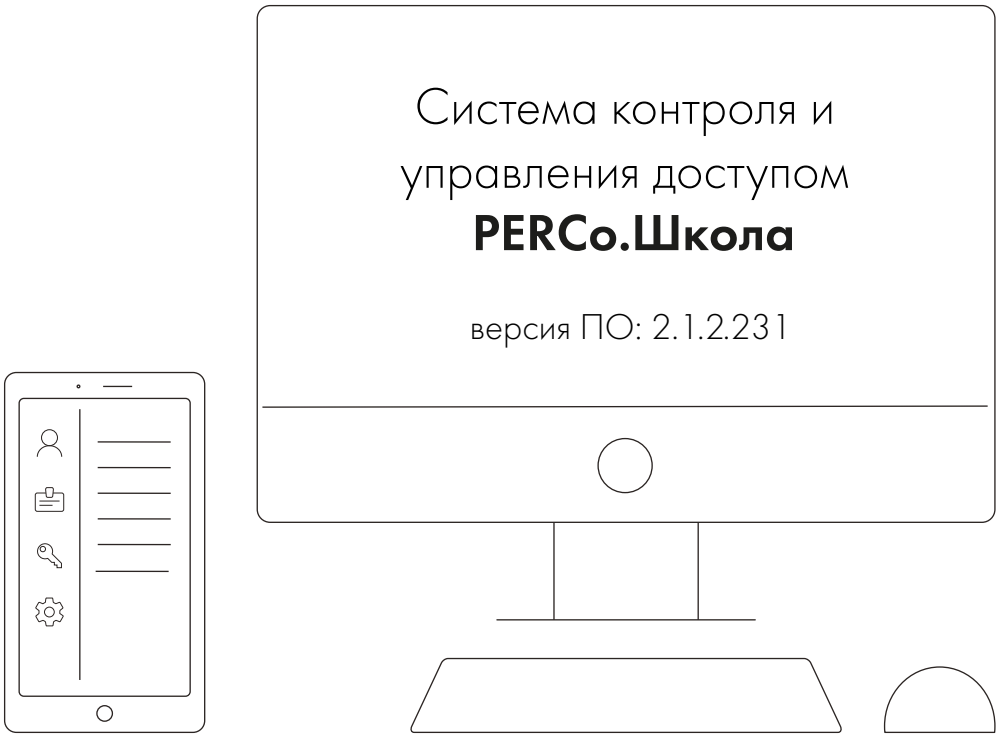
PERCo®

РУКОВОДСТВО АДМИНИСТРАТОРА



PERCo.Школа

Сетевое программное обеспечение

SEC.RU | Короткий путь к информации
Скачано с sec.ru

СОДЕРЖАНИЕ

1. Введение 4
2. Назначение 5
3. Основные особенности системы *PERCo.Школа* 6
4. Состав и принципы работы системы 7
5. Поддерживаемое оборудование 10
   5.1. Контроллеры управления дверьми 10
   5.2. Контроллеры управления турникетом 11
   5.3. Контроллеры регистрации 11
   5.4. Терминалы распознавания лиц 11
   5.5. Исполнительные устройства 12
   5.6. Считыватели 13
   5.7. Электронные проходные 13
   5.8. Устройства управления 13
   5.9. Контроллеры доступа со сканерами отпечатков пальцев 14
   5.10. Картоприемники 15
   5.11. Дополнительное оборудование 15
   5.12. Видеокамеры 15
6. Основные технические характеристики 16
7. Требования к аппаратным и программным средствам 18
8. Сетевые настройки 19
   8.1. Используемые сетевые порты и протоколы 19
   8.2. Организация широковещательной рассылки пакетов 20
   8.3. Добавление сетевого интерфейса ПК 21
   8.4. Сетевые настройки контроллера 23
   8.5. Настройка DHCP-сервера в ОС Windows 24
   8.6. Настройка DHCP-сервера в ОС Linux 26
   8.7. Внешнее подключение контроллера к серверу *PERCo.Школа* 27
   8.8. Проверка связи между ПК и контроллером 28
9. Установка системы 31
10. Управление лицензиями 35
11. Менеджер системы безопасности PERCo.Школа 38
   11.1. Вкладка «Мониторинг» 39
   11.2. Вкладка «Настройки» 40
   11.3. Вкладка «Резервные копии и логи» 42
   11.4. Вкладка «Настройки менеджера» 43
   11.5. Вкладка «Опасная зона» 43
12. Режим распределенной системы 45
   12.1. Настройка PERCo.Школа для работы в режиме распределенной системы 45
      12.1.1. Подключение базы данных 45
      12.1.2. Создание сегментов в PERCo.Школа 46
      12.1.3. Закрепление сегментов за серверами 47
   12.2. Особенности работы в режиме распределенной системы 48
13. Интеграция с 1С:Предприятие 8 49
14. API PERCo.Школа 50
15. Предварительная настройка 51
16. Функции Antipass и Global Antipass 53
17. Раздел «Администрирование» 55
   17.1. Подраздел «Конфигурация» 55

SEC.RU | Короткий путь к информации Скачано с sec.ru

17.1.1. Вкладка «Помещения» 55
17.1.1.1. Создание списка помещений 56
17.1.1.2. Размещение устройств в помещениях 57
17.1.2. Вкладка «Устройства» 58
17.1.2.1. Поиск устройств 60
17.1.2.2. Добавление камеры, шлюза и составного объекта 61
17.1.2.3. Настройка общих параметров контроллеров 64
17.1.2.4. Порядок работы с картами Mifare 69
17.1.2.5. Настройка параметров устройства 73
17.1.3. Вкладка «События» 74
17.1.3.1. Переименование события 75
17.1.4. Вкладка «Шаблоны камер» 75
17.1.4.1. Создание шаблона камеры 76
17.1.5. Вкладка «Система» 77
17.1.5.1. Подвкладка «Основные параметры» 78
17.1.5.2. Подвкладка «Рассылки и уведомления» 78
17.1.5.3. Добавление параметров почтовой рассылки 79
17.1.5.4. Добавление параметров рассылки SMS-уведомлений 79
17.1.5.5. Добавление параметров рассылки в Viber 80
17.1.5.6. Порядок создания паблик-аккаунта Viber 81
17.1.5.7. Настройки Telegram 82
17.1.5.8. Создание Telegram-бота 82
17.1.5.9. Подвкладка «Учебный год» 83
17.1.5.10. Подвкладка «Видеозапись» 83
17.1.5.11. Подвкладка «OpenID Connect» 84
17.1.5.12. Подвкладка «О системе» 86
17.2. Подраздел «События системы» 86
17.3. Подраздел «Реакция на события» 87
17.3.1. Добавление новой реакции 87
17.3.2. Добавление внутренней реакции на событие контроллера 90
17.4. Подраздел «Журнал уведомлений» 92
17.5. Подраздел «Задания» 93
17.5.1. Создание нового задания 94
17.6. Подраздел «Операторы» 97
17.6.1. Добавление оператора системы 98
17.7. Подраздел «Роли и права операторов» 99
17.7.1. Добавление роли оператора (набора полномочий) 99
17.8. Подраздел «Лицензии» 100
17.8.1. Ввод кода активации 101
18. Параметры контроллеров PERCo 103
18.1. Вкладка «Сеть» 103
18.2. Вкладка «Разное» 104
18.3. Вкладка ИУ («Замок», «Турникет», «Шлагбаум») 104
18.4. Вкладка «Входы» 105
18.5. Вкладка «Выходы» 106
18.6. Вкладка «Выводы» 107
18.7. Вкладка «Генератор тревоги» 108
18.8. Вкладка «Считыватель» 109
19. Параметры контроллеров CL15, CL15.1, CL15.3, CL15.7, CR11, CR11.1, CR02.9, CT/L14, CT/L14.1, CT13, CT13.1 111
19.1. Вкладка «Сеть» 111
19.2. Вкладка «Разное» 112
19.3. Вкладка ИУ 112

SEC.RU | Короткий путь к информации Скачано с sec.ru

19.4. Вкладка «Направление» ... 114
19.5. Вкладка «Генератор тревоги» ... 116
19.6. Вкладка «Входы» ... 117
19.7. Вкладка «Выходы» ... 118
19.8. Вкладки «Свойства» и «Направление №» (для CR11 и CR11.1) ... 119
19.9. Вкладка «Считыватели» ... 120
19.10. Вкладка «Шлюз» ... 121
19.11. Вкладка «Составной объект» ... 121
20. Параметры контроллеров Suprema ... 122
20.1. Вкладка «Сеть» ... 122
20.2. Вкладка «Разное» ... 123
20.3. Вкладка «Замок» ... 123
20.4. Вкладка «Считыватель» ... 125
21. Параметры контроллеров ZKTeco ... 128
21.1. Вкладка «Сеть» ... 128
21.2. Вкладка «Разное» ... 128
21.3. Вкладка «Замок» ... 129
21.4. Вкладка «Считыватель» ... 130
22. Параметры контроллеров BioSmart ... 132
22.1. Вкладка «Сеть» ... 132
22.2. Вкладка «Разное» ... 133
22.3. Вкладка «Замок» (для BioSmart Quasar) ... 133
22.4. Вкладка «Считыватель» ... 134
22.5. Подключение считывателя BioSmart PalmJet в системе PERCo.Школа ... 134
22.5.1. Подключение считывателя PalmJet через контроллер UniPass Pro ... 135
22.5.2. Подключение считывателя PalmJet через сервер BioSmart SmartHub ... 135
23. Параметры видеокамеры ... 139
23.1. Вкладка «Сеть» ... 139
23.2. Вкладка «Камера» ... 139
23.3. Вкладка «О камере» ... 139
23.4. Вкладка «Видео» ... 140
24. Настройка контроллера СКУД PERCo для работы с картоприемником ... 141
25. Настройка контроллера СКУД PERCo для работы с алкотестером «Алкобарьер», интегрированным в систему ... 145
25.1. Как узнать IP-адрес алкотестера «Алкобарьер»? ... 148
25.2. Как узнать порт, протокол и сетевое имя алкотестера «Алкобарьер»? ... 148
26. Настройка контроллера СКУД PERCo для работы с алкотестером «Алкобарьер» в качестве ВВУ ... 151
27. Настройка работы алкотестера «Алкобарьер» для контроля двух направлений прохода ИУ ... 154
28. Настройка контроллера СКУД PERCo для работы с алкотестером «Алкорамка | про», интегрированным в систему ... 158
29. Команды управления устройствами ... 161
30. Термины и определения ... 162
Приложение 1. Примеры построения работы системы распределенных серверов ... 164
Приложение 2. Реализация многоуровневой верификации ... 171

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1. Введение

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

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

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

Руководство должно использоваться совместно с руководствами пользователя на модули ПО системы ***PERCo.Школа***.

Примечание:

Эксплуатационная документация на оборудование и ПО системы ***PERCo.Школа*** доступна в электронном виде на сайте компании ***PERCo*** по адресу: www.perco.ru.

Принятые сокращения:

АРМ – автоматизированное рабочее место;
АТП – автотранспортная проходная;
БД – база данных;
ВВУ – внешнее верифицирующее устройство;
ИСО – интегрированная система охраны;
ИУ – исполнительное устройство;
КПП – контрольно-пропускной пункт;
ПДУ – пульт дистанционного управления;
ПК – персональный компьютер, ноутбук;
ПО – программное обеспечение;
РКД – режим контроля доступа;
СКУД – система контроля и управления доступом;
СУБД – система управления базами данных;
ТРЛ – терминал распознавания лиц;
УРВ – учет рабочего времени;
ЭП – электронная проходная.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Назначение

Система контроля и управления доступом *PERCo.Школа* (далее – *система*) предназначена для применения в учреждениях и организациях образовательной сферы деятельности. Система позволяет решать следующие задачи:

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3. Основные особенности системы *PERCo.Школа*

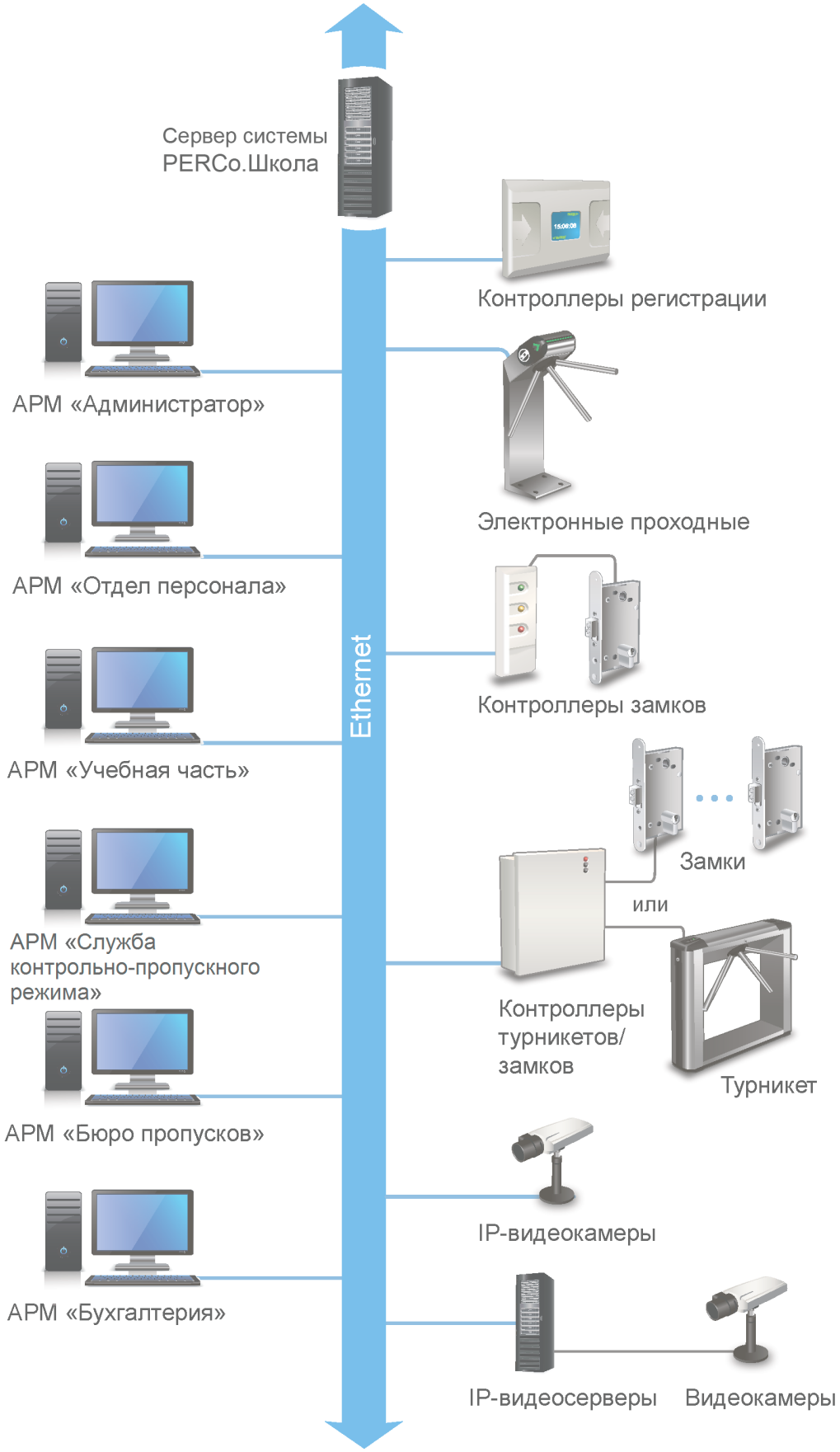
- Обмен данными между АРМ, БД и оборудованием системы осуществляется по сети *Ethernet*. Это позволяет при развертывании системы использовать уже существующую IT-инфраструктуру организации.
- Сервер системы, сервер БД и все необходимое для работы системы ПО устанавливается на одном ПК, подключенном к сети *Ethernet*. Установка дополнительного ПО на АРМ операторов системы не требуется. Доступ осуществляется удаленно, через Web-интерфейс сервера системы.
- Наличие постоянной связи контроллеров системы с сервером не требуется. В энергонезависимую память каждого контроллера передаются все права доступа владельцев карт. Там же сохраняются регистрируемые контроллером события. При восстановлении связи с сервером системы события переносятся в БД системы.
- Устройства системы поддерживают возможность обновления встроенного ПО (прошивки) по сети *Ethernet*.
- Система легко масштабируется, то есть возможно увеличение числа контроллеров (КПП) и АРМ с их интеграцией в уже существующую систему.
- При организации дополнительных АРМ достаточно добавить в систему нового оператора и выдать ему полномочия на доступ к соответствующим разделам и подразделам ПО системы.
- ПО системы позволяет гибко настраивать полномочия операторов АРМ. Полномочия выдаются операторам независимо на разделы и подразделы ПО, оборудование, помещения, подразделения и т.д. При этом АРМ связано не с конкретным ПК, а с учетной записью оператора.
- Система поддерживает биометрические технологии. Биометрические контроллеры ***PERCo*** снабжены сканерами отпечатков пальцев, помимо этого в системе реализована интеграция со сторонними производителями:
  - оборудование производства ***“Suprema”*** с поддержкой сканирования отпечатков пальцев и распознавания по лицу;
  - оборудование производства ***“ZKTeco”*** с поддержкой сканирования отпечатков пальцев, распознавания по лицу и идентификации по ладони (включает в себя распознавание по форме, отпечатку и рисунку вен ладони);
  - оборудование производства ***“BioSmart”*** с поддержкой распознавания по лицу и идентификации по рисунку вен ладони.

  Сканирование биометрических данных при необходимости дополняет стандартный метод верификации по картам доступа и позволяет увеличить надежность системы контроля и управления доступом на территории организации при проходе сотрудников, учеников, родственников учеников и посетителей, обеспечивая предотвращение случаев прохода по чужой карте доступа.
- Система, кроме стандартов бесконтактных карт *EMM* и *HID*, также поддерживает стандарт *Mifare*. Карты данного типа получили самое широкое распространение по всему миру и позволяют организовать контроль доступа и защиту персональных данных, записанных на карту, на самом высоком уровне.
- В системе предусмотрена возможность использования технологии *NFC* (технология беспроводной передачи данных малого радиуса действия) для эмуляции бесконтактных карт – проход и доступ осуществляется при помощи смартфона с технологией *NFC*.
- Система поддерживает интеграцию с оборудованием сторонних производителей (доступно после приобретения лицензий на соответствующие модули ПО):
  - видеокамеры ***TRASSIR*** производства ООО ***«ДССЛ-Первый»***;
  - устройства охранно-пожарной сигнализации производства ЗАО НВП ***«Болид»***;
  - видеокамеры, подключенные к серверам ***Интеллект X*** (***Axxon Next***) производства ООО ***«Ай Ти Ви групп»***.
- В системе предусмотрен режим мультисервера для объединения географически удаленных объектов в единую систему и повышения отказоустойчивости в сетях с большим количеством контроллеров.

SEC.RU | Короткий путь к информации Скачано с sec.ru

4. Состав и принципы работы системы

Состав системы представлен на схеме:



Структурная схема системы PERCo.Школа

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Основные элементы системы:

Сервер системы

На ПК сервера системы устанавливается ПО системы, состоящее из сервера, видеосервера, БД системы и другого вспомогательного ПО. В БД системы каждому сотруднику, ученику, родственнику ученика и посетителю ставится в соответствие пропуск-идентификатор (бесконтактная карта доступа, штрихкод, брелок или смартфон с функцией NFC), с уникальным номером и / или биометрическая информация (отпечатки пальцев, шаблон ладони, шаблон лица). Конфигурирование и управление системой осуществляется через Web-интерфейс сервера системы.

КПП

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

Возможны следующие варианты управления ИУ на КПП:

1. Оператором КПП в ручном режиме с помощью ПДУ.
2. Оператором КПП от ПК заданием для направлений ИУ одного из режимов контроля доступа (РКД): *«Открыто»*, *«Закрыто»*, *«Контроль»*. Это позволяет при необходимости обеспечить свободный проход в данном направлении или полностью его перекрыть. Для прохода по картам доступа (штрихкодам, отпечаткам пальцев, шаблонам ладони, шаблонам лица) используется РКД *«Контроль»*.
3. Автоматически контроллером КПП при проходе по картам доступа (штрихкодам, отпечаткам пальцев, шаблонам ладони, шаблонам лица). При этом в направлении прохода должен быть установлен РКД *«Контроль»*. При проходе через КПП сотрудник (ученик, родственник ученика или посетитель):
   - в случае идентификации по карте доступа – предъявляет карту считывателю;
   - в случае идентификации по штрихкоду – предъявляет штрихкод устройству с поддержкой сканера штрихкода;
   - в случае идентификации по отпечаткам пальцев – проходит процедуру сканирования отпечатков пальцев;
   - в случае идентификации по карте доступа и отпечаткам пальцев – предъявляет карту считывателю и проходит процедуру сканирования отпечатков пальцев;
   - в случае идентификации по карте доступа и ПИН-коду – предъявляет карту доступа и набирает ПИН-код на клавиатуре;
   - в случае идентификации по отпечаткам пальцев и ПИН-коду – проходит процедуру сканирования отпечатков пальцев и набирает ПИН-код на клавиатуре;
   - при наличии на КПП терминала распознавания лица:
     - в случае идентификации по лицу – распознавание лица происходит автоматически при проходе;
     - в случае идентификации по лицу и карте – после автоматического распознавания лица предъявляет карту считывателю;
     - в случае идентификации по лицу или карте – в случае неудачи распознавания лица предъявляет карту доступа;
     - для идентификации по лицу и ПИН-коду – после автоматического распознавания лица набирает ПИН-код на клавиатуре TPЛ;
     - для идентификации по лицу, карте и ПИН-коду – после автоматического распознавания лица предъявляет карту доступа и набирает ПИН-код на клавиатуре TPЛ.
   - при наличии на КПП сканера ладони (идентификация по ладони включает в себя распознавание по форме, отпечатку и рисунку вен ладони):
     - в случае идентификации по ладони – проходит процедуру сканирования ладони;
     - для идентификации по ладони или карте – в случае неудачи сканирования ладони предъявляет карту доступа;
     - для идентификации по ладони и карте – после прохождения процедуры сканирования ладони предъявляет карту доступа.

SEC.RU | Короткий путь к информации Скачано с sec.ru

На основании анализа полученной идентификационной информации, а также выданных ее владельцу прав доступа контроллер принимает решение на разрешение или запрет прохода, подавая соответствующую команду ИУ. Каждый факт получения идентификационной информации фиксируется в БД с указанием ее вида, места и времени ее получения, что позволяет системе отслеживать местонахождение, время пребывания и перемещения сотрудника (ученика, родственника ученика или посетителя) по территории и помещениям организации.

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

АРМ

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

- *«Администратор»* (раздел **«Администрирование»**);
- *«Учебная часть»* (разделы: **«Учащиеся»**, **«Расписание»**, описание разделов см. в *Руководствах пользователя* на модули ПО);
- *«Отдел персонала»* (раздел **«Персонал»**, описание см. в *Руководствах пользователя* на модули ПО);
- *«Служба контрольно-пропускного режима»* (разделы: «**Контроль доступа»**, **«Заказ пропуска»**, **«Верификация»**, **«Мониторинг»**, описание разделов см. в *Руководствах пользователя* на модули ПО);
- *«Бюро пропусков»* (раздел **«Бюро пропусков»**, описание см. в *Руководствах пользователя* на модули ПО);
- *«Бухгалтерия»* (раздел **«Учет рабочего времени»**, описание раздела см. в *Руководстве пользователя* на модуль ПО ***PERCo-WM01***).

SEC.RU | Короткий путь к информации Скачано с sec.ru

5. Поддерживаемое оборудование

Примечания:

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

Кроме указанного ниже оборудования в системе ***PERCo.Школа*** также поддерживается работа ранее снятых с производства контроллеров ***PERCo***: ***CL05***, ***CL05.x***, ***CT/L04***, ***CT03***, ***CR01***, ***CL201.x***, считывателей ***IR05***, ***IR08***, ***MR08***, конвертеров ***AC-02***, ***AC-02.1***.

5.1. Контроллеры управления дверьми

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

- ***CT/L14***, ***CT/L14.1***. Позволяет организовать четыре двухсторонние или односторонние точки прохода, при этом к контроллеру по интерфейсу *RS-485* подключается до 8-ми выносных считывателей. Может обеспечить полноценную работу шлюза из замков. Имеет возможность подключения сканера штрихкода по интерфейсу *USB*.
- ***CT/L04.2***. Позволяет организовать две двухсторонние точки прохода или четыре односторонние точки прохода, управляя соответственно двумя или четырьмя замками, при этом к контроллеру по интерфейсу *RS-485* подключается до 8-ми выносных считывателей.
- ***Биометрический контроллер CL15.1***. Позволяет организовать одну одностороннюю точку прохода, одно направление двухсторонней точки прохода (при использовании двух контроллеров данной модели) или одно направление прохода для шлюза (при использовании четырех контроллеров данной модели). Имеет светодиодную RGB-индикацию режимов работы, встроенный сканер отпечатка пальца и встроенный считыватель форматов *HID*, *EM-Marin* и *Mifare*, который позволяет работать в том числе с банковскими картами *PayPass* и смартфонами с технологией *NFC*.
- ***CL15.3***. Позволяет организовать одну одностороннюю точку прохода, одно направление двухсторонней точки прохода (при использовании двух контроллеров данной модели) или одно направление прохода для шлюза (при использовании четырех контроллеров данной модели). Имеет встроенный считыватель форматов *HID*, *EM-Marin* и светодиодную RGB-индикацию режимов работы.
- ***CL15.7***. Позволяет организовать одну одностороннюю точку прохода, одно направление двухсторонней точки прохода (при использовании двух контроллеров данной модели) или одно направление прохода для шлюза (при использовании четырех контроллеров данной модели). Имеет светодиодную RGB-индикацию режимов и встроенный считыватель формата *Mifare*, который позволяет работать в том числе с банковскими картами *PayPass* и смартфонами с технологией *NFC*.
- ***CL211.3***. Подключается в качестве контроллера второго уровня к контроллерам ***CT/L14***, ***CT/L14.1***, ***CT/L04.2*** или встроенному контроллеру ЭП ***CT13***, ***CT13.1***, ***CT03.2*** по интерфейсу *RS-485* и позволяет организовать один КПП с контролем проходов в одном направлении. Контроллер снабжен встроенным считывателем карт доступа формата *HID*, *EM-Marin* и RGB-светодиодным индикатором. Одновременно к контроллеру первого уровня может быть подключено до 8 контроллеров второго уровня.
- ***CL211.9***. Подключается в качестве контроллера второго уровня к контроллерам ***CT/L14***, ***CT/L14.1***, ***CT/L04.2*** или встроенному контроллеру ЭП ***CT13***, ***CT13.1***, ***CT03.2*** по интерфейсу *RS-485* и позволяет организовать один КПП с контролем проходов в одном направлении. Контроллер снабжен встроенным считывателем карт доступа формата *HID*, *EM-Marin*, *Mifare* и RGB-светодиодным индикатором. Поддерживает работу с банковскими картами *PayPass* и смартфонами с *NFC*. Одновременно к контроллеру первого уровня может быть подключено до 8 контроллеров второго уровня.

Примечание:

Подключение контроллеров второго уровня производится через Web-интерфейс контроллеров первого уровня

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.2. Контроллеры управления турникетом

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

- ***CT/L14***, ***CT/L14.1*** Позволяет организовать две двухсторонние точки прохода. При этом к контроллеру по интерфейсу *RS-485* подключаются встроенные считыватели обоих турникетов, сканер штрихкода, дополнительно устанавливаемые выносные считыватели или ИУ (замки). Может обеспечить полноценную работу шлюза из турникетов.
- ***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).
- ***CT03.2***, ***CT13***, ***CT13.1***. Встроенные контроллеры в составе ЭП, позволяют организовать одно КПП с контролем проходов в двух направлениях.
- ***Биометрический контроллер CL15.1***. Позволяет организовать одну одностороннюю точку прохода, одно направление двухсторонней точки прохода (при использовании двух контроллеров данной модели) или одно направление прохода для шлюза (при использовании четырех контроллеров данной модели). Имеет светодиодную RGB-индикацию режимов работы, встроенный сканер отпечатка пальца и встроенный считыватель форматов *HID*, *EM-Marin* и *Mifare*, который позволяет работать в том числе с банковскими картами PayPass и смартфонами с технологией NFC.
- ***CL15.3***. Позволяет организовать одну одностороннюю точку прохода, одно направление двухсторонней точки прохода (при использовании двух контроллеров данной модели) или одно направление прохода для шлюза (при использовании четырех контроллеров данной модели). Имеет встроенный считыватель форматов *HID*, *EM-Marin* и светодиодную RGB-индикацию режимов работы.
- ***CL15.7***. Позволяет организовать одну одностороннюю точку прохода, одно направление двухсторонней точки прохода (при использовании двух контроллеров данной модели) или одно направление прохода для шлюза (при использовании четырех контроллеров данной модели). Имеет светодиодную RGB-индикацию режимов и встроенный считыватель формата *Mifare*, который позволяет работать в том числе с банковскими картами PayPass и смартфонами с технологией NFC.

5.3. Контроллеры регистрации

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

- ***Биометрический терминал учета рабочего времени CR11***, ***CR11.1***. Снабжен встроенными сканером отпечатков пальцев и считывателем карт доступа форматов *HID*, *EM-Marin* и *Mifare*, который позволяет работать в том числе с банковскими картами PayPass и смартфонами с технологией NFC, а также цветным ЖКИ (дисплеем) с тачскрином и с диагональю 4,8''. Имеет возможность просмотра баланса рабочего времени и ввода оправдательных документов.
- ***CR01.2 LICON***. Снабжен двумя встроенными считывателями карт доступа формата *HID*, *EM-Marin* и ЖКИ с диагональю 2,8''.
- ***CR01.9***, ***CR02.9***. Снабжен двумя встроенными считывателями карт доступа формата *HID*, *EM-Marin* и *Mifare*, которые позволяют работать в том числе с банковскими картами PayPass и смартфонами с технологией NFC, и ЖКИ с диагональю 2,8''.

5.4. Терминалы распознавания лиц

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

В системе ***PERCo.Школа*** предусмотрена полная интеграция следующих типов ТРЛ:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Производства *“ZKTeco”***: терминалы ***FaceDepot-7A***, ***FaceDepot-7B***, ***ProFaceX***, ***SpeedFace-V5L-TD*** (с пирометром), ***ProFaceX[TI]*** и ***SpeedFace-V5L[TI]*** (с тепловизором),
- **Производства *“Suprema”***: терминалы ***FaceLight***, ***FaceStation 2***, ***FaceStation F2***, ***BioStation 3***;
- **Производства “*BioSmart*”**: терминал ***Quasar*** (с поддержкой ***BioSmart Thermoscan F***).

Внимание!

Рекомендуется в системе ***PERCo.Школа*** использовать ТРЛ производства ***“Suprema”*** только одной модели, так как у разных моделей терминалов используются разные алгоритмы распознавания лиц. В случае замены терминалов ***Suprema*** одного типа другим потребуется заново создать базу данных распознавания лиц.

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

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

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

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

5.5. Исполнительные устройства

Замки

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

Турникеты

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

Калитки

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

Шлагбаумы

- автоматические шлагбаумы серии ***PERCo-GS***;
- шлагбаумы сторонних производителей.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.6. Считыватели

Могут быть использованы считыватели карт формата *HID*, *EM-Marin* или *Mifare*. Внешние считыватели подключаются к контроллерам системы по интерфейсу *RS-485*. Для подключения считывателей с интерфейсом *Wiegand-26, -32, -34, -37, -40, -42*, *-48*, *-50*, *-56*, *-58*, *-64*, *-66* необходимо использовать конвертер интерфейса ***PERCo-AC-02.2***.

В качестве внешних считывателей карт доступа могут использоваться:

- считыватели ***PERCo*** серий ***IR*** и ***MR***;
- стойка-считыватель ***PERCo-IRP01***.

В качестве контрольных (подключаются к USB-разъему ПК) используются считыватели ***PERCo*** серий:

- ***IR15*** для карт доступа.
- ***IR18*** для карт доступа и отпечатков пальцев.

Предусмотрена интеграция следующих считывателей производства ***BioSmart***:

- ***BioSmart PalmJet*** – внешний считыватель карт доступа и рисунка вен ладоней. Считыватель используется совместно с контроллером ***BioSmart Unipass Pro*** или программным сервисом ***BioSmart SmartHub***.

Примечание:

Из-за аппаратных ограничений для считывателя ***BioSmart PalmJet*** не поддерживаются временные критерии доступа и срок действия идентификаторов, а также поддерживается только универсальный режим работы считывателей (8 байт).

- ***BioSmart AirPalm*** – контрольный считыватель рисунка вен ладоней. Перед началом работы со считывателем необходимо скачать драйвер, подробнее см. по ссылке https://bio-smart.ru/support#software#!/tab/185407858-3.

5.7. Электронные проходные

ЭП представляет собой готовый комплект оборудования для организации КПП с контролем проходов в двух направлениях, то есть ИУ, считыватели карт доступа и встроенный контроллер. В ЭП могут быть установлены считыватели для карт формата *HID*, *EM-Marin* или *Mifare*, а также сканеры отпечатков пальцев и сканеры штрихкода. Доступны следующие серии электронных проходных ***PERCo***:

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

5.8. Устройства управления

- ***H7, H6/4*** – проводные пульты дистанционного управления (ПДУ) производства ***PERCo***, предназначены для автономного управления ИУ. С помощью ПДУ можно разблокировать (открыть) ИУ для однократного прохода, установить режим свободного прохода или заблокировать (закрыть) ИУ. Также ПДУ снабжен светодиодной и звуковой индикацией. ПДУ входит в комплект поставки ИУ 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/L14.1***, ***CT/L14*** или ***CT/L04.2***.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Для приема ИК-сигнала от пульта ДУ необходимо установить и подключить к контроллеру по интерфейсу *RS-485* выносной блок индикации с ИК-приемником ***PERCo-AI01***.

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

5.9. Контроллеры доступа со сканерами отпечатков пальцев

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

1. Контроллеры доступа ***Suprema***

- ***BioEntry Plus*** (платформа ***BioStar 2***) – биометрический контроллер доступа с возможностью подключения по сети *Ethernet* и протоколу TCP/IP.
- ***BioEntry W2*** – биометрический контроллер доступа в прочном металлическом пыле- и влагозащитном корпусе с возможностью подключения по сети *Ethernet* и протоколу TCP/IP.
- ***BioEntry P2*** – биометрический контроллер доступа с подключением по сети *Ethernet* и протоколу TCP/IP.
- ***BioLite N2*** – биометрический контроллер доступа в прочном металлическом пыле- и влагозащитном корпусе с возможностью подключения по сети *Ethernet* и протоколу TCP/IP. Снабжен ЖК дисплеем и клавиатурой для набора ПИН-кода.

Примечание:

Для интеграции необходимо, чтобы биометрические контроллеры имели версию внутреннего ПО («прошивку») не старее чем:
- для контроллера ***BioEntry W2*** – 1.1.1;
- для контроллера ***BioEntry Plus*** (платформа ***BioStar 2***) – 2.3.1;
- для контроллера ***BioLite N2*** – 1.4.2.

Предусмотрено три варианта подключения данных контроллеров к системе:
- в качестве контроллера одностороннего замка. В этом случае ИУ подключается непосредственно к управляющему выходу контроллера ***Suprema***. Связь с контроллером ***Suprema*** в системе осуществляется по интерфейсу *Ethernet*;
- в качестве считывателя отпечатков пальцев при управлении одним из направлений двухстороннего замка (турникета). В этом случае контроллер ***Suprema*** подключается к контроллеру ***PERCo-CT/L14.1***, ***CT/L14*** или ***CT/L04.2*** по интерфейсу *Wiegand* через конвертер интерфейса ***AC-02.2***;
- для совместной работы с ЭП или контроллером ***PERCo***: релейный выход контроллера ***Suprema*** подключается на управляющий вход контроллера ***PERCo*** параллельно ПДУ, при этом конфигурация выхода ТРЛ должна быть нормально разомкнутой.

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

2. Контроллеры доступа ***ZKTeco***

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

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

5.10. Картоприемники

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

5.11. Дополнительное оборудование

- ***PERCo-AU05*** – табло системного времени (ТСВ) предназначено для отображения времени. ТСВ подключается по интерфейсу *RS-485* к контроллерам ***PERCo-CT/L14.1***, ***CT/L14***, ***CT/L04.2*** и встроенным контроллерам ЭП ***PERCo-CT13***, ***CT13.1***, ***CT03.2***.
- ***Алкотестер «Алкобарьер»*** производства компании «АЛКОТЕКТОР» – стационарный бесконтактный алкотестер, предназначен для предварительной проверки сотрудников на наличие алкогольного опьянения, подключается к контроллерам ***PERCo-CT/L14.1***, ***CT/L14***, ***CL15***, ***CL15.1***, ***CL15.3***, ***CL15.7***, а также к встроенным контроллерам ЭП ***PERCo-CT13.1***, ***CT13***.
- ***ДКЗП*** – датчик контроля зоны прохода предназначен для регистрации несанкционированного прохода или проникновения под преграждающими планками.
- ***Сирена*** – звуковой оповещатель.
- ***Сканер штрихкода*** (USB) – устройство для считывания штрихкода и передачи его в систему.

5.12. Видеокамеры

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

Примечание:

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6. Основные технические характеристики

Стандарт интерфейса связи.....*Ethernet (IEEE 802.3)*
Скорости передачи данных *Ethernet*, *Мбит/с* 10/100
Количество контроллеров СКУД
при работе в стандартном режиме..... не более 1000 на систему
при работе в режиме распределенной системы.....не более 1000 на сегмент
Интенсивность проходов со сменой пространственной зоны, *проходов/ секунду*
для контроллеров на 50000 карт ..... не более 50
для контроллеров на 10000 карт ..... не более 200
Формат карт доступа.....*HID*, *EM-Marin*, *Mifare*
Общее число карт доступа в системе, *шт.* ..... не ограничено
Максимальное количество сотрудников,
учеников, родственников учеников ..... не более 200 000
Максимальное количество посетителей..... не более 200 000
Число событий регистрации для каждого контроллера..... не более 140 000
Количество пространственных зон контроля ..... не более 1024
Количество критериев доступа по времени типа:
временная зона (до 4-х временных интервалов)..... не более 255
недельный график..... не более 255
скользящий посуточный график (в пределах 30 суток)..... не более 255
скользящий понедельный график (в пределах 54 недель)..... не более 255
Количество дней с особым статусом, праздников (до 8 типов)..... не более 365

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

Контроллер	Вариант конфигурации	К-во карт	К-во событий	К-во отпечатков пальцев
CT/L14.1, CT13.1	Контроллер для управления турникетами и / или замками, встроенный контроллер ЭП	до 50 000	до 150 000	5 000 пользователей по 2 отпечатка пальца
CT/L14, **CT13**	Контроллер для управления турникетами и / или замками, встроенный контроллер ЭП	нет ограничения	нет ограничения	5 000 пользователей по 2 отпечатка пальца
CT/L04.2, CT03.2	Универсальный контроллер турникета / замка, встроенный контроллер ЭП	до 50 000	до 230 000	-
		до 40 000	до 390 000	-
		до 30 000	до 550 000	-
		до 20 000	до 710 000	-
		до 10 000	до 870 000	-
CR11.1	Контроллер регистрации	до 50 000	до 150 000	5 000 пользователей по 2 отпечатка пальца
CR11	Контроллер регистрации	нет ограничения	нет ограничения	5 000 пользователей по 2 отпечатка пальца
CR02.9	Контроллер регистрации	до 50 000	до 150 000	-

SEC.RU | Короткий путь к информации Скачано с sec.ru

Контроллер	Вариант конфигурации	К-во карт	К-во событий	К-во отпечатков пальцев
CR01.2 LICON, CR01.9 LICON	Контроллер регистрации	до 50 000	до 125 000	-
		до 40 000	до 280 000	-
		до 30 000	до 440 000	-
		до 20 000	до 600 000	-
		до 10 000	до 760 000	-
CL15.1	Контроллер для управления замком	до 50 000	до 150 000	5 000 пользователей по 2 отпечатка пальца
CL15	Контроллер для управления замком	нет ограничения	нет ограничения	5 000 пользователей по 2 отпечатка пальца
CL15.3, CL15.7	Контроллер для управления замком	до 50 000	до 150 000	-

Примечания:

- Технические характеристики контроллеров сторонних производителей, имеющих возможность интеграции с системой ***PERCo.Школа***, указаны в эксплуатационной документации на эти контроллеры.
- Превышение указанной интенсивности проходов может привести к ошибкам в работе функции Antipass.
- События подключенных контроллеров второго уровня ***PERCo-CL211.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 шаблонов верификации..... не более 512

Примечание:

На каждой точке верификации может транслироваться изображение с одной камеры.

SEC.RU | Короткий путь к информации Скачано с sec.ru

7. Требования к аппаратным и программным средствам

Требования к аппаратным средствам сервера системы

Для стабильной работы ПО рекомендуется использовать ПК, отвечающий следующим требованиям:

- Процессор Intel Core i5-6600 с 3,3 ГГц или AMD Ryzen 5 1400 с 3,2 ГГц
- Оперативная память: 16 Гб.
- SSD-диск с объемом 500 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 64-битная лицензионная версия ОС семейства *Microsoft Windows* или ОС семейства *Linux*.

Рекомендованы к использованию:

- *Windows Server 2019,* возможно *Windows 10* (*Pro, Home, Corporate Edition*), но не ниже;
- *Ubuntu 18.04 Bionic* или *Ubuntu 20.04 Focal Fossa*
- *Debian 10 Buster* или выше
- *Red Hat Enterprise Linux 8* или выше
- *Fedora 30* или выше
- *Alt Linux 8* или выше.

Требования к аппаратным средствам АРМ

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

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

Требования к программным средствам АРМ

Для работы системы на ПК должна быть установлена лицензионная версия ОС семейства Microsoft Windows или Apple Mac OS. Рекомендованы к использованию ОС: Windows 10 и выше; MacOS X или выше, Ubuntu 17 или выше, Debian 10 Buster или выше, CentOS 7 или выше, Fedora 38 или выше, Alt Linux 9 или выше. На планшетах и смартфонах рекомендованы ОС: iOS 15.0 или выше, Android 10.0 или выше.

Для работы с системой необходима ОС с поддержкой одного из следующих Web-браузеров:

- *Google Chrome* версии 105 или выше;
- *Microsoft Edge* версии 105 или выше;
- *Mozilla Firefox* версии 105 или выше;
- *Opera* версии 95 или выше;
- *Apple Safari 14* или выше.

SEC.RU | Короткий путь к информации Скачано с sec.ru

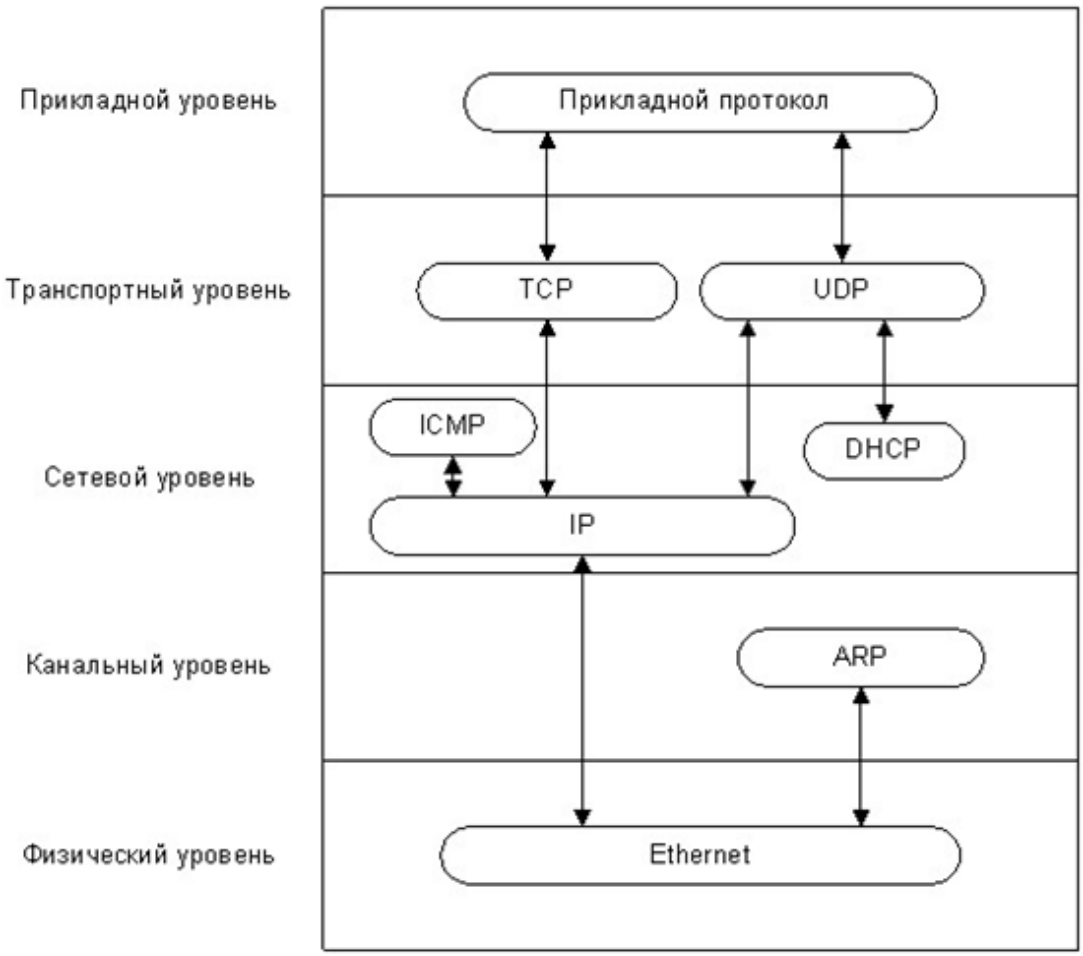
8. Сетевые настройки

8.1. Используемые сетевые порты и протоколы

Внимание!

В ОС семейства *MS Windows* для изменения максимального количества одновременных полуоткрытых исходящих TCP-соединений (half-open connections или connection attempts) рекомендуется использовать программу Half-open limit fix. По умолчанию в версии *XP SP2* и более поздних версиях ОС разрешается иметь не более 10 полуоткрытых исходящих TCP-соединений.

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



Стек протоколов, используемых для обмена в системе

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

Примечание:

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Используемые в системе сетевые порты

Протокол	Порт	Назначение
UDP	12345	для **CT/L14**, **CT/L14.1**, **CT13**, **CT13.1**, **CR11**, **CR11.1**, **CR02.9**, **CL15**, **CL15.1**, **CL15.3, CL15.7**
	18900 18901	для **CT/L04.2**, **CT03.2**, **CR01.2**, **CR01.9:** – конфигурация сетевых параметров контроллеров – широковещательные кадры между контроллерами внутри подсети
TCP	80 443	для **CT/L14**, **CT/L14.1**, **CT13**, **CT13.1**, **CR11**, **CR11.1**, **CR02.9**, **CL15**, **CL15.1**, **CL15.3, CL15.7**
	18902 18903 18904 18905 18906	для **CT/L04.2**, **CT03.2**, **CR01.2**, **CR01.9**: – конфигурация, управление и диагностика – прием журнала регистрации – регистрация индицирующего устройства – регистрация верифицирующего устройства – прием и анализ мониторинга

8.2. Организация широковещательной рассылки пакетов

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

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

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

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

   установите значение параметра: `IPEnableRouter=1`

Примечание:

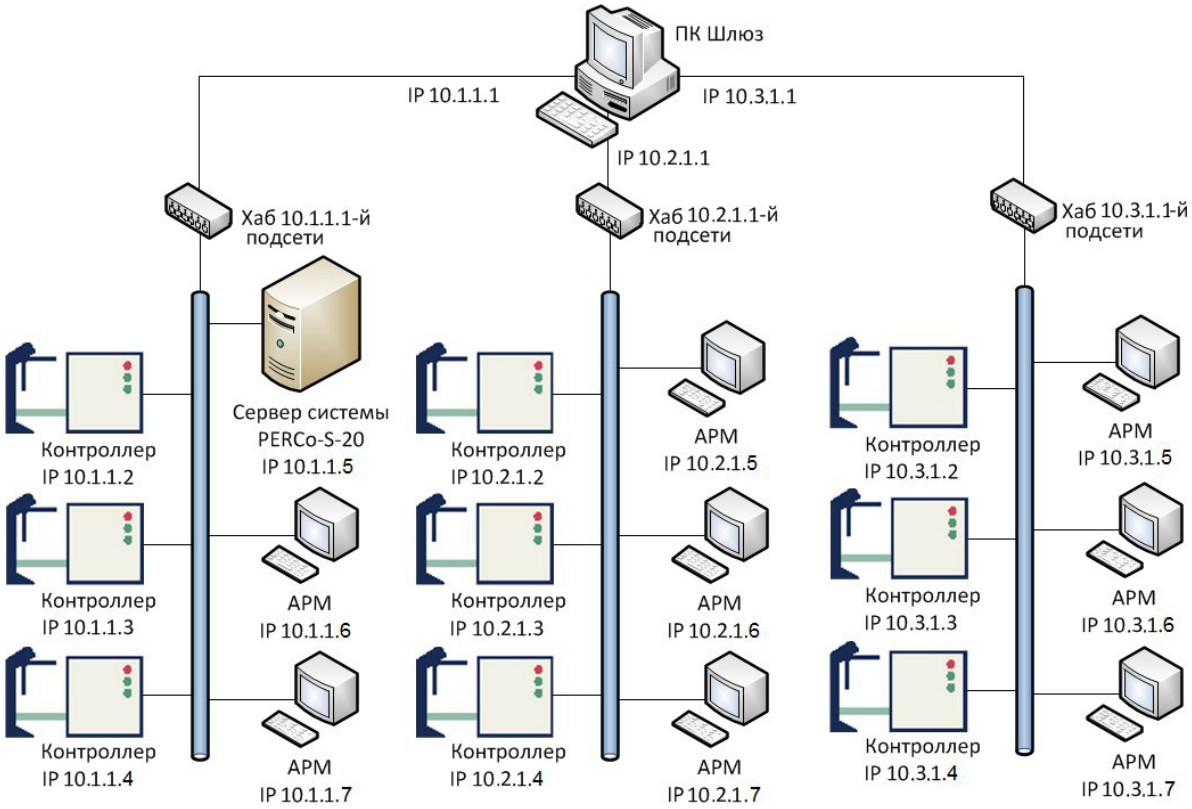
Дополнительная информация о включении маршрутизации пакетов в ОС *Microsoft Windows* доступна на сайте производителя по адресу: https://support.microsoft.com/

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

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

– Основной шлюз: `10.3.1.1`.

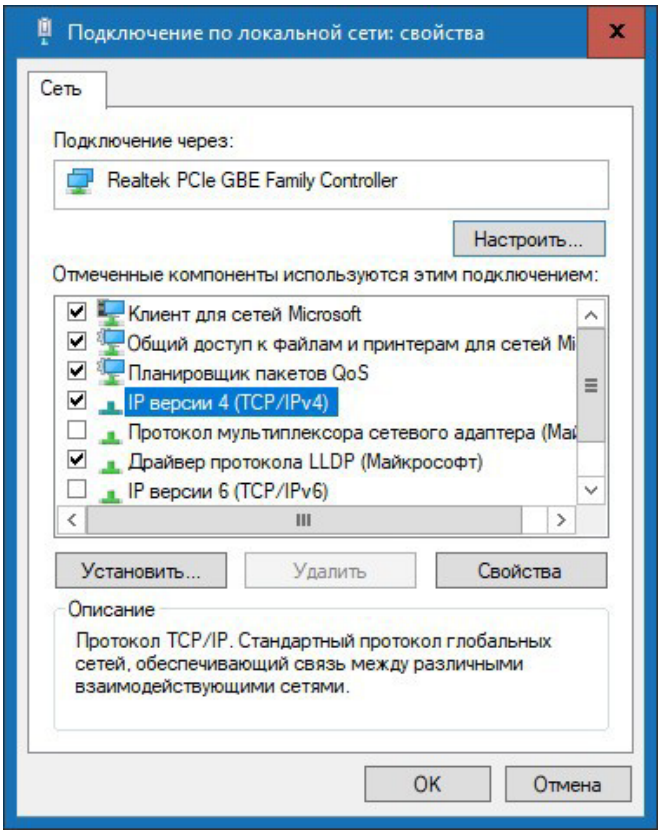


Пример схемы организации широковещательной рассылки

8.3. Добавление сетевого интерфейса ПК

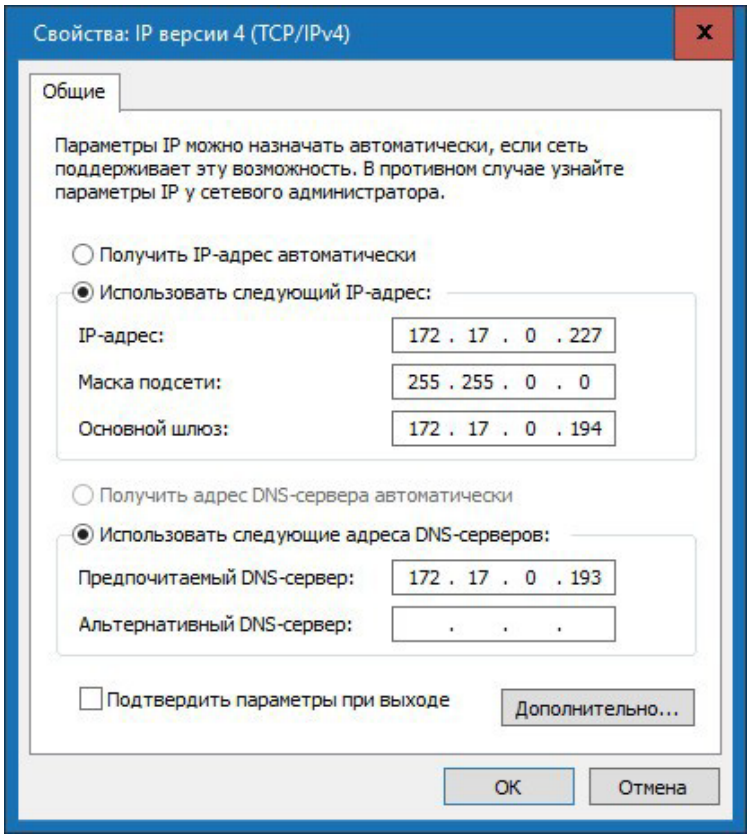
Для добавления сетевого интерфейса (IP-адреса и маски подсети) ПК выполните следующие действия:

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

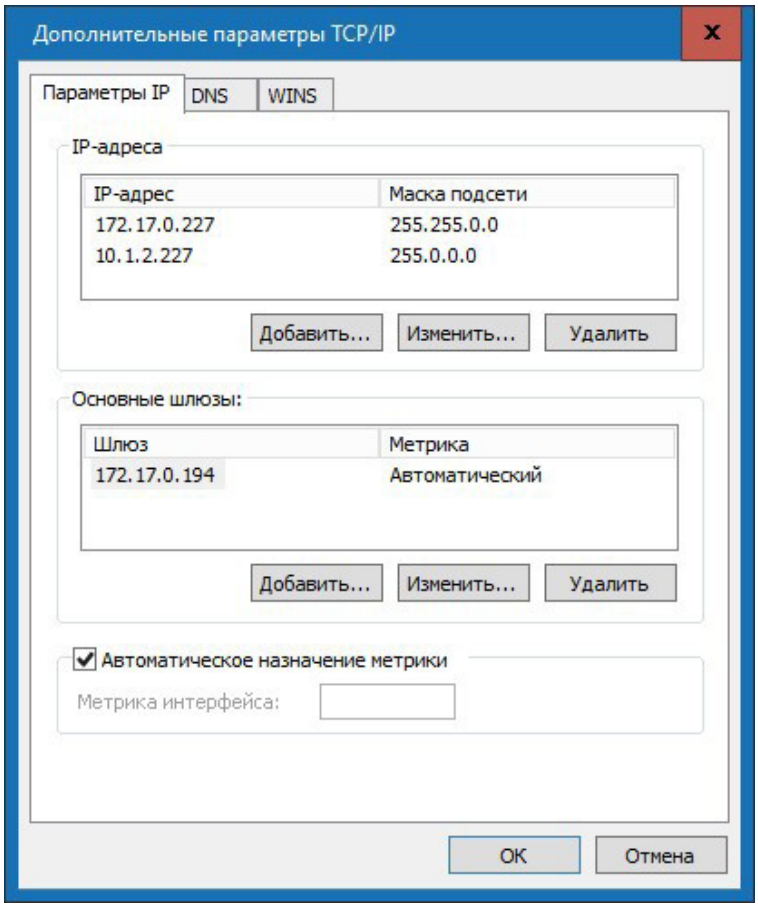


SEC.RU | Короткий путь к информации
Скачано с sec.ru

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

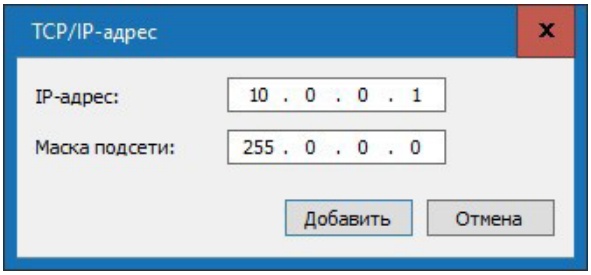


4. В открывшемся окне убедитесь, что переключатель находится в положении **Использовать следующий IP-адрес**, после этого нажмите кнопку **Дополнительно...**. Откроется окно **Дополнительные параметры TCP/IP**:



SEC.RU | Короткий путь к информации Скачано с sec.ru

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



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

8.4. Сетевые настройки контроллера

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

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

При производстве контроллерам системы заданы следующие сетевые настройки:

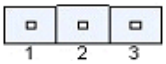
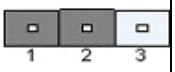
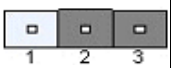
- **MAC-адрес:** уникальный, неизменяемый (указан в паспорте и на плате устройства);
- **IP-адрес:** `10.x.x.x` (указан в паспорте и на плате устройства);
- **Шлюз:** `0.0.0.0`;
- **Маска подсети:** `255.0.0.0`.

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

Внимание!

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

Варианты установки перемычки на разъем XP1 контроллера *PERCo*

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

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

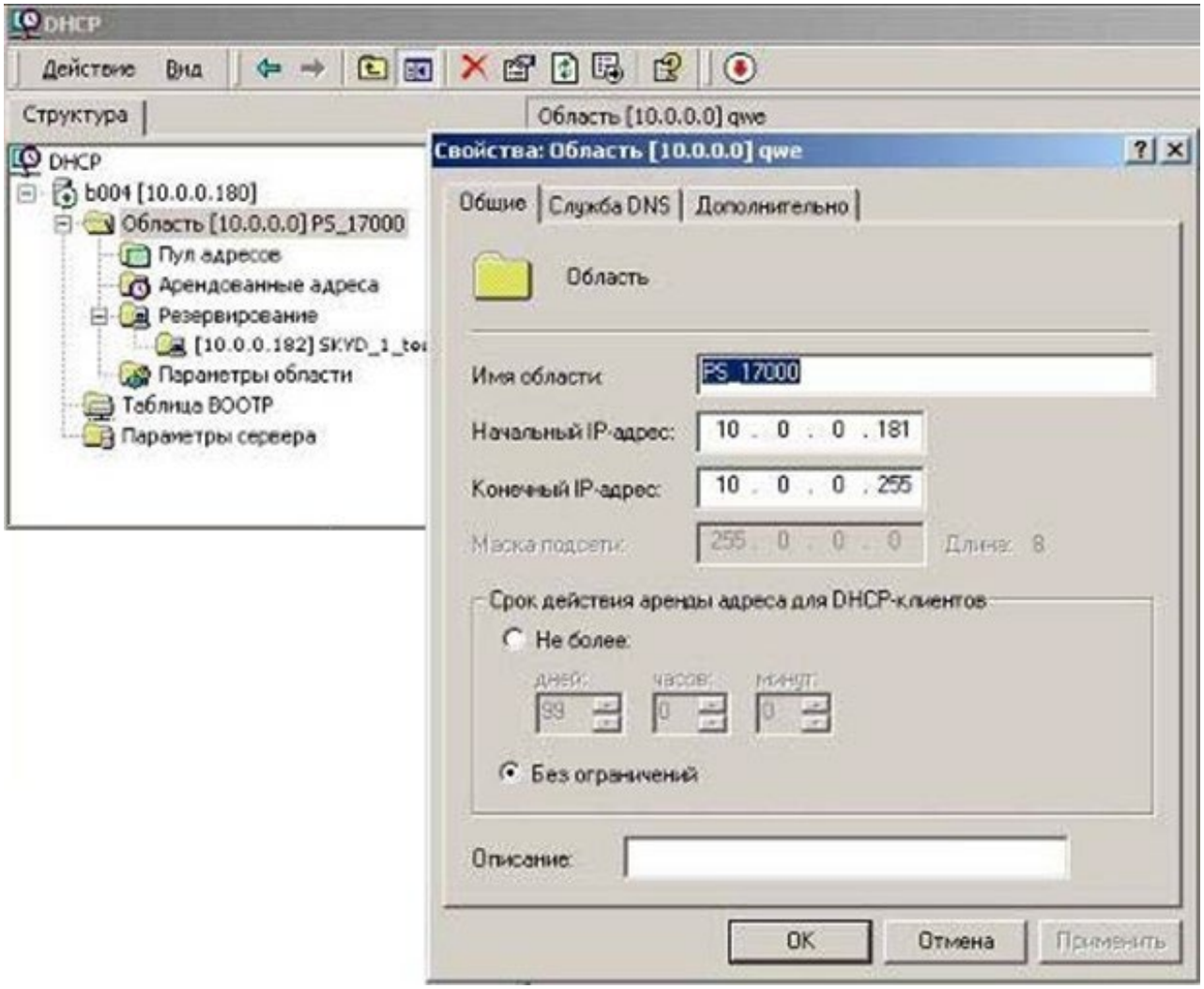
SEC.RU | Короткий путь к информации Скачано с sec.ru

8.5. Настройка DHCP-сервера в ОС Windows

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

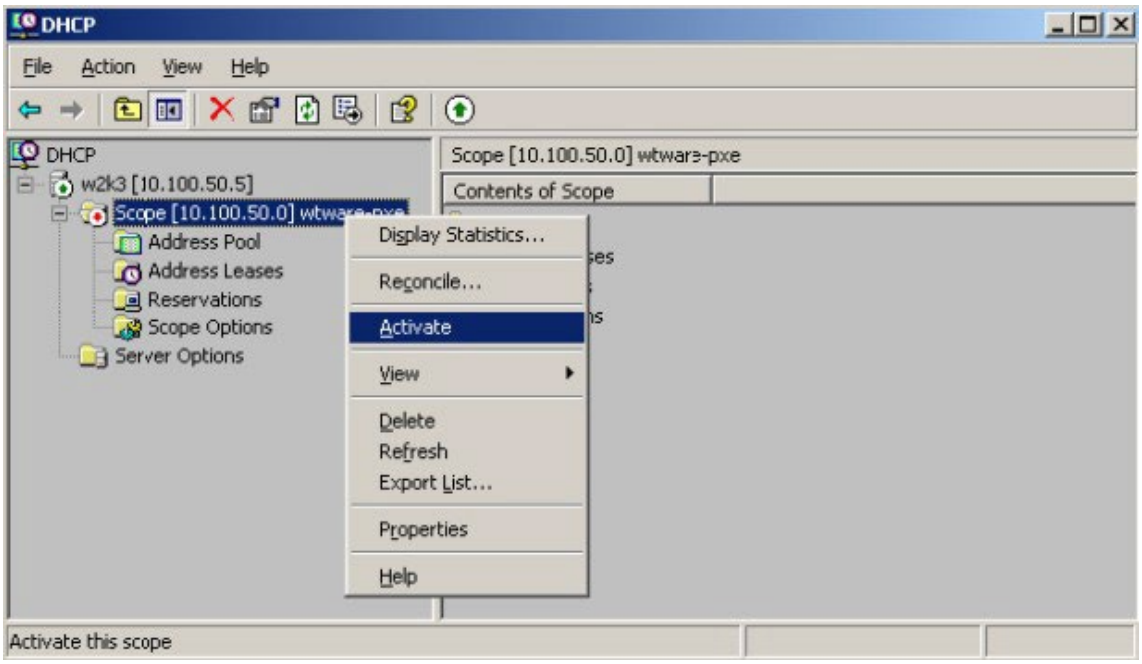
При настройке DHCP-сервера необходимо зарезервировать диапазон IP-адресов, выделяемых контроллерам системы. После чего привязать MAC-адреса контроллеров к IP-адресам из зарезервированного диапазона. Для этого (далее приведен пример настройки DHCP-сервера для системы *Windows XP*):

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



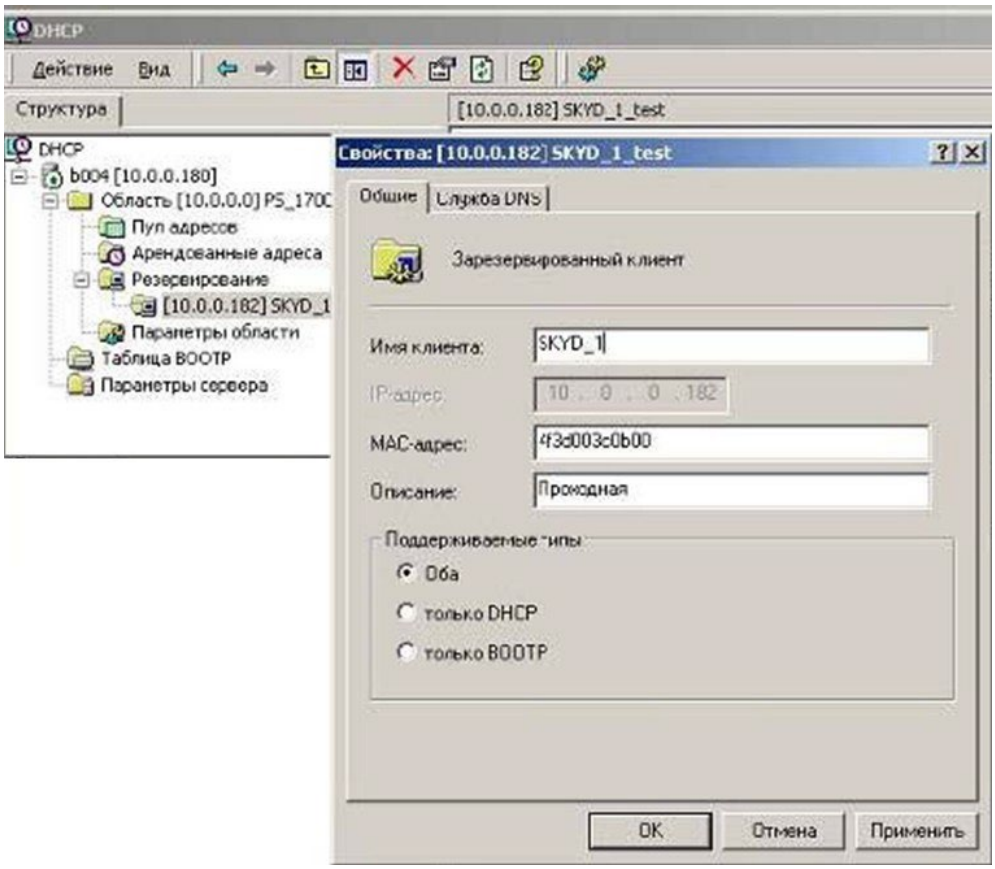
SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Произведите активацию области:



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

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



5. Выполните операцию для каждого контроллера системы.

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8.6. Настройка DHCP-сервера в ОС Linux

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

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

Пример варианта файла конфигурации:

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

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

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

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

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

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.7. Внешнее подключение контроллера к серверу *PERCo.Школа*

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

Внимание!

Данная функция возможна только для контроллеров ***CL15***, ***CL15.1***, ***CL15.3***, ***CL15.7***, ***CR11***, ***CR11.1***, ***CR02.9***, ***CT/L14***, ***CT/L14.1*** и для встроенных контроллеров ***CT13***, ***CT13.1*** электронных проходных.

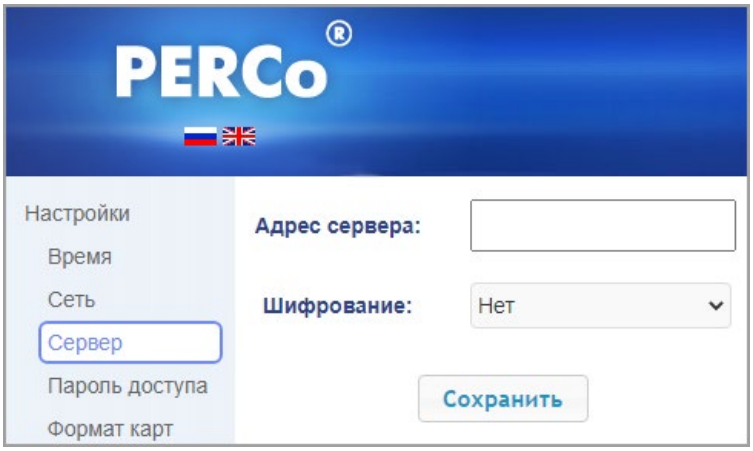
Для подключения контроллера к серверу ***PERCo.Школа*** по внешнему IP-адресу сервера:

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

Примечание:

Полное руководство по работе с Web-интерфейсом смотрите в руководствах по эксплуатации на контроллеры и электронные проходные.

