройках *Firebird*.
- **Не загружать изображения** – при установке флажка у параметра фотографии сотрудников / посетителей и прочие графические изображения не будут перенесены в систему ***PERCo-Web*** **(2.x.x.x)**. При выборе данного параметра импортирование файлов пройдет быстрее.
- **Не загружать данные событий, которые старше полугода** – при установке флажка у параметра в систему ***PERCo-Web*** **(2.x.x.x)** не будут перенесены события системы

PERCo-Web первой версии, которые были старше полугода. При выборе данного параметра импортирование файлов пройдет быстрее.

- **Путь до папки с *PERCo-Web* (2.x.x.x)** – поле предназначено для указания пути к папке с установленными файлами системы ***PERCo-Web* (2.x.x.x)**.
- **Начать миграцию** – кнопка предназначена для запуска процесса импортирования данных.
- **Окно отображения информации об операциях** – окно предназначено для отображения подробного процесса миграции БД. По завершении миграции в окне появится сообщение «Закончили».

Примечание:

Миграцию рекомендуется проводить в пустую базу данных ***PERCo-Web* (2.x.x.x)**.

Внимание!

При помощи утилиты миграции из БД более ранней версии ПО **не переносятся**:

- настройки оборудования;
- операторы;
- шаблоны пропусков;
- шаблоны верификации;
- отпечатки пальцев Suprema.

Эти данные необходимо будет перенести в БД новой версии ПО вручную.

15. API PERCo-Web

Раздел предназначен для помощи разработчикам в создании сторонних приложений на базе готовых решений системы ***PERCo-Web***.

Раздел предназначен для пользователей, обладающих высоким уровнем квалификации в области ИТ и практическими знаниями в Web разработке.

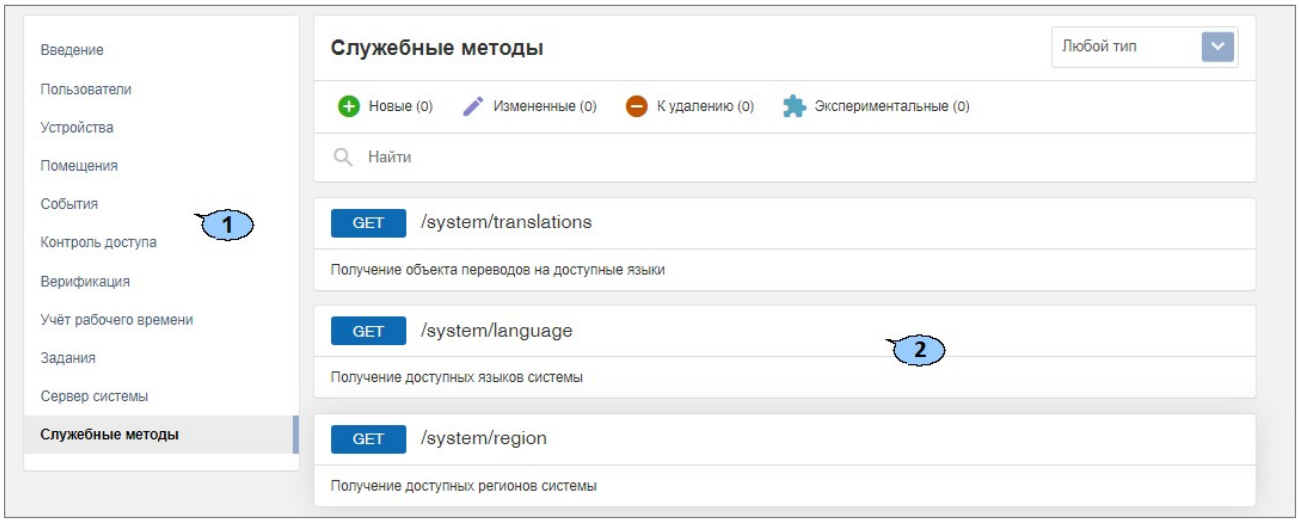
API (Application Programming Interface) – это интерфейс, который позволяет получать информацию из базы данных ***PERCo-Web*** с помощью HTTP-запросов к серверу.

В раздел можно перейти двумя способами:

1. Используя панель навигации, перейдите в раздел  **«Администрирование»**.

   Далее откройте подраздел **«Лицензии»** и выберите лицензию ***PERCo-WM04 «Интеграция с внешними системами»***. В открывшемся окне перейдите по ссылке ***Документация***.
2. В адресной строке добавьте к IP-адресу сервера */dev.*
   Например, *https://172.17.0.xx/dev*.

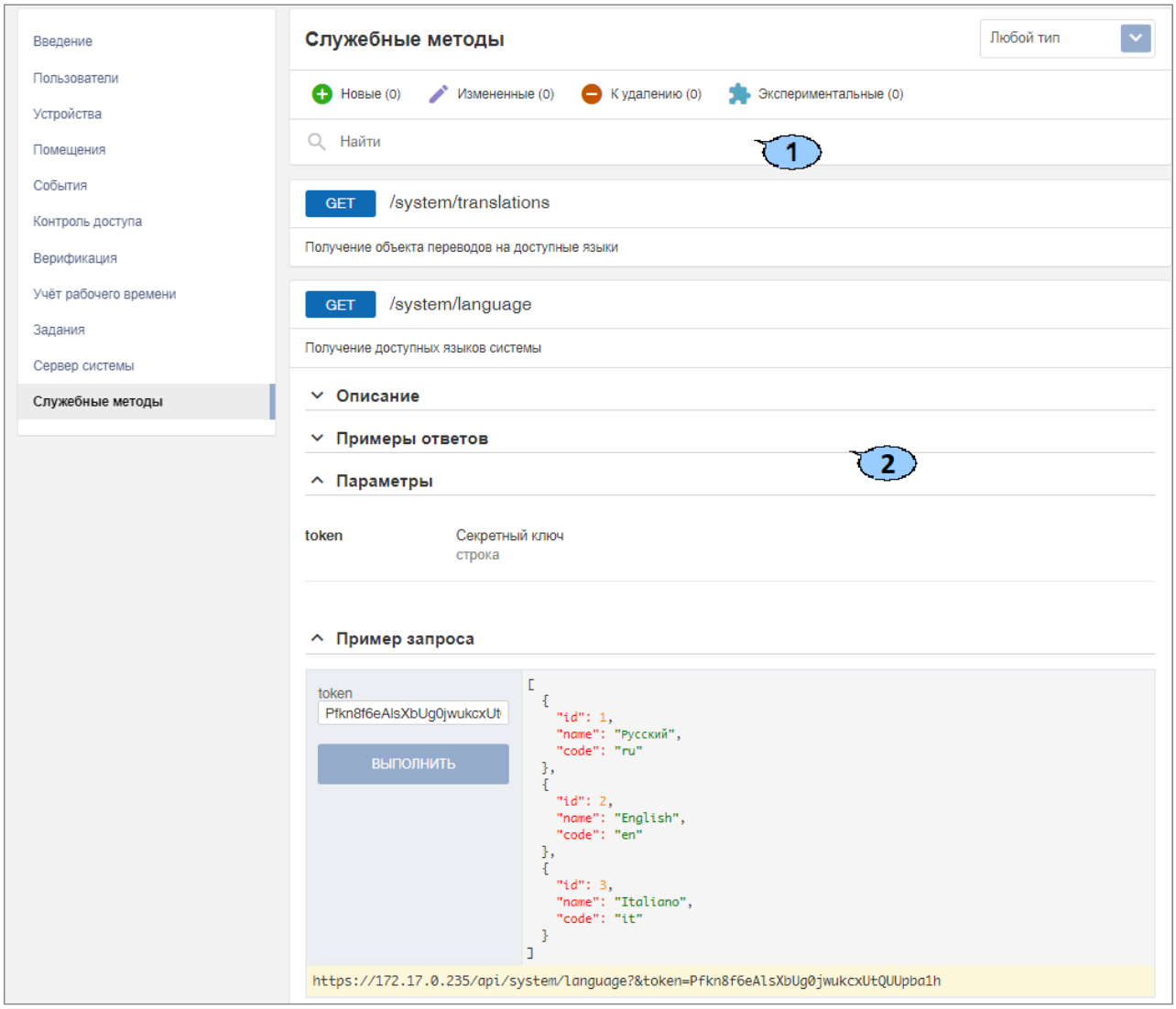
Раздел имеет следующий вид:



1. Список групп методов в зависимости от их функциональной принадлежности.
2. Рабочая область содержит служебные методы выбранной группы. Методы разбиты по группам в зависимости от их функциональной принадлежности.

15.1. Возможности API

Рабочая область имеет следующий вид и особенности:



1. Панель инструментов страницы:
   - – фильтр позволяет сделать выборку по следующим типам методов:
     - **Любой тип**;
     - **GET**;
     - **POST**;
     - **PUT**;
     - **DELETE**.
   - Вкладки по статусам методов. Актуальная информация отображается после обновления версии системы ***PERCo-Web***. Существуют следующие вкладки:
     - **Новые** – в рабочей области отобразятся добавленные методы.
     - **Измененные** – в рабочей области отобразятся методы, в которые вносились изменения. Метод будет отображен с пометкой новой версии, устаревшая версия метода будет помечена для удаления.
     - **К удалению** – в рабочей области отобразятся методы, которые будут удалены при следующих обновлениях версии системы ***PERCo-Web***.
     - **Экспериментальные** – в рабочей области отобразятся методы, которые в ближайших версиях системы будут изменяться.
   - Поле **Найти** предназначено для поиска метода по фрагменту наименования.

2. Список доступных методов.

   При выборе элемента открываются следующие поля:
   - **Описание** – содержит краткую характеристику выбранного метода.
   - **Примеры ответов** – предназначено для наглядного отображения информации.
   - **Параметры** – содержит описание параметров, которые можно передать в метод.
   - **Пример запроса** – панель позволяет проверить работу запроса.

16. Предварительная настройка

При подготовке системы к работе придерживайтесь следующей последовательности действий:

1. Войдите 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 **«Лицензии»** и активируйте необходимые пакеты и модули ПО, при необходимости введите приобретенные лицензионные ключи.
   - Откройте подраздел **«Конфигурация»**.
     - выберите регион и формат отображения дат в системе (вкладка **«Система»**);
     - произведите поиск и добавление контроллеров в конфигурацию системы (вкладка **«Устройства»**);
     - создайте список помещений предприятия (вкладка **«Помещения»**);
     - привяжите контроллеры к помещениям.
   - 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. В разделе  **«Бюро пропусков»** (см. *Руководство пользователя* ***PERCo-WB***, ***PERCo-WBE***, ***PERCo-WS***, ***PERCo-WSE***):
   - Откройте подраздел **«Шаблоны доступа»**.
     - При необходимости добавьте временные критерии доступа и отредактируйте праздничное расписание доступа (вкладка **«Временные критерии доступа»**).
     - Создайте шаблоны доступа для сотрудников предприятия и посетителей. При создании шаблона для каждого помещения устанавливаются индивидуальные права и критерии доступа (вкладка **«Шаблоны»**).

4. В разделе  **«Персонал»**:
   - Откройте подраздел **«Должности»** и создайте список должностей предприятия (см. *Руководство пользователя* ***PERCo-WB***, ***PERCo-WBE***, ***PERCo-WS***, ***PERCo-WSE***).
   - При необходимости в подразделе **«Дополнительные данные»** (см. *Руководство пользователя* ***PERCo-WS***, ***PERCo-WSE***) создайте поля для ввода дополнительных текстовых и графических данных.
   - При работе с УРВ (см. *Руководство пользователя* ***PERCo-WM01***, ***PERCo-WME01***):
     - В подразделе **«Графики работы»** создайте графики работы для сотрудников предприятия. Укажите для каждого графика регистрирующие помещения и параметры составления отчетов по дисциплине труда.
     - В подразделе **«Праздничные дни»** отредактируйте календарь праздничных дней.
   - Откройте подраздел **«Подразделения»** (см. *Руководство пользователя* ***PERCo-WB***, ***PERCo-WBE***, ***PERCo-WS***, ***PERCo-WSE***) и создайте список структурных подразделений предприятия. Для каждого подразделения укажите данные, которые будут автоматически устанавливаться сотрудникам и посетителям подразделения.

5. В разделе  **«Бюро пропусков»** (см. *Руководство пользователя* ***PERCo-WS***, ***PERCo-WSE***):
   - Откройте подраздел **«Дизайн пропуска»** и создайте шаблоны дизайна пропусков сотрудников и посетителей для подразделений предприятия.

6. В разделе  **«Персонал»** (см. *Руководство пользователя* ***PERCo-WB***, ***PERCo-WBE***, ***PERCo-WS***, ***PERCo-WSE***):
   - Откройте подраздел **«Сотрудники»** и создайте список сотрудников предприятия. Для каждого сотрудника:
     – Заполните учетную карточку (укажите ФИО, подразделение, должность, график работы и т.д.).
     – Добавьте фотографию.
     – Выдайте карту доступа (идентификатор) и установите шаблон доступа. При необходимости распечатайте пропуск или наклейку на карту доступа (см. *Руководство пользователя* ***PERCo-WS***, ***PERCo-WSE***).
7. В разделе  **«Бюро пропусков»** (см. *Руководство пользователя* ***PERCo-WB***, ***PERCo-WBE***, ***PERCo-WS***, ***PERCo-WSE***):
   - Откройте подраздел **«Шаблоны доступа»**, перейдите на вкладку **Комиссионирование** и при необходимости укажите для контроллеров сотрудников, карты доступа которых будут являться комиссионирующими.
8. Настройте функции контроля зональности доступа карт в системе (*Antipass* и *Global Antipass*).

17. Функции Antipass и Global Antipass

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

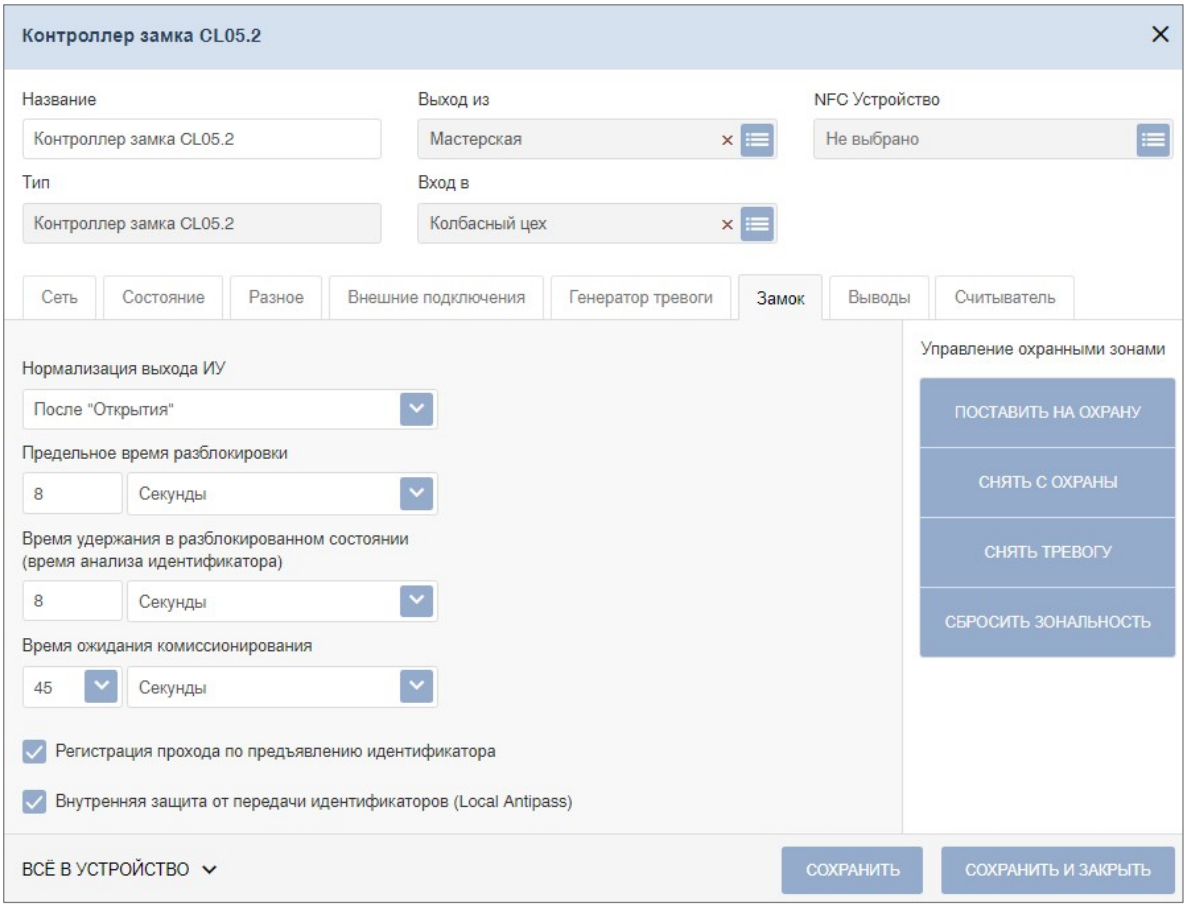
Функция Antipass

Примечание:

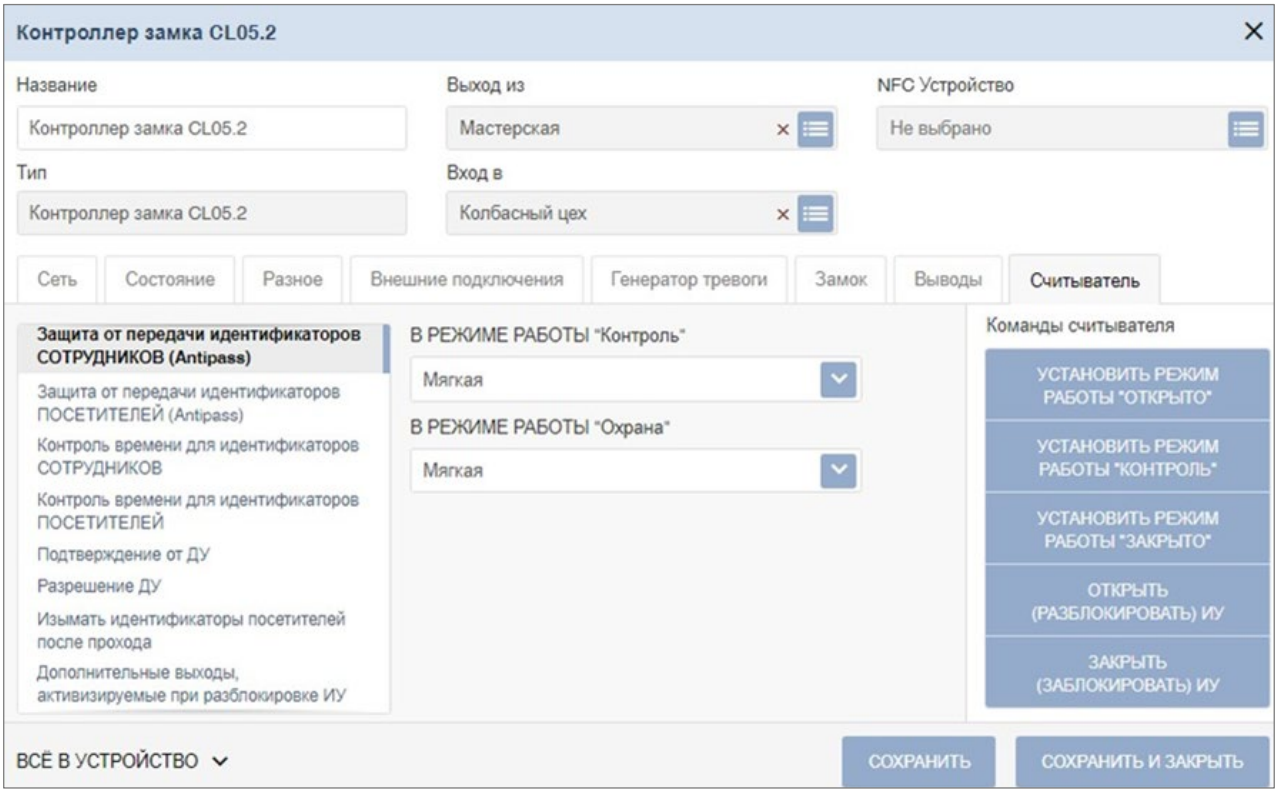
Для использования функции *Antipass* в шаблоне доступа карты необходимо указать помещения, при доступе в которые должен производиться контроль. Настройка шаблона проводится в подразделе **«Шаблон доступа»** раздела **«Бюро пропусков»**.

Для включения / отключения функции контроля зональности:

1. Используя панель навигации, перейдите в раздел **«Администрирование».**
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **Устройства**.
4. В рабочей области страницы выберите контроллер, для которого необходимо включить функцию контроля зональности.
5. Нажмите кнопку **Редактировать** на панели инструментов страницы.
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:



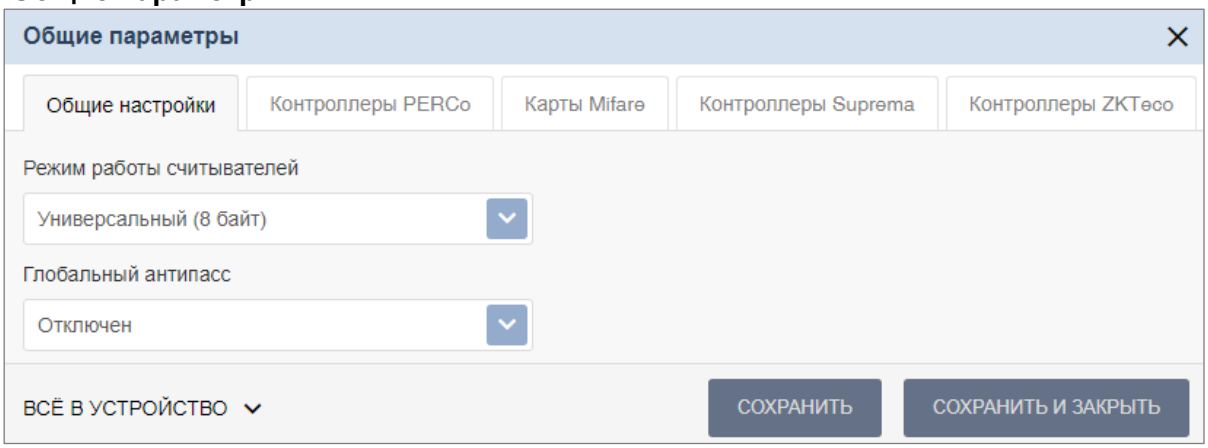
В рабочей области окна независимо для сотрудников и посетителей установите жесткий или мягкий режим контроля зональности при различных РКД.

9. Нажмите кнопку **Сохранить** или **Сохранить и закрыть**. Окно 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 **Устройства**.
4. В рабочей области страницы выберите корневой элемент списка **Общие параметры**.
5. Нажмите кнопку **Редактировать** на панели инструментов страницы. Откроется окно **Общие параметры**:



6. Для включения / отключения функции глобального контроля зональности в выпадающем списке **Глобальный антипасс** выберите **Включен** / **Отключен**.
7. Нажмите кнопку **Сохранить** или **Сохранить и закрыть**. Окно **Общие параметры** будет закрыто, измененные параметры будут переданы в контроллеры системы.

18. Раздел «Администрирование»

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

18.1. Подраздел «Конфигурация»

В подразделе доступны следующие вкладки:

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

Вкладка **Устройства** предназначена для:

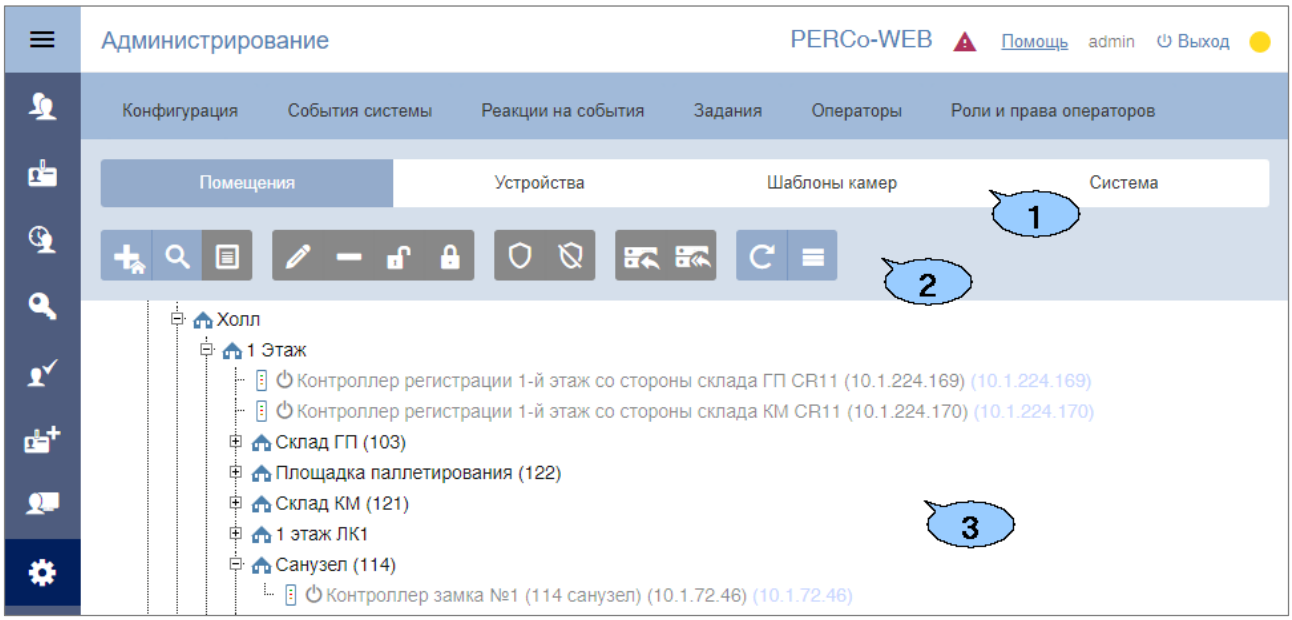
- поиска устройств в локальной сети и добавления их в конфигурацию системы;
- настройки параметров устройств и их ресурсов;
- подачи команд управления;
- временного исключения устройств из конфигурации.

Вкладка **Шаблоны камер** предназначена для создания шаблонов параметров для видеокамер системы.

Вкладка **Система** предназначена для изменения общих настроек системы, настройки рассылки и уведомлений.

18.1.1. Вкладка «Помещения»

Страница вкладки имеет следующий вид:



1. Переключатель выбора вкладки подраздела:
   - **Помещения**;
   - **Устройства**;
   - **Шаблоны камер**;
   - **Система**.
2. Панель инструментов страницы:
   - **Добавить помещение** – кнопка позволяет добавить вложенное помещение в помещение, выделенное в рабочей области страницы.
   - **Поиск устройств** – кнопка позволяет произвести поиск устройств (которые ранее не были добавлены в конфигурацию системы) в локальной сети и разместить их в выделенном в рабочей области страницы помещении.

-  **Установить устройство** – кнопка позволяет разместить устройства, добавленные ранее в конфигурацию системы, в выделенном в рабочей области страницы помещении.
-  **Редактировать** – кнопка позволяет изменить название выделенного в рабочей области страницы помещения или настроить параметры выделенного в рабочей области устройства.
-  **Удалить помещение / Отвязать устройство** – кнопка позволяет удалить выделенное в рабочей области страницы помещение или устройство из помещения.
-  **Активировать** – кнопка позволяет включить в конфигурацию системы ранее исключенное или найденное устройство.
-  **Деактивировать** – кнопка позволяет временно исключить из конфигурации системы устройство, выделенное в рабочей области страницы. При этом наименование исключенного устройства затеняется.
-  **Поставить на охрану** – кнопка позволяет перевести устройство / помещение в РКД *«Охрана»*.
-  **Снять с охраны** – кнопка позволяет перевести устройство / помещение из РКД *«Охрана»* в предыдущий РКД.
-  **Передать изменения конфигурации в устройства** – кнопка позволяет передать измененные параметры в устройства системы.
-  **Передать всю конфигурацию в устройства** – кнопка позволяет передать все параметры в устройства системы.
-  **Обновить помещения и устройства** – кнопка позволяет обновить информацию о состоянии устройств.
-  **Дополнительно** – кнопка позволяет открыть меню команд для выбора дополнительного действия:
  - **Экспорт** – позволяет сохранить данные рабочей области в файл электронных таблиц с выбранным расширением.

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

Примечание:

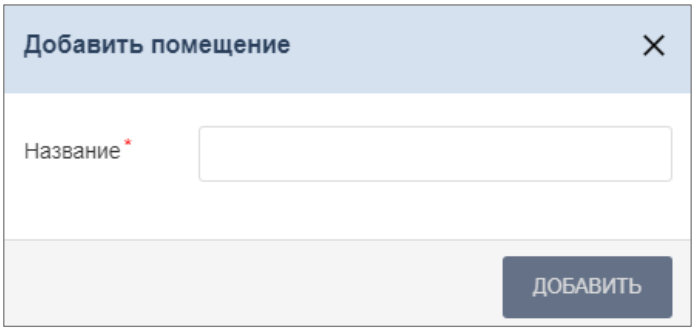
В рабочей области страницы реализована функция *Drag-and-drop*, позволяющая изменять расположение помещений в списке с помощью мыши.

18.1.1.1. Создание списка помещений

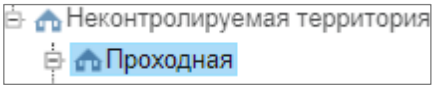
Для создания списка помещений:

1. Используя панель навигации, перейдите в раздел  **«Администрирование»**.
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **Помещения**.

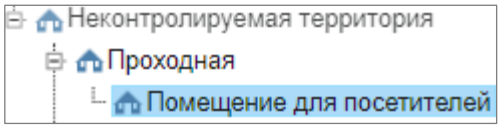
4. Нажмите на панели инструментов страницы кнопку  **Добавить помещение**. Откроется окно **Добавить помещение**:



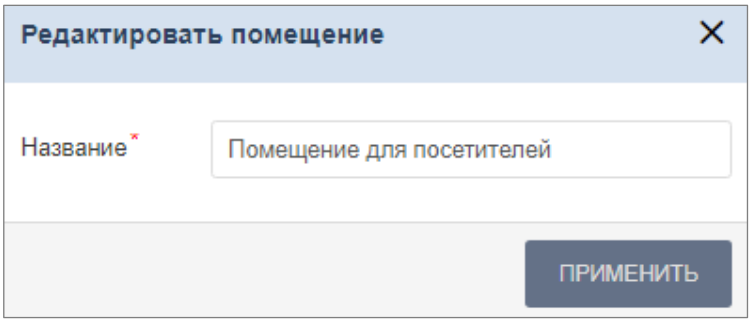
5. В открывшемся окне введите название нового помещения и нажмите кнопку **Добавить**. Окно будет закрыто, помещение будет добавлено в раскрывающийся список в рабочей области страницы как вложенное:



6. 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**.
7. В открывшемся окне введите название нового помещения и нажмите кнопку **Добавить**. Окно будет закрыто, помещение будет добавлено в выделенное в рабочей области страницы:



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

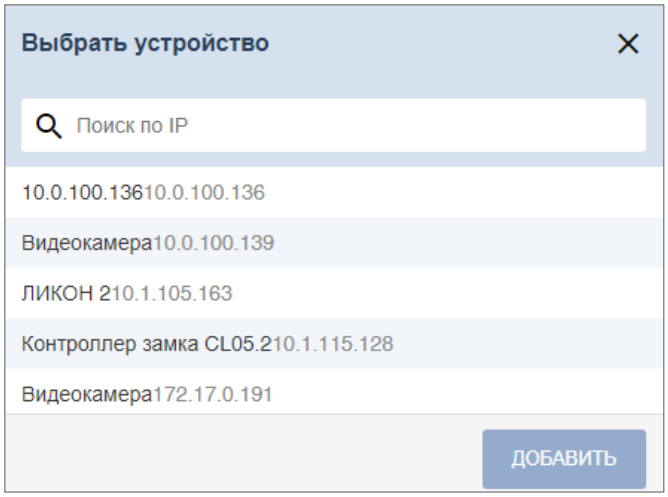


9. В открывшемся окне произведите необходимые изменения и нажмите кнопку **Применить**.
10. Для удаления добавленного ранее помещения выделите его в рабочей области страницы и нажмите кнопку  **Удалить помещение / Отвязать устройство** на панели инструментов страницы. В открывшемся окне подтверждения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

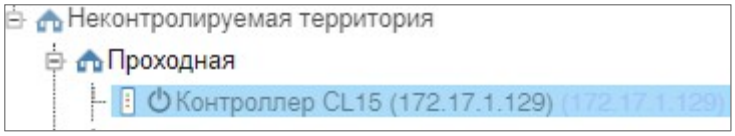
18.1.1.2. Размещение устройств в помещениях

После создания списка помещений необходимо расположить в них устройства, входящие в систему безопасности. Для размещения устройств в помещениях:

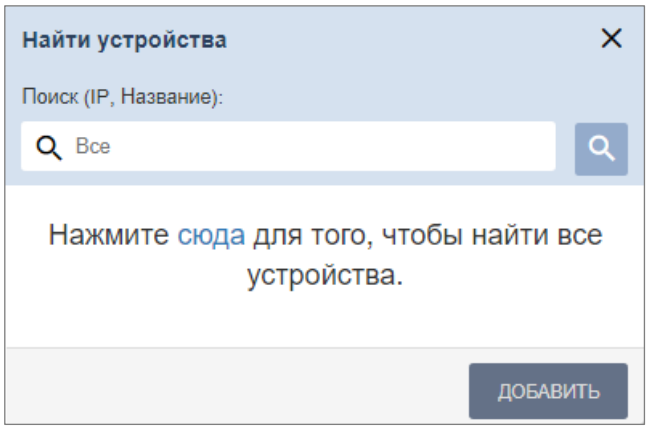
1. Выделите помещение в рабочей области страницы и нажмите на панели инструментов кнопку **Установить устройство**. Откроется окно **Выбрать устройство**, содержащее список устройств, добавленных ранее в конфигурацию системы:



2. В открывшемся окне выделите устройство и нажмите кнопку **Добавить**. Наименование устройства появится в выделенном помещении:



3. При необходимости в помещении можно расположить устройство, которое ранее не было добавлено в конфигурацию системы. Для этого выделите помещение и нажмите кнопку **Поиск устройств**. Откроется окно **Найти устройства**:



4. В открывшемся окне введите IP-адрес искомого устройства и нажмите кнопку .
5. Выберите необходимые устройства и нажмите кнопку **Добавить**. Устройства будут добавлены в помещение.
6. При необходимости произведите настройку параметров работы устройства. Для этого выделите устройство в рабочей области страницы и нажмите на панели инструментов страницы кнопку **Редактировать**. В открывшемся окне **Редактировать устройство** произведите необходимые изменения и нажмите кнопку **Сохранить и закрыть**.

Примечание:

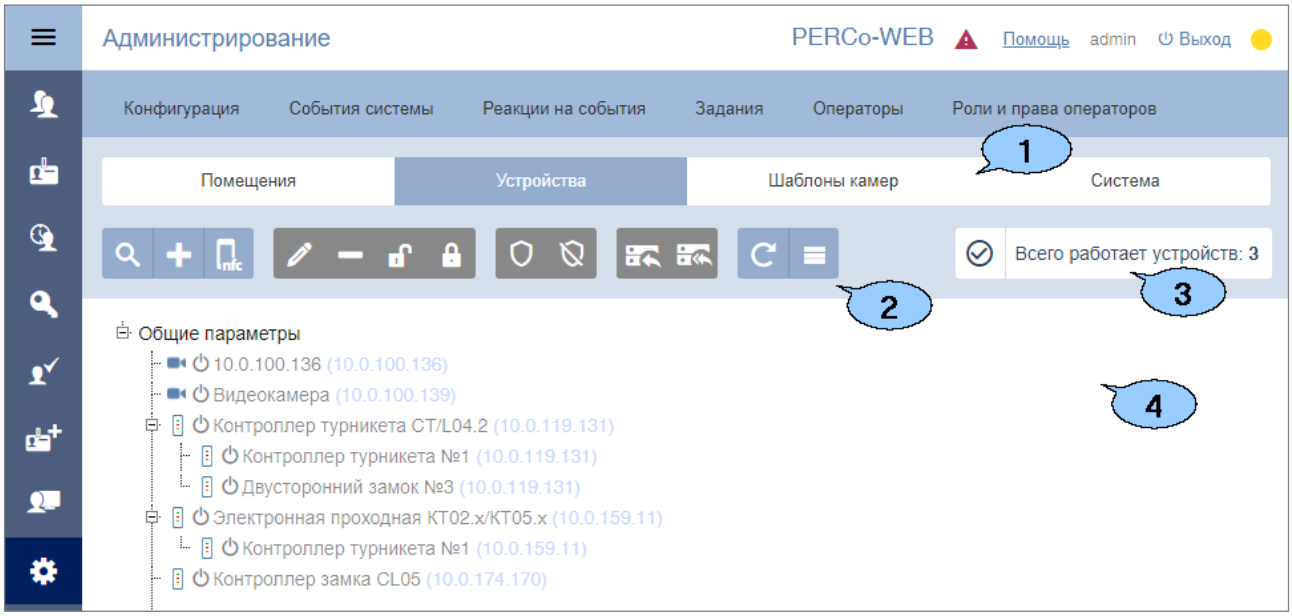
Для контроллеров электромеханических замков моделей ***PERCo-CL05.1*** и ***PERCo-CL05.2***, открывающихся при подаче напряжения, возможна совместная работа двух контроллеров при организации КПП с контролем проходов в двух направлениях. Для поддержки смены зональности при проходе через такое КПП, необходимо установить флажок у параметра **Смена зоны при проходе** соответствующего контроллеру ИУ ресурса в окне **Редактировать устройство**.

7. Для удаления контроллера, добавленного ранее в помещение, выделите его в рабочей области страницы и нажмите кнопку **Удалить помещение / Отвязать устройство** на панели инструментов. В открывшемся окне подтверждения нажмите кнопку **Удалить**. Контроллер будет удален из помещения.

8. Нажмите на панели инструментов страницы кнопку **Передать всю конфигурацию в устройства**.

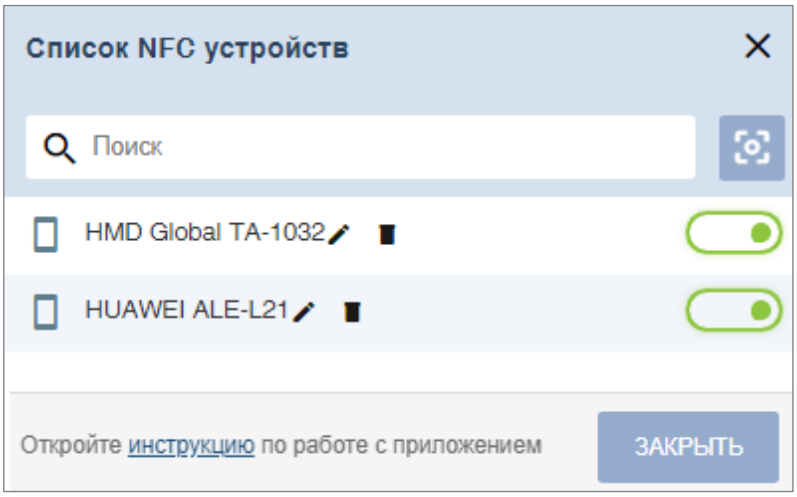
18.1.2. Вкладка «Устройства»

Страница вкладки имеет следующий вид:



1. Переключатель выбора вкладки подраздела:
   - **Помещения**;
   - **Устройства**;
   - **Шаблоны камер**;
   - **Система**.
2. Панель инструментов страницы:
   - **Поиск устройств** – кнопка позволяет произвести поиск в локальной сети устройств, которые ранее не были добавлены в конфигурацию системы.
   - **Добавить** – кнопка позволяет:
     – **Добавить камеру**;
     – **Добавить шлюз CTL14**;
     – **Добавить шлюз CL15**;
     – **Добавить составной объект CL15**.
   - **Список NFC устройств** – кнопка позволяет открыть окно **Список NFC устройств** для работы с устройствами, поддерживающими технологию NFC. Данная функция

позволяет добавить в систему устройство (смартфон), чтобы в дальнейшем можно было использовать его в качестве считывателя для выбранного контроллера. Для этого необходимо будет на смартфон установить приложение ***Perco.Регистрация***. Окно **Список NFC устройств** выглядит следующим образом:



– Поле **Поиск** – поле позволяет добавить устройство вручную.
– **Отобразить QR код** – кнопка позволяет открыть окно с QR-кодом для добавления устройства.
– **Редактировать** – кнопка позволяет присвоить новое имя выбранному устройству.
– **Удалить** – кнопка позволяет удалить из списка выбранное устройство.
– – кнопка позволяет временно активировать / деактивировать выбранное устройство.

- **Редактировать** – кнопка позволяет открыть окно **Редактировать устройство** для изменения параметров выделенного в рабочей области панели устройства и его ресурсов. Если в рабочей области страницы выделен корневой элемент *«Общие параметры»*, то открывается окно **Общие параметры**.
- **Удалить** – кнопка позволяет удалить выделенное в рабочей области страницы устройство из конфигурации системы.
- **Активировать** – кнопка позволяет включить в конфигурацию системы ранее исключенное или найденное устройство.
- **Деактивировать** – кнопка позволяет временно исключить из конфигурации системы устройство, выделенное в рабочей области страницы. При этом наименование устройства затеняется.
- **Поставить на охрану** – кнопка позволяет перевести устройство в РКД *«Охрана»*.
- **Снять с охраны** – кнопка позволяет перевести устройство из РКД *«Охрана»* в предыдущий РКД.
- **Передать изменения конфигурации в устройства** – кнопка позволяет передать измененные параметры в устройства системы.
- **Передать всю конфигурацию в устройства** – кнопка позволяет передать все параметры в устройства системы.

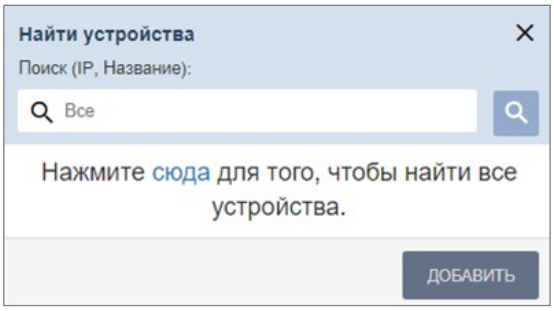
- **Обновить** – кнопка позволяет обновить информацию о состоянии устройств.
- **Дополнительно** – кнопка позволяет открыть меню команд для выбора дополнительных действий:
  - **Экспорт** – позволяет сохранить данные рабочей области в файл электронных таблиц с выбранным расширением.
  - **Выделить все устройства (Ctrl+A)** – позволяет выделить все устройства.

3. Панель информации о состоянии устройств системы.
4. Рабочая область страницы содержит список устройств, добавленных в конфигурацию системы. Значок **Валидность** слева от наименования указывает на то, что в устройство не были переданы измененные параметры.

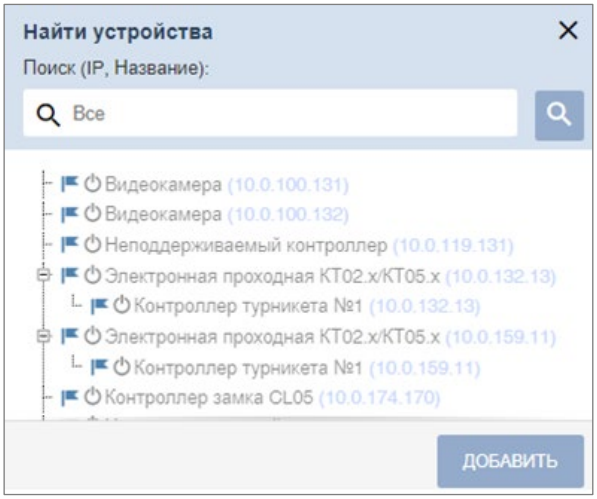
18.1.2.1. Поиск устройств

Для проведения автоматической конфигурации:

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



5. Если необходимо произвести поиск устройств по IP-адресу, то введите его в поле **Поиск (IP адрес, Название)** и нажмите кнопку . Если необходимо произвести поиск всех устройств в сети, то, не заполняя поле для поиска, нажмите кнопку или кнопку **«сюда»**.
6. По окончании поиска список найденных устройств появится в рабочей области окна:



7. Выделите в списке устройство или несколько устройств, которые необходимо добавить в конфигурацию системы. Нажмите кнопку **Добавить**. Окно будет закрыто, отмеченные устройства появятся в рабочей области страницы.
8. Активируйте добавленное устройство. Для этого выделите его в рабочей области страницы и нажмите кнопку **Активировать**.
9. Произведите настройку параметров добавленного устройства. Для этого выделите устройство или его ресурс в рабочей области страницы и нажмите на панели инструментов кнопку **Редактировать**. Откроется окно **Редактировать устройство**.
10. В открывшемся окне при необходимости в поле **Название** измените название устройства.
11. 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 **Выбрать помещение** выделите помещение, в которое осуществляется доступ через считыватель № 1, и нажмите кнопку **Сохранить**. Тем же образом в поле **Вход в** укажите помещение, в которое осуществляется доступ через считыватель № 2.
12. Для настройки параметров ресурсов устройства перейдите на вкладку, соответствующую наименованию ресурса, и произведите необходимые изменения. Список доступных параметров зависит от типа устройства и выбранного ресурса.
13. С помощью раскрывающегося списка в нижней части окна **Редактировать устройство** выберите способ сохранения параметров и нажмите кнопку **Сохранить и закрыть**. Окно **Редактировать устройство** будет закрыто.
14. Передайте конфигурацию в устройства. Для этого на панели инструментов страницы нажмите кнопку **Передать изменения конфигурации в устройства** или **Передать всю конфигурацию в устройства**.

