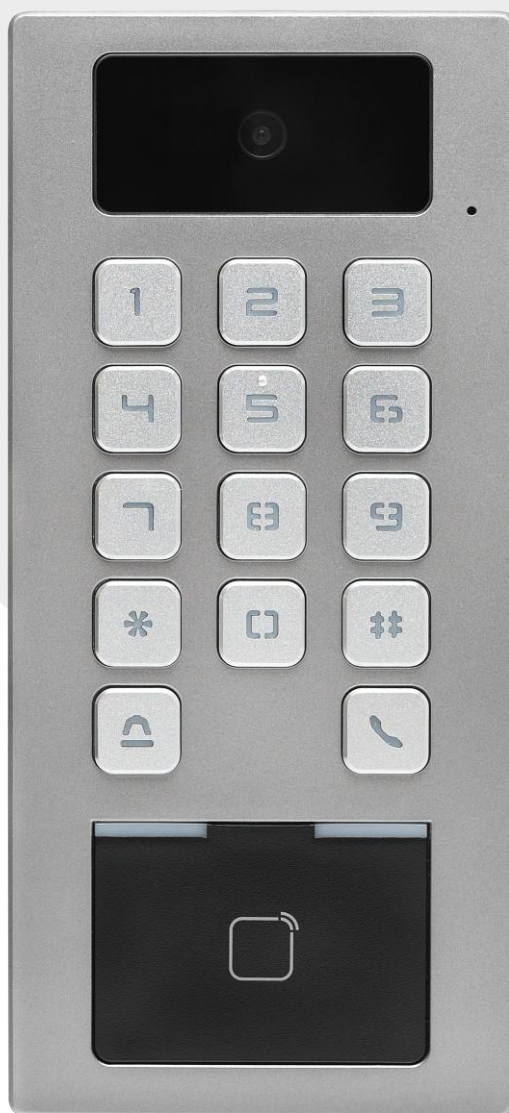


Руководство по эксплуатации



ЛКД-ВСМ-01

Многоабонентская вызывная IP панель



SEC.RU

ПОРТАЛ ПО БЕЗОПАСНОСТИ

www.luis.ru

Благодарим за приобретение оборудования торговой марки ЛКД.

Сведения, представленные в данном руководстве, верны на момент их публикации. Производитель оставляет за собой право в одностороннем порядке без уведомления потребителя вносить изменения в изделия для улучшения их технологических и эксплуатационных параметров. Вид изделий может незначительно отличаться от представленного на фотографиях. Обновления будут включены в новую версию данного руководства.

Оглавление

1. Техника безопасности.....	5
2. Описание	6
2.1 Обзор	6
2.2 Функции.....	6
2.3 Описание внешнего вида.....	7
3. Монтаж	8
3.1 Условия установки.....	8
3.2 Установка без монтажной коробки	8
4. Подключение.....	10
4.1 Описание клемм	10
4.2 Подключение внешних устройств	11
4.3 Подключение блока контроля двери	12
5. Активация	13
5.1 Активация через мобильный браузер	13
5.2 Активация через веб-браузер.....	13
5.3 Активация через LTV-CMS	14
5.4 Активация устройства через клиентское ПО LTV-CMS.....	15
6. Идентификация и аутентификация	16
6.1 Аутентификация по одному учётному данному	16
6.2 Аутентификация по нескольким учётным данным	16
7. Звонки и видеодомофон.....	17
8. Работа через веб-браузер.....	17
8.1 Вход в систему	17
8.2 Забыли пароль	17
8.3 Загрузка веб-плагина.....	18
8.4 Помощь.....	18
8.4.1 Лицензии на программное обеспечение с открытым исходным кодом	18
8.4.2 Просмотр документации онлайн-справки	18
8.5 Выход из системы	18
8.6 Быстрые операции в веб-браузере	18
8.6.1 Настройка контрольных вопросов	18
8.6.2 Выбор языка Вы можете выбрать язык для системы устройства.	18
8.6.3 Настройки времени	19
8.6.4 Настройки конфиденциальности	19
8.6.5 Нумерация и системные сетевые настройки	19
8.7 Управление персоналом.....	21
8.8 Управление контролем доступа.....	22
8.8.1 Обзор	22
8.8.2 Поиск событий	23
8.8.3 Конфигурация параметров двери	24
8.8.4 Настройки аутентификации	26
8.8.5 Настройки карт.....	30
8.8.6 Настройка реакций (Linkage Settings).....	32
8.8.7 Настройка рабочего режима через веб-интерфейс ПК.....	33
8.8.8 Настройка удаленной верификации	33
8.8.9 Настройки конфиденциальности	34
8.9 Настройки видеодомофона.....	35
8.9.1 Управление устройствами	35
8.9.2 Настройка номера устройства через веб-интерфейс	36
8.9.3 Настройка сетевых параметров видеодомофона через веб-браузер	37
8.9.4 Настройки вызова	38
8.9.5 Настройка вызова по нажатию кнопки через веб-интерфейс ПК	38
8.9.6 Настройка номеров через веб-интерфейс ПК.....	38
8.10 Конфигурация системы	39
8.10.1 Настройка локальных параметров.....	39



8.10.2 Просмотр информации об устройстве через веб-интерфейс ПК	39
8.10.3 Настройка времени	40
8.10.4 Настройка летнего времени (DST).....	40
8.10.5 Смена пароля администратора	41
8.10.6 Настройки безопасности учетной записи через веб-интерфейс ПК	41
8.10.7 Онлайн-пользователи	41
8.10.8 Просмотр статуса постановки/снятия с охраны устройства через веб-интерфейс ПК	41
8.10.9 Сетевые настройки	42
8.10.10 Настройка видео и аудио параметров через веб-интерфейс ПК	46
8.10.11 Настройки параметров изображения.....	47
8.10.13 Настройка тревоги через веб-интерфейс ПК.....	48
8.10.14 Конфигурация подключений	49
8.11 Система и обслуживание	51
8.11.1 Перезагрузка	51
8.11.2 Обновление.....	51
8.11.3 Восстановление	51
8.11.4 Экспорт параметров устройства через веб-интерфейс ПК	52
8.11.5 Импорт параметров устройства через веб-интерфейс ПК.....	52
8.11.6 Отладка устройства	52
8.11.7 Просмотр журнала через веб-интерфейс ПК	53
8.11.8 Настройки режима безопасности	53
8.11.9 Управление сертификатами	53
9. Настройка устройства через мобильный браузер.....	55
9.1 Вход в систему	55
9.2 Забыли пароль	55
9.3 Настройки безопасности учетной записи.....	56
9.4 Главный экран.....	56
9.5 Настройка	56
9.5.1 Просмотр информации об устройстве.....	56
9.5.2 Настройка времени	56
9.5.3 Настройка летнего времени (DST).....	57
9.5.4 Управление пользователями.....	58
9.5.5 Сеть	58
9.5.6 Управление пользователями.....	60
9.5.7 Поиск событий	62
9.5.8 Настройки аудио.....	62
9.5.9 Настройки контроля доступа	62
9.5.10 Настройки вызова.....	67
9.5.11 Настройка параметров конфиденциальности через мобильный веб-интерфейс.....	69
9.5.12 Режим пароля	69
9.5.13 Обновление и обслуживание	70
9.5.14 Просмотр пользовательской документации.....	70
9.5.15 Лицензии ПО с открытым исходным кодом	70
9.5.16 Выход из мобильного веб-интерфейса	71
10. Другие платформы для настройки	71
11. Приложение А. Советы по сканированию отпечатка пальца	71
12. Габаритные размеры	73
13. Гарантия	74
О бренде ЛКД.....	74

1. Техника безопасности

Инструкция по технике безопасности

Данные инструкции предназначены для обеспечения правильного использования изделия с целью исключения опасности или материального ущерба.

Меры предосторожности подразделяются на **ОПАСНОСТИ** и **МЕРЫ ПРЕДОСТОРОЖНОСТИ**:

ОПАСНОСТИ: Игнорирование этих предупреждений может привести к серьезной травме или смерти.

МЕРЫ ПРЕДОСТОРОЖНОСТИ: Игнорирование этих предостережений может привести к травме или повреждению оборудования.

ОПАСНОСТИ: Соблюдайте эти меры предосторожности для предотвращения серьезных травм или смерти.

- Все работы с электрооборудованием должны строго соответствовать правилам электробезопасности, противопожарным нормам и другим соответствующим правилам вашего региона.
- Пожалуйста, используйте источник питания, предоставленный официальным поставщиком. Мощность источника питания не должна быть меньше требуемого значения.
- Не подключайте несколько устройств к одному источнику питания, так как его перегрузка может вызвать перегрев или возгорание.
- Убедитесь, что питание отключено, перед выполнением подключения проводов, установки или демонтажа устройства.
- При установке изделия на стену или потолок устройство должно быть надежно закреплено.
- Если от устройства исходит дым, запах или шум, немедленно отключите питание и отсоедините кабель питания, а затем обратитесь в сервисный центр.
- Не глотайте батарею. Опасность химического ожога.

Это изделие содержит батарейку-таблетку. При проглатывании такая батарейка может вызвать тяжелые внутренние ожоги всего за 2 часа и привести к летальному исходу.

Храните новые и использованные батареи в недоступном для детей месте. Если отсек для батареи невозможно надежно закрыть, прекратите использование изделия и уберите его от детей. Если вы подозреваете, что батарейка могла быть проглочена или помещена в любую часть тела, немедленно обратитесь за медицинской помощью.

- Если изделие работает некорректно, обратитесь к вашему поставщику или в ближайший сервисный центр. Никогда не пытайтесь разобрать устройство самостоятельно. (Мы не несем ответственности за проблемы, вызванные несанкционированным ремонтом или обслуживанием.)

МЕРЫ ПРЕДОСТОРОЖНОСТИ: Соблюдайте эти меры предосторожности для предотвращения возможных травм или материального ущерба.

- Данное оборудование не предназначено для использования в местах, где вероятно присутствие детей.
- Не допускайте падения устройства или сильных физических воздействий, а также воздействия сильного электромагнитного излучения. Избегайте установки оборудования на вибрирующих поверхностях или в местах, подверженных ударам (пренебрежение может привести к повреждению оборудования).
- Не размещайте устройство в чрезвычайно жарких (см. спецификации устройства для подробного диапазона рабочих температур), холодных, пыльных или влажных местах и не подвергайте его сильному электромагнитному излучению.
- Корпус устройства, предназначенный для использования внутри помещений, должен быть защищен от дождя и влаги.
- Запрещается подвергать оборудование воздействию прямых солнечных лучей, размещать его в местах с плохой вентиляцией или вблизи источников тепла, таких как обогреватели или радиаторы (пренебрежение может создать опасность возгорания).
- Не направляйте устройство на солнце или на чрезмерно яркие источники света. В противном случае может возникнуть засветка или размытие (что, однако, не является неисправностью), что также может повлиять на долговечность сенсора.
- При открытии крышки устройства используйте предоставленные перчатки, чтобы избежать прямого контакта с ней, так как кислота в поте пальцев может повредить защитное покрытие поверхности крышки.

- Для очистки внутренних и внешних поверхностей крышки устройства используйте мягкую сухую ткань; не используйте щелочные моющие средства.
- Сохраните всю оригинальную упаковку для возможного будущего использования. В случае возникновения неисправности вам потребуется вернуть устройство на завод в оригинальной упаковке. Транспортировка без оригинальной упаковки может привести к повреждению устройства и дополнительным затратам.
- Неправильное использование или замена батареи может привести к ее взрыву. Заменяйте батарею только на батарею того же или эквивалентного типа. Утилизируйте использованные батареи в соответствии с инструкциями производителя.

2. Описание

2.1 Обзор

Данное устройство представляет собой терминал контроля доступа, предназначенный для аутентификации. Он поддерживает двустороннюю аудиосвязь, удаленный просмотр в реальном времени, захват изображения, запись видео через сетевой видеорегистратор и так далее.

2.2 Функции

- Управление контролем доступа, видеодомофонами и видеонаблюдением с одного устройства.
- Степень защиты IP65 и IK09, а также повышенная стабильность работы благодаря материалу из цинкового сплава.
- Несколько методов аутентификации, включая отпечаток пальца, карту и т.д.

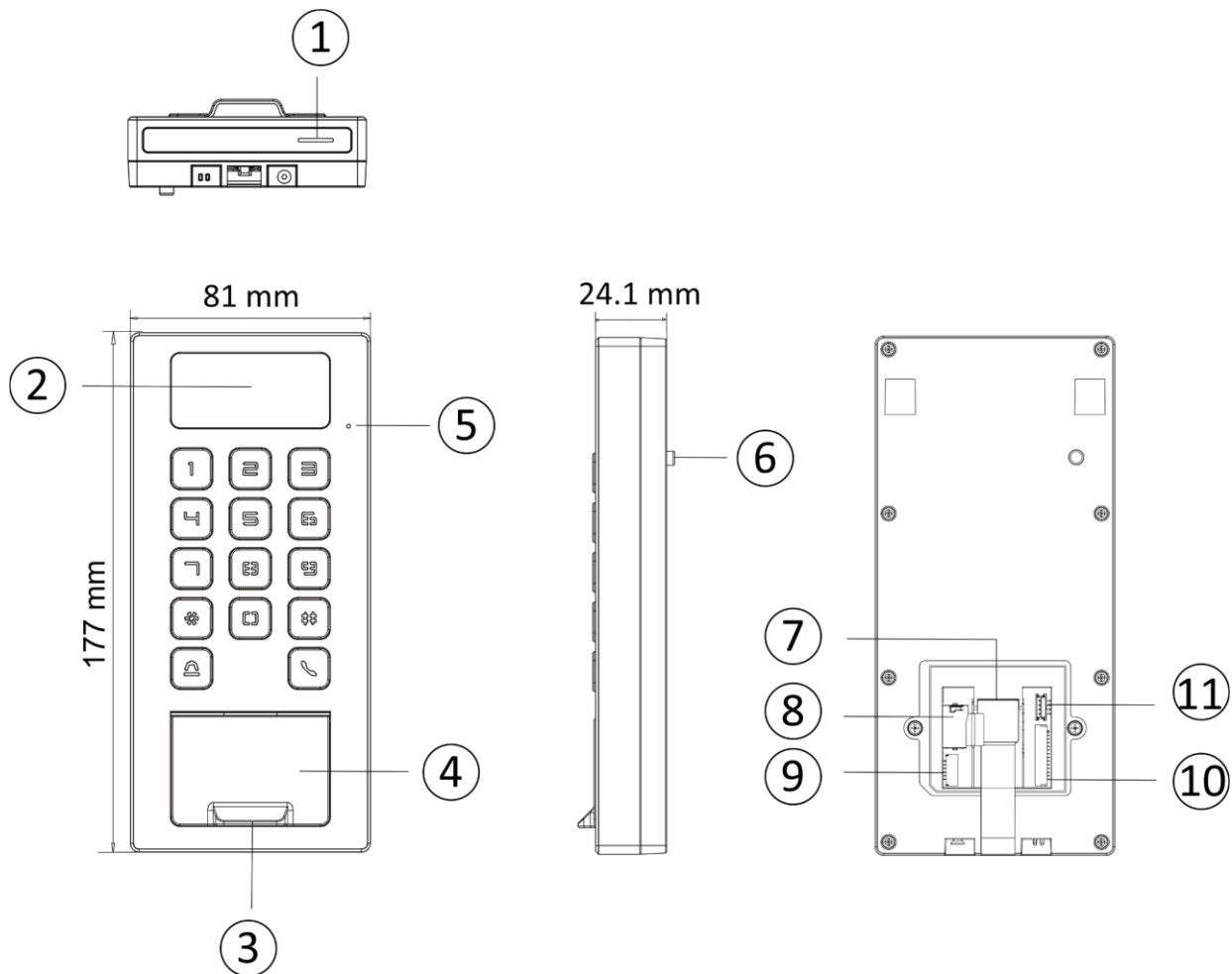
Примечание

Функция распознавания отпечатка пальца поддерживается только частью модулей устройства.

- Удаленное управление через мобильное приложение LTV-CMS Mobile2.
- Подключение к внешнему контроллеру доступа по протоколу Wiegand.
- Двусторонняя аудиосвязь по протоколу SIP 2.0.
- Связь по RS-485 для подключения внешнего считывателя карт.
- Поддержка сетевого подключения через точку доступа.
- Поддержка формата видео кодирования H.265.

2.3 Описание внешнего вида

Описание внешнего вида устройства приведено в соответствующем разделе.



1. Динамик
2. Камера (Поддерживается некоторыми моделями устройства)
3. Модуль отпечатка пальца (Поддерживается некоторыми моделями устройства)
4. Зона для прикладывания карты
5. Микрофон
6. Датчик вскрытия (Тампер)
7. Сетевой интерфейс
8. Слот для SD-карты
9. Клеммник для подключения входа/выхода тревоги
10. Клеммник для подключения
11. Отладочный порт (Только для отладки)

3. Монтаж

3.1 Условия установки

- Устанавливайте устройство на расстоянии не менее 2 метров от источников света и не менее 3 метров от окон или дверей.
- Убедитесь, что уровень освещенности помещения превышает 100 Люкс.

Примечание

Подробную информацию об условиях установки см. в разделе «*Рекомендации по условиям установки*».

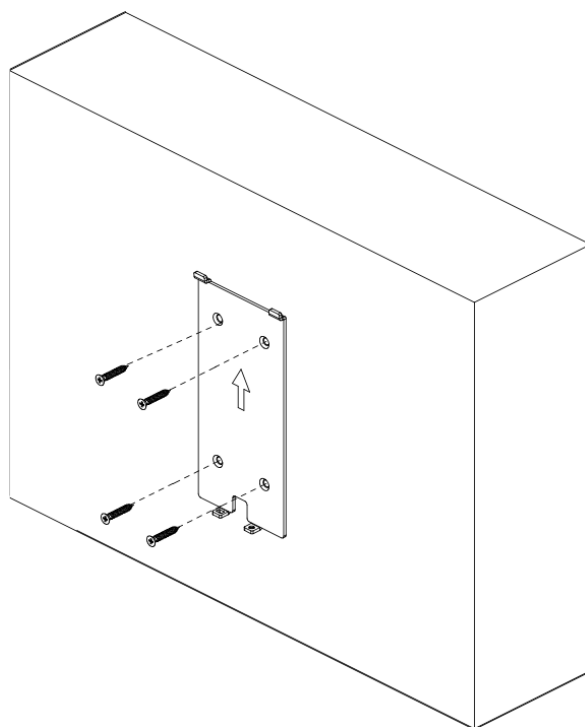
3.2 Установка без монтажной коробки

Шаги

Примечание

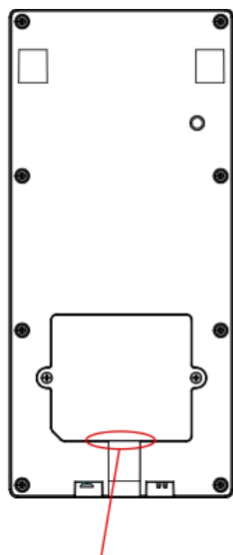
Прилагаемое дополнительное усилие должно в три раза превышать вес оборудования. Оборудование и связанные с ним средства крепления должны оставаться надежно закрепленными в процессе установки. После установки оборудование, включая любую монтажную пластину, не должно быть повреждено.

1. Закрепите монтажную пластину на стене с помощью 4 прилагаемых винтов (SC-KA4X25-SUS).