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



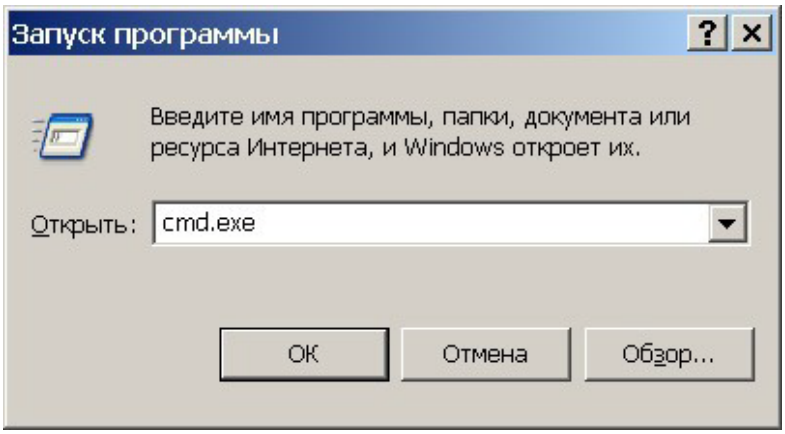
4. В открывшемся окне произведите необходимые изменения:
   - в поле **Адрес сервера** введите IP-адрес сервера, на котором установлена система ***PERCo.Школа***;
   - в параметре **Шифрование** задайте требуемый способ шифрования.
5. Нажмите кнопку **Сохранить**. Внесенные изменения будут сохранены.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8.8. Проверка связи между ПК и контроллером

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

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

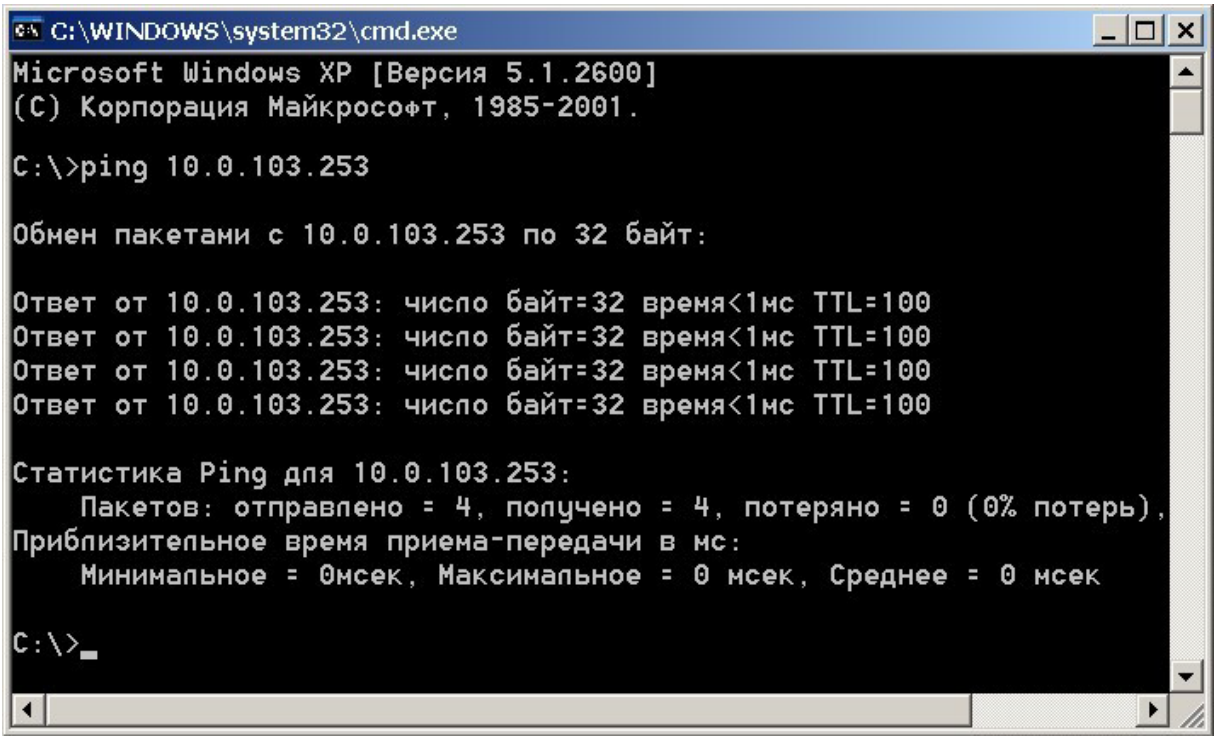


2. В открывшемся окне введите команду: **cmd.exe** и нажмите кнопку **ОК**.
3. Откроется окно интерфейса командной строки с заголовком:

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

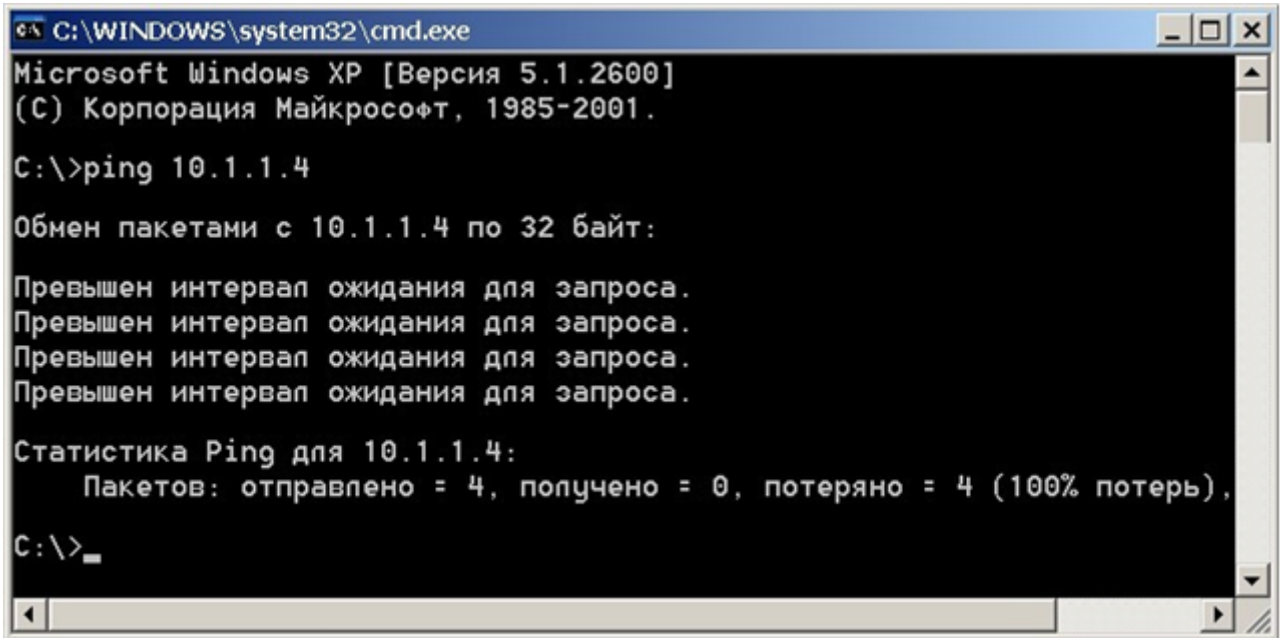
   `ping XX.XX.XX.XX`, где `XX.XX.XX.XX` – IP-адрес контроллера, с которым необходимо проверить связь (например 10.0.103.253).
5. Если связь будет установлена, то появится ответ следующего вида:

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



SEC.RU | Короткий путь к информации Скачано с sec.ru

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

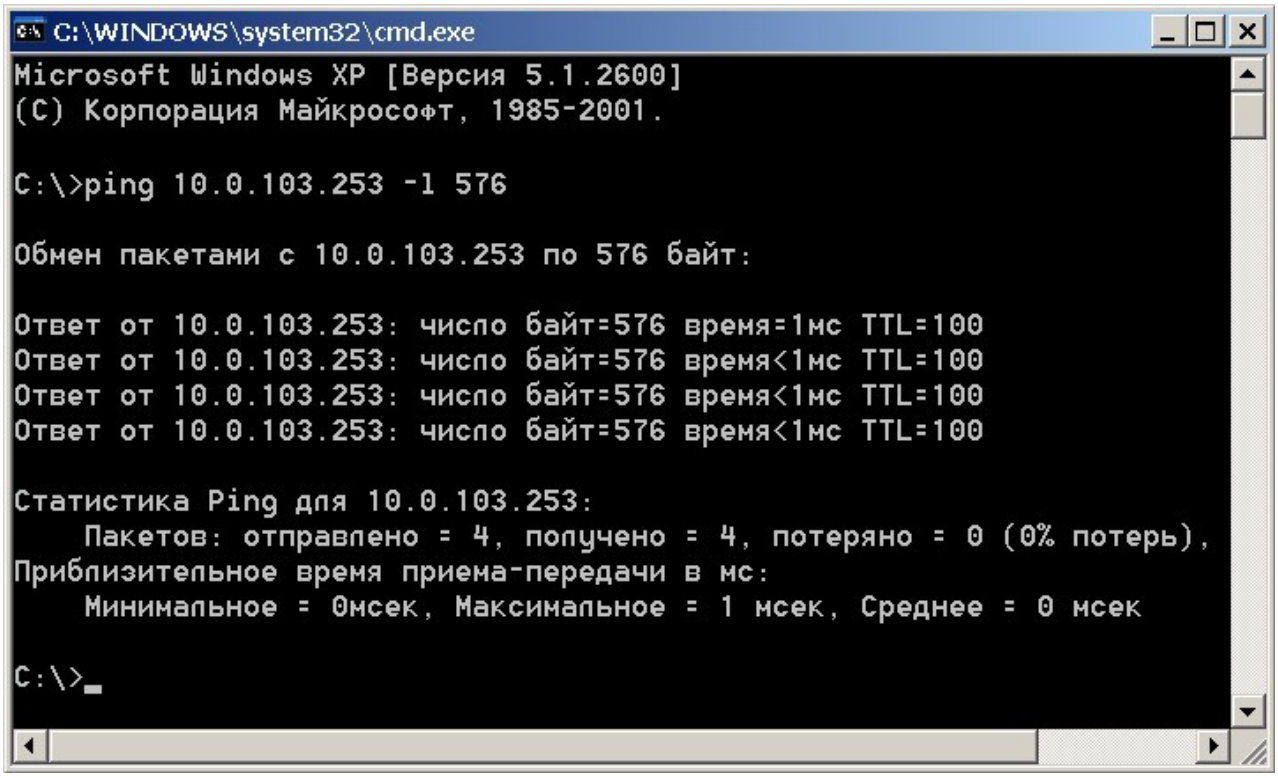


7. Контроллеры системы не поддерживают фрагментацию IP-пакетов. Поэтому необходимо удостовериться, что IP-пакеты на всем протяжении от сервера системы до контроллера не фрагментируются. Для этого введите ту же команду с ключом `-l` и указанием на размер отправляемого пакета данных, например, 576 байт:

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

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

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



SEC.RU | Короткий путь к информации
Скачано с sec.ru

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

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

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

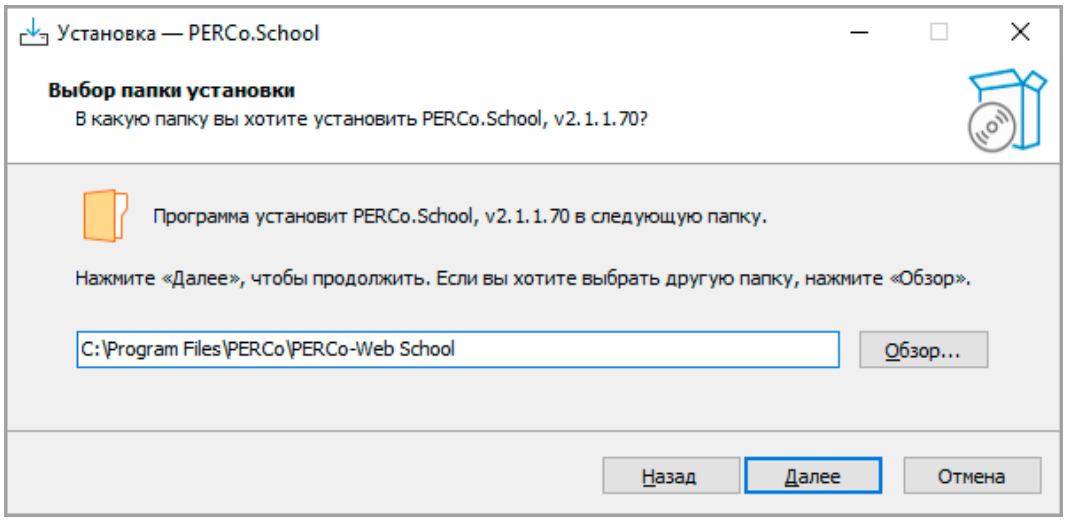
9. Установка системы

Внимание!

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

При установке системы придерживайтесь следующей последовательности действий:

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

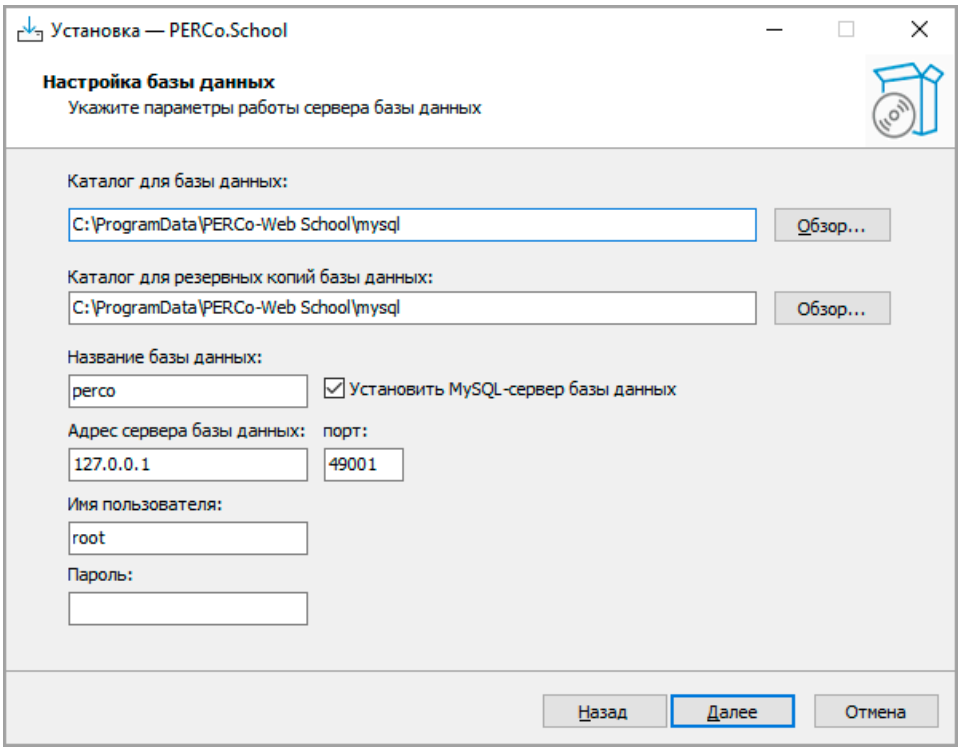


Для установки рекомендуется использовать папку, установленную по умолчанию. По умолчанию это *C:\Program Files\PERCo\PERCo-Web School*. Если необходимо, укажите другую папку или выберите ее, нажав кнопку **Обзор**. Для продолжения установки нажмите кнопку **Далее**.

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

Откроется новое окно:



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

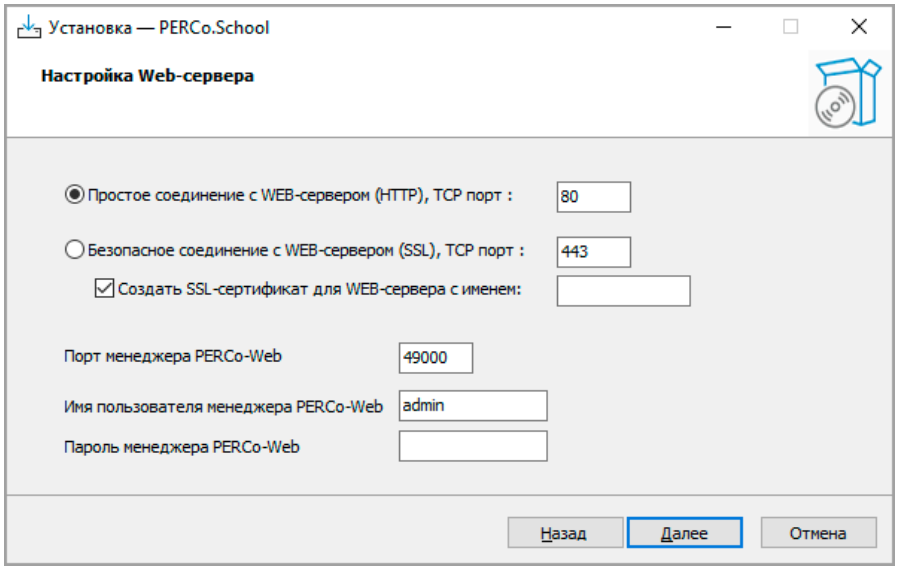
Примечание:

Если используется внешний MySQL-сервер, не входящий в дистрибутив, необходимо снять флажок у параметра **Установить MySQL-сервер** и указать учетные данные от необходимого сервера в соответствующих полях окна.

Примечание:

Для ОС *Astra Linux* используется СУБД PostgreSQL.

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



SEC.RU | Короткий путь к информации Скачано с sec.ru

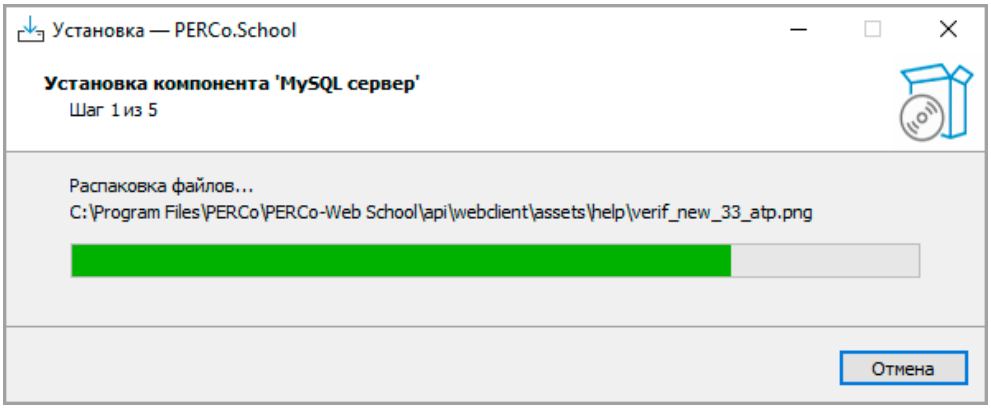
9. Произведите настройку сетевых параметров серверов системы. Для этого установите флажок **Простое соединение с WEB-сервером (HTTP), TCP** или **Безопасное соединение с WEB-сервером (SSL), TCP** и укажите свободный порт. Если указанный порт уже используется в системе, появится диалоговое окно. В окне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

Внимание!

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

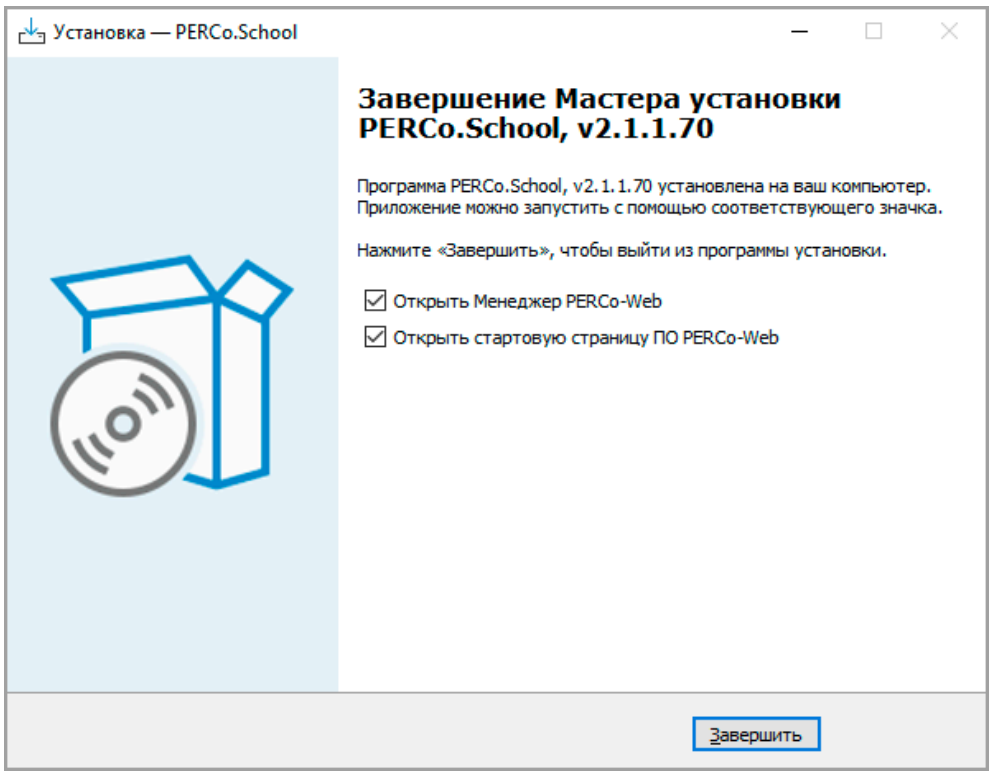
11. В поле **Порт менеджера PERCo-Web** укажите свободный порт для работы с **Менеджером системы безопасности PERCo-Web**. По умолчанию это порт: 49000. В полях **Имя пользователя менеджера PERCo-Web** и **Пароль менеджера PERCo-Web** необходимо указать данные учетной записи пользователя. Для продолжения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

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



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

SEC.RU | Короткий путь к информации Скачано с sec.ru



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

Примечание:

Для полного удаления всех модулей системы с ПК используйте стандартный компонент MS Windows *«Установка и удаление программ»*. Для запуска компонента выберите последовательно **Пуск > Параметры > Приложения**. В открывшемся окне выделите строку *«PERCo-Web School»* и нажмите кнопку **Удалить**.

Внимание!

Для установки версии ПО ***PERCo.Школа*** для ОС *Linux* необходимо открыть архив, скопировать установочный файл формата **.deb*, **.rpm*, и установить ПО ***PERCo.Школа*** согласно инструкции.

Для ОС *ROSA* при использовании *MariaDB* нужна версия *MariaDB 10.2* или выше. (*MariaDB* используется только в ОС *ROSA*).

SEC.RU | Короткий путь к информации Скачано с sec.ru

10. Управление лицензиями

Состав модулей ПО *PERCo.Школа*

Модуль ПО	Входящие в модуль разделы
PERCo-ES «Стандартный пакет ПО»	Разделы: **«Персонал»** с подразделами: • **«Сотрудники»**, • **«Подразделения»**, • **«Должности»**, • **«Дополнительные данные»**; **«Учащиеся»** с подразделами: • **«Ученики»**, • **«Классы»**; **«Бюро пропусков»** с подразделами: • **«Посетители»**, • **«Родственники»**, • **«Сотрудники»**, • **«Ученики»**; • **«Шаблоны доступа»**, • **«Дизайн пропуска»**, • **«Отчет по посетителям»**; **«Контроль доступа»** с подразделом: • **«Отчет о проходах»**, • **«Управление устройствами»**; • **«Отчет по доступу в помещения»**, • **«Выданные идентификаторы»** **«Администрирование»** с подразделами: • **«Конфигурация»**, • **«События системы»**, • **«Реакции на события»**, • **«Журнал уведомлений»**, • **«Задания»**, • **«Операторы»**, • **«Роли и права операторов»**, • **«Лицензии»**
PERCo-EM01 «УРВ и Расписание»	Все разделы, входящие в ***«Стандартный пакет ПО»***, а также добавляется: раздел **«Учет рабочего времени»** с подразделами: • **«Журнал отработанного времени»**, • **«Оправдательные документы»**, • **«Формирование табеля»**, • **«Отчеты по дисциплине»**, • **«Отчет УРВ»**, • **«Время присутствия»**, • **«Выданные документы»**; в раздел **«Персонал»** добавляется подраздел: • **«Графики работы»**; в раздел **«Учащиеся»** добавляются подразделы: • **«Журнал посещения уроков»**, • **«Время нахождения в школе»**, • **«Объяснительные»**, • **«Отчет по выданным объяснительным»**, • **«Отчет по учебной дисциплине»**; в раздел **«Расписание»** добавляются подразделы: • **«Расписание уроков»**, • **«Предметы»**,

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Модуль ПО	Входящие в модуль разделы
	• **«Расписание звонков»**, • **«Циклы обучения и праздничные дни»**; в раздел **«Контроль доступа»** добавляется подраздел: • **«Местонахождение»**
PERCo-EM02 «Верификация»	Все разделы, входящие в ***«Стандартный пакет ПО»***, а также добавляется: раздел **«Верификация»** с подразделами: • **«Верификация»**, • **«Конфигурация верификации»**; в раздел **«Контроль доступа»** добавляется подраздел: • **«Журнал верификации»**
PERCo-WM03 «Интеграция с 1С»	Модуль синхронизирует базы данных ***PERCo.Школа*** и ***1С:Предприятие***
PERCo-EM04 «Интеграция с внешними системами»	Модуль включает отображение документации по адресу: /dev для возможности работы с API
PERCo-EM05 «Мониторинг»	Все разделы, входящие в ***«Стандартный пакет ПО»***, а также добавляется: Раздел **«Мониторинг»** с подразделами: • **«Режим интерактивного плана»**, • **«Режим редактирования»**
PERCo-WM06 «Интеграция с TRASSIR»	Модуль позволяет провести интеграцию системы ***PERCo.Школа*** с видеоподсистемой ***Trassir***, что дает возможность использовать оборудование ***TRASSIR*** для видеонаблюдения и для распознавания пользователей по лицу / номеру транспортного средства
PERCo-WM07 «Интеграция с ИСО "Орион" (НВП "Болид")»	Модуль позволяет провести интеграцию системы ***PERCo.Школа*** с интегрированной системой охраны ***«Орион»***, что дает возможность управлять оборудованием охранно-пожарной сигнализации в интерфейсе системы ***PERCo.Школа***
PERCo-WM08 «Интеграция с Интеллект X» (ООО «Ай Ти Ви групп»)»	Модуль позволяет провести интеграцию системы ***PERCo.Школа*** с видеоподсистемой Интеллект X, что дает возможность использования ее для видеонаблюдения и для распознавания пользователей по лицу / номеру транспортного средства. В рамках модуля интеграции также поддерживается совместимость с видеоподсистемой ***Axxon Next***,

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-ES «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-EM01 Модуль «УРВ и Расписание»*** – позволяет вести учет рабочего времени сотрудников / учебного времени обучающихся, составлять отчеты о дисциплине труда и о школьной дисциплине. Лицензируется только совместно с ***PERCo-ES***.
- ***PERCo-EM02 Модуль «Верификация»*** – позволяет усилить контроль доступа на территорию организации за счет проведения оператором КПП процедуры верификации. Лицензируется только совместно с ***PERCo-ES***.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ***PERCo-WM03 «Интеграция с 1С»*** – позволяет синхронизировать базы данных ***PERCo.Школа*** и ***1С:Предприятие***. Модуль интеграции представляет собой приложение в виде файла внешней обработки для программного продукта ***«1С:Предприятие 8»***. Лицензируется только совместно с ***PERCo-ES*** и ***PERCo-EM01***.
- ***PERCo-EM04 «Интеграция с внешними системами»*** – позволяет включить отображение документации по адресу: /dev для возможности работы с API. Лицензируется только совместно с ***PERCo-ES***.
- ***PERCo-EM05 Модуль «Мониторинг»*** – позволяет организовать наблюдение за подконтрольной системе организацией, управлять устройствами системы в ручном режиме, а также создавать и редактировать план организации. Лицензируется только совместно с ***PERCo-ES***.
- ***PERCo-WM06 «Интеграция с TRASSIR»*** – позволяет провести интеграцию системы ***PERCo.Школа*** с видеоподсистемой ***Trassir***, что расширяет функциональные возможности ***PERCo.Школа*** за счет использования ресурсов видеоподсистемы ***Trassir***. Лицензируется только совместно с ***PERCo-ES***.
- ***PERCo-WM07 «Интеграция с ИСО "Орион" (НВП "Болид")»*** – позволяет провести интеграцию системы ***PERCo.Школа*** с интегрированной системой охраны ***«Орион»*** для создания комплексной системы безопасности, включающей СКУД и охранно-пожарную сигнализацию. Лицензируется только совместно с ***PERCo-ES***.
- ***PERCo-WM08 «Интеграция с Интеллект X»*** – позволяет провести интеграцию системы ***PERCo.Школа*** с видеоподсистемой ***Интеллект X*** (***Axxon Next)***, что расширяет функциональные возможности ***PERCo.Школа*** за счет создания системы видеонаблюдения и распознавания пользователей по лицу (по номеру ТС). Лицензируется только совместно с ***PERCo-ES***.

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

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

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 заявке необходимо указать:
   - MAC-адрес выбранного контроллера,
   - перечень приобретаемых модулей.
3. После получения лицензионного соглашения, содержащего коды активации модулей системы, необходимо ввести их в подразделе **«Лицензии»** раздела **«Администрирование»**.

Внимание!

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

11. Менеджер системы безопасности PERCo.Школа

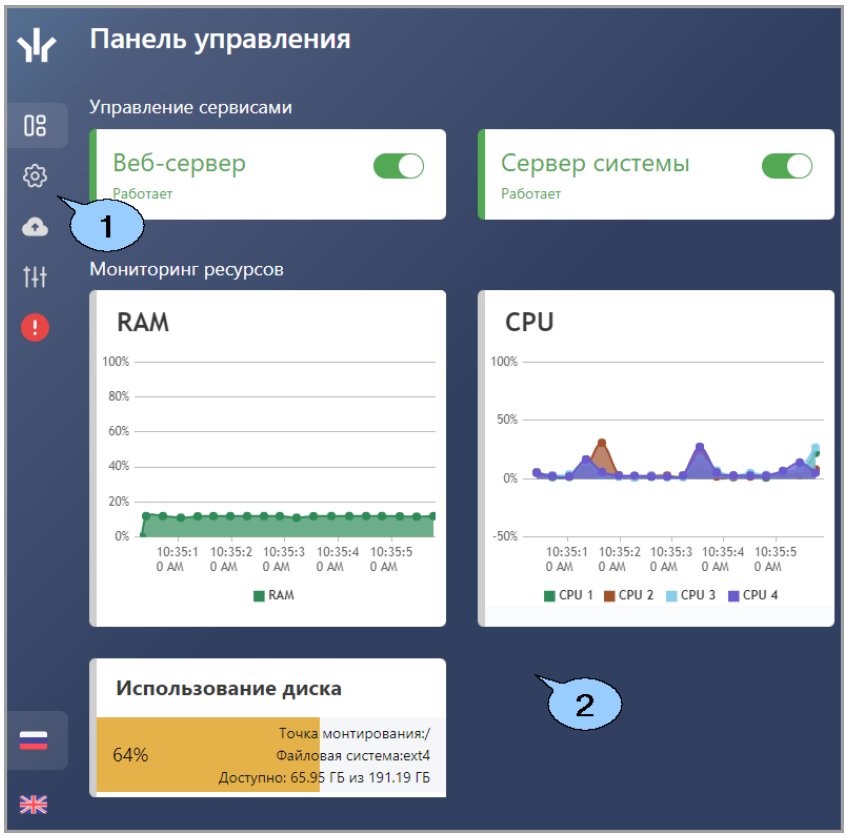
Окно **Менеджер PERCo-Web** открывается нажатием на иконку **Менеджер PERCo-Web** на рабочем столе или по IP-адресу в адресной строке браузера (например, http://127.x.x.x:49000/, где 127.x.x.x – IP-адрес компьютера с установленным сервером системы, :49000 – порт **Менеджера PERCo-Web**, указанный при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

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

Менеджер PERCo-Web предназначен для:

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

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



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

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

Примечание:

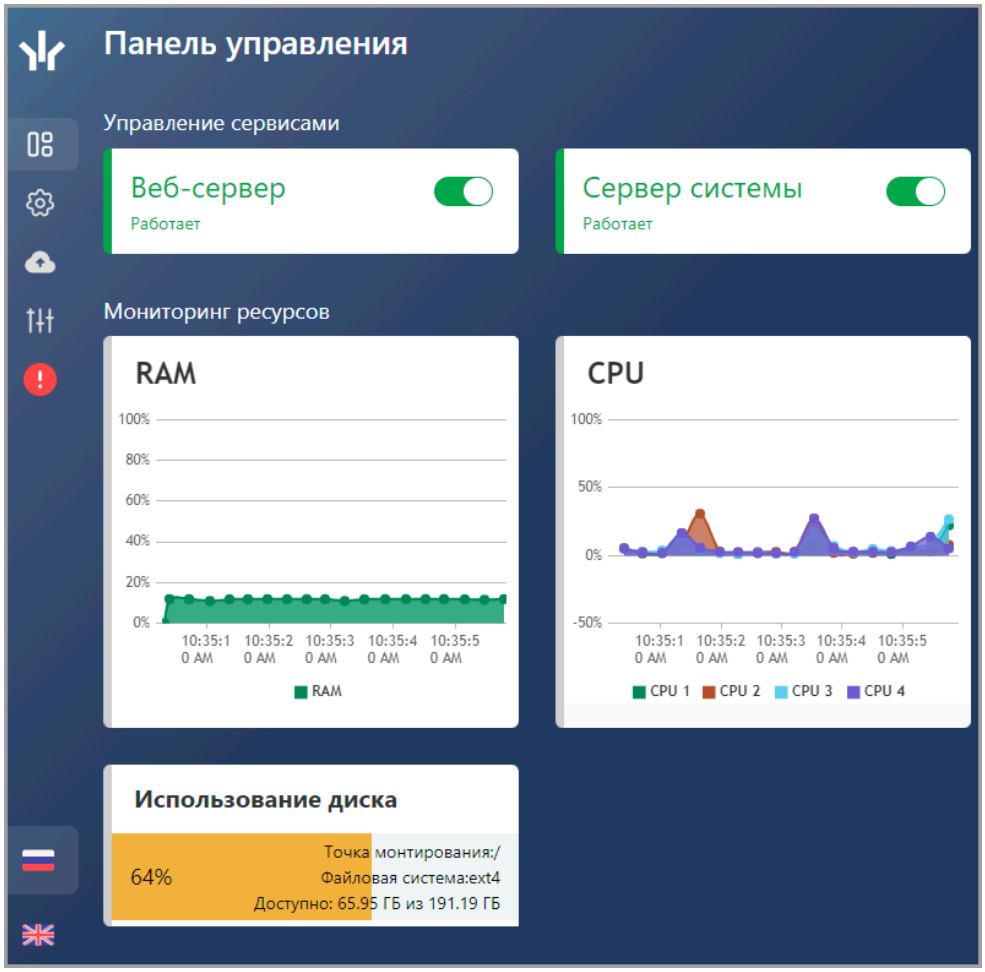
В системе предусмотрена возможность автоматического создания резервной копии БД по расписанию. Создание расписания производится в подразделе **«Задания»** раздела **«Администрирование»**.

SEC.RU | Короткий путь к информации Скачано с sec.ru

11.1. Вкладка «Мониторинг»

Вкладка **Мониторинг** (не путать с разделом **«Мониторинг»** системы ***PERCo.Школа***, он описывается в ***Руководстве пользователя модуля PERCo-EM05 «Мониторинг»***) предназначена для запуска и остановки серверов системы.

Вид вкладки:



Рабочая область вкладки содержит следующие элементы:

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

Примечание:

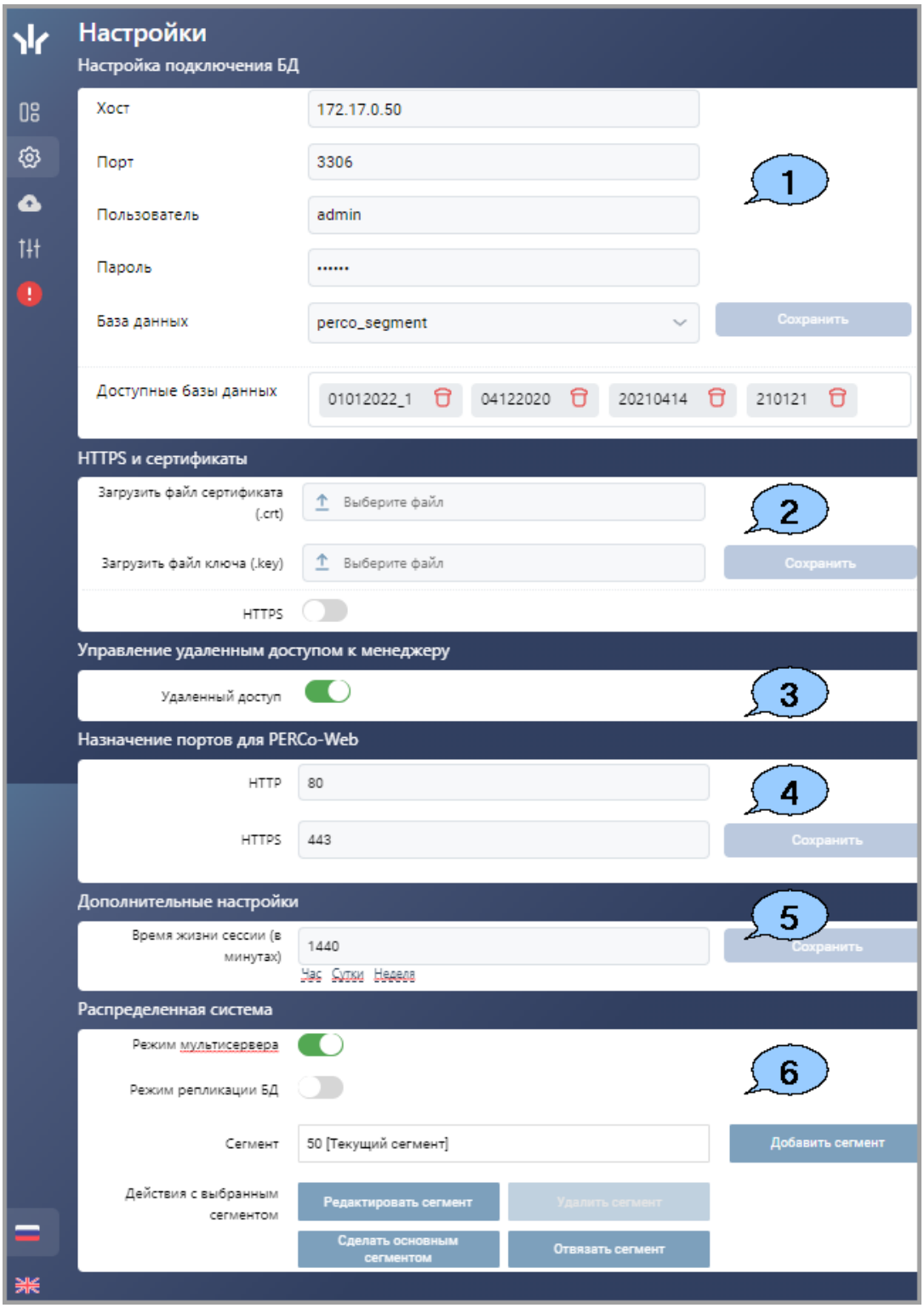
Состояние сервера отражает состояние памяти сервера и загрузки процессора всеми текущими процессами, то есть не только процессами ***PERCo.Школа***.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

11.2. Вкладка «Настройки»

Вкладка **Настройки** предназначена для управления БД системы, удаленным доступом, HTTPS и сертификатами, а также для настройки режима мультисервера.

Вид вкладки:



1. Панель **Настройка подключения БД** содержит следующие элементы:
   - **Хост** – в поле необходимо указать адрес сервера для созданной базы данных.
   - **Порт** – в поле необходимо указать порт для созданной базы данных.
   - **Пользователь** – в поле необходимо ввести имя пользователя для подключения к базе данных.
   - **Пароль** – в поле необходимо ввести пароль для указанного пользователя для подключения к базе данных.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **База данных** – в поле необходимо ввести название созданной базы данных. При вводе названия несозданной базы данных она будет создана автоматически.
- **Сохранить** – кнопка позволяет сохранить внесенные на панели изменения.
- **Доступные базы данных** – панель содержит список созданных БД и позволяет добавить новую.

2. Панель **HTTPS и сертификаты** содержит следующие элементы:
   - **Загрузить файл сертификата (.crt)** – панель позволяет загрузить публичный ключ. После загрузки файл будет храниться на сервере **Менеджера PERCo-Web**.
   - **Загрузить файл ключа (.key)** – панель позволяет загрузить секретный ключ сервера. После загрузки файл будет храниться на сервере **Менеджера PERCo-Web**.
   - **HTTPS** – переключатель позволяет включить / выключить шифрование данных. Чтобы включить SSL-шифрование, необходимо загрузить файл сертификата и файл ключа.
     При загрузке некорректных файлов ключа или сертификата при запуске **Менеджера PERCo-Web** отобразится ошибка:
     Не удалось корректно прочитать SSl-сертификат, менеджер работает по протоколу http.
   - Кнопка **Сохранить** сохраняет внесенные изменения.
3. Панель **Управление удаленным доступом к менеджеру** позволяет включить / выключить разрешение на подключение к **Менеджеру PERCo-Web** по удаленному доступу.
4. Панель **Назначение портов для PERCo-Web** позволяет указать, какой порт будет использоваться для обычного соединения (HTTP), а какой – для зашифрованного (HTTPS).
5. Панель **Дополнительные настройки** позволяет задать время жизни сессии в промежутке от 1 до 10080 минут (1 неделя). Эта настройка определяет время с момента последнего запроса, после которого токен авторизации станет недействительным, следовательно, по истечении заданного времени оператору потребуется заново пройти авторизацию в системе ***PERCo.Школа***, если с его стороны не было никакой активности.

Внимание!

После применения настройки **Время жизни сессии** необходимо перезагрузить Web-сервер.

Примечание:

Время жизни сессии не влияет на работу разделов «Верификация» и «Мониторинг». Если открыт один из этих разделов, сессия не будет прервана даже при отсутствии активности оператора.

6. Панель **Распределенная система** содержит следующие настройки:
   - Переключатель **Режим мультисервера** позволяет включить / выключить режим работы ***PERCo.Школа*** как распределенной системы.
   - Параметр **Режим репликации БД** должен быть активирован в случае использования системы репликации баз данных.
   - **Сегмент** – раскрывающийся список добавленных ранее сегментов.
   - Кнопка **Добавить сегмент** позволяет вызвать окно **Добавление сегмента**. В поле **Имя сегмента** введите наименование сегмента (например, «Начальная школа»), в поле **Хост** введите IP-адрес сегмента (т.е. локального сервера с установленной системой ***PERCo.Школа***).
   - Кнопка **Редактировать сегмент** позволяет вызвать окно **Редактирование сегмента** для изменения параметров выбранного сегмента.
   - Кнопка **Удалить сегмент** позволяет удалить выбранный сегмент.
   - Кнопка **Сделать основным сегментом** позволяет сделать выбранный сегмент основным. Благодаря этому связь с другими сегментами будет осуществляться через основной сегмент, а в событиях системы ***PERCo.Школа*** будет отображаться состояние связи с сегментами.
   - Кнопка **Привязать (Отвязать) сегмент** позволяет закрепить созданный сегмент за определенным сервером: после того, как сегменты будут созданы, необходимо зайти в ***Менеджер PERCo-Web*** с каждого сервера, в списке **Сегмент** выбрать сегмент с соответствующим IP-адресом и нажать кнопку **Привязать сегмент**.

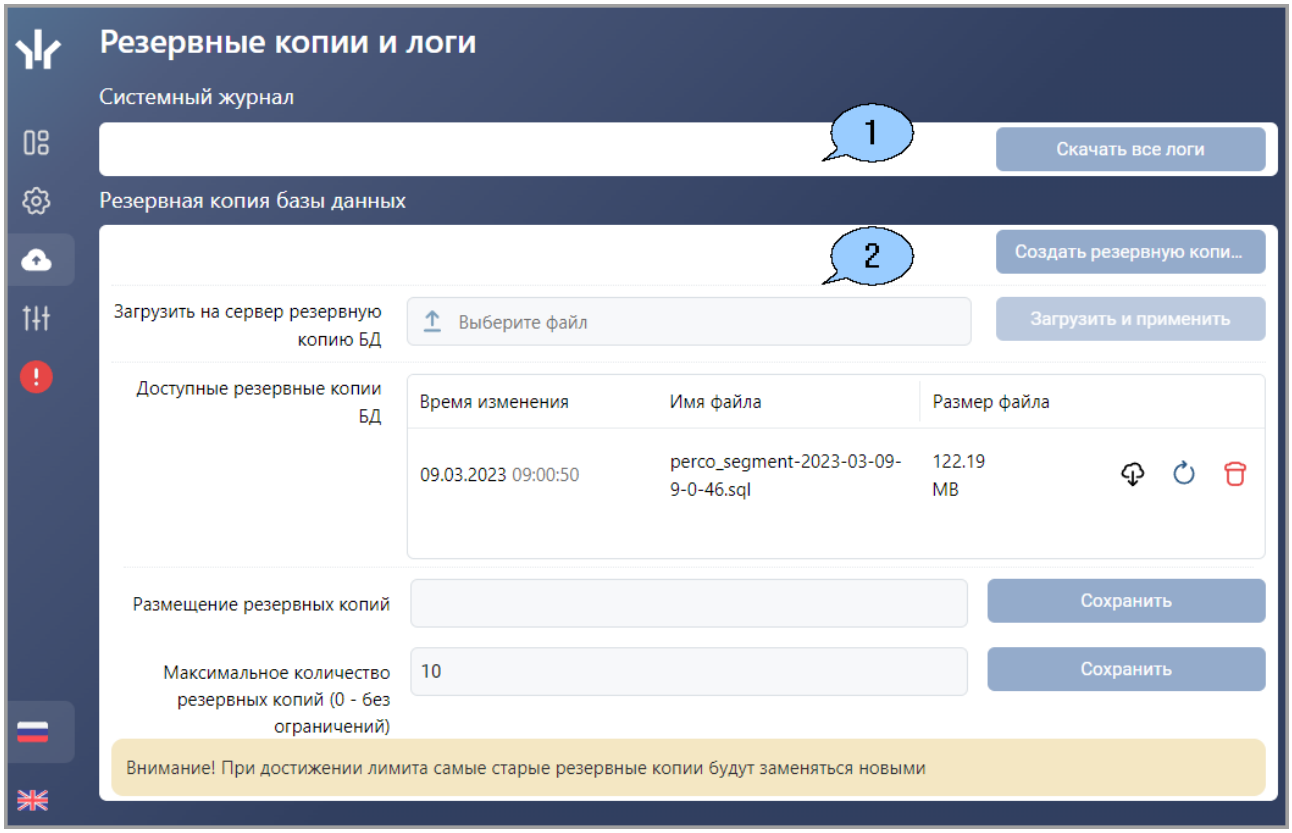
Подробнее о настройке ***PERCo.Школа*** для работы в режиме распределенной системы.

SEC.RU | Короткий путь к информации Скачано с sec.ru

11.3. Вкладка «Резервные копии и логи»

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

Вид вкладки:



Рабочая область вкладки содержит следующие элементы:

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

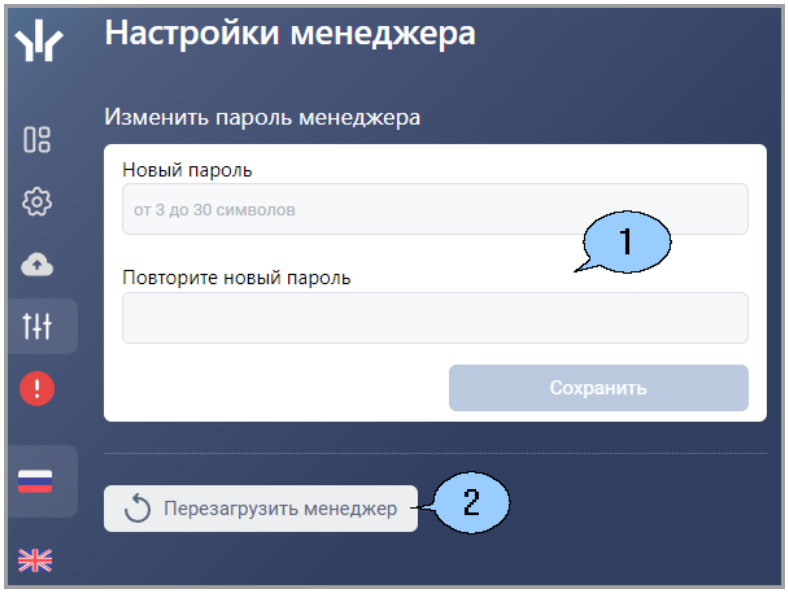
Внимание!

При достижении лимита самые старые резервные копии будут заменяться новыми.

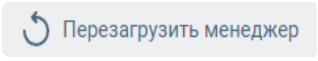
SEC.RU | Короткий путь к информации Скачано с sec.ru

11.4. Вкладка «Настройки менеджера»

Вкладка **Настройки менеджера** предназначена для изменения пароля. Вид вкладки:



Рабочая область вкладки содержит следующие элементы:

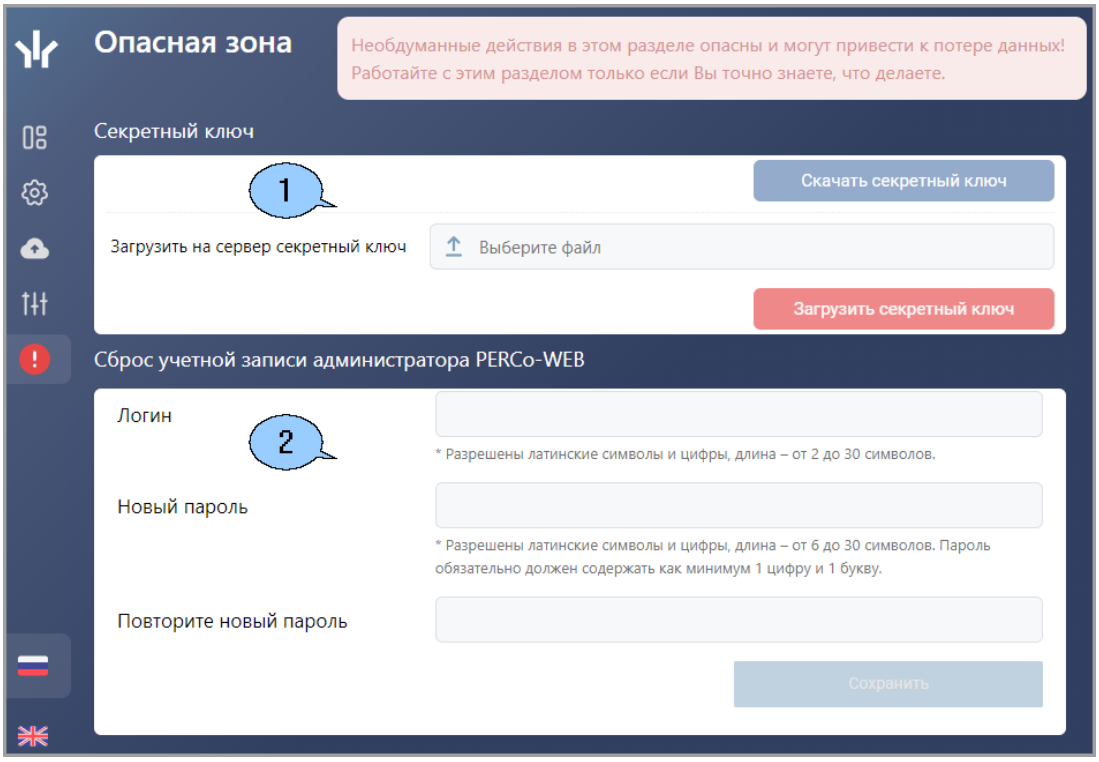
1. Панель **Изменить пароль менеджера** позволяет указать новый пароль для **Менеджера системы PERCo-Web**.
2. Кнопка 

позволяет перезапустить **Менеджер системы PERCo-Web**.

11.5. Вкладка «Опасная зона»

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

Вид вкладки:



Рабочая область вкладки содержит следующие элементы:

1. Панель **Секретный ключ**. Это ключ шифрования приватных данных, он генерируется при первом запуске системы ***PERCo.Школа*** и больше никогда не меняется. При утере

SEC.RU | Короткий путь к информации Скачано с sec.ru

ключа все пароли и зашифрованные данные становятся недоступными. После установки системы ***PERCo.Школа*** ключ необходимо скачать и сохранить в недоступном месте.

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

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

Внимание!

Необдуманные действия в этом разделе опасны и могут привести к потере данных! Работайте с этим разделом только если Вы точно знаете, что делаете.

SEC.RU | Короткий путь к информации Скачано с sec.ru

12. Режим распределенной системы

Распределенная система – это дополнительный режим работы ***PERCo.Школа***, предназначенный для:

- объединения географически удаленных объектов в единую систему;
- повышения уровня отказоустойчивости работы системы в сетях с большим количеством контроллеров.

Использование режима распределенной системы позволяет получить отказоустойчивую структуру, состоящую из несколько серверов ***PERCo.Школа***, которые взаимодействуют с централизованной базой данных.

Для создания распределенной системы сеть организации необходимо разделить на сегменты. Каждый сегмент – это локальный сервер, который синхронизируется с другими в режиме реального времени. Таким образом нагрузка распределяется равномерно и не зависит от удаленности сервера.

Примечание:

Для географически разделенных сетей сегментами могут быть подсети каждого из филиалов или подразделений, например: «Дошкольное отделение», «Начальная школа», «Средняя школа», «Старшая школа» и т.д. Для крупных организаций с большим количеством контроллеров – это разделение на логические подсети и распределение контроллеров по этим подсетям, например: часть контроллеров находится в подсети 172.17.*.*, другая часть – в подсети 10.0.*.*.

В каждом сегменте устанавливается сервер системы ***PERCo.Школа***, который работает с контроллерами только своего сегмента и передает информацию в централизованную базу данных. Каждый сервер системы ***PERCo.Школа*** из любого сегмента может получать информацию от всех остальных серверов системы ***PERCo.Школа*** в других сегментах.

12.1. Настройка PERCo.Школа для работы в режиме распределенной системы

Для работы в режиме распределенной системы необходимо:

1. Определить, как будет разделена сеть организации и что будет выделено в качестве сегментов – группы контроллеров, географически удаленные объекты и т.д.
2. На каждом сегменте установить сервер системы ***PERCo.Школа***.

Примечание:

На всех серверах (сегментах) ***PERCo.Школа*** рекомендуется использовать одинаковые сборки системы.

3. Выбрать способ работы с базой данных и произвести соответствующую настройку.
4. Создать необходимые сегменты в ***PERCo.Школа***.
5. Связать локальные сервера организации с созданными в системе ***PERCo.Школа*** сегментами.

Внимание!

Сегменты рекомендуется настроить на работу по одному и тому же протоколу (предпочтительнее – https). Для этого в ***Менеджере PERCo-Web*** на вкладке **Настройки** отключите или включите шифрование данных у всех сегментов. В противном случае некоторые функции могут выполняться некорректно.

12.1.1. Подключение базы данных

Распределенная система ***PERCo.Школа*** поддерживает следующие способы работы с базой данных:

1. Использование сторонней системы репликации баз данных. При выборе этого способа придерживайтесь следующей последовательности действий:
   - на одном из сегментов создайте базу данных;

SEC.RU | Короткий путь к информации Скачано с sec.ru

- откройте вкладку **Резервные копии и логи** ***Менеджера PERCo-Web***, создайте и сохраните резервную копию созданной БД;
- распространите сохраненную резервную копию на все остальные сегменты;
- откройте вкладку **Опасная зона** ***Менеджера PERCo-Web*** и скачайте секретный ключ;
- Распространите секретный ключ на все остальные сегменты. В результате на всех серверах должен быть загружен один и тот же секретный ключ;
- с помощью сторонней утилиты свяжите все базы данных репликацией. Таким образом любой сегмент может продолжать автономную работу со своей копией БД при потере связи с другими;
- на вкладке **Настройки** ***Менеджера PERCo-Web*** включите режим мультисервера и активируйте параметр **Режим репликации БД**.

Примечание:

Пример настройки распределенной системы приведен в приложении 1.

2. Использование общей базы данных. При выборе этого способа придерживайтесь следующей последовательности действий:
   - на одном из сегментов создайте базу данных;
   - откройте вкладку **Опасная зона** ***Менеджера PERCo-Web*** и скачайте секретный ключ;
   - распространите сохраненный секретный ключ на все остальные сегменты. В итоге на всех серверах должен быть загружен один и тот же секретный ключ;
   - подключитесь к созданной БД с остальных сегментов, указав хост, порт, имя пользователя, пароль и название БД на вкладке **Настройки** ***Менеджера PERCo-Web***.

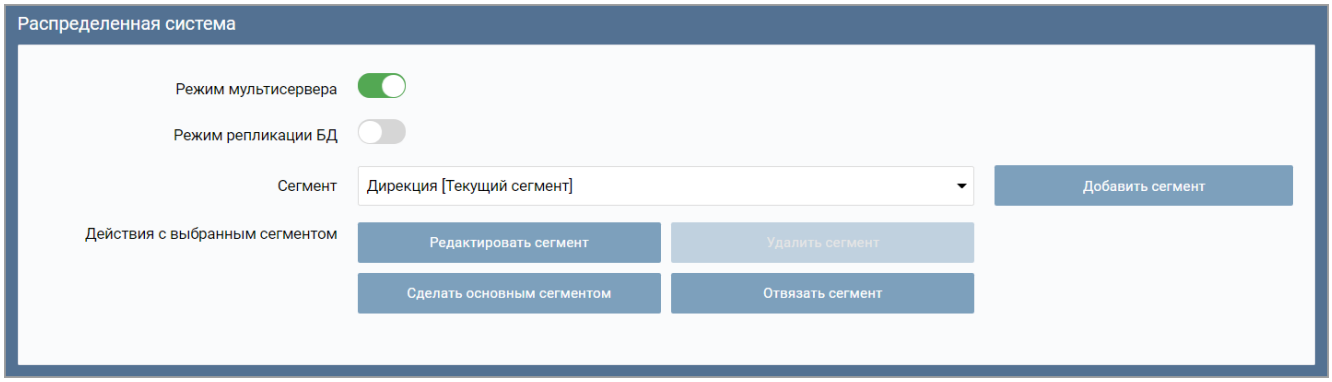
Внимание!

Если связь с базой данных будет нарушена, сервер ***PERCo.Школа*** прекратит работу.

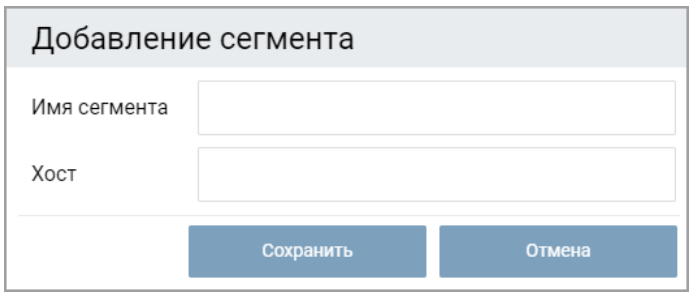
12.1.2. Создание сегментов в PERCo.Школа

Для создания сегментов в ***PERCo.Школа***:

1. Убедитесь, что на всех серверах подключена и настроена база данных.
2. С одного из серверов откройте ***Менеджер PERCo-Web*** и перейдите на вкладку **Настройки**.
3. На панели **Распределенная система** активируйте режим мультисервера. После этого на панели появятся дополнительные настройки:



4. С помощью кнопки **Добавить сегмент** вызовите окно **Добавление сегмента**:

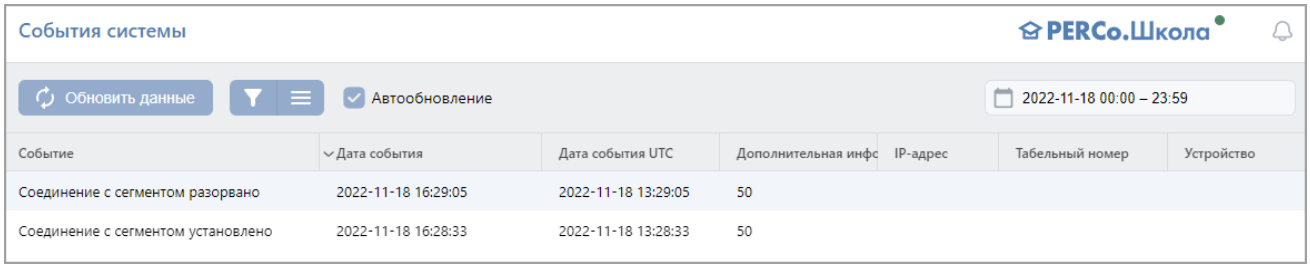


SEC.RU | Короткий путь к информации
Скачано с sec.ru

- в поле **Имя сегмента** введите наименование создаваемого сегмента, например, «Начальная школа»;
- в поле **Хост** укажите IP-адрес сегмента (т.е. локального сервера с установленной системой ***PERCo.Школа***);
- нажмите кнопку **Сохранить**.

Таким образом добавьте все нужные сегменты.

5. Сделайте один из сегментов основным с помощью соответствующей кнопки на панели **Распределенная система**. Благодаря этому связь с сегментами будет осуществляться через основной сегмент, а в событиях системы ***PERCo.Школа*** будет отображаться состояние связи:



Примечания:

После выбора основного сегмента необходимо перезапустить Веб-сервер и Сервер системы.
При остановке сервера системы на основном сегменте связь с другими сегментами не пропадает.

12.1.3. Закрепление сегментов за серверами

Поочередно с каждого сервера, для которого в ***PERCo.Школа*** был создан сегмент, выполните следующие действия:

1. Откройте ***Менеджер PERCo-Web*** и произведите необходимые настройки:
   - на вкладке **Настройки** на панели **Распределенная система** активируйте режим мультисервера и выберите в выпадающем списке сегмент с Вашим IP-адресом. Используя кнопку **Привязать сегмент**, закрепите выбранный сегмент за сервером;
   - на вкладке **Мониторинг** перезагрузите сервер системы и Web-сервер.
2. В системе ***PERCo.Школа*** перейдите на вкладку **Устройства** подраздела **«Конфигурация»** раздела **«Администрирование»**. Используя кнопку **Поиск устройств**, найдите и добавьте необходимые устройства. При добавлении устройство будет автоматически присвоено сегменту, с которого выполнялся поиск. При необходимости откройте параметры устройства и измените сегмент.

Примечания:

- При добавлении камеры, сервера ***TRASSIR***, ИСО ***«Орион» (Bolid)*** вручную укажите сегмент в соответствующем поле.
- При добавлении шлюза или составного объекта в их параметрах будут отображены только устройства, привязанные к сегменту, с которого происходит добавление шлюза или составного объекта.
- При активации режима распределенной системы ранее существовавшие помещения и устройства будут находиться вне сегментов, поэтому их необходимо переместить в соответствующий сегмент.

3. На вкладке **Система** подраздела **«Конфигурация»** раздела **«Администрирование»** укажите путь к каталогу для записи видеофайлов.

Внимание!

У каждого сегмента должен быть свой каталог для записи видеофайлов.

4. При необходимости настройте реакции на события и задания для сегмента.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

12.2. Особенности работы в режиме распределенной системы

- В разделе **«Мониторинг»** отображаются все сегменты, с которыми есть связь (раздел доступен только при активированной лицензии на модуль ПО ***PERCo-EM05 «Мониторинг»***).
- В разделе **«Верификация»** (доступен только при активированной лицензии на модуль ПО ***PERCo-EM02 «Верификация»***) запуск процесса верификации возможен только с используемого сегмента.
- В подразделе **«Журнал верификации»** раздела **«Контроль доступа»** отображаются события верификации со всех сегментов (подраздел доступен только при активированной лицензии на модуль ПО ***PERCo-EM02 «Верификация»***).
- В подразделе **«События системы»** раздела **«Администрирование»** отображаются события со всех сегментов. При большом количестве событий их загрузка может занять некоторое время.

SEC.RU | Короткий путь к информации Скачано с sec.ru

13. Интеграция с 1С:Предприятие 8

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

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

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

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

Для проведения интеграции:

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

Примечание:

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

14. API PERCo.Школа

Модуль предназначен для помощи разработчикам в создании сторонних приложений на базе готовых решений системы ***PERCo.Школа***.

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

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

В модуль можно перейти тремя способами:

1. Используя панель навигации, перейдите в раздел **«Администрирование»**. Откройте подраздел **«Лицензии»** и выберите лицензию ***PERCo-EM04 «Интеграция с внешними системами»***. В открывшемся окне перейдите по ссылке ***Документация***.
2. В адресной строке добавьте к IP-адресу сервера */dev*. Например, *https://172.17.0.xx/dev*.
3. После активации лицензии ***PERCo-EM04 «Интеграция с внешними системами»***

   на панели навигации появится раздел ***«Документация»***. Перейдите в данный раздел и откройте подраздел ***«Документация SDK»***.

Модуль имеет следующий вид:



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

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

15. Предварительная настройка

При подготовке системы к работе придерживайтесь следующей последовательности действий:

1. Войдите в систему, используя 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 учетной записи.

2. Используя панель навигации, перейдите в раздел  **«Администрирование»**:
   - Откройте подраздел **«Лицензии»** и активируйте необходимые пакеты и модули ПО, при необходимости введите приобретенные лицензионные ключи.
   - Откройте подраздел **«Конфигурация»**:
     - выберите регион и формат отображения дат в системе (вкладка **«Система»**);
     - настройте параметры учебного года;
     - произведите поиск и добавление контроллеров в конфигурацию системы (вкладка **«Устройства»**);
     - создайте список помещений школы (вкладка **«Помещения»**);
     - привяжите контроллеры к помещениям.
   - Откройте подраздел **«Роли и права операторов»**, создайте необходимые роли операторов и установите для них полномочия.

3. В разделе  **«Бюро пропусков»** (см. *Руководство пользователя* ***PERCo-ES***):
   - Откройте подраздел **«Шаблоны доступа»**.
     - при необходимости добавьте временные критерии доступа и отредактируйте праздничное расписание доступа (вкладка **«Временные критерии доступа»**);
     - создайте шаблоны доступа для сотрудников школы, учеников, родственников учеников и посетителей. При создании шаблона для каждого помещения устанавливаются индивидуальные права и критерии доступа (вкладка **«Шаблоны»**).

4. В разделе  **«Персонал»**:
   - Откройте подраздел **«Подразделения»** (см. *Руководство пользователя* ***PERCo-ES***) и создайте список структурных подразделений школы. Для каждого подразделения укажите данные, которые будут автоматически устанавливаться сотрудникам и посетителям подразделения.
   - Откройте подраздел **«Должности»** и создайте список должностей школы (см. *Руководство пользователя* ***PERCo-ES***).
   - При необходимости в подразделе **«Дополнительные данные»** (см. *Руководство пользователя* ***PERCo-ES***) создайте поля для ввода дополнительных текстовых и графических данных.
   - При работе с УРВ (см. *Руководство пользователя* ***PERCo-EM01***):
     - в подразделе **«Графики работы»** создайте графики работы для сотрудников учебного заведения. Укажите для каждого графика регистрирующие помещения и параметры составления отчетов по дисциплине труда.

5. При работе с расписанием уроков в разделе  **«Расписание»** (см. *Руководство пользователя* ***PERCo-EM01***)
   - Откройте подраздел **«Циклы обучения и праздничные дни»** и отредактируйте календарь учебных циклов и календарь праздничных дней на учебный год;
   - В подразделе **«Расписание звонков»** создайте список расписаний звонков.

6. В разделе  **«Учащиеся»** (см. *Руководство пользователя* ***PERCo-ES***):
   - Откройте подраздел **«Классы»** и настройте данные параллелей – укажите для каждой параллели цикл обучения и расписание звонков. Создайте список классов учебного заведения. Для каждого класса укажите данные, которые будут автоматически устанавливаться ученикам класса.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7. При работе с расписание уроков в разделе  **«Расписание»** (см. *Руководство пользователя **PERCo-EM01***):
   - Откройте подраздел **«Предметы»** и создайте список учебных предметов, изучаемых в учебном заведении;
   - Откройте подраздел **«Расписание уроков»** и создайте расписание уроков для каждого класса.
8. В разделе  **«Бюро пропусков»** (см. *Руководство пользователя **PERCo-ES***):
   - Откройте подраздел **«Дизайн пропуска»** и создайте шаблоны дизайна пропусков сотрудников, учеников, родственников учеников и посетителей.
9. В разделе  **«Персонал»** (см. *Руководство пользователя **PERCo-ES***):
   - Откройте подраздел **«Сотрудники»** и создайте список сотрудников школы. Для каждого сотрудника:
     – заполните учетную карточку (укажите ФИО, подразделение, должность, график работы и т.д.);
     – добавьте фотографию;
     – выдайте карту доступа (идентификатор) и установите шаблон доступа. При необходимости распечатайте пропуск (см. *Руководство пользователя **PERCo-ES***).
10. В разделе  **«Учащиеся»** (см. *Руководство пользователя **PERCo-ES***):
    - Откройте подраздел **«Ученики»** и создайте список учеников школы. Для каждого ученика:
      – заполните учетную карточку (укажите ФИО, класс, группу класса и т.д.);
      – добавьте фотографию;
      – выдайте карту доступа (идентификатор) и установите шаблон доступа. При необходимости распечатайте пропуск (см. *Руководство пользователя **PERCo-ES***).
11. В разделе  **«Администрирование»** откройте подраздел **«Операторы»** и создайте учетные записи для операторов системы, назначьте им созданные ранее роли и выдайте права на разделы.
12. В разделе  **«Бюро пропусков»** (см. *Руководство пользователя **PERCo-ES***):
    - Откройте подраздел **«Шаблоны доступа»**, перейдите на вкладку **Комиссионирование** и при необходимости укажите для контроллеров тех сотрудников, чьи карты доступа будут являться комиссионирующими.
13. Настройте функции контроля зональности доступа карт в системе (*Antipass* и *Global Antipass*).