18.1.2.2. Добавление камеры, шлюза и составного объекта

Примечание:

Перед добавлением камер создайте шаблоны для подключаемых моделей камер. Шаблоны создаются на вкладке **Шаблоны камер** подраздела **«Конфигурация»** раздела **«Администрирование»**. По умолчанию в системе установлены шаблоны параметров для видеокамер стандарта ONVIF и для видеокамер популярных производителей (TP-LINK, ACTi, AXIS).

Для добавления устройства:

1. Используя панель навигации, перейдите в раздел **«Администрирование»**.
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **Устройства**.

Примечание:

Камеры стандарта ONVIF могут быть добавлены с помощью кнопки **Поиск устройств**. Другие типы камер, например, mjpeg_over_http, добавляются с помощью кнопки **Добавить**.

4. Нажмите на панели инструментов страницы кнопку **Добавить**.
5. Из выпадающего списка выберите один из вариантов:
   - **Добавить камеру**;
   - **Добавить шлюз CTL14**;
   - **Добавить шлюз CL15**;

- **Добавить составной объект CL15**.

6. Вид окна зависит от выбранного объекта. В открывшемся окне настройте необходимые параметры.
7. При создании шлюза или составного объекта выберите один из способов сохранения изменений:
   - **Только в базу данных**;
   - **Все в устройство**;
   - **Измененные в устройство**.
8. Нажмите кнопку **Сохранить**. Объект будет добавлен в рабочую область страницы.

Для добавления камеры:

Примечание:

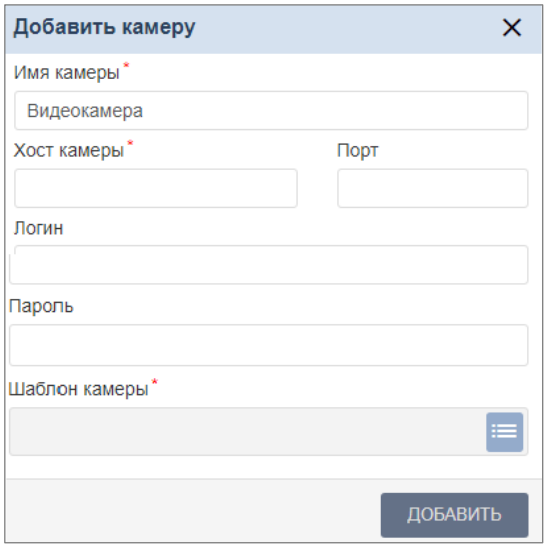
Перед добавлением камер создайте шаблоны для подключаемых моделей камер. Шаблоны создаются на вкладке **Шаблоны камер** подраздела **«Конфигурация»** раздела **«Администрирование»**.

1. Используя панель навигации, перейдите в раздел **«Администрирование»**.
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **«Устройства»**.

Примечание:

Камеры стандарта ONVIF могут быть добавлены с помощью кнопки **Поиск устройств**. Другие типы камер, например, mjpeg_over_http, добавляются с помощью кнопки **Добавить**.

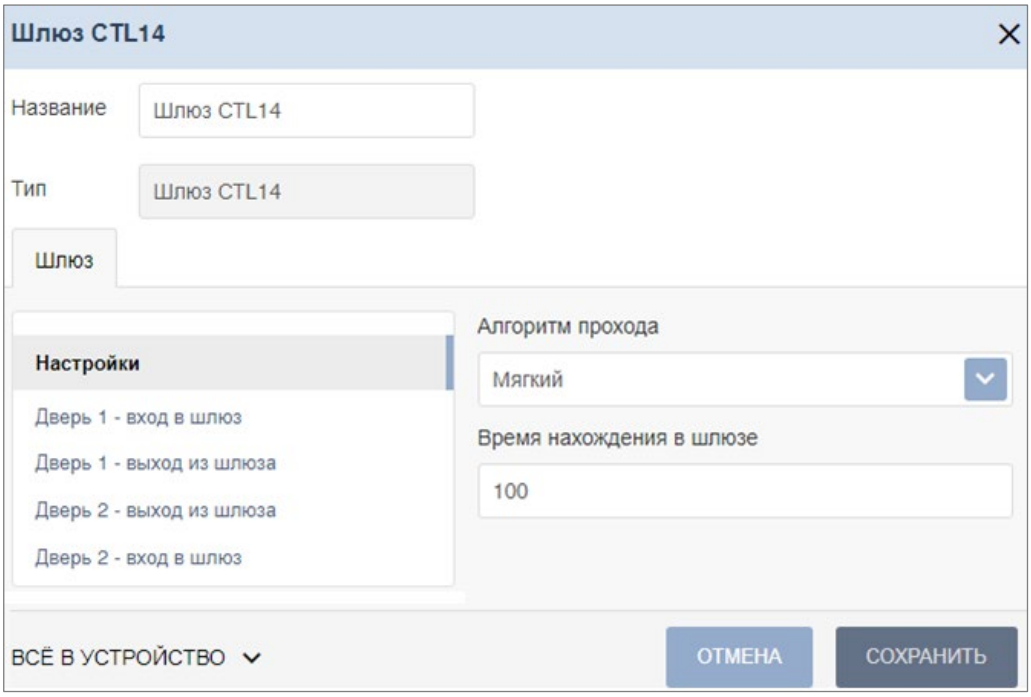
4. Нажмите на панели инструментов страницы кнопку **Добавить**. Из выпадающего списка выберите **Добавить камеру**. Откроется окно **Добавить камеру**:



5. В открывшемся окне введите имя камеры и укажите шаблон подключаемой камеры.
6. Произведите настройку других параметров. Нажмите кнопку **Добавить**. Окно **Добавить камеру** будет закрыто. Камера будет добавлена в рабочую область страницы.

Для создания шлюза *CTL14 / CL15*:

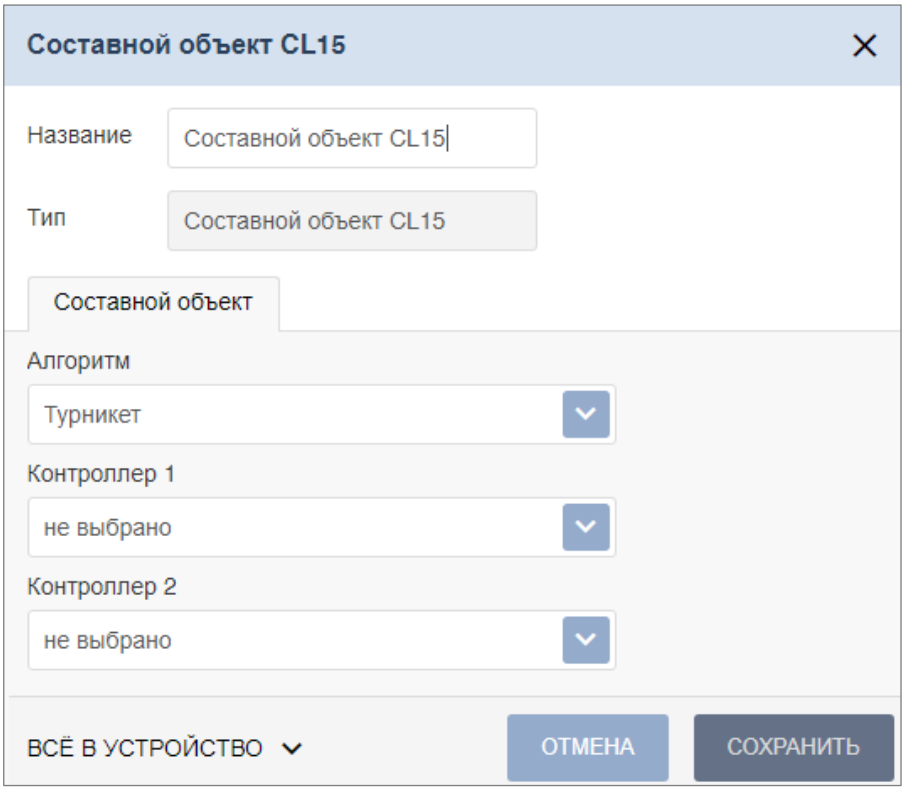
1. Используя панель навигации, перейдите в раздел **«Администрирование»**.
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **Устройства**.
4. Нажмите на панели инструментов страницы кнопку **Добавить**. Из выпадающего списка выберите **Добавить шлюз CTL14** или **Добавить шлюз CL15**. Название открывшегося окна зависит от типа выбранного шлюза и имеет следующий вид:



5. В открывшемся окне при необходимости в поле **Название** измените название шлюза.
6. Поле **Тип** неизменно, заполняется автоматически и содержит название выбранного типа шлюза.
7. На вкладке **Настройки** выберите значение для следующих параметров:
   - В поле **Алгоритм прохода** выберите алгоритм для прохода:
     - Тип **Мягкий**. При использовании данного режима, если человек находится внутри шлюза, возможен проход вперед и выход назад.
     - Тип **Жесткий**. При использовании данного режима, если человек находится внутри шлюза, возможен только проход вперед.
   - В поле **Время нахождения в шлюзе** установите время для нахождения в шлюзе.
8. На остальных вкладках для каждой двери на вход и выход из шлюза в поле **Контроллер** с помощью выпадающего списка выберите регистрирующий контроллер, в поле **Режим доступа** выберите один из режимов:
   - **По считывателю**;
   - **По ДУ**;
   - **По считывателю и ДУ**.
9. Используя выпадающий список внизу окна, выберите один из способов сохранения изменений:
   - **Только в базу данных**;
   - **Все в устройство**;
   - **Измененные в устройство**.
10. Нажмите кнопку **Сохранить**. Окно будет закрыто. Шлюз будет добавлен в рабочую область страницы.

Для создания составного объекта *CL15*:

1. Используя панель навигации, перейдите в раздел **«Администрирование»**.
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **Устройства**.
4. Нажмите на панели инструментов страницы кнопку **Добавить**. Из выпадающего списка выберите **Добавить составной объект CL15**. Откроется окно **Составной объект CL15**. Окно имеет следующий вид:

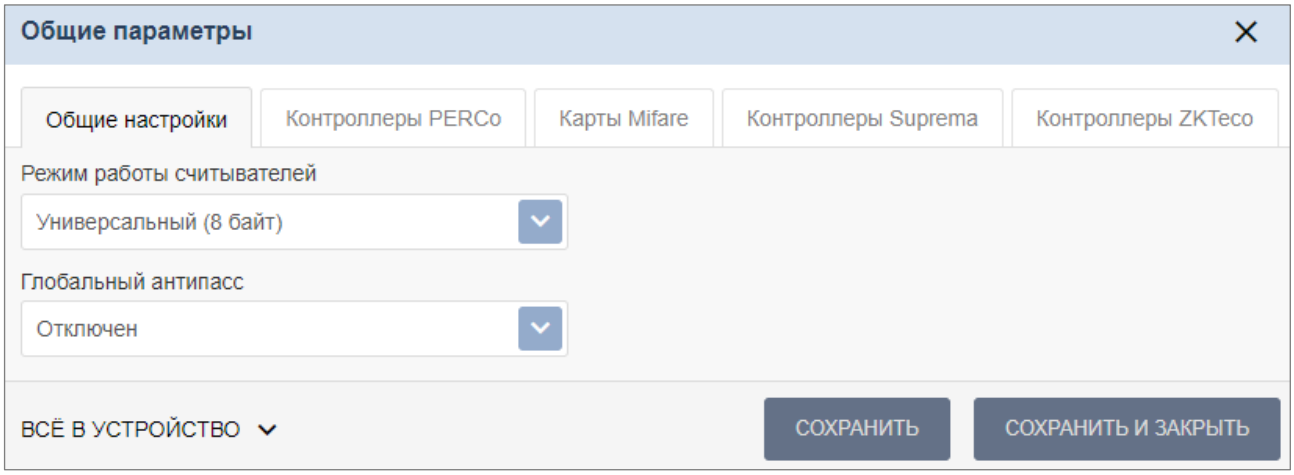


5. В открывшемся окне при необходимости в поле **Название** измените название составного объекта.
6. Поле **Тип** неизменно, заполняется автоматически и содержит название типа составного объекта.
7. На вкладке **Составной объект** выберите значение для следующих параметров:
   - В поле **Алгоритм** выберите тип ИУ: **Турникет** или **Двусторонний замок**.
   - В полях **Контроллер 1** и **Контроллер 2** с помощью выпадающего списка выберите регистрирующие контроллеры для составного объекта.
8. Используя выпадающий список внизу окна, выберите один из способов сохранения изменений:
   - **Только в базу данных**;
   - **Все в устройство**;
   - **Измененные в устройство**.
9. Нажмите кнопку **Сохранить**. Окно **Составной объект CL15** будет закрыто. Составной объект будет добавлен в рабочую область страницы.

18.1.2.3. Настройка общих параметров контроллеров

Для настройки общих параметров контроллеров системы:

1. Используя панель навигации, перейдите в раздел **«Администрирование»**.
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **Устройства**.
4. Выделите в рабочей области страницы корневой элемент **Общие параметры**.
5. Нажмите на панели инструментов страницы кнопку **Редактировать**, после чего откроется окно **Общие параметры** с вкладками:
   - **Общие настройки**;
   - **Контроллеры PERCo**;
   - **Карты Mifare**;
   - **Контроллеры Suprema**;
   - **Контроллеры ZKTeco**.
6. Вкладка **Общие настройки**. Вкладка выглядит следующим образом:



- **Режим работы считывателей** – позволяет изменить параметры режима работы считывателей.
- **Глобальный антипасс** – позволяет включить или отключить глобальный контроль зональности (Global Antipass).
- С помощью раскрывающегося списка в нижней части окна выберите способ сохранения параметров. Для завершения работы с окном **Общие параметры** нажмите кнопку **Сохранить**.

Примечание:

В системе безопасности ***PERCo-Web*** реализована возможность прохода по смартфонам с технологией NFC. Функция включена по умолчанию.

При работе со смартфоном на ОС “*Android*”, поддерживающим технологию NFC, в качестве идентификатора сотрудника (посетителя) используется уникальный идентификатор, генерируемый приложением ***«PERCo.Доступ»*** (бесплатное, имеется на ресурсе «Google Play»). двумя способами:

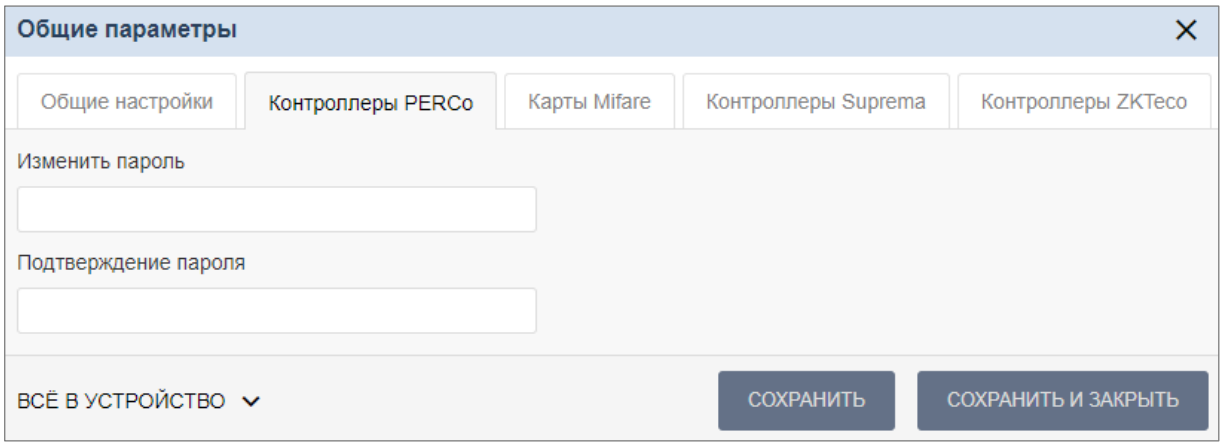
– либо случайным образом из следующих параметров смартфона: Build.BOARD, Build.BRAND, Build.CPU_ABI, Build.DEVICE, Build.MANUFACTURER, Build.MODEL, Build.PRODUCT (вероятность совпадения идентификаторов ничтожно мала);
– либо по желанию пользователя можно использовать *IMSI* – индивидуальный номер абонента, ассоциированный с SIM-картой смартфона, в этом случае приложение может запрашивать доступ к контактам телефона.

Подробное описание типа данных приведено на официальной странице ОС “*Android*” по адресу: https://developer.android.com/reference/android/os/Build.

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

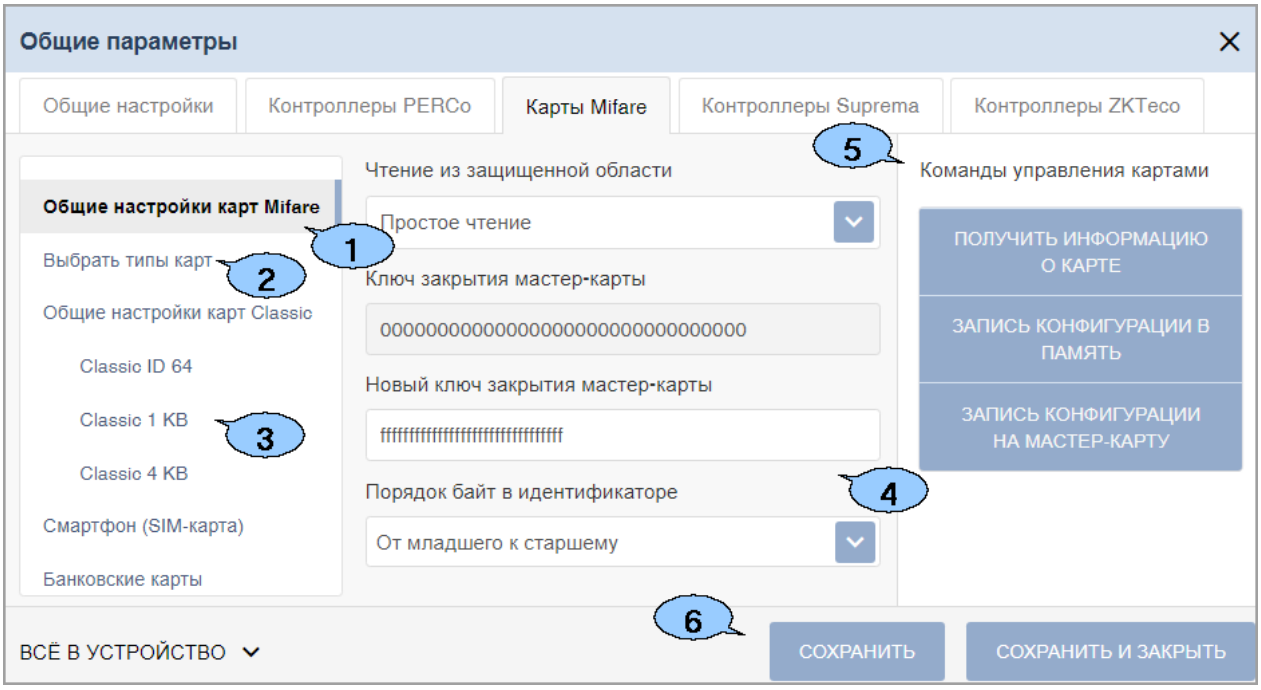
Уникальный идентификатор добавляется в систему аналогично другим картам.

7. Вкладка **Контроллеры PERCo** позволяет изменить общий пароль для доступа к контроллерам. Вкладка выглядит следующим образом:



- Для задания пароля введите в поле **Изменить пароль** новый пароль и подтвердите его в поле **Подтверждение пароля**.
- С помощью раскрывающегося списка в нижней части окна выберите способ сохранения параметров. Для завершения работы с окном **Общие параметры** нажмите кнопку **Сохранить**.

8. Вкладка **Карты Mifare** предназначена для настройки параметров работы с картами *Mifare*. Вкладка выглядит следующим образом:



1) Подвкладка **Общие настройки карт Mifare** – подвкладка предназначена для настройки общих параметров карт *Mifare*. Параметры общих настроек:
   - **Чтение из защищенной области** – определяет порядок работы с защищенной областью карт *Mifare*:
     – **Простое чтение** – чтение UID с карты;
     – **С записью карты** – чтение номера карты из защищенной области с последующей его перезаписью по заданному алгоритму генерации номера.

- **Ключ закрытия мастер-карты** – поле отображает текущий ключ закрытия мастер-карты.
- **Новый ключ закрытия мастер-карты** – поле позволяет ввести новый ключ закрытия мастер-карты.
- **Порядок байт в идентификаторе**:
  - **От старшего к младшему**;
  - **От младшему к старшему**.
- **Поля HID и EM-marine только для считывателя IR19 и контроллера замка CL211.9** – позволяет включить / отключить возможность работы со стандартами бесконтактных карт *HID* и *EM-Marine*. Если выбрать в полях параметр **Отключено**, считыватель ***IR19*** и контроллер замка ***CL211.9*** будут поддерживать только работу со стандартом *Mifare*.
  После настройки данного параметра запишите конфигурацию на мастер-карту.

2) Подвкладка **Выбрать тип карты** – позволяет выбрать форматы карт *Mifare* (смартфон, банковские карты), которые будут использоваться в СКУД. Для выбора доступны:
   - **Ultralight EV1 48 byte;**
   - **Ultralight EV1 128 byte;**
   - **Ultralight C 144 byte;**
   - **Classic ID 64;**
   - **Classic 1 KB;**
   - **Classic 4 KB;**
   - **Plus 2 KB;**
   - **Plus 4 KB;**
   - **Plus SE 1 KB;**
   - **DESFire;**
   - **МИР;**
   - **Смартфон (SIM-карта);**
   - **Банковские карты.**

   При выборе типа карты в левой части вкладки **Карты Mifare** появится область 3 со списком выбранных типов карт.
3) Область отображает выбранные типы карт *Mifare* (смартфон, банковские карты) в виде списка, позволяет переключаться между картами для конфигурации их параметров.
4) Область содержит список параметров, которые возможно конфигурировать для выбранного типа карты.

Примечание:
Список доступных **параметров карт** и **команд управления картам** меняется в зависимости от выбранного для конфигурирования типа карты.

5) Область **Команды управления картами** – область содержит список команд, доступных при работе с картами и контрольным считывателем:
   - **Запись конфигурации в память** – позволяет записать заданную для выбранных типов карт конфигурацию в энергонезависимую память контрольного считывателя;
   - **Запись конфигурации на мастер-карту** – позволяет записать заданную для выбранных типов карт конфигурацию на мастер-карту;

Примечание:
В качестве мастер-карт используются карты типа *Mifare DESFire*, которые также могут использоваться и в качестве простых карт.

   - **Изменить ключ** – команда позволяет записать измененные параметры для простых карт всех типов (*Ultralight, Classic, Plus, DESFire*). По команде считыватель определяет наличие карты в поле считывателя, ее тип, и изменяет **параметры карты** согласно параметрам, записанным в конфигурацию контрольного считывателя для данного типа карт;
   - **Получить информацию о карте** – позволяет прочесть информацию с выбранной карты. После успешного чтения карты во всплывающем окне **Информация о карте** будет отображена следующая информация:

- **Тип карты** – отображает тип карты *Mifare*;
- **UID** – отображает серию или номер уникального идентификатора пользователя;
- **Тип карты** – отображает тип карты: мастер-карта, простая карта;
- **Текущий уровень мастер-карты** – отображает текущий уровень мастер-карты (для карт *Mifare DESFire*);
- **Уровень безопасности** – отображает текущий уровень безопасности (для карт *Mifare Plus*).

- **Повысить уровень безопасности SL** – команда для всех типов карт *Mifare Plus* с SL1 и SL2, позволяет повысить уровень безопасности *SL* (*secure level*);

Примечание:

Работа с *SL2* не поддерживается. В случае использования карт с *SL2* рекомендуется переход на *SL3*.

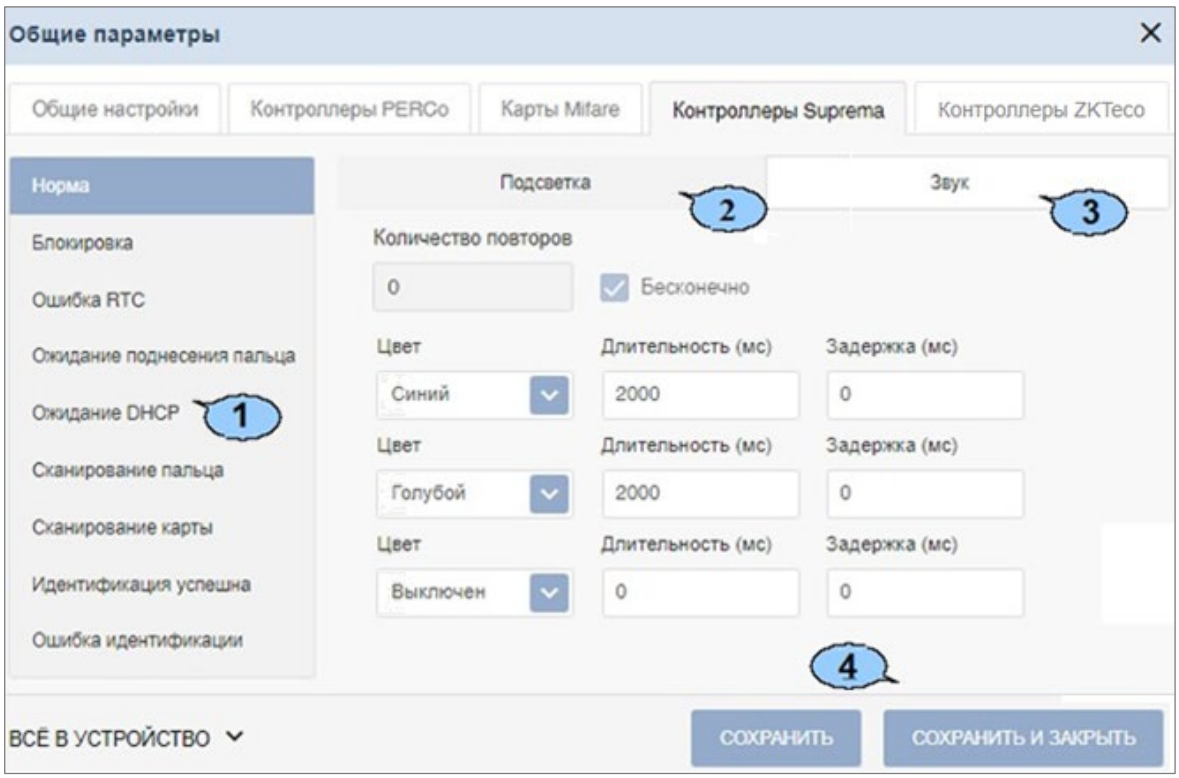
- **Форматировать** – применяется для простых карт типа *DESFire* (не мастер-карт) в том случае, если на карте уже записано несколько приложений и нет свободного места для создания нового приложения.

Примечания:

- Редактирование конфигурации карт *Mifare* в каждый момент времени может осуществляться только одним пользователем.
- В момент конфигурирования настроек карт *Mifare* блокируется работа со всеми контрольными считывателями системы (при попытке работы с контрольным считывателем всплывает окно с предупреждением «Идет изменение конфигурации»).
- Любое изменение конфигурации для карт *Mifare* сохраняется в базе данных системы только по факту успешной записи ее в контрольный считыватель, после чего она автоматически переписывается во все контрольные считыватели, подключенные в этот момент к СКУД.

6) Для сохранения внесенных изменений нажмите кнопку **Сохранить** или **Сохранить и закрыть**.

9. Вкладка **Контроллеры Suprema** позволяет настроить цветовую индикацию и звуковые сигналы контроллера для представленного списка событий. Вкладка выглядит следующим образом:



Примечание:

Изменение световой и звуковой индикации поддерживается только в контроллерах *Suprema* со сканерами отпечатков пальцев. В терминалах распознавания лиц световая и звуковая индикация не поддерживается.

1) **Список событий** – отображает список событий, для которых предусмотрена возможность настройки цветовой индикации и звуковых сигналов контроллера:
   - **Норма** – событие возникает в случае нормальной работы контроллера (режим работы **"Контроль"**);
   - **Блокировка** – событие возникает в случае блокировки контроллера (режим работы **"Закрыто"**);
   - **Ошибка RTC** (Real Time Clock) – событие возникает в случае несовпадения внутреннего времени контроллера со временем сети;
   - **Ожидание поднесения пальца** – событие возникает в случае, если был выбран тип прав доступа **Доступ по карте и пальцу** после предъявления карты;
   - **Ожидание DHCP** (Dynamic Host Configuration Protocol) – событие возникает в случае ожидания получения IP-адреса от DHCP-сервера;
   - **Сканирование пальца** – событие возникает в случае добавления отпечатков пальцев как идентификатора сотруднику или посетителю (если контроллер выбран как устройство для получения идентификатора);
   - **Сканирование карты** – событие возникает в случае добавления карты доступа как идентификатора сотруднику или посетителю (если контроллер выбран как устройство для получения идентификатора);
   - **Идентификация успешна** – событие возникает в случае успешной идентификации;
   - **Ошибка идентификации** – событие возникает в случае ошибки идентификации.
2) Область **Подсветка** – отображает параметры настройки световой индикации контроллера для выбранного события из списка событий:
   - **Бесконечно** – при установке флажка подсветка будет производиться бесконечно;
   - **Количество повторов** – счетчик позволяет задать количество повторений подсветки;

   Примечание:

   Параметры **Бесконечно** / **Количество повторов** являются взаимо-исключающими.

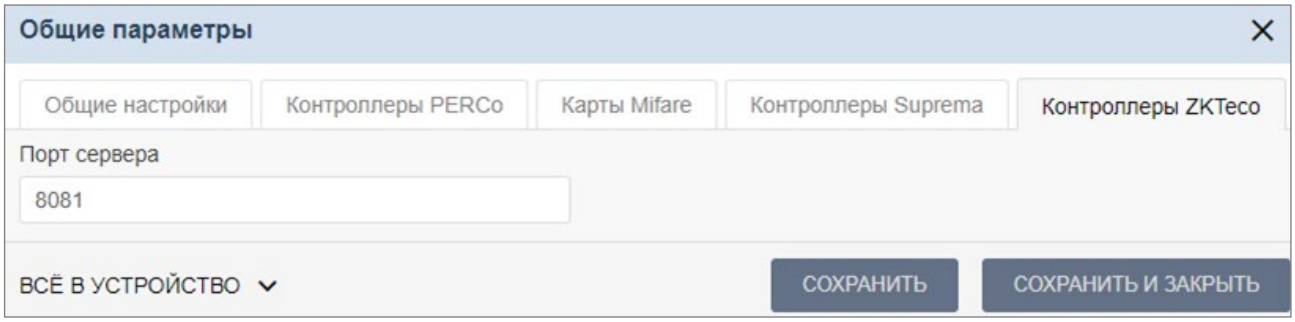
   - **Цвет** – параметр позволяет выбрать цвета индикации (не более трех);
   - **Длительность** – параметр позволяет задать длительность свечения индикации тем или иным цветом;
   - **Задержка** – параметр позволяет задать задержку перед началом свечения тем или иным цветом от начала цикла индикации.
3) Область **Звук** – отображает параметры настройки звуковых сигналов контроллера для выбранного события из списка событий:
   - **Бесконечно** – при установке флажка звук будет воспроизводиться бесконечно;
   - **Количество повторов** – счетчик позволяет задать количество повторений звучания;

   Примечание:

   Параметры **Бесконечно** / **Количество повторов** являются взаимо-исключающими.

   - **Тон** – параметр позволяет выбрать тон звучания;
   - **Длительность** – параметр позволяет задать длительность звучания индикации тем или иным тоном;
   - **Задержка** – параметр позволяет задать задержку перед началом звучания индикации тем или иным тоном от начала цикла индикации;
   - **Затухание** – при установке флажка происходит затухание звучания.
4) Для сохранения внесенных изменений нажмите кнопку **Сохранить** или **Сохранить и закрыть**.

10. Вкладка **Контроллеры ZKTeco** позволяет изменить **Порт сервера**, для терминалов распознавания лиц ***ZKTeco*** по умолчанию установлен порт 8081:



Примечание:

Убедитесь, что в брандмауэре установленный порт открыт для внешних подключений.

18.1.2.4. Порядок работы с картами Mifare

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

Примечание:

Карты *Mifare Ultralight* (кроме *Mifare Ultralight C*) не имеют защиты от копирования и по своим возможностям сопоставимы с обычными RFID-картами.

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

Внимание!

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

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

Основные характеристики разных чипов *Mifare*

Тип карты	**Mifare Ultralight**	**Mifare Classic ID 64/1KB/4KB**	**Mifare DESFire EV1 2K/4K/8K**	**Mifare Plus (S and X) 2K/4K**
Крипто-алгоритм	Нет	CRYPTO1	DES & 3DES/AES	CRYPTO1/AES
Длина серийного номера, байт	7	4/7	7	7
EEPROM, байт	64	1024/4096/4096	2048/4096/8192, гибкая файловая структура	2048/4096
Количество циклов перезаписи	10 000	100 000	500 000	200 000
Организация памяти	16 стр./4 байт	16 сект./ 64 байт, 32 сект./ 64 байт, 8 сект./ 256 байт	Определяется программно	32 сект./4 блока, 8 сект./1 блок

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

Примечание:

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

- **Уровень безопасности SL1**. На этом уровне карты *Mifare Plus* имеют 100%-ую совместимость с *Mifare Classic 1K (4K)*.
- **Уровень безопасности SL2**. Аутентификация по *AES* является обязательной. Для защиты данных используется *CRYPTO1.*

  Работа с *SL2* не поддерживается. В случае использования карт с *SL2* рекомендуется переход на *SL3.*
- **Уровень безопасности SL3**. Аутентификация, обмен данными, работа с памятью только по *AES*.

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

Чтобы защитить карту доступа *Mifare Classic 1KB (4KB)*, достаточно записать в один из блоков памяти идентификатор (например, ID длиной 3 байта для передачи по Wiegand-26) и закрыть доступ к этому блоку криптоключом, а считыватель вместо чтения UID-номера настроить на чтение ID-идентификатора из указанного блока памяти *Mifare Classic* с помощью такого же криптоключа, которым закрыта память карты.

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

1. Провести организационные мероприятия по предотвращению дискредитации ключевой информации.
2. Для карт *Mifare Plus* – выбрать уровень безопасности, на котором будут работать карты в данной СКУД: *SL1*, *SL2* или *SL3*. Тот или иной уровень должен быть выбран, исходя из специфики объекта и требований защищенности. Уровень *SL3* – самый высокий с точки зрения защиты.

Примечание:

Работа с *SL2* не поддерживается. В случае использования карт с *SL2* рекомендуется переход на *SL3*.

3. Провести подготовку считывателей. Каждый считыватель, подключаемый к контроллеру СКУД, должен быть запрограммирован на чтение данных из того же блока памяти и по тому же ключу *AES*, что и карта *Mifare*. При использовании считывателей ***PERCo*** необходимо через ПО настроить контрольный считыватель, записать мастер-карту и с ее помощью сконфигурировать все считыватели СКУД.
4. Эмиссия простых карт пользователей *Mifare* при помощи контрольного считывателя с интерфейсом USB ***PERCo-MR08***. Это запись идентификатора в соответствии с конфигурацией в выбранный сектор памяти *Mifare*, фактический перевод карт на выбранный уровень безопасности (*SL1*, *SL2* или *SL3* для *Mifare Plus*), закрытие выбранного сектора памяти секретным ключом с криптографией (*AES* или *CRYPTO1*). Этот идентификатор будет связан с конкретным работником и будет считываться в защищенном режиме.

Каждый тип карт *Mifare* (*Ultralight, Classic, Plus, DESFire,* смартфон с NFC, банковские карты) обладает определенным набором параметров, доступных для отображения или редактирования.

Примечание:

Поля с наименованиями типа **«Старый ключ аутентификации»**, **«Старый тип ключа аутентификации»** отображают текущие значения параметров конфигурации, записанной на контрольный считыватель ранее. Для записи в контрольный считыватель новых параметров конфигурации необходимо заполнить поля с наименованиями типа **«Ключ аутентификации»**, **«Тип ключа аутентификации»** после чего записать конфигурацию в контрольный считыватель.

Подвкладки **Ultralight**, **Общие настройки карт Classic**, **Общие настройки карт Plus**, **DESFire** позволяют задать рабочие параметры криптозащиты для соответствующих типов карт, отмеченных флажками в подвкладке **Выбрать типы карт**. Эти параметры будут задаваться простым картам пользователей при их эмиссии и персонализации с помощью контрольного считывателя, также эти параметры будут перенесены в конфигурацию считывателей на точках прохода с помощью мастер-карты.

Примечание:

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

Возможно конфигурирование параметров следующих типов карт:

- *Ultralight: EV1 48 bytes, EV1 128 bytes, C 144 bytes*;
- *Classic: ID64, 1KB, 4KB*;
- *Plus: 2KB, 4KB, SE1KB*;
- *DESFire*.

Подвкладки различных типов карт содержат следующие параметры криптозащиты:

- **Номер страницы, сектора, блока или приложения** – адрес в памяти карты, где будет храниться ID пользователя карты, используемый в СКУД.
- **Тип ключа аутентификации** – в поле отображается текущий тип ключа аутентификации мастер-карты.
- **Ключ аутентификации** – пароль, которым закрыт доступ к ID карты, отображается в формате Hex.
- **Старые параметры, Старый ключ аутентификации** – поля для отображения пароля доступа к ID и его характеристик, которые действуют до предстоящей переконфигурации параметров (при предыдущей конфигурации параметров они отображались в полях **Текущие параметры, Текущий ключ аутентификации**).
- **Текущие параметры, Текущий ключ аутентификации** – поля для отображения пароля доступа к ID и его характеристик, которые будут действовать после переконфигурации параметров (при следующей переконфигурации они будут отображены в полях **Старые параметры, Старый ключ аутентификации**).
- Для карт **Plus**, кроме того, имеются параметры, определяющие уровень безопасности (*SL1*, *SL2*, *SL3*).
- **Используемый идентификатор** – выпадающий список позволяет выбрать тип идентификатора для банковских карт: *PAN карты*, *ID Mifare Classic*, *ID приложения НСПК МИР*.

Внимание!

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

Алгоритм работы с защищенной областью памяти карт *Mifare* при записи в нее ID пользователя, который будет использоваться как номер карты для СКУД, на примере работы с картой *Mifare Classic 4KB*.

Для использования возможности чтения данных из защищенной области памяти необходимо выполнить ряд действий:

В первую очередь необходимо записать конфигурацию в контрольный считыватель. Для этого перейдите в раздел **«Администрирование» > «Конфигурация» > «Устройства»**. Выберите **Общие параметры** и нажмите кнопку  **Редактировать**. В открывшемся окне **Общие параметры:**

1 Перейдите на вкладку **Карты Mifare**.

2 Перейдите на подвкладку **Выбрать тип карты**. Установите флажок напротив карты **Mifare Classic 4KB**. Тип карты будет добавлен в список используемых карт в левой части вкладки **Карты Mifare**.
3 Перейдите на подвкладку **Mifare Classic 4KB** в левой части окна. Укажите **Номер сектора**. Он представляет собой часть памяти, в которую будет записан идентификатор и с которой он будет считываться при взаимодействии пользователя со СКУД. Номер выбирается произвольно.
4 Укажите **Номер блока**. Он представляет собой часть памяти, в которую будет записан идентификатор и с которой он будет считываться при взаимодействии пользователя со СКУД. Номер выбирается произвольно.
5 На вкладке **Карты Mifare** перейдите на подвкладку **Общие настройки карт Classic**.
6 В поле **Старый тип ключа для аутентификации** и поле **Старый ключ аутентификации** отображаются те параметры, которые были записаны на карту ранее.

Примечание:

Важно, чтобы значения параметров **Старый тип ключа для аутентификации** и **Старый ключ аутентификации** совпадали с типом ключа аутентификации и ключом аутентификации, которые записаны на карту в данный момент, иначе перезапись карты будет невозможна.

7. В поле **Тип ключа аутентификации** отображается текущий тип ключа аутентификации мастер-карты, то есть тип ключа, которым мастер-карта закрывалась ранее.
8 В поле **Ключ аутентификации** запишите новый ключ аутентификации, который будет использоваться в конфигурации как следующий ключ аутентификации.
9 Для записи новой конфигурации в память контроллера нажмите кнопку **Запись конфигурации в память**.

Далее необходимо записать конфигурацию из контроллера на мастер-карту. Для этого:

1. Приложите мастер-карту к контроллеру и нажмите кнопку **Запись конфигурации на мастер-карту**.

Примечание:

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

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

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

- Если простые карты пользователей, которые необходимо перепрограммировать, использовались ранее, то необходимо поднести карту к контрольному считывателю и нажать кнопку **Изменить ключ** в рабочей области вкладки **Карты Mifare**. На карту доступа запишутся изменения конфигурации.
- Если простые карты пользователей, которые необходимо перепрограммировать, не использовались ранее, то необходимо их персонифицировать, т.е. выдать им идентификатор. Это можно сделать в разделе «**Персонал» > «Сотрудники»** или в разделе «**Бюро пропусков» > «Сотрудники»** с помощью кнопки  **Выдать карту**.

При конфигурировании контрольного считывателя необходимо задать желаемые параметры карт. Параметры зависят от типа карты и подразделяются на:

- **Номер страницы, блока, сектора или приложения** – место, где будет храниться номер карты, используемый в СКУД.
- **Типы и ключи для аутентификации** – типы паролей и пароли, позволяющие получить доступ к карте.

- **Ключи для изменения уровня безопасности (SL)** – служебные пароли, позволяющие получить доступ изменению конфигурации карты, есть только у *Mifare Plus*.
- **Типы и ключи для доступа к данным на карте** – дополнительные пароли, позволяющие получить доступ к данным на карте, есть только у *Mifare DESFire*.

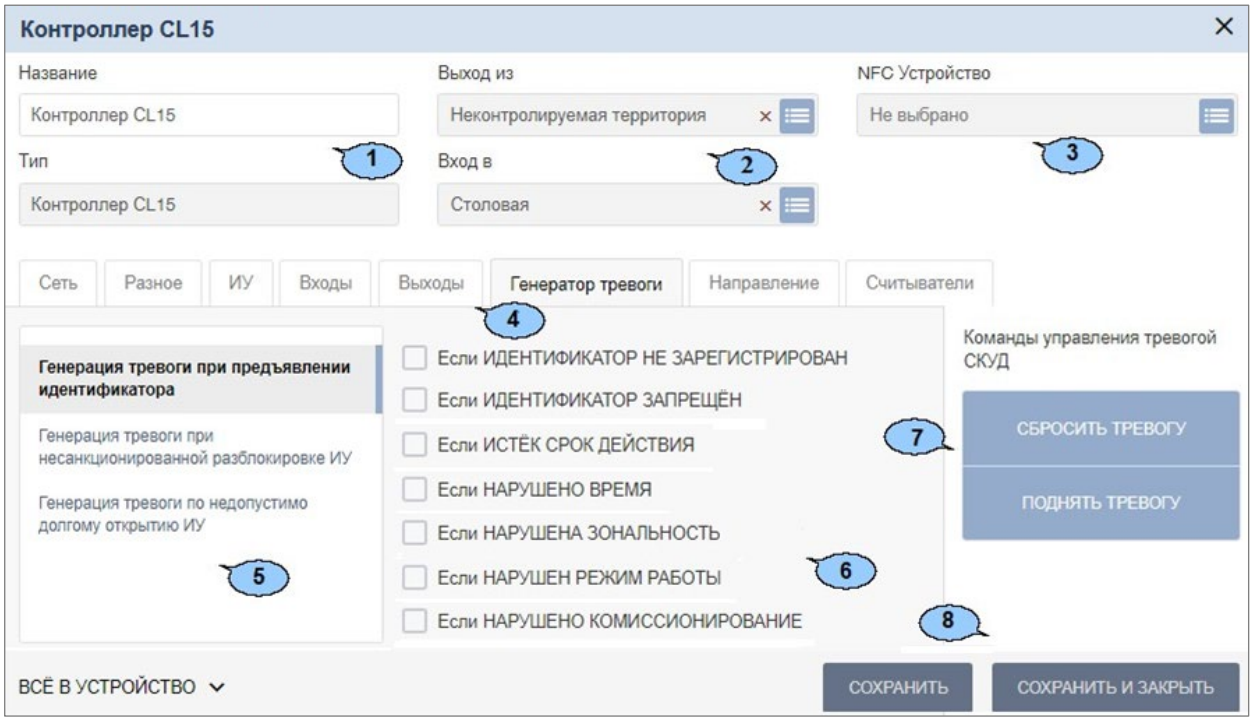
При необходимости изменения конфигурации необходимо повторить все действия, начиная с п.1, при этом учитывая, что:

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

18.1.2.5. Настройка параметров устройства

Для настройки общих параметров устройства (ИУ, контроллера, видеокамеры):

1. Используя панель навигации, перейдите в раздел  **«Администрирование»**.
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **Устройства**.
4. Выделите в рабочей области страницы настраиваемое устройство.
5. Нажмите на панели инструментов страницы кнопку  **Редактировать** или дважды кликните на строке с ИУ, после чего откроется окно с названием ИУ:



Элементы окна:

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

   - Поле **Выход из** – кнопка  справа от поля позволяет выбрать помещение, доступ в которое осуществляется через считыватель № 1. Кнопка **Сбросить** позволяет

удалить из поля выбранное ранее помещение.

