



**Система контроля и
управления доступом
PERCo-Web**

PERCo-WS

«Стандартный пакет ПО»

РУКОВОДСТВО АДМИНИСТРАТОРА

СОДЕРЖАНИЕ

1	Введение	4
2	Назначение	5
3	Основные особенности.....	6
4	Состав и принципы работы системы.....	7
5	Поддерживаемое оборудование.....	10
6	Основные технические характеристики	15
7	Требования к аппаратным и программным средствам	17
8	Установка системы.....	19
9	Управление лицензиями.....	24
10	Менеджер системы безопасности PERCo-Web.....	27
10.1	Управление серверами системы	28
10.2	Управление БД.....	29
10.2.1	Резервное копирование БД	30
10.2.2	Восстановление БД из резервной копии.....	31
11	Предварительная настройка	33
12	Функции Antipass и Global Antipass	35
13	Раздел «Администрирование».....	38
13.1	Подраздел «Конфигурация».....	38
13.1.1	Вкладка «Помещения»	38
	Создание списка помещений	38
	Размещение контроллеров в помещениях.....	38
13.1.2	Вкладка «Контроллеры»	43
	Поиск контроллеров43	
	Общие настройки контроллеров	43
	Окно «Свойства контроллера».....	43
	Создание списка комиссионующих карт	43
13.1.3	Вкладка «Система».....	70
13.2	Подраздел «События системы»	70
13.3	Подраздел «Задания»	72
13.3.1	Создание нового задания.....	73
13.4	Подраздел «Операторы»	74
13.4.1	Добавление оператора системы	75
13.5	Подраздел «Роли и права операторов»	77
13.5.1	Добавление роли оператора (набора полномочий)	78
13.6	Подраздел «Лицензии»	79
13.6.1	Ввод кода активации.....	80
14	Параметры контроллера PERCo.....	82
14.1	Вкладка «Общие».....	82
14.1.1	Подвкладка «Сеть»	82
14.1.2	Подвкладка «Разное»	83
14.2	Вкладка ИУ («Замок», «Турникет»)	83
14.3	Вкладка «Замок CL05».....	85
14.4	Вкладки «Свойства ЛИКОНА» и «Строки».....	86
14.5	Вкладка «Дополнительные входы»	87
14.6	Вкладка «Дополнительные выходы»	89
14.7	Вкладка «Дополнительный вывод»	89

14.8	Вкладка «Генератор тревоги»	90
14.9	Вкладка «Считыватель».....	90
15	Параметры контроллера Suprema	95
15.1	Вкладка «Общие».....	95
15.1.1	Подвкладка «Сеть»	95
15.1.2	Подвкладка «Разное»	96
15.2	Вкладка «Замок»	96
15.3	Вкладка «Считыватель».....	98
16	Пример конфигурирования картоприемника	100
17	Команды управления устройствами	103
18	Коды документов для «Табеля учета рабочего времени»	105
19	Термины и определения	107

1 Введение

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

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

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

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

Примечание:

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

Принятые сокращения:

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

2 Назначение

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

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

3 Основные особенности

- Обмен данными между АРМ, БД и оборудованием системы осуществляется по сети *Ethernet*. Это позволяет при развертывании системы использовать уже существующую ИТ-инфраструктуру предприятия.
- Сервер системы, сервер БД и все необходимое для работы системы ПО устанавливается на одном ПК, подключенном к сети *Ethernet*. Установка дополнительного ПО на АРМ операторов системы не требуется. Доступ осуществляется удаленно, через Web-интерфейс сервера системы.
- Наличие постоянной связи контроллеров системы с сервером не требуется. В энергонезависимую память каждого контроллера передаются все права доступа владельцев карт. Там же сохраняются регистрируемые контроллером события. При восстановлении связи с сервером системы события переносятся в БД системы.
- Контроллеры системы поддерживают возможность обновления встроенного ПО (прошивки) по сети *Ethernet*.
- Система легко масштабируется, то есть возможно увеличение числа контроллеров (КПП) и АРМ с их интеграцией в уже существующую систему.
- При организации дополнительных АРМ достаточно добавить в систему нового оператора и выдать ему полномочия на доступ к соответствующим разделам и подразделам ПО системы.
- ПО системы позволяет гибко настраивать полномочия операторов АРМ. Полномочия выдаются операторам независимо на разделы и подразделы ПО, оборудование, помещения, подразделения и т.д. При этом АРМ связано не с конкретным ПК, а с учетной записью оператора.
- Система поддерживает биометрические технологии, разработанные компанией **Suprema**. Сканирование отпечатков пальцев, при необходимости, дополняет стандартный метод верификации по картам доступа и позволяет увеличить надёжность системы контроля и управления доступом на территории предприятия при проходе сотрудников и посетителей, обеспечивая предотвращение случаев прохода по чужой карте доступа.
- Система поддерживает интеграцию бесконтактных карт **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.

4 Состав и принципы работы системы

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

Сервер системы

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

КПП

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

Возможны следующие варианты управления ИУ на КПП:

- Оператором КПП в ручном режиме с помощью ПДУ.
- Оператором КПП от ПК заданием для направлений ИУ одного из [режимов контроля доступа](#) (РКД): «Открыто», «Закрыто», «Контроль». Это позволяет при необходимости обеспечить свободный проход в данном направлении или полностью его перекрыть. Для прохода по картам доступа и/или отпечаткам пальцев используется РКД «Контроль».
- Автоматически контроллером КПП при проходе по картам доступа и/или отпечаткам пальцев. При этом в направлении прохода должен быть установлен РКД «Контроль». При проходе через КПП владелец карты доступа:
 - в случае верификации по карте доступа - предъявляет карту считывателю;
 - в случае верификации по отпечаткам пальцев - проходит процедуру сканирования отпечатков пальцев;
 - в случае верификации по карте доступа и отпечаткам пальцев - предъявляет карту считывателю и проходит процедуру сканирования отпечатков пальцев.

На основании анализа номера карты и/или биометрической информации, а также выданных ее владельцу прав доступа контроллер принимает решение на разрешение или запрет прохода, подавая соответствующую команду ИУ. Каждый факт предъявления карты и/или сканирования отпечатков пальцев фиксируется в БД с указанием места и времени предъявления/сканирования, что позволяет системе

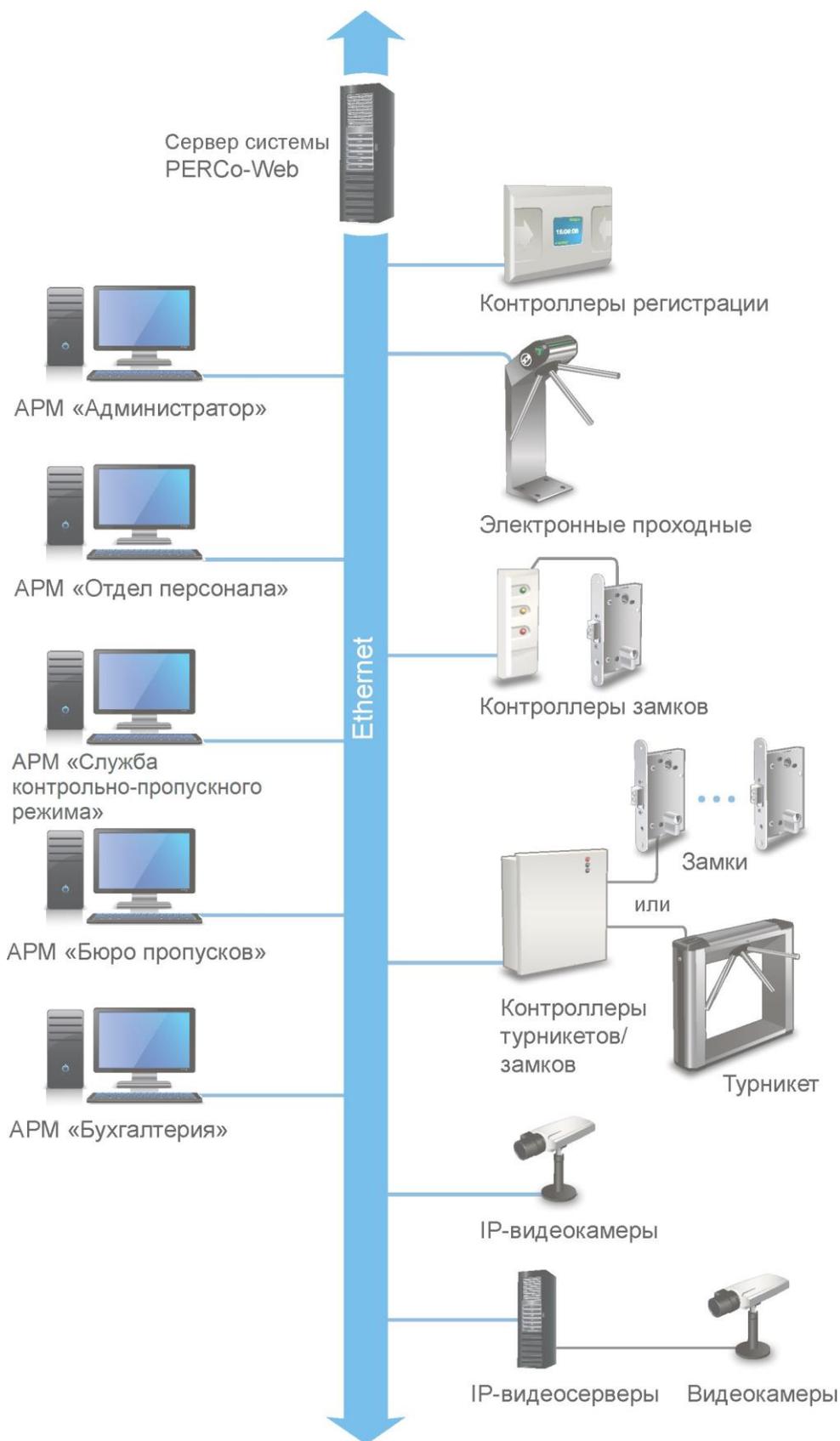
отслеживать местонахождение, время пребывания и перемещения владельца по территории и помещениям предприятия.

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 видеокameraми), подключенных к системе, для этого в состав ПО системы входит видеосервер.

АРМ

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

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



Структурная схема системы PERCo-Web

5 Поддерживаемое оборудование

Примечание:

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

Контроллеры управления дверьми

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

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

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

PERCo-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-Marine* 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 коммиссионированных 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.

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-Marine* 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** контроллера **PERCo-CT/L04.2, PERCo-CT03.2**, после чего становится доступным управление подключёнными контроллерами через интерфейс **PERCo-Web**.

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.

Контроллер регистрации

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

PERCo-CR01.2 LICON Снабжен двумя встроенными считывателями карт доступа формата *HID, EM-Marine* и ЖКИ (дисплеем). Контроллер предназначен для организации терминала учета рабочего времени и контроля трудовой дисциплины (даным контроллером не поддерживается возможность управления ИУ). В версии **PERCo-CR01.2 LICON** число пользовательских карт доступа увеличено до 50 000, улучшен Web-интерфейс управления.

ИУ – Замок

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

ИУ – Турникет

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

ИУ – Калитка

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

Считыватели

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

В качестве внешних считывателей карт доступа могут использоваться:

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

Для подключения к USB-разъему ПК используются контрольные считыватели серии **PERCo-IR05** для карт формата *HID*, *EM-Marin* и **PERCo-IR08**, **PERCo-MR08** для карт формата *MIFARE*.

Электронные проходные

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

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

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** или **PERCo-CT/L04.2**. 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.

Контроллеры SUPREMA

В целях расширения функциональных возможностей системы **PERCo-Web** по поддержке биометрических технологий в общую систему СКУД могут встраиваться контроллеры доступа **Suprema** для совместного использования с контроллерами доступа **PERCo**. Использование контроллеров доступа **Suprema** позволяет усилить контроль доступа на территорию предприятия при проходе сотрудников и посетителей.

- **BioEntry Plus** – 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.

Предусмотрено два 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** или **PERCo-CT/L04.2** по интерфейсу *Wiegand* через конвертер интерфейса **PERCo-AC02**.

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

Дополнительное оборудование

Картоприемники:

- Картоприемники серий **PERCo-IC02, PERCo-IC05**;
- Картоприемники сторонних производителей.

PERCo-AU05 (TCB) – табло системного времени предназначено для отображения времени. TCB подключается по интерфейсу *RS-485* к контроллерам серии **PERCo-CT/L04, PERCo-CT/L04.2** и встроенным контроллерам ЭП **PERCo-CT03, PERCo-CT03.2**.

ДКЗП – датчик контроля зоны прохода предназначен для регистрации несанкционированного прохода или проникновения под преграждающими планками.

Сирена – звуковой оповещатель.

Видеокамеры

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

Примечание:

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

6 Основные технические характеристики

Стандарт интерфейса связи	<i>Ethernet</i> (IEEE 802.3)
Скорости передачи данных <i>Ethernet</i> , Мбум/с	10/100
Количество контроллеров СКУД	не более 512
Интенсивность проходов со сменой пространственной зоны, <i>проходов/секунду</i>	
для контроллеров на 50 000 карт	не более 50
для контроллеров на 10 000 карт	не более 200
Формат карт доступа	<i>HID, EM-Marin, Mifare</i>
Общее число карт доступа в системе, шт	не более 100 000 000
из них временных карт посетителей	не более 50 000
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
скользящих понедельных графиков (в пределах 54 недель)	не более 255
Количество дней с особым статусом, праздников контроля	не более 365

Объем памяти контроллеров PERCo для хранения идентификаторов и событий журнала регистрации

Контроллер	Вариант конфигурации	К-во карт	К-во событий
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 1000 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
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 LICON¹	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
CL05.2¹	Контроллер замка	до 10 000	до 760 000
		до 50 000	до 230 000
		до 40 000	до 390 000
		до 30 000	до 550 000
		до 20 000	до 710 000
CT/L04.2¹	Универсальный контроллер турникета / замка	до 10 000	до 870 000
		до 50 000	до 230 000
		до 40 000	до 390 000
		до 30 000	до 550 000
		до 20 000	до 710 000
CT03.2¹	Встроенный контроллер электронной проходной	до 10 000	до 870 000
		до 50 000	до 230 000
		до 40 000	до 390 000
		до 30 000	до 550 000
		до 20 000	до 710 000

¹ Вариант распределения памяти контроллера (кол-во карт / кол-во событий) выбирается в его Web-интерфейсе.

Примечания:

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

Количество подключаемых:

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

Примечание:

На каждой точке верификации может транслироваться изображение с одной камеры.

7 Требования к аппаратным и программным средствам

Требования к аппаратным средствам сервера системы

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

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

Требования к программным средствам сервера системы

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

- Рекомендованы к использованию версии *ОС Windows Server: 2008 R2, 2012 R2, 2016*.
- Возможно использование *ОС Windows: 7, 8.1, 10*.

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: 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.

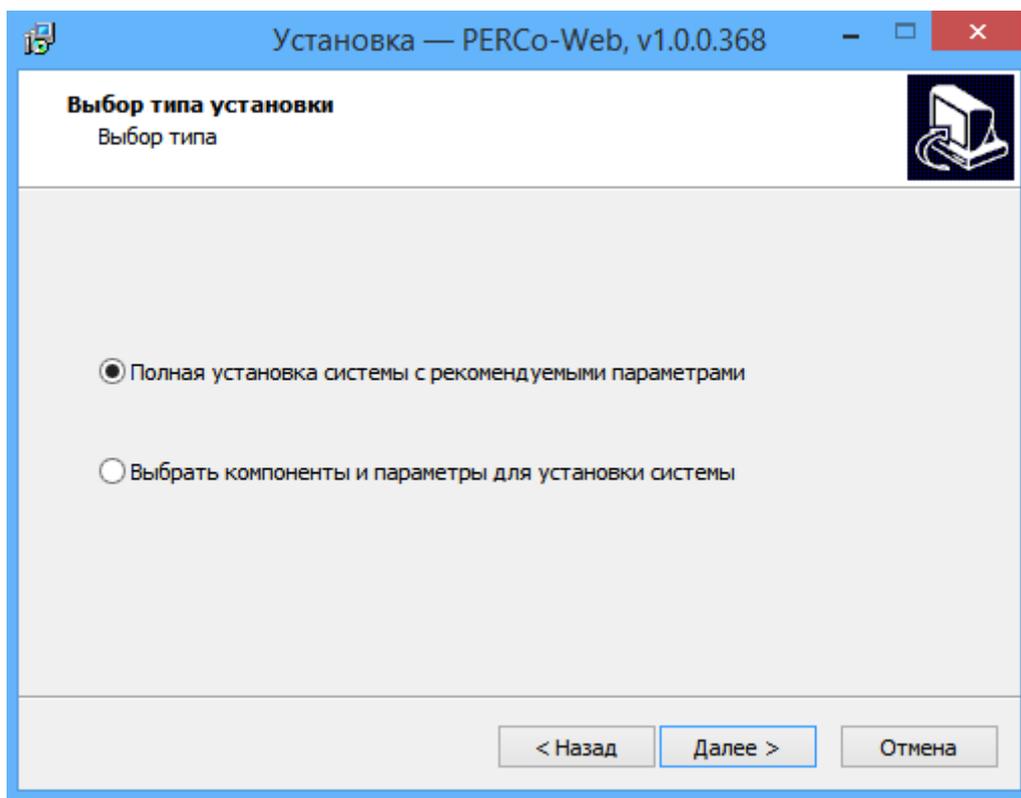
8 Установка системы

Внимание!

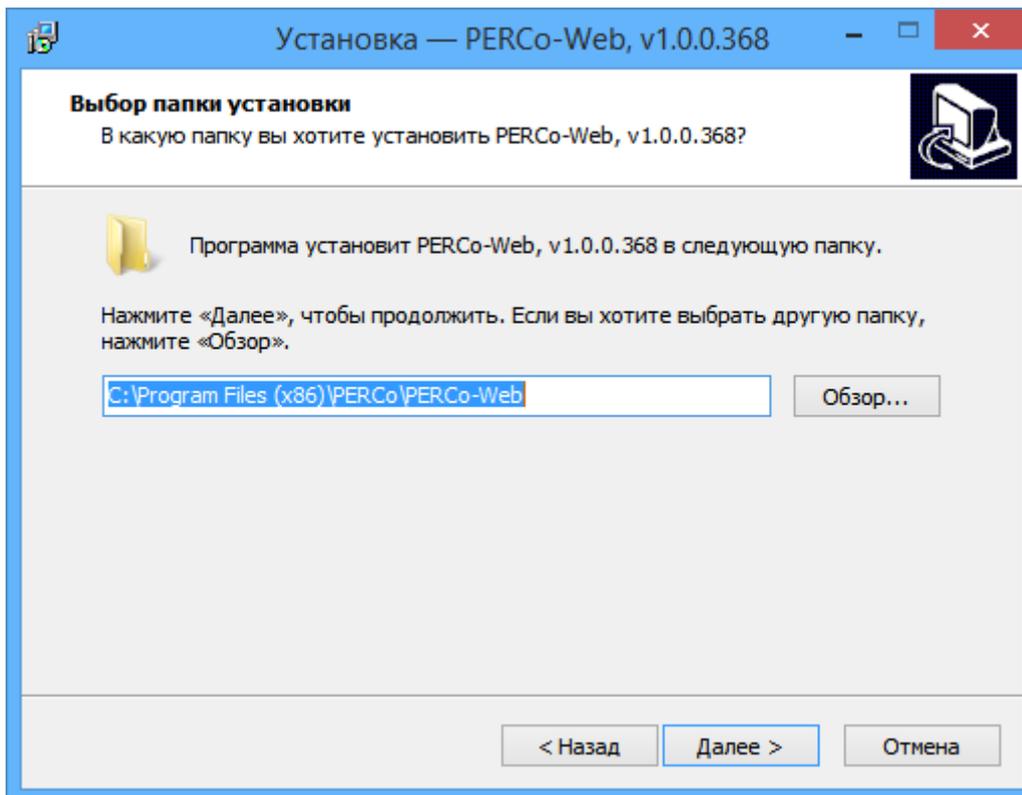
Для корректной работы сервера системы может потребоваться дополнительная настройка брандмауэра *Windows*.

