Автономный контроллер

AT-AC1000 WIFI

Руководство по эксплуатации

---

* Благодарим Вас за приобретение нашей продукции.

* Производитель вправе вносить изменения, направленные на улучшение технических характеристик продукции, которые могут привести к изменению параметров изделия.

* Пожалуйста, внимательно прочитайте инструкцию по эксплуатации (особенно, часть, касающуюся техники безопасности) перед использованием изделия, точно соблюдайте правила эксплуатации изделия.

* Производитель не несет ответственности за любой вред, нанесенный вследствие неправильного использования изделия.

* Руководство предназначено только для справки. В случае несоответствия между руководством и фактическим продуктом преимущественную силу имеет фактический продукт.

Содержание

Описание

Программируемый автономный контроллер AT-AC1000 WIFI предназначен для создания современной системы контроля и управления доступом. Для этого к нему могут быть подключены внешние считыватели по интерфейсу Wiegand и практически любой запирающий механизм.

Главной особенностью устройства является возможность работы с мобильным приложением Smart Life (Tuya Smart). Данное приложение позволяет управлять практически любым исполнительным механизмом удаленно, делать настройки, администрировать пользователей, а также генерировать временные пароли для гостей.

Память устройства рассчитана на обслуживание до 1000 пользователей. Автономный контроллер AT-AC1000 WIFI имеет тревожные вход и выход для подключения датчика двери и сирены. При наличии в системе второго такого контроллера можно без проблем организовать так называемый шлюз для прохода.

Корпус контроллера выполнен из пластика и предназначен для установки в труднодоступных местах.

Технические характеристики

Количество пользователей:	1000: (987 обычных пользователей, 10 посетителей, 2 тревожных пользователя, 1 блокирующий пользователь)
Входы:	1 вход для кнопки выхода, 1 вход для датчика положения двери
Wiegand вход:	Wiegand 26 - 58
Реле замка:	до 2А, 12 В (DC)
Время срабатывания реле замка:	1 – 99 с
Тревожный выход:	Открытый коллектор, 12В до 3 А
Питание:	12 В (DC) ±20%
Потребляемый ток:	не более 50 мА
Рабочая температура:	-40 - +60ºС
Влажность:	0% - 90%
Размеры:	91x49x21 мм

Комплект

Автономный контроллер ……..……....1 шт.

Пульт дистанционного управления (ПДУ).….1 шт.

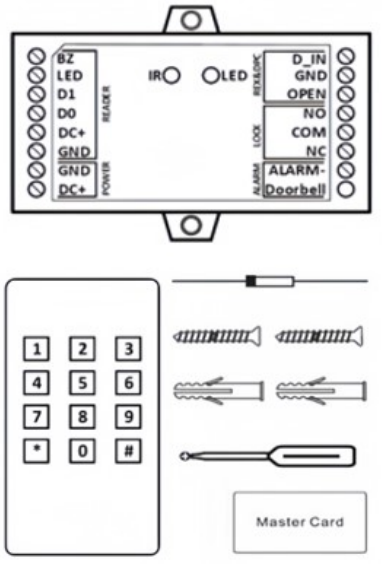
Защитный диод 1N4004 ……....1 шт.

Крепежный комплект ……..…1 шт.

Шлицевая отвертка ……..…1 шт.

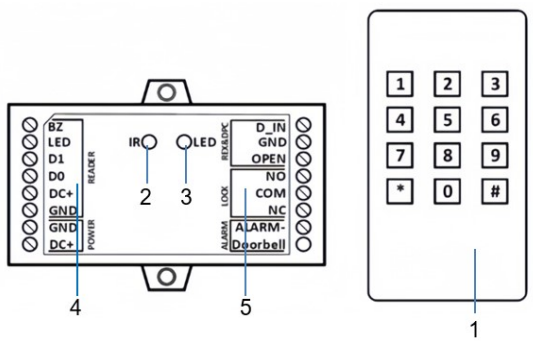
EM-Marin мастер-карта ……..…1 шт.

Паспорт и гарантийный талон ……1 шт.