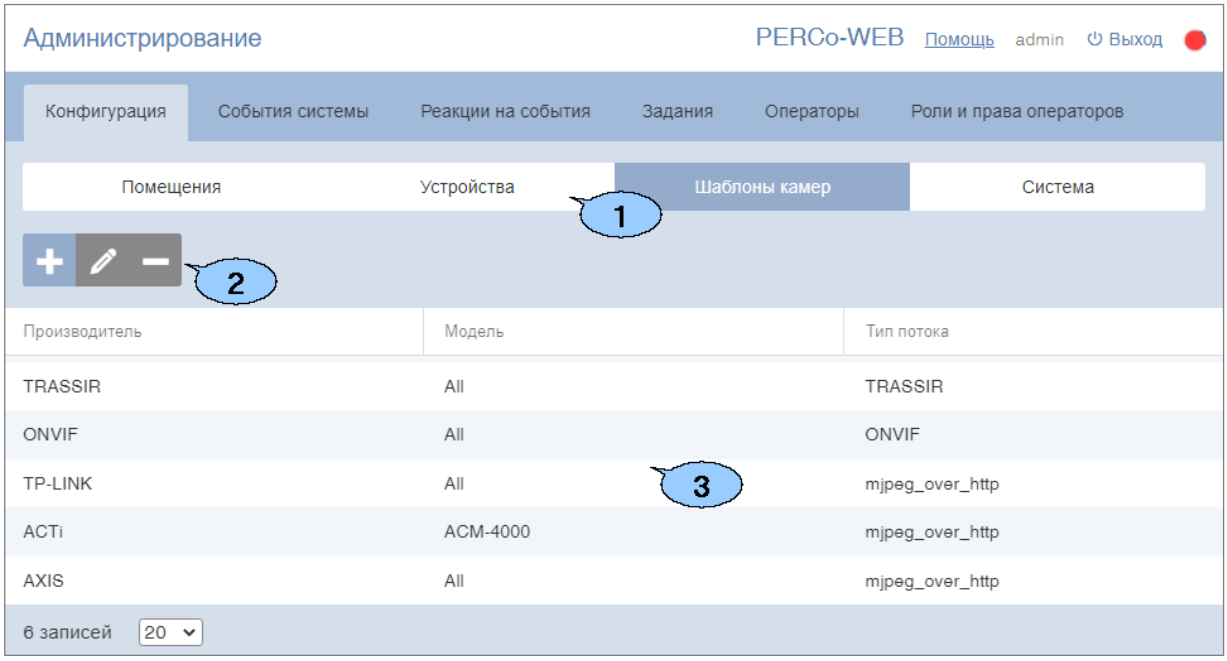
- Поле **Вход в** – кнопка справа от поля позволяет выбрать помещение, доступ в которое осуществляется через считыватель № 2. Кнопка **Сбросить** позволяет удалить из поля выбранное ранее помещение.

3) Поле **NFC Устройство** – кнопка справа от поля позволяет выбрать добавленное раннее устройство с поддержкой технологии NFC, чтобы использовать его в качестве имитации настраиваемого считывателя.
4) Выбор вкладки ресурса. В зависимости от типа устройства список ресурсов и соответствующих им вкладок может отличаться.
5) Параметры, доступные для данного ресурса.
6) Возможные значение и варианты настройки выделенного параметра ресурса.
7) Кнопки команд управления, доступных для выбранного ресурса. Для оперативного управления устройствами предназначен подраздел **«Управление устройствами»** раздела **«Контроль доступа»**.
8) 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 устройство** – в устройство передаются все параметры.
   - **Измененные в устройство** – в устройство передаются только измененные параметры.

18.1.3. Вкладка «Шаблоны камер»

Шаблон параметров видеокамеры используется при добавлении новой камеры в систему в разделе **«Конфигурация»** в подразделе **«Устройства»**. По умолчанию в системе уже установлены шаблоны параметров для видеокамер стандарта ONVIF и для видеокамер популярных производителей (TP-LINK, ACTi, AXIS).

Страница вкладки имеет следующий вид:



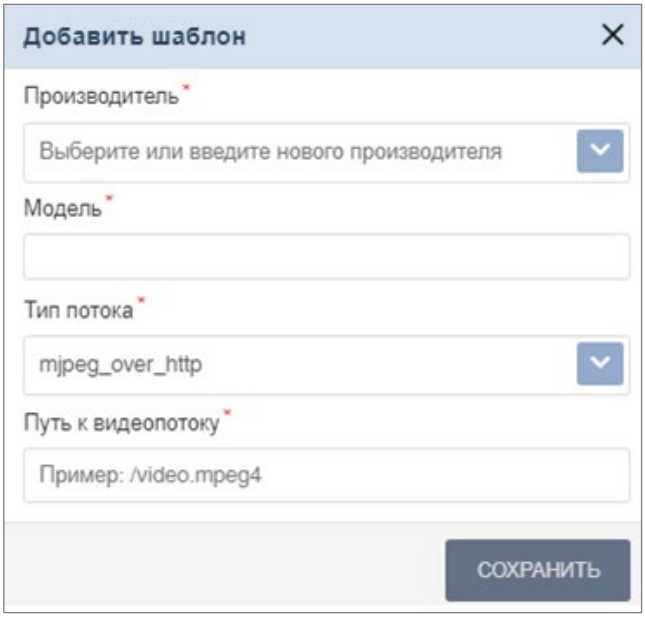
1. Переключатель выбора вкладки подраздела:
   - **Помещения**;
   - **Устройства**;
   - **Шаблоны камер**;
   - **Система**.

2. Панель инструментов страницы содержит:
   - **Добавить** – кнопка позволяет создать новый шаблон камеры.
   - **Редактировать** – кнопка позволяет изменить выделенный в рабочей области страницы шаблон камеры.
   - **Удалить** – кнопка позволяет удалить выделенный в рабочей области страницы шаблон камеры.
3. Рабочая область страницы содержит список созданных шаблонов камер, информацию о производителе, модели и типе видеопотока.

18.1.3.1. Создание шаблона камеры

Для создания нового шаблона камеры:

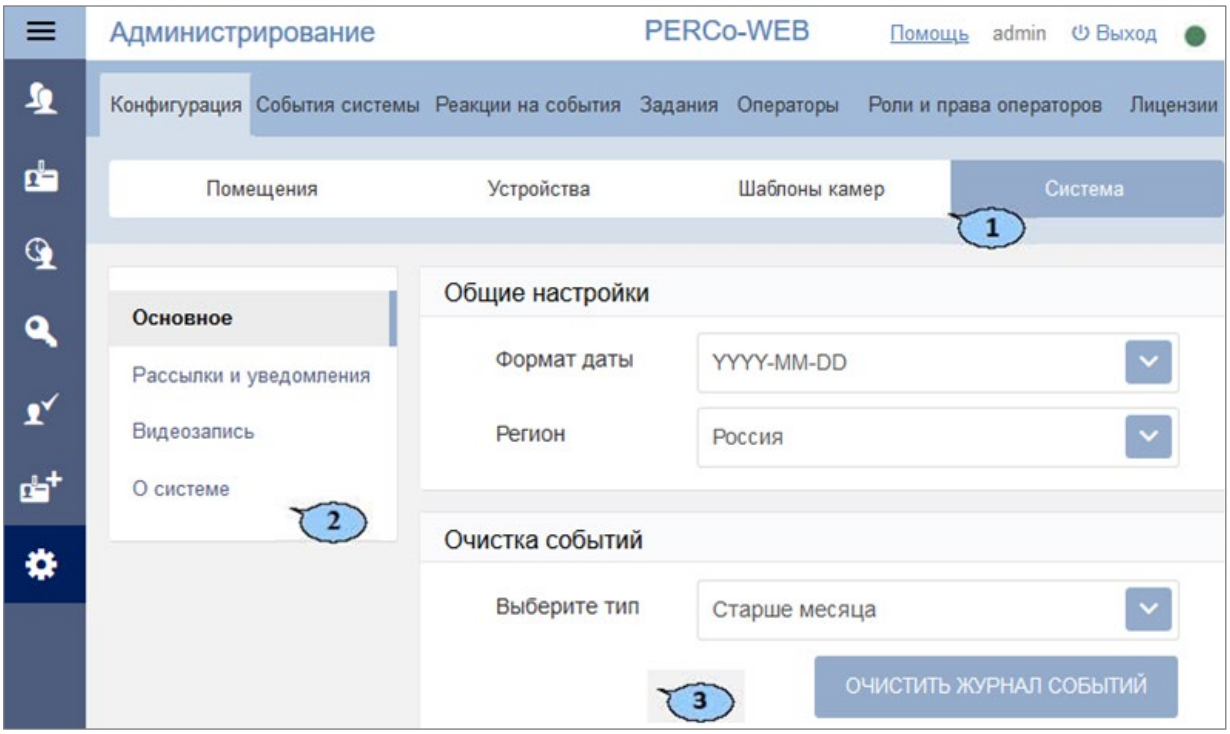
1. Используя панель навигации, перейдите в раздел **«Администрирование»**.
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **Шаблоны камер**.
4. Нажмите на панели инструментов страницы кнопку **Добавить**.
   Откроется окно **Добавить шаблон**:



5. В открывшемся окне произведите настройку параметров шаблона. Нажмите кнопку **Сохранить**. Окно **Добавить шаблон** будет закрыто, новый шаблон будет добавлен в рабочую область страницы.

18.1.4. Вкладка «Система»

Страница вкладки имеет следующий вид:



1. Переключатель выбора вкладки подраздела:
   - **Помещения**;
   - **Устройства**;
   - **Шаблоны камер**;
   - **Система**.
2. Панель содержит подвкладки:
   - **Основное**;
   - **Рассылки и уведомления**;
   - **Видеозапись**;
   - **О системе**.
3. Рабочая область страницы, вид зависит от выбранной подвкладки.

18.1.4.1. Подвкладка «Основное»

Подвкладка **Основное** предназначена для выбора региона, формата даты, очистки журнала событий системы.

Общие настройки (см. рисунок выше):

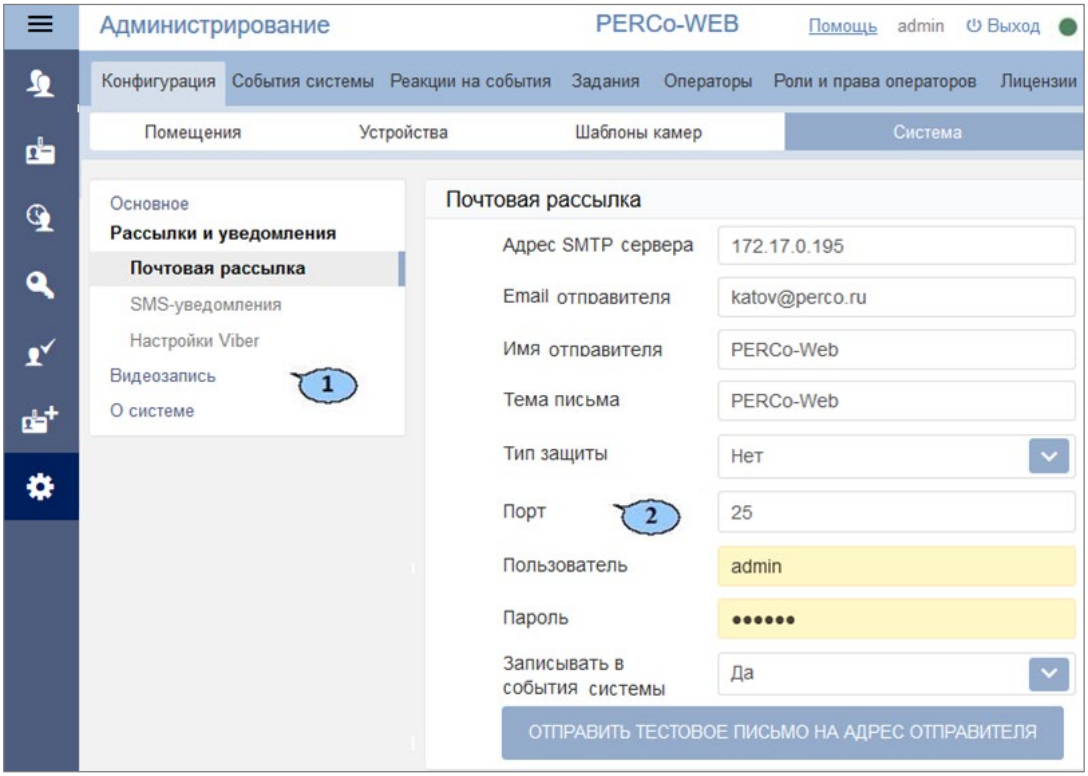
- **Формат даты** – поле содержит выпадающий список, который позволяет задать формат времени для отображения:
- **Регион** – поле содержит выпадающий список, который позволяет выбрать регион.

Очистка событий:

- **Выберите тип** – поле содержит выпадающий список, который позволяет удалить события системы за выбранный период времени. Доступны следующие типы:
  - **Старше месяца**;
  - **Старше трех месяцев**;
  - **Старше полугода**;
  - **Старше года**;
  - **Очистить все**, **кроме последних 50000**.

18.1.4.2. Подвкладка «Рассылки и уведомления»

Подвкладка **Рассылки и уведомления** предназначена для настройки почтовых рассылок. Окно имеет следующий вид:



1. Переключатель выбора способа рассылки:
   - **Почтовая рассылка**;
   - **SMS-уведомления**;
   - **Настройки Viber**.
2. Вид рабочей области страницы зависит от выбранного способа рассылки.

18.1.4.3. Добавление параметров почтовой рассылки

В поле подвкладки **Почтовая рассылка** задаются параметры для выполнения заданий по массовой или выборочной рассылке сотрудникам отчетов, формируемых в системе:

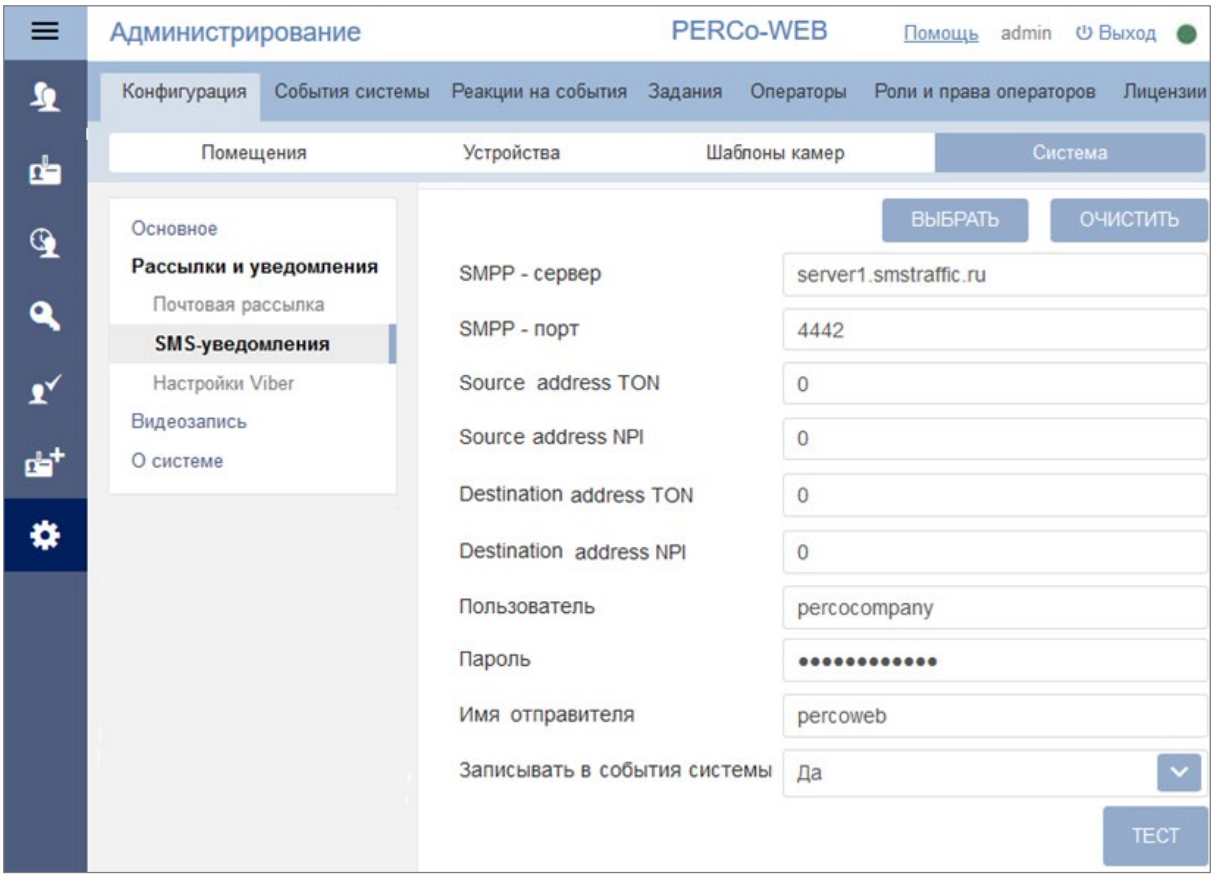
- **Адрес SMTP-сервера**, **Email отправителя** – поля для ввода адреса почтового сервера и адреса почтового ящика, с которого системой будет производиться рассылка почтовых отправлений;
- **Имя отправителя**, **Тема письма** – данные, которые будут отображаться в сообщениях, рассылаемых системой (по умолчанию ***PERCo-Web***);
- **Тип защиты** – определяется тип шифрования почтовых отправлений (**Нет**, **SSL**, **TLS**);
- **Порт** – номер порта. Определяется почтовым сервером (зависит от типа шифрования, узнать можно на сайте почтового сервиса);
- **Пользователь**, **Пароль** – логин и пароль почтового ящика отправителя, используемого системой;
- **Записывать в события системы** – возможны значения **Нет**, **Да**, **Ошибки**, в соответствии с которыми в системе будут записываться события почтовой рассылки;
- Кнопка **Отправить тестовое письмо на адрес отправителя** позволяет проверить актуальность почтового ящика системы.

Примечание:

Если параметры почтовой рассылки были введены некорректно, при отправке тестового письма отобразится сообщение об ошибке.

18.1.4.4. Добавление параметров рассылки SMS-уведомлений

В поле подвкладки **SMS-уведомления** задаются параметры для выполнения заданий по рассылке системой SMS-уведомлений сотрудникам:



- Кнопки **Выбрать** и **Очистить** позволяют выбрать / удалить Web-провайдера из списка возможных (открывается при нажатии на кнопку **Выбрать**). С данным провайдером заранее должен быть оформлен договор на осуществление SMS-рассылки;

Внимание!

Услуга отправки SMS-уведомлений обычно является платной, размер платы устанавливается выбранным SMS-провайдером.

- **SMPP-сервер, SMPP-порт, Source address TON, Source address NPI, Destination address TON**, **Destination address NPI** – параметры SMS-провайдера для осуществления SMS-рассылки, устанавливаются автоматически при выборе провайдера (могут быть изменены, при необходимости уточняйте у провайдера);

Примечание:

Список SMS-провайдеров, чьи параметры устанавливаются автоматически, выложен на сайте ***PERCo***: www.perco.ru/podderzhka/programmnoe-obespechenie.php. Имеется возможность ввести параметры другого SMS-провайдера, не из предложенного списка, но при этом все значения данных параметров придется вводить вручную.

- **Пользователь**, **Пароль** – логин и пароль учетной записи клиента SMS-провайдера, устанавливаются в личном кабинете на сайте провайдера;
- **Имя отправителя** – указывается имя отправителя, может быть любым (если не указывать, то определяется SMS-провайдером);
- **Записывать в события системы** – возможны значения **Нет**, **Да**, **Ошибки**, в соответствии с которыми в системе будут записываться события рассылки SMS-уведомлений;
- Кнопка **Тест** – позволяет отправить тестовое SMS-сообщение. Номер телефона получателя и тестовый текст набираются во всплывающем окне после нажатия кнопки.

Примечание:

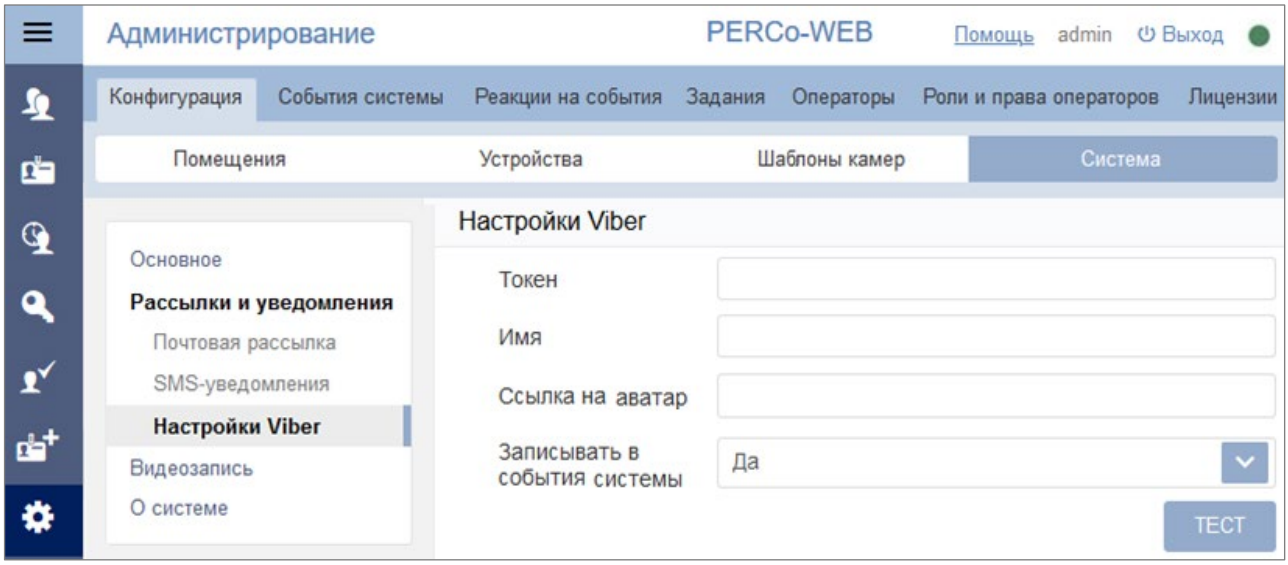
Если параметры SMS-рассылки были введены некорректно, при отправке тестового уведомления отобразится сообщение об ошибке.

18.1.4.5. Добавление параметров рассылки в Viber

Внимание!

Для отправки сообщений в *Viber* заранее должен быть создан паблик-аккаунт и на смартфоны сотрудников – получателей уведомлений установлено приложение *Viber*.

В поле подвкладки **Настройки Viber** задаются параметры для выполнения заданий по рассылке системой уведомлений сотрудникам:



- **Токен** – поле для ввода токена (числа-идентификатора), полученного при регистрации паблик-аккаунта Viber;
- **Имя** – указывается имя отправителя;
- **Записывать в события системы** – возможны значения **Нет**, **Да**, **Ошибки**, в соответствии с которыми в системе будут записываться события рассылки;
- Кнопка **Тест** – позволяет проверить правильность настройки параметров.

Примечание:

Если параметры SMS-рассылки были введены некорректно, при нажатии на кнопку отобразится сообщение об ошибке.

18.1.4.6. Порядок создания паблик-аккаунта Viber

1. Скачайте и установите приложение Viber на телефон администратора.
2. По ссылке: https://partners.viber.com/ перейдите на **Панель администратора Viber**:
   - в правом верхнем углу выберите язык: русский/английский.
   - введите номер телефона администратора, нажмите на кнопку **Войти** и введите код доступа, полученный через приложение Viber.

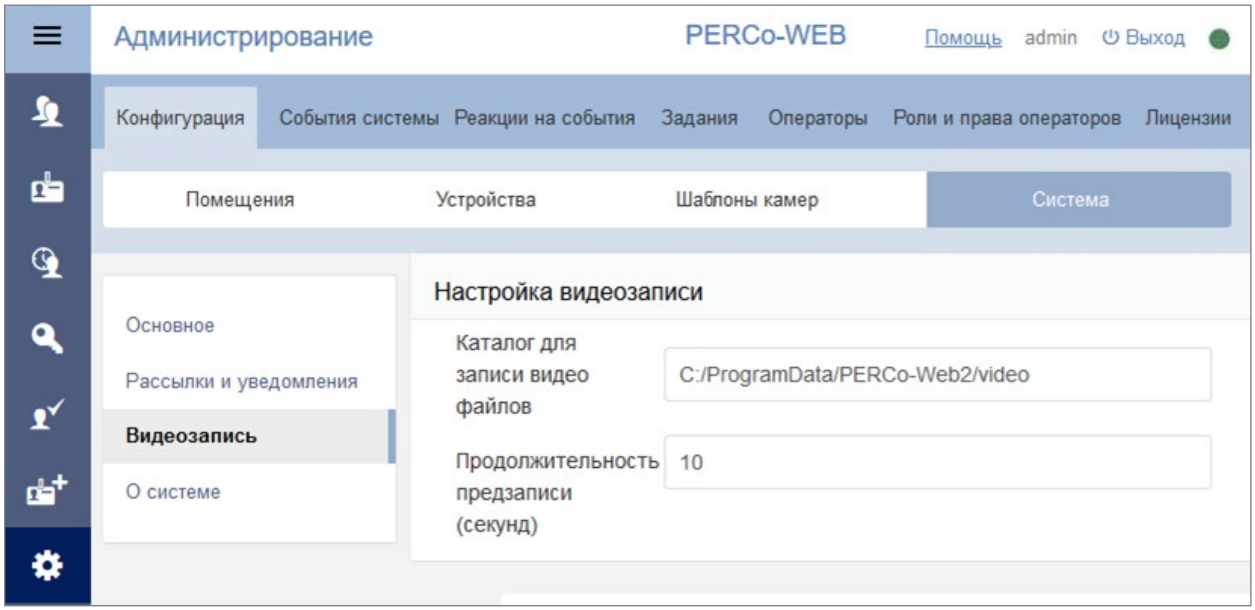
   Откроется окно управления паблик-аккаунтом.
3. В окне управления паблик-аккаунтом нажмите на кнопку **Создать бот**. В анкете заполните учетные данные паблик-аккаунта: название, *URL* адрес, описание, адрес электронной почты, категорию, подкатегорию, язык, локацию; выберите аватар аккаунта. Нажмите кнопку **Create**. Сформируется паблик-аккаунт, автоматически сгенерируется токен аккаунта.
4. Скопируйте токен в буфер обмена и введите его в поле ввода **Токен** в подвкладке **Настройка Viber** (вкладка **Система** подраздела **«Конфигурация»** раздела **«Администрирование»** ПО ***PERCo-Web***). В поле **Имя** укажите имя, от которого будут отправляться сообщения и уведомления.

5. В приложении Viber перейдите в меню **Еще** и с помощью сканера штрихкода зайдите в созданный паблик-аккаунт:
   - с помощью кнопки **Пригласить участников** пригласите в чат сотрудников, которые будут получать уведомления (номера их телефонов, привязанные к Viber-аккаунтам, должны быть предварительно записаны в списке контактов телефона администратора);
   - сотрудники, получившие приглашение в паблик-аккаунт, должны принять приглашение (при этом каждому необходимо будет принять соглашение по возрастным ограничениям);
   - с помощью кнопки **Изменить** в поле **Администраторы** добавьте в паблик-аккаунт данных сотрудников в качестве администраторов.
6. В ПО ***PERCo-Web*** (раздел **«Персонал»**, подраздел **«Сотрудники»**, вкладка **Действующие**):
   - в учетных карточках приглашенных сотрудников на подвкладке **Дополнительные поля** в поле **Viber** при помощи кнопки из общего списка выберите и закрепите за каждым сотрудником его Viber-аккаунт;
   - с помощью кнопки **Отправить сообщение по Viber** проверьте отправку системой сообщений каждому из сотрудников, в случае неудачи на экран будет выведено сообщение об ошибке.

18.1.4.7. Подвкладка «Видеозапись»

Подвкладка **Видеозапись** предназначена для настройки параметров видеозаписи.

Окно имеет следующий вид:



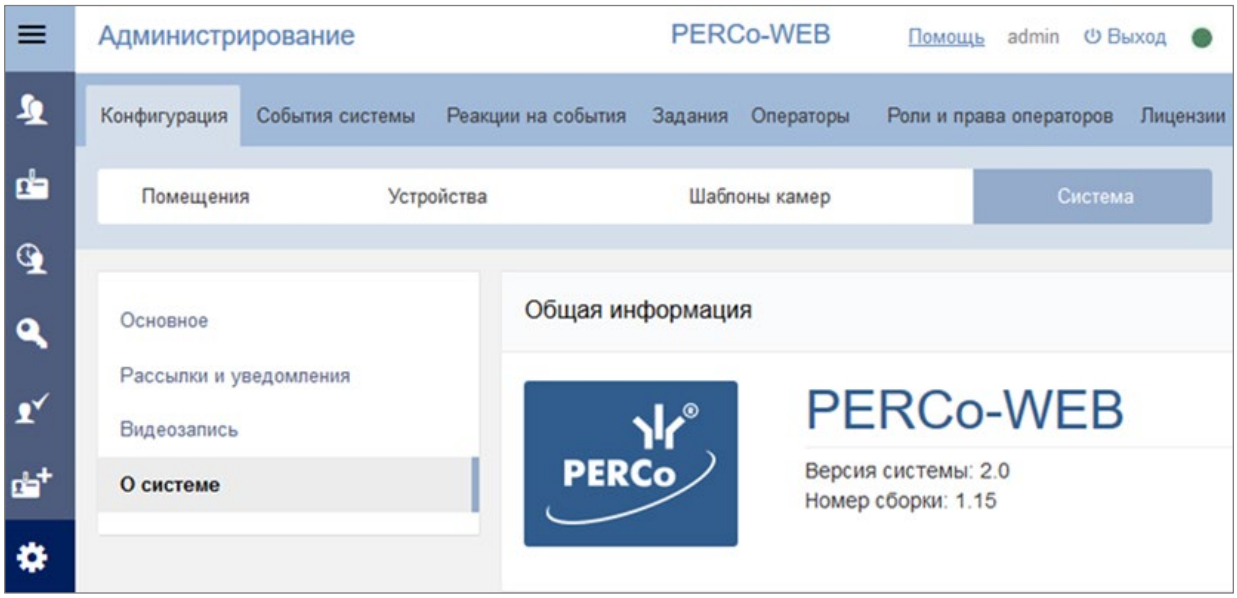
Доступны следующие настройки:

- **Каталог для записи видеофайлов** – позволяет задать путь к папке, в которой будут храниться все записанные видеофайлы.
- **Продолжительность предзаписи (секунд)** – позволяет задать время предзаписи видео в секундах.

18.1.4.8. Подвкладка «О системе»

Подвкладка **О системе** предназначена для просмотра версии программного обеспечения системы.

Окно имеет следующий вид:

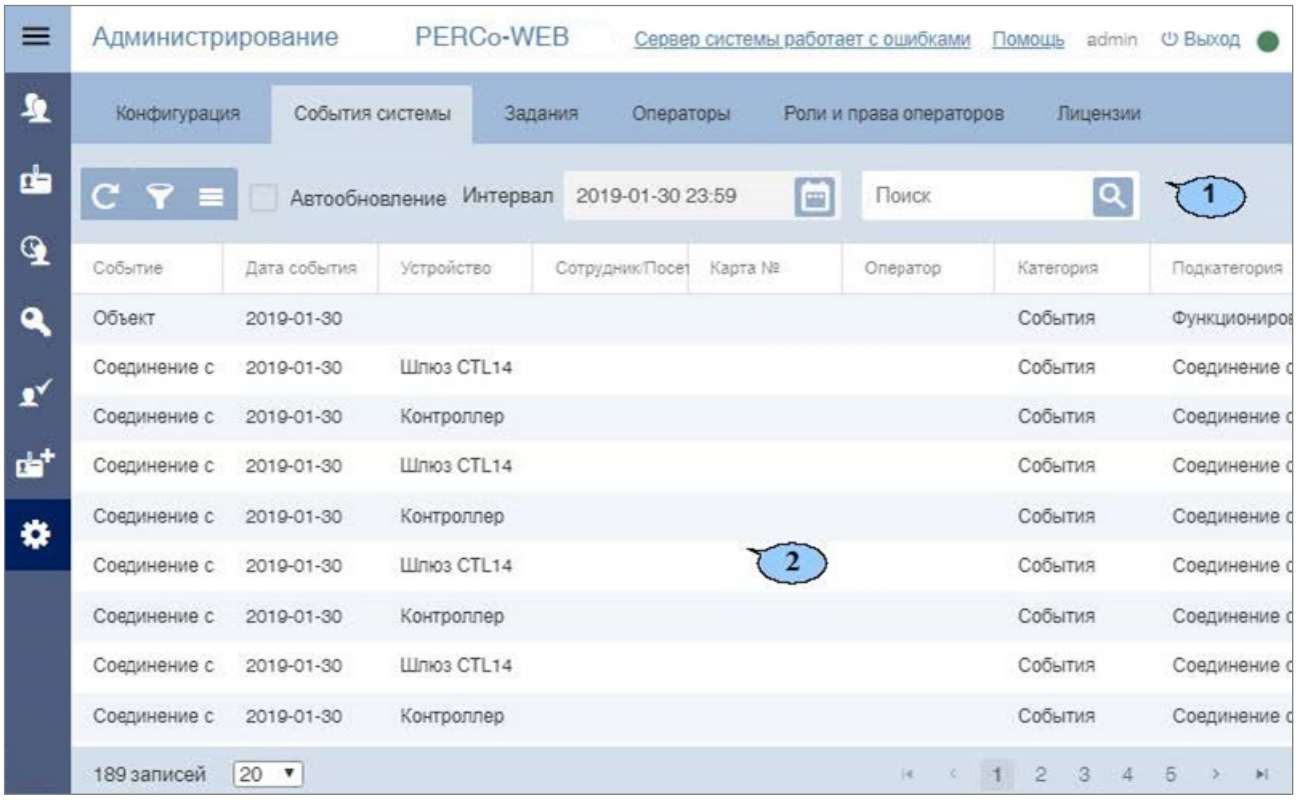


18.2. Подраздел «События системы»

Подраздел предназначен для:

- составления 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. Панель инструментов подраздела содержит:
   - **Обновить данные** – кнопка позволяет обновить данные в рабочей области в соответствии с установленным фильтром.
   - **Расширенный поиск** – позволяет применить фильтр к элементам, отображаемым в рабочей области страницы.
   - **Дополнительно** – кнопка позволяет открыть меню команд для выбора дополнительных действий:
     - **Печать таблицы** – позволяет произвести печать данных из рабочей области страницы.
     - **Экспорт** – позволяет сохранить список событий в файл электронных таблиц с выбранным расширением.
     - **Сбросить фильтры** – позволяет сбросить все фильтры рабочей области.
     - **Параметры отображения таблицы** – позволяет открыть дополнительное окно для выбора столбцов, отображаемых в рабочей области страницы.
   - **Автообновление** – при установке флажка регистрируемые в системе события отображаются в рабочей области в режиме реального времени.
   - – кнопка позволяет 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.
   - Поле **Поиск** – кнопка справа от поля **Поиск** позволяет произвести поиск по элементам столбцов в рабочей области страницы. Кнопка **Сбросить** позволяет очистить поле.
2. Рабочая область подраздела содержит события, зарегистрированные устройствами системы за указанный на панели инструментов период.

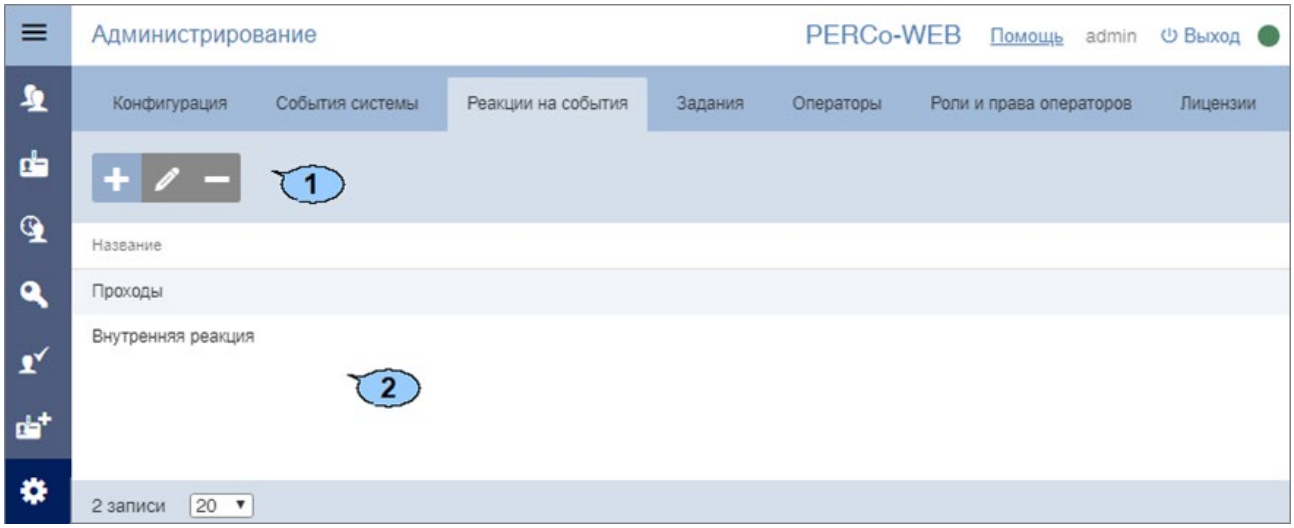
Примечания:

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

18.3. Подраздел «Реакция на события»

Подраздел предназначен для настройки реакций на события системы ***PERCo-Web***.

Страница подраздела имеет следующий вид:



1. Панель инструментов подраздела содержит кнопки:
   - **Добавить** – позволяет добавить реакцию на событие или внутреннюю реакцию на событие контроллера.
   - **Редактировать** – позволяет изменить параметры выбранной реакции.
   - **Удалить** – позволяет удалить выделенную в рабочей области страницы реакцию.
2. Рабочая область подраздела содержит список созданных реакций.

18.3.1. Добавление новой реакции

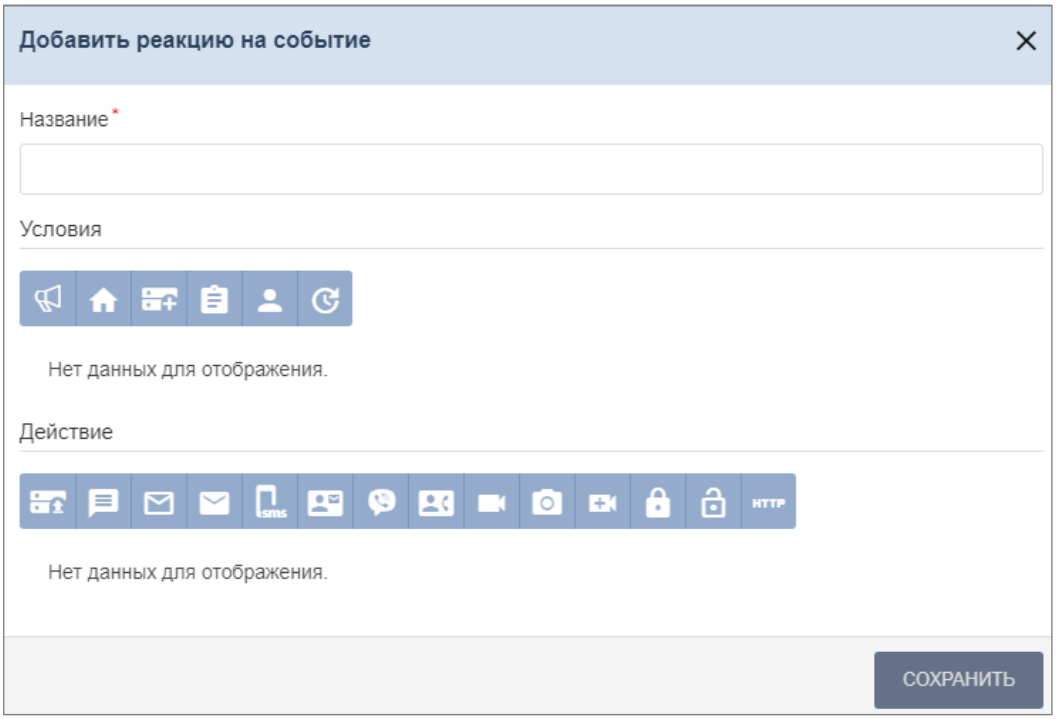
Примечание:

Для настройки оповещения системой ***PERCo-Web*** о выполнении реакций на события следует убедиться, что в *учетной карточке сотрудника* заполнены поля **Email** / **Телефон** / **Viber**. Для отправки сообщений в Viber должен быть создан паблик-аккаунт, в подвкладке **«Рассылки и уведомления»** заполнены соответствующие поля, а на смартфон сотрудника установлено приложение Viber.

Для добавления новой реакции на событие:

1. Используя панель навигации, перейдите в раздел **«Администрирование»**.
2. Откройте подраздел **«Реакции на события»**.
3. Нажмите на панели инструментов страницы кнопку **Добавить**, а затем **Добавить реакцию на событие**.

   Откроется окно, имеющее следующий вид:



4. В поле **Название** введите название для новой реакции.
5. В поле **Условия** выберите условия для новой реакции. Окна некоторых событий имеют выпадающий список в левом нижнем углу, который позволяет выбрать вариант **Содержит** или **Не содержит** реакция выбранное условие. В поле доступны следующие кнопки:
   - **Добавить событие** – позволяет открыть окно, в котором отображается список возможных событий для реакции, и добавить нужное событие.

-  **Добавить помещение** – позволяет открыть окно, в котором отображается список созданных ранее помещений, и добавить нужное помещение.
-  **Добавить устройство** – позволяет открыть окно, в котором отображается список добавленных в конфигурацию системы устройств, и добавить нужное устройство.
-  **Добавить подразделение** – позволяет открыть окно, в котором отображается список созданных ранее подразделений, и добавить нужное подразделение.
-  **Добавить сотрудника** – позволяет открыть окно, в котором отображается список добавленных ранее сотрудников, и добавить нужного сотрудника.
-  **Добавить ограничение по времени** – позволяет открыть окно, в котором есть возможность выбора даты и времени выполнения реакции: **Дни недели** или определенная **Дата**, а также **Время начала** и **Время окончания**.

6. В поле **Действие** выберите те действия, которые будут происходить при заданных условиях. Поле содержит следующие кнопки:
   -  **Команда в устройство** – позволяет выбрать команду для устройства, добавленного в конфигурацию системы ***PERCo-Web***. Для этого выберите устройство, а затем из выпадающего списка в левом нижнем углу команду для него. Нажмите кнопку **Сохранить**.
   -  **Сообщение оператору** – позволяет настроить отправку сообщений оператору системы. Для этого выберите оператора, заполните поле в окне **Текст сообщения** и нажмите кнопку **Сохранить**.
   -  **Сообщение по почте предъявившему идентификатор** – позволяет настроить отправку сообщений по электронной почте предъявившему идентификатор. Для этого заполните поле в окне **Текст сообщения** и нажмите кнопку **Сохранить**.
   -  **Сообщение по почте сотруднику** – позволяет настроить отправку сообщений по электронной почте сотруднику при выполнении системой реакции на событие. Для этого выберите сотрудника, заполните поле в окне **Текст сообщения** и нажмите кнопку **Сохранить**.
   -  **SMS-сообщение предъявившему идентификатор** – позволяет настроить отправку SMS-сообщений предъявившему идентификатор. Для этого заполните поле в окне **Текст сообщения** и нажмите кнопку **Сохранить**.
   -  **SMS-сообщение сотруднику** – позволяет настроить отправку SMS-сообщения сотруднику при выполнении системой реакции на событие. Для этого выберите сотрудника, заполните поле в окне **Текст сообщения** и нажмите кнопку **Сохранить**.
   -  **Viber-сообщение предъявившему идентификатор** – позволяет настроить отправку сообщений в мессенджер Viber предъявившему идентификатор. Для этого заполните поле в окне **Текст сообщения** и нажмите кнопку **Сохранить**.
   -  **Viber-сообщение сотруднику** – позволяет настроить отправку сообщений сотруднику в мессенджер Viber при выполнении системой реакции на события. Для этого выберите сотрудника, заполните поле в окне **Текст сообщения** и нажмите кнопку **Сохранить**.
   -  **Показать видеокамеру оператору** – позволяет настроить для оператора отображение видеокамеры. Для этого выберите оператора и нужную камеру, затем нажмите кнопку **Сохранить**.

- **Сохранить снимок с камеры** – позволяет сделать снимок экрана при выполнении системой реакции на событие. Для этого выберите камеру и нажмите кнопку **Сохранить**.

Примечание:

Чтобы просмотреть сделанный снимок, перейдите в раздел **Администрирование > События системы** и выберите из списка нужное событие.

- **Включить запись видео** – позволяет включить запись видео в процессе выполнения реакции на событие. Окно имеет выпадающий список в левом нижнем углу, который позволяет выбрать время записи (по умолчанию это 10 секунд). Для того, чтобы включить запись видео, необходимо выбрать камеру и нажать кнопку **Сохранить**.

Примечание:

Для того, чтобы настроить продолжительность предзаписи видео при выполнении реакции на событие (по умолчанию это 10 секунд), перейдите в раздел **Администрирование > Конфигурация > Система > Видеозапись**. Чтобы просмотреть записанное видео, перейдите в раздел **Администрирование > События системы** и выберите из списка нужное событие.

- **Заблокировать сотрудника** – позволяет заблокировать сотрудника, для которого было выполнено то или иное условие.
- **Разблокировать сотрудника** – позволяет разблокировать сотрудника, для которого было выполнено то или иное условие.
- **Выполнить http-запрос** – позволяет выполнить указанный http или https-запрос с типом POST. При его выполнении в теле запроса передается JSON-объект, содержащий следующие параметры:

  id – идентификатор события;
  time_label – дата и время события в формате YYYY-MM-DD HH:mm:SS;
  event_type – тип события;
  user_id – идентификатор пользователя;
  device_id – идентификатор устройства;
  resource_number – номер ресурса устройства;
  access_zone_id1 – идентификатор помещения входа;
  access_zone_id2 – идентификатор помещения выхода.