При установке системы придерживайтесь следующей последовательности действий:

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



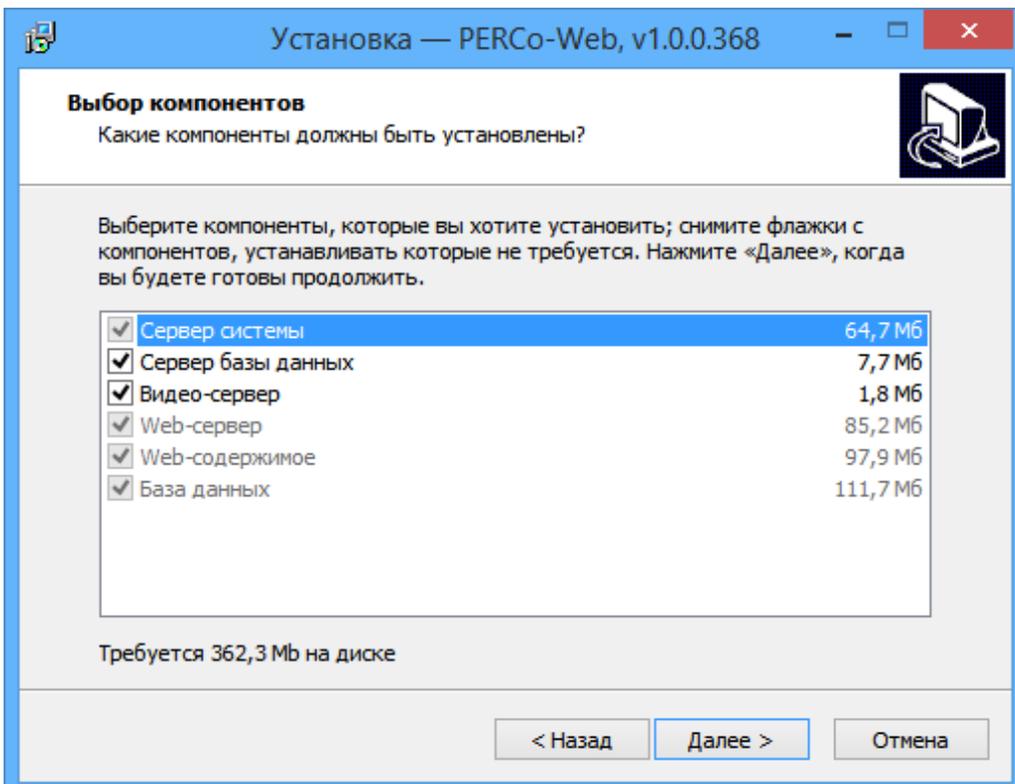
3. Укажите папку для установки системы. Нажмите кнопку **Далее**.



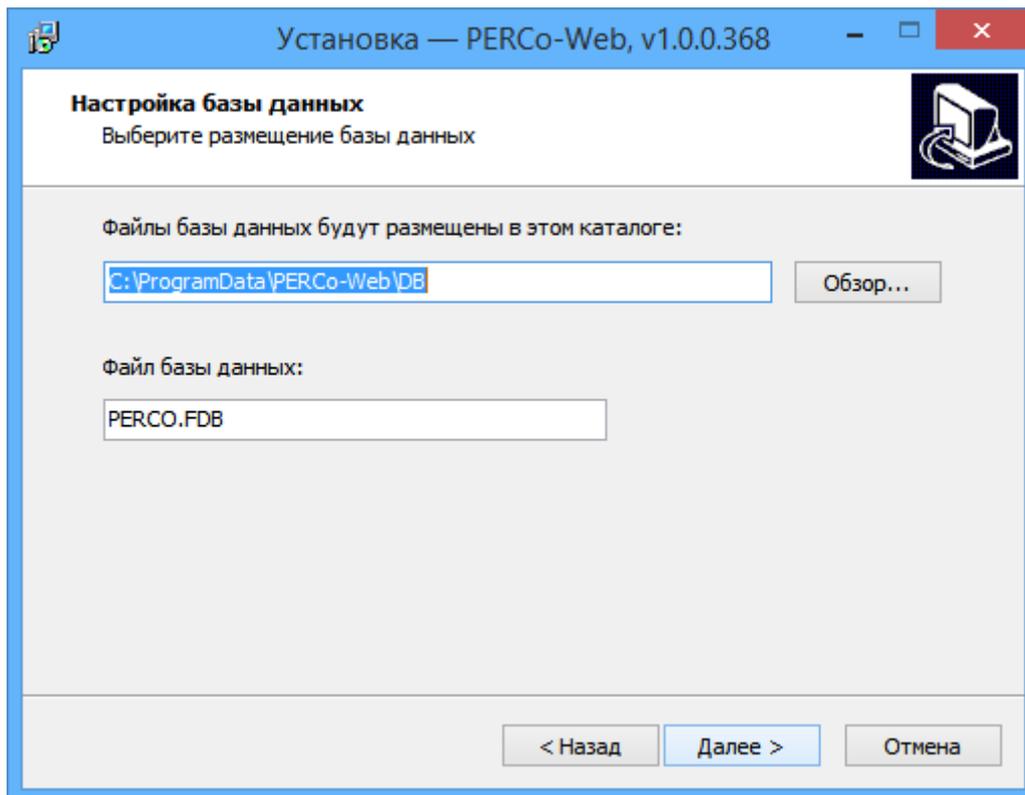
4. Отметьте флажками компоненты системы, которые необходимо установить на ПК. Нажмите кнопку **Далее**.

Примечание:

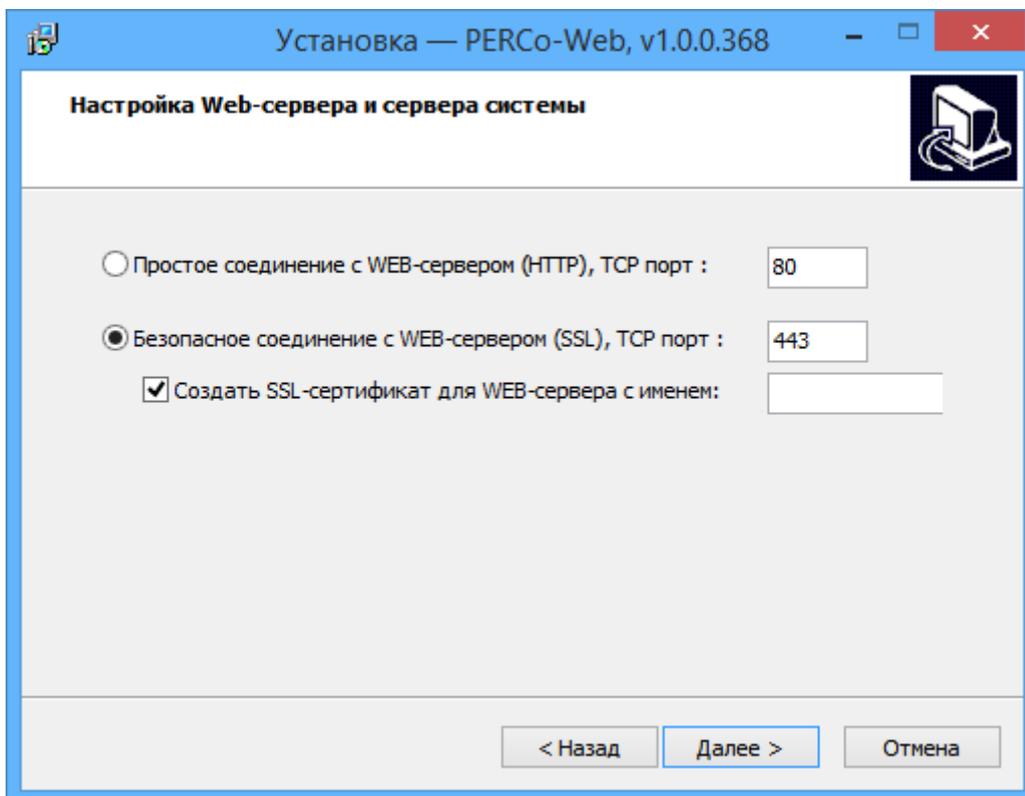
Если для установки был отмечен компонент **Сервер базы данных**, то перед установкой ПО системы будет запущен стандартный мастер установки SQL сервера *Firebird* и *FireBird ODBC Driver*.



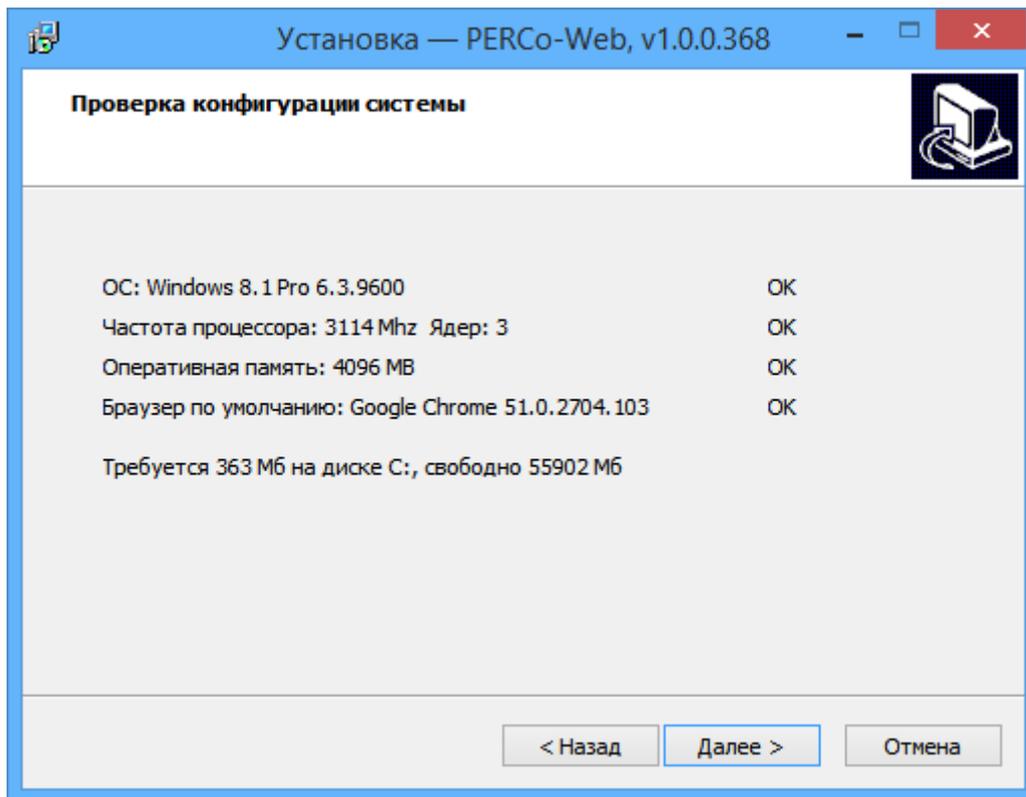
5. Укажите папку расположения БД системы. Нажмите кнопку **Далее**.



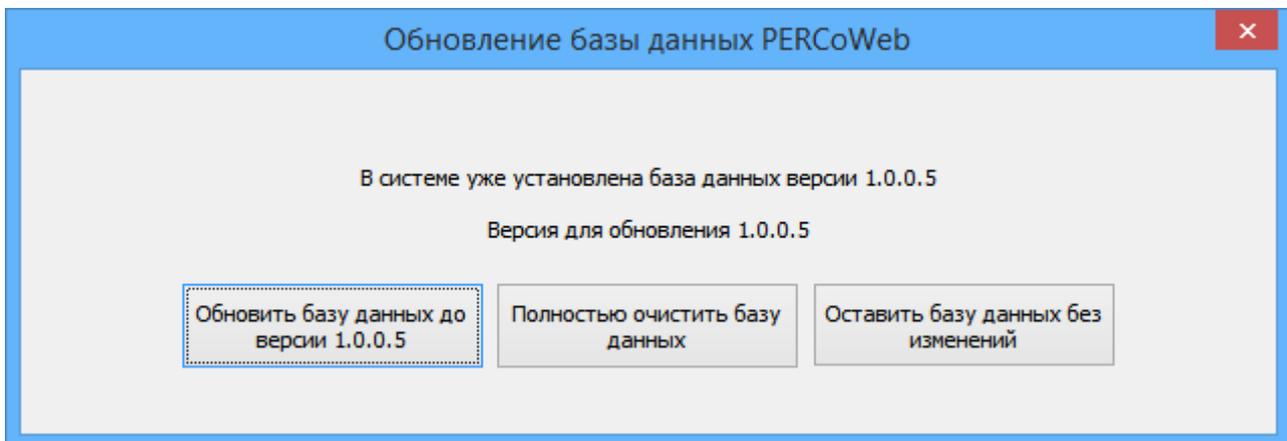
6. Произведите настройку сетевых параметров серверов системы. Нажмите кнопку **Далее**.



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



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



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

Примечание:

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

9 Управление лицензиями

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

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

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

После окончания ознакомительного периода доступ к дополнительным модулям ПО, для которых не введен код активации, будет запрещен. Если не была приобретена лицензия на **«Стандартный пакет ПО»**, то для дальнейшей работы с ПО необходимо получить и ввести код активации на бесплатный модуль **PERCo-WB «Базовый пакет ПО»** со следующими ограничениями:

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

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

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

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

Состав модулей ПО PERCo-Web

Модуль ПО	Входящие в модуль разделы
PERCo-WB «Базовый пакет ПО»	«Администрирование» «Персонал» «Бюро пропусков» , подразделы: <ul style="list-style-type: none"> • «Сотрудники» • «Шаблоны доступа» «Контроль доступа» , подразделы: <ul style="list-style-type: none"> • «Управление устройствами» • «Отчет по доступу в помещения»
PERCo-WS «Стандартный пакет ПО»	Все разделы, входящие в «Бесплатное ПО» , а также: <ul style="list-style-type: none"> • «Бюро пропусков» • «Посетители» • «Дизайн пропуска» • «Отчет по посетителям» «Контроль доступа» , подраздел: <ul style="list-style-type: none"> • «Отчет о проходах» • «Заказ пропуска»
PERCo-WM-01 «Учет рабочего времени»	«Учет рабочего времени» «Контроль доступа» , подраздел: <ul style="list-style-type: none"> • «Местонахождение»
PERCo-WM-02 «Верификация»	«Верификация» «Контроль доступа» , подраздел: <ul style="list-style-type: none"> • «Журнал верификации»

Порядок приобретения лицензии на ПО

Для приобретения лицензии и получения ключей активации модулей ПО:

1. Выберите один из приобретенных ранее контроллеров **PERCo**, который будет использоваться в качестве электронного ключа защиты ПО системы.
2. Заполните заявку для приобретения лицензии на ПО системы. Заявку можно заполнить на сайте компании **PERCo**, по адресу www.perco.ru в разделе **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»**.

10 Менеджер системы безопасности PERCo-Web

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

Вкладка **Состояние** предназначена для:

- запуска и остановки серверов системы;
- просмотра списка контроллеров, подключенных к серверу системы.

Вкладка **Базы данных** предназначена для:

- указания путей расположения файлов БД и резервной копии БД системы;
- [создания резервной копии БД системы](#);

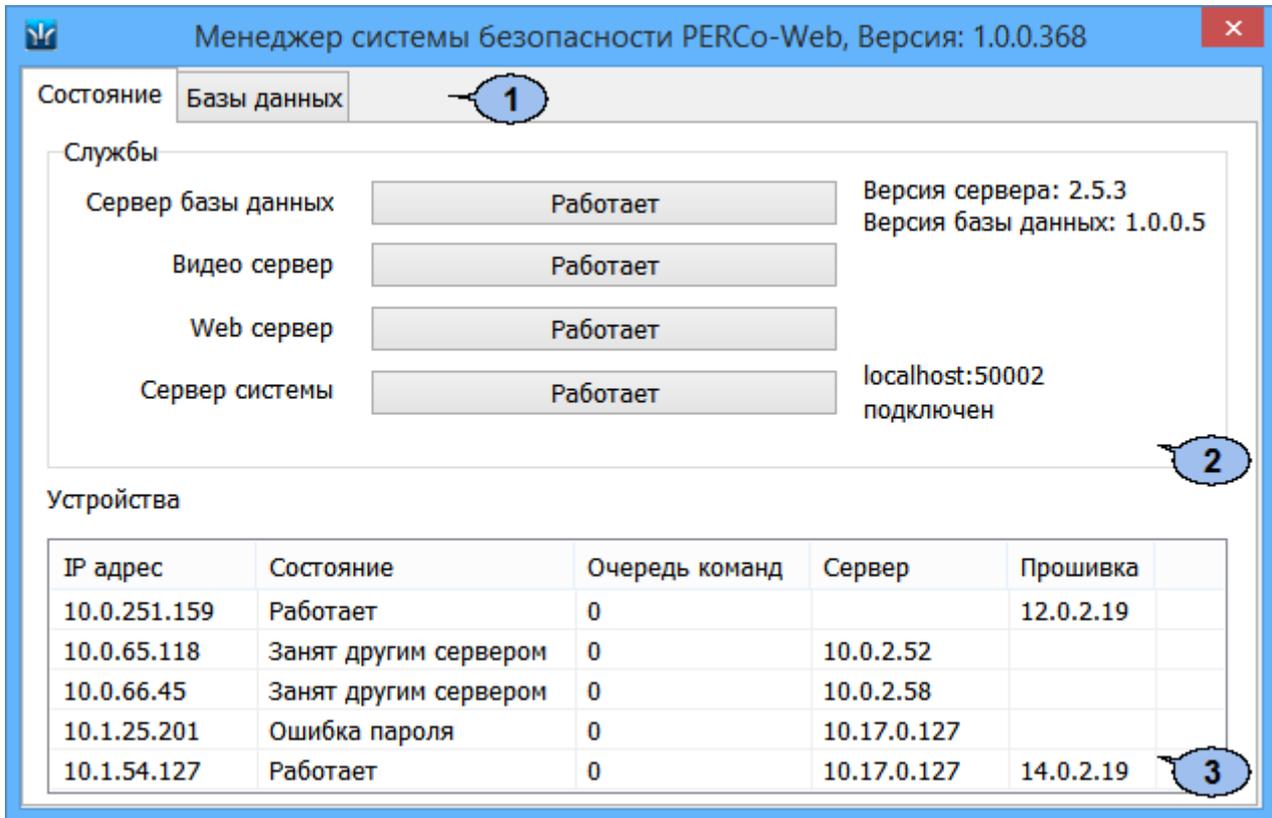
Примечание:

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

- [восстановления БД из созданного ранее файла резервной копии](#);
- импорт БД из файла более ранних версий БД системы.