Контроллер скуд wifi

1. Пульт дистанционного управления (ПДУ)
2. ИК-приемник для ПДУ
3. Световой индикатор состояний
4. Левая клеммная колодка для подключения источника питания и считывателей
5. Правая клеммная колодка для подключения датчика двери, кнопки выхода, запирающего механизма, сирены и кнопки звонка



Описание контактов

Название	**Назначение**
BZ	Управление зуммером на подключенных считывателях
LED	Управление светодиодом на подключенных считывателях
D1	D1 - Wiegand вход считывателя
D0	D0 - Wiegand вход считывателя
DC +	«+» для питания считывателей
GND	Общий контакт «-» для считывателей
GND	Общий контакт «-» контакт для подключения блока питания
DC +	«+» для подключения блок питания
D_IN	NC контакт для подключения датчика двери (геркона)
GND	Общий контакт для подключения датчика двери и кнопки выхода
OPEN	Контакт для подключения кнопки выхода
NO	Нормально-разомкнутый контакт реле («мокрый»/ «сухой») для подключения электромеханического замка
COM	Общий контакт реле для подключения замка
NC	Нормально-замкнутый контакт реле («мокрый»/ «сухой») для подключения электромагнитного замка
ALARM -	Контакт для подключения исполнительного устройства (сирены)
DOORBELL	Для подключения кнопки дверного звонка

Индикация

Режим	**Светодиод**	**Зуммер**
Дежурный режим	Постоянно красный	-
Вход в режим программирования	Мигает красный	Одиночный сигнал
Программирование	Постоянно оранжевый	Одиночный сигнал
Ошибка	-	Тройной сигнал
Выход из режима программирования	Постоянно красный	Одиночный сигнал
Разблокировка запирающего механизма	Зеленый на время разблокировки	Одиночный сигнал
Тревога	Быстро мигает красный	Прерывистый сигнал

Основные особенности

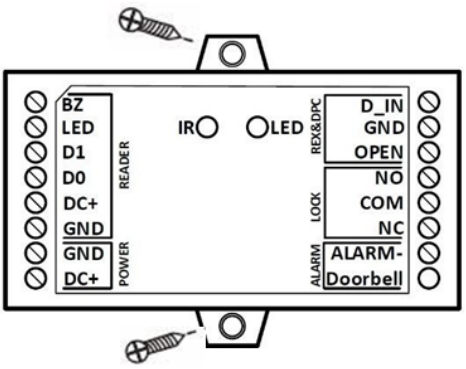
- Программирование с помощью ИК пульта или с помощью мастер-карт
- 1000 пользователей
- Режимы идентификации: КАРТА, КОД, КАРТА ИЛИ КОД
- Поддержка кода длиной от 4 до 6 знаков
- Режим блокировки доступа с помощью блокирующих карт
- Режим доступа для посетителей
- Поддержка считывателей Wiegand 26-58
- Поддержка считывателей с клавиатурой с выходным форматом данных 4/8 бит
- Выходное реле может иметь либо сухие контакты, либо коммутировать питающее напряжение
- Импульсный или триггерный режим работы реле замка
- Групповая регистрация карт
- Режим автоматического запоминания карт
- Копирование пользователей с одного контроллера в память другого
- Режим шлюза при использовании дополнительного контроллера со считывателем
- Встроенный зуммер и световая индикация
- Настройка, управление, администрирование, выдача временных паролей в приложении Smart Life/Tuya Smart

Установка и подключение

Рекомендации по установке

1. Подключение необходимо производить согласно соответствующей схеме, либо согласно обозначениям на устройстве с назначением контактов.
2. Вся коммутация должна производиться при отсутствии питания во всей системе.
3. Контроллер по умолчанию имеет "Мокрые" контакты реле для управления запирающим механизмом, то есть на контакты NO/NC подается/ снимается соответствующее напряжение от блока питания, питающего контроллер. Если необходимы "Сухие" контакты реле, то нужно снять крышку контроллера, удалить перемычки с пинов 1–2 и 3–4, а затем установить одну перемычку на пины 1–3.
4. Время задержки реле открытия замка может быть запрограммировано при настройке контроллера с помощью ПДУ или из приложения.
5. Не используйте блоки питания, которые по характеристикам не подходят для питания контроллера и запирающего механизма.
6. Если датчик двери (геркон) не используется, то для правильного отображения состояния двери в приложении рекомендуется сделать перемычку между контактами "D_IN" и "GND".
7. Не допускайте механические повреждения устройства.
8. Не устанавливайте устройство в местах:
   – с температурой, отличающейся от эксплуатационной;
   – с повышенной вибрацией;
   – повышенного испарения и парообразования;
   – с источниками мощных электромагнитных полей.

