

РУКОВОДСТВО АДМИНИСТРАТОРА

HTI-VB600

ТЕРМИНАЛ ДЛЯ ВИДЕОКОНФЕРЕНЦИИ



Содержание

1.	Системные настройки	4
1.1.	Системные настройки	4
1.1.1.	Настройка звука	4
1.1.2.	Настройка видео	5
1.1.3.	Вывод и отображение.....	6
1.1.4.	Настройки рабочего стола.....	6
1.1.5.	Диагностика	7
1.1.6.	Настройки обновления	8
1.1.7.	Конфигурация сервиса	8
1.1.8.	Интерфейс (общие настройки).....	9
1.1.9.	Системные настройки	9
1.1.10.	Информация об устройстве	10
1.1.11.	Bluetooth	11
1.1.12.	Пульт	11
1-8	Доступ к экрану	12
2.	Настройка вызова	14
2.1.	Набор	14
2.2.	Настройки набора.....	14
2.2.1.	Настройка H.323	15
2.2.2.	Настройка SIP.....	17
2.3.	Режим MCU.....	19
2.4.	Личные контакты.....	19
3.	Веб-интерфейс	20
3.1.	Авторизация.....	20
3.1.1.	Подготовка	20
3.1.2.	Авторизация.....	20
3.2.	Домашняя страница	20
3.2.1.	Выход из системы	21
3.2.2.	Свернуть или развернуть панель навигации.....	21
3.2.2.1.	Свернуть панель навигации	21
3.2.2.2.	Развернуть панель навигации	22
3.3.	Настройки веб-интерфейса	22
3.3.1.	Общие настройки	22
3.3.2.	Настройки звука	23
3.3.3.	Настройки камеры	23
3.3.4.	Вывод и отображение.....	24
3.3.5.	Bluetooth	24
3.3.6.	Дистанционное управление.....	25
3.3.7.	Управление периферийными устройствами	26
3.3.8.	Обновление	26
3.3.9.	Адрес сервисной службы.....	27
3.3.10.	Система	27
3.4.	Сетевые настройки.....	28

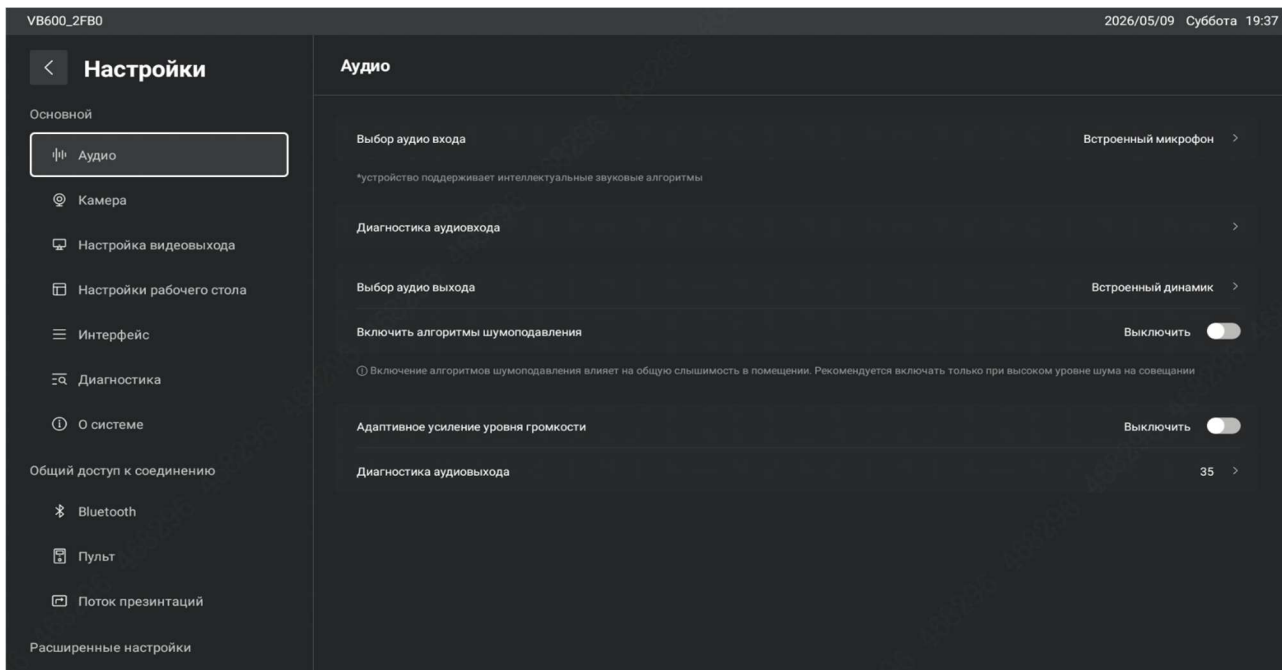
3.5.	Об устройстве.....	28
3.6.	Активация режима MCU	29
3.7.	LDAP	30
4.	Юридическая информация	31
5.	Рекомендации по кибербезопасности.....	33

1. Системные настройки

1.1. Системные настройки

Шаг 1 Выберите "Функции быстрого доступа → Системные настройки". Откроется окно «Системные настройки», см. рис. 1-1

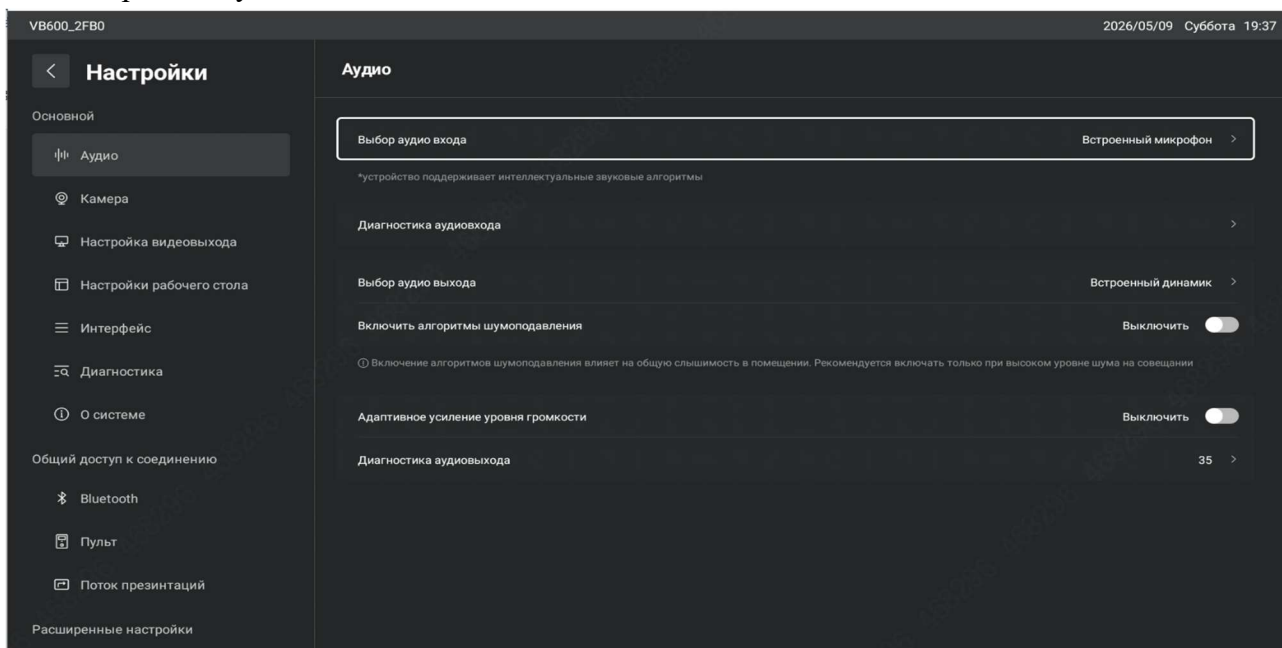
1-1 Системные настройки



1.1.1. Настройка звука

Шаг 1 Откройте меню настройки звука (см. рис. 1-2).

1-2 Настройка звука



Шаг 2 Описание параметров настройки звука приведено в табл. 1-3.

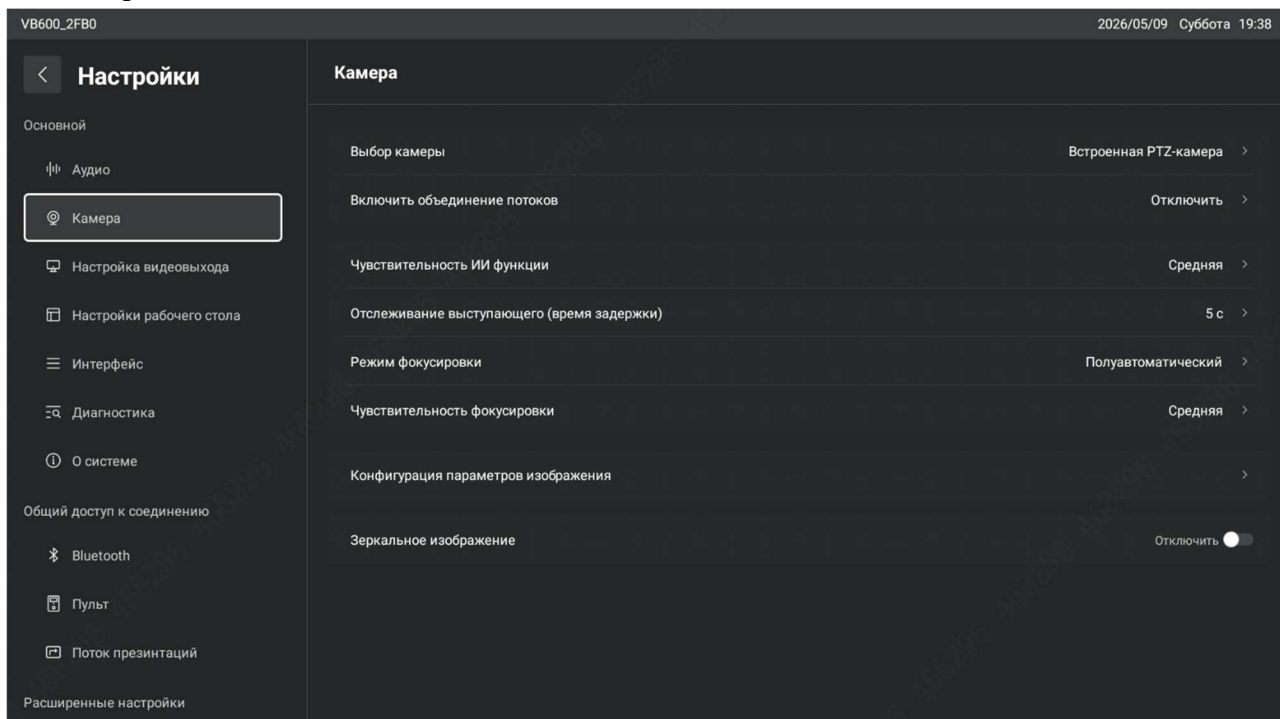
1-3 Инструкции по настройке звука

Настройка	Описание
Аудиовход	● Аудиовход — выбор источника звука: встроенный микрофон.
Аудиовыход	● Аудиовыход — выбор устройства воспроизведения: встроенный динамик, HDMI.

1.1.2. Настройка видео

Шаг 1 Меню настроек видео отображается так, см. рис. 1-4

1-4 Настройка видео



Шаг 2 Для подробного описания параметров настройки видеосигнала терминала обратитесь к таблице 1-5

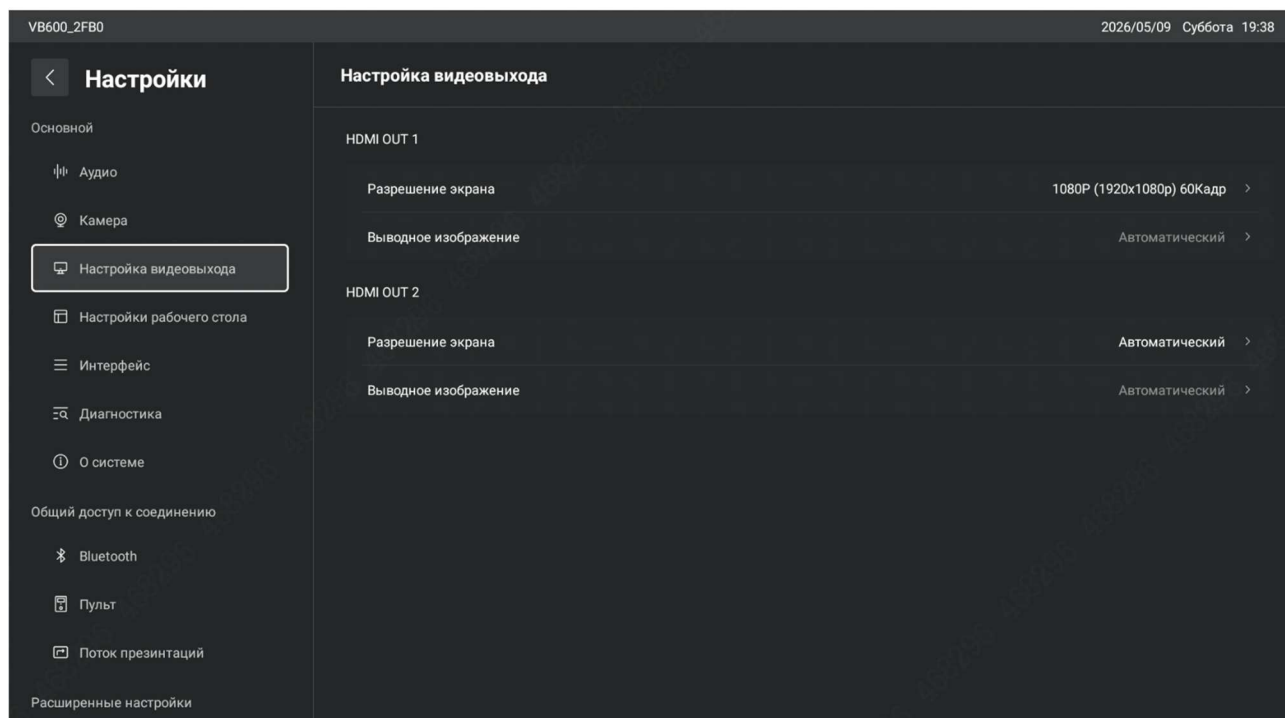
1-5 Инструкции по настройке видео

Настройка	Описание
Выбор камеры	● Встроенная камера ● Встроенная панорамная камера ● Встроенная камера + дополнительное изображение с объединением потоков
Чувствительность интеллектуального наведения	● высокая ● средняя ● низкая (по умолчанию — средняя)
Режим фокусировки	● Автоматический ● полуавтоматический, (по умолчанию — полуавтоматический)
Чувствительность фокусировки	● Высокая ● средняя ● низкая (по умолчанию используется значение — Высокая)
Настройка параметров изображения	Настройте режим изображения, параметры изображения и т.д.

1.1.3. Вывод и отображение

Шаг 1 Откройте меню вывода и отображения видеосигнала (см. рис. 1-6).