Закрепление монтажной пластины

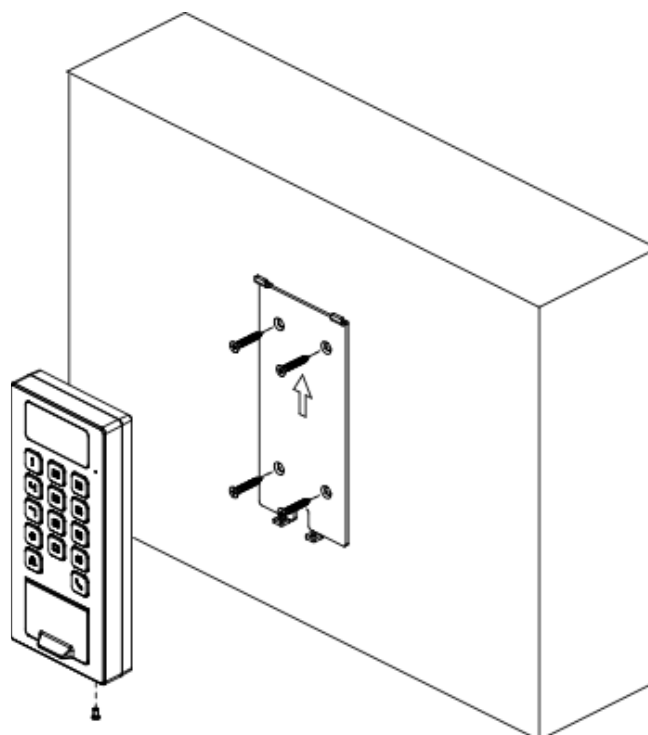
2. Проденьте кабель через отверстие в монтажной пластине и подключите его к кабелям соответствующих внешних устройств.
3. Нанесите силиконовый герметик на стыки между задней панелью устройства и стеной (кроме нижней стороны), чтобы предотвратить попадание дождевой воды.



Нанесите
силиконовый
герметик

Нанесение силиконового герметика по бокам

4. Совместите устройство с монтажной пластиной и закрепите устройство на пластине с помощью 1 прилагаемого винта (SC-KM3X6-T10-SUS).



Закрепление устройства

4. Подключение

4.1 Описание клемм

Клеммы включают вход питания, вход тревоги, выход тревоги, RS-485, выход Wiegand и замок.

Схема клеммного подключения представлена ниже:

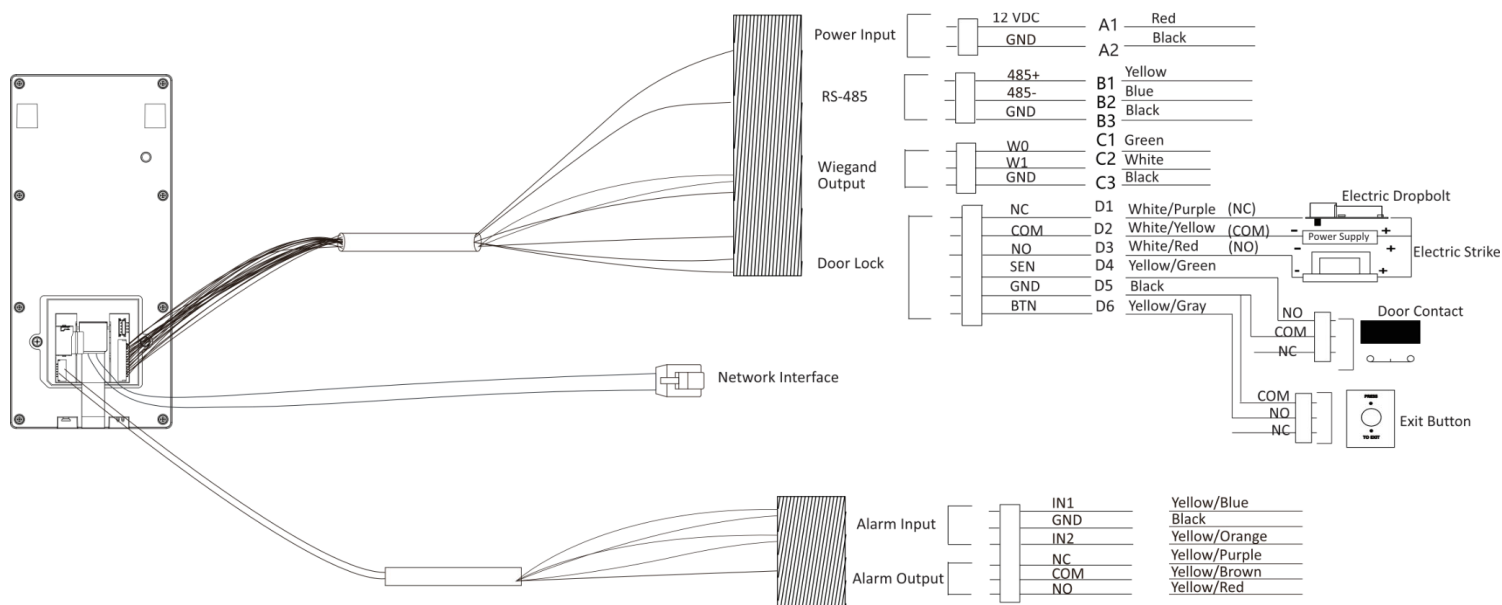


Схема клеммного подключения

Описание клемм приведено в следующей таблице:

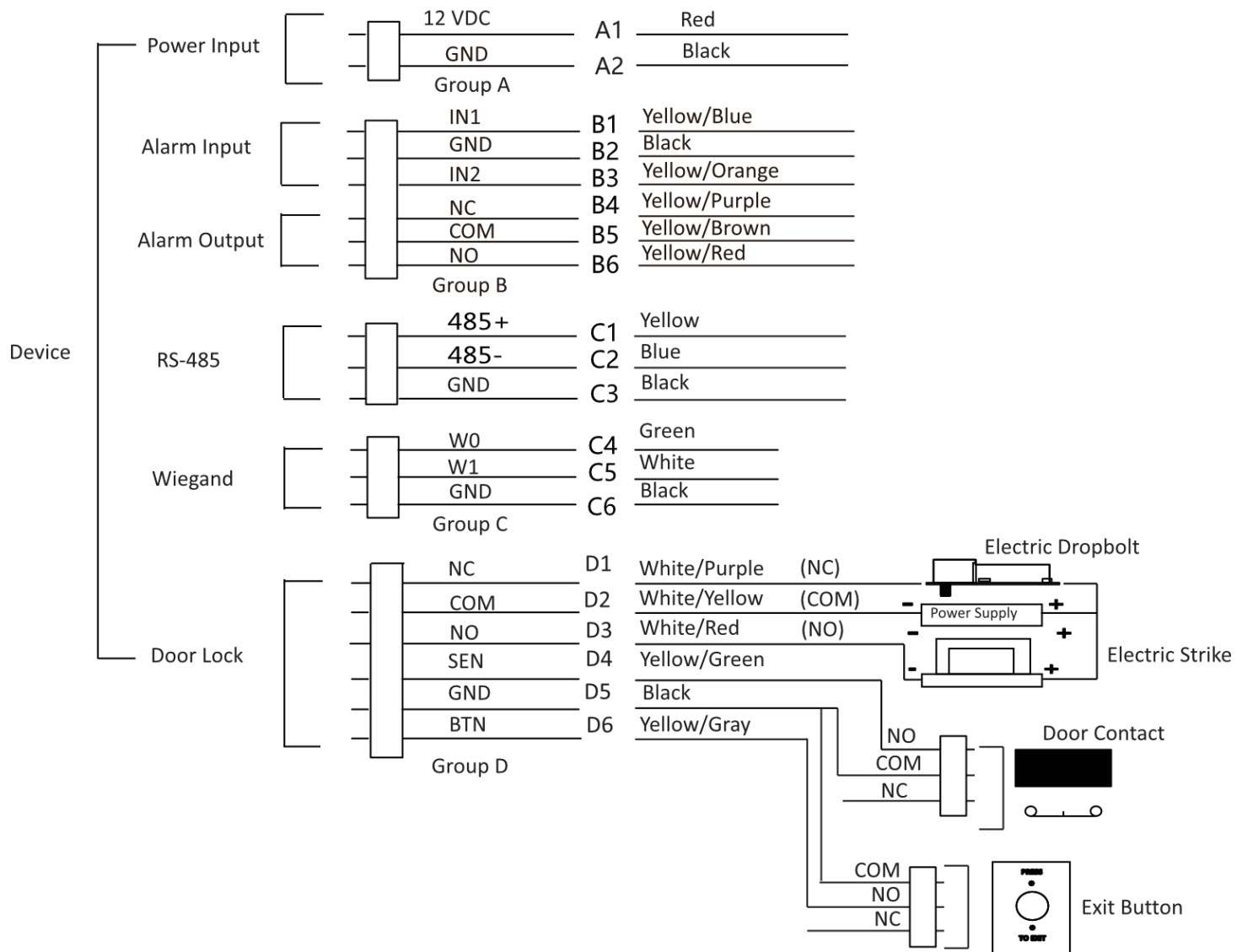
Описание клемм

Группа	Но.	Функция	Цвет	Наименование	Описание
Группа А	A1	Вход питания	Красный	+12 V	Питание 12 В (DC)
	A2		Черный	GND	Заземление
Группа В	B1	RS-485	Желтый	485+	RS-485
	B2		Синий	485-	
	B3		Черный	GND	Заземление
Группа С	C1	Wiegand	Зеленый	W0	Wiegand 0
	C2		Белый	W1	Wiegand 1
	C3		Черный	GND	Заземление
Группа D	D1	Замок	Белый/Фиолетовый	NC	Замок (H3)

	D2		Белый/Желтый	COM	Общий
	D3		Белый/Красный	NO	Замок (НО)
	D4		Желтый/Зеленый	SENSOR	Дверной контакт
	D5		Черный	GND	Заземление
	D6		Желтый/Серый	BTN	Подключение двери выхода

4.2 Подключение внешних устройств

Подключите внешние устройства.
Схема подключения представлена ниже.

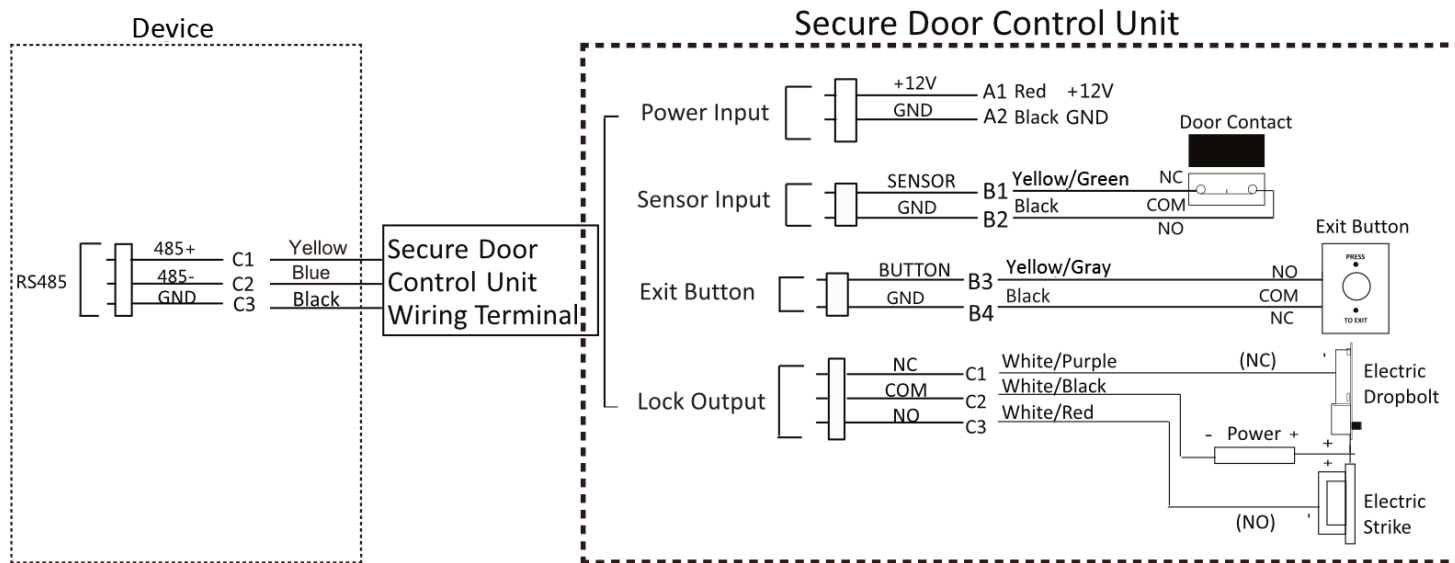


Подключение внешних устройств

4.3 Подключение блока контроля двери

Вы можете подключить клеммы к блоку контроля двери.

Схема подключения представлена ниже.



Подключение блока контроля двери

Примечание

- Блок контроля двери должен подключаться к отдельному внешнему источнику питания. Рекомендуемое напряжение источника питания — 12 В, 0,5 А.
- Для сценариев с высокими требованиями к безопасности рекомендуется в первую очередь использовать схему подключения с блоком контроля двери.
- Для приобретения блока контроля двери отдельно обратитесь в службу технической поддержки.
- На рисунке показана часть подключения. Подробности см. в руководстве пользователя блока контроля двери.
- Устройство поддерживает подключение блока контроля двери с функцией привязки. Блок контроля двери, который уже был привязан к другому устройству, необходимо отвязать перед привязкой к новому устройству.

5. Активация

Перед первым входом в систему необходимо активировать устройство. После включения питания система перейдет на страницу активации устройства.

Поддерживается активация через само устройство, утилиту LTV-CMS и клиентское программное обеспечение.

Значения по умолчанию для устройства приведены ниже:

- IP-адрес по умолчанию: 192.0.0.64
- Порт по умолчанию: 80
- Имя пользователя по умолчанию: admin

5.1 Активация через мобильный браузер

Вы можете активировать устройство через мобильный браузер.

Шаги

Примечание

После первого включения питания устройства функция точки доступа (hotspot) включена по умолчанию.

1. Включите функцию Wi-Fi на мобильном телефоне. Найдите и подключитесь к точке доступа устройства (hotspot) (имя точки доступа: AP_СерийныйНомер).

Примечание

- Имя точки доступа/пароль: AP_СерийныйНомер.
- Удерживайте клавишу 5 на клавиатуре устройства в течение 5 с, чтобы включить/выключить функцию точки доступа.
- Через 30 минут после включения питания устройства функция точки доступа будет автоматически отключена.
- После активации устройства пароль точки доступа будет изменен на пароль активации устройства.

2. Мобильный телефон автоматически перейдет на страницу в браузере. Создайте новый пароль (пароль администратора) и подтвердите его.

Примечание

Запрещается использовать символы, содержащие `admin` и `nimda`, в качестве пароля активации.

Внимание

РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ — Настоятельно рекомендуется создать надежный пароль по вашему выбору (используя минимум 8 символов, включая заглавные и строчные буквы, цифры и специальные символы) для повышения безопасности вашего продукта. Рекомендуется регулярно изменять ваш пароль, особенно в системах с высокими требованиями к безопасности; изменение пароля ежемесячно или еженедельно позволяет лучше защитить ваш продукт.

3. Нажмите «Активировать».
4. **Измените IP-адрес устройства.** Вы можете изменить IP-адрес с помощью утилиты LTV-CMS, веб-браузера на ПК или клиентского программного обеспечения.

5.2 Активация через веб-браузер

Вы можете активировать устройство через веб-браузер.

Шаги

1. Введите IP-адрес устройства по умолчанию (192.0.0.64) в адресную строку веб-браузера и нажмите Enter.

Примечание

Убедитесь, что IP-адрес устройства и компьютера находятся в одной IP-сети.

2. Создайте новый пароль (пароль администратора) и подтвердите его.

Внимание

РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ — Настоятельно рекомендуется создать надежный пароль по вашему выбору (используя минимум 8 символов, включая заглавные и строчные буквы, цифры и специальные символы) для повышения безопасности вашего продукта. Рекомендуется регулярно изменять ваш пароль, особенно в системах с высокими требованиями к безопасности; изменение пароля ежемесячно или еженедельно позволяет лучше защитить ваш продукт.

Примечание

Запрещается использовать символы, содержащие `admin` и `nimda`, в качестве пароля активации.

3. Нажмите «**Активировать**».
4. Измените IP-адрес устройства. Вы можете изменить IP-адрес с помощью утилиты LTV-CMS, самого устройства или клиентского программного обеспечения.

5.3 Активация через LTV-CMS

LTV-CMS — это утилита для обнаружения, активации и изменения IP-адреса устройства в локальной сети (LAN).

Перед началом работы

- Загрузите программное обеспечение LTV-CMS с прилагаемого диска.
- Устройство и ПК, на котором запущена утилита LTV-CMS, должны находиться в одной подсети.

Следующие шаги показывают, как активировать устройство и изменить его IP-адрес. Для пакетной активации и изменения IP-адресов обратитесь к **Руководству пользователя LTV-CMS**.

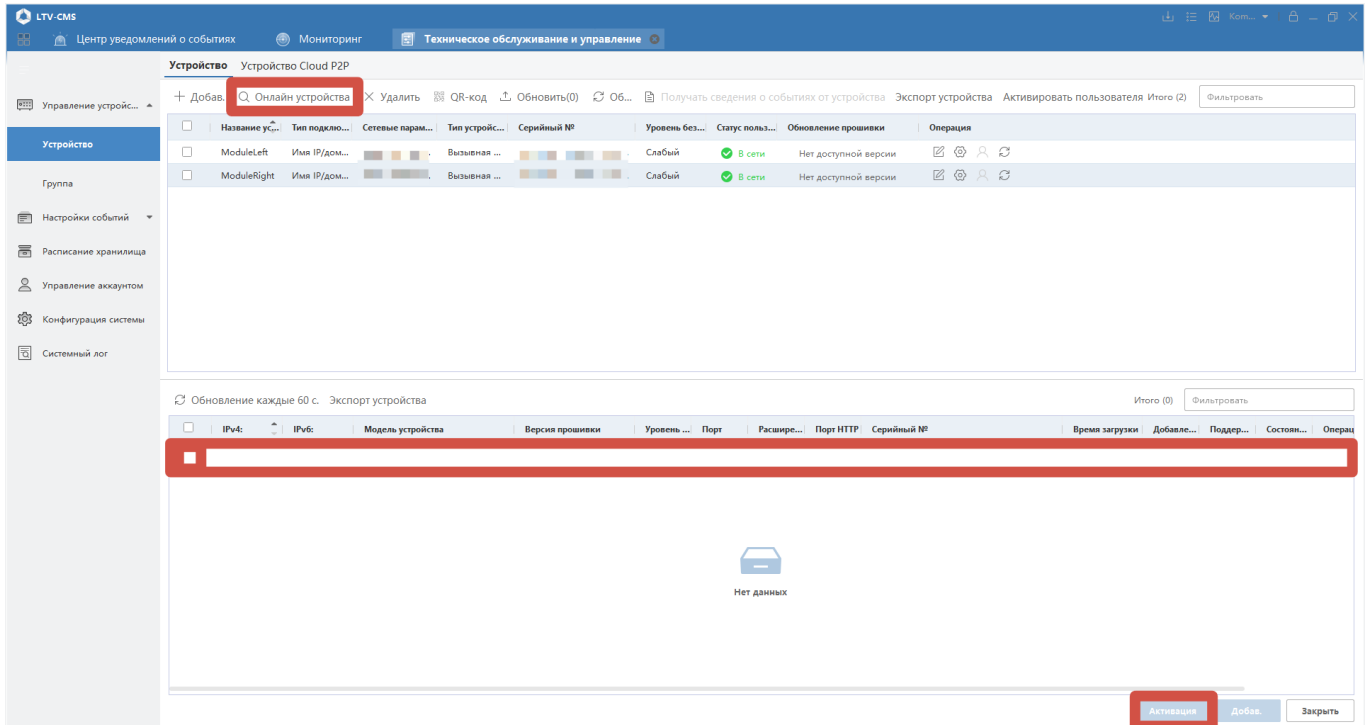
Шаги

1. Запустите программное обеспечение LTV-CMS и выполните поиск онлайн-устройств.
2. Найдите и выберите ваше устройство в списке онлайн-устройств.
3. Введите новый пароль (пароль администратора) и подтвердите его.