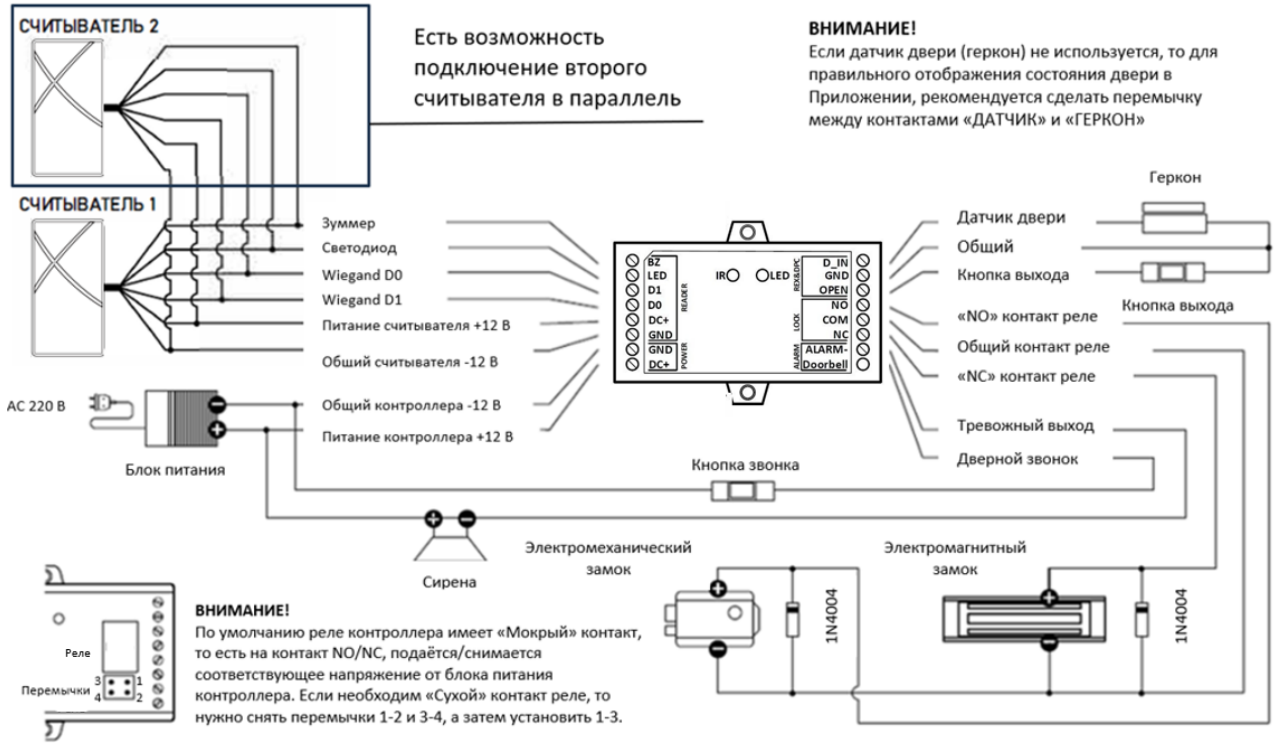
Монтаж контроллера



1. В соответствии с рисунком справа на вертикальной поверхности подготовьте 2 отверстия диаметром 6 мм на расстоянии 55 мм друг от друга для фиксации контроллера на поверхности.
2. В отверстия установите комплектные дюбеля.
3. Подключите кабеля к клеммным колодкам по соответствующей схеме подключения с помощью комплектной шлицевой отвертки.
4. Если необходимо, поменяйте тип контактов реле для управления запирающим механизмом. Контроллер по умолчанию имеет "мокрые" контакты реле, то есть на контакты NO/NC подается/снимается соответствующее напряжение от блока питания, питающего контроллер. Если необходимы "Сухие" контакты реле, то нужно снять крышку контроллера, удалить перемычки с пинов 1-2 и 3-4, а затем установить одну перемычку на пины 1-3. Затем установить крышку контроллера обратно.
5. Зафиксируйте устройство на поверхности двумя саморезами.