1-6 Вывод и отображение



Шаг 2 Для подробного описания параметров вывода терминала и элементов конфигурации отображения обратитесь к таблице 1-7

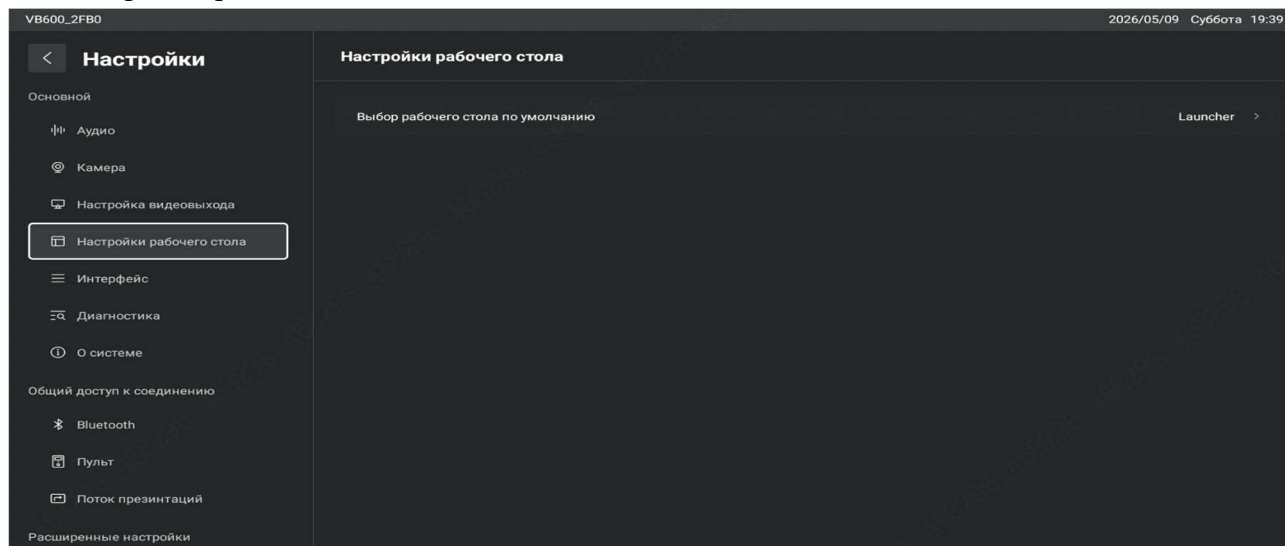
1-7 Инструкции по выводу и отображению

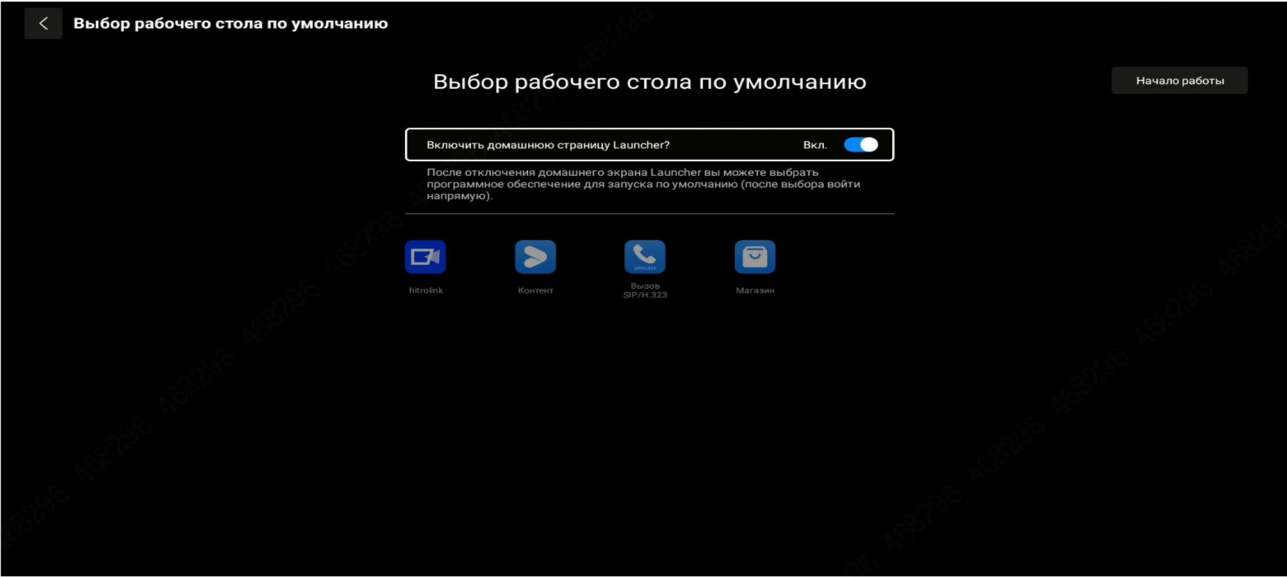
Настройка	Описание
HDMI1/HDMI2	установка выходного разрешения вплоть до 4K60.

1.1.4. Настройки рабочего стола

Меню настроек рабочего стола отображается, см. рис. 1-8.

1-8 Настройки рабочего стола

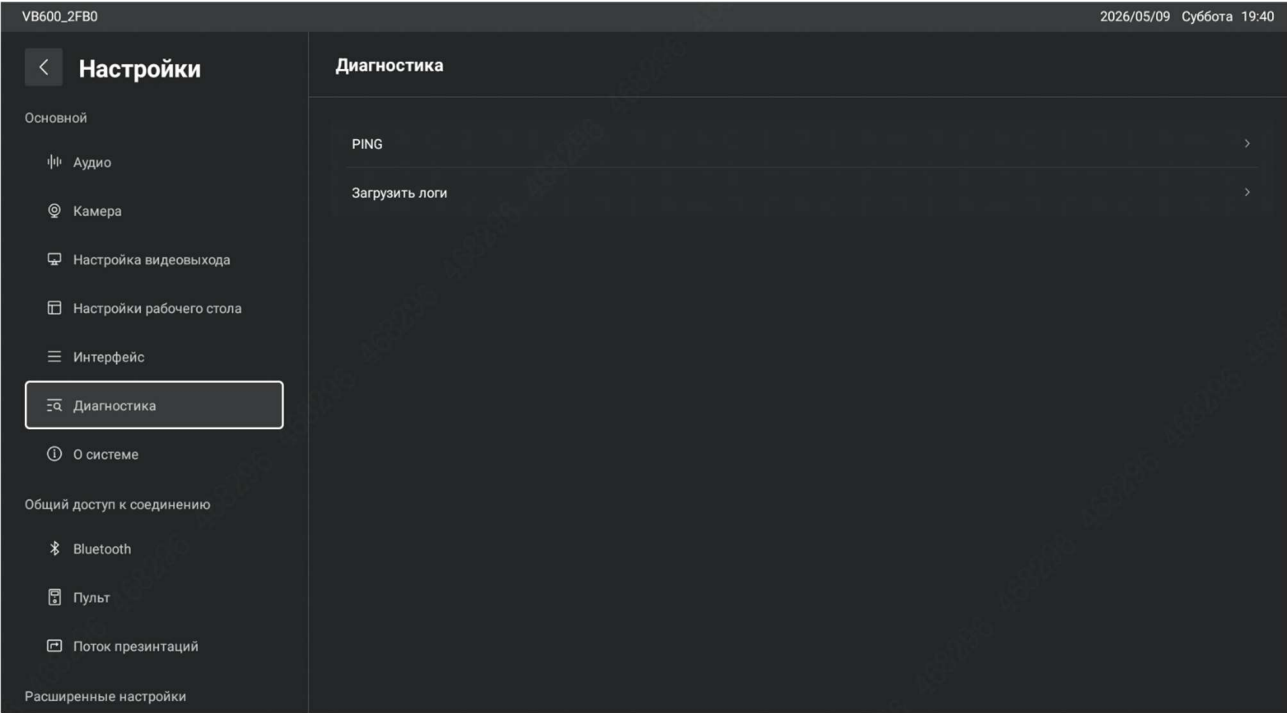




1.1.5. Диагностика

Шаг 1 Меню диагностических настроек отображается, см. рис. 1-9

1-9 Диагностика



Шаг 2 Описание параметров диагностики приведено в табл. 1-10

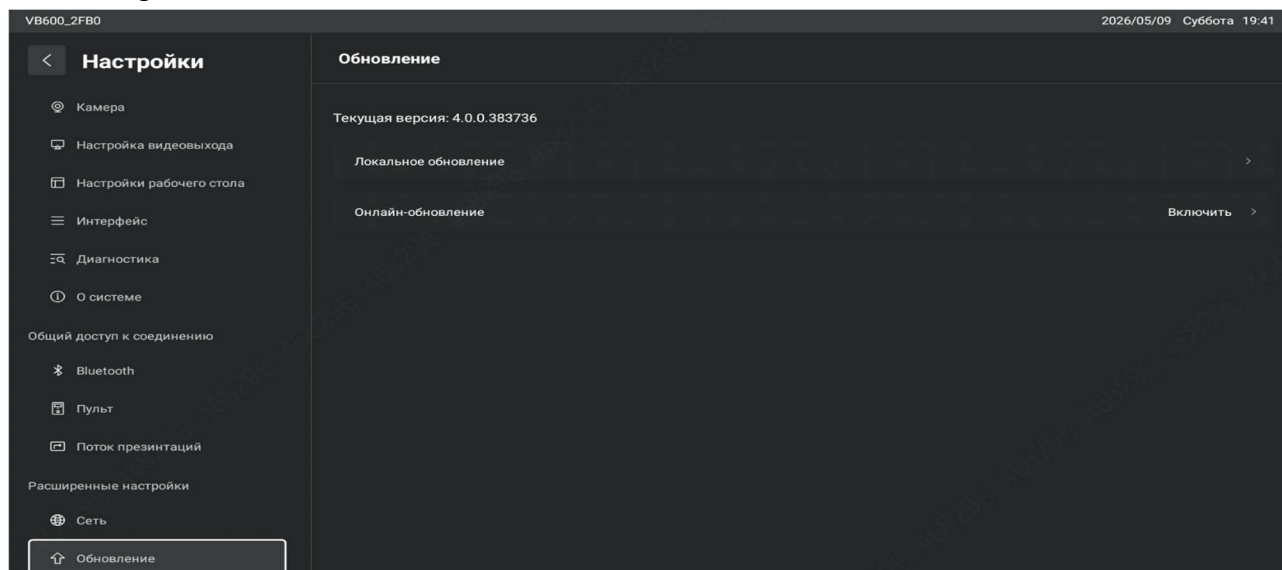
1-10 Инструкции по диагностике

Настройка	Описание
Диагностика аудиовхода	Выполните звуковые тесты микрофона, подключенного к терминалу.
Диагностика аудиовыхода	Выполните тесты звука на динамиках, подключенных к терминалу.
PING	Проверьте, правильно ли подключен терминал и проверьте IP-адрес.

1.1.6. Настройки обновления

Шаг 1 Откройте меню настроек обновления (см. рис. 1-11).

1-11 Настройки обновления



Шаг 2 Для подробного описания параметров конфигурации обновления обратитесь к таблице 1-12

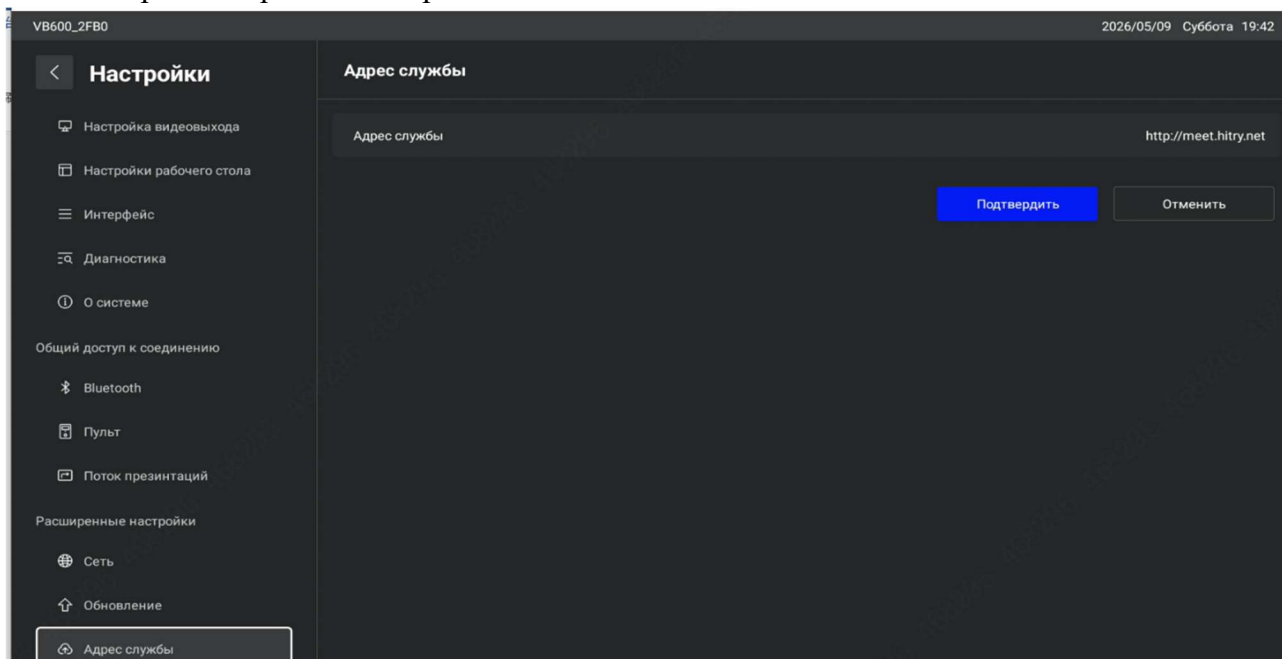
1-12 Инструкции по настройке обновления

Настройка	Описание
Локальное обновление	Обновление ПО с USB-накопителя, подключённого к устройству.
Автоматическое обновление	Автоматическое обновление (включено по умолчанию).

1.1.7. Конфигурация сервиса

Шаг 1. Откройте меню настроек сервиса (см. рис. 1-13).

1-13 Настройки сервисного адреса



Шаг 2 Подробное описание параметров конфигурации сервиса приведено в таблице 1-14

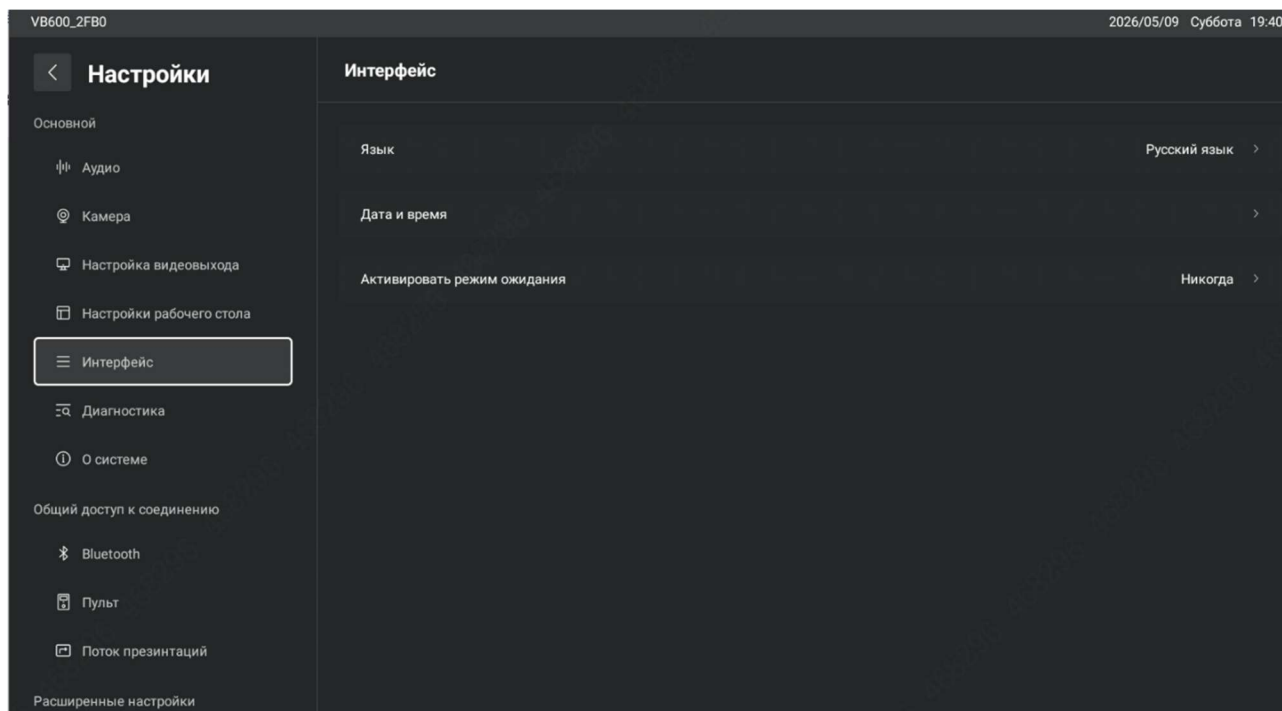
1-14 Описание конфигурации сервиса

Настройка	Описание
Сервисный адрес	Введите URL сервера, чтобы получить терминал к серверу.

1.1.8. Интерфейс (общие настройки)

Шаг 1 Меню интерфейса отображается, см. рис. 1-15.