Внимание

РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НАДЕЖНЫЙ ПАРОЛЬ — Настоятельно рекомендуется создать надежный пароль по вашему выбору (используя минимум 8 символов, включая заглавные и строчные буквы, цифры и специальные символы) для повышения безопасности вашего продукта. Рекомендуется регулярно изменять ваш пароль, особенно в системах с высокими требованиями к безопасности; изменение пароля ежемесячно или еженедельно позволяет лучше защитить ваш продукт.

4. Нажмите «**Активировать**» для начала активации.



После успешной активации статус устройства изменится на «**Активно**».

5. Измените IP-адрес устройства.
 - 1) Выберите устройство.
 - 2) Измените IP-адрес устройства на принадлежащий той же подсети, что и ваш компьютер, либо вручную, либо установив флажок «**Включить DHCP**».
 - 3) Введите пароль администратора и нажмите «**Изменить**», чтобы применить новое значение IP-адреса.

5.4 Активация устройства через клиентское ПО LTV-CMS

Для некоторых устройств требуется создать пароль и активировать их, прежде чем они смогут быть добавлены в ПО LTV-CMS и нормально функционировать.

Шаги

Примечание

Данная функция должна поддерживаться устройством.

1. Перейдите на страницу **Управление устройствами**.
2. Нажмите на значок  справа от раздела «**Управление устройствами**» и выберите **Устройство**.
3. Нажмите **Сетевое устройство**, чтобы отобразить область сетевых устройств. Обнаруженные сетевые устройства отображаются в списке.
4. Проверьте статус устройства (указывается в столбце «**Уровень безопасности**») и выберите неактивное устройство.
5. Нажмите **Активировать**, чтобы открыть диалоговое окно активации.
6. Создайте пароль в поле для ввода и подтвердите его.

Внимание

Надежность пароля проверяется автоматически. Настоятельно рекомендуется задать пароль по вашему выбору (используя минимум 8 символов, включая, по крайней мере, три категории из следующих: заглавные буквы, строчные буквы, цифры и специальные символы) для повышения безопасности вашего продукта. Рекомендуется регулярно изменять пароль, особенно в системах с высокими требованиями к безопасности; ежемесячная или еженедельная смена пароля лучше защитит ваш продукт. Ответственность за правильную настройку всех паролей и других параметров безопасности лежит на установщике и/или конечном пользователе.

Примечание

Запрещается использовать символы, содержащие `admin` и `nimda`, в качестве пароля активации.

7. Нажмите **ОК**, чтобы активировать устройство.

6. Идентификация и аутентификация

После настройки сети, системных параметров и пользователей можно вернуться на начальную страницу для проведения идентификации. Система будет проводить аутентификацию личности в соответствии с настроенным режимом.

6.1 Аутентификация по одному учётному данному

Перед аутентификацией необходимо задать тип аутентификации пользователя.

Аутентификация по отпечатку пальца, карте, PIN-коду или QR-коду:

Отпечаток пальца

Приложите зарегистрированный отпечаток пальца к модулю сканирования для начала аутентификации по отпечатку.

Карта

Приложите карту к зоне считывания для начала аутентификации по карте.

Примечание

Это может быть стандартная IC-карта или зашифрованная карта.

QR-код

Поднесите QR-код к камере устройства для аутентификации.

Примечание

- Динамические QR-коды должны быть аутентифицированы в течение периода их действия. После обновления QR-кода старый код аутентифицировать будет невозможно.
- Аутентификация по QR-коду должна поддерживаться устройством.

PIN-код

Введите PIN-код для аутентификации.

В случае успешной аутентификации появится сообщение «Аутентификация пройдена».

6.2 Аутентификация по нескольким учётным данным

Перед началом

Перед аутентификацией задайте тип аутентификации пользователя.

Шаги

1. Пройдите аутентификацию по любому из учётных данных в соответствии с инструкциями на странице просмотра в реальном времени.

Примечание

- Это может быть стандартная IC-карта или зашифрованная карта.
- Если функция сканирования QR-кода активирована, можно поднести QR-код к камере устройства для аутентификации.

2. После успешной аутентификации по первому учётному данным продолжите аутентификацию по другим данным.

Примечание

Подробную информацию о сканировании отпечатка пальца см. в **Рекомендациях по сканированию отпечатков пальцев**.

В случае успешной аутентификации появится сообщение «Аутентификация пройдена».

7. Звонки и видеодомофон

После настройки SIP-сервера становится возможным осуществление звонков и видеосвязи между устройствами.

Настройте Устройство А в качестве SIP-сервера и укажите IP-адрес Устройства А в качестве IP-адреса SIP-сервера. Все остальные устройства, которым необходимо связываться друг с другом, должны быть зарегистрированы на этом сервере.

Задайте номер помещения для устройства. Подробности см. в разделе «**Назначение номера устройству через веб-интерфейс**».

На главной странице устройства введите номер помещения вызываемого устройства. Когда вызов будет принят, можно будет осуществлять видеосвязь.

8. Работа через веб-браузер

8.1 Вход в систему

Вы можете войти в систему через веб-браузер или удаленную конфигурацию клиентского программного обеспечения.

Примечание

Убедитесь, что устройство активировано. Подробную информацию об активации см. в разделе «**Активация**».

Вход через веб-браузер

Введите IP-адрес устройства в адресной строке веб-браузера и нажмите Enter, чтобы перейти на страницу входа. Введите имя пользователя и пароль устройства. Нажмите «**Войти**».

Вход через удаленную конфигурацию клиентского ПО

Загрузите и откройте клиентское программное обеспечение. После добавления устройства нажмите  для перехода на страницу «**Конфигурация**».

8.2 Забыли пароль

Если вы забыли пароль при входе, вы можете изменить его с помощью адреса электронной почты или контрольных вопросов.

На странице входа нажмите «**Забыли пароль**».

Выберите **Режим проверки**.

Проверка контрольными вопросами

Ответьте на контрольные вопросы.

Проверка по электронной почте

1. Экспортируйте QR-код и отправьте его в виде вложения по адресу pw_recovery@hikvision.com.
2. В течение 5 минут вы получите проверочный код на вашу зарегистрированную электронную почту.
3. Введите проверочный код в соответствующее поле для подтверждения вашей личности.

Нажмите «**Далее**», создайте новый пароль и подтвердите его.

8.3 Загрузка веб-плагина

Доступен как просмотр в реальном времени без плагина, так и после его загрузки. Для лучшего качества видео рекомендуется скачать и установить плагин.

Нажмите  → **Загрузить веб-плагин**, чтобы скачать плагин на локальный компьютер.

8.4 Помощь

8.4.1 Лицензии на программное обеспечение с открытым исходным кодом

Вы можете просмотреть лицензии на программное обеспечение с открытым исходным кодом.

Нажмите  → **Заявление о программном обеспечении с открытым исходным кодом** в правом верхнем углу, чтобы просмотреть лицензии.

8.4.2 Просмотр документации онлайн-справки

Вы можете просмотреть документ справки по веб-конфигурации.

Нажмите  → **Онлайн-документация** в правом верхнем углу веб-страницы, чтобы просмотреть документ.

8.5 Выход из системы

Выйдите из учетной записи.

Нажмите **admin** → **Выйти** → **ОК** для выхода.

8.6 Быстрые операции в веб-браузере

8.6.1 Настройка контрольных вопросов

Если вы забыли пароль активации устройства, вы можете изменить его с помощью контрольных вопросов и электронной почты. Перед настройкой установите контрольные вопросы.

Нажмите на значок в правом верхнем углу веб-страницы , чтобы перейти на страницу «Изменение пароля».

Проверка контрольными вопросами

Ответьте на контрольные вопросы.

Проверка по электронной почте

1. Экспортируйте QR-код и отправьте его в виде вложения по адресу pw_recovery@hikvision.com.
2. В течение 5 минут вы получите проверочный код на вашу зарегистрированную электронную почту.
3. Введите проверочный код в соответствующее поле для подтверждения вашей личности.

Нажмите **Далее**. Или вы можете нажать **Пропустить**, чтобы пропустить этот шаг.

8.6.2 Выбор языка

Вы можете выбрать язык для системы устройства.

Нажмите на значок в правом верхнем углу веб-страницы , чтобы перейти на страницу **Настройки языка устройства**. Вы можете выбрать язык для системы устройства из раскрывающегося списка.

По умолчанию системным языком является английский.

Примечание

После изменения системного языка устройство автоматически перезагрузится.

8.6.3 Настройки времени

Нажмите на значок в правом верхнем углу веб-страницы , чтобы перейти на страницу мастера настройки.

Время устройства

Отображает текущее время устройства в реальном времени.

Часовой пояс

Выберите часовой пояс, в котором находится устройство, из раскрывающегося списка.

Режим синхронизации времени

- **NTP**
Необходимо задать IP-адрес NTP-сервера, номер порта и интервал синхронизации.
- **Вручную**
По умолчанию время устройства задается вручную. Вы можете установить время устройства вручную или установить флажок **Синхронизировать с временем компьютера**, чтобы синхронизировать время устройства с временем компьютера.

Летнее время (DST)

Вы можете включить функцию летнего времени, установить и просмотреть время начала, окончания и смещение для летнего времени.

Нажмите **Далее**, чтобы сохранить настройки и перейти к следующему параметру. Или нажмите **Пропустить**, чтобы пропустить настройку времени.

8.6.4 Настройки конфиденциальности

Установите параметры загрузки и хранения изображений.

Нажмите на значок в правом верхнем углу веб-страницы , чтобы перейти на страницу мастера настройки. После установки языка, времени и окружения устройства вы можете нажать **Далее**, чтобы перейти на страницу **Настройки конфиденциальности**.

Загрузка и хранение изображений

- **Загружать изображение после срабатывания связанной камеры**
Автоматически загружать изображения, снятые связанной камерой, на платформу.
- **Сохранять изображения после срабатывания связанной камеры**
Если эта функция включена, вы можете сохранять изображения, снятые связанной камерой, на устройстве.

Нажмите **Далее**, чтобы сохранить настройки и перейти к следующему параметру. Или нажмите **Пропустить**, чтобы пропустить настройки конфиденциальности.

8.6.5 Нумерация и системные сетевые настройки

Шаги

1. Нажмите на значок в правом верхнем углу веб-страницы , чтобы перейти на страницу мастера настройки. После предыдущих настроек нажмите **Далее**, чтобы перейти на страницу параметров **Нумерация и системные сетевые настройки**.
2. Установите тип устройства.

Примечание

- Если выбран тип устройства «**Вызывная панель**», можно задать **номер этажа, номер вызывной панели, номер жилого комплекса, номер здания, номер подъезда, номер этажа**.
- Если выбран тип устройства «**Внешняя вызывная панель**», можно задать ее **номер и номер жилого комплекса**.

Тип устройства

Устройство может использоваться как вызывная панель или внешняя вызывная панель. Выберите тип устройства из раскрывающегося списка.

Номер жилого комплекса

Задайте номер жилого комплекса для устройства.

Номер здания

Задайте номер здания для устройства.

Номер подъезда

Задайте номер подъезда для устройства.

Номер этажа

Задайте номер этажа, на котором установлено устройство.

Номер вызывной панели

Задайте номер вызывной панели, на которой установлено устройство.

Примечание

Основная вызывная панель имеет номер 0, а номер дополнительной вызывной панели может быть в диапазоне от 1 до 16.

Номер внешней вызывной панели

Задайте номер внешней вызывной панели, на которой установлено устройство.

Примечание

Номер может быть в диапазоне от 1 до 99.

3. Установите параметры сети видеодомофона.

Пароль регистрации

Задайте пароль регистрации для основной панели, используемый для связи.

IP-адрес основной панели

Введите IP-адрес основной панели, используемый для связи.

IP-адрес частного сервера

Указывает IP-адрес SIP-сервера. Введите IP-адрес основной станции, используемый для связи. В данном случае основная станция используется как SIP-сервер. Другие устройства домофона должны быть зарегистрированы на этом адресе сервера для осуществления связи.

Включить Протокол 1.0

Если функция включена, вызывная панель может регистрироваться на основной станции по старой версии протокола. Если отключена, вызывная панель регистрируется на основной станции по новой версии протокола.

4. После завершения конфигурации нажмите **Готово**, чтобы сохранить настройки.

8.7 Управление персоналом

Нажмите **Добавить**, чтобы добавить информацию о человеке, включая основные данные, учётные данные, настройки аутентификации и параметры.

Добавление основных данных

Нажмите **Управление персоналом → Добавить**, чтобы перейти на страницу добавления человека.

Добавьте основную информацию о человеке: идентификатор сотрудника, имя, пол и тип.

Если выбран тип «Гость», можно установить количество визитов.

Нажмите **Сохранить**, чтобы применить настройки.

Настройка времени действия прав доступа

Нажмите **Управление персоналом → Добавить**, чтобы перейти на страницу добавления человека.

Включите опцию **Долгосрочный пользователь** и установите период времени, в течение которого человек будет иметь права доступа, в соответствии с вашими потребностями.

Установите права доступа к дверям.

Нажмите **Сохранить**, чтобы применить настройки.

Добавление карты

Нажмите **Управление персоналом → Добавить**, чтобы перейти на страницу добавления человека.

Нажмите **Добавить карту**, введите номер карты, выберите **Свойство** и нажмите **ОК**, чтобы добавить карту.

Нажмите **Сохранить**, чтобы применить настройки.

Добавление отпечатка пальца

Примечание

Добавлять отпечаток пальца могут только устройства, поддерживающие эту функцию.

Нажмите **Управление персоналом → Добавить**, чтобы перейти на страницу добавления человека.

Нажмите **Добавить отпечаток пальца** и приложите палец к модулю сканирования отпечатков на устройстве для его добавления.

Нажмите **Сохранить**, чтобы применить настройки.

Добавление PIN-кода

Перед настройкой PIN-кодов необходимо определить, является ли PIN-код персональным кодом, заданным на устройстве, или примененным через платформу. Персональный PIN-код, заданный на устройстве, можно создавать или редактировать на устройстве или через веб-интерфейс, но нельзя задавать на других платформах. Персональный PIN-код, примененный через платформу, можно создавать или редактировать на платформе, и он должен быть выдан на устройство перед использованием; его нельзя задать на устройстве или через веб-интерфейс.

Нажмите **Конфигурация → Безопасность → Режим пароля**, выберите **Режим PIN-кода** как **Персональный PIN-код, заданный на устройстве**.

Нажмите **Управление персоналом → Добавить**, чтобы перейти на страницу добавления человека.

Установите PIN-код.

Нажмите **Сохранить**, чтобы применить настройки.

Настройки аутентификации

Нажмите **Управление персоналом → Добавить**, чтобы перейти на страницу добавления человека.

Установите тип аутентификации.

Нажмите **Сохранить**, чтобы применить настройки.

Удаление человека

На странице управления персоналом отметьте человека, которого необходимо удалить, и нажмите **Удалить**. Нажмите **Очистить все**, чтобы удалить всех людей.

Редактирование человека

На странице управления персоналом отметьте человека, которого необходимо редактировать. Нажмите на значок редактирования , чтобы изменить информацию о человеке.

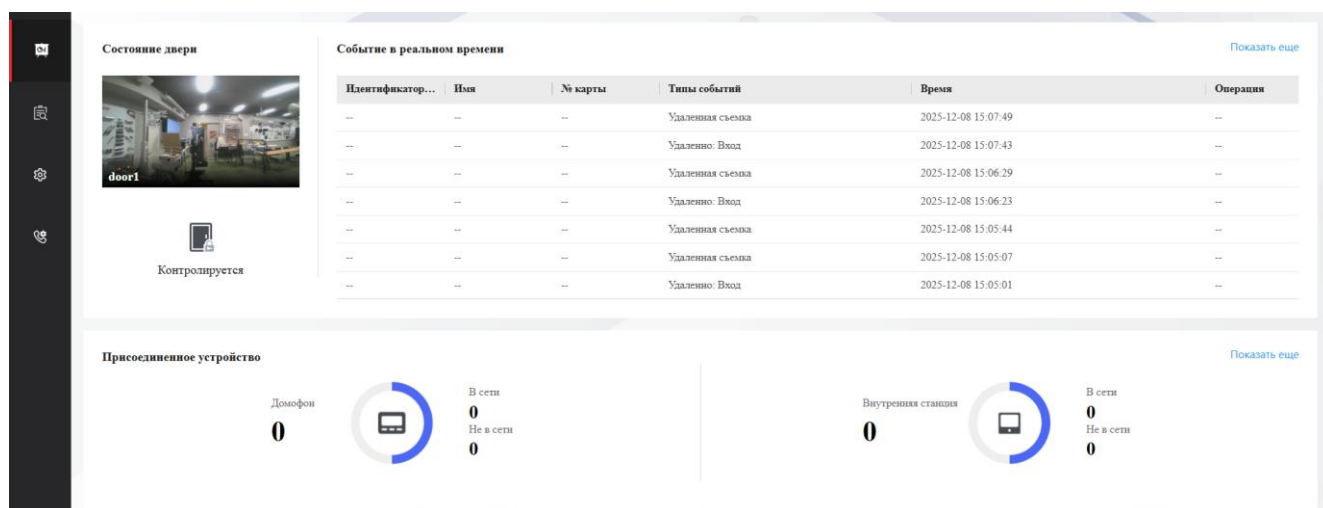
Фильтр

На странице управления персоналом введите **Идентификатор сотрудника / Имя / Номер карты**. Выберите **Статус учётных данных** и нажмите **Фильтр** для отбора людей. Нажмите **Сбросить**, чтобы очистить все условия.

8.8 Управление контролем доступа

8.8.1 Обзор

Вы можете просматривать живое видео с устройства, события в реальном времени, информацию о персонале, сетевой статус, основную информацию и емкость устройства.



Страница "Обзор"

Описание функций:

Статус двери

Нажмите  для просмотра живого видео с устройства.

 - Установите громкость при начале просмотра.

Примечание

При регулировке громкости во время начала двусторонней аудиосвязи возможны повторяющиеся звуки.

 - Вы можете сделать снимок во время просмотра.

 - Выберите тип потока при начале просмотра. Доступны основной и дополнительный потоки.

 - Полноэкранный режим.

Значки статуса двери:



Статус двери: открыта/закрыта/принудительно открыта/принудительно закрыта.

Управляемый статус

Вы можете выбрать статус открыто/закрыто/принудительно открыто/принудительно закрыто в соответствии с вашими потребностями.

События в реальном времени

Вы можете просматривать идентификатор сотрудника, имя, номер карты, тип события, время и действие. Вы также можете нажать **Подробнее**, чтобы задать условия поиска, включая тип события, идентификатор сотрудника, имя, номер карты, время начала и окончания, а затем нажать **Поиск**. Результаты будут отображены на правой панели.

Информация о персонале

Вы можете просмотреть информацию о добавленных и недобавленных лицах, картах и отпечатках пальцев.

Сетевой статус

Вы можете просмотреть статус подключения и регистрации проводной сети, беспроводной сети, Bluetooth, протокола ISUP, VoIP и облачного сервиса.

Основная информация

Вы можете просмотреть модель, серийный номер и версию прошивки.