Схемы подключения

Вариант подключения с "сухими" контактами реле

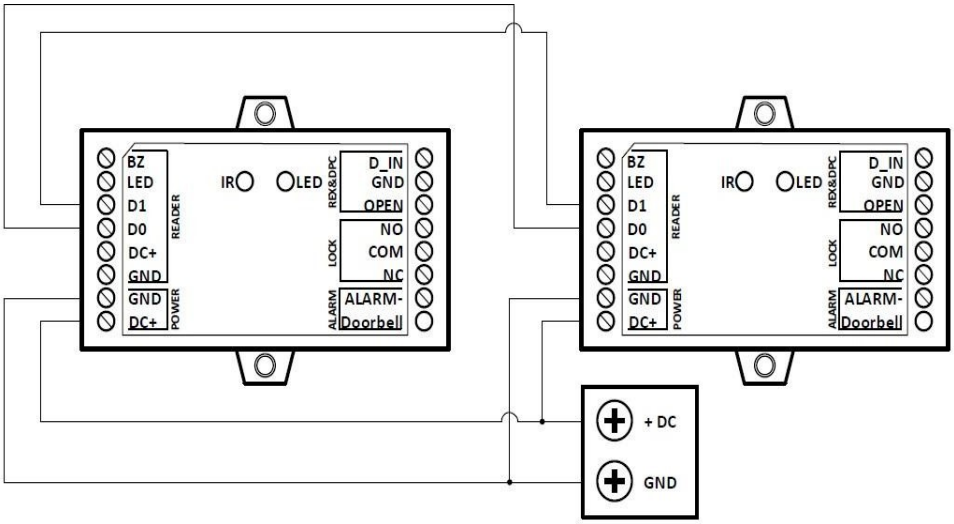


Примечание:

1. Параллельно замку в обратной полярности рекомендуется установить защитный диод 1N4004 (входит в комплект поставки), если конструкцией замка он не предусмотрен.
2. Контроллер по умолчанию имеет "Мокрые" контакты реле для управления запирающим механизмом, то есть на контакты NO/NC подается/снимается соответствующее напряжение от блока питания, питающего контроллер. Если необходимы "Сухие" контакты реле, то нужно снять крышку контроллера, удалить перемычки с пинов 1-2 и 3-4, а затем установить одну перемычку на пины 1-3.
3. Если датчик двери (геркон) не используется, то для правильного отображения состояния двери в приложении рекомендуется сделать перемычку между контактами D_IN и GND.

Вариант подключения контроллеров для передачи данных

Автономные контроллеры поддерживают копирование данных пользователей. Для копирования данных пользователей сделайте подключение, как показано ниже.



Примечание: Если питание контроллеров осуществляется от разных источников питания, необходимо объединить шины GND иначе копирование не будет выполнено.

1. Базовые настройки

1.1. Режим программирования

Для локального программирования устройства используется ИК-пульт дистанционного управления (ПДУ), входящий в комплект поставки. Для начала работы нужно удалить пластиковый язычок, защищающий пульт от разряда батареи. Во время ввода комбинаций ПДУ должен быть направлен на ИК-приемник контроллера.

Пароли и комбинации могут вводиться с помощью ПДУ и подключенных считывателей с кодонаборной клавиатурой, за исключением считывателей, которые имеют на выходе 10-значный виртуальный номер идентификатора на выходе.

Этап программирования	Комбинация клавиш
Вход в режим программирования	✱ (**Мастер-пароль**) **#** по умолчанию – 123456
Выход из режима программирования	✱

1.2. Изменение мастер-пароля

Этап программирования	Комбинация клавиш
Вход в режим программирования	✱ (**Мастер-пароль**) **#**.....По умолчанию мастер-код – 123456
Выход из режима программирования	✱
Смена мастер-кода	**0** (Новый **Мастер-пароль**) **#** (Повтор нового **Мастер-пароля**) **#** Мастер-пароль должен состоять из 6 цифр

1.3. Выбор режима работы

Контроллер предусматривает несколько режимов доступа. По умолчанию установлен доступ по RFID-ключам и паролям. Альтернативно можно выбрать режимы только по ключам или только по паролям. Кроме этого, имеется групповой доступ по нескольким ключам и/или паролям. То есть доступ будет разрешен при считывании нескольких действительных RFID-ключей и/или паролей в любой комбинации.

Этап программирования	Комбинация клавиш
Вход в режим программирования	✱ (**Мастер-пароль**) **#**По умолчанию мастер-код – 123456
Только по RFID-ключам	**40 #**
Только по паролям	**41 #**
По RFID-ключам или паролям	**43 #** По умолчанию
Групповой доступ	**43(2-9) #** 2-9 — Количество действительных RFID-ключей или паролей

Примечание: При работе в режиме группового доступа интервалы между считываниями RFID-ключей и вводами паролей должны быть не более 5 секунд. В противном случае контроллер автоматически вернется в режим ожидания.