10.1 Управление серверами системы

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



1. Выбор вкладки окна:

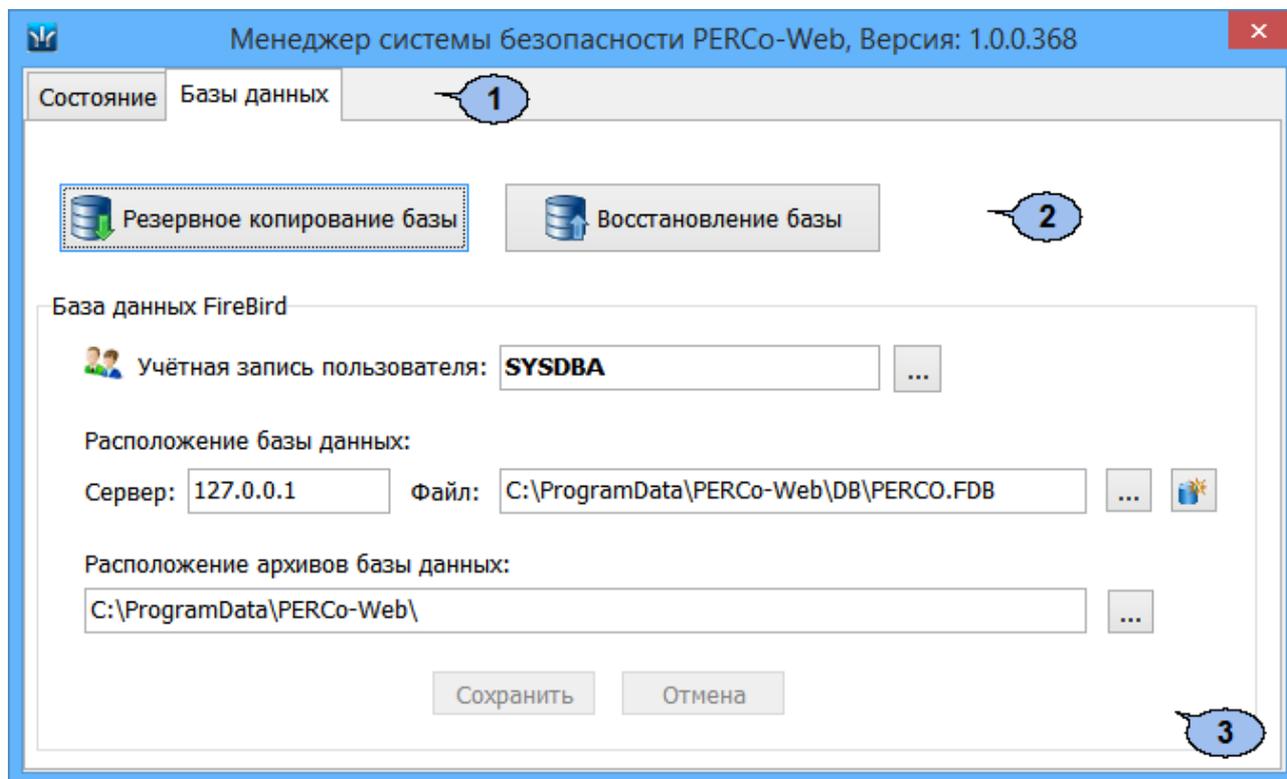
- **Состояние**
- **Базы данных**

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

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

10.2 Управление БД

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



1. Выбор вкладки окна:

- **Состояние**
- **Базы данных**

2. Кнопки управления БД:

Резервное копирование базы – кнопка позволяет создать резервную копию БД.

Восстановление базы – кнопка позволяет восстановить БД из созданной ранее резервной копии.

3. Панель **База данных FireBird** содержит следующие элементы:

Учетная запись пользователя: – при нажатии кнопки  справа от поля открывается окно для создания новой учетной записи пользователя БД или выбора одной из созданных ранее.

Расположение базы данных:

Сервер: – поле для ввода IP-адреса ПК, на котором установлена СУБД.

Файл: – при нажатии кнопки  справа от поля откроется окно проводника для выбора папки расположения БД.



Создать новую базу данных – кнопка позволяет создать новую БД в указанной папке.

Расположение архивов базы данных: – при нажатии кнопки  справа от поля откроется окно проводника для выбора папки

расположения резервной копии БД.

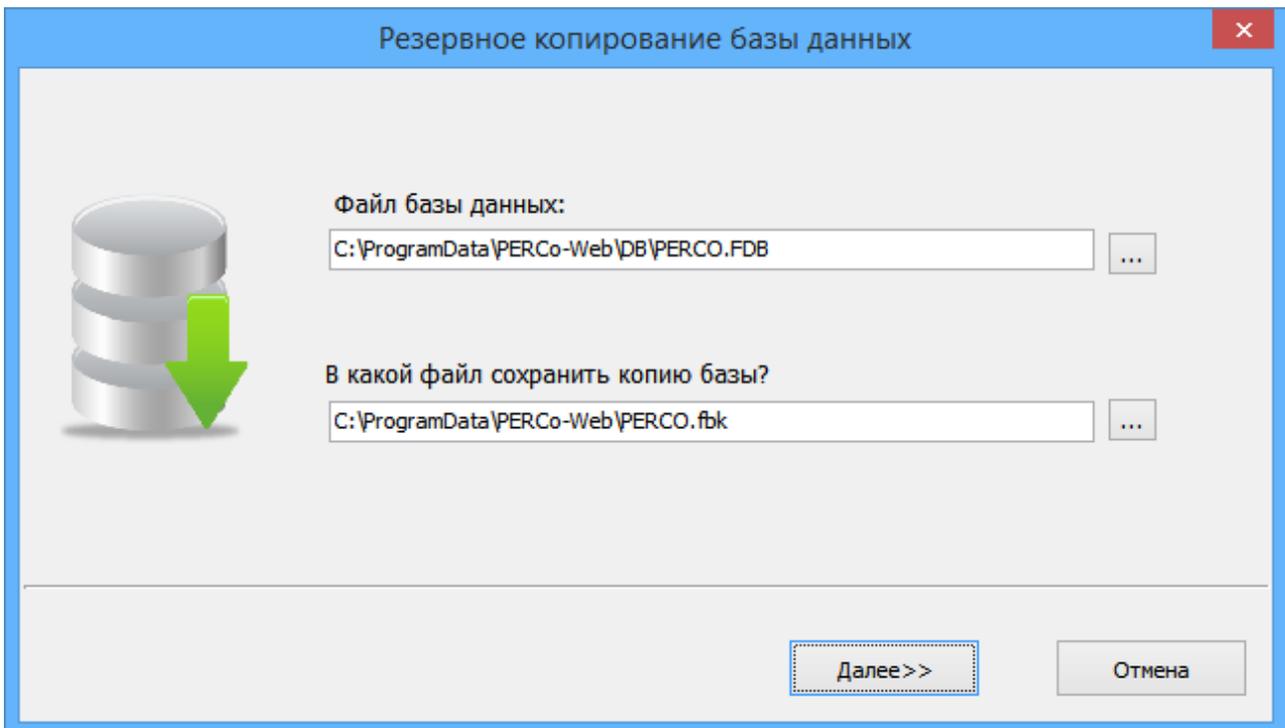
Сохранить – кнопка позволяет сохранить внесенные на панели изменения.

Отмена – кнопка позволяет отменить внесенные на панели изменения.

10.2.1 Резервное копирование БД

Для создания резервной копии БД:

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

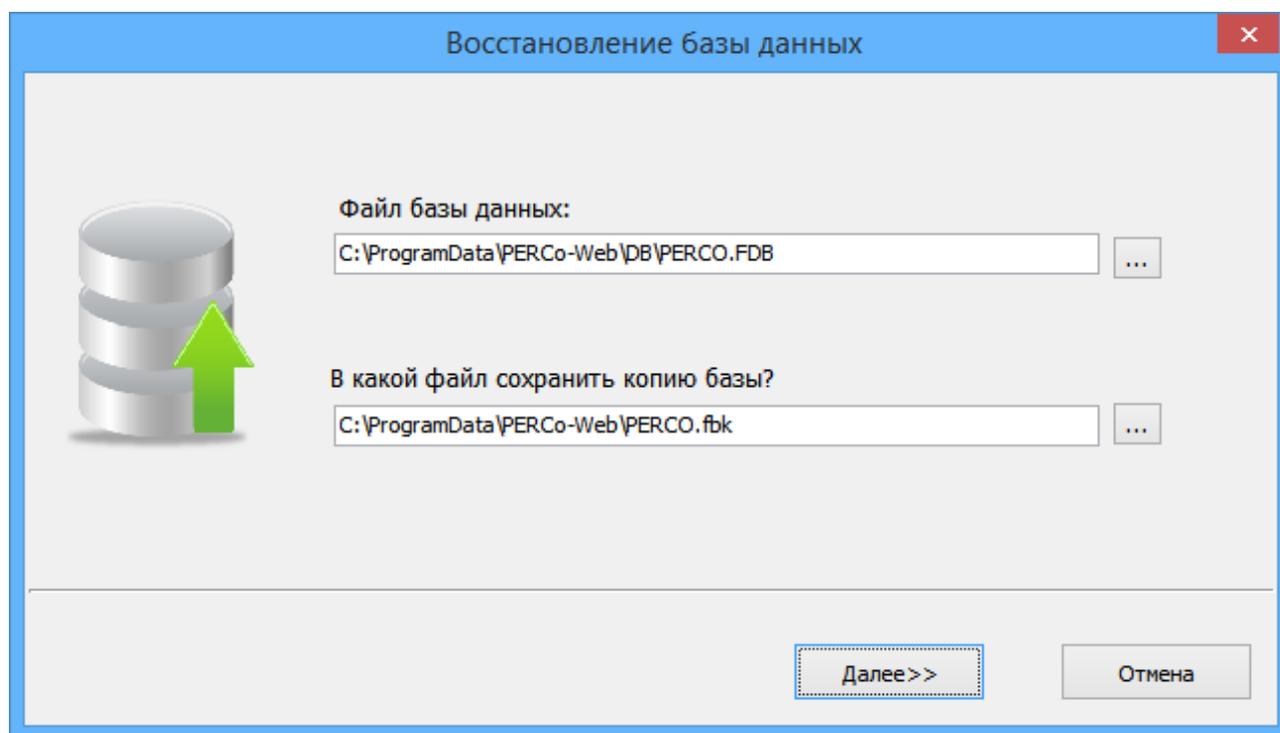


4. В открывшемся окне нажмите кнопку  справа от поля **Файл базы данных**. В открывшемся окне проводника выберите папку расположения БД.
5. Нажмите кнопку  справа от поля **В какой файл сохранить копию базы?**. В открывшемся окне проводника выберите папку, в которой необходимо сохранить резервную копию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

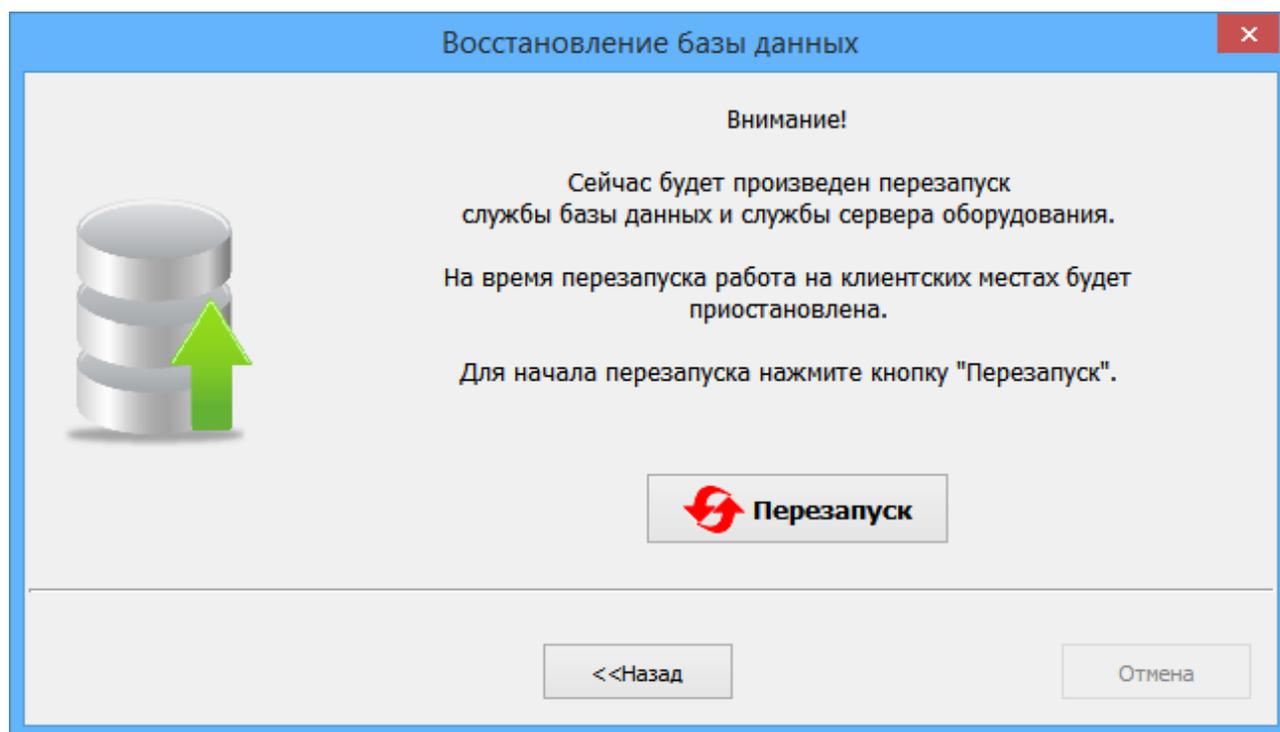
10.2.2 Восстановление БД из резервной копии

Для создания резервной копии БД:

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



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



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

11 Предварительная настройка

При подготовке системы к работе придерживайтесь следующей последовательности действий:

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

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

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

3. Используя панель навигации, перейдите в раздел  **«Бюро пропусков»**. Откройте подраздел **«Шаблоны доступа»**.

- Создайте шаблоны доступа для сотрудников предприятия и посетителей. При создании шаблона для каждого помещения устанавливаются индивидуальные права доступа и критерии доступа по времени.
- При необходимости отредактируйте календарь праздничных дней, доступ в которые будет ограничен или запрещен.

4. Используя панель навигации, перейдите в раздел  **«Персонал»**.

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

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

12 Функции Antipass и Global Antipass

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

Функция Antipass

Примечание:

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

Для включения/ отключения функции контроля зональности:

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

Свойства контроллера ✕

Имя контроллера:

Тип контроллера: **Контроллер замка [1]**

Выход из:  ✕

Вход в:  ✕

Генератор тревоги (1,2)

Замок

Считыватель

Состояние

Внешние подключения

Список коммисионирующих карт

Время удержания в разблокированном состоянии (время анализа идентификатора)

Время ожидания коммисионирования

Регистрация прохода по предъявлению идентификатора

Внутренняя защита от передачи идентификаторов (Local Antipass)

Режим работы выхода управления ИУ

Все в контроллер

Сохранить

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

8. Перейдите на вкладку **Считыватель** для настройки параметров контроля зональности при проходе в направлении считывателя.

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

10. Нажмите кнопку **Сохранить**. Окно **Свойства контроллера** будет закрыто, измененные параметры будут переданы в контроллер.

Функция Global Antipass

Для включения/ отключения функции глобального контроля зональности:

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

Общие настройки контроллеров ✕

Общие параметры контроллеров Карты Mifare Контроллеры Suprema

Пароль	Глобальный антипас
Режим работы считывателей	Отключен
Глобальный антипас	

Все в контроллер(ы) ▼ **Сохранить**

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

13 Раздел «Администрирование»

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

13.1 Подраздел «Конфигурация»

В подразделе доступны следующие вкладки:

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

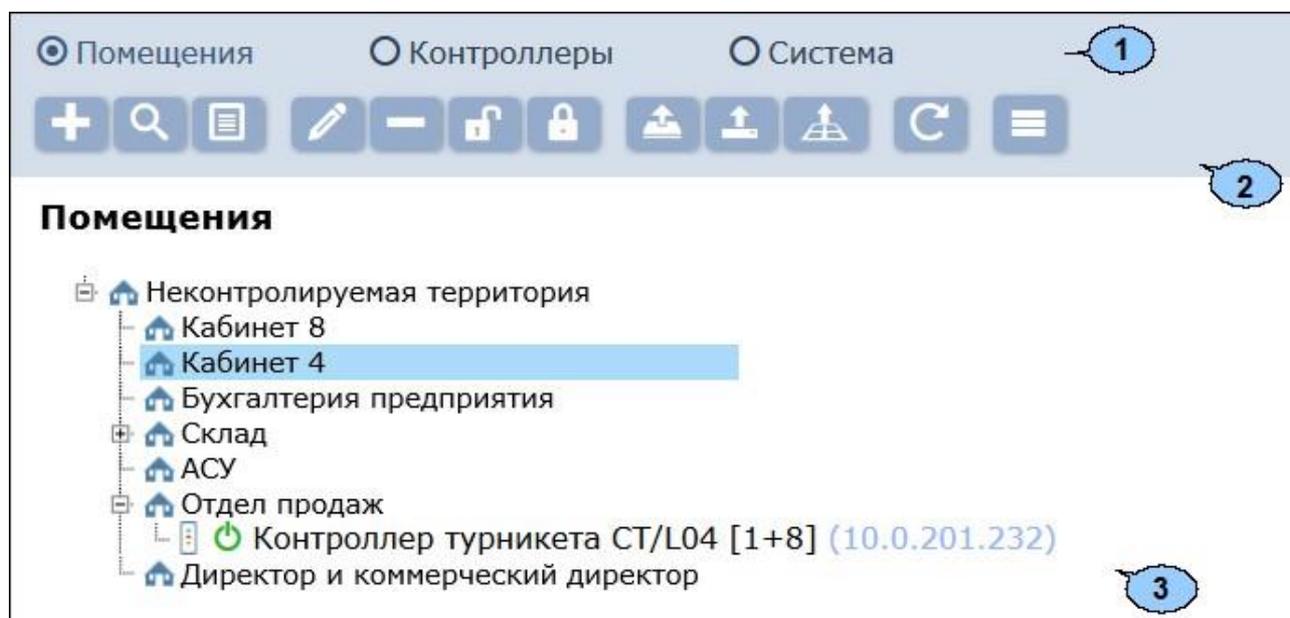
Вкладка **Контроллеры** предназначена для:

- [поиска контроллеров](#) в локальной сети и добавления в конфигурацию системы;
- [настройки параметров контроллеров](#) и их ресурсов;
- подачи команд управления;
- временного исключения контроллера из конфигурации;
- [создания списка коммисионирующих карт](#).