Емкость устройства

Вы можете просмотреть емкость для хранения данных о персонах, картах, событиях и отпечатках пальцев.

Примечание

Только устройства, поддерживающие функцию работы с отпечатками пальцев, отображают соответствующую емкость.

Подробнее

Вы можете нажать **Подробнее** для просмотра деталей событий.

8.8.2 Поиск событий

Нажмите **Поиск событий**, чтобы перейти на страницу поиска.

Типы событий

Событие контроля доступа

Главный тип

Все типы

Второстепенное событие

Все типы

Идентификатор сотрудника

Имя

№ карты

Время начала

2025-12-08 00:00:00

Время окончания

2025-12-08 23:59:59

☐

Просмотр только видеособытий

Поиск

№	Идентификатор сот...	Имя	№ карты	Типы событий	Время	IP-адрес удаленног...	Операция
1	--	--	--	Удаленно: Блокировка			--
2	--	--	--	Удаленно: Блокировка			--
3	--	--	--	Удаленная съемка			--
4	--	--	--	Удаленная съемка			--
5	--	--	--	Удаленно: Вход			--
6	--	--	--	Удаленная съемка			--
7	--	--	--	Удаленно: Вход			--
8	--	--	--	Удаленная съемка			--
9	--	--	--	Удаленная съемка			--
10	--	--	--	Удаленно: Вход			--

Всего: 10

24 / Страница

< 1 >

1 / 1 Страница

Перей...

Поиск событий

Введите условия поиска, включая **тип события, идентификатор сотрудника, имя, номер карты, время начала и время окончания**, и нажмите **Поиск**.

Результаты будут отображены на правой панели.

8.8.3 Конфигурация параметров двери

Настройте параметры для разблокировки дверей.

Настройка имени двери

Создайте название для двери.

Нажмите **Контроль доступа → Настройка параметров → Параметры двери**, чтобы перейти на страницу настроек. Задайте **Название двери** и нажмите **Сохранить**.

Настройка времени открытия через Веб-интерфейс ПК

Вы можете установить время, в течение которого дверь остается открытой после прикладывания карты.

Нажмите **Контроль доступа → Настройка параметров → Параметры двери**, чтобы перейти на страницу настроек.

Установите **Время открытия** — это продолжительность действия замка после разблокировки. Если дверь не открыта в течение установленного времени, она автоматически заблокируется. Доступный для настройки диапазон: от 1 до 255 секунд.

Нажмите **Сохранить**.

Настройка сигнала превышения времени открытия двери через Веб-интерфейс ПК

Если дверь не закрыта по истечении времени блокировки, точка контроля доступа подаст звуковой сигнал.

Нажмите **Контроль доступа → Настройка параметров → Параметры двери**, чтобы перейти на страницу настроек.

Установите параметр **сигнала превышения времени открытия двери**. Если дверь не закрыта по истечении времени блокировки, точка контроля доступа подаст звуковой сигнал. При значении 0 сигнализация отключена.

Нажмите **Сохранить**.

Настройка типа дверного датчика через Веб-интерфейс ПК

Вы можете выбрать тип дверного контакта в зависимости от способа подключения.

Нажмите **Контроль доступа → Настройка параметров → Параметры двери**, чтобы перейти на страницу настроек.

Выберите тип датчика: **нормально замкнутый** или **нормально разомкнутый**. По умолчанию используется **Нормально замкнутый** (если нет особых требований).

Нажмите **Сохранить**.

Настройка кнопки выхода через Веб-интерфейс ПК

Установите тип кнопки выхода как **нормально разомкнутый** или **нормально замкнутый** в соответствии с фактическим способом подключения.

Нажмите **Контроль доступа → Настройка параметров → Параметры двери**, чтобы перейти на страницу настроек.

Установите **Тип кнопки выхода**. По умолчанию используется **Нормально разомкнутый** (если нет особых требований).

Нажмите **Сохранить**.

Настройка расширенного времени открытия через Веб-интерфейс ПК

Для дверного контакта может быть установлена задержка срабатывания после того, как лицо с расширенным доступом приложит карту.

Нажмите **Контроль доступа → Настройка параметров → Параметры двери**, чтобы перейти на страницу настроек.

Установите **Расширенное время открытия**. Для дверного контакта может быть установлена задержка срабатывания после того, как лицо с расширенным доступом приложит карту.

Нажмите **Сохранить**.

Настройка времени принудительного открытия двери после первого лица через Веб-интерфейс ПК

После авторизации первого лица разрешается доступ нескольких лиц или другие действия аутентификации. Нажмите **Контроль доступа → Настройка параметров → Параметры двери**, чтобы перейти на страницу настроек. Установите **Время принудительного открытия после первого лица** и нажмите **Сохранить**.

Настройка кода принуждения через Веб-интерфейс ПК

После настройки кода принуждения, при его вводе в ситуации угрозы дверь откроется, а система контроля доступа зарегистрирует соответствующее событие.

Нажмите **Контроль доступа → Настройка параметров → Параметры двери**, чтобы перейти на страницу настроек. Установите **Код принуждения** и нажмите **Сохранить**.

Примечание

Код принуждения и суперпароль не должны совпадать; обычно состоят из 4–8 цифр.

Настройка суперпароля через Веб-интерфейс ПК

Администратор или уполномоченное лицо может ввести суперпароль для открытия двери.

Нажмите **Контроль доступа → Настройка параметров → Параметры двери**, чтобы перейти на страницу настроек. Установите **Суперпароль**; уполномоченное лицо может ввести его для открытия двери.

Нажмите **Сохранить**.

Примечание

Код принуждения и суперпароль не должны совпадать; обычно состоят из 4–8 цифр.

Настройка кода снятия тревоги через Веб-интерфейс ПК

Администратор или уполномоченное лицо может ввести код снятия тревоги для её деактивации.

Нажмите **Контроль доступа → Настройка параметров → Параметры двери**.

Задайте **Код снятия тревоги**. При срабатывании сигнализации ввод этого кода позволит её отключить.

Нажмите **Сохранить**.

8.8.4 Настройки аутентификации

Параметры двери

Настройки аутентификации

Настройки карты

Настройки привязки

Параметры терминала

Настройка параметров считывателя карт

Терминал

Основной

Вспомогательный

Тип терминала

Карта

Модель терминала

ВСМ-01

Включить устройство аутенти...

Аутентификация

Карта/PIN-код

Интервал аутентификации

0

s

Тревога макс. числа неуд...

Обнаружение взлома

Инверсия № карты

QR-код

Конфигурация параметров Bluetooth

Включить Bluetooth

* Имя устройства

ACCESS-FX6417084

Открыть дверь по Bluetooth

Чтобы использовать эту функцию, сначала включите Bluetooth на устройстве.

Сохранить

Настройки аутентификации

Выбор основного/дополнительного считывателя карты через веб-интерфейс ПК

Настройка терминала для использования биометрической аутентификации.

Нажмите **Контроль доступа** → **Настройки параметров** → **Настройки аутентификации**, чтобы перейти на страницу настроек.

Выберите тип терминала: основной или дополнительный считыватель.

Установите остальные параметры и нажмите **Сохранить**.

Просмотр типа и модели терминала через Веб-интерфейс ПК

Перейдите в раздел **Контроль доступа** → **Настройки параметров** → **Настройки аутентификации**, чтобы открыть страницу настроек.

Просмотрите поля **Тип терминала** и **Модель терминала**.

Активация устройства аутентификации через Веб-интерфейс ПК

После активации терминал аутентификации можно использовать для считывания карт.


SEC.RU
 ПОРТАЛ ПО БЕЗОПАСНОСТИ

Шаги:

1. Перейдите в раздел **Контроль доступа → Настройки параметров → Настройки аутентификации**, чтобы открыть страницу настроек.
2. **Активируйте устройство аутентификации.** После активации терминал можно будет нормально использовать для считывания карт.
3. Нажмите **Сохранить**.

Настройка аутентификации через Веб-интерфейс ПК

Настройте параметры проверки подлинности.

Перейдите в раздел **Контроль доступа → Настройки параметров → Настройки аутентификации**, чтобы открыть страницу настроек.

При выборе основного считывателя в качестве терминала вы можете выбрать **Аутентификацию** из выпадающего списка. Если аутентификаций больше одной, следует задать **Тайм-аут аутентификации по одному пропуску** и **Начальный тип аутентификации для контроля**.

Тайм-аут аутентификации по одному пропуску

Вы можете настроить продолжительность для каждой проверки.

Примечание:

Тайм-аут аутентификации по паролю по умолчанию составляет 20 с и не ограничивается указанными выше настройками.

Начальный тип аутентификации для контроля

Если эта функция включена, все выбранные типы можно использовать для первичной аутентификации.

При выборе дополнительного считывателя в качестве терминала вы также можете выбрать **Аутентификацию** из выпадающего списка.

Нажмите **Сохранить**.

Настройка интервала аутентификации через Веб-интерфейс ПК

Вы можете задать интервал аутентификации для одного и того же человека. Один и тот же человек сможет пройти аутентификацию только один раз в течение заданного интервала. Повторная попытка аутентификации в этот период будет неудачной. Если в течение заданного интервала аутентификацию проходит другой человек, он сможет сделать это без ограничений.

Перейдите в раздел **Контроль доступа → Настройки параметров → Настройки аутентификации**, чтобы открыть страницу настроек.

Когда выбран **основной считыватель** в качестве терминала, задайте **Интервал аутентификации** и нажмите **Сохранить**.

Активация сигнализации при превышении числа неудачных попыток через Веб-интерфейс ПК

Активируйте функцию для генерации тревоги, когда количество попыток считывания карты достигнет заданного значения.

Перейдите в раздел **Контроль доступа → Настройки параметров → Настройки аутентификации**, чтобы открыть страницу настроек.

Когда выбран **основной или дополнительный считыватель** в качестве терминала, переведите переключатель, чтобы активировать **Сигнализацию макс. числа неудач**, и задайте **Макс. число неудачных попыток аутентификации**. Нажмите **Сохранить**.

Включение/выключение обнаружения вскрытия через Веб-интерфейс ПК

Вы можете включить обнаружение вскрытия. Устройство будет автоматически генерировать события вскрытия, когда считыватель снят или унесен.

Перейдите в раздел **Контроль доступа → Настройки параметров → Настройки аутентификации**, чтобы открыть страницу настроек.

Включите или выключите **Обнаружение вскрытия** в соответствии с вашими потребностями. После включения функции устройство будет автоматически генерировать события вскрытия, когда считыватель снят или унесен. Если функция отключена, тревожные события генерироваться не будут.

Нажмите **Сохранить**.

Включение/выключение реверса номера карты через Веб-интерфейс ПК

Вы можете включить или выключить функцию реверса номера карты.

Перейдите в раздел **Контроль доступа → Настройки параметров → Настройки аутентификации**, чтобы открыть страницу настроек.

Включите **Реверс номера карты**, и считанный номер карты будет записан в обратной последовательности. Нажмите **Сохранить**.

Включение/выключение распознавания QR-кода через Веб-клиент

Вы можете включить/выключить функцию распознавания QR-кода.

Перейдите в раздел **Контроль доступа → Настройки параметров → Настройки аутентификации**, чтобы открыть страницу настроек.

Если устройство поддерживает распознавание QR-кода, вы можете активировать эту функцию, и устройство сможет считывать QR-код, сконвертированный из номера карты.

Нажмите **Сохранить**.

Настройка интервала связи с контроллером через Веб-интерфейс ПК

Вы можете задать интервал связи дополнительного считывателя с контроллером. Если считыватель не сможет соединиться с контроллером доступа в течение заданного времени, он будет считаться не в сети.

Перейдите в раздел **Контроль доступа → Настройки параметров → Настройки аутентификации**, чтобы открыть страницу настроек.

Когда выбран **дополнительный считыватель** в качестве терминала, задайте **Интервал связи с контроллером** и нажмите **Сохранить**.

Настройка тайм-аута ввода пароля через Веб-клиент

Задайте максимально допустимый интервал между вводом двух символов пароля. После ввода одного символа, если следующий символ не будет введен в течение заданного интервала, все введенные символы будут автоматически очищены.

Перейдите в раздел **Контроль доступа** → **Настройки параметров** → **Настройки аутентификации**, чтобы открыть страницу настроек.

Когда выбран **дополнительный считыватель** в качестве терминала, вы можете задать **Макс. интервал при вводе пароля** и нажать **Сохранить**.

Настройка полярности светодиодов OK и ERROR через Веб-интерфейс ПК

Выберите полярность светодиодов для интерфейсов OK и ERROR в соответствии с фактическим подключением. По умолчанию установлена положительная полярность.

Перейдите в раздел **Контроль доступа** → **Настройки параметров** → **Настройки аутентификации**, чтобы открыть страницу настроек.

Когда выбран **дополнительный считыватель** в качестве терминала, задайте **Полярность светодиода OK** и **Полярность светодиода ERROR** и нажмите **Сохранить**.

Включение/выключение Bluetooth через Веб-интерфейс ПК

Вы можете включить Bluetooth устройства для подключения Bluetooth-гарнитуры.

Шаги:

1. Перейдите в раздел **Контроль доступа** → **Настройки параметров** → **Настройки аутентификации**, чтобы открыть страницу настроек.
2. В разделе настройки параметров Bluetooth активируйте опцию **Включить Bluetooth**.
3. Введите имя внешней гарнитуры в поле **Имя устройства**. После подключения Bluetooth нажмите **Сохранить**.
4. Активируйте опцию **Открытие двери по Bluetooth** для возможности дистанционного управления дверью.

Примечание

Перед началом настройки необходимо добавить устройство в мобильное приложение.

8.8.5 Настройки карт

Параметры двери
Настройки аутентификации
Настройки карты
Настройки привязки

Тип карты

Включить карту NFC

Активировать карту M1

Шифрование карты M1

Сектор

Активировать карту EM

Активировать карту CPU

Активировать карту DESFire

Контент карты DESFire

Активировать карту FeliCa

Настройки аутентификации карты

Режим аутентификации карты

Полный номер карты

3 байта

4 байта

Сохранить

Настройки карт

Включение/выключение защиты NFC через Веб-интерфейс ПК

После включения функция позволяет устройству считывать NFC-карты.

Перейдите в раздел **Контроль доступа** → **Настройки параметров** → **Настройки карт**, чтобы открыть страницу настроек.

Активируйте опцию **Карта NFC** и нажмите **Сохранить**.

После включения устройства оно сможет считывать NFC-карты. Если данные устройств контроля доступа будут получены мобильными устройствами, может возникнуть ситуация неуполномоченного доступа. Чтобы предотвратить это, вы можете отключить функцию NFC.

Включение/выключение карт M1 через Веб-клиент

После включения устройство может распознавать карты M1, и пользователи могут использовать их для прохода.

Перейдите в раздел **Контроль доступа** → **Настройки параметров** → **Настройки карт**, чтобы открыть страницу настроек.

Активируйте опцию **Карта M1**.

Шифрование карт M1

Включение шифрования карт M1 повышает уровень безопасности карт доступа, что затрудняет их копирование.

Сектор

После включения шифрования карт M1 необходимо задать шифруемый сектор.

Примечание

Рекомендуется шифровать сектор 13.

Нажмите **Сохранить**.

Включение/выключение карт EM через Веб-клиент

После включения устройство может распознавать карты EM, и пользователи могут использовать их для прохода.

Перейдите в раздел **Контроль доступа** → **Настройки параметров** → **Настройки карт**, чтобы открыть страницу настроек.

Активируйте опцию **Карта EM** и нажмите **Сохранить**.

Примечание

Если подключен внешний считыватель, поддерживающий карты EM, то после активации функции можно использовать такие карты и в этом считывателе.

Включение/выключение CPU-карт через Веб-клиент

После включения устройство может распознавать CPU-карты, и пользователи могут использовать их для прохода.

Перейдите в раздел **Контроль доступа** → **Настройки параметров** → **Настройки карт**, чтобы открыть страницу настроек.

Активируйте опцию **CPU-карта**.

Активируйте опцию **Чтение содержимого CPU-карты**, чтобы устройство могло считывать данные с CPU-карт. Нажмите **Сохранить**.

Включение/выключение карт DESFire через Веб-клиент

После включения устройство может распознавать карты DESFire.

Перейдите в раздел **Контроль доступа** → **Настройки параметров** → **Настройки карт**, чтобы открыть страницу настроек.

Активируйте опцию **Карта DESFire**.

Активируйте опцию **Чтение содержимого DESFire** и нажмите **Сохранить**. После включения устройство сможет считывать карты DESFire.

После включения функция позволяет устройству считывать карты FeliCa.

Перейдите: **Контроль доступа** → **Параметры** → **Настройки карт**.

Включите опцию **«Активировать карты FeliCa»**.

Нажмите **«Сохранить»**.

Настройка режима карточной аутентификации через веб-браузер

Здесь можно задать, какую часть номера карты устройство считывает для аутентификации.

Перейдите: **Параметры** → **Настройки карт**.

Выберите нужный **режим карточной аутентификации**.

Нажмите **«Сохранить»**.

Полный номер карты: Считывается весь номер карты.

3 байта: Устройство считывает только 3 байта.

4 байта: Устройство считывает только 4 байта.

8.8.6 Настройка реакций (Linkage Settings)

Когда срабатывает заданное событие, его информация передается на центральную платформу указанным способом.

Шаги:

1. Перейдите: **Контроль доступа → Параметры → Настройка реакций**.

Настройка реакций

2. Нажмите **«+»**.

3. Настройте источник события. Выберите тип реакции: «Реакция на событие», «Реакция по карте» или «Привязка ID сотрудника».

- Если выбран тип «Реакция на событие»: вы можете выбрать типы событий в соответствии с вашими потребностями.
- Если выбран тип «Реакция по карте»: введите номер карты и выберите считыватель.
- Если выбран тип «Привязка ID сотрудника»: введите ID сотрудника и выберите считыватель.

4. Настройте действие реакции.

- 1) Активируйте «Реакция двери»: отметьте галочкой и выберите действие для двери.
- 2) Активируйте «Реакция тревожного выхода»: отметьте галочкой и выберите действие для тревожного выхода.
- 3) Активируйте «Связной захват».
- 4) Активируйте «Связная запись»: нажмите «Общие настройки реакций», чтобы задать время предзаписи и задержку записи, а также включить запись аудио вместе с видео. Нажмите «Сохранить».

Примечание

Для использования функции записи необходимо установить SD-карту. После записи вы можете нажать «Поиск событий» для просмотра записей. Подробнее см. раздел «Поиск событий».

5. Нажмите «Сохранить», чтобы применить настройки.

8.8.7 Настройка рабочего режима через веб-интерфейс ПК

Здесь вы можете настроить терминальные параметры устройства.

Примечание

Данная функция поддерживается только некоторыми моделями. Ориентируйтесь на конкретное устройство.

Перейдите: **Контроль доступа → Параметры → Параметры терминала.**

Рабочий режим

Вы можете выбрать рабочий режим: **Режим контроля доступа** или **Свободный режим**.

Режим контроля доступа

Это основной режим работы устройства. Для получения доступа необходимо пройти аутентификацию (предъявить карту, код и т.д.).

8.8.8 Настройка удаленной верификации

После включения этой функции устройство будет передавать данные для аутентификации человека на платформу, которая будет принимать решение об открытии двери.

1. Перейдите: **Контроль доступа → Параметры → Параметры терминала.**
2. Настройте необходимые параметры.
3. Нажмите «**Сохранить**».

Удаленная верификация

После активации этой функции, при попытке аутентификации устройство будет отправлять информацию на платформу, а платформа будет подтверждать, открывать ли дверь.