1.4 Настройка параметров реле

Реле имеет 2 режима работы: **Импульсный** и **Триггерный**. В **Импульсном** режиме реле меняет положение в течение заданного времени при использовании действительного ключа и/или пароля, нажатии кнопки выхода. В **Триггерном** режиме реле меняет положение на противоположное при каждом чтении действительного ключа или вводе пароля, нажатии кнопки выхода. Например, такой режим удобен в случаях, когда необходимо открывать или блокировать проход на определенный период (рабочий день, перерыв и т.д.), а также использовать устройство в качестве пульта управления для охранно-пожарной системы.

Этап программирования	Комбинация клавиш
Вход в режим программирования	✱ **(Мастер-пароль) #**....По умолчанию мастер-код – 123456
Импульсный режим	**3(1–99) #** (по умолчанию 3 секунды) 1-99 – время задержки реле от 1 до 99 секунд По умолчанию установлено 5 секунд
Триггерный режим	**30 #**
Выход из режим программирования	✱

1.5 Настройка входа Wiegand

Настройка входных параметров протокола Wiegand выполняется в соответствии с характеристиками подключаемого внешнего RFID-считывателя.

Этап программирования	Комбинация клавиш
Вход в режим программирования	**✱ (Мастер-пароль) #**....По умолчанию мастер-код –123456
Автодетекция параметров входа	**80 # (по умолчанию)**
Ручная установка битности входа	**8(26–44, 56, 58) #** Где 52-44, 56, 58 – битность входного формата Wiegand
Выход из режим программирования	**✱**

1.6. Настройка индикации

При необходимости у устройства можно отключить светодиод и звуковую индикацию.

Этап программирования	Комбинация клавиш
Вход в режим программирования	**✱ (Мастер-пароль) #**...По умолчанию мастер-код – 123456
Выключить зуммер	**70 #**
Включить зуммер	**71 #** По умолчанию
Выключить светодиод	**72 #**
Включить светодиод	**73 #** По умолчанию
Выход из режим программирования	**✱**

Примечание: Зуммер и светодиод отключаются только для типовых операций. В режиме программирования они также работают.

1.7. Функция предотвращения несанкционированного доступа

При активной функции предотвращения несанкционированного доступа, после 10 неудачных попыток считывания недействительного RFID-ключа включается зуммер и на 10 минут блокируется доступ. По умолчанию функция отключена.

Этап программирования	Комбинация клавиш
Вход в режим программирования	**✱ (Мастер-пароль) #** По умолчанию мастер-код - 123456
Выключить предотвращение несанкционированного доступа	**60 #** По умолчанию
Включить предотвращение несанкционированного	**61 #** Только блокировка доступа на 10 мин.

доступа	
Включить предотвращение несанкционированного доступа с установкой длительности тревоги	**62#5(0-3) #** Где 0-3 длительность тревоги (по умолчанию 1 мин.). Блокировка доступа на 10 минут, активация зуммера и тревожного выхода. Для отключения можно ввести действительный пароль или мастер-пароль/считать RFID-ключ или мастер-карт.
Выход из режим программирования	✱

Примечание: При активированной функции «предотвращение несанкционированного доступа» разблокировка по кнопке выхода актуальна всегда.

1.8 Детекция открытия двери (геркон)

Детекция открытия двери требует наличия подключенных к контроллеру датчика двери (геркона) и электромагнитного замка. Если дверь открывается несанкционировано силой, то атомический активируется зуммер и тревожный выход. По умолчанию функция отключена.

Этап программирования	Комбинация клавиш
Вход в режим программирования	✱ **(Мастер-пароль) #** По умолчанию мастер-код –123456
Выключить предотвращение несанкционированного доступа	**63 #** По умолчанию
Включить функцию детекции открытия силой с настройкой длительности тревоги	**64#5(0-3) #** где 0-3 длительность тревоги (по умолчанию 1 мин.). Активация зуммера и тревожного выхода. Для отключения можно ввести действующий пароль или мастер-пароль/считать действующий RFID-ключ или мастер-карту.
Выход из режим программирования	✱

1.9. Режим шлюза

С помощью 2-х контроллеров можно организовать так называемый шлюз. Режим шлюза обычно используется на объектах с повышенным уровнем безопасности (банки, исправительные учреждения и т.д.). Логика режима заключается в том, что пользователь не сможет пройти через вторую дверь пока открыта первая и наоборот.

Для организации шлюза:

1. Подключите все устройства согласно соответствующей схеме.