Например, если задана строка запроса http://127.0.0.1:50005, то получение события с помощью сервера на NodeJS может иметь следующий вид:

```
var server = http.createServer((req, res) => {
var event = '';
req.on('data', (data) => {
event += data;
});
req.on('end', async () => {
res.setHeader("Content-Type", "application/json");
res.setHeader('Access-Control-Allow-Origin', '*');
res.setHeader('Access-Control-Allow-Methods', 'GET, POST, OPTIONS, PUT, PATCH, DELETE');
res.setHeader('Access-Control-Allow-Headers', 'X-Requested-With,content-type');
if (event.length) {
console.log(`Event from PERCo-Web`,JSON.parse(event));
res.write('{"result":"ok"}');
}
res.end();
```

```
});
});
server.listen(50005, '0.0.0.0', (err) => {
if (err) console.log('Test server error', err);
else console.log('Test server started');
});
```

Примечание:
Функция предназначена для пользователей, обладающих достаточной квалификацией в области IT.

7. Нажмите кнопку **Сохранить**. Окно **Добавить реакцию на событие** будет закрыто, а новая реакция появится в рабочей области страницы.

18.3.2. Добавление внутренней реакции на событие контроллера

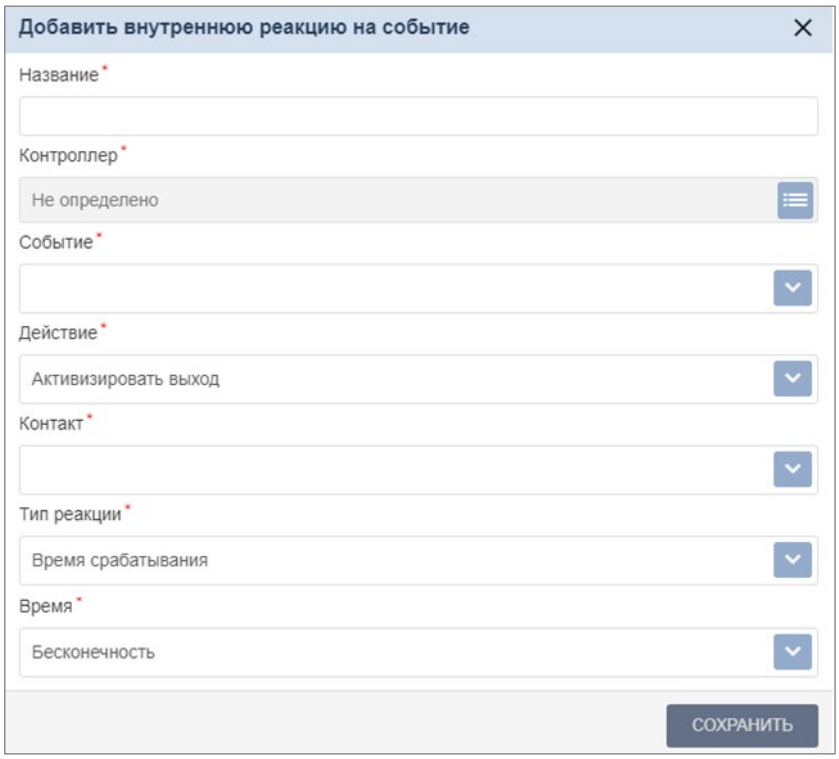
Данная функция предназначена для настройки внутренней реакции на событие новой линейки контроллеров ***PERCo 1.x (CT/L, CL, KT x.xB)***.

Примечание:
После добавления внутренняя реакция запишется в контроллер и будет выполняться им самостоятельно.

Для добавления внутренней реакции на событие контроллера:

1. Используя панель навигации, перейдите в раздел  **«Администрирование»**.
2. Откройте подраздел **«Реакции на события»**.
3. Нажмите на панели инструментов страницы кнопку  **Добавить** а затем **Добавить внутреннюю реакцию на событие контроллера**.

Окно имеет следующий вид:



4. В поле **Название** введите название для новой реакции.
5. В поле **Контроллер** нажмите кнопку  и выберите из списка нужный контроллер. Затем в выпадающем списке, появившемся в левом нижнем углу, выберите ресурс и нажмите кнопку **Сохранить**.

Внимание!

Список функций в некоторых полях страницы будет меняться в зависимости от контроллера и выбранного для него ресурса.

6. В поле **Событие** нажмите кнопку и выберите из списка событие для внутренней реакции.
7. В поле **Действие** нажмите кнопку и выберите из списка действие для выбранного ранее события:
   - **Активизировать выход**;
   - **Нормализовать выход**;
   - **Маскировать вход**.
8. В поле **Контакт** нажмите кнопку и выберите из списка один из вариантов (**Вход** или **Выход**).

Примечание:

Вход или **Выход** в конфигурации контроллера должен иметь тип **Обычный**.

9. В поле **Тип реакции** нажмите кнопку и выберите из списка тип реакции:
   - **Время срабатывания**;
   - **Время абсолютное**;
   - **Время после срабатывания**.
10. В поле **Время** нажмите кнопку и выберите один из вариантов (**Бесконечность** или **Секунды**).
11. Нажмите кнопку **Сохранить**. Окно **Добавить внутреннюю реакцию на событие** будет закрыто, а новая реакция появится в рабочей области страницы.

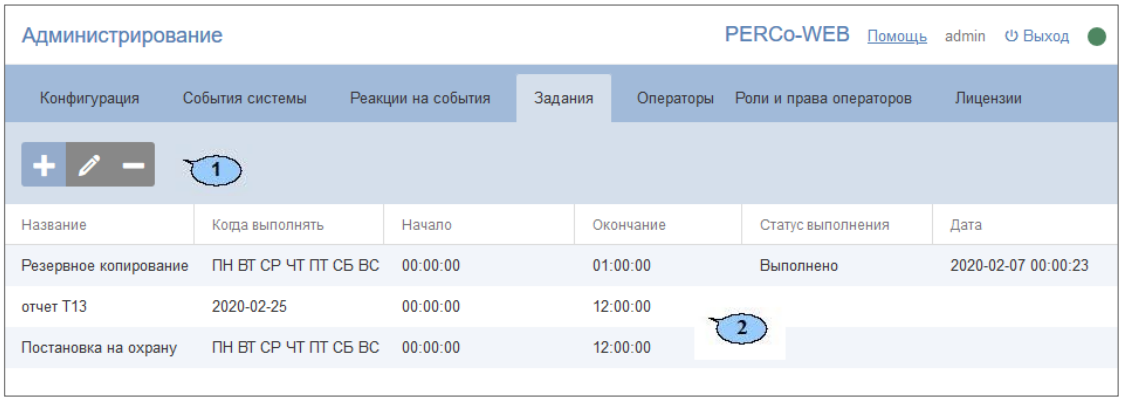
18.4. Подраздел «Задания»

Подраздел предназначен для создания заданий, автоматически выполняемых сервером системы по времени (по дням недели или по конкретной дате).

Доступны следующие виды заданий:

- выполнение заданной команды выбранным устройством системы;
- резервное копирование базы данных;
- отправка заданного отчета выбранному сотруднику (сотрудникам).

Страница подраздела имеет следующий вид:



1. Панель инструментов страницы содержит:
   - **Добавить** – кнопка позволяет создать 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 подраздела содержит список заданий сервера системы.

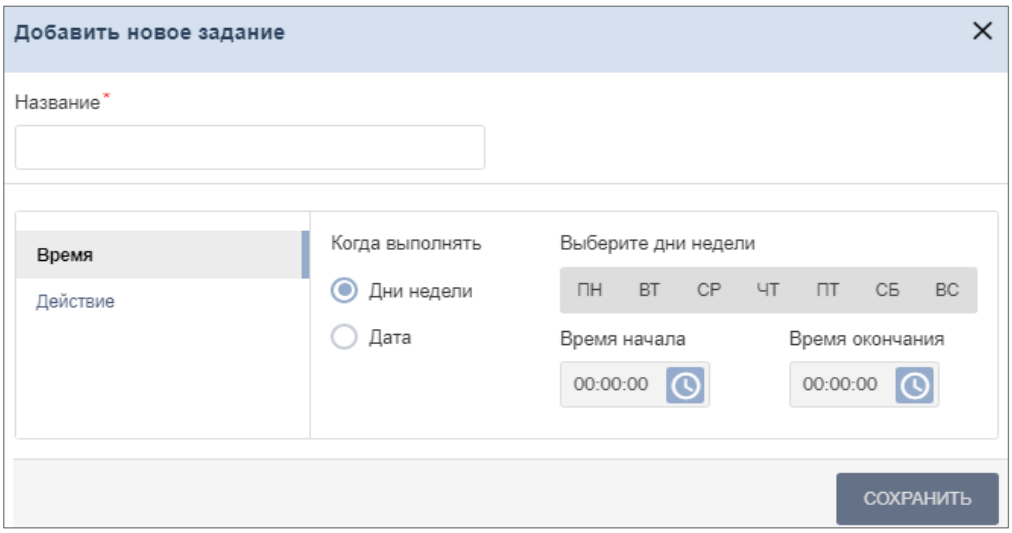
Примечание:

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

18.4.1. Создание нового задания

Для создания нового задания:

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



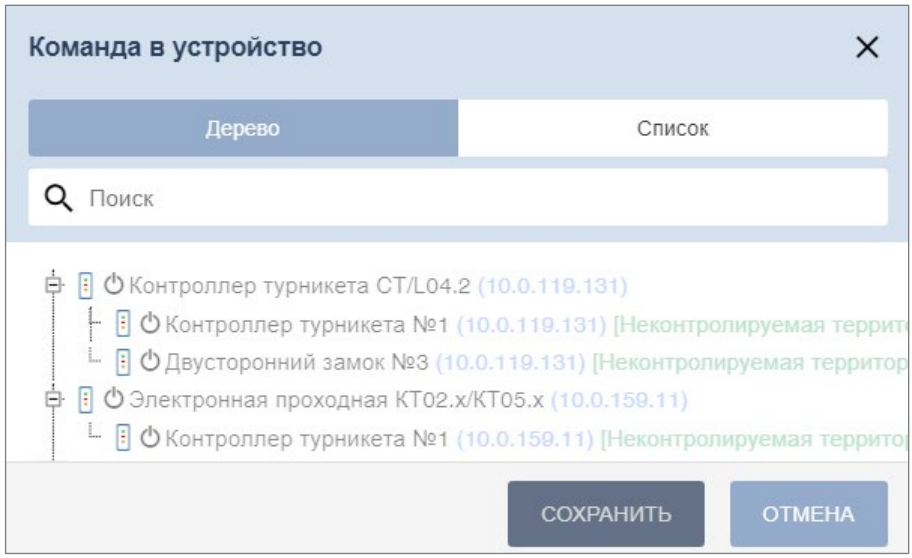
4. В поле **Название** введите название для нового задания.
5. На вкладке **Время** выберите с помощью переключателя периодичность выполнения задания:
   - **Дни недели** – если задание необходимо выполнять еженедельно. С помощью соответствующих кнопок укажите дни недели, в которые будет запускаться задание.
   - **Дата** – если задание необходимо выполнить один раз. С помощью календаря укажите дату запуска задания.
   - С помощью полей ввода **Время начала** и **Время окончания** укажите период времени в течение суток, в который задание необходимо запустить.

Примечание:

Для выполнения заданий рекомендуется выбирать период времени, когда совершается минимальное количество проходов и минимальное количество операторов подключено к серверу системы.

6. На вкладке **Действие** с помощью кнопки выберите один из следующих типов заданий:
   - **Команда в устройство** – позволяет выбрать команду для устройства, добавленного в конфигурацию системы ***PERCo-Web***. При выборе данного типа задания откроется окно

Команда в устройство:



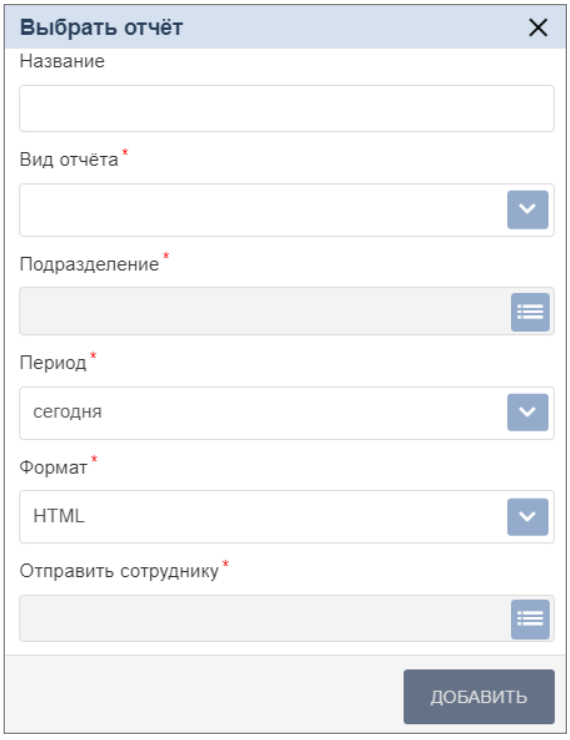
В окне **Команда в устройство** выберите устройство, а затем из выпадающего списка в левом нижнем углу – команду для него. Нажмите кнопку **Сохранить**, данное задание добавится в список на вкладке **Действие**.

- **Резервное копирование базы данных** – позволяет создать задание по сохранению резервной копии БД (по умолчанию БД сохраняется в папке *C:\ProgramData\PERCo-Web2\mysql* в файле с расширением *.sql*). Задание добавляется в список на вкладке **Действие**.

Примечание:

По умолчанию в подразделе создано одно ежедневное задание для резервного копирования базы данных, при необходимости можно изменить параметры этого задания. Удаление задания без добавления нового приведет к отключению резервного копирования базы данных.

- **Отправить отчет по email** – позволяет создать задание по отправке отчета выбранному сотруднику. При выборе данного типа задания откроется окно **Выбрать отчет**:



Окно содержит элементы:

- **Название** – поле предназначено для ввода названия отчета.
- **Вид отчета** – выпадающий список позволяет выбрать вид отчета:
  - **отчет о проходах сотрудников**,
  - **отчет о нарушениях сотрудников**,
  - **отчет о присутствующих на данный момент**,
  - **отчет об отсутствующих сегодня**,
  - **отчет об опоздавших сегодня**,
  - **отчет о переработке сотрудников**,
  - **отчет Т13**;
- **Подразделение** – при нажатии на кнопку  открывается окно **Выбрать подразделение**, позволяющее выбрать подразделение – объект отчетности.
- **Период** – выпадающий список позволяет выбрать период отчетности.
  При выборе отчета **Т13** в окне также появляется флажок **Показ минут**, при его установке в отчете будут выведены данные с точностью до минуты.
- **Формат** – выпадающий список позволяет выбрать формат файла отчета – **HTML**, **XLSX** или **CSV**.
- **Отправить сотруднику** – при нажатии на кнопку  открывается окно **Выбрать сотрудника**, позволяющее выбрать сотрудника, которому будет отправляться отчет. Для удобства имеется возможность поиска по имени и подразделению.

Внимание!

Для отправки отчета по e-mail необходимо, чтобы в учетной карточке сотрудника правильно было заполнено поле **Email**.

После заполнения параметров отчета нажмите кнопку **Добавить**, данное задание добавится в список на вкладке **Действие**.

7. После установки времени и действий для нового задания нажмите кнопку **Сохранить**. Окно **Добавить новое задание** будет закрыто, новое задание появится в рабочей области страницы.

Примечание:

В одном задании можно задать сразу несколько действий для выполнения в один и тот же период времени.

8. Для удаления задания из списка выделите его и нажмите кнопку  . Для удаления всех заданий нажмите кнопку  .

18.5. Подраздел «Операторы»

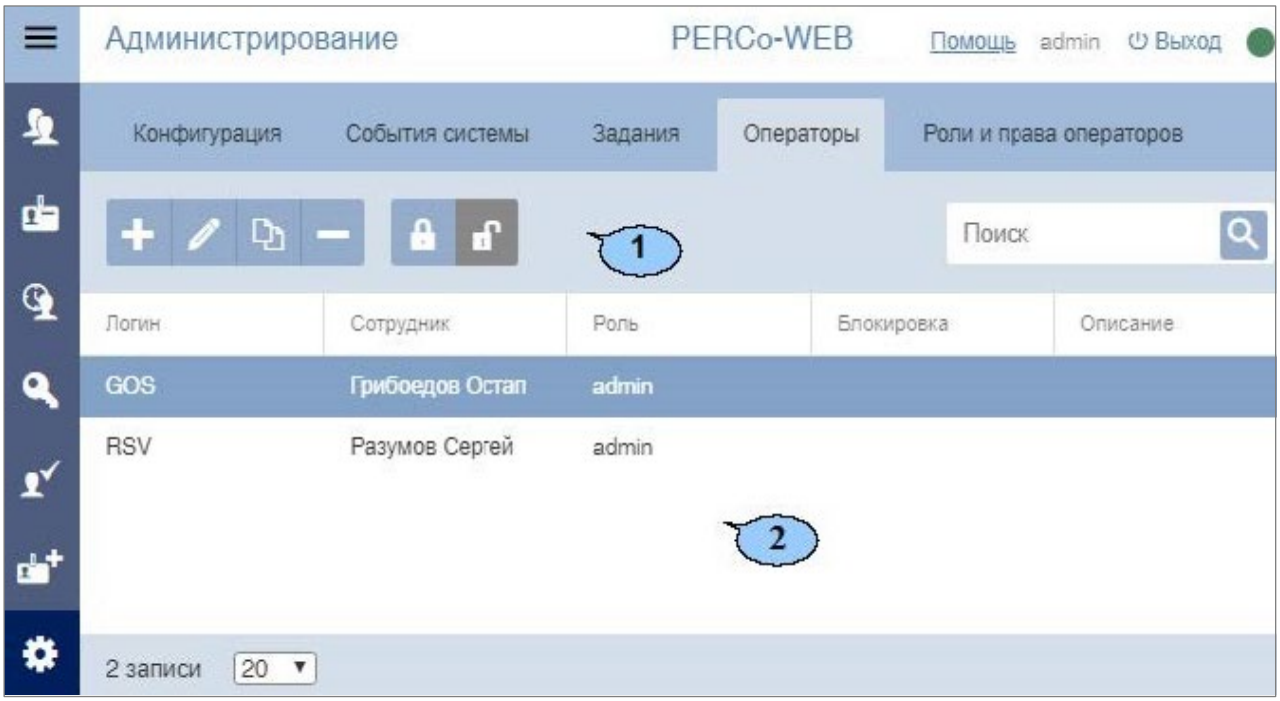
Примечание:

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 оператора** – кнопка позволяет добавить нового оператора.
   - **Редактировать оператора** – кнопка позволяет изменить данные оператора, выделенного в рабочей области страницы.
   - **Скопировать оператора** – кнопка позволяет скопировать данные оператора, выделенного в рабочей области страницы, для создания нового оператора.
   - **Удалить оператора** – кнопка позволяет удалить выделенного в рабочей области страницы оператора.
   - **Заблокировать оператора** – кнопка позволяет временно блокировать возможность доступа в систему оператора, выделенного в рабочей области страницы.
   - **Разблокировать оператора** – кнопка позволяет разблокировать ранее заблокированную возможность доступа в систему для оператора, выделенного в рабочей области страницы.
   - Поле **Поиск** – кнопка справа от поля **Поиск** позволяет произвести поиск по элементам столбцов 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.

18.5.1. Добавление оператора системы

Примечание:

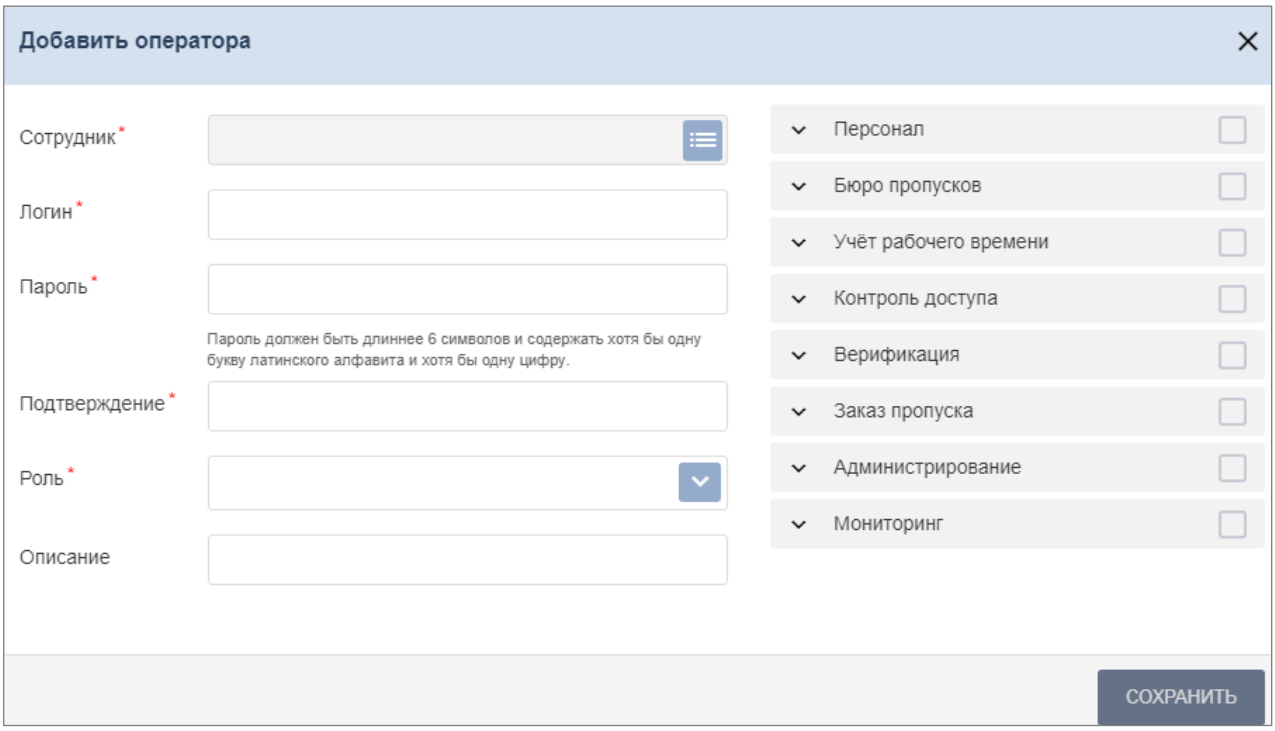
Перед добавлением операторов создайте в подразделе **«Роли и права операторов»** раздела **«Администрирование»** необходимые роли операторов и выдайте им полномочия.

Внимание!

При активации лицензии ***PERCo-WM03 «Интеграция с 1С»*** оператор 1s создается автоматически. Для дальнейшей работы с 1С оператору 1s необходимо задать пароль. Войти в систему ***PERCo-Web*** под данным оператором будет невозможно.

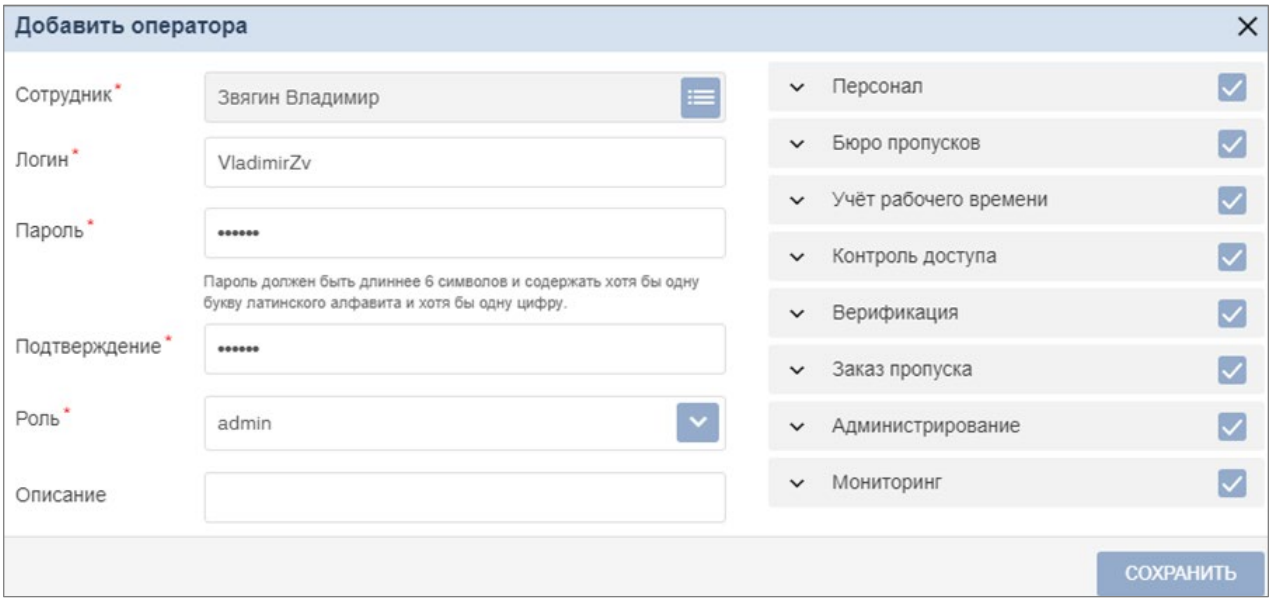
Для добавления нового оператора выполните следующие действия:

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



4. В поле **Сотрудник** с помощью кнопки выберите из выпадающего списка необходимого сотрудника.
5. В полях **Логин** и **Пароль** укажите для оператора его логин и пароль.
6. В поле **Роль** с помощью кнопки укажите для оператора его полномочия. Роли операторов создаются в подразделе **«Роли и права операторов»**.
7. При необходимости укажите для оператора **Описание**.
8. На панели **Доступ к разделам** установите флажки у разделов, подразделов и вкладок подразделов, доступ к которым будет разрешен оператору.

В зависимости от заданных параметров страница примет вид:



Внимание!

При выдаче 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.

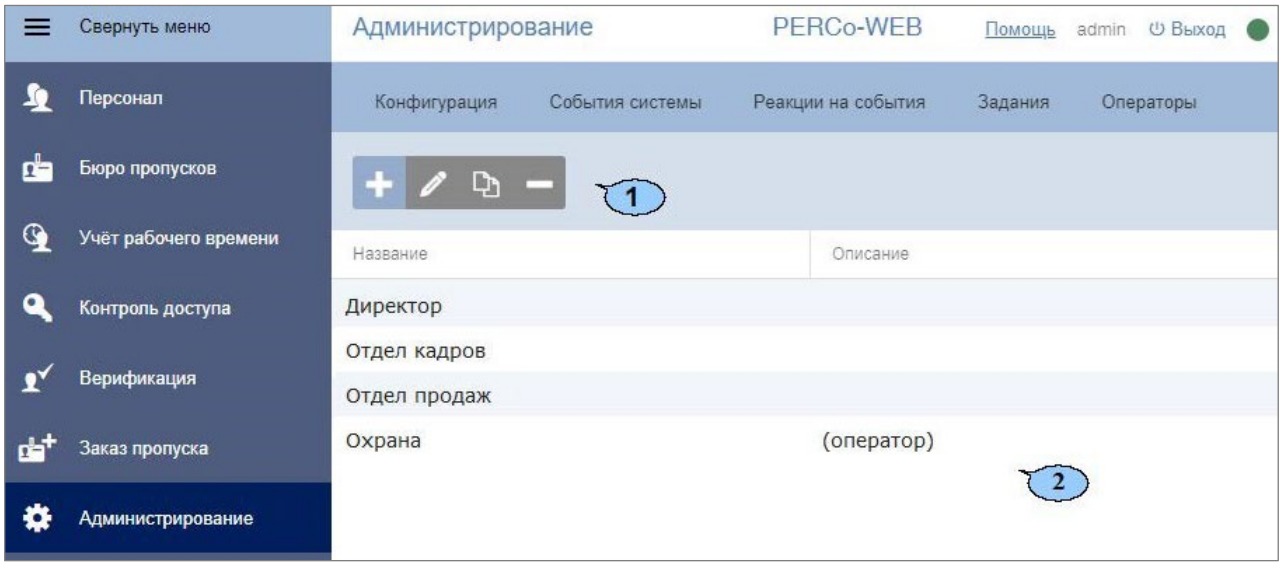
9. Нажмите кнопку **Сохранить**. Окно **Добавить оператора** будет закрыто. Новый оператор будет добавлен в список в рабочей области страницы.

18.6. 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.

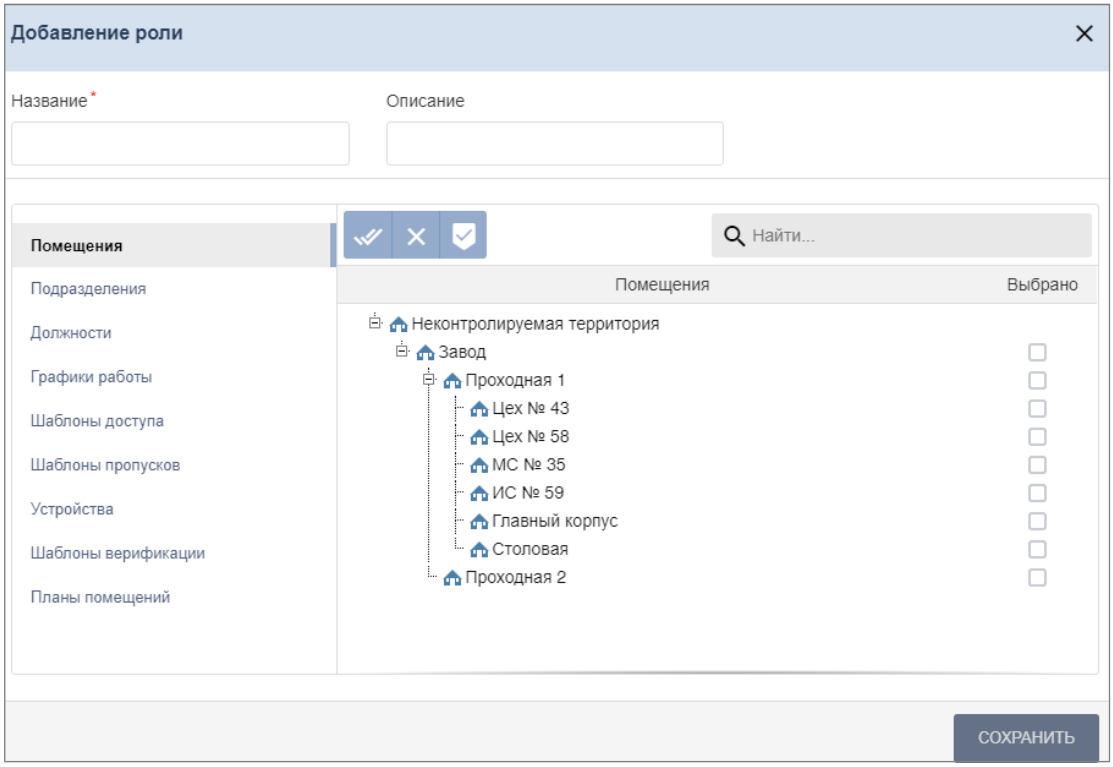
Примечание:

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

18.6.1. 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 страницы кнопку **Добавить**. Откроется окно **Добавление роли**:



4. В открывшемся окне в поле **Название** 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**;

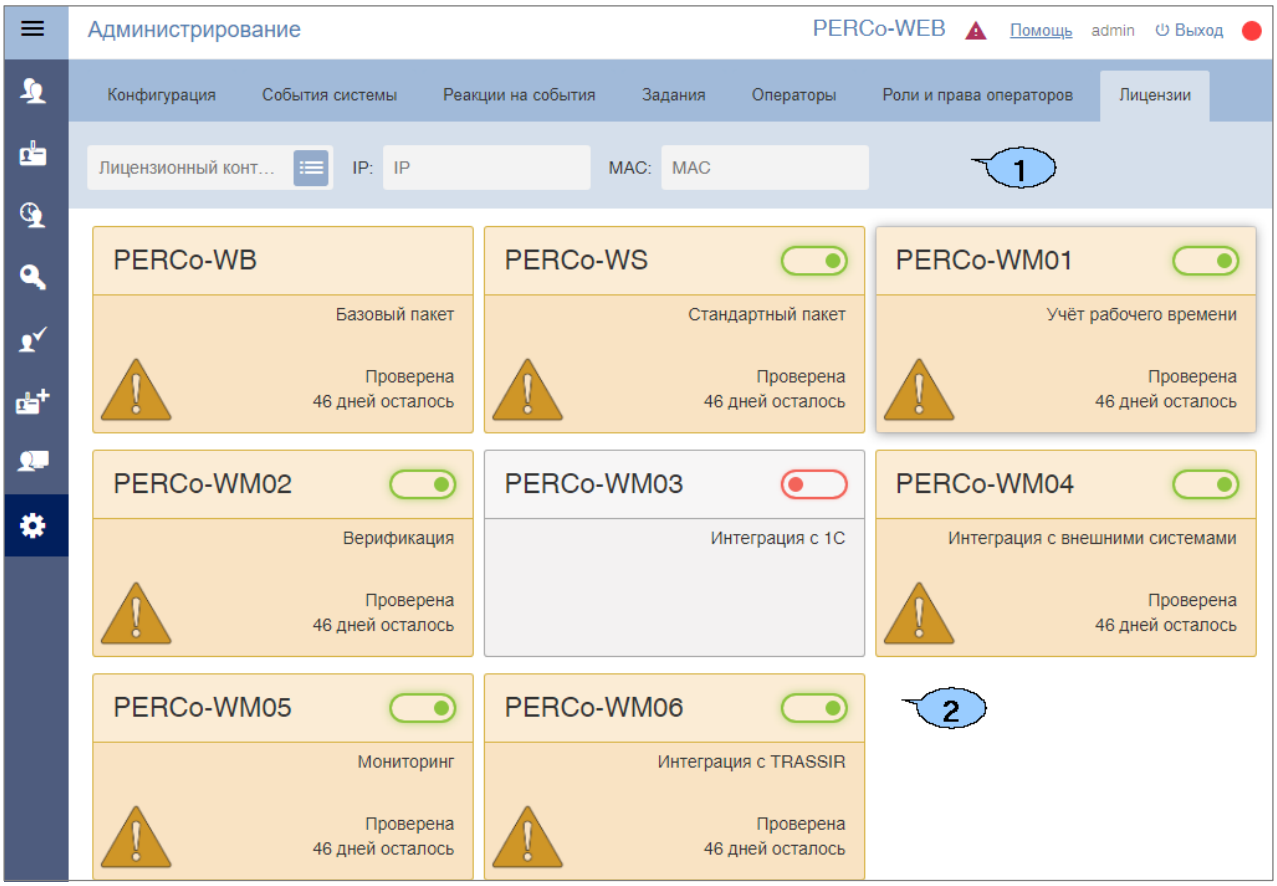
- **Подразделения**;
- **Должности**;
- **Графики работы**;
- **Шаблоны доступа**;
- **Шаблоны пропусков**;
- **Устройства**;
- **Шаблоны верификации**;
- **Планы помещений**.

6. Установите флажки у тех объектов, полномочия на которые должны быть доступны для созданной роли оператора. При необходимости используйте кнопки **Выбрать все** и **Снять выделение**. Также есть возможность включить в список все последующие добавленные элементы. Для этого воспользуйтесь кнопкой **Безусловные права**.
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»**.

18.7. Подраздел «Лицензии»

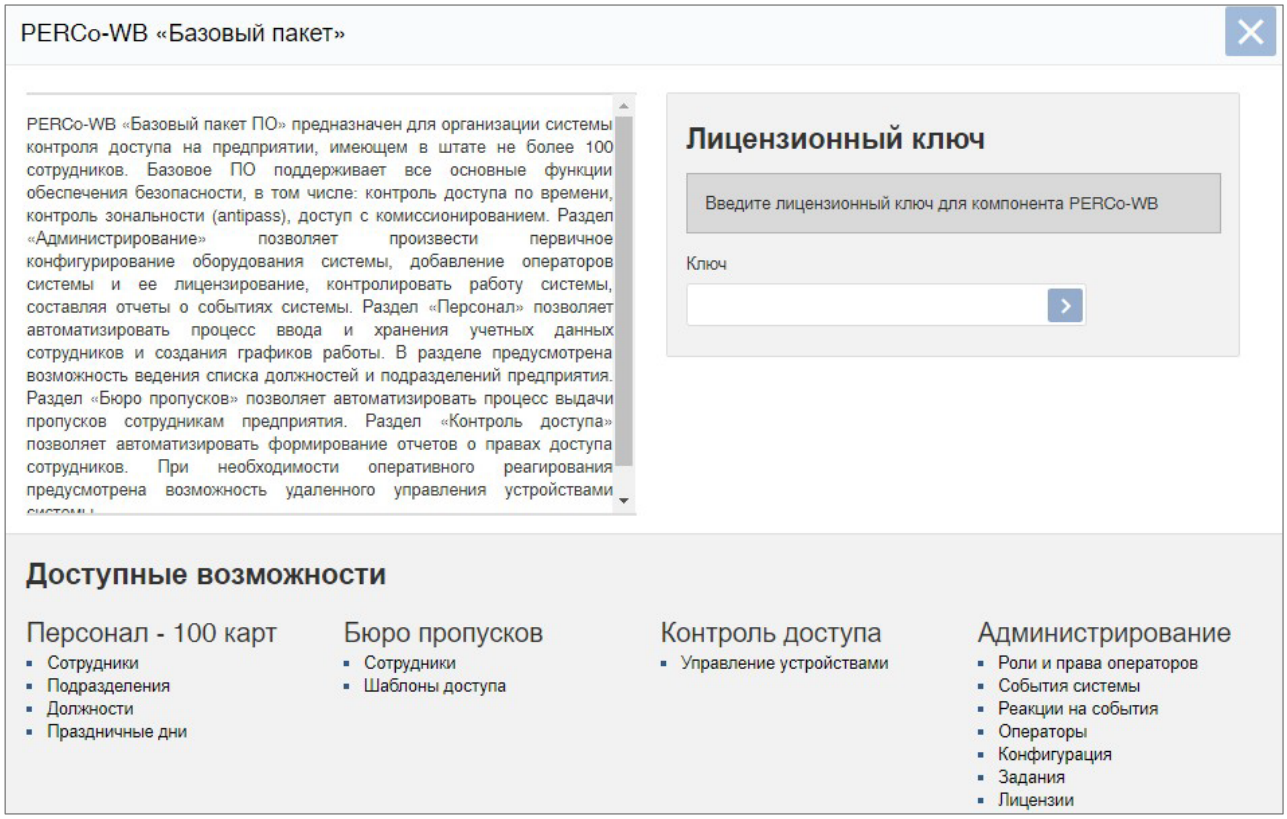
Подраздел предназначен для ввода кодов активации установленных модулей ПО системы.

Страница подраздела имеет следующий вид:



1. Поле **Лицензионный контроллер** позволяет 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 и информацию о лицензии.

После выбора в рабочей области страницы одного из модулей открывается панель активации лицензии, которая выглядит следующим образом:



Вид панели зависит от выбранного модуля.

Для активации лицензии в поле **Ключ** введите лицензионный ключ для выбранного компонента и нажмите кнопку  . При правильном вводе лицензия будет активирована, цвет модуля изменится на зеленый (бессрочная лицензия) или желтый (временное ограничение).

Панель **Доступные возможности** содержит список разделов и подразделов системы, доступных для выбранного в рабочей области страницы модуля.

18.7.1. Ввод кода активации

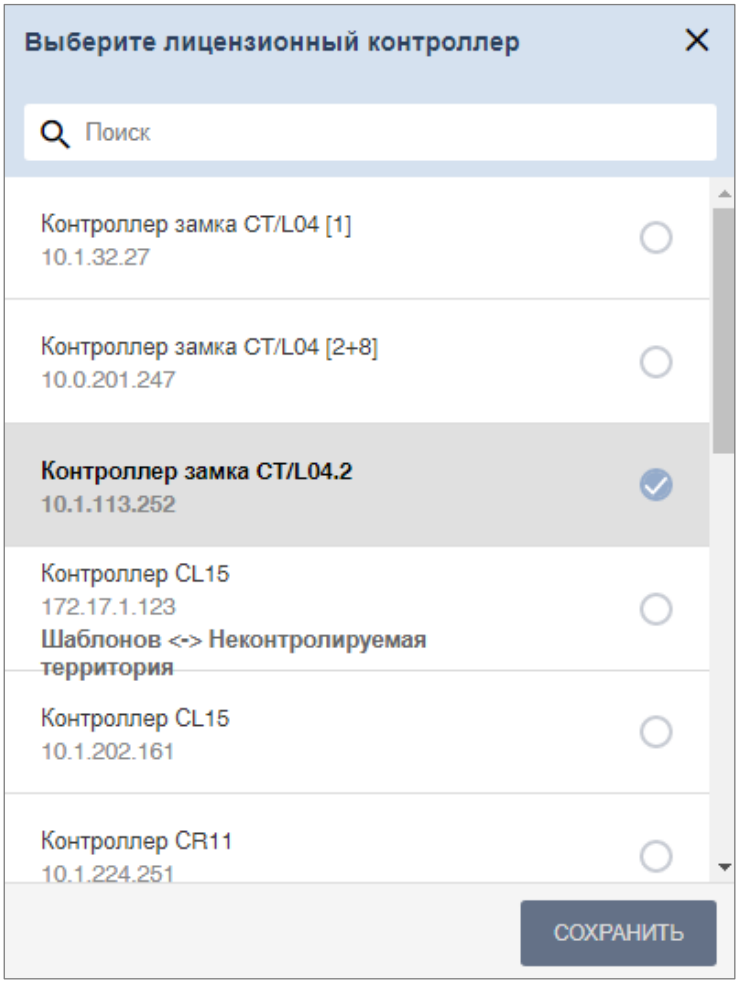
Для ввода кодов активации модулей ПО системы:

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 **«Устройства»** подраздела **«Конфигурация»**.

3. В поле **Лицензионный контроллер** нажмите кнопку  . Откроется окно **Выберите лицензионный контроллер**:



4. В открывшемся окне выделите контроллер, выбранный в качестве электронного ключа защиты ПО системы. Нажмите кнопку **Сохранить**.
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. Откроется панель активации лицензии выбранного модуля.
7. В поле **Лицензионный ключ** введите код активации, указанный для выделенного модуля в лицензионном соглашении. Код вводится без пробелов и разделителей. Нажмите кнопку  справа от поля.
8. Сервер системы проверит введенный код. При правильном вводе лицензия будет активирована, цвет модуля изменится на зеленый (бессрочная лицензия) или желтый (временное ограничение).
9. В случае ошибки при вводе кода активации, несоответствия кода выбранному модулю или контроллеру, нарушения связи с контроллером отобразится соответствующее предупреждение.

19. Параметры контроллера PERCo

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

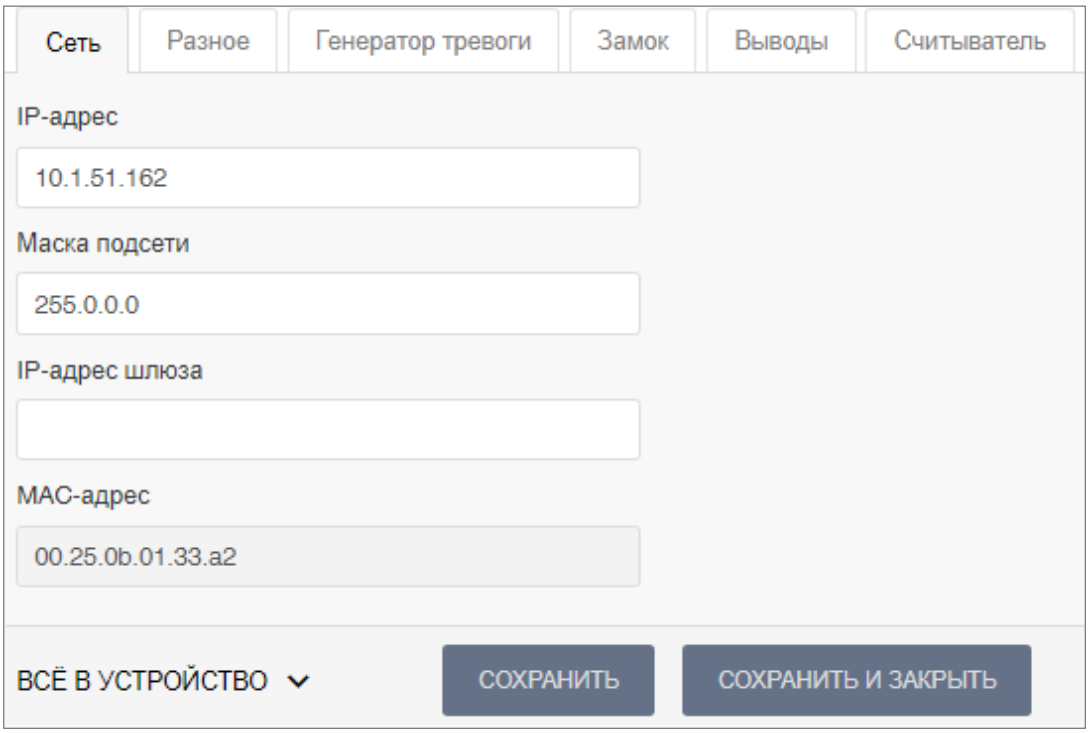
- **Внешние подключения** – информация о внешних подключениях контроллера;
- **Сеть**;
- **Разное**;
- **ИУ (Замок, Турникет)**;
- **Входы**;
- **Выходы**;
- **Выводы**;
- **Генератор тревоги**;
- **Свойства ЛИКОНА**;
- **Строки**;
- **Состояние** – информация о состоянии контроллера;
- **Считыватель**.

19.1. Вкладка «Сеть»

Вкладка **Сеть** отображает информацию о следующих сетевых параметрах:

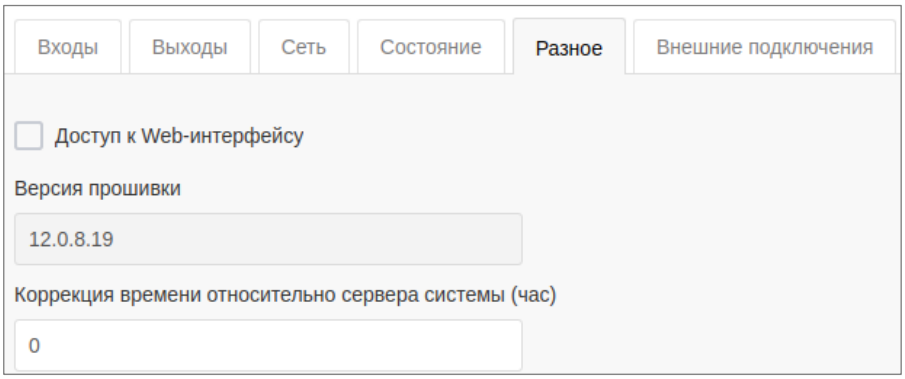
- **IP-адрес**;
- **Маска подсети**;
- **IP-адрес шлюза**;
- **MAC-адрес**.