SEC.RU | Короткий путь к информации Скачано с sec.ru

16. Функции Antipass и Global Antipass

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

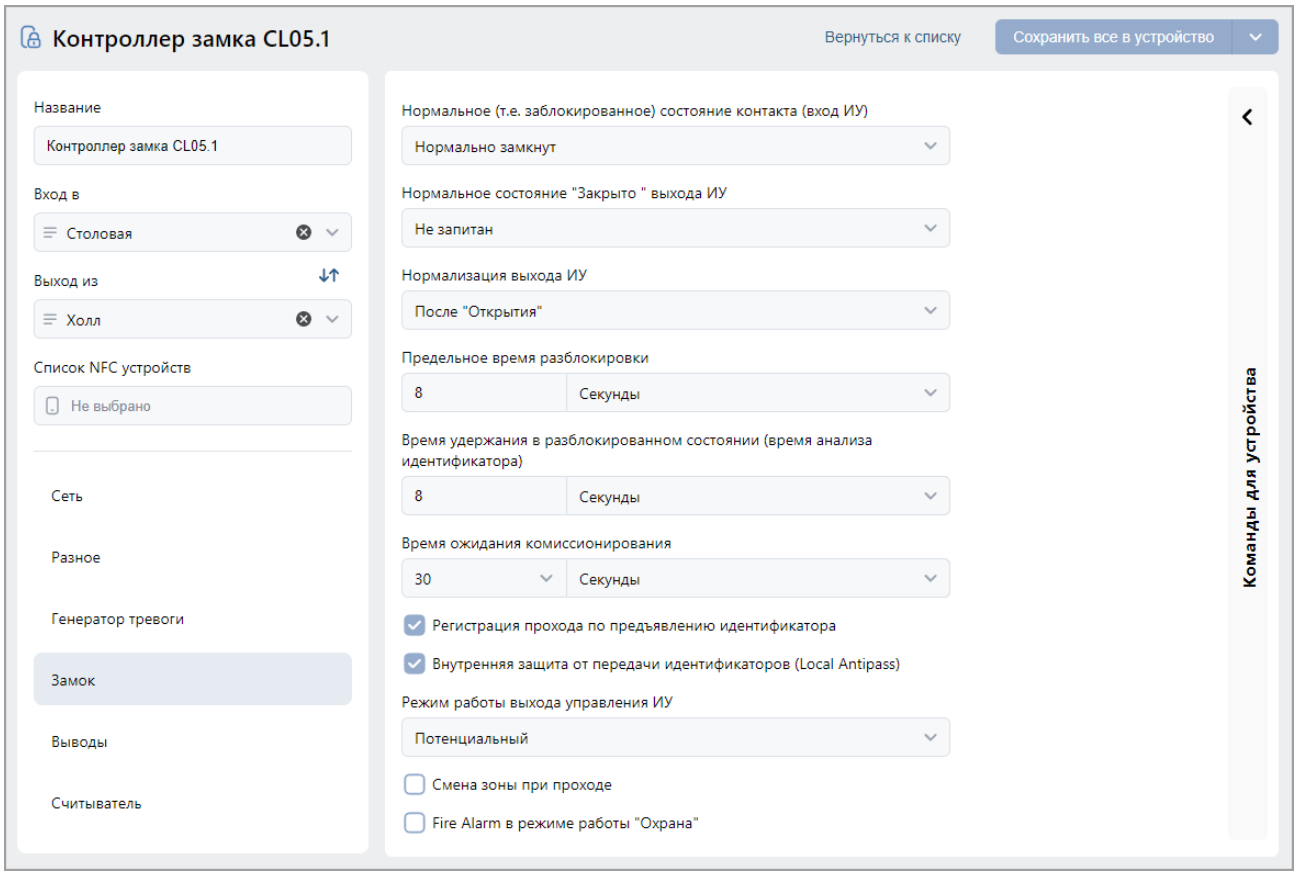
Функция Antipass

Примечание:

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

Для включения / отключения функции контроля зональности:

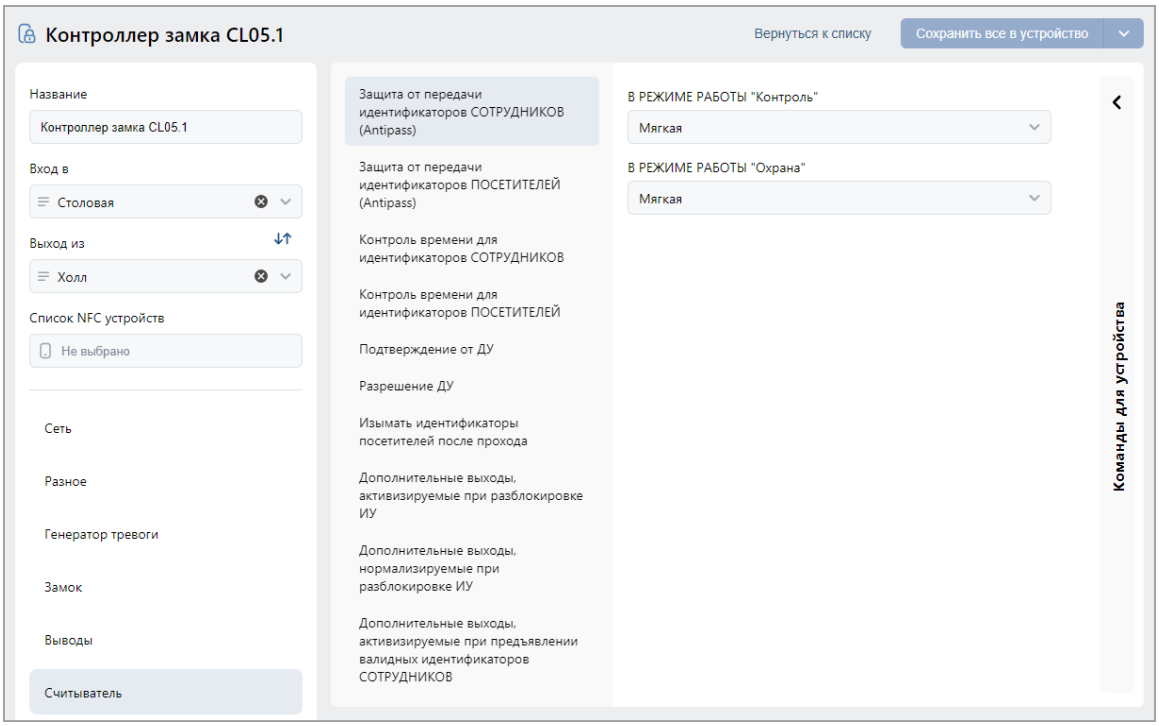
1. Используя панель навигации, перейдите в раздел **«Администрирование».**
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **Устройства**.
4. В рабочей области страницы выберите контроллер, для которого необходимо включить функцию контроля зональности.
5. Нажмите кнопку **Редактировать**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



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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

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



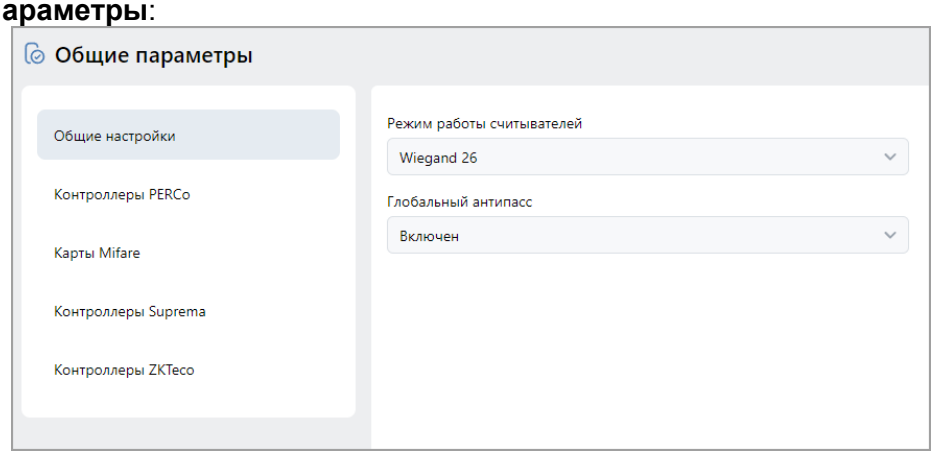
В рабочей области окна независимо для сотрудников (учеников, родственников учеников) и посетителей установите жесткий или мягкий режим контроля зональности при различных РКД.

9. Нажмите кнопку **Сохранить все в устройство**, измененные параметры будут переданы в контроллер.

Функция Global Antipass

Для включения / отключения функции глобального контроля зональности:

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



6. Для включения / отключения функции глобального контроля зональности в выпадающем списке **Глобальный антипасс** выберите **Включен** / **Отключен**.
7. Нажмите кнопку **Сохранить все в устройство**, измененные параметры будут переданы в контроллеры системы.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

17. Раздел «Администрирование»

Раздел предназначен для организации АРМ сотрудника организации, 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.

17.1. Подраздел «Конфигурация»

В подразделе доступны следующие вкладки:

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

Вкладка **Устройства** предназначена для:

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

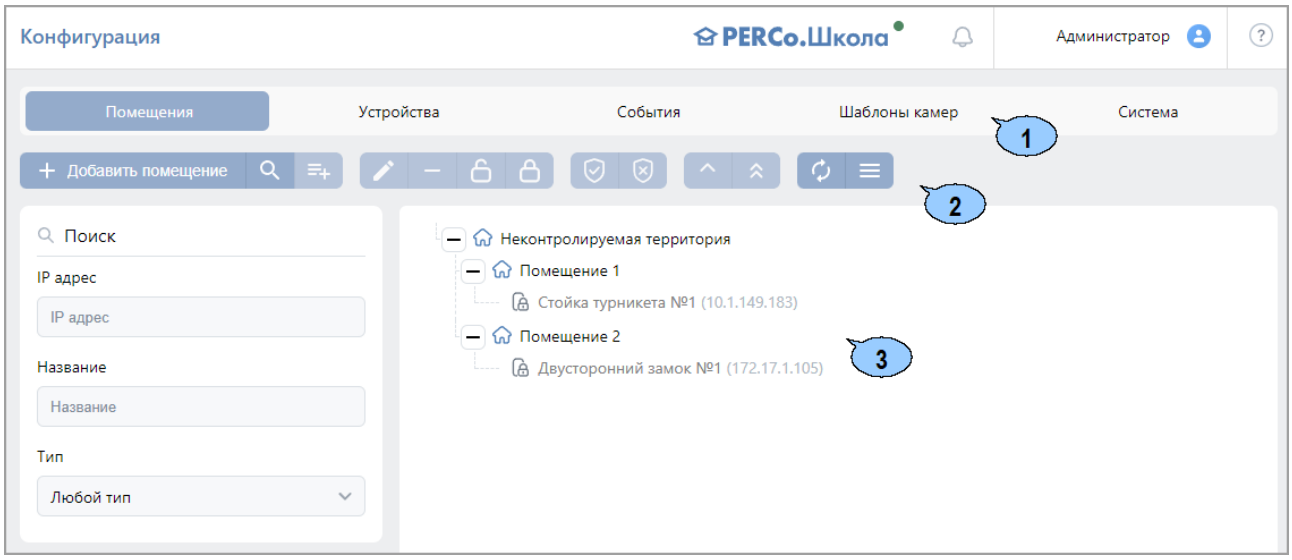
Вкладка **События** предназначена для переименования событий, регистрируемых устройствами системы.

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

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

17.1.1. Вкладка «Помещения»

Страница вкладки имеет следующий вид:



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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

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

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

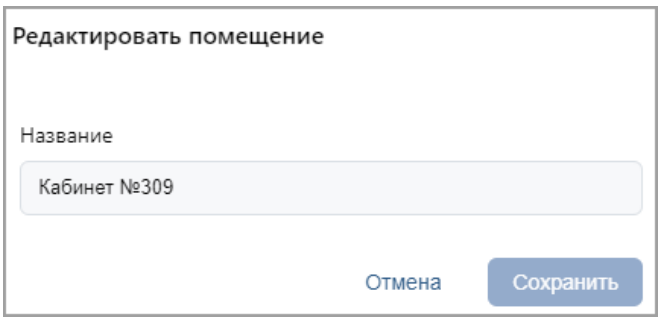
Примечание:

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

17.1.1.1. Создание списка помещений

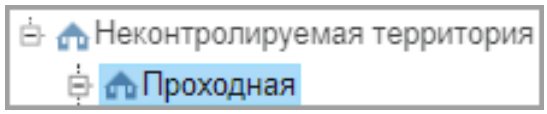
Для создания списка помещений:

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



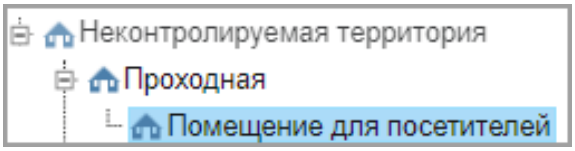
SEC.RU | Короткий путь к информации
Скачано с sec.ru

5. В открывшемся окне введите название нового помещения и нажмите кнопку **Сохранить**. При работе в режиме распределенной системы также укажите сегмент. Окно будет закрыто, помещение будет добавлено в раскрывающийся список в рабочей области страницы как вложенное:

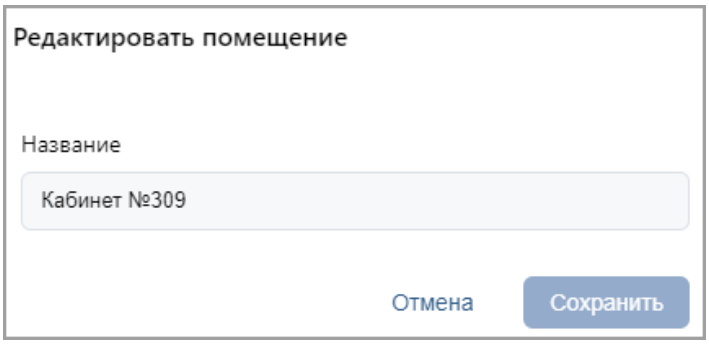


6. Для добавления вложенного помещения выделите в рабочей области страницы то помещение, в которое необходимо добавить вложенное, и нажмите кнопку **Добавить помещение**. Откроется окно **Добавить помещение**.

7. В открывшемся окне введите название нового помещения и нажмите кнопку **Сохранить**. Окно будет закрыто, новое помещение будет добавлено в выделенное:



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



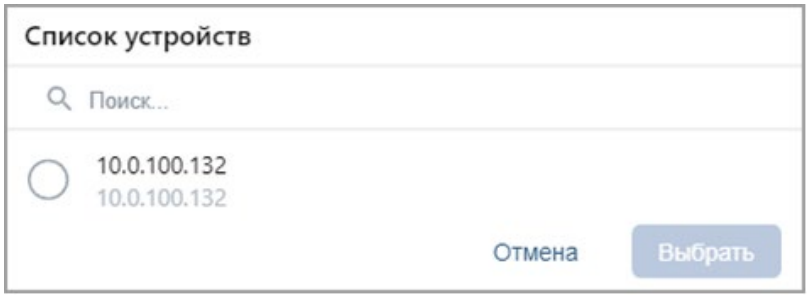
9. В открывшемся окне произведите необходимые изменения и нажмите кнопку **Применить**.

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

17.1.1.2. Размещение устройств в помещениях

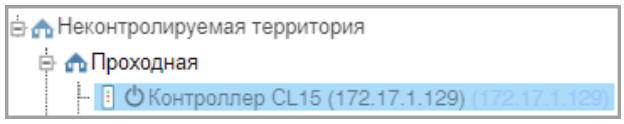
После создания списка помещений необходимо расположить в них устройства, входящие в систему безопасности. Для размещения устройств в помещениях:

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

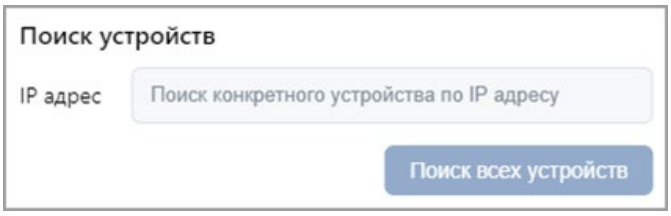


SEC.RU | Короткий путь к информации
Скачано с sec.ru

2. В открывшемся окне выделите устройство и нажмите кнопку **Выбрать**. При работе в режиме распределенной системы также укажите сегмент. Наименование устройства появится в выделенном помещении:



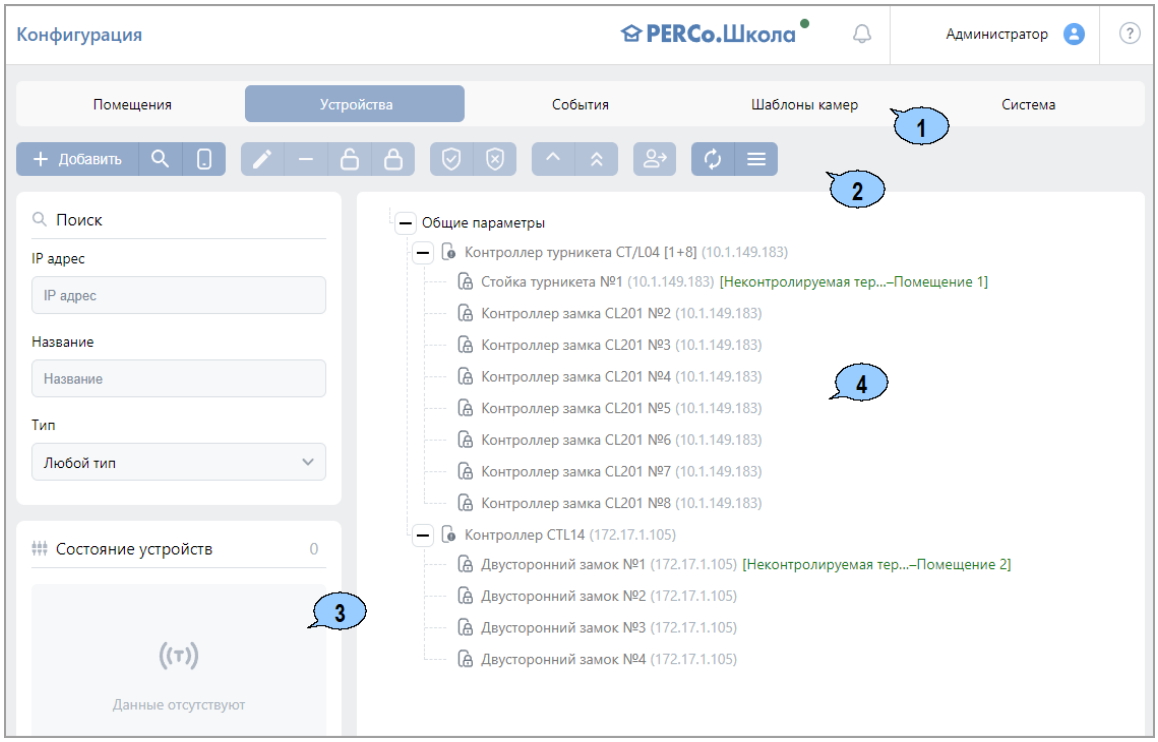
3. При необходимости в помещении можно расположить устройство, которое ранее не было добавлено в конфигурацию системы. Для этого выделите помещение и нажмите кнопку **Поиск устройств**. Откроется окно **Поиск устройств**:



4. В открывшемся окне введите IP-адрес искомого устройства и нажмите кнопку .
5. Выберите необходимые устройства и нажмите кнопку **Добавить**. Устройства будут добавлены в помещение.
6. При необходимости произведите настройку параметров работы устройства. Для этого выделите устройство в рабочей области страницы и нажмите на панели инструментов страницы кнопку **Редактировать**. В открывшемся окне **Редактировать устройство** произведите необходимые изменения и нажмите кнопку **Сохранить и закрыть**.
7. Для удаления контроллера, добавленного ранее в помещение, выделите его в рабочей области страницы и нажмите кнопку **Удалить помещение / Отвязать устройство** на панели инструментов. В открывшемся окне подтверждения нажмите кнопку **Удалить**. Контроллер будет удален из помещения.
8. Нажмите на панели инструментов страницы кнопку **Передать всю конфигурацию в устройства**.

17.1.2. Вкладка «Устройства»

Страница вкладки имеет следующий вид:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

1. Переключатель выбора вкладки подраздела:
   - **Помещения**;
   - **Устройства**;
   - **События**;
   - **Шаблоны камер**;
   - **Система**.
2. Панель инструментов страницы:
   - **Добавить** – кнопка позволяет:
     - **Добавить камеру**;
     - **Добавить сервер TRASSIR** (см. ***Руководство пользователя модуля PERCo-WM06 «Интеграция с TRASSIR»***);
     - **Добавить ИСО «Орион»** (см. ***Руководство пользователя модуля PERCo-WM07 «Интеграция с ИСО "Орион" (НВП "Болид")»***);
     - **Добавить сервер Biosmart SmartHub**;
     - **Добавить шлюз CTL14**;
     - **Добавить шлюз CL15**;
     - **Добавить составной объект CL15**.
   - **Поиск устройств** – кнопка позволяет произвести поиск в локальной сети устройств, которые ранее не были добавлены в конфигурацию системы.
   - **Редактировать** – кнопка позволяет открыть окно **Редактировать устройство** для изменения параметров выделенного в рабочей области панели устройства и его ресурсов. Если в рабочей области страницы выделен корневой элемент *«Общие параметры»*, то открывается окно **Общие параметры**.
   - **Удалить** – кнопка позволяет удалить выделенное в рабочей области страницы устройство из конфигурации системы.
   - **Активировать** – кнопка позволяет включить в конфигурацию системы ранее исключенное или найденное устройство.
   - **Деактивировать** – кнопка позволяет временно исключить из конфигурации системы устройство, выделенное в рабочей области страницы. При этом наименование устройства затеняется.
   - **Поставить на охрану** – кнопка позволяет поставить устройство / помещение на охрану.
   - **Снять с охраны** – кнопка позволяет снять устройство / помещение с охраны.
   - **Передать изменения конфигурации в устройства** – кнопка позволяет передать измененные параметры в устройства системы.
   - **Передать всю конфигурацию в устройства** – кнопка позволяет передать все параметры в устройства системы.
   - **Передать всех пользователей в устройства** – кнопка позволяет передать данные пользователей в устройство, выбранное в рабочей области страницы.
   - **Обновить** – кнопка позволяет обновить информацию о состоянии устройств.
   - **Дополнительно** – кнопка позволяет открыть меню команд для выбора дополнительных действий:
     - **Экспорт** – позволяет сохранить данные рабочей области в файл электронных таблиц с выбранным расширением.
     - **Выделить все устройства** – позволяет выделить все устройства.

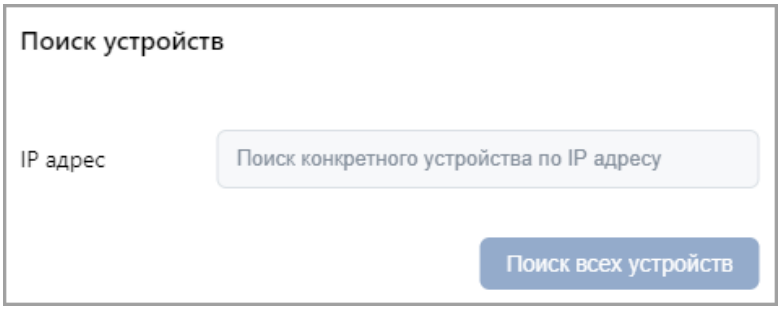
SEC.RU | Короткий путь к информации
Скачано с sec.ru

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

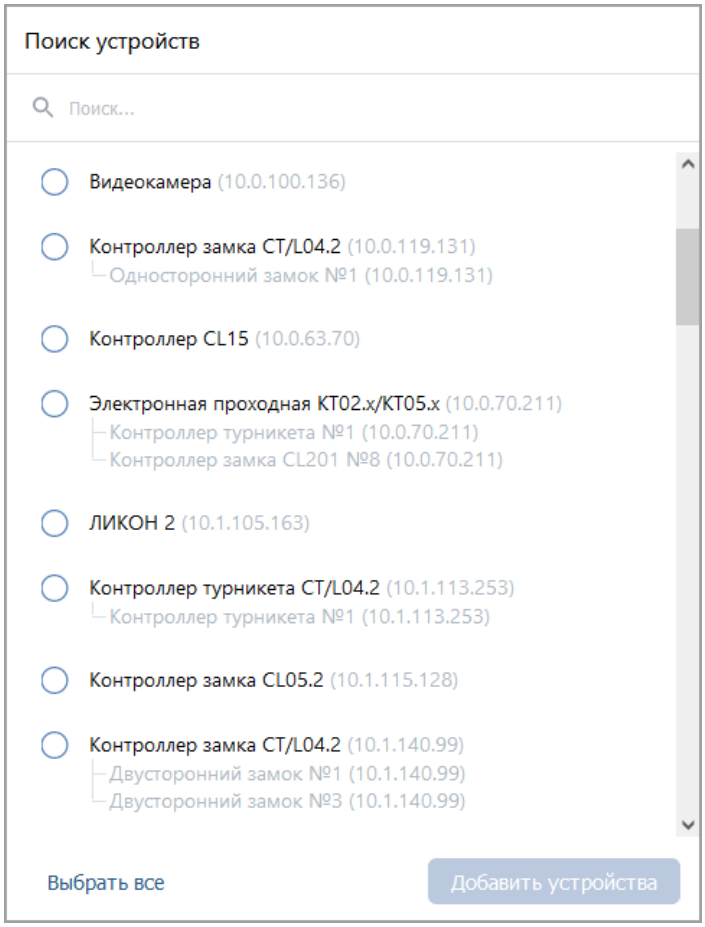
17.1.2.1. Поиск устройств

Для проведения автоматической конфигурации:

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



5. Если необходимо произвести поиск устройств по IP-адресу, то введите его в поле **Поиск конкретного устройства по IP адресу** и нажмите **Найти устройство по…**. Если необходимо произвести поиск всех устройств в сети, то, не заполняя поле для поиска, нажмите кнопку **Поиск всех устройств**.
6. По окончании поиска список найденных устройств появится в рабочей области окна:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

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

17.1.2.2. Добавление камеры, шлюза и составного объекта

Примечание:

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

Для добавления устройства:

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

Примечание:

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

4. Нажмите на панели инструментов страницы кнопку **Добавить**.
5. Из выпадающего списка выберите один из вариантов:
   - **Добавить камеру**;
   - **Добавить шлюз CTL14**;
   - **Добавить шлюз CL15**;
   - **Добавить составной объект CL15**.
6. В открывшемся окне настройте необходимые параметры. Вид окна зависит от выбранного объекта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

7. При создании шлюза или составного объекта выберите один из способов сохранения изменений:
   - **Только в базу данных**;
   - **Все в устройство**;
   - **Измененные в устройство**.
8. Нажмите кнопку **Сохранить**. Объект будет добавлен в рабочую область страницы.

Для добавления камеры:

Примечание:

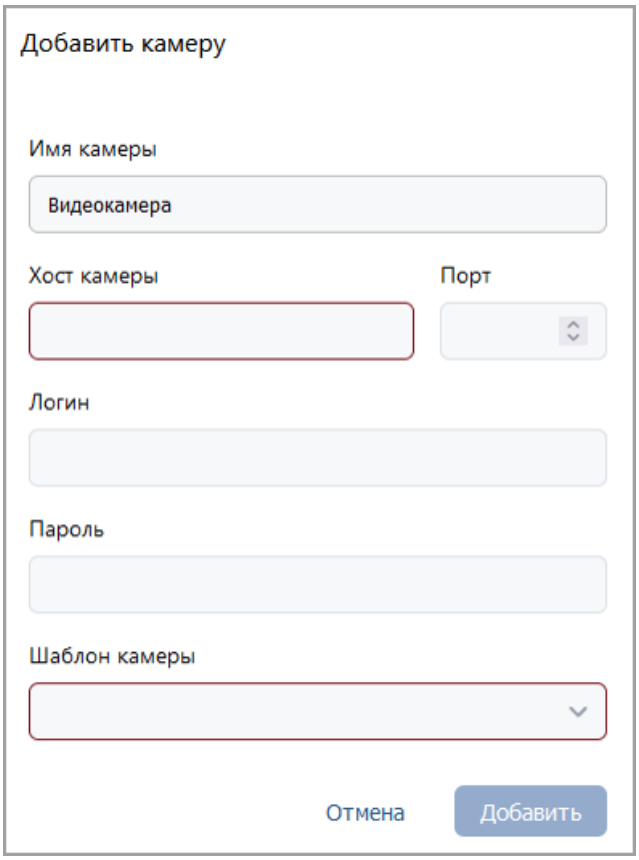
Перед добавлением камер создайте шаблоны для подключаемых моделей камер. Шаблоны создаются на вкладке **Шаблоны камер** подраздела **«Конфигурация»** раздела **«Администрирование»**.

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

Примечание:

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

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

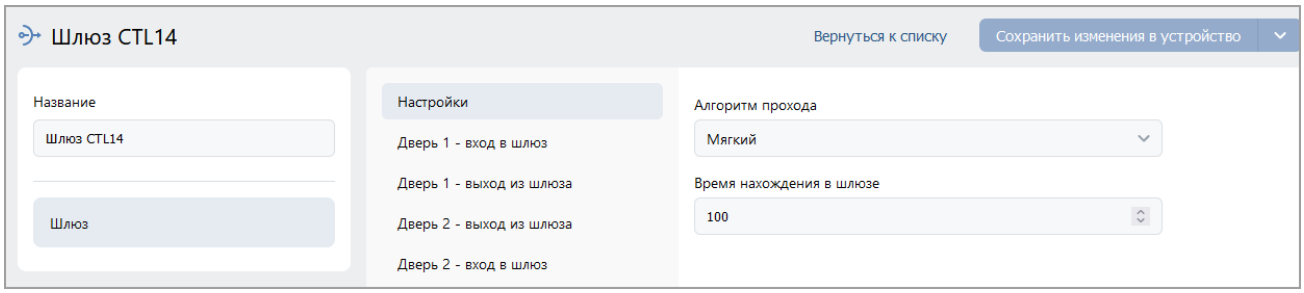


5. В открывшемся окне введите имя камеры и укажите шаблон подключаемой камеры. При работе в режиме распределенной системы также укажите сегмент.
6. Произведите настройку других параметров. Нажмите кнопку **Добавить**. Окно **Добавить камеру** будет закрыто. Камера будет добавлена в рабочую область страницы.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Для создания шлюза *CTL14 / CL15*:

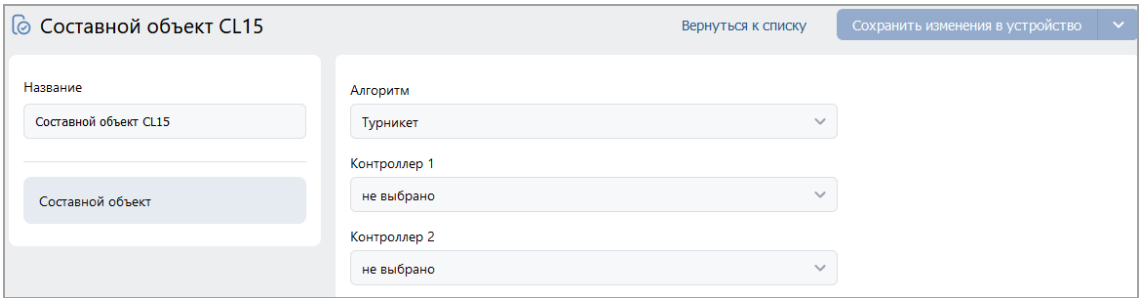
1. Используя панель навигации, перейдите в раздел **«Администрирование»**.
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **Устройства**.
4. Нажмите на панели инструментов страницы кнопку **Добавить**. Из выпадающего списка выберите **Добавить шлюз CTL14** или **Добавить шлюз CL15**.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



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

Для создания составного объекта *CL15*:

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



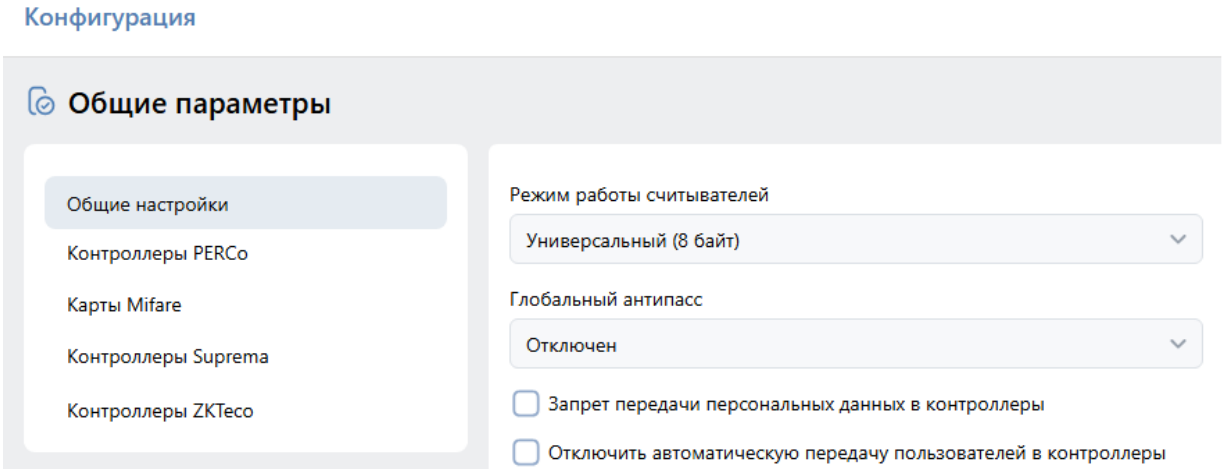
SEC.RU | Короткий путь к информации
Скачано с sec.ru

5. При необходимости в поле **Название** измените название составного объекта.
6. На вкладке **Составной объект** выберите значение для следующих параметров:
   - В поле **Алгоритм** выберите тип ИУ: **Турникет** или **Двусторонний замок**.
   - В полях **Контроллер 1** и **Контроллер 2** с помощью выпадающего списка выберите регистрирующие контроллеры для составного объекта.
7. Используя выпадающий список в верхней части страницы, выберите один из способов сохранения изменений:
   - **Только в базу данных**;
   - **Все в устройство**;
   - **Измененные в устройство**.
8. Нажмите кнопку **Сохранить…**. Составной объект будет добавлен в рабочую область страницы.

17.1.2.3. Настройка общих параметров контроллеров

Для настройки общих параметров контроллеров системы:

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



- **Режим работы считывателей** – позволяет изменить параметры режима работы считывателей.
- **Глобальный антипасс** – позволяет включить или отключить глобальный контроль зональности (Global Antipass).
- **Запрет передачи персональных данных в контроллеры** – установка флажка позволяет запретить передачу ФИО сотрудника (посетителя) в контроллеры, вместо них в контроллере используется номер личной карточки (аккаунта).
- **Отключить автоматическую передачу пользователей в контроллеры** – установка флажка разрешает только ручную передачу как данных для новых пользователей, так и изменения в данных для уже зарегистрированных пользователей.
- С помощью раскрывающегося списка в верхней части страницы выберите способ

SEC.RU | Короткий путь к информации Скачано с sec.ru

сохранения параметров. Для завершения работы с окном **Общие параметры** нажмите кнопку **Сохранить**.

Примечание:

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

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

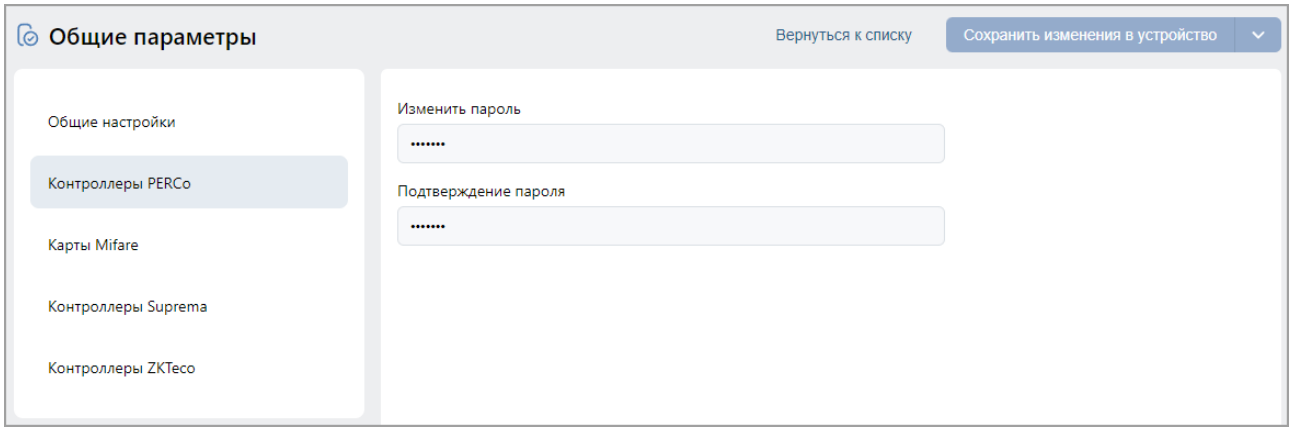
– либо случайным образом из следующих параметров смартфона: Build.BOARD, Build.BRAND, Build.CPU_ABI, Build.DEVICE, Build.MANUFACTURER, Build.MODEL, Build.PRODUCT (вероятность совпадения идентификаторов ничтожно мала);
– либо по желанию пользователя можно использовать *IMSI* – индивидуальный номер абонента,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

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

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

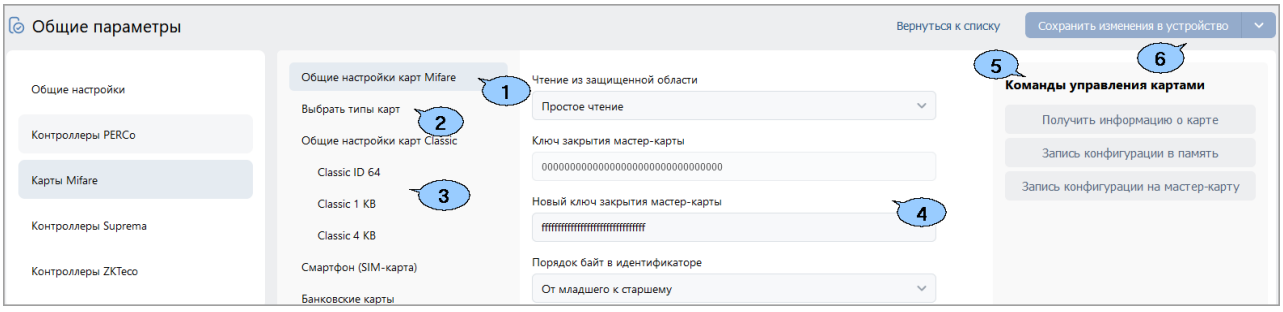
Уникальный идентификатор добавляется в систему аналогично другим картам.

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



- Для задания пароля введите в поле **Изменить пароль** новый пароль и подтвердите его в поле **Подтверждение пароля**. Пароль не должен превышать 10 символов.
- С помощью раскрывающегося списка в нижней части окна выберите способ сохранения параметров. Для завершения работы с окном **Общие параметры** нажмите кнопку **Сохранить**.

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



SEC.RU | Короткий путь к информации
Скачано с sec.ru

1) Подвкладка **Общие настройки карт Mifare** – подвкладка предназначена для настройки общих параметров карт *Mifare*. Параметры общих настроек:
   - **Чтение из защищенной области** – определяет порядок работы с защищенной областью карт *Mifare*:
     - **Простое чтение** – чтение UID с карты;
     - **С записью карты** – чтение номера карты из защищенной области с последующей его перезаписью по заданному алгоритму генерации номера.
   - **Ключ закрытия мастер-карты** – поле отображает текущий ключ закрытия мастер-карты.
   - **Новый ключ закрытия мастер-карты** – поле позволяет ввести новый ключ закрытия мастер-карты.
   - **Порядок байт в идентификаторе**:
     - **От старшего к младшему**;
     - **От младшему к старшему**.
   - **Поля HID и EM-marine только для считывателя IR19 и контроллера замка CL211.9** – позволяет включить / отключить возможность работы со стандартами бесконтактных карт *HID* и *EM-Marine*. Если выбрать в полях параметр **Отключено**, считыватель ***IR19*** и контроллер замка ***CL211.9*** будут поддерживать только работу со стандартом *Mifare*.
     После настройки данного параметра запишите конфигурацию на мастер-карту.
2) Подвкладка **Выбрать тип карты** – позволяет выбрать форматы карт *Mifare* (смартфон, банковские карты), которые будут использоваться в СКУД. Для выбора доступны:
   - **Ultralight EV1 48 byte**;
   - **Ultralight EV1 128 byte**;
   - **Ultralight C 144 byte**;
   - **Classic ID 64**;
   - **Classic 1 KB**;
   - **Classic 4 KB**;
   - **Plus 2 KB**;
   - **Plus 4 KB**;
   - **Plus SE 1 KB**;
   - **DESFire**;
   - **МИР**;
   - **Смартфон (SIM-карта)**;
   - **Банковские карты**.

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

   Примечание:
   Список доступных **параметров карт** и **команд управления картам** меняется в зависимости от выбранного для конфигурирования типа карты.
5) Область **Команды управления картами** – область содержит список команд, доступных при работе с картами и контрольным считывателем:
   - **Запись конфигурации в память** – позволяет записать заданную для выбранных типов карт конфигурацию в энергонезависимую память контрольного считывателя;
   - **Запись конфигурации на мастер-карту** – позволяет записать заданную для выбранных типов карт конфигурацию на мастер-карту;

     Примечание:
     В качестве мастер-карт используются карты типа *Mifare DESFire*, которые также могут использоваться и в качестве простых карт.
   - **Изменить ключ** – команда позволяет записать измененные параметры для простых карт всех типов (*Ultralight, Classic, Plus, DESFire*). По команде считыватель определяет наличие карты в поле считывателя, ее тип, и изменяет **параметры карты** согласно параметрам, записанным в конфигурацию контрольного считывателя для данного типа карт;

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Получить информацию о карте** – позволяет прочесть информацию с выбранной карты. После успешного чтения карты во всплывающем окне **Информация о карте** будет отображена следующая информация:
  - **Тип карты** – отображает тип карты *Mifare*;
  - **UID** – отображает серию или номер уникального идентификатора пользователя;
  - **Тип карты** – отображает тип карты: мастер-карта, простая карта;
  - **Текущий уровень мастер-карты** – отображает текущий уровень мастер-карты (для карт *Mifare DESFire*);
  - **Уровень безопасности** – отображает текущий уровень безопасности (для карт *Mifare Plus*).
- **Повысить уровень безопасности SL** – команда для всех типов карт *Mifare Plus* с SL1 и SL2, позволяет повысить уровень безопасности *SL* (*secure level*);

Примечание:

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

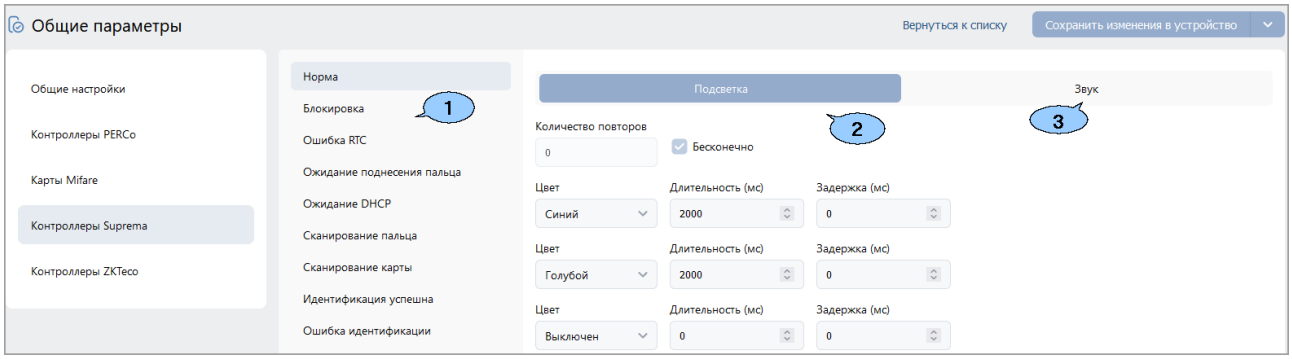
- **Форматировать** – применяется для простых карт типа *DESFire* (не мастер-карт) в том случае, если на карте уже записано несколько приложений и нет свободного места для создания нового приложения.

Примечания:

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

6) Для сохранения внесенных изменений нажмите кнопку **Сохранить…**.

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



Примечание:

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

1) **Список событий** – отображает список событий, для которых предусмотрена возможность настройки цветовой индикации и звуковых сигналов контроллера:
   - **Норма** – событие возникает в случае нормальной работы контроллера (режим работы **"Контроль"**);
   - **Блокировка** – событие возникает в случае блокировки контроллера (режим работы **"Закрыто"**);
   - **Ошибка RTC** (Real Time Clock) – событие возникает в случае несовпадения внутреннего времени контроллера со временем сети;
   - **Ожидание поднесения пальца** – событие возникает в случае, если был выбран тип

SEC.RU | Короткий путь к информации
Скачано с sec.ru

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, ученику, родственнику ученика или посетителю (если контроллер выбран как устройство для получения идентификатора);
- **Сканирование карты** – событие возникает в случае добавления карты доступа как идентификатора сотруднику, ученику, родственнику ученика или посетителю (если контроллер выбран как устройство для получения идентификатора);
- **Идентификация успешна** – событие возникает в случае успешной идентификации;
- **Ошибка идентификации** – событие возникает в случае ошибки идентификации.

2) Область **Подсветка** – отображает параметры настройки световой индикации контроллера для выбранного события из списка событий:
- **Бесконечно** – при установке флажка подсветка будет производиться бесконечно;
- **Количество повторов** – счетчик позволяет задать количество повторений подсветки;

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

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

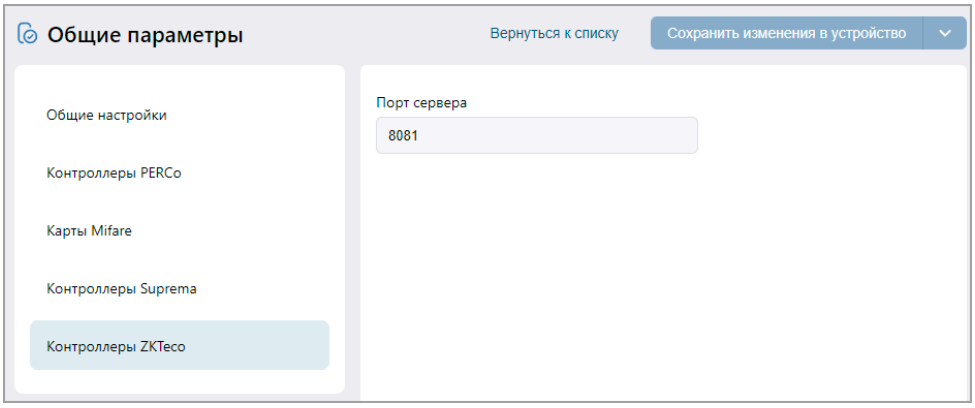
3) Область **Звук** – отображает параметры настройки звуковых сигналов контроллера для выбранного события из списка событий:
- **Бесконечно** – при установке флажка звук будет воспроизводиться бесконечно;
- **Количество повторов** – счетчик позволяет задать количество повторений звучания;

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

4) Для сохранения внесенных изменений нажмите кнопку **Сохранить…**.

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



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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

17.1.2.4. Порядок работы с картами Mifare

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

Примечание:

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

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

Внимание!

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

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

Примечание:

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

- После настройки параметров на вкладке **Карты Mifare** окна **Общие параметры** в командах управления картами нажмите кнопку **Запись конфигурации в память**;
- На вкладке **Устройства** подраздела **«Конфигурация»** раздела **«Администрирование»** выделите контроллер, в который будет передаваться конфигурация, и нажмите на панели инструментов кнопку **Передать изменения конфигурации в устройства** или **Передать всю конфигурацию в устройства**.

Основные характеристики разных чипов *Mifare*

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

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

Примечание:

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

- **Уровень безопасности SL1**. На этом уровне карты *Mifare Plus* имеют 100%-ую совместимость с *Mifare Classic 1K (4K)*.
- **Уровень безопасности SL2**. Аутентификация по *AES* является обязательной. Для защиты данных используется *CRYPTO1.*
  Работа с *SL2* не поддерживается. В случае использования карт с *SL2* рекомендуется переход на *SL3.*
- **Уровень безопасности SL3**. Аутентификация, обмен данными, работа с памятью только по *AES*.

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

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

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

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

Примечание:

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

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

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

Примечание:

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

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

Примечание:

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

Возможно конфигурирование параметров следующих типов карт:

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

Подвкладки различных типов карт содержат следующие параметры криптозащиты:

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

Внимание!

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

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

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

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

1 Перейдите на вкладку **Карты Mifare**.
2 Перейдите на подвкладку **Выбрать тип карты**. Установите флажок напротив карты **Mifare Classic 4KB**. Тип карты будет добавлен в список используемых карт в левой части вкладки **Карты Mifare**.
3 Перейдите на подвкладку **Mifare Classic 4KB** в левой части окна. Укажите **Номер сектора**. Он представляет собой часть памяти, в которую будет записан идентификатор и с которой он будет считываться при взаимодействии пользователя со СКУД. Номер выбирается произвольно.
4 Укажите **Номер блока**. Он представляет собой часть памяти, в которую будет записан идентификатор и с которой он будет считываться при взаимодействии пользователя со СКУД. Номер выбирается произвольно.
5 На вкладке **Карты Mifare** перейдите на подвкладку **Общие настройки карт Classic**.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6 В поле **Старый тип ключа для аутентификации** и поле **Старый ключ аутентификации** отображаются те параметры, которые были записаны на карту ранее.

Примечание:

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

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

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

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

Примечание:

В качестве мастер-карты используется мастер-карта *DESFire*. Чистая (т.е. без записей в защищенной области) карта типа *DESFire* также может быть записана в качестве дополнительной мастер-карты для СКУД. Для записи мастер-карты нужна карта типа DESFire емкостью не менее 2 Кб. Перезапись мастер-карты с целью перевода ее в состояние карты пользователя или чистой карты невозможна! Т.е. карта, однажды записанная как мастер-карта, может использоваться далее только в этом качестве.

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

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

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

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

- **Номер страницы, блока, сектора или приложения** – место, где будет храниться номер карты, используемый в СКУД.
- **Типы и ключи для аутентификации** – типы паролей и пароли, позволяющие получить доступ к карте.
- **Ключи для изменения уровня безопасности (SL)** – служебные пароли, позволяющие получить доступ изменению конфигурации карты, есть только у *Mifare Plus*.
- **Типы и ключи для доступа к данным на карте** – дополнительные пароли, позволяющие получить доступ к данным на карте, есть только у *Mifare DESFire*.

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

- Если в текущую конфигурацию СКУД добавляются новые типы карт пользователей, то ранее выданные карты будут работать.
- Если в конфигурации изменяются какие-либо параметры для уже выданных карт пользователей (номера страниц / секторов / блоков, типы и / или значения ключей,

SEC.RU | Короткий путь к информации Скачано с sec.ru

уровни безопасности SL), то ранее выданные карты пользователей не будут работать и их необходимо перепрограммировать с учетом новой конфигурации.

- Особенности работы с мастер-картами и рекомендации по паролям для них приведены в руководстве по эксплуатации на контрольные считыватели ***IR18***, ***IR15.9***, ***MR08***.

Запись отпечатков пальцев на карту Mifare

Контроллеры ***PERCo-CL15***, ***PERCo-CL15.1***, ***PERCo-CR11*** и биометрический контрольный считыватель ***PERCo-IR18*** поддерживают функцию записи отпечатков пальцев на карты доступа *Mifare* (такой возможностью обладают карты стандартов *MIFARE Classic 1K*, *MIFARE Classic 4K*, *MIFARE Plus* (*X*, *S*, *SE*) и *MIFARE DESFire Ev1)*. Данная функция позволяет ускорить процесс авторизации пользователя в системе, так как при этом системой не тратится время на поиск нужного отпечатка в базе данных – сравнение предъявленного отпечатка производится сразу с отпечатком, записанным на карте.

Внимание!

Запись отпечатка пальца производится в защищенную область карты, поэтому заранее необходимо персонифицировать карты пользователей, т.е. записать в них конфигурацию для считывателей и карт *Mifare*, заданную на данный момент в системе СКУД. Записать отпечаток пальца в не персонифицированную карту нельзя!

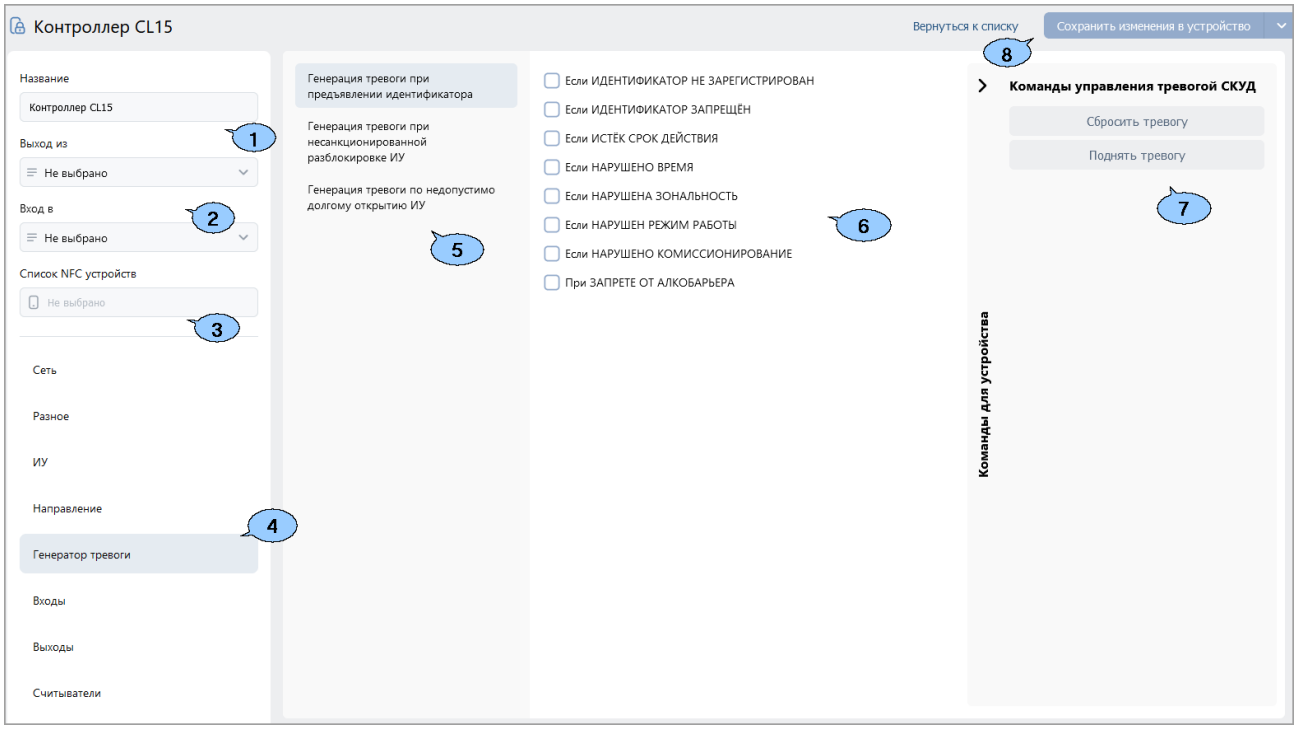
Запись отпечатков пальцев на карту осуществляется в учетных карточках сотрудников (учеников, родственников учеников, посетителей) системы ***PERCo.Школа*** (см. ***«Руководство пользователя „Стандартного пакета ПО“ PERCo-ES»***).

Количество отпечатков, записываемых на карту *Mifare*, зависит от наличия свободного места в ее памяти и ограничено производителем – не более 5 штук. После записи рекомендуется проверить попытками прохода, какие отпечатки записались, а какие – нет.

17.1.2.5. Настройка параметров устройства

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

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



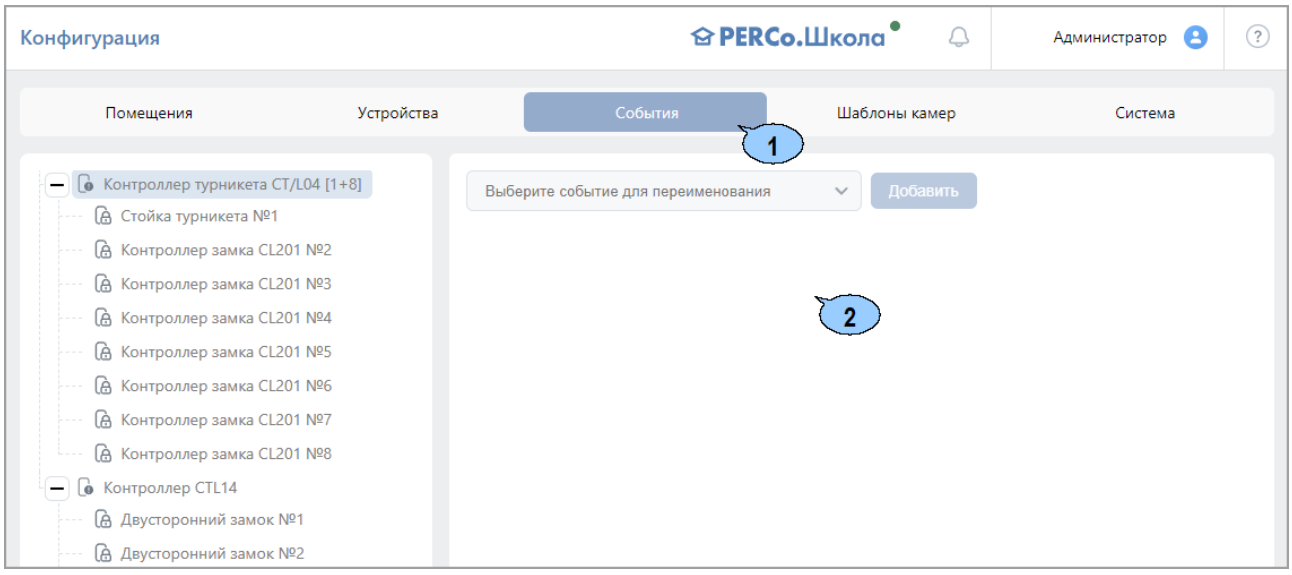
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Элементы страницы:

1) **Название** – поле для ввода описательного названия устройства.
2) Инструменты для указания или изменения помещений, доступ между которыми обеспечивается контроллером:
   - Поле **Выход из** – кнопка внутри поля позволяет выбрать помещение, доступ в которое осуществляется через считыватель № 1. Кнопка **Сбросить** позволяет удалить из поля выбранное ранее помещение.
   - Поле **Вход в** – кнопка внутри поля позволяет выбрать помещение, доступ в которое осуществляется через считыватель № 2. Кнопка **Сбросить** позволяет удалить из поля выбранное ранее помещение.
3) **Список NFC Устройство** – поле позволяет выбрать добавленное раннее устройство с поддержкой технологии NFC, чтобы использовать его в качестве имитации настраиваемого считывателя.
4) Выбор вкладки ресурса. В зависимости от типа устройства список ресурсов и соответствующих им вкладок может отличаться.
5) Параметры, доступные для данного ресурса.
6) Возможные значение и варианты настройки выделенного параметра ресурса.
7) Кнопки команд управления, доступных для выбранного ресурса. Для оперативного управления устройствами предназначен подраздел **«Управление устройствами»** раздела **«Контроль доступа»**.
8) Кнопки **Сохранить…** и раскрывающийся список способа сохранения изменений при нажатии:
   - **Только в базу данных** – параметры сохраняются только в БД системы и впоследствии должны быть переданы в контроллер(ы).
   - **Все в устройство** – в устройство передаются все параметры.
   - **Измененные в устройство** – в устройство передаются только измененные параметры.

17.1.3. Вкладка «События»

Страница вкладки имеет следующий вид:



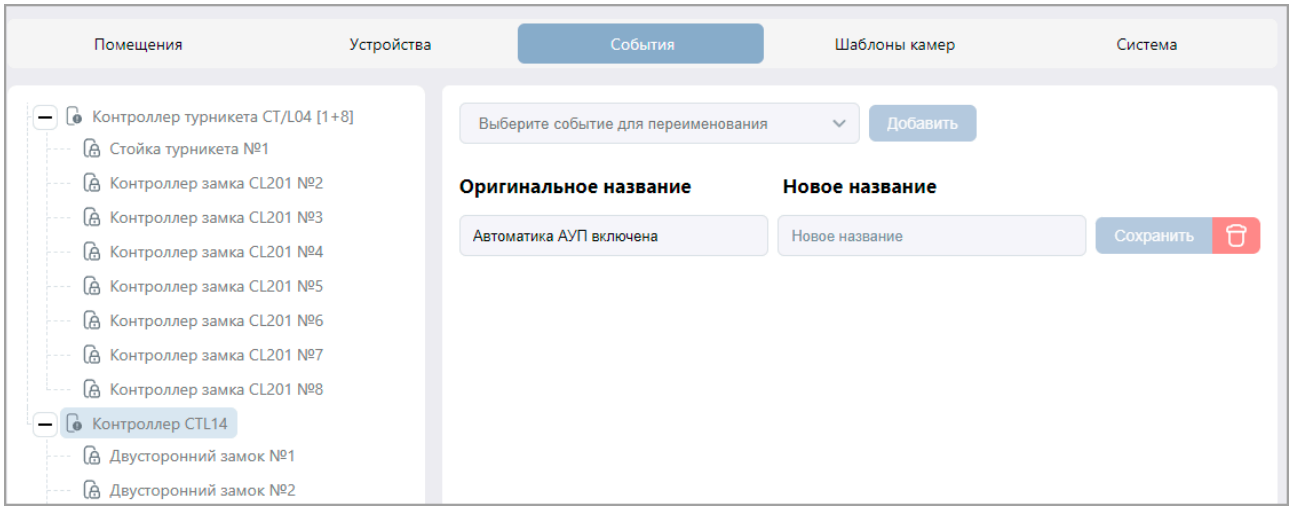
1. Переключатель выбора вкладки подраздела:
   - **Помещения**;
   - **Устройства**;
   - **События**;
   - **Шаблоны камер**;
   - **Система**.
2. Рабочая область страницы содержит список устройств, добавленных в конфигурацию системы, и область для переименования событий устройств.

SEC.RU | Короткий путь к информации Скачано с sec.ru

17.1.3.1. Переименование события

Для переименования события:

1. Используя панель навигации, перейдите в раздел **«Администрирование»**.
2. Откройте подраздел **«Конфигурация»**.
3. Перейдите на вкладку **События**.
4. Выберите в рабочей области устройство, для которого будет переименовываться событие.
5. С помощью соответствующего раскрывающегося списка выберите событие для переименования и нажмите кнопку **Добавить**. Выбранное событие добавится в список событий в рабочей области:

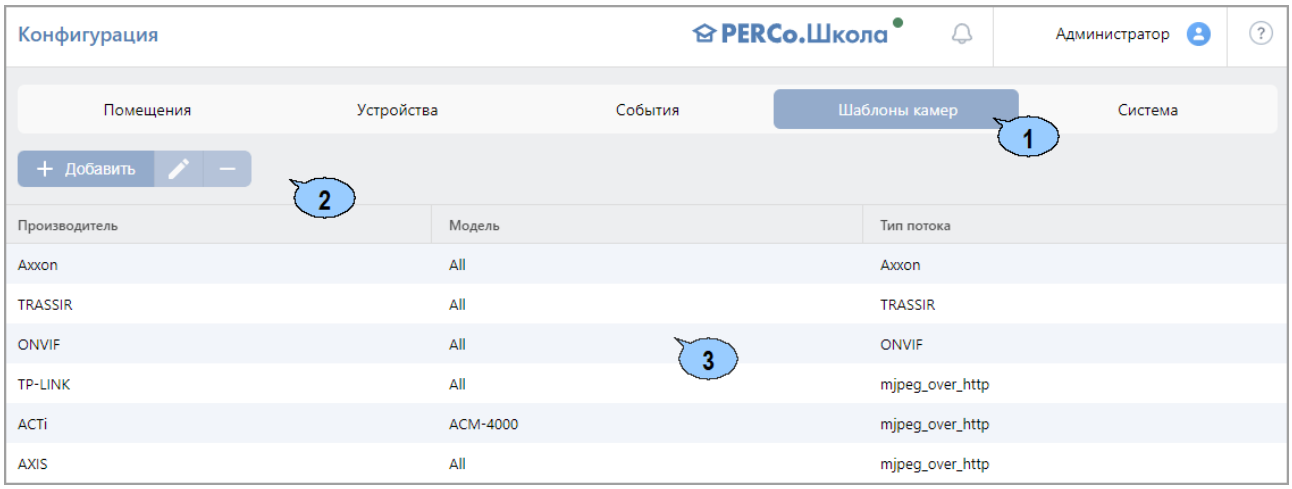


6. В поле **Новое название** введите новое название события и нажмите кнопку **Сохранить**.
7. Для удаления переименования события нажмите кнопку **Удалить** напротив соответствующего события.

17.1.4. Вкладка «Шаблоны камер»

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

Страница вкладки имеет следующий вид:



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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

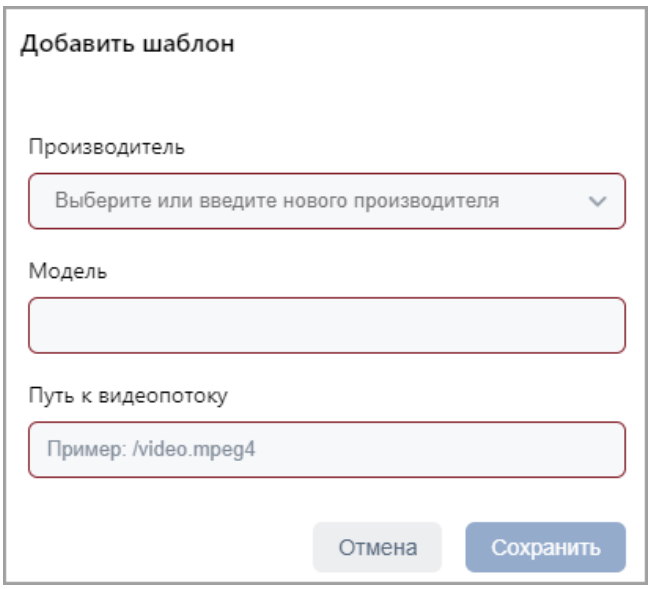
- **События**;
- **Шаблоны камер**;
- **Система**.

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

17.1.4.1. Создание шаблона камеры

Для создания нового шаблона камеры:

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

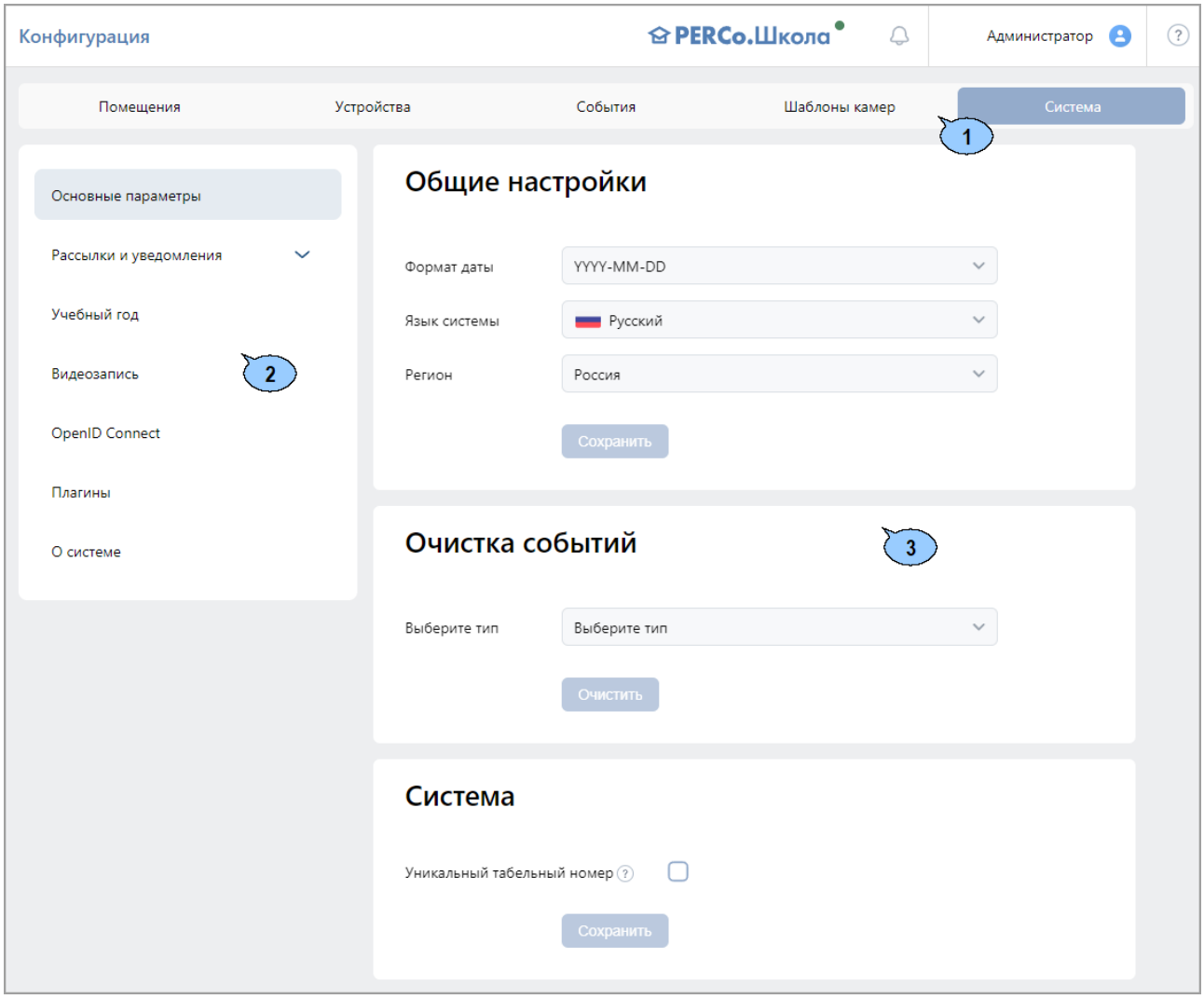


5. В открывшемся окне произведите настройку параметров шаблона. Нажмите кнопку **Сохранить**. Окно **Добавить шаблон** будет закрыто, новый шаблон будет добавлен в рабочую область страницы.

SEC.RU | Короткий путь к информации Скачано с sec.ru

17.1.5. Вкладка «Система»

Страница вкладки имеет следующий вид:



1. Переключатель выбора вкладки подраздела:
   - **Помещения**;
   - **Устройства**;
   - **События**;
   - **Шаблоны камер**;
   - **Система**.
2. Меню слева содержит подвкладки:
   - **Основные параметры**;
   - **Рассылки и уведомления**;
   - **Учебный год**;
   - **Видеозапись**;
   - **OpenID Connect**;
   - **Плагины**;
   - **О системе**.
3. Рабочая область страницы зависит от выбранной подвкладки.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

17.1.5.1. Подвкладка «Основные параметры»

Рабочая область подвкладки **Основные параметры** предназначена для выбора региона, формата даты, очистки журнала событий системы, настройки уникальности табельных номеров сотрудников.