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

13.1.1 Вкладка «Помещения»

Страница вкладки имеет следующий вид:



1. Переключатель выбора вкладки подраздела:
 - **Помещения**;
 - [Контроллеры](#);
 - [Система](#).

2. Панель инструментов страницы:



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



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



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



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



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



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



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



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



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



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



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



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

- **Печать таблицы** – позволяет распечатать список помещений с указанием расположенных в них контроллеров.
- **Экспорт в XLS** – позволяет сохранить список помещений

с указанием расположенных в них контроллеров в файл электронных таблиц *MS Office Excel* с расширением *.xls*.

-  **Экспорт в CSV** – позволяет сохранить список помещений с указанием расположенных в них контроллеров в файл электронных таблиц *OpenOffice Calc* с расширением *.csv*.

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

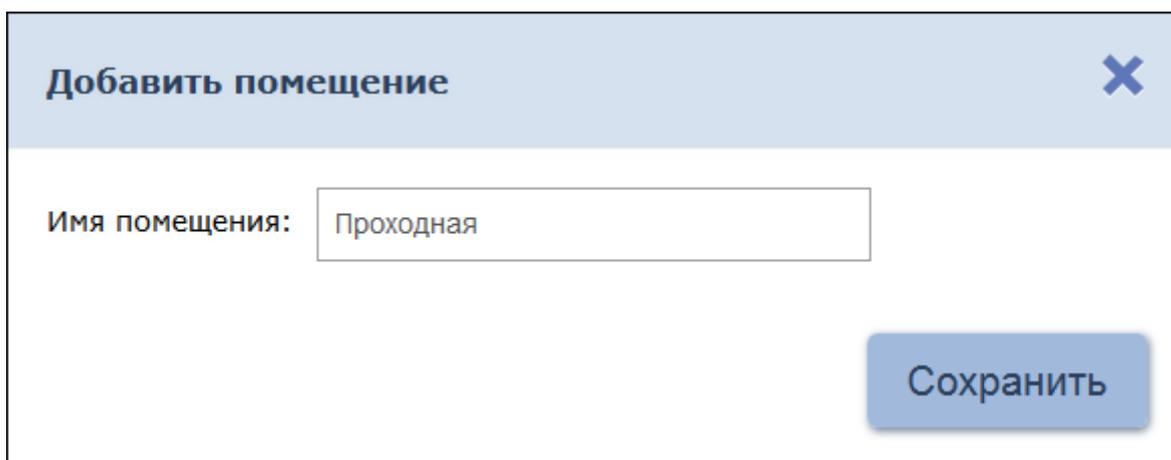
Примечание:

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

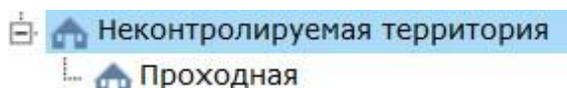
Создание списка помещений

Для создания списка помещений:

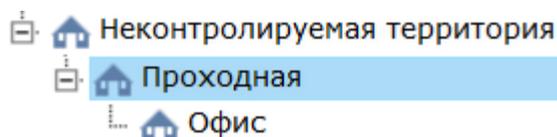
1. Используя панель навигации, перейдите в раздел  «**Администрирование**».
2. Откройте подраздел «**Конфигурация**».
3. Перейдите на вкладку **Помещения**.
4. Выделите в рабочей области страницы помещение «*Неконтролируемая территория*».
5. Нажмите на панели инструментов страницы кнопку **Добавить помещение**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



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



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



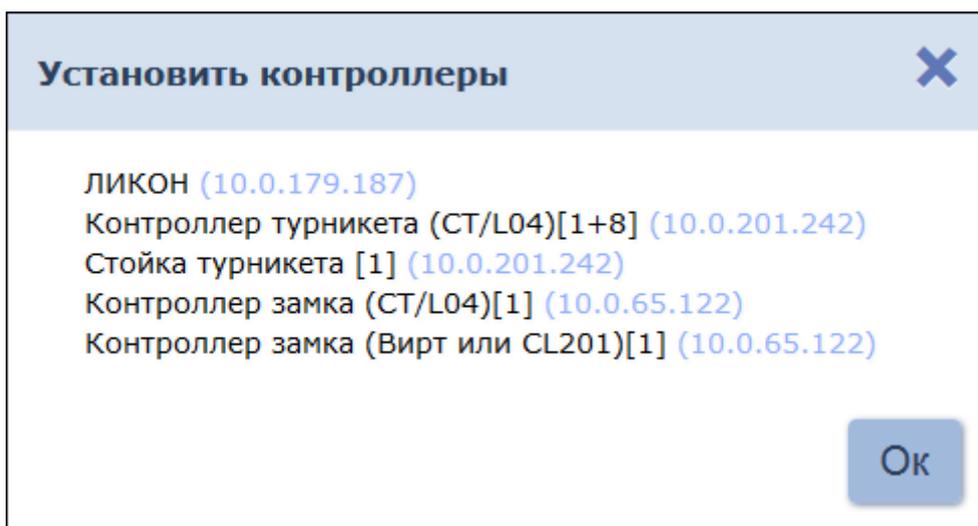
9. Для изменения названия добавленного ранее помещения выделите его в рабочей области страницы и нажмите на панели инструментов страницы кнопку **Редактировать** . Откроется окно **Редактировать помещение**:

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

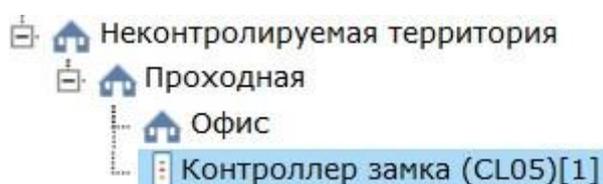
Размещение контроллеров в помещениях

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

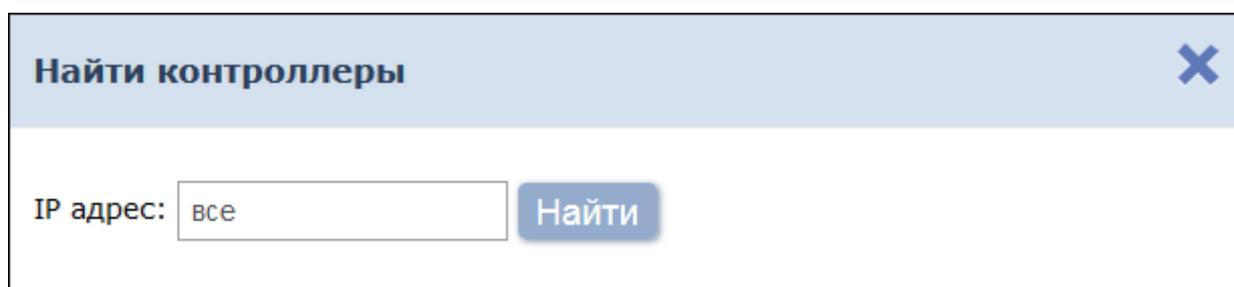
1. Для размещения контроллера в одно из помещений выделите это помещение в рабочей области страницы и нажмите на панели инструментов кнопку **Установить контроллер** . Откроется окно **Установить контроллеры**, содержащее список контроллеров, добавленных ранее в конфигурацию системы:



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



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



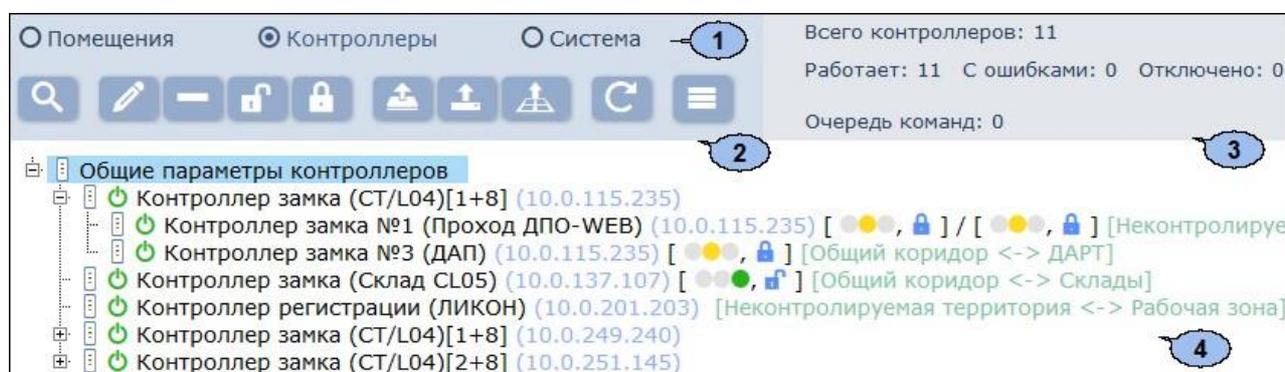
4. В открывшемся окне введите IP-адрес искомого контроллера и нажмите кнопку **Найти**. Найденный контроллер будет размещен в помещении и автоматически добавлен в конфигурацию системы.
5. При необходимости произведите настройку параметров работы контроллера. Для этого выделите контроллер в рабочей области страницы и нажмите на панели инструментов страницы кнопку **Редактировать** . В открывшемся окне **Свойства контроллера** произведите необходимые изменения и нажмите кнопку **Сохранить и закрыть**.
6. Для контроллеров электромеханических замков модели **PERCo-CL05.1** 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 **Свойства контроллера**.

- Для удаления добавленного ранее в помещение контроллера выделите его в рабочей области страницы и нажмите кнопку **Удалить помещение / Отвязать контроллер**  на панели инструментов. В открывшемся окне подтверждения нажмите кнопку **ОК**. Помещение будет удалено из списка.
- Нажмите на панели инструментов страницы кнопку **Передать всю конфигурацию в контроллеры** .

13.1.2 Вкладка «Контроллеры»

Страница вкладки имеет следующий вид:



- Переключатель выбора вкладки подраздела:

- [Помещения](#);
- [Контроллеры](#);
- [Система](#).

- Панель инструментов страницы:



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



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



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



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



Деактивировать – кнопка позволяет временно исключить из

конфигурации системы контроллер, выделенный в рабочей области страницы. При этом наименование контроллера затемняется.



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



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



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



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



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

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

3. Панель информации о состоянии контроллеров системы.

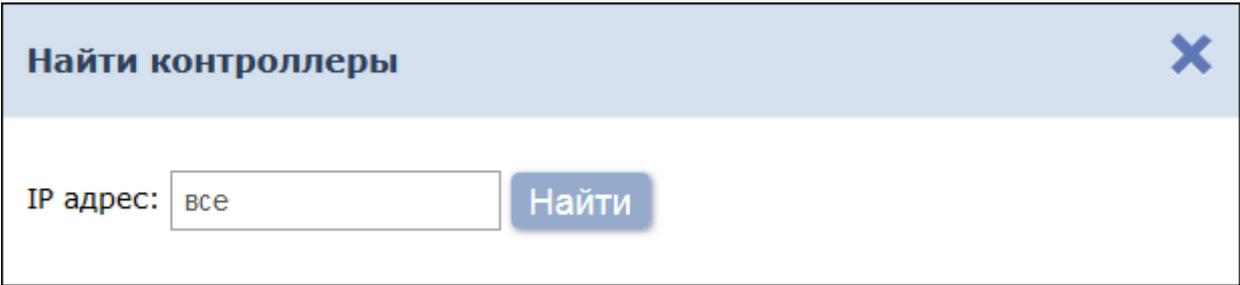
4. Рабочая область страницы содержит список контроллеров, добавленных в конфигурацию системы. Значок  **Валидность** слева от наименования указывает на то, что в контроллер не были переданы измененные параметры. Справа от наименования контроллера расположены значки, указывающие на установленный РКД и состояние ИУ:

-  – РКД «Открыто»,
-  – РКД «Контроль»,
-  – РКД «Закрото»,
-  – ИУ заблокировано,
-  – ИУ разблокировано,
-  – взлом ИУ.

Поиск контроллеров

Для проведения автоматической конфигурации:

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



Найти контроллеры 

IP адрес: 

5. Если необходимо произвести поиск контроллера по IP-адресу, то введите его в поле **IP адрес** и нажмите кнопку **Найти**.
6. Если необходимо произвести поиск всех контроллеров в сети, то нажмите кнопку **Найти**.
7. По окончании поиска список найденных контроллеров появится в рабочей области окна:

Найти контроллеры ✕

IP адрес:

Найдено контроллеров: **21**

- Контроллер замка №6 (10.1.32.28)
- Контроллер замка №7 (10.1.32.28)
- Контроллер замка №8 (10.1.32.28)
- Контроллер замка №9 (10.1.32.28)
- Контроллер замка №10 (10.1.32.28)
- Контроллер замка CL05.1 (10.1.33.126)
- Контроллер замка CL05.1 (10.1.33.131)
- Контроллер замка CL05.1 (10.1.33.144)
- Контроллер замка CL05.1 (10.1.33.146)
- Контроллер замка CL05.1 (10.1.47.235)
- Контроллер замка СТ/L04 [1+8] (10.1.49.183)
- Контроллер замка №1 (10.1.49.183)
- Контроллер замка №3 (10.1.49.183)
- Контроллер замка №4 (10.1.49.183)
- Контроллер замка №5 (10.1.49.183)
- Контроллер замка №6 (10.1.49.183)
- Контроллер замка №7 (10.1.49.183)
- Контроллер замка №8 (10.1.49.183)
- Контроллер замка №9 (10.1.49.183)
- Контроллер замка №10 (10.1.49.183)
- Контроллер замка CL05.1 (10.1.51.162)
- 172.17.0.0
- Контроллер Suprema BioEntry W2 (172.17.100.211)
- Контроллер Suprema BioEntry Plus (172.17.100.212)

8. Для поиска контроллера в списке введите его IP-адрес в поле, расположенное в нижней части окна, и нажмите кнопку **Найти**. Название контроллера будет выделено в списке желтым.

9. Выделите в списке контроллер (или несколько контроллеров), который необходимо добавить в конфигурацию системы. Нажмите кнопку **Добавить**. Окно будет закрыто, отмеченные контроллеры появятся в рабочей области страницы.

10. Активируйте добавленный контроллер. Для этого выделите его в рабочей области страницы и нажмите кнопку **Активировать** .

11. Произведите настройку параметров добавленного контроллера. Для этого выделите контроллер или его ресурс в рабочей области

страницы и нажмите на панели инструментов кнопку

Редактировать . Откроется окно **Свойства контроллера**.

12. В открывшемся окне при необходимости в поле **Имя контроллера** измените описательное название контроллера.

13. Укажите (или, при необходимости, измените) помещения, доступ между которыми обеспечивается контроллером. Для этого нажмите

кнопку **Выбрать из списка**  справа от поля **Выход из**. В открывшемся окне **Помещения** выделите помещение, в которое осуществляется доступ через считыватель №1, и нажмите кнопку **Ок**. Тем же образом в поле **Вход в** укажите помещение, в которое осуществляется доступ через считыватель №2.

14. Для настройки параметров ресурсов контроллера перейдите на вкладку, соответствующую наименованию ресурса, и произведите необходимые изменения. Список доступных параметров зависит от типа контроллера и выбранного ресурса.

15. С помощью раскрывающегося списка в нижней части окна **Свойства контроллера** выберите способ сохранения параметров и нажмите кнопку **Сохранить и закрыть**. Окно **Свойства контроллера** будет закрыто.

16. Передайте конфигурацию в контроллеры. Для этого на панели инструментов страницы нажмите кнопку **Передать изменения**

конфигурации в контроллеры  или **Передать всю**

конфигурацию в контроллеры .

Общие настройки контроллеров

Для настройки общих параметров контроллеров:

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

2. Откройте подраздел **«Конфигурация»**.

3. Перейдите на вкладку **Контроллеры**.

4. Выделите в рабочей области страницы корневой элемент **Общие параметры контроллеров**.

5. Нажмите на панели инструментов страницы кнопку **Редактировать**

, после чего откроется окно **Общие настройки контроллеров**.