2. Добавьте пользователей с одинаковыми RFID-ключами, паролями на оба контроллера. Если пользователей много, то можно использовать функцию передачи базы данных пользователей на другое устройство.

3. Активируйте режим шлюза на обоих контроллерах в соответствии с таблицей ниже

Этап программирования	Комбинация клавиш
Вход в режим программирования	✱ **(Мастер-пароль) #** По умолчанию мастер-код – 123456
Выключить режим	**90 #** По умолчанию

шлюза	
Включить режим шлюза	**91 #**
Выход из режим программирования	✱

1.10. Возврат к заводским настройкам и добавление Мастер-карты

Для сброса настроек выполните следующие действия:

1. Отключите питание устройства.
2. Нажмите и удерживайте кнопку «выход».
3. Подайте питание на устройство, прозвучит двукратный звуковой сигнал.
4. Отпустите кнопку выхода, LED индикатор загорится желтым светом.
5. Приложите к считывателю карту, которая будет мастер-картой. После программирования мастер-карты считыватель перейдет в дежурный режим.
6. Если мастер-карту добавлять не нужно, то удерживать кнопку выхода необходимо не менее 5 секунд после 2 звуковых сигналов.
7. Формат мастер-карты должен соответствовать формату считывателя.

Примечание: Функция сброса настроек не удаляет из контроллера информацию о пользователях.

1.11. Удаление устройства из аккаунта Приложения

Если доступ к аккаунту в приложении по каким-либо причинам утерян, то отвязать устройство можно с помощью следующей комбинации, набранной на ПДУ или считывателе с кодонаборной клавиатурой.

Этап программирования	Комбинация клавиш
Вход в режим программирования	✱ **(Мастер-пароль) #** По умолчанию мастер-код – 123456
Удаление из аккаунта	**9 (Мастер-пароль) #**
Выход из режим программирования	✱

2. Работа с Пользователями

User ID – это любое трехзначное число в диапазоне от 1 до 999, к которым присваиваются RFID-ключи и пароли.

Существуют 3 типа Пользователей:

Пользователь	Описание	User ID
Обычный	Разблокирует точку прохода по RFID-ключу или паролю.	1-986
Блокирующий	Блокирует всех остальных пользователей. Это может быть использовано для того, чтобы без ведома одного пользователя все остальные не могли разблокировать точку прохода, например в ночное время.	987
Тревожный	Активирует тревожный выход. Это может быть использовано для интеграции с охранно-пожарной системы.	988-989
Гость	Разово или временно разблокирует точку прохода.	990-999

Примечание:

1. User ID не должен начинаться с нулей!
2. Пароль может состоять из 4-6 цифр.

2.1. Добавление обычных Пользователей

Этап программирования	Комбинация клавиш
Вход в режим программирования	**✱ (Мастер-пароль) #** По умолчанию мастер-код – 123456
Добавление RFID-ключа с автоматическим присвоением следующего доступного User ID	**1 (Чтение ключа) #** можно добавлять все ключи по очереди
Добавление RFID-ключа по номеру с автоматическим присвоением следующего доступного User ID	**1 (8/ 10/ 17-значный номер ключа) #** можно добавлять все ключи по очереди
Добавление RFID-ключа с присвоением определенного User ID	**1 (User ID) # (Чтение ключа) #**
Добавление RFID-ключа по номеру с присвоением определенного User ID	**1 (User ID) # (8/ 10/ 17-значный номер ключа) #**
Групповое добавление	**1 (User ID) # (Количество ключей) # (8/10/17-значный номер первого ключа) #** можно добавить сразу все RFID-ключи за один шаг, если их номера по
Добавление пароля с автоматическим присвоением следующего доступного User ID	**1(Пароль) #** можно добавлять все пароли по очереди
Добавление пароля с присвоением определенного User ID	**1(User ID) # (Пароль) #**
Bsxod из режим программирования	**✱**

Примечание:

1. Для обычных пользователей нужно использовать User ID в интервале 1-986.
2. Пароль должен содержать 4-6 цифр.
3. Для обеспечения повышенной безопасности при вводе пароля для прохода предусмотрен ввод дополнительных произвольных цифр до и после пароля. Например, для пользователя задан пароль 123321. В этом случае можно использовать следующие комбинации: **123321* или *123321**, где * - любая цифра от 0 до 9, которая служит для маскирования пароля.