Вкладка выглядит следующим образом:



19.2. Вкладка «Разное»

Вкладка выглядит следующим образом:

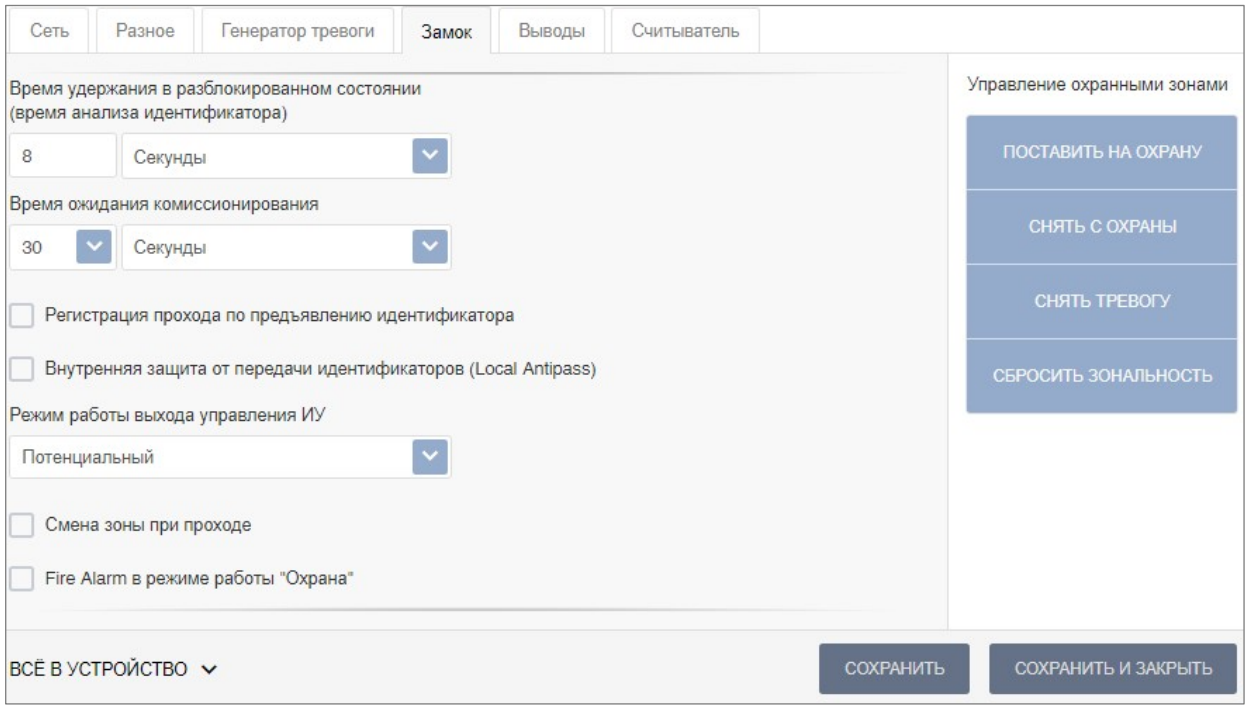


Вкладка **Разное** содержит следующие настройки:

- **Доступ к Web-интерфейсу** – при установке флажка появляется возможность разрешить подключение к Web-интерфейсу контроллера по IP-адресу.
- **Версия прошивки** – в поле отображается версия прошивки встроенного ПО контроллера.
- **Коррекция времени относительно сервера системы (час)** – поле позволяет произвести коррекцию времени относительно сервера системы, чтобы у событий контроллеров доступа, установленных в разных часовых поясах, записывалось корректное время на общем сервере ***PERCo-Web***. Часы следует вводить в интервале от -12 до 12.

19.3. Вкладка ИУ («Замок», «Турникет»)

Вкладка выглядит следующим образом:



Для настройки входов доступны следующие параметры:

- **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)**. Параметр позволяет задать время, которое должно пройти от разблокировки ИУ до его блокировки после успешной аутентификации. За это время необходимо совершить проход, иначе ИУ заблокируется. Параметр может быть задан в интервале: от 250 до 750 миллисекунд с шагом 250 миллисекунд; от 1 секунды до 4 минут; бесконечно.
- **Время ожидания комиссионирования**. Параметр позволяет ограничить интервал времени между предъявлением идентификатора пользователя (сотрудника / посетителя / служебного ТС) и комиссионирующей карты (сотрудника / охранника / водителя) в случае, если в правах идентификатора пользователя 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 идентификатора, 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 от ДУ** 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 одного и того же идентификатора 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**. Параметр нужен для смены пространственных зон при работе с функцией Global Antipass.
- **Fire Alarm 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.

19.4. Вкладка «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.
  - **Fire Alarm**. Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ Fire Alarm.
  - **Подтверждение от ВВУ**. Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае **разрешения** прохода.
  - **Запрет от ВВУ**. Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае **запрета** прохода.
- **Нормальное состояние контакта** (*Разомкнут / Замкнут*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

В зависимости от выбранного типа остальные параметры входа могут различаться.

Тип **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.

Тип **Специальный**:

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

Тип **Подтверждение от ВВУ / Запрет от ВВУ**:

- **Номер ИУ**. Параметр задает номер ИУ, к которому привязывается считыватель.

19.5. Вкладка «Выходы»

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

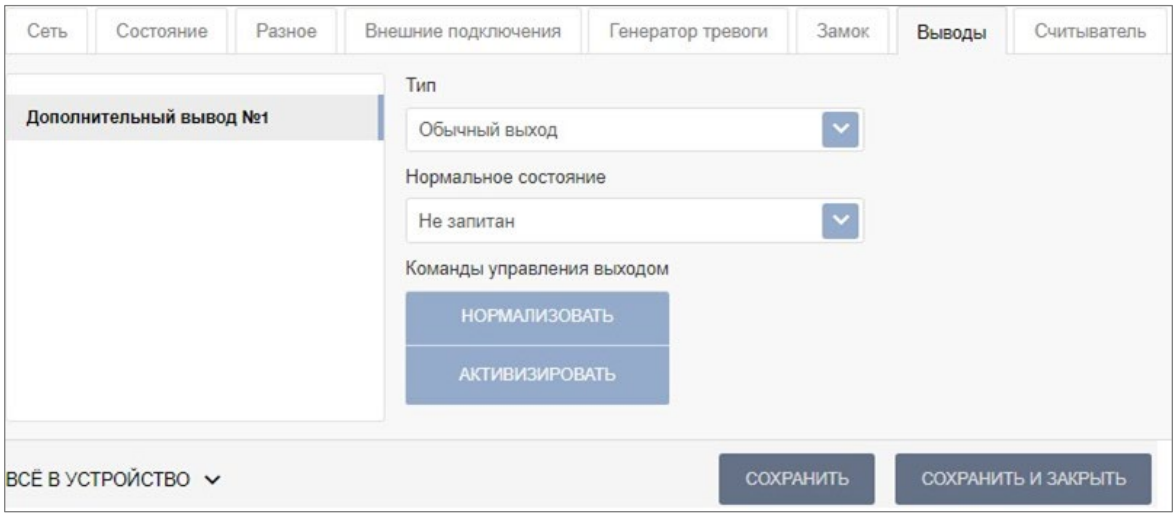
Примечание:

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.

19.6. Вкладка «Выводы»

Вкладка выглядит следующим образом:

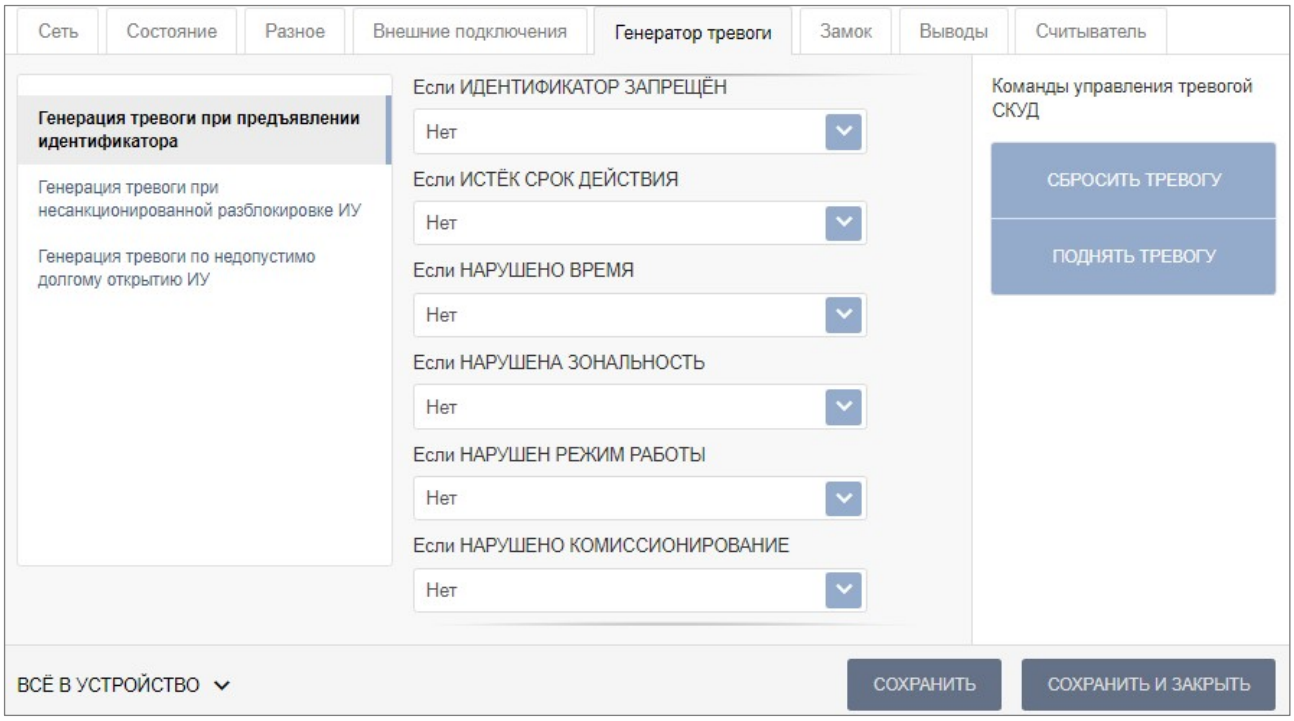


Для настройки доступны следующие параметры:

- **Тип**. Раскрывающийся список позволяет выбрать один из следующих типов:
  - **Нет**. К данному входу не подключено никакое внешнее оборудование.
  - **Обычный выход**. 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**.
  - **Вход Fire Alarm**. 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** (*Не запитан / Запитан*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

19.7. Вкладка «Генератор тревоги»

Вкладка выглядит следующим образом:



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:

- Вкладка **Генерация тревоги при предъявлении идентификатора** – параметр позволяет указать события, связанные с предъявлением карт доступа, при регистрации которых произойдет генерация тревоги:
  - **если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН**;
  - **если ИДЕНТИФИКАТОР ЗАПРЕЩЕН**;
  - **если ИСТЕК СРОК ДЕЙСТВИЯ**;
  - **если НАРУШЕНО ВРЕМЯ**;
  - **если НАРУШЕНА ЗОНАЛЬНОСТЬ**;
  - **если НАРУШЕН РЕЖИМ РАБОТЫ**;
  - **если НАРУШЕНО КОМИССИОНИРОВАНИЕ**.

  Для каждого 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.
- Вкладка **Генерация тревоги при несанкционированной разблокировке ИУ** – параметр позволяет для РКД *«Контроль»* и *«Закрыто»* указать, будет ли генерироваться тревога в случае механической разблокировки ИУ при помощи ключа, то есть без команды от контроллера:
  - **в РЕЖИМЕ РАБОТЫ "Контроль"**;
  - **в РЕЖИМЕ РАБОТЫ "Закрыто"**.
- Вкладка **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.

19.8. Вкладки «Свойства ЛИКОНА» и «Строки»

На вкладке **Свойства ЛИКОНА** расположены параметры настройки для контроллера регистрации ***PERCo-CR01 LICON***.

- **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:

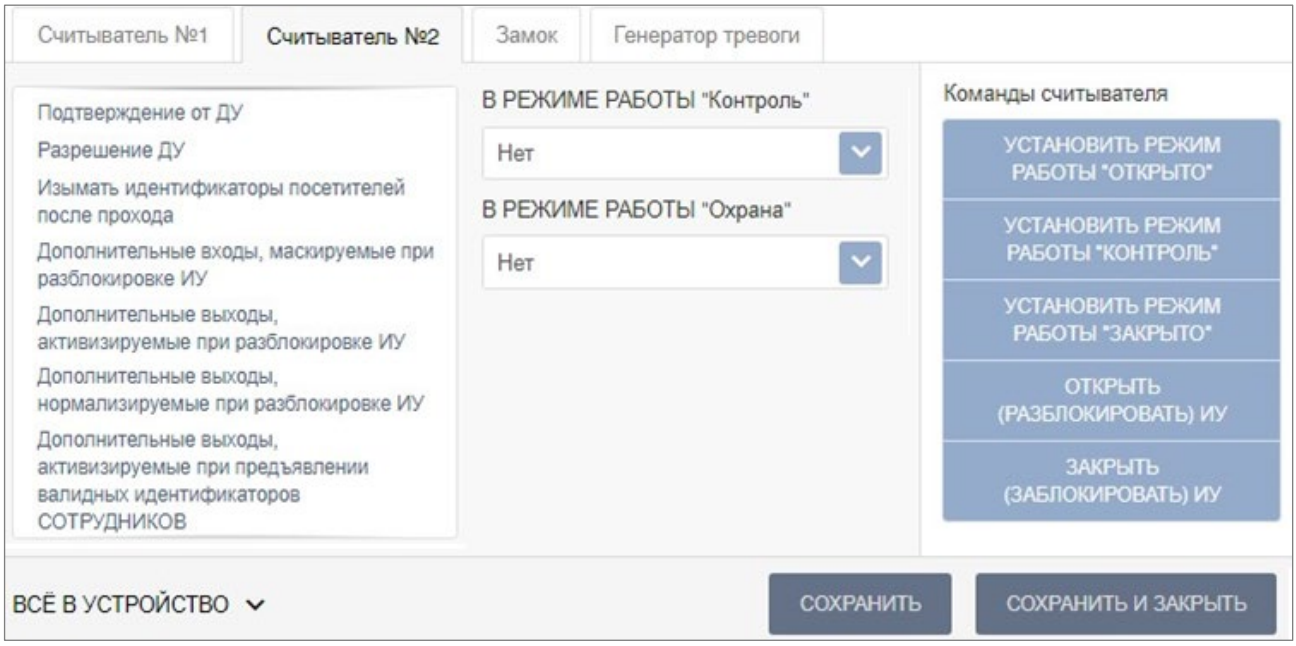
При изменении прямого направления прохода подписи указателей *«Вход»* и *«Выход»* на ЖКИ не меняются. Изменить текст надписей указателей можно в раскрывающемся меню **Локализация отображаемых строк**.

- **Время ожидания ответа на запрос от сервера системы (максимально 12 сек; по умолчанию 5 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.
- **Защита от передачи идентификаторов СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ (Antipass)**. Параметр позволяет для РКД *«Контроль»* 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 считывателю для параметра **Верификация** установлено значение **ПДУ** или **Софт**, 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 считывателю для параметра **Верификация** установлено значение **ПДУ** или **Софт**, то будет запущена процедура верификации.

Вкладка **Строки** позволяет изменить содержание сообщений, отображаемых на ЖКИ контроллера.

19.9. Вкладка «Считыватель»

Вкладка выглядит следующим образом:



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 считывателю для параметра **Верификация** установлено значение **ПДУ** или **Софт**, 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 считывателю для параметра **Верификация** установлено значение **ПДУ** или **Софт**, то будет запущена процедура верификации.

- **Разрешение ДУ**. При установке флажка **В РЕЖИМЕ РАБОТЫ "Контроль"** использование ПДУ при РКД *«Контроль»* в направлении данного считывателя будет разрешено.
- **Подтверждение от ДУ**. Параметр позволяет настроить проведение процедуры верификации от ПДУ. При установке типа контроля **Нет** в поле **В РЕЖИМЕ РАБОТЫ «Контроль»** задайте **Время ожидания подтверждения при верификации**. При установке типа контроля **Да** в поле **В РЕЖИМЕ РАБОТЫ «Контроль»** укажите, какие события должны быть верифицированы, и задайте **Время ожидания подтверждения при верификации**.
- **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.
- **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 срок 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.
- **Дополнительные выходы, активизируемые при разблокировке ИУ**. Параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при разблокировке ИУ. Для выбора отметьте те дополнительные выходы, которые должны быть активизированы. Укажите временной критерий активизации.
- **Дополнительные выходы, нормализируемые при разблокировке ИУ**. Параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализированы при разблокировке ИУ. Для выбора отметьте те дополнительные выходы, которые должны быть нормализированы. Укажите временной критерий нормализации.
- **Дополнительные 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.

20. Параметры контроллеров PERCo CT/L14, CL15, CR11, CT13

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

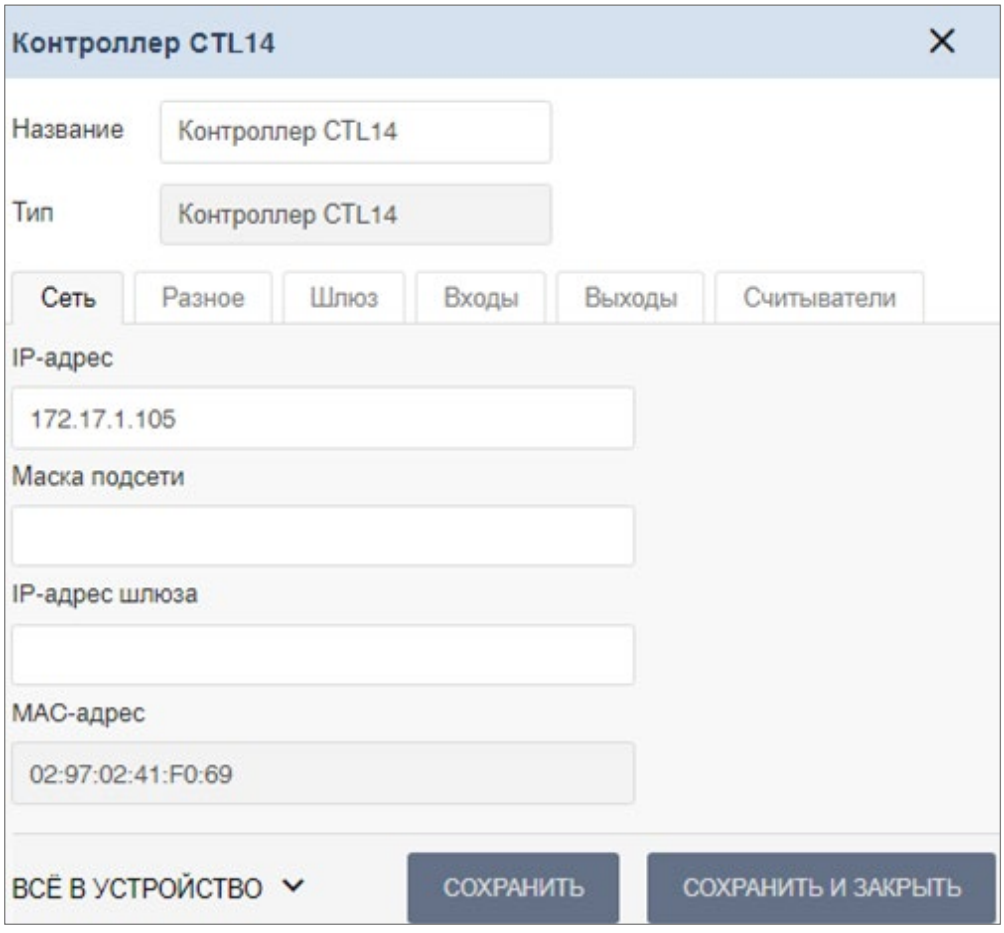
- **Сеть**;
- **Разное**;
- **ИУ**;
- **Направление**;
- **Генератор тревоги**;
- **Свойства**;
- **Направление №...**;
- **Входы**;
- **Выходы**;
- **Считыватели**;
- **Шлюз**;
- **Составной объект**.

20.1. Вкладка «Сеть»

Вкладка отображает информацию о следующих сетевых параметрах:

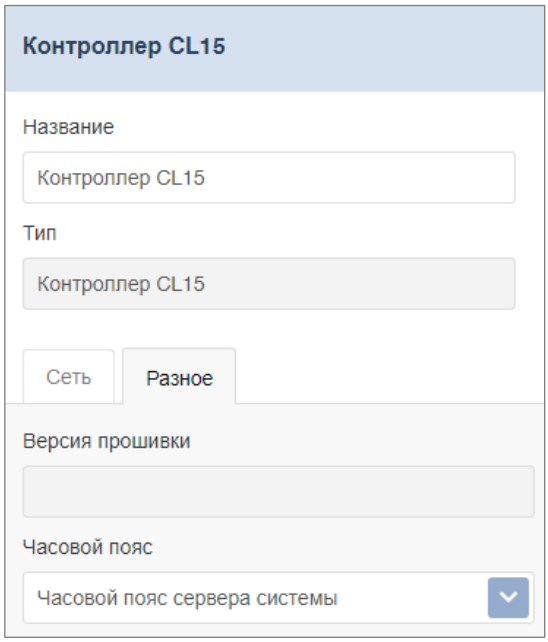
- **IP-адрес**;
- **Маска подсети**;
- **IP-адрес шлюза**;
- **MAC-адрес**.

Окно имеет следующий вид:



20.2. Вкладка «Разное»

Вкладка выглядит следующим образом:

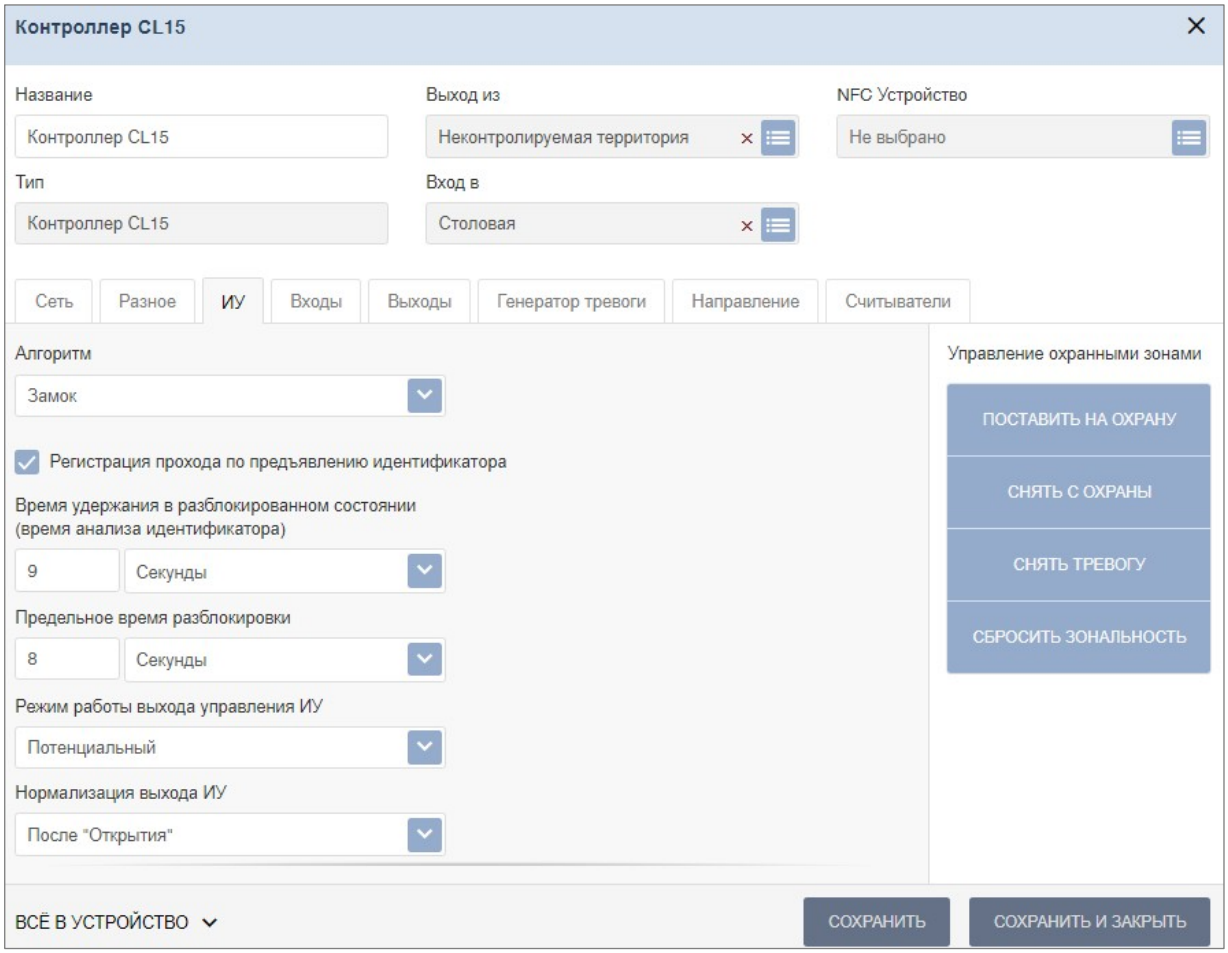


Вкладка содержит следующие настройки:

- **Версия прошивки** – в поле отображается версия прошивки встроенного ПО контроллера.
- **Часовой пояс** – выпадающий список позволяет выбрать часовой пояс контроллера.

20.3. Вкладка ИУ

Вкладка выглядит следующим образом:

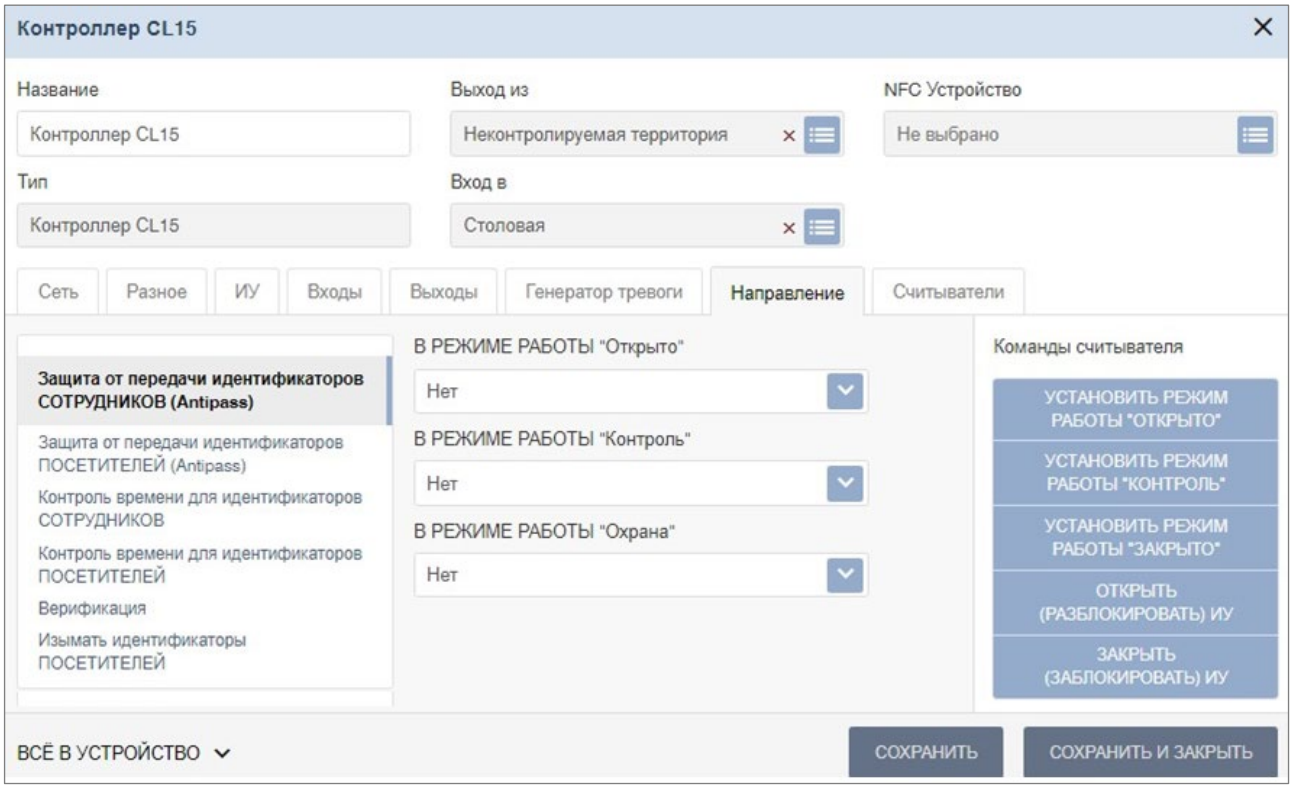


Для настройки доступны следующие параметры:

- **Алгоритм** – определяет алгоритм работы универсального ИУ:
  - **Замок**;
  - **Турникет**;
  - **АТП (Автотранспортная проходная)**;
  - **Шлюз**.
- **Регистрация прохода по предъявлению идентификатора** – если флажок установлен, событие совершения прохода регистрируется сразу после поднесения карты доступа / сканирования пальца без ожидания сигнала от датчика прохода. Если флажок не установлен, то событие совершения прохода регистрируется после поднесения карты доступа / сканирования пальца и срабатывания датчика прохода.
- **Время удержания в разблокированном состоянии (время анализа идентификатора)** – устанавливает время, которое должно пройти от разблокировки ИУ до его блокировки после успешной аутентификации. За это время необходимо совершить проход, иначе ИУ заблокируется. Параметр может быть задан в интервале: от 1 секунды до 4 минут; бесконечно.
- **Предельное время разблокировки** – параметр позволяет указать время, по истечении которого контроллер сформирует сообщение *«ИУ не закрыто после прохода по идентификатору»* по причине того, что ИУ не заблокировано. Параметр может быть задан в интервале: от 250 до 750 миллисекунд с шагом 250 миллисекунд; от 1 секунды до 4 минут; бесконечно.
- **Режим работы выхода управления ИУ** – описывает логику управления подключенным ИУ:
  - **Потенциальный**.
  - **Импульсный** – режим управления применяется только для замков, поддерживающих этот режим. Рекомендуется использовать для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки «CISA»).
- **Нормализация выхода ИУ** – параметр определяет, в какой момент нормализуется состояние выхода управления ИУ:
  - **После «Открытия»**;
  - **После «Закрытия»**.
- **Реакция на Fire Alarm в режиме работы «Охрана»** – определяет реакцию на команду от устройства Fire Alarm:
  - **Разблокировать ИУ**;
  - **Блокировать ИУ**.
- **Время идентификации постановки / снятия РКД «Охрана»** – устанавливает время, в течение которого пользователь для успешной идентификации для снятия ИУ с охраны должен предъявить палец после предъявления идентификатора, если *«Схема идентификации по охране»* в правах пользователя подразумевает последовательное предъявление идентификатора и пальца (см. *«Параметры доступа контроллеров PERCo-CR11, CT13, CT/L14 и CL15»* в подразделе **«Шаблоны доступа»** раздела **«Бюро пропусков»** *Руководства пользователя* ***PERCo-WB***, ***PERCo-WBE***, ***PERCo-WS***, ***PERCo-WSE***).
- **Внутренняя защита от передачи идентификаторов (Local Antipass)** – при установленном параметре контроллер отслеживает случаи повторного предъявления одной и той же карты доступа / биоидентификатора к тому же считывателю.

20.4. Вкладка «Направление»

Вкладка выглядит следующим образом:



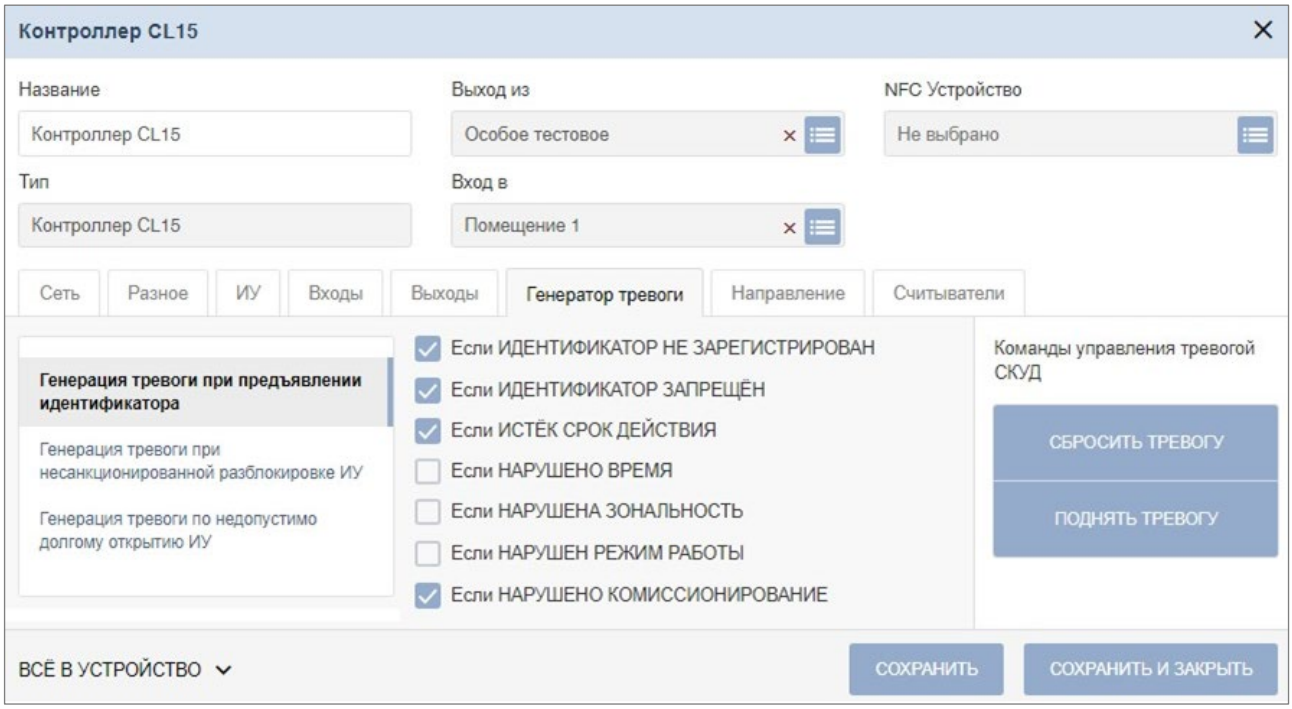
Для настройки доступны следующие параметры:

- **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 РКД *«Охрана»* и *«Контроль»* можно выбрать один из видов контроля:
  - **Нет** – контроллер не учитывает зональность идентификатора карты для разрешения доступа.
  - **Мягкая** – контроллер разрешит доступ по карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение зональности»*, после совершения прохода регистрируется событие «*Проход по карте с несоответствием текущему местоположению»*.
  - **Жесткая** – контроллер запретит доступ по карте, при этом передается событие мониторинга *«Предъявление карты с нарушением зональности»* и регистрируется событие *«Запрет прохода по причине нарушения зональности»*.
- **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 РКД *«Охрана»* и *«Контроль»* можно выбрать один из видов контроля:
  - **Нет** – контроллер не отслеживает временные критерии прав доступа карты.
  - **Мягкий** – контроллер разрешит доступ по предъявленной карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение времени»*, после совершения прохода регистрируется событие «*Проход по карте с несоответствием временным критериям доступа»*.
  - **Жесткий** – контроллер запретит доступ по карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение времени»* и регистрируется событие «*Запрет прохода, несоответствие временным критериям доступа»*.

- **Верификация**:
  - **Уровни верификации**. Параметр позволяет задать способ и очередность верификации. Доступны следующие уровни:
    - **Софт**;
    - **Софт, если подключен**;
    - **ПДУ**;
    - **ВВУ**;
    - **ПДУ выборочно**;
    - **ВВУ выборочно**;
    - **Счетчик проходов**.
  - **Софт**. Параметр позволяет задать время ожидания подтверждения.
  - **ПДУ и ВВУ**. Для вкладок доступны следующие параметры:
    - Подтверждение прохода:
      - ✓ **при проходе СОТРУДНИКОВ**;
      - ✓ **при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ**;
      - ✓ **при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**;
      - ✓ **при проходе ПОСЕТИТЕЛЕЙ**;
      - ✓ **при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ**;
      - ✓ **при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**.
    - **Подтверждение прохода для ПОСЕТИТЕЛЕЙ**. Параметр позволяет выбрать дополнительное условие проведения процедуры верификации для посетителей:
      - ✓ **Постоянно**. Верификация проводится независимо от срока действия карты.
      - ✓ **В последний день действия идентификатора**. Верификация проводится в случае, если дата предъявления совпадает с датой окончания срока действия карты.
    - **Время ожидания подтверждения**. Параметр позволяет установить время, в течение которого контроллер ожидает подтверждение запроса от верифицирующего устройства.
    - **По истечении времени ожидания подтверждения генерировать событие**. Параметр позволяет выбрать событие, регистрируемое в случае отсутствия подтверждения прохода от ВВУ:
      - ✓ **Запрет прохода от ВВУ**. Рекомендуется в случае подключения ВВУ, имеющего только один выход разрешения прохода.
      - ✓ **Отказ от прохода, нет ответа от ВВУ**. Рекомендуется в случае подключения ВВУ, имеющего выходы как для разрешения прохода, так и для запрета прохода.
    - **Вероятность запуска верификации (0..100%)**. Параметр позволяет настроить выборочную верификацию. Например, при установке вероятности в 20 % верифицироваться будет каждый пятый пользователь.
  - **Счетчик**. Параметр позволяет задать время ожидания подтверждения.
- **Комиссионирование**.
  - **Время ожидания**. Параметр позволяет установить время, в течение которого контроллер ожидает подтверждение запроса.
  - **Время идентификации**.
- **Изымать идентификаторы ПОСЕТИТЕЛЕЙ**. Функция доступна только при наличии связи контроллера с сервером системы. Параметр позволяет выбрать условие, при котором идентификатор предъявленной карты доступа посетителя автоматически удаляется.
  - **Нет**. Идентификатор не удаляется автоматически.
  - **После любого прохода**. Идентификатор удаляется при первом предъявлении.
  - **После прохода в последний день действия идентификатора**. Идентификатор удаляется, если дата предъявления совпадает с датой окончания срока действия карты.
- **Поддержка картоприемника для идентификаторов ПОСЕТИТЕЛЕЙ**.

20.5. Вкладка «Генератор тревоги»

Вкладка выглядит следующим образом:

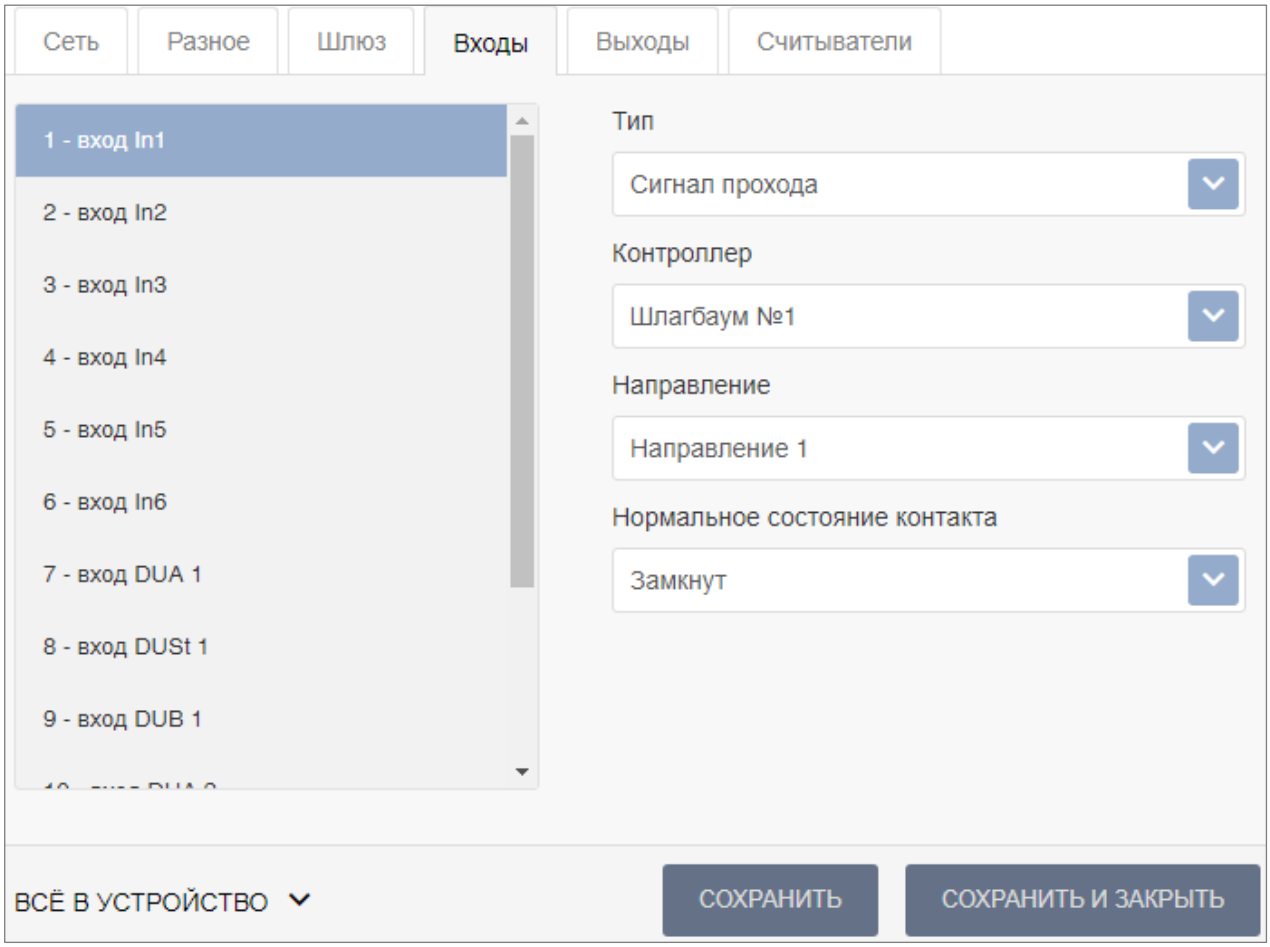


Ресурс связан с контроллером ИУ и позволяет выделить события, которые должны приводить к генерации тревоги в контроллере. Доступны следующие параметры:

- Вкладка **Генерация тревоги при предъявлении идентификатора** – параметр позволяет указать события, связанные с предъявлением карт доступа, при регистрации которых произойдет генерация тревоги:
  - **если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН**;
  - **если ИДЕНТИФИКАТОР ЗАПРЕЩЕН**;
  - **если ИСТЕК СРОК ДЕЙСТВИЯ**;
  - **если НАРУШЕНО ВРЕМЯ**;
  - **если НАРУШЕНА ЗОНАЛЬНОСТЬ**;
  - **если НАРУШЕН РЕЖИМ РАБОТЫ**;
  - **если НАРУШЕНО КОМИССИОНИРОВАНИЕ**.
- Вкладка **Генерация тревоги при несанкционированной разблокировке ИУ** – параметр позволяет для РКД *«Контроль»* и *«Закрыто»* указать, будет ли генерироваться тревога в случае механической разблокировки ИУ при помощи ключа, то есть без команды от контроллера:
  - **в РЕЖИМЕ РАБОТЫ "Контроль"**;
  - **в РЕЖИМК РАБОТЫ "Закрыто"**.
- Вкладка **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.