Общие настройки (см. рисунок выше):

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

Очистка событий:

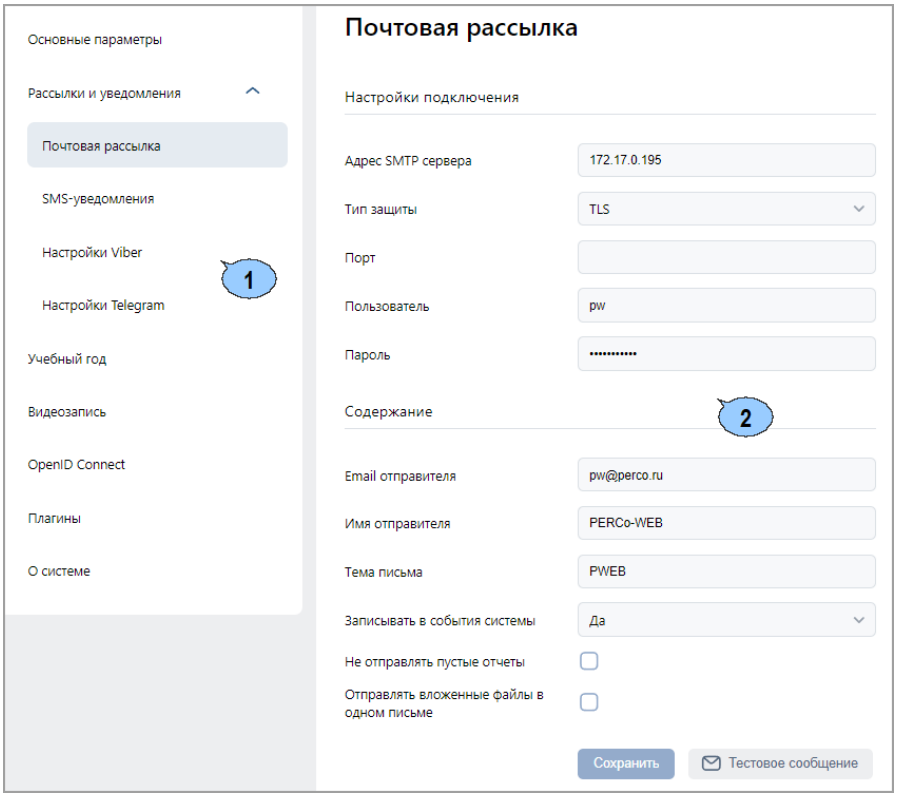
- **Выберите тип** – поле содержит выпадающий список, который позволяет удалить события системы за выбранный период времени. Доступны следующие типы:
  - **Старше месяца**;
  - **Старше трех месяцев**;
  - **Старше полугода**;
  - **Старше года**;
  - **Очистить все**, **кроме последних 50000**.

Система:

- **Уникальный табельный номер** – при установленном флажке невозможно создать сотрудников с одинаковыми табельными номерами.

17.1.5.2. Подвкладка «Рассылки и уведомления»

Рабочая область подвкладки **Рассылки и уведомления** предназначена для настройки рассылок. Страница имеет следующий вид:



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

SEC.RU | Короткий путь к информации Скачано с sec.ru

17.1.5.3. Добавление параметров почтовой рассылки

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

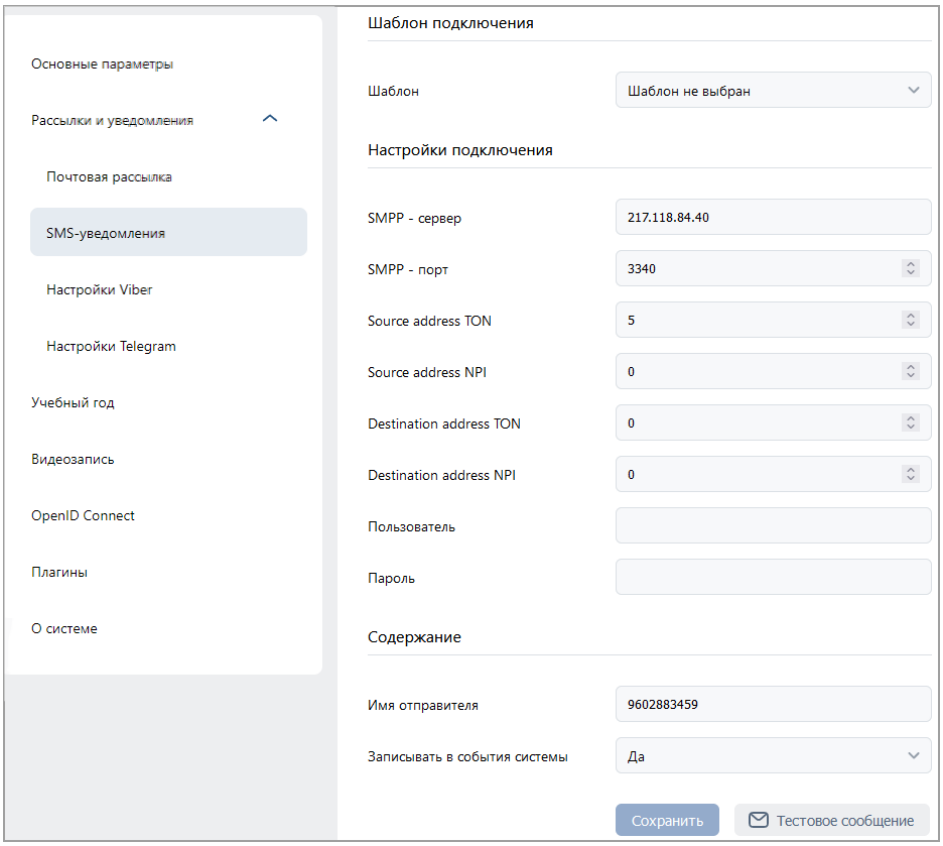
- **Адрес SMTP-сервера**, **Email отправителя** – поля для ввода адреса почтового сервера и адреса почтового ящика, с которого системой будет производиться рассылка почтовых отправлений;
- **Имя отправителя**, **Тема письма** – данные, которые будут отображаться в сообщениях, рассылаемых системой (по умолчанию ***PERCo.Школа***);
- **Тип защиты** – определяется тип шифрования почтовых отправлений (**Нет**, **SSL**, **TLS**);
- **Порт** – номер порта. Определяется почтовым сервером (зависит от типа шифрования, узнать можно на сайте почтового сервиса);
- **Пользователь**, **Пароль** – логин и пароль почтового ящика отправителя, используемого системой;
- **Записывать в события системы** – возможны значения **Нет**, **Да**, **Ошибки**, в соответствии с которыми в системе будут записываться события почтовой рассылки;
- **Не отправлять пустые отчеты** – при установленном флажке не будут отправляться пустые отчеты (например, отчеты по проходам сотрудников, находящихся в отпуске или в командировке);
- **Отправлять вложенные файлы в одном письме** – при установленном флажке все отчеты, относящиеся к одному заданию, будут отправляться получателю в одном письме. В противном случае каждый отчет будет отправляться в отдельном письме;
- Кнопка **Сохранить** позволяет сохранить установленные параметры;
- Кнопка **Тестовое сообщение** позволяет проверить актуальность почтового ящика системы.

Примечание:

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

17.1.5.4. Добавление параметров рассылки SMS-уведомлений

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



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Внимание!

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

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

Примечание:

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

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

Примечание:

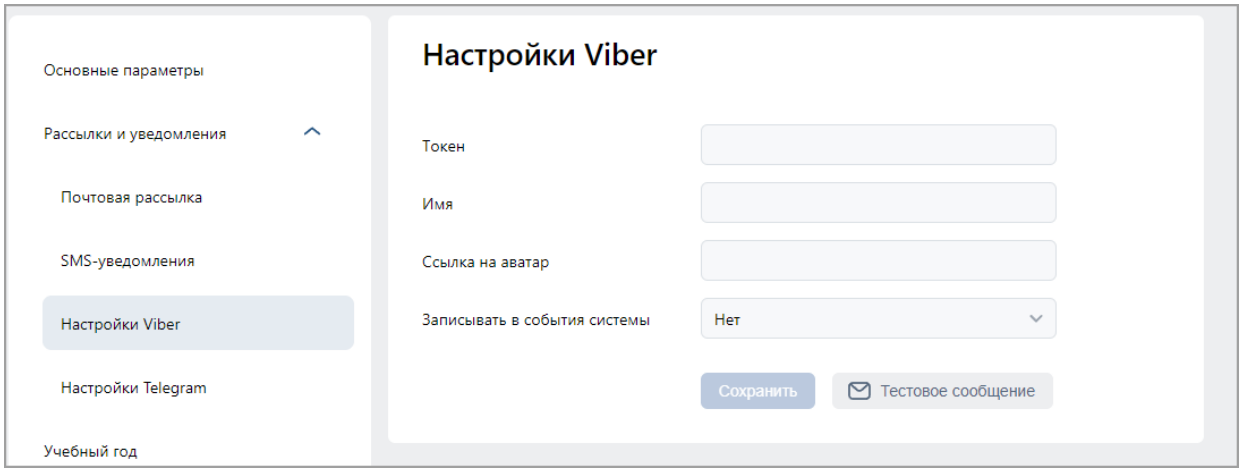
Если параметры SMS-рассылки были введены некорректно, при отправке тестового уведомления отобразится сообщение об ошибке.

17.1.5.5. Добавление параметров рассылки в Viber

Внимание!

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

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



- **Токен** – поле для ввода токена (числа-идентификатора), полученного при регистрации паблик-аккаунта Viber;
- **Имя** – указывается имя отправителя;
- **Ссылка на аватар** – поле предназначено для ввода URL адреса картинки, которая будет отображаться у получателя;

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Записывать в события системы** – возможны значения **Нет**, **Да**, **Ошибки**, в соответствии с которыми в системе будут записываться события рассылки;
- Кнопка **Сохранить** – позволяет сохранить указанные настройки;
- Кнопка **Тестовое сообщение** – позволяет проверить правильность настройки параметров.

Примечание:

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

17.1.5.6. Порядок создания паблик-аккаунта Viber

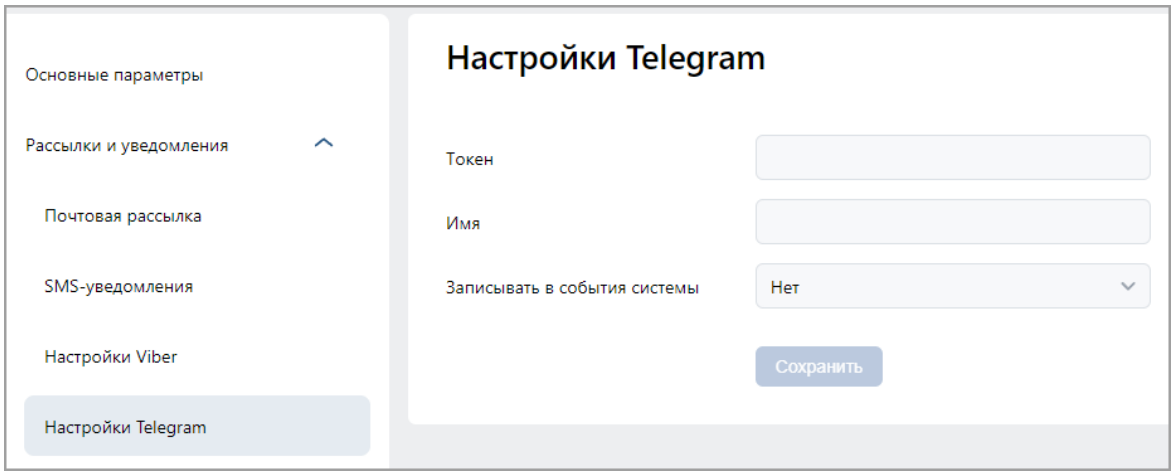
1. Скачайте и установите приложение Viber на телефон администратора.
2. По ссылке https://partners.viber.com/ перейдите на **Панель администратора Viber**:
   - в правом верхнем углу выберите язык: русский/английский;
   - введите номер телефона администратора, нажмите на кнопку **Войти** и введите код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

   Откроется окно управления паблик-аккаунтом.
3. В окне управления паблик-аккаунтом нажмите на кнопку **Создать бот**. В анкете заполните учетные данные паблик-аккаунта, выберите аватар аккаунта. Нажмите кнопку **Create**. Сформируется паблик-аккаунт, автоматически сгенерируется токен аккаунта.
4. Скопируйте токен в буфер обмена и введите его в поле ввода **Токен** в подвкладке **Настройка Viber** (вкладка **Система** подраздела **«Конфигурация»** раздела **«Администрирование»** ПО ***PERCo.Школа***). В поле **Имя** укажите имя, от которого будут отправляться сообщения и уведомления.
5. В приложении Viber перейдите в меню **Еще** и с помощью сканера штрихкода зайдите в созданный паблик-аккаунт:
   - пригласите в чат сотрудников, которые будут получать уведомления (номера их телефонов, привязанные к Viber-аккаунтам, должны быть предварительно записаны в списке контактов телефона администратора);
   - сотрудники, получившие приглашение в паблик-аккаунт, должны принять приглашение (при этом каждому необходимо будет принять соглашение по возрастным ограничениям);
   - с помощью кнопки **Изменить** в поле **Администраторы** добавьте в паблик-аккаунт данных сотрудников в качестве администраторов.
6. В ПО ***PERCo.Школа*** (раздел **«Персонал»**, подраздел **«Сотрудники»**, вкладка **Действующие**):
   - в учетных карточках приглашенных сотрудников в разделе **Дополнительные поля** в поле **Viber** при помощи кнопки  из общего списка выберите и закрепите за каждым сотрудником его Viber-аккаунт;
   - с помощью кнопки  **Отправить сообщение по Viber**, расположенной на панели инструментов, проверьте отправку системой сообщений каждому из сотрудников. В случае неудачи на экран будет выведено сообщение об ошибке.

SEC.RU | Короткий путь к информации Скачано с sec.ru

17.1.5.7. Настройки Telegram

В поле подвкладки **Настройки Telegram** задаются параметры для отправки сообщений сотрудникам:



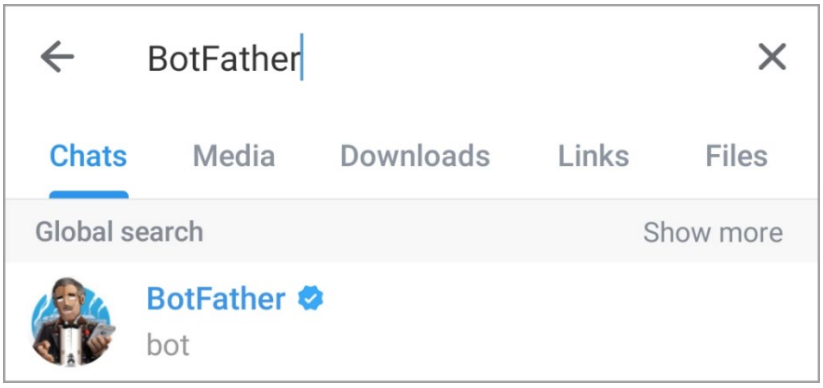
- **Токен** – поле для ввода токена (числа-идентификатора), полученного при создании Telegram-бота;
- **Имя** – поле для ввода имени, указанного при создании бота;
- **Записывать в события системы** – возможны значения **Нет**, **Да**, **Ошибки**, в соответствии с которыми в системе будут записываться события рассылки;
- Кнопка **Сохранить** позволяет сохранить заданные параметры.

Примечание:

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

17.1.5.8. Создание Telegram-бота

1. Скачайте и установите приложение Telegram.
2. Откройте приложение Telegram и введите в поиск «BotFather».

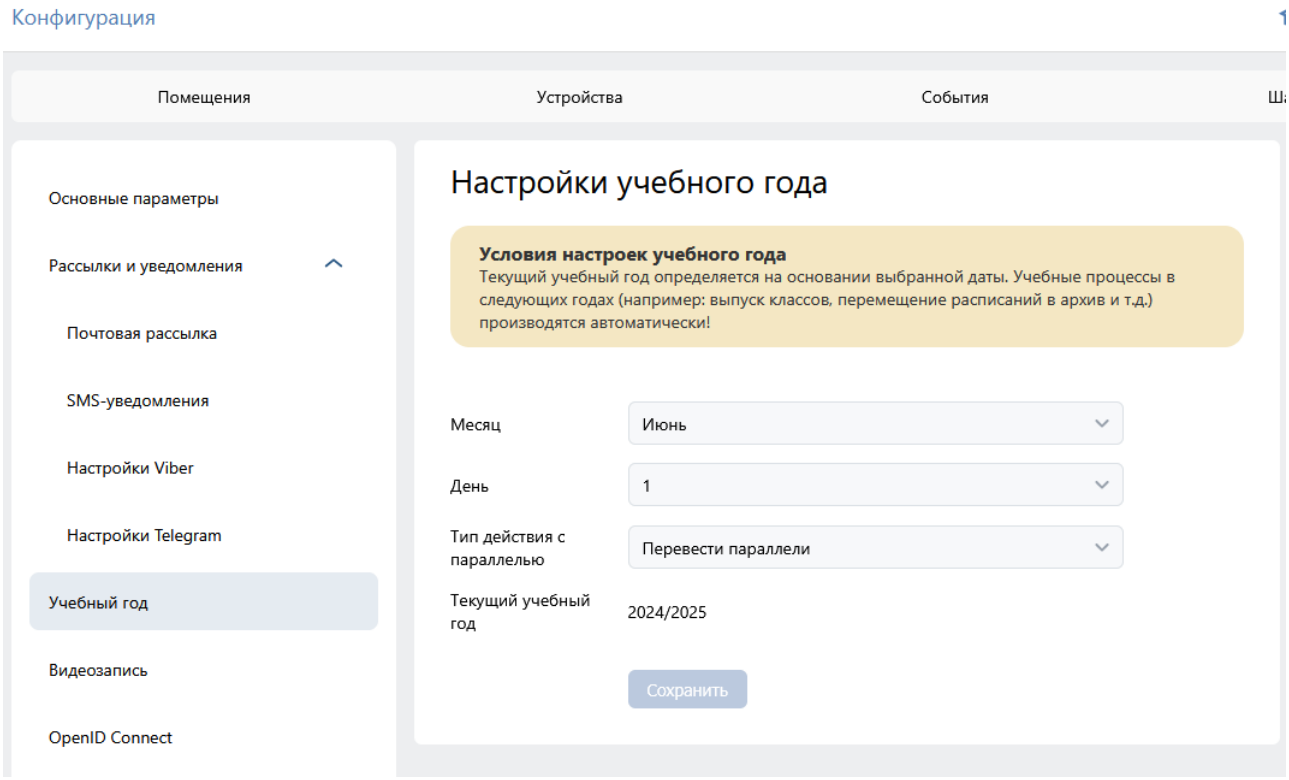


3. Начните разговор с ботом, нажав на кнопку **Начать**, расположенную внизу.
4. Нажмите на кнопку меню и выберите команду «/newbot».
5. Введите имя бота и нажмите **Отправить**.
6. Введите *username* бота. Он должен быть уникальным и заканчиваться на «bot».
7. По завершении настройки BotFather предоставит ссылку на созданного бота и секретный токен для обращения к нему.

SEC.RU | Короткий путь к информации Скачано с sec.ru

17.1.5.9. Подвкладка «Учебный год»

Подвкладка **Учебный год** предназначена для настройки параметров учебного года. Окно имеет следующий вид:

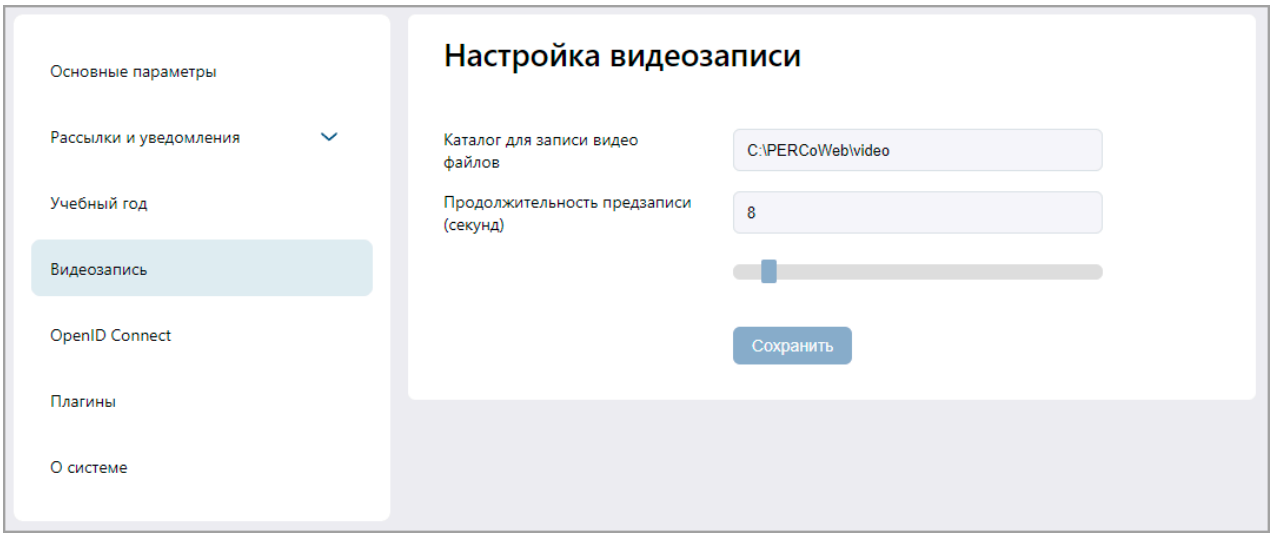


Доступны следующие настройки:

- **Месяц**, **День** – параметры позволяют задать дату окончания учебного года. После указанной даты одиннадцатые классы завершенного учебного года перейдут в архив;
- **Тип действия с параллелью** – параметр позволяет задать тип действия, применяемого к параллели по окончании учебного года (выставленной даты в полях **Месяц** и **День**). Доступны следующие типы:
  - **Архивировать параллели** – все параллели после наступления выбранной даты перейдут в архив;
  - **Перевести параллели** – все классы после наступления выбранной даты автоматически переводятся на следующий год обучения (параллель), последняя 11-я параллель архивируется.

17.1.5.10. Подвкладка «Видеозапись»

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



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Доступны следующие настройки:

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

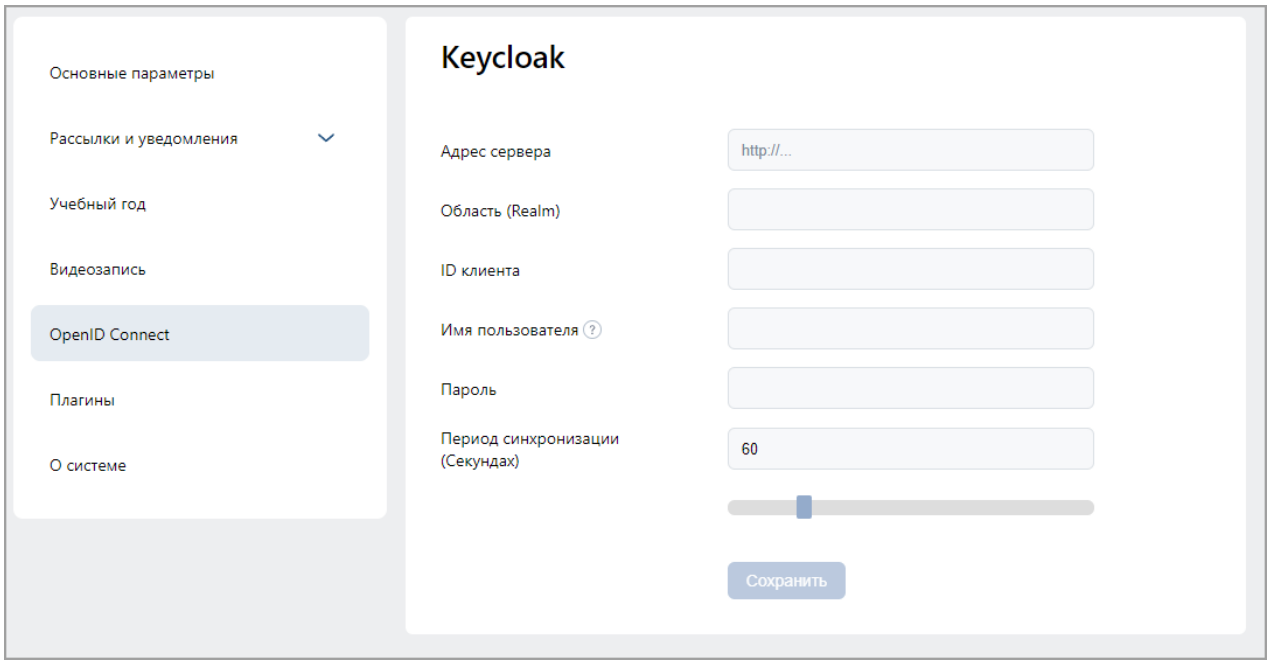
17.1.5.11. Подвкладка «OpenID Connect»

Keycloak – решение для управления идентификацией и доступом.

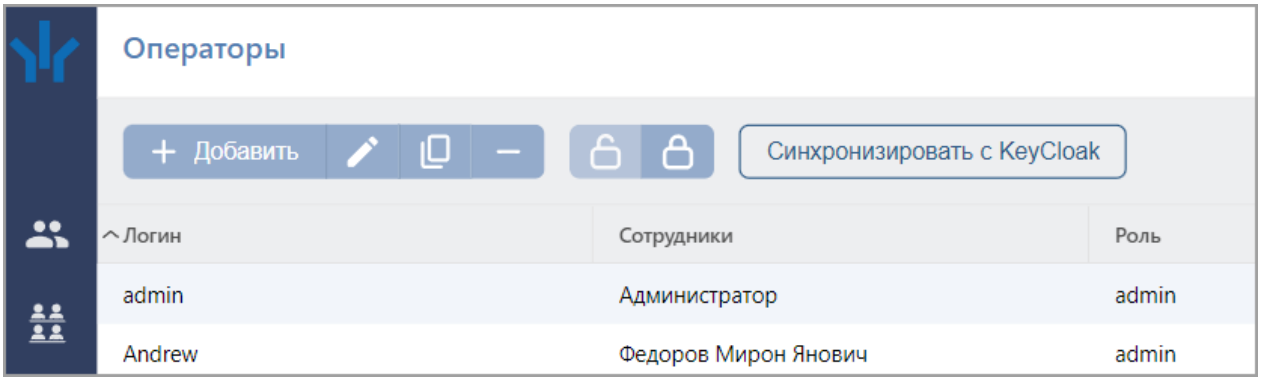
Благодаря синхронизации ***PERCo.Школа*** с ***Keycloak*** есть возможность аутентификации с помощью учетных данных ***Keycloak***. Также реализована автоматическая синхронизация статусов операторов – если оператор был заблокирован/разблокирован в ***Keycloak***, он будет заблокирован/разблокирован в ***PERCo.Школа***.

Для настройки синхронизации выполните следующие действия:

1. Перейдите на подвкладку **OpenID Connect** (***Администрирование > Конфигурация > > Система***):

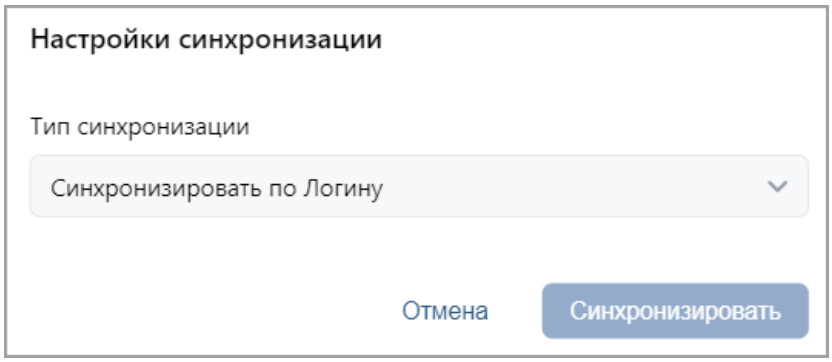


2. Заполните и сохраните данные для подключения к ***Keycloak***-серверу.
3. Перейдите к подразделу ***«Операторы»*** раздела ***«Администрирование»***:

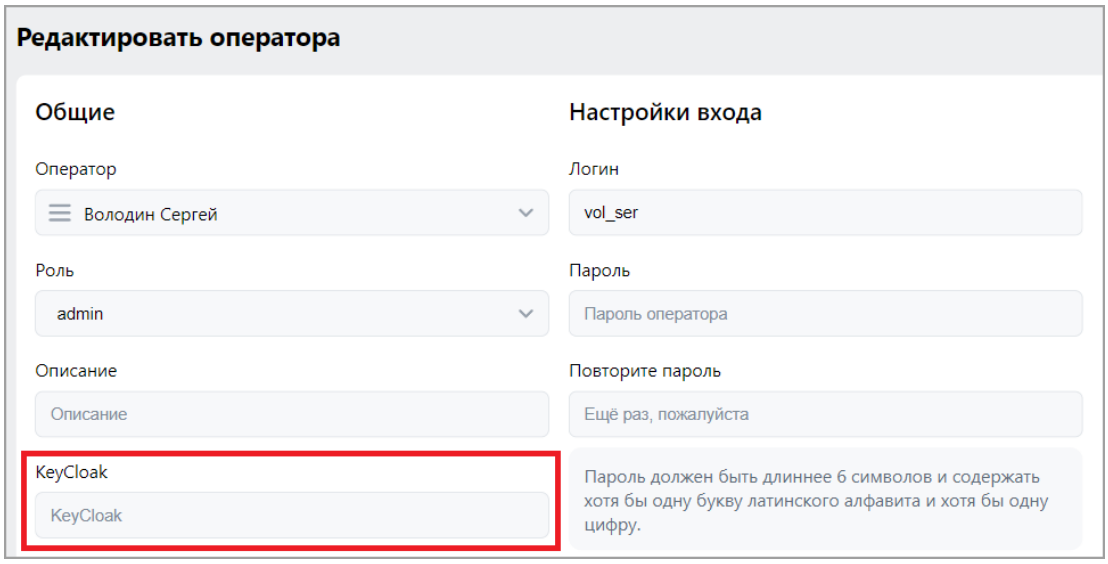


SEC.RU | Короткий путь к информации
Скачано с sec.ru

4. Нажмите на кнопку **Синхронизировать с Keycloak**, расположенную на панели инструментов страницы. Откроется окно:



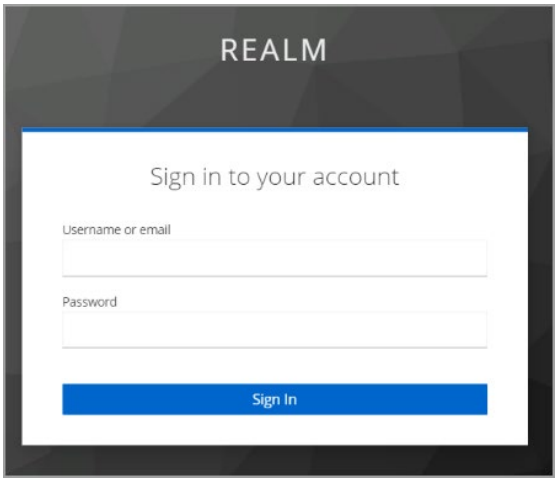
5. Выберите тип синхронизации и нажмите **Синхронизировать**.
6. Вернитесь к подразделу ***«Операторы»*** раздела ***«Администрирование»***.
7. Выберите нужного оператора и нажмите кнопку **Редактировать** на панели инструментов страницы. Откроется страница **Редактировать оператора**:



8. Введите ID пользователя в поле ***Keycloak*** для сопоставления данных.
9. Нажмите кнопку **Сохранить изменения**.

Для авторизации с помощью ***Keycloak***:

1. На странице для авторизации нажмите кнопку **Авторизоваться при помощи Keycloak**.
2. После нажатия произойдет переадресация на страницу авторизации в ***Keycloak***:



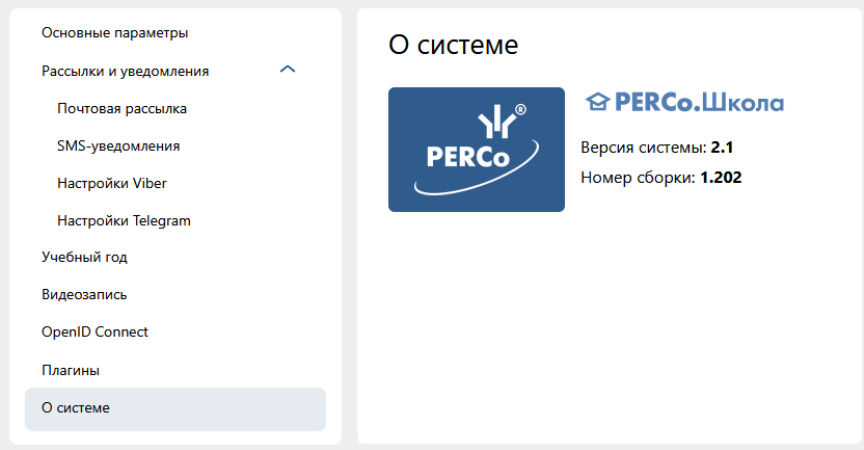
3. Заполните логин и пароль и нажмите кнопку **Sign In**.
4. Произойдет обратная переадресация в ***PERCo.Школа***, вход будет выполнен.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

17.1.5.12. Подвкладка «О системе»

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

Окно имеет следующий вид:

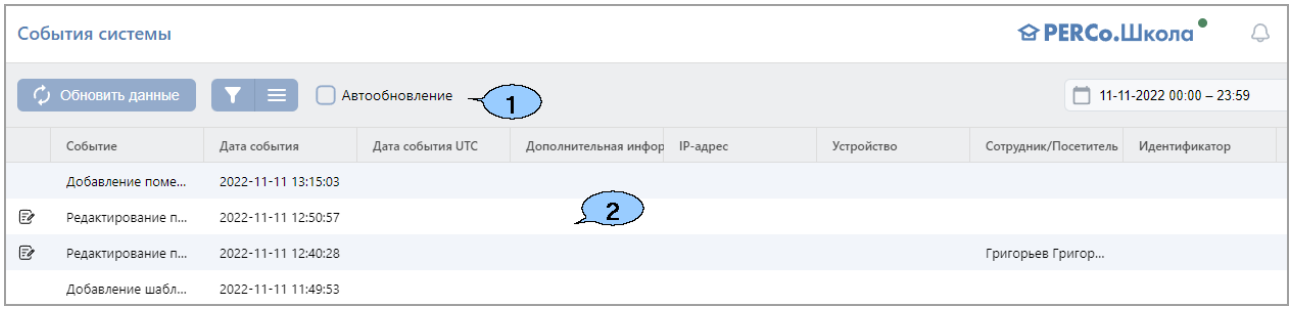


17.2. Подраздел «События системы»

Подраздел предназначен для:

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

Страница подраздела имеет следующий вид:



1. Панель инструментов подраздела содержит:
   - **Обновить данные** – кнопка позволяет обновить данные в рабочей области в соответствии с установленным фильтром.
   - **Расширенный поиск** – позволяет применить фильтр к элементам, отображаемым в рабочей области страницы.
   - **Дополнительно** – кнопка позволяет открыть меню команд для выбора дополнительных действий:
     - **Печать таблицы** – позволяет произвести печать данных из рабочей области страницы.
     - **Экспорт** – позволяет сохранить список событий в файл электронных таблиц с выбранным расширением.
     - **Сбросить фильтры** – позволяет сбросить все фильтры рабочей области.
     - **Параметры отображения таблицы** – позволяет открыть дополнительное окно для выбора столбцов, отображаемых в рабочей области страницы.
   - **Автообновление** – при установке флажка регистрируемые в системе события отображаются в рабочей области в режиме реального времени.
   - – кнопка позволяет открыть панель календаря для ввода даты и времени начала и конца периода, за который будут отображаться события в рабочей области. Установленные дата и время отображаются в поле справа от соответствующей кнопки.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Поиск** – поле позволяет произвести поиск по элементам столбцов в рабочей области страницы. Кнопка **Сбросить** очищает 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.

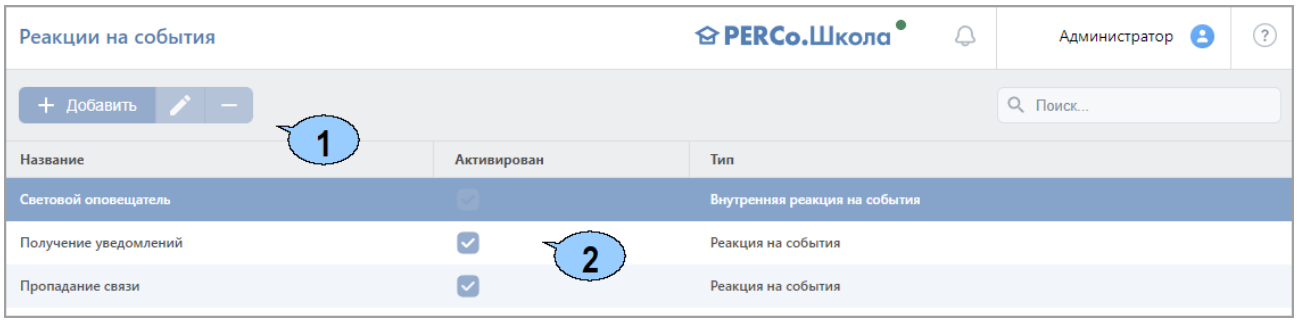
Примечание:

При использовании модуля ***BioSmart Thermoscan F*** температура проходящего будет отображаться в поле **Дополнительная информация**.

17.3. Подраздел «Реакция на события»

Подраздел предназначен для настройки реакций на события системы ***PERCo.Школа***.

Страница подраздела имеет следующий вид:



1. Панель инструментов подраздела содержит кнопки:
   - **Добавить** – позволяет добавить реакцию на событие или внутреннюю реакцию на событие контроллера.
   - **Редактировать** – позволяет изменить параметры выбранной реакции.
   - **Удалить** – позволяет удалить выделенную в рабочей области страницы реакцию.
2. Рабочая область подраздела содержит список созданных реакций. С помощью флажков в столбце **Активирован** можно включать/отключать добавленные реакции на события.

Примечание:

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

17.3.1. Добавление новой реакции

Примечание:

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

Внимание!

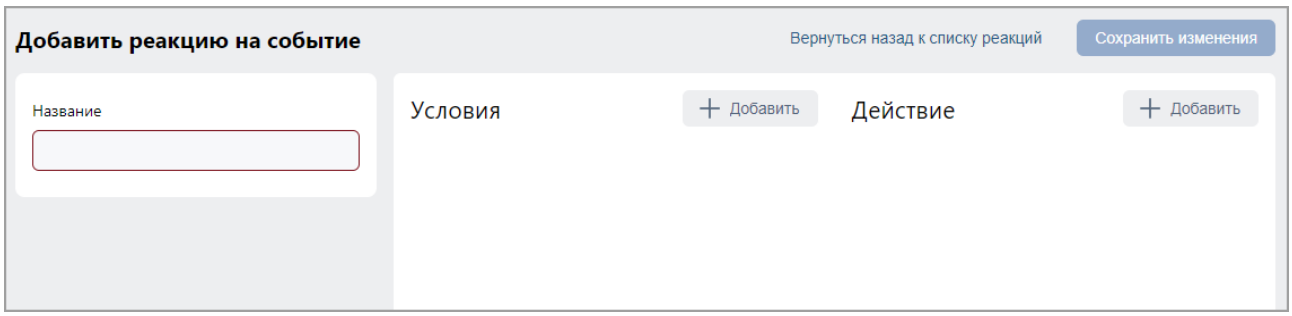
Для выполнения реакций на события необходимо наличие связи с сервером.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Для добавления новой реакции на событие:

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

   Откроется страница, имеющая следующий вид:



4. В поле **Название** введите название для новой реакции.
5. В разделе **Условия** выберите условия для новой реакции. Для этого нажмите кнопку **Добавить** и выберите из списка требуемые условия. В списке доступны следующие условия:
   - **Добавить событие** – позволяет открыть окно, в котором отображается список возможных событий для реакции, и добавить нужное событие.
   - **Добавить помещение** – позволяет открыть окно, в котором отображается список созданных ранее помещений, и добавить нужное помещение.
   - **Добавить устройство** – позволяет открыть окно, в котором отображается список добавленных в конфигурацию системы устройств, и добавить нужное устройство.
   - **Добавить подразделение** – позволяет открыть окно, в котором отображается список созданных ранее подразделений, и добавить нужное подразделение.
   - **Добавить сотрудника** – позволяет открыть окно, в котором отображается список добавленных ранее сотрудников, и добавить нужного сотрудника.
   - **Добавить ограничение по времени** – позволяет открыть окно, в котором есть возможность выбора даты и времени выполнения реакции: **Дни недели** или определенная **Дата**, а также **Время начала** и **Время окончания**.
   - **Добавить сегмент** – позволяет открыть окно, в котором отображается список созданных сегментов, и добавить нужный сегмент.
   - **Добавить класс** – позволяет открыть окно, в котором отображается список созданных ранее классов, и добавить нужный класс.

Примечание:

Кнопка доступна только при работе в режиме распределенной системы.

6. В разделе **Действие** выберите те действия, которые будут происходить при заданных условиях. Список содержит следующие действия:
   - **Команда в устройство** – позволяет выбрать команду для устройства, добавленного в конфигурацию системы ***PERCo.Школа***. Для этого выберите устройство, а затем из выпадающего списка команду для него. Нажмите кнопку **Выбрать**.
   - **Заблокировать сотрудника** – позволяет заблокировать сотрудника или доступ в выбранное помещение сотруднику, для которого было выполнено то или иное условие. Для этого выберите, в какое помещение будет заблокирован доступ. Если помещение не указано, то сотруднику будет заблокирован доступ во все помещения. При необходимости временной блокировки доступа заполните поле **Время блокировки (мин.)**. Нажмите кнопку **Выбрать**.
   - **Заблокировать сотрудника** – позволяет заблокировать сотрудника, для которого было выполнено то или иное условие.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Разблокировать сотрудника** – позволяет разблокировать сотрудника, для которого было выполнено то или иное условие.
- **Сообщение оператору** – позволяет настроить отправку сообщений оператору системы. Для этого выберите оператора, заполните поле в окне **Текст сообщения** и нажмите кнопку **Выбрать**.
- **Сообщение по почте предъявившему идентификатор** – позволяет настроить отправку сообщений по электронной почте предъявившему идентификатор. Для этого заполните поле в окне **Текст сообщения** и нажмите кнопку **Выбрать**.
- **Сообщение по почте сотруднику** – позволяет настроить отправку сообщений по электронной почте сотруднику при выполнении системой реакции на событие. Для этого выберите сотрудника, заполните поле в окне **Текст сообщения** и нажмите кнопку **Выбрать**.
- **SMS-сообщение предъявившему идентификатор** – позволяет настроить отправку SMS-сообщений предъявившему идентификатор. Для этого заполните поле в окне **Текст сообщения** и нажмите кнопку **Сохранить**.
- **SMS-сообщение сотруднику** – позволяет настроить отправку SMS-сообщения сотруднику при выполнении системой реакции на событие. Для этого выберите сотрудника, заполните поле в окне **Текст сообщения** и нажмите кнопку **Выбрать**.
- **Viber-сообщение предъявившему идентификатор** – позволяет настроить отправку сообщений в мессенджер Viber предъявившему идентификатор. Для этого заполните поле в окне **Текст сообщения** и нажмите кнопку **Выбрать**.
- **Viber-сообщение сотруднику** – позволяет настроить отправку сообщений сотруднику в мессенджер Viber при выполнении системой реакции на события. Для этого выберите сотрудника, заполните поле в окне **Текст сообщения** и нажмите кнопку **Выбрать**.
- **Telegram-сообщение предъявившему идентификатор** – позволяет настроить отправку сообщений в мессенджер Telegram предъявившему идентификатор. Для этого заполните поле в окне **Текст сообщения** и нажмите кнопку **Выбрать**.
- **Telegram-сообщение сотруднику** – позволяет настроить отправку сообщений сотруднику в мессенджер Telegram при выполнении системой реакции на события. Для этого выберите сотрудника, заполните поле в окне **Текст сообщения** и нажмите кнопку **Выбрать**.
- **Сообщение родственнику** – позволяет настроить отправку по электронной почте и в мессенджер Telegram родственнику ученика при выполнении системой реакции на событие. Для этого заполните поле в окне **Текст сообщения** и нажмите кнопку **Выбрать**.

Примечание:

Действия отправки сообщений не отображаются, если рассылка не настроена.

- **Показать видеокамеру оператору** – позволяет настроить для оператора отображение видеокамеры. Для этого выберите оператора и нужную камеру, затем нажмите кнопку **Выбрать**.
- **Сохранить снимок с камеры** – позволяет сделать снимок экрана при выполнении системой реакции на событие. Для этого выберите камеру и нажмите кнопку **Выбрать**.

Примечание:

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

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Примечание:

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

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

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

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

```
var server = http.createServer((req, res) => {
var event = '';
req.on('data', (data) => {
event += data;
});
req.on('end', async () => {
res.setHeader("Content-Type", "application/json");
res.setHeader('Access-Control-Allow-Origin', '*');
res.setHeader('Access-Control-Allow-Methods', 'GET, POST, OPTIONS, PUT, PATCH,
DELETE');
res.setHeader('Access-Control-Allow-Headers', 'X-Requested-With,content-type');
if (event.length) {
console.log(`Event from PERCo-Web`,JSON.parse(event));
res.write('{"result":"ok"}');
}
res.end();
});
});
server.listen(50005, '0.0.0.0', (err) => {
if (err) console.log('Test server error', err);
else console.log('Test server started');
});
```

Примечание:

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

7. Нажмите кнопку **Сохранить изменения**.

17.3.2. Добавление внутренней реакции на событие контроллера

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

Примечание:

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

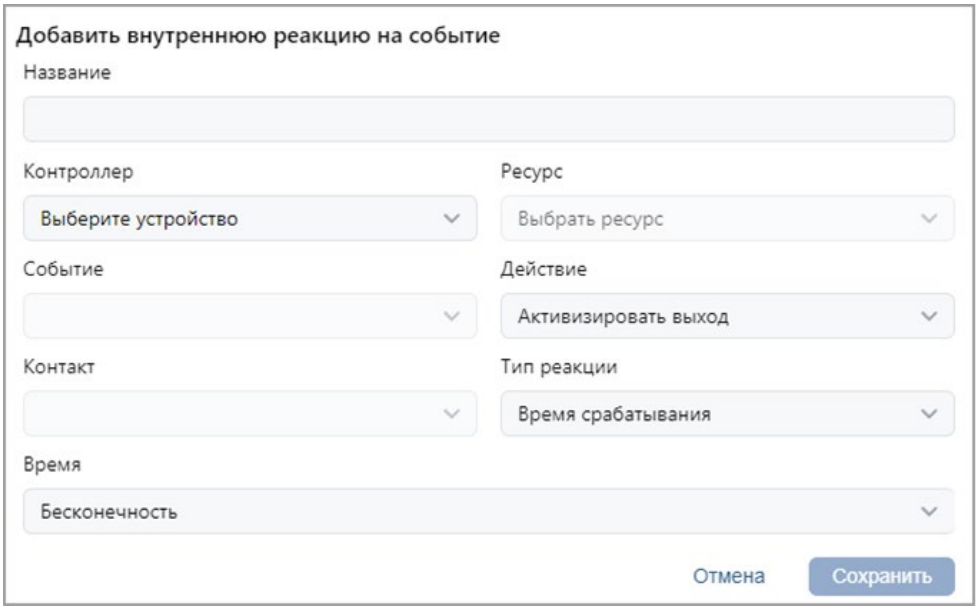
Для добавления внутренней реакции на событие контроллера:

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Откройте подраздел **«Реакции на события»**.

3. Нажмите на панели инструментов страницы кнопку **Добавить**, а затем **Добавить внутреннюю реакцию на событие контроллера**. Откроется окно:



4. В поле **Название** введите название для новой реакции.

5. В поле **Контроллер** нажмите кнопку и выберите из списка нужный контроллер.

Внимание!

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

6. В поле **Событие** нажмите кнопку и выберите из списка событие для внутренней реакции.

7. В поле **Действие** нажмите кнопку и выберите из списка действие для выбранного ранее события:
   - **Активизировать выход**;
   - **Нормализовать выход**;
   - **Маскировать вход**.

8. В поле **Контакт** нажмите кнопку и выберите из списка один из вариантов (**Вход** или **Выход**).

Примечание:

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

9. В поле **Тип реакции** нажмите кнопку и выберите из списка тип реакции:
   - **Время срабатывания**;
   - **Время абсолютное**;
   - **Время после срабатывания**.

10. В поле **Время** нажмите кнопку и выберите один из вариантов (**Бесконечность** или **Секунды**).

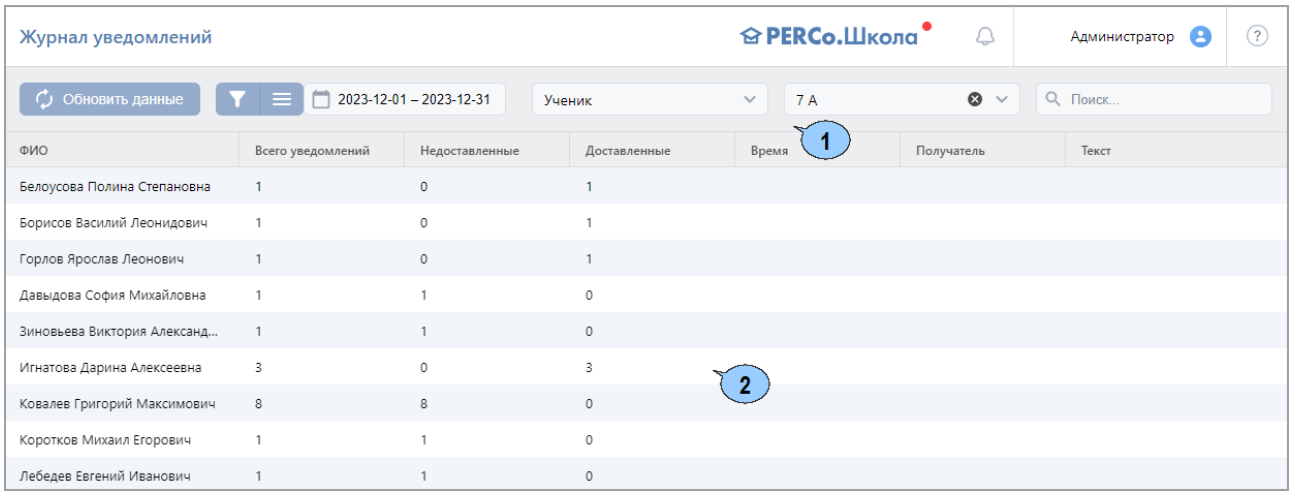
11. Нажмите кнопку **Сохранить**. Окно **Добавить внутреннюю реакцию на событие** будет закрыто, а новая реакция появится в рабочей области страницы.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

17.4. Подраздел «Журнал уведомлений»

Подраздел предназначен для просмотра всех отправленных системой уведомлений.

Страница подраздела имеет следующий вид:



1. Панель инструментов подраздела содержит кнопки:
   - **Обновить данные** – кнопка позволяет обновить данные в рабочей области в соответствии с установленным фильтром.
   - **Расширенный поиск** – позволяет применить фильтр к элементам, отображаемым в рабочей области страницы.
   - **Дополнительно** – кнопка позволяет открыть меню команд для выбора дополнительных действий:
     – **Печать таблицы** – позволяет произвести печать данных из рабочей области страницы.
     – **Экспорт** – позволяет сохранить данные рабочей области в файл электронных таблиц с выбранным расширением.
     – **Сбросить фильтры** – позволяет сбросить все фильтры рабочей области.
     – **Параметры отображения таблицы** – позволяет открыть дополнительное окно для выбора столбцов, отображаемых в рабочей области страницы.
   - – кнопка позволяет открыть панель календаря для ввода даты начала и конца периода, за который будут отображаться события в рабочей области. Установленнfz дата отображаттся в поле справа от соответствующей кнопки.
   - Поле **Выберите тип пользователя** – кнопка внутри поля позволяет выбрать тип пользователей, уведомления для которых будут отображаться в рабочей области страницы. Кнопка **Сбросить** очищает поле. Раскрывающийся список позволяет выбрать один из следующих типов пользователей:
     - **Сотрудник**;
     - **Посетитель**;
     - **Ученик**;
     - **Родственник**.
   - Поле **Подразделение/Класс** – кнопка внутри поля позволяет выбрать подразделение или класс, уведомления для сотрудников, учеников, родственников учеников или посетителей которого будут отображаться в рабочей области страницы. Кнопка **Сбросить** очищает поле.
   - **Поиск** – поле позволяет произвести поиск по элементам столбцов в рабочей области страницы. Кнопка **Сбросить** очищает поле.
2. Рабочая область страницы содержит список отправленных системой уведомлений выбранным пользователям за указанным на панели инструментов страницы период.

SEC.RU | Короткий путь к информации Скачано с sec.ru

17.5. Подраздел «Задания»

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

Внимание!

Для выполнения заданий необходимо наличие связи с сервером.

Доступны следующие виды заданий:

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

Страница подраздела имеет следующий вид:



1. Панель инструментов страницы содержит:
   - **Добавить** – кнопка позволяет создать новое задание.
   - **Редактировать** – кнопка позволяет изменить параметры выделенного в рабочей области страницы задания.
   - **Удалить** – кнопка позволяет удалить выделенное в рабочей области страницы задание.
2. Рабочая область подраздела содержит список заданий сервера системы.

Примечание:

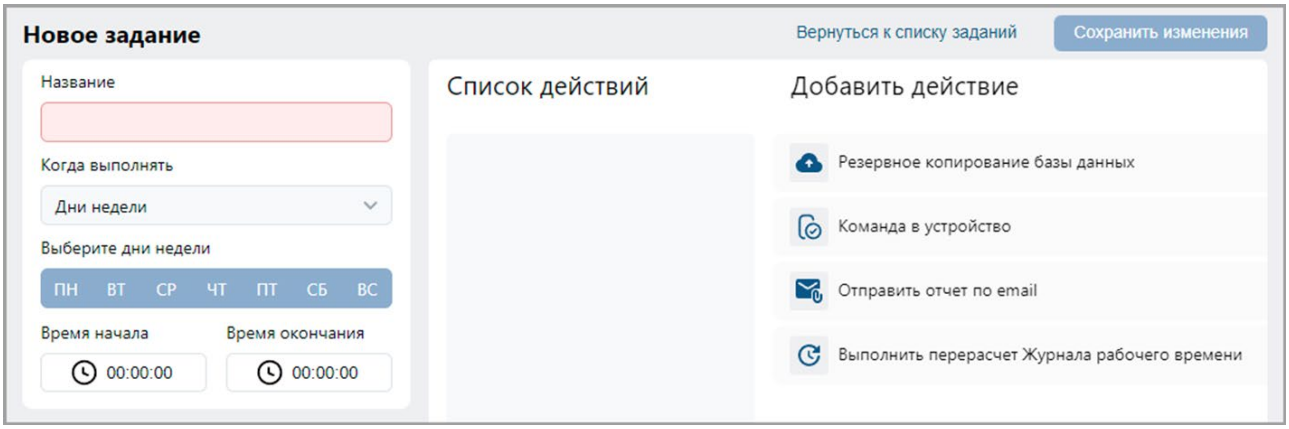
В рабочей области реализованы функции сортировки по элементам одного из столбцов и изменения ширины столбцов.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

17.5.1. Создание нового задания

Для создания нового задания:

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



4. В поле **Название** введите название для нового задания.
5. В списке **Когда выполнять** 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.
   - **День месяца** – если задание необходимо выполнять ежемесячно. С помощью соответствующих кнопок укажите день месяца, в который будет запускаться задание.
   - С помощью полей ввода **Время начала** и **Время окончания** укажите период времени в течение суток, в который задание необходимо запустить.

Примечание:

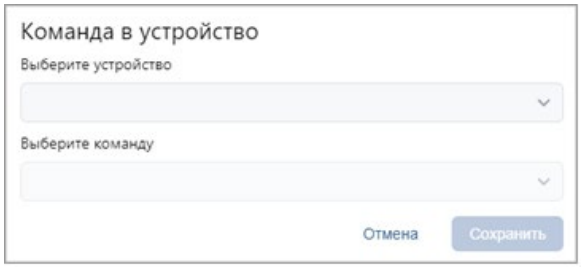
Для выполнения заданий рекомендуется выбирать период времени, когда совершается минимальное количество проходов и минимальное количество операторов подключено к серверу системы.

6. В разделе **Добавить действие** выберите один из следующих типов заданий:
   - **Резервное копирование базы данных** – позволяет создать задание по сохранению резервной копии БД (по умолчанию БД сохраняется в папке *C:\ProgramData\PERCo-Web School\mysql* в файле с расширением *.sql*). Задание добавляется в раздел **Список действий**.

Примечание:

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

   - **Команда в устройство** – позволяет выбрать команду для устройства, добавленного в конфигурацию системы ***PERCo.Школа***. При выборе данного типа задания откроются дополнительные настройки:

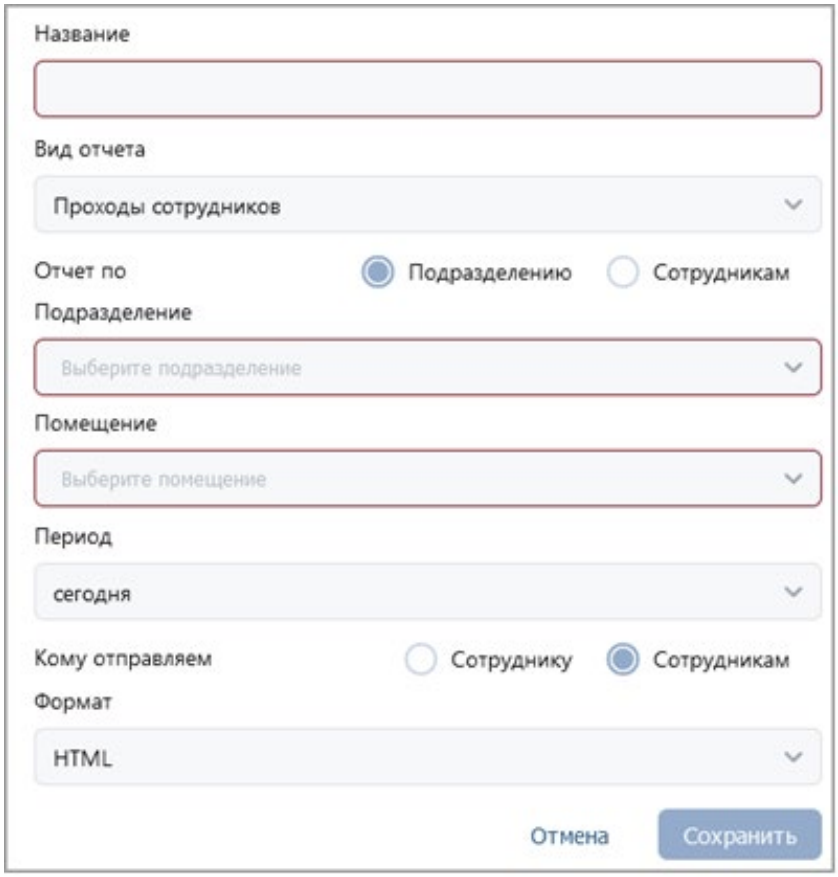


SEC.RU | Короткий путь к информации
Скачано с sec.ru

В поле **Выберите устройство** выберите из выпадающего списка устройство, а затем в поле **Выберите команду** – команду для него. Нажмите кнопку **Сохранить**, данное задание добавится в список.

- **Отправить отчет по email** – позволяет создать задание по отправке отчета одному или нескольким сотрудникам. При выборе данного типа задания откроются дополнительные настройки:

  Окно содержит элементы:



  – **Название** – поле предназначено для ввода названия отчета.
  – **Вид отчета** – выпадающий список позволяет выбрать вид отчета:
    - **отчет о проходах сотрудников**;
    - **отчет о нарушениях сотрудников**;
    - **отчет о времени присутствия сотрудников**;
    - **отчет о присутствующих на данный момент**;
    - **отчет об отсутствующих сегодня**;
    - **отчет об опоздавших сегодня**;
    - **отчет о переработке сотрудников**;
    - **отчет Т13;**
    - **отчет по проходам учеников;**
    - **отчет по выданным объяснительным;**
    - **присутствующие на данный момент ученики;**
    - **отсутствующие сегодня ученики;**
    - **опоздавшие сегодня ученики;**
    - **ушедшие раньше ученики**.
  – **Отчет по** – параметр позволяет выбрать объект отчетности:
    - **Подразделению** – для составления отчета по сотрудникам конкретного подразделения. При установке флажка появляется поле **Подразделение**, в котором с помощью кнопки необходимо выбрать требуемое подразделение.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- **Сотрудникам** – для составления отчета по определенным сотрудникам. При установке флажка появляется поле для вывода списка сотрудников, в котором с помощью кнопки необходимо выбрать сотрудников.

– **Период** – выпадающий список позволяет выбрать период отчетности. При выборе отчета **Т13** в окне также появляется флажок **Показ минут**, при его установке в отчете будут выведены данные с точностью до минуты.

– **Кому отправляем** – параметр позволяет выбрать получателя отчета:

- **Сотруднику** – при установке флажка появляется поле **Сотрудник**, в котором с помощью кнопки необходимо выбрать сотрудника, которому будет отправляться отчет.
- **Сотрудникам** – при установке флажка отчет будет высылаться всем сотрудникам, выбранным с помощью параметра **Отчет по сотрудникам**.

Каждый сотрудник будет получать отчет только по своим данным.

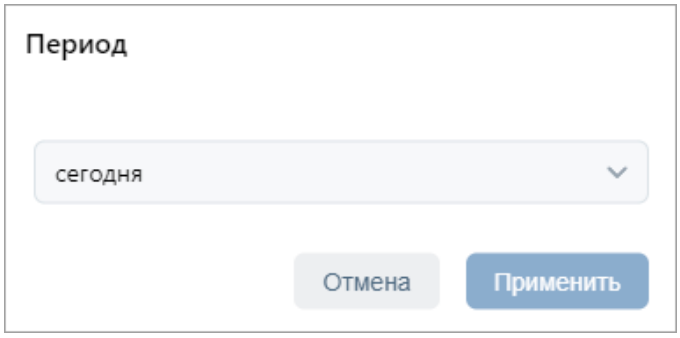
Внимание!

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

– **Формат** – выпадающий список позволяет выбрать формат файла отчета – **HTML**, **XLSX** или **CSV**.

После заполнения параметров отчета нажмите кнопку **Сохранить**, данное задание добавится в список действий.

- **Выполнить перерасчет Журнала рабочего времени** – позволяет создать задание по перерасчету рабочего времени сотрудников в подразделе ***«Журнал отработанного времени»*** раздела ***«Учет рабочего времени»***.
  При выборе данного типа задания откроется окно **Период** с выпадающим списком:



В выпадающем списке выберите период, за который будет сформирован отчет:

- **сегодня**;
- **вчера**;
- **с начала недели**;
- **с начала месяца**;
- **предыдущая неделя**;
- **предыдущий месяц**;
- **первая половина месяца**;
- **вторая половина предыдущего месяца**.

Нажмите кнопку **Сохранить**, данное задание добавится в список действий.

7. Для удаления действия из списка нажмите кнопку .
8. После установки времени и действий для нового задания нажмите кнопку **Сохранить изменения**, новое задание появится в рабочей области страницы.

Примечание:

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

17.6. Подраздел «Операторы»

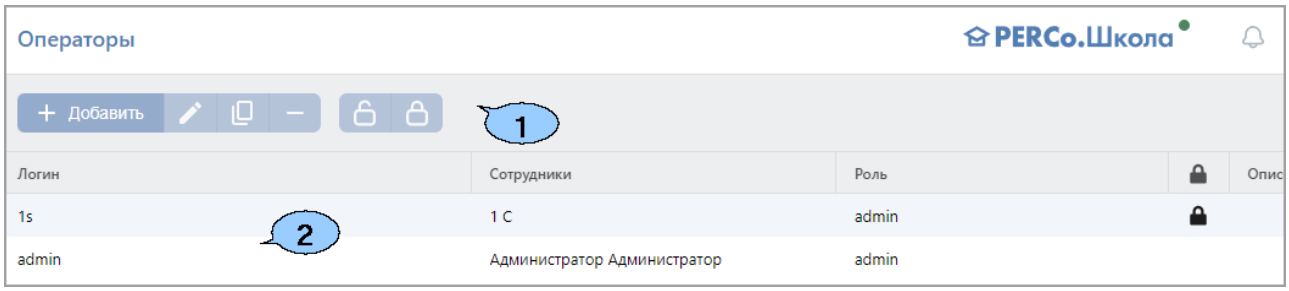
Примечание:

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

Подраздел предназначен для:

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

Страница подраздела имеет следующий вид:



1. Панель инструментов страницы:
   - **Добавить оператора** – кнопка позволяет добавить нового оператора.
   - **Редактировать оператора** – кнопка позволяет изменить данные оператора, выделенного в рабочей области страницы.
   - **Скопировать оператора** – кнопка позволяет скопировать данные оператора, выделенного в рабочей области страницы, для создания нового оператора.
   - **Удалить оператора** – кнопка позволяет удалить выделенного в рабочей области страницы оператора.
   - **Заблокировать оператора** – кнопка позволяет временно блокировать возможность доступа в систему оператора, выделенного в рабочей области страницы.
   - **Разблокировать оператора** – кнопка позволяет разблокировать ранее заблокированную возможность доступа в систему для оператора, выделенного в рабочей области страницы.
   - **Поиск** – поле позволяет произвести поиск по элементам столбцов в рабочей области страницы. Кнопка **Сбросить** очищает 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.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

17.6.1. Добавление оператора системы

Примечание:

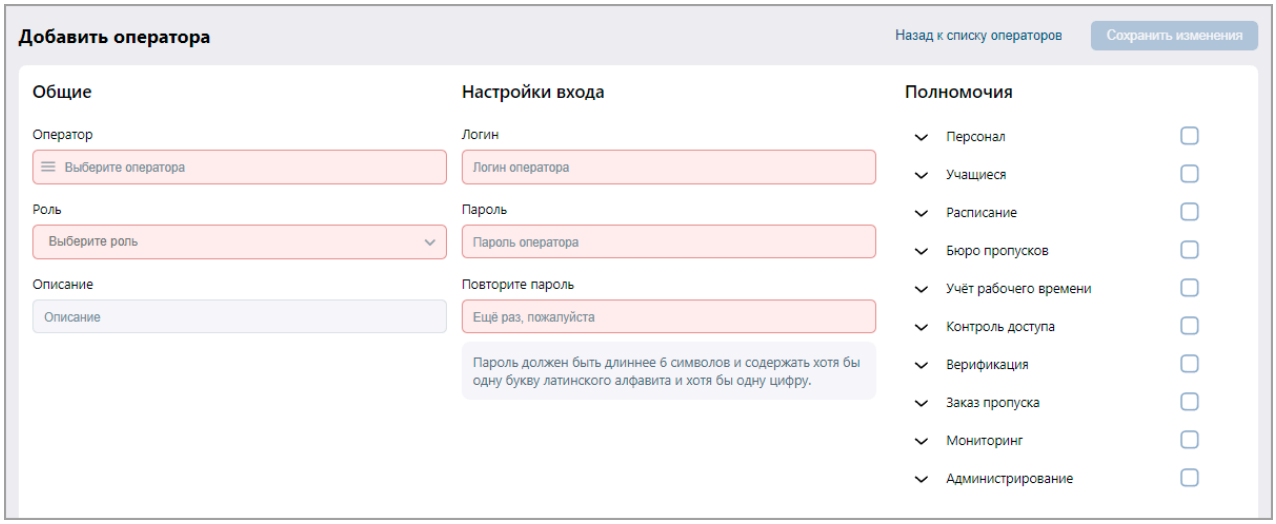
Перед добавлением операторов создайте в подразделе **«Роли и права операторов»** раздела **«Администрирование»** необходимые роли операторов и выдайте им полномочия.

Внимание!

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

Для добавления нового оператора выполните следующие действия:

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



4. В поле **Оператор** выберите из выпадающего списка необходимого сотрудника.
5. В полях **Логин** и **Пароль** укажите для оператора его логин и пароль.
6. В поле **Роль** с помощью кнопки укажите для оператора его полномочия. Роли операторов создаются в подразделе **«Роли и права операторов»**.
7. При необходимости укажите для оператора **Описание**.
8. В разделе **Полномочия** 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 выдачи оператору полномочий на подраздел **«Роли и права операторов»** раздела **«Администрирование»** ему предоставляется возможность создавать новые роли операторов и изменять права созданных ранее ролей. Это может привести к несанкционированному изменению полномочий ролей.

9. Нажмите кнопку **Сохранить изменения**, новый оператор будет добавлен в список в рабочей области страницы.

SEC.RU | Короткий путь к информации Скачано с sec.ru

17.7. 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.