2.2. Добавление тревожных Пользователей

При считывании идентификатора или набора пароля **пользователя управляющего тревожным входом,** система активируется.

Этап программирования	Комбинация клавиш
Вход в режим	**✱ (Мастер-пароль) #** По умолчанию мастер-код – 123456

программирования	
Добавление тревожного RFID-ключа	**1 (User ID) # (Чтение ключа) #**
Добавление тревожного RFID-ключа по номеру	**1(User ID) # (8/ 10/ 17-значный номер ключа) #**
Добавление тревожного пароля	**1 (User ID) # (Пароль) #**
Выход из режим программирования	**✱**

Примечание:

1. Для тревожных пользователей нужно использовать User ID 988 и 989.
2. Пароль для активации тревоги может содержать 4-6 цифр

2.3. Добавление гостевых пользователей

Для гостей предусмотрено 10 User ID, к которым можно присвоить RFID-ключи и пароли. Также, для этих пользователей можно задать количество проходов, по истечении которых ключи и пароли автоматически будут становиться недействительными.

Этап программирования	Комбинация клавиш
Вход в режим программирования	**✱ (Мастер-пароль) #** По умолчанию мастер-код – 123456
Добавление гостевого RFID-ключа	**1 (User ID) # (0-9) # (Чтение ключа) #** 0-9 количество проходов, где 0 означает 10 проходов
Добавление гостевого RFID-ключа по номеру	**1 (User ID) # (0-9) # (8/ 10/ 17-значный номер ключа) #** 0-9 количество проходов, где 0 означает 10 проходов
Добавление гостевого пароля	**1 (User ID) # (0-9) # (Пароль) #** 0-9 количество проходов, где 0 означает 10 проходов
Выход из режим программирования	**✱**

Примечание:

1. Для гостевых пользователей нужно использовать User ID в интервале от 990 до 999.
2. Гостевой пароль может содержать 4-6 цифр

2.4. Добавление блокирующего Пользователя

В системе предусмотрен блокирующий пользователь, к User ID которого могут быть присвоены RFID-ключ и/или пароль. При считывании ключа или вводе пароля блокирующего пользователя система перестает реагировать на все другие идентификаторы и пароли до тех пор, пока блокирующий пользователь не считает свой ключ или не введет свой пароль. Это позволяет заблокировать/разблокировать доступ всем пользователям с помощью одного ключа или пароля.

Этап программирования	Комбинация клавиш
Вход в режим программирования	**✱ (Мастер-пароль) #** По умолчанию мастер-код – 123456
Добавление блокирующего RFID-ключа	**1 (User ID) # (Чтение ключа) #**

Добавление блокирующего RFID-ключа по номеру	**1 (User ID) # (8/ 10/ 17-значный номер ключа) #**
Добавление блокирующего пароля	**1 (User ID) # (Пароль) #**
Выход из режим программирования	**✱**

Примечание:

1. Для блокирующего пользователя нужно использовать User ID 987.
2. Блокирующий пароль может содержать 4-6 цифр.

2.5. Удаление пользователей

Этап программирования	Комбинация клавиш
Вход в режим программирования	**✱ (Мастер-пароль) #** По умолчанию мастер-код – 123456
Удаление по RFID-ключу	**2 (Чтение ключа) #** Можно удалять по очереди
Удаление по номеру RFID-ключа	**2 (8/ 10/ 17-значный номер ключа) #**
Удаление по паролю	**2 (Пароль) #** Можно удалять по очереди
Удаление по User ID	**2 (User ID) #**
Удаление всех пользователей	**2 (Мастер-пароль) #**
Выход из режим программирования	**✱**

2.6. Добавление/Удаление Пользователей Мастер-картой

Этап программирования	Комбинация клавиш
Добавление пользователей	1. Считывание Мастер-карты
	2. Чтение RFID-ключа/ввод пароля. Можно добавлять ключи и пароли по очереди.
	3. Считывание Мастер-карты
Удаление пользователей	1. Считывание мастер-карты дважды с максимальным интервалом 5 секунд
	2. Чтение RFID-ключа/ввод пароля. Можно удалять ключи и пароли по очереди.
	3. Считывание Мастер-карты.

Примечание:

1. Мастер-карта формата EM-Marin поставляется в комплекте с контроллером. Если подключаемый считыватель имеет другой формат, то необходимо произвести сброс настроек контроллера и добавить Мастер-карту соответствующего формата.
2. Если заводская Мастер-карта утеряна, то можно добавить новую путем сброса устройства к заводским настройкам.
3. При добавлении или удалении паролей после каждого ввода пароля необходимо нажимать #. Например, 4321#.