20.6. Вкладка «Входы»

Вкладка выглядит следующим образом:

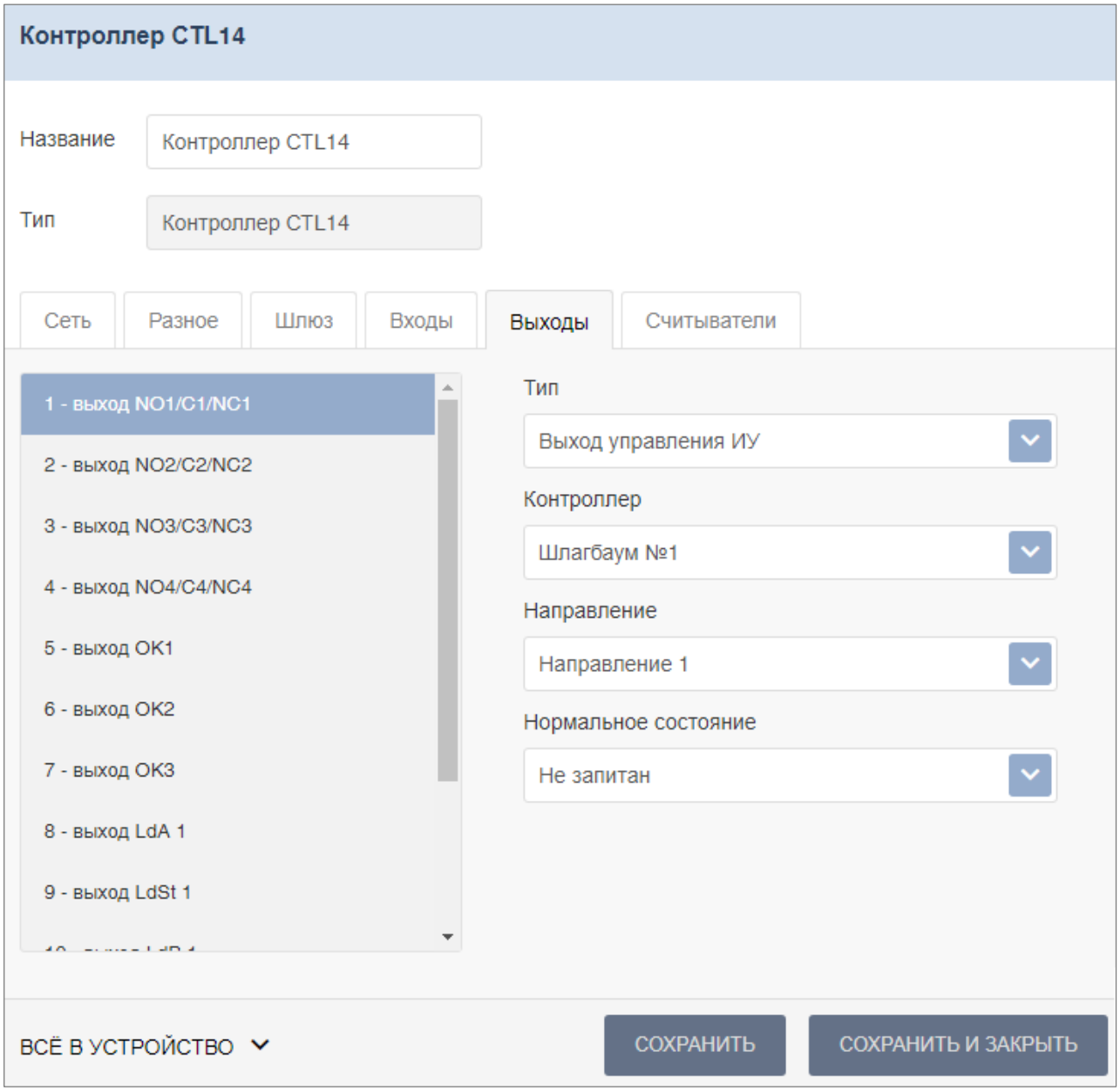


Для настройки входов доступны следующие параметры:

- **Тип**. Выпадающий список позволяет выбрать один из следующих типов:
  - **Обычный**. К данному входу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
  - **Кнопка ПДУ-выход**.
  - **Кнопка ПДУ-стоп**.
  - **Сигнал прохода**.
  - **Вход Fire Alarm**. Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода *ИУ Fire Alarm*.
  - **Вход подтверждения ВВУ**. Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае разрешения прохода.
  - **Вход запрета ВВУ**. Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае запрета прохода.
  - **Вход сброса тревоги**.
- **Контроллер**. Параметр позволяет выбрать контроллер.
- **Направление**. Параметр задает направление *ИУ*, к которому привязывается считыватель.
- **Нормальное состояние контакта** (*Замкнут / Разомкнут*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

20.7. Вкладка «Выходы»

Вкладка выглядит следующим образом:

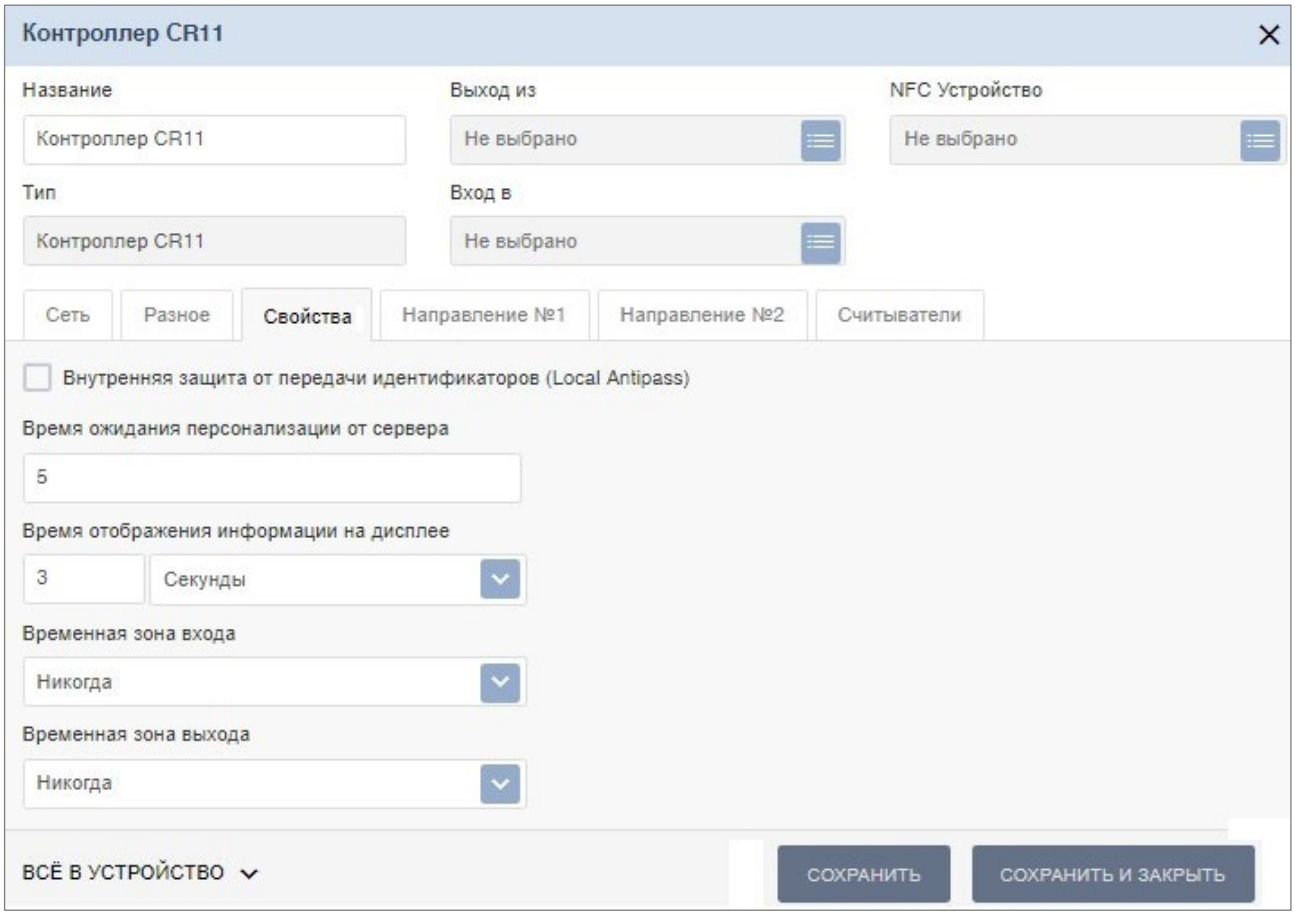


Для настройки выходов доступны следующие параметры:

- **Тип**. Выпадающий список позволяет выбрать один из следующих типов:
  - **Обычный**. К выходу подключено дополнительное оборудование, логика управления которым описывается через описание других устройств системы.
  - **Выход управления ИУ**. Предназначен для подключения к ИУ для передачи управляющих сигналов *Блокировать* / *Разблокировать*.
  - **Выход индикации ПДУ**. Предназначен для подключения к ПДУ для передачи управляющих сигналов смены индикации.
- **Контроллер**. Параметр позволяет выбрать контроллер.
- **Направление**. Параметр задает направление ИУ, к которому привязывается считыватель.
- **Нормальное состояние** (*Не запитан / Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода.

20.8. Вкладки «Свойства» и «Направление №» (для PERCo-CR11)

Вкладка **Свойства** выглядит следующим образом:



Для настройки доступны следующие параметры:

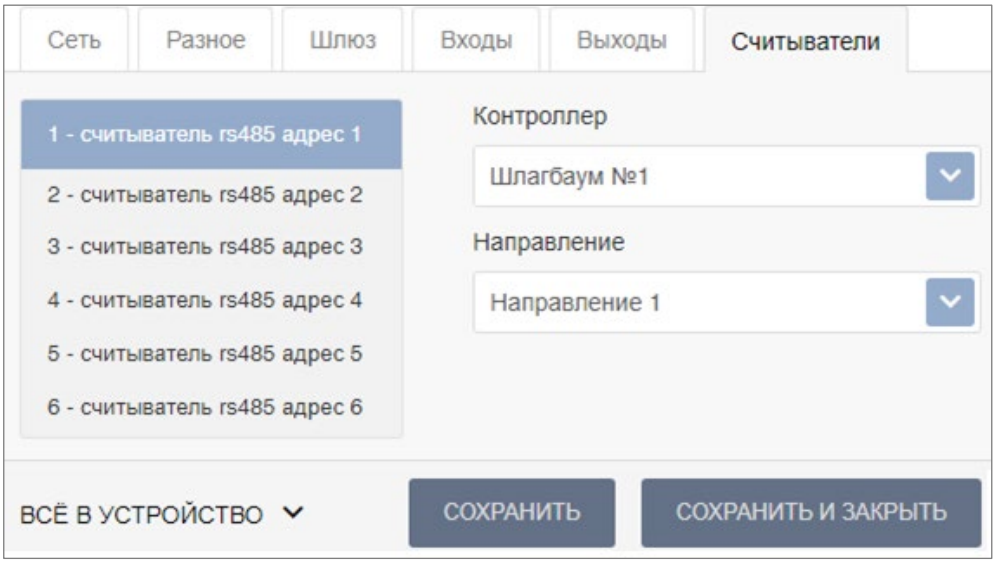
- **Внутренняя защита от передачи идентификаторов (Local Antipass)**. При установленном параметре контроллер отслеживает случаи повторного предъявления одного и того же идентификатора к тому же считывателю.
- **Время ожидания персонализации от сервера**. Время, в течении которого контроллер ожидает ответ сервера на запрос баланса.
- **Время отображения информации на дисплее**. Поле ввода позволяет задать время, в течение которого на ЖКИ контроллера отображается персональная информация, связанная с предъявленной картой доступа.
- **Временная зона входа**. Номер временной зоны, в соответствии с которой будет устанавливаться направление прохода "по умолчанию" = "Вход".
- **Временная зона выхода**. Номер временной зоны, в соответствии с которой будет устанавливаться направление прохода "по умолчанию" = "Выход".

На вкладке **Направление №...** доступны следующие параметры:

- **Защита от передачи идентификаторов СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ (Antipass)**. При установке флажка параметр позволяет отслеживать предъявление карты доступа сотрудника / посетителя к считывателю в случае нарушения им функции контроля зональности (Antipass).
- **Контроль времени для идентификаторов СОТРУДНИКОВ / ПОСЕТИТЕЛЕЙ**. При установке флажка параметр позволяет отслеживать предъявление карты доступа сотрудника / посетителя к считывателю в случае нарушения установленного критерия доступа по времени.
- **Время идентификации**.

20.9. Вкладка «Считыватели»

Вкладка выглядит следующим образом:

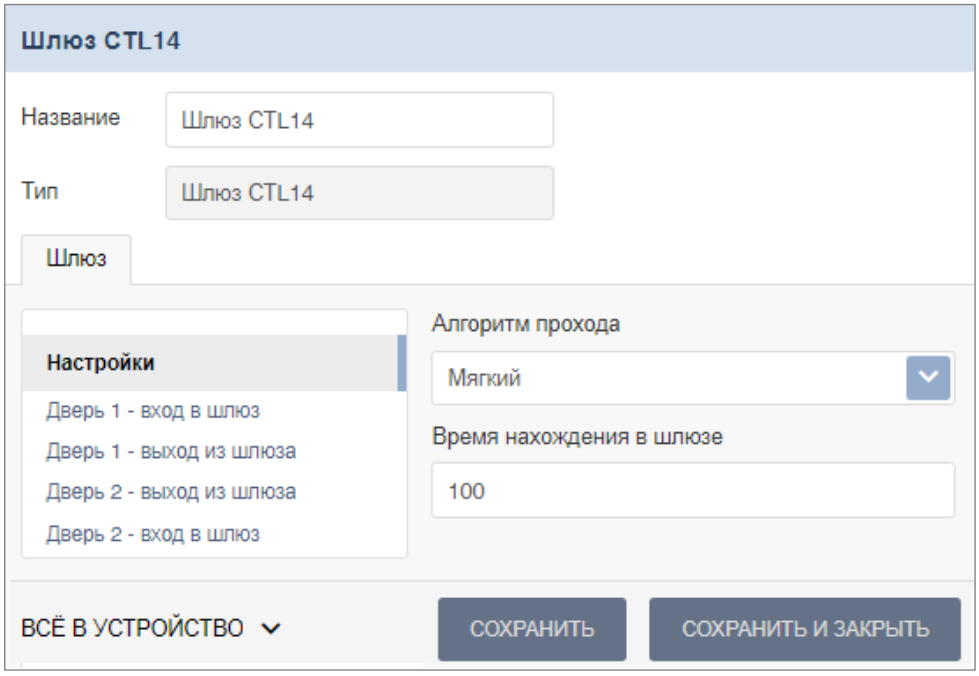


Для настройки доступны следующие параметры:

- **Контроллер**. Параметр позволяет выбрать контроллер.
- **Направление**. Параметр задает направление ИУ, к которому привязывается считыватель.

20.10. Вкладка «Шлюз»

Вкладка выглядит следующим образом:

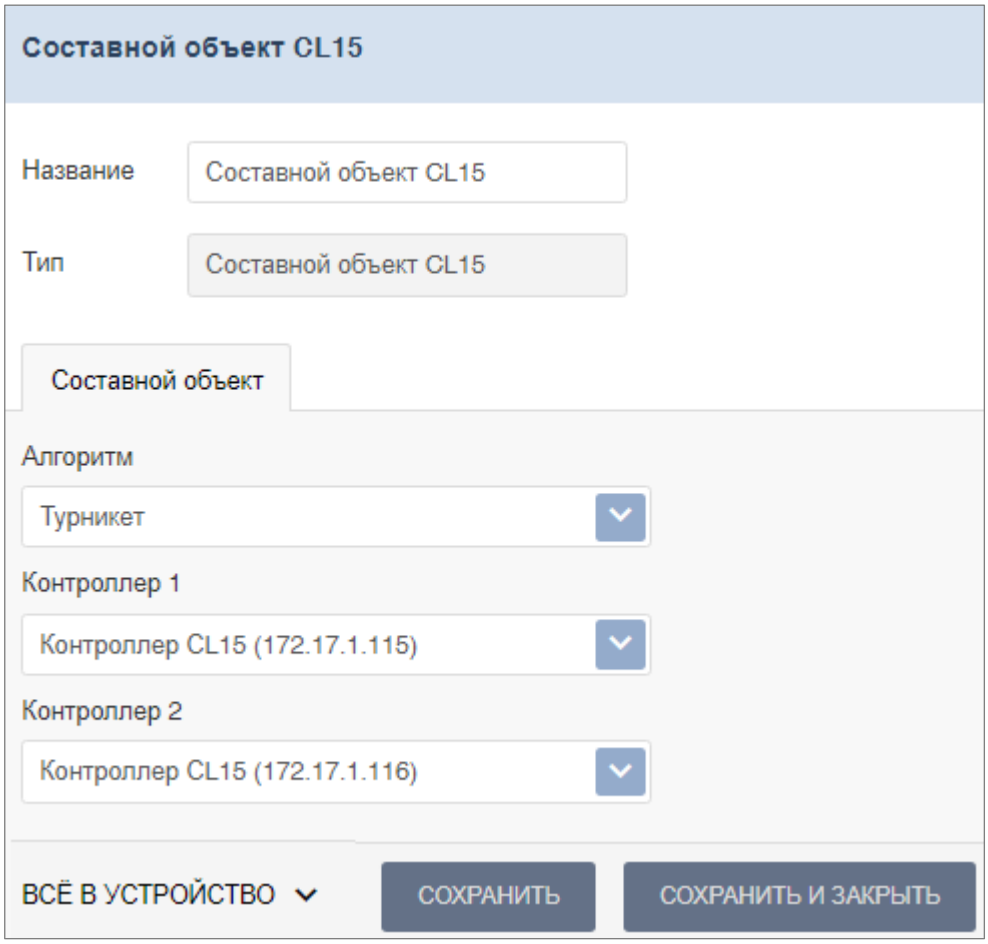


Для настройки доступны следующие параметры:

- **Алгоритм прохода**:
  - **Мягкий**. При использовании данного режима, если человек находится внутри шлюза, возможен проход вперед и выход назад.
  - **Жесткий**. При использовании данного режима, если человек находится внутри шлюза, возможен только проход вперед.
- **Время нахождения в шлюзе**. Параметр позволяет установить время для нахождения в шлюзе.

20.11. Вкладка «Составной объект»

Вкладка выглядит следующим образом:



Для настройки доступны следующие параметры:

- **Алгоритм прохода**. Выпадающий список позволяет выбрать один из алгоритмов прохода:
  - **Турникет**;
  - **Двусторонний замок**.
- **Контроллер**. Параметр предназначен для выбора устройств для формирования составного объекта.

21. Параметры контроллера Suprema

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

- **Сеть**;
- **Разное**;
- **Замок**;
- **Считыватель**.

Общие настройки световой и звуковой индикации для всех подключенных к системе контроллеров ***Suprema*** задаются на вкладке **Контроллеры Suprema** во всплывающем окне **Общие параметры**.

Примечание:

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

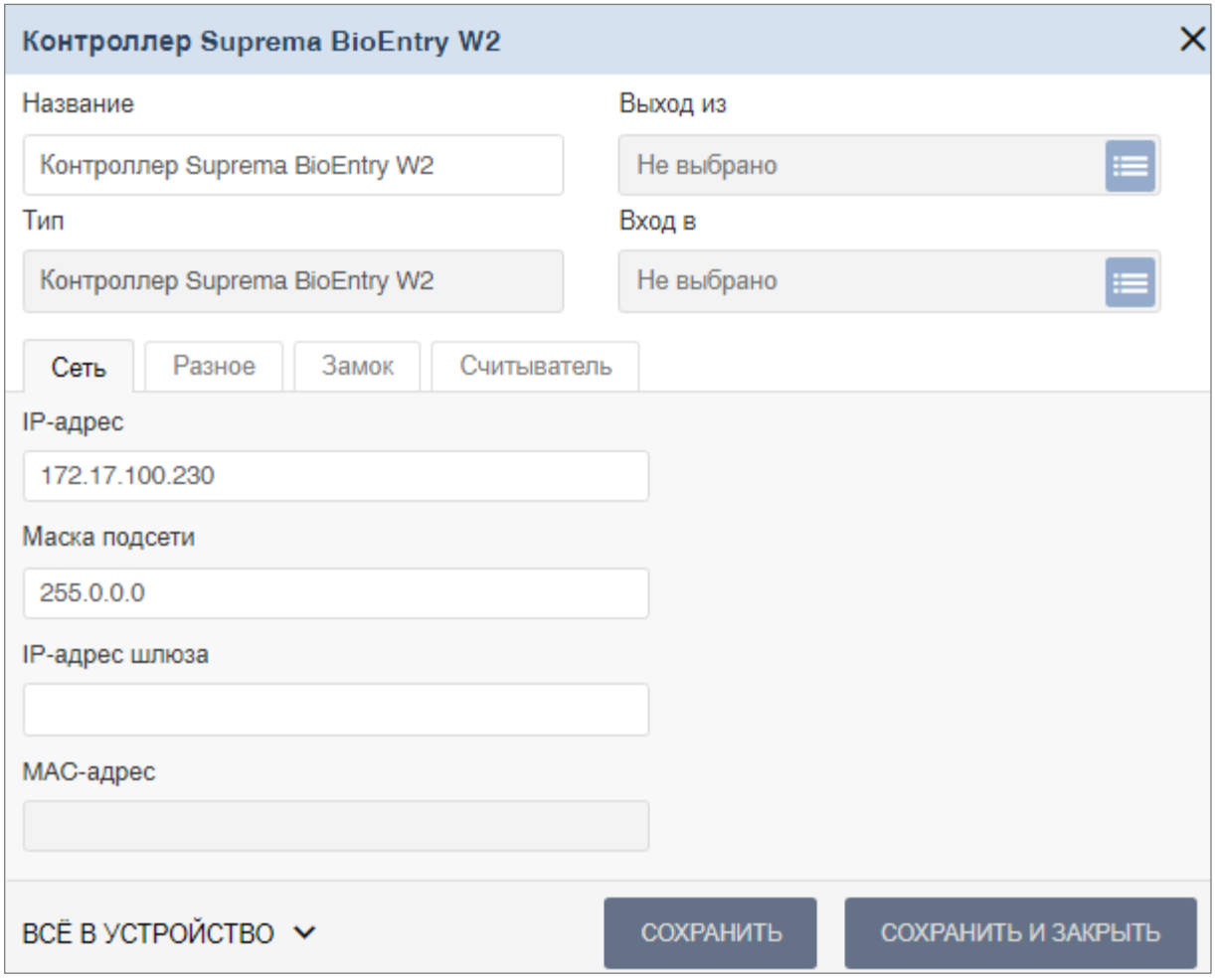
- для контроллера ***BioEntry W2*** – 1.1.1;
- для контроллера ***BioEntry Plus*** (платформа ***BioStar 2***) – 2.3.1.

21.1. Вкладка «Сеть»

Вкладка отображает информацию о следующих сетевых параметрах:

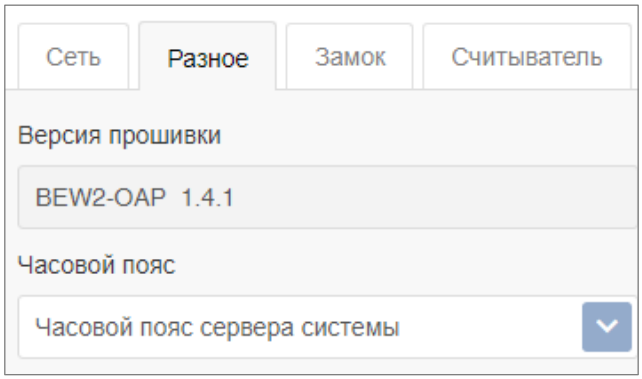
- **IP-адрес**;
- **Маска подсети**;
- **IP-адрес шлюза**;
- **MAC-адрес**.

Окно имеет следующий вид:



21.2. Вкладка «Разное»

Вкладка выглядит следующим образом:

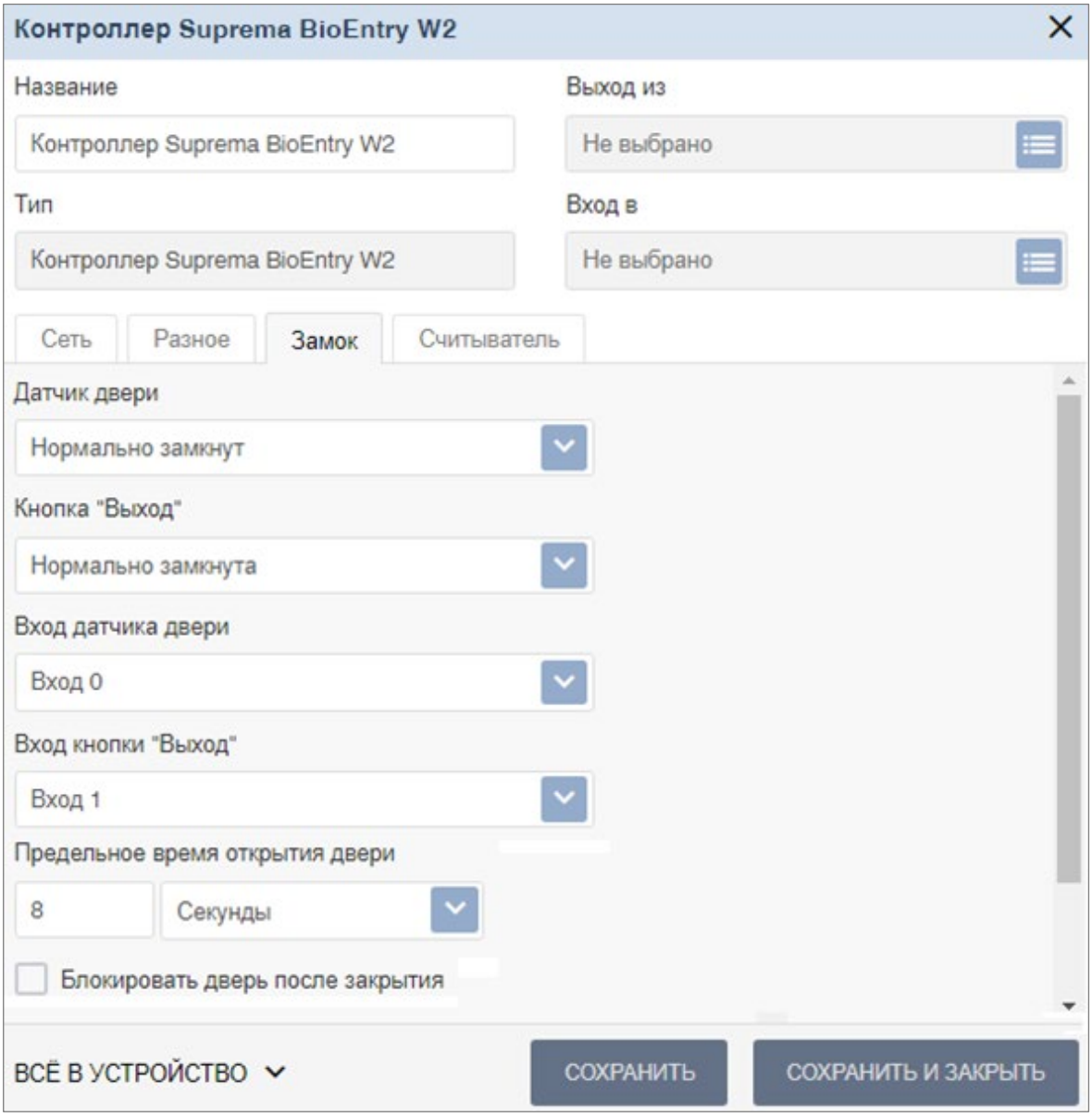


Вкладка содержит следующие настройки:

- **Версия прошивки** – в поле отображается версия прошивки встроенного ПО контроллера.
- **Часовой пояс** – выпадающий список позволяет выбрать часовой пояс контроллера.

21.3. Вкладка «Замок»

Вкладка **Замок** выглядит следующим образом:



Вкладка содержит следующие настройки:

- **Управление замком**. При установке флажка появляются другие настройки.
- **Датчик двери**. Раскрывающийся список позволяет выбрать нормальное состояние датчика двери (геркона):
  - **Нормально замкнут**;
  - **Нормально разомкнут**.

Примечание:

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

- **Кнопка "Выход"**. Раскрывающийся список позволяет выбрать нормальное состояние кнопки **"Выход"**:
  - **Нормально замкнута**;
  - **Нормально разомкнута**.

Примечание:

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

- **Вход датчика двери**. Раскрывающийся список позволяет выбрать, к какому входу контроллера будет подключаться **датчик двери**:
  - **Вход 0**;
  - **Вход 1**.
- **Вход кнопки "Выход"**. Раскрывающийся список позволяет выбрать, к какому входу контроллера будет подключаться **кнопка "Выход"**:
  - **Вход 0**;
  - **Вход 1**.

Примечание:

Категорически не рекомендуется подключать **датчик двери** и кнопку **' Выход'** на один и тот же вход контроллера.

- **Предельное время открытия двери** – время, по истечении которого контроллер управления доступом перейдет в состояние тревоги по причине того, что дверь не была закрыта и заблокирована. Раскрывающийся список позволяет задать значение и выбрать единицы измерения предельного времени открытия двери:
  - **Миллисекунды**;
  - **Секунды**;
  - **Бесконечность**.
- При установке флажка **Блокировать дверь после закрытия** дверь будет заблокирована сразу после закрытия.
- **Время открытия двери** – время, на которое дверь разблокируется контроллером управления доступом для открытия. Раскрывающийся список позволяет задать значение и выбрать единицы измерения времени открытия двери:
  - **Миллисекунды**;
  - **Секунды**;
  - **Бесконечность**.
- При установке флажка **Регистрация прохода по предъявлению идентификатора** факт прохода будет зарегистрирован сразу же после предъявления идентификатора, т.е. без ожидания соответствующих сигналов с турникета, датчика двери и т.д.
- **Подтверждение прохода от контроллера** – раскрывающийся список позволяет выбрать

для подтверждения прохода тот контроллер ***PERCo***, входом ПДУ которого управляет выход контроллера ***Suprema***.

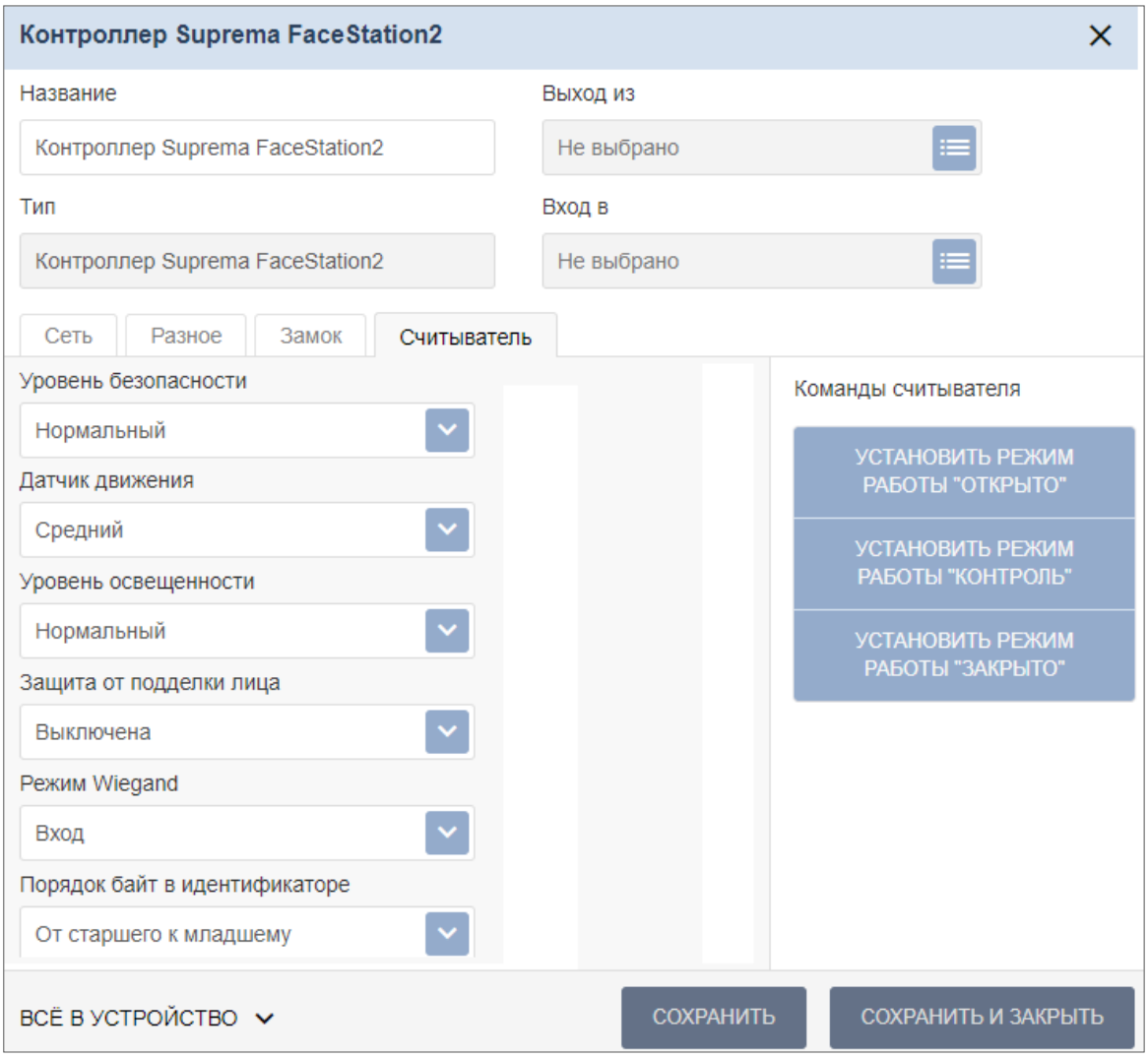
Примечание:

Опция используется при интеграции ЭП или контроллера ***PERCo*** с оборудованием ***Suprema*** для корректного учета рабочего времени.

Если выбран подтверждающий контроллер ***PERCo***, то после прохода от него ожидается событие *«Проход по команде от ДУ»*, после чего в журнал событий системы записывается событие прохода, в противном случае – событие *«Отказ от прохода»*.

21.4. Вкладка «Считыватель»

Вкладка **Считыватель** выглядит следующим образом:



Вкладка содержит следующие настройки:

1. **<u>Для контроллеров со сканерами отпечатков пальцев:</u>**
   - **Чувствительность**. Раскрывающийся список позволяет задать уровень чувствительности считывателя:
     - **Низкая**;
     - **Уровень 1**;
     - **Уровень 2**;
     - **Уровень 3**;
     - **Уровень 4**;
     - **Уровень 5**;

- **Уровень 6**;
- **Высокая**.

Примечание:

Параметр **Чувствительность** определяет чувствительность датчика сканирования отпечатков пальцев. При высоком заданном уровне чувствительности обеспечивается высокое качество и скорость сканирования, при низком уровне чувствительности уменьшается влияние факторов внешней среды – температуры, влажности воздуха, освещенности помещения, чистоты сканируемой поверхности (подушечек пальцев). Производителем рекомендовано использование высокого уровня чувствительности по умолчанию, понижение уровня чувствительности осуществляется при необходимости в зависимости от условий эксплуатации.

2. <u>Для терминалов распознавания лиц:</u>

Примечание:

Описание параметров настройки терминала распознавания лиц подробно дано в эксплуатационной документации на данное изделие.

- **Уровень безопасности**:
  - **нормальный**;
  - **высокий**;
  - **самый высокий**.
- **Датчик движения**:
  - **выключен**;
  - **близкий**;
  - **средний**;
  - **далекий**.
- **Уровень освещенности**:
  - **нормальный**;
  - **высокий**;
  - **автоматический**.
- **Защита от подделки лица**:
  - **выключена**;
  - **уровень 1**;
  - **уровень 2**;
  - **уровень 3**.
- **Режим Wiegand**:
  - **вход**;
  - **выход**.
- **Порядок байт в идентификаторе**:
  - **от старшего к младшему**;
  - **от младшего к старшему**.

Поддерживаются следующие команды считывателя:

- **Установить режим работы «Открыто»** – при переходе в режим работы **«Открыто»** происходит разблокировка исполнительного устройства, проход осуществляется свободно без предъявления карт доступа и / или сканирования биометрических данных;
- **Установить режим работы «Контроль»** – в режиме работы **«Контроль»** проход осуществляется в нормальном режиме по предъявлении карт доступа и / или сканированию биометрических данных;
- **Установить режим работы «Закрыто»** – в режиме работы **«Закрыто»** происходит блокировка исполнительного устройства, проход блокируется, считыватель не реагирует на предъявление карт доступа и / или сканирование биометрических данных.

22. Параметры контроллера ZKTeco

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

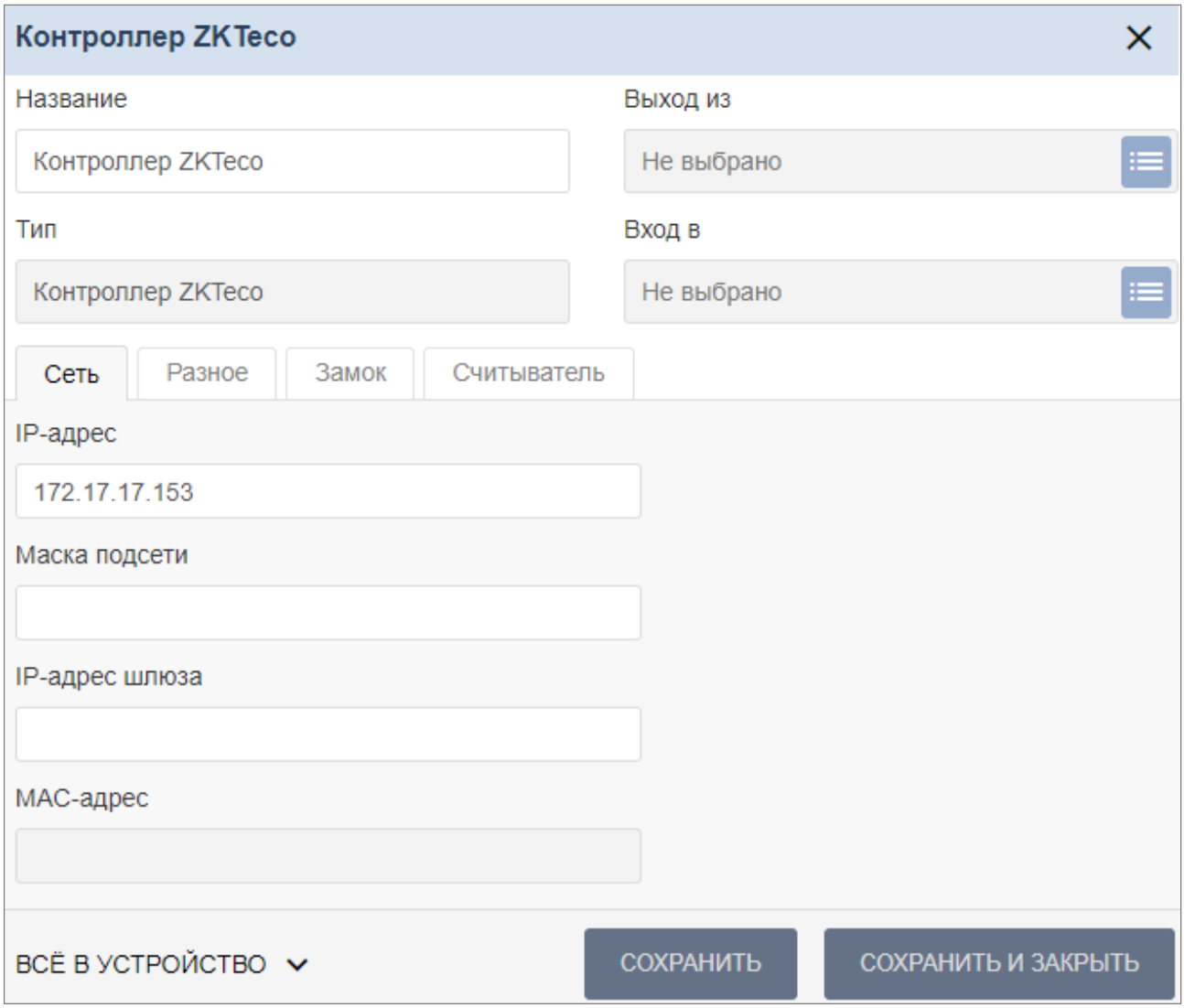
- **Сеть**;
- **Разное**;
- **Замок**;
- **Считыватель**.

22.1. Вкладка «Сеть»

Вкладка отображает информацию о следующих сетевых параметрах:

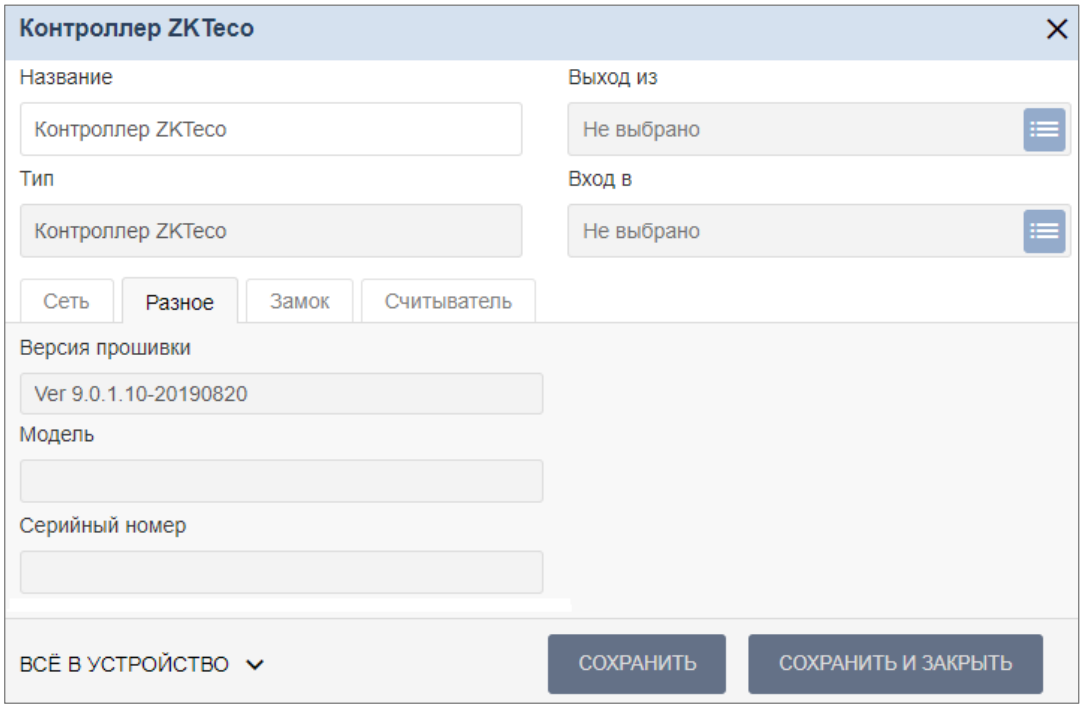
- **IP-адрес**;
- **Маска подсети**;
- **IP-адрес шлюза**;
- **MAC-адрес**.

Окно имеет следующий вид:



22.2. Вкладка «Разное»

Вкладка имеет следующий вид:

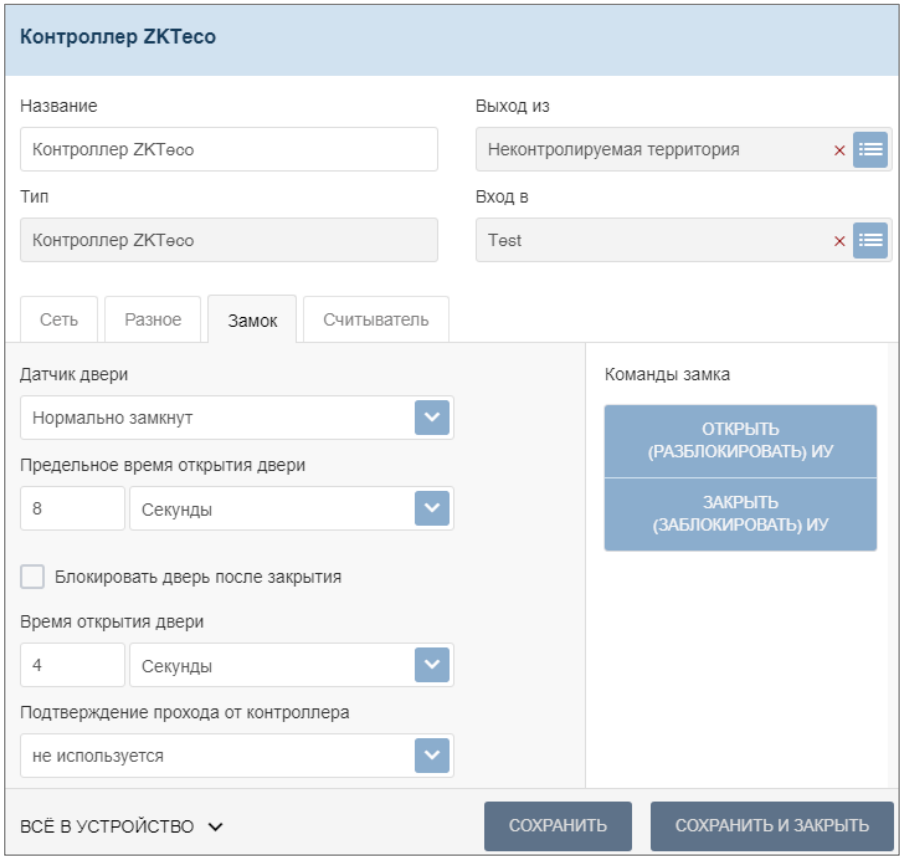


Вкладка содержит следующую информацию:

- **Версия прошивки** – в поле отображается версия прошивки встроенного ПО контроллера.
- **Модель** и **Серийный номер** – в этих полях отображается соответствующая информация о контроллере (не для всех моделей).

22.3. Вкладка «Замок»

Вкладка **Замок** имеет следующий вид:



Вкладка содержит следующие настройки:

- **Датчик двери**. Раскрывающийся список позволяет выбрать нормальное состояние датчика двери (геркона):
  - **Нормально замкнут**;
  - **Нормально разомкнут**.

Примечание:

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

- **Предельное время открытия двери** – время, по истечении которого контроллер перейдет в состояние тревоги по причине того, что дверь не была закрыта и заблокирована (в секундах).
- При установке флажка **Блокировать дверь после закрытия** дверь будет заблокирована сразу после закрытия.
- **Время открытия двери** – время, на которое дверь разблокируется контроллером управления доступом для открытия (в секундах).
- **Подтверждение прохода от контроллера** – раскрывающийся список позволяет выбрать для подтверждения прохода тот контроллер ***PERCo***, входом ПДУ которого управляет выход контроллера ***ZKTeco***.

Примечание:

Опция может использоваться при интеграции ЭП и контроллеров ***PERCo*** с оборудованием ***ZKTeco*** для корректного учета рабочего времени.

