Управляемый USB over IP концентратор DistKontrolUSB

(Устройство подключения USB по сети)

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Версия 6.3.1

Москва
2026 г

Управляемый USB over IP концентратор DistKontrolUSB

(Устройство подключения USB по сети)
РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Информация
Скачать документацию в формате pdf можно по ссылке

Оглавление

1 Общая информация
- 1.1 Назначение прибора
- 1.2 Модельный ряд управляемых USB over IP концентраторов
- 1.3 Область применения управляемых USB over IP концентраторов
  - 1.3.1 Основные функции
  - 1.3.2 Исполнение и интерфейсы
  - 1.3.3 Преимущества использования
  - 1.3.4 Применение в бизнесе
  - 1.3.5 Идеальное решение для совместного использования USB устройств
  - 1.3.6 Гибкость и безопасность
  - 1.3.7 Совместимость
- 1.4 Комплект поставки управляемого USB over IP концентратора
- 1.5 Устройство и работа управляемого USB over IP концентратора
  - 1.5.1 Габаритные размеры (в 19” стойку)
  - 1.5.2 Устройство прибора
  - 1.5.5 Эксплуатационные ограничения и рекомендации
  - 1.5.6 Меры безопасности
  - 1.5.7 Подготовка к работе
  - 1.5.8 Работа управляемого USB over IP концентратора
- 1.6 Пломбирование
- 1.7 Упаковка

2 Технические характеристики концентраторов
- 2.1 Защита и управление USB портами
- 2.2 Технические характеристики концентратора DistKontrolUSB4 3.0
- 2.3 Технические характеристики концентратора DistKontrolUSB8 3.0
- 2.4 Технические характеристики концентратора DistKontrolUSB16 2.0
- 2.5 Технические характеристики концентратора DistKontrolUSB16 3.0
- 2.6 Технические характеристики концентратора DistKontrolUSB24 3.0
- 2.7 Технические характеристики концентратора DistKontrolUSB32 2.0
- 2.8 Технические характеристики концентратора DistKontrolUSB32 3.0

- 2.9 Технические характеристики концентратора DistKontrolUSB48
- 2.10 Технические характеристики концентратора DistKontrolUSB64

3 Техническое обслуживание

- 3.1 Общие положения
- 3.2 Проверка работоспособности

4 Консервация и хранение

- 4.1 Консервация
- 4.2 Хранение, транспортировка и утилизация

5 Web интерфейс управления DistKontrolUSB

- **5.1 Вход в Web интерфейс и начальный экран**
- **5.2 Система**
  - 5.2.1 Общие настройки
  - 5.2.2 Дата и время
  - 5.2.3 Сеть
  - 5.2.4 Сертификаты
  - 5.2.5 Плагины
- **5.3 USB**
  - 5.3.1 USB-порты
  - 5.3.2 Типы USB-устройств
- **5.4 Управление правами доступа**
  - 5.4.1 Пользователь
  - 5.4.2 IP адрес
  - 5.4.3 Группы
- **5.5 Сервисы**
  - 5.5.1 SSH
- **5.6 Диагностика**
  - 5.6.1 Доска
  - 5.6.2 Системная информация
  - 5.6.3 Системный журнал
  - 5.6.3.1 Журналы
  - 5.6.3.2 Настройки
  - 5.6.3.3 Сообщения системы авторизации
  - 5.6.3.4 Сообщения системы управления питанием
  - 5.6.3.5 Сообщения о некорректной работе USB
  - 5.6.3.6 Прочие сообщения
- **5.7 Информация**
  - 5.7.1 Управление версиями ПО
  - 5.7.1.1 Сброс и восстановление

        - 5.7.1.2 Проверить обновление
        - 5.7.1.3 Поддержка
        - 5.7.1.4 Патч
    - **5.8 Сброс настроек в исходное состояние**
    - **5.9 Обновление ПО**
        - 5.9.1 Установленные ПО
    - **5.10 Сохранение и восстановление настроек**
    - **5.11 Аппаратная перезагрузка**

6 Вариант использования, управляемого USB over IP концентратора

Внимание!

1 **Актуальность документации**

- Работа над ПО и аппаратной частью ведется непрерывно. Возможны расхождения между описанием и текущим функционалом.
- Некоторые опции могут отсутствовать в вашей модели устройства.

2 **Совместимость**

- Устройство поддерживает большинство распространенных USB-устройств, но не гарантирует подключение всех типов.

3 **Рекомендации по использованию**:

- Перед эксплуатацией изучите руководство.
- Соблюдайте правила техники безопасности при работе с электроустановками.

4 **Актуальность версии**

- Руководство соответствует версии **6.1.8**.
- Для предыдущих версий см. документацию на устройстве или историю версий.

5 **Плагины**

- Часть разделов WEB-интерфейса не относящихся к осносному функционалу USBoverIP предоставляется плагинами. См. Плагины DistKontrol.

1 Общая информация

Управляемый USB over IP концентратор (далее — концентратор) относится к серии оборудования **DistKontrolUSB**, разработанной для обеспечения безопасности и удобства использования USB-устройств. Серия включает:

- **Управляемые USB over IP концентраторы** — для удалённого подключения, аппаратного отключения и включения USB-устройств по сети.
- **USB over IP хабы** — для удалённого подключения USB-устройств по сети.
- **Управляемые USB-хабы** — для аппаратного отключения и включения USB-устройств, подключённых через USB-интерфейс.

1.1 Назначение прибора

Управляемый USB over IP концентратор предназначен для подключения USB-устройств (включая ключи электронной защиты, такие как eToken, ruToken и их аналоги, ключи для программных продуктов 1С, сканеры, принтеры, МФУ, сенсоры и т.д.) к компьютерной сети. Это устройство позволяет пользователям сети удалённо подключать USB-устройства к своему компьютеру или ноутбуку, пользоваться ими и управлять их физическим включением и подключением.

Концентратор обеспечивает двухступенчатую защиту USB-устройств при их совместном использовании в сети:

1. **Удалённое физическое включение и выключение USB-устройств.**
2. **Авторизация для подключения USB-устройств** по логину, паролю и IP-адресу.

В журнале концентратора сохраняется вся информация о действиях с USB-портами **DistKontrolUSB** и подключёнными устройствами:

- Подключения и отключения USB-портов и устройств;
- Попытки некорректного ввода пароля;
- Прочая дополнительная информация.

1.2 Модельный ряд управляемых USB over IP концентраторов



Управляемый USB over IP концентратор на 16 портов



Управляемый USB over IP концентратор на 32 порта



Управляемый USB over IP концентратор на 48 портов



Управляемый USB over IP концентратор на 64 порта

1.3 Область применения управляемых USB over IP концентраторов

Управляемые USB over IP концентраторы, такие как **DistKontrolUSB**, предоставляют уникальные возможности для удаленного управления USB устройствами через **WEB-интерфейс**. Это решение позволяет включать и отключать USB устройства физически, обеспечивая гибкость, безопасность и удобство в работе с периферийными устройствами.



1.3.1 Основные функции

1. **Удаленное управление USB устройствами**:
    - Включение и отключение USB портов через WEB-интерфейс без физического доступа.
    - Авторизация по логину, паролю и IP-адресу для повышения уровня безопасности.
    - Настройка прав доступа для разных пользователей.
2. **Система оповещений**:
    - Уведомления о событиях (подключение/отключение устройств, попытки несанкционированного доступа).
    - Возможность отправки уведомлений на электронную почту или другие каналы связи.
3. **Журнал событий**:
    - Фиксация всех подключений и отключений USB устройств с указанием пользователей и IP-адресов.
    - Экспорт данных журнала для анализа и аудита.
4. **Гибкое управление питанием**:
    - Настройка режимов резервирования питания.
    - Автоматическое переключение между блоками питания для обеспечения бесперебойной работы.
5. **Интеграция с системами виртуализации**:
    - Поддержка платформ виртуализации, таких как VMware и Hyper-V.
6. **Дополнительные функции безопасности**:
    - Встроенный брандмауэр и шифрование трафика.
    - Ограничение доступа по IP-адресу.

1.3.2 Исполнение и интерфейсы

- **Исполнение**: настольное (с возможностью установки в 19" стойку).
- **Интерфейсы**:
  - Ethernet (RJ-45) со скоростью до 1000 Мбит/с.
  - Встроенный Wi-Fi модуль.
- **Корпус**: металлический.

1.3.3 Преимущества использования

1. **Эффективность**:
   - Совместное использование USB устройств в сети повышает эффективность работы.
2. **Экономия**:
   - Централизованное управление устройствами экономит время и средства.
3. **Безопасность**:
   - Шифрование трафика, авторизация и ограничение доступа обеспечивают высокий уровень защиты данных.
4. **Удобство**:
   - Удаленное управление через WEB-интерфейс упрощает администрирование.

1.3.4 Применение в бизнесе

Использование USB over IP концентраторов позволяет:

- Повысить **безопасность информации** за счет удаленного хранения и управления USB устройствами.
- Обеспечить безопасное совместное использование ключей электронной подписи и других USB устройств.
- Удаленно подключать устройства по мере необходимости, избегая потери или повреждения ключей.
- Оптимизировать затраты на оборудование и повысить удобство работы.

1.3.5 Идеальное решение для совместного использования USB устройств

Устройство **DistKontrolUSB** идеально подходит для совместного использования USB устройств между несколькими пользователями в сети, через Интернет или в облаке. Ключевые особенности:

- USB устройство на компьютере пользователя выглядит так, как если бы оно было подключено напрямую.
- Совместимость с существующими драйверами и программным обеспечением без необходимости изменений.
- Управление доступом к USB устройствам для разных пользователей.

1.3.6 Гибкость и безопасность

- **Гибкость**: возможность подключения к нескольким USB хостам одновременно, что полезно в кластерных системах.
- **Безопасность**: шифрование трафика, авторизация и ограничение доступа по IP-адресу.
- **Надежность**: резервирование питания и автоматическое переключение между блоками питания.

1.3.7 Совместимость

Устройство **DistKontrolUSB** совместимо с популярными платформами виртуализации:

- **VMware**.
- **Microsoft Hyper-V**.

1.4 Комплект поставки управляемого USB over IP концентратора

Для 4-портовой модели:

1. **Управляемый USB over IP концентратор** — 1 шт.
2. **Паспорт** — 1 шт.
3. **Шнур питания** — 1 шт.
4. **Ножка для настольной установки** — 4 шт.

Для 16/32/48/64-портовых моделей:

1. **Управляемый USB over IP концентратор** — 1 шт.
2. **Паспорт** — 1 шт.
3. **Шнур питания** — 1 шт.
4. **Крепление в стойку 19"** — 2 шт.
5. **Винты крепления** — 8 шт.
6. **Ножка для настольной установки** — 4 шт.

1.5 Устройство и работа управляемого USB over IP концентратора

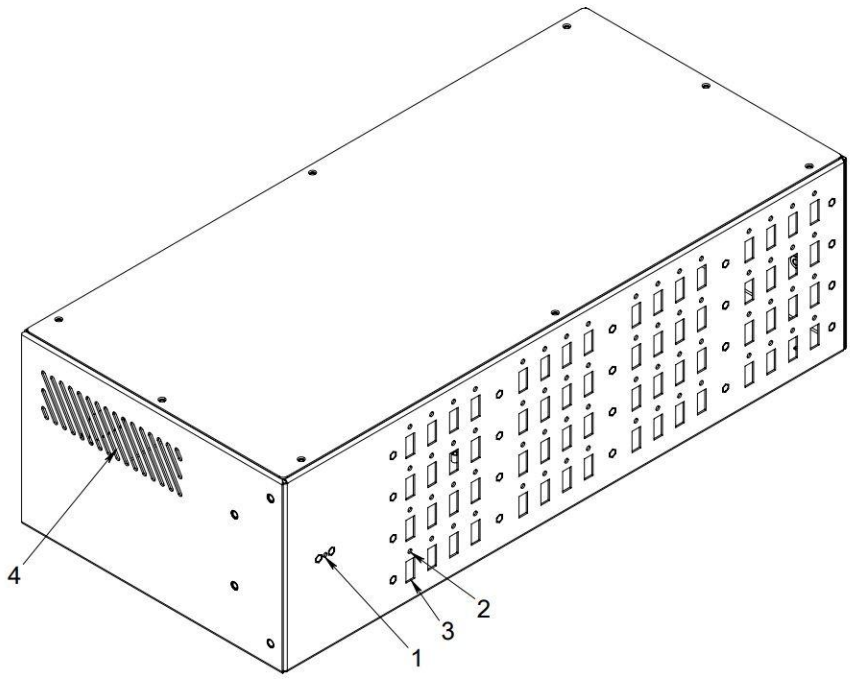
1.5.1 Габаритные размеры управляемых USB over IP концентраторов (в 19" стойку)

Габариты изделия и упаковки указаны в милиметрах в последовательности высота ширина глубина

Количество портов	Высота в U	Габариты изделия	Габариты упаковки
16 портов USB	1	44x440x285	50x500x320
32 порта USB	2	85x440x205	128x500x240
48 портов USB	3	130x440x205	128x500x240
64 порта USB	3	130x440x205	171x500x240

1.5.2 Устройство прибора

Концентратор выполнен в металлическом корпусе, допускающем его установку на стол или монтаж в стойку форм-фактора 19".

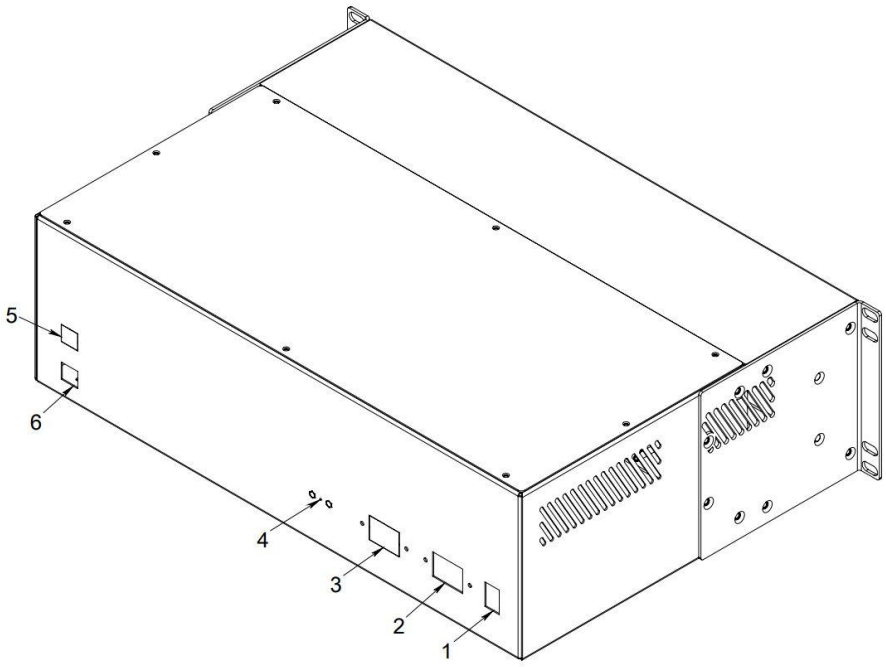


На передней панели расположены:

1. Индикатор включения питания
2. Индикатор активности USB-порта
3. Разъемы типа USB-A нисходящих портов для подключения устройств, поддерживающих протокол USB

На боковых панелях размещены:

1. Вентиляционные отверстия



На задней панели установлены:

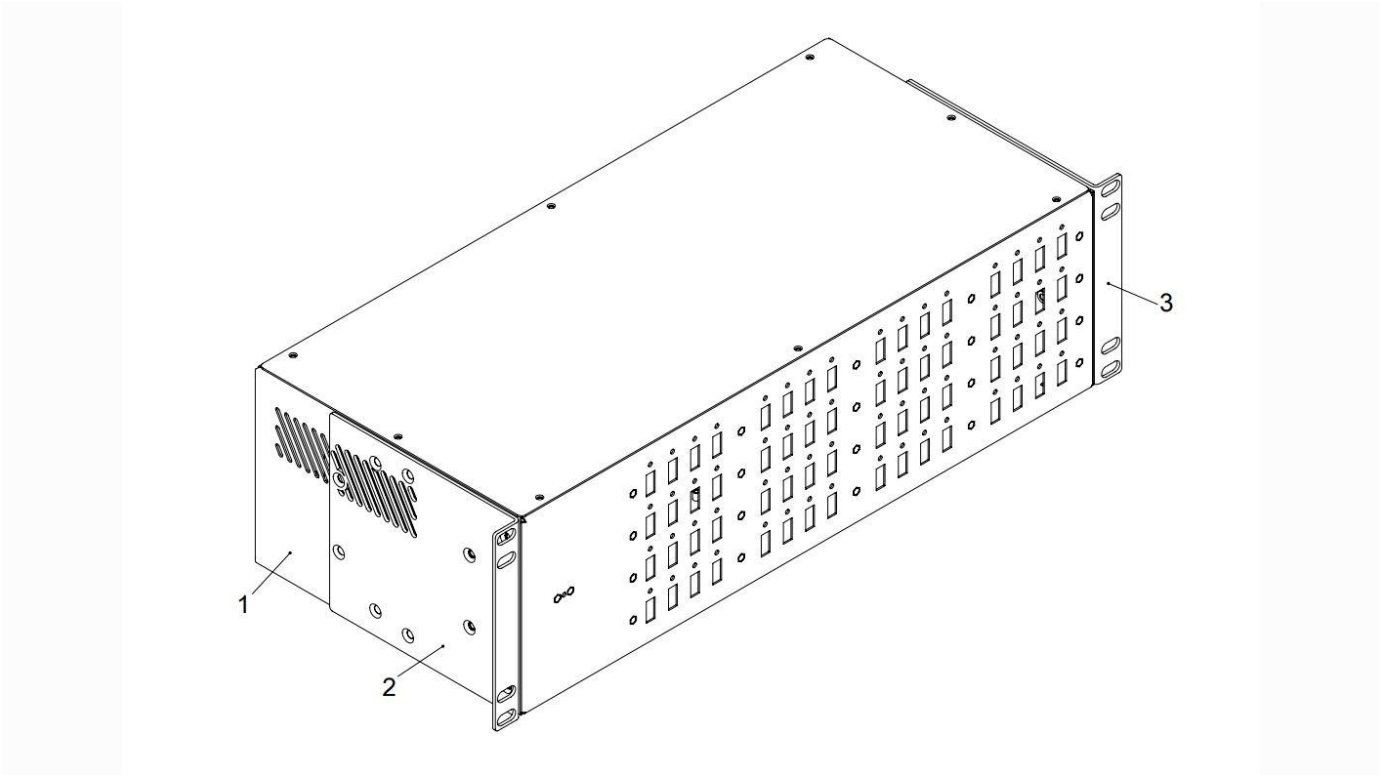
1. Выключатель питания «Питание»
2. Разъем для подключения сетевого кабеля 1
3. Разъем для подключения сетевого кабеля 2 (опционально)
4. Кнопка сброса настроек «Reset»
5. Разъем типа RJ45 для сети Ethernet «LAN» 2 (опционально)
6. Разъем типа RJ45 для сети Ethernet «LAN» 1

По углам нижней панели концентратора имеется четыре отверстия для монтажа приборных ножек для его установки на поверхность (стол).

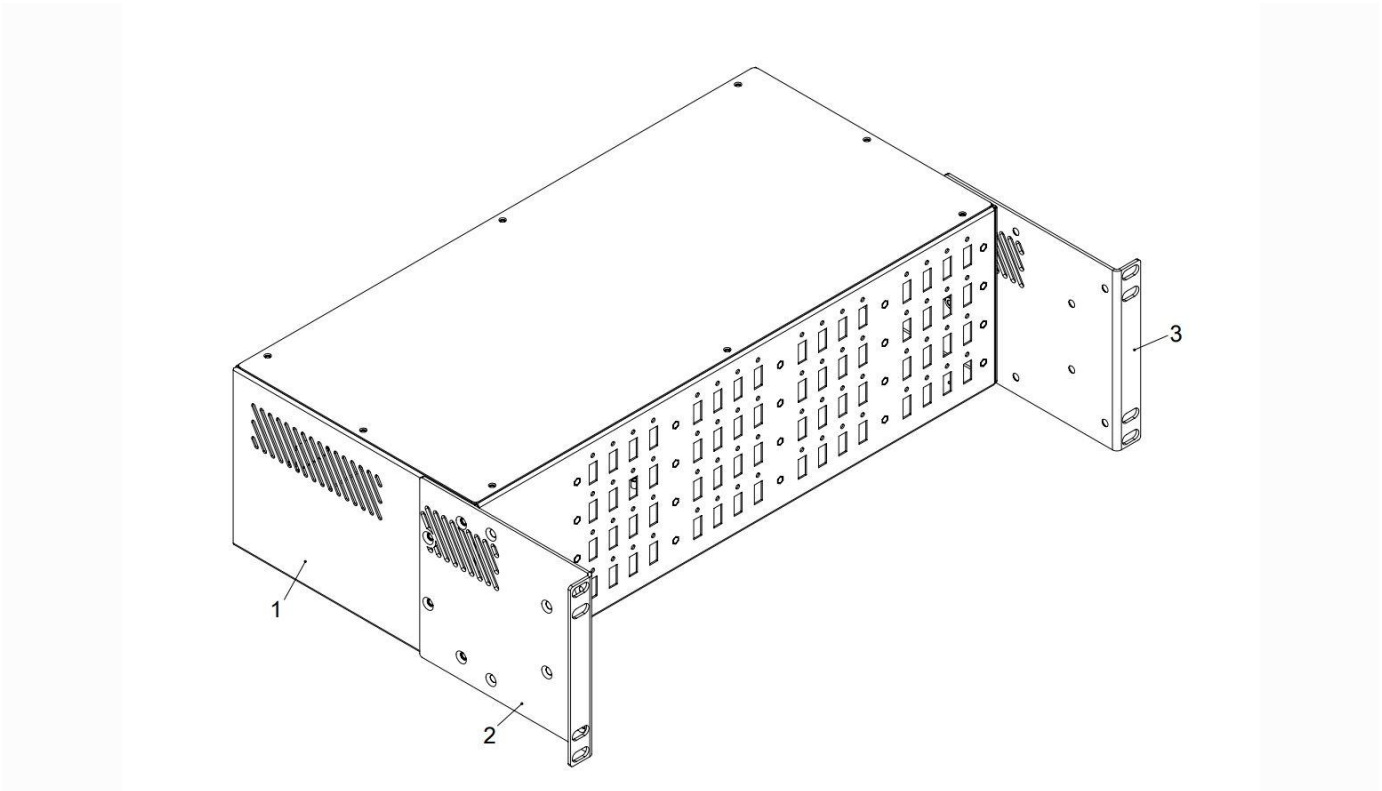
В комплекте с устройством поставляются крепления в стойку/шкаф 19” с возможностью крепления в двух положениях

На рис:

1 – Устройство
2,3 – Крепления в стойку/шкаф 19”



Сборка устройства для крепления в стойку 19”.



1.5.5 Эксплуатационные ограничения и рекомендации

Концентратор обеспечивает непрерывную круглосуточную работу и является восстанавливаемым и обслуживаемым.

Концентратор сохраняет работоспособность при:

- Температуре от **-5°C до +50°C**

- Влажности **до 98%** при +25°C
- Синусоидальной вибрации в диапазоне частот от 10 до 55 Гц при амплитуде смещения до 0,35 мм (в любом направлении) в соответствии с требованиями ГОСТ 12997.

1.5.6 Меры безопасности

При эксплуатации прибора следует соблюдать «Межотраслевые правила по охране труда (правила безопасности) при эксплуатации электроустановок».

- Класс безопасности: **I (**ГОСТ 12.2.007.0-75**)**
- Конструкция прибора обеспечивает степень защиты: **IP20 (**ГОСТ 14254-96**)**
- Источниками опасности прибора являются цепи сетевого напряжения **~220В**, контакты **~220В** разъёма подключения кабеля питания и встроенный преобразователь напряжения.
- Прибор устанавливается горизонтально на столах или других конструкциях, в стойку 19`, в местах, где отсутствует доступ посторонних лиц.
- Установку (снятие), монтаж, ремонт производить при отключенном сетевом напряжении ~220В от прибора.
- Не рекомендуется закрывать вентиляционные отверстия концентратора на боковых панелях.

1.5.7 Подготовка к работе

Подготовка концентратора к использованию включает в себя следующие операции:

1. После распаковки, визуально проверить, нет ли на концентраторе повреждений (при перевозке транспортной компанией осмотр производить при получении устройства);
2. Разместить концентратор на устойчивой, ровной поверхности (столе) или закрепить в стойке 19";
3. Подключить шнур питания на задней панели концентратора;
4. Подключить вилку сетевого шнура к сети 220В 50 Гц;
5. Подключить к USB-портам, расположенным на передней панели прибора, устройства, поддерживающие протокол USB;
6. Подключить прибор к сети Ethernet;
7. Включить питание.

Внимание!

Не включайте концентратор, если его температура ниже комнатной! (Это может возникнуть при перевозке концентратора в холодное время года). Дайте концентратору нагреться до комнатной температуры, прежде чем включать его.

1.5.8 Работа управляемого USB over IP концентратора

Для работы с USB устройством, подключенным к управляемому USB over IP концентратору, необходимо:

1. Включить USB устройство (удаленно подать питание на устройство USB);
2. Подключить USB устройство к своему компьютеру (ноутбуку, планшету, телефону и т.п.).

Включение и отключение USB устройств, подключенных к управляемому USB over IP концентратору возможно (включение и отключение USB входов устройства):

- Через WEB интерфейс;
- С помощью планировщика задач и назначенных заданий;
- С помощью утилиты управления устройством (скриптами, из командной строки или своего приложения).

Подключение и отключение USB устройств, подключенных к управляемому USB over IP концентратору возможно:

- Через клиентское приложение, работающее в графическом режиме или в виде службы;
- С помощью API (скриптами, из командной строки или своего приложения).

Для использования, управляемого USB over IP концентратора, необходимо:

1. Подключить устройство к LAN (через Ethernet или WiFi) и произвести его настройку.
2. На каждом компьютере, к которому необходимо пробросить USB устройство запустить программное обеспечение DistKontrolUSB Client, работающее под управлением версий Linux, Windows, OSX.
3. Настройка и управление устройством подключения USB по сети осуществляется через Web интерфейс.
4. Настройка клиентского компьютера проста и интуитивно понятна. DistKontrolUSB Client работает под управлением версий Linux, Windows, а также OSX. Клиент позволяет интуитивно понятного и простого подключать и отключать удаленные устройства USB. DistKontrolUSB Client не требует установки. Клиент может запускаться в качестве сервиса.

1.6 Пломбирование

После проведения приемо-сдаточных испытаний на предприятии-изготовителе прибор пломбируется.

Устанавливаемые пломбы (печати) должны исключать возможность несанкционированного внесения изменений в электрическую принципиальную схему прибора. Пломбы (печати) устанавливаются на приборе таким образом, чтобы исключить возможность снятия крышки прибора без повреждения пломбы (печати).

1.7 Упаковка

Готовой продукцией считается прибор, принятый представителем технического контроля и упакованный в потребительскую тару.

2 Технические характеристики

Технические характеристики управляемых USB over IP концентраторов

Защита и управление USB портами

Управляемый USB over IP концентратор обеспечивает следующие функции защиты и управления:

Ограничение тока и защита от перегрева

- **Ограничение тока**: Каждый USB порт ограничен по току, что предотвращает перегрузку.
- **Защита от перегрева**: При возникновении перегрева порт автоматически блокируется до устранения неисправности.
- **Перезагрузка порта**: Удаление нагрузки приводит к перезагрузке USB порта.

Плавный запуск USB портов

- **Схема плавного запуска**: Минимизирует броски пускового тока, что особенно важно при высокой емкостной нагрузке.

Ток нагрузки

- **Модели USB 2.0**: номинальный ток 0,5 А на порт, предельный — 0,9 А.
- **Модели USB 3.0**: номинальный ток 1 А на порт (опционально 2 А), предельный — 2,1 А.

DistKontrolUSB4 3.0



- **Сетевые интерфейсы**: Ethernet (RJ-45), 802.11n Wireless
- **Порт Ethernet**: 1 x 10/100/1000 Mb (опционально: 2 x 10/100/1000 Mb)
- **Количество USB портов**:
  - Неуправляемые: 4 (2 x USB 3.0, 2 x USB 2.0)
  - Управляемые: -
- **IP адреса**: 2 static / DHCP (IPv4/IPv6)
- **Индикация**:
  - Питание
  - LAN порт статус
- **Поддержка USB**: USB 3.0, 2.0, 1.1, 1.0
- **Защита USB портов**: -
- **Ток нагрузки на порт USB**:
  - Номинальный: 0,5 A
  - Предельный: 0,9 A
- **Условия эксплуатации**:
  - Температура: 0°C до +50°C
  - Влажность: ≤ 80% (при +35°C и ниже)

- **Поддержка ОС**:
    - Windows® Server 2016/2019/2022
    - Windows® 10/11
    - Linux (ядро ≥ 4.9+)
    - OSX (10.9.5-10.13, 12 Monterrey)
- **Габаритные размеры (В/Ш/Г, мм)**: 35 / 140 / 110
- **Крепление в 19” стойку**: Нет
- **Размеры в Unit**: -
- **Безопасность**:
    - HTTPS, SSL: Есть
    - Шифрование трафика USB: Есть
    - Встроенный брандмауэр: Есть
    - Ограничение по IP (устройство/порт): Есть
    - Авторизация (устройство/порт): Есть
    - Групповые политики доступа: Нет
    - Управление видимостью USB устройств: Нет
    - Модуль защиты USB устройств: Нет
    - Резервирование питания: Нет
    - Отказоустойчивость Ethernet портов: Нет (опционально: есть)

DistKontrolUSB8 3.0



- **Сетевые интерфейсы**: Ethernet (RJ-45), 802.11n Wireless
- **Порт Ethernet**: 1 x 10/100/1000 Mb
- **Количество USB портов**:
  - Неуправляемые: -
  - Управляемые: 8
- **IP адреса**: 1 static / DHCP (IPv4/IPv6)
- **Индикация**:
  - Питание
  - LAN порт статус
  - Наличие питания порта USB-устройства
- **Поддержка USB**: USB 3.2 Gen1 (SS, HS, FS, LS)
- **Защита USB портов**:
  - Ограничение по току, выключение при перегреве
  - Плавный запуск
- **Ток нагрузки на порт USB**:
  - Номинальный: 1 A (опционально: 2 A)
  - Предельный: 2,1 A

- **Условия эксплуатации**:
  - Температура: 0°C до +50°C
  - Влажность: ≤ 80% (при +35°C и ниже)
- **Поддержка ОС**:
  - Windows® Server 2016/2019/2022
  - Windows® 10/11
  - Linux (ядро ≥ 4.9+)
  - OSX (10.9.5-10.13, 12 Monterrey)
- **Габаритные размеры (В/Ш/Г, мм)**: 45 / 440 / 285
- **Крепление в 19" стойку**: Есть
- **Размеры в Unit**: 1
- **Сенсорный дисплей**: Есть
- **Безопасность**:
  - HTTPS, SSL: Есть
  - Шифрование трафика USB: Есть
  - Встроенный брандмауэр: Есть
  - Ограничение по IP (устройство/порт): Есть
  - Авторизация (устройство/порт): Есть
  - Групповые политики доступа: Есть (до 8 групп)
  - Управление видимостью USB устройств: Есть (до 8 групп)
  - Модуль защиты USB устройств: Нет (опционально: есть)
  - Резервирование питания: Нет (опционально: есть)
  - Отказоустойчивость Ethernet портов: Нет

DistKontrolUSB16 2.0



- **Сетевые интерфейсы**: Ethernet (RJ-45), 802.11n Wireless
- **Порт Ethernet**: 1 x 10/100/1000 Mb (опционально: 2 x 10/100/1000 Mb, 10 Gb)
- **Количество USB портов**:
    - Неуправляемые: -
    - Управляемые: 16
- **IP адреса**: 2 static / DHCP (IPv4/IPv6)
- **Индикация**:
    - Питание
    - LAN порт статус
    - Питание USB портов
- **Питание**: Встроенный блок питания 220В, 50 Гц, 75 Вт (опционально: второй блок питания)
- **Поддержка USB**: USB 2.0, 1.1, 1.0
- **Защита USB портов**:
    - Ограничение по току, выключение при перегреве
    - Плавный запуск
- **Ток нагрузки на порт USB**:
    - Номинальный: 0,5 А

- Предельный: 0,9 А

• **Условия эксплуатации**:

- Температура: 0°C до +50°C
- Влажность: ≤ 80% (при +35°C и ниже)

• **Поддержка ОС**:

- Windows® Server 2016/2019/2022
- Windows® 10/11
- Linux (ядро ≥ 4.9+)
- OSX (10.9.5-10.13, 12 Monterrey)

• **Габаритные размеры (В/Ш/Г, мм)**: 44 / 440 / 285

• **Крепление в 19” стойку**: Есть

• **Размеры в Unit**: 1

• **Безопасность**:

- HTTPS, SSL: Есть
- Шифрование трафика USB: Есть
- Встроенный брандмауэр: Есть
- Ограничение по IP (устройство/порт): Есть
- Авторизация (устройство/порт): Есть
- Групповые политики доступа: Есть (до 16 групп)
- Управление видимостью USB устройств: Есть (до 16 групп)
- Модуль защиты USB устройств: Нет (опционально: есть)
- Резервирование питания: Нет (опционально: есть)
- Отказоустойчивость Ethernet портов: Нет (опционально: есть)

DistKontrolUSB16 3.0



- **Сетевые интерфейсы**: Ethernet (RJ-45), 802.11n Wireless
- **Порт Ethernet**: 1 x 10/100/1000 Mb (опционально: 2 x 10/100/1000 Mb, 10 Gb)
- **Количество USB портов**:
    - Неуправляемые: -
    - Управляемые: 16
- **IP адреса**: 1 static / DHCP (IPv4/IPv6)
- **Индикация**:
    - Питание
    - LAN порт статус
    - Наличие питания порта USB-устройства
- **Поддержка USB**: USB 3.2 Gen1 (SS, HS, FS, LS)
- **Защита USB портов**:
    - Ограничение по току, выключение при перегреве
    - Плавный запуск
- **Ток нагрузки на порт USB**:
    - Номинальный: 1 A (опционально: 2 A)
    - Предельный: 2,1 A

- **Условия эксплуатации**:
  - Температура: 0°C до +50°C
  - Влажность: ≤ 80% (при +35°C и ниже)
- **Поддержка ОС**:
  - Windows® Server 2016/2019/2022
  - Windows® 10/11
  - Linux (ядро ≥ 4.9+)
  - OSX (10.9.5-10.13, 12 Monterrey)
- **Габаритные размеры (В/Ш/Г, мм)**: 132 / 440 / 205
- **Крепление в 19" стойку**: Есть
- **Размеры в Unit**: 3
- **Сенсорный дисплей**: Есть
- **Безопасность**:
  - HTTPS, SSL: Есть
  - Шифрование трафика USB: Есть
  - Встроенный брандмауэр: Есть
  - Ограничение по IP (устройство/порт): Есть
  - Авторизация (устройство/порт): Есть
  - Групповые политики доступа: Есть (до 16 групп)
  - Управление видимостью USB устройств: Есть (до 16 групп)
  - Модуль защиты USB устройств: Нет (опционально: есть)
  - Резервирование питания: Нет (опционально: есть)
  - Отказоустойчивость Ethernet портов: Нет (опционально: есть)

DistKontrolUSB24 3.0



- **Сетевые интерфейсы**: Ethernet (RJ-45), 802.11n Wireless
- **Порт Ethernet**: 1 x 10/100/1000 Mb (опционально: 2 x 10/100/1000 Mb, 10 Gb)
- **Количество USB портов**:
  - Неуправляемые: -
  - Управляемые: 24
- **IP адреса**: 1 static / DHCP (IPv4/IPv6)
- **Индикация**:
  - Питание
  - LAN порт статус
  - Наличие питания порта USB-устройства
- **Поддержка USB**: USB 3.2 Gen1 (SS, HS, FS, LS)
- **Защита USB портов**:
  - Ограничение по току, выключение при перегреве
  - Плавный запуск
- **Ток нагрузки на порт USB**:
  - Номинальный: 1 A (опционально: 2 A)
  - Предельный: 2,1 A
- **Условия эксплуатации**:
  - Температура: 0°C до +50°C
  - Влажность: ≤ 80% (при +35°C и ниже)
- **Поддержка ОС**:
  - Windows® Server 2016/2019/2022
  - Windows® 10/11
  - Linux (ядро ≥ 4.9+)
  - OSX (10.9.5-10.13, 12 Monterrey)
- **Габаритные размеры (В/Ш/Г, мм)**: 132 / 440 / 205

- **Крепление в 19" стойку**: Есть
- **Размеры в Unit**: 3
- **Безопасность**:
    - HTTPS, SSL: Есть
    - Шифрование трафика USB: Есть
    - Встроенный брандмауэр: Есть
    - Ограничение по IP (устройство/порт): Есть
    - Авторизация (устройство/порт): Есть
    - Групповые политики доступа: Есть (до 16 групп)
    - Управление видимостью USB устройств: Есть (до 16 групп)
    - Модуль защиты USB устройств: Нет (опционально: есть)
    - Резервирование питания: Нет (опционально: есть)
    - Отказоустойчивость Ethernet портов: Нет (опционально: есть)

DistKontrolUSB32 2.0



- **Сетевые интерфейсы**: Ethernet (RJ-45), 802.11n Wireless
- **Порт Ethernet**: 1 x 10/100/1000 Mb (опционально: 2 x 10/100/1000 Mb, 10 Gb)
- **Количество USB портов**:
    - Неуправляемые: -
    - Управляемые: 32
- **IP адреса**: 2 static / DHCP (IPv4/IPv6)
- **Индикация**:
    - Питание
    - LAN порт статус
    - Питание USB портов
- **Питание**: Встроенный блок питания 220В, 50 Гц, 100 Вт (опционально: второй блок питания)
- **Поддержка USB**: USB 2.0, 1.1, 1.0
- **Защита USB портов**:
    - Ограничение по току, выключение при перегреве
    - Плавный запуск
- **Ток нагрузки на порт USB**:
    - Номинальный: 0,5 А

    - Предельный: 0,9 А
- **Условия эксплуатации**:
    - Температура: 0°C до +50°C
    - Влажность: ≤ 80% (при +35°C и ниже)
- **Поддержка ОС**:
    - Windows® Server 2016/2019/2022
    - Windows® 10/11
    - Linux (ядро ≥ 4.9+)
    - OSX (10.9.5-10.13, 12 Monterrey)
- **Габаритные размеры (В/Ш/Г, мм)**: 85 / 440 / 205
- **Крепление в 19” стойку**: Есть
- **Размеры в Unit**: 2
- **Безопасность**:
    - HTTPS, SSL: Есть
    - Шифрование трафика USB: Есть
    - Встроенный брандмауэр: Есть
    - Ограничение по IP (устройство/порт): Есть
    - Авторизация (устройство/порт): Есть
    - Групповые политики доступа: Есть (до 16 групп)
    - Управление видимостью USB устройств: Есть (до 16 групп)
    - Модуль защиты USB устройств: Нет (опционально: есть)
    - Резервирование питания: Нет (опционально: есть)
    - Отказоустойчивость Ethernet портов: Нет (опционально: есть)

DistKontrolUSB32 3.0



- **Сетевые интерфейсы**: Ethernet (RJ-45), 802.11n Wireless
- **Порт Ethernet**: 1 x 10/100/1000 Mb (опционально: 2 x 10/100/1000 Mb, 10 Gb)
- **Количество USB портов**:
    - Неуправляемые: -
    - Управляемые: 32
- **IP адреса**: 1 static / DHCP (IPv4/IPv6)
- **Индикация**:
    - Питание
    - LAN порт статус
    - Наличие питания порта USB-устройства
- **Поддержка USB**: USB 3.2 Gen1 (SS, HS, FS, LS)
- **Защита USB портов**:
    - Ограничение по току, выключение при перегреве
    - Плавный запуск
- **Ток нагрузки на порт USB**:
    - Номинальный: 1 A (опционально: 2 A)
    - Предельный: 2,1 A

- **Условия эксплуатации**:
  - Температура: 0°C до +50°C
  - Влажность: ≤ 80% (при +35°C и ниже)
- **Поддержка ОС**:
  - Windows® Server 2016/2019/2022
  - Windows® 10/11
  - Linux (ядро ≥ 4.9+)
  - OSX (10.9.5-10.13, 12 Monterrey)
- **Габаритные размеры (В/Ш/Г, мм)**: 132 / 440 / 205
- **Крепление в 19" стойку**: Есть
- **Размеры в Unit**: 3
- **Безопасность**:
  - HTTPS, SSL: Есть
  - Шифрование трафика USB: Есть
  - Встроенный брандмауэр: Есть
  - Ограничение по IP (устройство/порт): Есть
  - Авторизация (устройство/порт): Есть
  - Групповые политики доступа: Есть (до 16 групп)
  - Управление видимостью USB устройств: Есть (до 16 групп)
  - Модуль защиты USB устройств: Нет (опционально: есть)
  - Резервирование питания: Нет (опционально: есть)
  - Отказоустойчивость Ethernet портов: Нет (опционально: есть)

DistKontrolUSB48



- **Сетевые интерфейсы**: Ethernet (RJ-45), 802.11n Wireless
- **Порт Ethernet**: 1 x 10/100/1000 Mb (опционально: 2 x 10/100/1000 Mb, 10 Gb)
- **Количество USB портов**:
  - Неуправляемые: -
  - Управляемые: 48
- **IP адреса**: 2 static / DHCP (IPv4/IPv6)
- **Индикация**:
  - Питание
  - LAN порт статус
  - Питание USB портов
- **Питание**: Встроенный блок питания 220В, 50 Гц, 150 Вт (опционально: второй блок питания)
- **Поддержка USB**: USB 2.0, 1.1, 1.0
- **Защита USB портов**:
  - Ограничение по току, выключение при перегреве
  - Плавный запуск
- **Ток нагрузки на порт USB**:
  - Номинальный: 0,5 А
  - Предельный: 0,9 А
- **Условия эксплуатации**:
  - Температура: 0°С до +50°С
  - Влажность: ≤ 80% (при +35°С и ниже)
- **Поддержка ОС**:
  - Windows® Server 2016/2019/2022
  - Windows® 10/11

- Linux (ядро ≥ 4.9+)
- OSX (10.9.5-10.13, 12 Monterrey)

• **Габаритные размеры (В/Ш/Г, мм)**: 130 / 440 / 205
• **Крепление в 19” стойку**: Есть
• **Размеры в Unit**: 3
• **Безопасность**:

- HTTPS, SSL: Есть
- Шифрование трафика USB: Есть
- Встроенный брандмауэр: Есть
- Ограничение по IP (устройство/порт): Есть
- Авторизация (устройство/порт): Есть
- Групповые политики доступа: Есть (до 16 групп)
- Управление видимостью USB устройств: Есть (до 16 групп)
- Модуль защиты USB устройств: Нет (опционально: есть)
- Резервирование питания: Нет (опционально: есть)
- Отказоустойчивость Ethernet портов: Нет (опционально: есть)

DistKontrolUSB64



- **Сетевые интерфейсы**: Ethernet (RJ-45), 802.11n Wireless
- **Порт Ethernet**: 1 x 10/100/1000 Mb (опционально: 2 x 10/100/1000 Mb, 10 Gb)
- **Количество USB портов**:
  - Неуправляемые: -
  - Управляемые: 64
- **IP адреса**: 2 static / DHCP (IPv4/IPv6)
- **Индикация**:
  - Питание
  - LAN порт статус
  - Питание USB портов
- **Питание**: Встроенный блок питания 220В, 50 Гц, 300 Вт (опционально: второй блок питания)
- **Поддержка USB**: USB 2.0, 1.1, 1.0
- **Защита USB портов**:
  - Ограничение по току, выключение при перегреве
  - Плавный запуск
- **Ток нагрузки на порт USB**:
  - Номинальный: 0,5 А
  - Предельный: 0,9 А
- **Условия эксплуатации**:
  - Температура: 0°C до +50°C
  - Влажность: ≤ 80% (при +35°C и ниже)
- **Поддержка ОС**:
  - Windows® Server 2016/2019/2022
  - Windows® 10/11

- Linux (ядро ≥ 4.9+)
- OSX (10.9.5-10.13, 12 Monterrey)

• **Габаритные размеры (В/Ш/Г, мм)**: 130 / 440 / 205
• **Крепление в 19” стойку**: Есть
• **Размеры в Unit**: 3
• **Безопасность**:

- HTTPS, SSL: Есть
- Шифрование трафика USB: Есть
- Встроенный брандмауэр: Есть
- Ограничение по IP (устройство/порт): Есть
- Авторизация (устройство/порт): Есть
- Групповые политики доступа: Есть (до 16 групп)
- Управление видимостью USB устройств: Есть (до 16 групп)
- Модуль защиты USB устройств: Нет (опционально: есть)
- Резервирование питания: Нет (опционально: есть)
- Отказоустойчивость Ethernet портов: Нет (опционально: есть)

3 Техническое обслуживание

3.1 Общие положения

Техническое обслуживание прибора проводится по планово-предупредительной системе и осуществляется Потребителем. Персонал, обслуживающий данные изделия, должен иметь группу по электробезопасности не ниже III.

Техническое обслуживание заключается в периодическом (не реже одного раза в год):

- внешнем осмотре хаба, с удалением пыли мягкой тканью;
- внешнем осмотре состояния разъемов и проводов.
- очистке вентиляционных отверстий

При техническом обслуживании должны соблюдаться требования техники безопасности, а также требования:

- **ГОСТ 12.1.006**;
- **ГОСТ 12.1.019**;
- **ГОСТ 12.2.003**;
- **«Правил технической эксплуатации электроустановок потребителей»**;
- **«Правил техники безопасности при эксплуатации электроустановок потребителей»**.