1-15 Общие настройки



Шаг 2 Общие параметры настройки и подробные описания параметров приведены в таблице 1-16

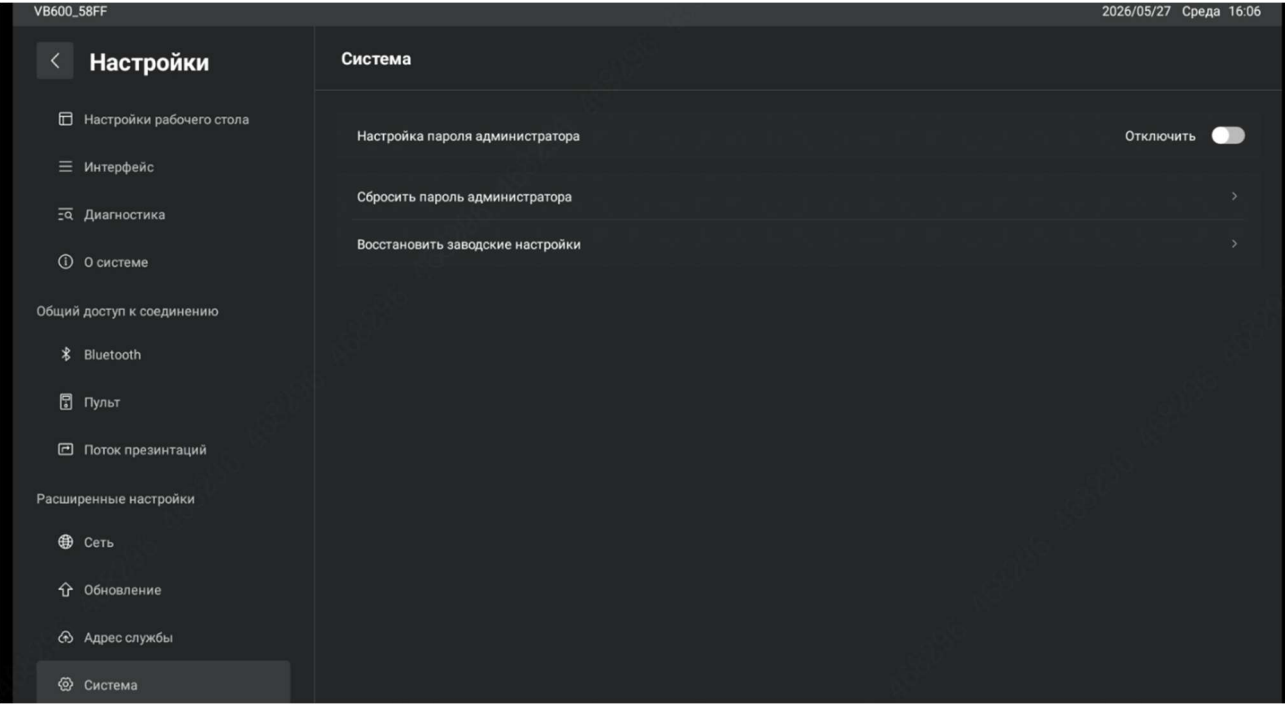
1-16 Общие инструкции по настройке

Настройка	Описание
Язык	упрощенный китайский, английский, русский
Настройки даты и времени	● Формат времени ● Формат даты ● Автоматическая установка времени ● Часовой пояс
Время до перехода в режим ожидания	5 минут, 10 минут, 15 минут, 20 минут, никогда.

1.1.9. Системные настройки

Шаг 1 Меню системных настроек показано на рисунке 1-17.

1-17 Системные настройки



Шаг 2 Подробные описания параметров элементов конфигурации системы приведены в таб. 1-18.

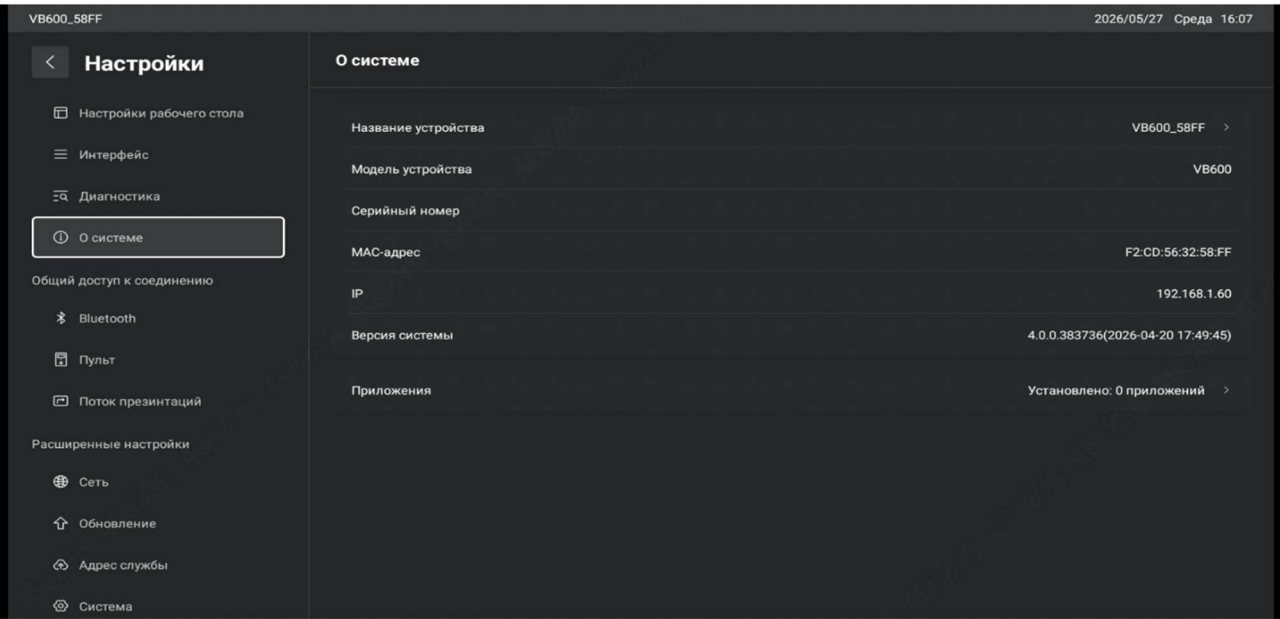
1-18 Инструкции по системным настройкам

Настройка	Описание
Сброс пароля администратора	Возврат пароля администратора к значению по умолчанию
Сброс к заводским настройкам	Возврат всех параметров устройства к заводским значениям

1.1.10. Информация об устройстве

Шаг 1 Меню с информацией об устройстве отображается, см. рис. 1-19.

1-19 Информация об устройстве

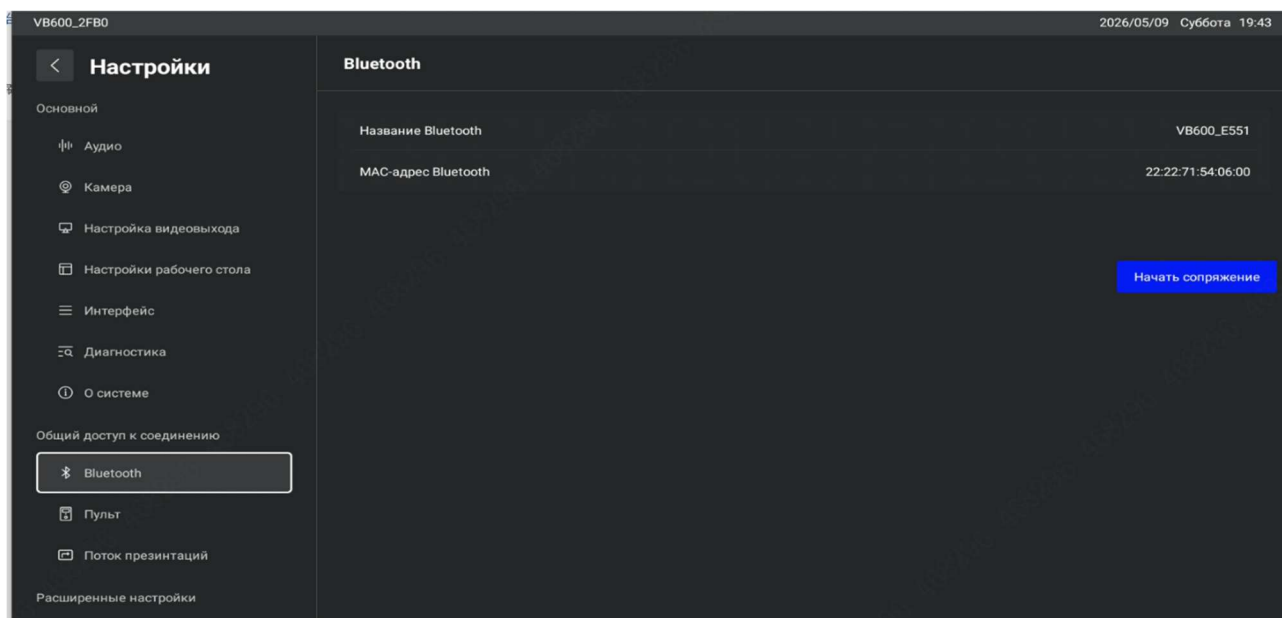


Шаг 2 В настройках можно посмотреть модель устройства, серийный номер, MAC-адрес, IP-адрес, версии системы и платформы конференц-связи, а также задать имя устройства.

1.1.11. Bluetooth

Шаг 1 Меню настроек Bluetooth отображается, см. рис. 1-20.

1-20 Bluetooth

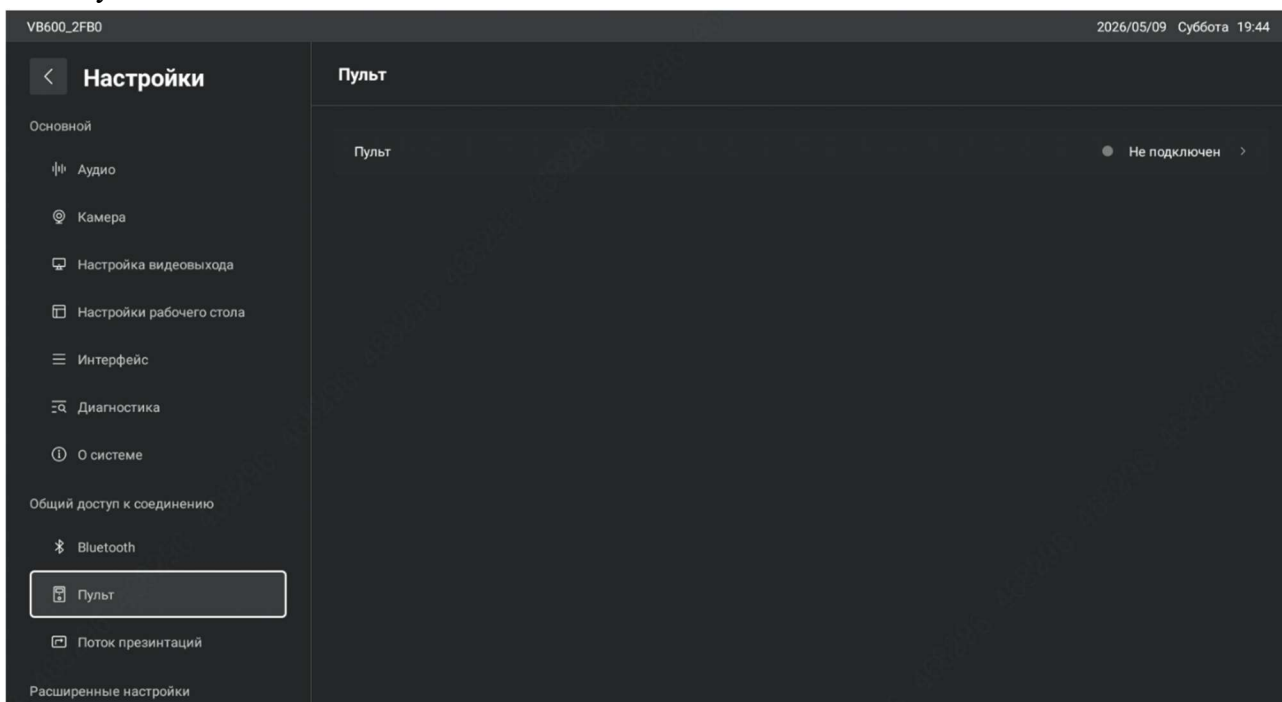


Шаг 2 Нажмите «Начать сопряжение», чтобы подключить Bluetooth-устройства — например, микрофоны или колонки.

1.1.12. Пульт

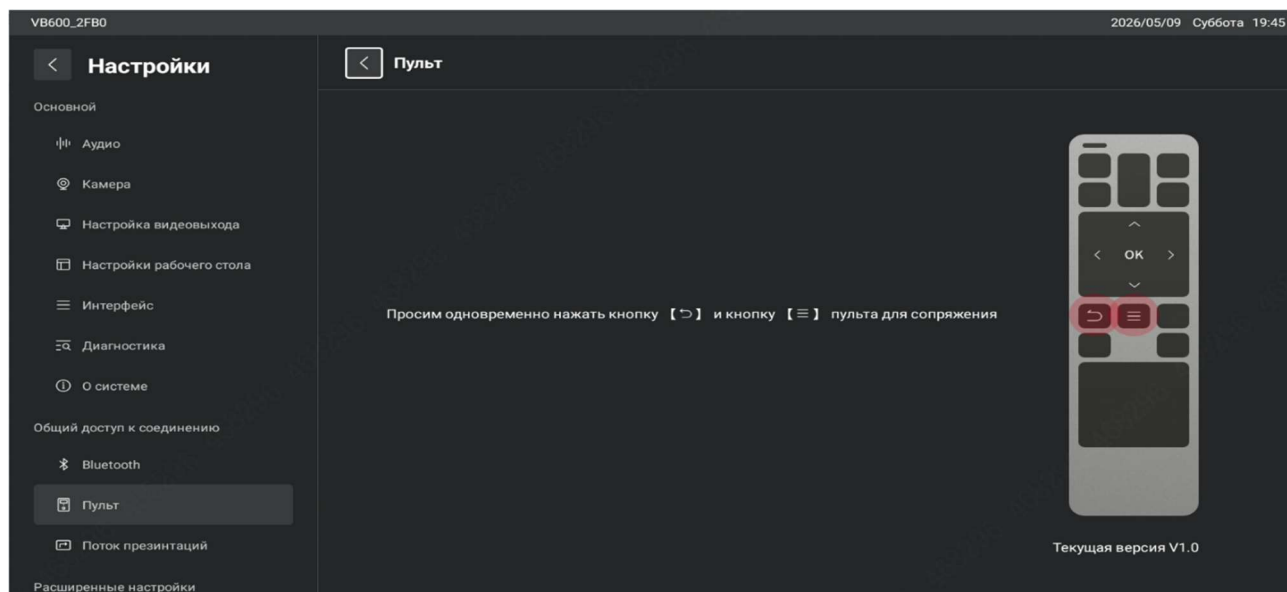
Шаг 1 Меню настроек пульта отображается так, см. рис. 1-21.

1-21 Пульт



Шаг 2 На этом экране можно проверить состояние сопряжения пульта или нажать «Сопряжение с пультом», чтобы перейти к процедуре сопряжения (см. рис. 1-22).

1-22 Сопряжение с пультом дистанционного управления



Инструкции по сопряжению пульта дистанционного управления Bluetooth

При первом использовании пульта дистанционного управления, когда он еще не сопряжен с устройством, направьте пульт на устройство и одновременно нажмите и удерживайте кнопки  и  в течение 3 секунд. Когда индикатор на пульте загорится синим цветом, отпустите кнопки — сопряжение завершено.

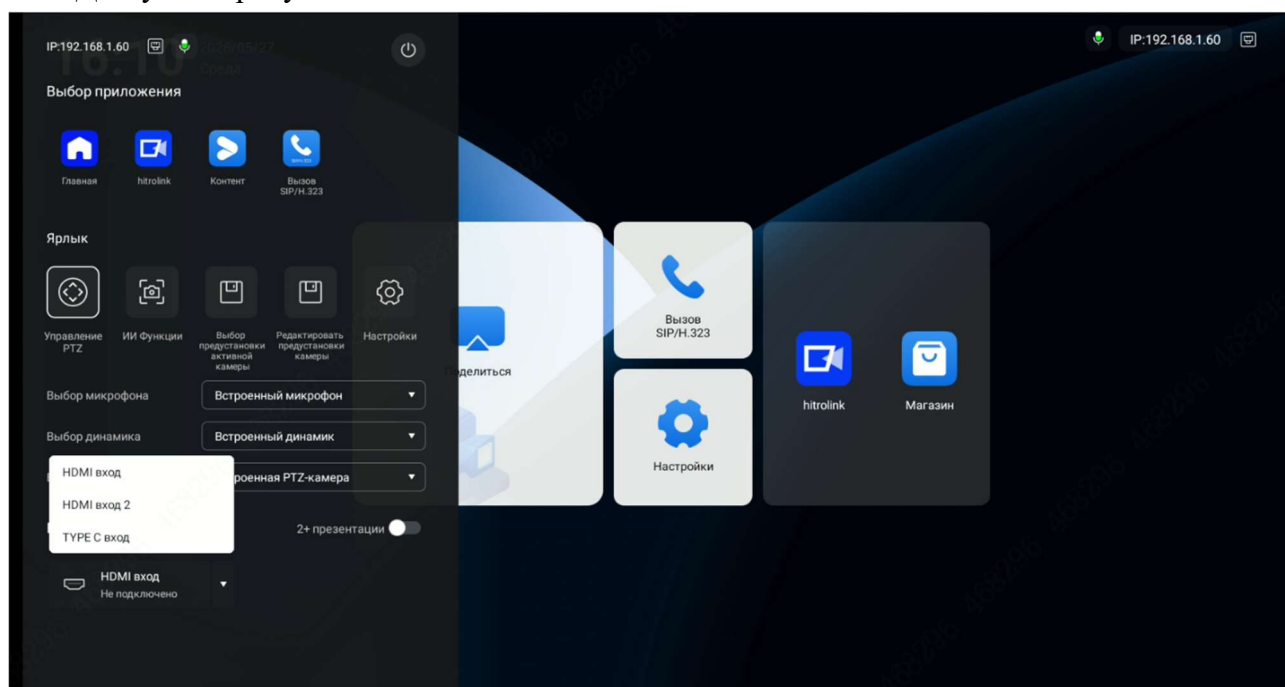
Если в процессе использования потребуется заменить пульт, повторите вышеуказанные действия для повторного сопряжения.