Во вкладке **Общие параметры контроллеров** окна [Общие настройки контроллеров](#) представлены следующие опции:

Общие настройки контроллеров



Общие параметры контроллеров

Карты Mifare

Контроллеры Suprema

Пароль

Изменить пароль

••••••

Режим работы считывателей

Подтверждение

••••••

Глобальный антипас

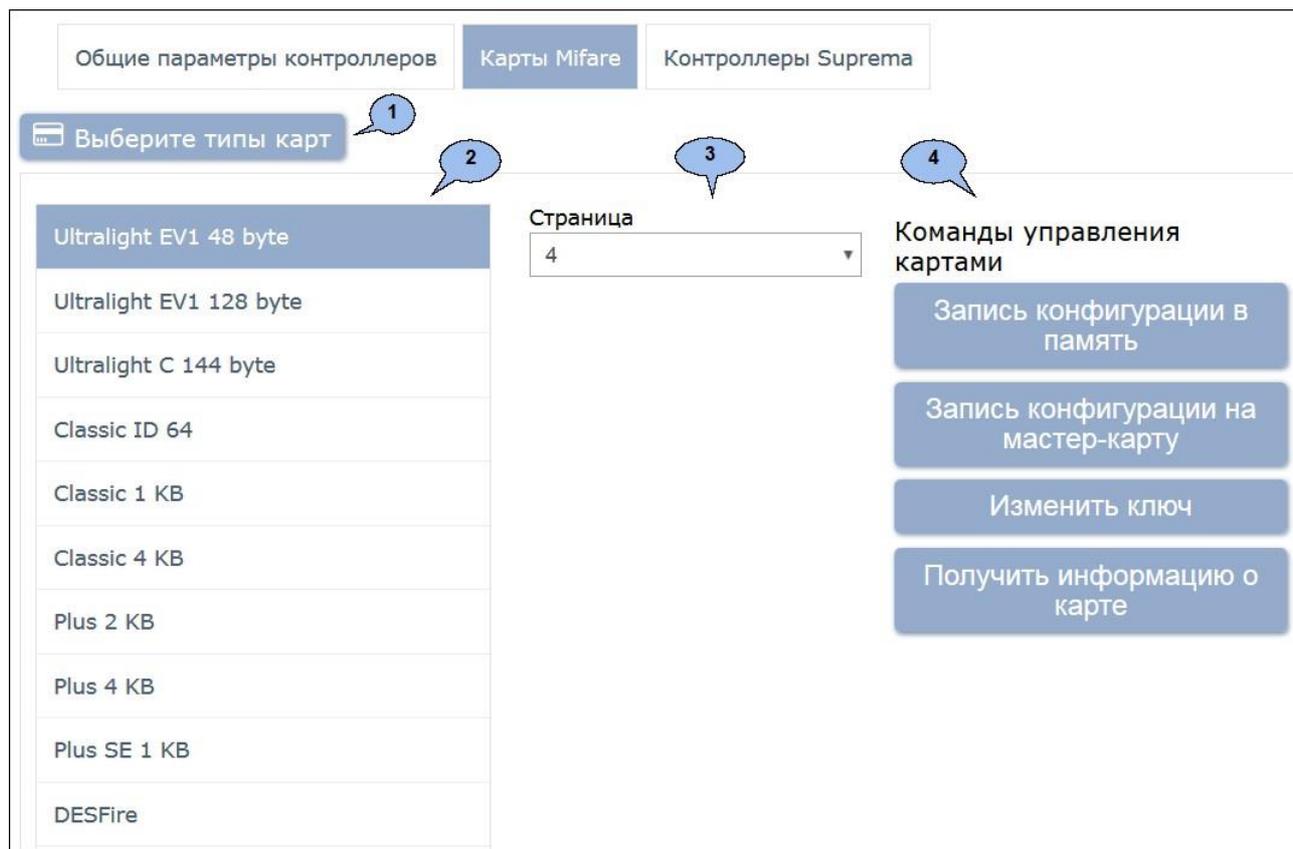
Все в контроллер(ы)

Сохранить

1. **Пароль** - позволяет изменить общий пароль для доступа к контроллерам.
2. **Режим работы считывателей** - позволяет изменить параметры режима работы считывателей.
3. **Глобальный антипас** - позволяет включить или отключить глобальный контроль зональности.

С помощью раскрывающегося списка в нижней части окна выберите способ сохранения параметров. Остальные параметры можно изменить во вкладках [Карты Mifare](#) и [Контроллеры Suprema](#). Для завершения работы с окном **Общие настройки контроллеров** нажмите кнопку **Сохранить**.

На вкладке **Карты Mifare** представлены следующие опции:



1. Кнопка  **Выберите типы карт** – позволяет с помощью всплывающего окна **Типы карт Mifare** выбрать те карты, которые будут использоваться в СКУД. Для выбора доступны следующие типы карт:

- **Ultralight EV1 48 byte,**
- **Ultralight EV1 128 byte,**
- **Ultralight C 144 byte,**
- **Classic ID 64 byte,**
- **Classic 1KB,**
- **Classic 4KB,**
- **Plus 2KB,**
- **Plus 4KB,**
- **Plus SE 1KB,**
- **DESFire Ev1.**

2. Область **Список карт** – отображает выбранные типы карт **Mifare** в виде списка, позволяет переключаться между картами для конфигурации их параметров.

3. Область **Параметры карт** – содержит список параметров, которые возможно конфигурировать для выбранного типа карты.

Примечание:

Список доступных **параметров карт и команд управления картами** может меняться в зависимости от выбранного для конфигурирования типа карты.

4. Область **Команды управления картами** – 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 изменённые параметры для простых карт всех типов ([Ultralight](#), [Classic](#), [Plus](#), [DESFire](#)). По команде считыватель определяет наличие карты в поле считывателя, её 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**;
 - **Серия UID** – отображает серию уникального идентификатора пользователя;
 - **Номер UID** – отображает номер уникального идентификатора пользователя;
 - **Тип карты** – отображает тип карты: мастер-карта, обычная 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 уровнем безопасности 1 и 2, позволяет повысить уровень безопасности [SL \(secure level\)](#);
- **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.

Примечание:

- 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 её в контрольный считыватель, после чего она автоматически переписывается во все контрольные считыватели, подключенные в этот момент к СКУД.

Режим работы считывателей позволяет перейти к настройке дополнительных параметров режима работы считывателей.

Скриншот интерфейса настройки считывателей. В центре внимания — выпадающее меню «Режим работы считывателей» (1) и панель «Общие настройки карт Mifare» (2).

1. Раскрывающееся меню **Режим работы считывателей** позволяет выбрать режим работы считывателей из следующих доступных вариантов:
 - Универсальный (8 байт);
 - Wiegand 26.
2. Область **Общие настройки карт Mifare** позволяет выбрать следующие параметры:
 - **Чтение из защищённой области** – определяет порядок работы с защищённой областью карт **Mifare**:
 - **Простое чтение** – чтение UID с карты;
 - **С записью карты** – чтение номера карты из защищённой области с последующей его перезаписью по заданному алгоритму генерации номера.
 - **Генерация номера** – определяет порядок генерации номера

карты, записываемого в защищённую область карт **Mifare** и используемого в СКУД в качестве идентификатора:

- **Ручной ввод** – в этом случае в момент выдачи карты номер карты вводится вручную;
 - **Случайный номер** – в этом случае в момент выдачи случайный номер карты генерируется автоматически;
 - **По возрастанию** – в этом случае в момент выдачи карты программой автоматически будет сгенерирован номер, значение которого на единицу больше, чем значение предыдущего выданного номера карты.
- **Ключ закрытия мастер-карты** – поле отображает текущий ключ закрытия мастер-карты.
 - **Новый ключ закрытия мастер-карты** – поле позволяет ввести новый ключ закрытия мастер-карты.

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

Примечание:

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

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

Внимание!

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

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

Основные характеристики разных чипов MIFARE

Тип карты	MIFARE Ultralight	MIFARE Classic ID 64/1KB/4KB	MIFARE DESFire E V1 2K/4K/8K	MIFARE Plus (S and X) 2K/4K
Крипто-	Нет	CRYPTO1	DES & 3DES/AES	CRYPTO1/AES

Тип карты	MIFARE Ultralight	MIFARE Classic ID 64/1KB/4KB	MIFARE DESFire EV1 2K/4K/8K	MIFARE Plus (S and X) 2K/4K
алгоритм				
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%-ную совместимость с **MIFARE Classic 1K (4K)**.
- **Уровень безопасности SL2.** Аутентификация по AES является обязательной. Для защиты данных используется CRYPTO1.
- **Уровень безопасности SL3.** Аутентификация, обмен данными, работа с памятью только по AES.

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

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

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

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

с точки зрения защиты.

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

Алгоритм работы с защищённой областью памяти карт **Mifare** при записи в неё 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 >> Контроллеры**. Выберите пункт **Общие параметры контроллеров** и нажмите кнопку  **Редактировать**. В открывшемся окне **Общие настройки контроллеров** перейдите на вкладку **Карты Mifare**.

1. На вкладке **Карты Mifare** нажмите на кнопку  **Выберите типы карт**. После того, как откроется окно **Типы карт Mifare**, установите флажок напротив карты **Mifare Classic 4KB** и нажмите кнопку **Ок**.
2. 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.
3. 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.
4. 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 карт будет невозможна.

5. В поле **Тип ключа аутентификации** отображается текущий тип ключа аутентификации мастер-карты, то есть тип ключа, которым мастер-карта закрывалась ранее.
6. В поле **Ключ аутентификации** запишите новый ключ аутентификации, который будет использоваться в конфигурации как следующий ключ аутентификации.
7. 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 в **СКУД PERCo-S-20** используется мастер-карта **DESFire**. Чистая (т.е. без записей в защищенной области) карта типа **DESFire** также может быть записана в качестве дополнительной мастер-карты для СКУД. Перезапись мастер-карты с целью перевода её в состояние карты пользователя или чистой карты невозможна! (Т.е. карта, однажды записанная как мастер-карта, может использоваться далее только в этом качестве.)

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:

- а. Если в текущую конфигурацию СКУД добавляются новые типы карт пользователей, то ранее выданные карты будут работать.
- б. 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.
- в. Особенности работы с мастер-картами и рекомендации по паролям для них приведены в руководстве по эксплуатации на контрольный считыватель **PERCo-MR08**.

Каждый тип карт **Mifare (Ultralight, Classic, Plus, DESFire)** обладает определённым 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, Classic, Plus, DESFire** позволяют задать рабочие параметры криптозащиты для соответствующих типов карт, отмеченных флажками в окне **Типы карт Mifare**, вызываемом нажатием кнопки **Выберите 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.

Область **Список карт** отображает подвкладки, предназначенные для конфигурирования параметров соответствующих 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, номер сектора, номер блока** – адрес в памяти карты, где будет храниться ID пользователя карты, используемый в СКУД.
- **Ключ аутентификации** – пароль, которым закрыт доступ к ID карты, отображается в формате Hex.
- **Старые параметры, Старый ключ аутентификации** – поля для отображения пароля доступа к ID и его характеристик, которые действуют до предстоящей переконфигурации параметров (при предыдущей конфигурации параметров они 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).

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.

Параметры, отображающиеся для выбранного типа карты **Mifare Ultralight**.

• **Ultralight EV1 48 byte**

- **Страница** – номер страницы памяти карты, на которой будет храниться номер карты, используемый в СКУД, допустимые значения: 4-15.

• **Ultralight EV1 128 byte**

- **Страница** – номер страницы памяти карты, на которой будет

храниться номер карты, используемый в СКУД, допустимые значения: 4-35.

- **Ultralight C 144 byte**

- **Страница** – номер страницы памяти карты, на которой будет храниться номер карты, используемый в СКУД, допустимые значения: 4-39.
- **Старый ключ аутентификации** – отображает старый ключ аутентификации, длина 6 байт в формате *Hex*;
- **Ключ аутентификации** – ключ, используемый для аутентификации пользователя, длина 6 байт в формате *Hex*.

Параметры, отображающиеся для выбранного типа карты **Mifare Classic**.

- **Classic ID 64**

- **Номер блока** – номер блока, в котором будет храниться номер карты, используемый в СКУД, допустимые значения: 1, 2;
- **Старый тип ключа для аутентификации** – отображает старый тип ключа аутентификации, допустимые значения: А, В;
- **Старый ключ аутентификации** – отображает старый ключ аутентификации, длина 6 байт в формате *Hex*;
- **Тип ключа аутентификации** – тип ключа аутентификации, допустимые значения: А, В;
- **Ключ аутентификации** – ключ, используемый для аутентификации пользователя, длина 6 байт в формате *Hex*.

- **Classic 1 KB**

- **Номер сектора** – номер сектора, в котором находится блок для хранения номера карты, допустимые значения: 0-15;
- **Номер блока** – номер блока, в котором будет храниться номер карты, используемый в СКУД, допустимые значения:
 - 1, 2 – для сектора номер 0,
 - 0, 1, 2 – для секторов номер 1-15;
- **Старый тип ключа для аутентификации** – отображает старый тип ключа аутентификации, допустимые значения: А, В;
- **Старый ключ аутентификации** – отображает старый ключ аутентификации, длина 6 байт в формате *Hex*;
- **Тип ключа аутентификации** – тип ключа аутентификации, допустимые значения: А, В;
- **Ключ аутентификации** – ключ, используемый для аутентификации пользователя, длина 6 байт в формате *Hex*.

- **Classic 4 KB**

- **Номер сектора** – номер сектора, в котором находится блок для хранения номера карты, допустимые значения: 0-39;
- **Номер блока** – номер блока, в котором будет храниться номер карты, используемый в СКУД, допустимые номера:

- 1, 2 – для сектора номер 0,
- 0, 1, 2 – для секторов номер 1-31,
- 0-14 – для секторов номер 32-39;
- **Старый тип ключа для аутентификации** – отображает старый тип ключа аутентификации, допустимые значения: А, В;
- **Старый ключ аутентификации** – отображает старый ключ аутентификации, длина 6 байт в формате *Hex*;
- **Тип ключа аутентификации** – тип ключа аутентификации, допустимые значения: А, В;
- **Ключ аутентификации** – ключ, использующийся для аутентификации пользователя, длина 6 байт в формате *Hex*.

Примечание:

- **Номер сектора** – номер части внутренней области памяти карты, которая содержит в себе несколько блоков данных для хранения информации.
- **Номер блока** – номер минимальная часть памяти карты. Блоки данных доступны для чтения/записи при условии успешной авторизации по ключу.

Параметры, отображающиеся для выбранного типа карты **Mifare Plus:**

• **Plus 2 KB**

- **Номер сектора** – номер сектора, в котором находится блок для хранения номера карты, допустимые значения: 0-31.
- **Номер блока** – номер блока, в котором будет храниться номер карты, используемый в СКУД, допустимые значения:
 - 1, 2 – для сектора номер 0,
 - 0, 1, 2 – для секторов номер 1-31;
- **Старый тип ключа аутентификации** – отображает старый тип ключа аутентификации, допустимые значения: А, В;
- **Старый ключ аутентификации** – отображает ранее записанный ключ аутентификации, который используется при работе карт на уровне безопасности SL1 и SL2, длина 6 байт в формате *Hex*;
- **Старый ключ для уровня безопасности SL3 при типе ключа А** – отображает ключ для аутентификации на уровне SL3 при типе ключа А, длина 16 байт в формате *Hex*;
- **Старый ключ для уровня безопасности SL3 при типе ключа В** – отображает ключ для аутентификации на уровне SL3 при типе ключа А, длина 16 байт в формате *Hex*;
- **Тип ключа аутентификации** – тип ключа аутентификации, допустимые значения: А, В;
- **Ключ аутентификации** – ключ аутентификации, который используется при работе карт на уровне безопасности SL1 и SL2, длина 6 байт в формате *Hex*;

- **Ключ для уровня безопасности SL3 при типе ключа А**
– ключ для аутентификации на уровне SL3 при типе ключа А, длина 16 байт в формате *Hex*;
- **Ключ для уровня безопасности SL3 при типе ключа В**
– ключ для аутентификации на уровне SL3 при типе ключа В, длина 16 байт в формате *Hex*;
- **Уровень безопасности SL** – уровень безопасности для карт серии **Mifare Plus**, допустимые значения: 1-3;

Ключи для изменения уровня безопасности (SL):

- **Мастер ключ** – ключ, длина 16 байт в формате *Hex*;
- **Конфигурационный ключ** – ключ, длина 16 байт в формате *Hex*;
- **Ключ аутентификации для уровня безопасности SL1**
– ключ AES, длина 16 байт в формате *Hex*;
- **Ключ переключения на уровень безопасности SL2**
– ключ, длина 16 байт в формате *Hex*;
- **Ключ переключения на уровень безопасности SL3**
– ключ, длина 16 байт в формате *Hex*.

Примечание:

В отличие от ключей аутентификации, которые могут быть изменены при необходимости, ключи для изменения уровня безопасности (SL):

- **Мастер ключ,**
- **Конфигурационный ключ,**
- **Ключ аутентификации для уровня безопасности SL1,**
- **Ключ переключения на уровень безопасности SL2,**
- **Ключ переключения на уровень безопасности SL3)**

записываются на карту **Mifare Plus** только один раз и не могут быть изменены!!!

• Plus 4 KB

- **Номер сектора** – номер сектора, в котором находится блок для хранения номера карты, допустимые значения: 0-31;
- **Номер блока** – номер блока, в котором будет храниться номер карты, используемый в СКУД, допустимые значения:
 - 1, 2 – для сектора номер 0,
 - 0, 1, 2 – для секторов номер 1-31,
 - 0 - 14 – для секторов номер 32-39;
- **Старый тип ключа аутентификации** – отображает старый тип ключа аутентификации, допустимые значения: А, В;
- **Старый ключ аутентификации** – отображает ранее записанный ключ аутентификации, который используется при работе карт на уровне безопасности SL1 и SL2, длина 6 байт в формате *Hex*;
- **Старый ключ для уровня безопасности SL3 при типе ключа А** – отображает ключ для аутентификации на уровне SL3

- при типе ключа А, длина 16 байт в формате *Hex*;
- **Старый ключ для уровня безопасности SL3 при типе ключа В** – отображает ключ для аутентификации на уровне SL3 при типе ключа В, длина 16 байт в формате *Hex*;
- **Тип ключа аутентификации** – тип ключа аутентификации, допустимые значения: А, В;
- **Ключ аутентификации** – ключ аутентификации, который используется при работе карт на уровне безопасности SL1 и SL2, длина 6 байт в формате *Hex*;
- **Ключ для уровня безопасности SL3 при типе ключа А** – ключ для аутентификации на уровне SL3 при типе ключа А, длина 16 байт в формате *Hex*;
- **Ключ для уровня безопасности SL3 при типе ключа В** – ключ для аутентификации на уровне SL3 при типе ключа В, длина 16 байт в формате *Hex*;
- **Уровень безопасности SL** – уровень безопасности для карт серии **Mifare Plus**, допустимые значения: 1-3;

Ключи для изменения уровня безопасности (SL):

- **Мастер ключ** – ключ, длина 16 байт в формате *Hex*;
- **Конфигурационный ключ** – ключ, длина 16 байт в формате *Hex*;
- **Ключ аутентификации для уровня безопасности SL1** – ключ AES, длина 16 байт в формате *Hex*;
- **Ключ переключения на уровень безопасности SL2** – ключ, длина 16 байт в формате *Hex*;
- **Ключ переключения на уровень безопасности SL3** – ключ, длина 16 байт в формате *Hex*.

• Plus SE 1 KB

- **Номер сектора** – номер сектора, в котором находится блок для хранения номера карты, допустимые значения: 0-15;
- **Номер блока** – номер блока, в котором будет храниться номер карты, используемый в СКУД, допустимые значения:
 - 1, 2 – для сектора номер 0,
 - 0, 1, 2 – для секторов номер 1-15;
- **Старый тип ключа аутентификации** – отображает старый тип ключа аутентификации, допустимые значения: А, В;
- **Старый ключ аутентификации** – отображает ранее записанный ключ аутентификации, который используется при работе карт на уровне безопасности SL1 и SL2, длина 6 байт в формате *Hex*;
- **Старый ключ для уровня безопасности SL3 при типе ключа А** – отображает ключ для аутентификации на уровне SL3 при типе ключа А, длина 16 байт в формате *Hex*;
- **Старый ключ для уровня безопасности SL3 при типе ключа В** – отображает ключ для аутентификации на уровне SL3

- при типе ключа В, длина 16 байт в формате *Hex*;
- **Тип ключа аутентификации** – тип ключа аутентификации, допустимые значения: А, В;
- **Ключ аутентификации** – ключ аутентификации, который используется при работе карт на уровне безопасности SL1 и SL2, длина 6 байт в формате *Hex*;
- **Ключ для уровня безопасности SL3 при типе ключа А** – ключ для аутентификации на уровне SL3 при типе ключа А, длина 16 байт в формате *Hex*;
- **Ключ для уровня безопасности SL3 при типе ключа В** – ключ для аутентификации на уровне SL3 при типе ключа В, длина 16 байт в формате *Hex*;
- **Уровень безопасности SL** – уровень безопасности для карт серии **Mifare Plus**, допустимые значения: 1-3;

Ключи для изменения уровня безопасности (SL):

- **Мастер ключ** – ключ, длина 16 байт в формате *Hex*;
- **Конфигурационный ключ** – ключ, длина 16 байт в формате *Hex*;
- **Ключ аутентификации для уровня безопасности SL1** – ключ AES, длина 16 байт в формате *Hex*;
- **Ключ переключения на уровень безопасности SL2** – ключ, длина 16 байт в формате *Hex*;
- **Ключ переключения на уровень безопасности SL3** – ключ, длина 16 байт в формате *Hex*.