3.2 Проверка работоспособности управляемого USB хаба

Для проверки прибора необходимо:

1. К каждому из портов подключить USB флеш-накопитель с записанными на него произвольными файлами.
2. Подключив этот накопитель к ПК, посредством **WEB-интерфейса** (индикатор активности порта должен гореть) произвести чтение файла.
3. Возможность чтения файла свидетельствует об исправности проверяемого порта.
4. После отключения порта индикатор включения порта должен погаснуть.

Примечание:

В случае отсутствия необходимого количества USB флеш-накопителей можно производить указанные операции с портами последовательно.

4 Консервация и хранение управляемого USB over IP концентратора

4.1 Консервация

Консервация прибора при длительном хранении не предусматривается.

4.2 Хранение, Транспортировка и Утилизация

Хранение прибора рекомендуется производить в отапливаемых складских помещениях.
В помещениях не должно быть паров кислот, щелочей, агрессивных газов и других вредных примесей, вызывающих коррозию.

Транспортировка прибора может осуществляться:

- любыми видами автомобильного,
- железнодорожного,
- авиа транспорта

В закрытых кузовах (контейнерах, вагонах).
Условия транспортировки должны соответствовать условиям хранения **5 по** ГОСТ 15150-69.

После транспортировки прибор перед включением должен быть выдержан в нормальных условиях **не менее 12 часов**.

Утилизация:
Специальных требований к утилизации прибора не предъявляется.

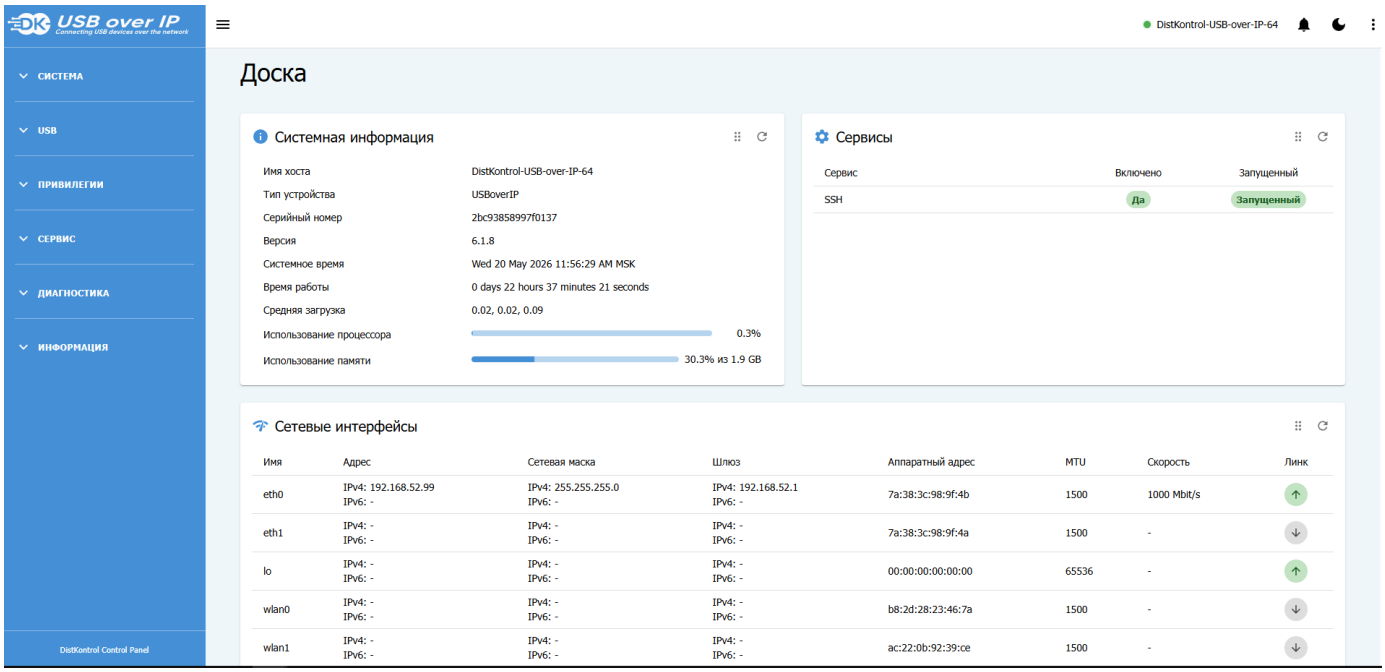
5 Web интерфейс управления DistKontrolUSB

5.1 Вход в WEB-интерфейс и начальный экран

Управление USB over IP концентратором осуществляется через **мультиязычный WEB интерфейс администратора**.
После авторизации доступно управление настройками.

Вид главной страницы можно настроить, добавив или убрав нужные панели.

Вид WEB интерфейса управления настройками устройства подключения USB по сети:



По умолчанию DistKontrolUSB имеет следующие сетевые настройки:

- **Статический IP адрес Сетевой интерфейс 1** – `192.168.1.180`
- **Логин** к панели WEB интерфейса – `admin`
- **Пароль** к панели WEB интерфейса – `admin`
- **Порт подключения клиентов** – `6565` (по умолчанию)
- **SSL порт подключения клиентов** – `7575` (при включенном режиме)
- **Интерфейс WiFi (wlan0)** – отключен

Внимание!

При некорректном вводе пароля **до 3 раз**, пользователь, для которого были попытки ввода, блокируется на **5 минут**.
Каждый последующий ввод (даже корректного пароля) **обновляет таймер блокировки**.

5.2 Система

5.2.1 Общие настройки

5.2.1.1 WEB администратор

В данном разделе находятся настройки Web интерфейса.

SSL настраивается для Web интерфейса.

Внимание!

При отключении ранее настроенного шифрования требуется очистить кэш браузера, так как некоторые браузеры кэшируют переадресацию с http на https.

Внимание!

Пользователь может изменить порты:

- HTTP с `80` на произвольный
- HTTPS с `443` на произвольный
- SSH с `22` на произвольный

При изменении портов **не допускайте их совпадения** с портами групп USB концентратора.

Некорректное назначение портов может привести к потере доступа к WEB интерфейсу.

Для восстановления потребуется **полный сброс устройства** к заводским настройкам.

5.2.1.2 Пароль WEB-администратора

В данном разделе возможно изменить пароль пользователя `admin`.

Внимание!

При утере пароля потребуется **сброс настроек** управляемого USB over IP концентратора в исходное состояние.

5.2.2 Дата и время

Настройки по умолчанию:

- Используется NTP-сервер

Ручная настройка:

1. Отключите опцию «Использование сервера NTP».
2. Укажите время вручную.
3. Нажмите кнопку «Обновить сейчас» (доступно только в ручном режиме).

Внимание!

При изменении NTP-сервера **требуется перезагрузка устройства**.

Информация:

Текущее время отображается статично (загружается при открытии раздела «Дата и время»).

5.2.3 Сеть

5.2.3.1 Общий

- Имя хоста - имя, которое будет отображено в клиенте DistKontrolUSB.

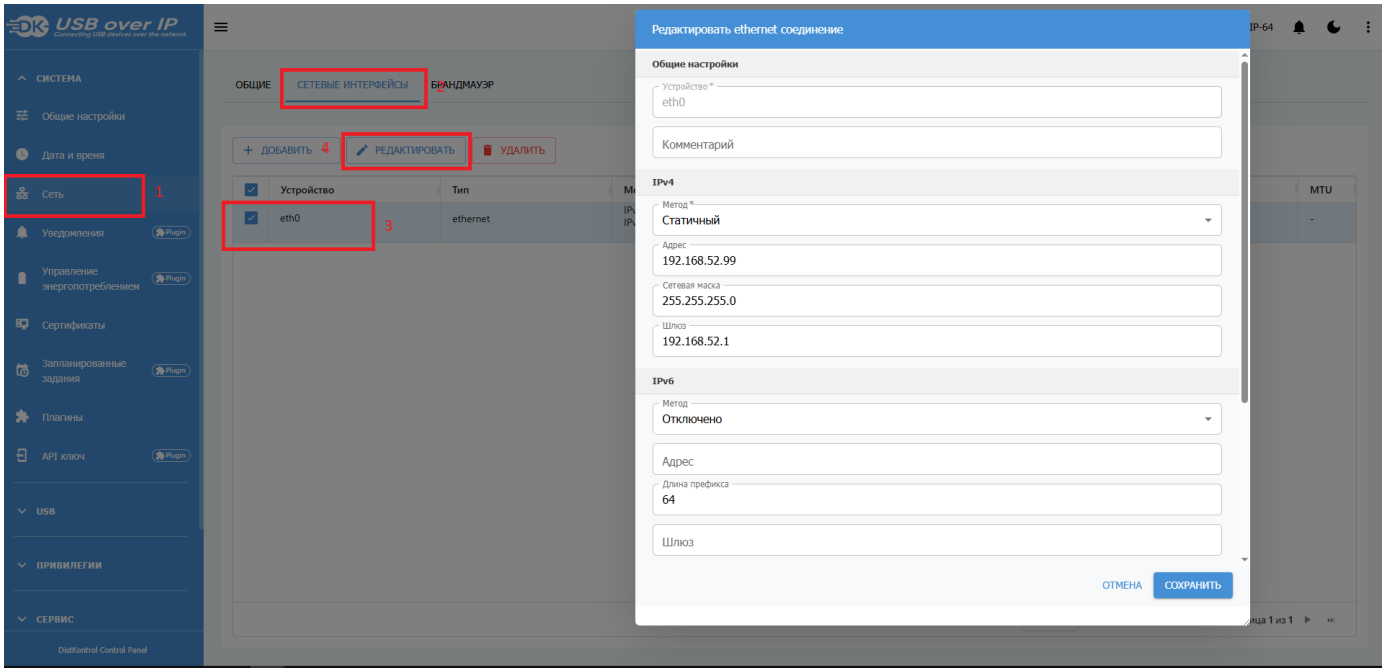
Информация:

- Рекомендуется изменить при нескольких концентраторах в сети.
- При наличии несколько сетевых интерфейсов, рекомендуется добавлять концентратор по имени хоста. В этом случае, независимо от активного интерфейса, устройство будет отображено в клиенте.

- Доменное имя – добавляет имя домена 2-го и более уровня. Не влияет на подключение к домену, используется для графического отображения в клиентском приложении.

5.2.3.2 Интерфейсы

IP адрес меняется при двойном клике на соответствующем сетевом интерфейсе (по пути **Система** → **Сеть** → **Интерфейсы**). Возможно, как совместное использование интерфейсов LAN(eth0) и WiFi(wlan0), так и самостоятельное использование любого из интерфейсов. При использовании только одного сетевого интерфейса, второй рекомендуется отключать.



5.2.3.2.1 Bond интерфейс

> **Информация:**
> Для настройки Bond соединения необходимо, по крайней мере, два физических сетевых интерфейса.

Для создания соединения Bond, необходимо удалить все интерфейсы, которые будут участвовать в соединении. При удалении интерфейса Eth0, IP адрес устройства станет динамическим. После применения настроек, зайдите в Web - интерфейс по новому адресу и настройте Bond соединения, добавив все необходимые интерфейсы. См. База знаний — Как создать Bond интерфейс.

Web - интерфейс позволяет выбрать менее двух. Это сделано специально для целей конфигурации. Рабочий процесс для двух сетевых карт выглядит следующим образом:

1) Если основной сетевой адаптер уже работает с помощью установщика, настройте его через Web - интерфейс как статический. Если установлено как статическое, используя тот же IP-адрес, указанный DHCP, не должно быть необходимости повторно входить в Web-интерфейс.

2) Выберите второй доступный сетевой адаптер, выберите режим подключения, заполните поле IP - адреса и значения маски подсети, оставьте шлюз и DNS пустыми. Сохраните и нажмите применить.

3) Выйдите из системы и получите доступ к Web - интерфейсу, используя новый IP - адрес, назначенный созданному bond интерфейсу.

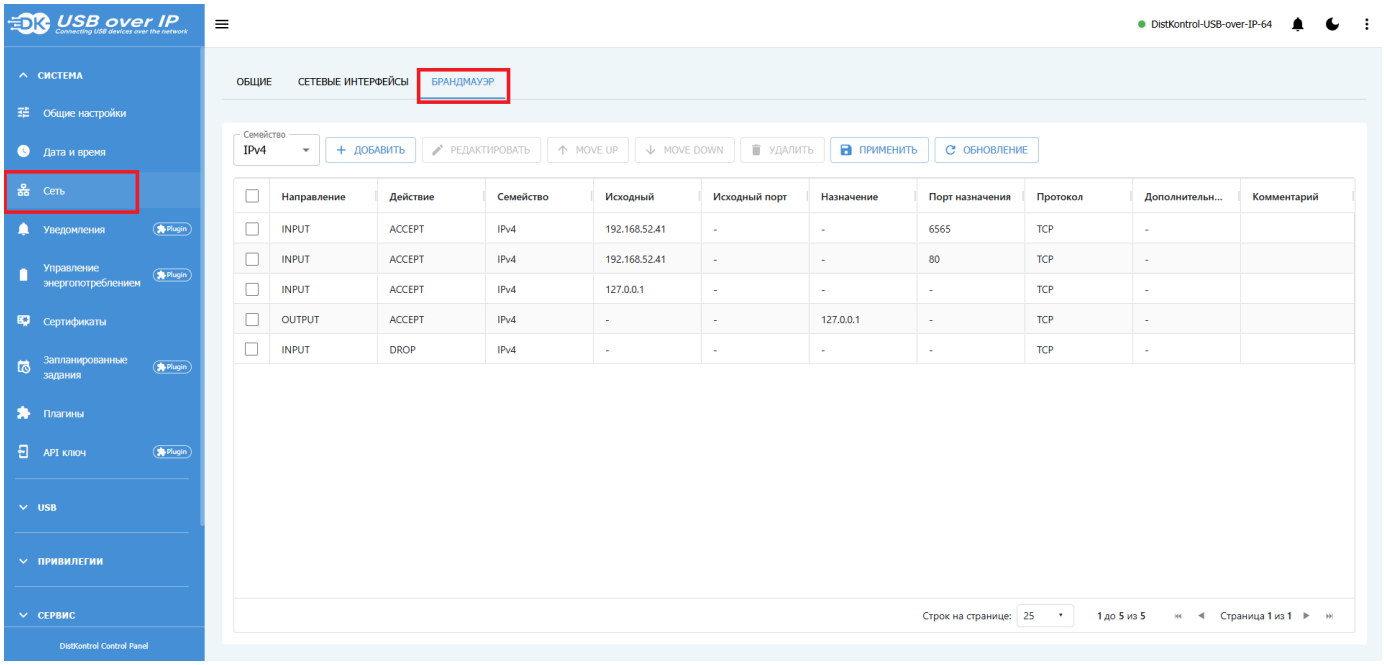
4) Теперь выберите основной интерфейс, настроенный через Web - интерфейс на первом шаге, и удалите его. Сохраните и нажмите применить.

5) Выберите вновь созданный интерфейс связи, нажмите "Изменить", теперь для выбора должна быть доступна физическая сетевая карта, удаленная с предыдущего шага. Сохраните и нажмите применить.

6) Теперь панель мониторинга должна отображать информацию об bond интерфейсе (включая скорость).

5.2.3.3 Брандмуэр

Брандмауэр концентратора работает на базе `iptables`. Он может быть полезен, если вам необходимо полностью исключить доступ к концентратору каким-то компьютерам в локальной сети. Или предоставить доступ только с определенных компьютеров. Можно создать соответствующие правила в таблице фильтров.



Пример настройки:
Требуется предоставить доступ к концентратору (WEB - интерфейсу - порт `80`
и USB устройствам – порт `6565`) только с одного компьютера в локальной сети с IP `192.168.1.105`.

Необходимо:

1. Разрешить доступ с IP `192.168.1.105` к концентратору для клиентского приложения.
2. Разрешить доступ с IP `192.168.1.105` к WEB - интерфейсу концентратора.
3. Разрешить доступ с localhost `127.0.0.1`
4. Все остальные соединения запретить.

Внимание!

Внимательно настраивайте правила, не закройте доступ к WEB интерфейсу концентратора (для восстановления контроля над ним потребуется **сброс настроек**, управляемого USB over IP концентратора в исходное состояние).

5.2.4 Сертификаты

Управляемый USB over IP концентратор поддерживает импорт имеющихся сертификатов и создание самоподписанных сертификатов SSL/SSH. Управление — на странице «Система» → «Сертификаты».

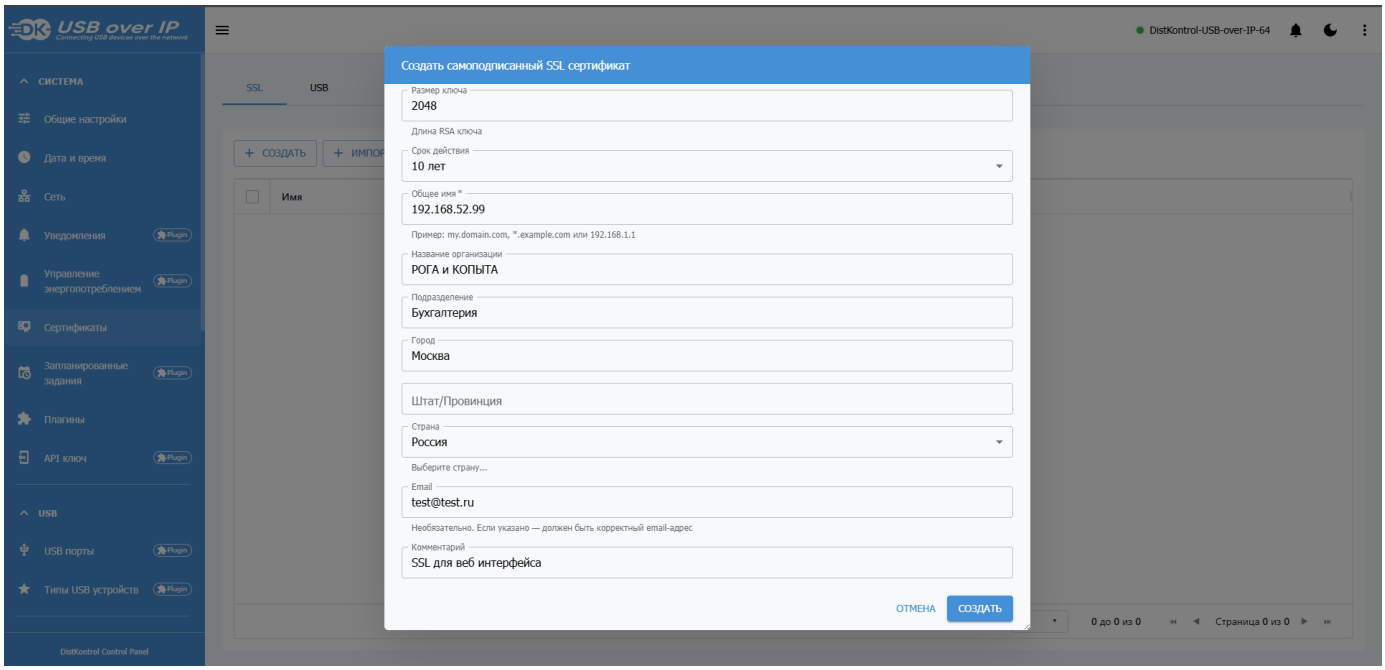
Типы сертификатов:

1. **SSL** — безопасное соединение с WEB-интерфейсом.
2. **USB** — шифрование трафика USB-устройств между клиентом и концентратором.

Примечание:

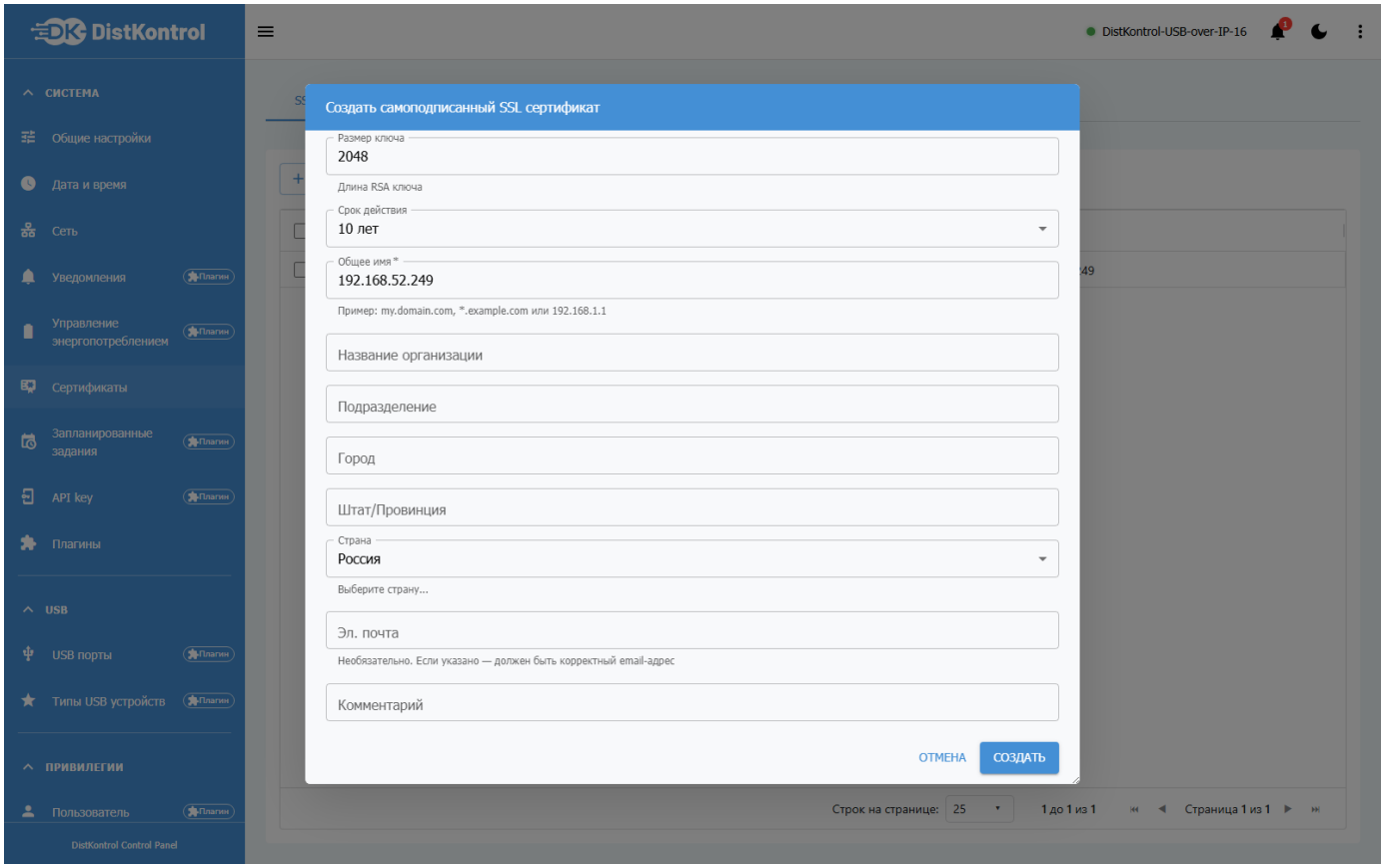
Для корректной работы SSL устройство должно получать время по NTP (5.2.2 Дата и время).

SSL для WEB-интерфейса

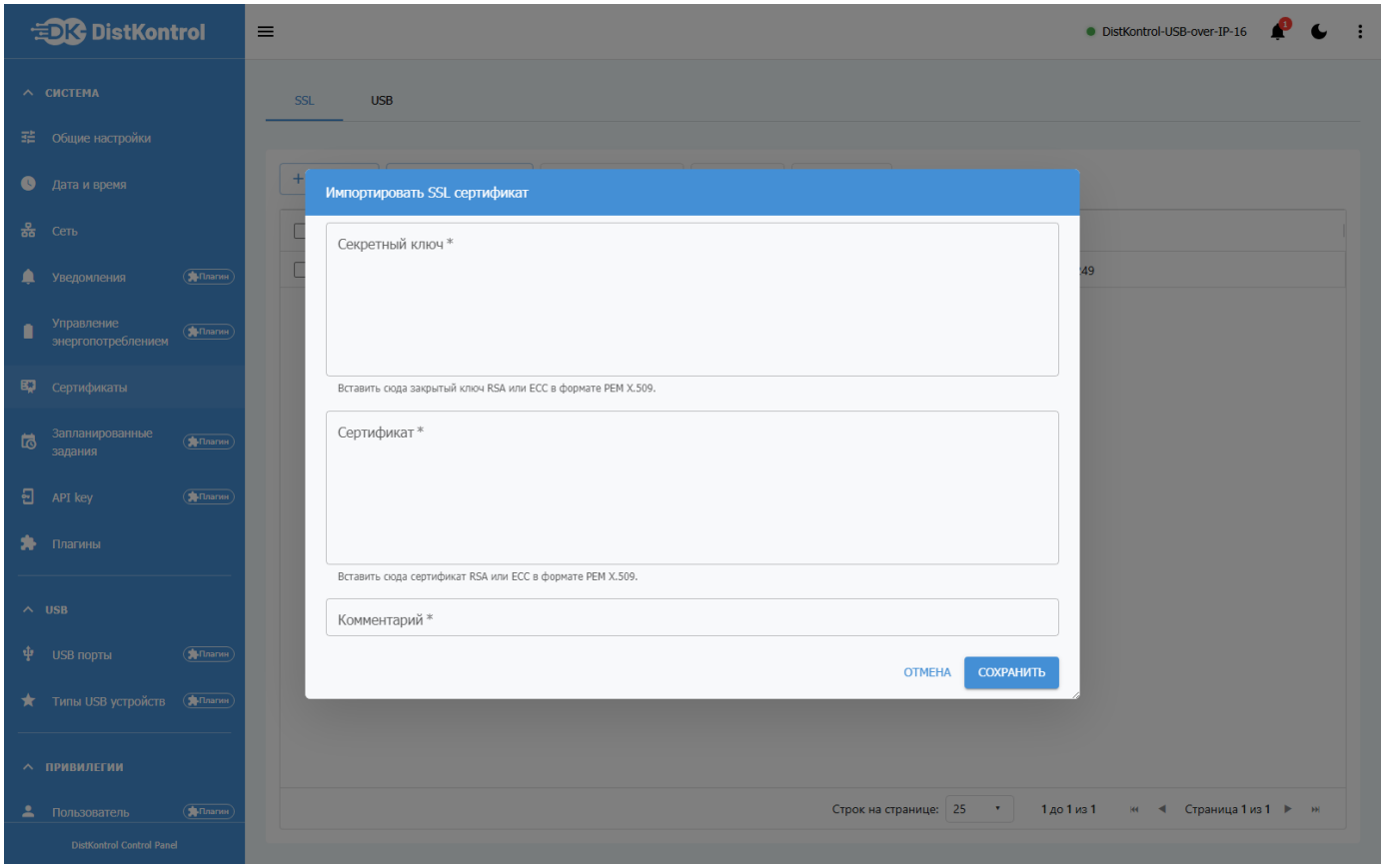


Безопасное соединение включается на странице «Общие настройки». Там же можно включить принудительное использование только HTTPS.

Создание самоподписанного сертификата: «Сертификаты» → вкладка «SSL» → **«СОЗДАТЬ»**.



Импорт сертификата (приватный RSA-ключ и сертификат X.509 в формате PEM): вкладка «SSL» → **«ИМПОРТИРОВАТЬ»**.



Также можно использовать самоподписанный сертификат DistKontrolUSB: «Сертификаты» → «SSL» → «Скачать сертификат» или «Информация» → «Поддержка».

Внимание!

Для шифрования трафика используется OpenSSL. При создании сертификата вне устройства:

```
openssl genrsa -out usb.key 2048
openssl req -new -x509 -days 3650 -key usb.key -out usb.crt
openssl x509 -in usb.crt -out usb.pem -outform PEM
```

В пути к сертификату **не должно быть кириллицы**.

SSL для трафика USB-устройств

Концентратор поддерживает SSL (TLS) для связи клиент/сервер — это повышает защиту при работе через Интернет. Допустимы коммерческие и самоподписанные сертификаты.

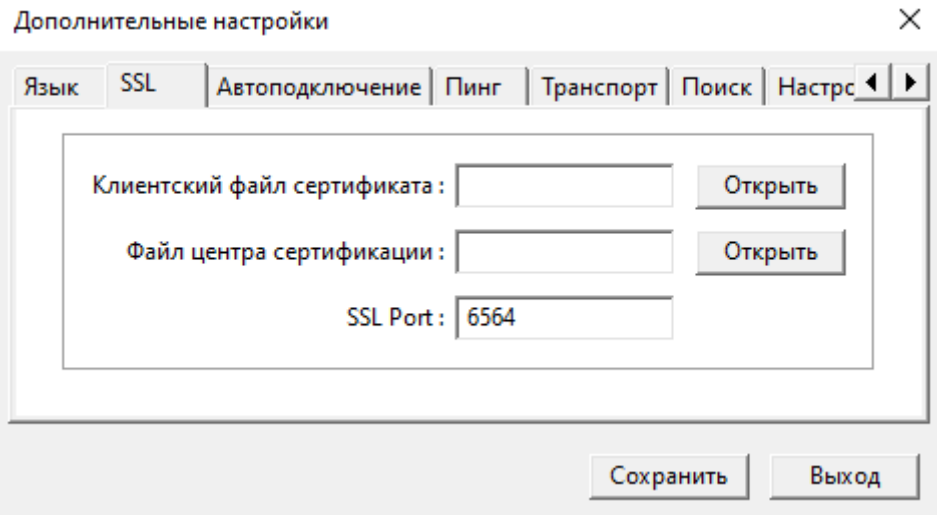
Включение на устройстве:

1. Создайте или импортируйте сертификат на вкладке «USB» (или используйте сертификат со вкладки «SSL»).
2. Назначьте сертификат группе, в которой он будет использоваться (5.4.3 Группы).
3. В настройках группы включите **«Включение SSL для USB-трафика»**.
4. После включения режима и/или добавления сертификатов **перезагрузите устройство**.

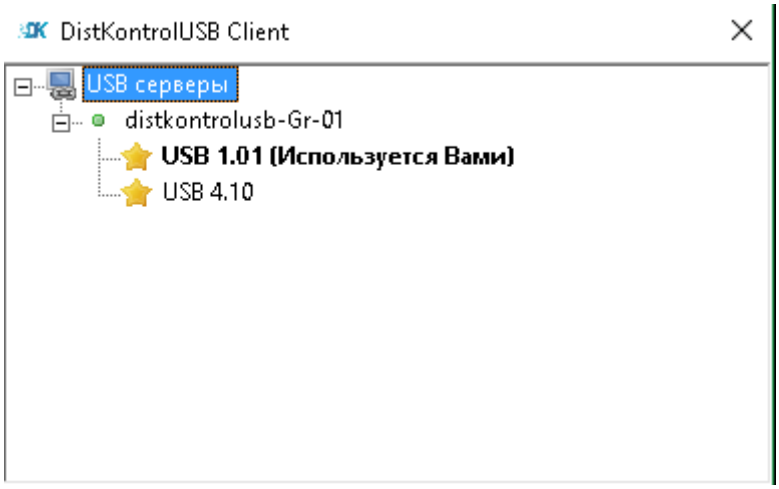
Сертификат для клиентского приложения: «Система» → «Сертификаты» → «USB» → «Скачать сертификат».

Настройка клиентского приложения (DistKontrolUSB Client):

1. ПКМ по «USB серверы» → «Дополнительные настройки».
2. Вкладка «SSL» → «Файл центра сертификации» → «Открыть» → выберите файл `*.pem`.
3. Укажите SSL-порт группы (по умолчанию для Group1: `6564`).
4. Нажмите «Сохранить» и согласитесь с перезапуском клиента.



Если используется несколько групп с разными SSL-сертификатами — скачайте все сертификаты, объедините их в один файл PEM в текстовом редакторе. Порты укажите через запятую.



После настройки клиент подключается по TLSv1.2 через SSL-порт (по умолчанию `6564`). Без «Автоматического поиска» в «Specify Hubs» укажите адрес концентратора и порт SSL.

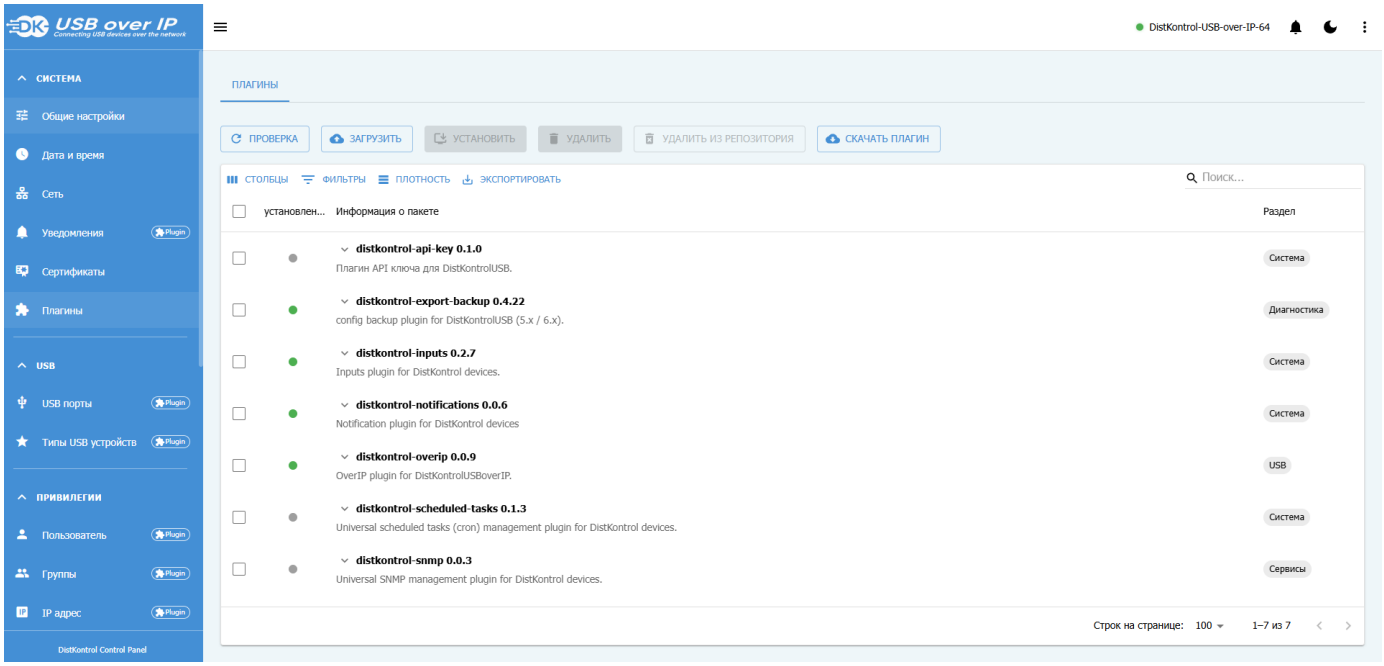
Внимание!

На ряде ОС в пути к сертификату не должно быть кириллицы.

При долгом подключении с SSL это нормально: База знаний — SSL и скорость подключения.
Дополнительно: настройка клиента с SSL, консольный клиент с SSL.

5.2.5 Плагины

Раздел **«Плагины»** предназначен для установки и управления дополнительными модулями, расширяющими функциональность системы.



- Для установки плагина необходимо выполнить следующее:
- Скачайте плагин с нашего сайта: https://www.distkontrol.com/support/download
- В **Web-интерфейсе**, в разделе **«Плагины»** нажмите на кнопку **«Загрузить»**.
- В открывшемся окне нажмите выберите скаченный плагин.
- После загрузки выберите плагин и нажмите кнопку **«Установить»**.
- Перезагрузите страницу браузера.
- Для отключения и удаления плагина:
- Выберите плагин и нажмите **«Удалить»** — плагин будет отключен.
- Для полного удаления плагина из концентратора выберите отключенный плагин и нажмите на **«Удалить из репозитория»**.

Внимание!

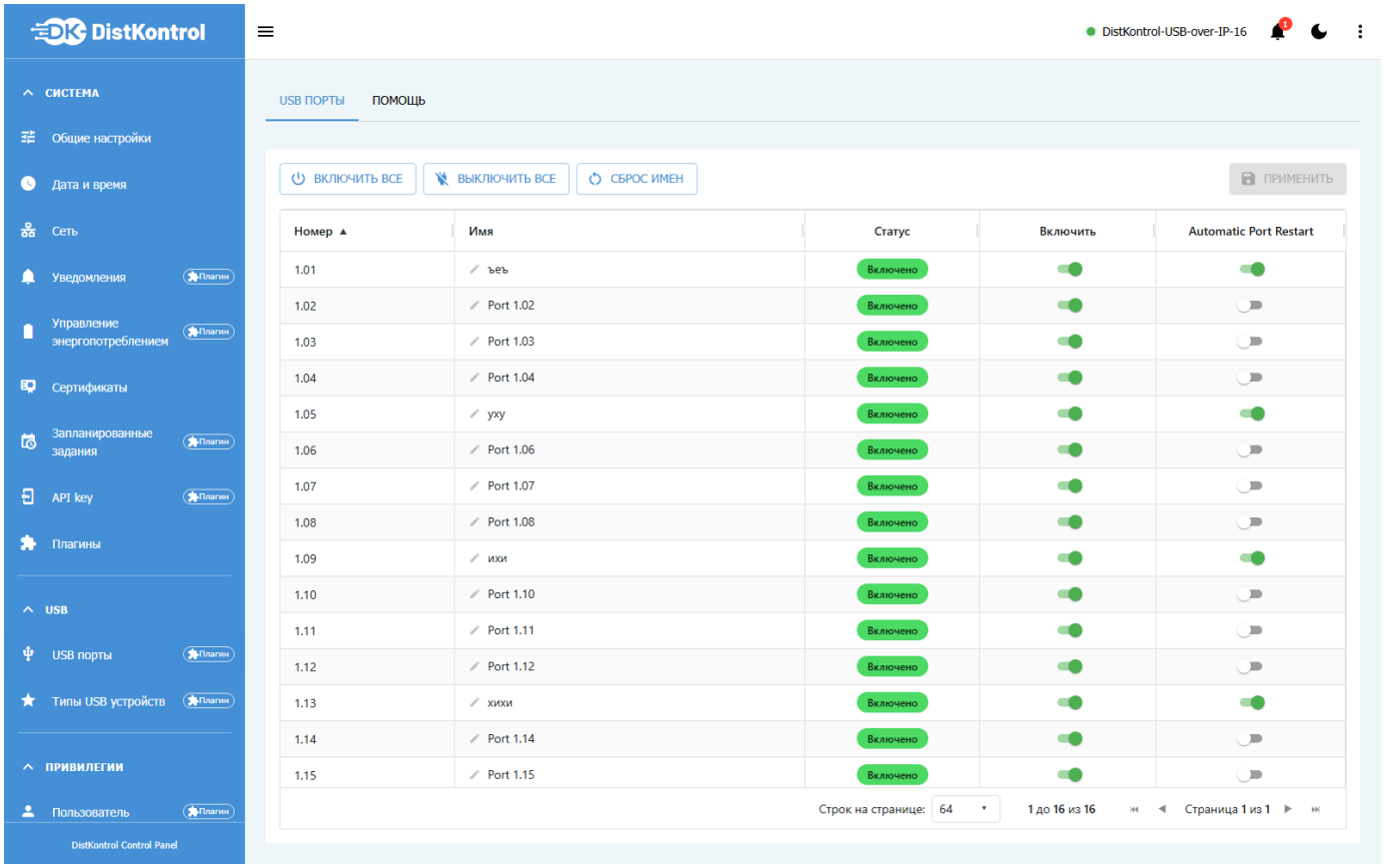
Подробная документация по плагинам и актуальный их список указан на официальном сайте и в Руководстве пользователя по плагинам

5.3 USB

Раздел **USB** включает управление портами концентратора и регистрацию типов USB-устройств для настройки прав доступа.

5.3.1 USB-порты

Возможно изменение наименования порта USB. Включение и выключение USB портов управляемого USB over IP концентратора осуществляется переключателем в строке порта или кнопками панели.

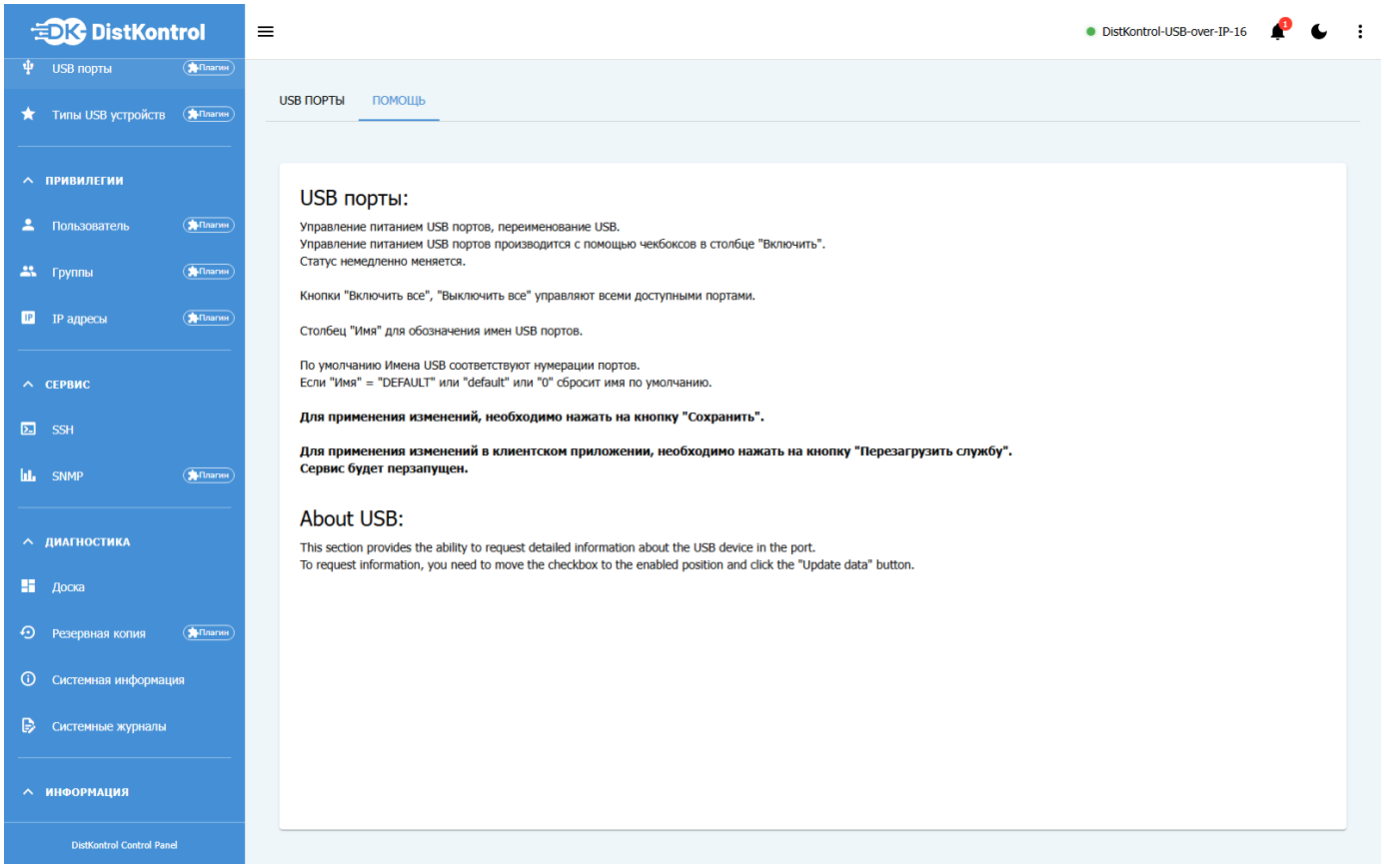


Кнопки **«Включить все»**, **«Выключить все»** управляют всеми доступными портами. Кнопка **«Сброс имён»** возвращает имена портов к значениям по умолчанию. Столбец **«Имя»** — для обозначения имён USB-портов.

Если отображаемое имя равно `DEFAULT`, `default` или `0`, имя сбрасывается к значению по умолчанию. Для применения изменений нажмите кнопку **«Применить»**.

Автоматический перезапуск порта предназначен для снятия и подачи питания на порт, если пользователь отключится от USB-устройства в данном порту.

На вкладке **«Помощь»** — краткая справка по разделу.



5.3.2 Типы USB-устройств

Раздел **«Типы USB устройств»** необходим для настройки прав доступа к подключаемым USB-устройствам. Концентратор работает по принципу «запрещено всё, что явно не разрешено»: пока устройство не добавлено в этот список, доступ к нему через клиентское приложение не предоставляется.

На странице отображается таблица зарегистрированных типов USB-устройств. Для каждой записи указываются:

Столбец	Описание
Номер	Порядковый идентификатор устройства в системе (используется при назначении прав и в командах SSH).
Имя	Произвольное наименование (обычно — модель устройства).
Vendor ID	Идентификатор производителя USB (VID).
Product ID	Идентификатор продукта USB (PID).
Serial №	Серийный номер экземпляра устройства.
Пользователи	Список пользователей, которым назначен доступ к данному устройству.