Один пульт может быть сопряжён только с одним устройством; новое сопряжение автоматически отменяет предыдущее.

1-8 Доступ к экрану

Шаг 1 При подключении меню настроек доступа к экрану выглядит так, см. рис. 1-23

1-23 Доступ к экрану



Шаг 2 Подробные описания параметров элементов конфигурации системы приведены в таб. 1-24.

1-24 Инструкции по настройке доступа к экрану

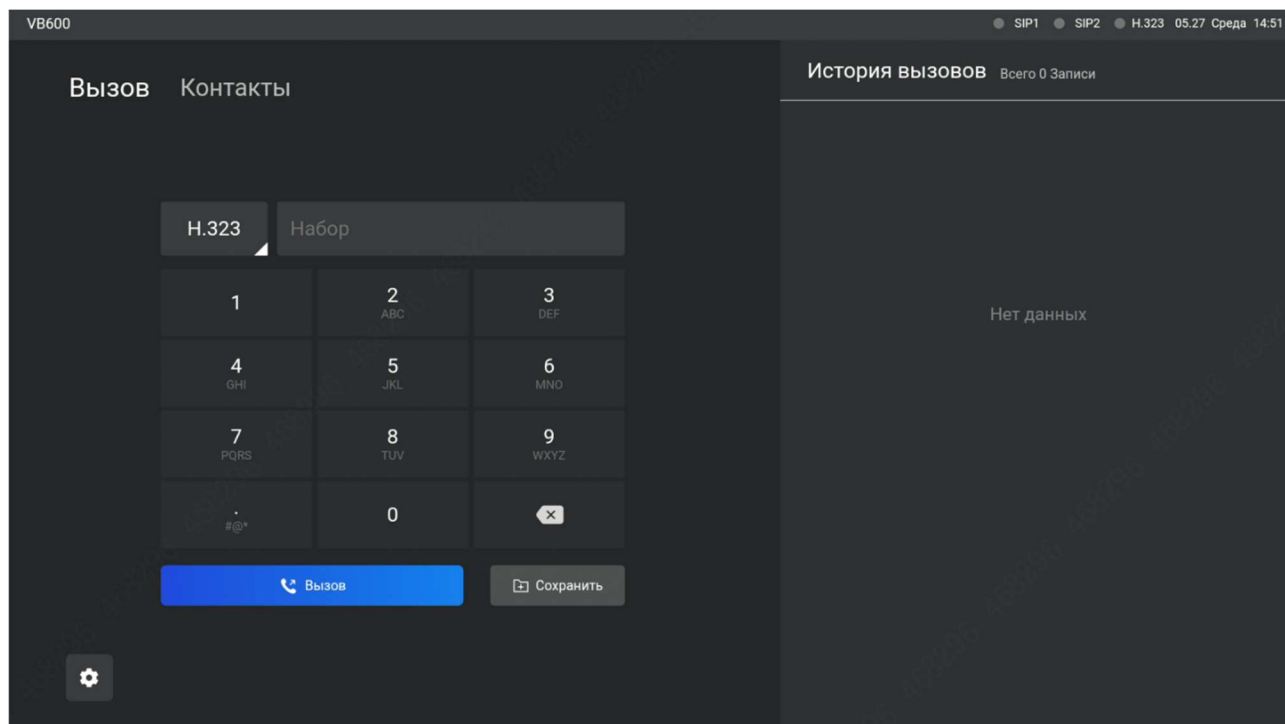
Настройка	Описание
Выбор интерфейса	Выбор интерфейса — HDMI IN, HDMI IN 2 или USB Type-C IN.
Режим совместного просмотра	Режим совместного просмотра — включает или отключает совместный просмотр экрана (по умолчанию выключен).

2. Настройка вызова

2.1. Набор

Шаг 1 В главном меню выберите «Вызов» — откроется меню набора (см. рис. 2-1).

2-1 Набор



Шаг 2 Введите адрес вызова, нажмите «Вызвать» и подключитесь к конференции.

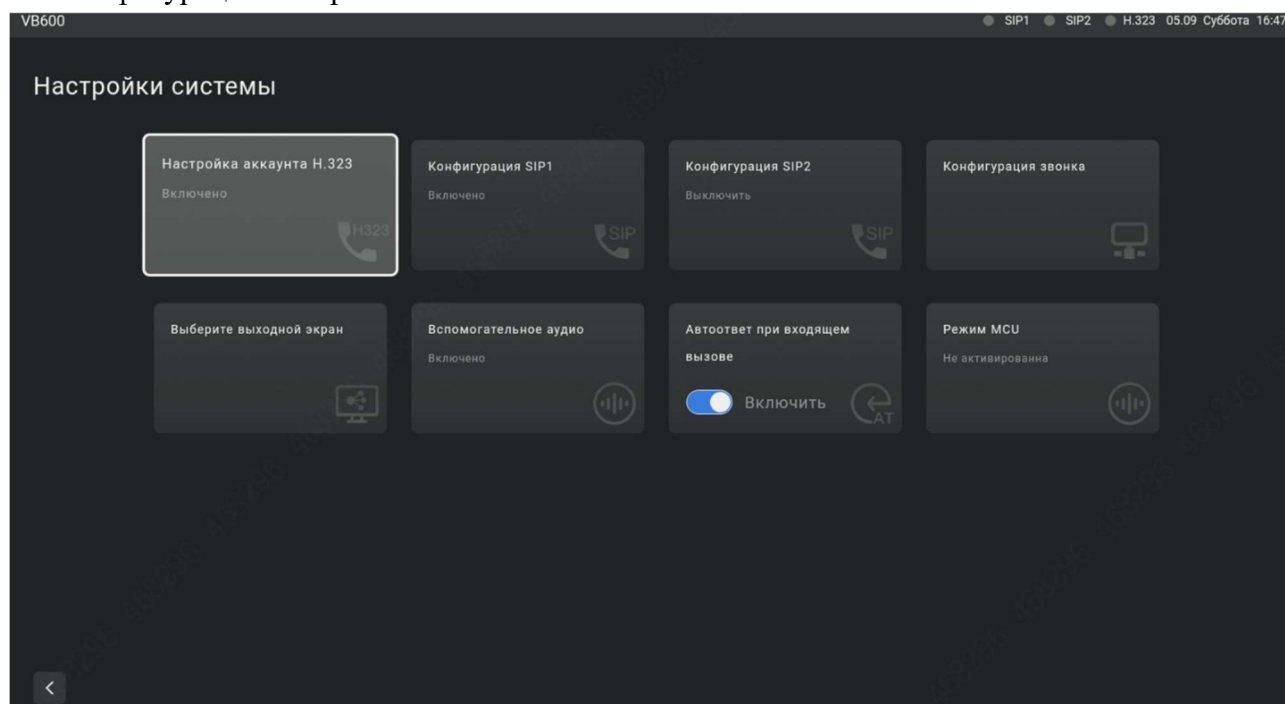
После завершения вызова нажмите «Сохранить», чтобы добавить контакт в личную адресную книгу.

- Если шлюз H.323 не зарегистрирован, устройство может вызывать только терминалы той же марки. Введите IP-адрес вызываемого терминала в поле адреса вызова и нажмите «Вызвать», чтобы начать конференцию.
- Если шлюз H.323 зарегистрирован, можно вызывать терминалы сторонних производителей: введите идентификатор такого терминала или идентификатор конференции и нажмите «Вызвать», чтобы присоединиться к конференции
-

2.2. Настройки набора

Перед вызовом можно открыть настройки кнопкой в левом нижнем углу окна вызова и задать параметры H.323, SIP и общие параметры вызова (см. рис. 2-2).

2-2 Конфигурация набора



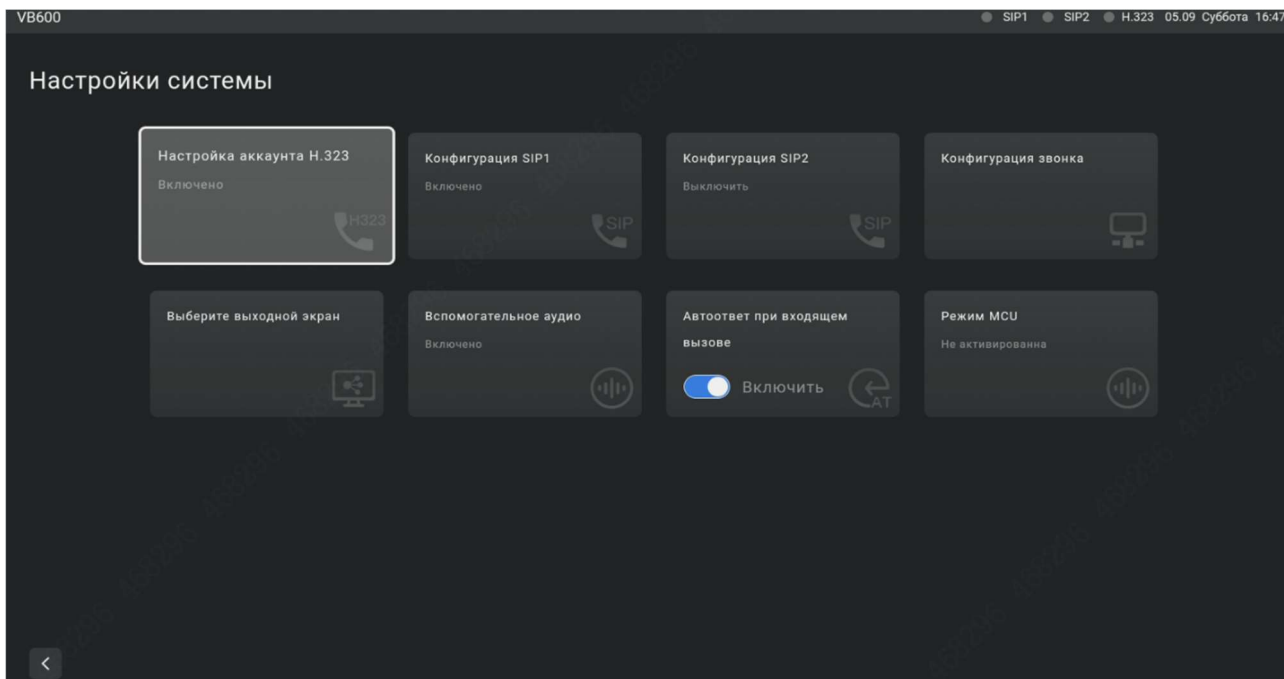
2-3 Инструкции по настройке набора

Настройка	Описание
Настройка H.323	Настройте H.323. Настройте параметры H.323
SIP	Настройте параметры SIP терминала (можно зарегистрировать два сервера).
Набор номера	Настройте параметры набора номера терминала
Аудиоисточник для демонстрации	Источник звука при демонстрации — включить или отключить передачу звука с источника демонстрации (по умолчанию включено).
Эхоподавление	Устанавливает уровень эхоподавления; значение по умолчанию "выкл."
Шумоподавление	Включает или отключает подавление фонового шума (по умолчанию выключено). При активации доступны два уровня интенсивности — низкий и высокий (по умолчанию высокий).
Автоматическая регулировка усиления	Включается отдельно для воспроизведения и для записи (оба регулятора по умолчанию выключены).
Деревверберация	Уровень подавления реверберации (по умолчанию выключено).
Автоматическое присоединение к собранию	Если включено, терминал автоматически присоединяется к входящему вызову; если выключено, требуется подтверждение вручную (по умолчанию включено).
Настройки по умолчанию	Импорт конфигурации, экспорт конфигурации, восстановление настроек системы по умолчанию.
Управление безопасностью	Веб-доступ к устройству (по умолчанию включён).

2.2.1. Настройка H.323

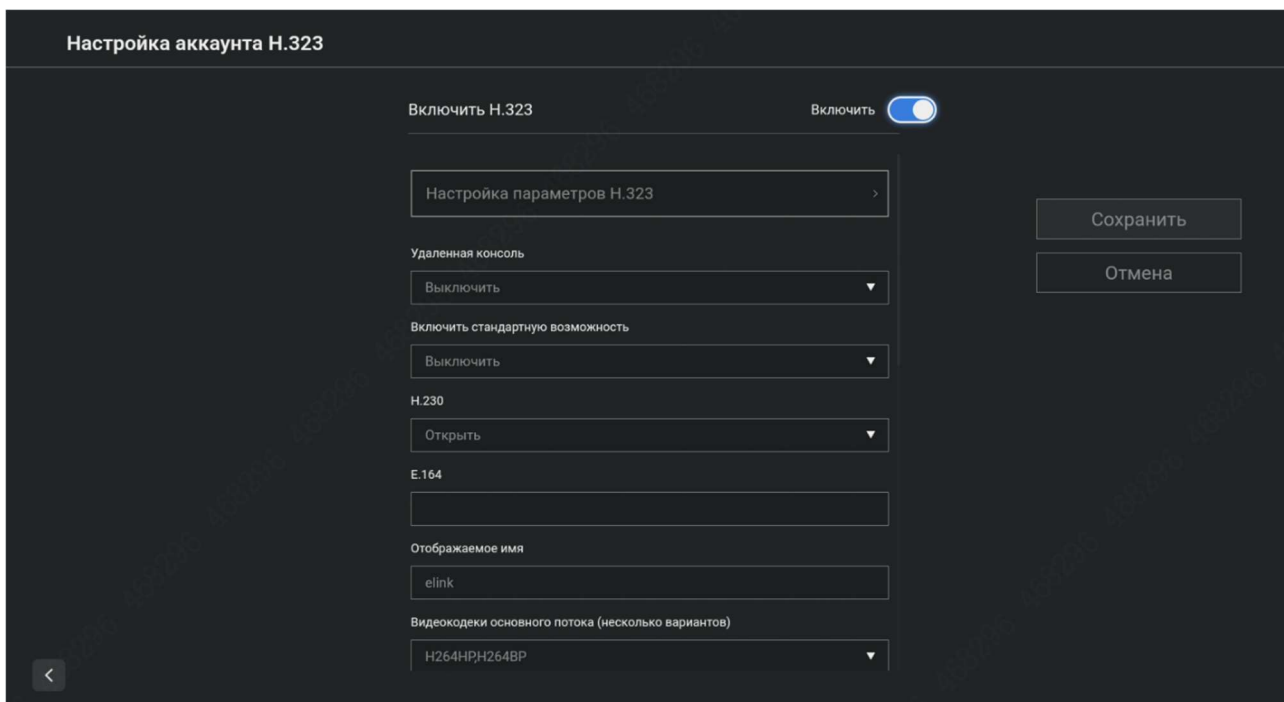
Шаг 1 В настройках вызова откройте раздел «H.323» и включите переключатель «H.323». Задайте «Отображаемое имя». Остальные параметры рекомендуется оставить по умолчанию. Меню показано на рисунке 2-4.

2-4 Настройка H.323



Шаг 2 Выберите "Настройка регистрации H.323", см. рис. 2-5

2-5 Настройка регистрации H.323



Шаг 3 Чтобы задать режим шлюза, выберите «Указать IP», откроется окно настроек (см. рис. 2-6).
2-6 Регистрация шлюза

Шаг 4 Введите IP-адрес шлюза платформа другого вендора, порт шлюза, зарегистрированное имя пользователя (необязательно) и пароль (необязательно), затем нажмите Сохранить.

Если платформа другого вендора требует аутентификации, введите имя пользователя и пароль, заданные для этого H.323-терминала на стороне платформы.

Настройка параметров H.323

Контроллер шлюза
Указать IP

IP-адрес контроллера шлюза
127.0.0.1

Порт контроллера шлюза
1719

Имя пользователя

Пароль

Сохранить

Отмена

2.2.2. Настройка SIP

Шаг 1 В настройках вызова откройте раздел «SIP» и включите переключатель «SIP». Задайте «Отображаемое имя». Остальные параметры рекомендуется оставить по умолчанию. Меню показано на рисунке 2-7.