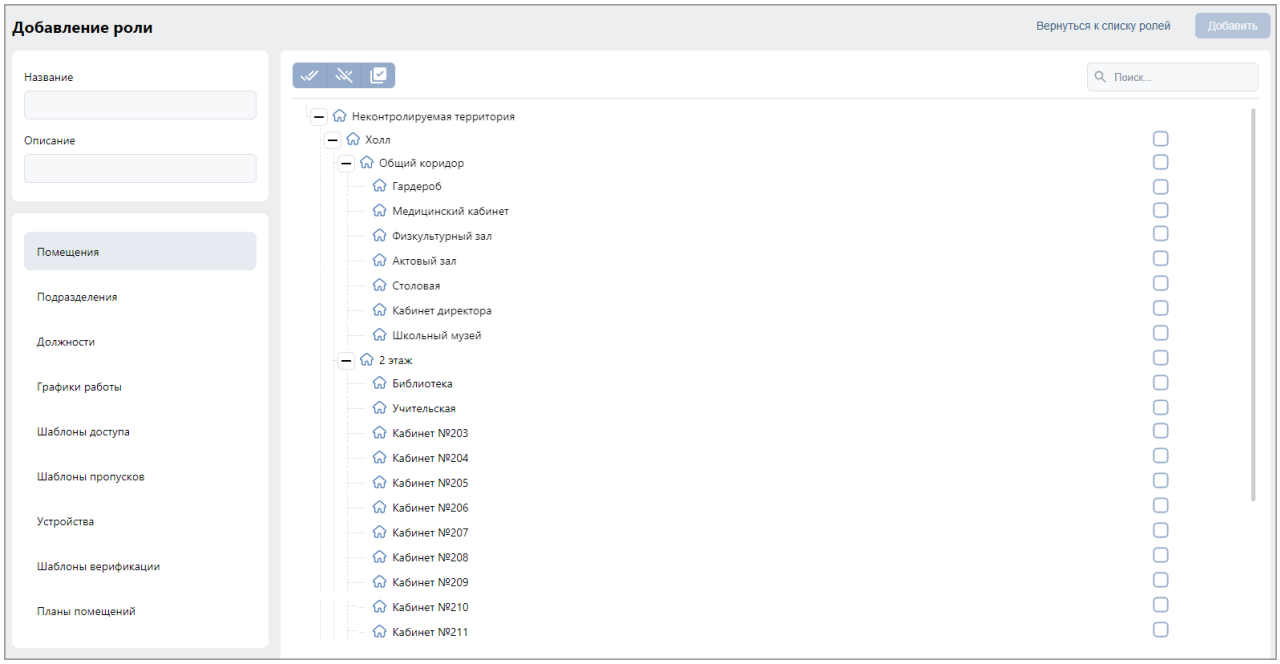
Примечание:

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

17.7.1. Добавление роли оператора (набора полномочий)

Для добавления новой роли оператора:

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



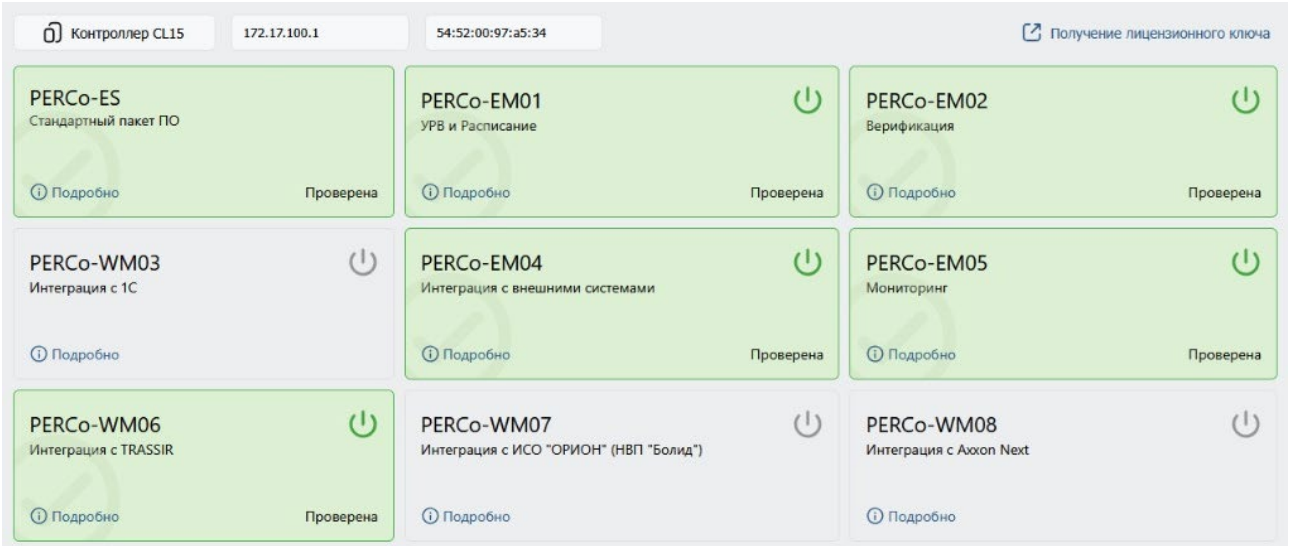
SEC.RU | Короткий путь к информации
Скачано с sec.ru

4. В поле **Название** введите название роли, в поле **Описание** при необходимости введите дополнительную информацию о роли.
5. Выдайте полномочия созданной роли. Для этого с помощью переключателя выберите тип полномочий. При этом в рабочей области страницы появится список объектов данного типа, доступных в системе. Доступны следующие типы полномочий:
   - **Помещения**;
   - **Подразделения**;
   - **Должности**;
   - **Графики работы**;
   - **Шаблоны доступа**;
   - **Шаблоны пропусков**;
   - **Устройства**;
   - **Шаблоны верификации**;
   - **Планы помещений**.
6. Установите флажки у тех объектов, полномочия на которые должны быть доступны для созданной роли оператора. При необходимости используйте кнопки **Выбрать все** и **Снять выделение**. Также есть возможность включить в список все последующие добавленные элементы. Для этого воспользуйтесь кнопкой **Безусловные права**.
7. С помощью переключателя выберите другой тип объектов и выдайте на них полномочия.
8. Нажмите кнопку **Добавить**, новая роль будет добавлена в список в рабочей области страницы.
9. Для добавления нового оператора системы откройте подраздел **«Операторы»**.

17.8. Подраздел «Лицензии»

Подраздел предназначен для ввода кодов активации установленных модулей ПО системы.

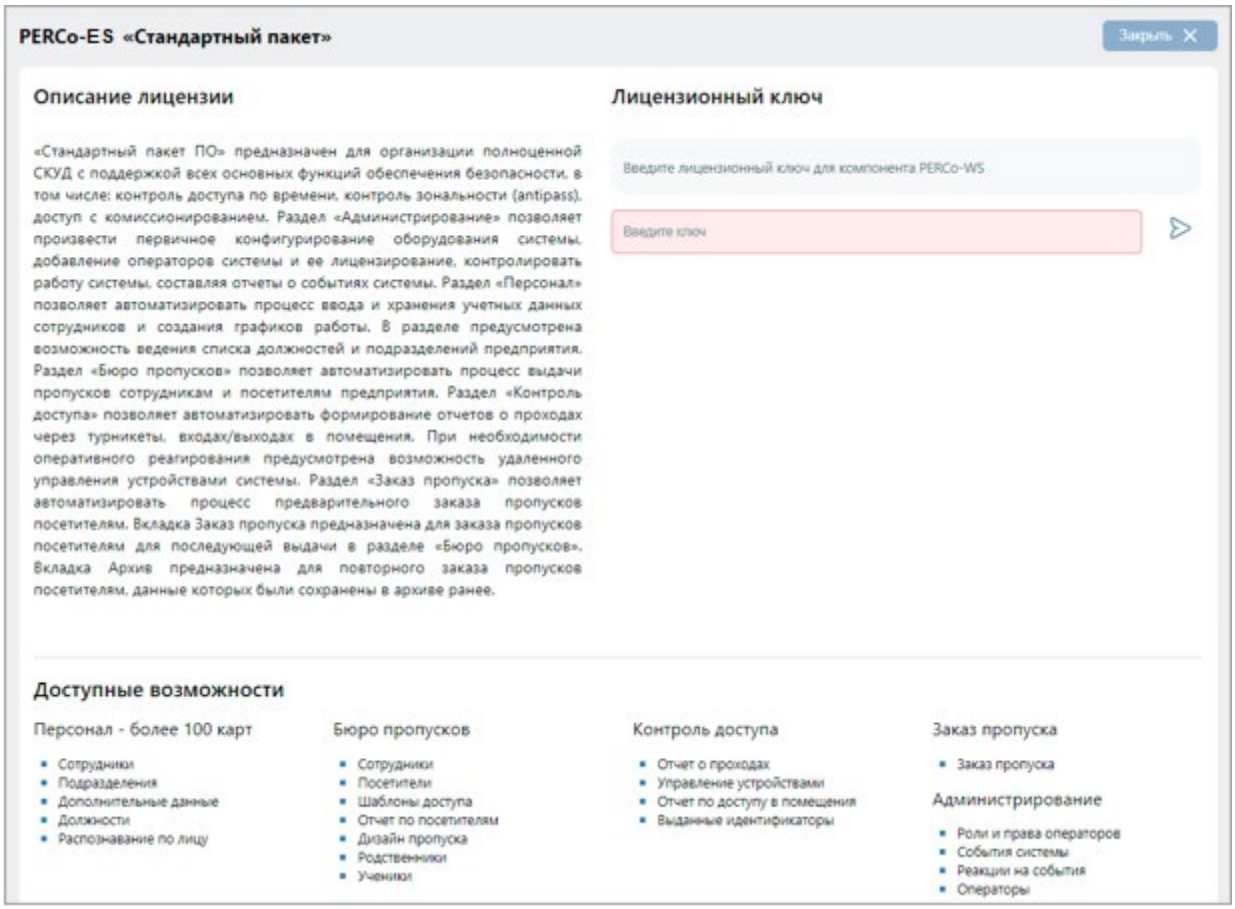
Страница подраздела имеет следующий вид:



1. Кнопка **Лицензионный контроллер** позволяет выбрать контроллер, который будет использоваться в качестве электронного ключа защиты ПО системы, и поля для отображения IP- и MAC-адресов выбранного контроллера.
2. Рабочая область вкладки содержит список установленных модулей и информацию о лицензии.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

После нажатия на **Подробно** одного из модулей открывается панель активации лицензии, которая выглядит следующим образом:



Вид панели зависит от выбранного модуля.

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

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

17.8.1. Ввод кода активации

Для ввода кодов активации модулей ПО системы:

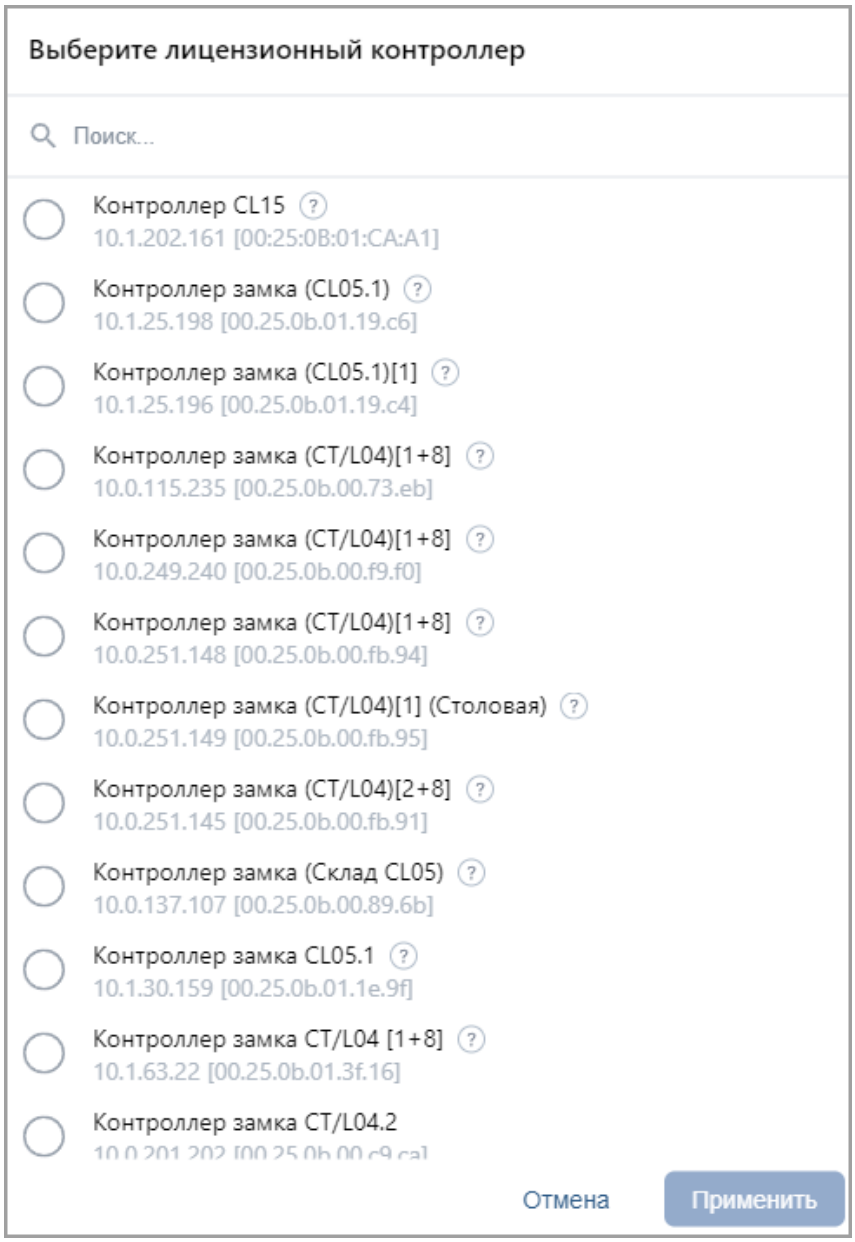
1. Используя панель навигации, перейдите в раздел  **«Администрирование»**.
2. Откройте подраздел **«Лицензии»**.

Примечание:

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3. Нажмите на кнопку **Лицензионный контроллер**. Откроется окно **Выберите лицензионный контроллер**:



4. В открывшемся окне выделите контроллер, выбранный в качестве электронного ключа защиты ПО системы. Нажмите кнопку **Применить**.
5. Окно **Выберите лицензионный контроллер** будет закрыто. На панели **Лицензионный контроллер** появятся IP-, MAC-адреса и наименование выбранного контроллера.
6. В рабочей области вкладки выделите название модуля, для которого необходимо ввести код активации. Откроется панель активации лицензии выбранного модуля.
7. В поле **Лицензионный ключ** введите код активации, указанный для выделенного модуля в лицензионном соглашении. Код вводится без пробелов и разделителей. Нажмите кнопку справа от поля.
8. Сервер системы проверит введенный код. При правильном вводе лицензия будет активирована, цвет модуля изменится на зеленый (бессрочная лицензия) или желтый (временное ограничение).
9. В случае ошибки при вводе кода активации, несоответствия кода выбранному модулю или контроллеру, нарушения связи с контроллером отобразится соответствующее предупреждение.

SEC.RU | Короткий путь к информации Скачано с sec.ru

18. Параметры контроллеров PERCo

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

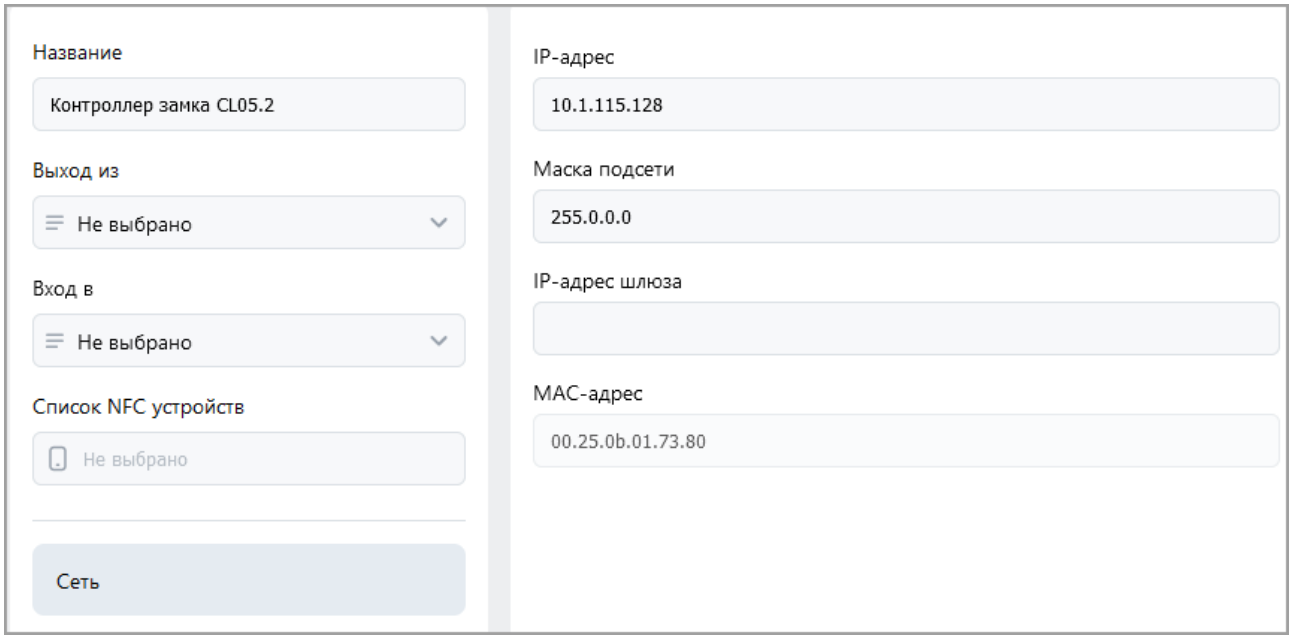
- **Внешние подключения** – информация о внешних подключениях контроллера;
- **Сеть**;
- **Разное**;
- **ИУ (Замок, Турникет, Шлагбаум)**;
- **Входы**;
- **Выходы**;
- **Выводы**;
- **Генератор тревоги**;
- **Свойства ЛИКОНА**;
- **Строки**;
- **Состояние** – информация о состоянии контроллера;
- **Считыватель**.

18.1. Вкладка «Сеть»

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

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

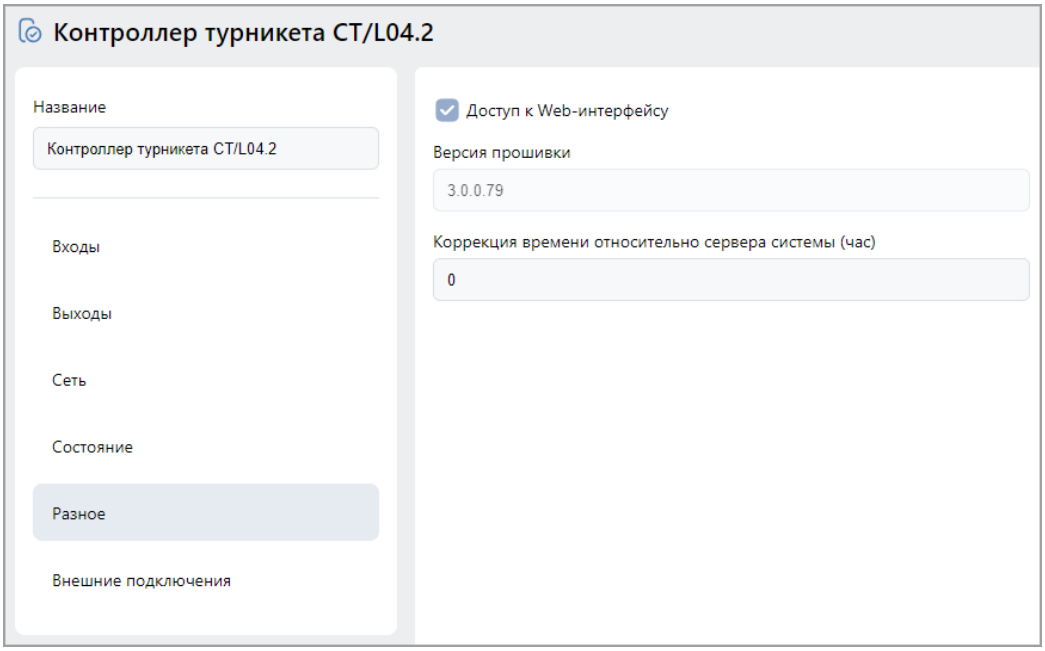
Вкладка выглядит следующим образом:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

18.2. Вкладка «Разное»

Вкладка выглядит следующим образом:

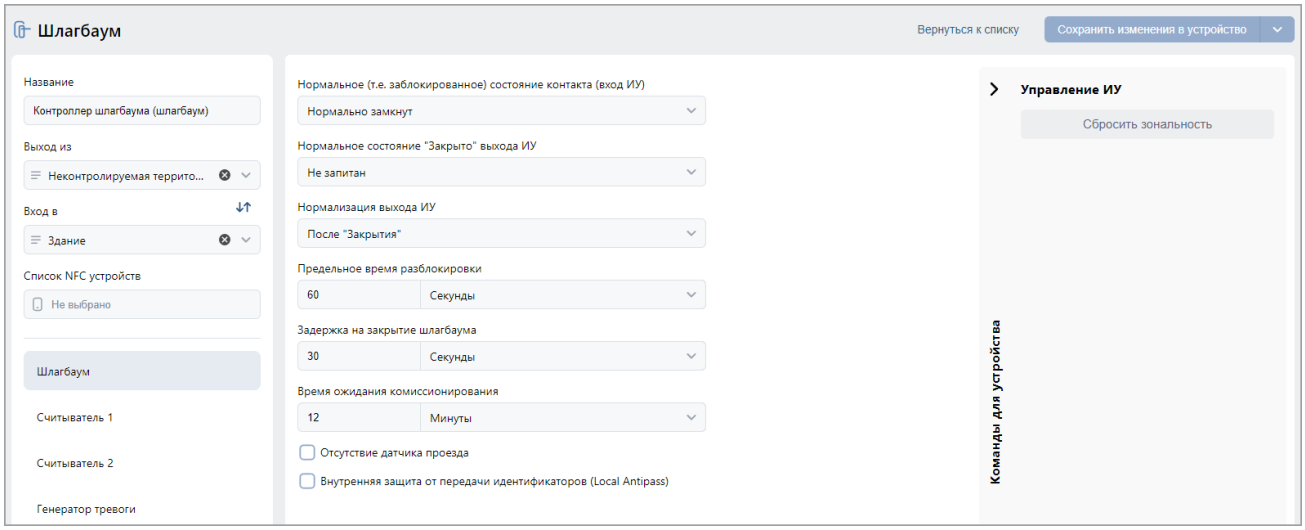


Вкладка **Разное** содержит следующие настройки:

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

18.3. Вкладка ИУ («Замок», «Турникет», «Шлагбаум»)

Вкладка выглядит следующим образом:



Для настройки входов доступны следующие параметры:

- **Нормальное (т.е. заблокированное) состояние контакта (вход ИУ)** (*Нормально разомкнут* / *Нормально замкнут*). Параметр позволяет указать состояние датчика двери / выхода PASS турникета при заблокированном состоянии данного ИУ.
- **Нормальное состояние «Закрыто» выхода ИУ** (*Не запитан* / *Запитан*). Параметр указывает, активизирован ли выход управления ИУ (подано управляющее напряжение на реле или транзистор) при заблокированном ИУ.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **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 / задержка на закрытие шлагбаума)**. Параметр позволяет задать время, которое должно пройти от разблокировки ИУ до его блокировки после успешной аутентификации. За это время необходимо совершить проход / проезд, иначе ИУ заблокируется. Параметр может быть задан в интервале: от 250 до 750 миллисекунд с шагом 250 миллисекунд; от 1 секунды до 4 минут; бесконечно.
- **Время ожидания комиссионирования**. Параметр позволяет ограничить интервал времени между предъявлением идентификатора пользователя (сотрудника / ученика / родственника ученика / посетителя / служебного ТС) и комиссионирующей карты (сотрудника / охранника / водителя) в случае, если в правах идентификатора пользователя установлен доступ с комиссионированием / доступ с досмотром / подтверждение проезда картой водителя.
- **Регистрация прохода по предъявлению идентификатора (отсутствие датчика проезда)**. 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!

Функции верификации и контроля зональности (Antipass) не будут работать при активной регистрации прохода по предъявлению идентификатора.

- **Внутренняя защита от передачи идентификаторов (Local Antipass)**. При установленном параметре контроллер отслеживает случаи повторного предъявления одного и того же идентификатора к тому же считывателю.
- **Режим работы выхода управления ИУ**. Параметр позволяет выбрать режим управления подключенным ИУ:
  - **Потенциальный**.
  - **Импульсный** – режим управления применяется только для замков, поддерживающих этот режим. Рекомендуется использовать для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки «CISA»).
- **Смена зоны при проходе**. Параметр нужен для смены пространственных зон при работе с функцией Global Antipass.
- **Fire Alarm в режиме «Охрана»**. При установленном флажке аварийная разблокировка (открытие прохода ИУ) в случае поступления управляющего сигнала от устройства Fire Alarm произойдет также при взятой на охрану ОЗ, включающей данное ИУ. При снятом параметре (по умолчанию) в РКД *«Охрана»* сигналы на входах **Тип: Fire Alarm** игнорируются.

18.4. Вкладка «Входы»

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

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

  - **Подтверждение от ВВУ**. Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае **разрешения** прохода.
  - **Запрет от ВВУ**. Предназначен для подключения выхода ВВУ, на который подается управляющий сигнал в случае **запрета** прохода.
- **Нормальное состояние контакта** (*Разомкнут / Замкнут*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

В зависимости от выбранного типа остальные параметры входа могут различаться.

Тип **Обычный**:

- **Временной критерий маскирования / активизации / нормализации**:
  - **На указанное время**. Выбранные дополнительные входы будут маскированы / активизированы / нормализованы на указанное время.
  - **На время срабатывания**. Выбранные дополнительные входы будут маскированы / активизированы / нормализованы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
  - **На время срабатывания и после срабатывания**. Выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы / активизированы / нормализованы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал, плюс указанное время.
- **Дополнительные входы, маскируемые при активизации**. Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы (т.е. не воспринимать управляющий сигнал от внешнего оборудования) при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные входы, которые должны быть маскированы. Укажите временной критерий маскирования.
- **Дополнительные выходы, активизируемые при активизации**. Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть активизированы. Укажите временной критерий активизации. Следует заметить, что активизация релейного выхода, привязанная к активизации дополнительного входа, не учитывает возможного шунтирования этого входа. Это очень важно для случаев применения ДКЗП.
- **Дополнительные выходы, нормализируемые при активизации**. Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте те дополнительные выходы, которые должны быть нормализированы. Укажите временной критерий нормализации.

Тип **Специальный**:

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

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

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

18.5. Вкладка «Выходы»

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

- **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**).

SEC.RU | Короткий путь к информации Скачано с sec.ru

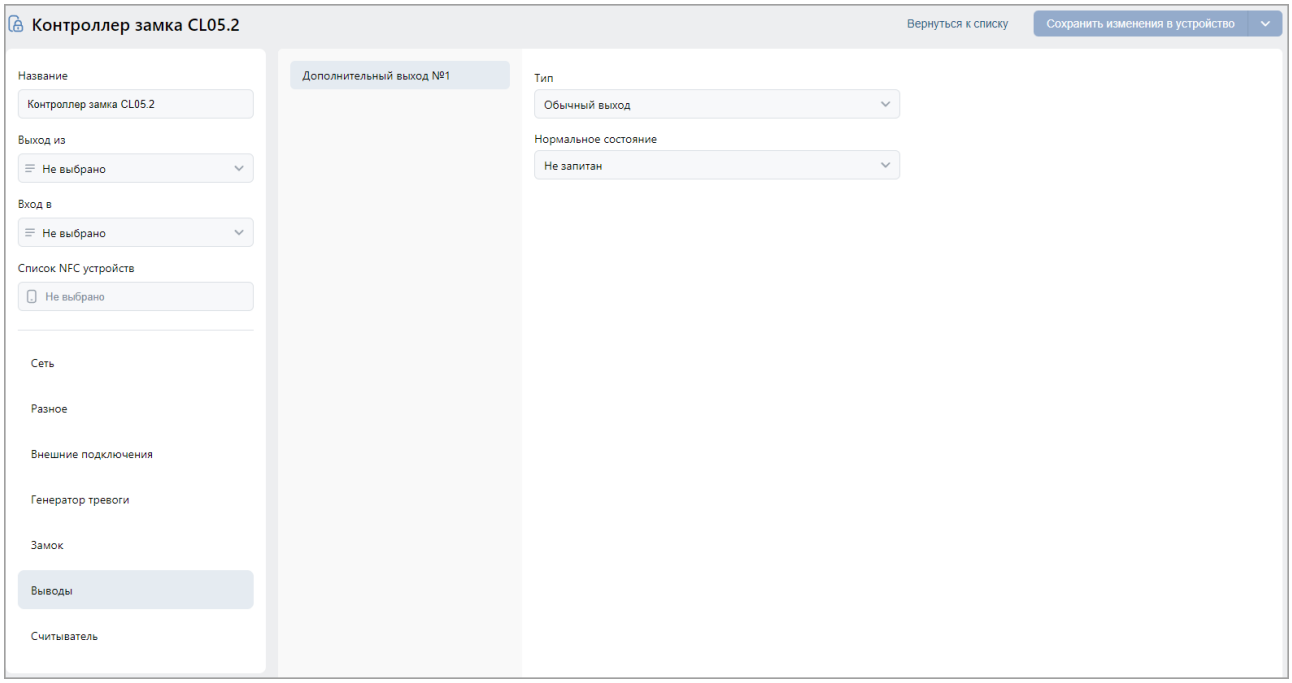
  - **Генератор тревоги**. Решение об активизации дополнительного выхода принимается в соответствии с параметрами, заданными для ресурса **Генератор тревоги**.
- **Нормализованное состояние** (*Не запитан* / *Запитан*). Параметр определяет, подано ли управляющее напряжение на реле выхода при нормализованном состоянии выхода. Для выходов № 1 и № 2 нормализованное состояние: **Не запитан**.
- **Время активизации**. Время, на которое выход, при наличии активизирующего управляющего воздействия, меняет свое состояние из нормализированного на противоположное.

Примечание:

После включения питания все выходы нормализуются.

18.6. Вкладка «Выводы»

Вкладка выглядит следующим образом:



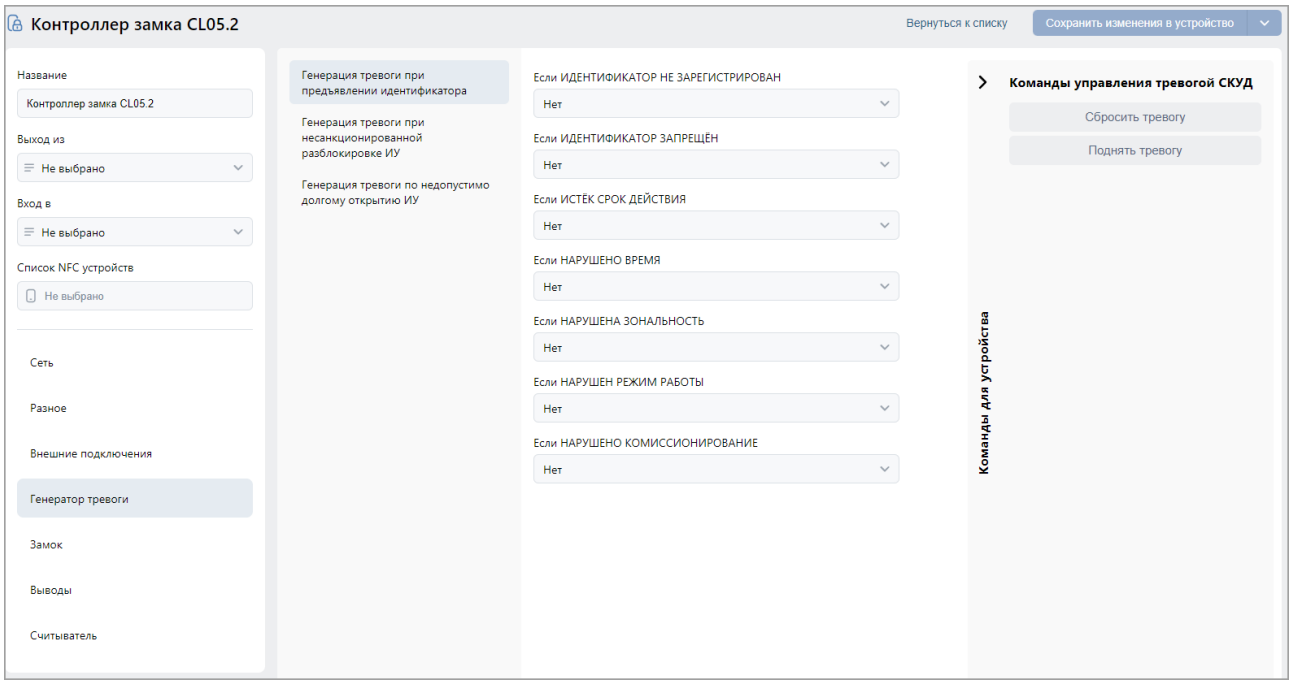
Для настройки доступны следующие параметры:

- **Тип**. Раскрывающийся список позволяет выбрать один из следующих типов:
  - **Нет**. К данному входу не подключено никакое внешнее оборудование.
  - **Обычный выход**. К выходу подключено дополнительное оборудование, логика управления которым описывается через описание других устройств системы (за исключением ресурса **Генератор тревоги**).
  - **Генератор тревоги**. Решение об активизации дополнительного выхода принимается в соответствии с параметрами, заданными для ресурса **Генератор тревоги**.
  - **Вход Fire Alarm**. Предназначен для подключения устройства подачи команды аварийной разблокировки (открытия) прохода ИУ Fire Alarm.
  - **Синхронизирующий вход / выход**. Вывод используется для синхронизации совместной работы двух контроллеров при организации КПП с контролем проходов в двух направлениях. В этом режиме выводы контроллеров соединяются друг с другом.
- **Нормальное состояние** (*Не запитан / Запитан*). Выбор параметра зависит от типа подключенного оборудования. Параметр определяет, какой уровень сигнала на входе контроллера считается нормализованным.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

18.7. Вкладка «Генератор тревоги»

Вкладка выглядит следующим образом:



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

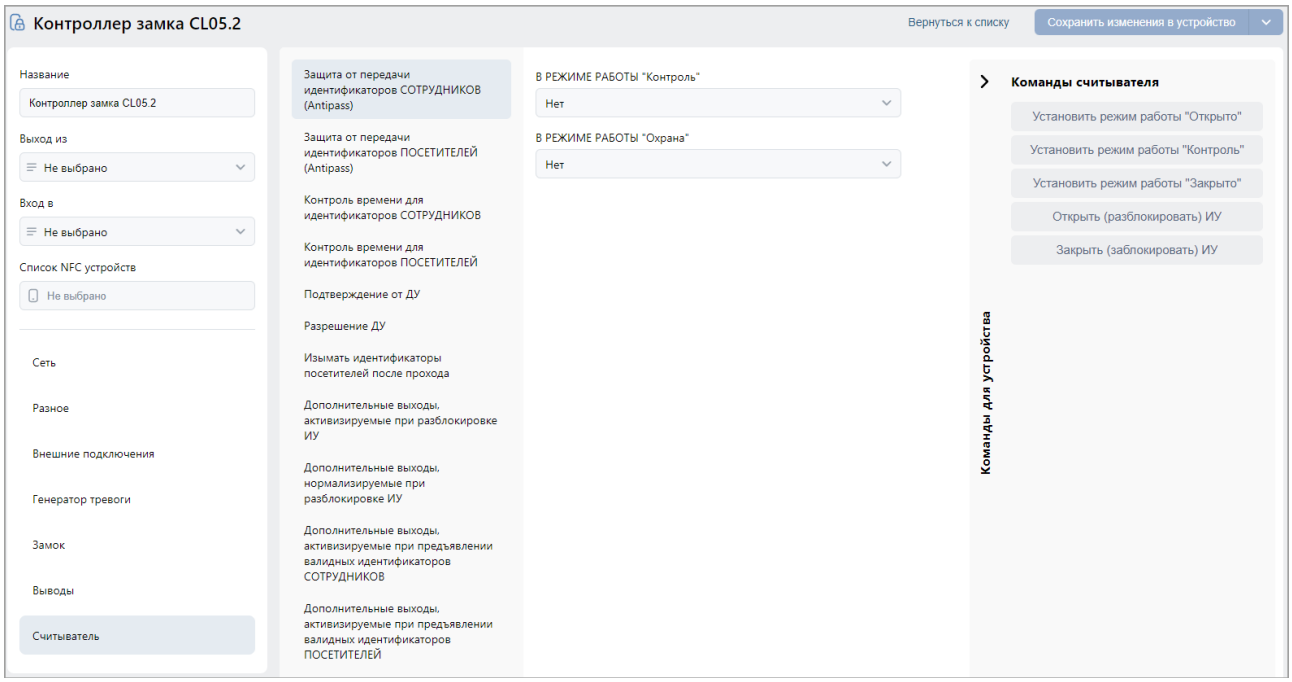
- Вкладка **Генерация тревоги при предъявлении идентификатора** – параметр позволяет указать события, связанные с предъявлением карт доступа, при регистрации которых произойдет генерация тревоги:
  - **если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН**;
  - **если ИДЕНТИФИКАТОР ЗАПРЕЩЕН**;
  - **если ИСТЕК СРОК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

  Для каждого события есть возможность выбрать тип тревоги:
  - **Нет**.
  - **Тихая**. Тревога генерируется, но при этом не активизируются выходы, для которых выбран **Тип: Генератор тревоги**.
  - **Громкая**. Генерируется тревога.
- Вкладка **Генерация тревоги при несанкционированной разблокировке ИУ** – параметр позволяет для РКД *«Контроль»* и *«Закрыто»* указать, будет ли генерироваться тревога в случае механической разблокировки ИУ при помощи ключа, то есть без команды от контроллера:
  - **в РЕЖИМЕ РАБОТЫ "Контроль"**;
  - **в РЕЖИМЕ РАБОТЫ "Закрыто"**.
- Вкладка **Генерация тревоги по недопустимо долгому открытию ИУ** – параметр позволяет для РКД «*Контроль*» указать, будет ли генерироваться тревога в случае, если после открытия ИУ оно не было нормализовано в течение **Предельного времени разблокировки**, заданного в параметрах этого ИУ.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

18.8. Вкладка «Считыватель»

Вкладка выглядит следующим образом:



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

- **Защита от передачи идентификаторов СОТРУДНИКОВ** (учеников, родственников учеников) **/ ПОСЕТИТЕЛЕЙ (Antipass)**. Параметр позволяет для выбранных РКД определить реакцию контроллера на предъявление карты доступа сотрудника, ученика, родственника ученика / 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** (учеников, родственников учеников) **/ ПОСЕТИТЕЛЕЙ**. Параметр позволяет для выбранных РКД определить реакцию контроллера на предъявление карты доступа сотрудника, ученика, родственника ученика / 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*

SEC.RU | Короткий путь к информации
Скачано с sec.ru

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

- **Разрешение ДУ**. При установке флажка **В РЕЖИМЕ РАБОТЫ "Контроль"** использование ПДУ при РКД *«Контроль»* в направлении данного считывателя будет разрешено.
- **Подтверждение от ДУ**. Параметр позволяет настроить проведение процедуры верификации от ПДУ. При установке типа контроля **Нет** в поле **В РЕЖИМЕ РАБОТЫ «Контроль»** задайте **Время ожидания подтверждения при верификации**. При установке типа контроля **Да** в поле **В РЕЖИМЕ РАБОТЫ «Контроль»** укажите, какие события должны быть верифицированы, и задайте **Время ожидания подтверждения при верификации**.
- **Изымать идентификаторы посетителей после прохода**. При установке флажка предъявленная карта доступа после прохода изымается из учетных данных посетителя, данные посетителя отправляются в архив. Функция доступна только при наличии связи контроллера с сервером системы.
- **Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов СОТРУДНИКОВ** (учеников, родственников учеников) **/ ПОСЕТИТЕЛЕЙ**. Параметр позволяет указать выходы, активизируемые при предъявлении карты доступа сотрудника, ученика, родственника ученика / посетителя, которой выданы права доступа на контроллер (карта не заблокирована и ее срок действия не истек). Этот параметр может быть использован в случае, если к дополнительным выходам подключена индикация, информирующая оператора о статусе предъявленной карты. Для выбора отметьте те дополнительные выходы, которые должны быть активизированы. Укажите временной критерий активизации.
- **Дополнительные выходы, активизируемые при разблокировке ИУ**. Параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при разблокировке ИУ. Для выбора отметьте те дополнительные выходы, которые должны быть активизированы. Укажите временной критерий активизации.
- **Дополнительные выходы, нормализируемые при разблокировке ИУ**. Параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализированы при разблокировке ИУ. Для выбора отметьте те дополнительные выходы, которые должны быть нормализированы. Укажите временной критерий нормализации.
- **Дополнительные входы, маскируемые при разблокировке ИУ**. Параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы (т.е. не воспринимать управляющий сигнал от внешнего оборудования) при разблокировке ИУ. Для выбора отметьте те дополнительные входы, которые должны быть маскированы. Укажите временной критерий маскирования.

SEC.RU | Короткий путь к информации Скачано с sec.ru

19. Параметры контроллеров CL15, CL15.1, CL15.3, CL15.7, CR11, CR11.1, CR02.9, CT/L14, CT/L14.1, CT13, CT13.1.

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

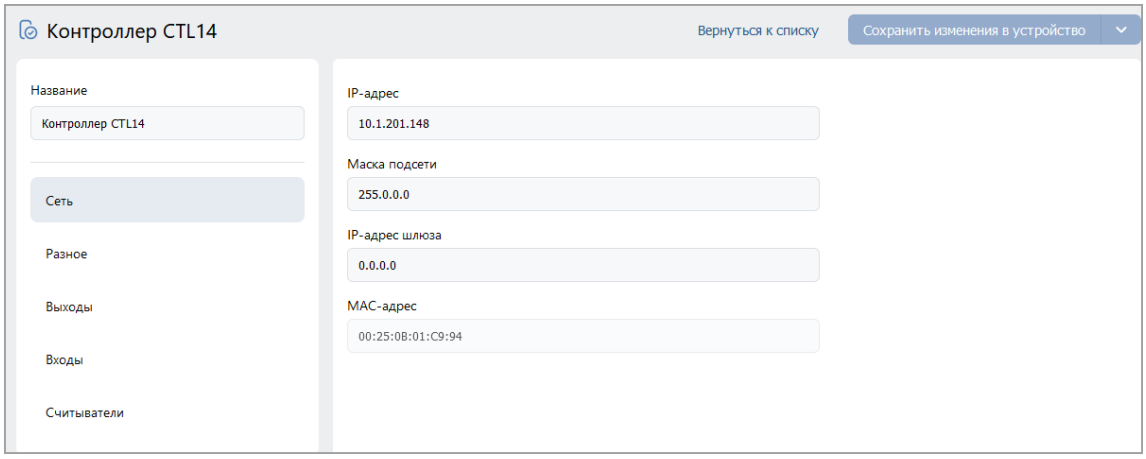
- **Сеть**;
- **Разное**;
- **ИУ**;
- **Направление**;
- **Генератор тревоги**;
- **Свойства**;
- **Направление №...**;
- **Входы**;
- **Выходы**;
- **Считыватели**;
- **Шлюз**;
- **Составной объект**.

19.1. Вкладка «Сеть»

Вкладка отображает информацию о следующих сетевых параметрах:

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

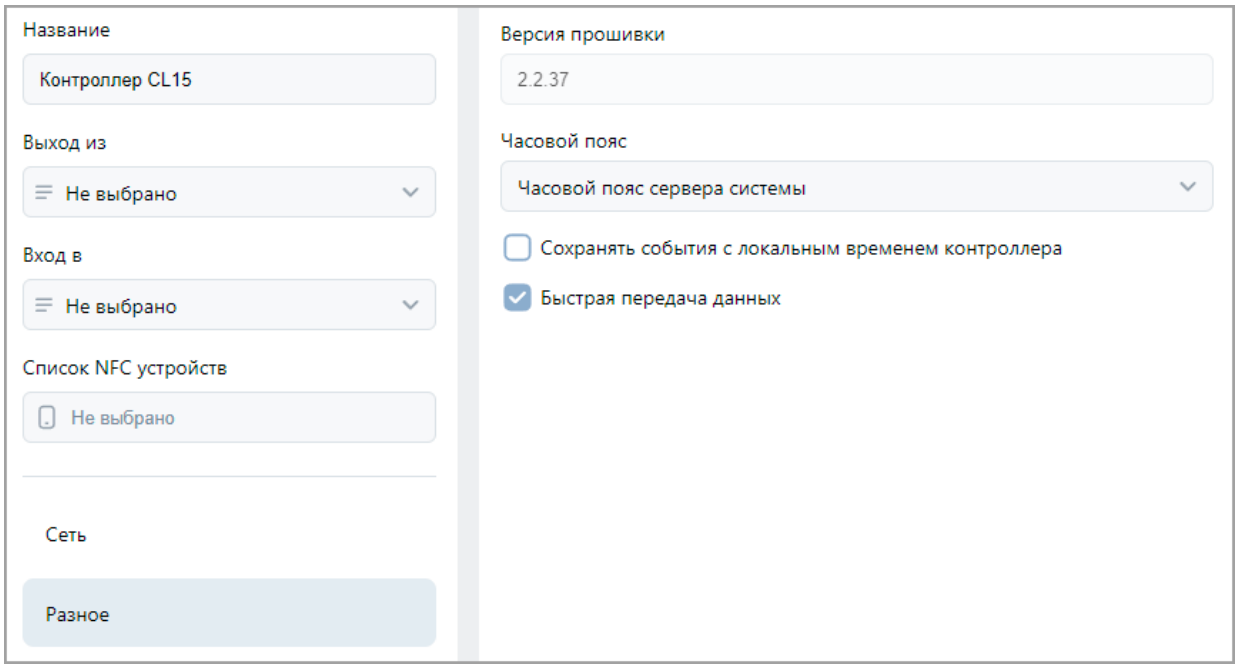
Окно имеет следующий вид:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

19.2. Вкладка «Разное»

Вкладка выглядит следующим образом:

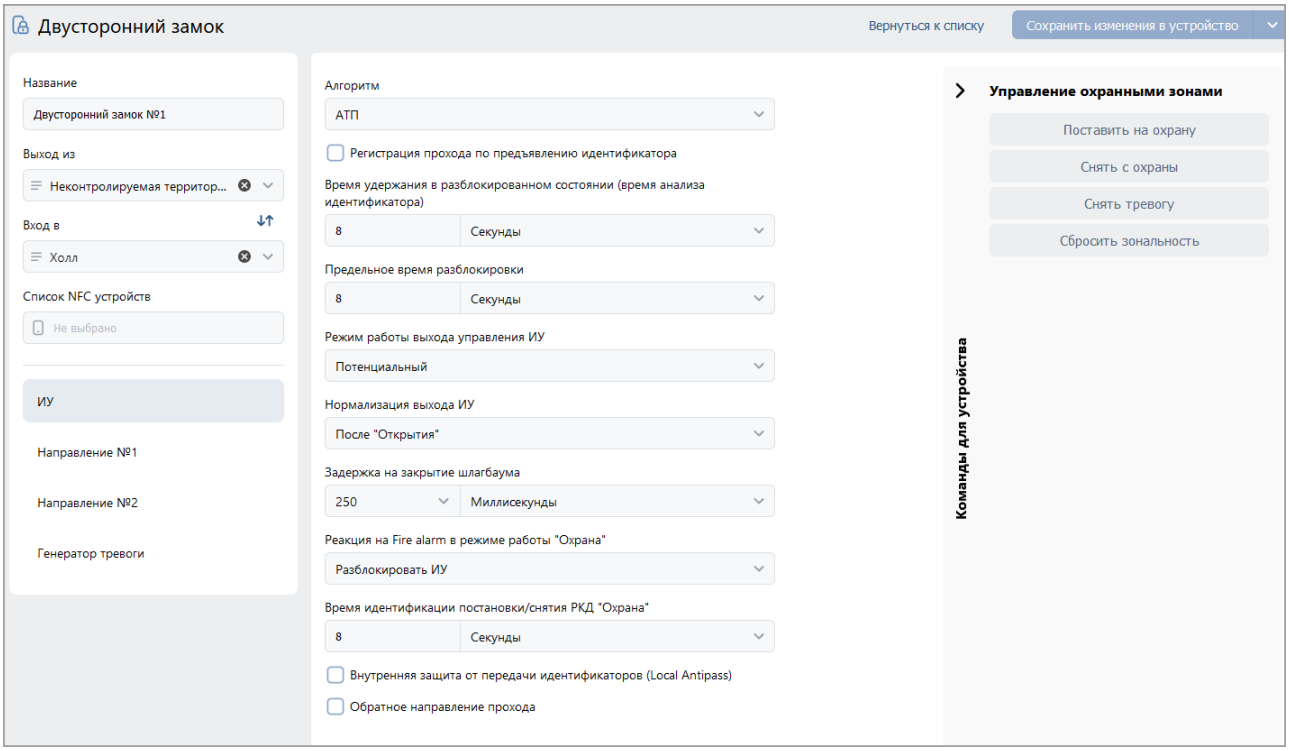


Вкладка содержит следующие настройки:

- **Версия прошивки** – в поле отображается версия прошивки встроенного ПО контроллера.
- **Часовой пояс** – выпадающий список позволяет выбрать часовой пояс контроллера.
- **Сохранять события с локальным временем контроллера** – при установленном флажке события сохраняются в соответствии с временем и датой, установленными в Web-интерфейсе контроллера.
- **Быстрая передача данных** – если в процессе передачи данных возникли проблемы, флажок с параметра необходимо снять для проведения полной диагностики специалистами техподдержки.

19.3. Вкладка ИУ

Вкладка выглядит следующим образом:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

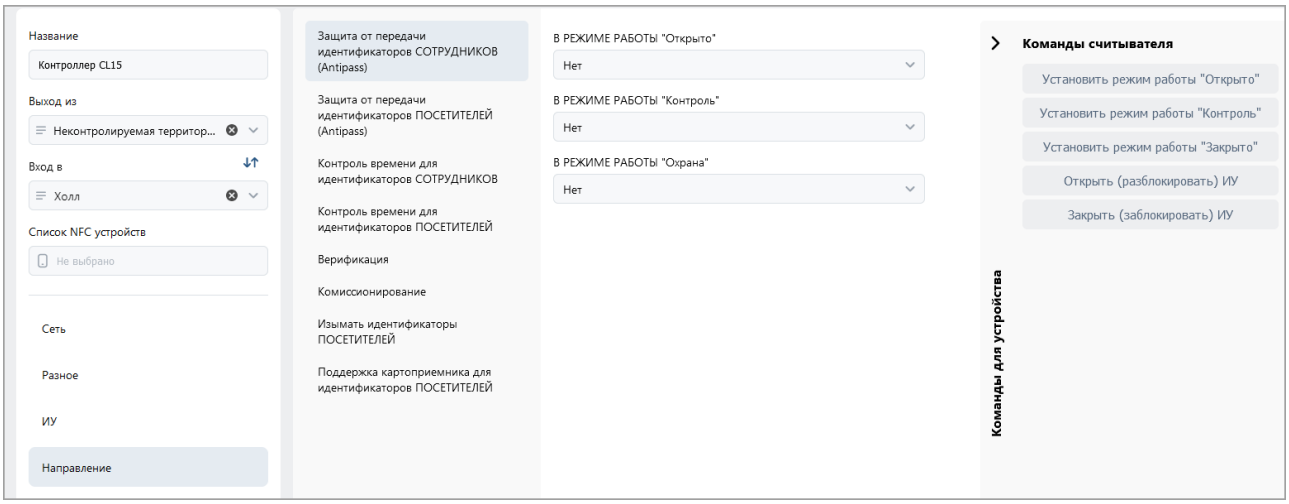
Для настройки доступны следующие параметры:

- **Алгоритм** – определяет алгоритм работы универсального ИУ:
  - **Замок**;
  - **Турникет**;
  - **АТП**;
  - **Шлюз**.
- **Регистрация прохода по предъявлению идентификатора** – если флажок установлен, событие совершения прохода регистрируется сразу после поднесения карты доступа / сканирования пальца без ожидания сигнала от датчика прохода. Если флажок не установлен, то событие совершения прохода регистрируется после поднесения карты доступа / сканирования пальца и срабатывания датчика прохода.
- **Время удержания в разблокированном состоянии (время анализа идентификатора)** – устанавливает время, которое должно пройти от разблокировки ИУ до его блокировки после успешной аутентификации. За это время необходимо совершить проход, иначе ИУ заблокируется. Параметр может быть задан в интервале: от 1 секунды до 4 минут; бесконечно.
- **Предельное время разблокировки** – параметр позволяет указать время, по истечении которого контроллер сформирует сообщение *«ИУ не закрыто после прохода по идентификатору»* по причине того, что ИУ не заблокировано. Параметр может быть задан в интервале: от 250 до 750 миллисекунд с шагом 250 миллисекунд; от 1 секунды до 4 минут; бесконечно.
- **Режим работы выхода управления ИУ** – описывает логику управления подключенным ИУ:
  - **Потенциальный**.
  - **Импульсный** – режим управления применяется только для замков, поддерживающих этот режим. Рекомендуется использовать для электромеханических замков с самовзводом, открывающихся коротким импульсом (например, замки «CISA»).
- **Нормализация выхода ИУ** – параметр определяет, в какой момент нормализуется состояние выхода управления ИУ:
  - **После «Открытия»**;
  - **После «Закрытия»**.
- **Реакция на Fire Alarm в режиме работы «Охрана»** – определяет реакцию на команду от устройства Fire Alarm:
  - **Разблокировать ИУ**;
  - **Блокировать ИУ**.
- **Время идентификации постановки / снятия РКД «Охрана»** – устанавливает время, в течение которого пользователь для успешной идентификации для снятия ИУ с охраны должен предъявить палец после предъявления идентификатора, если *«Схема идентификации по охране»* в правах пользователя подразумевает последовательное предъявление идентификатора и пальца (см. *«Параметры доступа контроллеров CL15, CL15.1, CL15.3, CL15.7, CR11, CR11.1, CR02.9, CT/L14, CT/L14.1 CT13, CT13.1.»* в подразделе **«Шаблоны доступа»** раздела **«Бюро пропусков»** *Руководства пользователя* ***PERCo-ES***).
- **Внутренняя защита от передачи идентификаторов (Local Antipass)** – при установленном параметре контроллер отслеживает повторные случаи предъявления карты доступа / биоидентификатора одного и того же сотрудника, ученика, родственника ученика к тому же считывателю.

SEC.RU | Короткий путь к информации Скачано с sec.ru

19.4. Вкладка «Направление»

Вкладка выглядит следующим образом:



Для настройки доступны следующие параметры:

- **Защита от передачи идентификаторов СОТРУДНИКОВ** (учеников, родственников учеников) **/ ПОСЕТИТЕЛЕЙ (Antipass)**. Параметр позволяет для выбранных РКД определить реакцию контроллера на предъявление карты доступа сотрудника, ученика, родственника ученика / посетителя к считывателю в случае нарушения им функции контроля зональности (Antipass). Для РКД *«Охрана»* и *«Контроль»* можно выбрать один из видов контроля:
  - **Нет** – контроллер не учитывает зональность идентификатора карты для разрешения доступа.
  - **Мягкая** – контроллер разрешит доступ по карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение зональности»,* после совершения прохода регистрируется событие «*Проход по карте с несоответствием текущему местоположению»*.
  - **Жесткая** – контроллер запретит доступ по карте, при этом передается событие мониторинга *«Предъявление карты с нарушением зональности»* и регистрируется событие *«Запрет прохода по причине нарушения зональности».*
- **Контроль времени для идентификаторов СОТРУДНИКОВ** (учеников, родственников учеников) **/ ПОСЕТИТЕЛЕЙ**. Параметр позволяет для выбранных РКД определить реакцию контроллера на предъявление карты доступа сотрудника, ученика, родственника ученика / посетителя к считывателю в случае нарушения установленного критерия доступа по времени. Для РКД *«Охрана»* и *«Контроль»* можно выбрать один из видов контроля:
  - **Нет** – контроллер не отслеживает временные критерии прав доступа карты.
  - **Мягкий** – контроллер разрешит доступ по предъявленной карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение времени»*, после совершения прохода регистрируется событие «*Проход по карте с несоответствием временным критериям доступа»*.
  - **Жесткий** – контроллер запретит доступ по карте, при этом передается событие мониторинга *«Предъявление идентификатора, нарушение времени»* и регистрируется событие «*Запрет прохода, несоответствие временным критериям доступа»*.
- **Верификация**:
  - **Уровни верификации** (от 1 до 4). Параметр позволяет задать тип и очередность верификации. Доступны следующие типы верификации для каждого уровня:
    - **Софт**;
    - **Софт, если подключен**;
    - **ПДУ**;
    - **ВВУ**;
    - **ВВУ2**;

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **ВВУ3**;
- **ПДУ выборочно**;
- **ВВУ выборочно**;
- **ВВУ2 выборочно**;
- **ВВУ3 выборочно**;
- **Счетчик проходов**;
- **Алкобарьер**;
- **Алкобарьер выборочно**.

– **Софт**. Параметр позволяет задать время ожидания подтверждения.
– **ПДУ** и **ВВУ**. Для вкладок доступны следующие параметры:
  - Подтверждение прохода:
    - ✓ **при проходе СОТРУДНИКОВ** (учеников, родственников учеников);
    - ✓ **при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ВРЕМЕНИ** (учеников, родственников учеников);
    - ✓ **при проходе СОТРУДНИКОВ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ** (учеников, родственников учеников);
    - ✓ **при проходе ПОСЕТИТЕЛЕЙ**;
    - ✓ **при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ВРЕМЕНИ**;
    - ✓ **при проходе ПОСЕТИТЕЛЕЙ с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**.
  - **Подтверждение прохода для ПОСЕТИТЕЛЕЙ**. Параметр позволяет выбрать дополнительное условие проведения процедуры верификации для посетителей:
    - ✓ **Постоянно**. Верификация проводится независимо от срока действия карты.
    - ✓ **В последний день действия идентификатора**. Верификация проводится в случае, если дата предъявления совпадает с датой окончания срока действия карты.
  - **Время ожидания подтверждения**. Параметр позволяет установить время, в течение которого контроллер ожидает подтверждение запроса от верифицирующего устройства.
  - **По истечении времени ожидания подтверждения генерировать событие**. Параметр позволяет выбрать событие, регистрируемое в случае отсутствия подтверждения прохода от ВВУ:
    - ✓ **Запрет прохода от ВВУ**. Рекомендуется в случае подключения ВВУ, имеющего только один выход разрешения прохода.
    - ✓ **Отказ от прохода, нет ответа от ВВУ**. Рекомендуется в случае подключения ВВУ, имеющего выходы как для разрешения прохода, так и для запрета прохода.
  - **Вероятность запуска верификации (0..100%)**. Параметр позволяет настроить выборочную верификацию пользователей в случае необходимости (например, для увеличения пропускной способности точки контроля). При установке какого-то значения для данного параметра, отличного от 0 и 100, верификация будет запускаться в соответствии с указанной вероятностью по псевдослучайному алгоритму.

– **Счетчик**. Параметр позволяет задать время ожидания подтверждения.
– **Алкобарьер**. Для вкладки доступны следующие параметры:
  - **IP-адрес алкобарьера**;
  - **Порт алкобарьера**;
  - **Сетевое имя алкобарьера**;
  - **Протокол**:
    - ✓ **HTTP** (обычное соединение);
    - ✓ **HTTPS** (зашифрованное соединение).
  - **Подтверждение прохода**:
    - ✓ **при проходе СОТРУДНИКОВ** (учеников, родственников учеников);
    - ✓ **при проходе ПОСЕТИТЕЛЕЙ**.
  - **Подтверждение прохода для ПОСЕТИТЕЛЕЙ.** Параметр позволяет выбрать дополнительное условие проведения процедуры верификации для посетителей:
    - ✓ **Постоянно**. Верификация проводится независимо от срока действия карты.
    - ✓ **В последний день действия идентификатора**. Верификация проводится в случае, если дата предъявления совпадает с датой окончания срока действия карты.

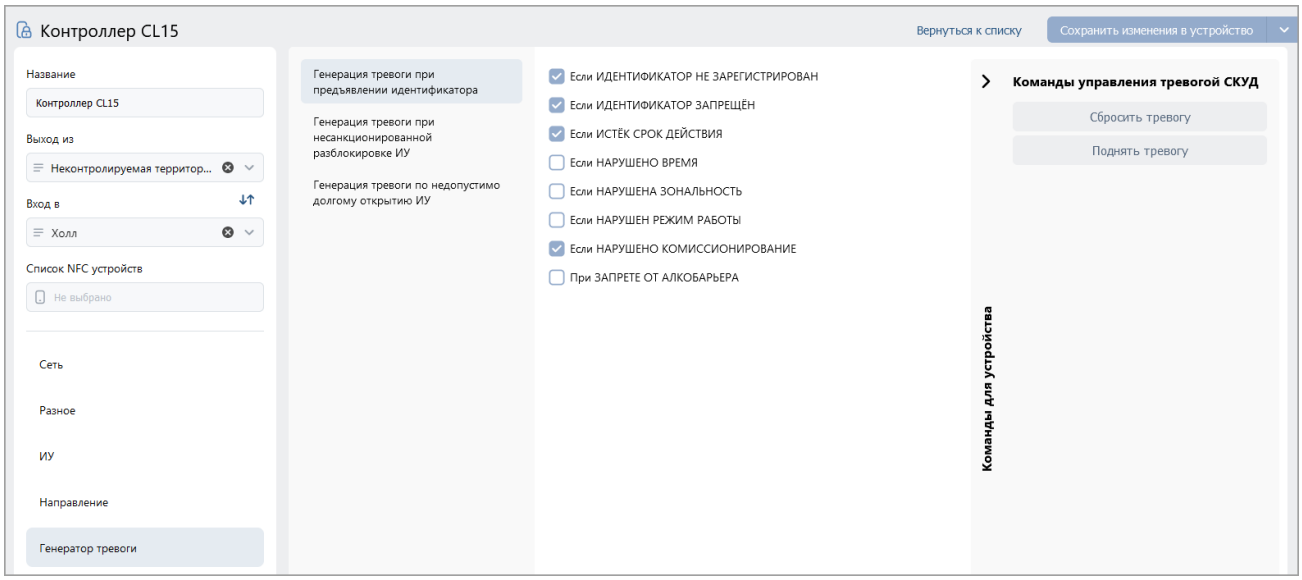
SEC.RU | Короткий путь к информации
Скачано с sec.ru

- **Время ожидания подтверждения.** Параметр позволяет установить время, в течение которого контроллер ожидает подтверждение запроса от Алкобарьера;
- **При отсутствии ответа от Алкобарьера.** Параметр позволяет выбрать событие, регистрируемое в случае отсутствия подтверждения прохода от Алкобарьера:
  - ✓ **Запрет прохода от Алкобарьера**.
  - ✓ **Отказ от прохода, нет ответа от Алкобарьера**.
- **Вероятность запуска верификации (0..100%)**. Параметр позволяет настроить выборочную верификацию пользователей в случае необходимости (например, для увеличения пропускной способности точки контроля). При установке какого-то значения для данного параметра, отличного от 0 и 100, верификация будет запускаться в соответствии с указанной вероятностью по псевдослучайному алгоритму.

- **Комиссионирование**.
  - **Время ожидания**. Параметр позволяет установить время, в течение которого контроллер ожидает подтверждение запроса.
  - **Время идентификации**.
  - **Включить комиссионирование для данного направления**. Параметр позволяет установить комиссионирование для данного направления. При добавлении в шаблоне доступа помещения с комиссионированием данный параметр устанавливается автоматически. В случае двусторонней точки прохода параметр установится на обеих вкладках направлений прохода (**Направление 1** и **Направление 2**).
- **Изымать идентификаторы ПОСЕТИТЕЛЕЙ**. Функция доступна только при наличии связи контроллера с сервером системы. Параметр позволяет выбрать условие, при котором идентификатор предъявленной карты доступа посетителя автоматически удаляется.
  - **Нет**. Идентификатор не удаляется автоматически.
  - **После любого прохода**. Идентификатор удаляется при первом предъявлении.
  - **После прохода в последний день действия идентификатора**. Идентификатор удаляется, если дата предъявления совпадает с датой окончания срока действия карты.
- **Поддержка картоприемника для идентификаторов ПОСЕТИТЕЛЕЙ**.

19.5. Вкладка «Генератор тревоги»

Вкладка выглядит следующим образом:



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

- Вкладка **Генерация тревоги при предъявлении идентификатора** – параметр позволяет указать события, связанные с предъявлением карт доступа, при регистрации которых произойдет генерация тревоги:

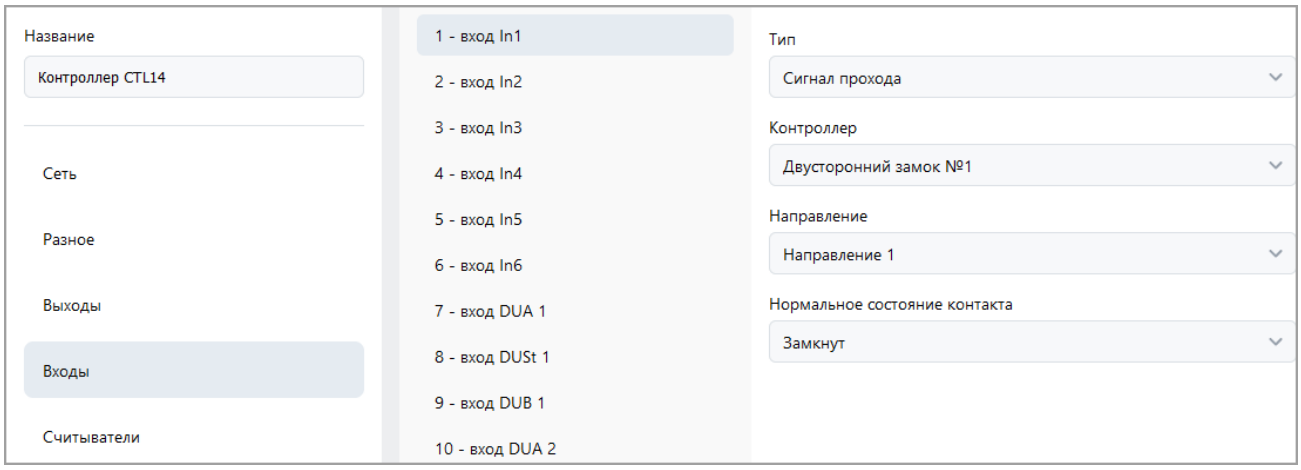
SEC.RU | Короткий путь к информации Скачано с sec.ru

- **если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН**;
- **если ИДЕНТИФИКАТОР ЗАПРЕЩЕН**;
- **если ИСТЕК СРОК ДЕЙСТВИЯ**;
- **если НАРУШЕНО ВРЕМЯ**;
- **если НАРУШЕНА ЗОНАЛЬНОСТЬ**;
- **если НАРУШЕН РЕЖИМ РАБОТЫ**;
- **если НАРУШЕНО КОМИССИОНИРОВАНИЕ**;
- **при ЗАПРЕТЕ ОТ АЛКОБАРЬЕРА**.