Кнопки панели:

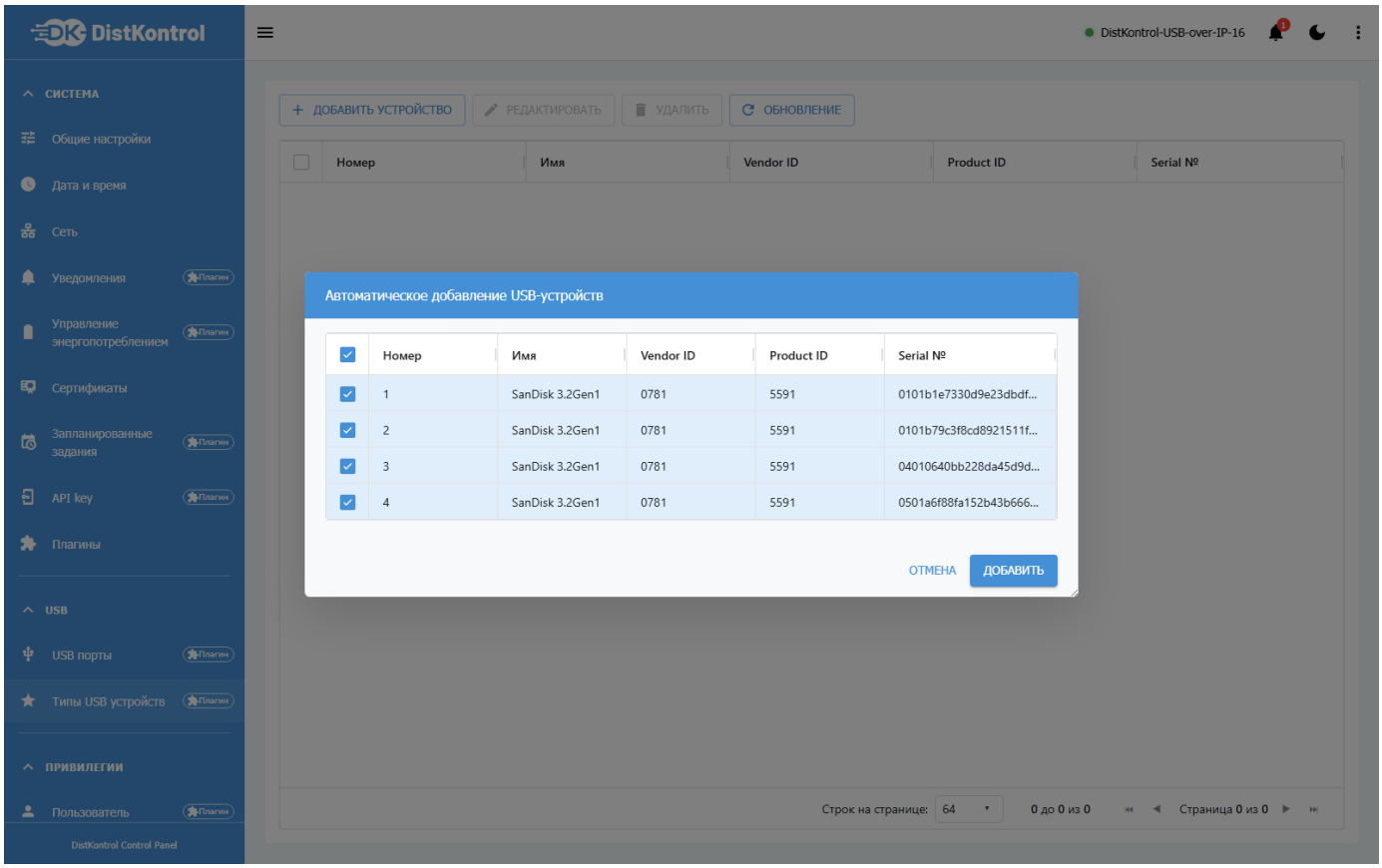
- **«Добавить устройство»** — добавление вручную или через автопоиск.
- **«Редактировать»** / **«Удалить»** — изменение или удаление выбранной записи (активны после выбора строки).

• **«Обновление»** — обновление списка в таблице.

Добавление через автопоиск

Рекомендуемый способ. USB-устройство должно быть подключено к включённому порту концентратора (см. 5.3.1 USB-порты).

1. Нажмите **«Добавить устройство»** → **«Автопоиск»**.
2. В диалоге отметьте нужные устройства из списка обнаруженных.
3. Нажмите **«Добавить»**.

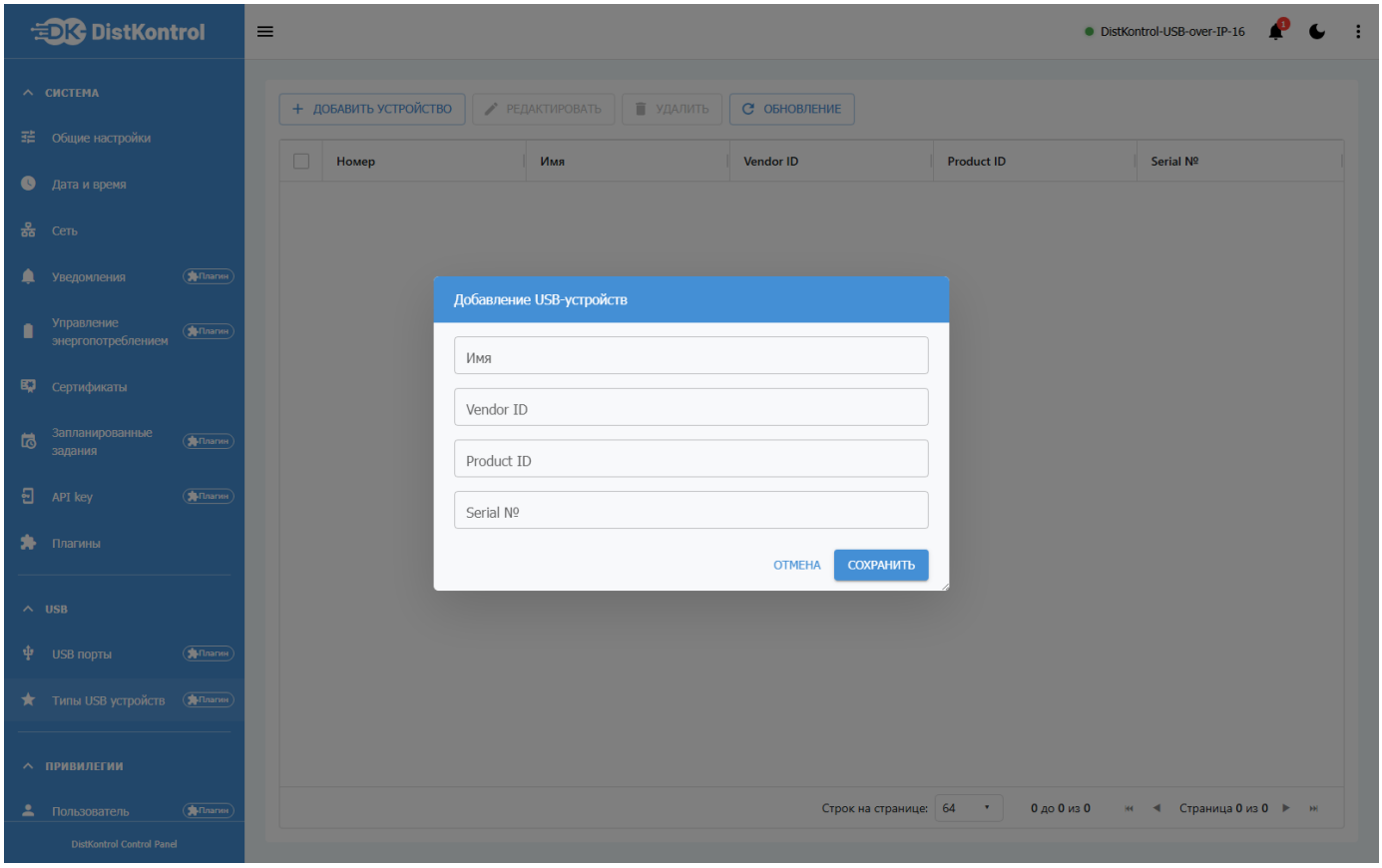


Система сформирует отчёт о результате добавления. У каждого устройства в списке должен быть уникален хотя бы один из параметров: **Vendor ID**, **Product ID** или **Serial №**.

Добавление вручную

Используется, если автопоиск не обнаружил устройство или оно временно не подключено. Необходимо знать **Vendor ID**, **Product ID** и **Serial №** — их можно посмотреть в клиентском приложении DistKontrolUSB Client или в системном журнале (см. 5.6.3 Системный журнал).

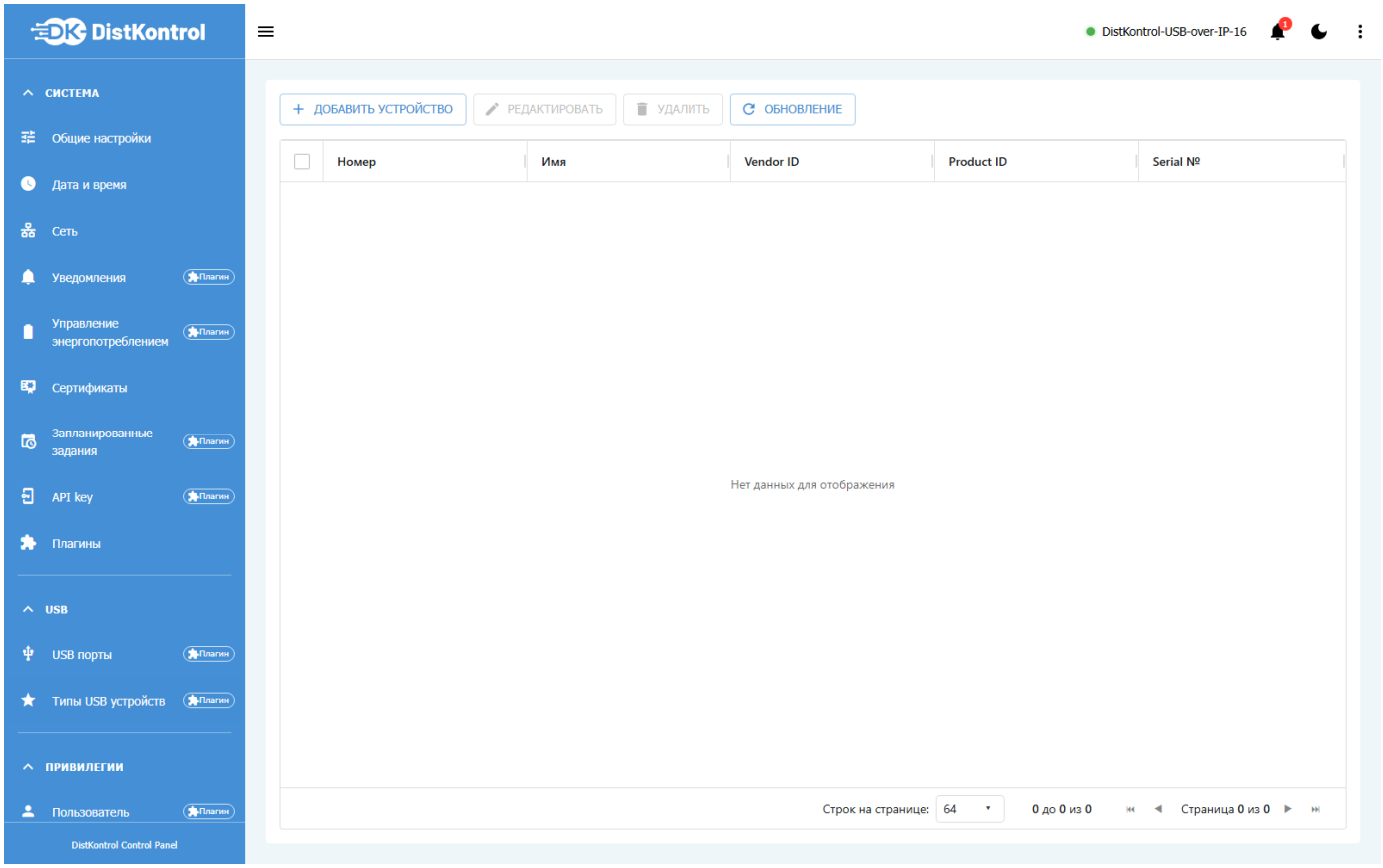
1. Нажмите **«Добавить устройство»** → **«Добавить вручную»**.
2. Заполните поля и сохраните запись.



Vendor ID, Product ID и Serial № должны содержать только цифры и латинские буквы.

Редактирование и удаление

Выберите строку в таблице и нажмите **«Редактировать»** для изменения имени или идентификаторов, либо **«Удалить»** для удаления записи из списка.



После регистрации устройств назначьте права пользователям или IP-адресам в разделе 5.4 Управление правами доступа.

На вкладке **«Помощь»** — краткая справка по разделу.

Внимание!

Некоторые USB-устройства могут работать некорректно. В этом случае они будут пропускаться при автопоиске. Возможно некорректное отображение списка поиска. Отключите и повторно включите питание USB-порта и повторите поиск устройств.

5.4 Управление правами доступа

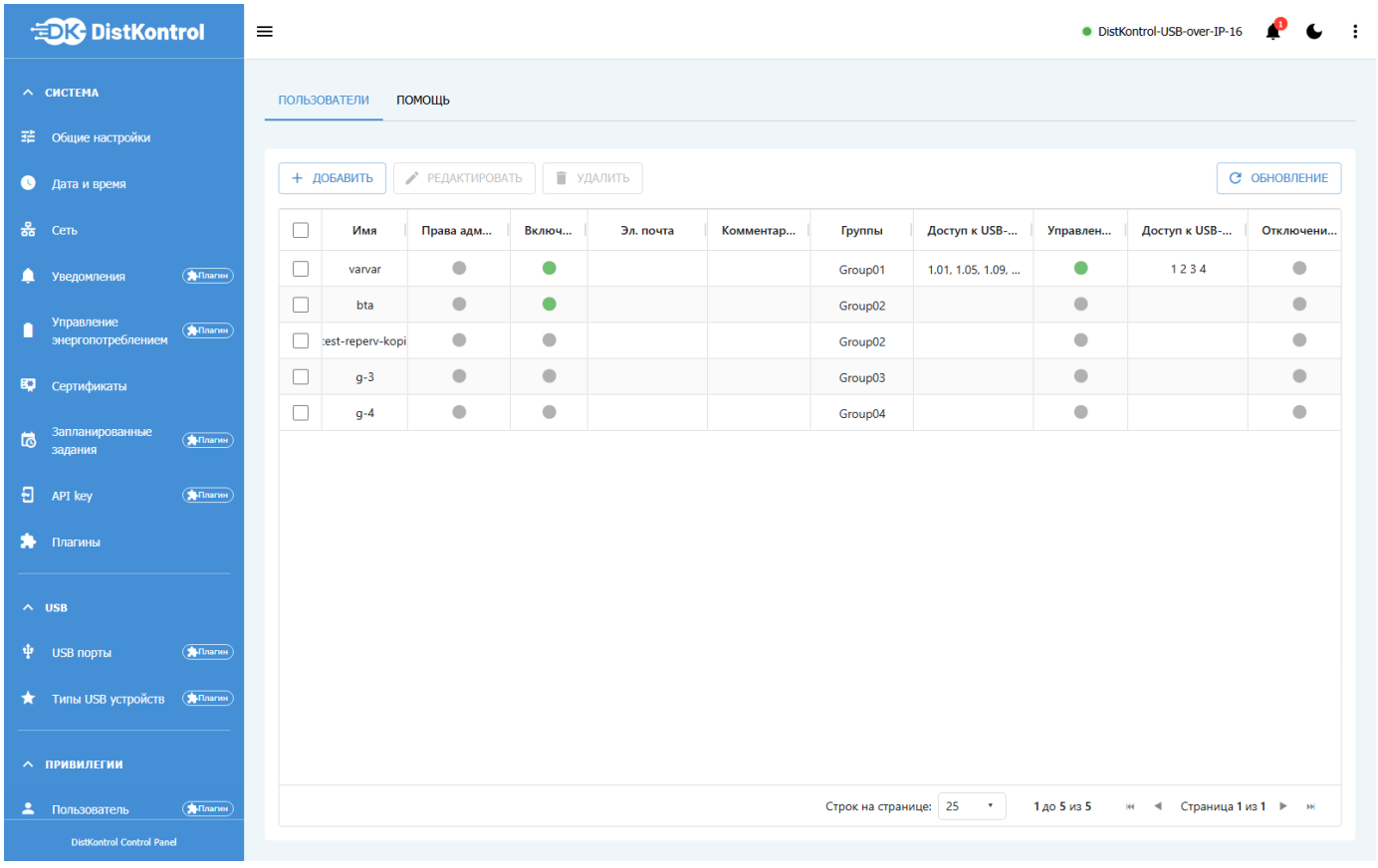
Раздел **«Привилегии»** (пользователи, группы, IP-адреса) и связанные настройки доступа доступны при установленном плагине `distkontrol-overip`. Установка — в 5.2.5 Плагины и в руководстве по плагинам.

5.4.1 Пользователь

Для корректной настройки групп, ограниченного предоставления прав на включение и отключение USB-устройств необходимо на странице «**Управление правами доступа**» — «**Пользователь**» создать пользователей управляемого USB over IP концентратора,
активировать, дать доступ к необходимым портам и устройствам и добавить в группу.

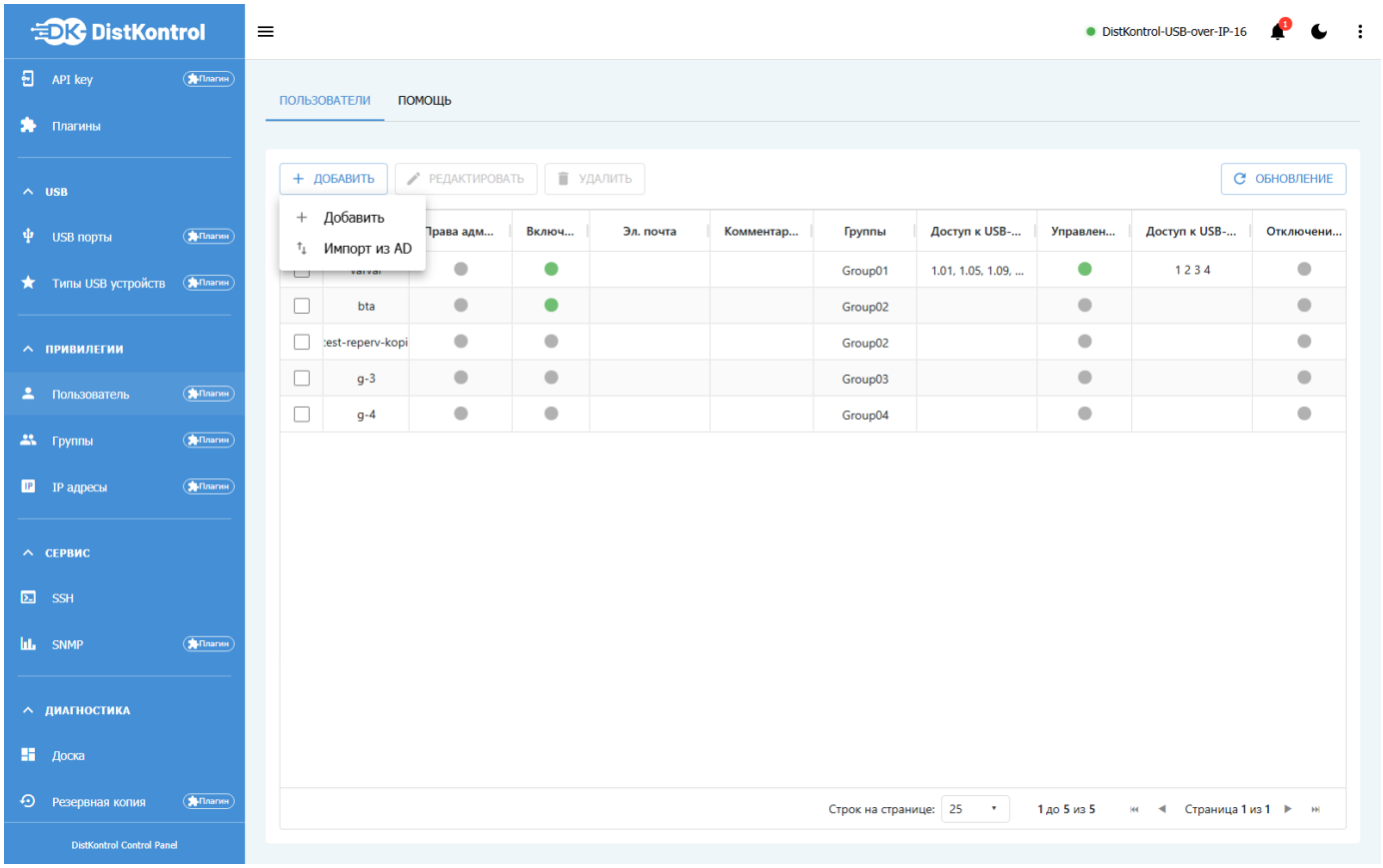
Внимание!

- Имя пользователя может быть введено только на латинской раскладке.
- Регистр имеет значение!
- В пароле пользователя заблокировано использование запятой.



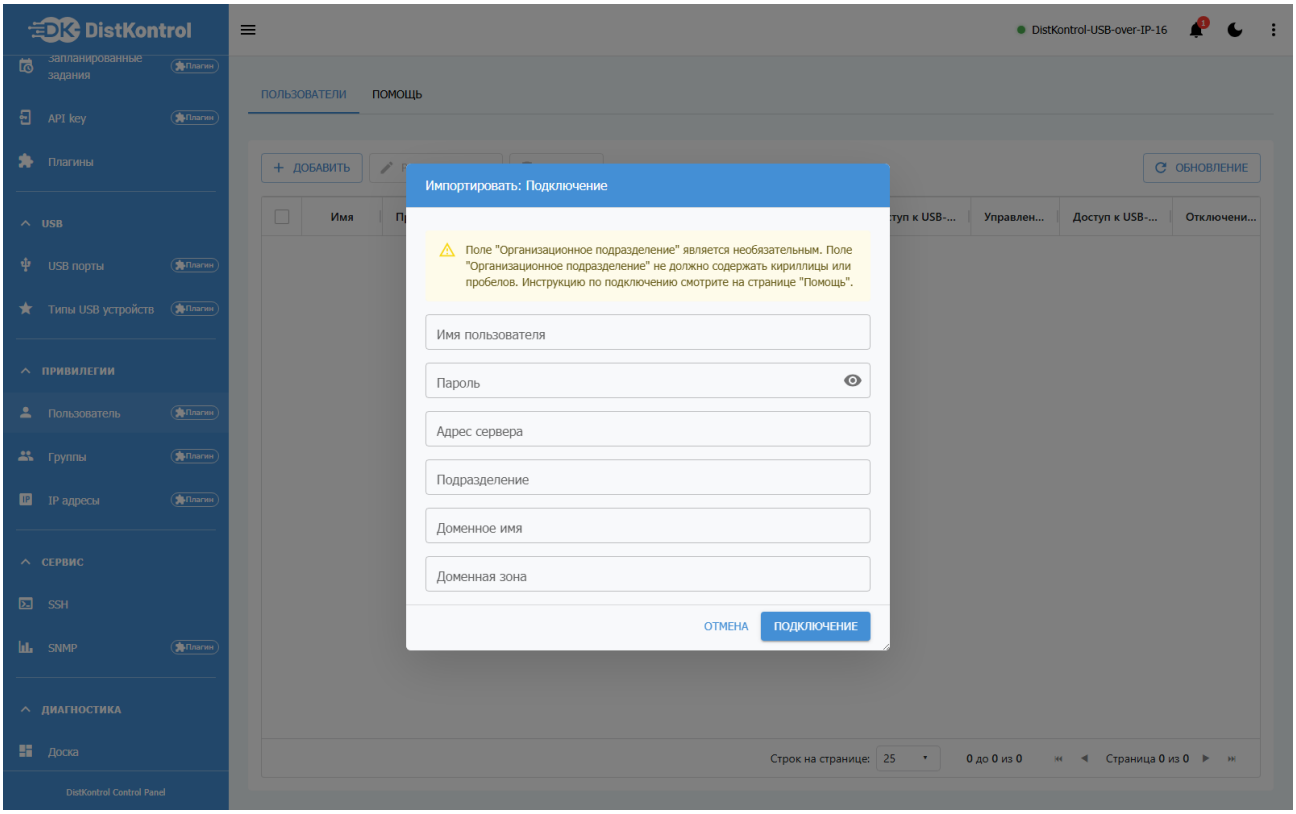
При входе в WEB-интерфейс управляемого USB over IP концентратора под правами созданных пользователей им доступно только управление разрешенными входами (портами) USB, изменение пароля и адреса электронной почты для отправки уведомлений. Возможность изменения данных пользователя может быть отключена в настройках.

Для управления (включения и выключения) USB входов DistKontrolUSB пользователю доступны только входы, назначенные его группам и в WEB-интерфейсе пользователя на странице «USB порты» будут отображены только те входы, к которым пользователю предоставлены права на управление. См. раздел настройки ограничений доступа.



Импорт пользователей из Active Directory (AD).

1. **Подключение:**



- Введите корректные данные для подключения к вашему AD.
- **Имя пользователя** — пользователь должен иметь доступ к получению списка пользователей.
- **Пароль** — пароль пользователя в AD.
- **Адрес сервера** — IP адрес сервера AD.
- **Подразделение** — подразделение в AD из которой будут выгружены имена пользователей.
    - Поле "Подразделение" является необязательным.
    - Поле "Подразделение" не должно содержать кириллических символов или пробелов.
- **Доменное имя** — имя домена вашей сети, например, "myad".
- **Доменная зона** — зона вашей сети, например, "com" или "local".
    - Доменные имя и зона будут выглядеть как "myad.local".
    - В случае использования домена 3-го уровня, (Например: “myad.ad.com”) для корректной
      работы необходимо ввести “myad.ad” в Доменное имя.
- Нажмите кнопку "Подключение" для перехода к следующему шагу.
- Если вы ввели некорректные данные, вы получите соответствующее уведомление системы.

2. **Выбор пользователей:**

- Выберите из списка тех пользователей, которых необходимо добавить.
- Добавленные пользователи будут иметь случайные пароли.
- У пользователей будут настройки по умолчанию.

- Нажмите кнопку "Импортировать" для перехода к следующему шагу.
- Применять настройки необходимо по завершению следующего шага.

3. **Редактирование пользователей:*
4.
   - Нажмите на кнопку "Обновление" для получения актуального списка пользователей.
   - Отредактируйте всех добавленных пользователей.
   - Задайте корректный пароль.
   - Назначьте необходимые права.
   - Примените настройки.
   - (Желтое всплывающее окно в верхней части экрана).

5.4.1.1 Отключение подключенного пользователя

Отключение подключенных пользователей к USB-устройству может осуществляться несколькими способами:

- Путем отключения питания с определенного USB-порта (см. «USB порты», «Утилита USBControl»)
- Предоставлением прав пользователю на отключение других пользователей (требуется запуск клиентского приложения с параметром `-a` см. «Дополнительные возможности при работе с клиентским приложением»)
- Предоставлением прав IP-адресу на отключение других пользователей (требуется запуск клиентского приложения с параметром `-a` см. «Дополнительные возможности при работе с клиентским приложением»)

> **Внимание!**
> Имя пользователя, введённое в WEB-интерфейсе, **ДОЛЖНО СОВПАДАТЬ** с именем учетной записи системы, с которой происходит отключение подключенных к USB-порту пользователей.

Пользователь может выключить питание на к USB-порту или отключать подключённых пользователей, только с тех USB-портов, которые ему назначены в разделе «Пользователи», вкладка «Доступ к USB-портам».

Пример настройки отключения пользователей:

1. В разделе «Пользователи» создаем пользователя, имя которого будет совпадать с именем системы (например, имя моей учетной записи “Petrov”, следовательно, имя пользователя должно быть “Petrov”).
2. Даем пользователю соответствующие права на “управление питанием USB-портов” и “отключение других пользователей”
3. Во вкладке «Доступ к USB-портам» указываем USB-порты, к которым пользователь может подключать USB-устройства, управлять их питанием, а также отключать других пользователей, если те подключились к назначенным USB-портам пользователя “Petrov”.
4. Запустить клиентское приложение Distkontrol Client с параметром запуска –a (см. «Дополнительные возможности при работе с DistKontrolUSB Client»)
5. После чего, в клиентском приложении, можно отключить уже подключенных пользователей.

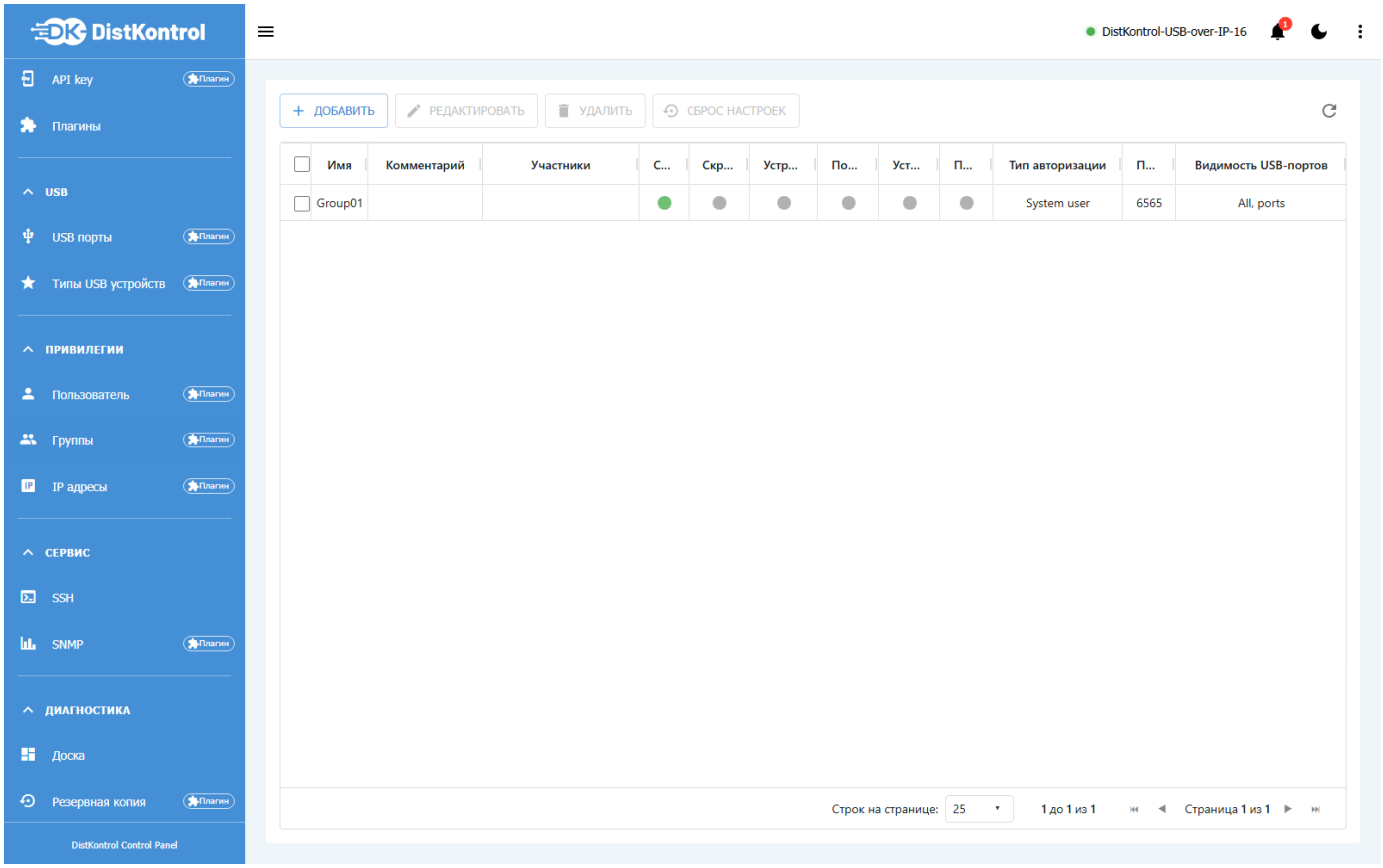
5.4.2 IP адрес

Данный раздел необходим для настройки прав доступа, более подробно см. «Настройки доступа».

IP можно добавлять, редактировать, удалять. При создании, редактировании устройства выберите семейство IP (IPv4 или IPv6).

5.4.3 Группы

Данный раздел необходим для настройки групп USB портов. Существует 16 групп, в которые можно добавить пользователей, настроить права доступа для группы, настроить видимость USB-портов.



В данном разделе для пользователя возможно настроить отображение только доступных ему USB-портов. Для этого:

1. Необходимо создать SSL-сертификат для трафика USB-устройств и добавить его в группу (см. 5.2.4 Сертификаты).
2. Скачать данный сертификат и добавить в DistKontrolUSB Client.
3. Добавить сервер в DistKontrolUSB Client с указанием SSL порта (по умолчанию для Group1: 6564). Для корректного отображения нескольких групп USB-устройств необходимо добавить все используемые сервера с указанием SSL порта, указанного в настройках группы.
4. В Web-интерфейсе добавить пользователя, активировать его и добавить в группу, к которой у пользователя будет доступ, дать доступ к необходимым устройствам\портам.
5. В разделе «Группы» — открыть настройки группы, перевести ползунки «Включить», «Включение SSL для USB-трафика» в активное состояние.
6. При необходимости установить настройки прав доступа, более подробно см. «Настройки доступа».

7. Включить в список видимости необходимые USB-порты.
8. Сохранить настройки, включить порты.

В случае необходимости разделения USB-устройств между пользователями, настройте другую группу в том же порядке.

Для корректного отображения нескольких групп USB-устройств в DistKontrolUSB Client необходимо добавить все используемые сервера с указанием SSL порта, указанного в настройках группы (по умолчанию Group2:7572, Group3:7573, Group4:7574 и т.д.).

Для сброса настроек — необходимо выбрать нужную группу и сбросить настройки.

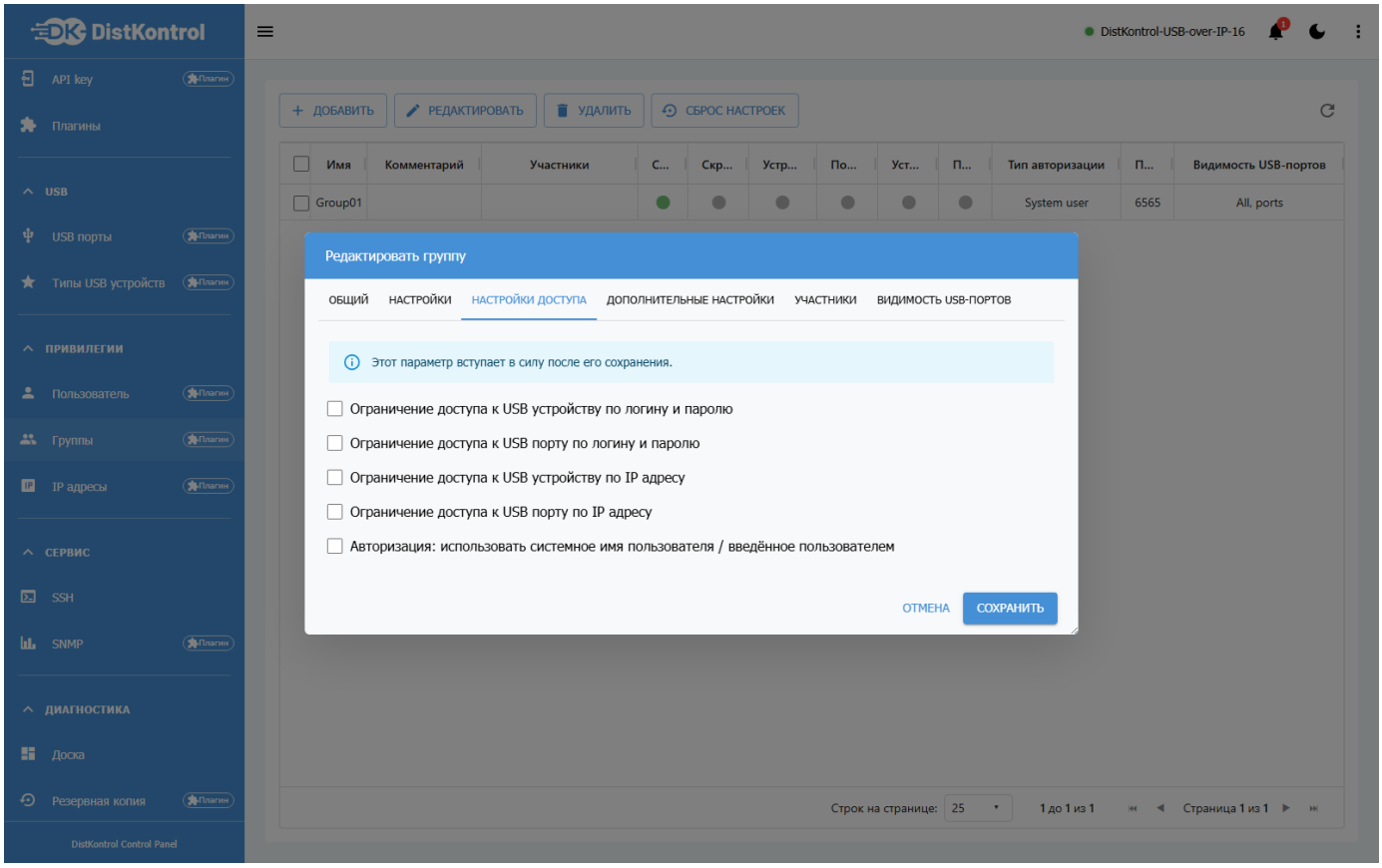
Внимание!

В исходном состоянии все USB-порты будут добавлены в "Group1". Для того чтобы увидеть порты в другой группе, необходимо в первой группе назначить только необходимые порты. Оставшиеся порты станут доступны в других группах. В случае необходимости настроить для каждого устройства доступ определенным пользователям видимость всех портов необходимо оставить в "Group1".Создать пользователей, разграничить права на доступ к определенным устройствам портам, добавить всех пользователей в группу, включить ограничения в настройках группы.

5.4.3.1 Настройки доступа

В управляемом USB over IP концентраторе реализована возможность ограничения доступа пользователей к подключаемым USB-устройствам и портам (авторизация для доступа к USB устройствам и/или портам). Предусмотрены четыре способа ограничения:

1. Ограничение доступа к USB-устройству по логину и паролю (авторизация по логину и паролю для доступа к USB-устройству).
2. Ограничение доступа к USB-порту по логину и паролю (авторизация по логину и паролю для доступа к USB-порту).
3. Ограничение доступа к USB-устройству по IP адресу (авторизация по IP адресу).
4. Ограничение доступа к USB-порту по IP адресу (авторизация по IP адресу для доступа к USB-порту).



Режимы ограничения включаются на странице WEB-интерфейса странице «Управление правами доступа» — «Группы» — «Настройки доступа». По умолчанию все способы авторизации отключены. Для включения ограничения доступа пользователей к подключаемым USB-устройствам необходимо нажать соответствующую кнопку интерфейса.

Режимы ограничения доступа пользователей к USB-устройствам (авторизация для доступа к USB-устройствам) могут использоваться как независимо друг от друга, так и совместно в целях повышения безопасности использования USB-устройств.

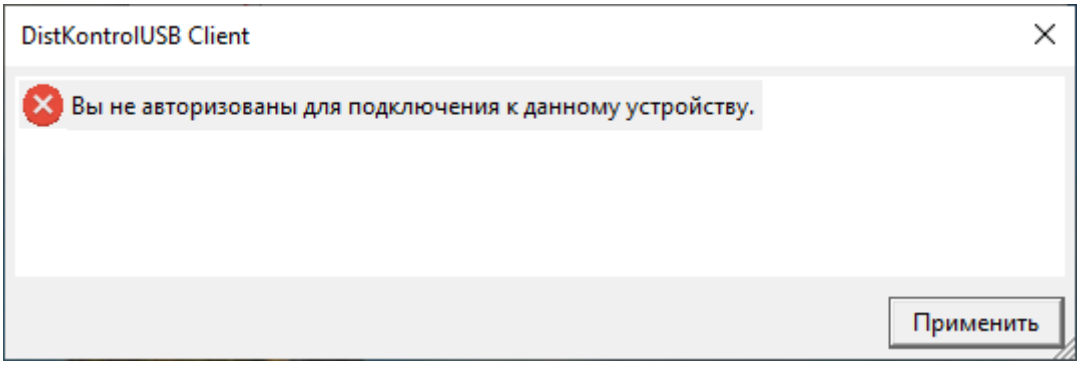
Внимание!

Настройки доступа настраиваются для каждой группы отдельно.

Внимание!

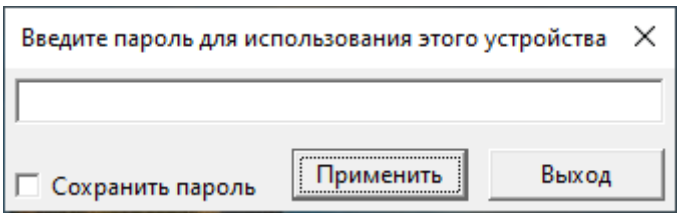
При совместном использовании правила применяются через «И». Для предоставления доступа к устройству должны будут выполняться все включенные правила. Настройку правил доступа рекомендуется выполнять по одному правилу, после чего включать совместные режимы ограничения.

При попытке подключения USB-устройства, в отсутствии на это прав, пользователю будет выведено соответствующее сообщение:



5.4.3.1.1 Ограничение доступа к USB-устройству по логину и паролю

При включенном ограничении доступа к USB-устройству по логину и паролю – при подключении к USB-устройству, пользователю будет предложено ввести пароль для доступа к устройству USB (не порту управляемого USB over IP концентратора, а именно USB-устройству, не зависимо от того в какой порт оно подключено). Логин при подключении используется системный (имя текущего пользователя компьютера, с которого производится подключение к USB-устройству) и вводить его при подключении не нужно.

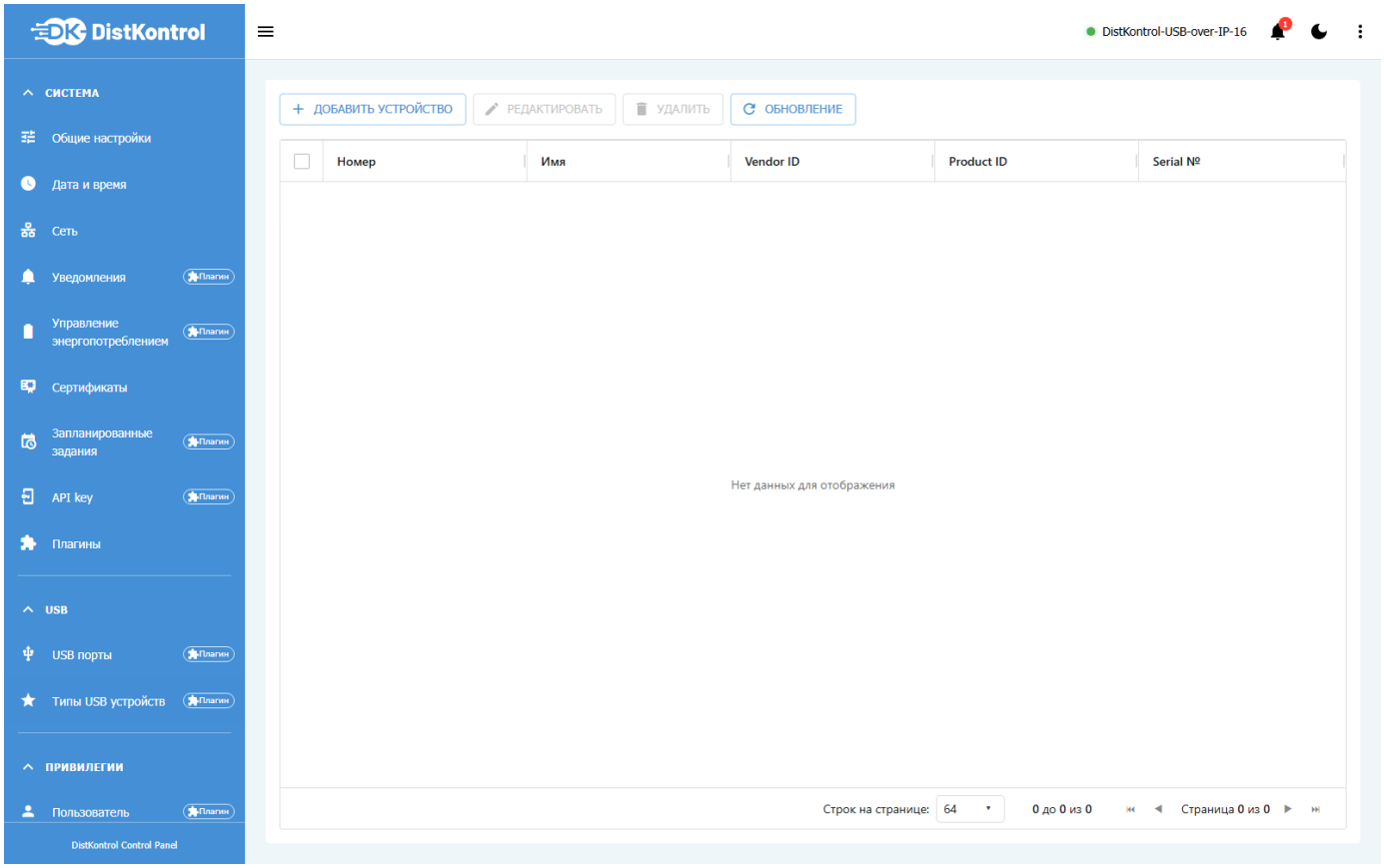


При правильном вводе пароля устройство USB будет подключено к компьютеру пользователя и до перезапуска клиента. Ввод пароля больше не потребуется даже при отключении и повторном подключении к устройству.