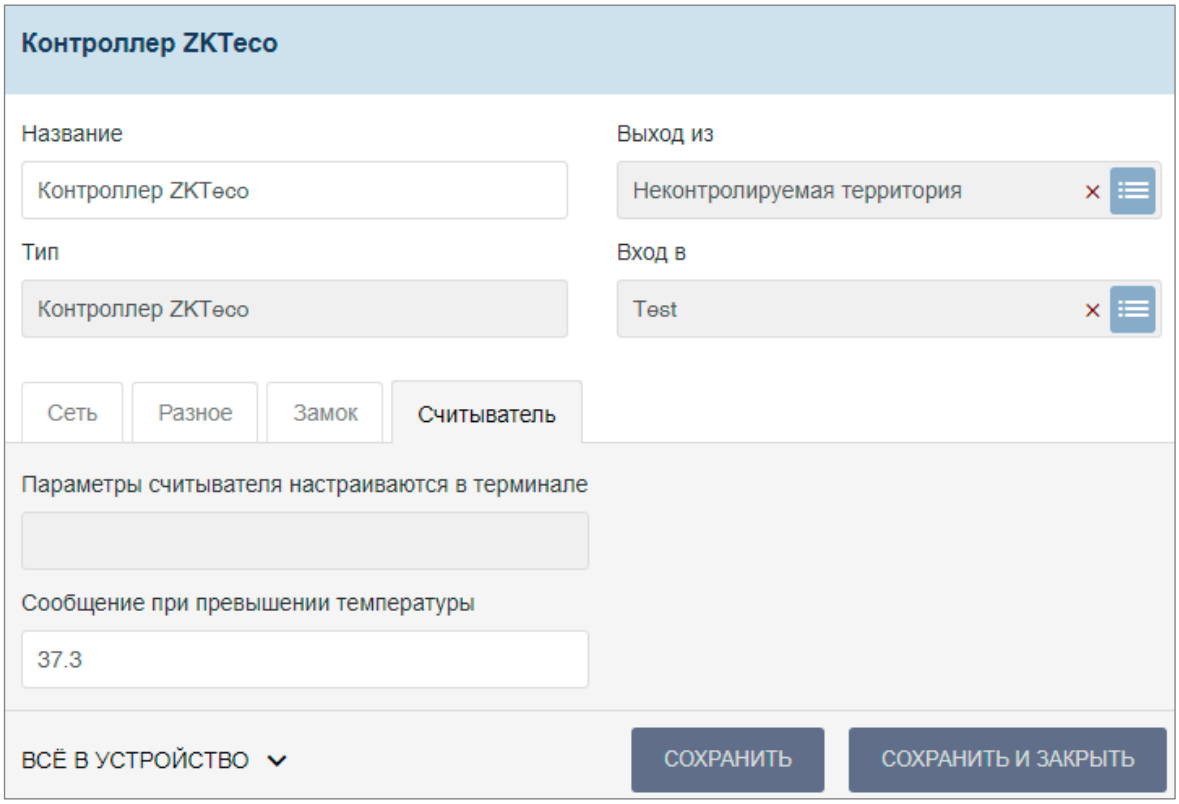
Если выбран подтверждающий контроллер ***PERCo***, то после прохода от него ожидается событие *«Проход по команде от ДУ»*, после чего в журнал событий системы записывается событие прохода, в противном случае – событие *«Отказ от прохода»*.

Поддерживаются следующие команды замка:

- **Открыть (разблокировать) ИУ**;
- **Закрыть (заблокировать) ИУ**;
- **Снять тревогу**.

22.4. Вкладка «Считыватель»

Вкладка **Считыватель** выглядит следующим образом:



Вкладка содержит следующие настройки:

Примечание:

Параметры считывателя и режимы доступа настраиваются в терминале (см. эксплуатационную документацию на терминал).

- **Сообщение при превышении температуры** – поле для ввода порогового значения температуры, при превышении которого в журнале событий системы будет формироваться сообщение *«Проход с повышенной температурой»*. При необходимости по этому сообщению можно настроить реакции на события в подразделе **«Реакции на события»** раздела **«Администрирование»**.

  Сообщения в системе ***PERCo-Web*** формируются только в том случае, если в терминале ***ZKTeco*** не стоит запрет прохода при указанной температуре.

  Также возможен вариант сообщения *«Проход без медицинской маски»*, если в терминале ***ZKTeco*** активна опция *«Обнаруживать ношение маски»*, но не стоит запрет прохода при ее отсутствии.

Внимание!

Перед началом работы задайте необходимые параметры в терминале ***ZKTeco*** в подразделе *«Управление защитой»* раздела *«Система»*.

Примеры реализации:

Пример № 1:

- В терминале ***ZKTeco***:
  - активируйте опцию *«Измерять температуру с ИК»*;
  - укажите верхний порог температуры тревоги 37°С;
  - поставьте запрет прохода при превышении порога.
- В системе ***PERCo-Web***:
  - в поле **Сообщение при превышении температуры** укажите 37°С.

  В таком случае при превышении порога температуры проход будет запрещен, сообщения в журнале событий системы формироваться не будут.

Пример № 2:

- В терминале ***ZKTeco***:
  - активируйте опцию *«Измерять температуру с ИК»*;
  - укажите верхний порог температуры тревоги 37°С;
  - не ставьте запрет прохода при превышении порога.
- В системе ***PERCo-Web***:
  - в поле **Сообщение при превышении температуры** укажите 37°С.

  В таком случае при превышении порога температуры проход будет разрешен, а в журнале событий системы будут формироваться сообщения *«Проход с повышенной температурой»*.

Пример № 3:

- В терминале ***ZKTeco***:
  - активируйте опцию *«Измерять температуру с ИК»*;
  - укажите верхний порог температуры тревоги 38°С;
  - поставьте запрет прохода при превышении порога.
- В системе ***PERCo-Web***:
  - в поле **Сообщение при превышении температуры** укажите 37°С.

  В таком случае при температуре от 38°С проход будет запрещен, сообщения в журнале событий системы формироваться не будут. Однако при температуре от 37°С до 38°С проход будет разрешен, а в журнале событий системы будут формироваться сообщения *«Проход с повышенной температурой»*.

Пример № 4:

- В терминале ***ZKTeco***:
  - активируйте опцию *«Обнаруживать ношение маски»*;
  - поставьте запрет прохода без ношения маски.

  В таком случае при отсутствии на сотруднике / посетителе медицинской маски проход будет запрещен, сообщения в журнале событий системы формироваться не будут.

Пример № 5:

- В терминале ***ZKTeco***:
  - активируйте опцию *«Обнаруживать ношение маски»*;
  - не ставьте запрет прохода без ношения маски.

  В таком случае при отсутствии на сотруднике / посетителе медицинской маски проход будет разрешен, а в журнале событий системы будут формироваться сообщения *«Проход без медицинской маски»*.

23. Параметры видеокамеры

Перечисленные ниже вкладки предназначены для настройки IP-видеокамер (в т.ч. видеокамер стандарта ONVIF) и аналоговых видеокамер, подключенных к IP-видеосерверам. Доступны следующие вкладки:

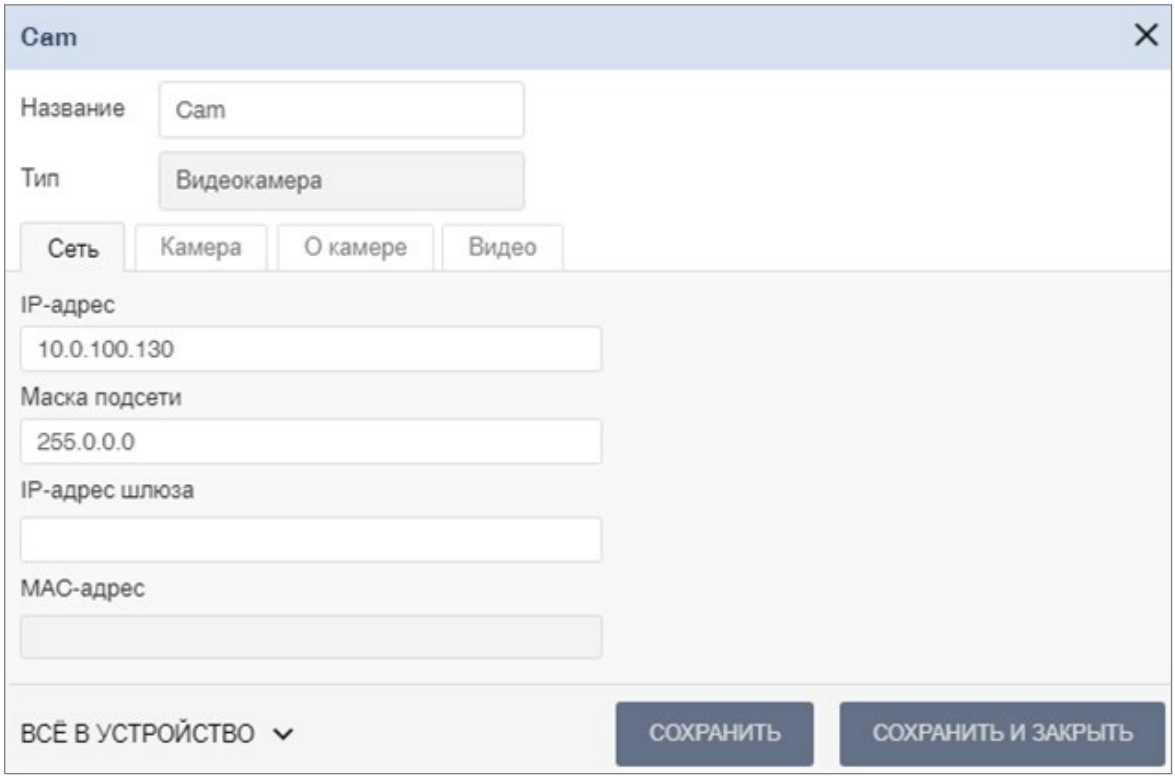
- **Сеть**;
- **Камера**;
- **О камере**;
- **Видео**.

23.1. Вкладка «Сеть»

Вкладка **Сеть** отображает информацию о следующих сетевых параметрах:

- **IP-адрес**;
- **Маска подсети**;
- **IP-адрес шлюза**;
- **MAC-адрес**.

Окно имеет следующий вид:



23.2. Вкладка «Камера»

На вкладке **Камера** необходимо ввести данные для авторизации при управлении камерой.

Параметры камеры:

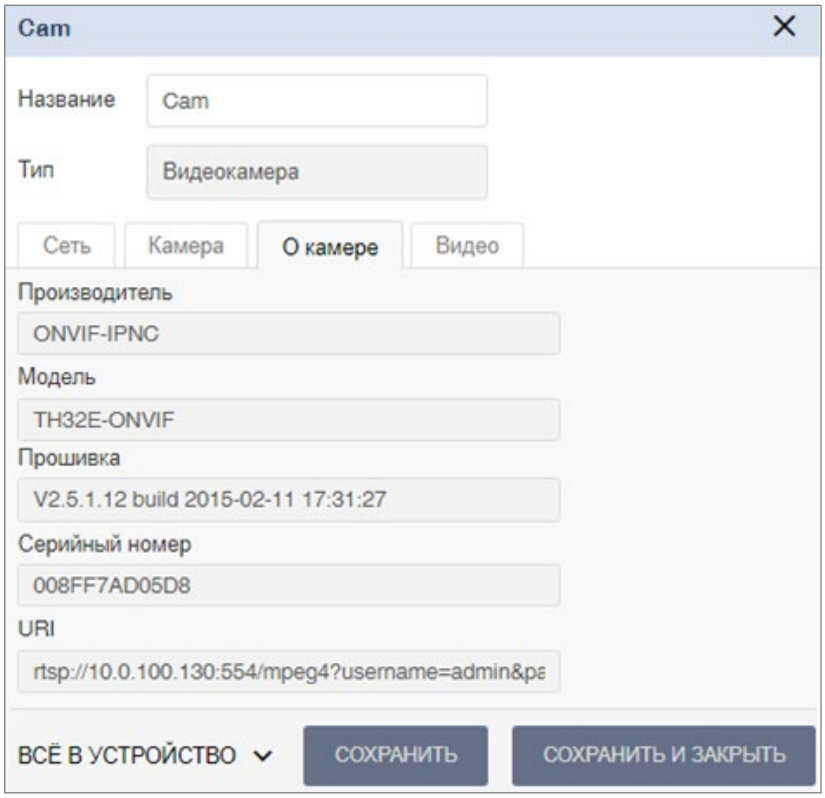
- **Логин**;
- **Пароль**.

23.3. Вкладка «О камере»

Вкладка **О камере** отображает информацию о следующих сетевых параметрах:

- **Производитель**. Поле отображает наименование производителя камеры.
- **Модель**. Поле отображает наименование модели камеры.
- **Прошивка**. Поле отображает текущую версию прошивки камеры.
- **Серийный номер**. Поле отображает серийный номер камеры.
- **URI**. Поле отображает URI (Uniform Resource Identifier) – унифицированный идентификатор ресурса (камеры).

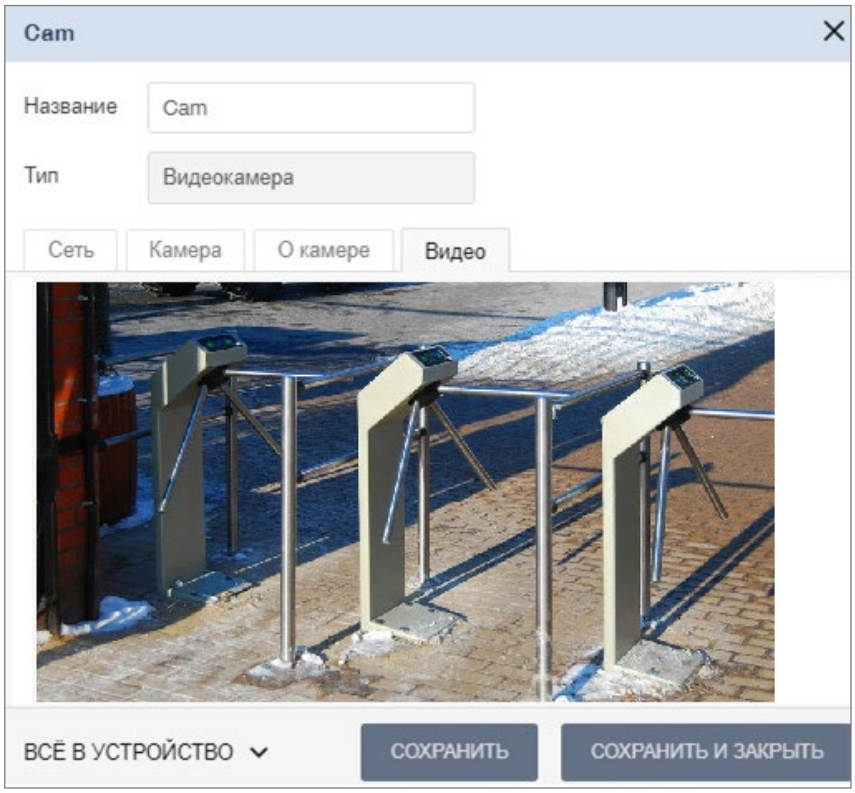
Окно имеет следующий вид:



23.4. Вкладка «Видео»

На вкладке **Видео** отображается видеосъемка с выбранной камеры в режиме реального времени. Для того, чтобы перейти в полноэкранный режим, кликните левой кнопкой мыши по иконке в правом верхнем углу изображения с камеры. Для выхода из полноэкранного режима кликните левой кнопкой мыши по иконке в правом верхнем углу изображения с камеры.

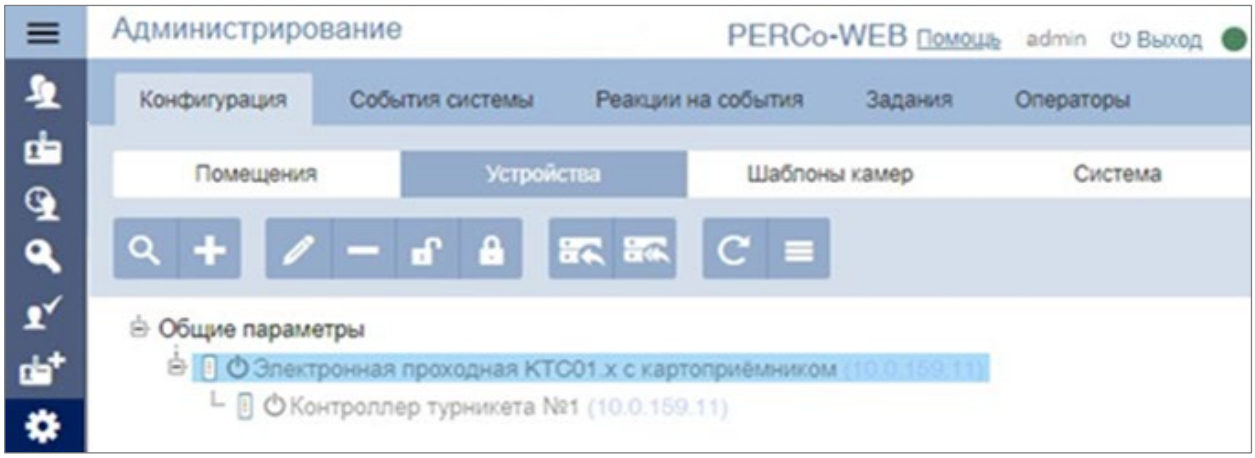
Окно имеет следующий вид:



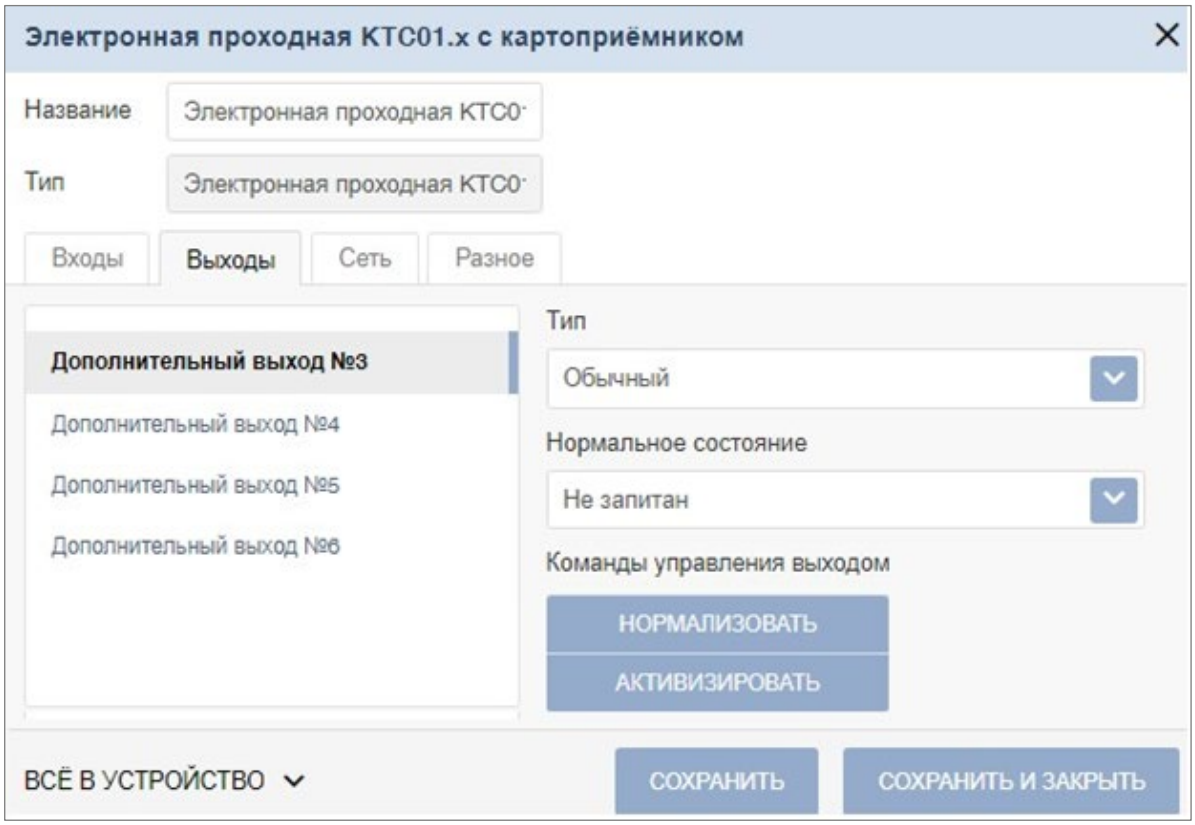
24. Настройка контроллера СКУД PERCo для работы с картоприемником

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:

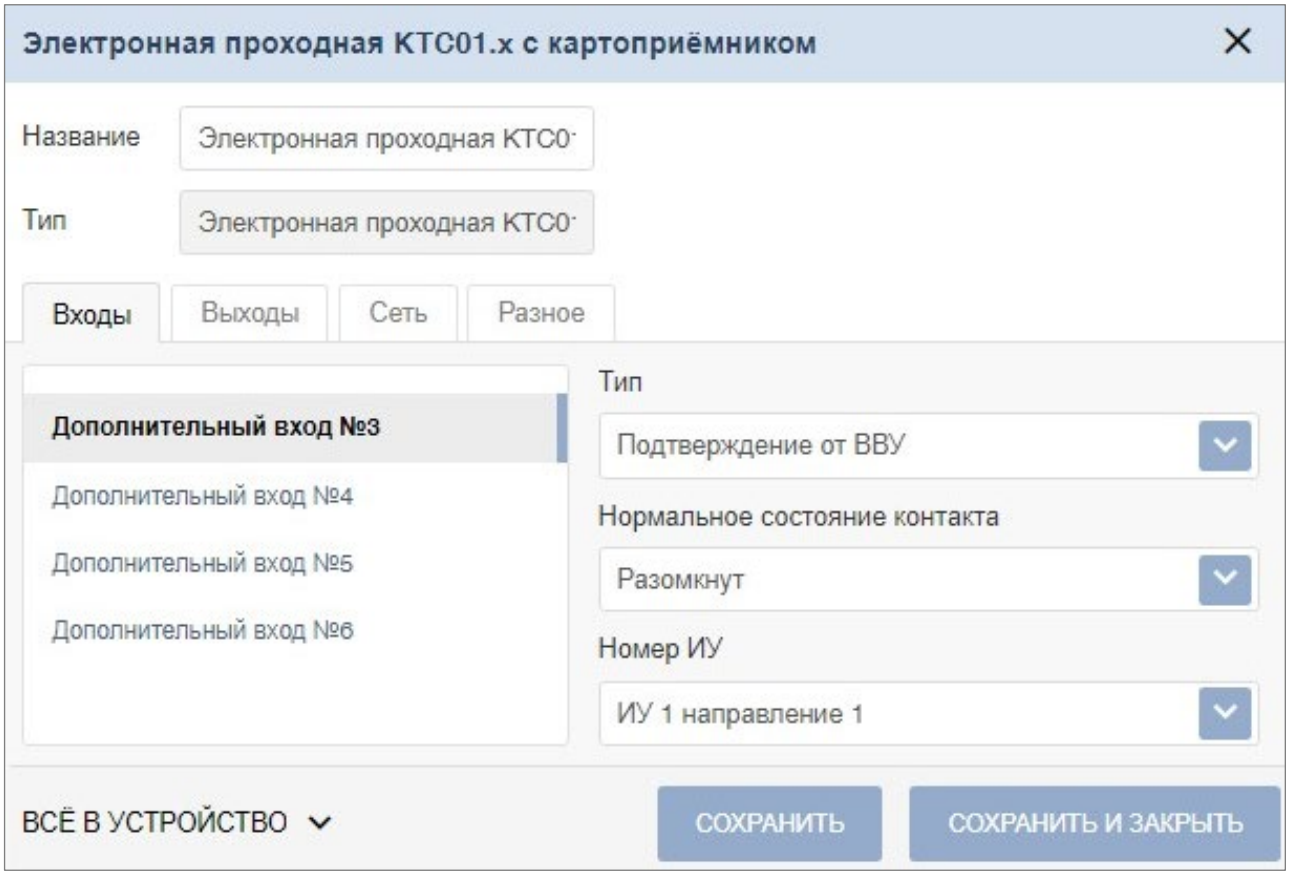
1. Войдите в систему, используя Web-браузер.
2. Используя панель навигации, перейдите в раздел **«Администрирование»** в подраздел **«Конфигурация»** на вкладку **Помещения**.
3. В рабочей области страницы выделите основной контроллер, к которому физически подключен картоприемник:



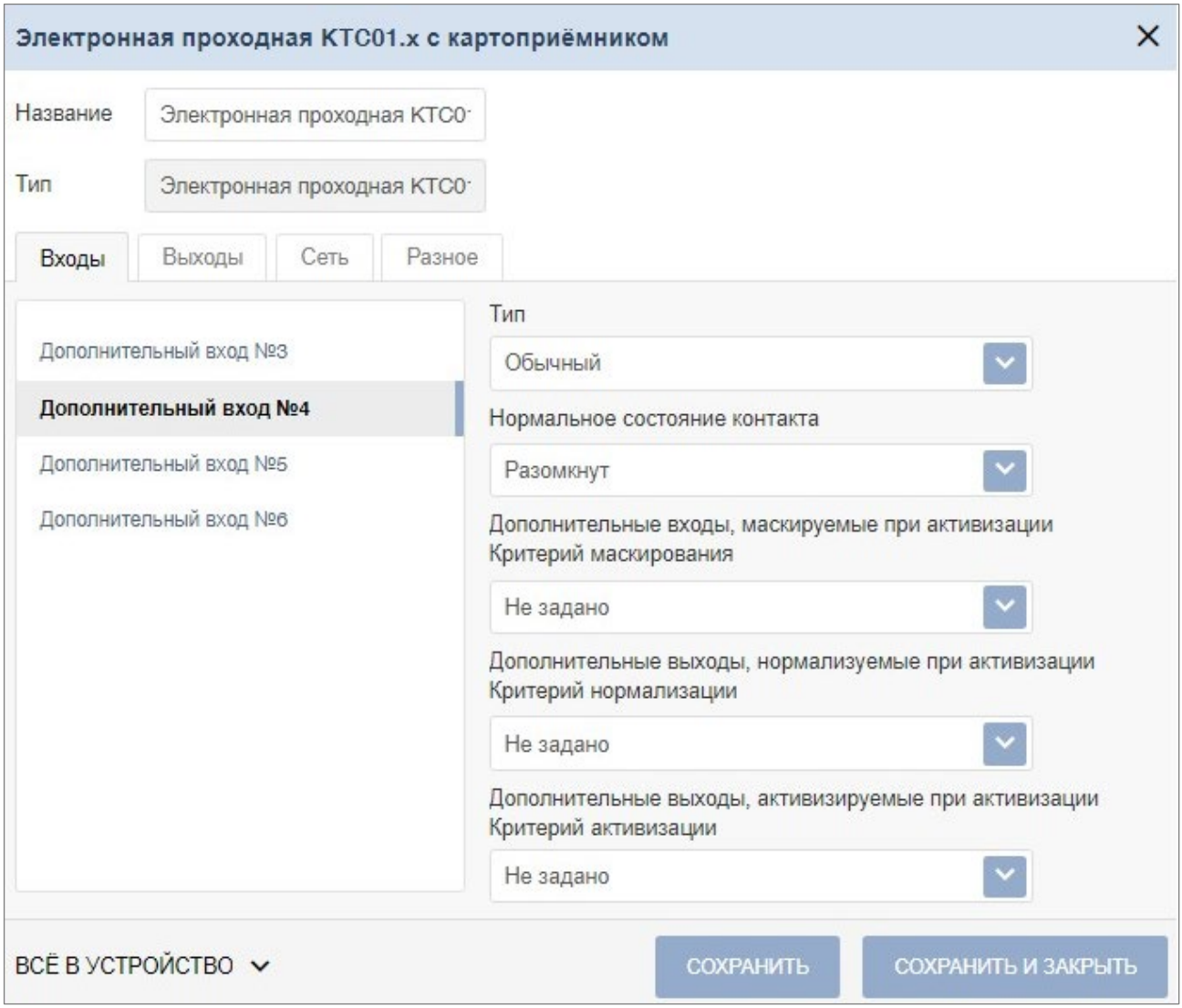
4. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется окно, отражающее название контроллера.
5. В открывшемся окне перейдите на вкладку **Выходы**:



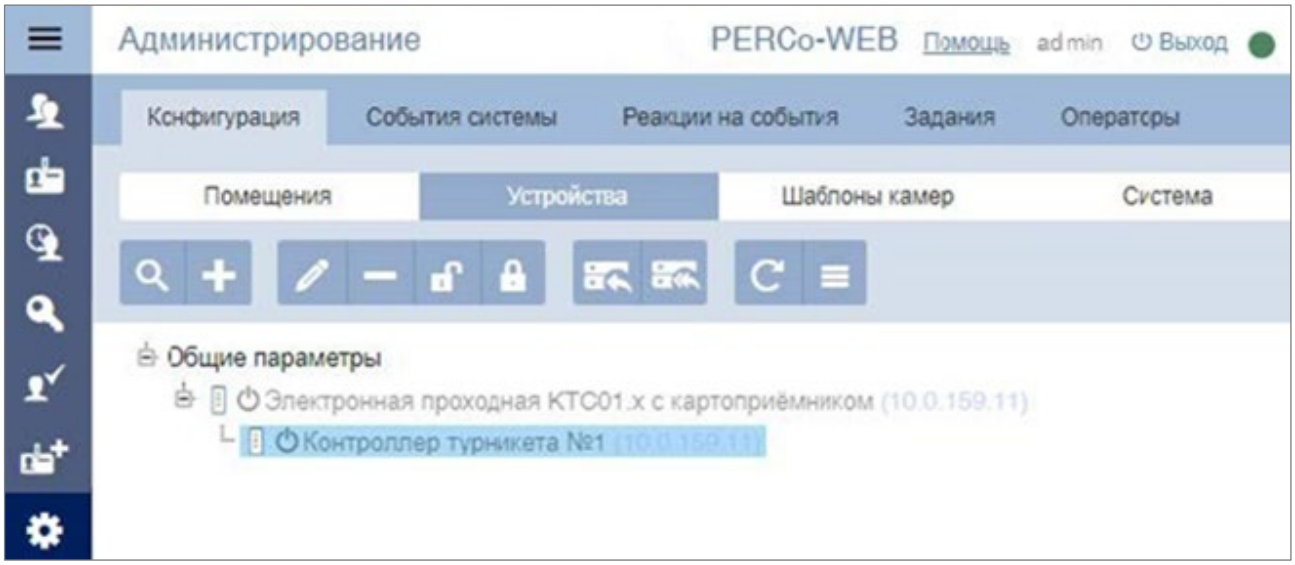
6. В рабочей области окна выберите **Дополнительный выход №…** (номер выхода должен соответствовать выходу контроллера, к которому физически подключен вход *«Изъять карту»* картоприемника).
7. Установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
   - для параметра **Тип** значение **Обычный**;
   - для параметра **Нормальное состояние** значение **Не запитан**.
8. Перейдите на вкладку **Входы**.
9. Если картоприемник выступает в качестве внешнего верифицирующего устройства для контроллера (сигнал *«Карта изъята»* поступает на отдельный вход контроллера), то в рабочей области окна выберите **Дополнительный вход №…** (номер входа контроллера, к которому физически подключен выход *«Карта изъята»* картоприемника) и установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
   - для параметра **Тип** значение **Вход подтверждения ВВУ**;
   - для параметра **Нормальное состояние контакта** значение **Разомкнут**;
   - для параметра **Номер ИУ** значение **ИУ… направление…** (номер ИУ и номер направления должны соответствовать тем, которые контролируются картоприемником):



10. При необходимости настройте реакцию системы на сигнал от картоприемника *«Авария»*. Для этого в рабочей области окна выберите **Дополнительный вход №…** (номер входа должен соответствовать входу контроллера, к которому физически подключен выход *«Авария»* картоприемника) и установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
    - для параметра **Тип** значение **Обычный**;
    - для параметра **Нормальное состояние контакта** значение **Разомкнут**.
11. Используя параметры активизации или нормализации выходов, настройте требуемую реакцию контроллера.



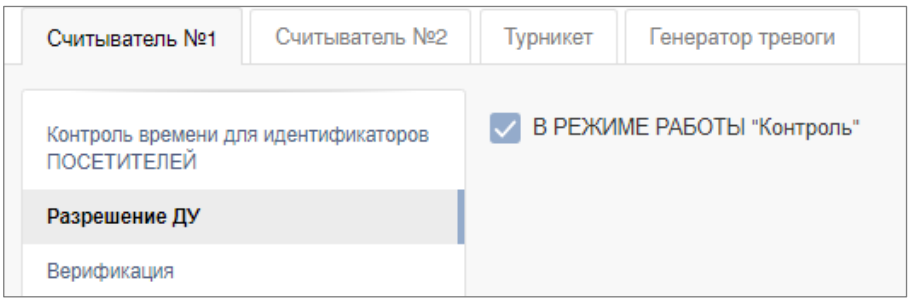
12. Нажмите кнопку **Сохранить и закрыть**. Окно, отражающее название контроллера, будет закрыто.
13. В рабочей области страницы в составе основного контроллера выделите контроллер ИУ, который контролируется картоприемником:



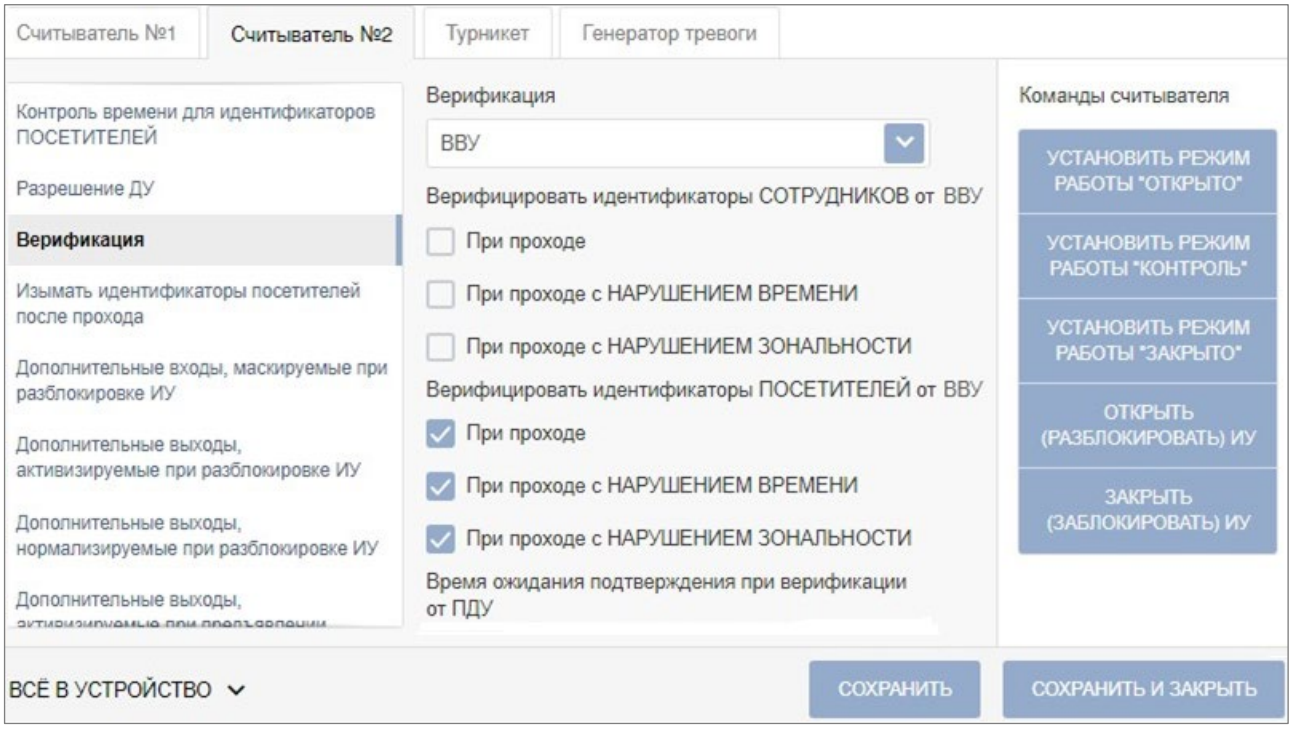
14. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется окно,

отражающее название контроллера.

15. Перейдите на вкладку ресурса **Считыватель №…** (номер считывателя должен соответствовать считывателю, контролируемому картоприемником).
16. Подтверждением изъятия карты для контроллера доступа является сигнал от картоприемника *«Карта изъята»*. Для настройки подтверждения в левой части рабочей области окна для параметра **Верификация** установите значение:
    - **ВВУ**, если картоприемник выступает в качестве внешнего верифицирующего устройства для контроллера (сигнал *«Карта изъята»* поступает на отдельный вход контроллера);
    - **ПДУ**, если выход *«Карта изъята»* картоприемника подключен к контроллеру параллельно ПДУ. В этом случае также нужно установить для параметра из левой части окна **Разрешение ДУ** флажок в рабочей области для значения **В РЕЖИМЕ РАБОТЫ «Контроль»**:



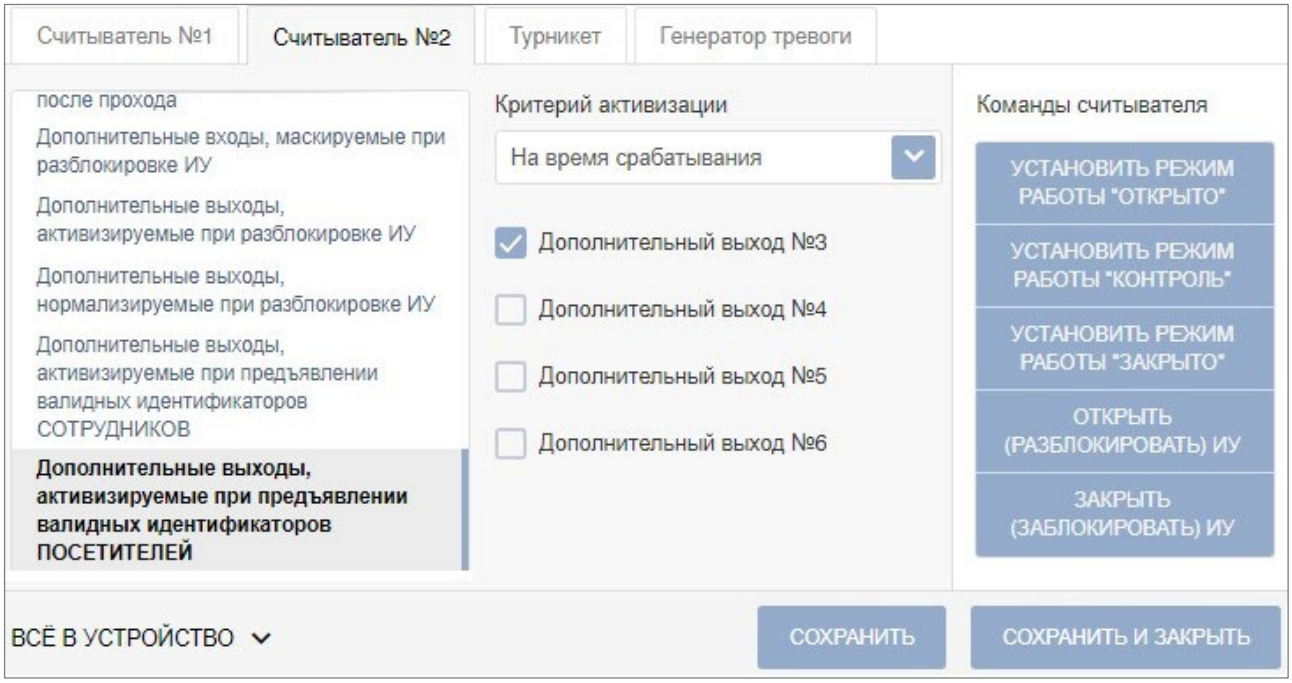
17. Установите в рабочей области окна для параметра **Верифицировать идентификаторы ПОСЕТИТЕЛЕЙ от ВВУ** (или, соответственно, **от ПДУ**) флажки:
    - **при проходе**;
    - **при проходе с НАРУШЕНИЕМ ВРЕМЕНИ**;
    - **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**.
18. Установите в рабочей области окна необходимое значение параметра **Время ожидания подтверждения при верификации от ВВУ** (или, соответственно, **от ПДУ**), в течение которого контроллер должен ожидать сигнал *«Карта изъята»*:



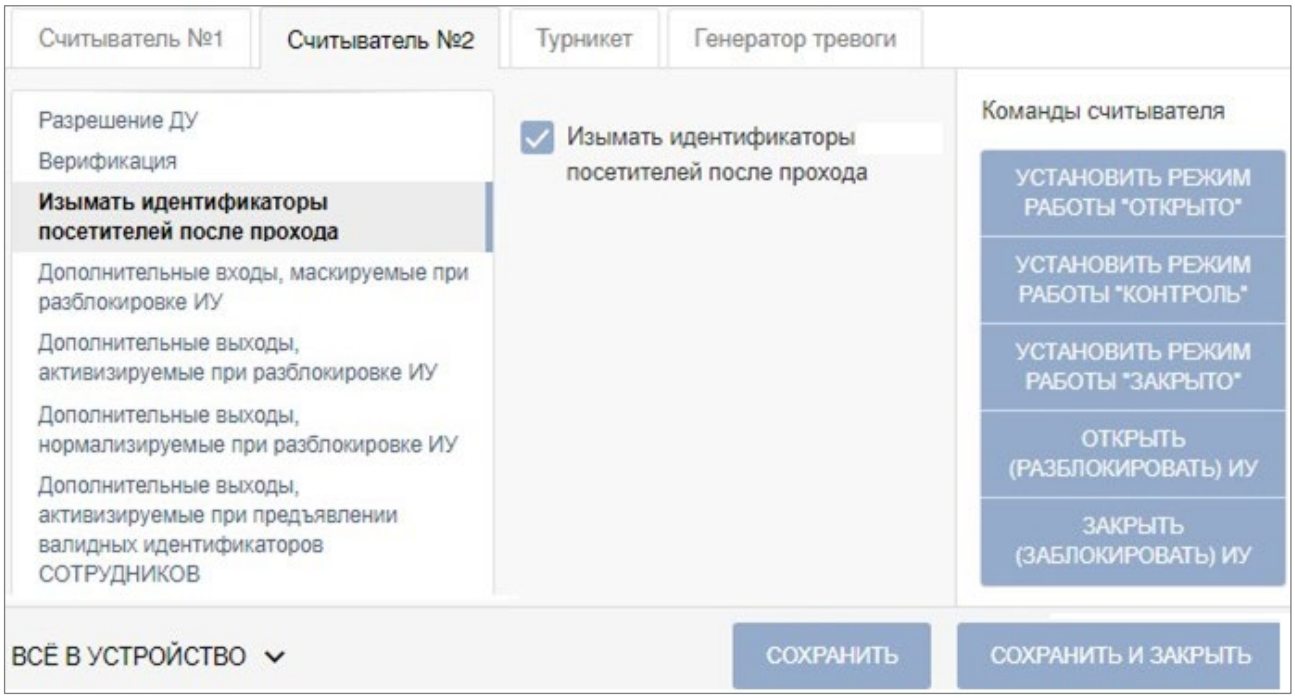
19. В левой части рабочей области окна выберите параметр **Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ**.
20. Установите с помощью раскрывающегося списка в рабочей области окна для параметра

Критерий активизации значение **На время срабатывания**.

21. Установите в рабочей области окна флажок **Дополнительный выход №…** (номер выхода, к которому подключен вход *«Изъять карту»* картоприемника):



22. В левой части рабочей области окна выберите параметр **Изымать идентификаторы посетителей после прохода** и установите для него флажок:

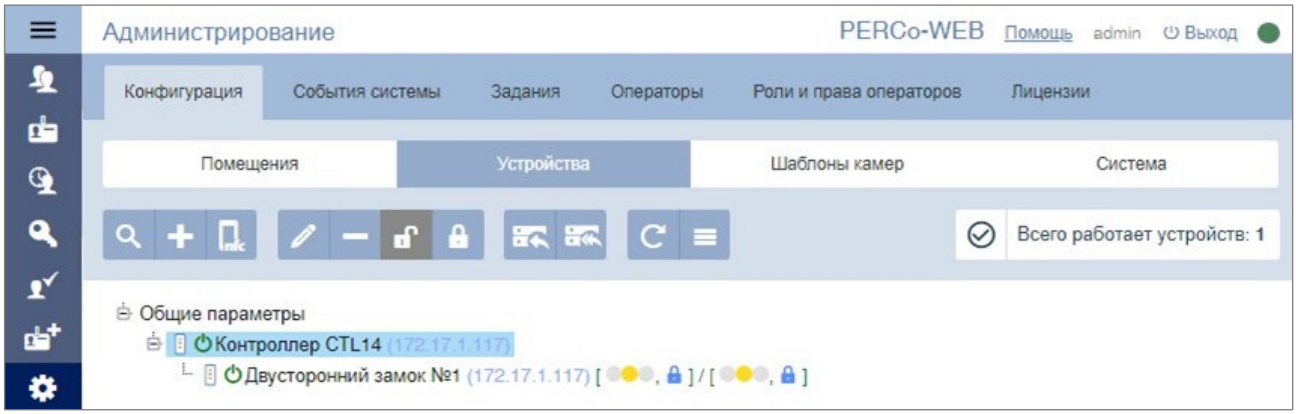


23. Нажмите кнопку **Сохранить и закрыть**. Окно **Свойства контроллера** будет закрыто, настройки сохранены.