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

19.6. Вкладка «Входы»

Вкладка выглядит следующим образом:



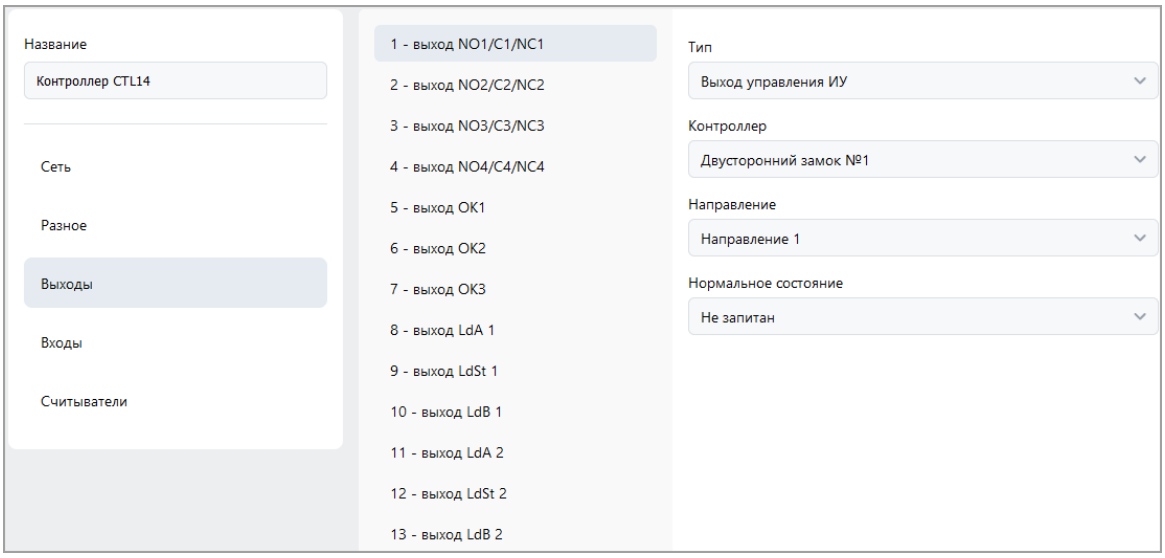
Для настройки входов доступны следующие параметры:

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

19.7. Вкладка «Выходы»

Вкладка выглядит следующим образом:



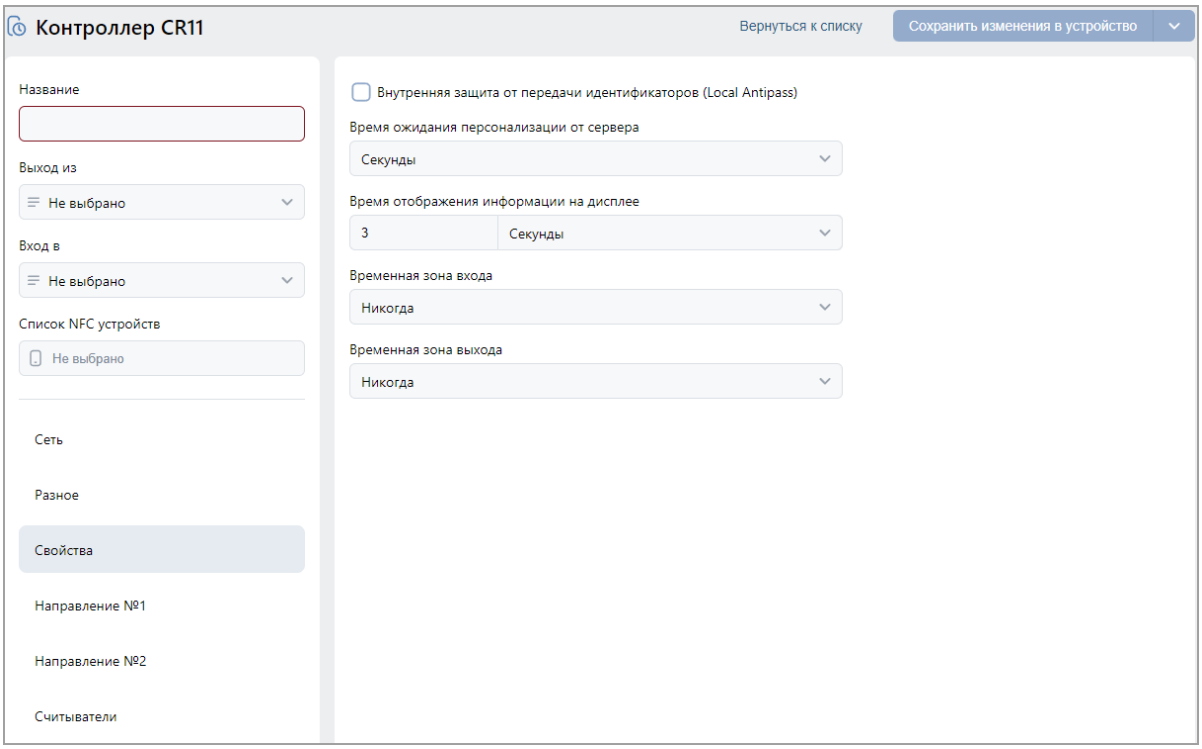
Для настройки выходов доступны следующие параметры:

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

19.8. Вкладки «Свойства» и «Направление №» (для CR11 и CR11.1)

Вкладка **Свойства** выглядит следующим образом:



Для настройки доступны следующие параметры:

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

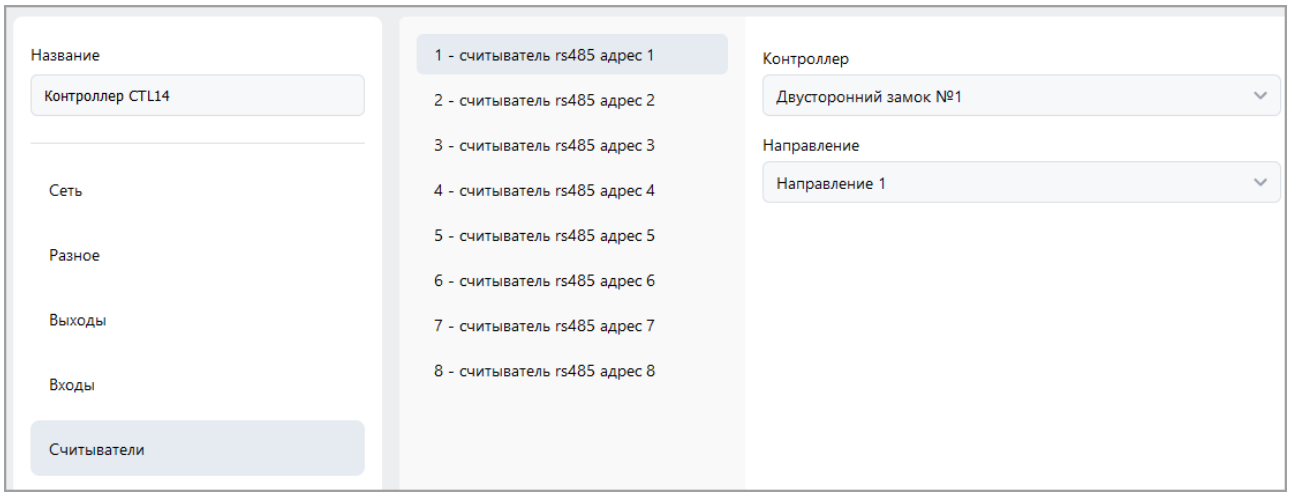
На вкладке **Направление №...** доступны следующие параметры:

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

19.9. Вкладка «Считыватели»

Вкладка выглядит следующим образом:



Для настройки доступны следующие параметры:

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

При использовании системы распознавания автомобильных номеров ***AutoTRASSIR*** у *считывателя TRASSIR* будут доступны следующие параметры:

- **Видеокамера TRASSIR**. Параметр позволяет выбрать видеокамеру ***TRASSIR*** для автоматического распознавания номеров транспортных средств.
- **Полоса движения**. Параметр позволяет указать номер полосы движения, по которой будут двигаться ТС, государственные номера которых необходимо распознавать. Если оставить поле незаполненным, камера будет распознавать номера ТС с любой полосы.

Примечание:

Настройка полосы движения приводится в *«Руководстве администратора TRASSIR»*, которое можно найти на сайте разработчика по адресу: www.dssl.ru.

- **Направление движения ТС**. Параметр позволяет задать направление движения транспортных средств по отношению к видеокамере ***TRASSIR*** для корректной работы АТП. Например, во избежание распознавания номера на заднем бампере транспортного средства при выезде с территории организации.

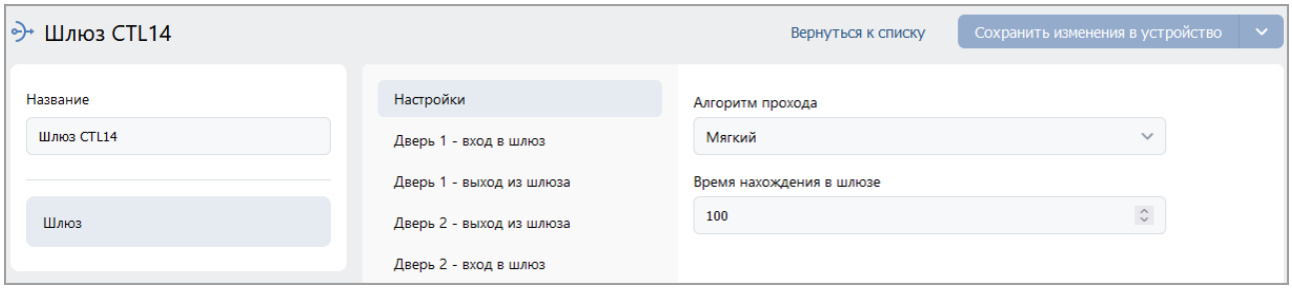
Примечание:

Работа с оборудованием ***TRASSIR*** описывается в ***Руководство пользователя модуля PERCo-WM06 «Интеграция с TRASSIR»***.

SEC.RU | Короткий путь к информации Скачано с sec.ru

19.10. Вкладка «Шлюз»

Вкладка выглядит следующим образом:

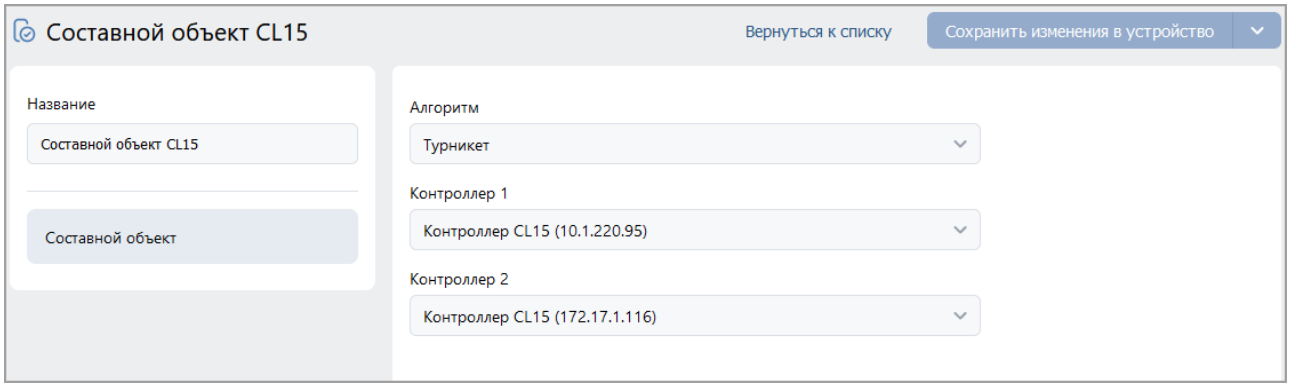


Для настройки доступны следующие параметры:

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

19.11. Вкладка «Составной объект»

Вкладка выглядит следующим образом:



Для настройки доступны следующие параметры:

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

20. Параметры контроллеров Suprema

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

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

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

Примечание:

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

– для контроллера ***BioEntry W2*** – 1.1.1;

– для контроллера ***BioEntry Plus*** (платформа ***BioStar 2***) – 2.3.1;

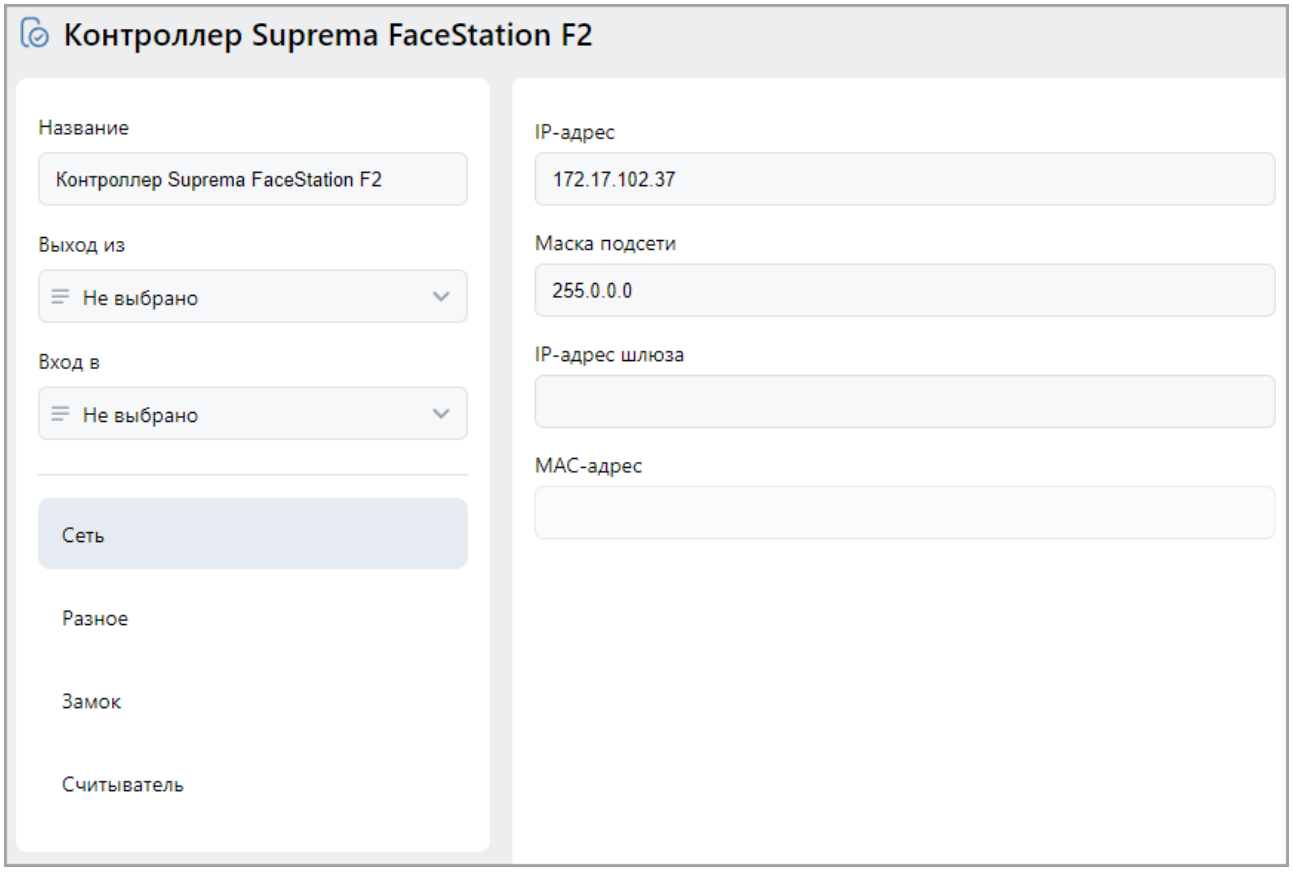
– – для контроллера ***BioLite N2*** – 1.4.2.

20.1. Вкладка «Сеть»

Вкладка отображает информацию о следующих сетевых параметрах:

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

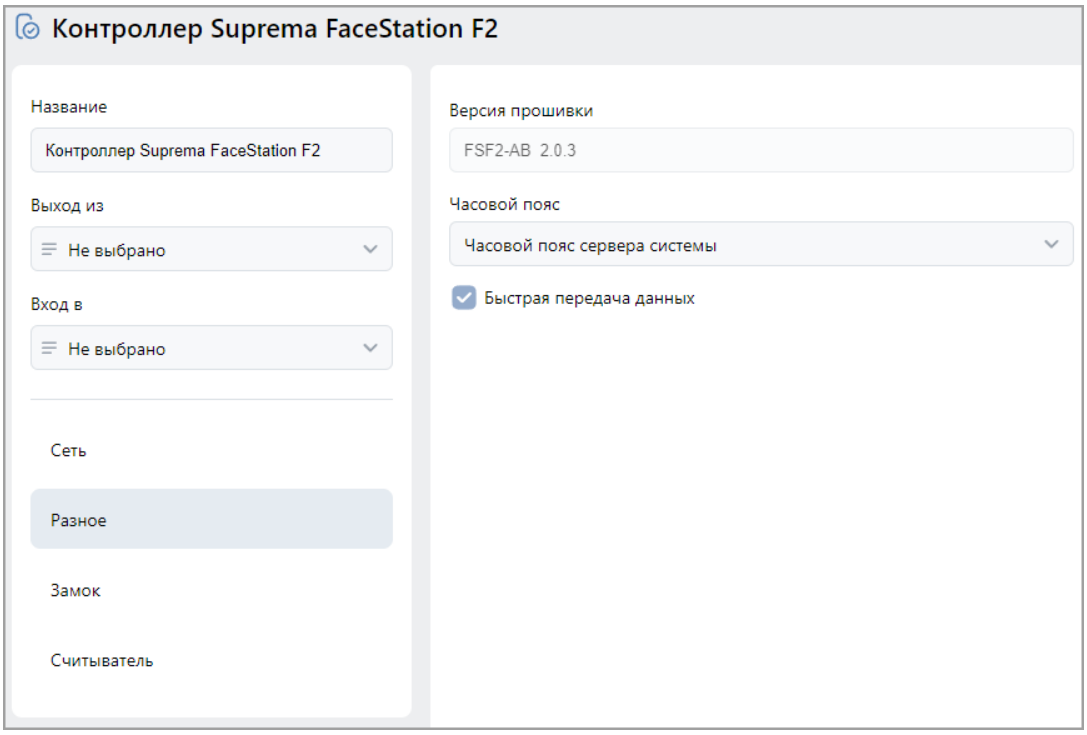
Окно имеет следующий вид:



SEC.RU | Короткий путь к информации Скачано с sec.ru

20.2. Вкладка «Разное»

Вкладка выглядит следующим образом:

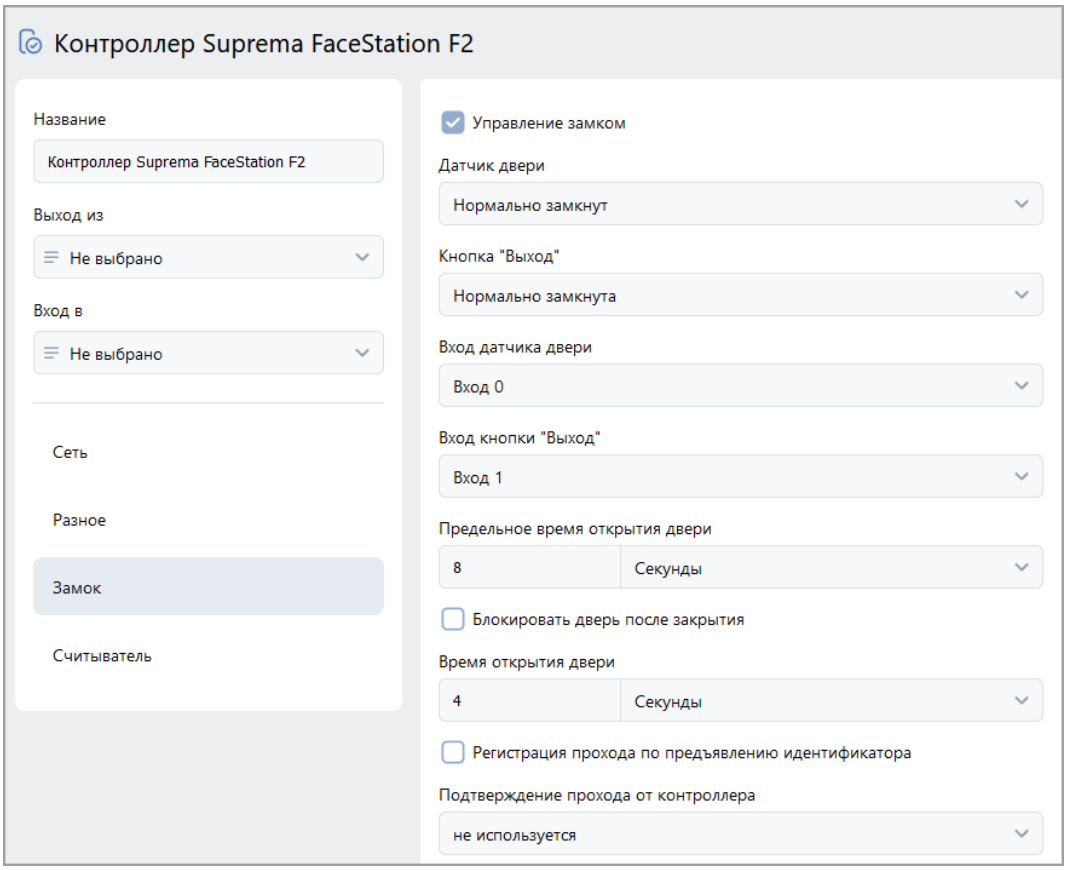


Вкладка содержит следующие настройки:

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

20.3. Вкладка «Замок»

Вкладка **Замок** выглядит следующим образом:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Вкладка содержит следующие настройки:

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

Примечание:

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

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

Примечание:

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

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

Примечание:

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

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

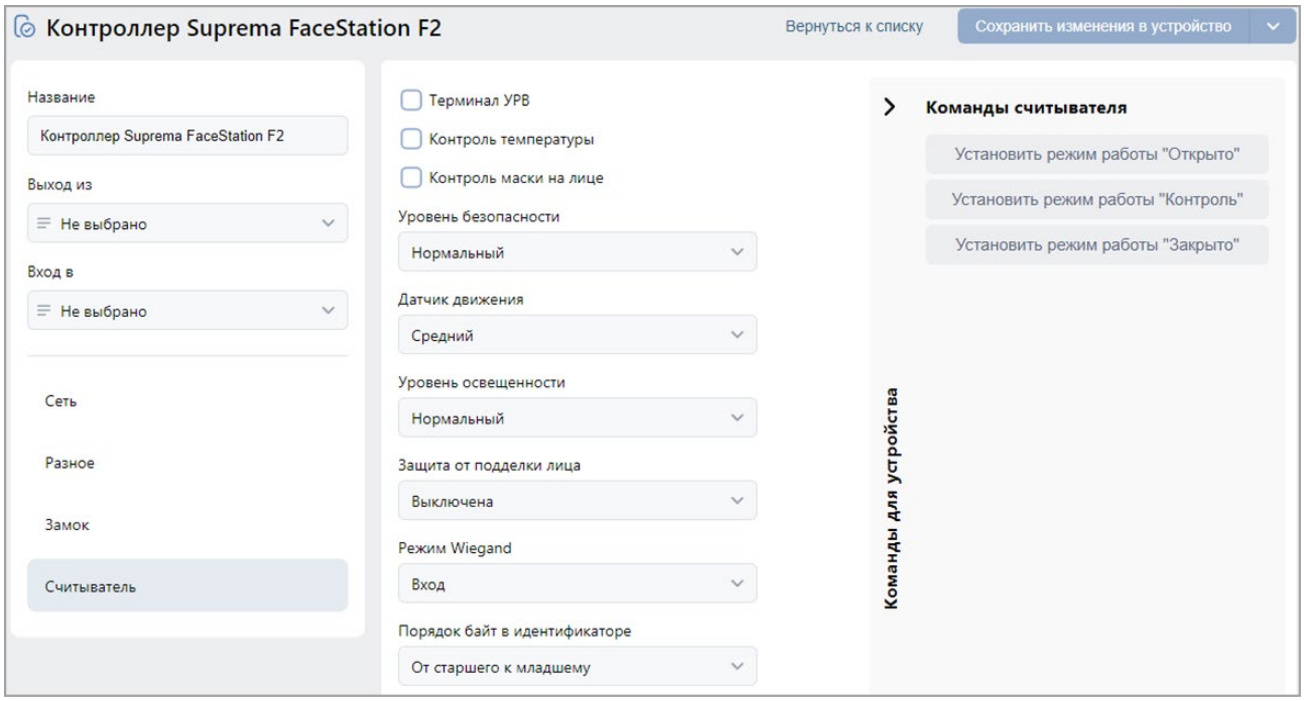
- **Подтверждение прохода от контроллера** – раскрывающийся список позволяет выбрать для подтверждения прохода тот контроллер ***PERCo***, входом ПДУ которого управляет выход контроллера ***Suprema***.

Примечание:

Опция используется при интеграции ЭП или контроллера ***PERCo*** с оборудованием ***Suprema*** для корректного учета рабочего времени.
Если выбран подтверждающий контроллер ***PERCo***, то после прохода от него ожидается событие *«Проход по команде от ДУ»*, после чего в журнал событий системы записывается событие прохода, в противном случае – событие *«Отказ от прохода»*.

20.4. Вкладка «Считыватель»

Вкладка **Считыватель** выглядит следующим образом:



Вкладка содержит следующие настройки:

1. **Для контроллеров со сканерами отпечатков пальцев:**
   - **Чувствительность**. Раскрывающийся список позволяет задать уровень чувствительности считывателя:
     – **Низкая**; **Уровень (от 1 до 6)**; **Высокая**.

Примечание:

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

2. **Для терминалов распознавания лиц:**

Внимание!

Рекомендуется в системе ***PERCo.Школа*** использовать ТРЛ производства ***“Suprema”*** только одной модели, так как у разных моделей терминалов используются разные алгоритмы распознавания лиц. В случае замены терминалов ***Suprema*** одного типа другим потребуется заново создать базу данных распознавания лиц.

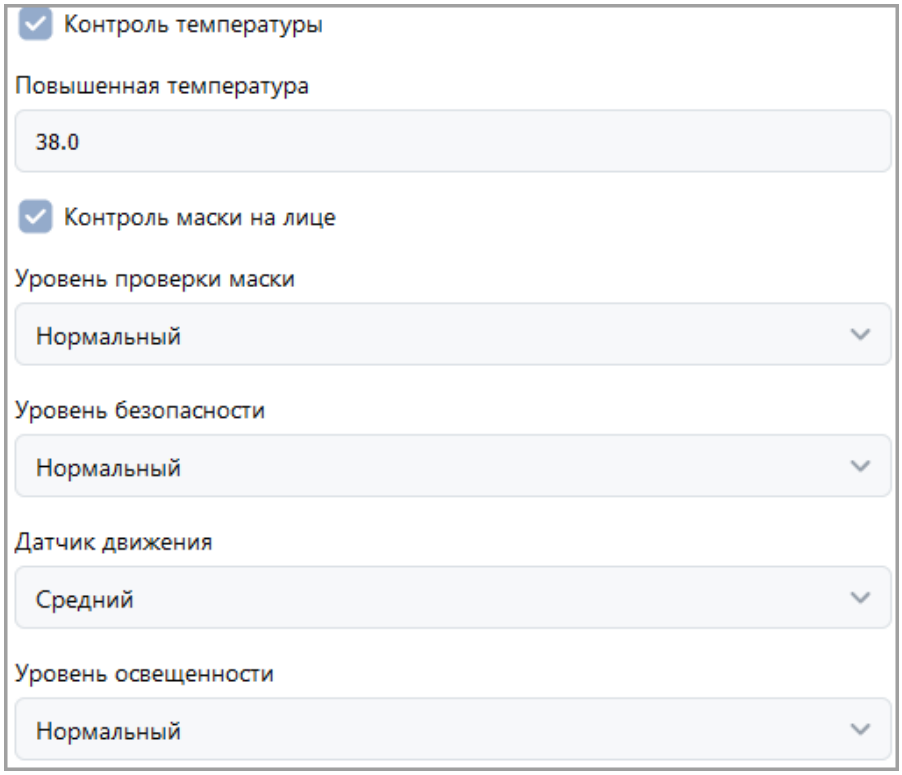
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Примечание:

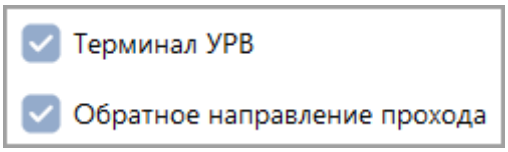
Описание параметров настройки терминала распознавания лиц подробно дано в эксплуатационной документации на данное изделие.

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

Для моделей контроллеров Suprema ***FaceStation F2*** и ***BioStation 3*** поддерживаются опции измерения температуры (при наличии термальной камеры) и контроля маски на лице:



Для моделей контроллеров Suprema ***FaceStation F2***, ***FaceStation 2*** и ***BioStation 3*** поддерживаются опции:



- **Терминал УРВ** – включение данной опции позволяет выбрать направление прохода на экране терминала.
- **Обратное направление прохода** меняет местами «Вход» и «Выход» на экране терминала.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Примечание:

Настройка иконок для событий «Вход» и «Выход» осуществляется в меню администратора терминала в разделе ***Authentication > T&A Code***.

Поддерживаются следующие команды считывателя:

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

21. Параметры контроллеров ZKTeco

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

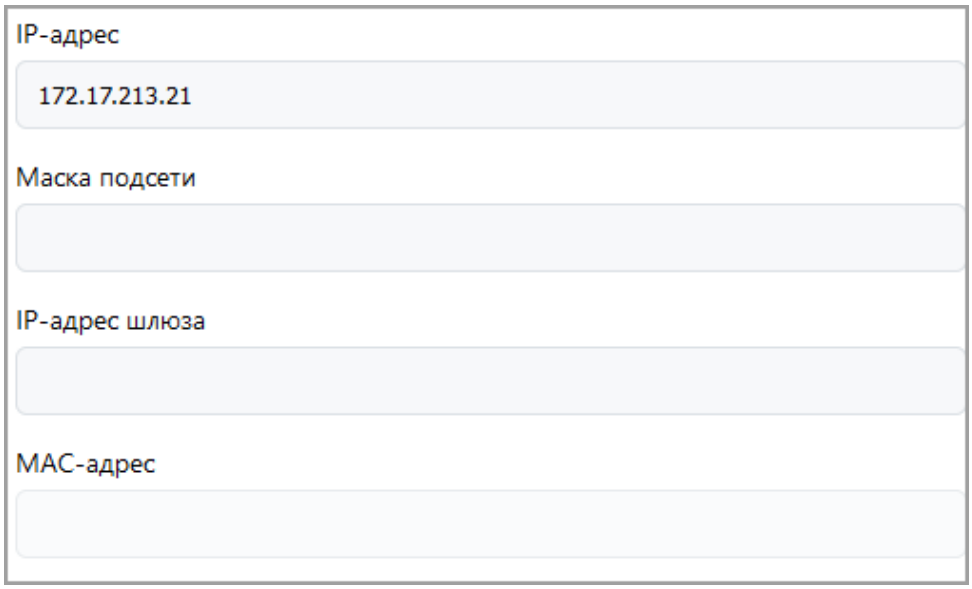
- **Сеть**;
- **Разное**;
- **Замок**;
- **Считыватель**.

21.1. Вкладка «Сеть»

Вкладка отображает информацию о следующих сетевых параметрах:

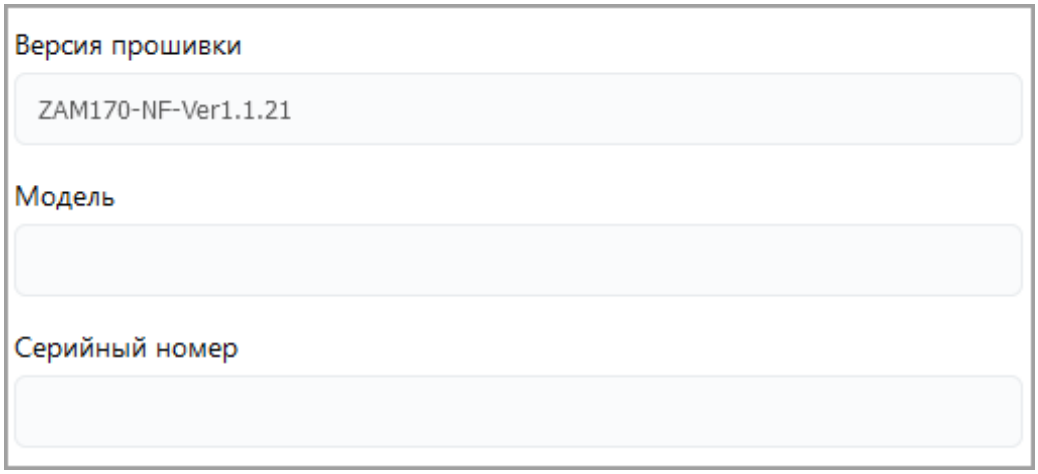
- **IP-адрес**;
- **Маска подсети**;
- **IP-адрес шлюза**;
- **MAC-адрес**.

Окно имеет следующий вид:



21.2. Вкладка «Разное»

Вкладка имеет следующий вид:



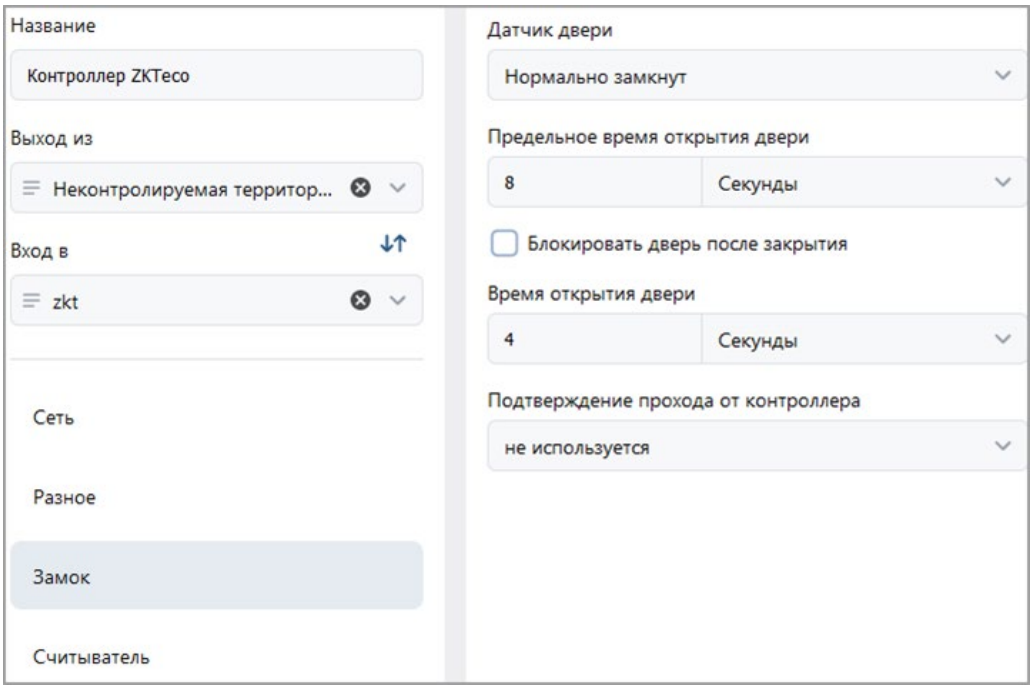
Вкладка содержит следующую информацию:

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

21.3. Вкладка «Замок»

Вкладка **Замок** имеет следующий вид:



Вкладка содержит следующие настройки:

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

Примечание:

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

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

Примечание:

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

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

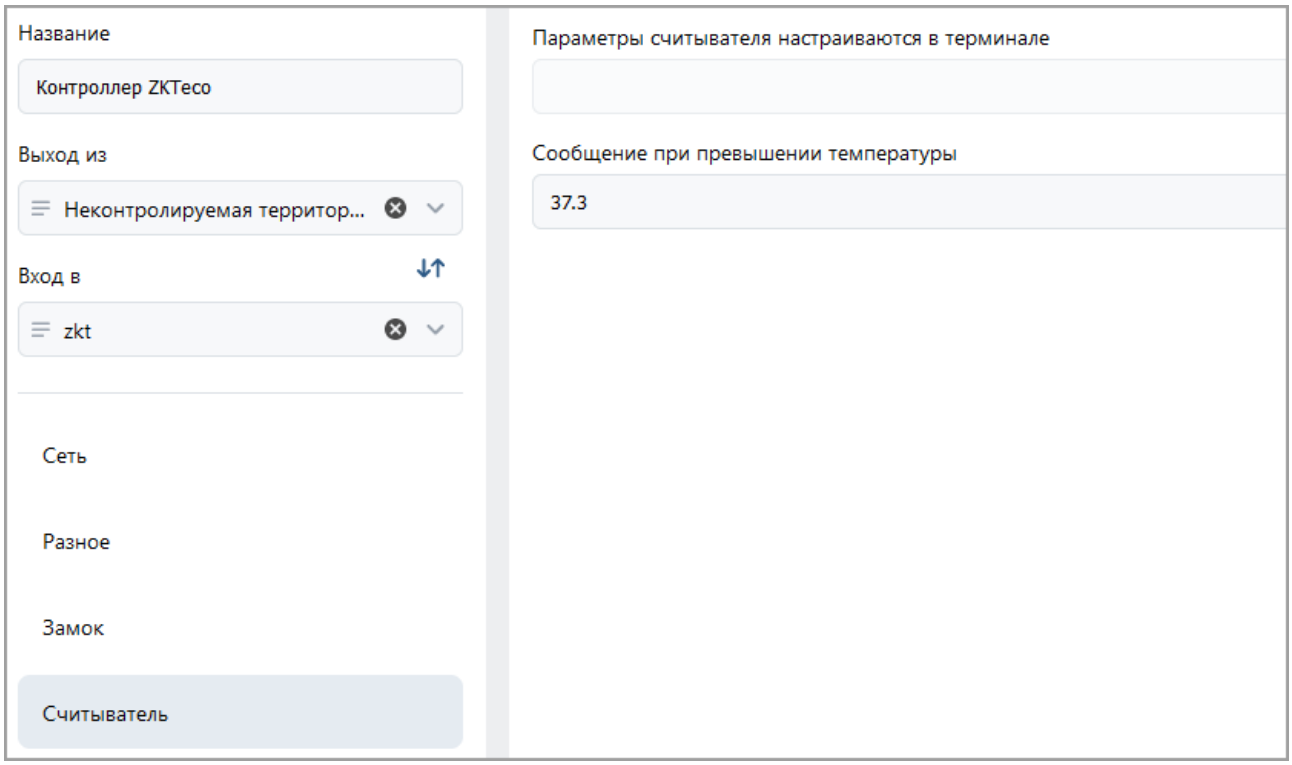
Поддерживаются следующие команды замка:

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

21.4. Вкладка «Считыватель»

Вкладка **Считыватель** выглядит следующим образом:



Вкладка содержит следующие настройки:

Примечание:

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

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

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

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

Внимание!

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

Примеры реализации:

Пример № 1:

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

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

Пример № 2:

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

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

Пример № 3:

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

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

Пример № 4:

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

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

Пример № 5:

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

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

22. Параметры контроллеров BioSmart

Примечание:

Подробная эксплуатационная документация на терминал доступна на сайте производителя по адресу: https://bio-smart.ru/.

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

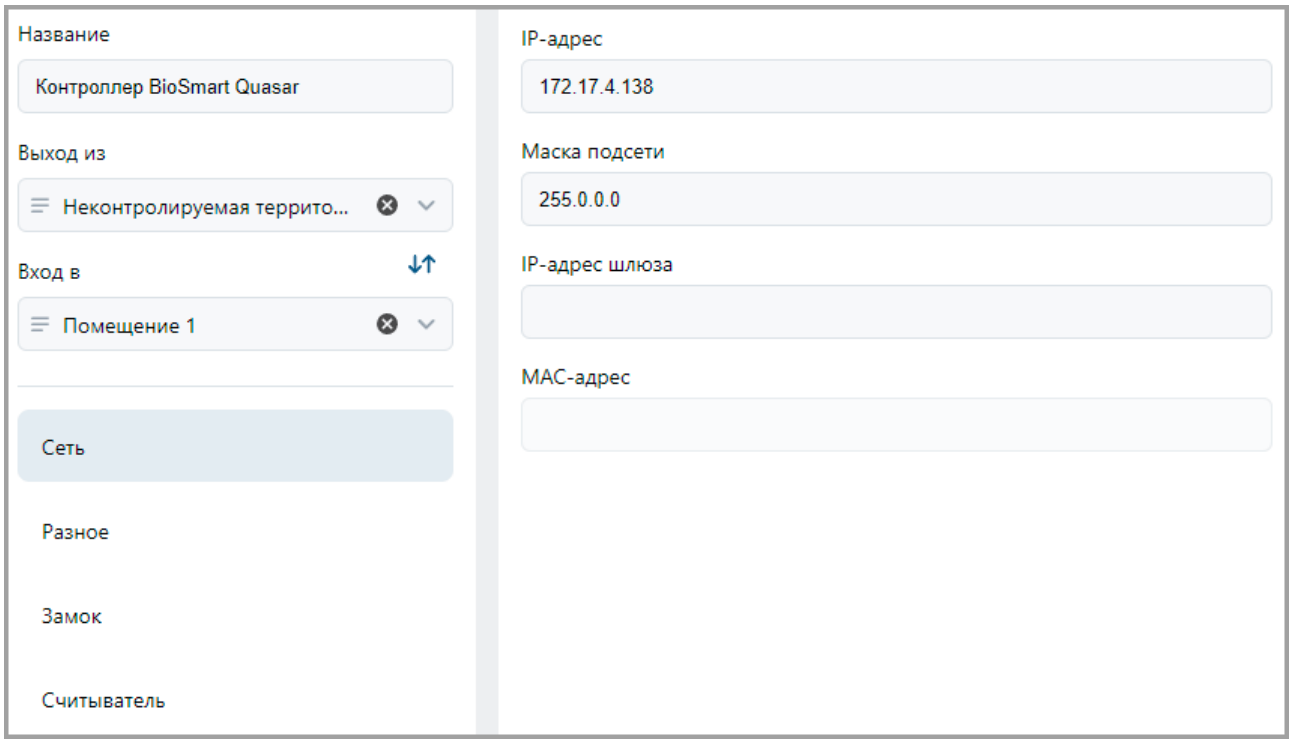
- **Сеть**;
- **Разное**;
- **Замок**;
- **Считыватель**.

22.1. Вкладка «Сеть»

Вкладка отображает информацию о следующих сетевых параметрах:

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

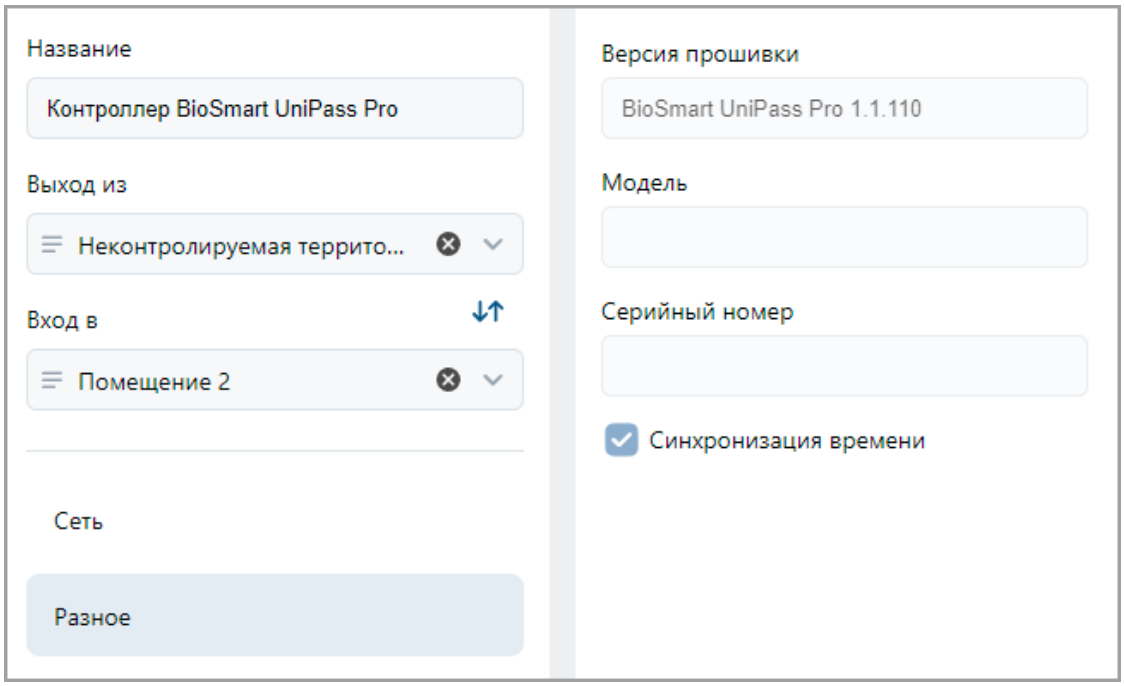
Вкладка имеет следующий вид:



SEC.RU | Короткий путь к информации Скачано с sec.ru

22.2. Вкладка «Разное»

Вкладка имеет следующий вид:

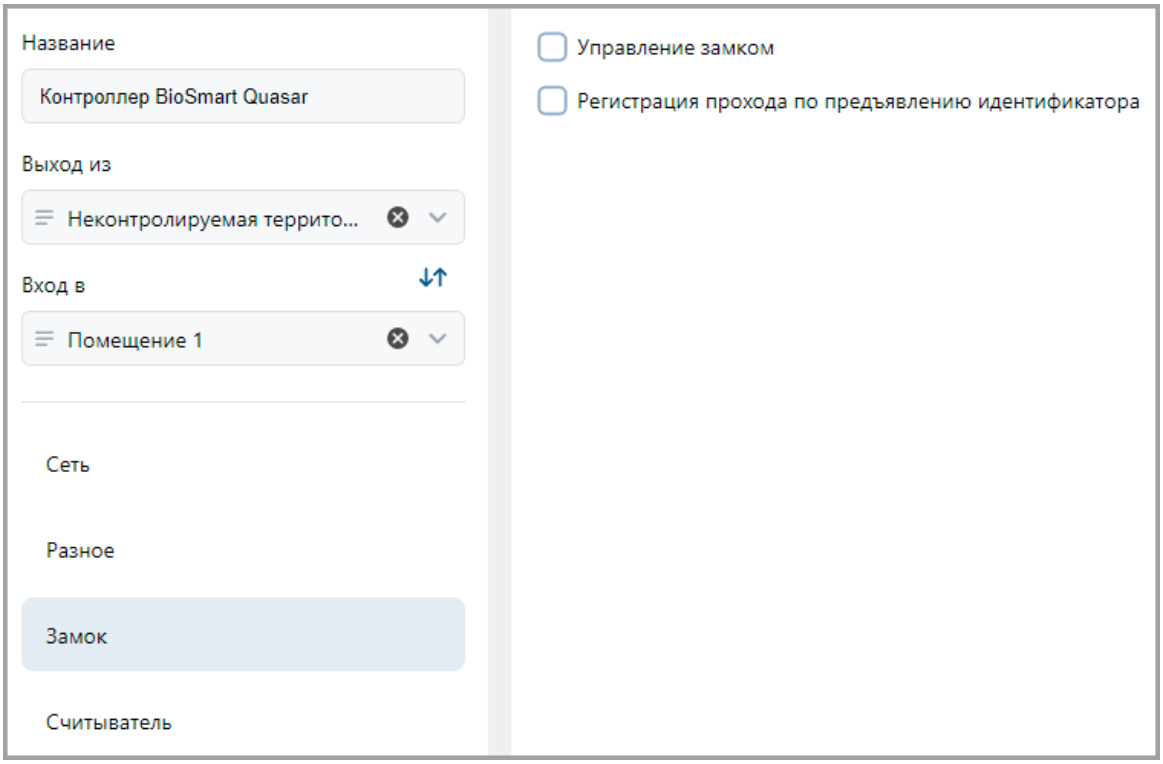


Вкладка содержит следующую информацию:

- **Версия прошивки** – в поле отображается версия прошивки встроенного ПО контроллера.
- **Модель** и **Серийный номер** – в этих полях отображается соответствующая информация о контроллере (не для всех моделей).
- **Синхронизация времени**:
  - для терминала ***BioSmart Quasar*** параметр необходимо включить в случае, если в параметрах терминала установлена синхронизация времени через NTP-сервер;
  - для остальных устройств параметр включен по умолчанию.

22.3. Вкладка «Замок» (для BioSmart Quasar)

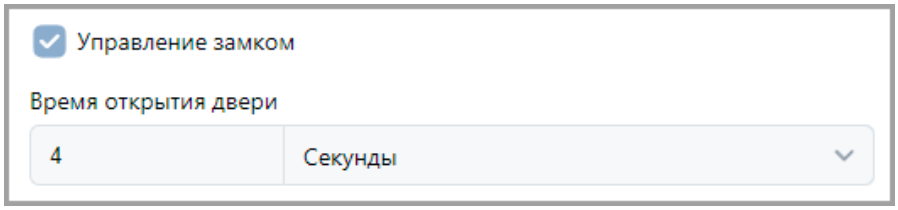
Вкладка **Замок** имеет следующий вид:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Вкладка содержит следующие настройки:

- **Управление замком**. При установке флажка на данном параметре появляется параметр **Время открытия двери** – время, на которое дверь разблокируется контроллером управления доступом для открытия (в секундах):



- **Регистрация прохода по предъявлению идентификатора**. Установленный параметр позволяет регистрировать проход после предъявления идентификатора. При отсутствующем параметре проход будет регистрироваться по факту самого прохода.

22.4. Вкладка «Считыватель»

Вкладка содержит следующие настройки:

1. **Для терминала распознавания лиц BioSmart Quasar:**
   - **Строгость сравнения шаблонов**. Раскрывающийся список позволяет выбрать вероятность ошибочного допуска (FAR) и определяет, насколько точно должны совпадать биометрические данные лица пользователя, полученные с камеры, с биометрическим шаблоном, хранящимся в базе данных. Чем выше строгость сравнения шаблонов, тем меньше вероятность ошибочного допуска:
     - **Нормальная**.
     - **Повышенная**.
     - **Высокая**.
     - **Пониженная**.
     - **Низкая**.

Примечание:

Подробнее о строгости сравнения шаблонов для терминала ***BioSmart Quasar*** можно узнать в разделе **7.10 Выбор уровня строгости идентификации** эксплуатационной документации на терминал, доступной на сайте производителя по адресу: https://bio-smart.ru/quasar.

2. **Для контроллера BioSmart UniPass Pro:**
   - **Тип считывателя карт** – раскрывающийся список позволяет указать формат карт доступа, с которым работает подключенный к данному контроллеру считыватель:
     - **EMarine** (EM-Marine);
     - **Mifare**.
3. **Для считывателя BioSmart PalmJet:**
   - **Тип доступа**. Раскрывающийся список позволяет выбрать один из типов прав доступа:
     - **Ладонь**.
     - **Карта**.
     - **Ладонь или карта**.
     - **Ладонь и карта**.

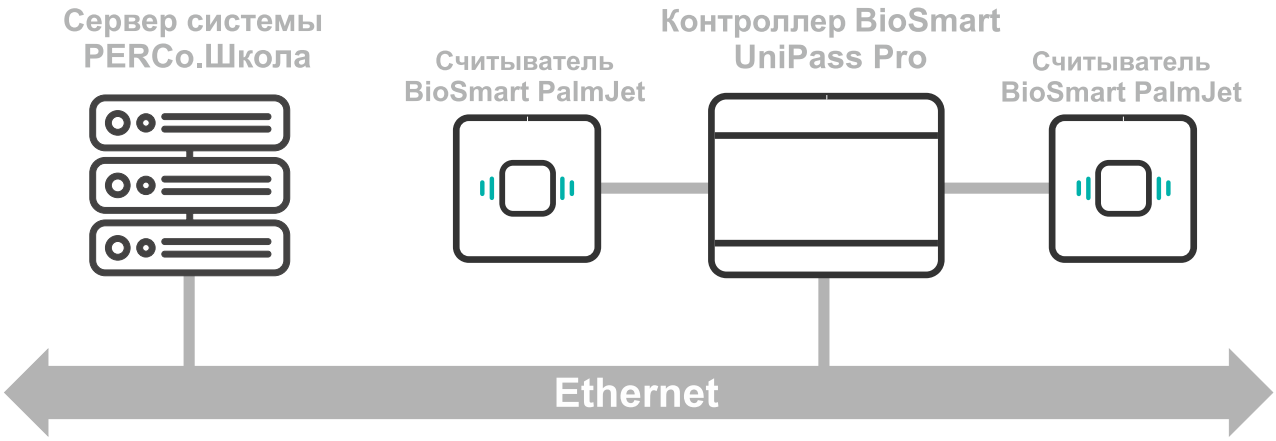
22.5. Подключение считывателя BioSmart PalmJet в системе PERCo.Школа

Подключение считывателя ***BioSmart PalmJet*** в системе ***PERCo.Школа*** возможно через контроллер ***BioSmart Unipass Pro*** или сервер ***BioSmart SmartHub***, который будет выполнять роль контроллера при отсутствии ***BioSmart UniPass Pro***.

SEC.RU | Короткий путь к информации Скачано с sec.ru

22.5.1. Подключение считывателя PalmJet через контроллер UniPass Pro

Считыватели ***BioSmart PalmJet*** подключаются к контроллеру ***BioSmart UniPass Pro***, который в свою очередь взаимодействует с сервером ***PERCo.Школа*** по сети *Ethernet*. Возможно подключение до двух считывателей к контроллеру.



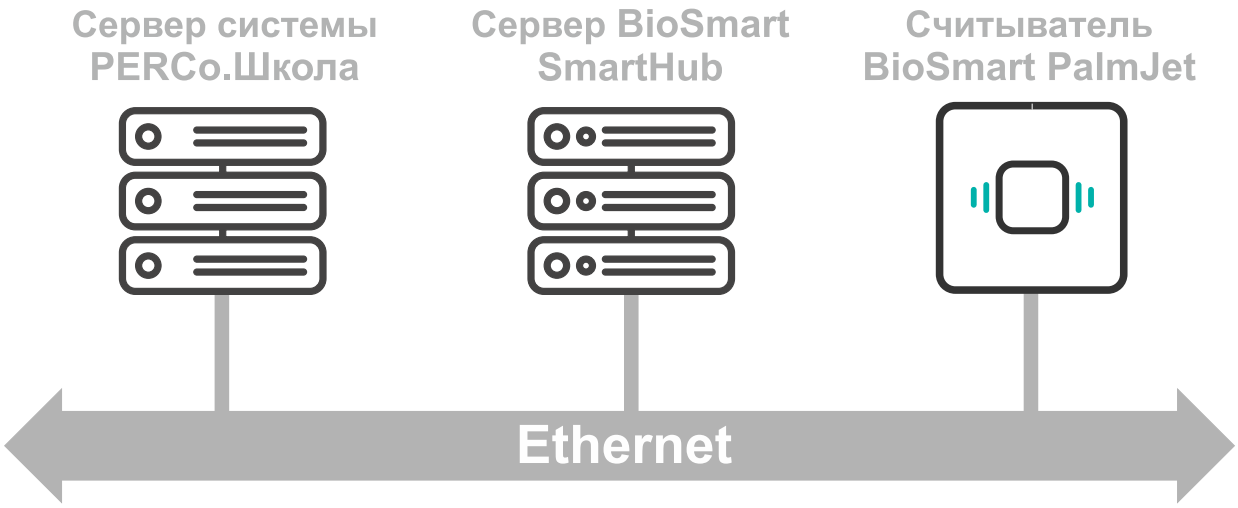
В системе ***PERCo.Школа*** необходимо настроить контроллер ***BioSmart UniPass Pro***, к которому подключены считыватели ***BioSmart PalmJet***. Для этого добавьте контроллер в конфигурацию системы, настройте параметры добавленного устройства и активируйте его. Добавление контроллера ***BioSmart UniPass Pro*** аналогично добавлению других устройств.

Настройка параметров контроллера ***BioSmart UniPass Pro*** осуществляется с помощью внутреннего интерфейса контроллера. Подробнее см. в руководстве по эксплуатации контроллера, доступном по ссылке https://confluence.prosyst.ru/pages/viewpage.action?pageId=127214298.

Считыватели ***BioSmart PalmJet*** не отображаются в дереве устройств в ***PERCo.Школа***, их подключение и настройка также выполняется через внутренний интерфейс контроллера ***BioSmart UniPass Pro***.

22.5.2. Подключение считывателя PalmJet через сервер BioSmart SmartHub

При подключении считывателя ***BioSmart PalmJet*** через сервер ***BioSmart SmartHub***, считыватель взаимодействует с сервером ***BioSmart SmartHub*** и с сервером ***PERCo.Школа*** по сети *Ethernet*.

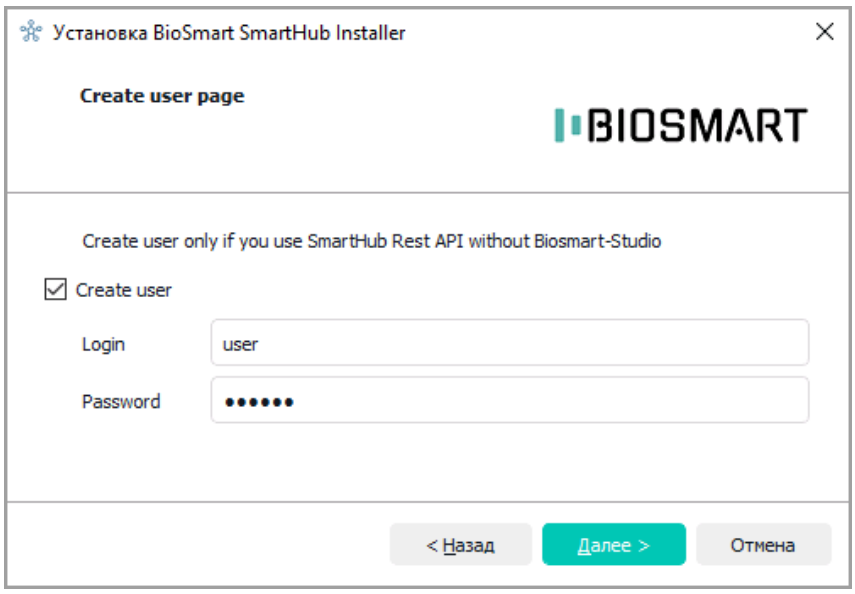


Для добавления сервера ***BioSmart SmartHub*** в конфигурацию системы ***PERCo.Школа*** и подключения считывателя ***BioSmart PalmJet***:

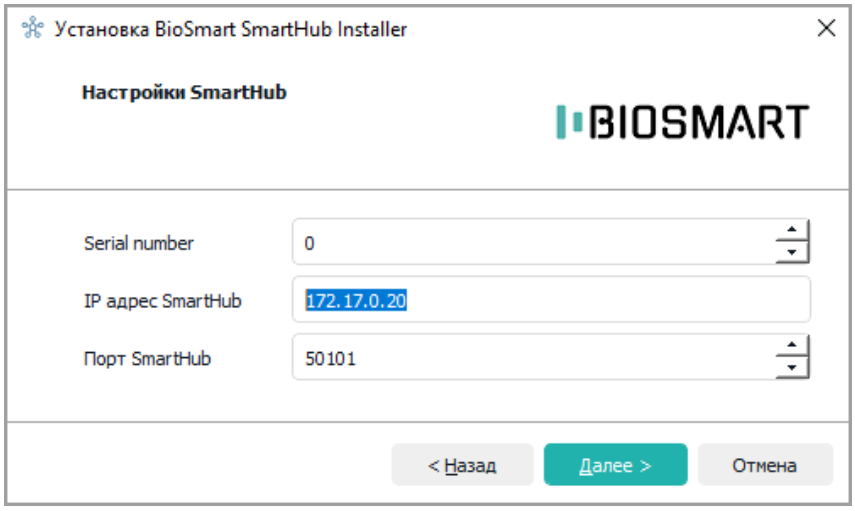
1. Скачайте последнюю актуальную версию программного сервиса ***BioSmart SmartHub***, доступной по ссылке https://bio-smart.ru/support#!/tab/185407858-4, файл **biosmart-smarthub-x.x.x.exe**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

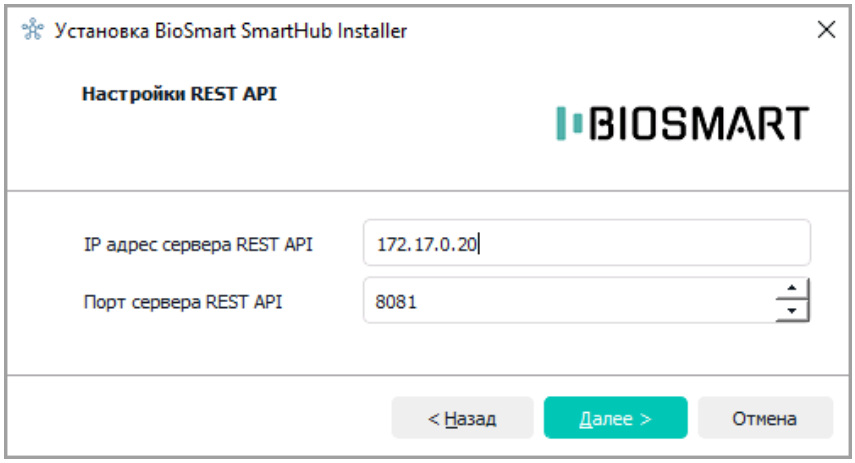
2. Установите ПО и произведите его дальнейшую настройку, следуя инструкции, доступной по ссылке https://confluence.prosyst.ru/pages/viewpage.action?pageId=91054105:
   - При установке необходимо создать пользователя, для этого на этапе **Create user page** установите флажок у параметра **Create user**. Задайте логин и пароль пользователя в полях **Login** и **Password**. Запомните введенные значения:



   - На этапе **Настройки SmartHub** в поле **IP адрес SmartHub** задайте IP-адрес сервера SmartHub. Поля **Serial number** и **Порт SmartHub** рекомендуется не изменять:

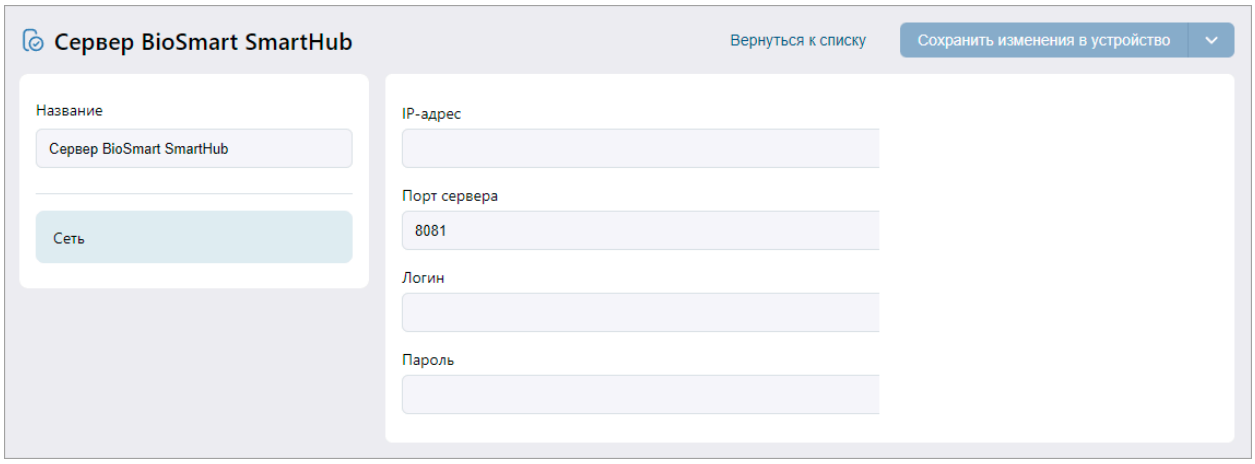


   - На этапе **Настройки REST API** в поле **IP адрес сервера REST API** повторно укажите IP-адрес сервера SmartHub, заданный на этапе **Настройки SmartHub**. В поле **Порт сервера REST API** укажите порт сервера. Запомните введенные значения:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

3. В системе ***PERCo.Школа*** перейдите в подраздел **«Конфигурация»** раздела **«Администрирование»**, используя панель навигации.
4. Перейдите на вкладку **Устройства**.
5. Нажмите на панели инструментов страницы кнопку **Добавить**. Из выпадающего списка выберите **Добавить сервер BioSmart SmartHub**. Откроется страница **Сервер BioSmart SmartHub**:

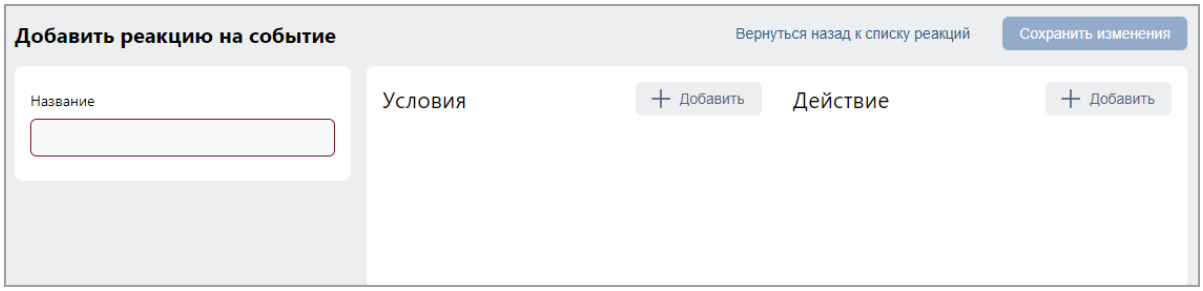


6. При необходимости в поле **Название** измените название сервера. При работе в режиме распределенной системы укажите сегмент.
7. В рабочей области страницы заполните значения следующих параметров:
   - В поле **IP-адрес** введите IP-адрес сервера ***BioSmart SmartHub***, заданный при установке в поле **IP адрес сервера REST API**.
   - Поле **Порт сервера** введите порт сервера ***BioSmart SmartHub***, заданный при установке в поле **Порт сервера REST API**.
   - В поле **Логин** введите логин пользователя, заданный при установке сервера ***BioSmart SmartHub***.
   - В поле **Пароль** введите пароль пользователя, заданный при установке сервера ***BioSmart SmartHub***.
8. Используя выпадающий список, находящийся справа от кнопки **Сохранить…**, выберите один из способов сохранения изменений:
   - **Только в базу данных** – параметры сохраняются только в БД системы и впоследствии должны быть переданы в устройство.
   - **Все в устройство** – в устройство передаются все параметры.
   - **Измененные в устройство** – в устройство передаются только измененные параметры.
9. Нажмите кнопку **Сохранить…**. Покиньте страницу с помощью кнопки **Вернуться к списку**, сервер ***BioSmart SmartHub*** будет добавлен в рабочую область страницы.
10. Активируйте добавленный сервер. Для этого выделите его в рабочей области страницы и нажмите кнопку **Активировать** на панели инструментов.
11. Используя кнопку **Поиск устройств**, вызовите окно **Найти устройства**. Добавьте и активируйте считыватель ***BioSmart PalmJet***. Настройте параметры добавленного считывателя.
12. В подразделе ***«Реакции на события»*** раздела ***«Администрирование»*** задайте реакции для системы ***PERCo.Школа*** на события со считывателем ***BioSmart PalmJet***. Например, разблокировка исполнительного устройства при успешной идентификации сотрудника с использованием считывателя ***BioSmart PalmJet***. Для настройки приведенной реакции:

SEC.RU | Короткий путь к информации Скачано с sec.ru

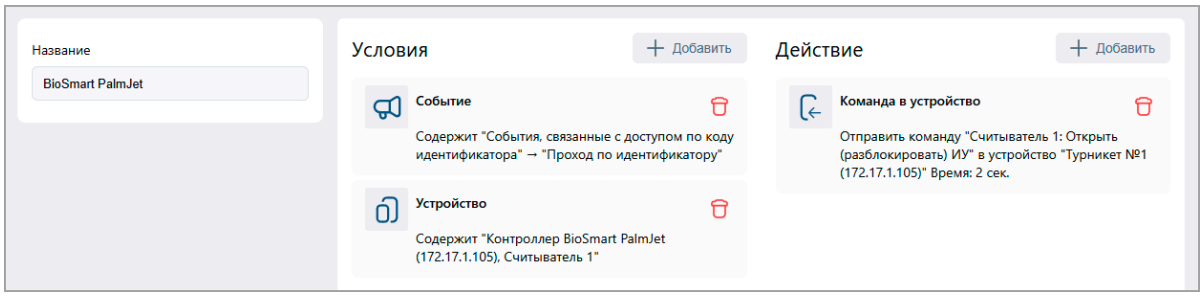
- Нажмите на панели инструментов страницы кнопку **Добавить**, а затем **Добавить реакцию на событие**.

  Откроется страница, имеющая следующий вид:



- В поле **Название** введите название для новой реакции.
- В разделе **Условия** выберите условия для новой реакции. Для этого нажмите кнопку **Добавить** и выберите из списка **Добавить событие**. В открывшемся окне выберите событие **Проход по идентификатору**. Нажмите кнопку **Выбрать**. Окно закроется, выбранное событие отобразится в рабочей области окна.
- Аналогично в условия добавьте считыватель ***BioSmart PalmJet***, для этого выберите условие **Добавить устройство**. В открывшемся окне в качестве устройства выберите соответствующий считыватель ***BioSmart PalmJet***, в поле **Ресурс** укажите **Считыватель 1**.
- В разделе **Действие** выберите действия, которые будут происходить при заданных условиях. Для этого нажмите кнопку **Добавить** и выберите из списка **Команда в устройство**. В открывшемся окне укажите устройство, на которое необходимо подать команду. В поле **Команда** укажите команду **Открыть (разблокировать ИУ)** соответствующего направления прохода.

  В данном примере реакция после настройки будет иметь следующий вид:



- Нажмите кнопку **Сохранить изменения**, новая реакция появится в рабочей области страницы.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

23. Параметры видеокамеры

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

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

Примечание:

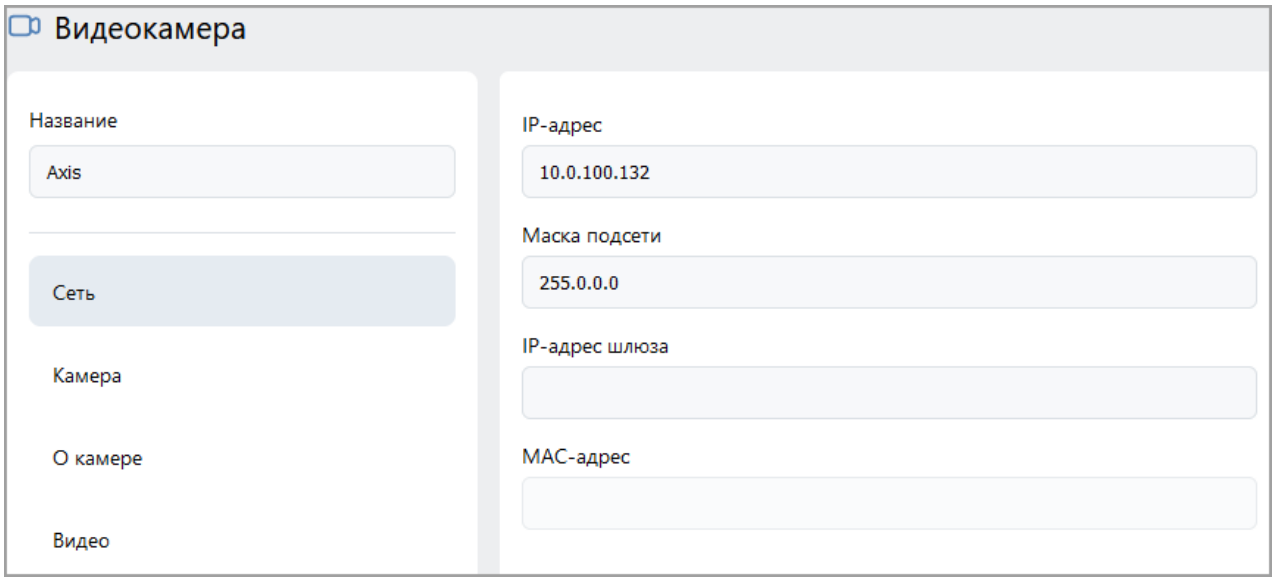
Параметры видеокамеры ***TRASSIR*** описываются в ***Руководстве пользователя модуля PERCo-WM06 «Интеграция с TRASSIR»***.

23.1. Вкладка «Сеть»

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

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

Окно имеет следующий вид:



23.2. Вкладка «Камера»

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

Параметры камеры:

- **Логин**;
- **Пароль**.