При подключении к USB-устройству (порту), при запросе пароля, можно выбрать «Save Password», пароль пользователя будет сохранен, и при последующих запусках приложения его ввод не потребуется. В случае, если пароль пользователя будет изменен, то необходимо вначале удалить запомненный пароль из файла настроек пользователя, и при следующем запросе пароля – ввести новый. Для удаления запомненного пароля необходимо закрыть приложение (не свернуть, что является действием по умолчанию при нажатии на крестик в правом верхнем углу интерфейса программы). Внести изменения в файл настроек клиентского приложения см. п. «Настройка клиентского приложения» (можно просто удалить файл настроек, для сброса всех настроек клиентского приложения к исходным).

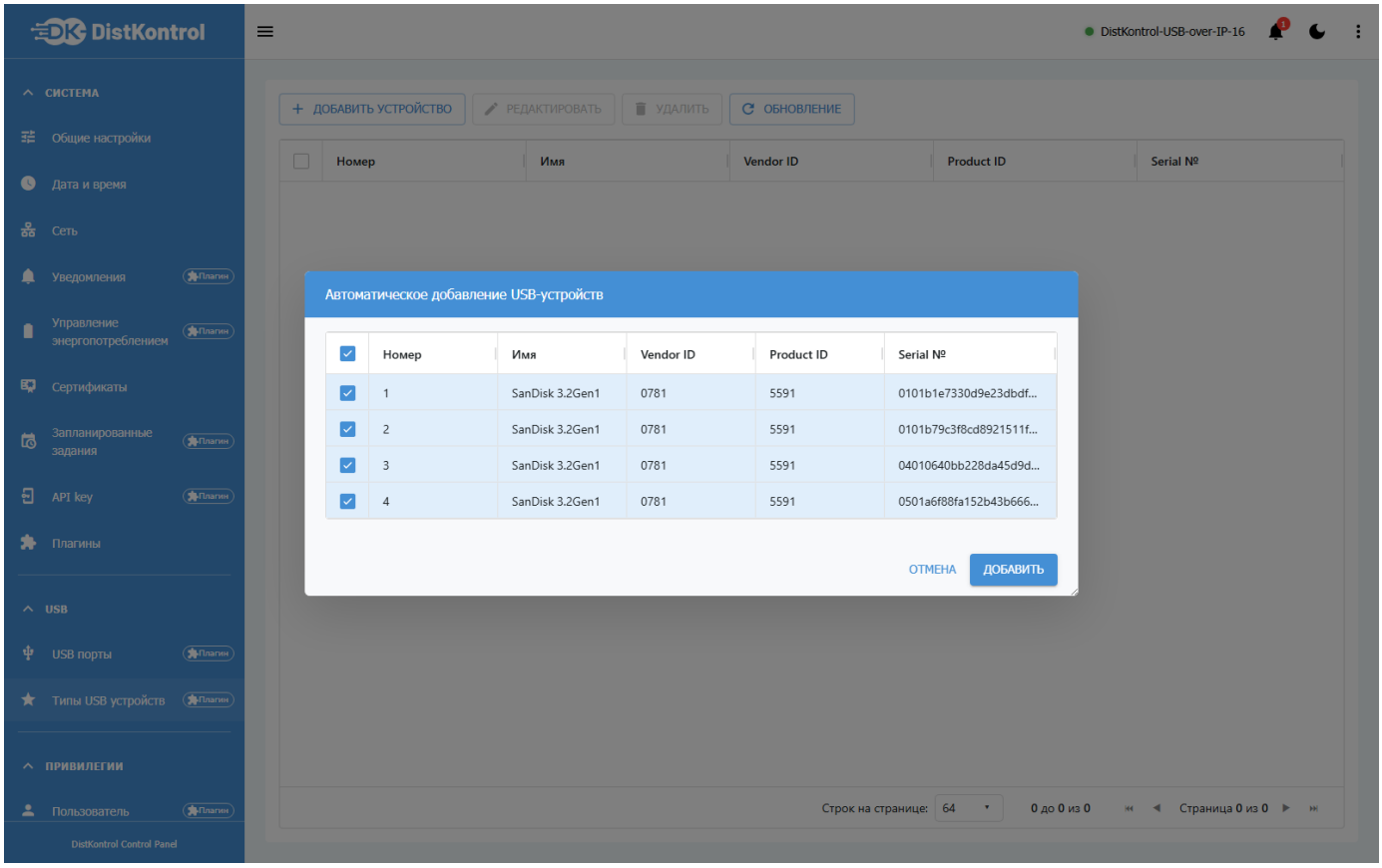
Для настройки режима ограничения доступа к USB-устройству по логину и паролю необходимо:

1 На странице WEB-интерфейса администратора «USB» — «Типы USB-устройств» добавить ВСЕ USB-устройства, которые будут использоваться. Устройство работает по принципу: «Запрещено все, что явно неразрешено».



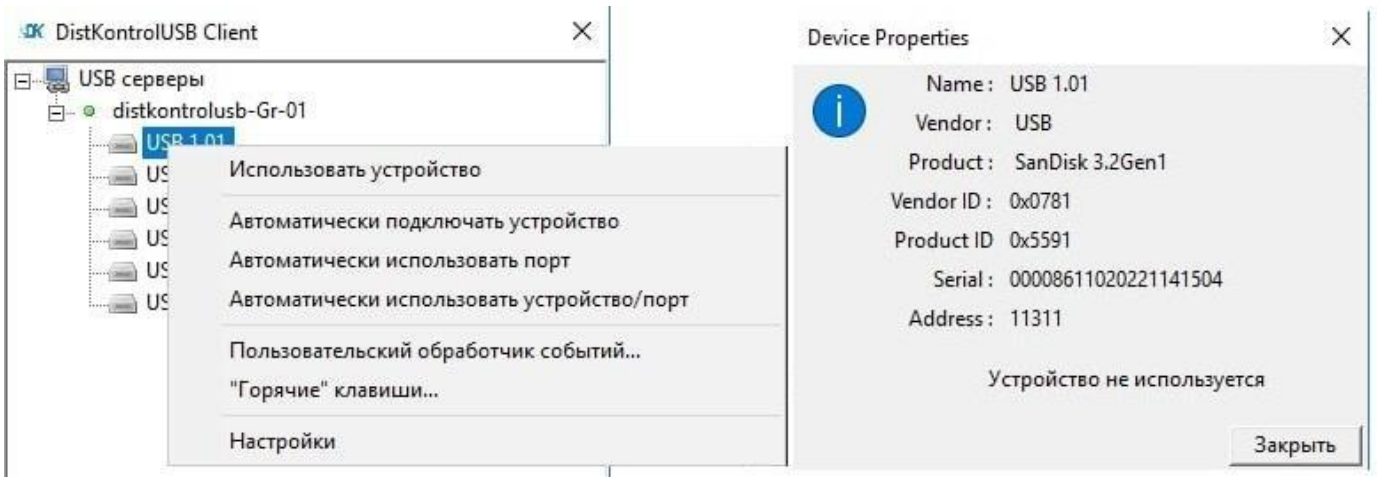
USB-устройства можно добавить:

1.1 Из автоматически генерируемого списка подключенных к концентратору USB-устройств (включенных на странице «USB входы»). «Добавить устройства» — «Автопоиск». В списке выбрать добавляемые USB устройства и нажать кнопку «Сохранить».



Будет выдан отчет о результате добавления USB-устройств в список.

1.2 Вручную:

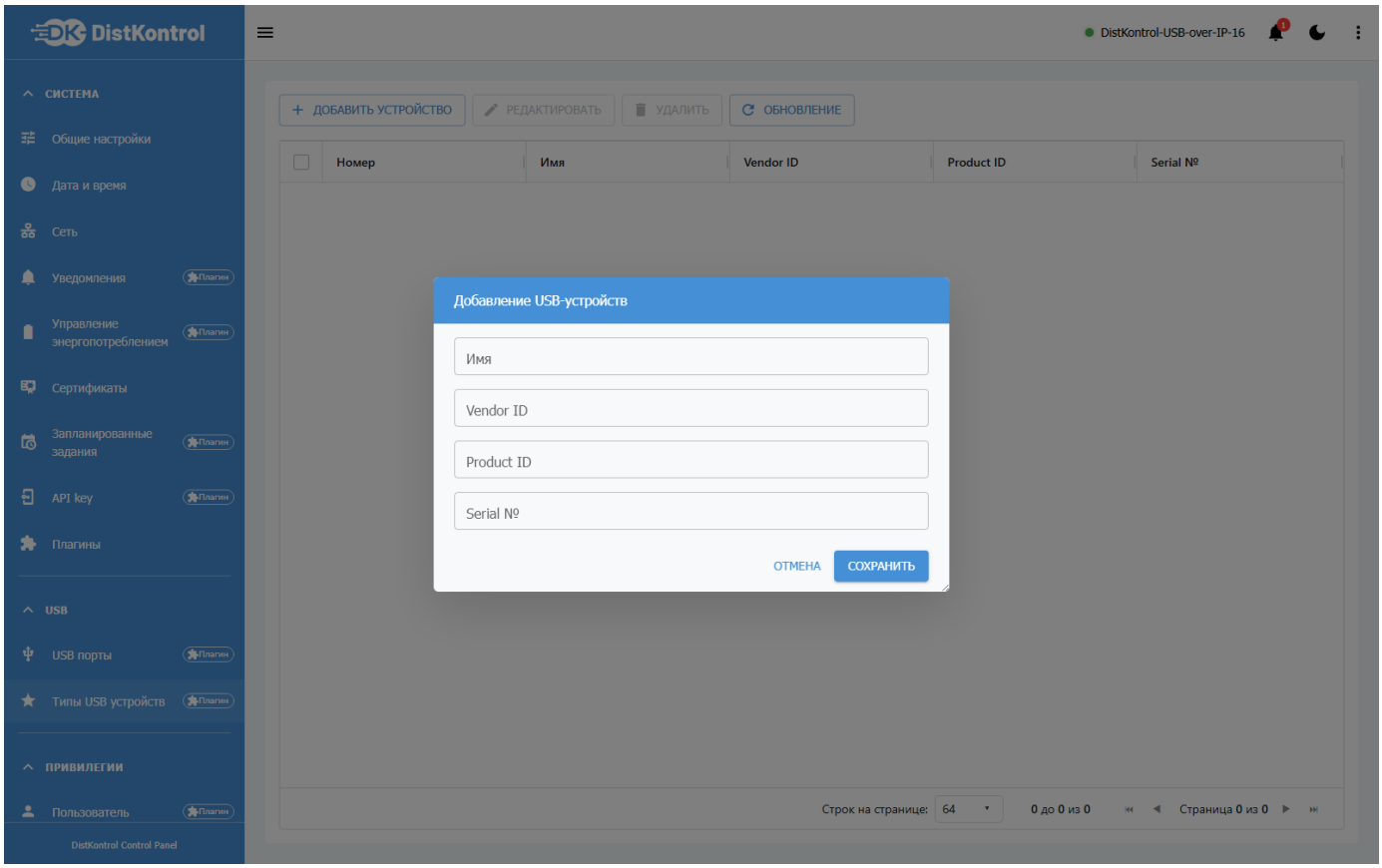


Для добавления USB-устройств вручную, необходимо знать их VendorID, ProductID и Serial №. Их можно посмотреть в клиенте или на странице WEB-интерфейса администратора «Диагностика» — «Системные журналы» в стоке вида:

```
`Sep 25 22:56:28 USBoverIP64: Authorizing parameters -> '8564' '1000' Ivanov (Ivanov)' '192.168.1.5' '05KVOF66TU4IHDTZ' "`
```

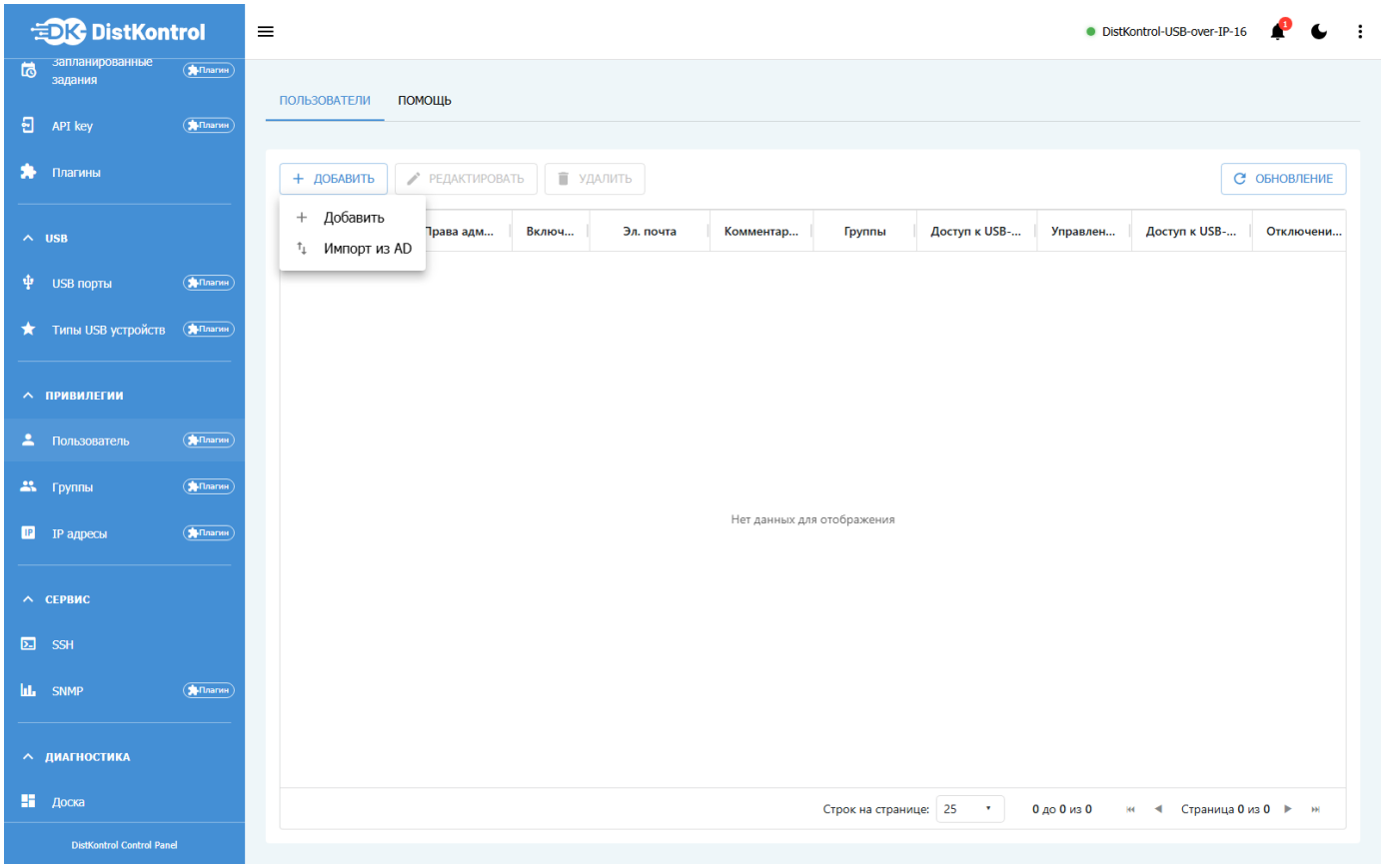
- **VendorID** - 8564
- **ProductID** – 1000

• **Serial №.** - '05KVOF66TU4IHDTZ'
VendorID и ProductID и Serial № должны содержать только цифры и латинские буквы.
«Добавить устройства» — «Добавить вручную».



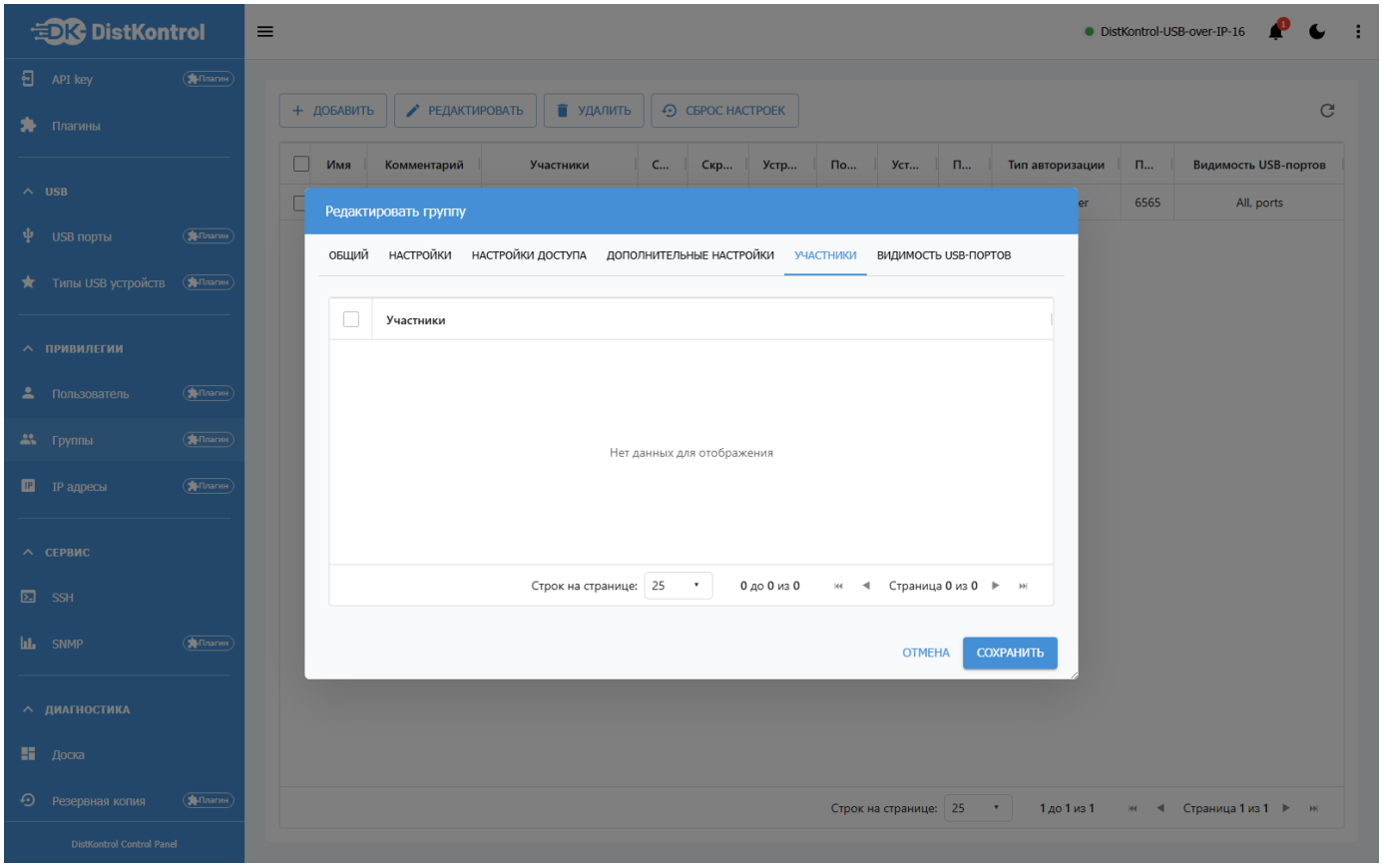
В дальнейшем возможно удаление и редактирование информации о USB-устройстве:

2 На странице «Управление правами доступа» — «Пользователь» добавить пользователей.



Имена пользователей должны СОВПАДАТЬ с системным именем пользователя (имя текущего пользователя компьютера, с которого производится подключение к USB-устройству). При необходимости его так же можно посмотреть (после попытки подключения к USB-устройству) в системном журнале. См. пример выше. Email и пароль пользователя – любые. Рекомендуется использовать сложные пароли.

3 В диалоге редактирования группы на вкладке «Участники» добавьте пользователя в настраиваемую группу. Назначьте пользователю необходимые USB-устройства на вкладке «Доступ к USB-устройствам» в карточке пользователя. Нажмите **«Сохранить»**.



4 Настроить в группе видимость необходимых портов. При назначении прав пользователю будет доступно подключение USB-устройств (к которым был назначен доступ при создании) в видимых портах. Если ни одного устройства не назначено, пользователь получит соответствующие уведомление об отсутствии прав на управление портами.

При подключении USB-устройств пользователю будут доступны для подключения только назначенные ему устройства. При попытке подключения USB-устройств, не назначенных пользователю, в клиентском приложении будет выдаваться сообщение об отсутствии прав доступа к USB-устройству.

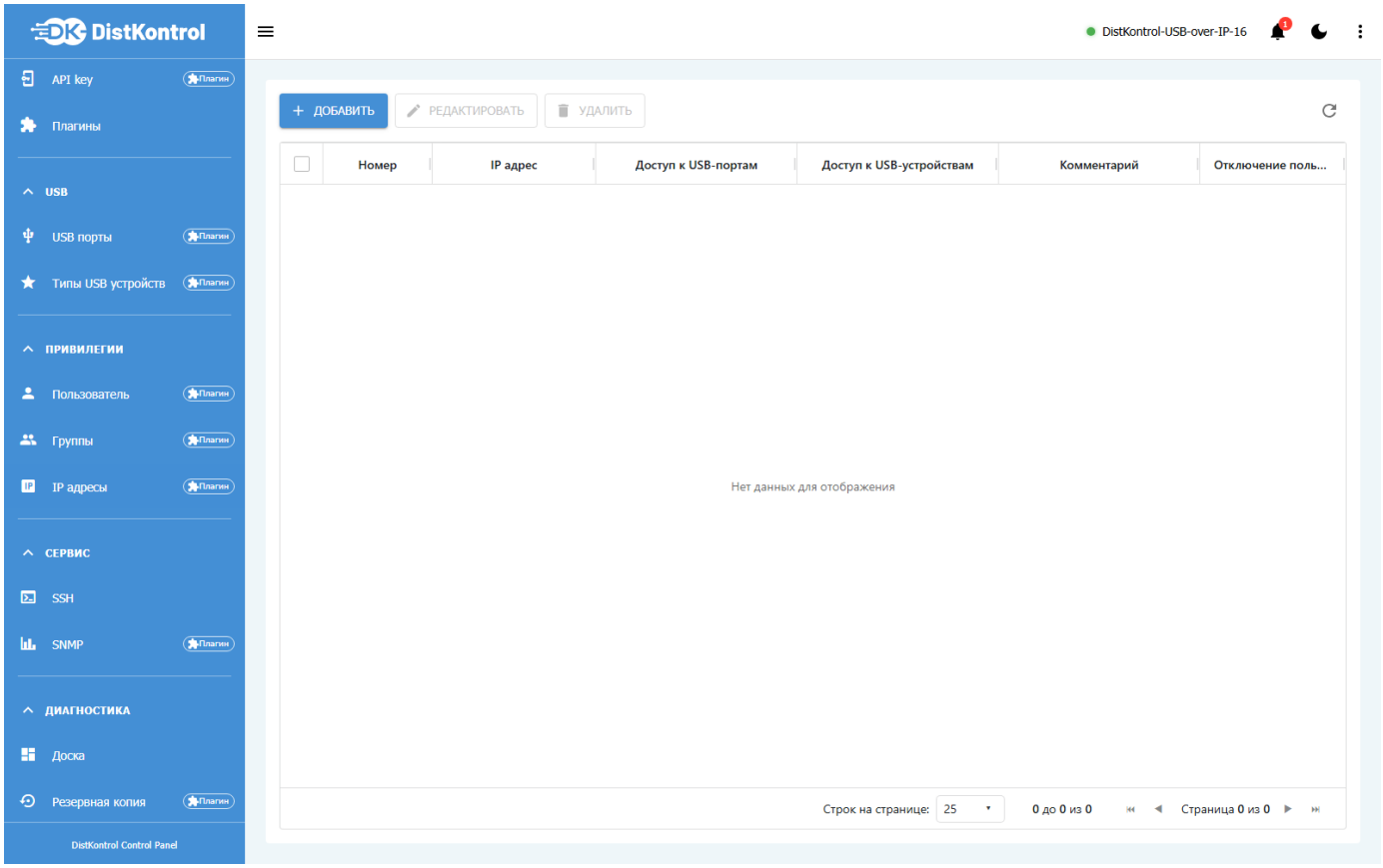
5.4.3.1.2 Ограничение доступа к USB-порту по логину и паролю

При включенном ограничении доступа к USB порту по логину и паролю – при подключении к USB порту, пользователю будет предложено ввести пароль для доступа к USB порту. Логин при подключении используется системный (имя текущего пользователя компьютера, с которого производится подключение к USB-устройству) и вводить его при подключении не нужно. Не зависимо от того какое устройство USB подключено к порту, если пользователю разрешено использовать USB порт, ему будет предоставлен доступ к USB-устройству.

Настройка прав доступа к устройству подробно описана предыдущем параграфе.

5.4.3.1.3 Ограничение доступа к USB-устройству по ip адресу

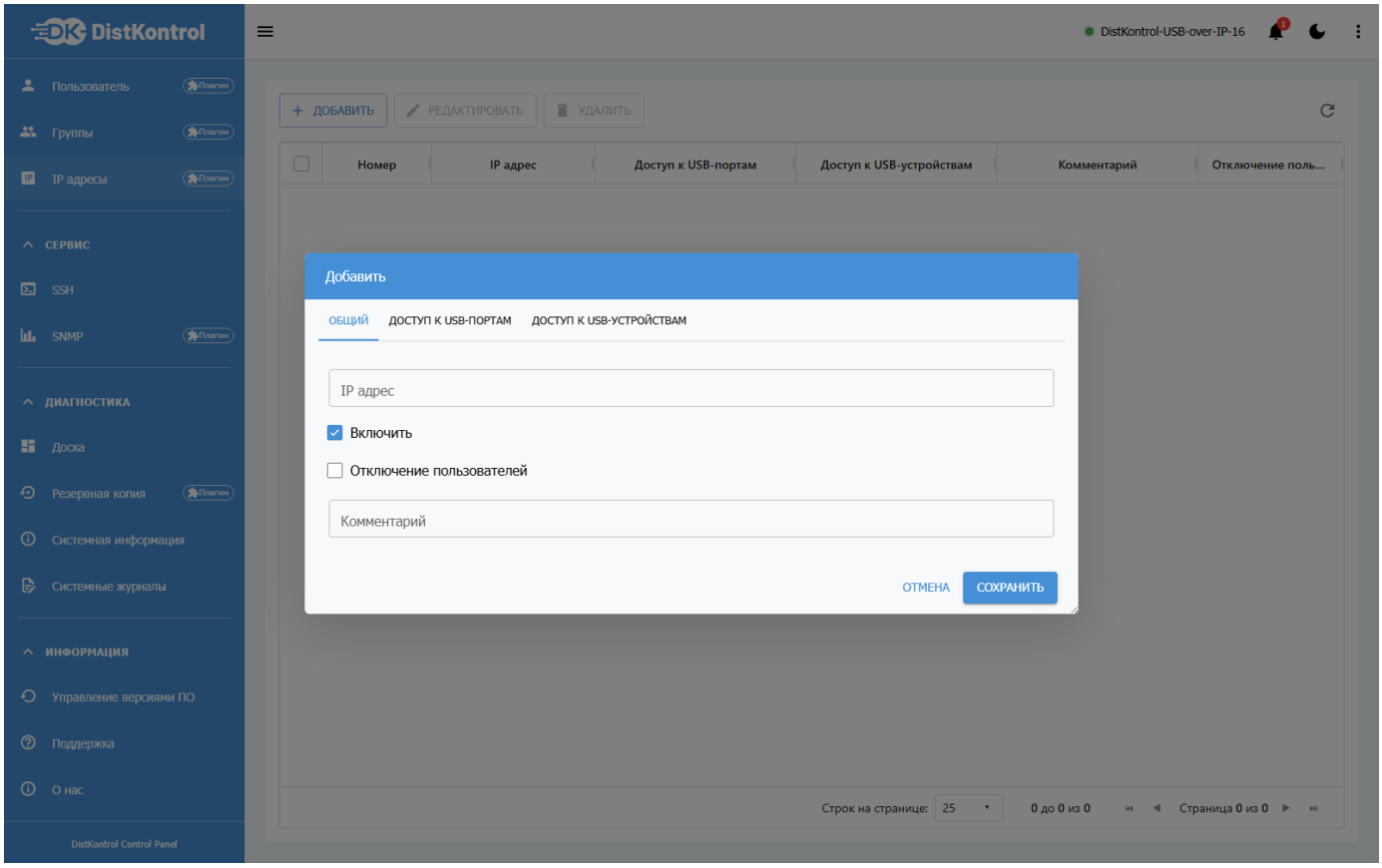
При включенном ограничении доступа к USB-устройству по IP адресу – подключение пользователем USB-устройства будет возможно только с IP адреса с правом доступа к устройству USB (не порту управляемого USB over IP концентратора, а именно USB-устройству, не зависимо от того в какой порт оно подключено).



Для настройки режима необходимо:

На странице WEB-интерфейса администратора «Управление правами доступа» — «IP адреса» добавить ВСЕ IP адреса, которые будут использоваться. Устройство работает по принципу: «Запрещено все, что явно не разрешено».
Возможно добавление и удаление информации. При добавлении необходимо назначить все необходимые права во вкладках «Доступ к USB портам», «Доступ к USB-устройству». Редактирование невозможно.

Для ввода доступны IP адреса формата 192.168.1.1. Если необходимо добавить формат IPv6, включите переключатель IPv4/IPv6.



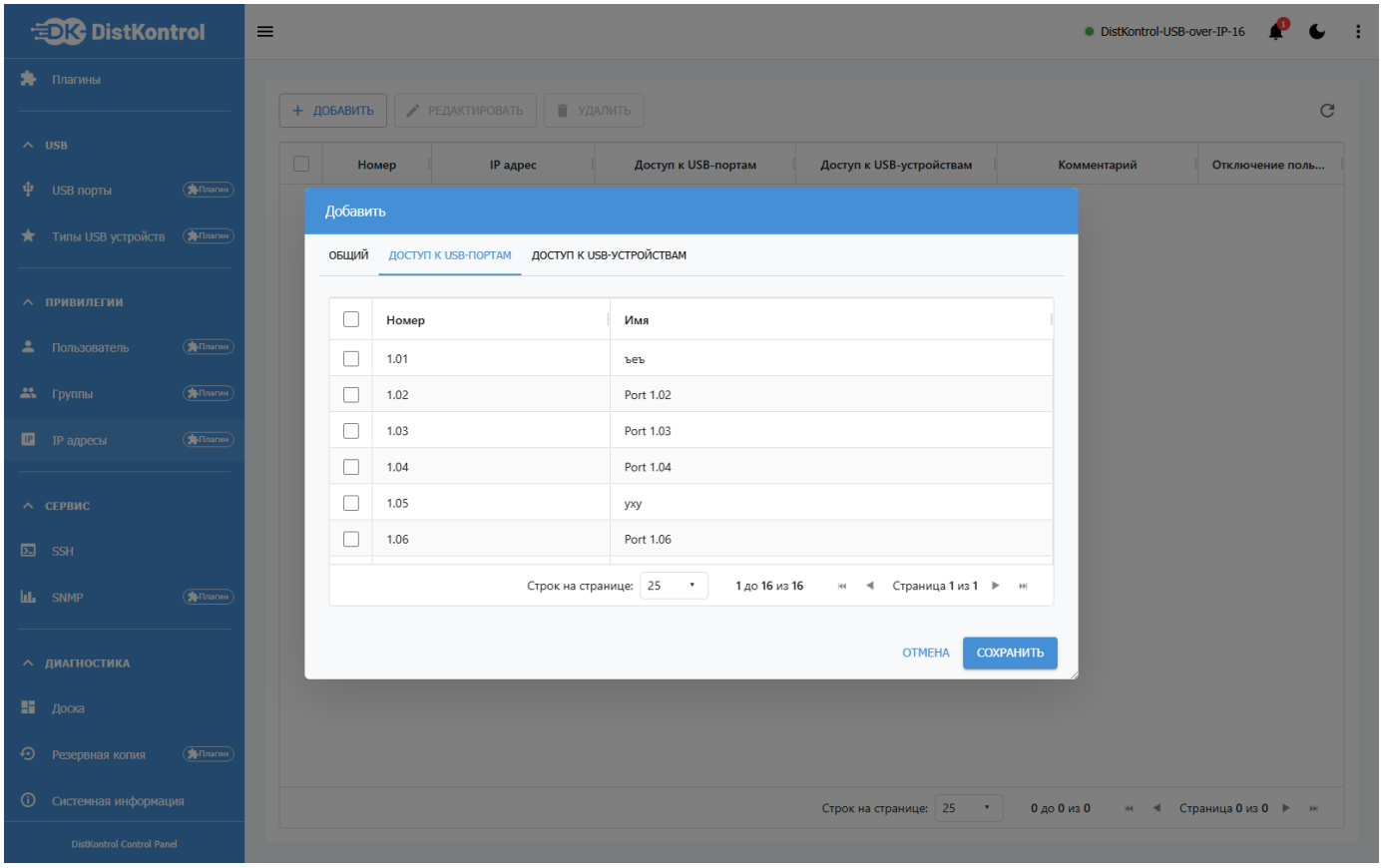
5.4.3.1.4 Ограничение доступа к USB-порту по ip адресу

При включенном ограничении доступа к USB порту по IP адресу – подключение пользователем USB-устройства будет возможно только с IP адреса с правом доступа к порту USB (не USB-устройству, а именно USB порту управляемого USB over IP концентратора, не зависимо от того какое USB устройство к нему подключено).

Для настройки режима необходимо:

На странице WEB-интерфейса администратора «Управление правами доступа» — «IP адреса» добавить ВСЕ IP адреса, которые будут использоваться. Устройство работает по принципу: «Запрещено все, что явно не разрешено».
Возможно добавление и удаление информации. При добавлении необходимо назначить все необходимые права во вкладках «Доступ к USB портам», «Доступ к USB-устройству». Редактирование невозможно.

Для ввода доступны IP адреса формата 192.168.1.1. Если необходимо добавить формат IPv6, включите переключатель IPv4/IPv6.



В вкладке «Доступ к USB-устройствам» необходимо отметить USB-устройства, к которым пользователю будет разрешен.

Аналогично, во вкладке «Доступ к USB портам» отметить USB порты (входы) к которым пользователю будет разрешен.

Для завершения создания нажать на кнопку «Сохранить» в диалоговом окне.

5.4.3.2 Настройки прав

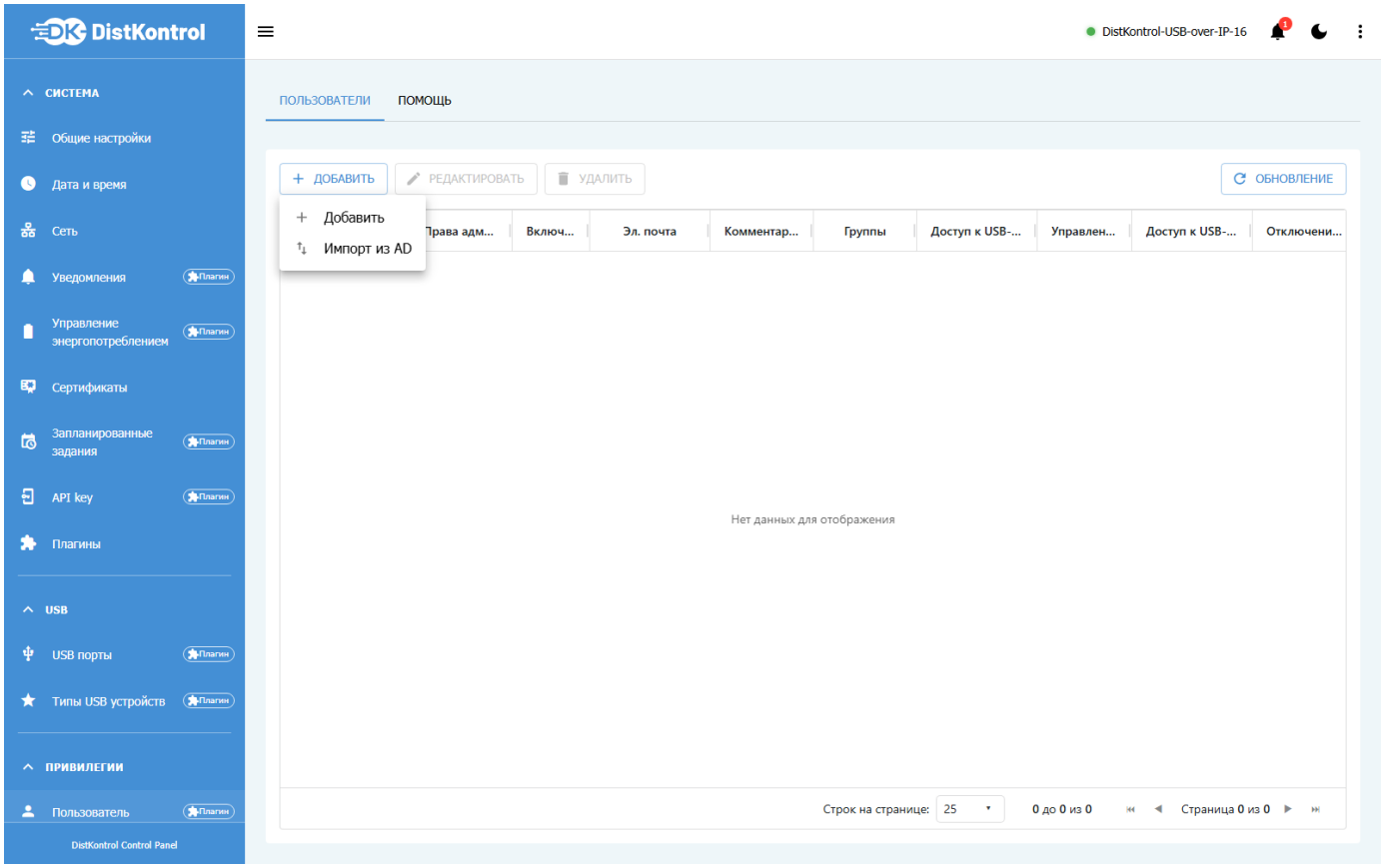
Настройка прав зависит от выбранной настройки доступа.

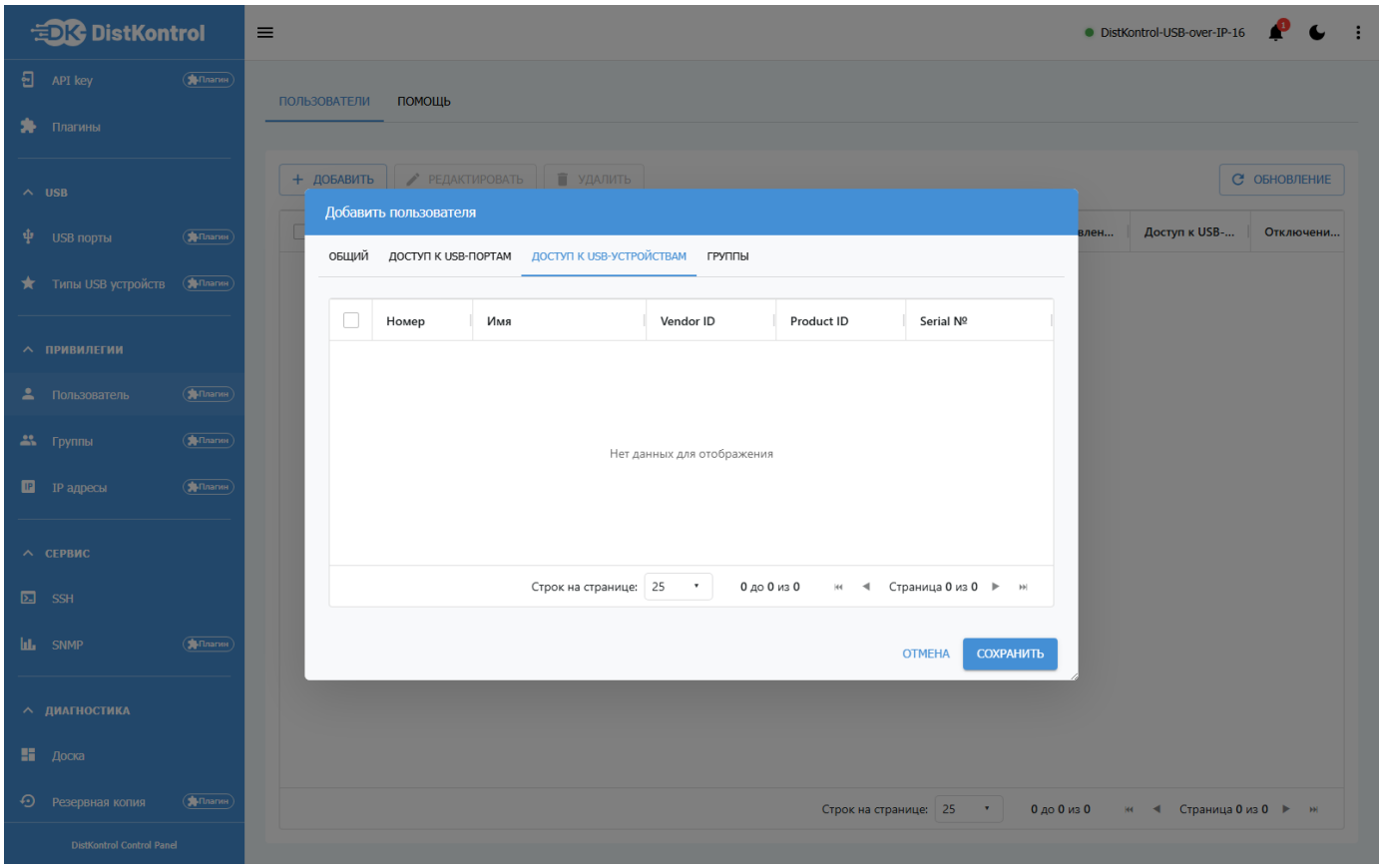
В случае выбора «Ограничение прав по логину и паролю»:

1. Необходимо создать пользователя и назначить ему права.
2. Права пользователю задаются при создании, по умолчанию все права отключены.
3. В интерфейсе все права обозначены зеленым или серым маркером в зависимости от состояния.

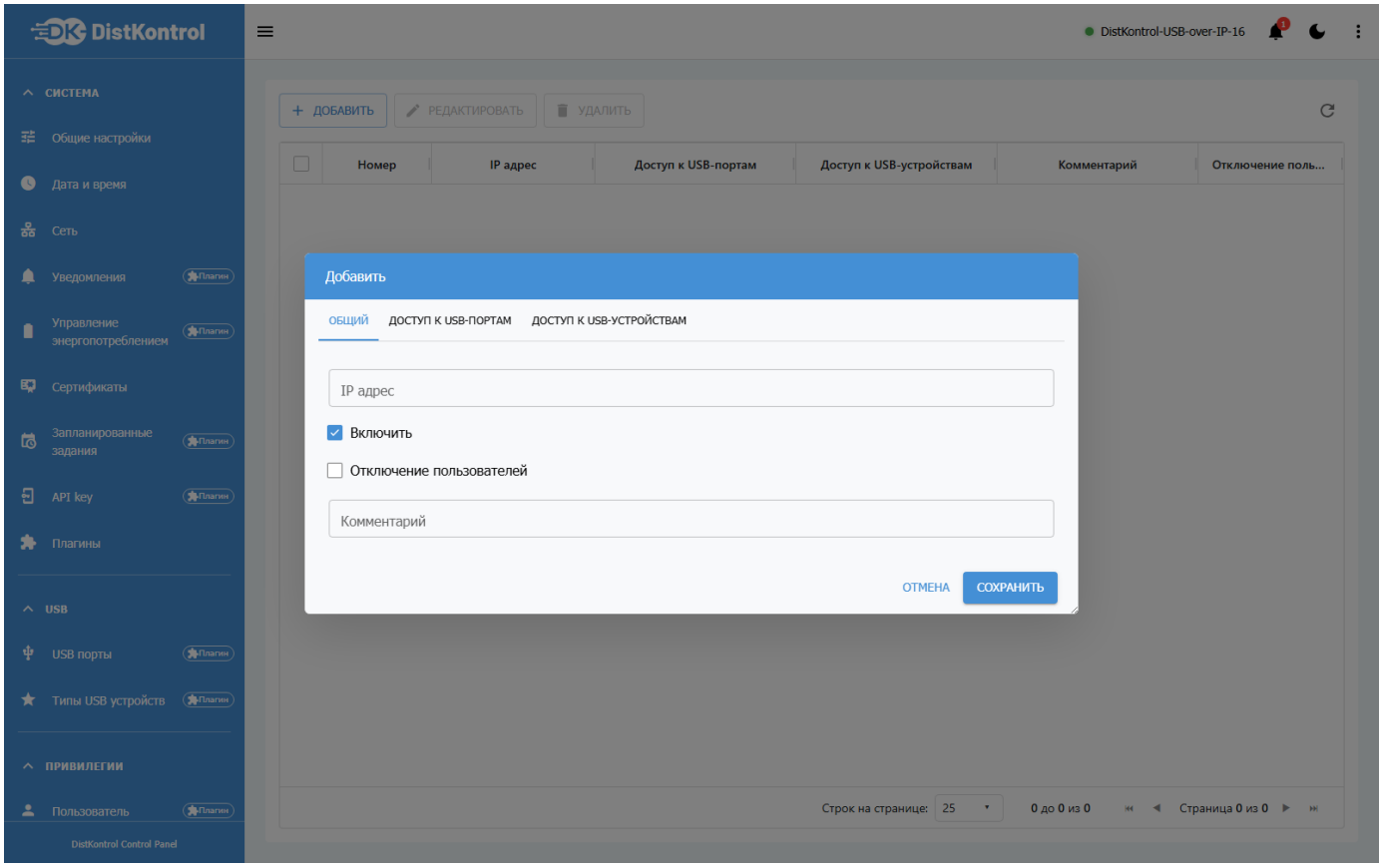
Доступные права для новых пользователей:

- Права администратора Web-интерфейса;
- Назначение пользователя определенной группе;
- Доступ к определенным USB-устройствам;
- Доступ к определенным USB-портам;
- Отключение других пользователей в клиентском приложении DistKontrolUSB Client (при запуске с параметром `-a`).