2-7 Настройка SIP

VB600 SIP1 SIP2 H.323 05.09 Суббота 16:51

Настройки системы

Настройка аккаунта H.323 Конфигурация SIP1 Конфигурация SIP2 Конфигурация звонка

Конфигурация SIP1

Включить SIP Включить

Настройка параметров SIP

Удаленная консоль
Выключить

Отображаемое имя
elink

Видеокодеки основного потока (несколько вариантов)
H264HR;H264BP

Тип дополнительного потока (несколько вариантов)
H264HR;H264BP

Тип аудио (несколько вариантов)
G711A,G711U,G722,OPUS

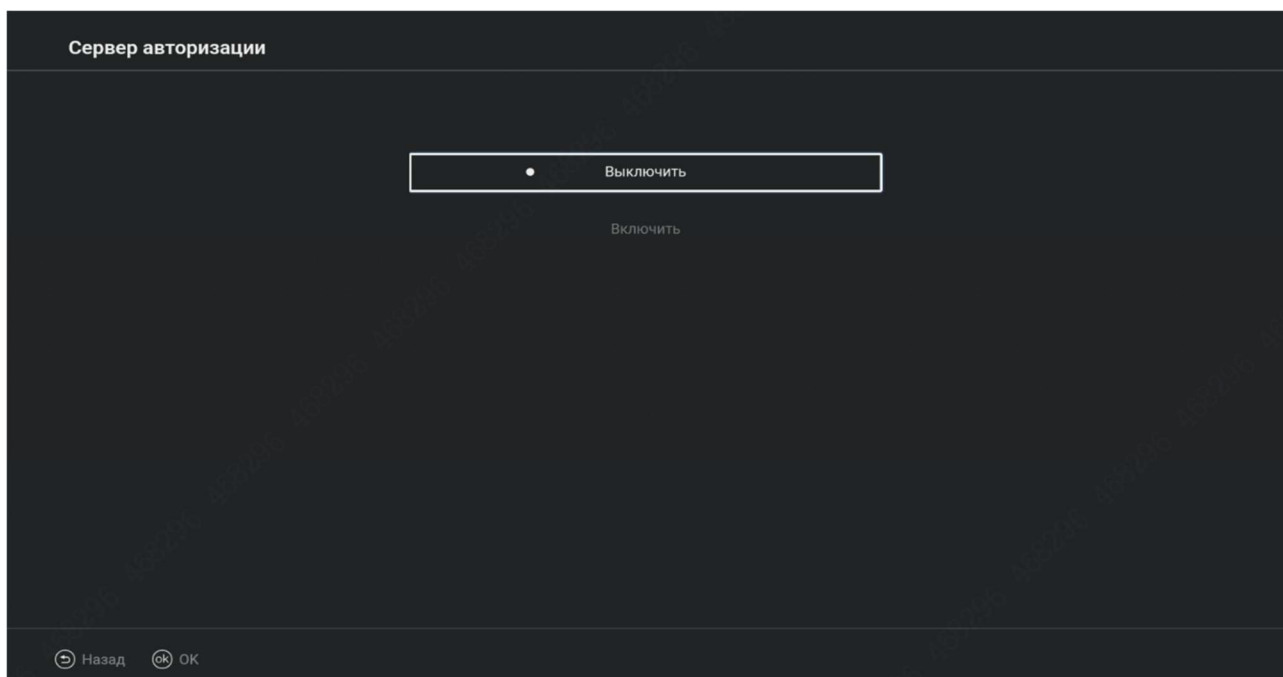
Максимальное разрешение основного потока
1080P

Сохранить

Отмена

Шаг 2 Выберите "Настройка регистрации SIP ", и система будет выглядеть так, см. рис. 2-8

2-8 Настройка параметров SIP



Шаг 3 Чтобы установить режим сервера регистрации, выберите "Включить". Система отобразит меню, см. рис. 2-9

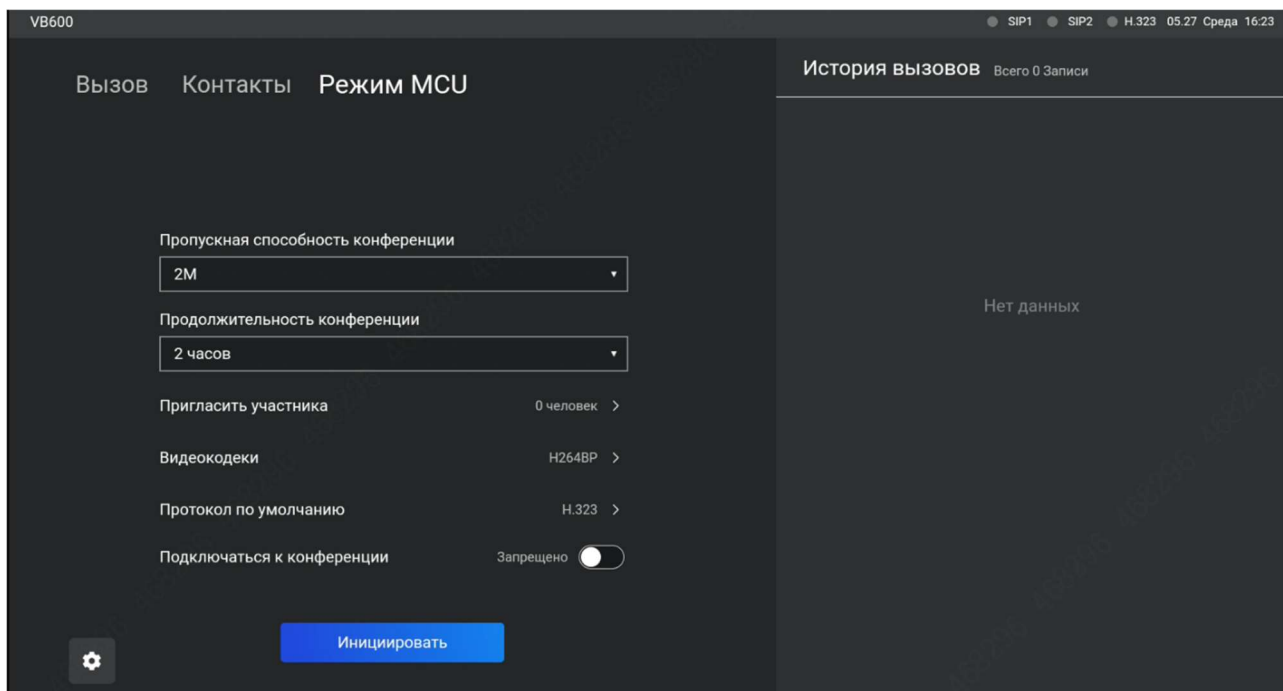
2-9 Сервер регистрации

Шаг 4 Введите IP-адрес прокси-сервера, порт сервера, URI, имя пользователя для аутентификации (необязательно) и пароль для аутентификации (необязательно), затем нажмите Сохранить. Имя пользователя и пароль должны совпадать с учётными данными SIP-терминала, заведёнными на сторонней платформе.

2.3. Режим MCU

Шаг 1 В главном меню вызова выберите «Режим MCU» - откроется окно настроек (см. рис.2-10).

2-10 Режим MCU



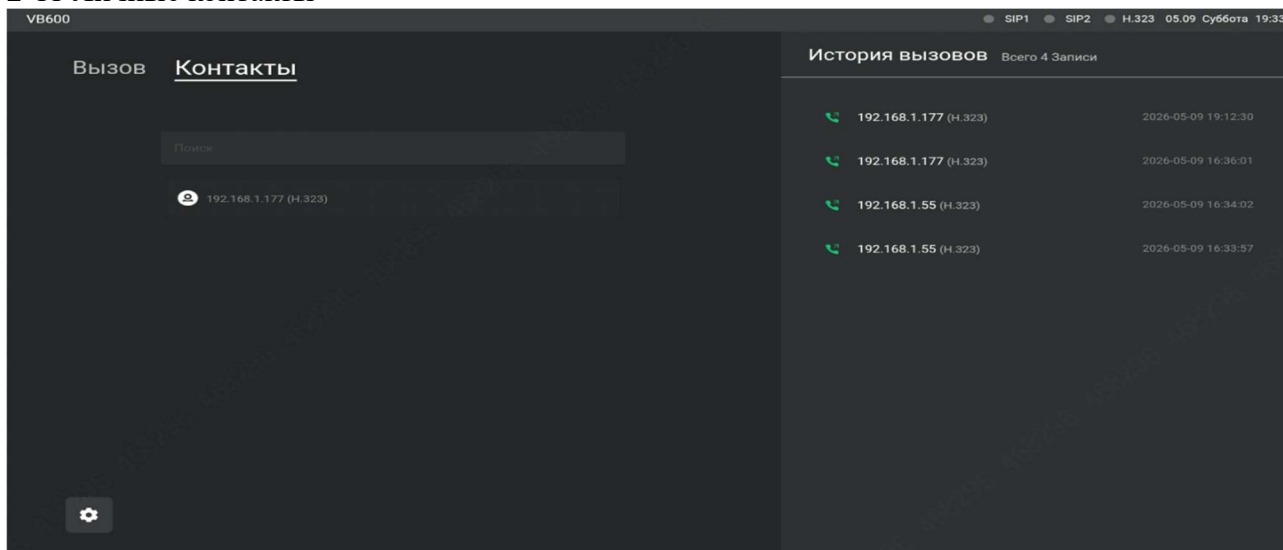
Шаг 2 Задайте пропускную способность конференции, её продолжительность, видеокодеки, параметры вызова и режим присоединения, после чего нажмите «Пригласить участников».

Шаг3 Выберите "Инициировать" чтобы открыть окно конференции.

2.4. Личные контакты

В главном меню вызова выберите «Личные контакты» (см. рис. 2-11). В правой части окна отображаются сохранённые записи вызовов.

2-11 Личные контакты

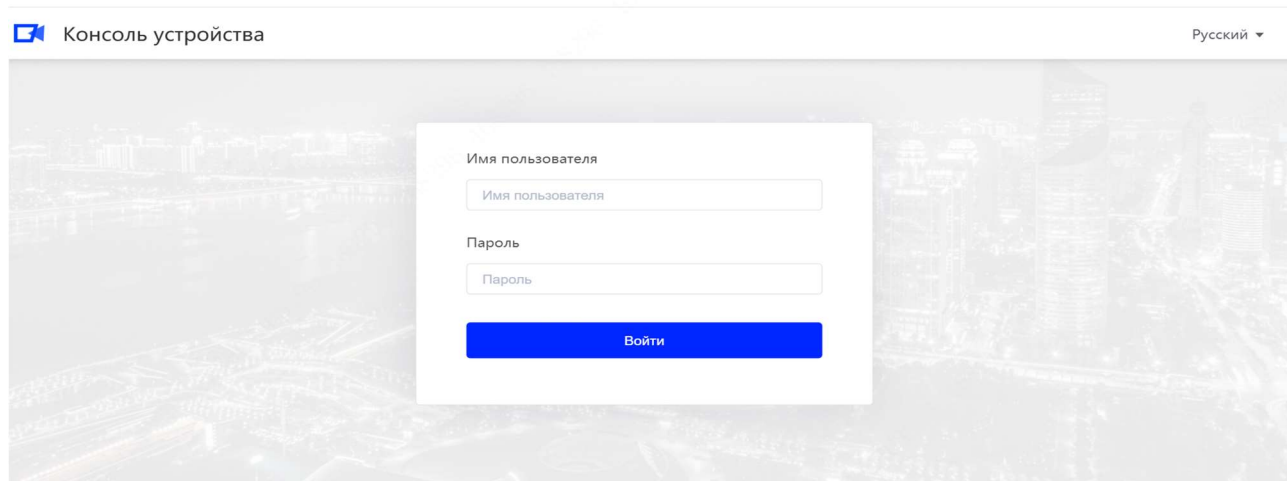


3. Веб-интерфейс

3.1. Авторизация

Войдите на веб-страницу устройства с помощью браузера (см. рис. 3-1).

3-1 Авторизация



3.1.1. Подготовка

- Перед входом убедитесь, что компьютер и устройство находятся в одной подсети (например, при IP-адресе устройства 192.168.1.108 у компьютера должен быть адрес из той же сети, например 192.168.1.2).

3.1.2. Авторизация

Шаг 1 Откройте браузер, введите IP-адрес устройства в адресной строке и нажмите Enter.

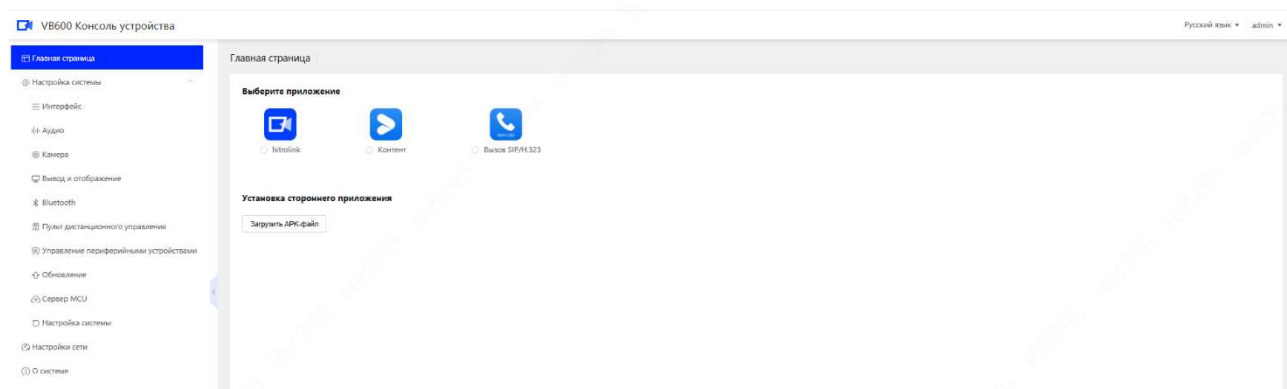
Шаг 2 Введите свое имя пользователя и пароль.

По умолчанию: имя пользователя — admin, пароль — 1234.

Шаг 3 Нажмите "Войти"

3.2. Домашняя страница

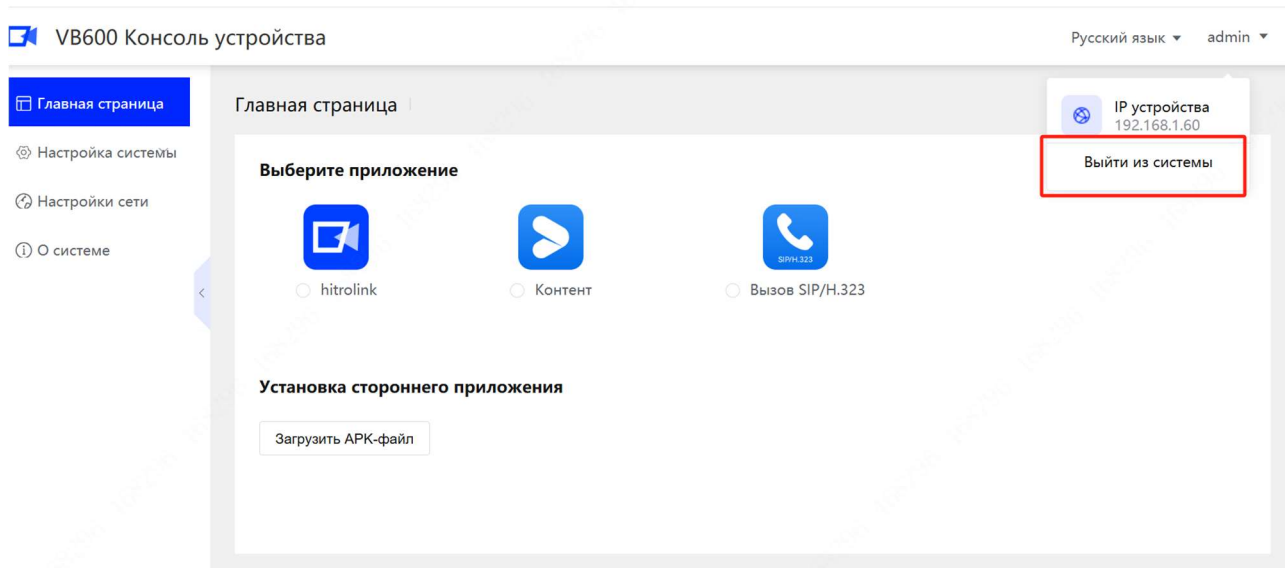
3-2 Домашняя страница



3.2.1. Выход из системы

Нажмите имя пользователя в правом верхнем углу и выберите «Выход» (см. рис 3-3).