8.8.9 Настройки конфиденциальности

Параметры двери
Настройки аутентификации
Настройки карты
Настройки привязки
Параметры терминала
Настройки конфиденциально...

Настройки хранилища событий

Тип хранилища событий
☐ Периодически удалять старые события
☐ Удалять старые события к указанному времени
☒ Перезаписать

Загрузка и сохранение изображения

Сохранение изображений пос...
☐
Если этот параметр включен, полученные изображения будут автоматически сохранены на устройстве.

Удалить все изображения на устройстве

Удалить снятые изображения

Режим PIN-кода

Режим PIN-кода
☒ Персон. PIN-код на платформе ⓘ
☐ Персон. PIN-код на устройстве ⓘ

Меню настроек конфиденциальности

Настройка типа хранения событий через веб-браузер ПК

Здесь вы можете настроить способ хранения событий в системе.

Шаги:

1. Перейдите: **Контроль доступа → Параметры → Настройки конфиденциальности.**

Тип хранения событий:

Вы можете выбрать один из следующих вариантов:

- **Удаление старых событий периодически**
Перетащите ползунок или введите число, чтобы задать интервал (в днях) для автоматического удаления всех событий.
- **Удаление старых событий по заданному времени**
Установите конкретную дату и время, когда все события будут удалены.
- **Перезапись**
Самые ранние 5% событий будут удаляться, когда система обнаружит, что занятый объем памяти превысил 95% от полного.

Нажмите «**Сохранить**».

Настройка параметров загрузки и хранения изображений

Настройте параметры загрузки и сохранения изображений.

Перейдите: **Контроль доступа → Параметры → Настройки конфиденциальности.**

Активируйте функцию.

Сохранять снимки после привязанного захвата: Если включить эту функцию, захваченные изображения будут автоматически сохраняться на устройстве.

Нажмите «**Сохранить**».

Удаление всех изображений с устройства через веб-интерфейс ПК

Вы можете удалить все сохраненные на устройстве изображения.

Перейдите: **Контроль доступа → Параметры → Настройки конфиденциальности.**

Нажмите **«Очистить»**. Все захваченные изображения будут удалены.

Настройка режима ПИН-кода через веб-интерфейс ПК

Перед настройкой убедитесь, что ПИН-код применяется через платформу или задается непосредственно на устройстве. Если ПИН-код задается на **устройстве**, его можно редактировать на самом устройстве или через веб-интерфейс, но не на платформе. Если ПИН-код применяется через **платформу**, его необходимо задавать на платформе, а не на устройстве или в веб-интерфейсе.

Перейдите: **Контроль доступа → Параметры → Настройки конфиденциальности**.

В модуле **«Режим ПИН-кода»** настройте следующие параметры и нажмите **«Сохранить»**:

- **ПИН-код, применяемый через платформу**
ПИН-код создается на платформе и затем применяется к устройству. Создать или отредактировать такой ПИН-код на устройстве или в веб-интерфейсе невозможно.
- **ПИН-код, задаваемый на устройстве**
ПИН-код можно создавать или редактировать непосредственно на устройстве или через веб-интерфейс. Задать такой ПИН-код на платформе невозможно.

Нажмите **«Сохранить»**.

8.9 Настройки видеодомофона

8.9.1 Управление устройствами

На этой странице вы можете просмотреть номер устройства, тип, IP-адрес, серийный номер, модель, версию, номер этажа, номер комнаты, номер, статус постановки на охрану, имя пользователя, статус сети и доступные действия. На странице управления устройствами также можно добавить внутреннюю панель и дополнительную вызывную панель, а также управлять устройствами, обновлять или удалять их.

Шаги:

1. Нажмите **Управление устройствами**.
2. Нажмите **Добавить**.
3. Выберите **Тип устройства**, введите **Пароль устройства**, **Пароль регистрации**, **Серийный номер**, **IP-адрес**, **Маска подсети IPv4**, **Шлюз по умолчанию IPv4**, **Порт**, **Номер этажа** и **Номер** (для внутренней панели не требуется вводить Номер этажа и Номер, но требуется **Номер комнаты**).
4. Нажмите **Сохранить**.
5. *Опционально:* Вы также можете выполнить следующие действия:

Удалить устройство

Отметьте устройства, которые необходимо удалить, и нажмите **«Удалить»**.

Импортировать устройства

Нажмите **«Импорт»**, скачайте шаблон. После заполнения информации нажмите  для импорта устройств.

Экспортировать устройства

Нажмите **«Экспорт»**, чтобы выгрузить файлы с информацией об устройствах на локальный ПК.

8.9.2 Настройка номера устройства через веб-интерфейс

Устройство может использоваться как дверная панель или внешняя дверная панель. Перед использованием необходимо задать номер устройства.

1. Перейдите: **Контроль доступа** → **Настройки вызова** → **Номер устройства**.

Номер устройства
Сеть видеодомофона
Параметры времени
Нажмите кнопку для вызова

Тип устройства Домофон

* Этаж 1

* Номер домофона 0

^ Больше

* Период № 1

* № дома 1

* № блока 1

Сохранить

Настройка номера устройства

2. Если в качестве **Типа устройства** установлена **Вызывная панель**, вы можете задать **Номер этажа**, **Номер вызывной панели**, **Номер жилого комплекса**, **Номер здания** и **Номер подъезда**.

Тип устройства

Устройство может использоваться в качестве вызывной панели или внешней вызывной панели. Выберите тип устройства из выпадающего списка.

Примечание

При изменении типа устройства необходимо перезагрузить устройство.

Номер этажа

Укажите номер этажа, на котором установлено устройство.

Номер вызывной панели

Задайте номер вызывной панели.

Примечание

- При изменении номера необходимо перезагрузить устройство.
- Главной вызывной панели присваивается номер 0, а дополнительным вызывным панелям — номера в диапазоне от 1 до 16.

Номер жилого комплекса

Укажите номер жилого комплекса, в котором установлено устройство.

Номер здания

Укажите номер здания.

Номер подъезда

Укажите номер подъезда.

Примечание

При изменении номера необходимо перезагрузить устройство.

Нажмите **«Сохранить»** после завершения настройки.

Если задан тип устройства **«Внешняя вызывная панель»**, вы можете задать номер внешней дверной панели и номер жилого комплекса.

Номер внешней вызывной панели

Если выбран тип устройства «Внешняя дверная панель», укажите число в диапазоне от 1 до 99.

Примечание

При изменении номера необходимо перезагрузить устройство.

Номер жилого комплекса

Укажите номер жилого комплекса, в котором установлено устройство.

8.9.3 Настройка сетевых параметров видеодомофона через веб-браузер

Вы можете установить пароль регистрации, IP-адрес главной панели и IP-адрес частного сервера, а также при необходимости включить поддержку протокола версии 1.0.

Перейдите: **Настройки вызова → Сеть видеодомофона**.

Пароль регистрации

Задайте пароль регистрации главной станции для обеспечения связи.

IP-адрес главной станции

Введите IP-адрес главной станции, используемый для связи.

IP-адрес частного сервера

Относится к IP-адресу SIP-сервера. Введите IP-адрес главной станции, используемый для связи. В этом случае главная станция используется как SIP-сервер. Другие переговорные устройства должны регистрироваться на этом сервере для осуществления связи.

Включить протокол 1.0

Если функция включена, дверная панель может регистрироваться на главной станции по старой версии протокола. Если отключена — используется новая версия протокола.

* Пароль регистрации

* IP главной станции

* IP-адрес частного сервера

Активировать протокол 1.0 ☐

Сохранить

Сеть видеодомофона

После настройки будет обеспечена связь между устройствами контроля доступа, видеодомофоном, дверной панелью, внутренней панелью, главной станцией, платформами и т.д.

Нажмите **«Сохранить»**.

8.9.4 Настройки вызова

Настройте максимальное время связи.

Перейдите: **Контроль доступа → Настройки вызова → Настройки вызова.**

Макс. время связи s

Сохранить

Настройки вызова

Макс. время связи

Максимальное время связи между главной панелью и другими устройствами во время разговора.

При превышении заданного времени связь прерывается. Допустимый диапазон времени связи: от 90 с до 120 с.

8.9.5 Настройка вызова по нажатию кнопки через веб-интерфейс ПК

Настройте устройство, вызываемое при нажатии кнопки.

Шаги:

1. Перейдите: **Контроль доступа → Настройки вызова → Вызов по нажатию кнопки.**

№ Настройки кнопок

01 ☐ Вызов центра видеонаблюдения ☒ Вызов внутренней станции ☐ Вызов указанной внутренней стан... ☐ app

Сохранить

Вызов по нажатию кнопки

2. Настройте назначение кнопки: **Вызов центра управления, Вызов внутренней панели, Вызов указанной внутренней панели или вызов в приложение.**

Примечание

- При выборе "Вызов указанной вызывной панели" необходимо задать номер связанной комнаты.
- При выборе "приложение" доступен вызов НС или НСС.

4. Нажмите **«Сохранить»**.

8.9.6 Настройка номеров через веб-интерфейс ПК

Назначьте SIP-номера комнатам. Комнаты могут связываться друг с другом через SIP-номера.

Шаги:

1. Перейдите: **Контроль доступа → Настройки вызова → Настройки номеров.**

Номер устройства Сеть видеодомфона Параметры времени Нажать кнопку для вызова **Настройки номеров**

+ Добавить - Удалить

№	№ комнаты	Номер SIP	Операция

Настройки номеров

2. Нажмите **«Добавить»** и введите **номер комнаты** и **SIP1-номер**.

3. **Опционально:** Нажмите **«Добавить»**, чтобы добавить SIP-номер, или нажмите  , чтобы удалить номер.

4. Нажмите **«Сохранить»**.

5. **Опционально:** Вы можете нажать **«Удалить»**, чтобы удалить номер комнаты и связанный с ним SIP-номер.

8.10 Конфигурация системы

8.10.1 Настройка локальных параметров

Настройте параметры живого просмотра, путь сохранения файлов записи и путь сохранения захваченных изображений.

Настройка параметров живого просмотра:

Перейдите: **Система и обслуживание** → **Локальные настройки**.

Настройте тип потока, производительность воспроизведения, автоматический запуск живого просмотра и формат изображения.

Нажмите **«Сохранить»**.

Настройка пути сохранения файлов записи:

Перейдите: **Конфигурация** → **Локальные настройки**.

Выберите размер файла записи и укажите путь для сохранения на вашем локальном компьютере.

Нажмите **«Сохранить»**.

Вы также можете нажать **«Открыть»**, чтобы открыть папку и просмотреть файлы.

Настройка пути сохранения захваченных изображений:

Перейдите: **Конфигурация** → **Локальные настройки**.

Выберите путь для сохранения на вашем локальном компьютере.

Нажмите **«Сохранить»**.

Вы также можете нажать **«Открыть»**, чтобы открыть папку и просмотреть изображения.

8.10.2 Просмотр информации об устройстве через веб-интерфейс ПК

Просмотр имени устройства, номера устройства, языка, модели, серийного номера, версии, количества каналов, дискретных входов/выходов, состояния замка, тревожных входов/выходов и емкости устройства.

Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Система** → **Системные настройки** → **Основная информация**.

На этой странице вы можете просмотреть имя устройства, номер устройства, язык, модель, серийный номер, версию, количество каналов, дискретные входы, дискретные выходы, замок, тревожные входы, тревожные выходы и емкость устройства и т.д.

Нажав **«Обновить»** в разделе «Версия прошивки», вы перейдете на страницу обновления для обновления устройства.

8.10.3 Настройка времени

Настройте часовой пояс устройства, режим синхронизации, адрес сервера, порт NTP и интервал.

Перейдите: **Система и обслуживание → Конфигурация системы → Система → Системные настройки → Настройки времени.**

Настройки времени

После завершения конфигурации нажмите **«Сохранить»**, чтобы применить настройки.

Часовой пояс

Выберите часовой пояс, в котором находится устройство, из выпадающего списка.

Синхронизация времени

NTP

Необходимо ввести IP-адрес NTP-сервера, номер порта и интервал синхронизации.

Вручную

По умолчанию время на устройстве задается вручную. Вы можете установить время устройства самостоятельно или установить флажок **«Синхронизировать с временем компьютера»**.

Тип адреса сервера / Адрес сервера / Порт NTP / Интервал

Здесь можно задать тип адреса сервера, адрес сервера, порт NTP и интервал синхронизации.

8.10.4 Настройка летнего времени (DST)

Шаги:

1. Перейдите: **Система и обслуживание → Конфигурация системы → Система → Системные настройки → Настройки времени.**
2. Включите опцию **«Летнее время (DST)»**.
3. Установите **время начала** и **окончания** летнего времени, а также **величину корректировки**.
4. Нажмите **«Сохранить»**, чтобы применить настройки.

8.10.5 Смена пароля администратора

Шаги:

1. Перейдите: **Система и обслуживание → Конфигурация системы → Система → Управление пользователями → Управление пользователями.**
2. Нажмите .
3. Введите старый пароль и создайте новый пароль.
4. Подтвердите новый пароль.
5. Нажмите **«Сохранить»**.

Внимание!

- Устройство автоматически проверяет надежность пароля. Настоятельно рекомендуется задать собственный надежный пароль (длиной не менее 8 символов, включая как минимум три категории из следующих: заглавные буквы, строчные буквы, цифры и специальные символы) для повышения безопасности вашего продукта.
- Рекомендуется регулярно менять пароль, особенно в системах с повышенными требованиями к безопасности. Ежемесячная или еженедельная смена пароля лучше защитит ваше устройство.
- Ответственность за правильную настройку всех паролей и других параметров безопасности лежит на установщике и/или конечном пользователе.

8.10.6 Настройки безопасности учетной записи через веб-интерфейс ПК

Вы можете изменить контрольные вопросы и ответы или адрес электронной почты, привязанный к устройству. После изменения этих настроек, если вы забудете пароль устройства, для его сброса нужно будет ответить на новые контрольные вопросы или использовать новый адрес электронной почты.

Шаги:

1. Перейдите: **Система и обслуживание → Конфигурация системы → Система → Управление пользователями → Управление пользователями → Настройки безопасности учетной записи.**
2. Измените контрольные вопросы или адрес электронной почты в соответствии с вашими потребностями.
3. Введите пароль устройства и нажмите **«ОК»** для подтверждения изменений.

8.10.7 Онлайн-пользователи

На этой странице отображается информация о пользователях, вошедших в систему устройства.

Шаги:

1. Перейдите: **Система и обслуживание → Конфигурация системы → Система → Управление пользователями → Онлайн-пользователи.**
2. Здесь вы можете просмотреть список пользователей, находящихся в сети.

8.10.8 Просмотр статуса постановки/снятия с охраны устройства через веб-интерфейс ПК

Просматривайте тип постановки на охрану и IP-адрес, с которого было выполнено управление охраной.

Перейдите: **Система и обслуживание → Конфигурация системы → Система → Управление пользователями → Журнал постановки/снятия с охраны.**

На этой странице вы можете просмотреть информацию о операциях постановки и снятия с охраны. Для обновления списка нажмите **«Обновить»**.

8.10.9 Сетевые настройки

Настройка основных сетевых параметров

Перейдите: Система и обслуживание → Конфигурация системы → Сеть → Сетевые настройки → TCP/IP.

Страница настройки TCP/IP

Установите необходимые параметры и нажмите «Сохранить».

Тип сетевого интерфейса

Выберите тип сетевого интерфейса (NIC) из выпадающего списка. По умолчанию используется значение «Авто».

DHCP

Если флажок **DHCP** снят, необходимо вручную задать следующие параметры:

IPv4-адрес, Маску подсети IPv4, Основной шлюз IPv4, Режим IPv6, IPv6-адрес, Длину префикса IPv6-подсети, Основной шлюз IPv6, MAC-адрес, Значение MTU.

Если флажок **DHCP** установлен, система автоматически назначит:

IPv4-адрес, Маску подсети IPv4, Основной шлюз IPv4, Режим IPv6, IPv6-адрес, Длину префикса IPv6-подсети, Основной шлюз IPv6.

DNS-сервер

Задайте предпочитаемый и альтернативный DNS-серверы в соответствии с вашими потребностями.

Настройка параметров Wi-Fi

Настройте параметры беспроводного подключения устройства.

Шаги:

Примечание

Функция должна поддерживаться вашим устройством.

1. Перейдите: Система и обслуживание → Конфигурация системы → Сеть → Сетевые настройки → Wi-Fi.

TCP/IP **Wi-Fi** Точка доступа устройства

Wi-Fi ☒

Список сетей Wi-Fi + Ручное добавление Обновить

№	SSID	Рабочий режим	Режим безопасности	Сила сигнала	Состояние подключения	Операция
Нет данных.						

WLAN

DHCP ☒

Адрес IPv4

Маска подсети IPv4 для устройс...

Шлюз по умолчанию IPv4 для...

Режим IPv6 ☐ Ручное ☒ DHCP

Адрес IPv6

Длина префикса подсети IPv6

Шлюз IPv6 по умолчанию

DNS-сервер

DHCP ☒

Предпочтительный DNS-сервер

Альтернативный DNS сервер

Сохранить

Страница настройки Wi-Fi

2. Активируйте опцию **Wi-Fi**.

3. Выберите сеть Wi-Fi:

- Нажмите на  рядом с нужной сетью в списке, введите пароль.
- Или нажмите **«Добавить»**, введите имя сети, пароль и тип шифрования, затем нажмите **«Подключить»**. После успешного подключения нажмите **«ОК»**.

4. **Опционально:** Настройте параметры WLAN.

1) Задайте IP-адрес, маску подсети и шлюз по умолчанию вручную. Или активируйте **DHCP**, и система автоматически назначит IP-адрес, маску подсети и шлюз по умолчанию.

5. Нажмите **«Сохранить»**.

Точка доступа устройства

Настройте точку доступа (хот-спот) на устройстве.

Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Сеть** → **Сетевые настройки** → **Точка доступа устройства**.

Нажмите **«Включить точку доступа устройства»**, чтобы активировать функцию, и просмотрите имя точки доступа.

Примечание

По умолчанию имя точки доступа имеет формат **AP_СерийныйНомерУстройства**.

Нажмите **«Сохранить»**.

Настройка портов через веб-интерфейс ПК

Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Сеть** → **Сетевые службы**.

HTTP

Порт, через который браузер получает доступ к устройству. Например, если HTTP-порт изменен на 81, для входа в браузере нужно ввести `http://192.0.0.65:81`.

HTTPS

Настройте HTTPS-порт для безопасного доступа через браузер. При использовании HTTPS требуется сертификат.

HTTP-уведомления

Устройство может отправлять тревожные сообщения на указанный IP-адрес или доменное имя через протокол HTTP/HTTPS. Настройте IP-адрес или доменное имя для уведомлений, URL-адрес, порт и протокол.

Примечание

Указанный IP-адрес или доменное имя должны поддерживать протокол HTTP/HTTPS для приема тревожных сообщений.

Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Сеть** → **Сетевые службы** → **RTSP**.

RTSP

Порт протокола RTSP (Real Time Streaming Protocol), используемый для передачи видео в реальном времени.

Настройка параметров ISUP через веб-интерфейс ПК

Настройте параметры протокола ISUP для доступа к устройству.

Шаги:

Примечание: Функция должна поддерживаться устройством.

1. Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Сеть** → **Доступ к устройству** → **ISUP**.
2. Активируйте опцию «**Включить**».
3. Задайте параметры: **Версия ISUP**, **Адрес сервера**, **ID устройства** и **Статус ISUP**.

Примечание: При выборе версии **5.0** необходимо также задать **Ключ шифрования**.

4. Настройте параметры прослушивания ISUP, включая **IP-адрес/доменное имя центра сигнализации ISUP**, **URL центра сигнализации ISUP** и **Порт центра сигнализации ISUP**.
5. Нажмите «**Сохранить**».