В случае выбора «Ограничение прав IP адресу»:



1. Необходимо создать IP-адрес и назначить ему права.
2. Возможно задать **только** отключение других пользователей в клиентском приложении DistKontrolUSB Client (при запуске с параметром `-a`).

Примечание:

Разрешения для пользователей и IP-адресов работают по правилу **«ИЛИ»**.

Пример 1:

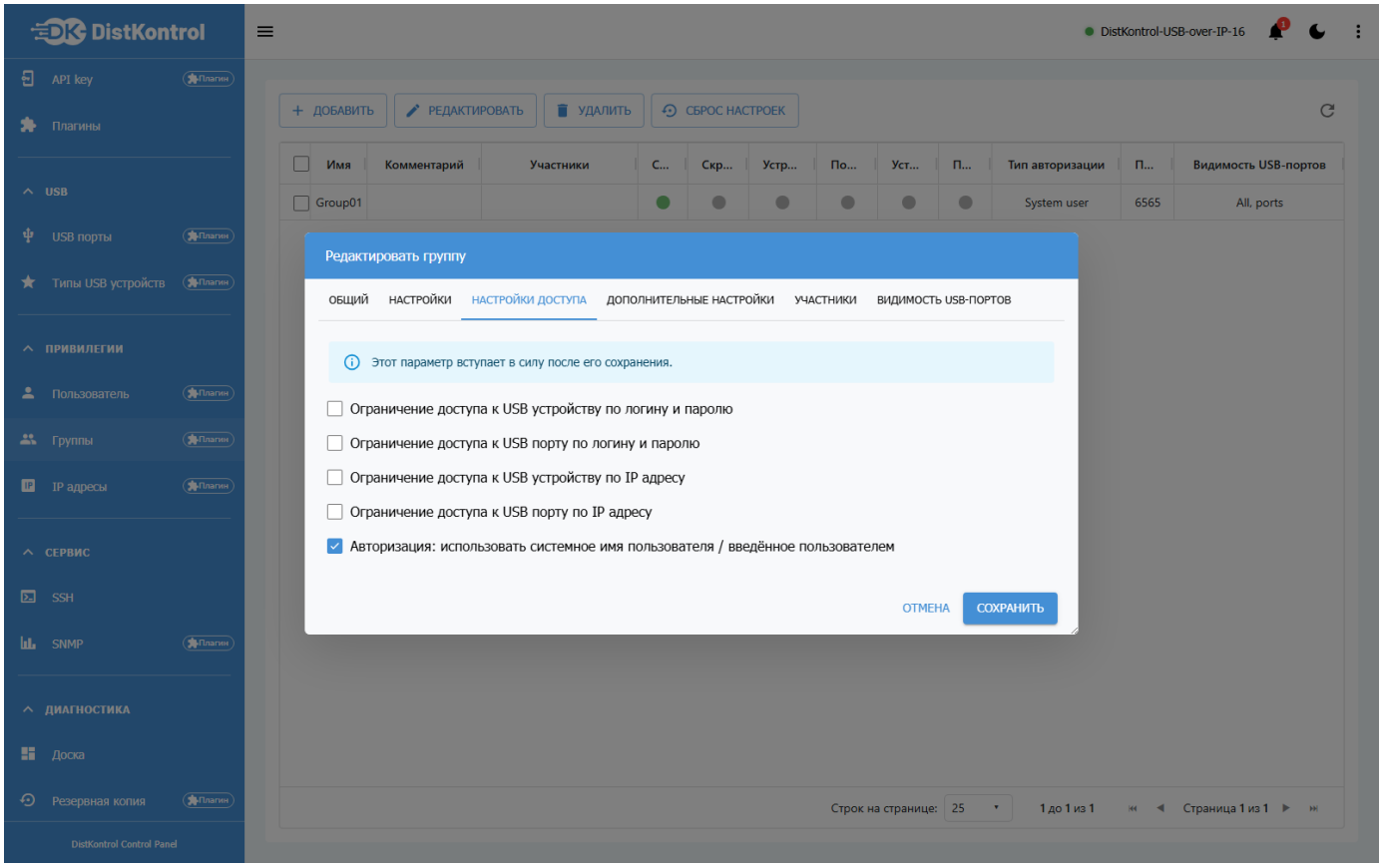
- Пользователю **Ivanov** не разрешили ни одного из правил.
- IP-адресу **192.168.1.10** разрешили отключать другого пользователя.

Результат:

- Пользователь **Ivanov** не сможет изменять имя USB-устройства, если его IP-адрес не будет **192.168.1.10**.
- Любой пользователь с адресом **192.168.1.10** сможет отключать другого пользователя.

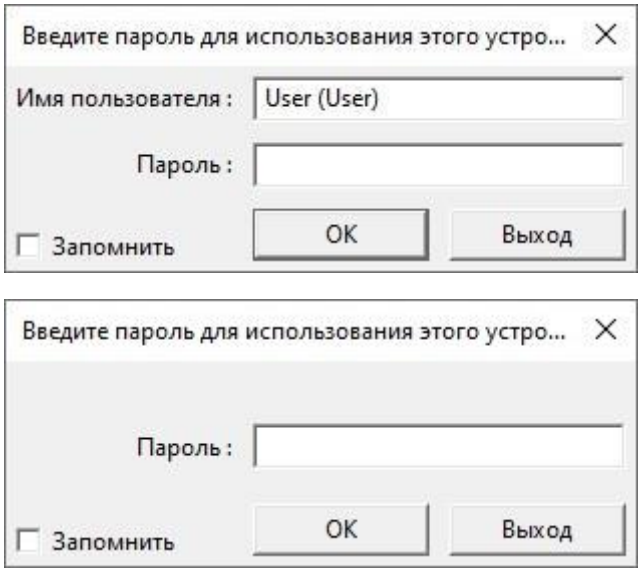
Опция авторизации: использовать системное имя пользователя / введённое пользователем

- По умолчанию: *«Использовать системное имя пользователя»*.
- Окно с запросом пароля будет выводиться только при включенных ограничениях прав доступа по логину и паролю.



При активации опции *«Авторизация: использовать введённое пользователем имя»*:

- Пользователь сможет вводить логин, отличный от системного, во время подключения USB-устройства.



Настройка SSL для трафика USB-устройств и клиентского приложения — в разделе 5.2.4 Сертификаты.

5.5 Сервисы

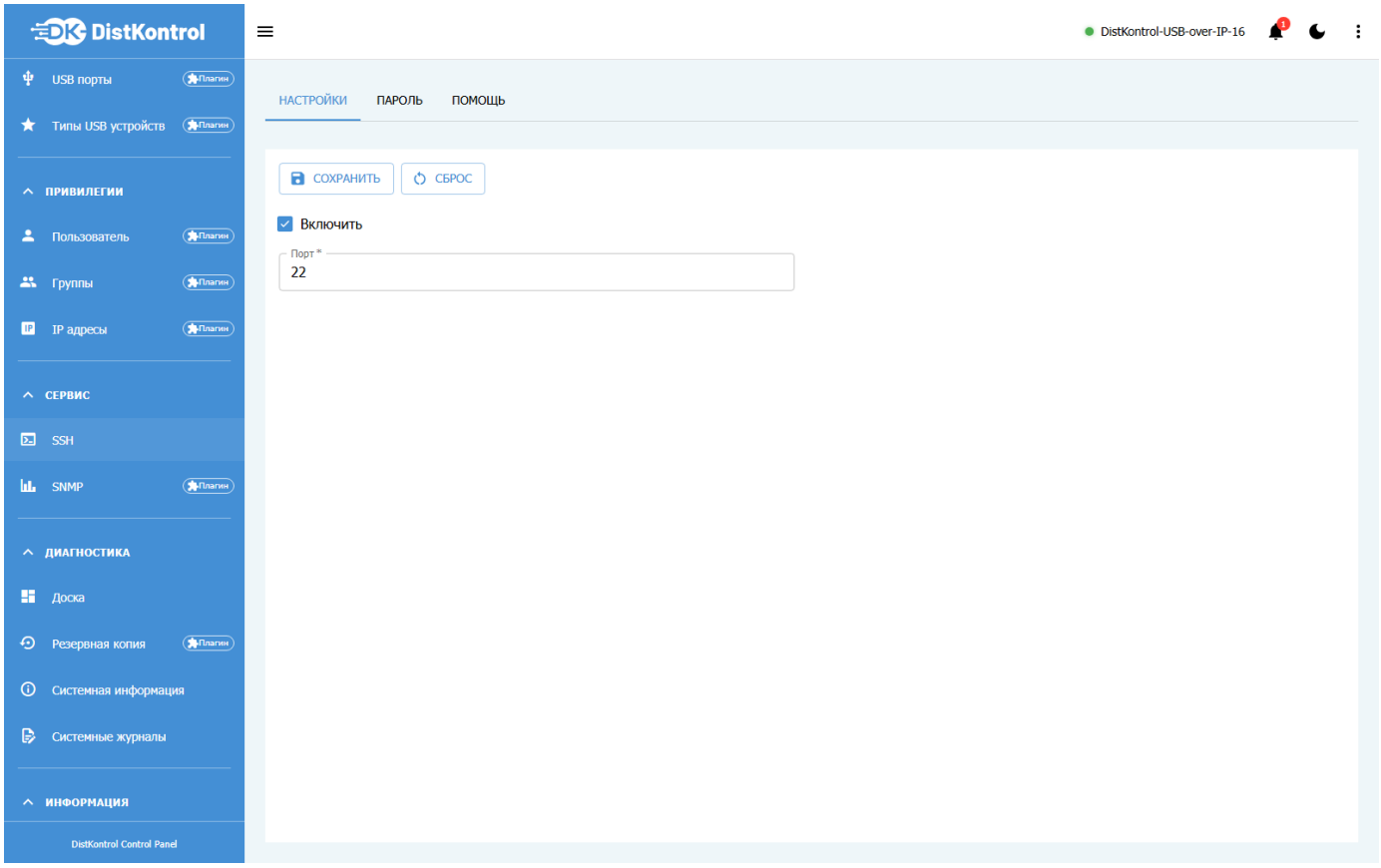
5.5.1 SSH

SSH используется для управления питанием USB-портов и создания (редактирования, удаления) пользователей концентратора. Эти возможности реализованы плагинами `distkontrol-inputs` (управление портами) и `distkontrol-overip` (управление пользователями и правами доступа). Аналогичные действия доступны в WEB-интерфейсе в разделах 5.3.1 USB-порты и 5.4 Управление правами доступа.

Подключение выполняется под служебной учётной записью `usbcontrol`. Перед первым использованием задайте пароль на странице «Сервисы» → «SSH» → «Пароль». Более подробно о клиентской утилите — в разделе «Краткая инструкция по использованию утилиты управления портами».

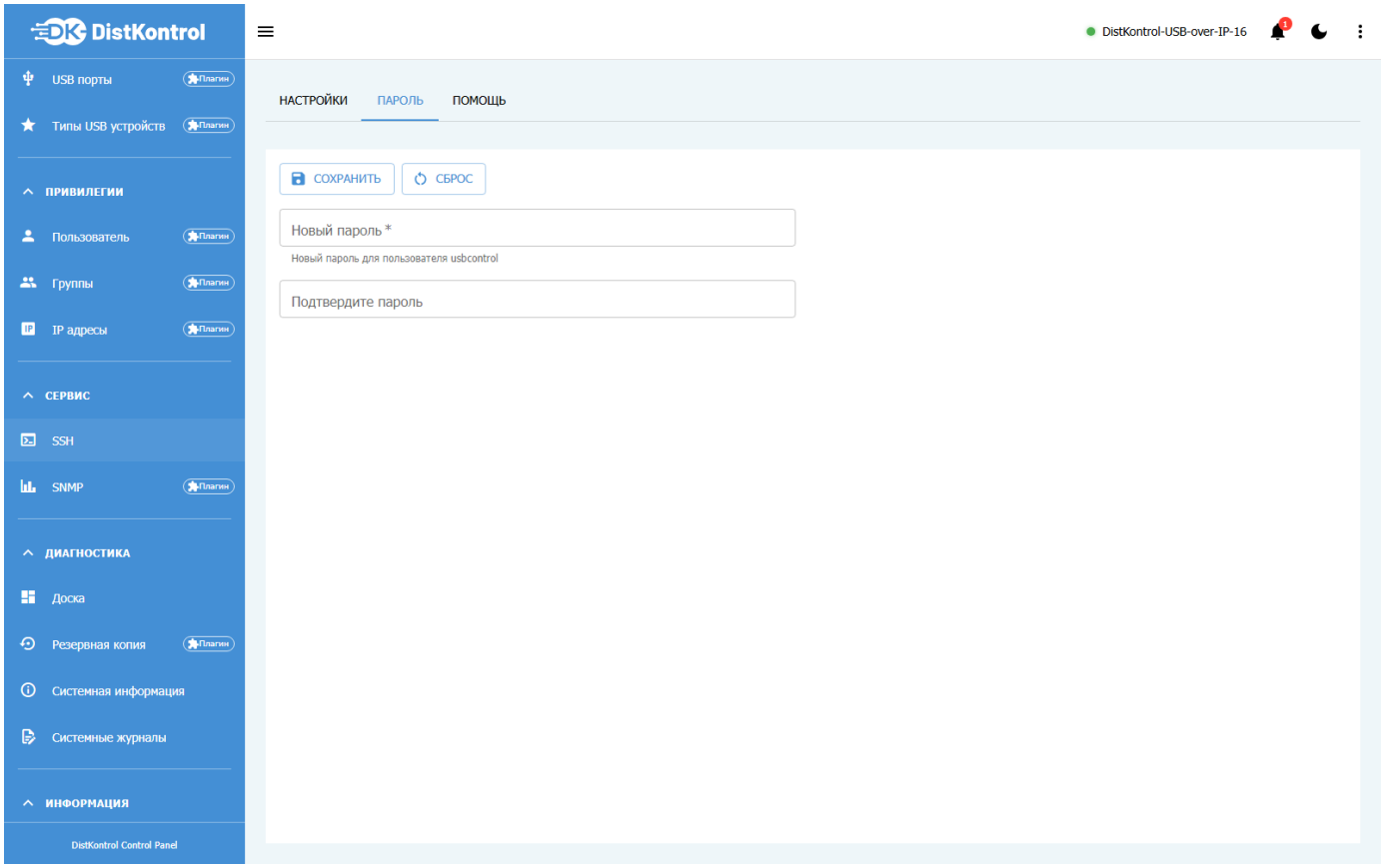
5.5.1.1 Настройки SSH

На вкладке «Настройки» можно изменить порт SSH и включить или отключить сервис.



5.5.1.2 Пароль

На вкладке «Пароль» задаётся или изменяется пароль пользователя `usbcontrol`. Рекомендуется сделать это при первом подключении по SSH. В пароле допустимы спецсимволы, кроме одинарной кавычки.



5.5.1.3 Помощь

Инструкция по использованию команд пользователя `usbcontrol`:

1) `usercontrolapi` — управление пользователями (создание, редактирование и удаление) с различными параметрами. Функционал соответствует разделу WEB «Привилегии» → «Пользователь» (плагин `distkontrol-overip`).

Команды:

- `create` — создать нового пользователя.
- `edit` — редактировать существующего пользователя.
- `delete` — удалить пользователя.

Синтаксис:

```
usercontrolapi <команда> [аргументы]
```

Аргументы:

- `-u` — имя пользователя (обязательный).
- `-p` — пароль (обязательный).
- `--enable` — включить пользователя.
- `--disable` — отключить пользователя.
- `--groups` — группы, разделённые запятыми (например: `Group01,Group02`).

- `--comment <комментарий>` — комментарий.
- `--email` — email.
- `--disallowusermod` / `--allowusermod` — запретить/разрешить изменение пользователя.
- `--accessControlPorts` / `--noAccessControlPorts` — разрешить/запретить доступ к управлению портами.
- `--accessDevices <DeviceID>` — доступ к устройствам (ID устройств через запятую: `1,2,3`).
- `--accessKickUser` / `--noAccessKickUser` — разрешить/запретить отключение других пользователей.
- `--accessPorts <Ports>` — доступ к портам (например: `1.1,1.2,1.3`).
- `--thisAdmin` — предоставить права администратора WEB-интерфейса.
- `--notAdmin` — убрать права администратора.

Примеры:

```
usercontrolapi create -u user1 -p 123 --enable --groups Group01,Group02 --comment "Test User" --email test@example.com
usercontrolapi edit -u user1 -p 321 --disable --comment "Updated Comment"
usercontrolapi delete -u username
```

2) `usbcontrolapi` — управление питанием USB-портов (включение и отключение). Функционал соответствует разделу WEB «USB» → «USB порты» (плагин `distkontrol-inputs`).

Синтаксис:

```
usbcontrolapi <status> <port>
```

Где:

- `<status>` — `0` (выключить) или `1` (включить).
- `<port>` — идентификатор порта (например, `1.1`), ряда (`1.0`) или всех портов (`0.0`).

Примеры:

```
usbcontrolapi 1 1.1    # включить порт 1.1
usbcontrolapi 0 1.0    # выключить ряд 1
usbcontrolapi 1 0.0    # включить все порты
usbcontrolapi 0 2.0,3.0 # выключить ряды 2 и 3
```

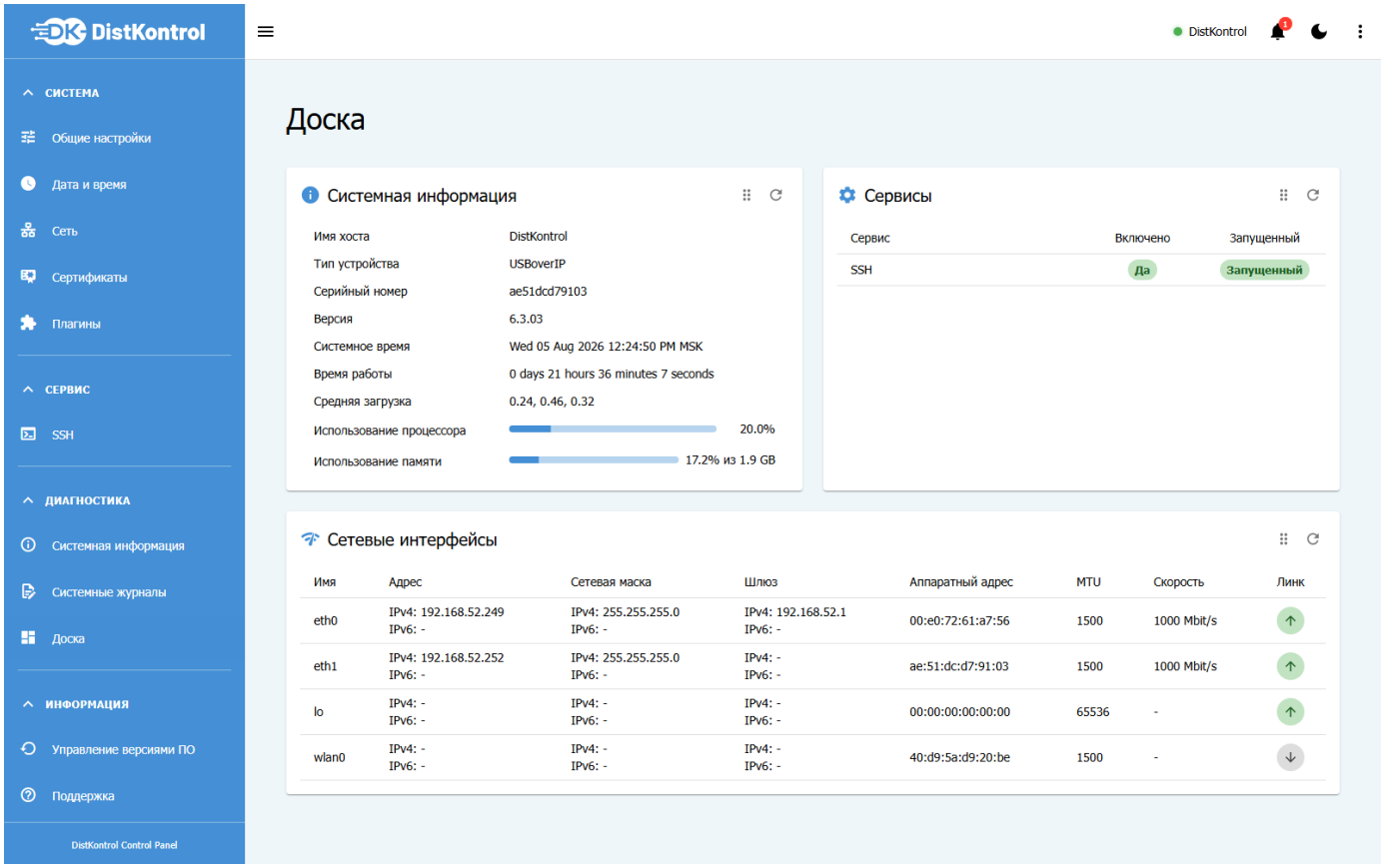
5.6 Диагностика

5.6.1 Доска

Доска с информацией. Возможно добавлять, скрывать, закрывать, изменять размер, а также перетаскивать окна. Является начальной страницей при входе в Web-интерфейс.

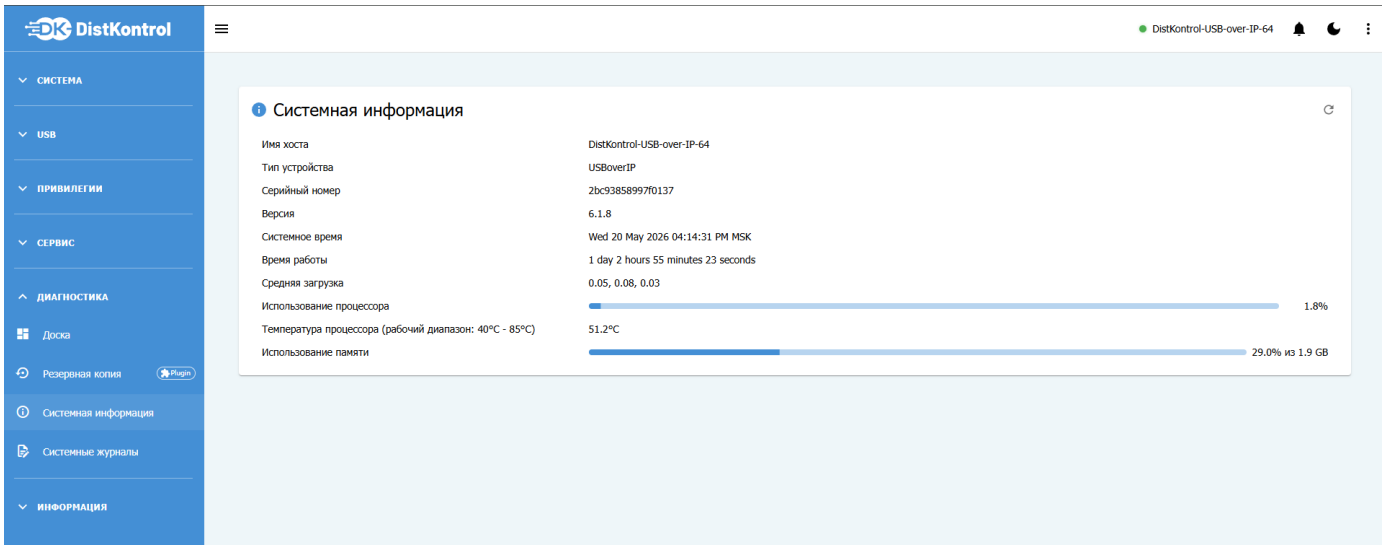
Для добавления доступны следующие окна:

- **"Сетевые интерфейсы"**, отображает следующую информацию:
- Имя
- IP-адрес
- Сетевая маска
- Шлюз
- Аппаратный адрес(MAC-адрес)
- MTU
- Скорость интерфейса
- Состояние интерфейса
- **"Системная информация"**, отображает следующую информацию:
- Имя хоста
- Версия ПО
- Системное время
- Время работы(uptime)
- Средняя загрузка
- Использование процессора
- Температура процессора
- Использование памяти
- **"Сервисы"**, отображает следующую информацию:
- Состояние SNMP(если установлен плагин)
- Состояние SSH



5.6.2 Системная информация

В данном разделе представлена информация о версии прошивки, системное время, параметры нагрузки CPU и RAM. А также время работы USB over IP концентратора.



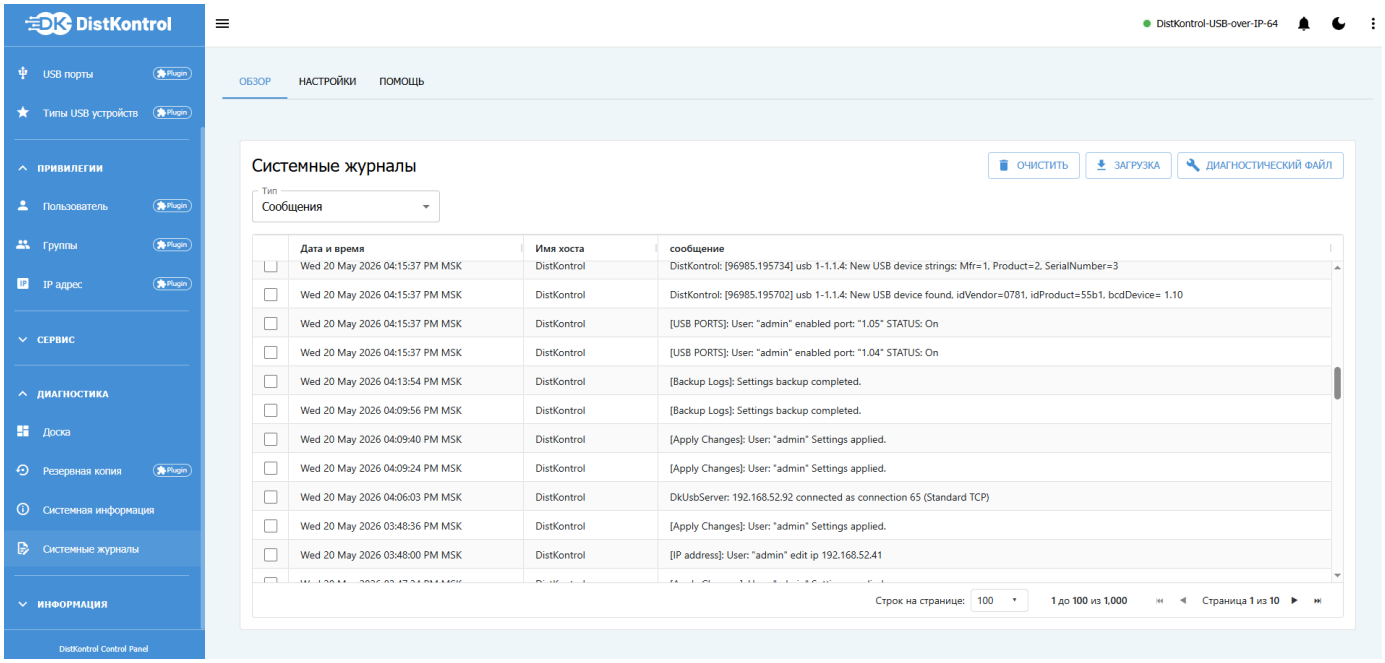
5.6.3 Системный журнал

Просмотр системного журнала возможен на странице WEB интерфейса администратора «Диагностика» - «Системные журналы».

5.6.3.1 Журналы

На странице журналы хранится вся информация о подключениях и отключениях как USB входов (портов) DistKontrolUSB, так и любого из USB-устройств, а также попытках неправильного ввода пароля. Так же записываются изменения настроек концентратора и прочая служебная информация.

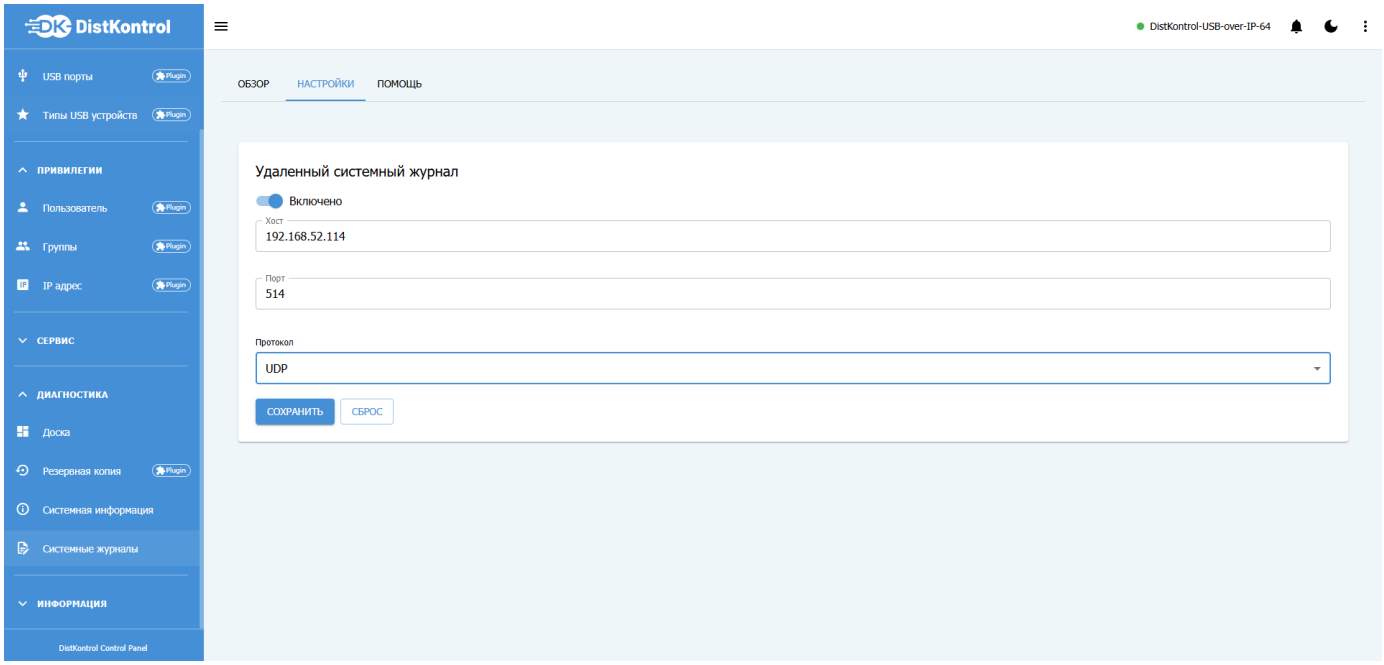
- **Фильтрация сообщений:**
- Сообщения, присылаемые системой
- E-mail сообщения (настраивается в выпадающем списке)
- **Кнопка «Очистить»** для очистки журнала.
- **Кнопки «Загрузка» и «Диагностический файл»** предназначены для загрузки системной информации при обращении в техническую поддержку.



5.6.3.2 Настройки

На странице «Настройки» возможно настроить удаленный системный журнал.

В концентраторе предусмотрена возможность отправки журнала (syslog) на удаленный сервер. Включение опции и ее настройка осуществляются на странице WEB - интерфейса администратора «Диагностика» - «Системные журналы» - «Настройки».



Для настройки перенаправления журналов на сторонний сервер со стороны концентратора достаточно включить отправку журнала, указать хост порт и протокол.

В сети вам необходимо иметь настроенный действующий сервер приема логов.

5.6.3.3 Сообщения системы авторизации

Авторизация по логину и паролю для доступа к USB устройству.

- `[Authorization Client] The user ‘ИМЯ’ was not found in the database` – Пользователь не найден в базе концентратора.
- `[Authorization Client] The user ' ИМЯ ' found` – Пользователь найден в базе концентратора.
- `[Authorization Client] Password OK (или BAD)` – Неуспешная (или успешная) проверка имени пользователя и пароля для подключения к USB устройству. В квадратных скобках Имя пользователя, от которого производится подключение.
- `[Authorization Client] The USB device was not found in the database` – Подключаемое USB устройство отсутствует в списке USB устройств.
- `[Authorization Client] The user 'ИМЯ' does not have permission to connect USB devices.` – Пользователь не имеет ни одного разрешенного USB устройства.
- `[Authorization Client] DEVICE OK (или BAD)` – Неуспешная (или успешная) проверка разрешения пользователю использовать подключаемое USB устройство. В квадратных скобках первый параметр № USB устройства к которому производится подключение, второй – перечень разрешенных для пользователя USB устройств.

Авторизация по логину и паролю для доступа к USB порту концентратора.

- `[Authorization Client] The user ‘ИМЯ’ was not found in the database` – Пользователь не найден в базе концентратора.
- `[Authorization Client] The user ' ИМЯ ' found` – Пользователь найден в базе концентратора.

- `[Authorization Client] Password OK (или BAD)` – Неуспешная (или успешная) проверка имени пользователя и пароля для подключения к USB устройству. В квадратных скобках Имя пользователя, от которого производится подключение.
- `[Authorization Client] PORT OK (или BAD)` – Неуспешная (или успешная) проверка разрешения пользователю пользоваться подключаемым портам. В квадратных скобках первый параметр номер порта, к которому производится подключение, второй – перечень разрешенных для данного пользователя портов.

Авторизация по IP адресу для доступа к USB устройству.

- `[Authorization Client] The IP 'IP адрес' not found in the database` – IP адрес не найден в базе концентратора.
- `[Authorization Client] The IP 'IP адрес' found` – IP адрес найден в базе концентратора.
- `[Authorization Client] DEVICE OK (или BAD)` – Неуспешная (или успешная) проверка разрешения подключения USB устройств с данного IP. В квадратных скобках первый параметр номер USB устройства из списка USB устройств, второй – список USB устройств, разрешенных для данного IP.

Авторизация по IP адресу для доступа к USB порту концентратора.

- `[Authorization Client] The IP 'IP адрес' not found in the database` – IP адрес не найден в базе концентратора.
- `[Authorization Client] The IP 'IP адрес' found` – IP адрес найден в базе концентратора.
- `[Authorization Client] PORT OK (или BAD)` – Неуспешная (или успешная) проверка разрешения подключения USB порта с данного IP. В квадратных скобках первый параметр номер USB порта к которому производится подключение, второй – перечень разрешенных портов для данного IP.
- `BOUND to connection X` – Успешное подключение USB устройства;
- `UNBOUND from connection X` – Успешное отключение USB устройства.
- `SURPRISE UNBOUND` – неожиданное отключение USB-устройства. Возникает при непредвиденном отключении USB-устройства от клиентского приложения. Может быть вызвано обрывом соединения или завершением процесса клиентского приложения.
- `BIND UNKNOWN ERROR` – неожиданная ошибка при подключении USB-устройства клиентским приложением. Возникает при включённой авторизации к USB-порту по логину/паролю и автоподключении USB-устройства в клиентском приложении.

5.6.3.4 Сообщения системы управления питанием USB-устройств

- `[USB PORTS]//Control port// USER: Petrov USB in: 2.3 STATUS: turnOn (turnoff)` – Включение (выключение) USB порта 2.3 пользователем «Petrov».

5.6.3.5 Сообщения связанные с некорректной работой USB-устройства

- `device not accepting address, error -71` – ошибка протокола (устройство не может завершить процедуру перечисления). Решение: замена USB-устройства.

- `device not accepting address, error -22` – некорректный или недопустимый аргумент в функции, связанной с USB. Решение: замена USB-устройства.
- `device descriptor read/64, error -110` – устройство не ответило на запрос вовремя. Решение: замена USB-устройства.

5.6.3.6 Прочие сообщения

Все сообщения в системном журнале записываются с датой и временем. Служба времени настраивается в разделе «Система» → «Дата и время».

В журнале также фиксируется служебная информация о работе устройства. Журнал можно очистить или загрузить на компьютер для анализа.

По сообщениям журнала можно диагностировать проблемы при ограничении доступа к USB-устройствам и портам.

Общая структура сообщений:

```
[USB Settings] Restricting access to the USB port by login and password – DISABLED:
```

- `[USB Settings]` — лог раздела настроек USB;
- `Restricting access to the USB port by login and password` — название изменённого параметра;
- `DISABLED` — статус параметра.

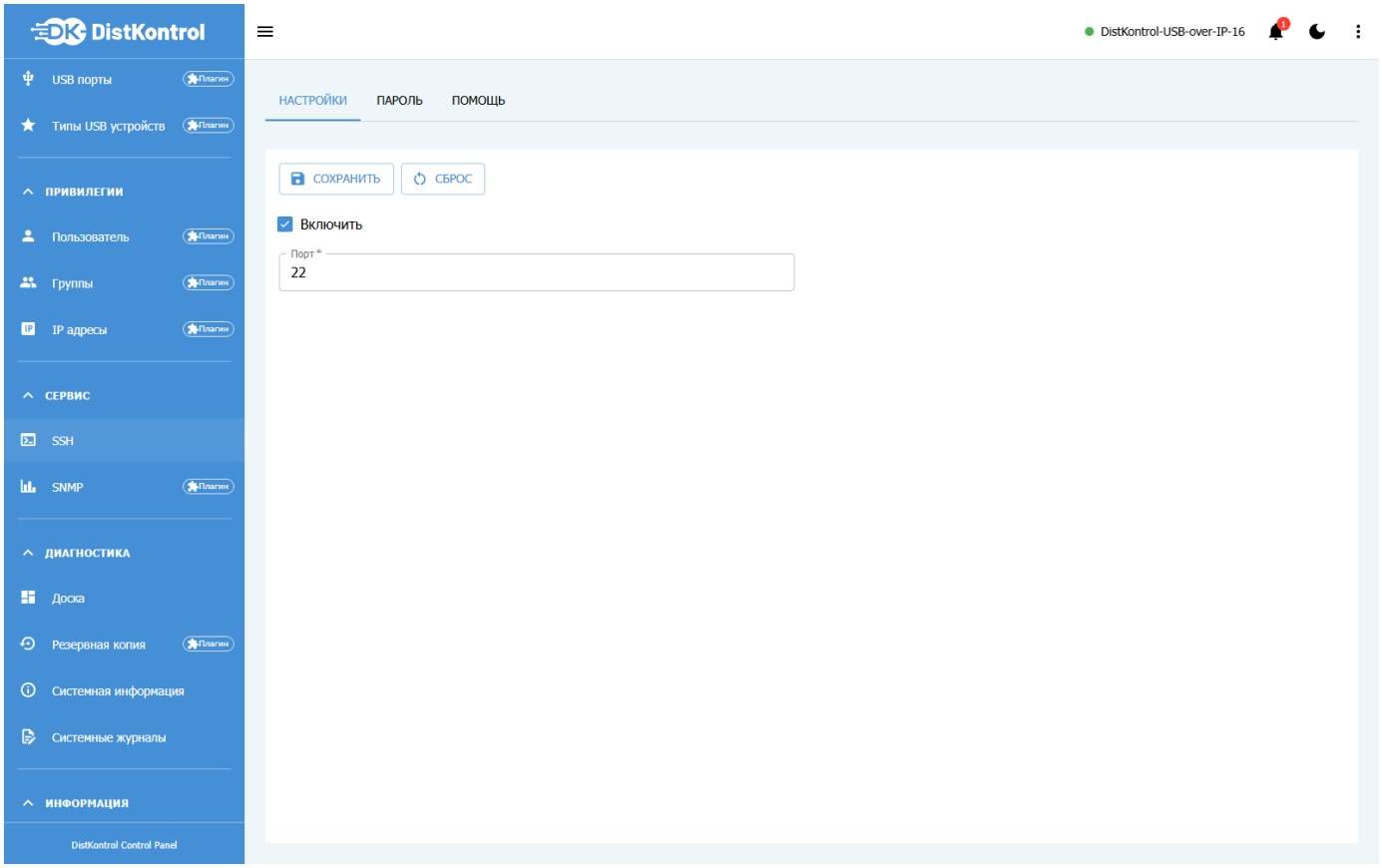
5.7 Информация

5.7.1 Управление версиями ПО

5.7.1.1 Сброс и восстановление

Вкладка **«Сброс и восстановление»** расположена в разделе **«Управление версиями ПО»**.

Страница позволяет: 1. Произвести сброс настроек программного обеспечения до состояния по умолчанию. 2. Сохранить и скачать резервную копию настроек. 3. Восстановить ранее сохраненные настройки.



- **Сброс настроек** программного обеспечения к параметрам по умолчанию осуществляется нажатием на кнопку **«Сброс настроек»**. В появившемся окне будет необходимо подтвердить сброс.
- **Сохранить имеющиеся настройки ПО** возможно нажатием кнопки **«Сохранить настройки»**. Далее необходимо подтвердить загрузку копии.
- **Восстановить настройки ПО** возможно нажатием на кнопку **«Загрузить»**. После чего выбрать сохраненный файл настроек. После загрузки файла устройство будет перезагружено.

Внимание!

- При переименовании файла настроек не используйте пробелы.

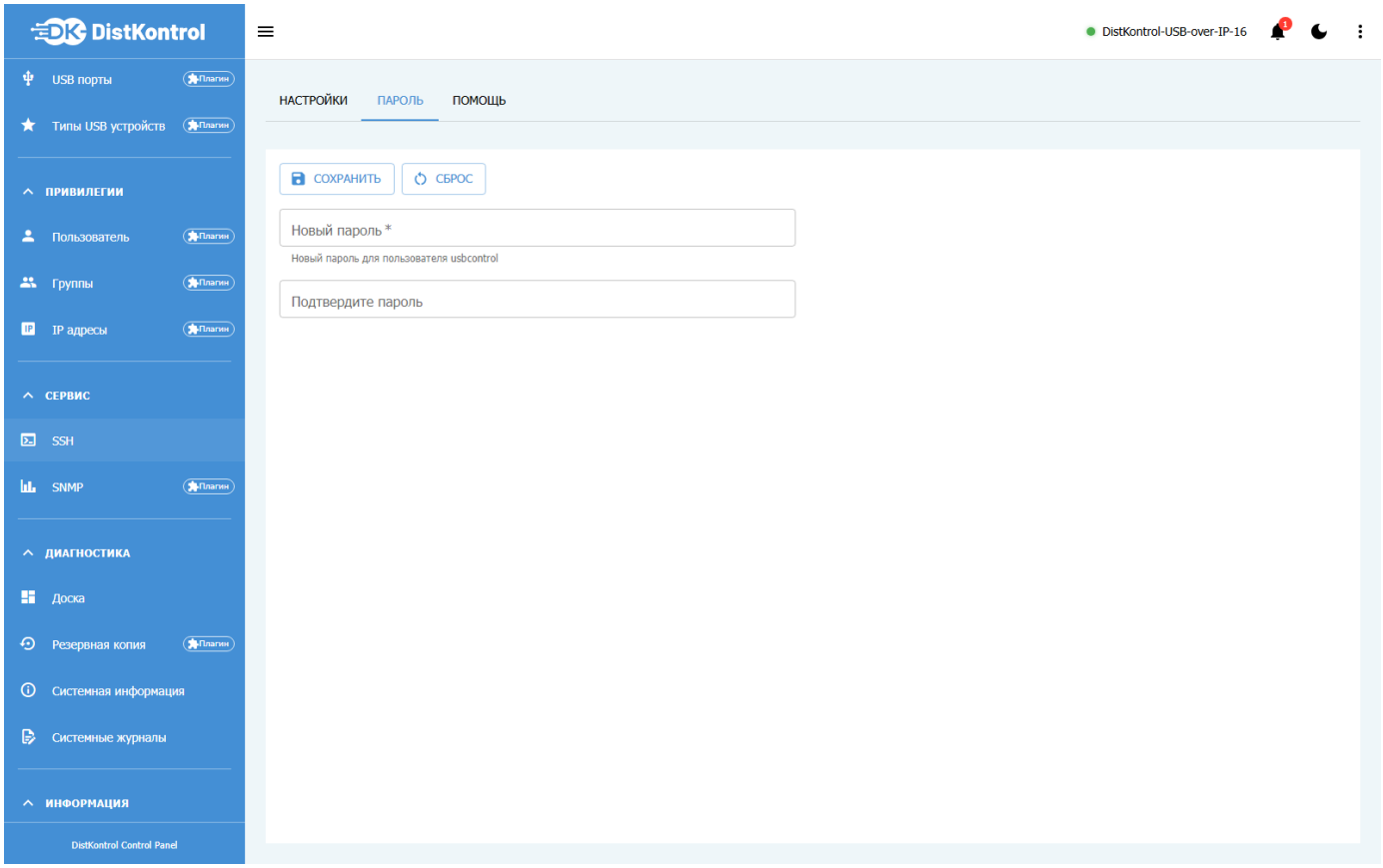
Внимание!

Сброс настроек происходит на той версии ПО, которая стоит по умолчанию.

5.7.1.2 Проверить обновление

Данный пункт меню позволяет: 1. Проверить наличие новой версии ПО концентратора и, при наличии, скачать его для обновления через USB-накопитель. 2. Проверить наличие новой версии ПО загрузчика концентратора, и при наличии, установить его.

Для работы опций требуется доступ концентратора в интернет.



- **Кнопка «Проверка»** — проверка наличия обновлений.
- **Кнопка «История версий ПО»** — открывает страницу с историей изменений в новом окне.
- **Кнопка «Подписаться на рассылку»** — уведомления о выходе новых продуктов и обновлений.
- **Кнопка «Загрузка»** — позволяет скачать последнюю доступную версию ПО для обновления концентратора с USB-накопителя (подробнее см. **«Обновление ПО»**).
- **Кнопка «Установить с USB-накопителя»** — устанавливает обновление с USB-накопителя, находящегося в порту 1.1.
- **«SHA1»** — контрольная сумма файла прошивки.

Внимание!

Не выключайте питание до завершения обновления. Выключение питания может вызвать сбой в устройстве, дальнейшее исправление сбоя будет возможно только в сервисном центре.