Примечание:

- **Номер сектора** – номер части внутренней области памяти карты, которая содержит в себе несколько блоков данных для хранения информации.
- **Номер блока** – номер минимальная часть памяти карты. Блоки данных доступны для чтения/записи при условии успешной авторизации по ключу.
- **SL (secure level)** – уровень безопасности, уровень защиты. Карты **Mifare Plus** поддерживают 3 уровня безопасности:
 - **Уровень безопасности 0, или начальный уровень.** На этом уровне карты **Mifare Plus** находятся до ввода в эксплуатацию. С SL0 карта переводится на требуемый уровень безопасности;
 - **Уровень безопасности 1.** На этом уровне карты **Mifare Plus** имеют полную совместимость с картами **Mifare Classic 1K, Mifare Classic 4K** и могут работать в рамках однойСКУД;
 - **Уровень безопасности 2.** Аутентификация по крипто-алгоритму **AES** является обязательной. Для защиты данных используется крипто-алгоритм **CRYPTO1**;
 - **Уровень безопасности 3.** Для аутентификации, обмена и шифрования данных, для работы с памятью используется крипто-алгоритм **AES**.

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

Параметры, отображающиеся для выбранного типа карты **Mifare DESFire**:

Примечание:

Карты **Mifare DESFire**, в отличие от остальных типов карт, используются как в качестве простых карт, так и в качестве мастер-карт. Простая карта типа **DESFire** может быть записана в качестве дополнительной мастер-карты для СКУД. Перезапись мастер-карты **DESFire** с целью перевода её в состояние простой карты невозможна! (Т.е. – карта типа **DESFire**, однажды записанная как мастер-карта, останется в этом состоянии даже после перезаписи.)

• **DESFire Ev1**

- **Старый номер приложения** – отображает старый номер приложения, в котором хранится номер карты, используемый в СКУД, длина 3 байта в формате *Hex*;
- **Старый тип ключа карты** – отображает старый тип ключа карты, допустимые значения:
 - AES (AES 128 Key [16 Bytes]) – тип ключа, использующий симметричный алгоритм блочного шифрования, длина ключа 16 байт;
 - 2K3DES (2 Key Triple Des [16 Bytes]) – тип ключа, использующий симметричный алгоритм блочного шифрования, использует трехкратное шифрование двумя ключами, длина ключа 16 байт;
 - 3K3DES (3 Key Triple Des [24 Bytes]) – тип ключа, использующий симметричный алгоритм блочного шифрования, использует трехкратное шифрование тремя ключами, длина ключа 24 байт.
- **Старый ключ карты** – отображает старый ключ карты, длина зависит от типа ключа:
 - AES – длина ключа 16 байт в формате *Hex*;
 - 2K3DES – длина ключа 16 байт в формате *Hex*;
 - 3K3DES – длина ключа 24 байт в формате *Hex*.
- **Старый тип ключа приложения** – отображает старый тип ключа приложения, варианты:
 - AES (AES 128 Key [16 Bytes]) – тип приложения, использующий симметричный алгоритм блочного шифрования, длина ключа 16 байт;
 - 2K3DES (2 Key Triple Des [16 Bytes]) – тип приложения,

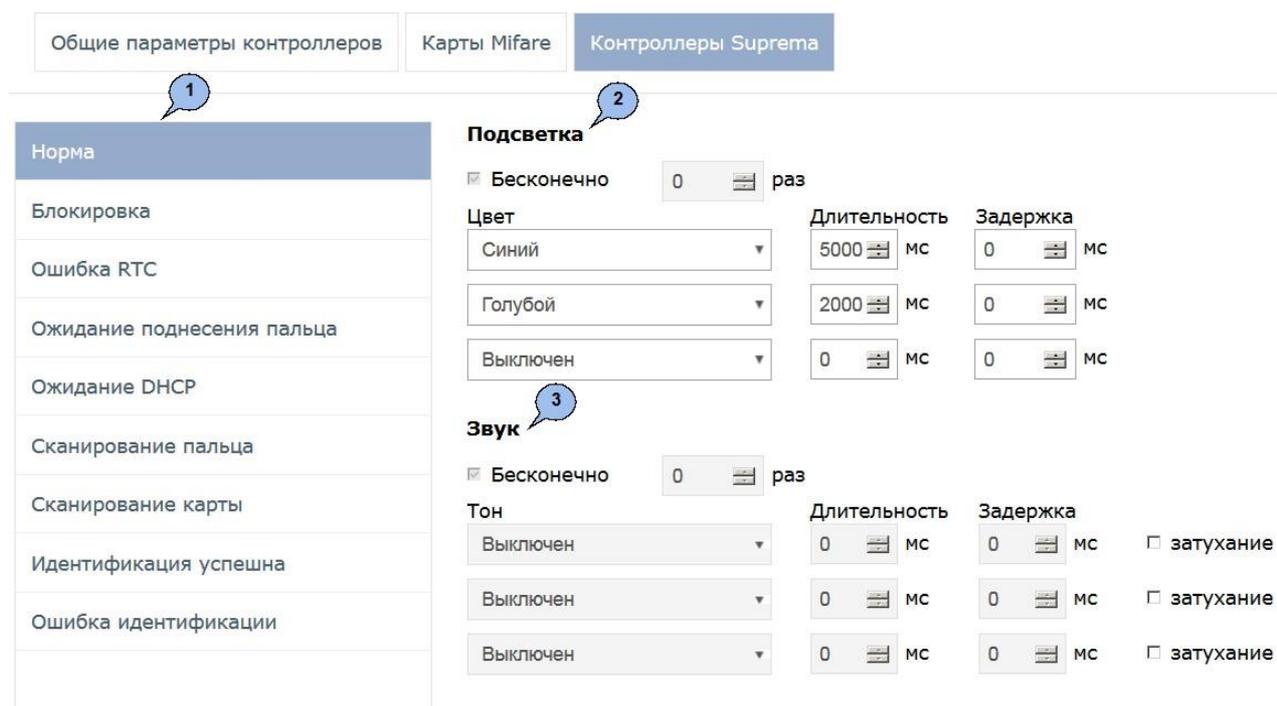
- использующий симметричный алгоритм блочного шифрования, использует троекратное шифрование двумя ключами, длина ключа 16 байт;
- 3K3DES (3 Key Triple Des [24 Bytes]) – тип приложения, использующий симметричный алгоритм блочного шифрования, использует троекратное шифрование тремя ключами, длина ключа 24 байт.
- **Старый ключ приложения** – отображает старый ключ приложения, длина зависит от типа ключа:
 - AES – длина ключа 16 байт в формате Hex;
 - 2K3DES – длина ключа 16 байт в формате Hex;
 - 3K3DES – длина ключа 24 байт в формате Hex.
 - **Номер приложения** – номер приложения, в котором будет храниться номер карты, используемый в СКУД длиной 3 байта в формате Hex;
 - **Тип ключа карты** – тип ключа карты, варианты:
 - AES (AES 128 Key [16 Bytes]) – тип ключа, использующий симметричный алгоритм блочного шифрования, длина ключа 16 байт;
 - 2K3DES (2 Key Triple Des [16 Bytes]) – тип ключа, использующий симметричный алгоритм блочного шифрования, использует троекратное шифрование двумя ключами, длина ключа 16 байт;
 - 3K3DES (3 Key Triple Des [24 Bytes]) – тип ключа, использующий симметричный алгоритм блочного шифрования, использует троекратное шифрование тремя ключами, длина ключа 24 байт.
 - **Ключ карты** – ключ карты, длина зависит от типа ключа:
 - AES – длина ключа 16 байт в формате Hex;
 - 2K3DES – длина ключа 16 байт в формате Hex;
 - 3K3DES – длина ключа 24 байт в формате Hex.
 - **Тип ключа приложения** – тип ключа приложения, варианты:
 - AES (AES 128 Key [16 Bytes]) – тип приложения, использующий симметричный алгоритм блочного шифрования, длина ключа 16 байт;
 - 2K3DES (2 Key Triple Des [16 Bytes]) – тип приложения, использующий симметричный алгоритм блочного шифрования, использует троекратное шифрование двумя ключами, длина ключа 16 байт;

- 3K3DES (3 Key Triple Des [24 Bytes]) – тип приложения, использующий симметричный алгоритм блочного шифрования, использует троекратное шифрование тремя ключами, длина ключа 24 байт.
- **Ключ приложения** – ключ приложения, длина зависит от типа ключа:
 - AES – длина ключа 16 байт в формате Hex;
 - 2K3DES – длина ключа 16 байт в формате Hex;
 - 3K3DES – длина ключа 24 байт в формате Hex.

Примечание:

- **Номер приложения** – номер файла памяти, расположенного во внутренней области памяти карты, в который записывается информация;

Вкладка **Контроллеры Suprema** позволяет настроить цветовую индикацию и звуковые сигналы контроллера для представленного списка событий:



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 "**Закр**то");
- **Ошибка RTC** (Real Time Clock) – событие возникает в случае не совпадения 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;
- **... раз** – счётчик позволяет задать количество повторений подсветки;

Примечание:

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

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

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

- **Бесконечно** – при установке флажка звук будет воспроизводиться бесконечно;
- **... раз** – счётчик позволяет задать количество повторений звучания;

Примечание:

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

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

Для того, чтобы сохранить изменения индикации, нажмите на кнопку

Сохранить, в противном случае на кнопку .

Окно «Свойства контроллера»

Окно **Свойства контроллера** имеет следующий вид:

1. **Имя контроллера** – поле для ввода описательного названия контроллера.

2. Инструменты для указания или изменения помещений, доступ между которыми обеспечивается контроллером.

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

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

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

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

4. Параметры, доступные для данного ресурса.

5. Возможные значение и варианты настройки выделенного параметра ресурса.

6. Кнопки **команд управления**, доступных для выбранного ресурса. Для оперативного управления устройствами предназначен подраздел **«Управление устройствами»** раздела **«Контроль доступа»**.

7. Кнопка **Сохранить**, **Сохранить и закрыть** и раскрывающийся список способа сохранения изменений при нажатии:

- **Только в базу данных** – параметры сохраняются только в БД системы и впоследствии должны быть переданы в контроллер(ы).
- **Все в контроллер(ы)** – в контроллер(ы) передаются все параметры.
- **Измененные в контроллер(ы)** – в контроллер(ы) передаются только измененные параметры.

Создание списка коммиссионированных карт

Примечание:

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

Для создания списка коммисионирующих карт контроллера:

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

Генератор тревоги	Турникет	Считыватель 1	Считыватель 2	Список коммисионирующих карт
+ -				
Сотрудник	Подразделение	Идентификатор карты		
Бестужева Нина Аркадьевна	Бухгалтерия	4349726234		
Ермолаев Вадим Петрович	Отдел продаж	197571970647		

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

Персонал ✕

🔍
 ☰ ✕

Архипов Максим Юрьевич [ОКС]

Ахрамович Инесса Григорьевна [ДТК]

Бабушкина Юлия Дмитриевна [ДЗП]

Барабанов Александр Олегович [ДМТО]

Басов Андрей Григорьевич [Склад КиМ]

Бахменд Альберт Борисович [ОКС]

Белоусов Игорь Иванович [АСУ]

Белоусов Олег Владиславович [ДАС]

Богданова Ольга Владимировна [ГФБУ]

↑
↓

Ок

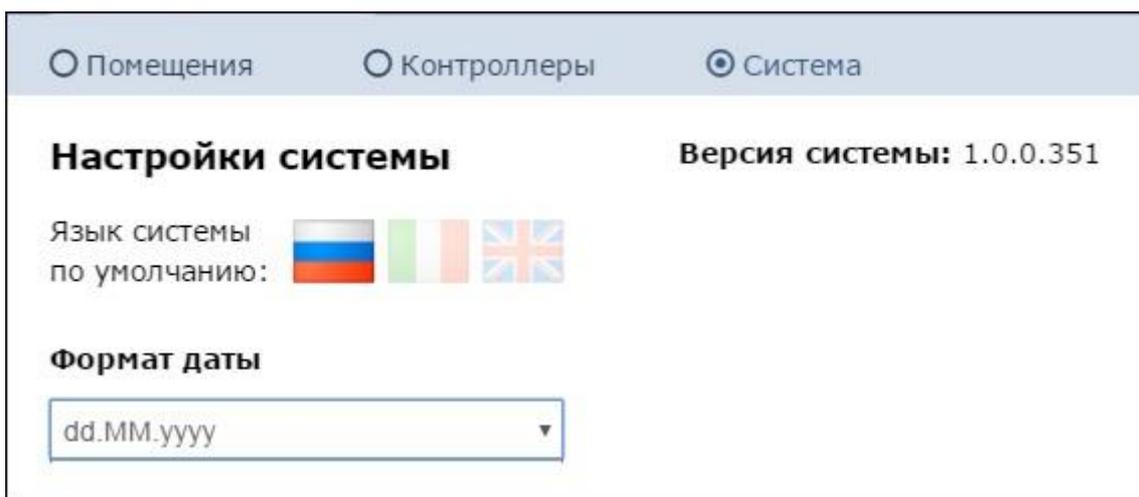
8. В открывшемся окне, используя стандартные средства **Поиск** и **Выбрать подразделение**, выделите одного или несколько сотрудников карты доступа, выданные которым, будут являться коммисионирующими для данного контроллера.
9. Нажмите кнопку **Ок**. Окно **Персонал** будет закрыто, номера карт отмеченных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

Примечание:

При работе с контроллерами второй версии (**PERCo-CT/L04.2**, **PERCo-CR01.2 LICON**, **PERCo-CL05.2**) после добавления коммисионирующих карт для сохранения изменений необходимо передать новую конфигурацию в контроллеры.

13.1.3 Вкладка «Система»

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



13.2 Подраздел «События системы»

Подраздел предназначен для:

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

Страница подраздела имеет следующий вид:

Дата события	Событие	IP-адрес	Ресурс устройства
2015-01-19 11:	Редактирование контроллера		
2014-11-21 09:	Объект контроллер создан	10.0.1.54	
2014-11-21 09:	Объект контроллер создан	10.0.82.204	
2014-11-21 10:	Включение питания контроллера	10.0.82.204	Причина сброса 3
2014-11-21 10:	Восстановление ИП: При условии, что напряжение питания в рабочем	10.0.82.204	
2014-11-21 10:	Несанкционированный проход через ИУ (взлом ИУ)	10.0.82.204	Считыватель 2
2014-11-21 10:	Восстановление связи	10.0.82.204	

• Пользователь [root (Самый главный)] произвел действия в разделе [Администрирование, Конфигурация].
 • Изменено значение: `Вход [Сч. 1]`. Было [], Стало [Бухгалтерия предприятия].
 • Изменено значение: `Выход [Сч. 2]`. Было [], Стало [Неконтролируемая территория].

1. Панели инструментов подраздела содержит:



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

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



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



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



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



Применить – кнопка позволяет сформировать список событий за указанный период.

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

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

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

Примечания:

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

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

13.3 Подраздел «Задания»

Вкладка предназначена для [создания заданий](#), автоматически выполняемых сервером системы. Доступны задания следующих типов:

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

Внимание!

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

- к отключению резервного копирования базы данных,
- к увеличению продолжительности расчета отчетов по учету рабочего времени.

Страница подраздела имеет следующий вид:

Когда выполнять ↓	Начало	Окончание	Задание	Дата выполнения	Статус выполнения
ПН ВТ СР ЧТ ПТ СБ ВС	09:00:00	10:00:00	Резервное копирование базы данных		
ПН ВТ СР ЧТ ПТ СБ ВС	09:30:00	10:00:00	Учет рабочего времени		

1. Панель инструментов страницы содержит:



Добавить – кнопка позволяет добавить новое задание.