Доступ к платформе через веб-интерфейс ПК

Функция доступа к платформе предоставляет возможность управления устройствами через платформу.

Шаги:

1. Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Сеть** → **Доступ к устройству**

Примечание: *LTV-CMS Mobile2* — это приложение для мобильных устройств. С помощью приложения вы можете просматривать live-изображение с устройства, получать уведомления о тревогах и т.д.

2. Активируйте опцию «**Включить**» для включения функции.
3. **Опционально:** Активируйте опцию «**Пользовательский**», чтобы вручную задать адрес сервера.
4. Введите Код проверки (верификации).
5. Нажмите «**Просмотреть**», чтобы отобразился QR-код устройства. Отсканируйте его для привязки учетной записи.

Примечание: Код проверки должен содержать от 8 до 32 символов (буквы a-z, A-Z и/или цифры 0-9). Регистр символов учитывается. Рекомендуется использовать комбинацию не менее чем из 8 букв и/или цифр.

6. Нажмите «**Сохранить**» для применения настроек

Настройки Bluetooth

Вы можете активировать функцию Bluetooth.

Перейдите: **Конфигурация → Сеть → Сетевые настройки → Bluetooth.**

Включить: Активируйте эту опцию, чтобы включить функцию Bluetooth.

Имя устройства: Вы можете изменить имя устройства, отображаемое при подключении по Bluetooth.

Статус подключения: Здесь отображается текущий статус подключения.

Открытие двери по Bluetooth

После включения этой функции вы можете открывать двери через приложения *HikCentral Connect* или *HikCentral Access Control*.

Примечание

Перед использованием этой функции необходимо добавить устройства в НСС или НСАС. Через НСАС также можно реализовать функцию автоматического открытия двери. Подробнее см. в руководстве пользователя НСАС.

Настройки учетной записи VoIP

Вы можете осуществлять голосовые вызовы по сети.

Шаги:

1. Перейдите: **Система и обслуживание → Конфигурация системы → Сеть → Доступ к устройству → VoIP.**
2. Включите **VoIP-шлюз**.
3. Задайте следующие параметры:
 - **Имя пользователя для регистрации**
 - **Пароль для регистрации**
 - **IP-адрес сервера**
 - **Порт сервера**
 - **Время истечения**
 - **Статус регистрации**
 - **Номер**
 - **Отображаемое имя пользователя**

ISUP

Guarding Vision

VoIP

Включить VoIP-шлюз

Регистрация имени пользоват...

Пароль регистрации

IP-адрес сервера

Порт сервера 5060

Срок действия 60 Минута

Статус регистрации Не зарегистрирован Обновить

Количество

Показать имя пользователя

Сохранить

Настройки учетной записи VoIP

Пароль регистрации

Введите пароль регистрации для связи через SIP-сервер. Этот пароль обычно настраивается в параметрах SIP главной станции.

IP-адрес сервера

Введите IP-адрес главной станции, используемый для VoIP-связи. В этом случае главная станция используется как SIP-сервер. Другие переговорные устройства должны быть зарегистрированы на этом сервере для осуществления связи.

Номер / Отображаемое имя пользователя

Номер вызова и имя пользователя, отображаемые на устройстве.

4. Нажмите «**Сохранить**».

8.10.10 Настройка видео и аудио параметров через веб-интерфейс ПК

Настройка видео параметров через веб-браузер

Вы можете настроить качество, разрешение и другие параметры камеры устройства.

Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Видео/Аудио** → **Видео**.

Задайте следующие параметры: Имя камеры, Тип потока, Тип видео, Разрешение, Тип битрейта, Качество видео, Частота кадров, Макс. битрейт, Видеокодек, Интервал I-кадра.

Нажмите «**Сохранить**».

Настройка аудио параметров через веб-интерфейс ПК

Вы можете настроить громкость устройства.

Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Видео/Аудио** → **Аудио**.

Тип потока: **Основной поток** | Дополнительный п...

Шифрование аудио: G.711ulaw

Входная громкость: 7

Выходная громкость: 7

Включить голосовые подсказки: ☒

Эквализация звука: ☐

Сохранить

Аудио

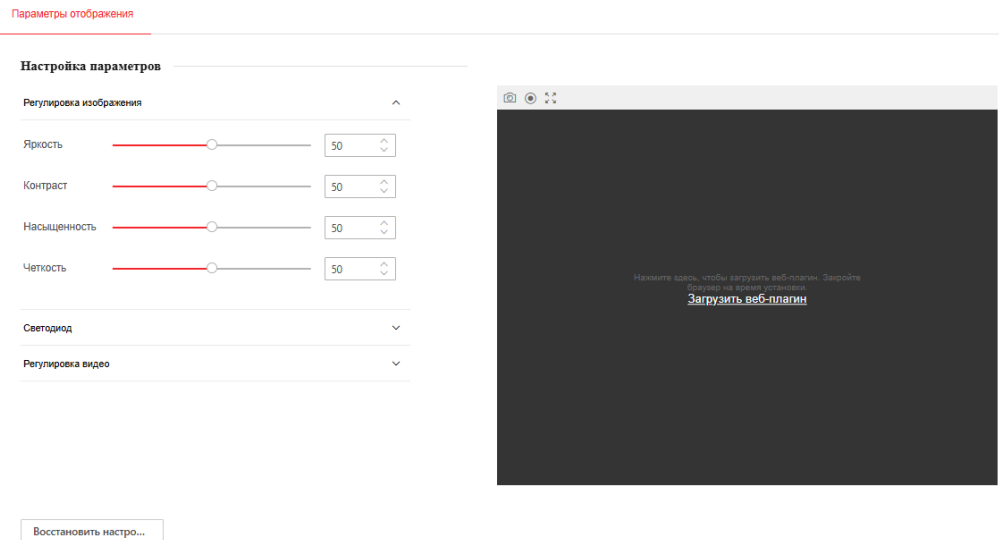
Установите **тип потока** и **аудиокодек** в соответствии с вашими потребностями. С помощью ползунков установите уровень **входной** и **выходной** громкости.

Активируйте ползунок «**Голосовые подсказки**», чтобы включить их.

Вы можете включить «**Эквалайзер**» — устройство будет автоматически корректировать частоту с помощью аудиоалгоритма для улучшения качества звука и выравнивания аудиоэффекта.

Нажмите «**Сохранить**».

8.10.11 Настройки параметров изображения



Настройки отображения

Настройка яркости/контрастности/насыщенности/резкости через веб-интерфейс ПК

Вы можете настроить параметры изображения, такие как яркость, контрастность, насыщенность и резкость на странице живого просмотра.

Перейдите: Система и обслуживание → Конфигурация системы → Изображение → Настройки отображения.

Коррекция изображения:

Перетащите ползунки или введите числовые значения, чтобы задать **яркость, контрастность, насыщенность и резкость**.

Нажмите **«Восстановить настройки по умолчанию»**, чтобы сбросить параметры к заводским предустановкам.

Настройка подсветки через веб-интерфейс ПК

Вы можете настроить яркость дополнительной подсветки.

Шаги:

1. Перейдите: Система и обслуживание → Конфигурация системы → Изображение → Настройки отображения.
2. Установите **тип, режим и яркость** дополнительной подсветки.
3. *Опционально:* Нажмите **«Восстановить настройки по умолчанию»**.

Настройка стандарта видео через веб-интерфейс ПК

Вы можете задать видеостандарт для страницы живого просмотра.

Перейдите: Система и обслуживание → Конфигурация системы → Изображение → Настройки отображения.

Коррекция видео:

Установите частоту кадров для удаленного просмотра. После изменения настроек устройство необходимо **перезагрузить**.

- **PAL**
25 кадров в секунду. Стандарт для материкового Китая, Гонконга (Китай), стран Ближнего Востока, Европы и т.д.
- **NTSC**
30 кадров в секунду. Стандарт для США, Канады, Японии, Тайваня (Китай), Кореи, Филиппин и т.д.

Нажмите **«Восстановить настройки по умолчанию»**, чтобы сбросить параметры.

8.10.12 Настройка детектора движения через веб-интерфейс ПК

После настройки детектора движения устройство будет сообщать на платформу о срабатывании правила при обнаружении движущихся объектов.

Перейдите: **Система и обслуживание** → **Конфигурация системы** → **События** → **Детектор движения**.

Включите опцию «**Детектор движения**».

Настройте зону детекции в области живого просмотра:

-  - Нажмите  и выделите область на изображении. При попадании движущихся объектов в эту зону будет срабатывать тревога.
-  - Нажмите  для удаления зоны.
-  - Нажмите  для захвата изображения.
-  - Нажмите  для начала записи (повторное нажатие остановит запись). Запись сохраняется на локальный ПК.
-  - Нажмите  для полноэкранного просмотра.

Чувствительность

Настройте уровень чувствительности срабатывания правила. Чем выше чувствительность, тем легче срабатывает правило.

Расписание активности

Настройте расписание работы детектора:

1. Нажмите «**Редактировать**», затем «**Активировать**».
2. На временной шкале выделите периоды активности и нажмите «**Сохранить**».
3. В активные периоды срабатывание правила будет передаваться на платформу.

Уведомление центра наблюдения

При включении функции устройство будет отправлять уведомления на платформу при срабатывании правил.

HTTP-уведомления

При активации устройство будет передавать уведомления на платформу по протоколу HTTP.

Нажмите «**Сохранить**» для применения настроек.

8.10.13 Настройка тревоги через веб-интерфейс ПК

Настройте параметры тревожного выхода.

Шаги:

1. Перейдите: **Система и обслуживание** → **Конфигурация системы** → **События** → **Настройки тревоги** → **Тревожный выход**.
2. Задайте **Название тревоги** и **Режим длительности сигнала**.

Тревожный Выход

№ 1

Имя сигнала тревоги

Продолжительность сигнала ... ☐ Непрерывный сигнал тревоги ☒ Продолжительность пользовательского сигнала тревоги

Пользовательский s

Настройки тревоги

Непрерывный сигнал

При активации тревоги сигнал будет звучать непрерывно.

Заданная длительность

Вы можете установить конкретное **Время длительности сигнала** для устройства при срабатывании тревоги.

8.10.14 Конфигурация подключений

Настройка параметров RS-485 через веб-интерфейс ПК

Вы можете настроить параметры RS-485, включая тип периферийного устройства, адрес, скорость передачи и т.д.

Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Конфигурация подключений** → **RS-485**.

Выберите **Протокол RS-485** из выпадающего списка.
Активируйте «**Включить RS-485**» и задайте параметры.
Нажмите «**Сохранить**» после завершения настройки.

Номер

Задайте номер линии RS-485.

Тип периферийного устройства

Выберите тип устройства из выпадающего списка в соответствии с фактической ситуацией. Доступные варианты: **Считыватель карт**, **Модуль расширения**, **Контроллер доступа** или **Отключено**.

Примечание

После изменения и сохранения типа периферийного устройства произойдет автоматическая перезагрузка устройства.

Адрес RS-485

Задайте адрес RS-485 в соответствии с вашими потребностями.

Примечание

Если выбран **Контроллер доступа**: При подключении устройства к терминалу через интерфейс RS-485, установите адрес RS-485 равным **2**. При подключении устройства к контроллеру, установите адрес RS-485 в соответствии с номером двери.

Скорость передачи (Baud Rate)

Скорость обмена данными между устройствами по протоколу RS-485.

Настройка параметров Wiegand через веб-интерфейс ПК

Вы можете настроить направление передачи данных по протоколу Wiegand.

Примечание

Некоторые модели устройств не поддерживают эту функцию. Ориентируйтесь на фактический продукт при настройке.

1. Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Конфигурация подключений** → **Настройки Wiegand**.

Страница настроек Wiegand

2. Активируйте опцию **Wiegand**, чтобы включить функцию.
3. Установите направление передачи данных.

Выход (Output)

Устройство может быть подключено к внешнему контроллеру доступа. Устройства будут обмениваться номерами карт с использованием форматов **Wiegand 26** или **Wiegand 34**.

4. Нажмите «**Сохранить**» для применения настроек.

Примечание

При изменении типа периферийного устройства и последующем сохранении параметров устройство автоматически перезагрузится.

Управление лифтом через веб-интерфейс ПК

Шаги:

1. Перейдите: **Система и обслуживание** → **Конфигурация системы** → **Конфигурация подключений** → **Параметры управления лифтом**.

Управление лифтом

2. Включите опцию «**Управление лифтом**».
3. Настройте параметры лифта:

Модель главного контроллера лифта

Просмотрите модель лифта.

Тип интерфейса

Выберите тип связи из выпадающего списка для коммуникации с лифтом.

- При выборе **RS-485** убедитесь, что устройство подключено к контроллеру лифта с помощью кабеля RS-485.
- При выборе **Сетевой интерфейс** введите **IP-адрес контроллера лифта, порт, имя пользователя и пароль** для связи.

Вместимость подземных этажей

Задайте количество подземных этажей.

Примечание

- К одному устройству можно подключить до **4** контроллеров лифта.
- Можно добавить до **10** подземных этажей.
- Убедитесь, что **типы интерфейсов** контроллеров лифта, подключенных к одному устройству, **одинаковы**.

8.11 Система и обслуживание**8.11.1 Перезагрузка**

Вы можете перезагрузить устройство.

Перейдите: **Система и обслуживание → Обслуживание → Перезагрузка**.

Нажмите «**Перезагрузить**», чтобы выполнить перезагрузку устройства.

8.11.2 Обновление**Локальное обновление через веб-интерфейс ПК**

Вы можете выполнить локальное обновление устройства.

Перейдите: **Система и обслуживание → Обслуживание → Обновление**.

Выберите **тип обновления** из выпадающего списка.

Нажмите «» и укажите файл обновления на вашем локальном ПК.

Нажмите «**Обновить**» для начала процесса.

Онлайн-обновление через веб-интерфейс ПК

Вы можете выполнить онлайн-обновление устройства.

Перейдите: **Система и обслуживание → Обслуживание → Обновление**.

Нажмите «**Проверить обновления**», чтобы узнать наличие новых версий.

Если устройство подключено к сети и добавлено в приложение LTV-CMS Mobile2, вы можете выполнить обновление непосредственно в приложении, выбрав «**Обновление устройства → Онлайн-обновление**», когда новая версия станет доступна.

8.11.3 Восстановление**Сброс к заводским настройкам через веб-браузер**

Вы можете восстановить заводские настройки устройства.

Перейдите: **Система и обслуживание → Обслуживание → Резервная копия и сброс**. Нажмите **«Сбросить все»**. Все параметры будут восстановлены до заводских настроек. После этого потребуется **активировать устройство** перед использованием.

Восстановление настроек по умолчанию через веб-интерфейс ПК

Вы можете восстановить настройки устройства по умолчанию.

Перейдите: **Система и обслуживание → Обслуживание → Резервная копия и сброс**.

Нажмите **«Восстановить»**. Устройство восстановит настройки по умолчанию, за исключением IP-адреса устройства и пользовательской информации.

8.11.4 Экспорт параметров устройства через веб-интерфейс ПК

Экспорт параметров устройства.

Перейдите: **Система и обслуживание → Обслуживание → Резервная копия и сброс**.

Резервная копия:

Нажмите **«Экспорт»** для выгрузки параметров устройства.

Примечание

Экспортированные параметры можно импортировать на другие устройства.

8.11.5 Импорт параметров устройства через веб-интерфейс ПК

Импорт конфигурационных параметров.

Перейдите: **Система и обслуживание → Обслуживание → Резервная копия и сброс**.

Импорт файла конфигурации:

Нажмите  и укажите файл на локальном ПК. Нажмите **«Импорт»**.

8.11.6 Отладка устройства

Вы можете настроить параметры отладки устройства.

Включение/отключение SSH через веб-браузер

Вы можете включить SSH для проведения удаленной отладки.

Перейдите: **Система и обслуживание → Обслуживание → Отладка устройства → Журнал отладки**.

Включить SSH:

SSH используется для удаленной отладки. Когда эта служба не нужна, рекомендуется **отключить SSH** для повышения безопасности.

Тестирование протокола через веб-интерфейс ПК

Выберите адрес протокола и введите команду для тестирования. Вы можете выполнить отладку устройства на основе полученного заголовка ответа и возвращаемого значения.

Перейдите: **Система и обслуживание → Обслуживание → Отладка устройства → Тестирование протокола**.

Журнал для отладки

Тестирование протокола

* Введите адрес протокола

GET

Введ./ISAPI/...

Выполнить

Результат тестирования

Заголовок ответа

Возвращаемое значение

Тестирование протокола

Выберите **адрес протокола** и введите **команду протокола**. Нажмите «**Выполнить**».

Анализируйте **заголовок ответа** и **возвращаемое значение** для отладки устройства.

8.11.7 Просмотр журнала через веб-интерфейс ПК

Вы можете осуществлять поиск и просмотр журналов (логов) устройства.

Перейдите: **Система и обслуживание** → **Обслуживание** → **Журнал**.

Установите **основной** и **вспомогательный** тип журнала. Задайте **время начала** и **время окончания** для поиска и нажмите «**Поиск**».

Результаты будут отображены ниже и будут включать: **№**, **время**, **основной тип**, **вспомогательный тип**, **№ канала**, **информацию о локальном/удаленном пользователе**, **IP-адрес удаленного узла** и т.д.

8.11.8 Настройки режима безопасности

Настройте режим безопасности для входа в клиентское программное обеспечение.

На странице «**Управление устройством**» перейдите: **Обслуживание и безопасность** → **Безопасность** → **Служба безопасности**.

Выберите режим безопасности и нажмите «**Сохранить**».

Режим безопасности

Высокий уровень безопасности: Обеспечивает строгую проверку пользовательской информации при входе в клиентское программное обеспечение.

Режим совместимости: Проверка пользовательской информации совместима со старыми версиями клиентского программного обеспечения.

8.11.9 Управление сертификатами

Позволяет управлять сертификатами сервера, клиента и корневым сертификатом (CA).

Примечание

Функция поддерживается только некоторыми моделями устройств.

Создание и импорт самоподписанного сертификата

Шаги:

1. Перейдите: **Система и обслуживание → Безопасность → Управление сертификатами**.
2. В области **«Файлы сертификатов»** выберите **тип сертификата** из выпадающего списка.
3. Нажмите **«Создать»**.
4. Введите информацию о сертификате.
5. Нажмите **«ОК»** для сохранения и установки сертификата.
 - Созданный сертификат отобразится в области **«Сведения о сертификате»**.
 - Сертификат будет сохранен автоматически.
6. Скачайте сертификат и сохраните его как запрос (CSR-файл) на локальном компьютере.
7. Отправьте файл запроса в центр сертификации для подписи.
8. Импортируйте подписанный сертификат:
 1. В области **«Импорт ключа»** выберите тип сертификата, укажите файл на локальном компьютере и нажмите **«Импорт»**.
 2. В области **«Импорт сертификата связи»** выберите тип сертификата, укажите файл на локальном компьютере и нажмите **«Импорт»**.

Импорт другого авторизованного сертификата

Если у вас уже есть авторизованный сертификат (не созданный на устройстве), вы можете импортировать его напрямую.

Шаги:

1. Перейдите: **Система и обслуживание → Безопасность → Управление сертификатами**.
2. В областях **«Импорт ключа»** и **«Импорт сертификата связи»** выберите тип сертификата и загрузите файлы сертификата.
3. Нажмите **«Импорт»**.

Импорт CA-сертификата

Перед началом

Заранее подготовьте CA-сертификат.

Шаги:

1. Перейдите: **Система и обслуживание → Безопасность → Управление сертификатами**.
2. В области **«Импорт CA-сертификата»** создайте идентификатор (ID).