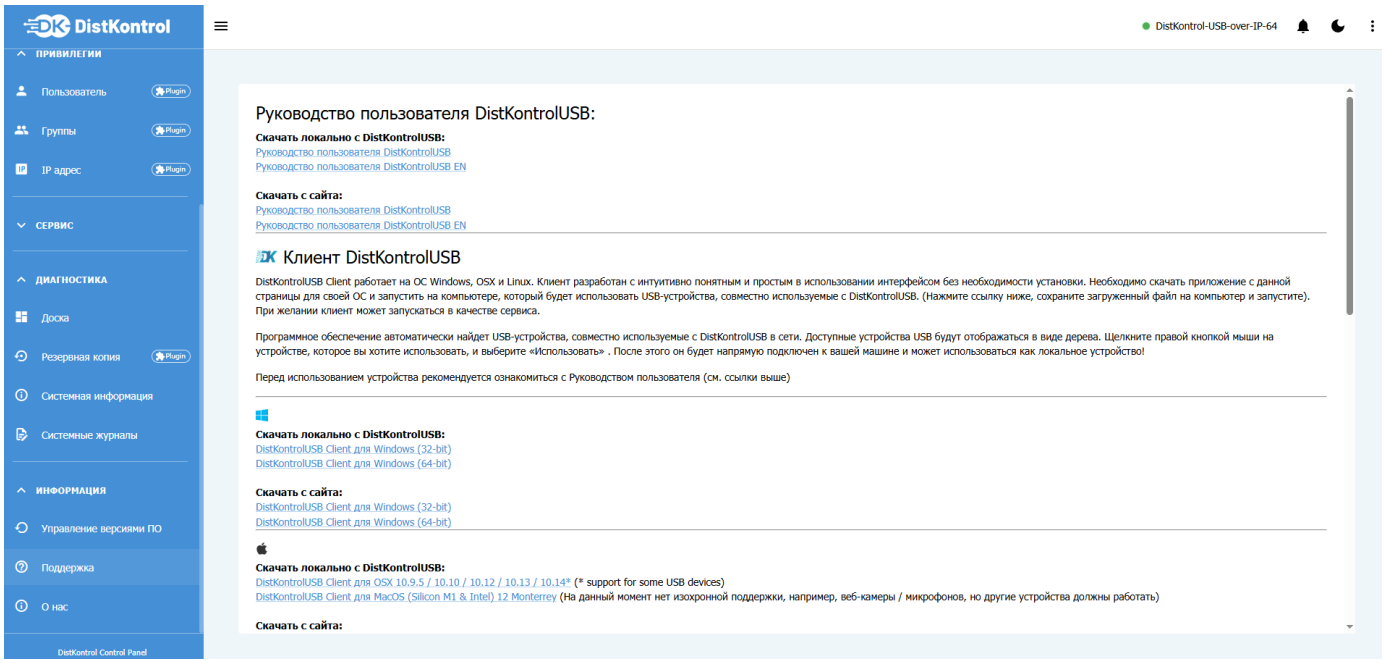
5.7.1.3 Поддержка

В данном разделе можно скачать:

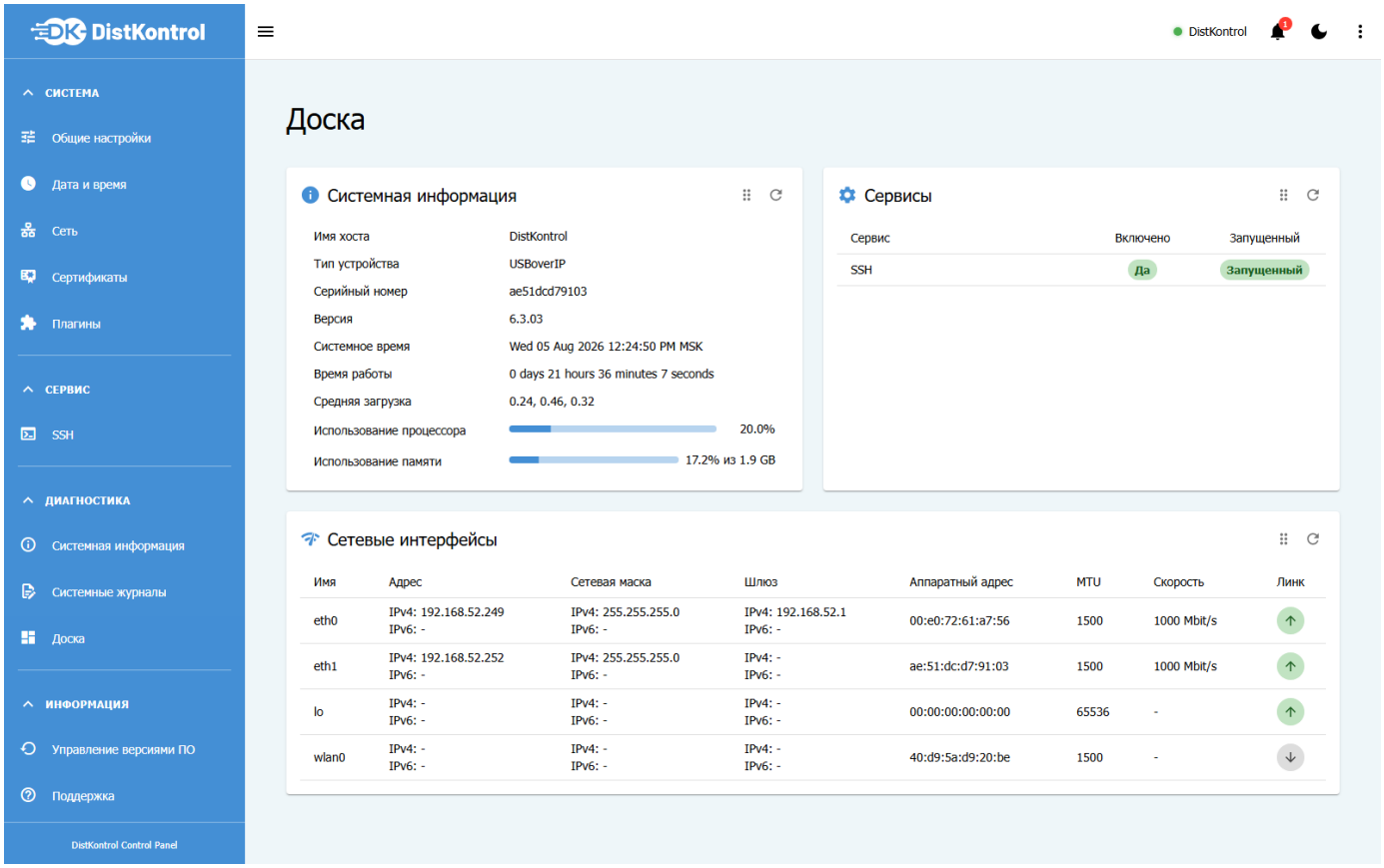
- **Руководство пользователя**.
- **Клиент DistKontrolUSB** под вашу операционную систему.

Скачивание доступно локально и с сайта через интернет.

Руководство по клиенту: DistKontrolUSB Client. См. также База знаний — Где скачать DistkontrolUSB Client.



5.7.1.4 Патч


DistKontrol
DistKontrol
СИСТЕМА
Общие настройки
Дата и время
Сеть
Сертификаты
Плагины
СЕРВИС
SSH
ДИАГНОСТИКА
Системная информация
Системные журналы
Доска
ИНФОРМАЦИЯ
Управление версиями ПО
Поддержка
DistKontrol Control Panel
DistKontrol
Доска
Системная информация
Имя хоста DistKontrol
Тип устройства USBoverIP
Серийный номер ae51dcd79103
Версия 6.3.03
Системное время Wed 05 Aug 2026 12:24:50 PM MSK
Время работы 0 days 21 hours 36 minutes 7 seconds
Средняя загрузка 0.24, 0.46, 0.32
Использование процессора 20.0%
Использование памяти 17.2% из 1.9 GB
Сервисы
Сервис Включено Запущенный
SSH Да Запущенный
Сетевые интерфейсы
Имя Адрес Сетевая маска Шлюз Аппаратный адрес MTU Скорость Линк
eth0 IPv4: 192.168.52.249 IPv6: - IPv4: 255.255.255.0 IPv6: - IPv4: 192.168.52.1 IPv6: - 00:e0:72:61:a7:56 1500 1000 Mbit/s
eth1 IPv4: 192.168.52.252 IPv6: - IPv4: 255.255.255.0 IPv6: - IPv4: - IPv6: - ae:51:dc:d7:91:03 1500 1000 Mbit/s
lo IPv4: - IPv6: - IPv4: - IPv6: - IPv4: - IPv6: - 00:00:00:00:00:00 65536 -
wlan0 IPv4: - IPv6: - IPv4: - IPv6: - IPv4: - IPv6: - 40:d9:5a:d9:20:be 1500 -

5.8 Сброс настроек управляемого USB over IP концентратора в исходное состояние

Выполнить сброс настроек возможно **двумя способами**:

1. **Через WEB-интерфейс устройства**
   (см. раздел «Сброс и восстановление»).
2. **С помощью аппаратной кнопки «Reset»**, расположенной с тыльной части устройства:
3. Выключите концентратор.
4. Нажмите и удерживайте кнопку «Reset».
5. Подайте питание на устройство.
6. Через **40 секунд** отпустите кнопку «Reset».
7. Устройство сброшено до заводских настроек.

Внимание!

- Сброс настроек происходит на той версии ПО, которая установлена по умолчанию.
- После сброса и обновления первая загрузка устройства может занимать **до 5 минут**.
- После сброса потребуется **повторный ввод лицензионного ключа** (см. раздел «Лицензия»).

Внимание!

Не прерывайте процесс сброса и обновления! Это может привести к необратимым сбоям в работе устройства.

Если после сброса WEB-интерфейс выдаёт ошибки **500** или **502**, см. База знаний. Перед сбросом рекомендуется экспорт настроек: 5.10 Сохранение и восстановление, плагин «Резервная копия».

5.9 Обновление программного обеспечения управляемого USB over IP концентратора

Внимание!

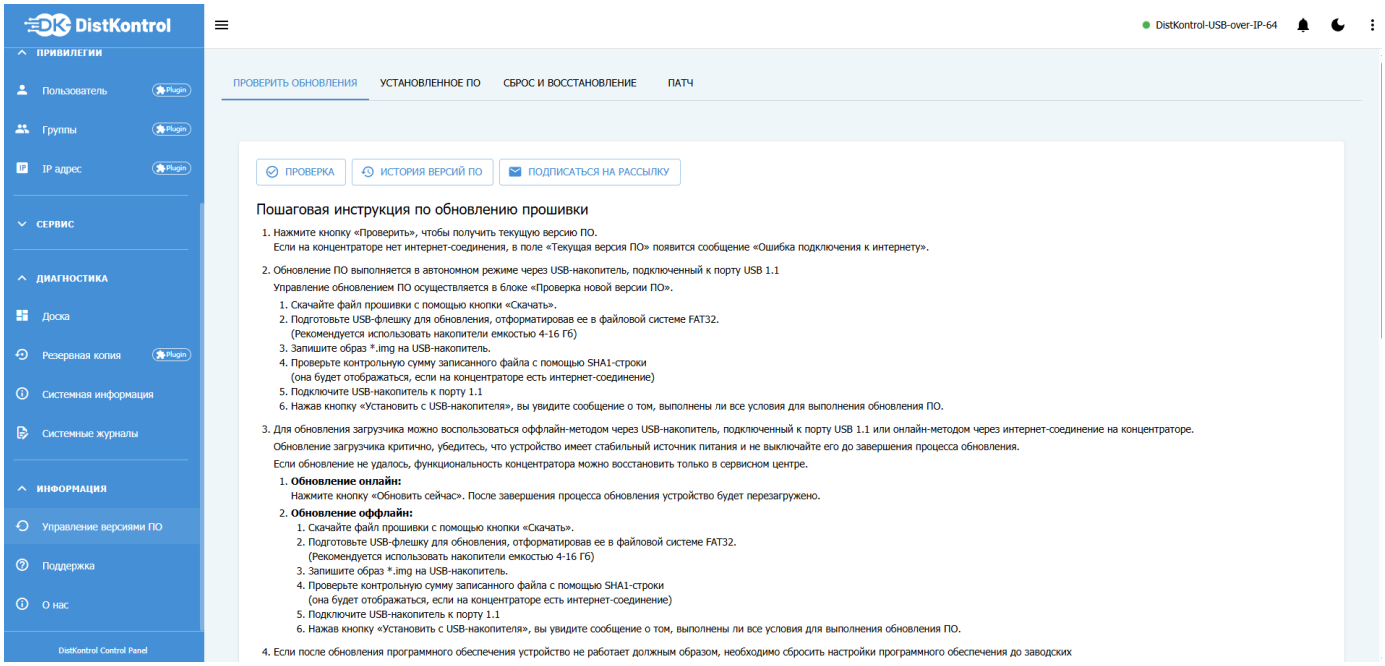
При обновлении программного обеспечения управляемого USB over IP концентратора его настройки не сохраняются и сбрасываются к исходным. Необходимо до обновления устройства выполнить экспорт настроек и их импорт после обновления (см. раздел руководства «Сохранение и восстановление настроек») или осуществить повторную настройку устройства, при этом потребуется ввод лицензионного ключа к ПО управляемого USB over IP концентратора по методике, изложенной в разделе «Лицензия».

Для обновления программного обеспечения управляемого USB over IP концентратора необходимо перейти в раздел **«Управление версиями ПО»** (5.7.1 Управление версиями ПО).
Обновление возможно одним способом — **с флэш-носителя**.

Общий порядок (включая обновление загрузчика и сброс после обновления): База знаний — Обновление ПО. Перед обновлением сохраните настройки: 5.10 Сохранение и восстановление или плагин «Резервная копия».

Пошаговая инструкция по обновлению ПО концентратора:

1 Нажмите кнопку **«Проверить»**, чтобы получить текущую версию ПО.
Если на концентраторе нет интернет-соединения, в поле **«Текущая версия ПО»** появится сообщение **«Ошибка подключения к интернету»**.



---

2 **Обновление ПО выполняется в автономном режиме через USB-накопитель, подключенный к порту USB 1.1.**
Управление обновлением ПО осуществляется в блоке **«Проверка новой версии ПО»**.

2.1. Скачайте файл ПО с помощью кнопки **«Загрузка»**.

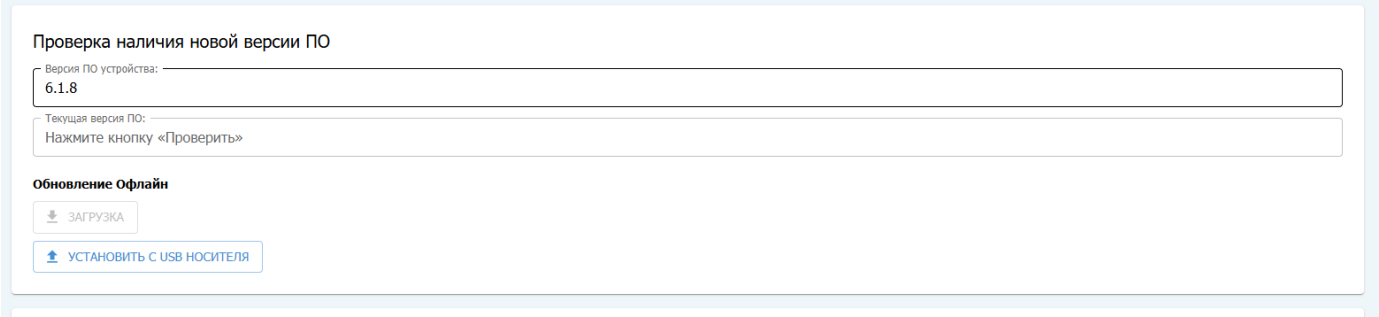
2.2. Подготовьте USB-флеш накопитель для обновления, отформатировав ее в файловой системе **FAT32**.
(Рекомендуется использовать накопители емкостью 4–16 Гб)

2.3. Запишите образ `*.img` на USB-накопитель.

2.4. Проверьте контрольную сумму записанного файла с помощью **SHA1-строки**
(она будет отображаться, если на концентраторе есть интернет-соединение).

2.5. Подключите USB-накопитель к порту **1.1**.

2.6. Нажав кнопку **«Установить с USB-накопителя»**, вы увидите сообщение о том, выполнены ли все условия для выполнения обновления ПО.



---

3 **Для обновления загрузчика** можно воспользоваться:

- **Офлайн-методом** через USB-накопитель, подключенный к порту USB 1.1.
- **Онлайн-методом** через интернет-соединение на концентраторе.

Обновление загрузчика критично! Убедитесь, что устройство имеет стабильный источник питания и не выключайте его до завершения процесса обновления.
Если обновление не удалось, функциональность концентратора можно восстановить только в сервисном центре.

3.1. **Обновление онлайн:**

3.1.1. Нажмите кнопку **«Обновить сейчас»**. После завершения процесса обновления устройство будет перезагружено.

3.2. **Обновление офлайн:**

3.2.1. Скачайте файл прошивки с помощью кнопки **«Скачать»**.

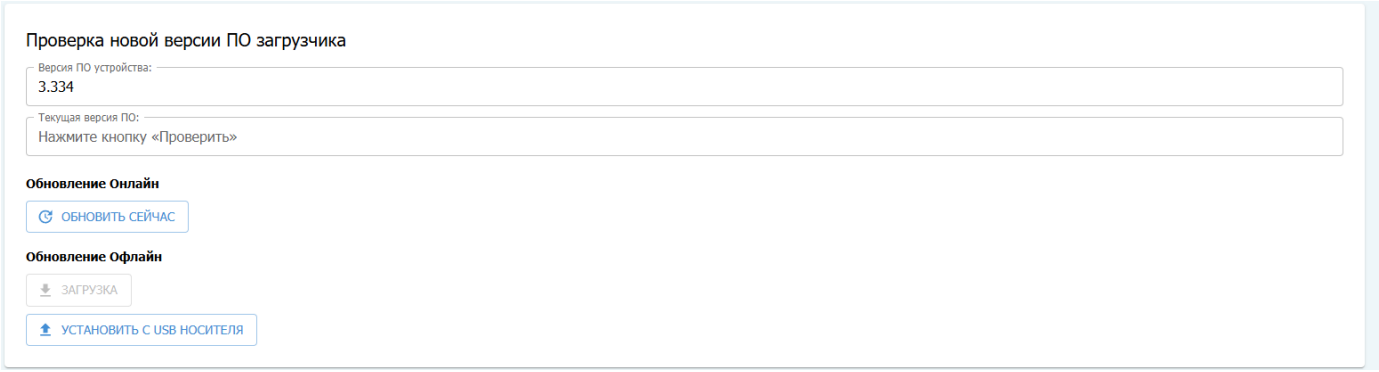
3.2.2. Подготовьте USB-флеш накопитель для обновления, отформатировав ее в файловой системе **FAT32**.
(Рекомендуется использовать накопители емкостью 4–16 Гб)

3.2.3. Запишите образ `*.img` на USB-накопитель.

3.2.4. Проверьте контрольную сумму записанного файла с помощью **SHA1-строки**
(она будет отображаться, если на концентраторе есть интернет-соединение).

3.2.5. Подключите USB-накопитель к порту **1.1**.

3.2.6. Нажав кнопку **«Установить с USB-накопителя»**, вы увидите сообщение о том, выполнены ли все условия для выполнения обновления ПО.



4 **Если после обновления программного обеспечения устройство не работает должным образом**, необходимо сбросить настройки программного обеспечения до заводских:

4.1. Нажмите на кнопку **«Управление версиями программного обеспечения»** в главном меню устройства.

4.2. Выберите **«Сброс и восстановление»**.

4.3. Нажмите на кнопку **«Сохранить настройки»**, чтобы сохранить резервную копию настроек.

4.4. Нажмите на кнопку **«Сброс настроек»**.

4.5. В появившемся окне подтвердите сброс, нажав **«Да»**.

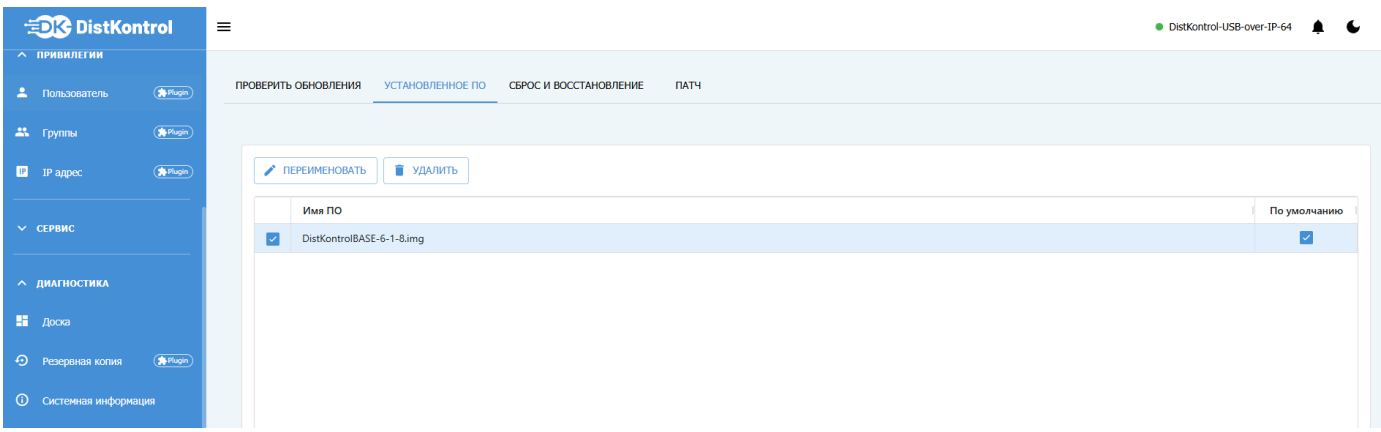
4.6. Дождитесь завершения процесса сброса и перезагрузки устройства.

4.7. После перезагрузки устройства необходимо выполнить настройку устройства в соответствии с инструкциями.

5.9.1 Установленные ПО

Вкладка **«Установленное ПО»** раздела **«Управление версиями ПО»** в Web-интерфейсе концентратора позволяет:

- Выбрать по умолчанию.
- Переименовать.
- Удалить имеющиеся версии ПО.



При обновлении на новую версию ПО концентратора предыдущая версия ПО будет доступна в данной вкладке. При желании на неё возможно откатиться, нажав на соответствующий чекбокс.

После нажатия на чекбокс откроется окно уведомления, информирующее о том, что ПО выбрано по умолчанию и концентратор необходимо перезагрузить.

Перезагрузить устройство возможно:

- Через Web-интерфейс.
- С помощью аппаратного тумблера на тыльной стороне концентратора.

Внимание!

После установки по умолчанию предыдущей версии ПО концентратора настройки Web-интерфейса используются именно с предыдущей версии ПО.

5.10 Сохранение и восстановление настроек программного обеспечения, управляемого USB over IP концентратора

Внимание!

При необходимости удаление импортированных настроек осуществляется простым сбросом настроек управляемого USB over IP концентратора в исходное состояние. Подробнее в разделе **«**Сброс настроек управляемого USB over IP концентратора в исходное состояние**»**.

Расширенные возможности резервного копирования (расписание, экспорт на ПК): плагин «Резервная копия», База знаний — перенос настроек.

5.11 Аппаратная перезагрузка управляемого USB over IP концентратора

Для перезагрузки концентратора нажмите и удерживайте кнопку **«Reset»**, расположенную с тыльной стороны устройства, в течении **15 секунд**. Концентратор будет корректно перезагружен.

6 Вариант использования, управляемого USB over IP концентратора

Управляемый USB over IP концентратор не является абсолютным средством обеспечения безопасности при подключении USB устройств по сети. Необходимо его использование сочетать с дополнительными организационными и техническими мерами обеспечения информационной безопасности.

Возможный сценарий использования:

Задача: организация доступа к USB устройствам:

- из региональных офисов (условно NET №1 …… NET № N),
- для ограниченного ряда компьютеров и ноутбуков, подключающих USB устройства через глобальную сеть,
- для пользователей, опубликованных на терминальных серверах приложений.



1. Организационные меры безопасности

- Управляемый USB over IP концентратор установлен в качественно закрывающийся на ключ серверный шкаф.
- Физический доступ к нему упорядочен (СКД в само помещение, видеонаблюдение, ключи и права доступа у строго ограниченного круга лиц).

Все используемые в организации USB устройства условно разделены на 3 группы:

- **Критичные.** Финансовые ЭЦП – используются в соответствии с рекомендациями банков (не через USB over IP).
- **Важные.** ЭЦП для торговых площадок, услуг, ЭДО, отчетности и т.д., ряд ключей для ПО — используются с применением управляемого USB over IP концентратора.
- **Не критичные.** Ряд ключей для ПО, камеры, ряд флеш-носителей и дисков с не критичной информацией, USB-модемы — используются с применением управляемого USB over IP концентратора.

---

2. Технические меры безопасности

- Сетевой доступ к управляемому USB over IP концентратору предоставляется только внутри изолированной подсети.
- Доступ в изолированную подсеть предоставляется:
- с фермы терминальных серверов,
- по VPN (сертификат и пароль) ограниченному количеству компьютеров и ноутбуков, по VPN им выдаются постоянные адреса,
- по VPN-туннелям, соединяющим региональные офисы.

Настроенные функции на USB over IP концентраторе DistKontrolUSB:

- Шифрование SSL для доступа к USB устройствам.
- Ограничение доступа к USB устройствам по IP-адресу.
- Ограничение доступа к USB порту по логину и паролю (пользователям назначены права на доступ к USB устройствам).

Физическое включение/выключение USB портов:

- **Ключи от ПО и ЭДО** – по расписанию (планировщик задач: например, 9:00–18:00 или 13:00–16:00).
- **Ключи от торговых площадок и ПО** – через WEB-интерфейс (разрешенными пользователями).
- **Камеры, флеш-носители, диски** – включены всегда.

Плагины
DistKontrol

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

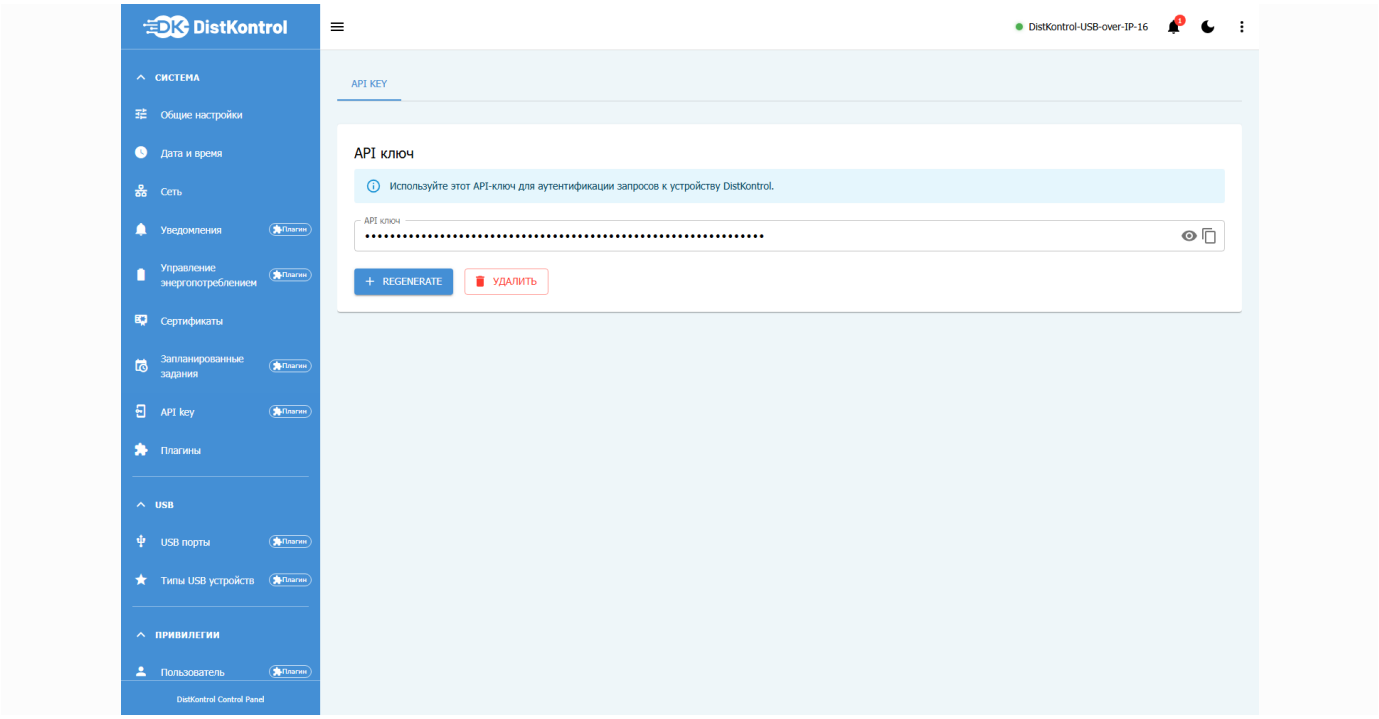
Москва
2026 г

Плагин «API ключ»

Идентификатор: `distkontrol-api-key`
Скачивание: страница плагинов

Модуль добавляет в WEB-интерфейс раздел **Система** → **API key** для выдачи ключа авторизации при работе с DistKontrol: Systems Control Center.

Установка и удаление — в общей инструкции.



1. Краткое описание

Плагин позволяет сгенерировать в WEB-интерфейсе устройства ключ доступа и использовать его в SCC вместо логина и пароля WEB-интерфейса.

2. На какое оборудование устанавливается

Оборудование	Примечание
DistKontrolUSB **v4 / v5 / v6**	При наличии раздела **«Плагины»**
Сценарии с DistKontrol: SCC	Обязателен для авторизации по кнопке **«API ключ»**

3. Для чего нужен

- подключать концентраторы к SCC без передачи пароля WEB-интерфейса;
- централизованно управлять устройствами после авторизации по ключу;
- отозвать доступ — сгенерировать новый ключ и обновить его в SCC.

4. Как пользоваться

На концентраторе

1. Установите плагин и перезагрузите страницу браузера.
2. Откройте **Система** → **API key**.
3. Нажмите **«Regenerate»** (или **«Сгенерировать»**), чтобы создать ключ.
4. Скопируйте ключ (кнопка копирования рядом с полем) — он понадобится в SCC.
5. При необходимости удалите ключ кнопкой **«Удалить»**.

В DistKontrol: SCC

1. Добавьте концентратор в 2.3.1 Список устройств.
2. Нажмите **«API ключ»** для нужного устройства.
3. Введите ключ из WEB-интерфейса концентратора.

См. также: руководство SCC, Плагины (v6).

Плагин «Резервная копия»

Идентификатор: `distkontrol-export-backup`
Скачивание: страница плагинов

Модуль добавляет раздел **Диагностика** → **Резервная копия** для создания, хранения, экспорта и восстановления настроек устройства.

Установка и удаление — в общей инструкции.

---

1. Краткое описание

Плагин сохраняет выбранные или все настройки в файл на устройстве, позволяет скачать копию на ПК, загрузить на другое устройство и применить конфигурацию кнопкой **«Установить»**.

Необходим для **резервного копирования**, **синхронизации** и **кластеризации** в DistKontrol: SCC.

---

2. На какое оборудование устанавливается

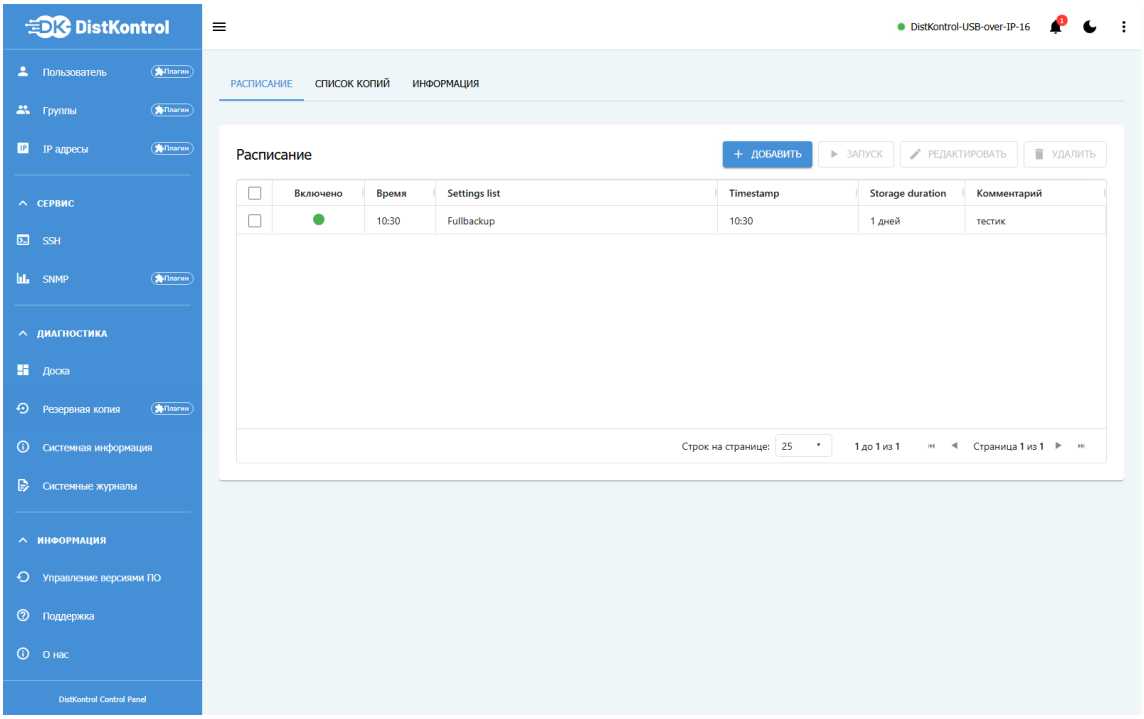
Оборудование	Примечание
DistKontrolUSB **v4 / v5 / v6**	ПО с разделом **«Плагины»**
DistKontrolPDU	При наличии раздела **«Плагины»**
Работа с SCC	ПО концентратора не ниже **5.03.01**

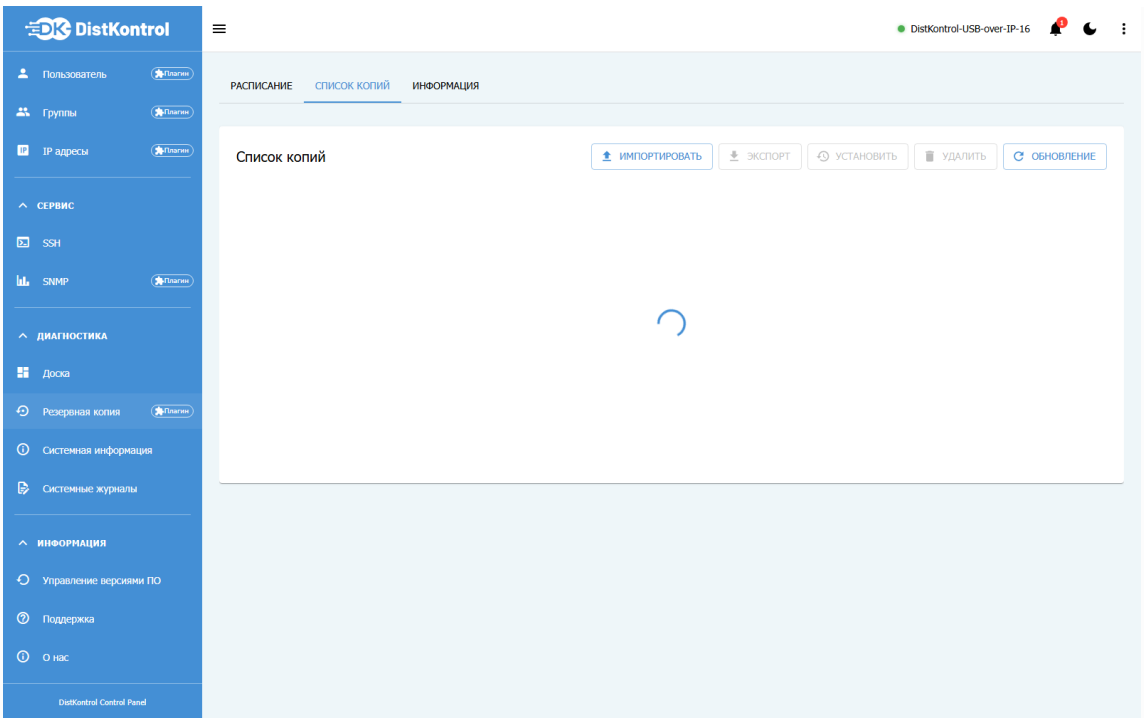
---

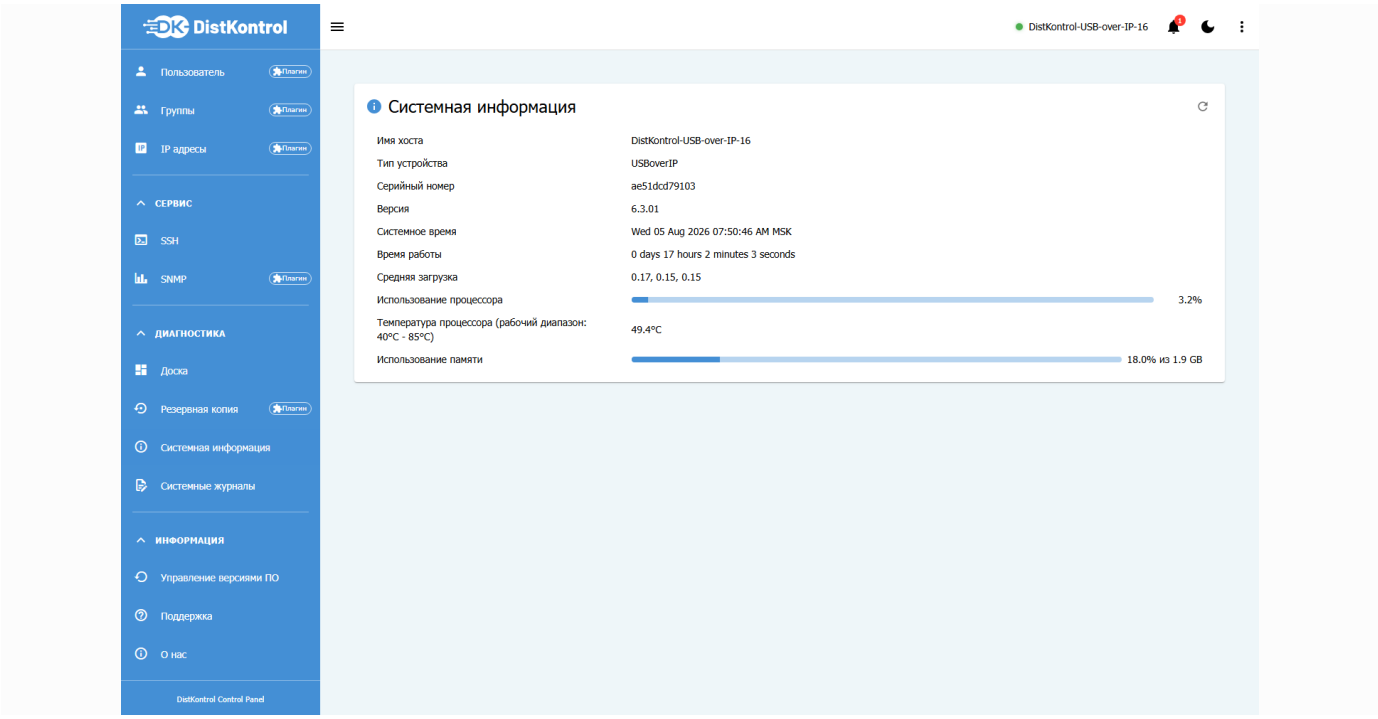
3. Раздел в WEB-интерфейсе

Вкладки:

Вкладка	Назначение
Расписание	Задания по расписанию, запуск копии
Список копий	Экспорт, импорт, установка, удаление файлов
Информация	Справка по плагину

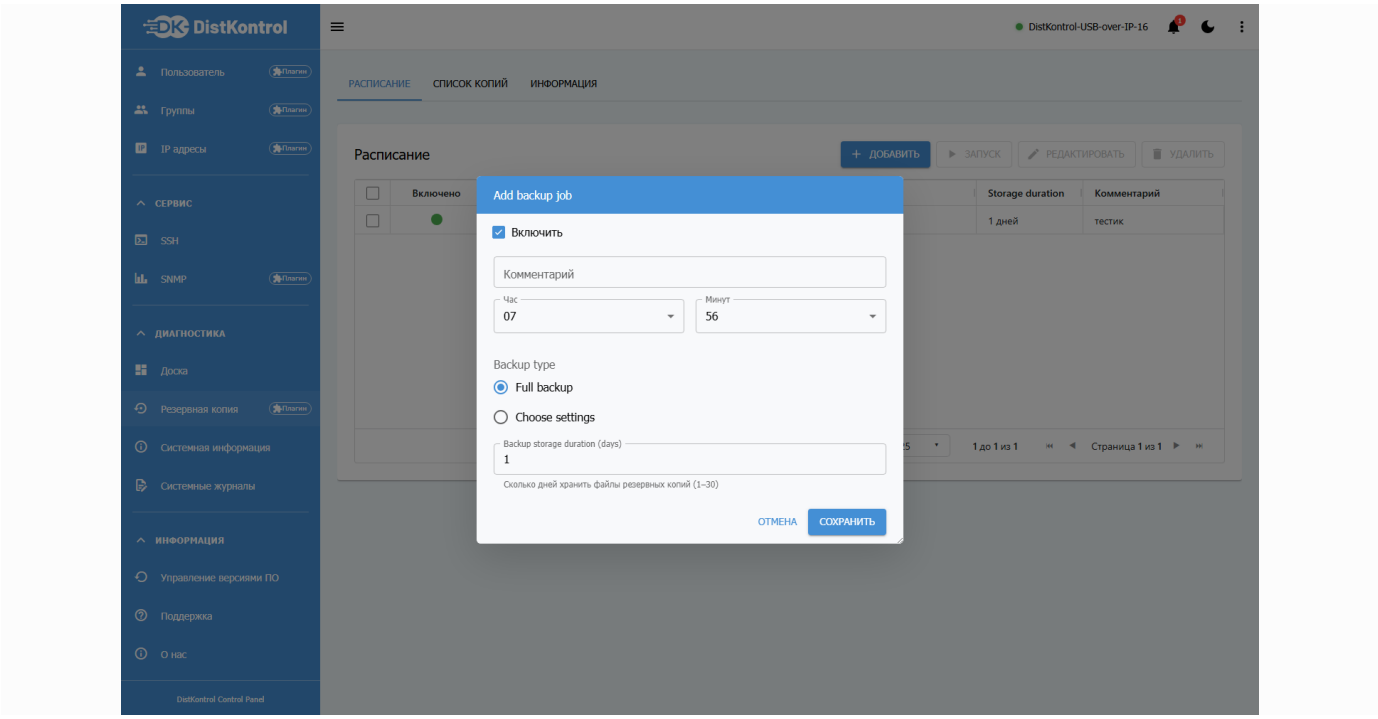

DistKontrol
DistKontrol-USB-over-IP-16
Пользователь
Группы
IP адресы
СЕРВИС
SSH
SNMP
ДИАГНОСТИКА
Доска
Резервная копия
Системная информация
Системные журналы
ИНФОРМАЦИЯ
Управление версиями ПО
Поддержка
О нас
DistKontrol Control Panel
РАСПИСАНИЕ
СПИСОК КОПИЙ
ИНФОРМАЦИЯ
Расписание
ДОБАВИТЬ
ЗАПУСК
РЕДАКТИРОВАТЬ
УДАЛИТЬ
Включено
Время
Settings list
Timestamp
Storage duration
Комментарий
10:30
Fullbackup
10:30
1 дней
тестик
Строк на странице: 25
1 до 1 из 1
Страница 1 из 1


DistKontrol
DistKontrol-USB-over-IP-16
Пользователь
Группы
IP адресы
СЕРВИС
SSH
SNMP
ДИАГНОСТИКА
Доска
Резервная копия
Системная информация
Системные журналы
ИНФОРМАЦИЯ
Управление версиями ПО
Поддержка
О нас
DistKontrol Control Panel
РАСПИСАНИЕ
СПИСОК КОПИЙ
ИНФОРМАЦИЯ
Список копий
ИМПОРТИРОВАТЬ
ЭКСПОРТ
УСТАНОВИТЬ
УДАЛИТЬ
ОБНОВЛЕНИЕ



4. Создание задания

1. **Диагностика → Резервная копия → Расписание → Добавить**.
2. Укажите время, тип копии (**полная** или **выбранные настройки**), срок хранения и комментарий.
3. Нажмите **«Сохранить»**.
4. Для немедленного создания файла выберите задачу и нажмите **«Запуск»**.



5. Перенос настроек на другое устройство

Экспорт (исходное устройство):

1. Создайте и при необходимости запустите задание.
2. Откройте **«Список копий»** → выберите файл → **«Экспортировать»** → сохраните на ПК.

Импорт (целевое устройство):

1. Установите плагин на целевом устройстве.
2. **Список копий** → **Импортировать** → загрузите файл с ПК.
3. Выберите файл → **«Установить»**.

> **Внимание**
> **«Установить»** заменяет текущие настройки устройства.

---

6. Использование с DistKontrol: SCC

Централизованные задания и кластер: 2.4.1 Резервные копии, 2.5 Кластер.