3-3 Выход

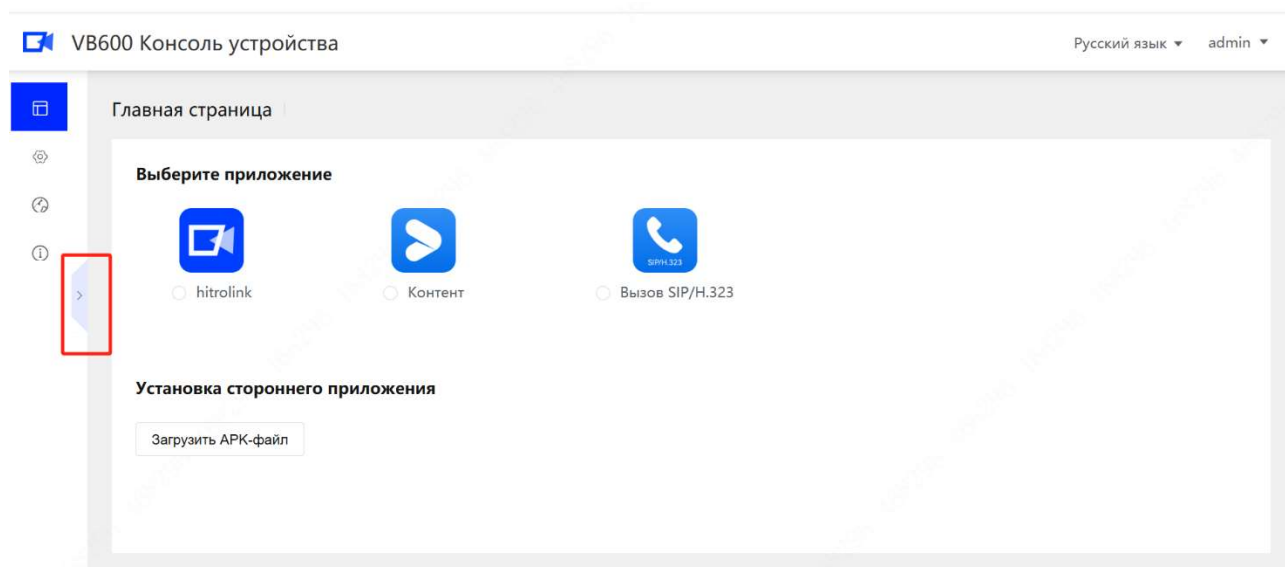


3.2.2. Свернуть или развернуть панель навигации

3.2.2.1. Свернуть панель навигации

Нажмите, чтобы свернуть панель навигации и отобразить уменьшенную версию для облегчения просмотра содержимого веб-страницы (см. рис 3-4).

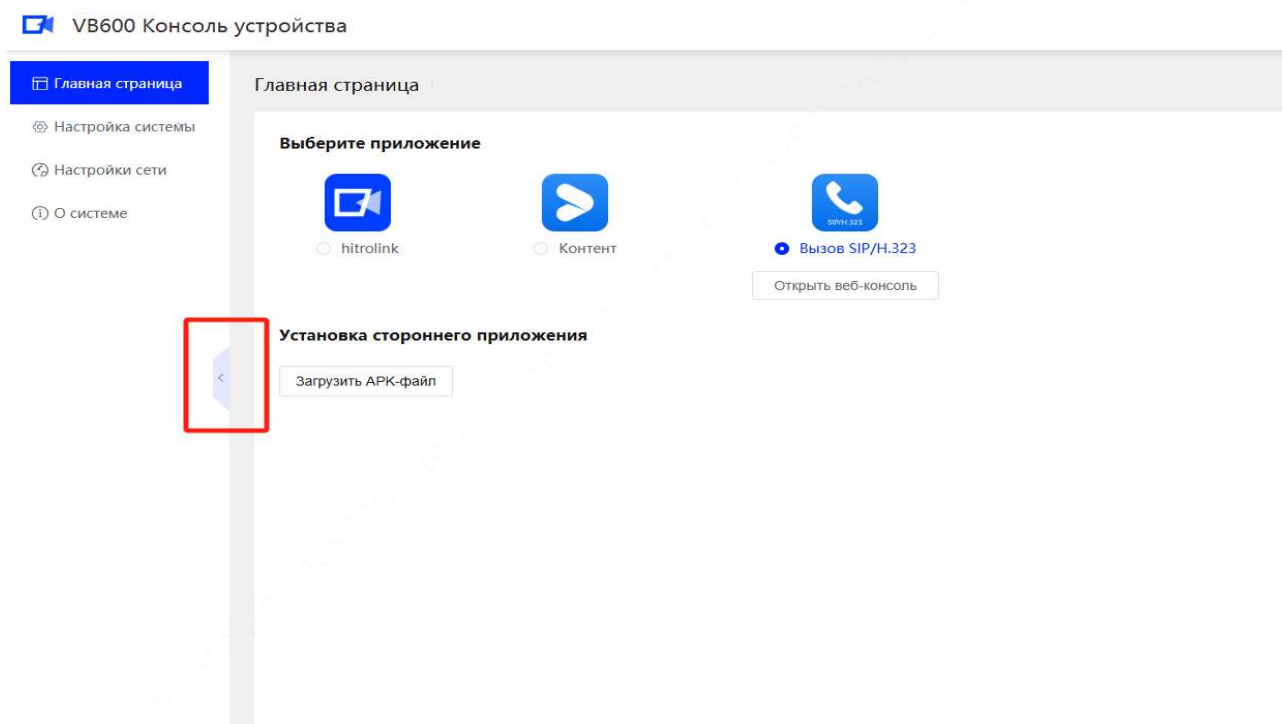
3-4 Свернуть панель навигации



3.2.2.2. Развернуть панель навигации

Повторное нажатие развернёт панель навигации в полную версию (см. рис. 3-5).

3-5 Развернуть панель навигации

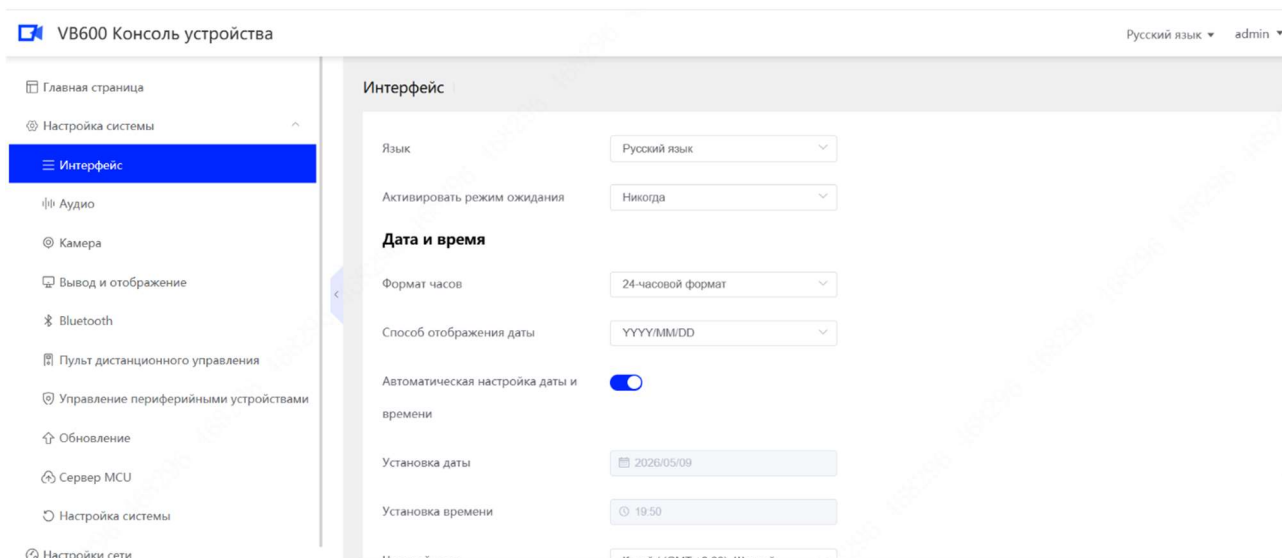


3.3. Настройки веб-интерфейса

3.3.1. Общие настройки

На странице общих настроек задаются язык, дата и время (см. рис. 3-6).

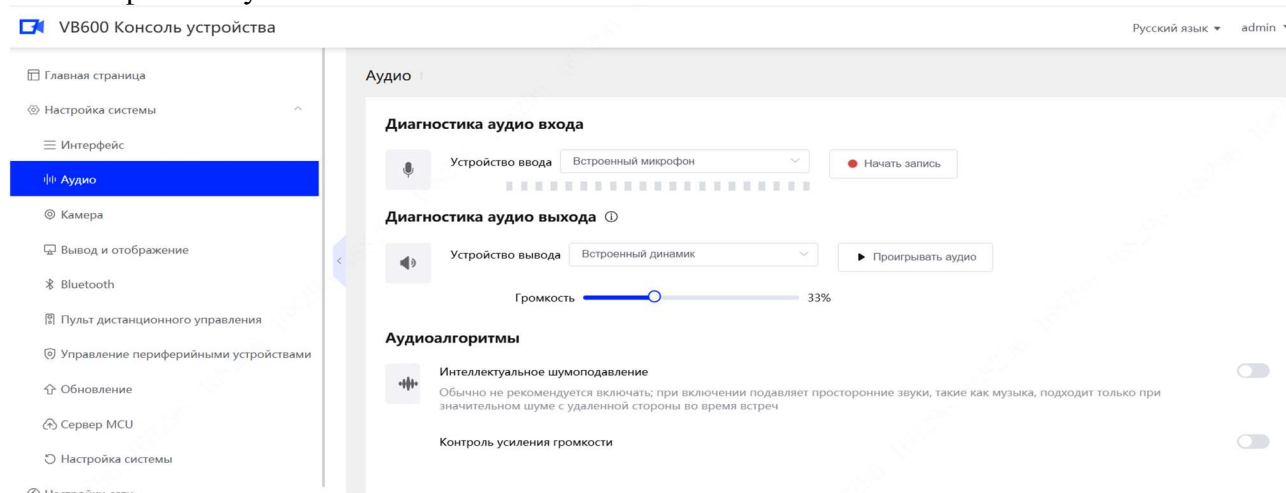
3-6 Общие настройки



3.3.2. Настройки звука

На странице настроек звука задаются параметры входа и выхода аудио (см. рис. 3-7).

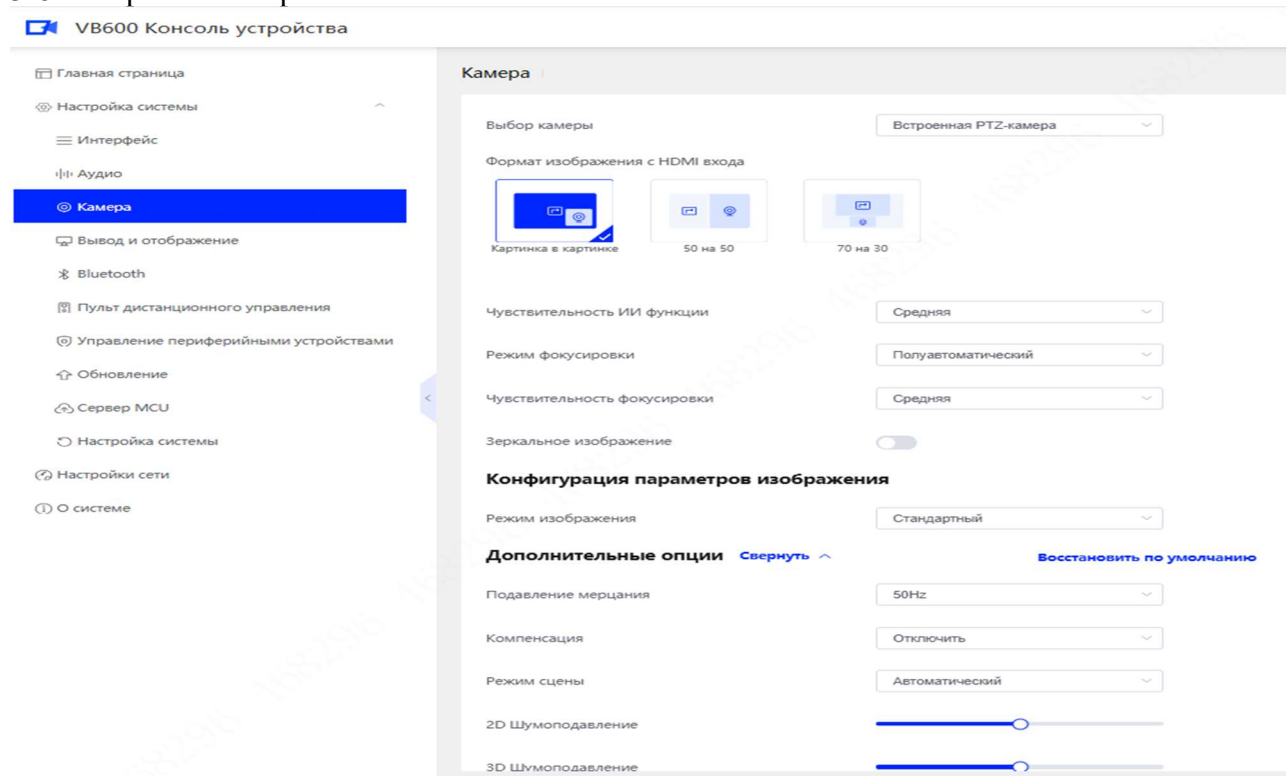
3-7 Настройки звука



3.3.3. Настройки камеры

На странице настроек камеры выбираются модель камеры и параметры изображения (см. рис. 3-8).

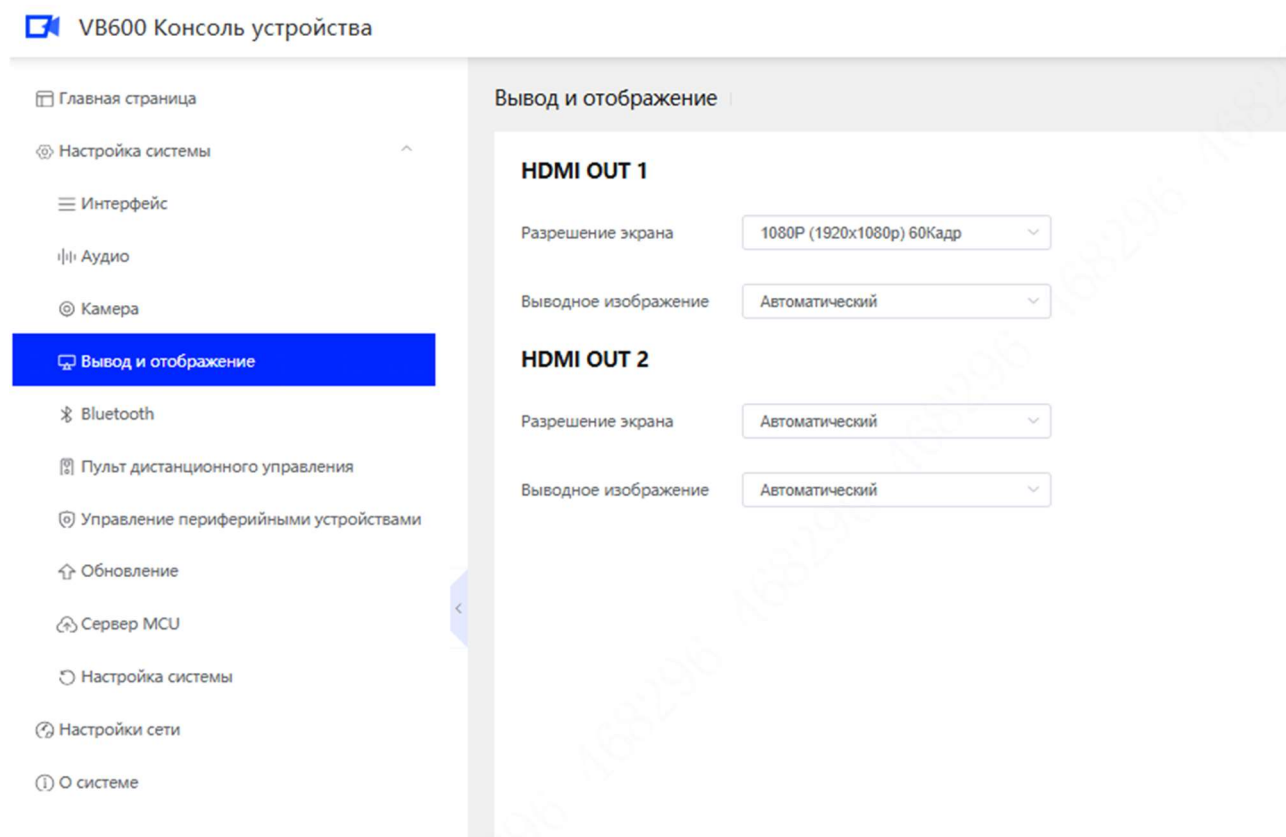
3-8 Настройки камеры



3.3.4. Вывод и отображение

На странице вывода и отображения задаются параметры кодирования основного и дополнительного потоков. Основной поток обеспечивает наилучшее качество; при низкой пропускной способности рекомендуется переключиться на дополнительный (см. рис. 3-9).