Примечание

Вводимый идентификатор сертификата не должен совпадать с существующими.

3. Загрузите файл сертификата с локального компьютера.
4. Нажмите **«Импорт»**.

9. Настройка устройства через мобильный браузер

Настройка сети через TCP/IP (Проводное подключение)

Если устройство подключено к проводной сети, настройте его IP-адрес и активируйте точку доступа устройства через веб-браузер. Подробности см. в инструкции по настройке через веб-интерфейс ПК.

Включите Wi-Fi на телефоне и найдите точку доступа устройства.

Откройте браузер на телефоне, введите IP-адрес устройства, чтобы перейти на страницу настроек мобильного браузера.

Настройка сети через Wi-Fi

Если устройство подключено к сети Wi-Fi, настройте его IP-адрес и активируйте точку доступа устройства через веб-браузер. Подробности см. в инструкции по настройке через веб-интерфейс ПК.

Включите Wi-Fi на телефоне и найдите точку доступа устройства.

Примечание

Устройство и телефон должны находиться в **одной сети Wi-Fi**, иначе доступ к устройству через браузер телефона будет невозможен.

Откройте браузер на телефоне, введите IP-адрес устройства, чтобы перейти на страницу настроек мобильного браузера.

9.1 Вход в систему

Вы можете войти в систему через мобильный браузер.

Примечание

- Некоторые модели поддерживают настройку Wi-Fi.
- Убедитесь, что устройство **активировано**.
- Убедитесь, что устройство и мобильный телефон находятся в **одной сети Wi-Fi**.

Введите IP-адрес устройства в адресную строку мобильного браузера и нажмите "Перейти", чтобы открыть страницу входа.

Введите имя пользователя и пароль устройства. Нажмите **«Войти»**.

9.2 Забыли пароль

Если вы забыли пароль при входе в систему, вы можете сбросить его с помощью контрольных вопросов.

Шаги

1. На странице входа нажмите **«Забыли пароль»**.
2. Выберите **«Способ проверки»**.

Проверка контрольным вопросом

Если вы ранее настроили контрольные вопросы на устройстве или в веб-интерфейсе, вы можете ввести ответы для сброса пароля. Нажмите **«Проверка контрольным вопросом»**, затем **«Далее»**.

3. Введите ответ на контрольный вопрос и нажмите **«Далее»**.
4. Введите новый пароль и подтвердите его.
5. Нажмите **«Далее»**.

9.3 Настройки безопасности учетной записи

Измените резервный номер телефона. Если вы забудете пароль, вы сможете использовать этот номер для его смены.

Шаги

Примечание: Настройки доступны только если устройство и телефон находятся в одной локальной сети (LAN).

1. Нажмите  → **Управление пользователями** →  → **Безопасность учетной записи**.
2. Измените **резервный номер телефона**. Если вы забудете пароль для входа, вы сможете ввести этот номер телефона для его изменения.
3. Нажмите «**Сохранить**».

9.4 Главный экран

Вы можете просматривать статус двери, переходить на страницы конфигурации через быстрый доступ, проверять состояние сети и просматривать основную информацию.

Статус двери

Вы можете просматривать и изменять состояние двери (открыта/закрыта).

Быстрый доступ

Нажмите на название функции конфигурации, чтобы перейти на соответствующую страницу.

Состояние сети

Вы можете проверить статус сетевого подключения.

Основная информация

Вы можете просмотреть модель устройства, серийный номер и версию прошивки или перейти на страницу с подробной информацией.

9.5 Настройка

9.5.1 Просмотр информации об устройстве

Просмотр имени устройства, языка, модели, серийного номера, версии, количества дискретных входов, количества локальных интерфейсов RS-485, количества тревожных выходов, регистрационного номера, MAC-адреса и емкости устройства и т.д.

Нажмите  → **Системные настройки** → **Основная информация**.

На странице отобразится имя устройства, язык, модель, серийный номер, версия, количество дискретных входов, количество интерфейсов RS-485, количество тревожных выходов, регистрационный номер, MAC-адрес и емкость устройства и т.д.

9.5.2 Настройка времени

Настройте часовой пояс, режим синхронизации и отображаемое время.

Нажмите  → **Системные настройки** → **Настройка времени**.

Настройка времени

Нажмите **«Сохранить»** для применения настроек.

Часовой пояс

Выберите часовой пояс, в котором находится устройство, из выпадающего списка.

Режим синхронизации

Вручную

По умолчанию время на устройстве задается вручную. Вы можете установить время устройства самостоятельно.

NTP

Задайте IP-адрес NTP-сервера, номер порта и интервал синхронизации.

9.5.3 Настройка летнего времени (DST)

Шаги:

1. Нажмите  → **Системные настройки** → **Настройка времени**.

Летнее время

2. Нажмите **«Включить Летнее время (DST)»**.
3. Установите **время начала**, **время окончания** и **смещение** для летнего времени.
4. Нажмите **«Сохранить»**.

9.5.4 Управление пользователями

Шаги:

1. Нажмите  → **Управление пользователями** → **Управление пользователями** → **admin**.
2. Введите старый пароль и создайте новый пароль.
3. Подтвердите новый пароль.
4. Нажмите **«Сохранить»**.

Примечание

- Устройство автоматически проверяет надежность пароля. Настоятельно рекомендуется задать собственный надежный пароль (длиной от 8 до 16 символов, включая как минимум две категории из следующих: заглавные буквы, строчные буквы, цифры и специальные символы) для повышения безопасности вашего продукта.
- Рекомендуется регулярно менять пароль, особенно в системах с повышенными требованиями к безопасности. Ежемесячная или еженедельная смена пароля лучше защитит ваше устройство.

9.5.5 Сеть

Вы можете настроить параметры проводной сети, Wi-Fi и точки доступа устройства.

Проводная сеть

Настройка проводного сетевого подключения.

1. Нажмите  → **Настройки связи** → **Проводная сеть**.

DHCP

- Если функция **отключена**, необходимо вручную задать: **IPv4-адрес**, **Маску подсети IPv4**, **Основной шлюз IPv4**, **Режим IPv6**, **IPv6-адрес**, **Длину префикса IPv6-подсети**, **Основной шлюз IPv6**, **MAC-адрес** и **MTU**.
- Если функция **включена**, система автоматически назначит: **IPv4-адрес**, **Маску подсети IPv4**, **Основной шлюз IPv4**, **Режим IPv6**, **IPv6-адрес**, **Длину префикса IPv6-подсети** и **Основной шлюз IPv6**.

DNS-сервер

Задайте **Предпочитаемый** и **Альтернативный DNS-серверы** в соответствии с вашими потребностями.

Настройка Wi-Fi

Настройте параметры Wi-Fi устройства.

Перед началом

После добавления устройства в приложение вы можете включить функцию Wi-Fi на устройстве. Затем вы сможете настроить параметры Wi-Fi в мобильном браузере.

Шаги:

1. На главной странице нажмите  → **Настройки связи** → **Wi-Fi**.
2. Включите **Wi-Fi**.
3. Выберите сеть Wi-Fi из списка и введите пароль для подключения.
4. *Опционально: Добавление сети Wi-Fi*
 1. Прокрутите страницу до конца и нажмите **«Добавить сеть»**.
 2. Введите **Имя сети Wi-Fi** и выберите **Тип шифрования**.
 3. Нажмите **«ОК»**.
5. *Опционально: Настройка WLAN*
 1. Просмотрите имя подключенной сети Wi-Fi и детали сети.
 2. Нажмите **«Настройки WLAN»**.
 3. Задайте параметры WLAN.

Включить DHCP

При включении DHCP и опции **«Авто DNS»** устройство автоматически назначит IP-адрес и DNS-серверы.

Отключить DHCP

Вручную задайте IP-адрес и DNS-серверы.

4) Нажмите «Сохранить».

Результат

После настройки Wi-Fi и WLAN вы можете ввести WLAN IP-адрес устройства в мобильном браузере для входа в систему.

Настройка точки доступа устройства

Настройте точку доступа на устройстве, чтобы мобильный телефон мог подключиться к нему для доступа через мобильный браузер.

Шаги:

1. Нажмите  → **Настройки связи** → **Точка доступа устройства**.
2. Вы можете **включить точку доступа устройства** и просмотреть ее имя.

Примечание

По умолчанию имя точки доступа имеет формат `AP_СерийныйНомерУстройства`.

3. Нажмите «Сохранить».

Настройка параметров портов

Вы можете задать параметры HTTP и HTTPS в соответствии с фактическими потребностями при сетевом доступе к устройству.

1. Нажмите  → **Сетевые службы** → **HTTP(S)**.

HTTP

Порт, используемый браузером для доступа к устройству. Например, если HTTP-порт изменен на 81, для входа в браузер потребуется ввести `http://192.0.0.65:81`.

HTTPS

Настройте HTTPS-порт для безопасного доступа через браузер. При использовании HTTPS требуется сертификат.

Доступ к платформе

Функция доступа к платформе предоставляет возможность управления устройствами через платформу.

Шаги:

1. Нажмите  → **Доступ к устройству**

Примечание

LTV-CMS Mobile2 — это приложение для мобильных устройств. С помощью приложения вы можете просматривать изображение в реальном времени с устройства, получать уведомления о тревоге и т.д.



2. Установите флажок **«Включить»**, чтобы активировать функцию.
3. Вы можете включить опцию **«Выборочный»**, чтобы ввести адрес сервера.

Примечание

- От 6 до 12 символов (буквы a–z, A–Z) или цифры (0–9), с учетом регистра. Рекомендуется использовать комбинацию не менее 8 букв и/или цифр.
 - Проверочный код не может быть **123456** или **abcdef** (регистр не учитывается).
4. Вы можете просмотреть **Статус Регистрации** и **Статус Привязки**.
 5. Вы можете нажать **«Привязать учетную запись»** → **«Просмотреть QR-код»**, отсканировать QR-код для привязки учетной записи.
 6. Нажмите **«Сохранить»**, чтобы применить настройки.

Настройка параметров ISUP

Настройте параметры ISUP для доступа к устройству по протоколу ISUP.

Шаги

Примечание: Функция должна поддерживаться устройством.



1. Нажмите  → **«Доступ к устройству»** → **«ISUP»**, чтобы перейти на страницу настроек.
2. Включите **ISUP**.
3. Установите версию ISUP, адрес сервера, порт, идентификатор устройства и ключ шифрования.

Примечание: Если вы выбираете версию 5.0, необходимо также задать ключ шифрования.

4. Нажмите **«Сохранить»**, чтобы применить настройки.

Настройки VoIP



Нажмите  → **«Доступ к устройству»** → **«VoIP»**, чтобы перейти на страницу настроек.

Нажмите **Включить VoIP шлюз**.

Установите параметры VoIP и нажмите **«Сохранить»**, чтобы применить параметры.

9.5.6 Управление пользователями

Вы можете добавлять, редактировать, удалять и искать пользователей через мобильный веб-браузер.

Шаги



1. Нажмите  → **Управление персоналом**, чтобы перейти на страницу настроек.
2. Добавление пользователя
 - 1) Нажмите +.

Добавление пользователя

2) Задайте следующие параметры:

Идентификатор сотрудника

Введите идентификатор сотрудника. Идентификатор не может быть равен 0 или превышать 32 символа. Можно использовать комбинацию заглавных, строчных букв и цифр.

Имя

Введите имя. Поле поддерживает цифры, заглавные и строчные английские буквы, а также символы. Рекомендуется использовать не более 32 символов.

№ этажа/№ комнаты

Введите номер этажа и/или номер комнаты.

Постоянное действие

Установите права доступа пользователя как действующие бессрочно.

Дата начала/Дата окончания

Установите **дату начала** и **дату окончания** действия прав доступа пользователя.

Администратор

Если пользователя необходимо назначить администратором, активируйте опцию «**Администратор**».

Роль пользователя

Выберите роль пользователя.

Отпечаток пальца

Добавление отпечатка пальца. Нажмите «**Отпечаток пальца**», затем нажмите «+» и добавьте отпечаток с помощью модуля сканирования.

Карта

Добавление карты. Нажмите «**Добавить карту**». Введите **номер карты** или поднесите карту к считывателю устройства и нажмите «**Считать**», затем выберите **свойство**. Нажмите «**Сохранить**», чтобы добавить карту.

Пароль

Примечание

- Перед настройкой паролей необходимо выяснить, является ли пароль персональным PIN-кодом, задаваемым на устройстве, или применяемым на платформе. Если это PIN-код, задаваемый на устройстве, его можно создавать и редактировать через веб-интерфейс, но нельзя на платформе. Если это PIN-код,

применяемый на платформе, его необходимо настраивать на платформе, и он не может быть отредактирован через веб-интерфейс.

- Убедитесь, что в качестве **режима пароля** выбран **Пароль устройства**.

Нажмите «**Управление персоналом**» → «**Добавить**», чтобы перейти на страницу добавления пользователя.

Введите пароль.

3) Нажмите «**Сохранить**».

3. Нажмите на пользователя в списке, которого необходимо отредактировать, чтобы изменить информацию.
4. Нажмите на пользователя в списке, которого необходимо удалить, и нажмите  для удаления пользователя.
5. Вы можете найти пользователя, введя его идентификатор сотрудника или имя в строке поиска.

9.5.7 Поиск событий

Нажмите  → **Поиск событий**.

Введите условия поиска, включая идентификатор сотрудника, имя, номер карты, время начала и время окончания, и нажмите «**Поиск**».

Примечание

Поддерживается поиск по именам в пределах 32 знаков.

Результаты будут отображены в списке.

9.5.8 Настройки аудио

Вы можете включать или регулировать звук.

Нажмите  → **Аудио**.

Включите опцию **Включить голосовые подсказки** в соответствии с фактическими потребностями. Устройство будет воспроизводить голосовые инструкции.

Вы также можете настроить громкость звука.

Вы можете включить **Эквалайзер**. Устройство будет автоматически регулировать частоты с помощью аудиоалгоритма для улучшения качества звука и выравнивания звукового эффекта.

Нажмите **Сохранить**.

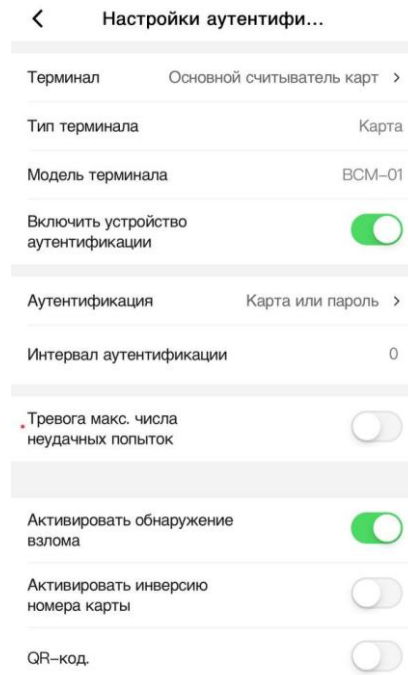
9.5.9 Настройки контроля доступа

Настройка параметров аутентификации

Настройте параметры аутентификации.

Шаги

1. Нажмите  → **Контроль доступа** → **Настройки аутентификации**.



Настройки аутентификации

2. Нажмите **Сохранить**.

Терминал

Основной считыватель карт

Вы можете настроить параметры считывателя карт устройства. При выборе основного считывателя карт необходимо настроить следующие параметры: **Тип терминала**, **Модель терминала**, **Активировать считыватель карт**, **Аутентификация**, **Интервал распознавания (с)**, **Минимальный интервал между прикладываниями карты (с)**, **Тревога при превышении макс. количества неудачных попыток аутентификации**, **Включить обнаружение вскрытия** и **Включить обратный порядок номера карты**.

Тип считывателя карт

Получить тип считывателя карт.

Описание считывателя карт

Получить описание считывателя карт. Параметр доступен только для чтения.

Активировать считыватель карт

Включить функцию считывателя карт.

Аутентификация

Выберите режим аутентификации из выпадающего списка в соответствии с вашими потребностями.

Интервал аутентификации

Вы можете задать интервал аутентификации для одного и того же человека. Один и тот же человек может пройти аутентификацию только один раз в течение заданного интервала. Повторная попытка аутентификации в течение этого интервала будет неудачной.

Тревога при превышении макс. количества неудачных попыток аутентификации

Включите эту функцию для генерации тревоги, когда количество попыток считывания карты достигнет установленного значения.

Включить обнаружение вскрытия

Включите функцию антивандальной защиты считывателя карт.

Включить обратный порядок номера карты

После включения функции номер карты будет считываться в обратной последовательности.

QR-код

Активируйте функцию, чтобы пользователь мог использовать QR-код для открытия двери.

Примечание

- При включении функции QR-кода необходимо отключить ИК-подсветку. Изображение в условиях слабой освещенности может ухудшиться из-за отключения ИК-подсветки.
- При настройке функции QR-кода через НСС или НСЕС следует выбрать совместимость с версией 1.0 или 2.0. Рекомендуется версия 2.0.

Настройка параметров двери

Настройте параметры двери, включая название двери, время открытия, тип кнопки выхода, время удержания двери открытой после первого человека, тревогу превышения времени открытия, дверной контакт, дополнительное время открытия, код принуждения, суперпароль и код сброса.

Нажмите  → **Контроль доступа** → **Параметры двери**.

После настройки нажмите **Сохранить**.

Название

Задайте название для двери.

Время открытия

Задайте длительность разблокировки двери после прикладывания карты.

Тип кнопки выхода

Вы можете настроить кнопку выхода в режим **Оставлять открытым** (Remain Open) или **Оставлять закрытым** (Remain Closed) в соответствии с вашими потребностями. По умолчанию установлено значение «Оставлять открытым».

Время удержания двери открытой после первого человека

Задайте время, в течение которого дверь остается открытой после прохода первого человека. После авторизации первого человека разрешается проход нескольких лиц или другие действия аутентификации.

Порог тревоги превышения времени открытия

Если дверь не закрыта по истечении времени блокировки, точка контроля дохода подаст звуковой сигнал тревоги. При установке значения «0» тревога отключается.

Дверной контакт

Вы можете настроить дверной контакт в режим **Оставлять открытым** (Remain Open) или **Оставлять закрытым** (Remain Closed) в соответствии с вашими потребностями. По умолчанию установлено значение «Оставлять закрытым».

Дополнительное время открытия

Для дверного контакта может быть установлена задержка срабатывания после того, как человек с расширенным доступом приложит карту.

Код принуждения

При вводе кода принуждения дверь откроется, а система отправит уведомление о событии принуждения.

Суперпароль

Администратор или уполномоченное лицо может ввести суперпароль для открытия двери.

Код сброса

Задайте код сброса тревоги. При активации тревоги ввод этого кода отключит сигнал.

Примечание

Коды принуждения и суперпароли не должны повторяться и обычно состоят из 4–8 цифр.

Контроль доступа и управление лифтом**Шаги**

1. Нажмите  → **Контроль доступа** → **Параметры управления лифтом**.
2. Включите **Управление лифтом** и задайте параметры: **Вместимость подвальных этажей**, **Модель основного контроллера лифта** и **Тип интерфейса**.

Примечание

- Только главная дверная станция поддерживает управление лифтом.
- При выборе типа интерфейса «**Сетевой**» необходимо указать адрес сервера, порт, пользователя и пароль.

3. Нажмите **Сохранить**.

Параметры терминала

Вы можете настроить параметры терминала для доступа.

Нажмите  → **Контроль доступа** → **Параметры терминала**.

Вы можете установить **Режим работы** как **Режим контроля доступа**. Это стандартный режим работы устройства, требующий аутентификации для получения доступа.

Нажмите **Сохранить** после завершения настройки.