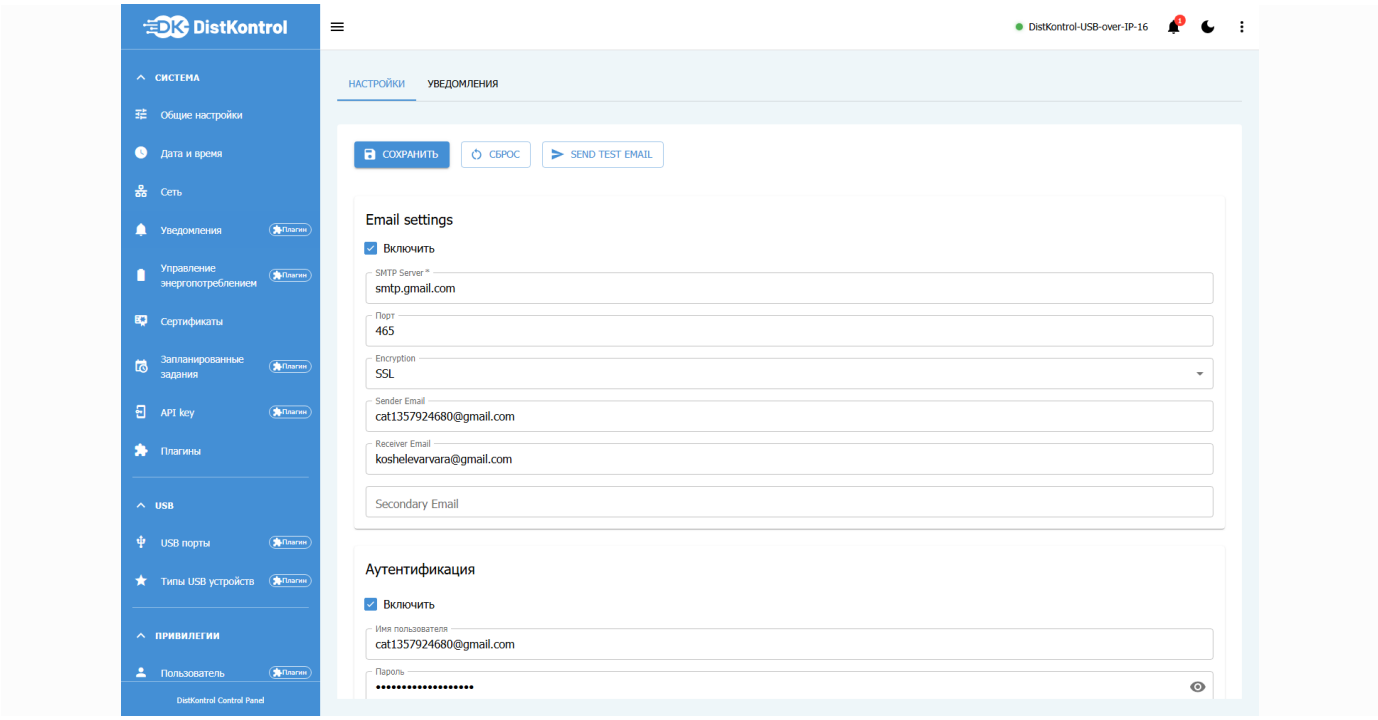
Перенос настроек: База знаний.

Плагин «Уведомления»

Идентификатор: `distkontrol-notifications`

Модуль добавляет раздел **Система** → **Уведомления** для настройки сообщений по email о событиях устройства.

Установка и удаление — в общей инструкции.



1. Краткое описание

Плагин отправляет уведомления на указанные адреса при входе в WEB-интерфейс, ошибках авторизации, блокировке входа и при критических показателях состояния устройства.

2. Настройки

Вкладки раздела: **Настройки** и **Уведомления** (список/типы событий).

Email

Параметр	Описание
Включить	Включение отправки писем
SMTP Server	Адрес SMTP-сервера
Порт	Порт SMTP (например, `465` для SSL)
Encryption	Тип шифрования (`SSL`, `TLS` и т.п.)
Sender Email	Адрес отправителя
Receiver Email	Основной получатель
Secondary Email	Дополнительный получатель

Аутентификация

Параметр	Описание
Включить	Использовать логин/пароль SMTP
Имя пользователя	Учётная запись SMTP
Пароль	Пароль SMTP

Кнопки: **Сохранить**, **Сброс**, **Send test email** (проверка отправки).

---

3. Когда отправляются уведомления

Типовые события:

- успешный вход в WEB-интерфейс;
- неверный логин или пароль;
- блокировка входа;
- высокая загрузка CPU / памяти / load average;
- изменение состояния портов;
- изменение состояния блоков питания (при наличии второго БП).

Примечание

После восстановления настроек или обновления ПО повторно введите пароль SMTP (очистите поле, сохраните, введите пароль снова и сохраните).

Плагин «Запланированные задания»

Идентификатор: `distkontrol-scheduled-tasks`

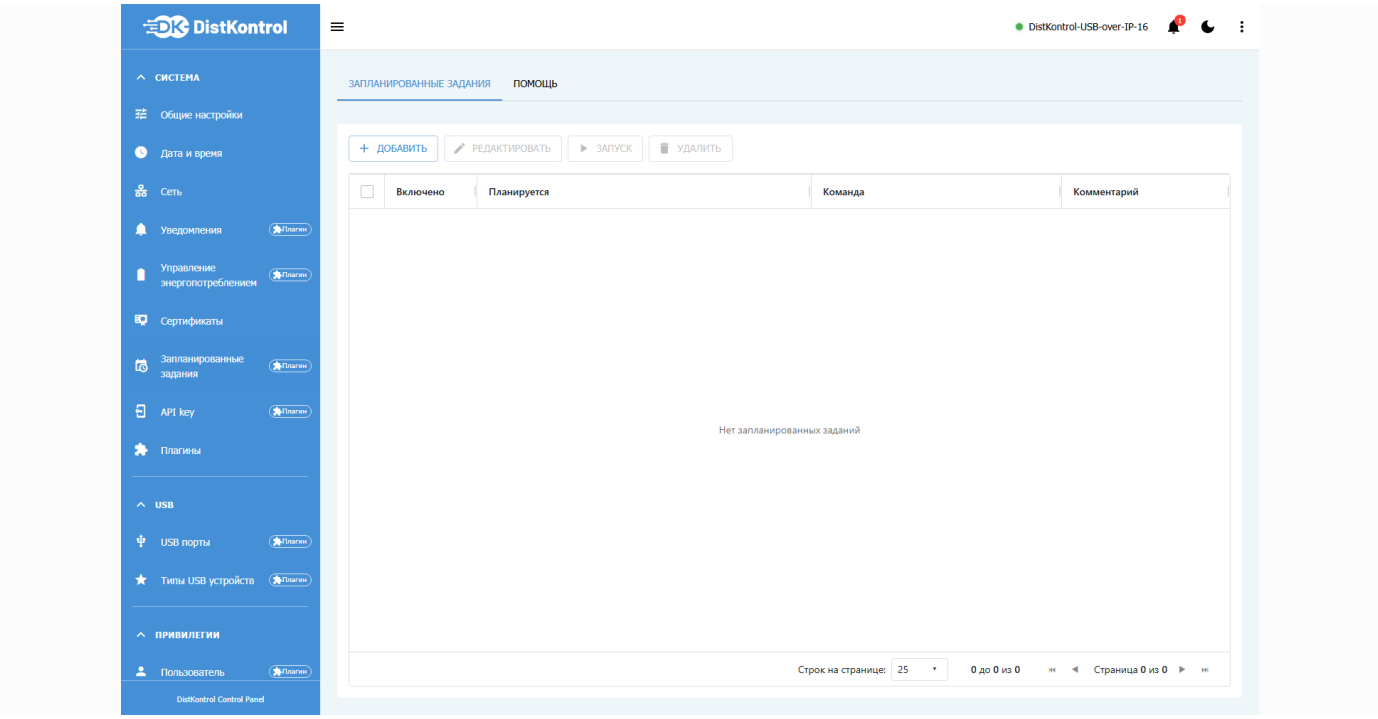
Модуль добавляет разделы:

- **Система → Запланированные задания** — задания cron (в т.ч. управление питанием USB-портов);
- **Система → Управление энергопотреблением** — выключение/перезагрузка устройства и режимы резервирования питания.

Установка и удаление — в общей инструкции.

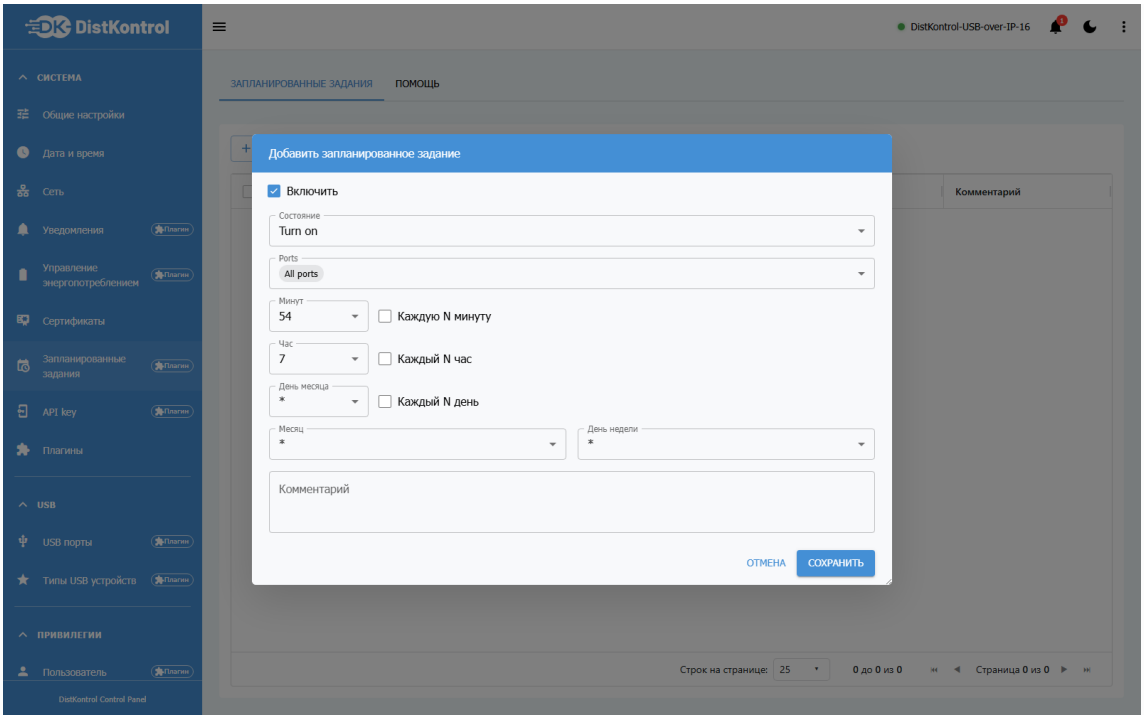
---

1. Запланированные задания



Кнопки: **Добавить**, **Редактировать**, **Запуск**, **Удалить**.

Колонки таблицы: **Включено**, **Планируется** (cron), **Команда**, **Комментарий**.



Формат cron

```
.---------------- минута (0 - 59)
| .-------------- час (0 - 23)
| | .------------ день месяца (1 - 31)
| | | .---------- месяц (1 - 12) ИЛИ jan, feb, mar ...
| | | | .-------- день недели (0 - 6) (Воскресенье=0 или 7)
| | | | |
* * * * *  команда
```

Примеры:

```
* 7 * * *        # каждый день в 7:00
*/40 */10 * * *  # повтор с интервалом по минутам/часам
```

Команды управления USB-портами

Синтаксис: `usbcontrolapi <0|1> <порт>`

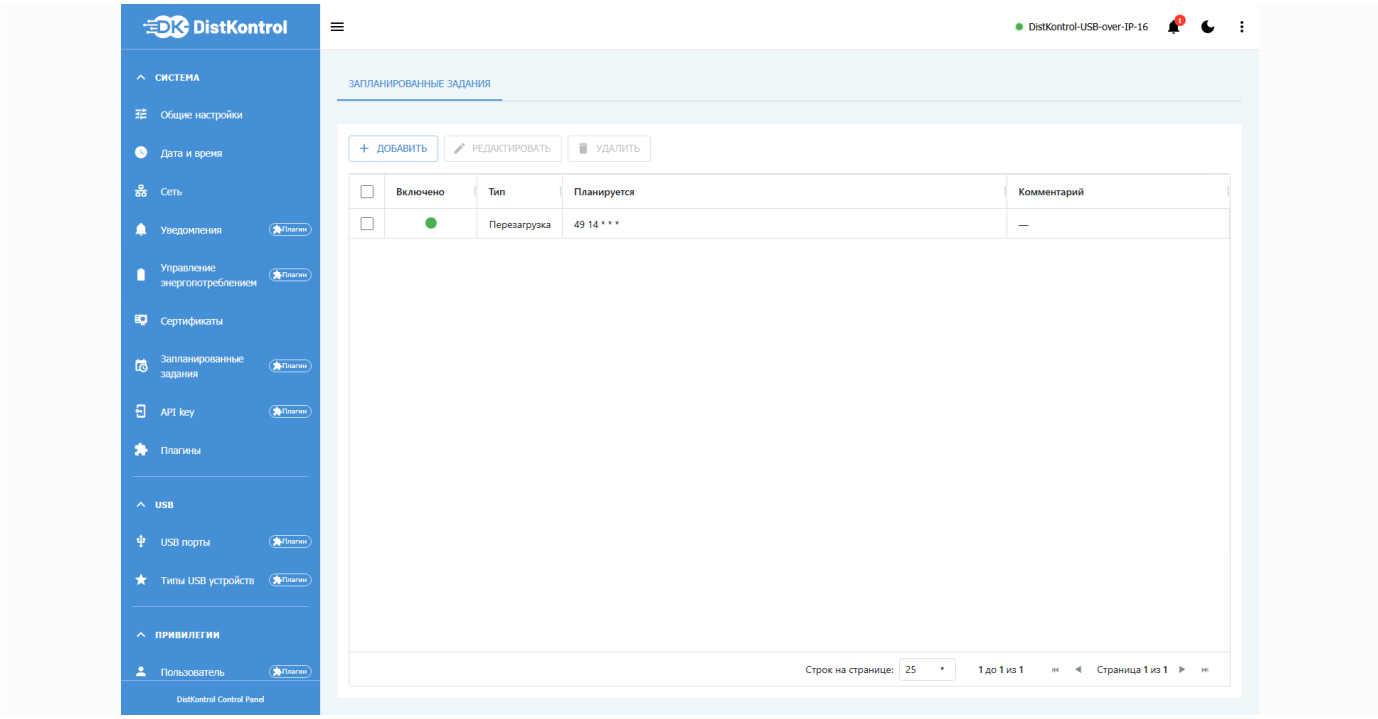
- `0` — выключить питание порта, `1` — включить;
- порт: `1.1` … `4.16`; группы: `0.0` (все), `1.0`–`4.0` (ряд).

```
usbcontrolapi 0 1.9    # выключить USB 1.9
usbcontrolapi 1 1.12   # включить USB 1.12
usbcontrolapi 1 0.0    # включить все порты
usbcontrolapi 0 2.0,3.0 # выключить ряды 2 и 3
```

Примечание

Устройство должно корректно получать время по NTP (**Система** → **Дата и время**).

2. Управление энергопотреблением



Доступные задания:

1. Выключение управляемого USB over IP концентратора.
2. Перезагрузка управляемого USB over IP концентратора.

На устройствах с **двумя блоками питания** доступны режимы резервирования:

- оба БП работают постоянно (отказоустойчивость без перезагрузки при отказе одного БП);
- работает один БП, при отказе включается второй (устройство перезагружается).

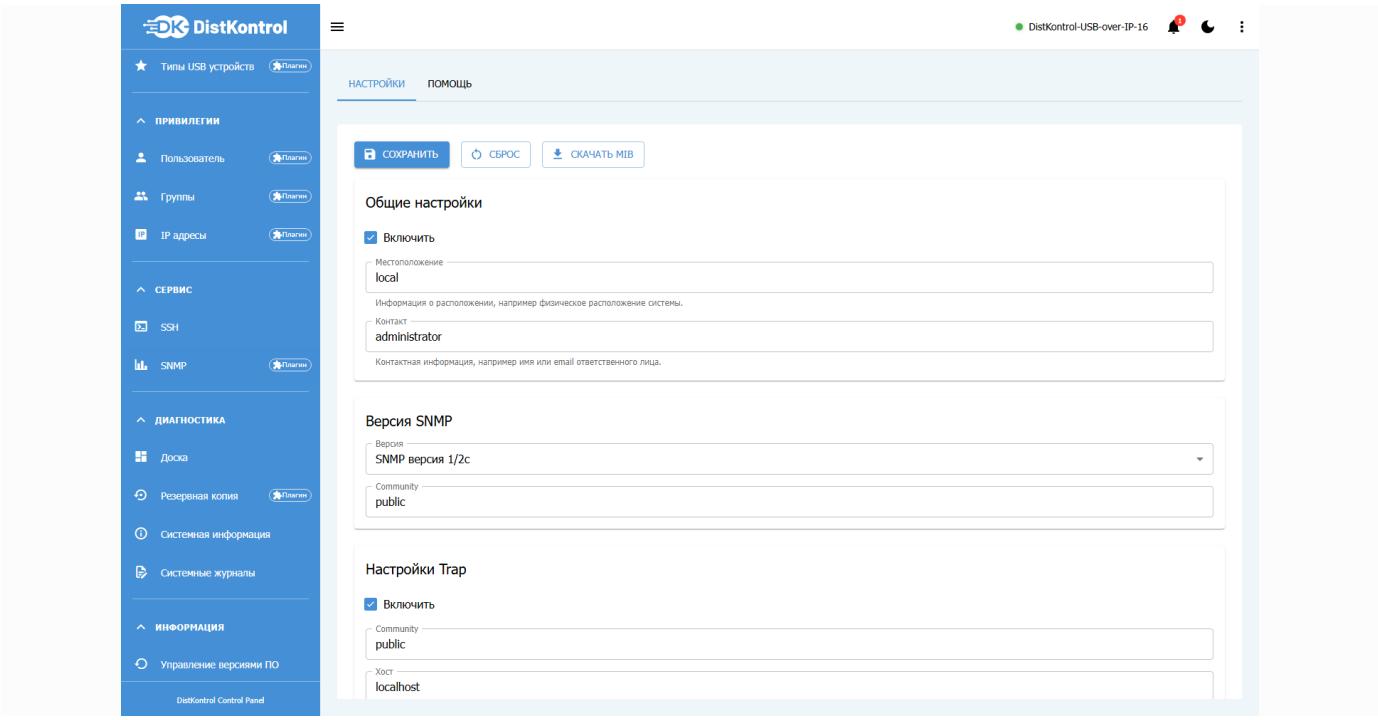
Актуальное состояние БП отображается на этой же странице; после смены режима обновите страницу.

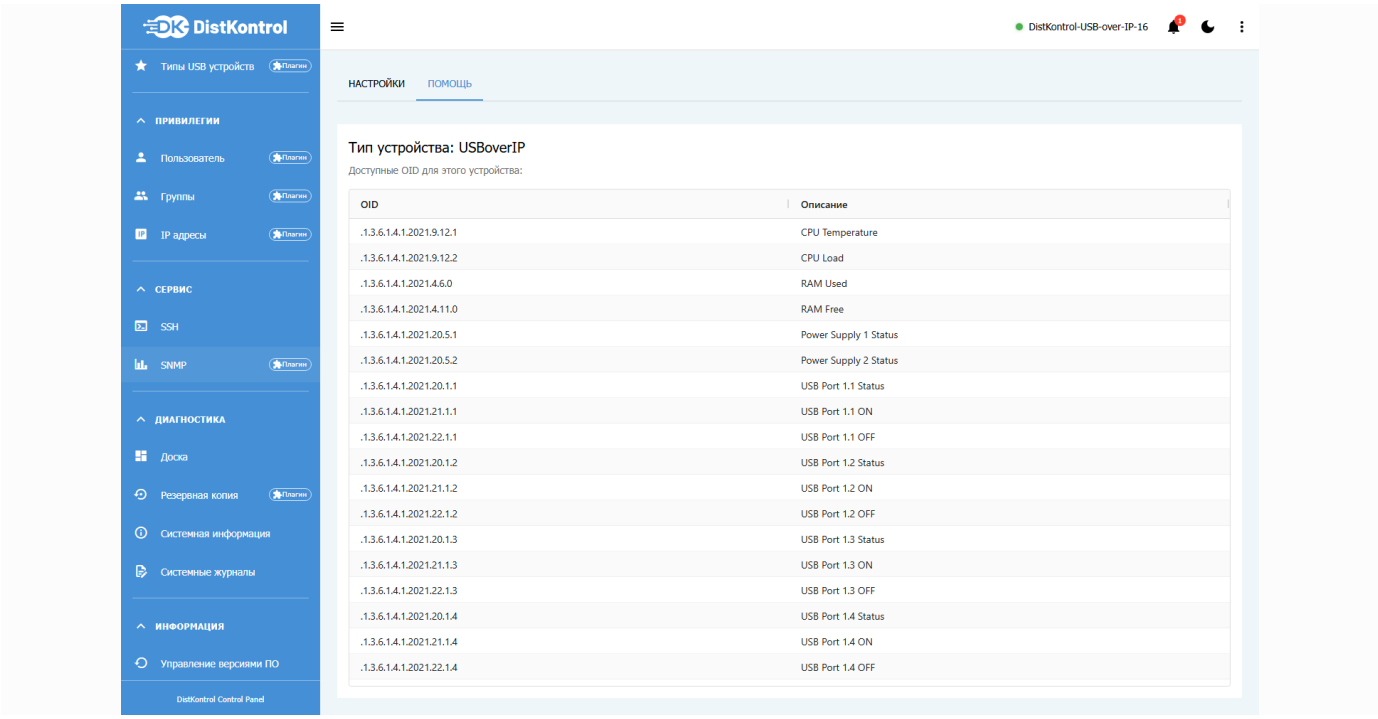
Плагин «SNMP»

Идентификатор: `distkontrol-snmp`

Модуль добавляет раздел **Сервис** → **SNMP** для мониторинга состояния устройства и USB-портов системами вроде Zabbix, Nagios и др.

Установка и удаление — в общей инструкции.





---

1. Краткое описание

Поддерживаются SNMP **v1**, **v2c**, **v3**. В заводской настройке SNMP может быть отключён — включение и настройка выполняются в этом разделе.

Кнопки: **Сохранить**, **Сброс**, **Скачать MIB**.

---

2. Настройки

Общие

Параметр	Описание
Включить	Включение службы SNMP
Местоположение	Физическое расположение (до 64 символов)
Контакт	Контакт ответственного лица (до 64 символов)

Версия SNMP

Для **v1 / v2c** задаётся **Community** (до 32 символов).

Для **v3** дополнительно:

- имя пользователя;
- уровень безопасности: `NoAuthNoPriv`, `AuthNoPriv`, `AuthPriv`;
- тип и пароль аутентификации;
- тип конфиденциальности и пароль (для `AuthPriv`).

Trap

Параметр	Описание
Включить	Отправка SNMP trap
Community	Community для trap
Хост	Адрес получателя trap

---

3. Примеры OID

OID	Параметр
`.1.3.6.1.2.1.1.5.0`	Имя хоста
`.1.3.6.1.4.1.2021.9.12.1`	Температура CPU
`.1.3.6.1.4.1.2021.9.12.2`	CPU Load
`.1.3.6.1.4.1.2021.10.1.3.1`	1 minute CPU Load
`.1.3.6.1.4.1.2021.10.1.3.2`	5 minute CPU Load
`.1.3.6.1.4.1.2021.10.1.3.3`	15 minute CPU Load
`.1.3.6.1.4.1.2021.11.11.0`	Idle CPU time (%)
`.1.3.6.1.4.1.2021.4.6.0`	Total RAM used
`.1.3.6.1.4.1.2021.4.11.0`	Total RAM Free
`.1.3.6.1.2.1.25.1.1.0`	Uptime

OID	Параметр
`.1.3.6.1.4.1.2021.20.5.1` / `.2`	Состояние БП 1 / 2 (1/0)
`.1.3.6.1.4.1.2021.20.<ряд>.<порт>`	Состояние USB-порта (1/0)

Порт SNMP: **161/UDP**. Перед настройкой мониторинга проверьте получение данных (`snmpget` / SnmpGet).

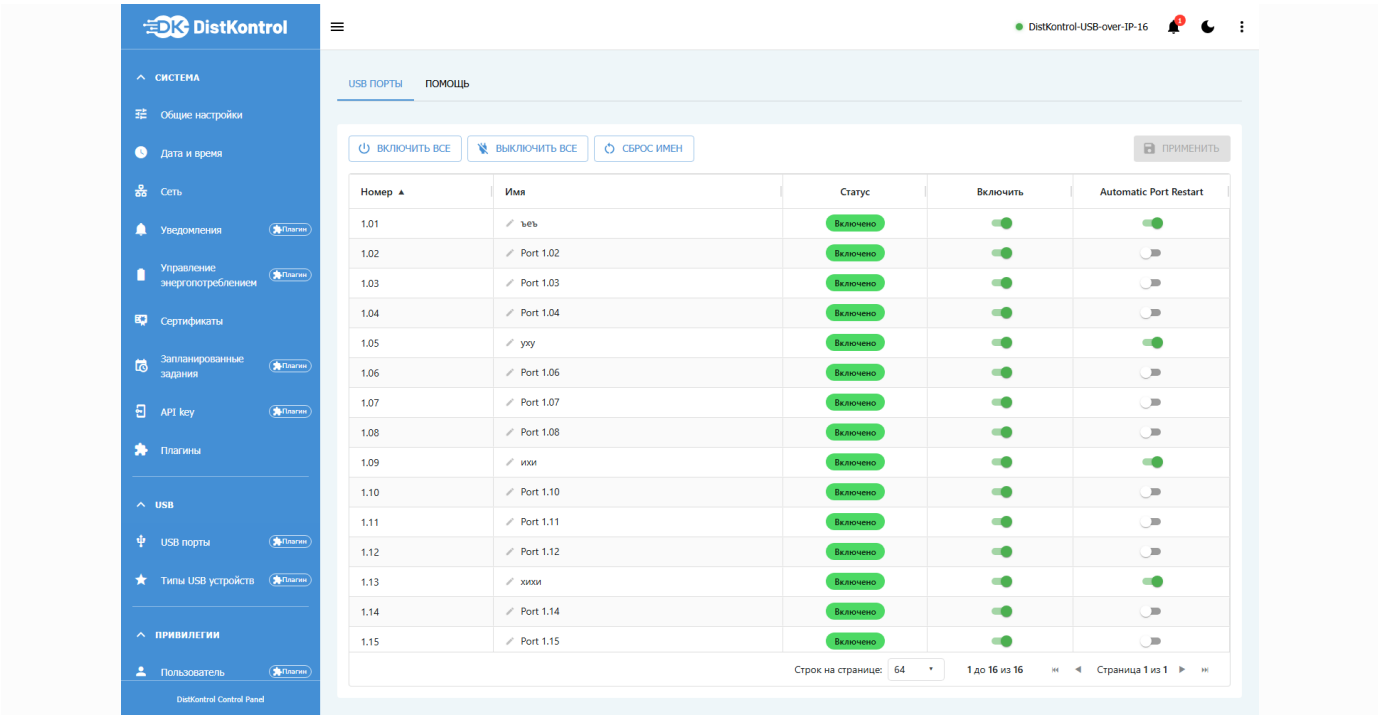
Плагин «Входы» (USB/PDU)

Идентификатор: `distkontrol-inputs`

Модуль добавляет раздел управления входами устройства. На USB over IP концентраторах это **USB → USB порты**.

Установка и удаление — в общей инструкции.

Подробное описание для DistKontrolUSB v6: 5.3 USB.



1. Краткое описание

Плагин позволяет включать и выключать питание портов (входов), задавать отображаемые имена и настраивать автоматический перезапуск порта.

2. USB порты (USB over IP)

Кнопки:

Кнопка	Действие
Включить все	Подать питание на все порты
Выключить все	Снять питание со всех портов
Сброс имён	Вернуть имена портов по умолчанию
Применить	Сохранить изменения имён и переключателей

Колонки таблицы:

- **Номер** — идентификатор порта (`1.01` …);
- **Имя** — отображаемое имя (редактирование по месту);

- **Статус** — включён / выключен;
- **Включить** — тумблер питания порта;
- **Автоматический перезапуск порта** — снятие и подача питания при отключении пользователя от USB-устройства в порту.

Если отображаемое имя равно `DEFAULT`, `default` или `0`, имя сбрасывается к значению по умолчанию. Для применения изменений нажмите **«Применить»**.

На вкладке **«Помощь»** — краткая справка по разделу.

Плагин «USB over IP»

Идентификатор: `distkontrol-overip`

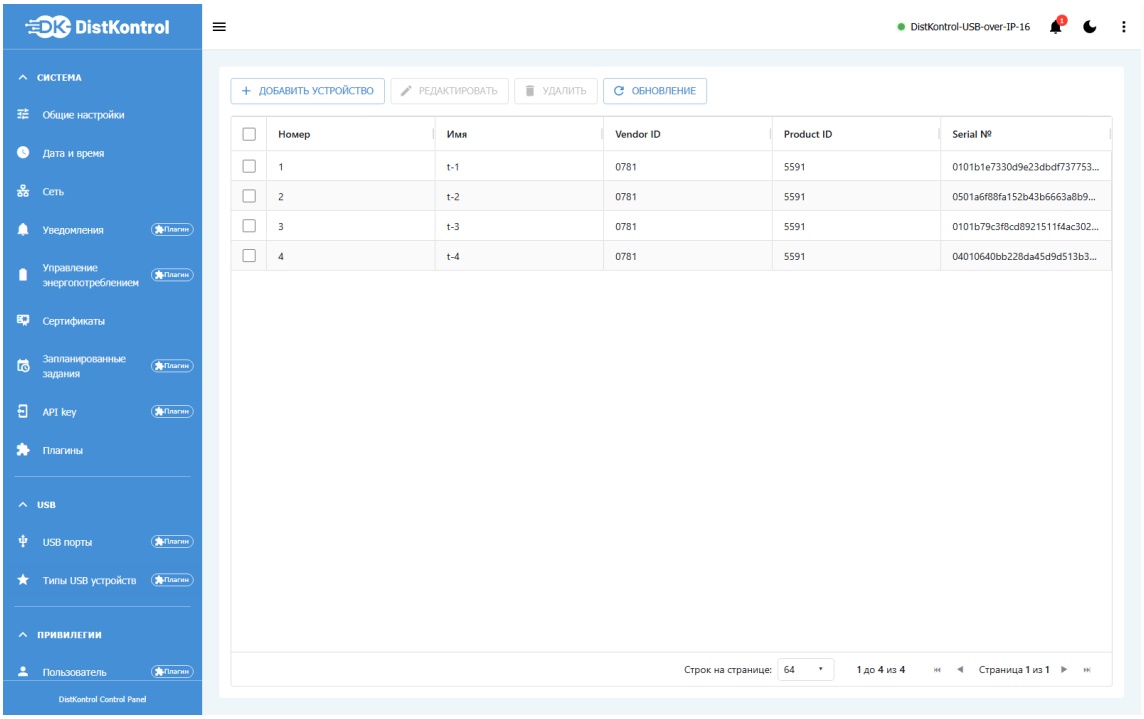
Модуль добавляет функции USB over IP в WEB-интерфейс:

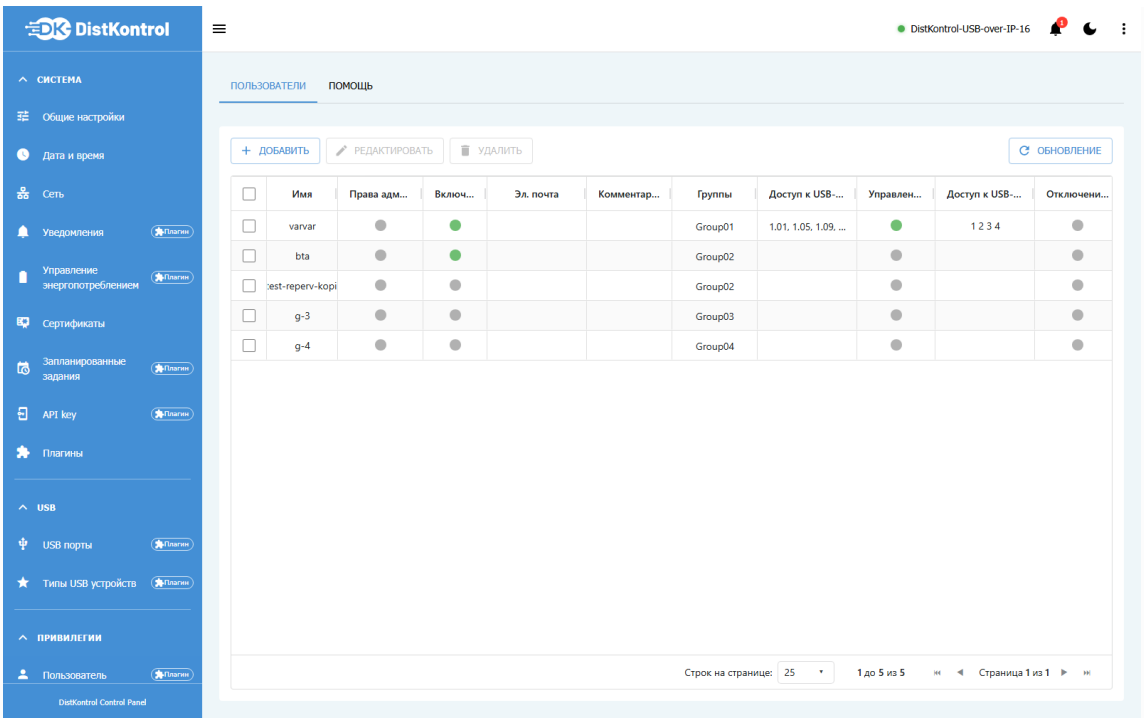
- **USB → Типы USB устройств**
- **Привилегии → Пользователь**
- **Привилегии → Группы**
- **Привилегии → IP адреса**

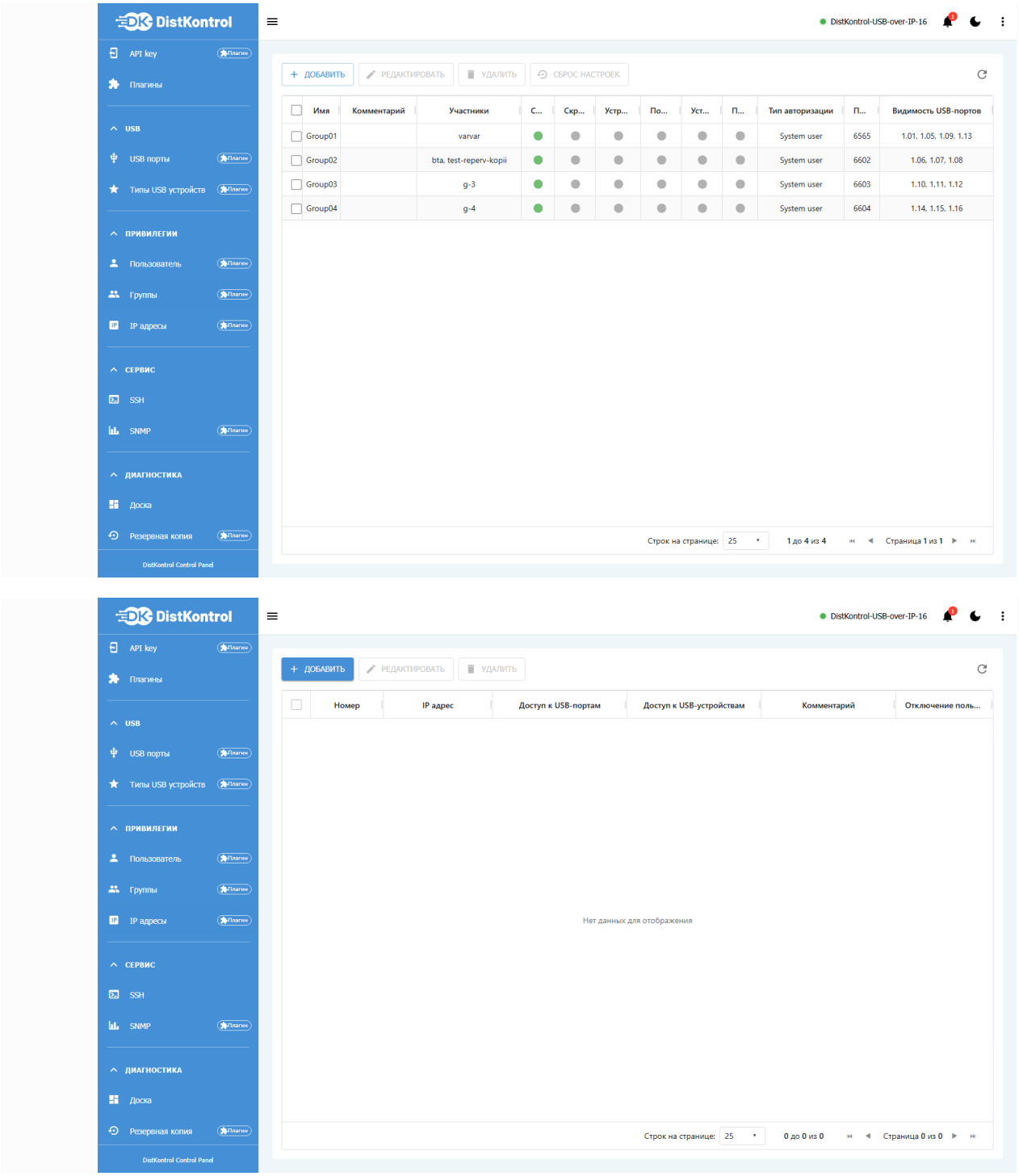
Установка и удаление — в общей инструкции.

Полное описание для DistKontrolUSB v6: 5.4 Управление правами доступа, также 5.3.2 Типы USB-устройств.

Управление питанием портов см. в плагине distkontrol-inputs.


DistKontrol
DistKontrol-USB-over-IP-16
СИСТЕМА
Общие настройки
Дата и время
Сеть
Уведомления
Управление энергопотреблением
Сертификаты
Запланированные задания
API key
Плагины
USB
USB порты
Типы USB устройств
ПРИВИЛЕГИИ
Пользователь
DistKontrol Control Panel
ДОБАВИТЬ УСТРОЙСТВО
РЕДАКТИРОВАТЬ
УДАЛИТЬ
ОБНОВЛЕНИЕ
Номер
Имя
Vendor ID
Product ID
Serial №
1 t-1 0781 5591 0101b1e7330d9e23dbdf737753...
2 t-2 0781 5591 0501a6f88fa152b43b6663a8b9...
3 t-3 0781 5591 0101b79c3f8cd892511f4ac302...
4 t-4 0781 5591 04010640bb228da45d9d513b3...
Строк на странице: 64
1 до 4 из 4
Страница 1 из 1


DistKontrol
DistKontrol-USB-over-IP-16
СИСТЕМА
ПОЛЬЗОВАТЕЛИ
ПОМОЩЬ
Общие настройки
Дата и время
Сеть
Уведомления
Управление энергопотреблением
Сертификаты
Запланированные задания
API key
Плагины
USB
USB порты
Типы USB устройств
ПРИВИЛЕГИИ
Пользователь
DistKontrol Control Panel
ДОБАВИТЬ
РЕДАКТИРОВАТЬ
УДАЛИТЬ
ОБНОВЛЕНИЕ
Имя
Права адм...
Включ...
Эл. почта
Комментар...
Группы
Доступ к USB-...
Управлен...
Доступ к USB-...
Отключени...
varvar Group01 1.01, 1.05, 1.09, ... 1 2 3 4
bta Group02
est-reperv-kopi Group02
g-3 Group03
g-4 Group04
Строк на странице: 25
1 до 5 из 5
Страница 1 из 1



Расширенный текст раздела (черновик / полный разбор настроек доступа) также сохранён в docs/distkontrol-overip.md.

Плагин «Phones and Modems»

Идентификатор: `distkontrol-fix-phone-and-modem`

Плагин улучшает совместимость USB-телефонов и модемов с DistKontrolUSB. Отдельного пункта меню в WEB-интерфейсе не добавляет — работает в фоне после установки.

Установка и удаление — в общей инструкции.

---

1. Краткое описание

После установки и включения плагина в разделе **Система** → **Плагины** (категория **USB**) устройство корректнее обрабатывает ряд USB-телефонов и модемов при работе через USB over IP.

---

2. Как пользоваться

1. Установите плагин из файла сборки.
2. Убедитесь, что в списке плагинов статус активен (зелёный индикатор).
3. Перезагрузите страницу браузера при необходимости.
4. Подключите телефон/модем к порту и проверьте работу в клиентском приложении.

Отдельных настроек в WEB-интерфейсе у плагина нет.

Клиентское приложение
DistKontrolUSB Client

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Москва
2026 г

Клиентское приложение DistKontrolUSB Client

Информация

Скачать документацию в формате pdf можно по ссылке

Оглавление

1 Установка клиента DistKontrolUSB Client

- 1.1 Скачивание
- 1.2 Установка
- 1.3 Первоначальная настройка
- 1.4 Установка драйвера
- 1.5 Внешний вид

2 Настройка клиента DistKontrolUSB Client

- 2.1 Добавление концентратора
- 2.2 Управление отображением информации о пользователях USB устройств
- 2.3 Настройка меню клиентского приложения
- 2.4 Сброс настроек клиентского приложения
- 2.5 Комбинации клавиш клиентского приложения DistKontrolUSB
- 2.6 Изменение языка

3 Управление клиентом DistKontrolUSB Client скриптами или из командной строки

4 Дополнительные возможности при работе с клиентом DistKontrolUSB

5 Примеры управления клиентом DistKontrolUSB Client для Windows и Linux

---

Связанная документация: руководство USB over IP v5 (5.4 Управление правами, 5.3 USB). **База знаний:** настройка клиента, ошибки Hub failed (0x00000001), (0x00000103), Linux — драйверы USBIP.

- 5.1 Алгоритм создания пакетного файла управления клиентом для Windows
- 5.2 Алгоритм установки и настройки демона для Linux

1 Установка клиента DistKontrolUSB Client

1.1 Скачивание

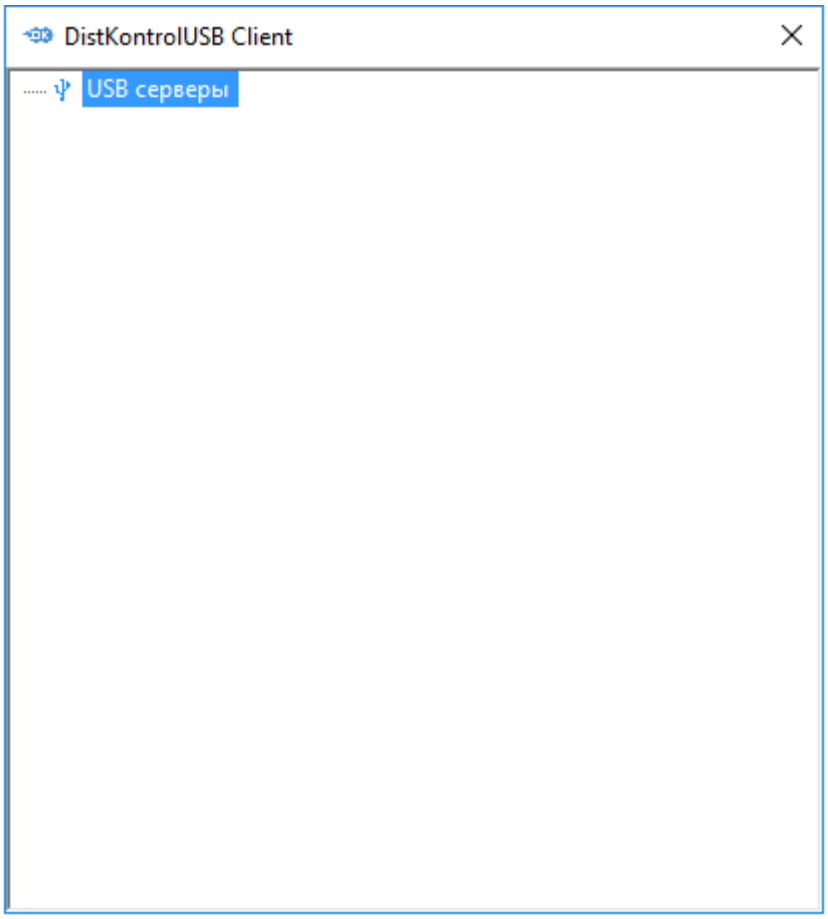
Клиент USB можно скачать с самого устройства подключения USB по сети (пройдя в WEB-интерфейсе по пути **"Информация" - "Поддержка"**, см. 5.7.1.3 Поддержка) или с сайта. Необходимо скачать и запустить соответствующее ПО.

См. База знаний — Где скачать DistkontrolUSB Client.