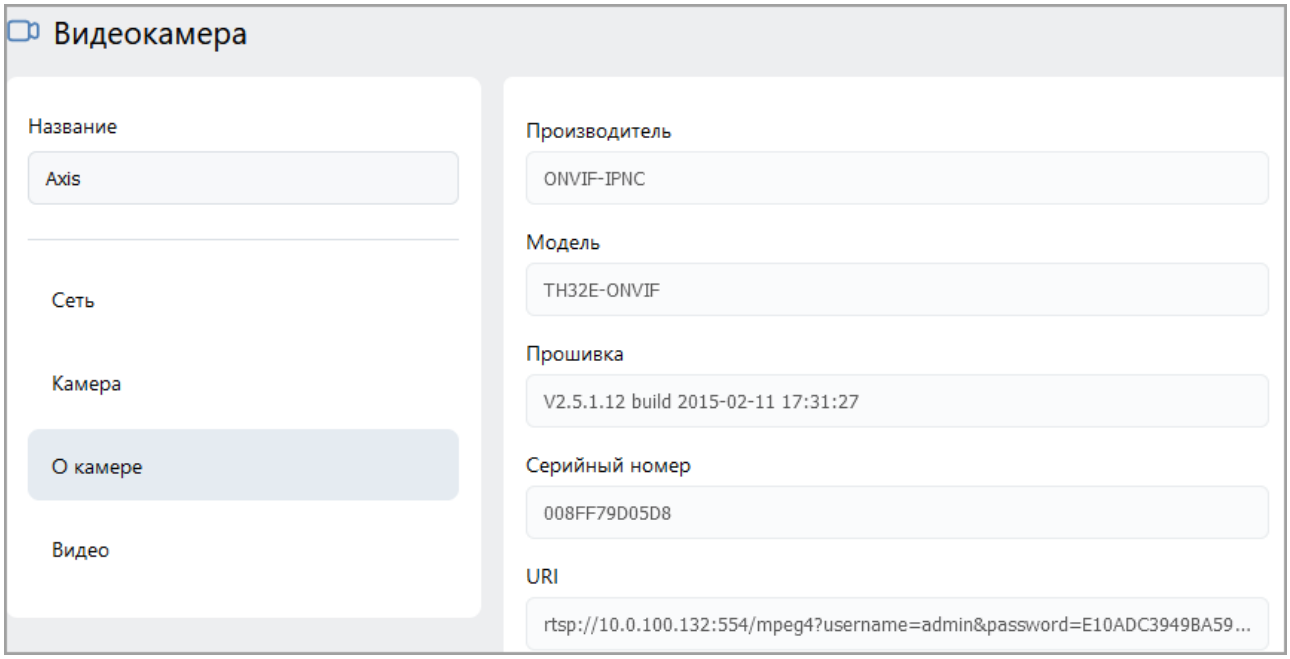
23.3. Вкладка «О камере»

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

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

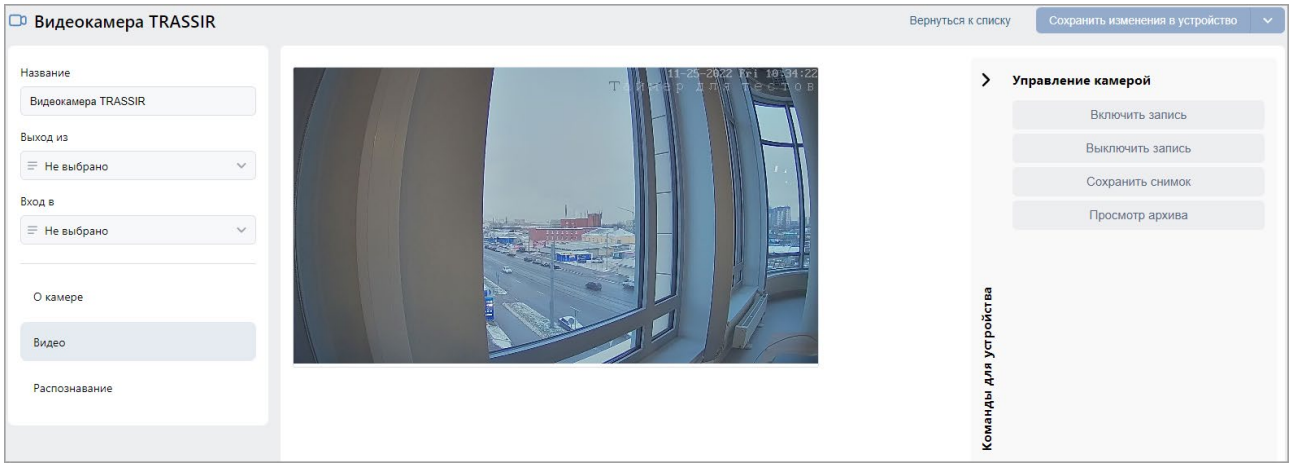
Окно имеет следующий вид:



23.4. Вкладка «Видео»

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

Окно имеет следующий вид:

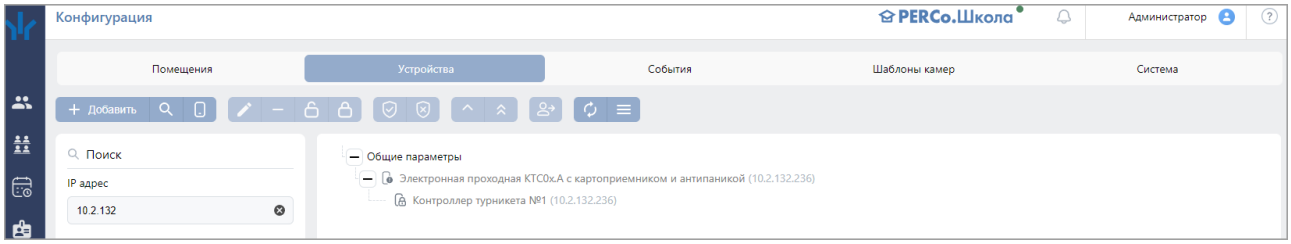


SEC.RU | Короткий путь к информации
Скачано с sec.ru

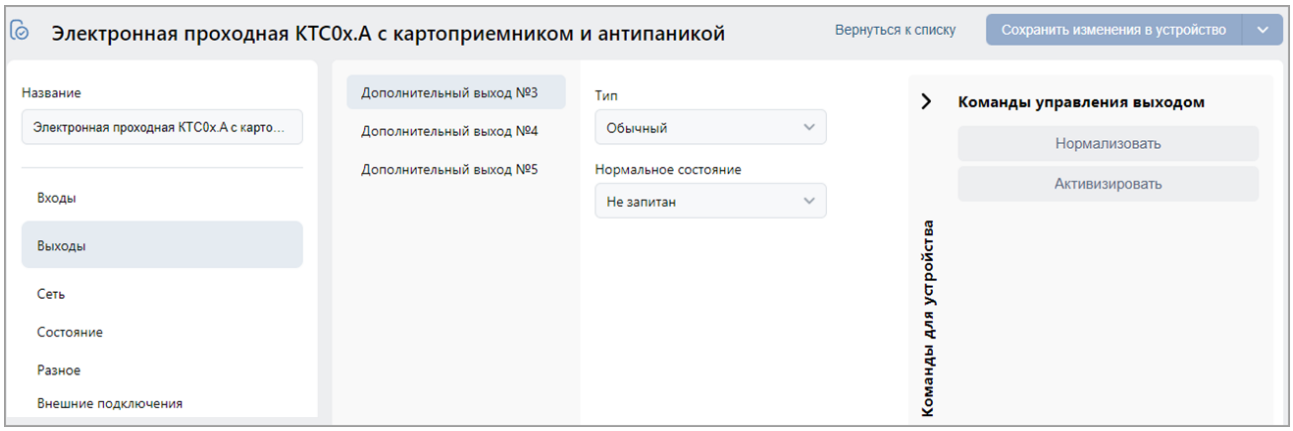
24. Настройка контроллера СКУД PERCo для работы с картоприемником

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

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



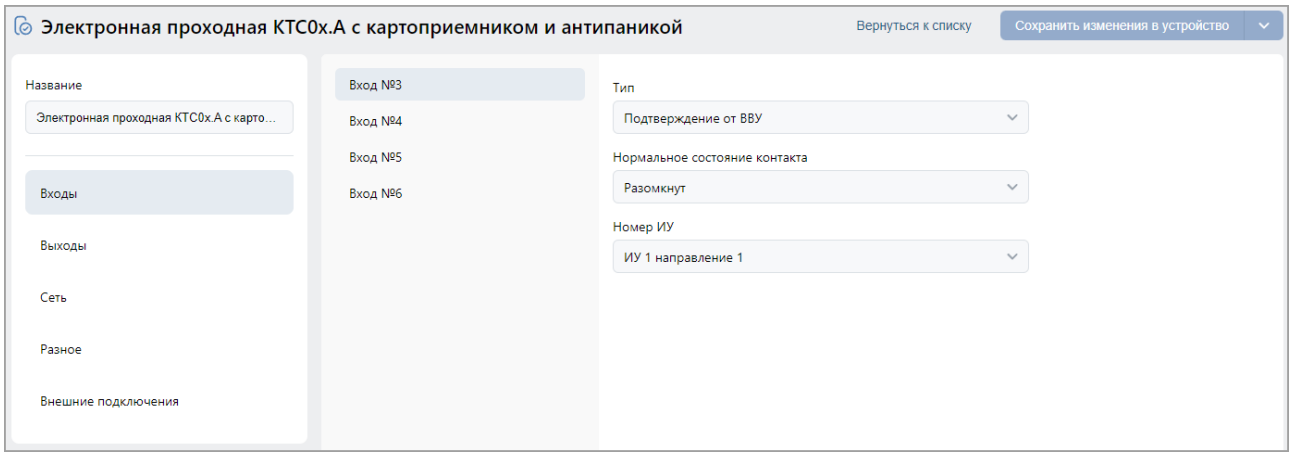
4. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется страница, отражающая название контроллера.
5. Перейдите на вкладку **Выходы**:



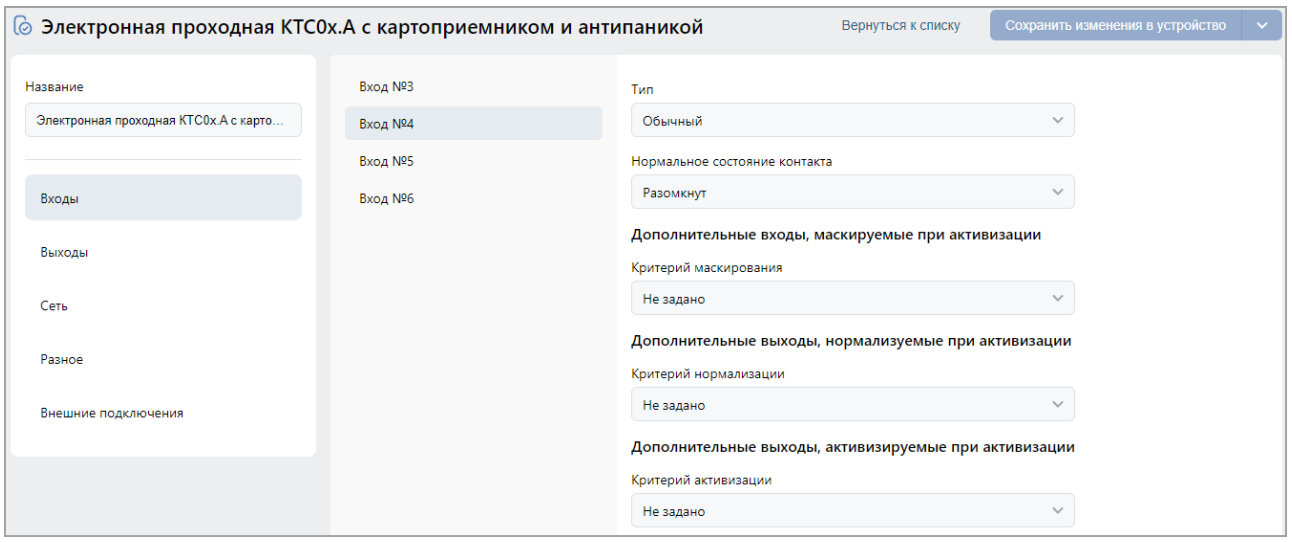
6. В рабочей области страницы выберите **Дополнительный выход №…** (номер выхода должен соответствовать выходу контроллера, к которому физически подключен вход *«Изъять карту»* картоприемника).
7. Установите с помощью соответствующего раскрывающегося списка в рабочей области страницы:
   - для параметра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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- для параметра **Номер ИУ** значение **ИУ… направление…** (номер ИУ и номер направления должны соответствовать тем, которые контролируются картоприемником):



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

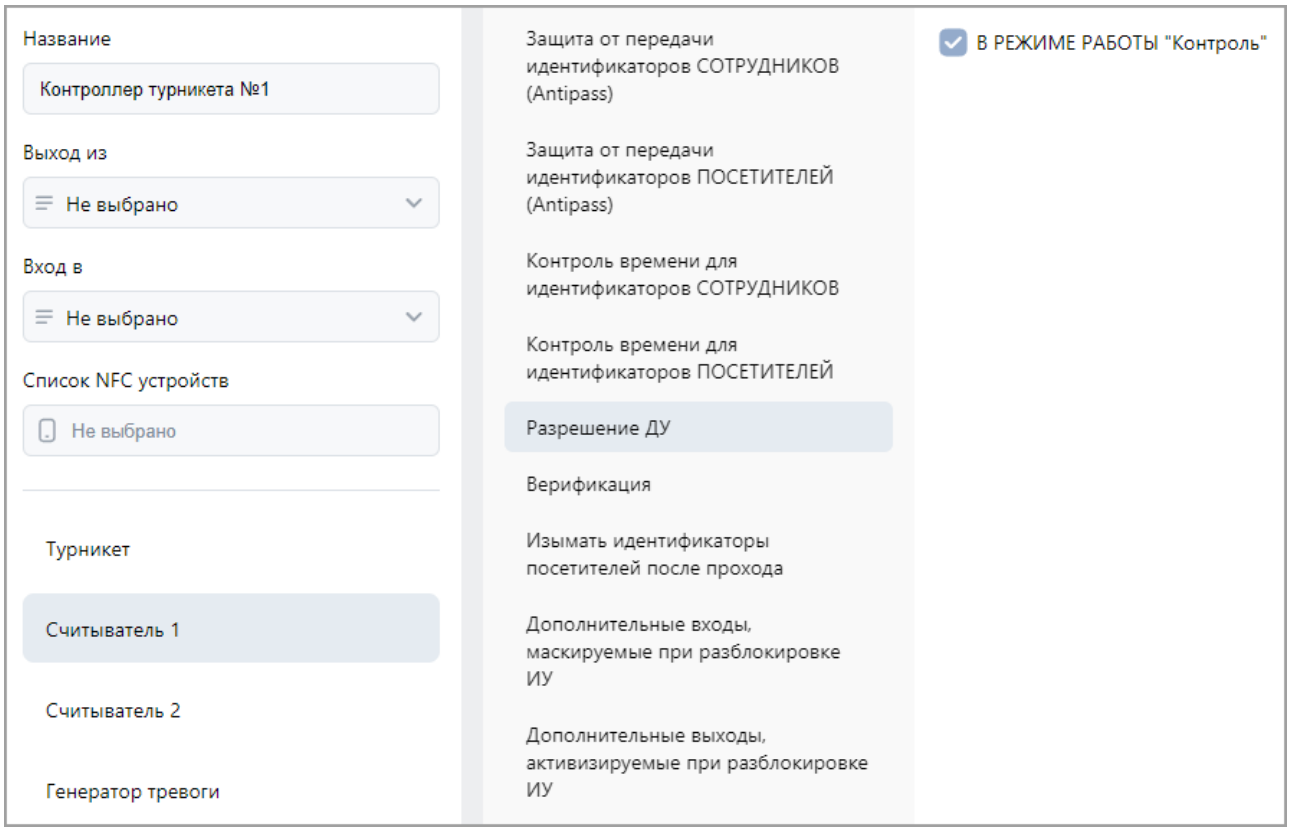


12. Поочередно нажмите кнопки **Сохранить изменения в устройство** и **Вернуться к списку**. Страница, отражающая название контроллера, будет закрыта.
13. В рабочей области страницы в составе основного контроллера выделите контроллер ИУ, который контролируется картоприемником.
14. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется страница, отражающая название контроллера.
15. Перейдите на вкладку ресурса **Считыватель №…** (номер считывателя должен соответствовать считывателю, контролируемому картоприемником).
16. Подтверждением изъятия карты для контроллера доступа является сигнал от картоприемника *«Карта изъята»*. Для настройки подтверждения для параметра **Верификация** установите значение:
    - **ВВУ**, если картоприемник выступает в качестве внешнего верифицирующего

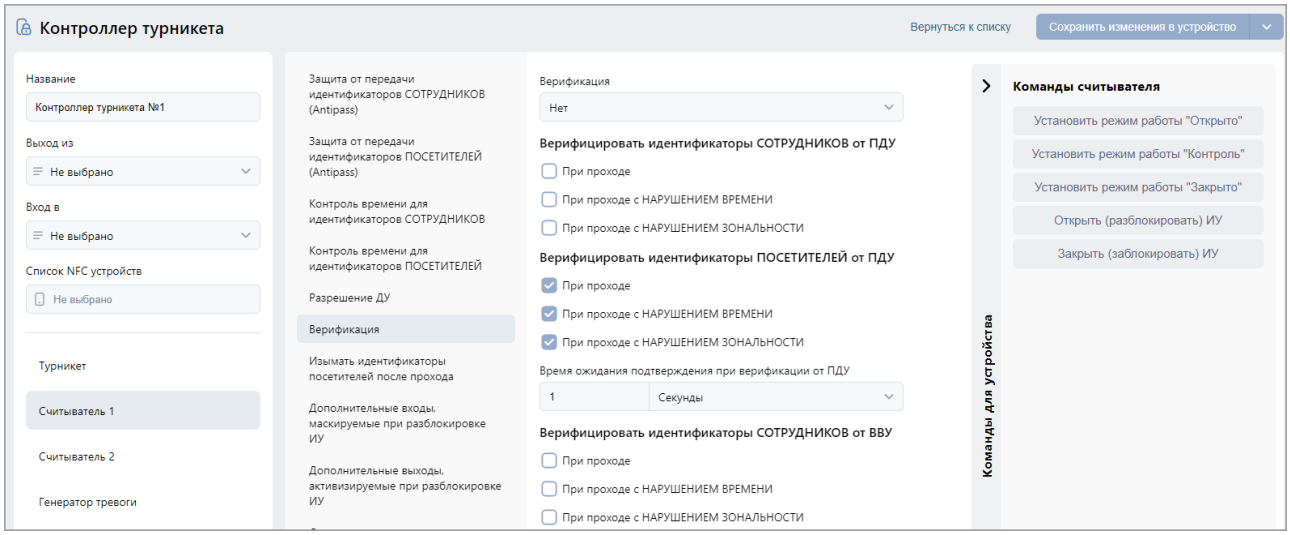
SEC.RU | Короткий путь к информации
Скачано с sec.ru

устройства для контроллера (сигнал *«Карта изъята»* поступает на отдельный вход контроллера);

- **ПДУ**, если выход *«Карта изъята»* картоприемника подключен к контроллеру параллельно ПДУ. В этом случае также нужно установить для параметра **Разрешение ДУ** флажок для значения **В РЕЖИМЕ РАБОТЫ «Контроль»**:



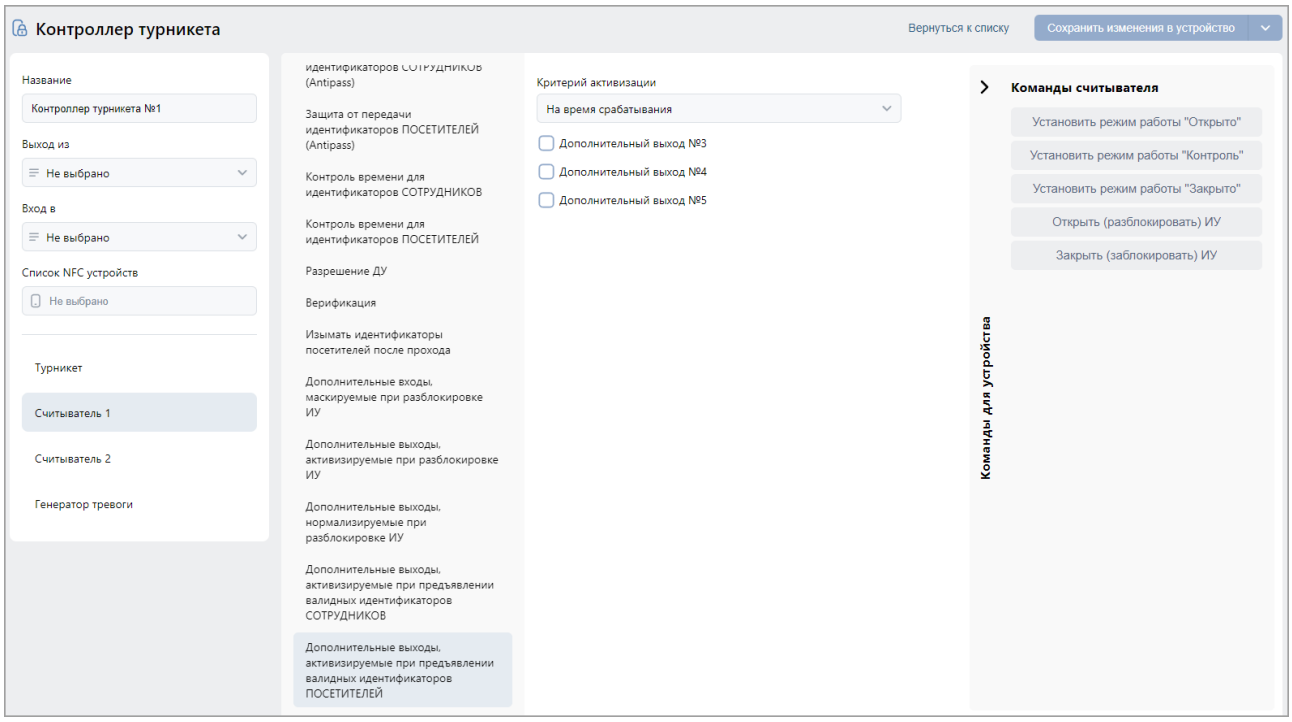
17. Установите в рабочей области страницы для параметра **Верифицировать идентификаторы ПОСЕТИТЕЛЕЙ от ВВУ** (или, соответственно, **от ПДУ**) флажки:
    - **при проходе**;
    - **при проходе с НАРУШЕНИЕМ ВРЕМЕНИ**;
    - **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**.
18. Установите в рабочей области страницы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



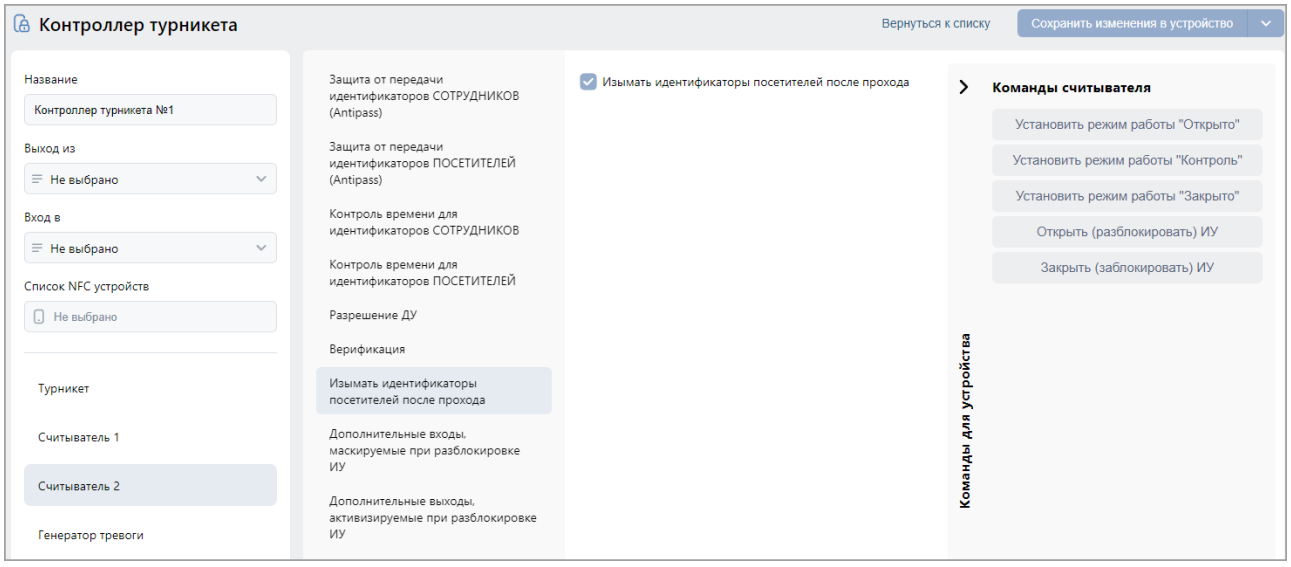
19. Выберите параметр **Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов ПОСЕТИТЕЛЕЙ**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

20. Установите с помощью раскрывающегося списка в рабочей области страницы для параметра **Критерий активизации** значение **На время срабатывания**.
21. Установите флажок **Дополнительный выход №…** (номер выхода, к которому подключен вход *«Изъять карту»* картоприемника):



22. Выберите параметр **Изымать идентификаторы посетителей после прохода** и установите для него флажок:



Примечание:

При изъятии идентификатора данные посетителя автоматически переносятся на вкладку **Архив** раздела ***«Бюро пропусков»*** (см. ***«Руководством пользователя „Стандартного пакета ПО“ PERCo-ES»***).

23. Поочередно нажмите кнопки **Сохранить изменения в устройство** и **Вернуться к списку**. Страница **Контроллер турникета** будет закрыта, настройки сохранены.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

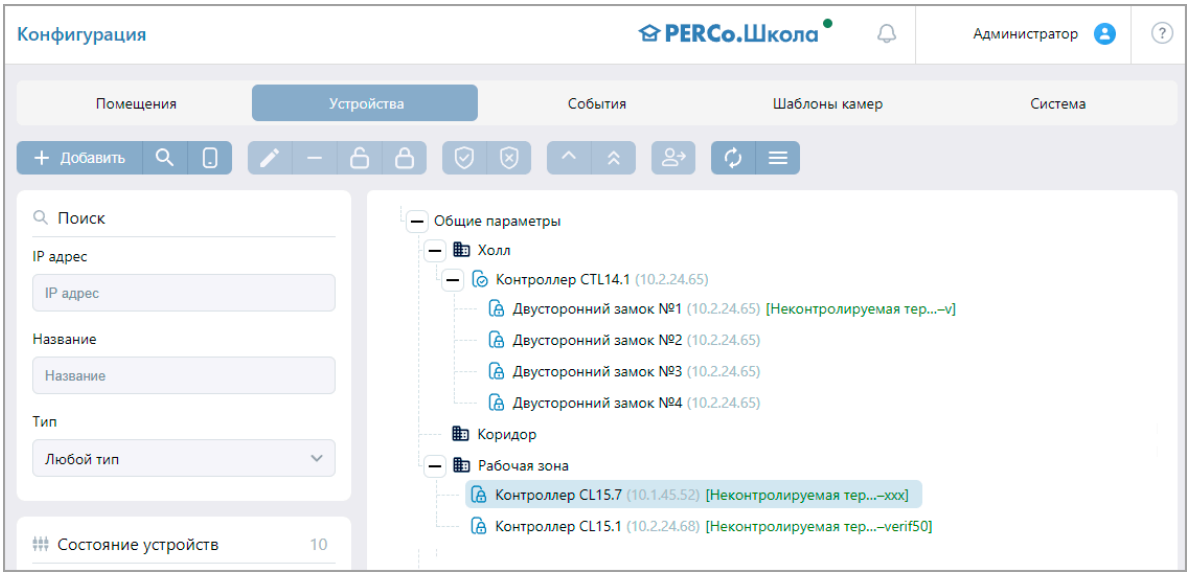
25. Настройка контроллера СКУД PERCo для работы с алкотестером «Алкобарьер», интегрированным в систему

Примечание:

Работа алкотестера «Алкобарьер» по сети *Ethernet* возможна только с контроллерами ***PERCo-CT/L14***, ***PERCo-CT/L14.1***, ***PERCo-CL15***, ***PERCo-CL15.1***, ***PERCo-CL15.3***, ***PERCo-CL15.7*** и со встроенными контроллерами ***CT13***, ***CT13.1*** электронных проходных ***PERCo***.

После монтажа и включения алкотестера «Алкобарьер» необходимо произвести его конфигурирование в системе, для этого:

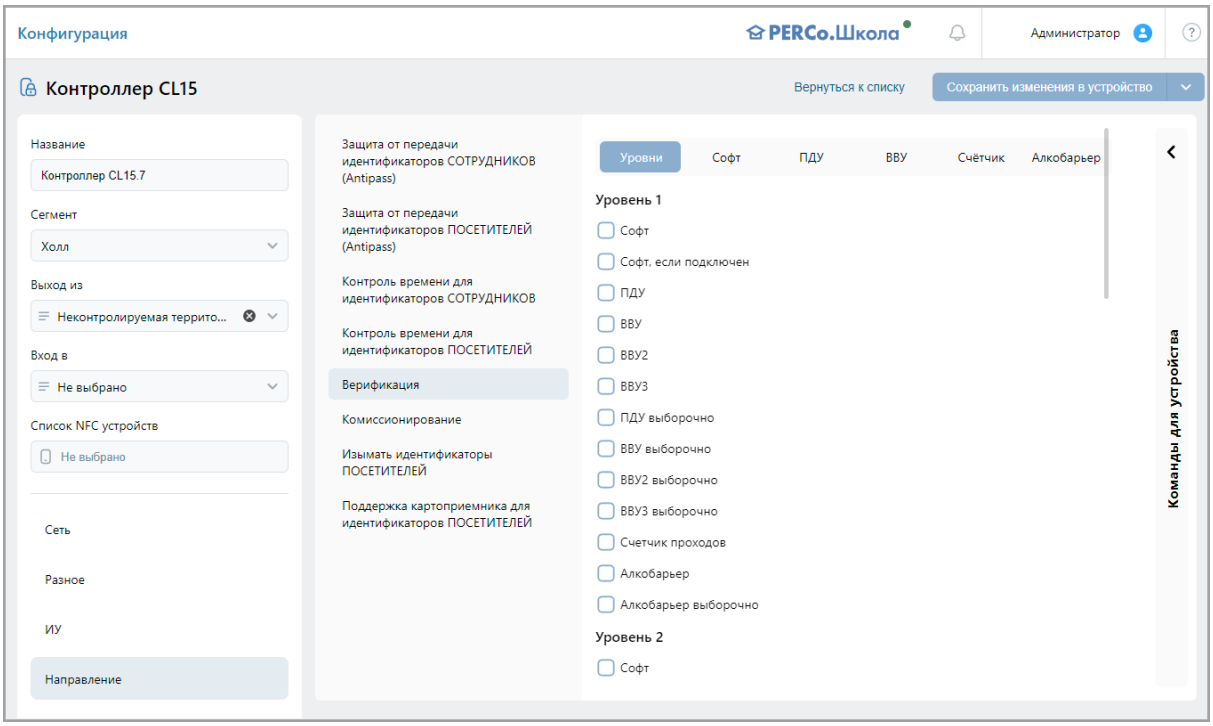
1. Войдите в систему, используя браузер.
2. Используя панель навигации, перейдите в подраздел **«Конфигурация»** раздела **«Администрирование»**.
3. В рабочей области страницы выделите контроллер, к которому физически подключен алкотестер «Алкобарьер» (либо при наличии выделите исполнительное устройство, контролируемое алкотестером «Алкобарьер»):



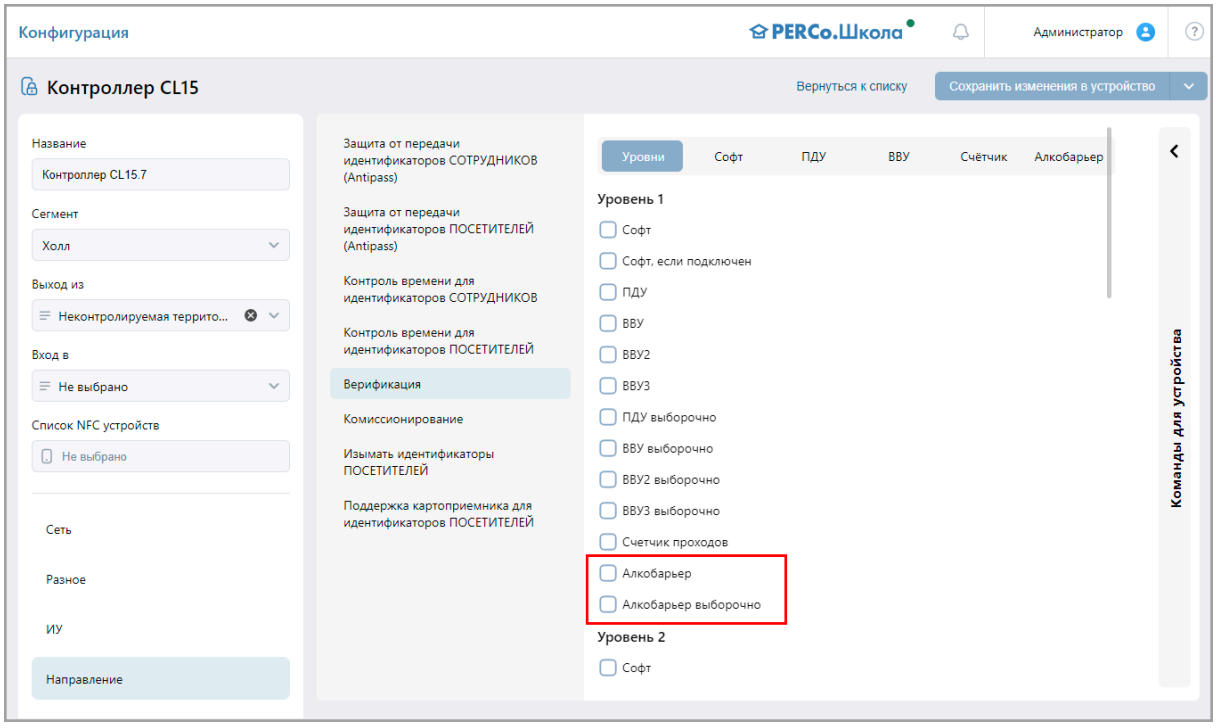
4. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется страница, отражающая название контроллера или исполнительного устройства.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5. В открывшемся окне перейдите на вкладку **Направление**. В рабочей области выберите вкладку **Верификация -> Уровни**:

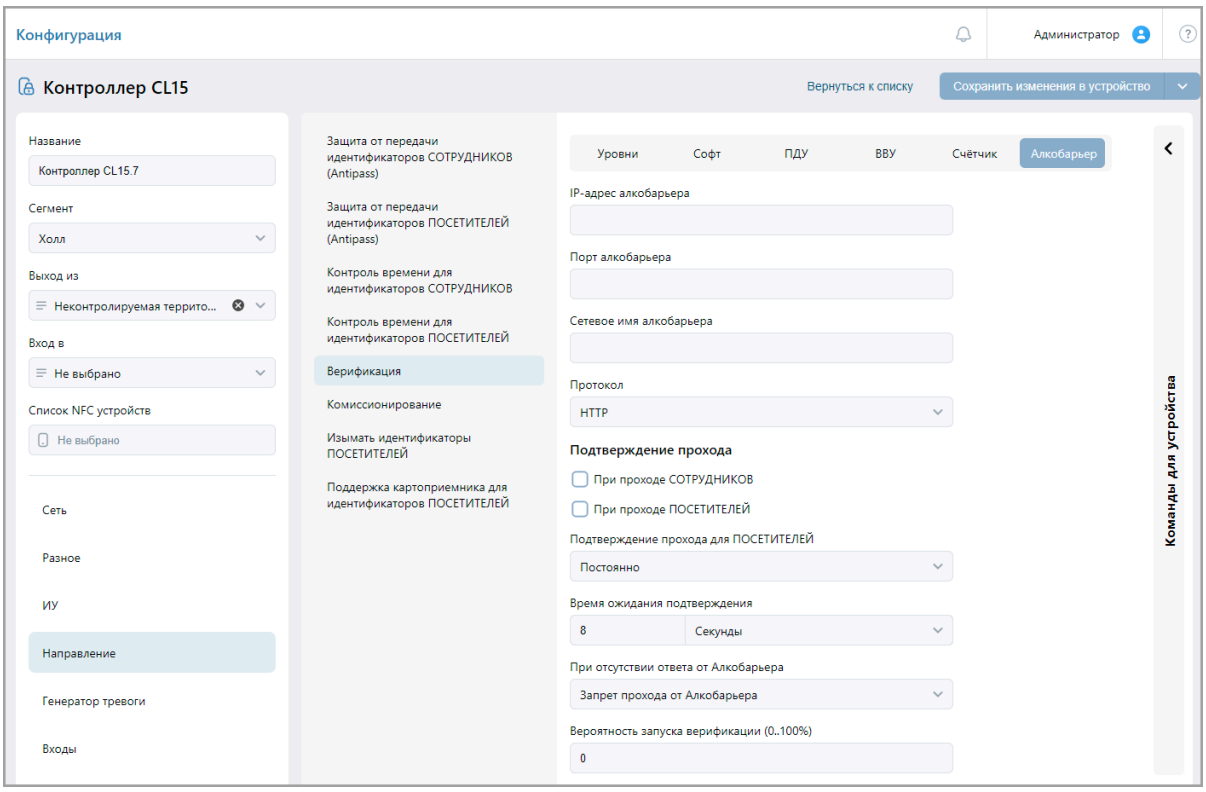


6. В соответствующем уровне верификации выберите тип используемой верификации **Алкобарьер** или **Алкобарьер выборочно** (позволяет запускать верификацию с определенной вероятностью):

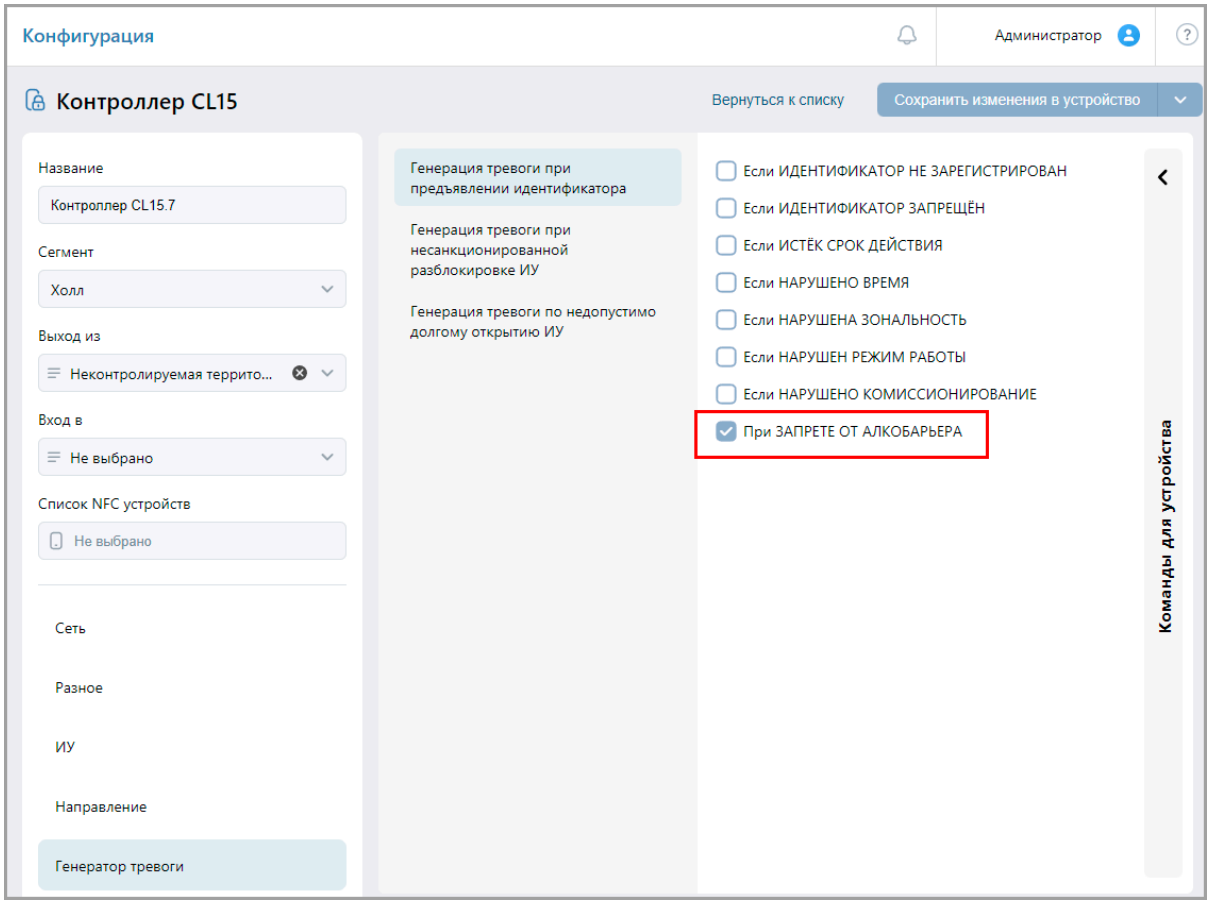


Перейдите на вкладку **Алкобарьер**. Заполните данные устройства: **IP-адрес алкобарьера**, **Порт алкобарьера**, **Сетевое имя алкобарьера**, **Протокол** и т.д.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



7. Перейдите на вкладку **Генератор тревоги -> Генерация тревоги при предъявлении идентификатора**. Поставьте флажок напротив значения **При ЗАПРЕТЕ ОТ АЛКОБАРЬЕРА**:



8. Нажмите поочередно кнопки **Сохранить изменения в устройство** и **Вернуться к списку**. Страница контроллера или исполнительного устройства будет закрыта, настройки сохранены.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

25.1. Как узнать IP-адрес алкотестера «Алкобарьер»?

Чтобы узнать IP-адрес алкотестера «Алкобарьер», необходимо зайти в его настройки:

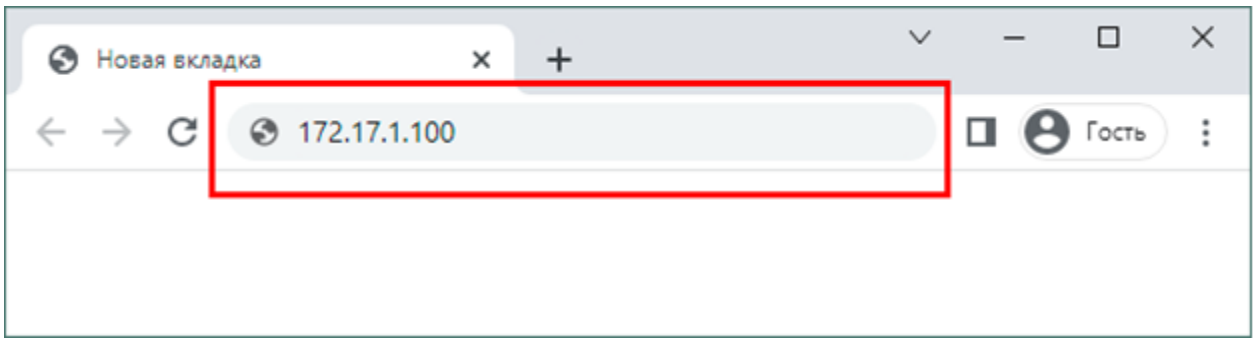
1. Снимите верхнюю крышку алкотестера «Алкобарьер».
2. Нажмите кнопку **Назад** на алкотестере «Алкобарьер». На экране будет написано **Настройки газоанализатора**.
3. Нажимайте кнопку **Вниз** до появления на экране надписи **Модуль Ethernet Настройки**.
4. Нажмите кнопку **Ввод**. На экране будет написано **Настройки адреса**.
5. Снова нажмите кнопку **Ввод**.
6. Нажимайте кнопку **Вниз** до появления на экране надписи **IP-адрес xxx.xxx.xxx.xxx** (в данном случае IP-адрес 172.17.1.100):



25.2. Как узнать порт, протокол и сетевое имя алкотестера «Алкобарьер»?

Чтобы узнать порт, тип соединения и сетевое имя алкотестера «Алкобарьер», необходимо зайти в Web-интерфейс алкотестера «Алкобарьер»:

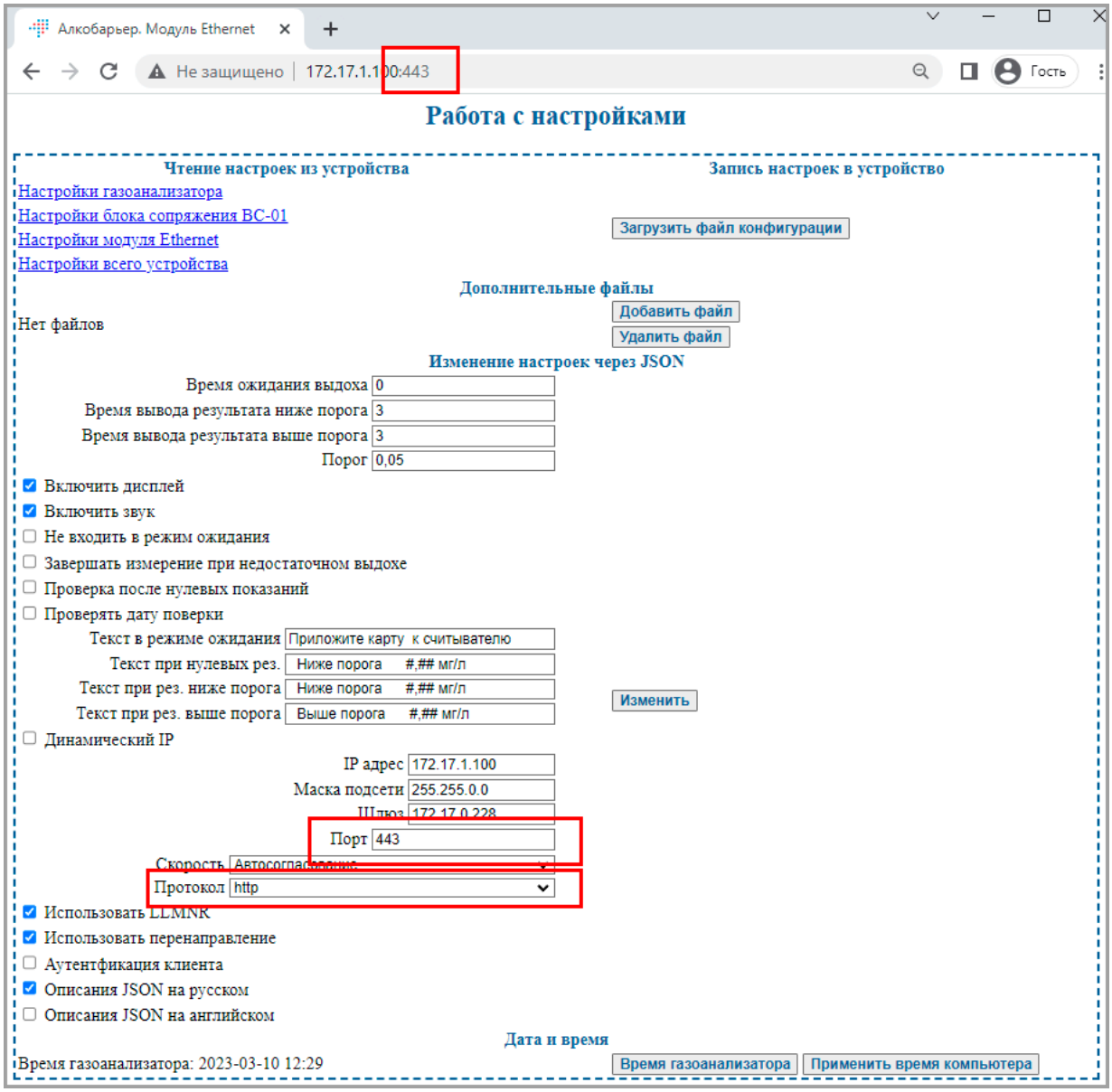
1. В браузере в адресной строке введите IP-адрес алкотестера «Алкобарьер»:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

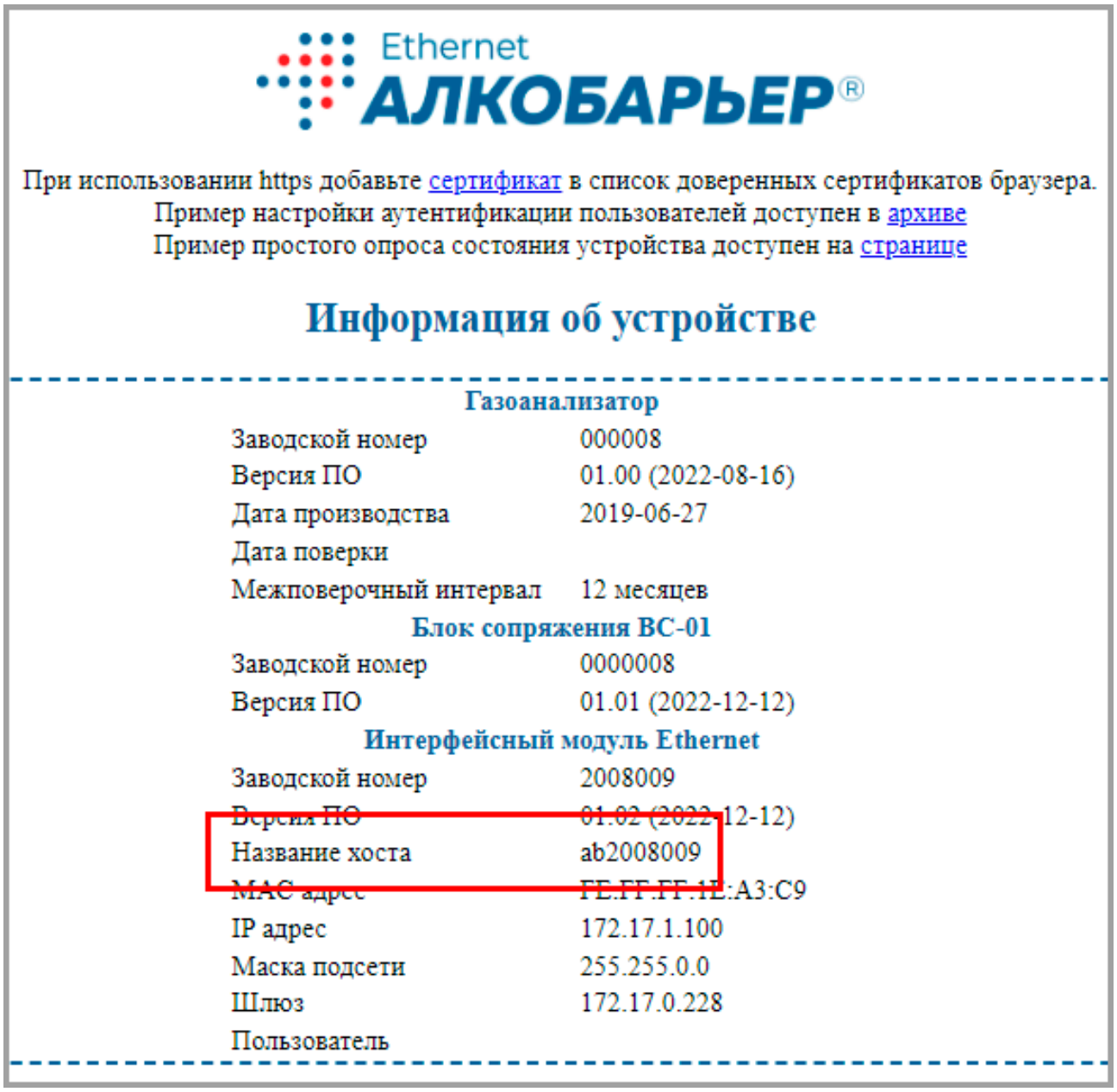
2. Откроется страница *Алкобарьер. Модуль Ethernet*. Порт можно узнать в адресной строке в URL-адресе страницы (число после двоеточия), либо в разделе **Работа с настройками** в поле **Порт**. Тип соединения, простое HTTP или зашифрованное HTTPS, можно узнать в разделе **Работа с настройками** в поле **Протокол**.

   В данном примере порт – 443, протокол – http:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

3. Сетевое имя можно узнать в разделе **Информация об устройстве** в подразделе **Интерфейсный модуль Ethernet** характеристика **Название хоста** (в данном случае сетевое имя – ab2008009):

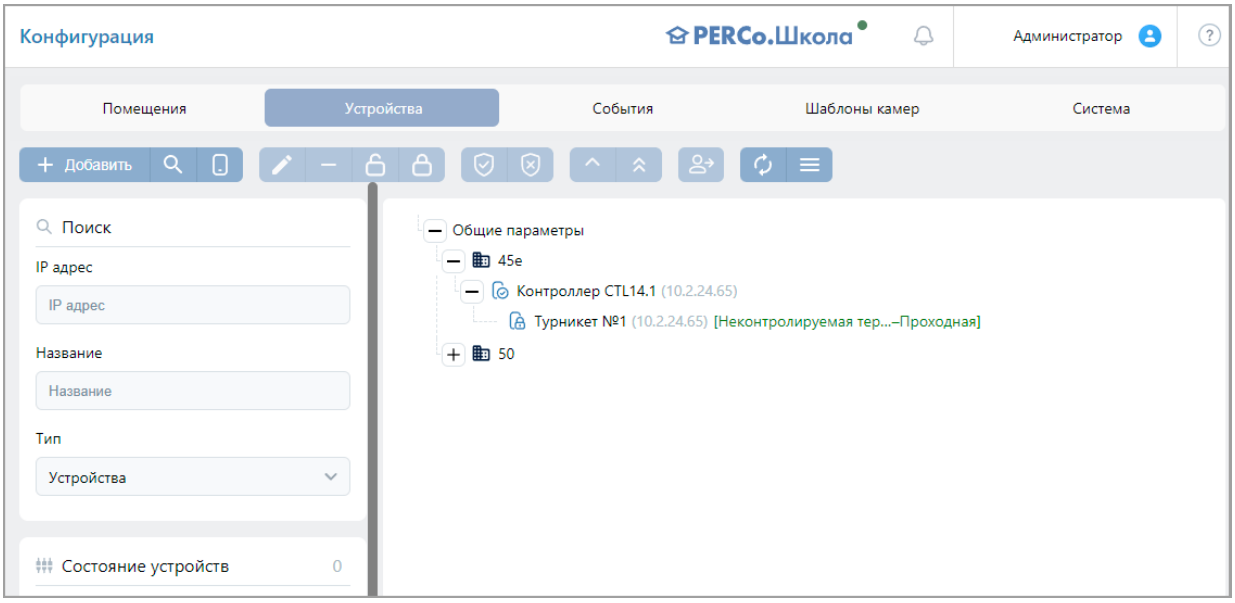


SEC.RU | Короткий путь к информации Скачано с sec.ru

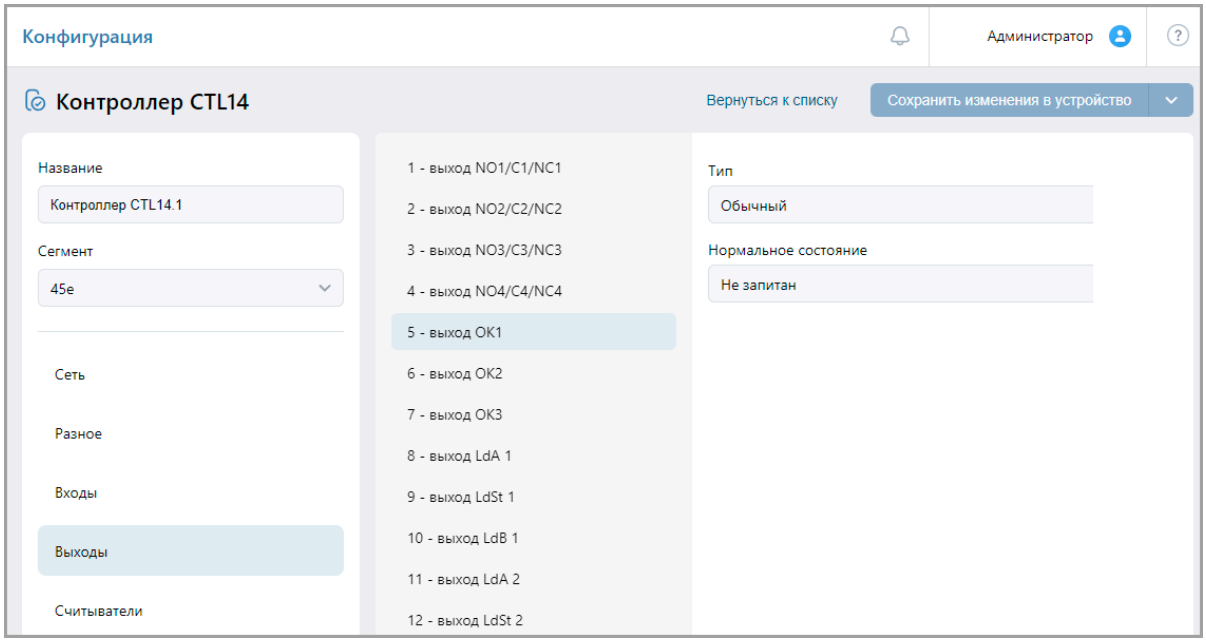
26. Настройка контроллера СКУД PERCo для работы с алкотестером «Алкобарьер» в качестве ВВУ

После монтажа и включения алкотестера «Алкобарьер» необходимо произвести его конфигурирование в системе, для этого:

1. Войдите в систему, используя браузер.
2. Используя панель навигации, перейдите в подраздел **«Конфигурация»** раздела **«Администрирование»**.
3. В рабочей области страницы выделите основной контроллер, к которому физически подключен алкотестер «Алкобарьер»:



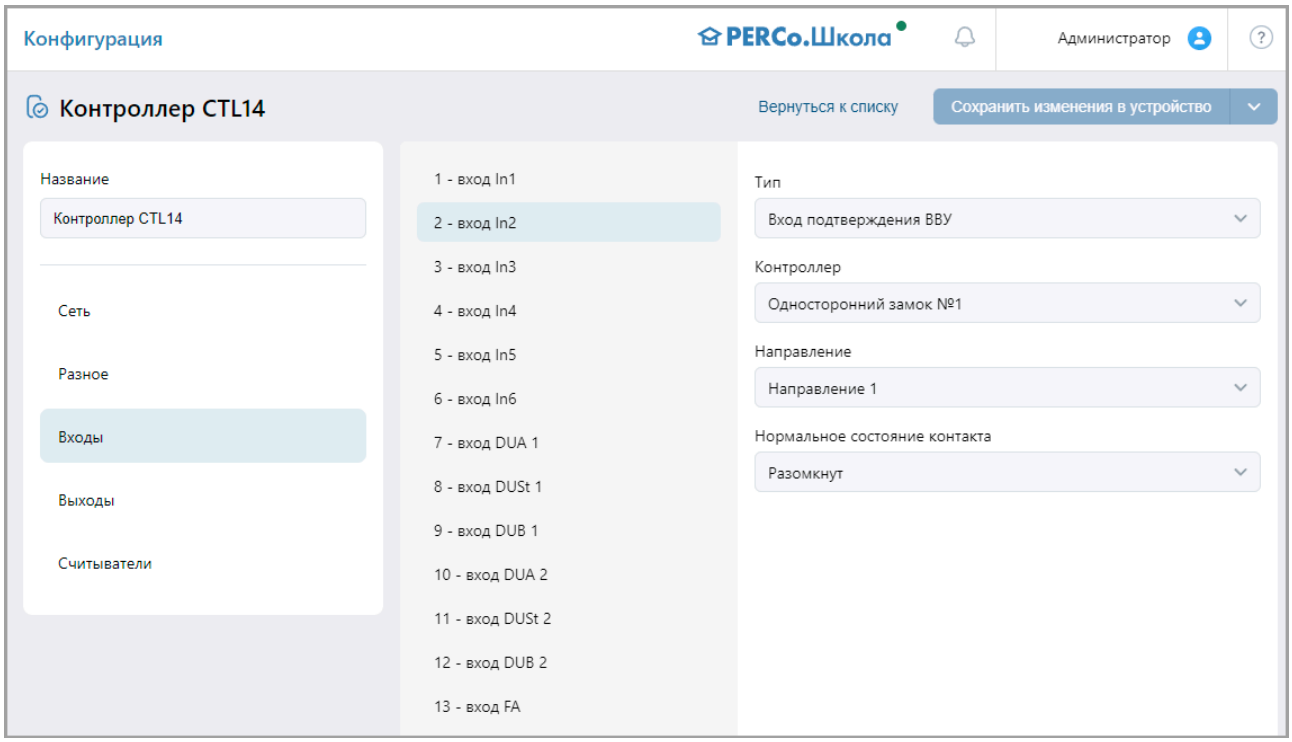
4. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется страница, отражающая название контроллера.
5. В открывшемся окне перейдите на вкладку **Выходы**, выберите выход контроллера, к которому физически подключен вход «Начать анализ» алкотестера «Алкобарьер»:



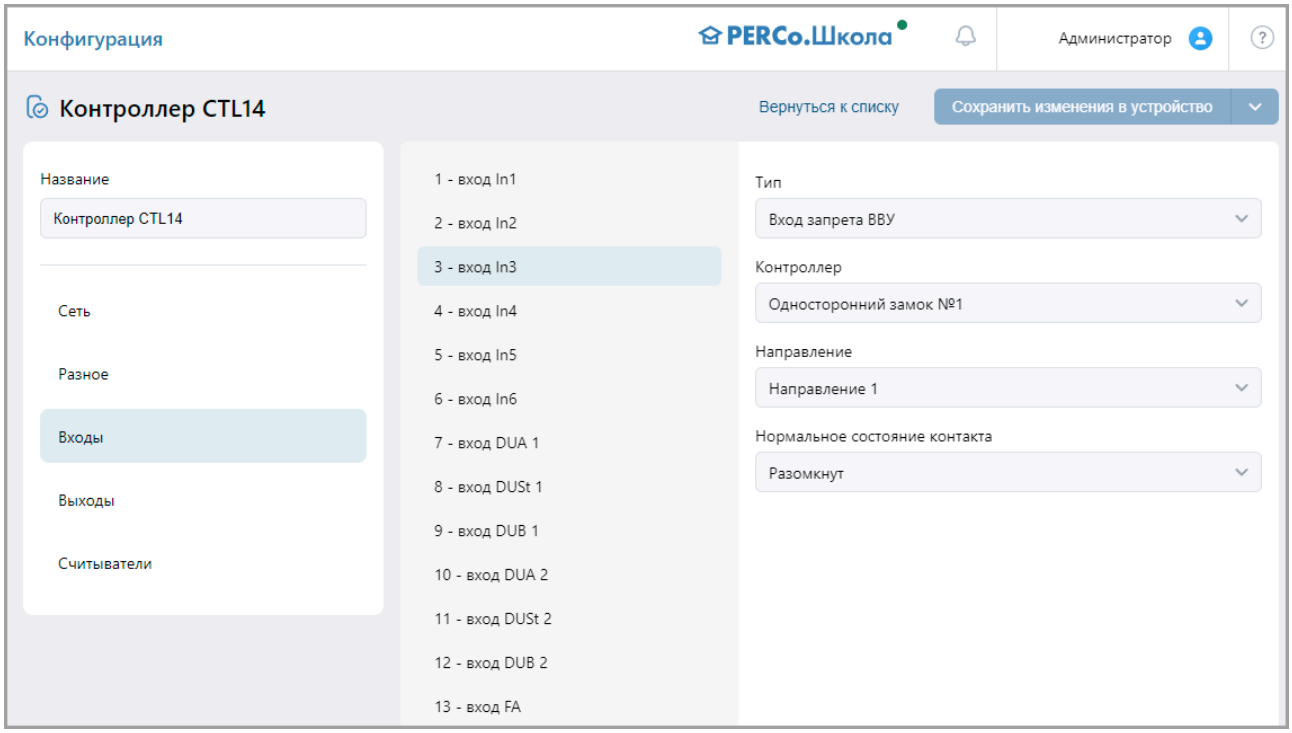
6. Установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
   - для параметра **Тип** – значение **Обычный**;
   - для параметра **Нормальное состояние** – значение **Не запитан**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7. Перейдите на вкладку **Входы**, выберите вход контроллера, к которому физически подключен выход «Разрешение» алкотестера «Алкобарьер»:



8. Установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
   - для параметра **Тип** – значение **Вход подтверждения ВВУ**;
   - для параметра **Контроллер** выберите исполнительное устройство;
   - для параметра **Направление** – значение направления, контролируемое алкотестером;
   - для параметра **Нормальное состояние** – значение **Разомкнут**.
9. Выберите вход контроллера, к которому физически подключен выход «Запрет» алкотестера «Алкобарьер»:

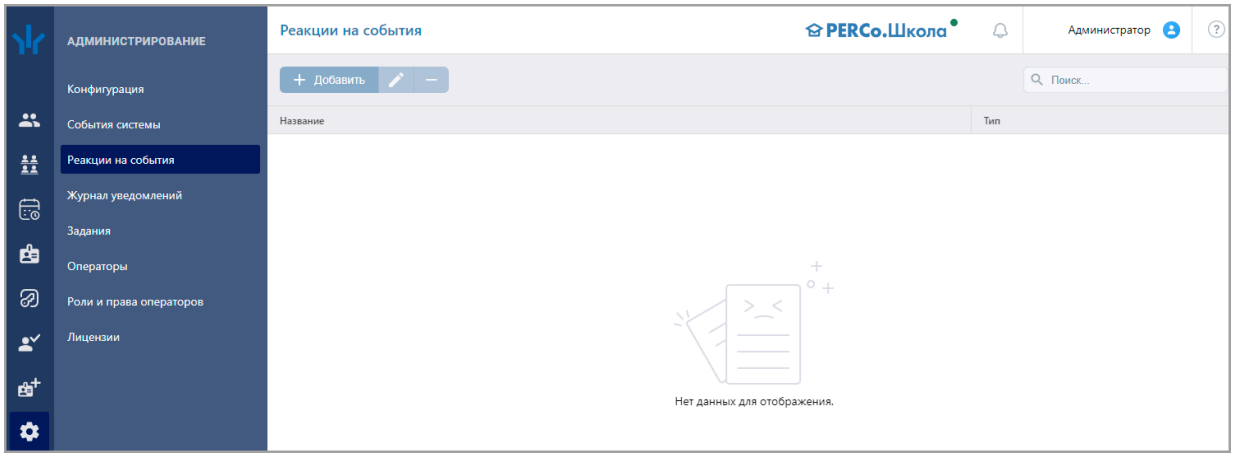


10. Установите с помощью соответствующего раскрывающегося списка в рабочей области окна:
    - для параметра **Тип** – значение **Вход запрета ВВУ**;
    - для параметра **Контроллер** выберите исполнительное устройство;

SEC.RU | Короткий путь к информации
Скачано с sec.ru

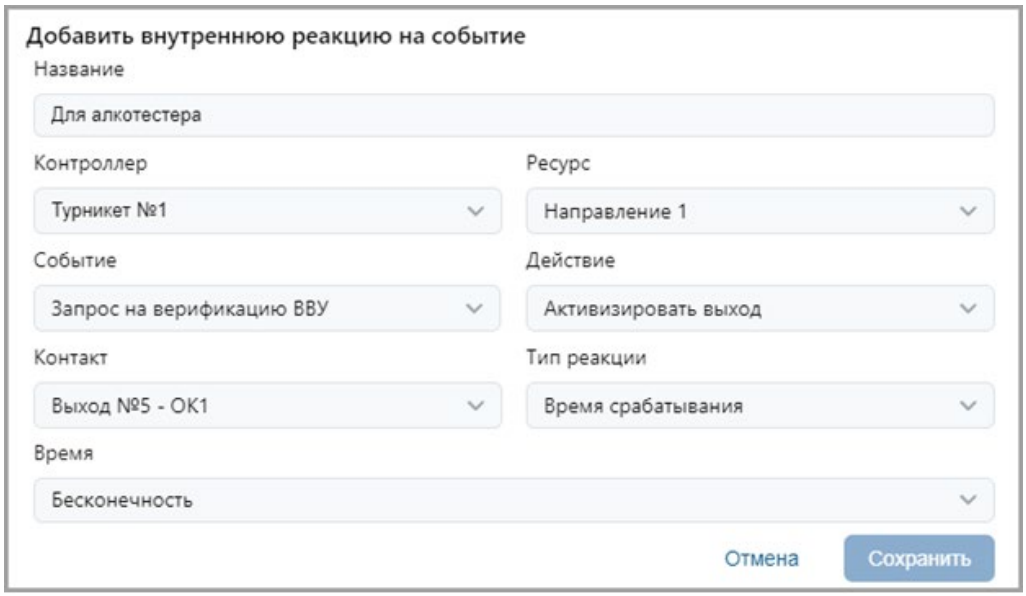
- для параметра **Направление** – значение направления, контролируемое алкотестером;
- для параметра **Нормальное состояние** – значение **Разомкнут**.

11. Поочередно нажмите кнопки **Сохранить изменения в устройство** и **Вернуться к списку**. Страница контроллера будет закрыта, настройки сохранены.
12. Используя панель навигации, перейдите в раздел **«Администрирование»** подраздел **«Реакции на события»**:



13. В рабочей области нажмите на кнопку 

. В выпадающем списке выберите **Добавить внутреннюю реакцию на событие контроллера**.
14. В появившемся окне **Добавить внутреннюю реакцию на событие** введите название реакции на событие и установите с помощью соответствующего раскрывающегося списка:
    - для параметра **Контроллер** выберите исполнительное устройство;
    - для параметра **Ресурс** выберите направление;
    - для параметра **Событие** – значение **Запрос на верификацию ВВУ**;
    - для параметра **Действие** – значение **Активизировать выход**;
    - для параметра **Контакт** – значение выхода контроллера, к которому физически подключен вход «Начать анализ» алкотестера «Алкобарьер»;
    - для параметра **Тип реакции** – значение **Время срабатывания**;
    - для параметра **Время** – значение **Бесконечность**.



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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

27. Настройка работы алкотестера «Алкобарьер» для контроля двух направлений прохода ИУ

В системе предусмотрена возможность настройки алкотестера «Алкобарьер», подключенного по сети Ethernet, для проведения верификации в двух направлениях прохода исполнительного устройства, для этого:

1. Убедитесь, что версия встроенного ПО контроллера, к которому подключено ИУ, проход через которое верифицируется алкотестером «Алкобарьер», соответствует требованиям:
   - 1.2.0.35 и выше для контроллеров ***PERCo CL15.x***, ***CT13.1*** и ***CT/L14.1***;
   - 2.2.1.85 и выше для контроллеров ***PERCo CL15***, ***CT13*** и ***CT/L14***.