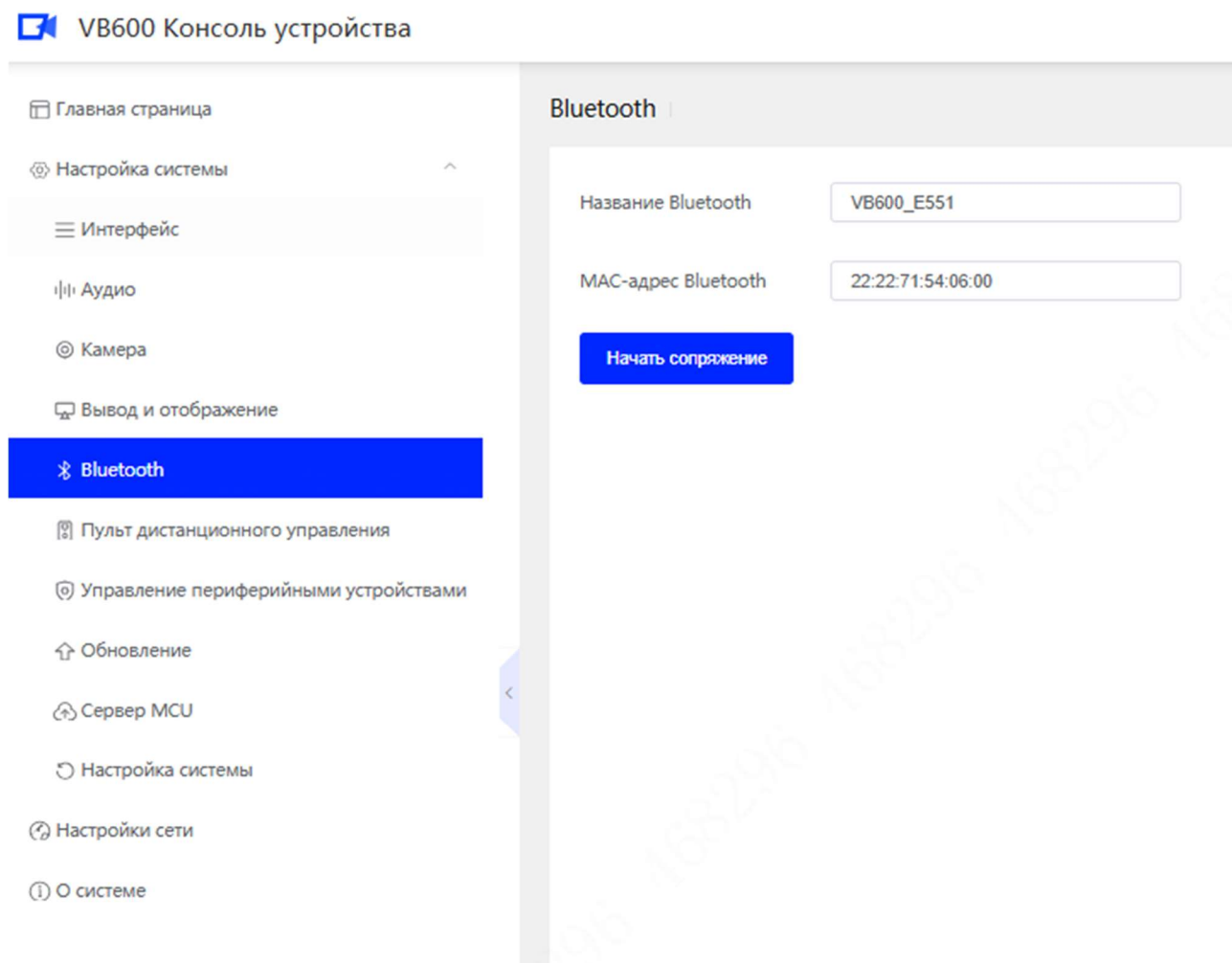
3-9 Вывод и отображение



3.3.5. Bluetooth

В настройках Bluetooth задаются имя устройства Bluetooth и его MAC-адрес (см. рис. 3-10).

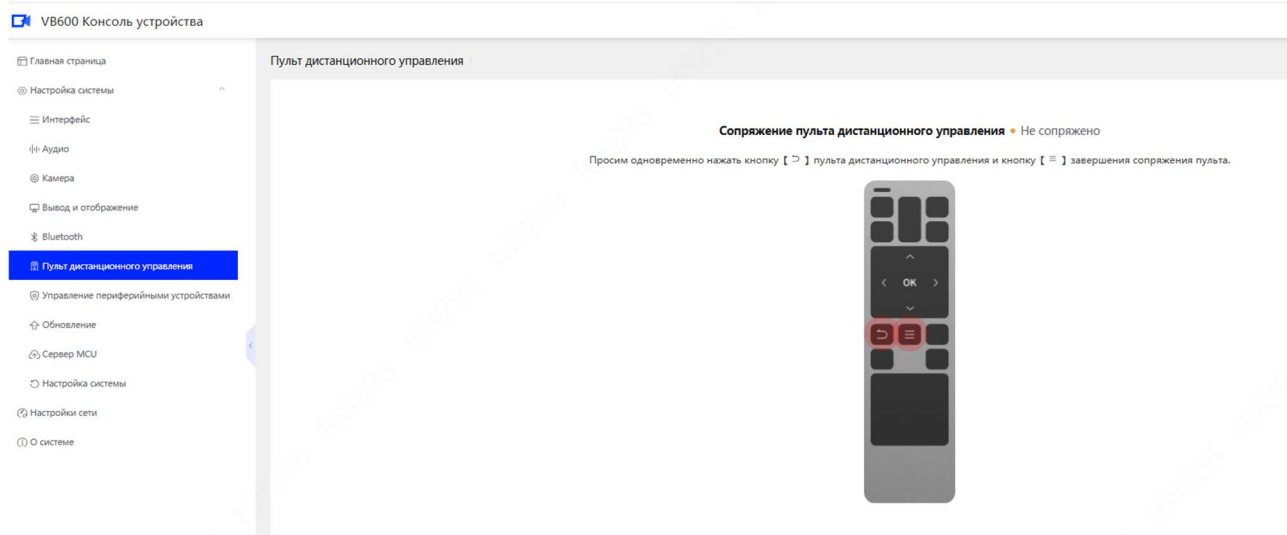
3-10 Bluetooth



3.3.6. Дистанционное управление

В интерфейсе настроек пульта дистанционного управления можно выполнить сопряжение с пультом дистанционного управления, см. рис. 3-11.

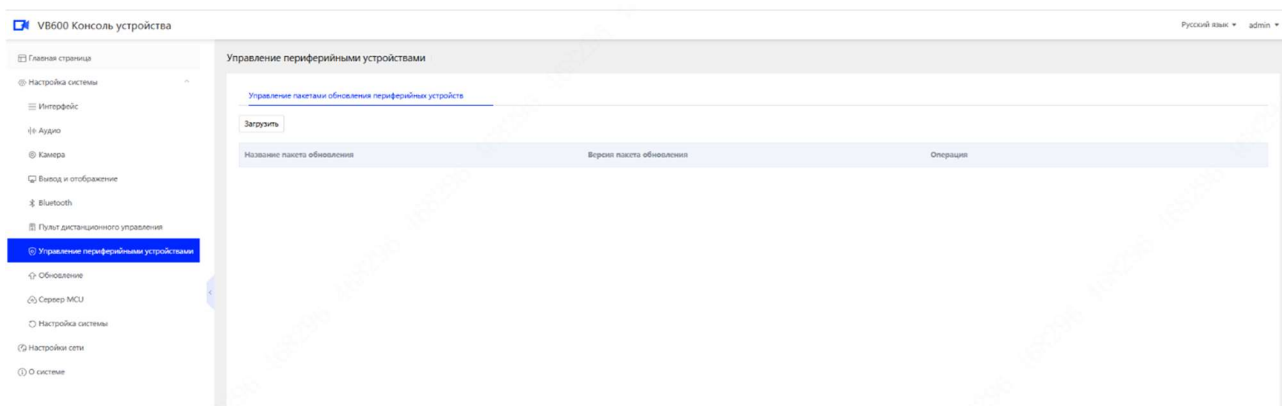
3-11 Дистанционное управление



3.3.7. Управление периферийными устройствами

В интерфейсе настроек управления периферийными устройствами можно управлять обновлением периферийных устройств, см. рис. 3-12.

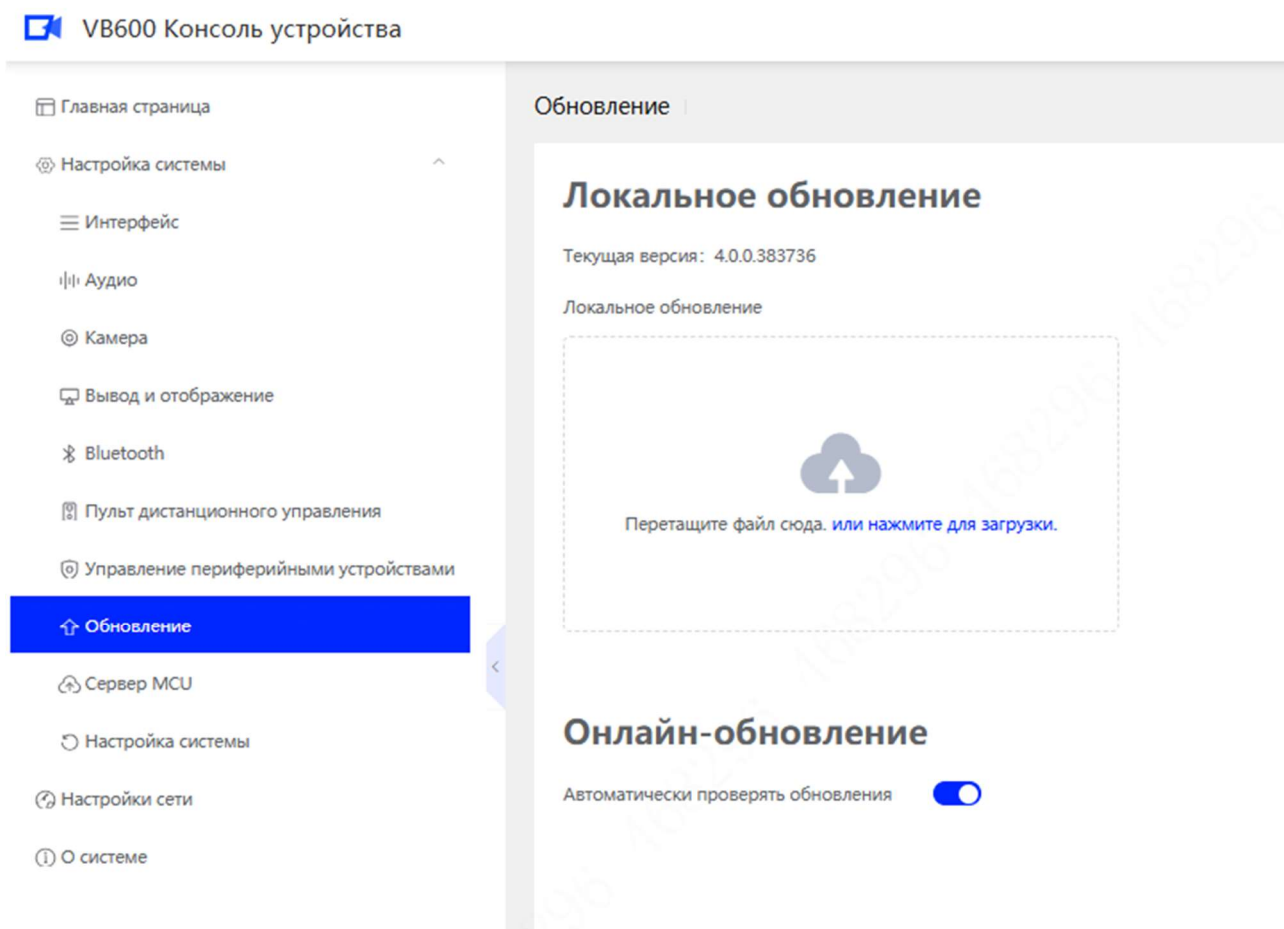
3-12 Управление периферийными устройствами



3.3.8. Обновление

В интерфейсе настроек обновления можно выполнить локальное обновление программного обеспечения на устройстве, см. рис. 3-13.

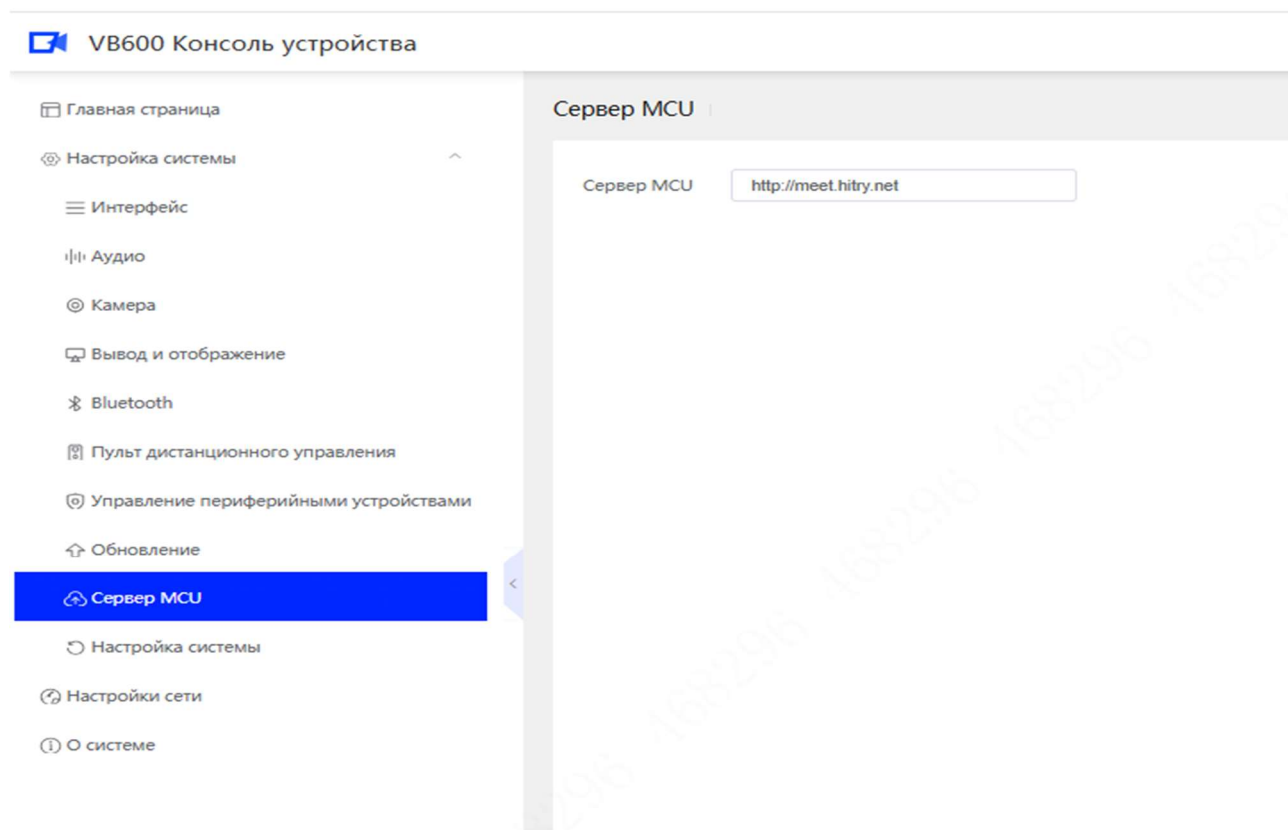
3-13 Обновление



3.3.9. Адрес сервисной службы

На странице адреса сервисной службы введите адрес сервера, чтобы получить соответствующую информацию о версии обновления, см. рис. 3-14.

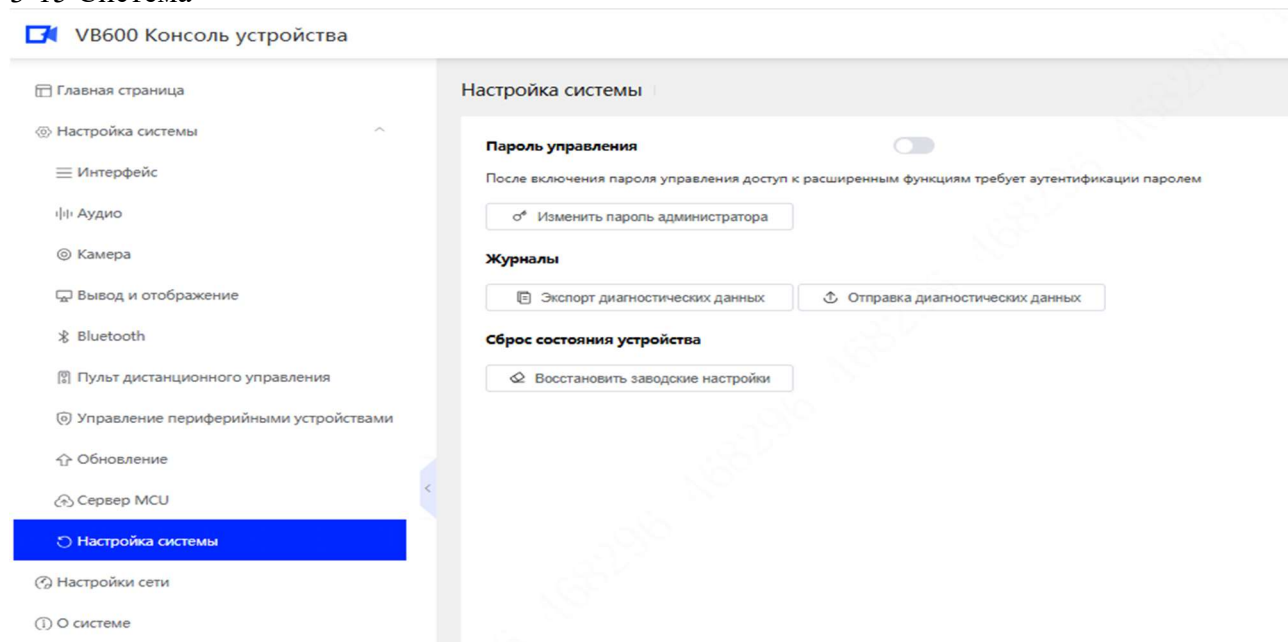
3-14 Адрес сервисной службы



3.3.10. Система

Изменить пароль управления, восстановить заводские настройки, экспортировать журналы и загружать журналы можно в разделе «система», см. рис. 3-15.