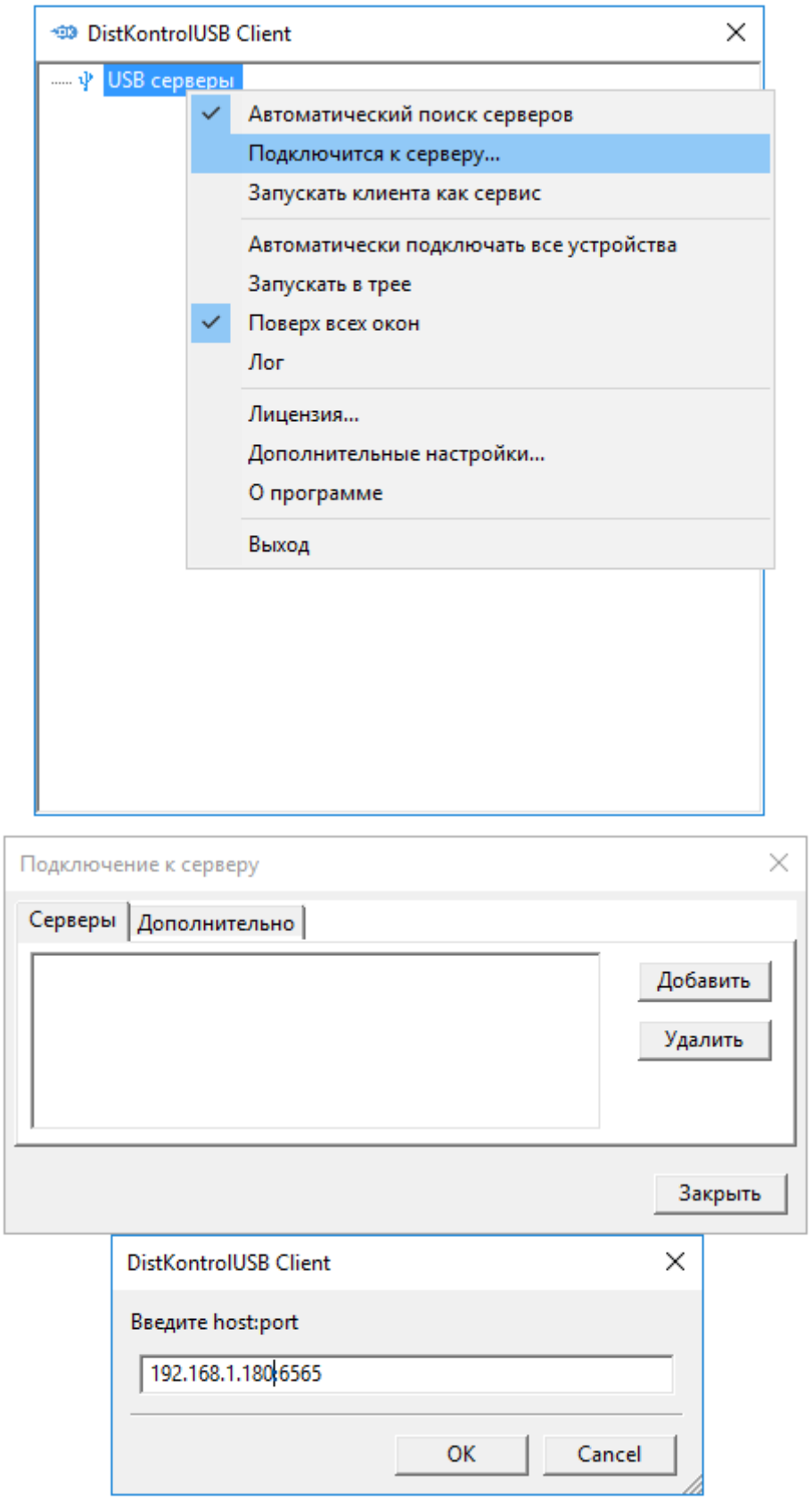
1.2 Установка

Во время установки появится уведомление центра безопасности Windows. Необходимо разрешить приложению внесение изменений.

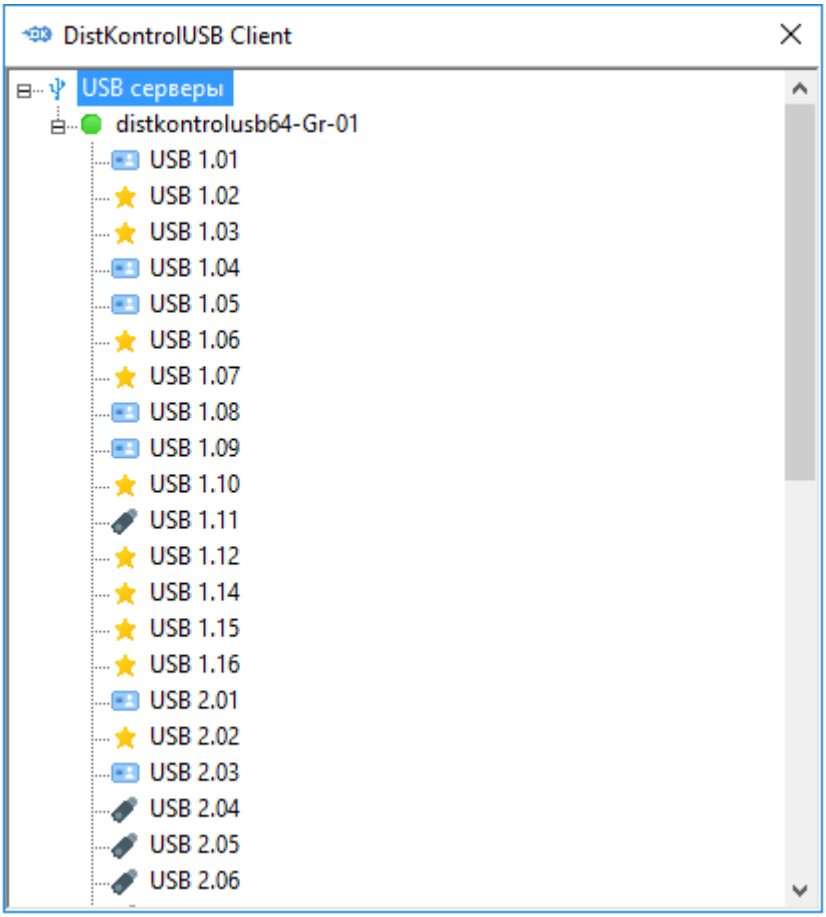
1.3 Первоначальная настройка



Для отображения USB-устройств подключенных к концентратору необходимо добавить группу концентратора в клиентском приложении:

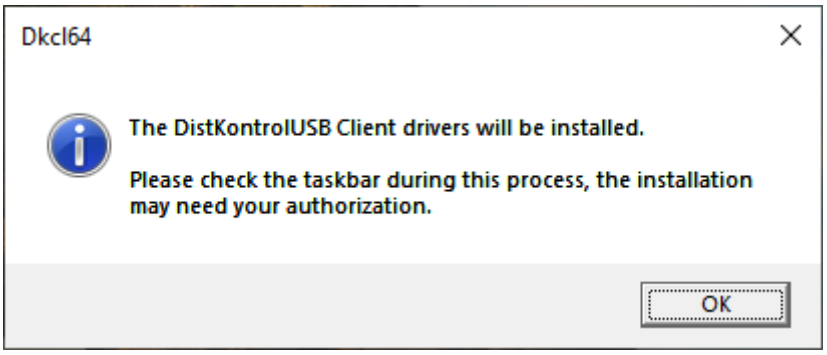


При подключении к USB over IP USB устройств они будут видны в клиенте и их будет можно подключить к компьютеру:

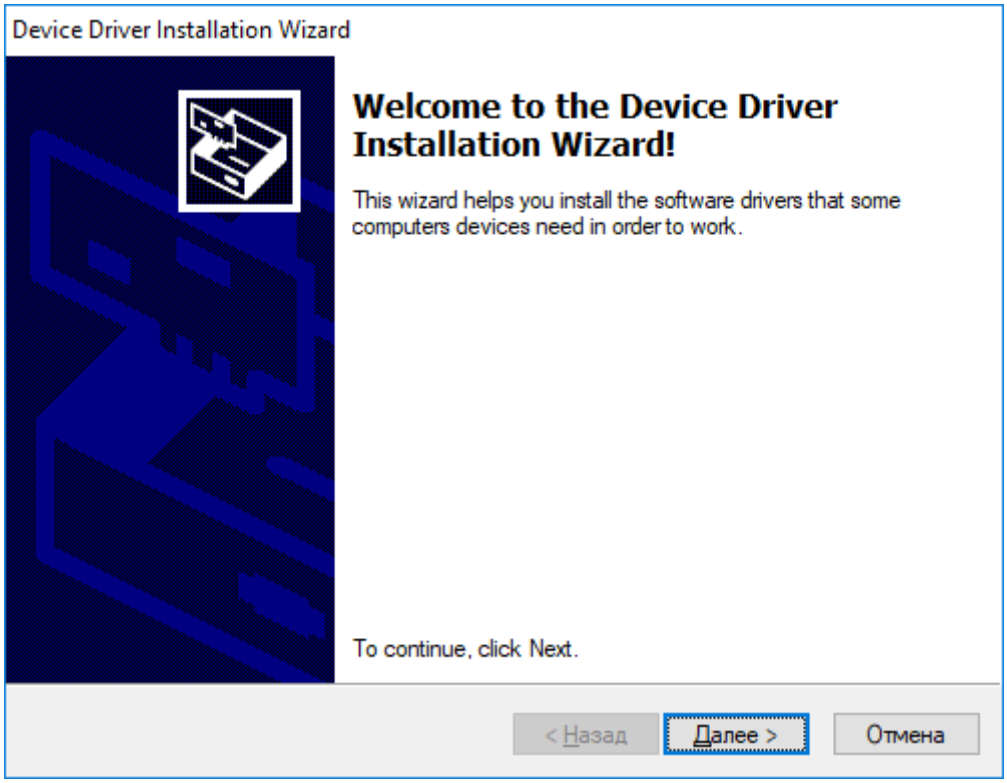


1.4 Установка драйвера

При первом подключении к USB устройству будет предложена установка драйвера USB over IP:



Во время установки появится уведомление центра безопасности Windows. Необходимо разрешить приложению внесение изменений. Нажать «Установить».

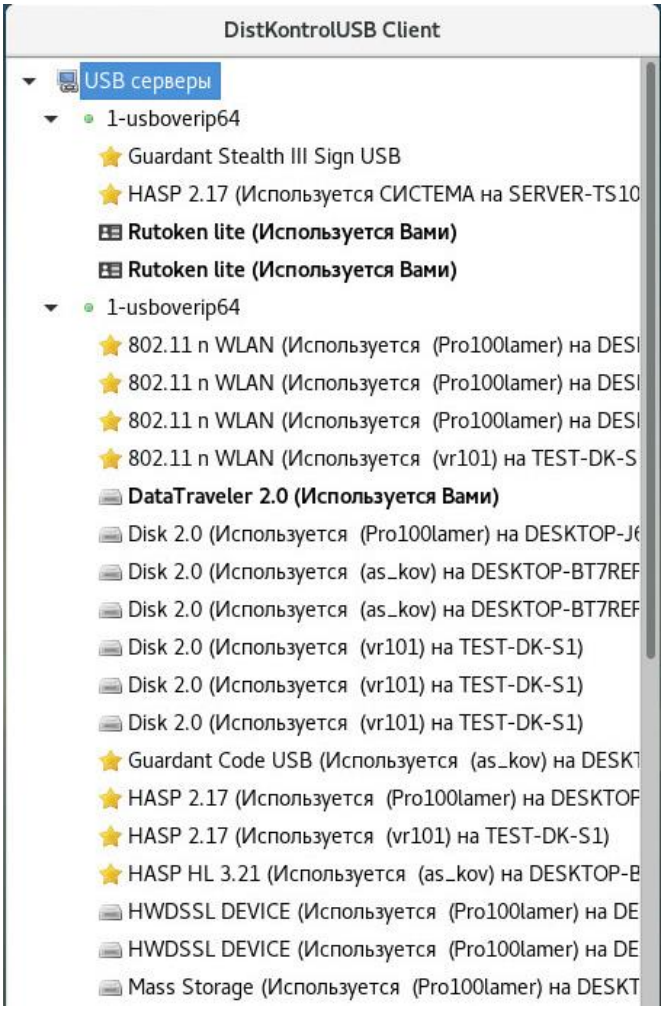


После запуска отобразится окно USB клиента.

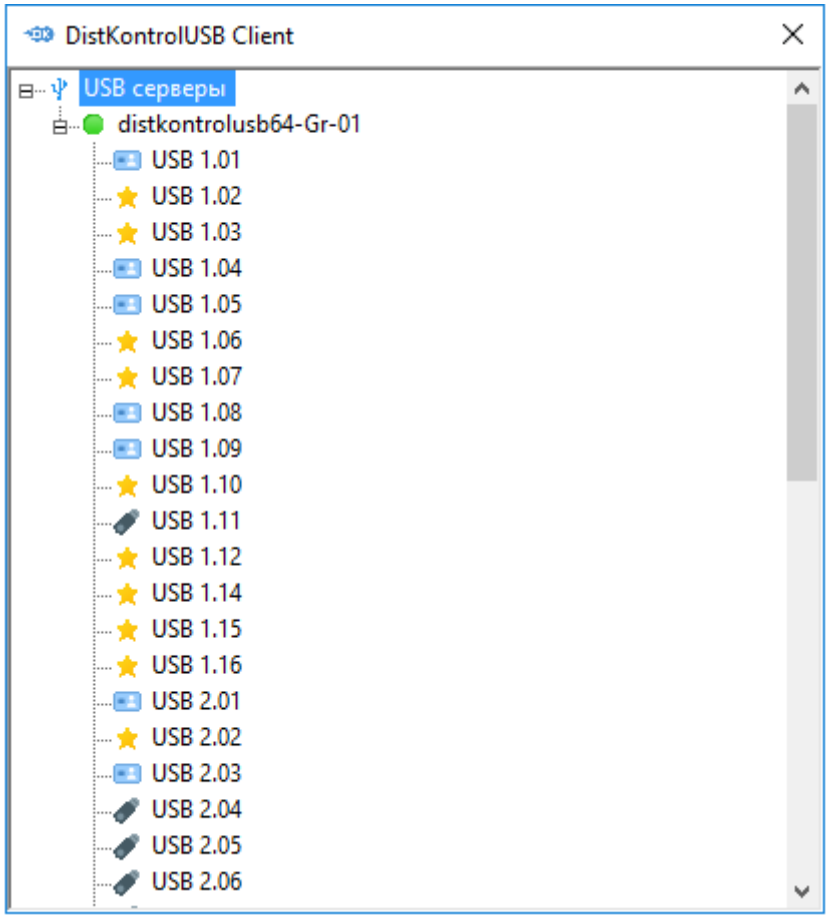
1.5 Внешний вид

Доступные устройства USB будут отображаться в виде дерева. Щелкните правой кнопкой мыши на устройстве, которое вы хотите использовать, и выберите «Использовать». После этого он будет напрямую подключен к вашему компьютеру (машине) и может использоваться как локальное устройство.

Linux


DistKontrolUSB Client
USB серверы
1-usboverip64
Guardant Stealth III Sign USB
HASP 2.17 (Используется СИСТЕМА на SERVER-TS10
Rutoken lite (Используется Вами)
Rutoken lite (Используется Вами)
1-usboverip64
802.11 n WLAN (Используется (Pro100lamer) на DESI
802.11 n WLAN (Используется (Pro100lamer) на DESI
802.11 n WLAN (Используется (Pro100lamer) на DESI
802.11 n WLAN (Используется (vr101) на TEST-DK-S
DataTraveler 2.0 (Используется Вами)
Disk 2.0 (Используется (Pro100lamer) на DESKTOP-J6
Disk 2.0 (Используется (as_kov) на DESKTOP-BT7REF
Disk 2.0 (Используется (as_kov) на DESKTOP-BT7REF
Disk 2.0 (Используется (vr101) на TEST-DK-S1)
Disk 2.0 (Используется (vr101) на TEST-DK-S1)
Disk 2.0 (Используется (vr101) на TEST-DK-S1)
Guardant Code USB (Используется (as_kov) на DESKT
HASP 2.17 (Используется (Pro100lamer) на DESKTOP
HASP 2.17 (Используется (vr101) на TEST-DK-S1)
HASP HL 3.21 (Используется (as_kov) на DESKTOP-B
HWDSSL DEVICE (Используется (Pro100lamer) на DE
HWDSSL DEVICE (Используется (Pro100lamer) на DE
Mass Storage (Используется (Pro100lamer) на DESKT

Windows



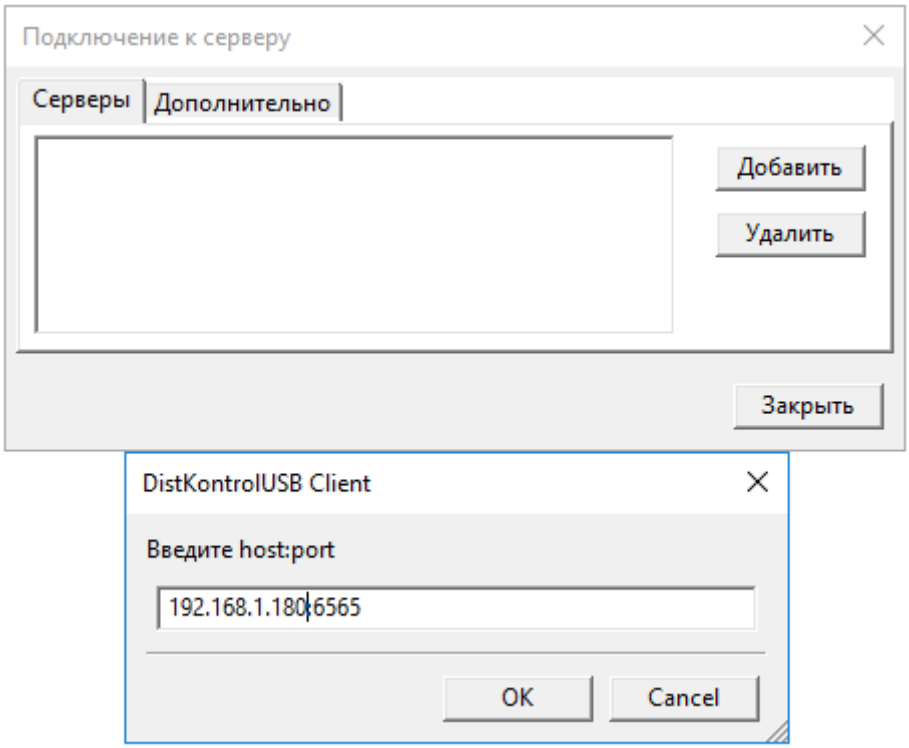
Информация

DistKontrolUSB Client для Linux устройства аппаратного подключения USB посети использует встроенный драйвер usbip для Linux. (Рекомендуется использовать ядро (4.9+) для максимальной совместимости).

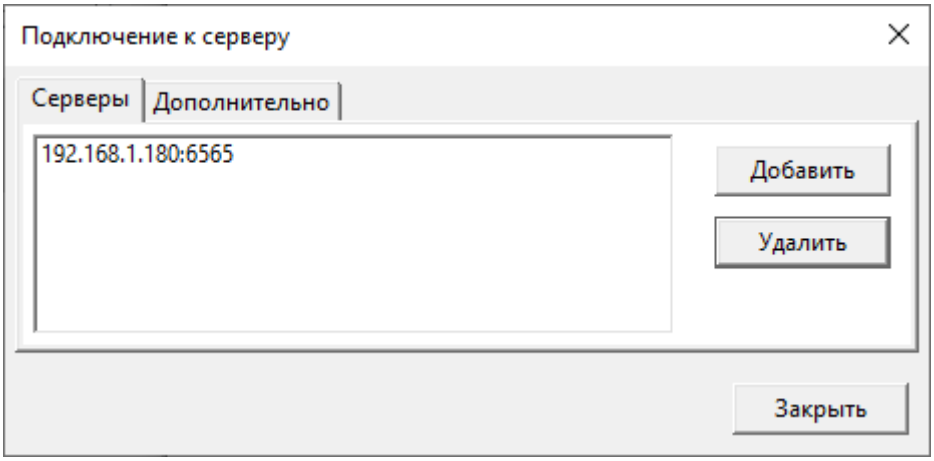
2 Настройка клиента DistKontrolUSB Client

2.1 Добавление концентратора

Для добавления адреса управляемого USB over IP концентратора можно указать (для использования, например, в глобальной сети), для этого правой кнопкой мыши нажать на **USB серверы** и выбрать **"Подключиться к серверу"**.



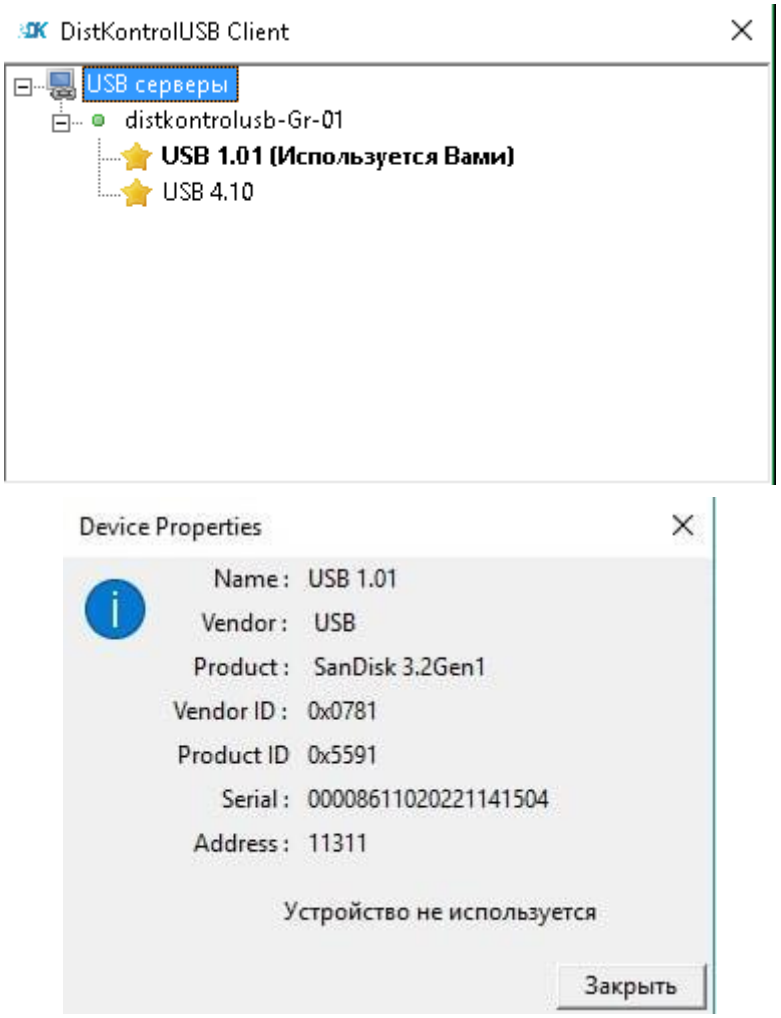
В окне **"Подключиться к серверу"** нажать **"Добавить"**.
Ввести настройки сервера в формате `адрес:порт` и нажать **ОК**. Порт: `6565`. Здесь необходимо указать IP-адрес концентратора.



В окне **"Подключиться к серверу"** нажать **"Закрыть"**.

2.2 Управление отображением информации о пользователях USB-устройств

Управляемый USB over IP концентратор позволяет включать и выключать отображение информации в клиентском приложении о пользователях, использующих USB устройства.
По умолчанию отображение информации включено. В примере ниже, на **USBoverIP64** концентраторе отображение информации включено, на **USBoverIP32** концентраторе выключено.



Управление отображением информации о пользователях USB устройств осуществляется в **WEB-интерфейсе** устройства на странице **"Группы" - "Редактировать" - "Скрывать"** информацию о пользователях USB в клиенте» (Для применения, включить и сохранить).

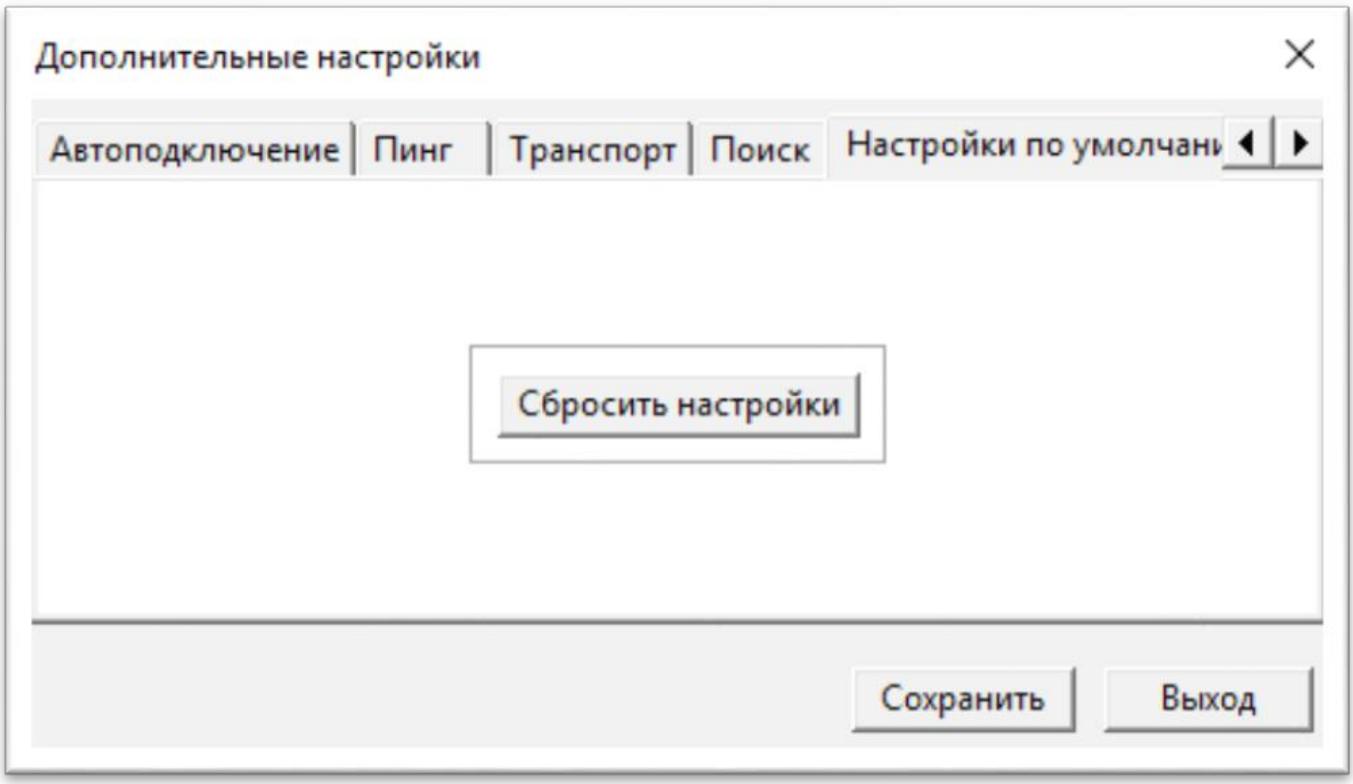
2.3 Настройка меню клиентского приложения

Клиент сохраняет все свои параметры в одном текстовом файле:

- **Windows**: `c:\Users\Username\AppData\Roaming\dkcl.ini`
- **OSX**: `/Users/Username/Library/Preferences/dkcl Preferences`
- **Linux**: `~/.dkcl`

Этот файл обновляется при изменении настроек. При первом запуске клиент создает файл конфигурации по умолчанию.
Для сброса ранее сохранённого пароля, необходимо сбросить настройки клиента:

1. Правой кнопкой мыши по **"USB серверы"** → **"Дополнительные настройки"**.
2. Вкладка **"Настройки по умолчанию"** расположена в самом конце.



2.4 Сброс настроек клиентского приложения

Для сброса всех настроек клиентского приложения:

1. Правой кнопкой мыши по **"USB серверы"** → **"Дополнительные настройки"**.
2. Вкладка **"Настройки по умолчанию"** расположена в самом конце.

Будут сброшены:

- Номера портов
- Настройки SSL
- Отображение скрытых устройств
- Имена и скрытие устройств.

2.5 Комбинации клавиш клиентского приложения

Для удаления сохраненных паролей:

1. Нажмите `SHIFT+F9` — удаление сохраненного пароля выбранного порта.
2. Нажмите `SHIFT+F8` — удаление всех сохраненных паролей для всех устройств.

2.6 Изменение языка

Интерфейс клиента мультиязычный. Для выбора языка:

1. Клик правой кнопкой мыши на **USB серверы** → **Дополнительные настройки**.
2. На вкладке **Язык** выбрать язык интерфейса → **Сохранить**.

3 Управление клиентом DistKontrolUSB скриптами или из командной строки

Клиент USB может управляться скриптами или из командной строки. Это полезно, когда:

- Вы хотите управлять клиентом при запуске в качестве службы
- Вы хотите управлять клиентом только через консольный сеанс, например, ssh
- Вы хотите создать собственный графический интерфейс
- Вы хотите управлять с помощью пакетного файла (Windows) или bash (OSX/Linux) скрипта

Запустите клиент с аргументом `-t HELP`, чтобы получить список доступных команд:

```
C:\Users\user1> dkcl64.exe -t help
List devices:
 "LIST"
Get the detailed full client state as an XML Document:
 "GET CLIENT STATE"
Use a device:
 "USE,<address>[,password]"
Stop using a device:
 "STOP USING,<address>"
Stop using all devices on all clients:
 "STOP USING ALL"
Stop using all devices just for this client:
 "STOP USING ALL LOCAL"
Rename server:
 "SERVER RENAME,<hubaddress:port>,<new name>"
Turn auto-use all devices on:
 "AUTO USE ALL"
Turn Auto-use all devices on this hub on/off:
 "AUTO USE HUB,<server name>"
Turn Auto-use any device on this port on/off:
 "AUTO USE PORT,<address>"
Turn Auto-use this device on any port on/off:
 "AUTO USE DEVICE,<address>"
Turn Auto-use this device on this port on/off:
 "AUTO USE DEVICE PORT,<address>"
Clear all auto-use settings:
 "AUTO USE CLEAR ALL"
Manually specify a hub to connect to:
 "MANUAL HUB ADD,<address>[:port]"
Remove a manually specified hub:
 "MANUAL HUB REMOVE,<address>[:port]"
Remove all manually specified hubs:
 "MANUAL HUB REMOVE ALL"
List manually specified hubs:
 "MANUAL HUB LIST"
Clear client log:
 "CLEAR LOG"
```

```
Set a custom device event:
 "CUSTOM EVENT,<address>,<event>"
Turn auto-find off:
 "AUTOFIND"
Shutdown the client:
 "EXIT"
Help:
 "HELP"
```

Пример использования в Windows:

1. Убедитесь, что клиент уже работает (зеленый значок USB на панели задач или фоновая служба):

```
C:\Users\user1> dkcl64.exe -t list
DistKontrolUSB Client IPC, below are the available devices:
(Value in brackets = address, * = Auto-Use)
USBoverIP16-1 (USBoverIP16:6565)
 --> Mass Storage Device (USBoverIP16.114)
 --> USB Optical Mouse (USBoverIP16.113)
 --> USB Keyboard (USBoverIP16.115)
...
```

2. Использование устройства:

```
dkcl64.exe -t "USE, USBoverIP16.1122"
# Ответ: "OK"
```

3. Остановка использования устройства:

```
dkcl64.exe -t "STOP USING, USBoverIP16.1122"
```

4. Автоматическое использование устройств на хабе:

```
dkcl64.exe -t "AUTO USE HUB, USBoverIP16:6565"
```

Запуск клиента как службы/демона:

- Windows/OSX:
  ПКМ на **USB Hubs** → **Install Client as a Service** (если установлено: **Uninstall Client Service**)
- Linux:

```
sudo ./dkclientx86_64 -n  # Запуск демона
./dkclientx86_64 -t "HELP"  # Консольный режим
```

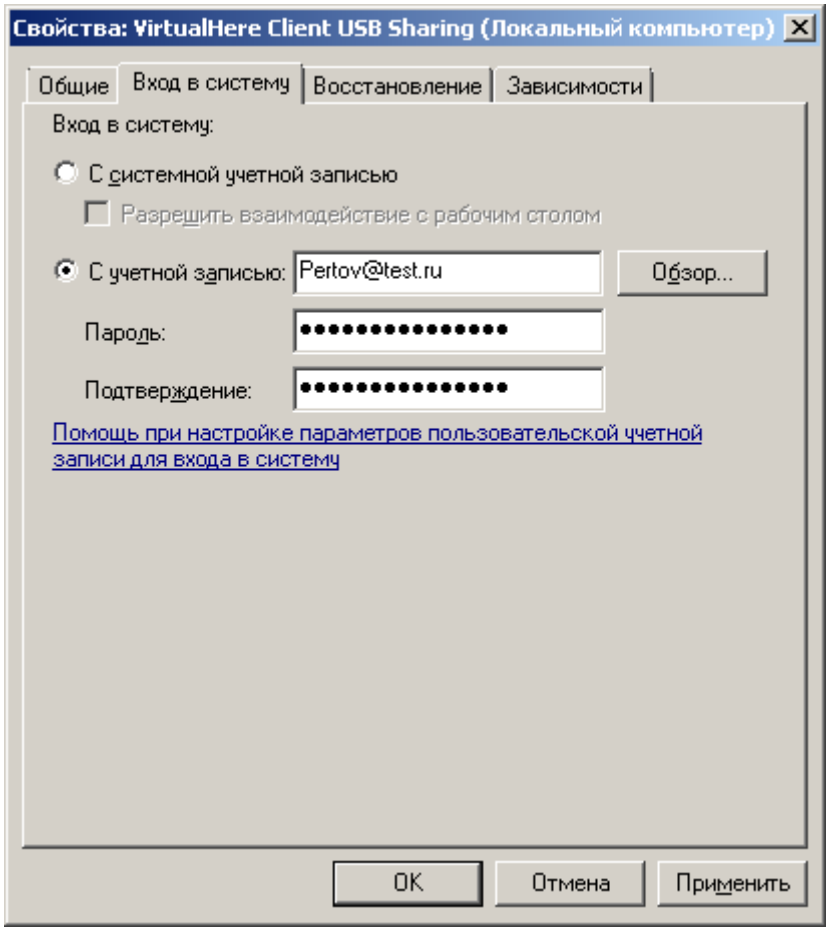
Особенности режима службы:

- Работает в фоне без входа пользователя
- Управление через `.bat`/скрипты

• Графический интерфейс доступен только для мониторинга

Авторизация в терминальном режиме:

1. Запуск службы от имени пользователя:




```
dkcl64.exe -t "USE,USBoverIP64.114,pssword"
```

1. Указание параметров в скриптах:

```
dkcl64.exe -t "USE,USBoverIP64.114,user\pssword"
```

Журналирование:

• Windows: **Просмотр событий**

• OSX: **Console Viewer**

• Linux:

```
tail /var/log/syslog
```

4 Дополнительные возможности при работе с клиентом DistKontrolUSB

Клиент управляемого USB over IP концентратора имеет несколько аргументов командной строки:

Синтаксис вызова:

- **Windows**:
  `dkcl32.exe <аргумент>` или `dkcl64.exe <аргумент>`
- **OSX**:
  `/Applications/DistKontrolUSB/DistKontrolUSB.app/Contents/MacOS/dkcl <аргумент>`
- **Linux**:
  `dkclt64` или `dkclientx86_64 <аргумент>`

Перечень аргументов командной строки:

- `-h`
  Справка по командной строке.
- `-l=<path>`
  Указать файл для записи всех сообщений (вместо окна "Системные Сообщения").
- `-c`
  Использовать кастомный файл конфигурации вместо файла по умолчанию.
- `-a`
  Запуск клиента в **режиме администратора**. Позволяет отключать других пользователей от устройств удалённо.
- `-d`
  Установка драйверов клиента и завершение работы.
  Требует прав администратора. Используется для массовой установки через сети (например, Microsoft SMS).
- `-x`
  Извлечение драйверов (актуально для ручной установки в **Windows XP Embedded**).
- `-i`
  Установка клиента в качестве службы.
  Требует прав администратора.
- `-b`
  Аналогично `-i`, но с включённым **автопоиском устройств** по умолчанию.
- `-u`
  Удаление службы клиента.
  Требует прав администратора.
- `-y`
  Удалить все драйверы USB клиента (если установлены).
  Требует прав администратора.
- `-t`
  Отправить команду работающему клиенту (см. раздел 3).

- `-r=<file>`
  Перенаправление выходных данных в указанный файл.
  Пример:

```
dkcl64.exe -t "LIST" -r=output.txt  # Запись результатов команды LIST в файл output.txt
```

Важно

- Для работы с аргументами `-i`, `-u`, `-d`, `-y` требуются **права администратора**.
- Аргумент `-r` используется совместно с другими командами (например, `-t`, `-x`, `-i`).
- В режиме службы (`-i` / `-b`) клиент работает в фоне без графического интерфейса.

5 Примеры управления клиентом DistKontrolUSB для Windows и Linux

5.1 Алгоритм создания пакетного файла управления клиентом для Windows

Запускаем `dkcl64.exe` как службу или в графическом интерфейсе в Windows.
Запускаем командную строку, переходим в каталог программы.
Набираем:

```
dkcl64.exe -t "LIST"
```

Копируем адрес устройства (то, что в скобках).

Например он - `USBoverIP16.115`, тогда:
Для подключения USB устройства:

```
dkcl64.exe -t "USE,USBoverIP16.115"
```

Для отключения USB устройства:

```
dkcl64.exe -t "STOP USING,USBoverIP16.115"
```

(адрес USB устройства вводится без пробела после запятой)

Для подключения USB порта:

```
dkcl64.exe -t "AUTO USE PORT,USBoverIP16.115"
```

Для отключения USB порта:

```
dkcl64.exe -t "STOP USING,USBoverIP16.115"
dkcl64.exe -t "AUTO USE CLEAR ALL"
```

(адрес USB устройства вводится без пробела после запятой)

5.2 Алгоритм установки и настройки демона для Linux

Пример установки и настройки (для подключения USB устройств с SSL шифрованием и авторизацией) консольного клиента USB over IP концентратора в качестве демона на Debian (Ubuntu):

Клиента USB over IP концентратора для Linux использует встроенный драйвер Linux `usbip`.
В большинстве версий Linux он включен по умолчанию. Рекомендуется использовать последнее ядро (4.9+) для максимальной совместимости.

Пользователь должен иметь разрешение на `sudo` для запуска демона. Команды управления демоном выполняются без `sudo`. *(подключаемся по ssh к ОС, создаем пользователя, добавляем его в группу sudo)*.

IP адрес концентратора `192.168.1.180` из примера — замените на адрес Вашего устройства, пользователя «testuser» и пароль «pass» на соответствующие Ваши.

Путь до сертификата для USB трафика возможно посмотреть в Web-интерфейсе в Разделе «Система» — «Сертификаты» вкладка «USB». Необходимо открыть настройки сертификата и скопировать путь.

Скачиваем с концентратора сертификат и консольный клиент:

```
wget --no-check-certificate http://192.168.1.180/client/********.pem
wget --no-check-certificate http://192.168.1.180/client/dkclientx86_64
```

`/client/********.pem` — *Необходимо указать путь до сертификата скопированный в Web-интерфейсе.*

Устанавливаем права на клиента и запускаем его в качестве демона:

```
chmod +x ./dkclientx86_64
sudo ./dkclientx86_64 -n
```

Добавляем IP адрес концентратора:

```
./dkclientx86_64 -t 'MANUAL HUB ADD,192.168.1.180:6565'
./dkclientx86_64 -t 'list'
```

Далее настроим SSL и авторизацию. Включаем SSL шифрование, ограничение доступа к USB порту по логину и паролю и добавляем пользователя в WEB интерфейсе концентратора (см. соответствующие разделы инструкции).

Добавляем в конфигурационный файл клиента путь к сертификату (пользователя «testuser» замените на имя Вашего пользователя):

```
echo "[General]" >> ./.dkcl
echo "SSLCAFile=/home/testuser/distkontrolusb.pem" >> ./.dkcl
cat ./.dkcl
```

Проверяем, в выводе должны присутствовать строки:

```
.....
[Settings]
ManualHubs=192.168.1.180:6564
[General]
SSLCAFile=/home/testuser/distkontrolusb.pem
.....
```

Перезапускаем демона:

```
sudo ps aux | grep [d]kc
```

Видим:

```
root 6345 0.0 1.0 13624 10432 ? Ssl 17:25 0:00 ./dkclientx86_64 -n
```

Вводим:

```
sudo kill -9 6345
sudo ./dkclientx86_64 –n
```

Проверяем:

```
./dkclientx86_64 -t 'list'
```

Должно быть:

```
DistKontrolUSB Client IPC, below are the available devices:
(Value in brackets = address, * = Auto-Use)
usboverip64 (usboverip64:6565)
--> Guardant Stealth III Sign USB (usboverip64.11512)
--> DataTraveler 410 (usboverip64.11511)
Auto-Find currently on
Auto-Use All currently off
Reverse Lookup currently off
Reverse SSL Lookup currently off
DistKontrolUSB Client is running as a service
```

Подключаем USB-устройство, доступ к порту, которого разрешен для пользователя `testuser` со стороны устройства:

```
./dkclientx86_64 -t "USE,usboverip64.11512,pass"
```

Для автоматического использования USB-порта:

```
./dkclientx86_64 -t "AUTO USE PORT,usboverip64.11512,pass"
```

В выводе должны увидеть:

```
OK
```

USB устройство подключено к ОС с SSL шифрованием и ограничением доступа к USB порту управляемого USB over IP концентратора по логину и паролю.

Если в выводе:

```
FAILED
```

Смотрим результат попытки подключения в WEB интерфейсе устройства (подробнее см. Сообщения системы авторизации в разделе *Просмотр системного журнала DistKontrolUSB*).

Анализируем, что сделано не так, вносим коррективы.

Утилита для управления питанием USB-портов USBControl

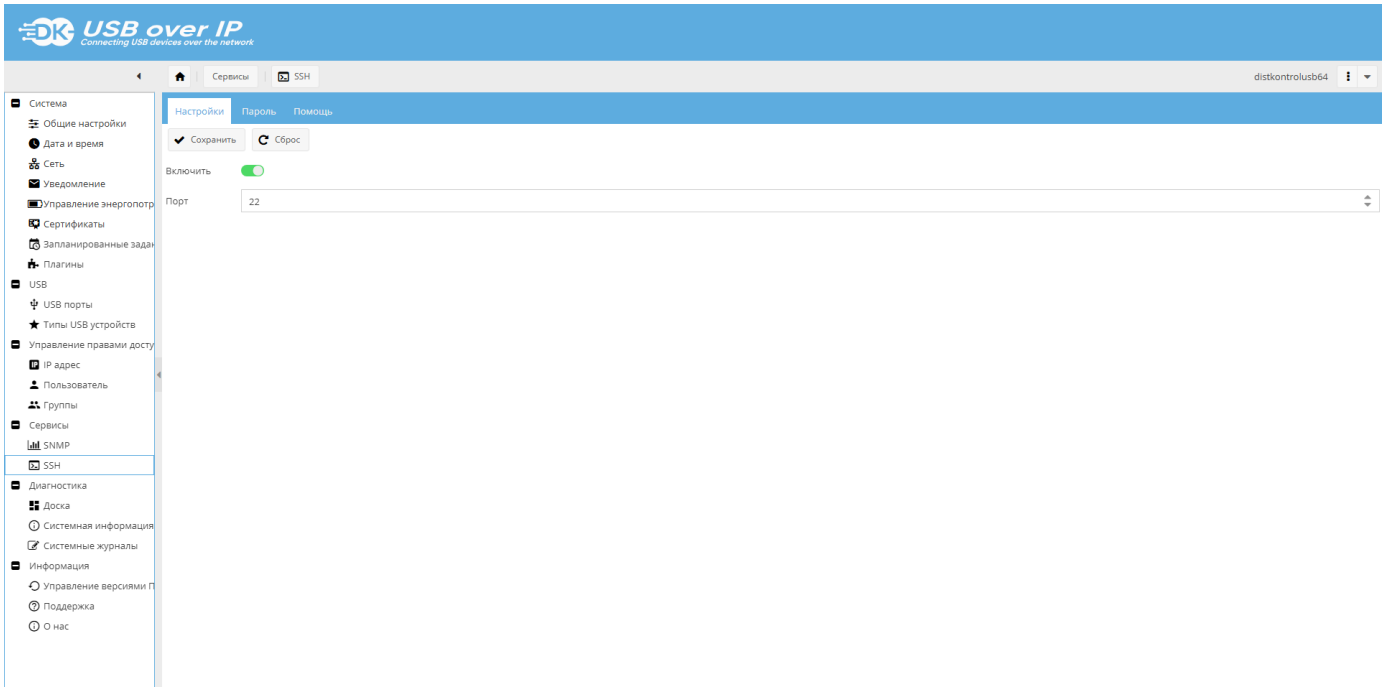
РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Москва
2026 г

Инструкция по использованию утилиты управления портами управляемого USB over IP концентратора\хаба

> **Информация**
>
> Скачать документацию в формате pdf можно по ссылке

Для использования утилиты необходимо включить «API SSH» на странице «Сервисы» - «Настройки USB». Утилита работает с 22 портом.



Общий формат запуска утилиты

```
usbcontrol.exe ipaddress status UsbPort pass
```

Все аргументы разделяются пробелами.

В случае запуска утилиты без параметров (без аргументов) на экран будет выведена краткая справка на английском языке.

Описание аргументов

1. **ipaddress** - IP-адрес(или сетевое имя) устройства к которому необходимо подключиться;
2. **status** - "0" или "1".
   `0` - Выключить USB порт.
   `1` - Включить USB порт.
3. **UsbPort** - номер USB порта который необходимо включить/выключить (от 1.1 до 4.16);
4. **pass** - пароль пользователя usbcontrol (задается в WEB интерфейсе: *Управление правами доступа - Пользователь - usbcontrol*)

Пример

```
usbcontrol.exe 192.168.1.180 1 3.12 TestPass
```

(Включить USB порт № 3.12)

Пример запуска в *.bat файле: см. usbcontrol.bat

Внимание

Пароль пользователя usbcontrol передается на устройство безопасным способом, но его хранение в файлах скриптов управления не безопасно. Необходимо принимать дополнительные меры по обеспечению безопасности используемых Вами скриптов, приложений и т.д.

Самостоятельное написание скриптов

Подключение возможно от пользователя «usbcontrol». Пароль задается при редактировании прав пользователя. Доступны команды:

```
q (выход)
usbcontrolapi status UsbPort
```

Пример выполнения на концентраторе

```
usbcontrol@192.168.1.180's password:
> ucbcontrolapi 1 3.15
Status OK. USB port: 3.15 Status: 1
```