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



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

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

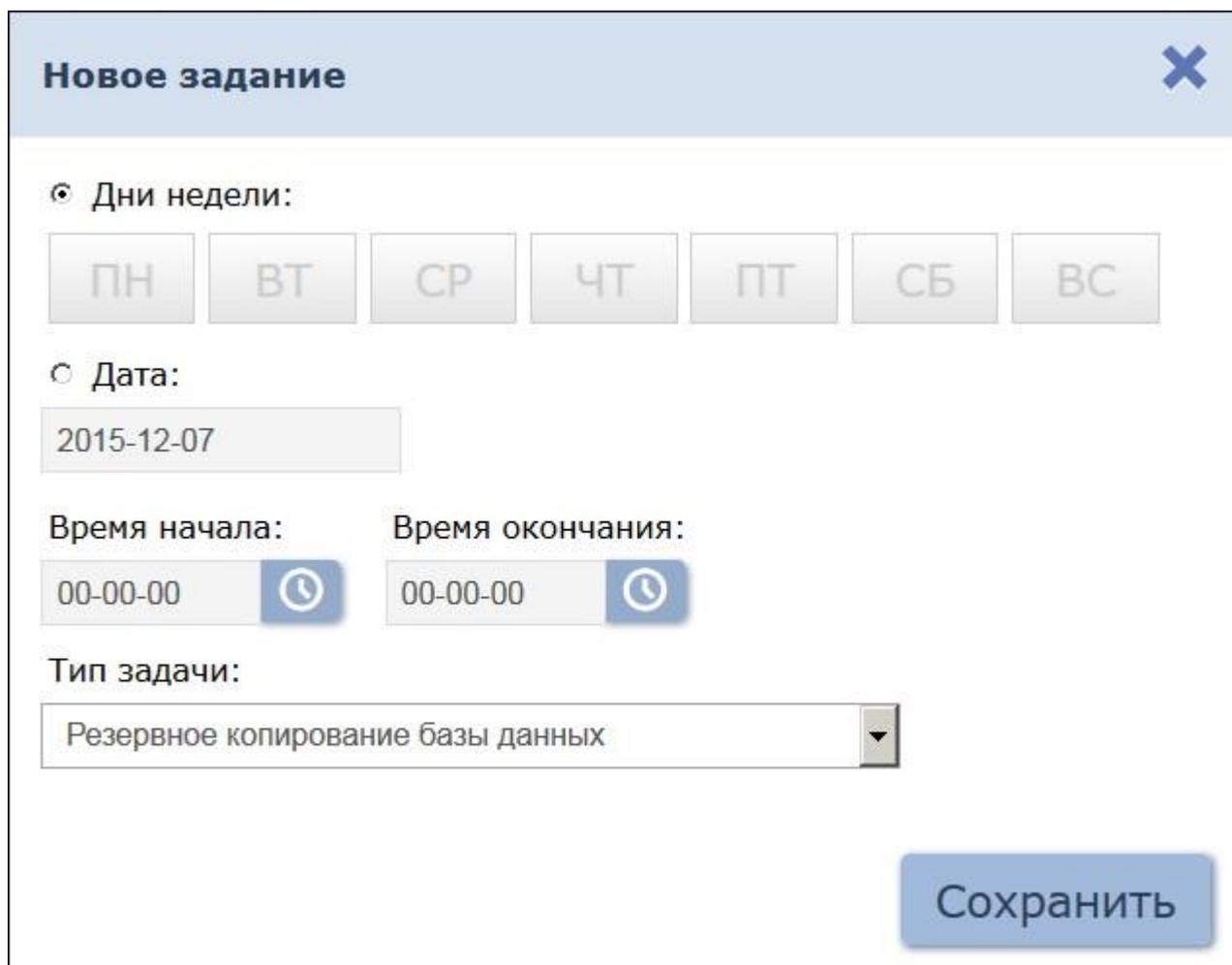
Примечание:

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

13.3.1 Создание нового задания

Для создания нового задания сервера системы:

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



Новое задание 

Дни недели:

Дата:

2015-12-07

Время начала:  Время окончания: 

Тип задачи:

Резервное копирование базы данных 

4. С помощью раскрывающегося списка **Тип задания** выберите тип нового задания:
 - **Резервное копирование базы данных**
 - **Учет рабочего времени за предыдущий день**
5. В открывшемся окне с помощью переключателя выберите

периодичность выполнения задания:

- **Дни недели** – если задание необходимо выполнять еженедельно. С помощью соответствующих кнопок укажите дни недели, в которые будет запускаться задание.
- **Дата** – если задание необходимо выполнить один раз. С помощью календаря укажите дату запуска задания.

Примечание:

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

6. С помощью полей ввода **Время начала** и **Время окончания** укажите период времени в течение суток, в который задание необходимо запустить.
7. После указания всех параметров задания нажмите кнопку **ОК**. Окно **Задание** будет закрыто. Новое задание появится в рабочей области страницы.

13.4 Подраздел «Операторы»

Примечание:

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

Подраздел предназначен для:

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

Страница подраздела имеет следующий вид:

Логин	Имя	Роль	Блок	Контроллер	Описание
Admin		АРМ			Администратор системы
Office manager	Юлия Петрова	АРМ			
Sales 1	Александр Иванов	Охрана		Контроллер замка	
Sales 2	Сергей Есенин	Отдел продаж	🔒		
Tester	Антон Алексеев	АРМ		Контроллер замка	Тестирующий
root	Самый главный				Предопределённый пользователь

1. Панель инструментов страницы:



Добавить – кнопка позволяет добавить нового оператора.



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



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



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



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

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

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

Примечание:

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

13.4.1 Добавление оператора системы

Примечание:

Перед добавлением операторов создайте в подразделе [«Права операторов»](#) раздела **«Администрирование»** необходимые роли операторов и выдайте им полномочия.

Для добавления нового оператора:

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

Добавление оператора ✕

Логин:

Пароль:

Пароль должен быть длиннее 6 символов и содержать хотя бы одну букву латинского алфавита и хотя бы одну цифру.

Подтверждение:

Роль:

Имя:

Описание:

Разделы

- Персонал
- Бюро пропусков
- Учёт рабочего времени
- Контроль доступа
- Верификация
- Заказ пропуска
- Администрирование

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

Добавление оператора ✕

Логин:

Пароль:

Пароль должен быть длиннее 6 символов и содержать хотя бы одну букву латинского алфавита и хотя бы одну цифру.

Подтверждение:

Роль:

Имя:

Описание:

Разделы

- Персонал
- Бюро пропусков
 - Посетители
 - Сотрудники
 - Шаблоны доступа
 - Дизайн пропуска
 - Отчет по посетителям
- Учёт рабочего времени
- Контроль доступа
- Верификация
- Заказ пропуска
- Администрирование

7. На панели **Доступ к разделам** установите флажки у разделов, подразделов и вкладок подразделов, доступ к которым будет разрешен оператору.

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 выдаче 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.

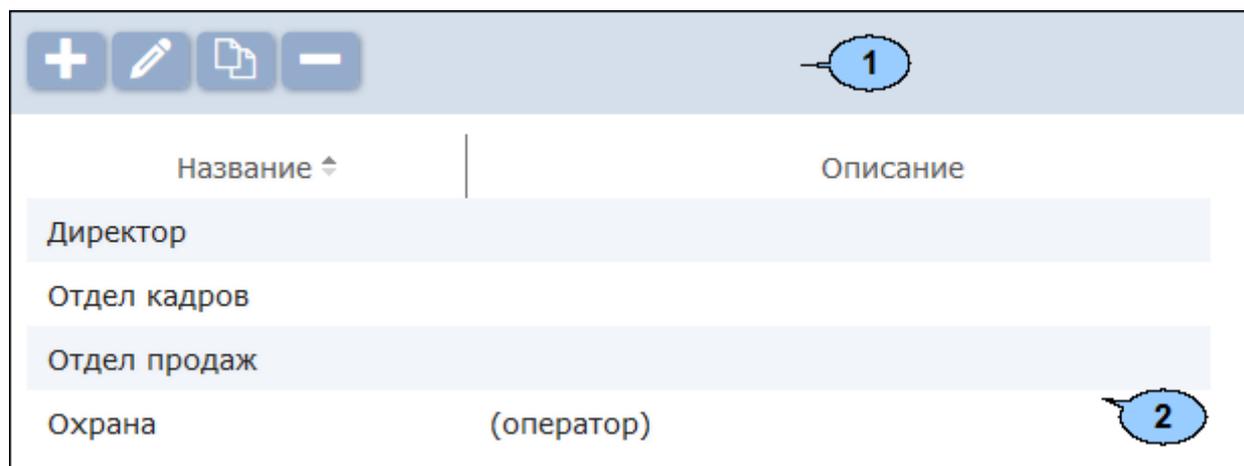
8. Нажмите кнопку **Сохранить**. Окно **Добавление оператора** будет закрыто. Новый оператор будет добавлен в список в рабочей области страницы.

13.5 Подраздел «Роли и права операторов»

Подраздел предназначен для:

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

Страница подраздела имеет следующий вид:



1. Панель инструментов страницы:



Добавить – кнопка позволяет добавить новую роль оператора.



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



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



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

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

Примечание:

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

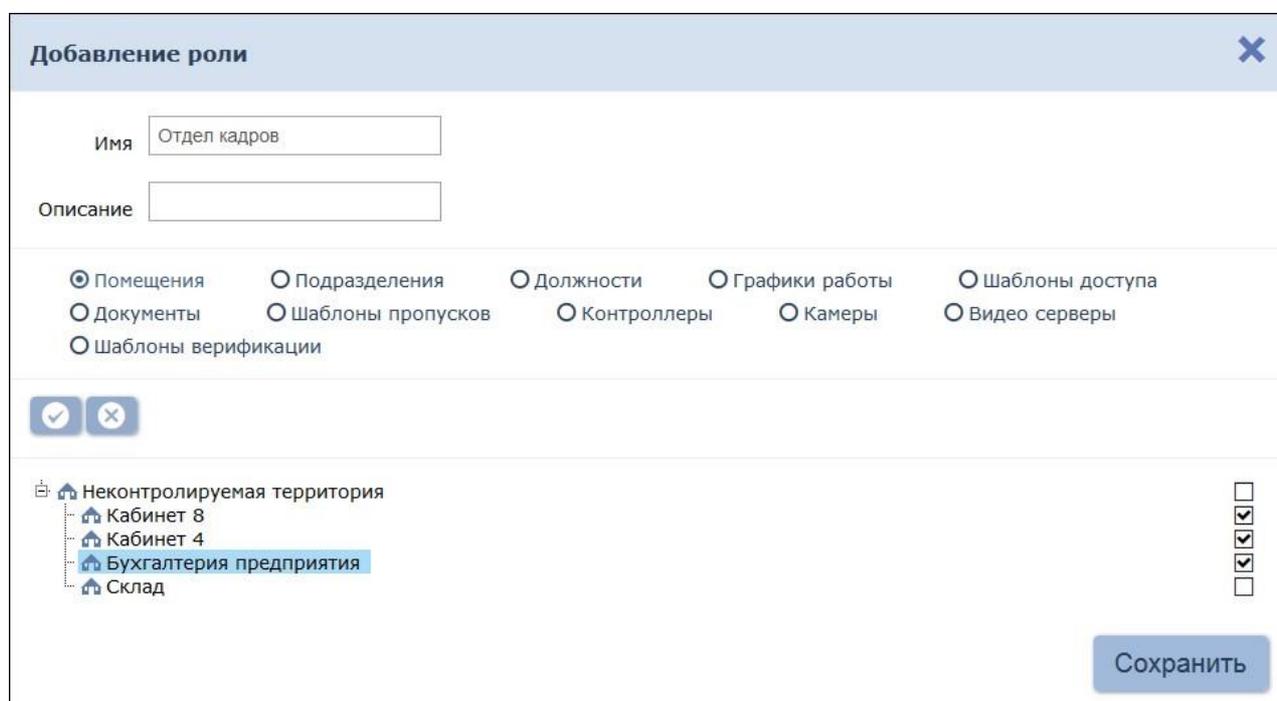
13.5.1 Добавление роли оператора (набора полномочий)

Для добавления новой роли оператора:

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

2. Откройте подраздел «Роли и права операторов».

3. Нажмите на панели инструментов вкладки кнопку **Добавить** . Откроется окно **Добавление роли**:



4. В открывшемся окне в поле **Имя** введите название роли, в поле **Описание** при необходимости введите дополнительную информацию о роли.

5. Выдайте полномочия созданной роли. Для этого с помощью переключателя выберите тип полномочий. При этом в рабочей области страницы появится список объектов данного типа, доступных в системе. Доступны следующие типы полномочий:

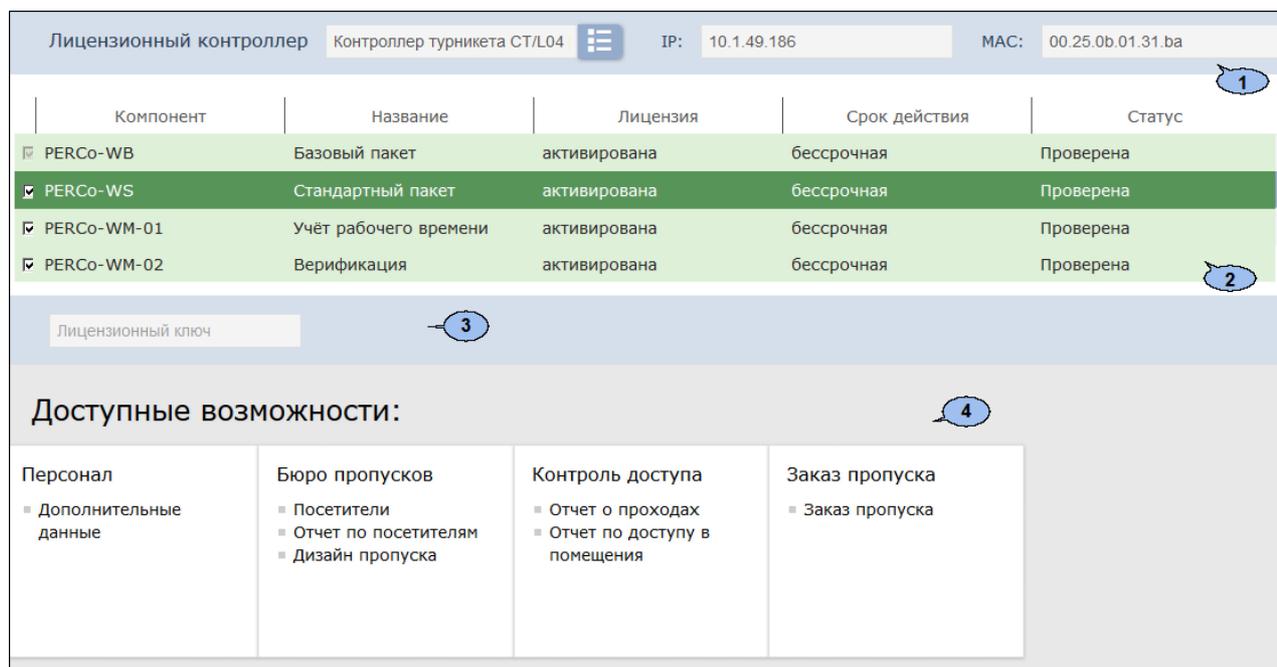
- Помещения
- Подразделения
- Должности
- Графики работы
- Шаблоны доступа
- Шаблоны верификации
- Шаблоны пропусков

- Контроллеры
- Камеры
- Видеосерверы

- Установите флажки у тех объектов, полномочия на которые должны быть доступны для созданной роли оператора. При необходимости используйте кнопки **Выделить все**  и **Снять выделение** .
- С помощью переключателя выберите другой тип объектов и выдайте на них полномочия.
- Нажмите кнопку **Сохранить**. Окно **Добавление роли** будет закрыто. Новая роль будет добавлена в список в рабочей области страницы.
- Для добавления нового оператора системы откройте подраздел «[Операторы](#)».

13.6 Подраздел «Лицензии»

Подраздел предназначен для [ввода кодов активации](#) установленных модулей ПО системы. Страница подраздела имеет следующий вид:



Компонент	Название	Лицензия	Срок действия	Статус
<input type="checkbox"/> PERCo-WB	Базовый пакет	активирована	бессрочная	Проверена
<input checked="" type="checkbox"/> PERCo-WS	Стандартный пакет	активирована	бессрочная	Проверена
<input checked="" type="checkbox"/> PERCo-WM-01	Учёт рабочего времени	активирована	бессрочная	Проверена
<input checked="" type="checkbox"/> PERCo-WM-02	Верификация	активирована	бессрочная	Проверена

Лицензионный ключ

Доступные возможности:

Персонал <input type="checkbox"/> Дополнительные данные	Бюро пропусков <input type="checkbox"/> Посетители <input type="checkbox"/> Отчет по посетителям <input type="checkbox"/> Дизайн пропуска	Контроль доступа <input type="checkbox"/> Отчет о проходах <input type="checkbox"/> Отчет по доступу в помещения	Заказ пропуска <input type="checkbox"/> Заказ пропуска
---	---	---	--

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

Примечание:

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

3. Поле **Лицензионный ключ** для ввода кода активации. Панель открывается после выбора в рабочей области страницы одного из модулей.
4. Панель **Доступные возможности** содержит список разделов и подразделов системы, доступных для выбранного в рабочей области страницы модуля.

13.6.1 Ввод кода активации

Для ввода кодов активации модулей ПО системы:

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

Примечание:

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

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

Выберите лицензионный контроллер ✕

IP ↕	Название	Вход	Выход
10.0.201.232	Контроллер турникета СТ/L04 [1+8]		

Выбрать

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

9. В случае ошибки при вводе кода активации, несоответствии кода выбранному модулю или контроллеру, нарушении связи с контроллером откроется окно с соответствующим предупреждением.

14 Параметры контроллера PERCo

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

- **Внешние подключения** – вкладка с информацией о внешних подключениях контроллера;
- [Генератор тревоги](#);
- [Дополнительные входы](#);
- [Дополнительные выходы](#);
- [Дополнительный вывод](#);
- [Замок CL-05](#);
- [ИУ](#) (Замок, Турникет);
- [Общие](#);
- [Свойства ЛИКОНА и Строки](#);
- **Состояние** – вкладка с информацией о состоянии контроллера;
- [Список коммиссионированных карт](#);
- [Считыватель](#).

14.1 Вкладка «Общие»

Вкладка содержит две подвкладки:

- [Разное](#);
- [Сеть](#).

14.1.1 Подвкладка «Сеть»

Подвкладка отображает информацию о следующих сетевых параметрах:

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

Сеть	Сеть
Разное	IP-адрес <input type="text" value="172.17.100.200"/>
	Маска подсети <input type="text" value="255.0.0.0"/>
	IP-адрес шлюза <input type="text"/>
	MAC-адрес <input type="text"/>

14.1.2 Подкладка «Разное»

Подкладка содержит следующие настройки:

Сеть	Разное
Разное	Версия прошивки <input type="text"/>

- **Версия прошивки** – в поле отображается версия прошивки встроенного ПО контроллера.

14.2 Вкладка ИУ («Замок», «Турникет»)

Прямое направление прохода. Параметр позволяет указать, в направлении какого из считывателей проход считается входом.

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

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

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

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

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

Время удержания в разблокированном состоянии (Время анализа идентификатора). Время, на которое разблокируется ИУ при разрешении доступа.

Время ожидания комиссионирования. Параметр позволяет ограничить интервал времени между предъявлением идентификатора пользователя (сотрудника / посетителя / служебного ТС) и комиссионующей 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 разрешения** значение отличное от **Нет**, то есть запрещено проведение процедуры верификации от ПДУ;
- проводить процедуру верификации из ПО.

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

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

Внутренняя защита от передачи идентификаторов (Local Antipass). При установленном параметра 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»).

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

14.3 Вкладка «Замок CL05»

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

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

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

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

Время удержания в разблокированном состоянии (Время анализа идентификатора). Время, на которое разблокируется ИУ при разрешении доступа.

Время ожидания комиссионирования. Параметр позволяет ограничить интервал времени между предъявлением идентификатора пользователя (сотрудника / посетителя / служебного ТС) и комиссионированием 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 разрешения** значение отличное от **Нет**, то есть запрещено проведение процедуры верификации от ПДУ;
- проводить процедуру верификации из ПО.

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

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

Внутренняя защита от передачи идентификаторов (Local Antipass). При установленном параметра 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. При установленном флажке в случае прохода через ИУ регистрируется переход из одной пространственной зоны контроля в другую.

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

14.4 Вкладки «Свойства ЛИКОНА» и «Строки»

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

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

Примечание:

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

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

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

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

14.5 Вкладка «Дополнительные входы»

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

Тип. Раскрывающийся список позволяет выбрать один из следующих типов:

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

Примечание:

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

В зависимости от выбранного типа остальные параметры выхода могут различаться.

Обычный

Временной Критерий маскирования/активизации/ нормализации:

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

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

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

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

Специальный

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

Подтверждение от ВВУ/Запрет от ВВУ

Номер ИУ. Параметр задаёт номер ИУ, к которому привязывается считыватель.