   При необходимости обновите встроенное ПО контроллера. Актуальные версии встроенного ПО контроллеров доступны на сайте компании ***PERCo*** по ссылке https://www.perco.ru/partneram/programmnoe-obespechenie.php, вкладка **Прошивки оборудования**.
2. Создайте текстовый файл *addport.csv*. Данный файл должен содержать две строки вида:

   {Протокол};{Порт}

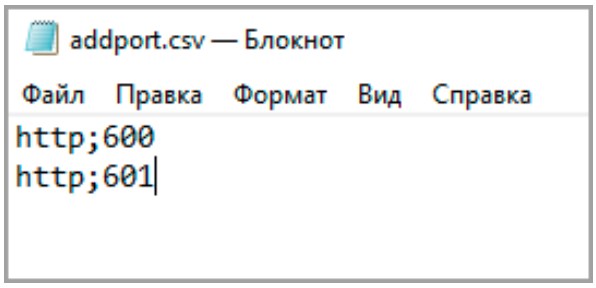
   - **{Протокол}** – протокол, который будет использоваться для установления соединения через указанный порт: **http** или **https**.
   - **{Порт}** – десятичное значение порта.

   Указанные порты в дальнейшем будут использоваться при настройке направлений прохода. Значение **{Порт}** не должно конфликтовать с уже используемыми модулем алкотестера «Алкобарьер» портами:
   - должно отличаться от основного порта, если указан **{Протокол}** отличный от основного протокола. Основные протокол и порт можно посмотреть в Web-интерфейсе алкотестера «Алкобарьер» в разделе **Работа с настройками**, параметры **Порт** и **Протокол**.
   - не должен быть равен 5355 или 137, если в Web-интерфейсе алкотестера «Алкобарьер» в разделе **Работа с настройками** включен параметр **Использовать LLMNR**.
   - не должен быть равен 80, если в Web-интерфейсе алкотестера «Алкобарьер» в разделе **Работа с настройками** включен параметр **Использовать перенаправление** и одновременно в параметре **Протокол** указано значение **https** или в поле **Порт** указано значение, отличное от **80**.
   - не должен быть равен 68, если в Web-интерфейсе алкотестера «Алкобарьер» в разделе **Работа с настройками** включен параметр **Динамический IP**.

   Примечание:

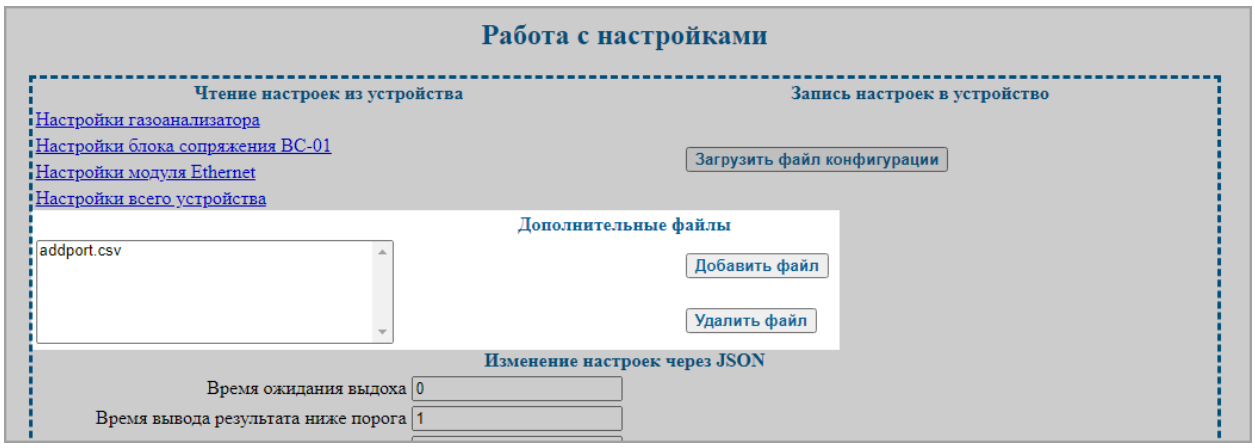
   Для подключения к Web-интерфейсу алкотестера «Алкобарьер» введите в адресную строку браузера IP-адрес алкотестера «Алкобарьер».

   Файл будет иметь следующий вид (значения **{Протокол}** и **{Порт}** могут отличаться):



3. Загрузите созданный файл *addport.csv*, для этого в Web-интерфейсе алкотестера «Алкобарьер» в разделе **Работа с настройками** в подразделе **Дополнительные файлы** нажмите кнопку **Добавить файл**. В открывшемся окне выберите созданный файл *addport.csv*. Файл отобразится в списке дополнительных файлов:

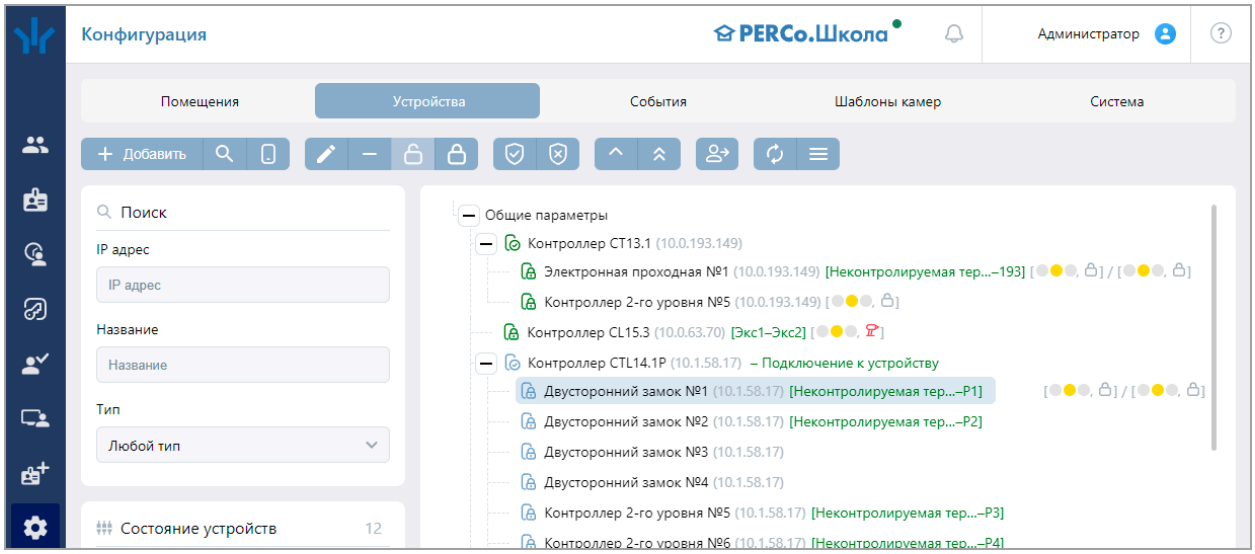
SEC.RU | Короткий путь к информации Скачано с sec.ru



4. Войдите в систему ***PERCo.Школа***.

5. Используя панель навигации, перейдите в подраздел **«Конфигурация»** раздела **«Администрирование»**.

6. В рабочей области страницы выделите исполнительное устройство, проход через которое будет верифицироваться алкотестером «Алкобарьер»:



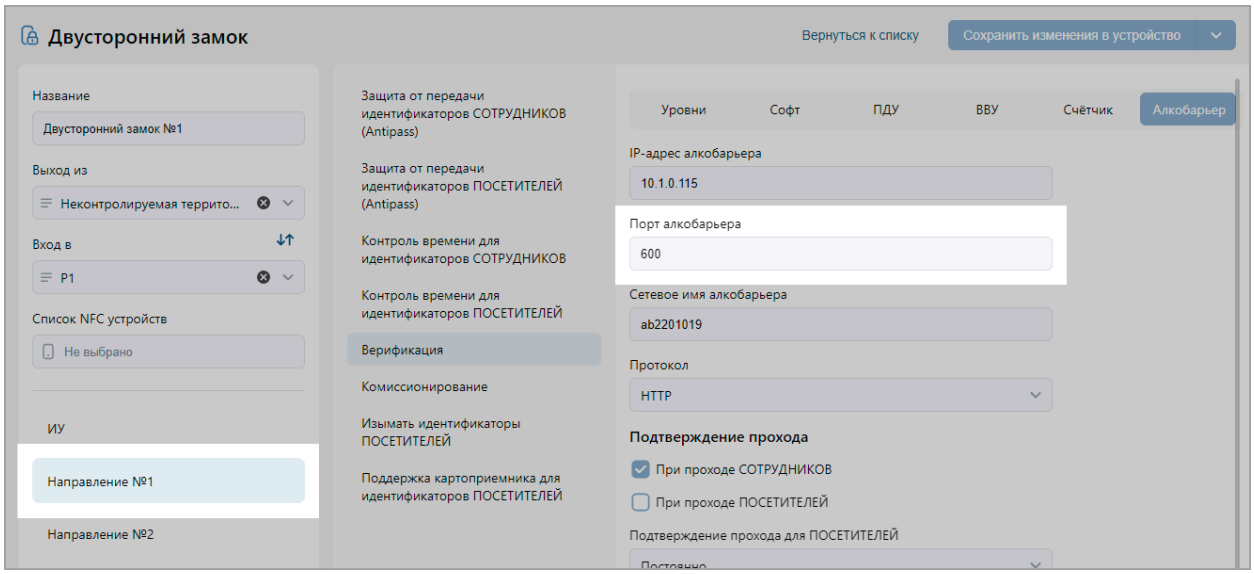
7. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется страница, отражающая название исполнительного устройства.

8. Настройте первое направление прохода для работы алкотестера «Алкобарьер»:

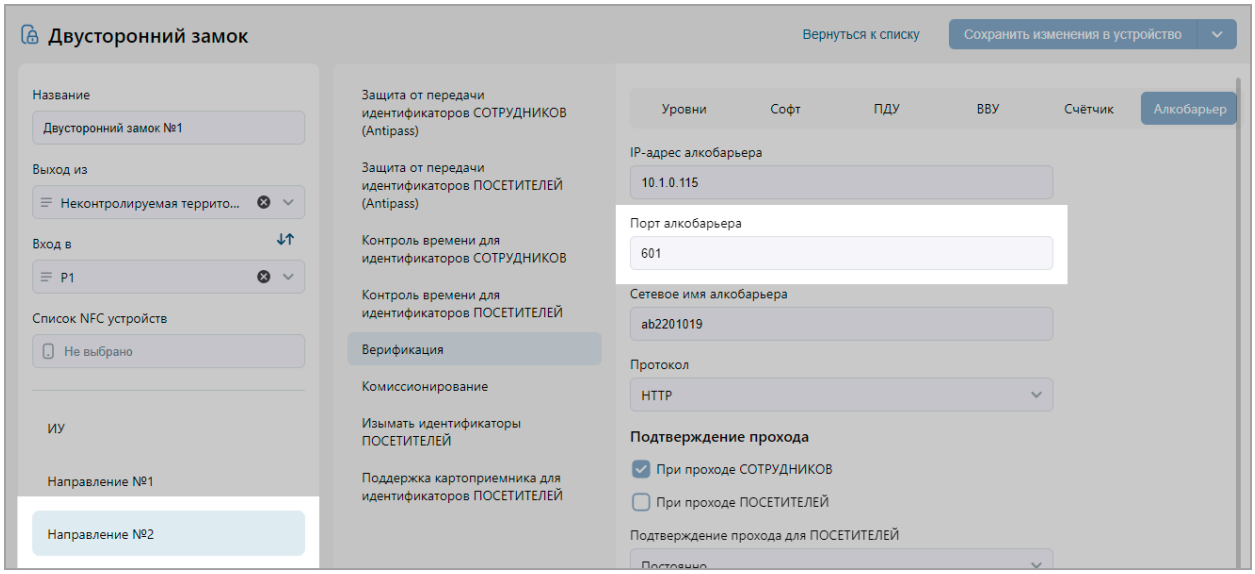
   - В открывшемся окне перейдите на вкладку **Направление 1**. В рабочей области выберите вкладку **Верификация -> Уровни**.
   - В соответствующем уровне верификации выберите для первого направления тип используемой верификации **Алкобарьер** или **Алкобарьер выборочно** (позволяет запускать верификацию с определенной вероятностью):

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Перейдите на вкладку **Алкобарьер**. Заполните данные устройства: **IP-адрес алкобарьера**, **Сетевое имя алкобарьера**, **Протокол** и т.д. В поле **Порт алкобарьера** введите один из портов, указанный раннее в файле *addport.csv*:

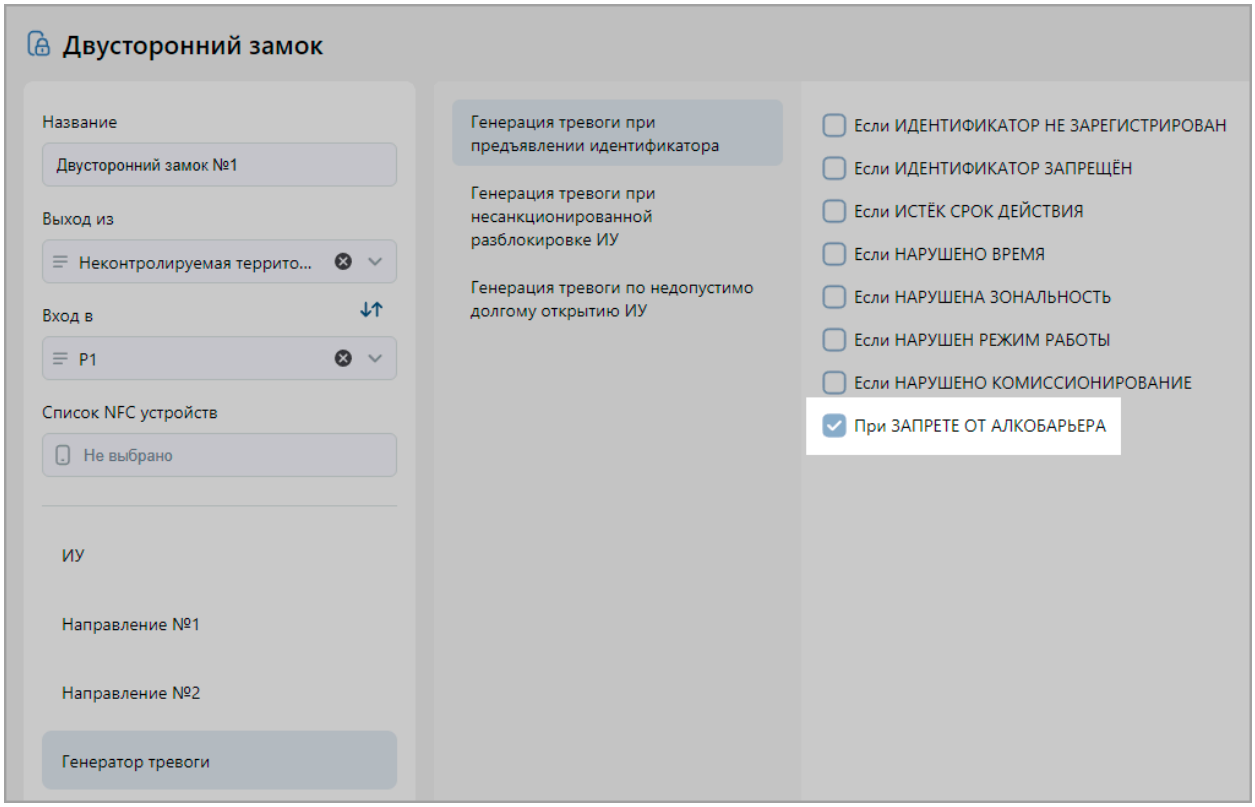


9. Перейдите на вкладку **Направление 2**. Аналогично п. 9 настройте второе направление прохода. В поле **Порт алкобарьера** укажите второй порт из файла *addport.csv*, который еще не был введен:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

10. Перейдите на вкладку **Генератор тревоги -> Генерация тревоги при предъявлении идентификатора**. Поставьте флажок напротив значения **При ЗАПРЕТЕ ОТ АЛКОБАРЬЕРА**:



11. Поочередно нажмите кнопки **Сохранить изменения в устройство** и **Вернуться к списку**. Страница исполнительного устройства будет закрыта, настройки сохранены.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

28. Настройка контроллера СКУД PERCo для работы с алкотестером «Алкорамка | про», интегрированным в систему

Примечание:

Работа алкотестера «Алкорамка | про» возможна только с контроллерами ***CT/L14***, ***CT/L14.1***, ***CL15***, ***CL15.1***, ***CL15.3***, ***CL15.7*** и со встроенными контроллерами ***CT13***, ***CT13.1*** электронных проходных ***PERCo***.

В системе ***PERCo.Школа*** алкотестер «Алкорамка | про» возможно настроить для верификации только в одном направлении прохода исполнительного устройства.

Интеграция алкотестера «Алкорамка | про» осуществляется путем подключения к одной сети с сервером ***PERCo.Школа*** по интерфейсу *Ethernet*. Порядок подключения алкотестера по интерфейсу *Ethernet* см. в руководстве по монтажу алкотестера.

Примечание:

Для обеспечения корректной работы рекомендуется подключать алкотестер и контроллер, между которыми происходит обмен данными, к одному коммутатору.

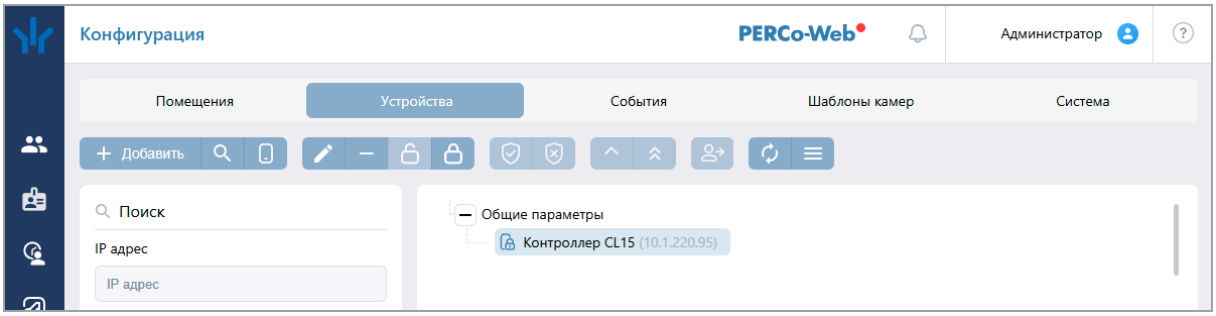
После монтажа и включения алкотестера «Алкорамка | про» необходимо произвести его конфигурирование в системе, для этого:

1. В Web-интерфейсе алкотестера «Алкобарьер | про» в разделе **«Основные настройки»** настройте следующие параметры:
   - для параметра **Режим** с помощью раскрывающегося списка укажите **Дистанционный**.
   - для параметра **Ожидание выдоха, мс** рекомендуется установить значение 15 000 миллисекунд.

Примечание:

Для подключения к Web-интерфейсу алкотестера введите его IP-адрес в адресной строке браузера. Для входа используйте логин **admin**, пароль **alkotest20**.

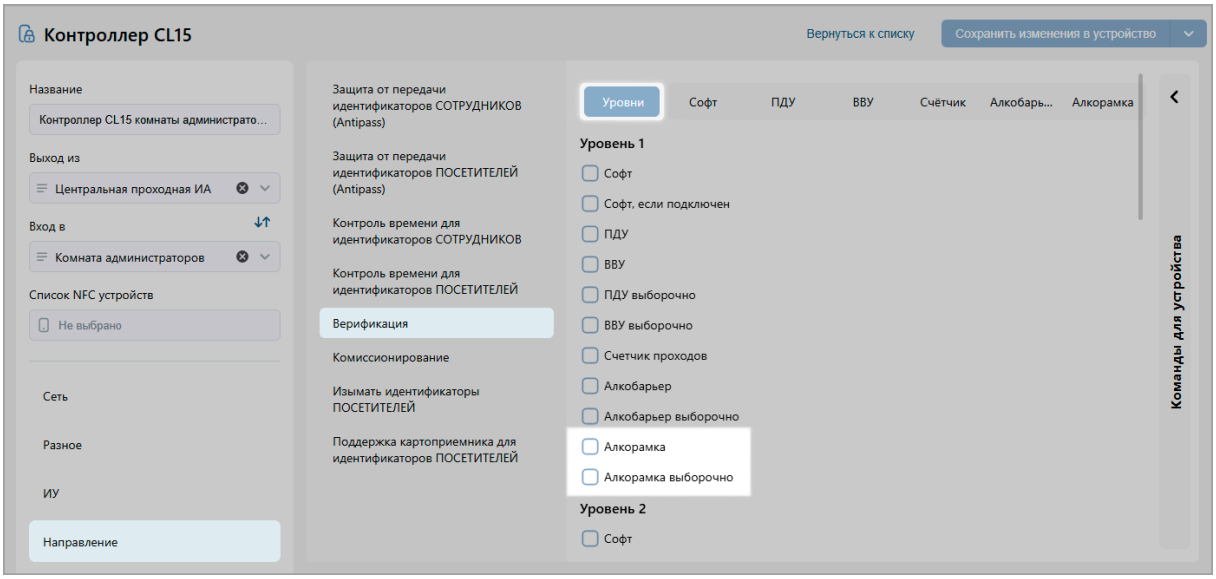
2. В системе ***PERCo.Школа***, используя панель навигации, перейдите в подраздел **«Конфигурация»** раздела **«Администрирование»**.
3. В рабочей области страницы выделите контроллер или исполнительное устройство, выбранное для работы с алкотестером «Алкорамка | про»:



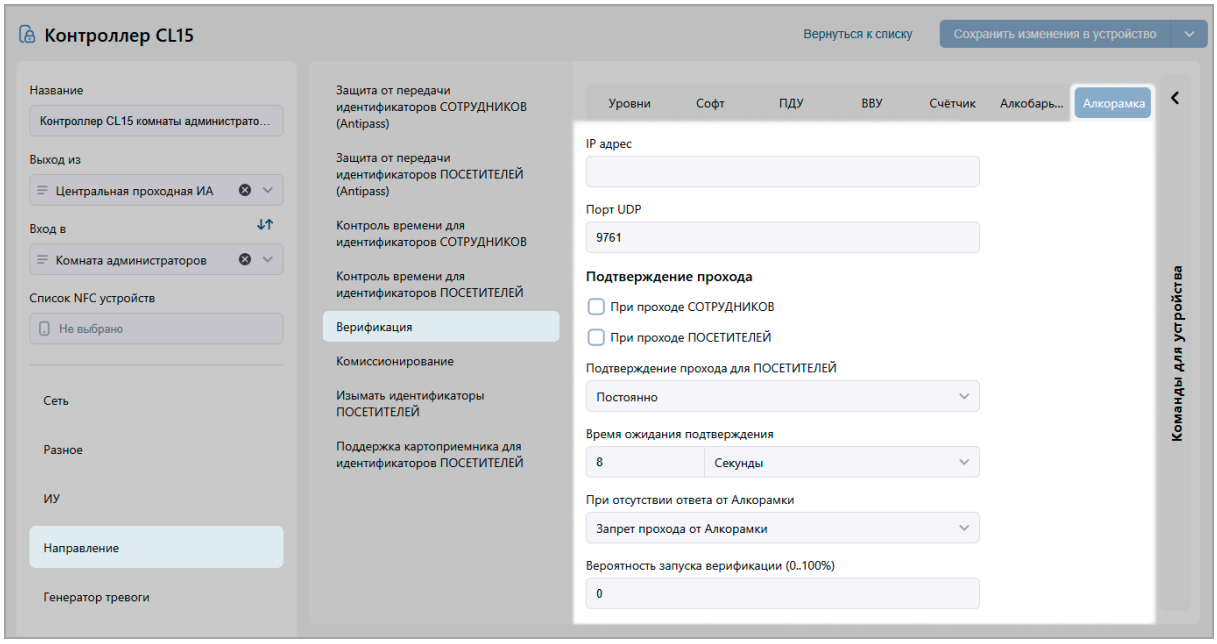
4. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется страница, отражающая название контроллера или исполнительного устройства.

SEC.RU | Короткий путь к информации Скачано с sec.ru

5. В открывшемся окне перейдите на вкладку **Направление**. В рабочей области выберите вкладку **Верификация -> Уровни**. В соответствующем уровне верификации выберите тип используемой верификации **Алкорамка** или **Алкорамка выборочно** (позволяет запускать верификацию с определенной вероятностью):



6. Перейдите на вкладку **Алкорамка**:

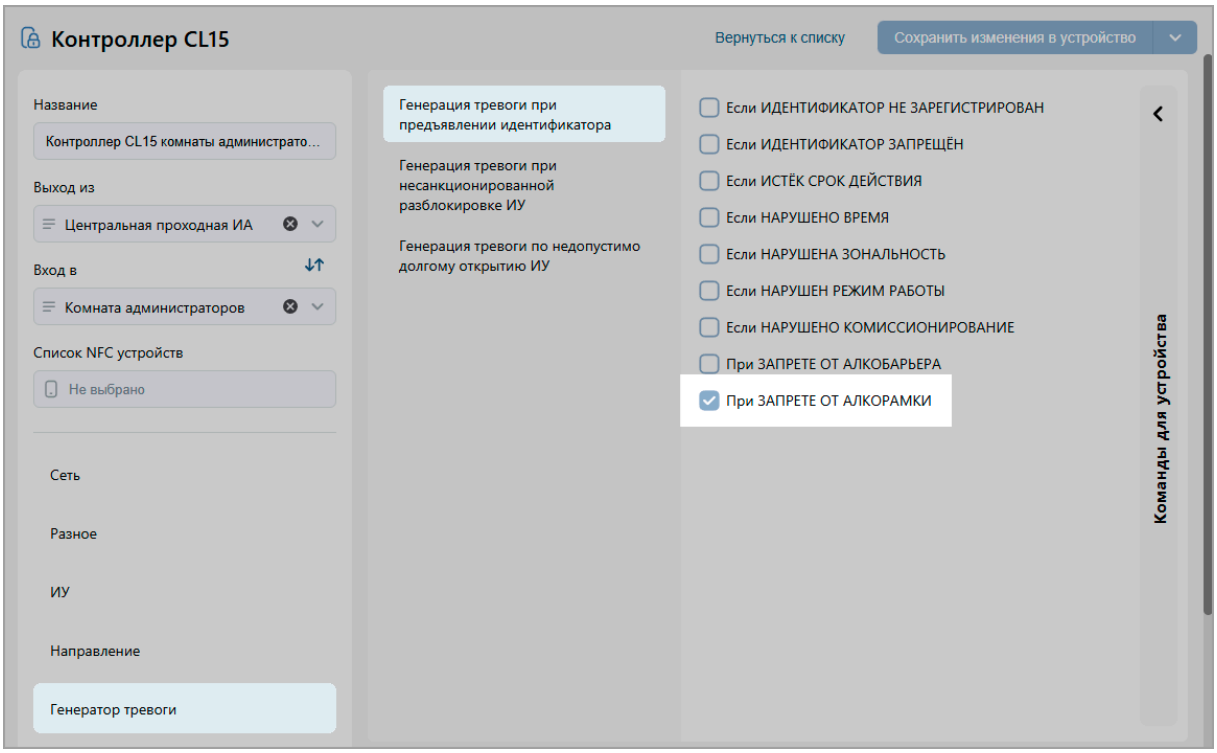


Заполните параметры для настройки устройства:

- **IP-адрес** – IP-адрес алкотестера «Алкорамка|про» отображается на экране устройства при включении.
- **Порт UDP** – порт UDP указан в интерфейсе алкотестера «Алкорамка|про», параметр **UDP-порт приема команд** в разделе **«Сеть»**. По умолчанию установлен порт 9761.
- С помощью флажков **При проходе СОТРУДНИКОВ** и **При проходе ПОСЕТИТЕЛЕЙ** укажите, для кого требуется запускать проверку.
- В поле **Время ожидания подтверждения** рекомендуется установить значение, превышающее минимум на 5 секунд значение параметра **Ожидание выдоха, мс** в разделе «Основные настройки» в Web-интерфейсе алкотестера «Алкорамка|про». Обратите внимание, что в ***PERCo.Школа*** указывается значение в секундах, а в Web-интерфейсе алкотестера в миллисекундах.
- Если тип используемой верификации **Алкорамка выборочно**, установите значение параметра **Вероятность запуска верификации (0..100%)**, отличное от 0 и 100.
- При необходимости настройте прочие параметры вкладки **Алкорамка**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7. Перейдите на вкладку **Генератор тревоги -> Генерация тревоги при предъявлении идентификатора**. Поставьте флажок напротив значения **При ЗАПРЕТЕ ОТ АЛКОРАМКИ**:



8. Нажмите поочередно кнопки **Сохранить изменения в устройство** и **Вернуться к списку**. Страница контроллера или исполнительного устройства будет закрыта, настройки сохранены.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

29. Команды управления устройствами

Примечание:

Команды управления видеокамерами ***TRASSIR*** и оборудованием ИСО ***«Орион»*** описываются в руководствах пользователя на соответствующие модули.

Генератор тревоги

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

Турникет, шлагбаум

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

Замок

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

Дополнительный выход

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

Примечание:

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

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

Считыватель

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

30. Термины и определения

Antipass – функция системы безопасности, заключающаяся в контроле повторного прохождения (регистрации) через одно КПП в том же направлении. Для контроллеров ***PERCo CT/L14***, ***CT/L14.1***, ***CT13***, ***CT13.1***, ***CL15***, ***CL15.1***, ***CL15.3***, ***CL15.7***, ***CR02.9***, ***CR11***, ***CR11.1***, ***CL211.3***, ***CL211.9*** отслеживается повторное прохождение одного и того же пользователя, вне зависимости от предъявленной из закрепленных за ним карты доступа / идентификатора. Для контроллеров ***PERCo CT03.2***, ***CT/L04.2***, ***CR01.2***, ***CR01.9*** отслеживается повторное предъявление одной и той же карты доступа / идентификатора, вне зависимости от закрепленного за ней пользователя.

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

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

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

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

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

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

Идентификатор – некоторое устройство или признак, по которому определяется пользователь. Каждый идентификатор характеризуется определенным уникальным кодом. В качестве идентификатора в системе используются бесконтактные карты форматов *EM-Marin*, *HID* и *Mifare*, а также биометрические идентификаторы (отпечатки пальцев, шаблоны ладони, шаблоны лица).

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

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

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

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

Обновление встроенного ПО – для обновления встроенного ПО и форматирования памяти

SEC.RU | Короткий путь к информации Скачано с sec.ru

контроллеров системы используется программа *«Прошиватель»*. Программа вместе с файлами прошивок входит в состав *«Внутреннее ПО ("прошивка") контроллеров PERCo»*. Актуальную версию программы можно загрузить с сайта компании www.perco.ru.

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

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

Распределенная система (режим мультисервера) – режим работы системы ***PERCo Web.Школа***, при котором сеть организации разделена на сегменты, работающие с централизованной базой данных, для повышения отказоустойчивости работы системы.

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

Сегмент – в качестве сегмента в распределенной системе ***PERCo.Школа*** может выступать группа контроллеров, отделение организации и пр. Деление на сегменты рекомендуется для снижения нагрузки на систему при использовании большого количества контроллеров.

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.

Цикл обучения – учебный год, делится на более мелкие периоды: 4 четверти, 3 триместра или 2 семестра.

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

Приложение 1. Примеры построения работы системы распределенных серверов

1. Настройка распределенной системы репликации баз данных с использованием сторонней утилиты на базе ПО SymmetricDS

1. На одном из серверов ***PERCo.Школа*** создайте базу данных.
2. Откройте вкладку **Резервные копии и логи** ***Менеджера PERCo-Web***, создайте и сохраните резервную копию созданной БД.
3. Откройте вкладку **Опасная зона** в ***Менеджере PERCo-Web*** и скачайте секретный ключ.

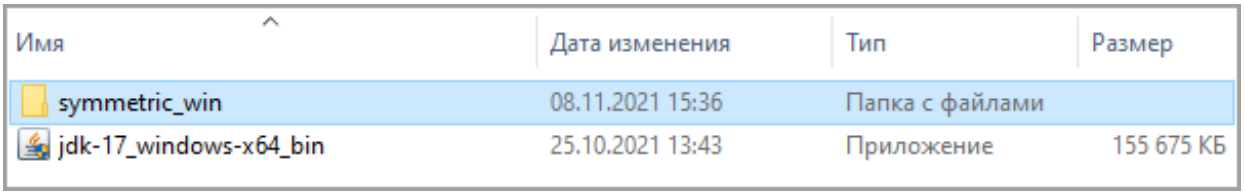


4. Секретный ключ необходимо распространить на все остальные сервера. Обратите внимание, что на всех серверах ***PERCo.Школа*** должен быть загружен один и тот же секретный ключ.
5. Для корректной работы ПО ***SymmetricDS*** установите на все сервера (сегменты) *Java SE Development Kit (Open JDK).* Утилиту можно скачать с официального сайта: https://www.oracle.com/java/technologies/downloads/#jdk17
6. Настройте утилиту для ПО ***SymmetricDS***.

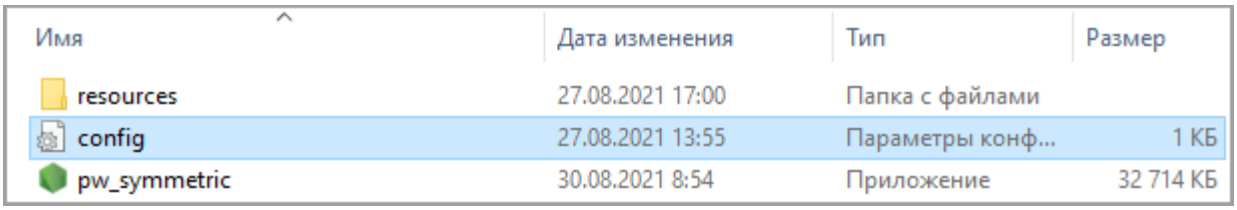
   Для упрощения работы с ПО ***SymmetricDS*** воспользуйтесь специальной утилитой, доступной по ссылке: https://github.com/percodev/symmetric-simple-config/releases. Выберите архив под операционную систему, на которой установлен ***PERCo.Школа***: *symmetric_win.zip* для ОС *Windows, symmetric_linux.zip* для ОС *Linux*.

   Последовательность установки утилиты:

   1) Распакуйте архив и откройте папку symmetric.



   2) Для корректной синхронизации баз данных в файле *config* требуется правильно описать настройки всех серверов.



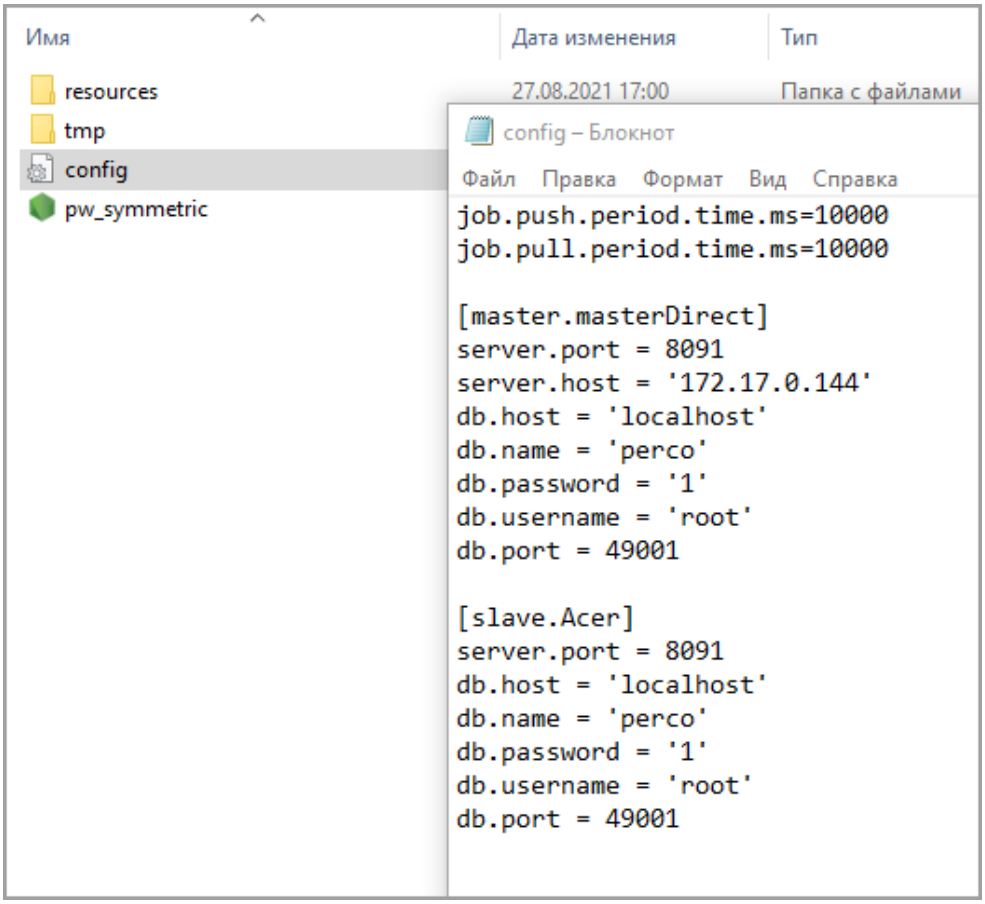
   3) Настройки включают следующие параметры:
      - Длительность отправки и получения данных (рекомендовано установить 10000 мс).
      - Наименование сервера *Master*. Наименование должно быть указано на латинице в формате [master.masterServerName]. Наличие ключевого слова *master* до точки обязательно. Каждое наименование должно быть уникальным.
      - Наименования серверов *Slave*. Наименование должно быть указано на латинице в формате [slave.servername]. Наличие ключевого слова *slave* до точки обязательно. Каждое наименование должно быть уникальным.
      - Порты сервера *Master* и серверов *Slave* (выбранные порты должны быть свободны)

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Внешний IP-адрес или доменное имя (сервер должен быть доступен остальным сегментам сети);
- Название БД;
- Пароль пользователя БД;
- Имя пользователя БД;
- Порт БД. Стандартный порт *MySQL* – 3306. При использовании *MySQL*, который поставляется в *Windows*-версии ***PERCo.Школа***, стандартный порт – 49001.

Примечание:

Помимо настроек сервера *Master*, в файле *config* также необходимо описать параметры всех сегментов *Slave*. Учтите, что количество сегментов должно соответствовать количеству серверов системы ***PERCo.Школа***.

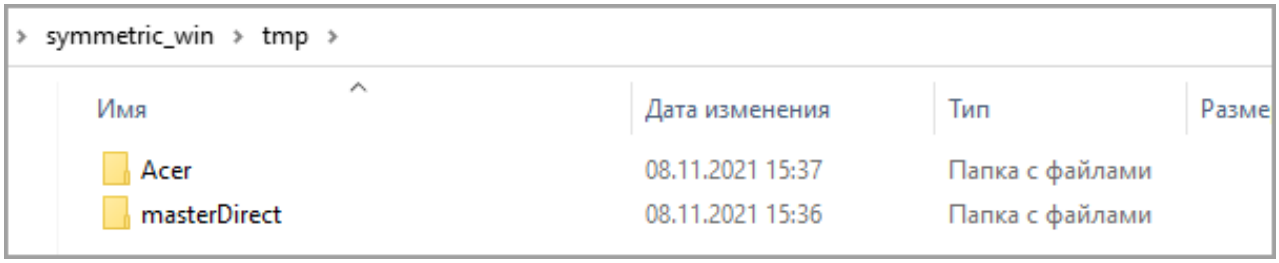


4) По завершении редактирования сохраните изменения и закройте файл *config*.
5) Запустите утилиту генерации настроек ***SymmetricDS***: *pw_symmetric.exe* для ОС *Windows*, *sudo ./pw_symmetric* для ОС *Linux*.

Внимание!

Утилиту генерации настроек ***SymmetricDS*** необходимо запускать от имени администратора.

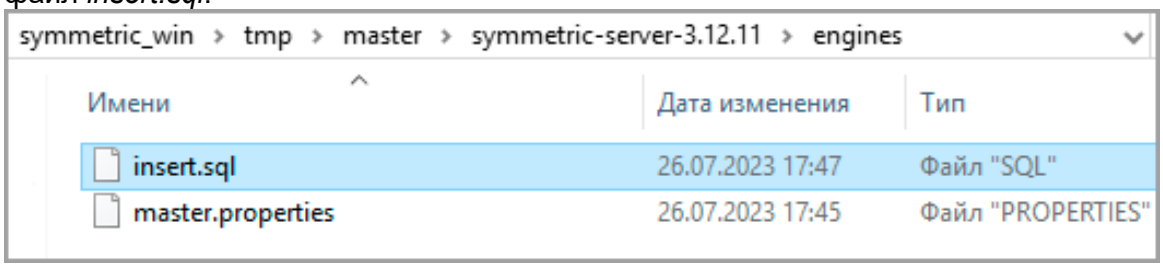
6) Результатом работы утилиты является папка tmp. Внутри tmp находятся папки, названия которых соответствуют указанным в файле *config* наименованиям серверов.



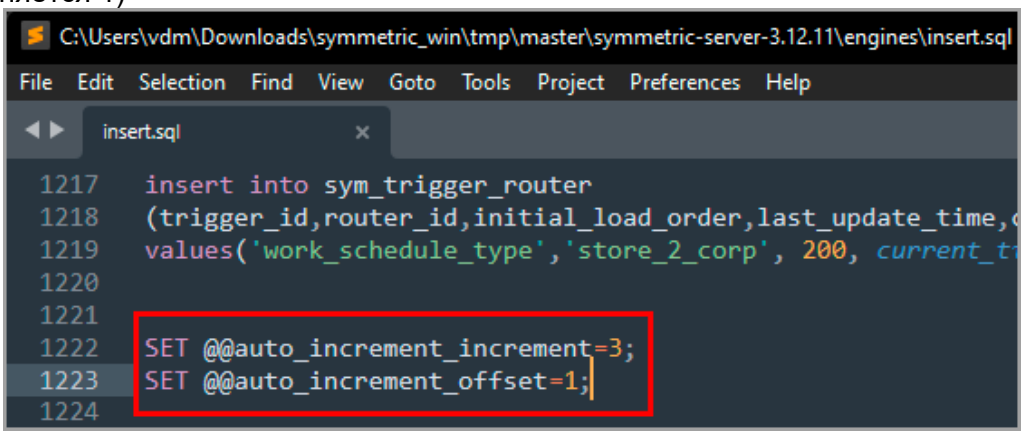
7) Папку сервера *Master* необходимо оставить на текущем (основном) сервере, а папки серверов *Slave* скопировать на каждый сегмент (сервер).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

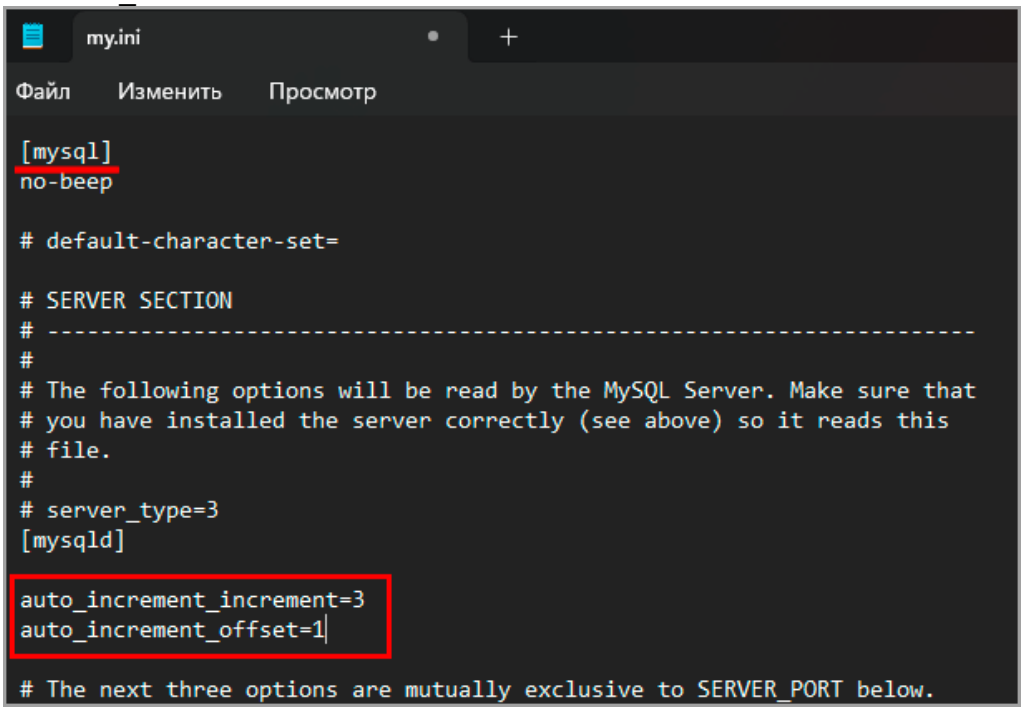
8) Настройте автоинкремент для каждого сегмента (сервера) в *MySQL*, для этого перейдите в папку symmetric соответствующего сегмента и в папке engines откройте файл *insert.sql*:



9) В открытом файле скопируйте следующие строки (цифры могут отличаться в зависимости от количества сегментов):
   - SET @@auto_increment_increment=3; (общее число сегментов, в данном случае равняется 3)
   - SET @@auto_increment_offset=1; (порядковый номер сегмента, в данном случае равняется 1)



10) Откройте файл конфигурации *MySQL* в папке с установленными файлами ***PERCo.Школа*** (по умолчанию это *C:\Program Files\PERCo\PERCo-Web School\mysql\my.ini*).
11) В открытом файле в блоке [mysql] вставьте скопированные строки, удалив в начале «SET @@» и в конце точку с запятой «;». Для данного примера строки примут следующий вид:
auto_increment_increment=3
auto_increment_offset=1



SEC.RU | Короткий путь к информации Скачано с sec.ru

12) Сохраните файл и перезапустите службу *MySQL*.
13) Повторите п. 8-12 для каждого сегмента (сервера).

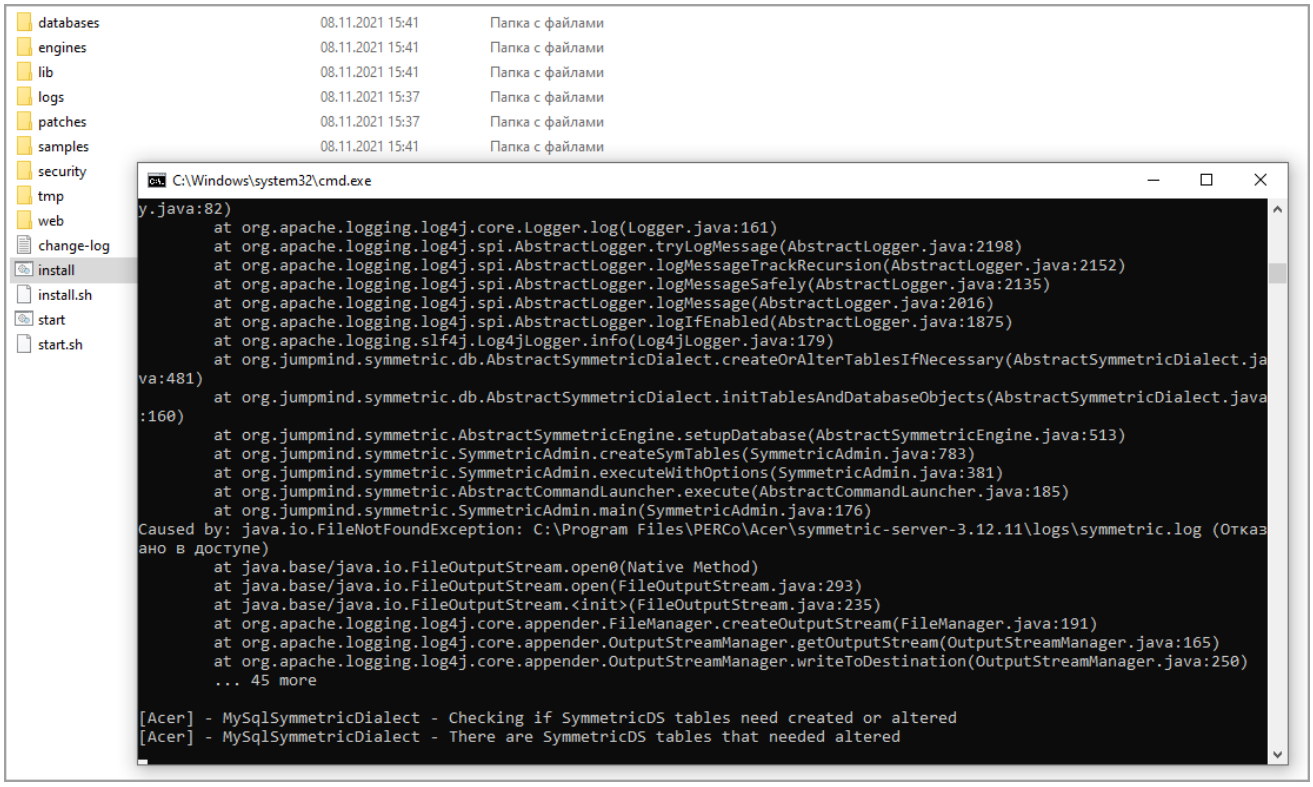
7. Установите ПО ***SymmetricDS***:
   1) Перейдите в папку symmetric-server-3.12.11 на сервере *Master* и запустите требуемый файл: *install* для ОС *Windows*, *sudo bash ./install.sh* для ОС *Linux*.

Внимание!

Запуск файла должен производиться под правами администратора.

Примечание:

Запуск файла можно произвести с помощью инструментов Windows PowerShell. Для этого в командой строке Windows PowerShell введите .\instal.bat.



2) Произведите аналогичный набор действий с файлом *install* на каждом сервере.
3) По завершении установки рабочее окно командной строки автоматически закроется.

8. Запустите ПО ***SymmetricDS***:
   1) Перейдите в папку symmetric-server-3.12.11 на сервере Master и запустите требуемый файл: *start* для ОС *Windows*, *sudo bash ./start.sh* для ОС *Linux*.

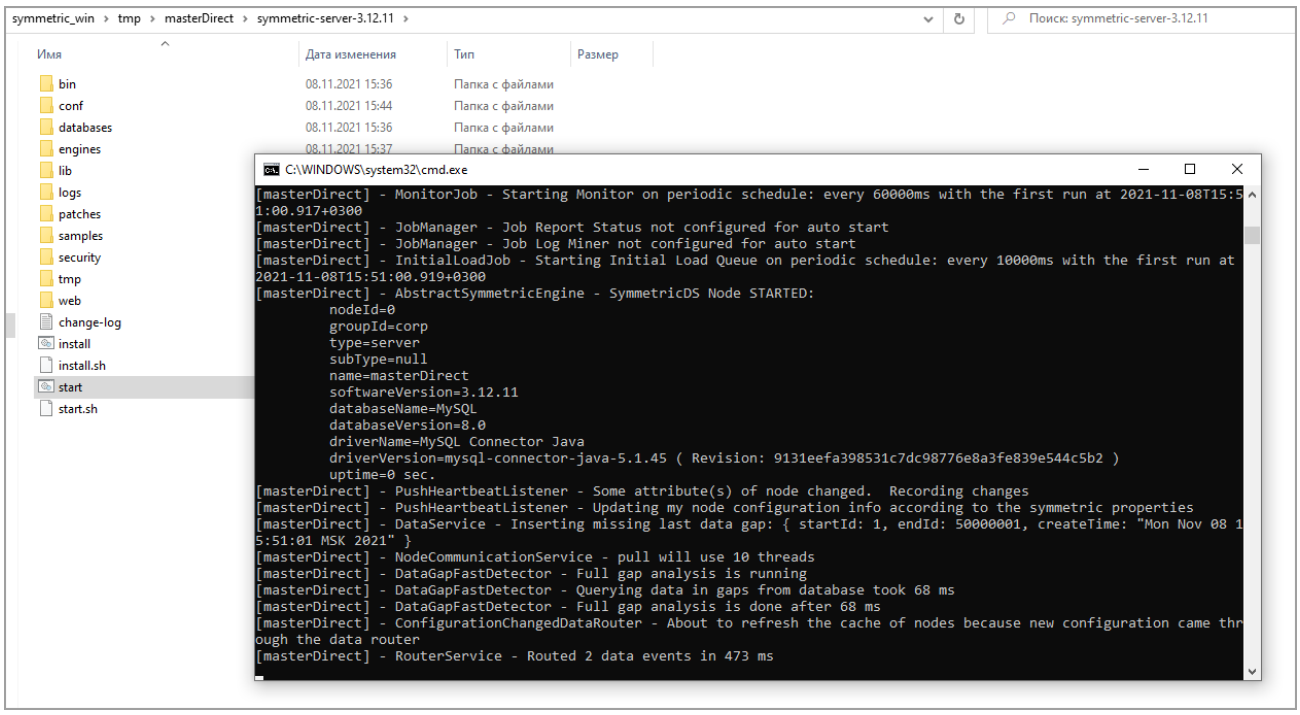
Внимание!

Запуск файла должен производиться под правами администратора.

Примечание:

Запуск файла можно произвести с помощью инструментов Windows PowerShell. Для этого в командой строке Windows PowerShell введите .\start.bat.

SEC.RU | Короткий путь к информации Скачано с sec.ru



2) Аналогичный набор действий с файлом *start* необходимо произвести на каждом сервере *Slave*.

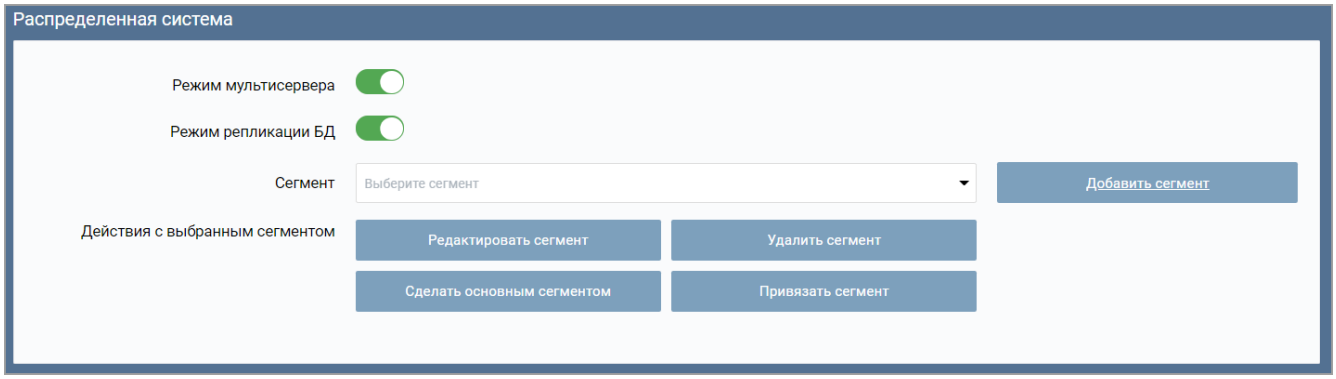
   Рекомендуемая последовательность действий:
   - Запустите сервер *Master*;
   - Ожидайте завершения запуска;
   - Запустите сервера *Slave*. Рекомендуется запускать сервера по очереди;
   - Ожидайте завершения запуска и установления связи с сервером *Master*.

3) При корректной работе режима репликации БД в окне будет отображаться длительность обмена данными.
4) Для настройки сегментов и корректной работы режима репликации БД рабочие окна файла *start* на серверах *Master* и *Slave* должны быть запущены всегда.

Примечание:

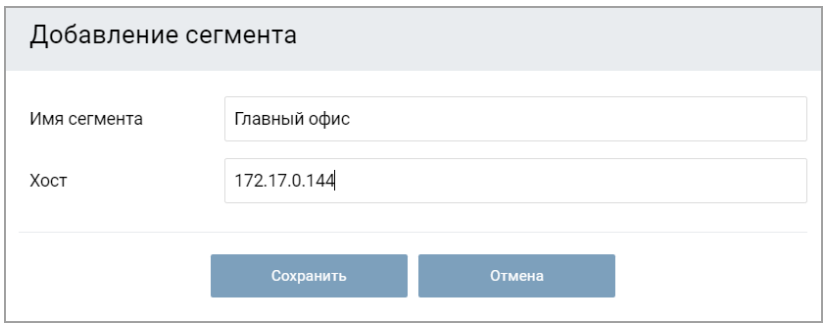
В случае закрытия одного из файлов *start* синхронизация данных будет потеряна.

9. Создайте сегменты в менеджере ***PERCo-Web***:
   1) Откройте ***Менеджер PERCo-Web*** и перейдите на вкладку **Настройки**. На панели **Распределенная система** активируйте режимы мультисервера и репликации БД.



   2) С помощью кнопки **Добавить сегмент** вызовите окно **Добавление сегмента**. Создайте сегменты для серверов *Master* и *Slave*.

SEC.RU | Короткий путь к информации
Скачано с sec.ru



3) Выберите сегмент сервера *Master* основным с помощью кнопки **Сделать основным сегментом**.

Примечание:

После выбора основного сегмента необходимо перезапустить **Сервер системы** и **Web-сервер**.

Закрепление выбранного сегмента за сервером должно происходить на том же сервере, который необходимо привязать.

4) В случае нарушения работы одного из сегментов, другие сегменты продолжат функционировать.

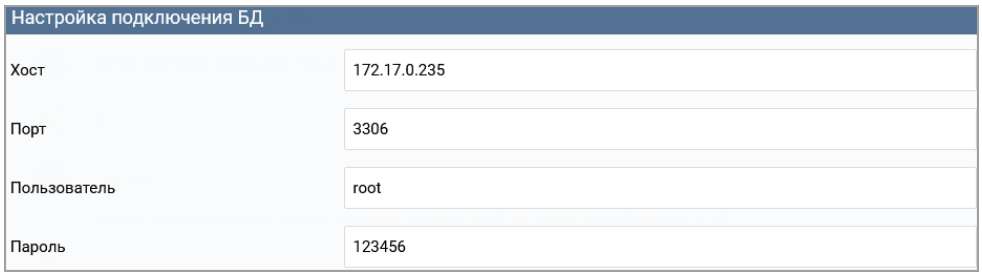
SEC.RU | Короткий путь к информации
Скачано с sec.ru

2. Настройка распределённой системы с использованием общей базы данных

1. На одном из серверов ***PERCo.Школа*** создайте базу данных.
2. Откройте вкладку **Опасная зона *Менеджера PERCo-Web*** и скачайте секретный ключ.



3. Распространите сохраненный секретный ключ на все остальные сегменты. В итоге на всех серверах должен быть загружен один и тот же секретный ключ.
4. Подключитесь к созданной БД с остальных сегментов, указав хост, порт, имя пользователя, пароль и название БД на вкладке **Настройки *Менеджера PERCo-Web***.

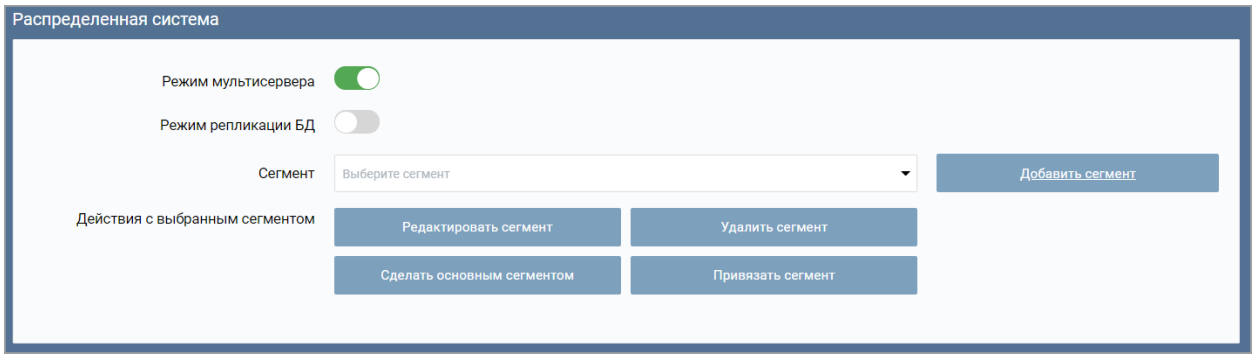


Обратите внимание, что для корректной работы данного режима на всех серверах ***PERCo.Школа*** должны быть установлены одинаковые настройки подключения БД.

Примечание:

Пользователь *MySQL* должен обладать правами подключения к БД со всех хостов, где установлены сервера ***PERCo.Школа***.

5. Откройте ***Менеджер PERCo-Web*** и перейдите на вкладку **Настройки**. На панели **Распределенная система** активируйте режим мультисервера.



6. С помощью кнопки **Добавить сегмент** вызовите окно **Добавление сегмента**. Создайте сегменты для серверов *Master* и *Slave*.
7. Выберите сегмент сервера *Master* основным с помощью кнопки Сделать основным сегментом.

Примечание:

После выбора основного сегмента необходимо перезапустить **Сервер системы** и **Web-сервер**. Закрепление выбранного сегмента за сервером должно происходить на том же сервере, который необходимо привязать.

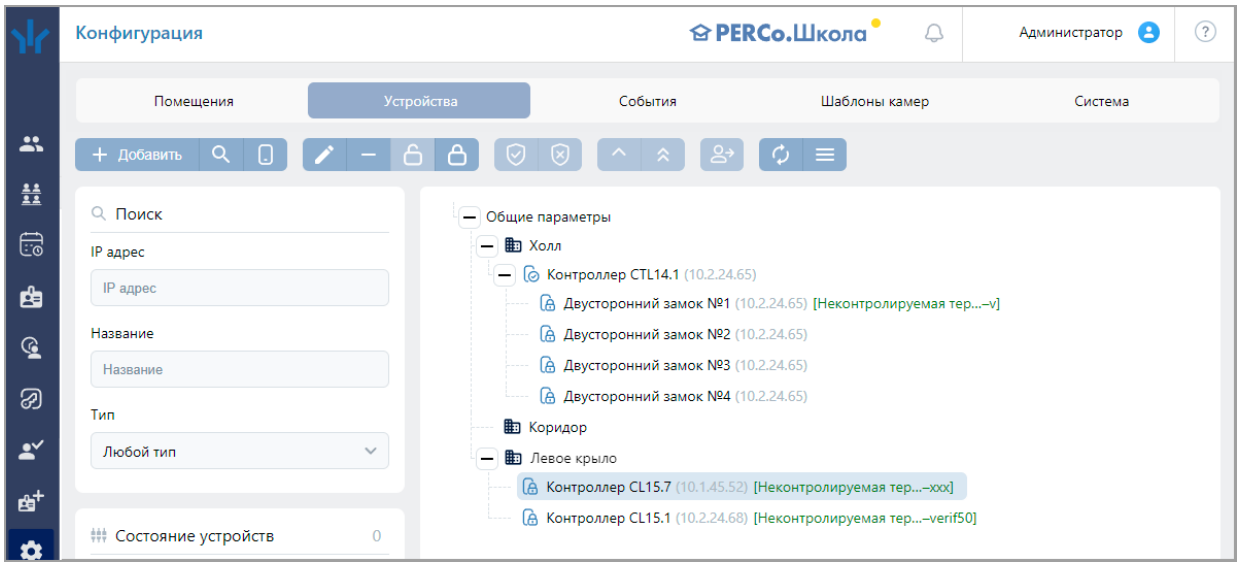
SEC.RU | Короткий путь к информации Скачано с sec.ru

Приложение 2. Реализация многоуровневой верификации

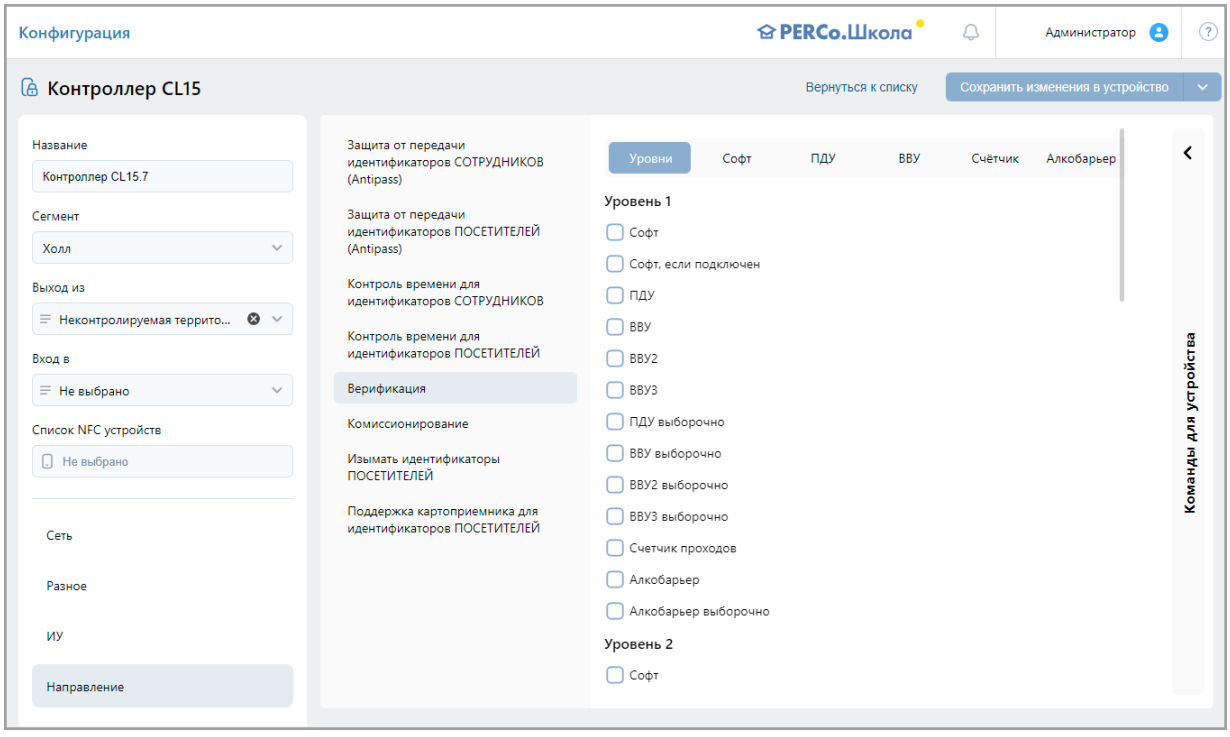
В системе предусмотрена возможность многоуровневой верификации сотрудников, учеников, родственников учеников и посетителей. Разрешение на проход будет выдано только после последовательного подтверждения пользователем прав доступа на каждом уровне. Уровень верификации определяет очередность запуска типа верификации. Возможно выбрать от 1 до 4 уровней верификации.

Для того, чтобы задать многоуровневую верификацию:

1. Используя панель навигации, перейдите в подраздел **«Конфигурация»** раздела **«Администрирование»**.
2. В рабочей области страницы выделите контроллер или исполнительное устройство, для которого будет производится конфигурирование многоуровневой верификации:

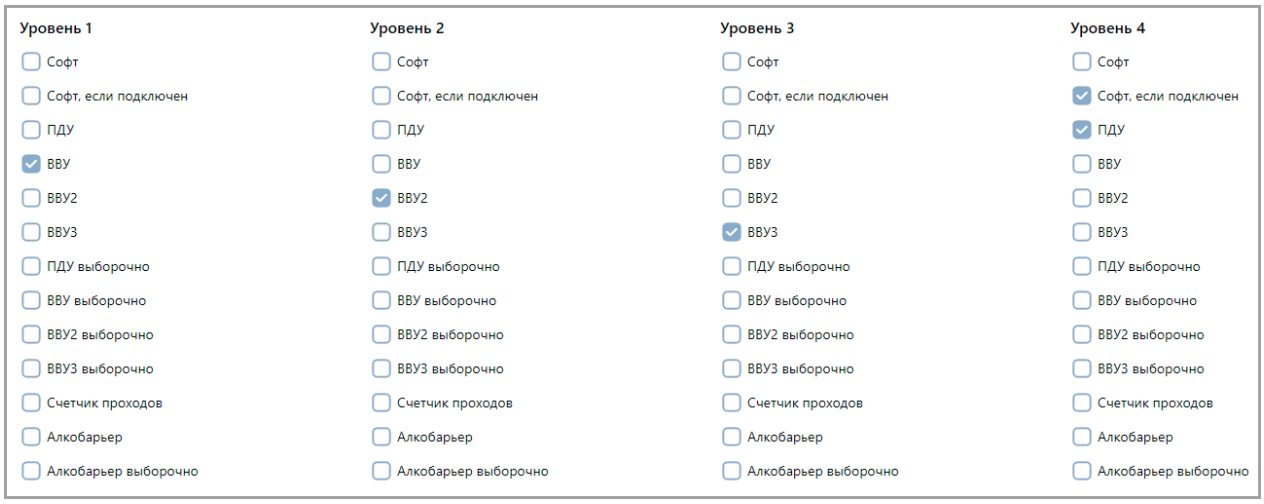


3. Нажмите кнопку  **Редактировать** на панели инструментов страницы. Откроется страница, отражающая название контроллера или исполнительного устройства.
4. В открывшемся окне перейдите на вкладку **Направление**. В рабочей области выберите вкладку **Верификация -> Уровни**:



SEC.RU | Короткий путь к информации
Скачано с sec.ru

5. Выберите типы верификации для соответствующих уровней. Пример параметров для многоуровневой верификации:



Выбраны следующие параметры:

- **Уровень 1** – **ВВУ**;
- **Уровень 2** – **ВВУ2**;
- **Уровень 3** – **ВВУ3**;
- **Уровень 4** – **Софт, если подключен** и **ПДУ**.

6. Нажмите поочередно кнопки **Сохранить изменения в устройство** и **Вернуться к списку**. Страница контроллера или исполнительного устройства будет закрыта, настройки сохранены.

Теперь при проходе сотрудника, ученика, родственника ученика или посетителя будет запускаться верификация в следующем порядке:

- **Уровень 1 – ВВУ**;
- **Уровень 2** – **ВВУ2**;
- **Уровень 3** – **ВВУ3**;
- **Уровень 4** – на выбор либо верификация через **Софт, если подключен**, либо **ПДУ**. Для успешной верификации будет достаточно разрешения от одного из типа верификации одного уровня.

Примечание:

Для алкотестера «Алкобарьер», интегрированного в систему, предусмотрены отдельные типы верификации: **Алкобарьер** и **Алкобарьер выборочно**. Для других моделей алкотестеров используйте тип верификации **ВВУ**, **ВВУ2** или **ВВУ3**.

SEC.RU | Короткий путь к информации Скачано с sec.ru

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 - системы контроля доступа

turniket@perco.ru - турникеты и ограждения

locks@perco.ru - электромеханические замки

barrier@perco.ru - шлагбаумы, система паркинга

www.perco.ru

Кор. 13.11.2025

SEC.RU | Короткий путь к информации
Скачано с sec.ru

www.perco.ru

SEC.RU | Короткий путь к информации
Скачано с sec.ru