3-15 Система



3.4. Сетевые настройки

В интерфейсе «сетевых настроек» вы можете установить такие параметры, как режим IP, IP-адрес, маску подсети, шлюз, настроить точки доступа и выполнить диагностические тесты, (см. рис. 3-16).

3-16 Сетевые настройки

VB600 Консоль устройства

Главная страница

Настройка системы

Интерфейс

Аудио

Камера

Вывод и отображение

Bluetooth

Пульт дистанционного управления

Управление периферийными устройствами

Обновление

Сервер MCU

Настройка системы

Настройки сети

О системе

Настройки сети

Проводная сеть | Точка доступа | Диагностика

Статус подключения: ● Подключено

Режим IP: IPv4

IPv4

DHCP: ●

IP-адрес: 192.168.1.60

Маска подсети: 255.255.255.0

Шлюз: 192.168.1.1

Главный DNS: 0.0.0.0

Резервный DNS: 0.0.0.0

Сохранить изменения

3.5. Об устройстве

На странице «Об устройстве» отображаются имя устройства, номер модели, серийный номер, MAC-адрес, IP-адрес и версия ПО (см. рис. 3-17).

3-17 Об устройстве

VB600 Консоль устройства

Главная страница

Настройка системы

Интерфейс

Аудио

Камера

Вывод и отображение

Bluetooth

Пульт дистанционного управления

Управление периферийными устройствами

Обновление

Сервер MCU

Настройка системы

О системе

Настройка сети

О системе

Название устройства: VB600_2FB0

Модель устройства: VB600

Серийный номер:

MAC-адрес: 22:01:48:FF:2F:B0

IP: 192.168.1.60

Версия системы: 4.0.0.383736(2026-04-20 17:49:45)

Версия платформы для проведения конференций

hitrolink: 4.1.5.382883

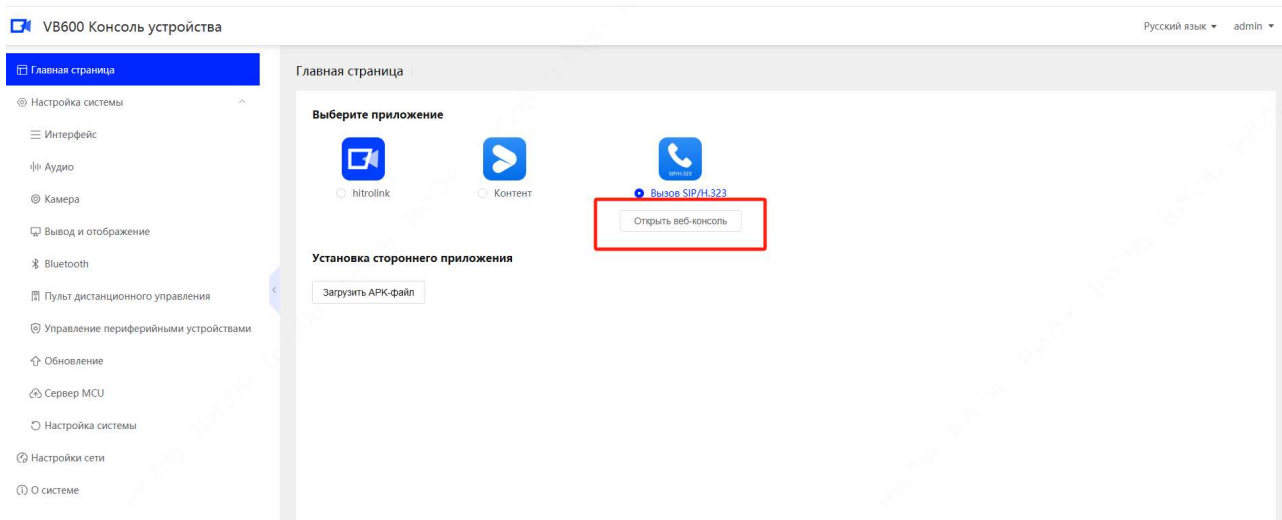
Контент: 1.0.383419

Вызов SIP/H.323: 4.1.5.383726

3.6. Активация режима MCU

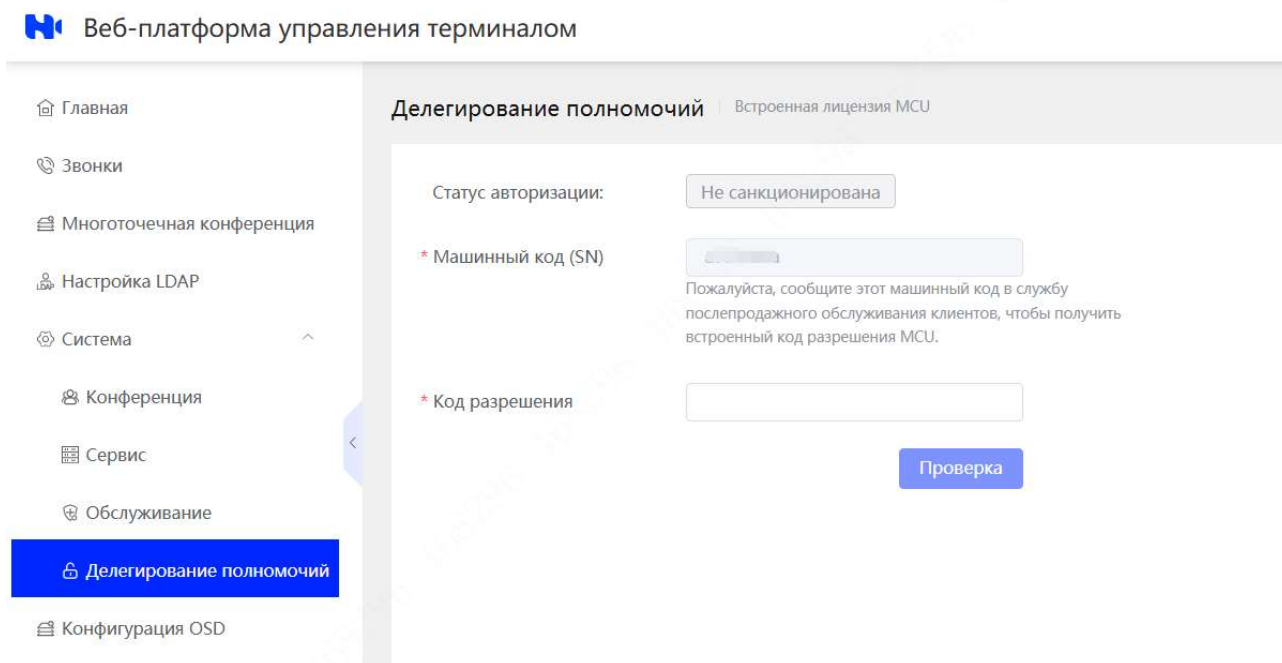
Откройте веб-консоль со стартовой страницы веб-терминала, чтобы перейти к интерфейсу управления устройством (см. рис. 3-18).

3-18 Режим MCU



После входа в веб-интерфейс управления терминалом нажмите «Авторизация функций» и введите код активации, чтобы включить встроенный режим MCU (см. рис. 3-19)

3-19 Активация режима MCU



3.7. LDAP

Задайте адрес сервера LDAP и его параметры. Рекомендуется начать с конфигурации по умолчанию и затем при необходимости её скорректировать (см. рис. 3-20).

3-20 Сервер LDAP

Веб-платформа управления терминалом

Главная
Звонки
Многоточечная конференция
Настройка LDAP
Система
Конференция
Сервис
Обслуживание
Делегирование полномочий
Конфигурация OSD

Настройка LDAP | Настройка LDAP

Включить LDAP ☐

Основные настройки

* Адрес сервера

* Порт

* Тип TLS LDAP

* Имя пользователя

* Пароль

* Базовый DN

Расширенные настройки

* Атрибут имени

4. Юридическая информация

Декларация о товарном знаке

- VGA является торговой маркой IBM Corporation.
- Windows logo и Windows являются товарными знаками или зарегистрированными товарными знаками корпорации Microsoft Corporation.
- Другие товарные знаки и наименования компаний, упоминаемые в настоящем документе, принадлежат их законным владельцам.

Отказ от ответственности

- В пределах, допускаемых применимым законодательством, Компания ни при каких обстоятельствах не несёт ответственности за специальные, случайные или косвенные убытки, возникающие в результате или в связи с содержанием этого документа и описанных здесь продуктов, ни за какую потерю прибыли, данных, деловой репутации, документации или ожидаемой экономии.
- Продукты, описанные в настоящем документе, предоставляются «как есть»; за исключением случаев, прямо предусмотренных законодательством, Компания не предоставляет никаких прямых или подразумеваемых гарантий, включая, в частности, гарантии товарной пригодности, соответствия ожиданиям клиента, пригодности для конкретной цели и ненарушения прав третьих лиц.

Напоминание о защите конфиденциальности

При использовании продукта могут собираться персональные данные: биометрические данные лица, отпечатки пальцев, номерные знаки, адреса электронной почты, номера телефонов и данные геолокации. При использовании нашего продукта вы должны соблюдать законы и нормативные акты о конфиденциальности вашего региона или страны и защищать законные права и интересы других лиц. Например, вы должны установить четкие и заметные вывески, информирующие соответствующих правообладателей о существовании зоны видеонаблюдения и предоставляющие их контактную информацию.

Об этом документе

- Настоящий документ описывает несколько моделей изделий. За точными сведениями о внешнем виде и функциях обращайтесь к фактическому изделию.
- Любые убытки, понесенные из-за несоблюдения инструкций, содержащихся в этом документе, несет пользователь.
- Настоящий документ периодически обновляется в соответствии с законами и нормативными актами соответствующих регионов. Пожалуйста, обратитесь к бумажной версии, электронному компакт-дису, QR-коду или официальному веб-сайту продукта для получения подробной информации. При расхождениях между бумажной и электронной версиями приоритет имеет электронная версия.
- Компания оставляет за собой право изменять любую информацию в этом документе в любое время. Измененный контент будет добавлен в новую версию этого документа без

предварительного уведомления.

- Этот документ может содержать технические неточности, несоответствия функциям и эксплуатации продукта или типографские ошибки. Окончательная интерпретация компании имеет преимущественную силу.

5. Рекомендации по кибербезопасности

Основные меры по обеспечению базовой сетевой безопасности оборудования:

1. Используйте сложные пароли

Пожалуйста, ознакомьтесь со следующими рекомендациями при установке пароля:

- Длина должна быть не менее 8 символов.
- Он должен содержать по крайней мере два типа символов, включая прописные и строчные буквы, цифры и условные обозначения.
- Не указывайте имена учетных записей или названия учетных записей в обратном порядке.
- Не используйте символы, идущие подряд, такие как 123, abc и т.д.
- Избегайте использования повторяющихся символов, таких как 111, aaa и т.д.

2. Незамедлительно обновляйте встроенное ПО и клиентское программное обеспечение

- Согласно стандартным операционным процедурам в технологической отрасли, встроенное ПО устройства необходимо своевременно обновлять до последней версии, чтобы гарантировать, что устройство обладает новейшими функциями и безопасностью. Когда устройство подключено к сети общего пользования, рекомендуется включить функцию автоматического обнаружения онлайн-обновления, чтобы обеспечить своевременный доступ к информации об обновлении встроенного программного обеспечения, опубликованной производителем.
- Мы рекомендуем вам загрузить и использовать последнюю версию клиентского программного обеспечения.

Рекомендации по повышению сетевой безопасности устройства:

1. Физическая защита

Мы рекомендуем вам принять меры физической защиты вашего оборудования (особенно устройств хранения данных), такие как размещение оборудования в выделенном серверном помещении или шкафу, а также реализовать контроль доступа и управление ключами, чтобы предотвратить физический доступ неуполномоченного персонала к оборудованию или внешним устройствам (таким как USB флэш-накопители или последовательные порты).

2. Регулярно меняйте свой пароль

Мы рекомендуем вам регулярно менять свой пароль, чтобы снизить риск его взлома.

3. Оперативно устанавливайте и обновляйте информацию о сбросе пароля

Устройство поддерживает функцию сброса пароля. Чтобы снизить риск использования этой функции злоумышленниками, своевременно вводите информацию о сбросе пароля, включая зарегистрированный номер вашего мобильного телефона / адрес электронной почты и контрольные вопросы. Если эта информация изменится, немедленно обновите ее. При установке контрольных вопросов рекомендуется не использовать ответы, которые легко угадать.

4. Включить блокировку учетной записи

Блокировка учетной записи включена по умолчанию на заводе-изготовителе. Мы рекомендуем вам сохранить ее включенной для обеспечения безопасности вашей учетной записи. После того, как злоумышленнику не удастся ввести пароль несколько раз, его учетная запись и исходный IP-адрес будут заблокированы.

5. Измените порты по умолчанию для HTTP и других сервисов

Мы рекомендуем вам изменить порты по умолчанию для HTTP и других служб на любые порты между 1024 и 65535, чтобы снизить риск того, что злоумышленники угадают порты ваших служб.

6. Включите HTTPS

Мы рекомендуем вам включить протокол HTTPS для доступа к веб-службам по защищенному каналу.

7. Включить белый список

IP-адресам из белого списка будет разрешен доступ к вашему устройству. Поэтому, обязательно внесите IP адрес вашего компьютера и IP адрес соответствующего устройства в белый список.

8. MAC адрес

Привяжите IP-адрес и MAC-адрес вашего шлюзового устройства, чтобы снизить риск ARP подмены.

9. Соответствующим образом распределите учетные записи и разрешения

Добавляйте новых пользователей разумно, в соответствии с потребностями бизнеса и руководства, и назначайте им минимальный набор разрешений.

10. Отключите ненужные службы и используйте безопасный режим

- Если нет необходимости, рекомендуется отключить SNMP, SMTP, UPnP и другие подобные функции, чтобы снизить риски взлома для вашего устройства.
- При необходимости мы настоятельно рекомендуем вам использовать безопасный режим, включая, но не ограничиваясь:
 - ◊ SNMP: Выберите SNMP v3 и установите сложный пароль шифрования и пароль аутентификации.
 - ◊ SMTP: Выберите TLS для доступа к почтовому серверу.
 - ◊ FTP: Выберите SFTP и установите сложный пароль.
 - ◊ Точка доступа: выберите режим шифрования WPA2-PSK и установите сложный пароль.

11. Зашифрованная передача аудио- и видеосигналов

Если ваши аудио- и видеоданные содержат важный или конфиденциальный контент, рекомендуется включить зашифрованную передачу, чтобы снизить риск кражи при передаче аудио- и видеоданных.

12. Подключайте устройства с помощью PoE

Если устройство поддерживает PoE, рекомендуется использовать PoE для подключения устройства и изоляции камеры от других сетей.

13. Аудит безопасности

- Проверять онлайн-пользователей: Мы рекомендуем вам периодически проверять онлайн-пользователей на предмет выявления любых неавторизованных пользователей, входящих в систему.
- Просмотр журналов устройств: просматривая журналы, можно получить информацию об IP-адресах устройств, которые пытались войти в систему, а также ключевую информацию об операциях вошедших в систему пользователей.

14. Веб-журнал

Из-за ограничений по объему памяти устройства объем хранилища журналов ограничен. Если вам необходимо сохранять журналы в течение длительного времени, рекомендуется включить функцию сетевого журнала, чтобы гарантировать синхронизацию важных журналов с сервером сетевых журналов для упрощения отслеживания проблем.

15. Создание безопасной сетевой среды

Чтобы лучше обеспечить безопасность устройства и снизить риски кибербезопасности, мы рекомендуем вам:

- Отключите функцию переадресации портов маршрутизатора, чтобы внешние сети не могли напрямую обращаться к службам устройств во внутренней сети маршрутизатора.
- Разделите сеть на зоны в зависимости от реальных сетевых потребностей: если между двумя подсетями нет необходимости в связи, рекомендуется использовать VLAN, сетевые шлюзы или другие методы для сегментирования сети и достижения сетевой изоляции.
- Установите систему аутентификации доступа 802.1x, чтобы снизить риск

несанкционированного доступа терминалов к частной сети.

- Включите брандмауэр устройства или функцию "черный список", чтобы снизить риск атаки на устройство.