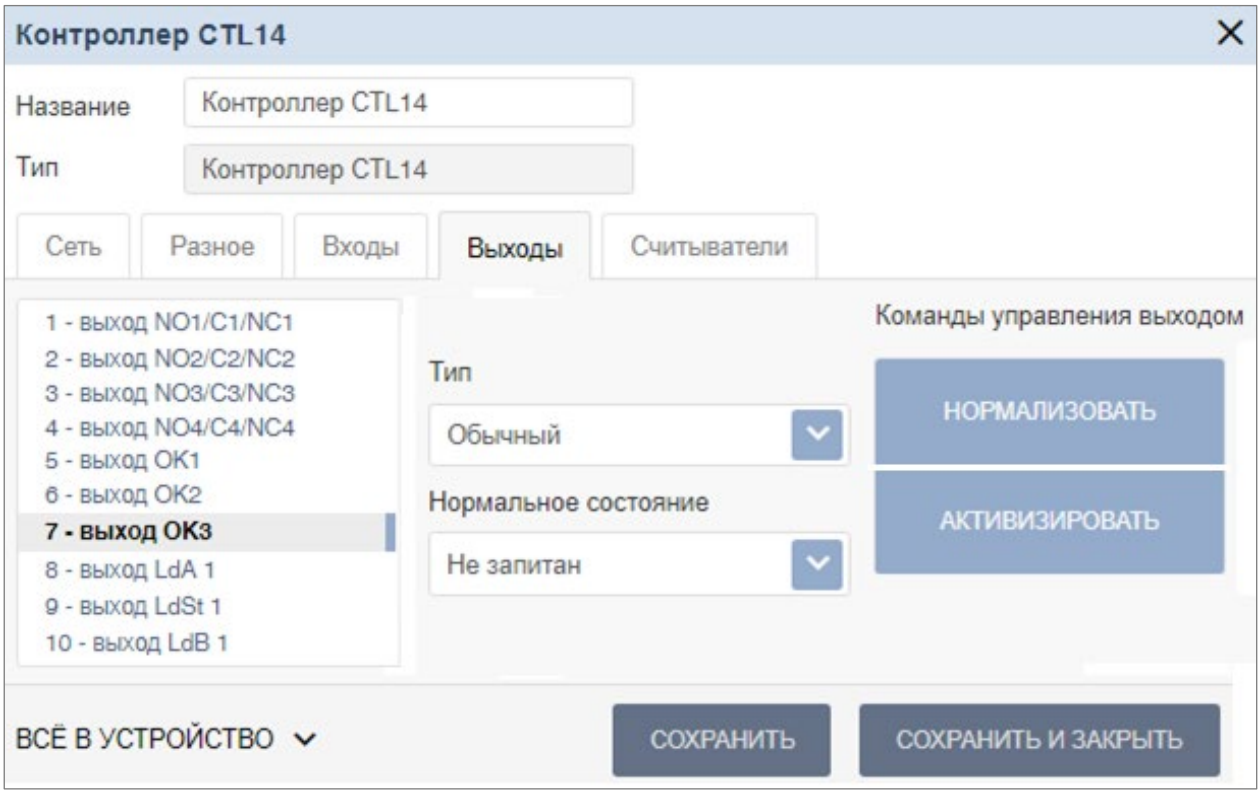
25. Настройка контроллера PERCo-CT/L14 для работы с картоприемником

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. Войдите в систему, используя Web-браузер.
2. Используя панель навигации, перейдите в раздел **«Администрирование»** в подраздел **«Конфигурация»** на вкладку **Помещения**.
3. В рабочей области страницы выделите основной контроллер, к которому физически подключен картоприемник:



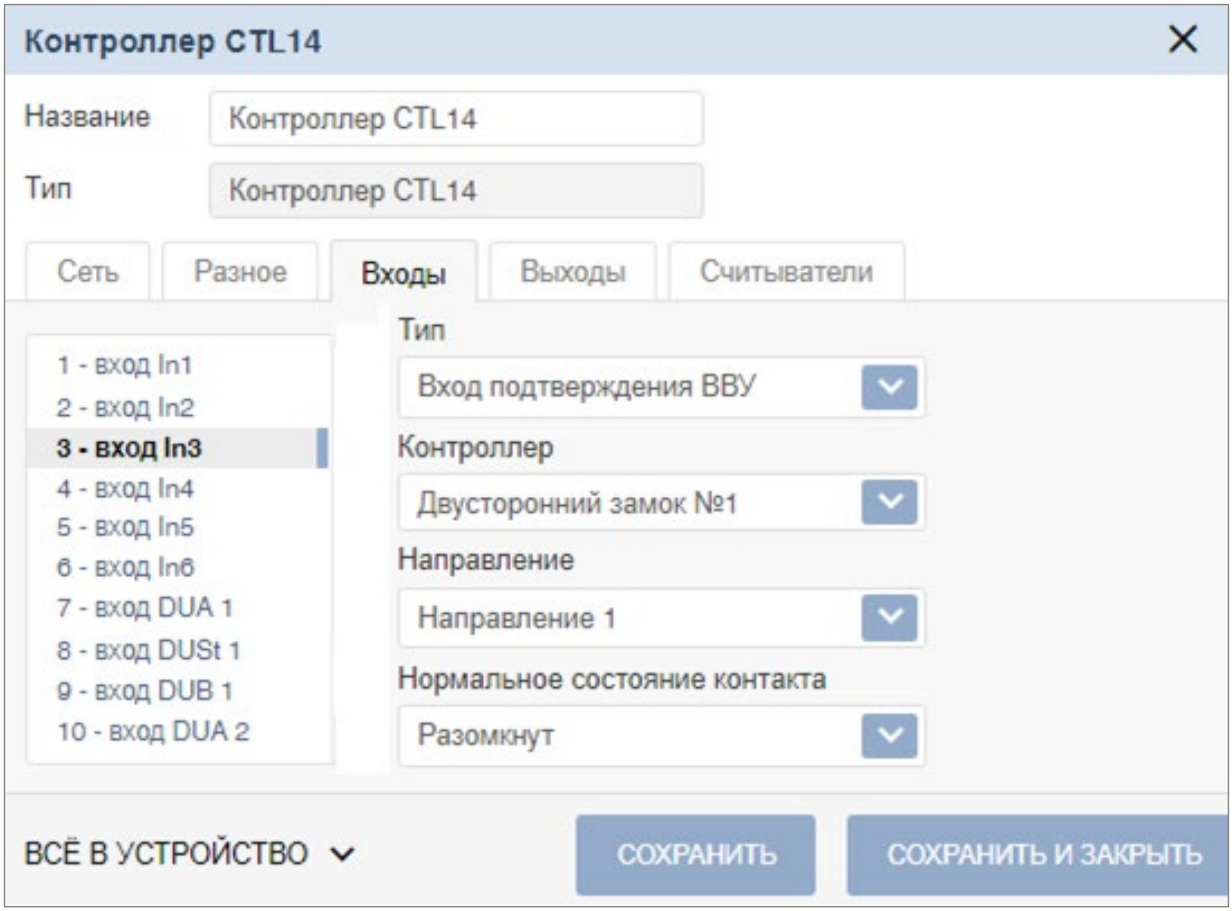
4. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется окно, отражающее название контроллера.
5. В открывшемся окне перейдите на вкладку **Выходы**.



6. В рабочей области окна выберите **Выход…** (номер выхода должен соответствовать выходу контроллера, к которому физически подключен вход *«Изъять карту»*

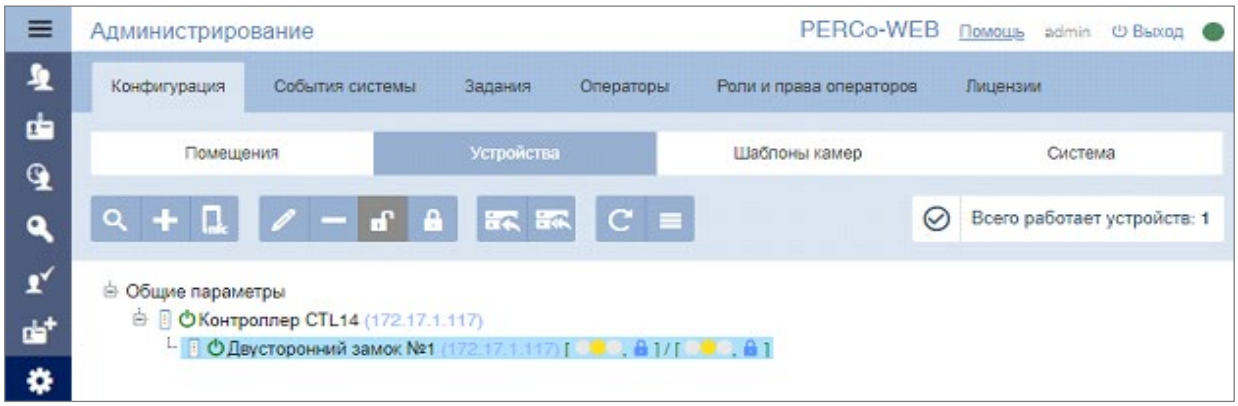
картоприемника).

7. Установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
   - для параметра **Тип** значение **Обычный**;
   - для параметра **Нормальное состояние** значение **Не запитан**.
8. Перейдите на вкладку **Входы**.
9. Если картоприемник выступает в качестве внешнего верифицирующего устройства для контроллера (сигнал *«Карта изъята»* поступает на отдельный вход контроллера), то в рабочей области окна выберите **Вход…** (номер входа контроллера, к которому физически подключен выход *«Карта изъята»* картоприемника) и установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
   - для параметра **Тип** значение **Вход подтверждения ВВУ**;
   - для параметров **Контроллер** и **Направление** устройство и направление должны соответствовать тем, которые контролируются картоприемником);
   - для параметра **Нормальное состояние контакта** значение **Разомкнут**:



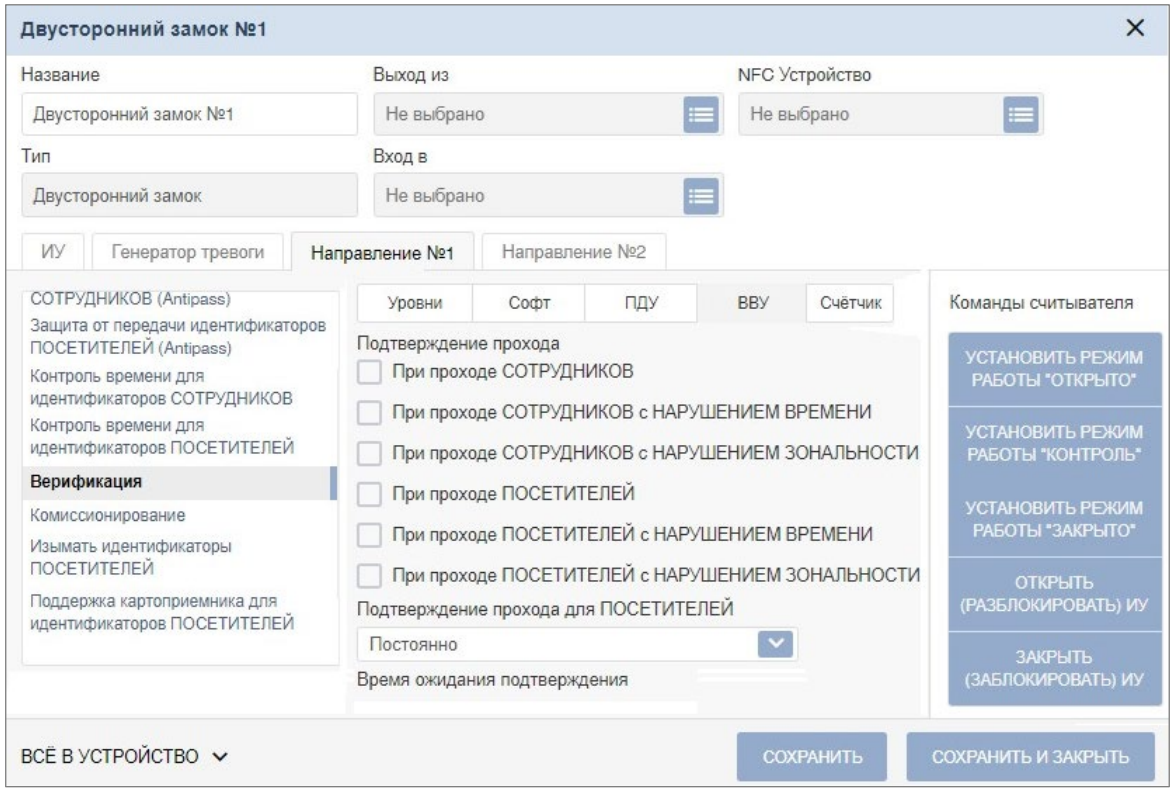
10. При необходимости настройте реакцию системы на сигнал от картоприемника *«Авария»*. Для этого в рабочей области окна выберите **Вход №…** (номер входа должен соответствовать входу контроллера, к которому физически подключен выход *«Авария»* картоприемника) и установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
    - для параметра **Тип** значение **Обычный**;
    - для параметра **Нормальное состояние контакта** значение **Разомкнут**.
11. Используя параметры активизации или нормализации выходов, настройте требуемую реакцию контроллера.
12. Нажмите кнопку **Сохранить и закрыть**. Окно с названием контроллера будет закрыто.

13. В рабочей области страницы в составе основного контроллера выделите контроллер, который контролируется картоприемником:

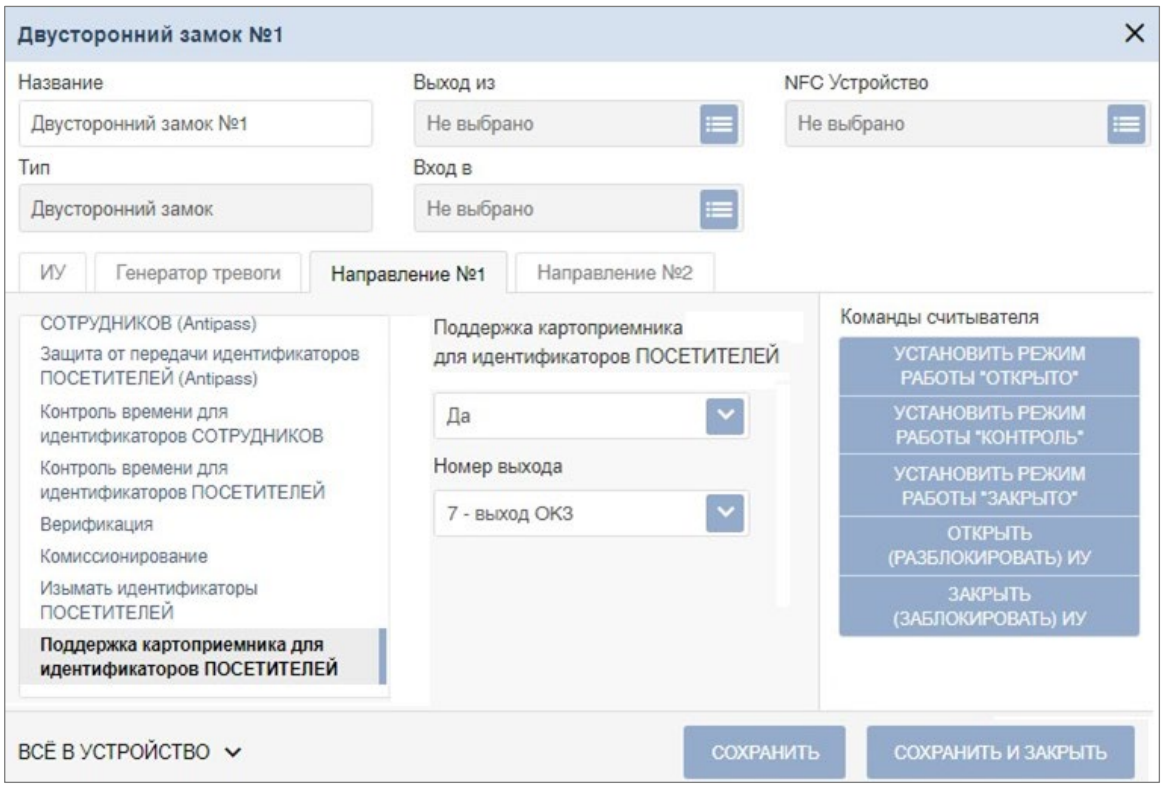


14. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется окно, отражающее название контроллера.
15. Перейдите на вкладку ресурса **Направление №…** (номер направления должен соответствовать считывателю, контролируемому картоприемником).
16. Подтверждением изъятия карты для контроллера доступа является сигнал от картоприемника *«Карта изъята»*. Для настройки подтверждения в левой части рабочей области окна для параметра **Верификация** установите значение:
    - **ВВУ**, если картоприемник выступает в качестве внешнего верифицирующего устройства для контроллера (сигнал *«Карта изъята»* поступает на отдельный вход контроллера);
    - **ПДУ**, если выход *«Карта изъята»* картоприемника подключен к контроллеру параллельно ПДУ.
17. В рабочей области окна на вкладке **ВВУ** или **ПДУ** для параметра **Подтверждение прохода** установите флажки:
    - **При проходе СОТРУДНИКОВ**;
    - **При проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ**;
    - **При проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**;
    - **При проходе ПОСЕТИТЕЛЕЙ**;
    - **При проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ**;
    - **При проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**.

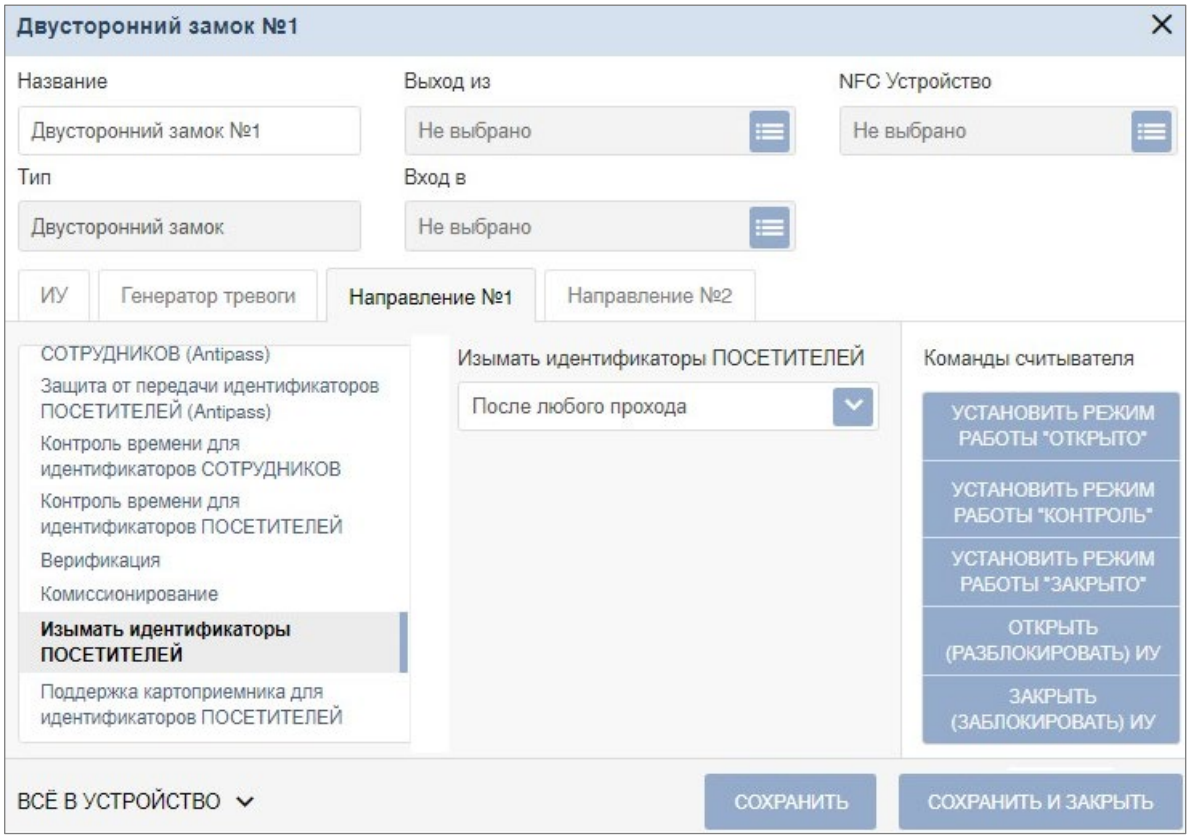
18. Установите в рабочей области окна необходимое значение параметра **Время ожидания подтверждения**, в течение которого контроллер должен ожидать сигнал *«Карта изъята»*:



19. В левой части рабочей области окна выберите параметр **Поддержка картоприемника для идентификаторов ПОСЕТИТЕЛЕЙ**.
20. Установите с помощью раскрывающегося списка в рабочей области окна для параметра **Поддержка картоприемника для идентификаторов ПОСЕТИТЕЛЕЙ** значение **Да**.
21. С помощью выпадающего списка выберите номер выхода, к которому подключен вход *«Изъять карту»* картоприемника.



22. В левой части рабочей области окна выберите параметр **Изымать идентификаторы посетителей** и выберите из выпадающего списка одно из значений:
    - **Нет**;
    - **После любого прохода**;
    - **После прохода в последний день действия идентификатора**.



23. Нажмите кнопку **Сохранить и закрыть**. Окно **Свойства контроллера** будет закрыто, настройки сохранены.

26. Команды управления устройствами

Генератор тревоги

- **Сбросить тревогу** – режим *«Тревога»* генератора тревоги будет снят.
- **Поднять тревогу** – контроллер перейдет в режим *«Тревога»,* будут активизированы выходы, для которых установлен **Тип: Генератор тревоги**.

Турникет

- **Сбросить зональность** – позволяет сбросить зональность турникета.

Замок

- **Поставить на охрану** – ИУ будет переведено в РКД *«Охрана»*.
- **Снять с охраны** – ИУ будет снято из РКД *«Охрана»* в предыдущий РКД.
- **Снять тревогу** – режим *«Тревога»* будет снят. ИУ будет переведено в РКД *«Охрана»*.
- **Блокировать** – ИУ будет заблокировано.
- **Разблокировать** – ИУ будет разблокировано.
- **Сбросить зональность** – позволяет сбросить зональность замка.

Дополнительный выход

- **Активизировать** – все выходы, для которых установлен **Тип: Обычный**, будут активизированы на время, определенное параметром **Время активизации**.

Примечание:

Дополнительные выходы, для которых установлен **Тип: Генератор тревоги**, не могут быть активизированы командой **Активизировать**.

- **Нормализовать** – все выходы, для которых установлен **Тип: Обычный**, будут нормализованы.

Считыватель

- **Установить режим работы «Открыто»** – ИУ в направлении считывателя будет переведено в РКД *«Открыто»*.
- **Установить режим работы «Контроль»** – ИУ в направлении считывателя будет переведено в РКД *«Контроль»*.
- **Установить режим работы «Закрыто»** – ИУ в направлении считывателя будет переведено в РКД *«Закрыто»*.
- **Открыть (разблокировать) ИУ** – ИУ в направлении считывателя будет разблокировано на время, установленное параметром **Время разблокировки**. Команда доступна при установленном РКД *«Контроль»* и предназначена для кратковременной разблокировки ИУ.
- **Закрыть (заблокировать) ИУ** – ИУ в направлении считывателя будет заблокировано. Команда доступна при установленном РКД *«Контроль»* и предназначена для блокировки ИУ после выполнения команды **Открыть (разблокировать) ИУ**.

Видеокамера TRASSIR (доступно только при приобретенной лицензии на модуль ПО ***PERCo-WM06 «Интеграция с TRASSIR»***)

- **Включить запись** – позволяет вручную включить запись на канале записи сервера ***TRASSIR***. В таком случае в рабочей области страницы подраздела ***«Конфигурация»*** появится надпись *«Идет запись»*.

Внимание!

Запись видео может производиться сервером ***TRASSIR*** автоматически по настроенным алгоритмам, то есть надпись *«Идет запись»* может появляться без включения записи вручную.

- **Выключить запись** – позволяет выключить текущую запись.
- **Сохранить снимок** – позволяет сохранить скриншот «живого видео». Сохранение скриншота осуществляется в архив видеоподсистемы ***Trassir***.
- **Просмотр архива** – позволяет найти определенную видеозапись, выбрав дату и время начала записи. Полный архив хранится на сервере ***TRASSIR*** в подразделе ***«Веб-сервер»***.

27. Мобильный терминал доступа PERCo

Мобильный терминал доступа PERCo обеспечивает контроль доступа сотрудников / посетителей, имеющих соответствующий пропуск (идентификатор), на территорию, не оборудованную классической точкой доступа, в местах, где использование турникета, двери, шлагбаума и т.д. либо нецелесообразно, либо невозможно. **Мобильный терминал доступа PERCo** представляет собой мобильный телефон на ОС *«Android»* версии не ниже 5.0 с установленным приложением **«PERCo.Регистрация»**, а также настроенную точку доступа (контроллер) в системе ***PERCo-Web***.

Использование терминала позволяет значительно сократить временные затраты на регистрацию сотрудников на рабочих местах.

Внимание!

На смартфоне с установленным **Мобильным терминалом доступа PERCo** должен быть обеспечен достаточный объем свободной памяти для размещения базы данных сотрудников из ***PERCo-Web*** из расчета не менее 80 Кб на одного сотрудника. Как правило, максимальный объем БД на смартфоне не превышает 4 Гб.

27.1. Назначение и принципы работы

Мобильный терминал доступа PERCo предназначен для:

- Мобильного контроля доступа сотрудников / посетителей, имеющих соответствующий пропуск (идентификатор), на территорию, не оборудованную классической точкой доступа: турникетом, дверью или шлагбаумом. В качестве такой территории может выступать временная строительная площадка или автотранспортная проходная.
- Сверки данных сотрудника на предмет принадлежности пропуска, разрешенного времени пребывания, возможности нахождения на той или иной территории предприятия и т.д.
- Ведения полноценного учета рабочего времени с последующим построением отчетов в системе ***PERCo-Web***.

Основные возможности терминала:

- Мобильный контроль доступа сотрудников / посетителей;
- Сверка данных сотрудников / посетителей на предмет принадлежности пропуска (идентификатора);
- Учет рабочего времени;
- Отображение информации о сотруднике на экране терминала при поднесении карты (идентификатора).

Идентификация

Мобильный терминал PERCo позволяет читать:

1. Карты типа **Mifare**, а именно стандарты *Mifare Ultralight, Mifare Classic, Mifare Plus, Mifare DESFire*. Для чтения карт используется встроенный NFC-модуль смартфона.
2. Штрихкоды. Для чтения штрихкода используется камера смартфона.

Режим работы

Мобильный терминал доступа PERCo может работать в трех режимах: ВХОД, ВЫХОД и ВЕРИФИКАЦИЯ.

Связь с сервером

Связь с сервером ***PERCo-Web*** осуществляется посредством Wi-Fi соединения или мобильного интернета.

В случае, если телефон оказывается вне сети, транзакции накапливаются в буфере мобильного терминала и при восстановлении связи информация передается на сервер автоматически (при установке автоматической синхронизации) или вручную. Также при синхронизации с сервером обновляется информация о данных пользователей.

27.2. Установка приложения PERCo.Регистрация

Для установки приложения ***PERCo.Регистрация*** на устройство необходимо выполнить следующие действия:

1. Зайдите в магазин приложений **Google Play** на своем устройстве, где в строке поиска введите ***PERCo.Регистрация***, или перейдите по ссылке на страницу приложения в **Google Play**:

https://play.google.com/store/apps/details?id=com.nobokani.percoterminal

2. Для автоматической загрузки приложения нажмите кнопку **Установить**.
3. После успешной загрузки приложения на экране устройства отобразится ярлык. Для запуска приложения нажмите на иконку  . При первом запуске необходимо разрешить приложению доступ к запрашиваемым ресурсам устройства.

27.3. Подготовка к работе

Примечание:

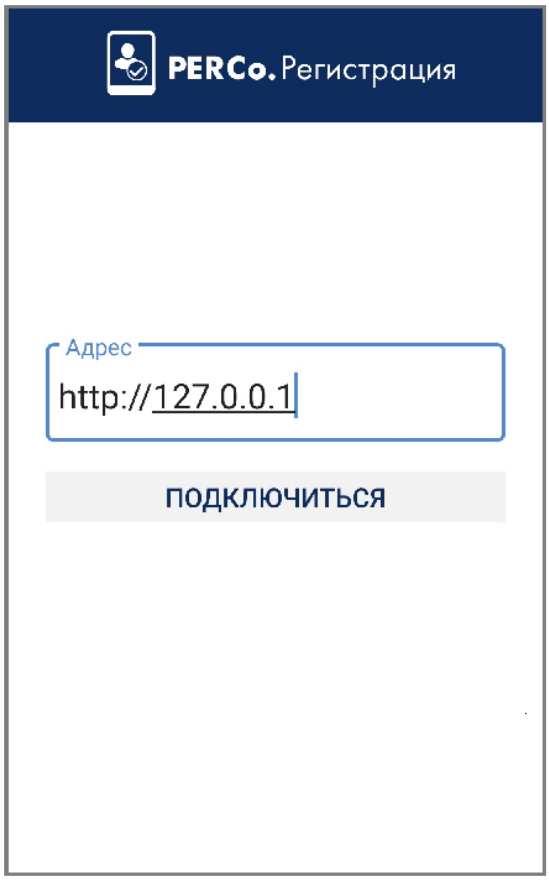
Связь с сервером ***PERCo-Web*** осуществляется посредством Wi-Fi соединения или мобильного интернета. В случае, если сервер ***PERCo-Web*** расположен внутри сети, то доступ возможен только, если телефон тоже подключен к данной сети.

Перед началом работы необходимо выполнить следующие действия:

1. Запустите приложение, нажав на иконку  , которая расположена в меню мобильного устройства. Откроется окно для ввода адреса сервера вручную или с помощью сканирования QR кода:

Добавление адреса сервера системы вручную

Для добавления адреса сервера системы вручную необходимо на стартовой странице приложения ***PERCo.Регистрация*** выбрать **ввести вручную**. Откроется новое окно:



- В поле **Адрес** введите адрес сервера, на котором установлена система ***PERCo-Web***, и нажмите кнопку **Подключиться**.
- В интерфейсе системы ***PERCo-Web***, используя панель навигации, перейдите в раздел **«Администрирование»**.
- Откройте подраздел **«Конфигурация»** и перейдите на вкладку **Устройства**.
- Нажмите кнопку **Список NFC устройств** и проверьте, чтобы имя настраиваемого терминала отобразилось в списке NFC устройств.
- Активируйте устройство с помощью переключателя .

Добавление адреса сервера системы с помощью QR кода

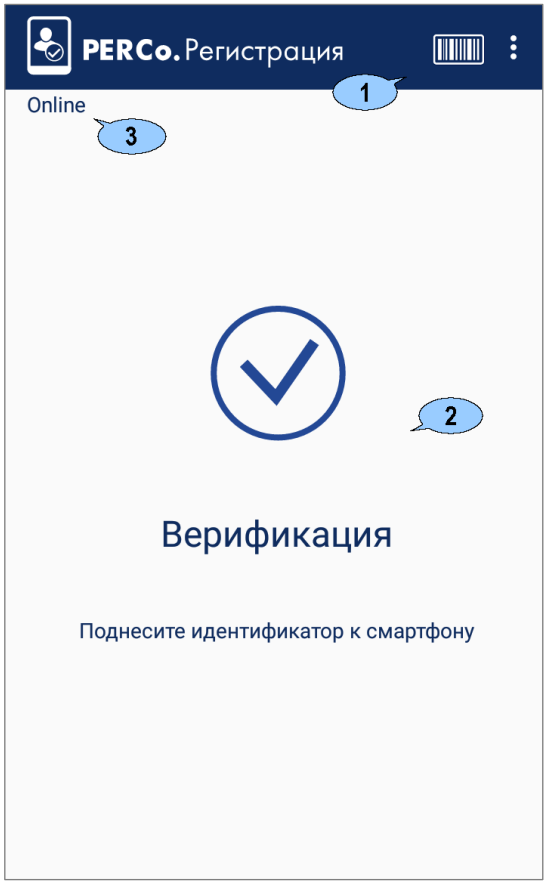
Для добавления адреса сервера системы с помощью QR кода необходимо:

- На стартовой странице приложения ***PERCo.Регистрация*** выбрать способ **Отсканировать с помощью камеры**. Откроется окно для сканирования QR кода.
- В интерфейсе системы ***PERCo-Web***, используя панель навигации, перейдите в раздел **«Администрирование»**.
- Откройте подраздел **«Конфигурация»** и перейдите на вкладку **Устройства**.
- Нажмите кнопку **Список NFC устройств**, затем кнопку **Отобразить QR код**. На экране появится QR код.
- С помощью устройства отсканируйте открывшийся QR код.
- Проверьте, чтобы имя настраиваемого терминала отобразилось в списке NFC устройств, и активируйте устройство с помощью переключателя .

2. В интерфейсе системы ***PERCo-Web*** в разделе  **«Администрирование»** откройте подраздел **«Конфигурация»** и перейдите на вкладку **Помещения** или **Устройства**. Выберите контроллер, шаблон доступа которого будет использовать мобильный терминал. В поле **NFC устройство** выберите имя настраиваемого мобильного терминала.
3. Устройство готово к работе.

27.4. Главное окно приложения

Главное окно приложения ***PERCo.Регистрация*** имеет следующий вид:



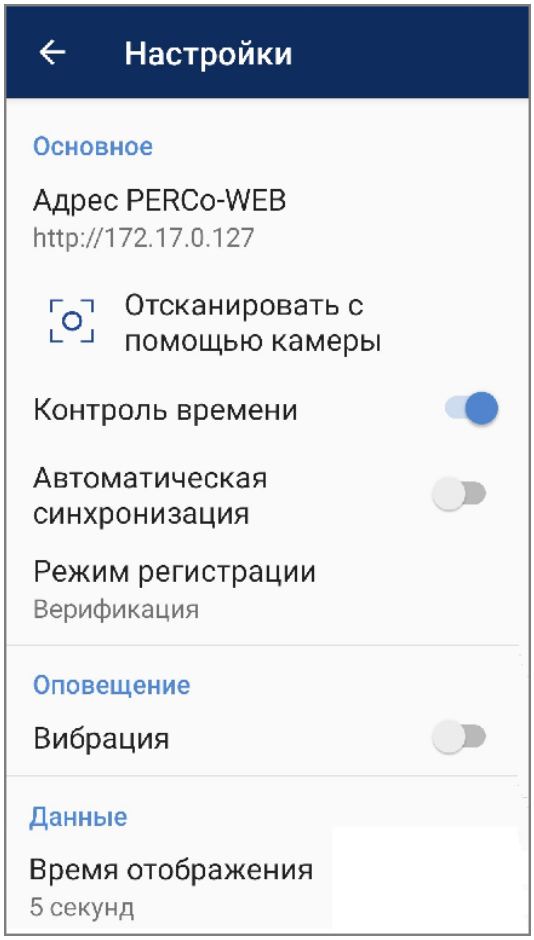
1. Верхняя панель:
   -  Выпадающий список функций:
     - **Настройки** – функция позволяет открыть окно для настройки параметров приложения;
     - **Синхронизация** – функция предназначена для ручной передачи данных о проходах сотрудников / посетителей (отображается только при выключенной в настройках автоматической синхронизации);
     - **О приложении** – при выборе элемента открывается новое окно, которое содержит краткую информацию о приложение. После ознакомления с информацией для выхода из окна нажмите кнопку **Закрыть**.
   -  Иконка для чтения штрихкода.
2. Рабочая область приложения. Вид рабочей области зависит от выбранного режима регистрации. При имитации прохода (при поднесении идентификатора к терминалу) в рабочей области приложения отображается информация о сотруднике / посетителе. Данные о проходе передаются в систему автоматически или при синхронизации.
3. Индикация статуса системы:
   - *online* в случае, если у телефона есть связь с сервером ***PERCo-Web***;

- *offline* в случае, если телефон оказался вне сети;
- загрузка данных, если в данный момент происходит синхронизация с сервером ***PERCo-Web*** (отображается в формате *Sync: current 0 of 1000)*.

27.5. Настройка параметров приложения

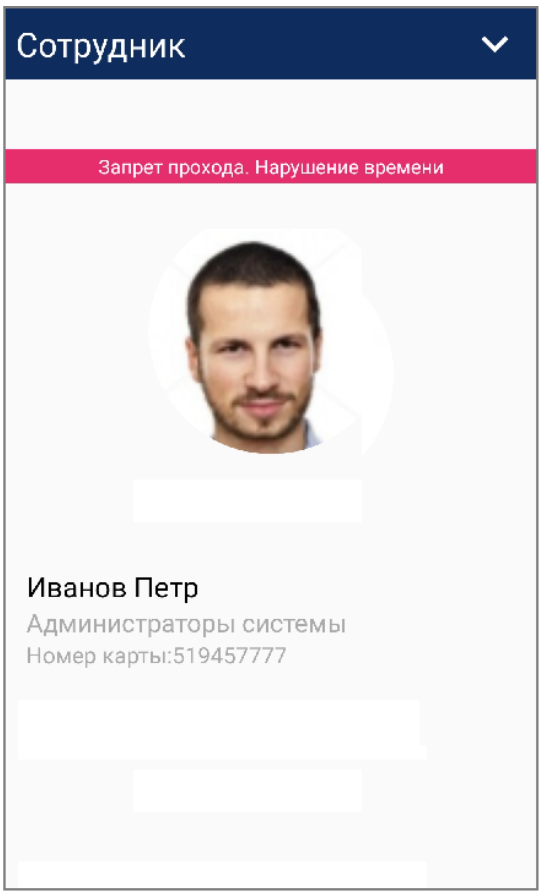
Для настройки параметров приложения ***PERCo.Регистрация*** выполните следующие действия:

1. Откройте приложение ***PERCo.Регистрация*** на устройстве.
2. Введите адрес сервера системы.
3. В главном окне приложения в верхнем правом углу выберите из выпадающего списка пункт **Настройки**. Откроется новое окно:



Окно **Настройки** содержит следующие элементы:

- **Основное**:
  - **Адрес PERCo-Web** – поле предназначено для смены адреса сервера с установленной системой вручную;
  - **Отсканировать с помощью камеры** – поле предназначено для смены адреса сервера с установленной системой с помощью сканирования камерой QR-кода;
  - **Контроль времени** – при установке флажка в случае, если проход совершен не в рамках временной зоны, на экране смартфона будет выводиться сообщение *«Запрет прохода. Нарушение времени»*:



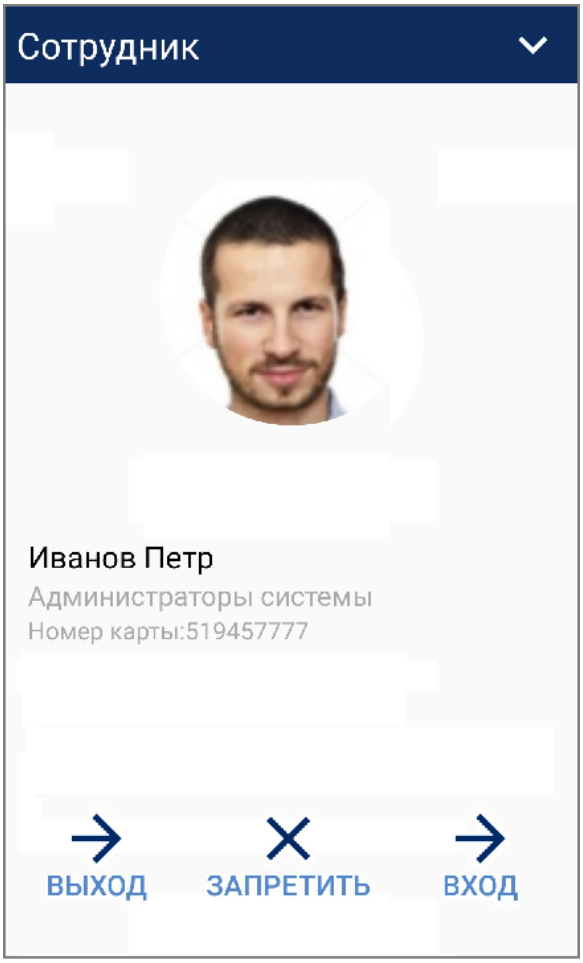
  - **Автоматическая синхронизация** – при установке флажка данные о проходах передаются в систему автоматически;
  - **Режим регистрации** – выпадающий список позволяет выбрать способ регистрации проходов. Доступны следующие варианты:
    - **Автоматический Вход** – при установке флажка при прикладывании идентификатора к терминалу формируется событие **Вход**;
    - **Автоматический Выход** – при установке флажка при прикладывании идентификатора к терминалу формируется событие **Выход**;
    - **Верификация** – при установке флажка автоматическое формирование события будет отсутствовать. От оператора будет требоваться принять решение: зарегистрировать вход, выход или запрет прохода (отмена).
- **Оповещение**:
  - **Вибрация** – при установке флажка будет включено дублирование оповещения вибрацией телефона.
- **Данные**:
  - **Время отображения** – параметр позволяет выбрать время отображения информации о проходе на экране устройства. Доступны следующие варианты:
    - **5 секунд**;
    - **10 секунд**;
    - **30 секунд**;
    - **Закрывать вручную**.

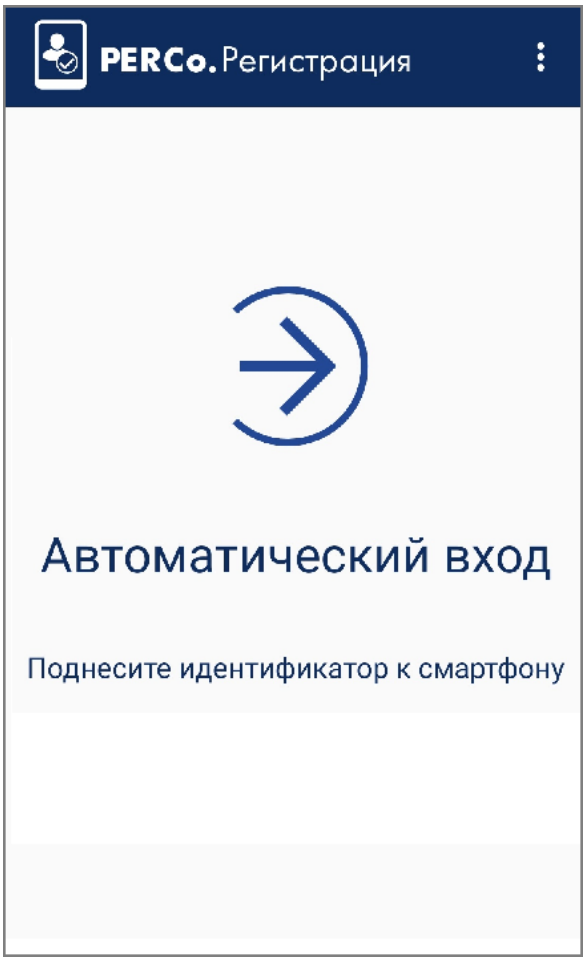
27.6. Алгоритм работы с мобильным терминалом PERCo

Для работы с **Мобильным терминалом PERCo** необходимо выполнить следующие действия:

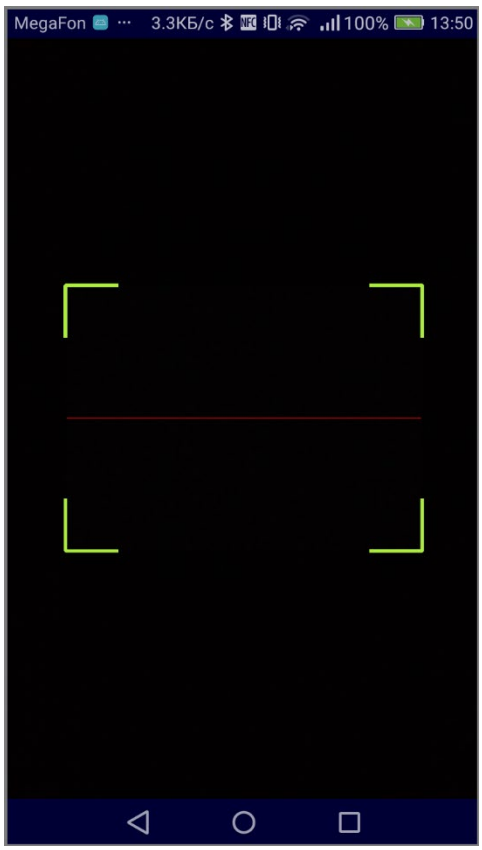
1. В настройках своего устройства активируйте режим NFC (технология беспроводной высокочастотной связи малого радиуса действия). При попытке запуска приложения с выключенным режимом NFC на стартовой странице появится сообщение *«Активируйте NFC модуль».*

2. Запустите приложение ***PERCo.Регистрация***, нажав на иконку , которая расположена в меню мобильного устройства. Откроется окно для ввода адреса сервера.
3. При необходимости настройте необходимые параметры для мобильного терминала.
4. В интерфейсе системы ***PERCo-Web*** в разделе **«Администрирование»** откройте подраздел **«Конфигурация»** и перейдите на вкладку **Устройства**.
5. Нажмите кнопку **Список NFC устройств** и проверьте, чтобы имя настраиваемого терминала отобразилось в списке NFC устройств. Активируйте устройство с помощью переключателя .
6. В разделе **«Администрирование»** на вкладке **Помещения** или **Устройства** выберите контроллер, шаблон доступа которого будет использовать мобильный терминал. В поле **NFC устройство** выберите свое настраиваемое устройство.
7. Устройство готово к использованию. Мобильный терминал можно использовать двумя способами:
   - Для чтения карты доступа:
     – Поднесите к телефону карту доступа сотрудника.
     – Откроется окно (вид окна может меняться в зависимости от выбранного способа режима регистрации):





   - Для чтения штрихкода:
     – Нажмите на иконку для чтения штрихкода .
     – Откроется камера смартфона с границами для фокусировки на штрихкоде:



– Поднесите штрихкод под область, выделенную зеленым. После этого штрихкод прочитается автоматически.

28. 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 состояния 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-Marin*, *HID* и *Mifare*, а также биометрические идентификаторы (отпечатки пальцев, шаблоны ладони, шаблоны лица).

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 *«Внутреннее ПО ("прошивка") контроллеров PERCo»*. Актуальную версию программы можно загрузить с сайта компании www.perco.ru из раздела **Поддержка > Программное обеспечение > ПО PERCo-Web**.

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, планы помещений.

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, два считывателя и ПО.

ООО «ПЭРКо»

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

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

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

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

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

locks@perco.ru - по вопросам обслуживания замков

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

www.perco.ru

Кор. 27.11.2020

www.perco.ru

тел: 8 (800) 333-52-53