Настройка параметров RS-485

Вы можете настроить параметры интерфейса RS-485, включая тип подключаемого устройства, адрес, скорость передачи и другие.

Нажмите  → **Контроль доступа** → **RS-485**.

Нажмите **Сохранить** после завершения настройки.

Тип подключаемого устройства

Выберите тип устройства из выпадающего списка в соответствии с фактической ситуацией. Доступные варианты: **Считыватель карт**, **Модуль расширения** или **Контроллер доступа**.

Примечание:

После изменения типа подключенного устройства и сохранения настроек устройство перезагрузится автоматически.

Протокол RS-485**Приватный:**

Устройство может взаимодействовать со сторонними устройствами через RS-485.

OSDP:

Стандартный протокол RS-485.

Адрес RS-485

Задайте адрес устройства в сети RS-485 в соответствии с вашими потребностями.

Примечание:

При выборе типа "**Контроллер доступа**": если устройство подключается к терминалу через интерфейс RS-485, установите адрес RS-485 равным 2. При подключении к контроллеру задайте адрес RS-485 в соответствии с номером двери.

Скорость передачи (Baud Rate)

Скорость обмена данными при коммуникации между устройствами по протоколу RS-485.

Бит данных

Количество битов данных в коммуникации между устройствами по протоколу RS-485.

Стоповый бит

Стоповый бит при передаче данных между устройствами по протоколу RS-485.

Четность/Управление потоком/Режим связи

По умолчанию включено.

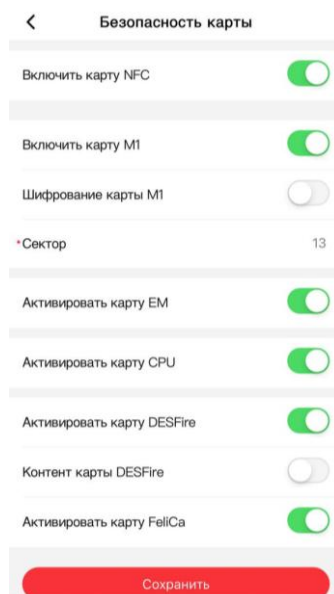
Тип выхода

Установите тип выхода в соответствии с вашими фактическими потребностями.

Настройка защиты карт

Настройте карты для устройства.

Нажмите  → **Контроль доступа** (Access Control) → **Защита карт** (Card Security).

**Защита карт**

Настройте параметры карты и нажмите **Сохранить**.

Активировать NFC-карту

Для предотвращения считывания данных СКУД мобильным телефоном вы можете отключить функцию NFC-карты для повышения уровня защиты данных.

Активировать M1-карту

Включите функцию M1-карты для возможности аутентификации с её использованием.

Шифрование M1-карты

Шифрование M1-карты повышает уровень безопасности при аутентификации.

Сектор

Активируйте функцию и задайте сектор для шифрования.

Примечание

Рекомендуется шифровать сектор 13.

Активировать EM-карту

Включите функцию EM-карты для возможности аутентификации с её использованием.

Примечание

Если подключенный считыватель карт поддерживает работу с EM-картами, в настройках также будет доступно включение/отключение данной функции.

Активировать DESFire-карту

Устройство сможет считывать данные с карты DESFire при активации этой функции.

Считывание содержимого DESFire-карты

После включения функции считывания содержимого DESFire-карты устройство сможет читать данные с карты.

Активировать FeliCa-карту

Устройство сможет считывать данные с карты FeliCa при активации этой функции.

9.5.10 Настройки вызова**Назначение номера устройству через мобильный веб-интерфейс**

Устройство может использоваться как контроллер доступа, дверная станция или вызывная панель. Вы можете назначить номер устройству для организации видеосвязи.

Нажмите  → **Переговорное устройство** → **Настройки ID устройства**.

Нажмите **Сохранить**.

Если в качестве типа устройства выбрано **Вызывная панель** или **Контроллер доступа**, вы можете задать номер периода/корпуса, номер здания, номер подъезда, номер этажа и номер вызывной панели.

Тип устройства

Устройство может использоваться как дверная станция. Вы можете выбрать другой тип устройства из выпадающего списка.

Номер квартала/корпуса

Введите номер квартала/корпуса устройства.

Номер здания

Введите номер здания.

Номер

Назначьте пользовательский номер устройства.

Примечание

- Если тип устройства — «**Вызывная панель**» или «**Контроллер доступа**», номер должен находиться в диапазоне от 0 до 99.



- После изменения типа устройства или его номера необходимо перезагрузить устройство для применения изменений.

Номер подъезда

Введите номер подъезда устройства.

Номер этажа

Введите номер этажа устройства.

Если выбран тип устройства «**Внешняя вызывная панель**» (Outer Door Station), можно задать номер корпуса/периода и номер вызывной панели.

Тип устройства

Устройство может использоваться как внешняя вызывная панель. Вы можете выбрать другой тип устройства из выпадающего списка.

Номер ЖК

Введите номер ЖК устройства.

Номер

Назначьте пользовательский номер устройства.

Примечание

- Если тип устройства — «Внешняя вызывная панель», номер должен находиться в диапазоне от 1 до 99.
- После изменения типа устройства или его номера необходимо перезагрузить устройство для применения изменений.

Настройки сессии

Вы можете задать пароль регистрации, IP-адрес главной панели и IP-адрес частного сервера, а также включить поддержку протокола 1.0 в соответствии с вашими потребностями.

Нажмите  → **Переговорное устройство** → **Настройки сессии**.

Пароль регистрации

Задайте пароль регистрации главной панели для осуществления связи.

IP-адрес главной панели

Введите IP-адрес главной панели, используемый для связи.

IP-адрес частного сервера

Относится к IP-адресу SIP-сервера. Введите IP-адрес главной панели, используемый для связи. В данном случае главная панель используется как SIP-сервер. Другие переговорные устройства должны регистрироваться на этом адресе сервера для осуществления связи.

Включить протокол 1.0

Если функция включена, вызывная панель может регистрироваться на главной панели по старой версии протокола. Если отключена — используется новая версия протокола.

После настройки вы можете обеспечить связь между контроллерами доступа и видеодомофонными панелями, комнатными панелями, главной панелью, платформами и т.д.

Нажмите **Сохранить**.

Настройки вызова

Вы можете задать максимальную длительность связи между главной панелью и другими устройствами.

Нажмите  → **Переговорное устройство** → **Настройки вызова**.

Макс. время связи

Максимальное время связи между главной панелью и другими устройствами во время разговора. При превышении заданного времени связь прервется. Допустимый диапазон времени связи — от 90 до 120 секунд.

Настройки номеров

Назначьте SIP-номера для комнат. Комнаты могут связываться друг с другом через SIP-номера.

Шаги

1. Нажмите  → **Переговорное устройство** → **Настройки номеров**.
2. Введите **Номер комнаты** и **SIP-номер 1**.
3. Нажмите **Сохранить**.
4. **Опционально:** Нажмите на настроенный номер комнаты для редактирования или нажмите **+Добавить**, чтобы добавить еще один SIP-номер.
5. **Опционально:** Нажмите **Удалить** для удаления номера комнаты.

Вызов по нажатию кнопки через мобильный веб-интерфейс

Вы можете совершать вызовы нажатием кнопки.

Шаги

1. Нажмите  → **Переговорное устройство** → **Вызов по нажатию кнопки**.
2. Нажмите **1** для перехода на страницу настройки.

Примечание

- При выборе опции "Вызов указанной вызывной панели" необходимо задать номер связанной комнаты.
 - По умолчанию можно нажать кнопку для вызова комнатной панели и удерживать кнопку для вызова центра.
3. Выберите действие, привязанное к кнопке. При выборе "**Вызов указанной вызывной панели**" необходимо задать номер комнаты.
 4. Нажмите "**Сохранить**".

9.5.11 Настройка параметров конфиденциальности через мобильный веб-интерфейс

Настройте параметры загрузки и хранения изображений.

Нажмите  → **Настройки конфиденциальности**.

Загрузка и хранение изображений

Вы можете включить опции "**Сохранять снимки после срабатывания связи**" или "**Загружать снимки после срабатывания связи**". Снятые изображения будут загружаться или сохраняться на платформе.

Нажмите "**Сохранить**".

9.5.12 Режим пароля

Перед настройкой паролей необходимо определить, является ли пароль персональным PIN-кодом, задаваемым на устройстве, или применяемым на платформе.

Шаги

1. Нажмите  → **Конфигурация** → **Безопасность** → **Режим пароля**

Персональный PIN-код, задаваемый на устройстве

Может создаваться или редактироваться на устройстве или через веб-интерфейс, но не может быть установлен на других платформах.

Персональный PIN-код, применяемый на платформе

Может создаваться или редактироваться на платформе и должен быть выдан устройству перед использованием. Не может быть задан на устройстве или через веб-интерфейс.

2. Нажмите **"Сохранить"**.

9.5.13 Обновление и обслуживание

Перезагрузка устройства, восстановление параметров и обновление версии прошивки.

Перезагрузка устройства

Нажмите  → **Перезагрузка устройства**.

Нажмите **Перезагрузить**, чтобы выполнить перезагрузку устройства.

Обновление

Нажмите  → **Обновление**.

Нажмите **Обновить** для обновления прошивки устройства.

Примечание

Не отключайте питание во время процесса обновления.

Восстановление параметров

Нажмите  → **Сброс**.

Восстановление настроек по умолчанию

Устройство восстановит заводские настройки, за исключением IP-адреса и информации о пользователях.

Полный сброс до заводских настроек

Все параметры будут восстановлены до заводских значений. После сброса потребуется заново активировать устройство перед использованием.

9.5.14 Просмотр пользовательской документации

Просмотр документации для пользователя.

Примечание

Функция доступна только при входе в мобильный веб-интерфейс по IP-адресу. При входе через точку доступа эта функция не поддерживается.

Нажмите  для перехода на соответствующую страницу.

Нажмите **Просмотреть документацию онлайн**, чтобы открыть руководство пользователя.

9.5.15 Лицензии ПО с открытым исходным кодом

Вы можете просмотреть лицензии используемого программного обеспечения с открытым исходным кодом.

Нажмите  для перехода на страницу.

Нажмите **Лицензии ПО с открытым исходным кодом**.

9.5.16 Выход из мобильного веб-интерфейса

Выход со страницы конфигурации мобильного веб-интерфейса.

На главной странице нажмите  → **Выход**, затем подтвердите действие, нажав **ОК**, для завершения сеанса. Если потребуется снова перейти на страницу конфигурации, необходимо будет повторно ввести имя пользователя и пароль.

10. Другие платформы для настройки

Устройство также можно настраивать с помощью системы **HikCentral Access Control**. Подробности смотрите в руководствах пользователя соответствующих платформ.

HikCentral Access Control (HCAC)

Нажмите на ссылку, чтобы просмотреть руководство пользователя для HCAC:

<http://enpinfodata.hikvision.com/analysisQR/showQR/f2f6cf42>

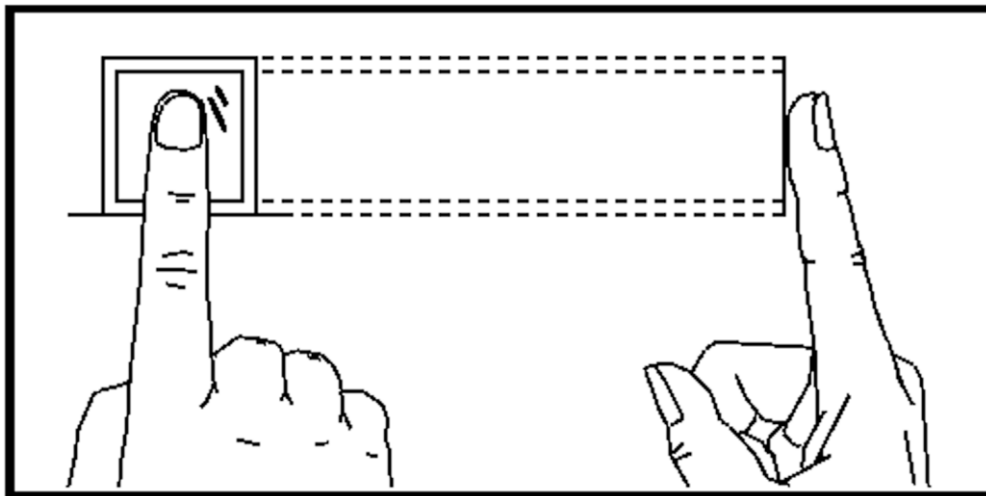
11. Приложение А. Советы по сканированию отпечатка пальца

Рекомендуемые пальцы

Указательный, средний или безымянный палец.

Правильное сканирование

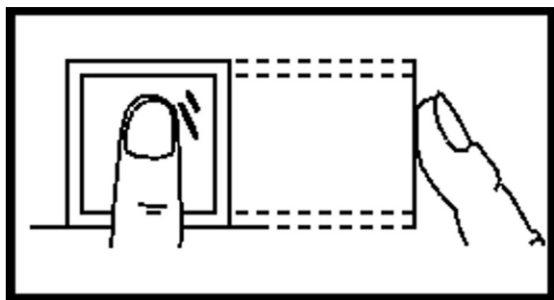
На рисунке ниже показан правильный способ сканирования:



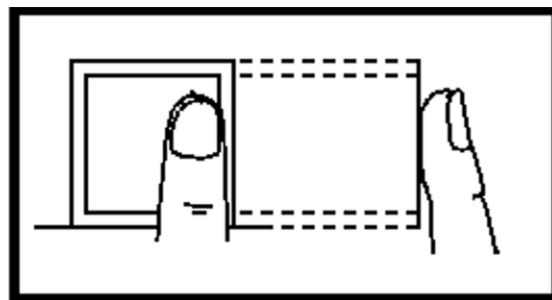
Прикладывайте палец к сканеру горизонтально. Центр сканируемого пальца должен совпадать с центром сканирующего элемента.

Неправильное сканирование

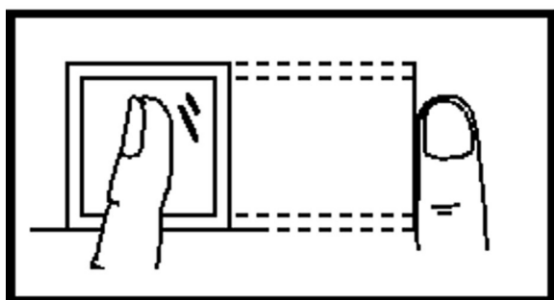
Ниже показаны примеры некорректного сканирования отпечатка пальца:



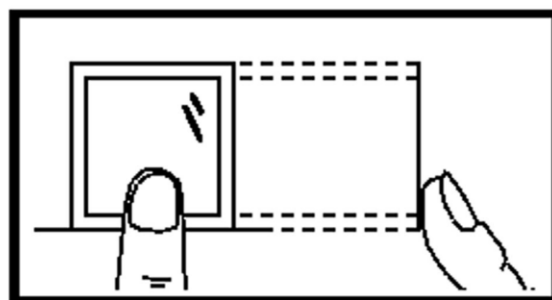
Vertical



Edge I



Side



Edge II

Окружающая среда

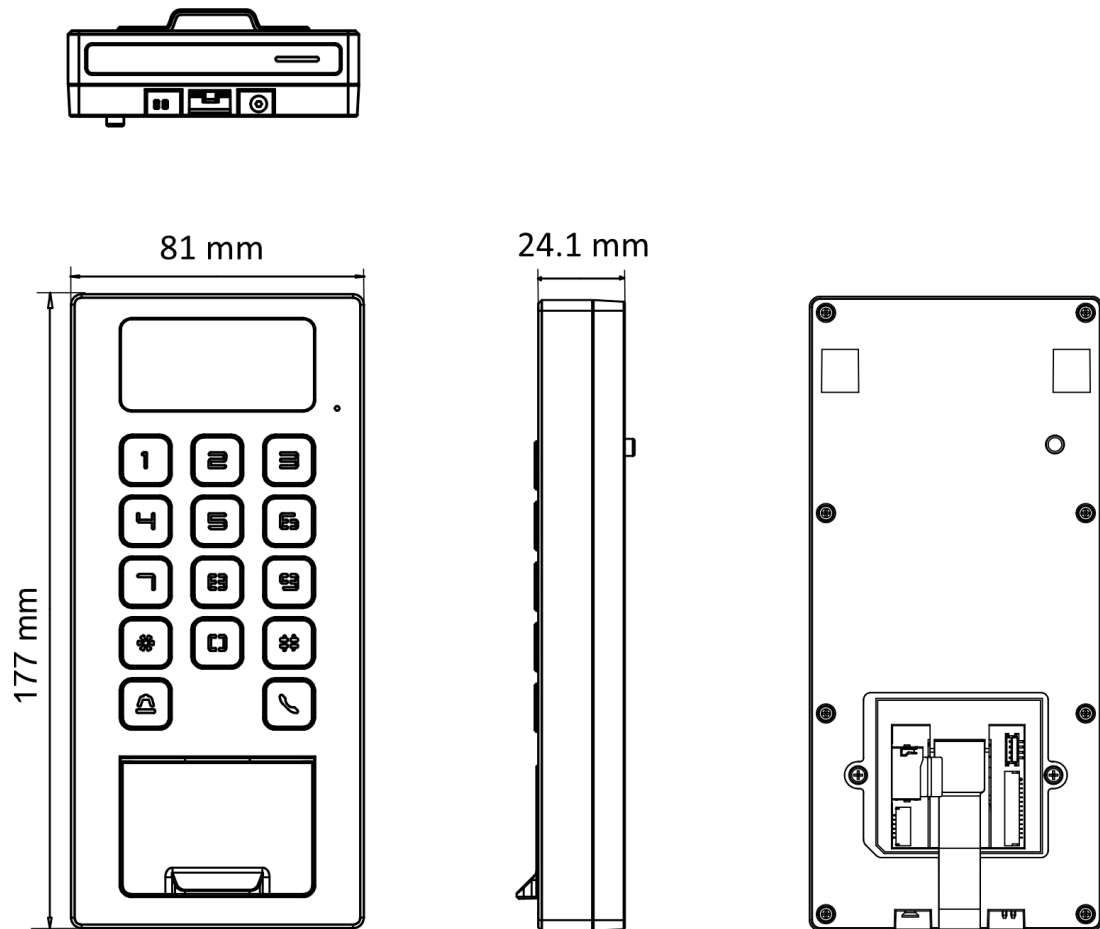
Сканер следует защищать от прямых солнечных лучей, высоких температур, повышенной влажности и дождя. Если кожа пальца сухая, сканер может не распознать отпечаток. В этом случае можно подуть на палец и повторить сканирование.

Дополнительные рекомендации

Если у вас слабовыраженный отпечаток пальца или возникают трудности со сканированием, рекомендуем использовать другие способы аутентификации.

Если на сканируемом пальце есть повреждения, сканер может не распознать отпечаток. Попробуйте использовать другой палец.

12. Габаритные размеры



13. Гарантия

На устройство распространяется гарантия 12 месяцев с момента приобретения.

Ознакомиться с условиями гарантийного обслуживания вы можете на веб-сайте <https://luis.ru/>.

О бренде ЛКД

Торговая марка ЛКД принадлежит торговому дому ЛУИС+ и известна на российском рынке с 2015 года. Линейка оборудования ЛКД – это полнофункциональный набор устройств, оптимальных по соотношению «цена/качество», ассортимент которых постоянно пополняется, следуя новым тенденциям на рынке СКУД и создавая их. Марка ЛКД представлена во всех основных подгруппах оборудования для создания систем СКУД любой сложности.

Спасибо за то, что приобрели оборудование ЛКД!