14.6 Вкладка «Дополнительные выходы»

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

Примечание:

После включения питания все выходы нормализуются.

Тип. Раскрывающийся список позволяет выбрать следующие типы выхода:

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

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

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

14.7 Вкладка «Дополнительный вывод»

Тип. Раскрывающийся список позволяет выбрать один из следующих типов:

- **Нет.** К данному входу не подключено никакое внешнее оборудование.
- **Обычный.** К данному входу подключено внешнее оборудование, состояние которого должно отслеживаться контроллером. Можно указать алгоритм действий контроллера при получении управляющего сигнала от подключенного оборудования.
- **Генератор тревоги.** Решение об активизации дополнительного выхода принимается в соответствии с параметрами, заданными для ресурса **Генератор тревоги**.
- **FireAlarm.** Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ Fire Alarm.

- **Синхронизирующий вход/выход.** Вывод используется для синхронизации совместной работы двух контроллеров при организации КПП с контролем проходов в двух направлениях. В этом режиме выводы контроллеров соединяются друг с другом.

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

14.8 Вкладка «Генератор тревоги»

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

Генерация тревоги при предъявлении идентификатора. Параметр позволяет указать события, связанные с предъявлением идентификаторов, при регистрации которых произойдет генерация тревоги. 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.

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

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

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

14.9 Вкладка «Считыватель»

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

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

- **Нет.** Контроллер не учитывает зональность номера карты для разрешения доступа.
- **Мягкая.** Контроллер разрешит доступ по карте, при этом регистрируется событие мониторинга *«Предъявление идентификатора, нарушение зональности»*, после совершения прохода регистрируется событие *«Проход по карте с несоответствием текущему местоположению»*.
- **Жесткая.** Контроллер запретит доступ по карте, при этом регистрируется событие мониторинга *«Предъявление карты с нарушением зональности»* и регистрируется событие *«Запрет прохода по причине нарушения зональности»*. Если 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.

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

Временной критерий маскирования:

- **На указанное время.** Выбранные дополнительные входы будут маскированы на указанное время.
- **На время срабатывания.** Выбранные дополнительные входы будут

маскированы на протяжении всего времени, пока ИУ будет разблокировано.

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

Дополнительные выходы, активизируемые при разблокировке ИУ.

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

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

Временной критерий активизации/нормализации:

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

Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ.

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

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

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

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

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

Примечание:

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

- **ПДУ.** Для настройки картоприемника и верификации от ПДУ или ПО. Имеется возможность настроить запуск процедуры верификации при предъявлении карт доступа независимо для сотрудников и посетителей.
- **Софт.** Для верификации от оператора с помощью раздела ПО «**Верификация**».
- **ВВУ.** Для верификации от алкотестера (алкометра) или другого оборудования. Имеется возможность настроить запуск процедуры верификации при предъявлении карт доступа независимо для сотрудников и посетителей.
- **При доступности Софт, иначе ПДУ;**
- **ПДУ или Софт;**
- **Сначала ПДУ, затем Софт;**
- **Сначала ВВУ, затем ПДУ;**
- **Сначала ВВУ, затем софт;**
- **При доступности софт, иначе ВВУ.**

Верифицировать идентификаторы СОТРУДНИКОВ/ПОСЕТИТЕЛЕЙ от ПДУ/ВВУ – имеется возможность гибко настроить условия проведения верификации независимо для карт доступа сотрудников и посетителей в следующих случаях:

- **при проходе** – верификация проводится при каждой попытке прохода;
- **при проходе с НАРУШЕНИЕМ ВРЕМЕНИ** – верификация проводится при попытке прохода в случае нарушения времени (параметр **Контроль времени для идентификаторов** должен быть установлен на значение **Жесткий**).
- **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ** – верификация проводится в случае попытке повторного входа без предварительного выхода (параметр **Защита от передачи идентификаторов** должен быть установлен на значение **Жесткая**).

Время ожидания подтверждения при верификации от ПДУ/ ВВУ.

Параметр позволяет установить время, в течение которого контроллер ожидает подтверждение запроса от верифицирующего устройства или пульта дистанционного управления.

При отсутствии ответа от ВВУ. Параметр позволяет выбрать событие, регистрируемое в случае отсутствия подтверждения прохода от ВВУ:

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

Примечание:

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

15 Параметры контроллера Suprema

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

- [Общие](#);
- [Замок](#);
- [Считыватель](#).

Общие настройки световой и звуковой индикации для всех подключенных к системе контроллеров **Suprema** задаются на вкладке [Контроллеры Suprema](#).

15.1 Вкладка «Общие»

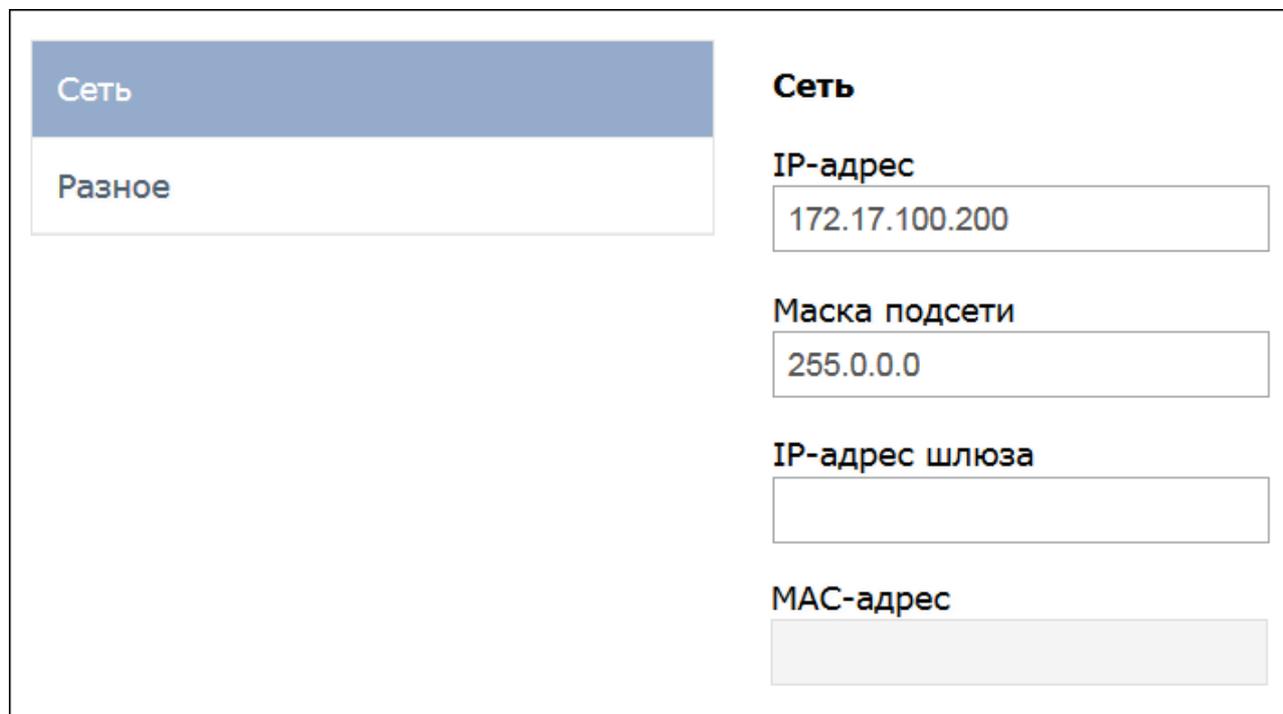
Вкладка содержит две подвкладки:

- «[Сеть](#)»;
- «[Разное](#)».

15.1.1 Подвкладка «Сеть»

Подвкладка отображает информацию о следующих сетевых параметрах:

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



Сеть	Сеть
Разное	IP-адрес 172.17.100.200
	Маска подсети 255.0.0.0
	IP-адрес шлюза <input type="text"/>
	MAC-адрес <input type="text"/>

15.1.2 Подкладка «Разное»

Подкладка содержит следующие настройки:

- **Версия прошивки** – в поле отображается версия прошивки встроенного ПО контроллера.

15.2 Вкладка «Замок»

Вкладка «**Замок**» 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.**

- **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.

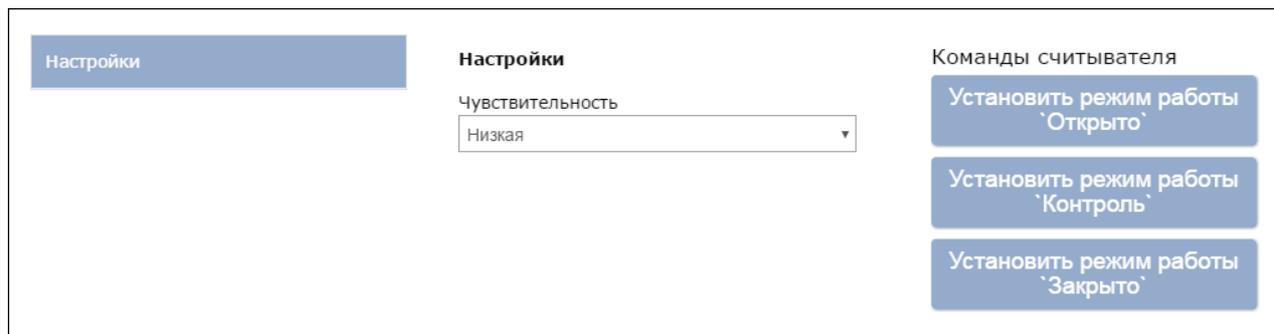
- **Предельное время открытия двери** – время, по истечении которого контроллер управления доступом перейдет в состояние тревоги по причине того, что дверь не была закрыта и заблокирована. Раскрывающийся список позволяет задать значение и выбрать единицы измерения предельного времени открытия двери:
 - **Миллисекунды**;
 - **Секунды**;
 - **Бесконечность**.
- **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 **Блокировать дверь после закрытия** дверь будет заблокирована сразу после закрытия.

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.

15.3 Вкладка «Считыватель»

Вкладка «Считыватель» содержит следующие настройки:



The screenshot displays the 'Настройки' (Settings) interface for the reader. On the left, there is a blue header 'Настройки'. The main area is titled 'Настройки' and contains a dropdown menu for 'Чувствительность' (Sensitivity) with 'Низкая' (Low) selected. To the right, under the heading 'Команды считывателя' (Reader Commands), there are three blue buttons: 'Установить режим работы "Открыто"' (Set mode 'Open'), 'Установить режим работы "Контроль"' (Set mode 'Control'), and 'Установить режим работы "Закрыто"' (Set mode 'Closed').

- **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, освещённости 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.

Поддерживаются следующие команды считывателя:

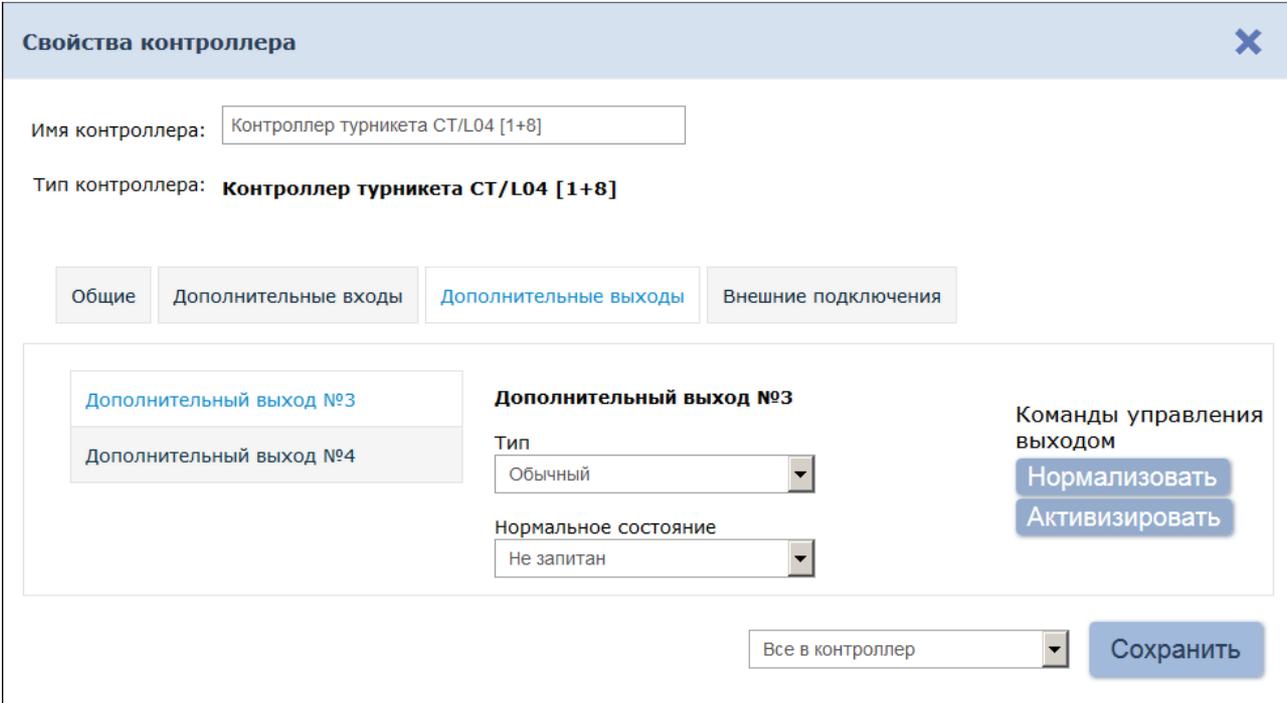
- **Установить режим работы "Открыто"** – при переходе в режим работы **"Открыто"** происходит разблокировка исполнительного устройства, проход осуществляется свободно без предъявления карт доступа и/или сканирования отпечатков пальцев;
- **Установить режим работы "Контроль"** – в режиме работы **"Контроль"** проход осуществляется в нормальном режиме по предъявлении карт доступа и/или сканированию отпечатков пальцев;

- **Установить режим работы "Закрото"** – в режиме работы **"Закрото"** происходит блокировка исполнительного устройства, проход блокируется, считыватель не реагирует на предъявление карт доступа и/или сканирование отпечатков пальцев.

16 Пример конфигурирования картоприемника

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

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



Свойства контроллера

Имя контроллера:

Тип контроллера: **Контроллер турникета СТ/L04 [1+8]**

Общие Дополнительные входы **Дополнительные выходы** Внешние подключения

Дополнительный выход №3

Дополнительный выход №4

Дополнительный выход №3

Тип: Обычный

Нормальное состояние: Не запитан

Команды управления выходом

Нормализовать

Активизировать

Все в контроллер

Сохранить

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

Свойства контроллера ✕

Имя контроллера:

Тип контроллера: **Контроллер турникета СТ/L04 [1+8]**

Общие
Дополнительные входы
Дополнительные выходы
Внешние подключения

Дополнительный вход №1

Дополнительный вход №1

Тип

Нормальное состояние контакта

Дополнительные входы, маскируемые при активизации

Критерий маскирования

Дополнительный вход №2

Дополнительный вход №2

Сохранить

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

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

17 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**.

Замок

Поставить на охрану – ИУ будет переведено в РКД «Охрана».

Снять с охраны – ИУ будет снято из РКД «Охрана» в предыдущий РКД.

Сбросить 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.

Закреть (заблокировать) ИУ – ИУ в направлении считывателя будет заблокировано. Команда доступна при установленном РҚД «Контроль» и предназначена для блокировки ИУ после выполнения команды **Открыть (разблокировать) ИУ**.

18 Коды документов для «Табеля учета рабочего времени»

Условные обозначения (коды) документов, используемые при заполнении «Табеля учета рабочего времени» в форме № Т-12

Наименование документа	Буквенный код	Цифровой код
Продолжительность работы в дневное время	Я	01
Продолжительность работы в ночное время	Н	02
Продолжительность работы в выходные и нерабочие, праздничные дни	РВ	03
Продолжительность сверхурочной работы	С	04
Продолжительность работы вахтовым методом	ВМ	05
Служебная командировка	К	06
Повышение квалификации с отрывом от работы	ПК	07
Повышение квалификации с отрывом от работы в другой местности	ПМ	08
Ежегодный основной оплачиваемый отпуск	ОТ	09
Ежегодный дополнительный оплачиваемый отпуск	ОД	10
Дополнительный отпуск в связи с обучением с сохранением среднего заработка работникам, совмещающим работу с обучением	У	11
Сокращенная продолжительность рабочего времени для обучающихся без отрыва от производства с частичным сохранением заработной платы	УВ	12
Дополнительный отпуск, в связи с обучением без сохранения заработной платы	УД	13
Отпуск по беременности и родам (отпуск в связи с усыновлением новорожденного ребенка)	Р	14
Отпуск по уходу за ребенком до достижения им возраста трех лет	ОЖ	15
Отпуск без сохранения заработной платы, предоставленный работнику по разрешению работодателя	ДО	16
Отпуск без сохранения заработной платы в случаях, предусмотренных законодательством	ОЗ	17
Ежегодный дополнительный отпуск без сохранения заработной платы	ДБ	18
Временная нетрудоспособность (кроме случаев, предусмотренных кодом "Т") с назначением пособия согласно законодательству	Б	19
Временная нетрудоспособность без назначения пособия в случаях, предусмотренных законодательством	Т	20
Сокращенная продолжительность рабочего времени против нормальной продолжительности рабочего дня в случаях, предусмотренных законодательством	ЛЧ	21
Время вынужденного прогула в случае признания увольнения, перевода на другую работу или отстранения от работы незаконными с восстановлением на прежней работе	ПВ	22
Невыходы на время исполнения государственных или общественных обязанностей согласно законодательству	Г	23

Наименование документа	Буквенный код	Цифровой код
Прогулы (отсутствие на рабочем месте без уважительной причины в течение времени, установленного законодательством)	ПР	24
Продолжительность работы в режиме неполного рабочего времени по инициативе работодателя в случаях, предусмотренных законодательством	НС	25
Выходные дни (еженедельный отпуск) и нерабочие праздничные дни	В	26
Дополнительные выходные дни (оплачиваемые)	ОВ	27
Дополнительные выходные дни (без сохранения заработной платы)	НВ	28
Забастовка (при условиях и в порядке, предусмотренных законом)	ЗБ	29
Неявки по невыясненным причинам (до выяснения обстоятельств)	НН	30
Время простоя по вине работодателя	РП	31
Время простоя по причинам, не зависящим от работодателя и работника	НП	32
Время простоя по вине работника	ВП	33
Отстранение от работы (недопущение к работе) с оплатой (пособием) в соответствии с законодательством	НО	34
Отстранение от работы (недопущение к работе) по причинам, предусмотренным законодательством, без начисления заработной платы	НБ	35
Время приостановки работы в случае задержки выплаты заработной платы	НЗ	36

19 Термины и определения

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ООО «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



www.perco.ru
тел: 8 (800) 333-52-53