4. Пароль может содержать 4-6 цифр.

2.7. Режим ACCEPT

При активации режима ACCEPT контроллер разрешает доступ всем RFID-ключам и заносит их в свою память. Таким образом, проработав некоторое время в этом режиме, контроллер автоматически формирует базу данных действительных RFID-ключей. После формирования базы данных режим нужно отключить.

Этап программирования	Комбинация клавиш
Вход в режим программирования	**✱ (Мастер-пароль) #** По умолчанию мастер-код –123456
Выключение режима ACCEPT	**92 #** По умолчанию
Включение режима ACCEPT	**93 #**
Выход из режим программирования	**✱**

2.8. Передача базы данных на другое устройство

Устройство поддерживает передачу базы данных пользователей (RFID-ключи, пароли) на другое аналогичное устройство путем проводного подключения.

Этап программирования	Комбинация клавиш
Вход в режим программирования	**✱ (Мастер-пароль) #** По умолчанию мастер-код – 123456
Активация передачи базы данных пользователей	**98 #** По умолчанию
Выход из режим программирования	**✱**

Примечание:

1. Устройства, поддерживающие передачу базу данных пользователей, должны быть из одной модели.
2. Убедитесь, что устройства подключены по соответствующей схеме для передачи базы данных.
3. Убедитесь, что мастер-пароли передающего и принимающего устройств совпадали.
4. Активация функции передачи базы данных производится только на передающем устройстве.
5. Если на принимающем устройстве уже имеются какие-либо данные пользователей, то после передачи они будут удалены.
6. Для передачи базы данных из 1000 пользователей потребуется около 30 секунд.
7. В течение максимум 30 секунд светодиод будет мигать зеленым. По окончанию прозвучит 1 звуковой сигнал и светодиод станет красным. Это будет означать, что передача данных успешно завершена.

3. ТИПОВЫЕ ОПЕРАЦИИ

Этап программирования	Комбинация клавиш
Проход по RFID-ключу	Чтение действительного RFID-ключа
Проход по паролю	**Пароль #**

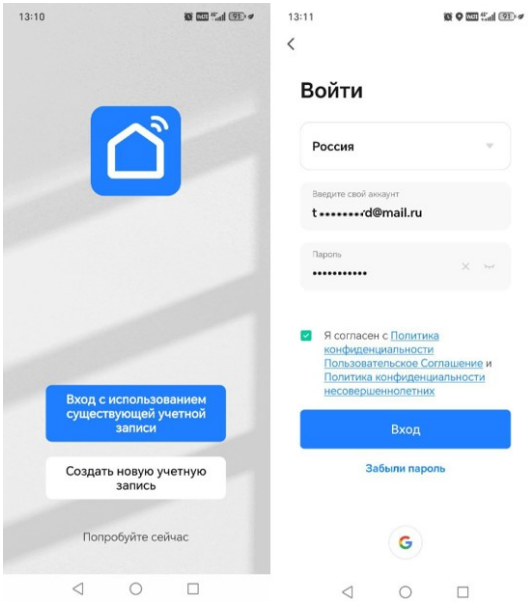
Отключение тревоги	• Чтение действительного RFID-ключа • Чтение мастер-карты • **Мастер-пароль #** • **Действующий пароль #**

4. Начало работы с Приложением

В данном разделе описываются процедуры, которые необходимо выполнить, чтобы активировать функции доступные при использовании мобильного приложения для смартфона.

4.1 установка Приложения

Скачайте и установите приложение **Smart Life/Tuya Smart** из Play Market для устройств на базе ОС Android или из App Store для устройств на базе iOS.



Smart Life

Tuya Smart

Приложение Smart Life – для Android & iOS.

Примечание:

Приложение Tuya Smart может быть недоступно в вашем регионе. В таком случае используйте Приложение Smart Life.

4.2 регистрация аккаунта

Запустите приложение Smart Life/Tuya Smart и зарегистрируйте аккаунт для работы с контроллером СКУД. Для регистрации укажите страну и адрес электронной почты, к которому будет привязан аккаунт. Также в процессе регистрации необходимо согласиться с пользовательским соглашением. Далее на указанную электронную почту будет выслан 6-значный цифровой код. Его следует ввести для подтверждения регистрации. После этого система предложит ввести свой пароль для последующего доступа к зарегистрированному аккаунту.

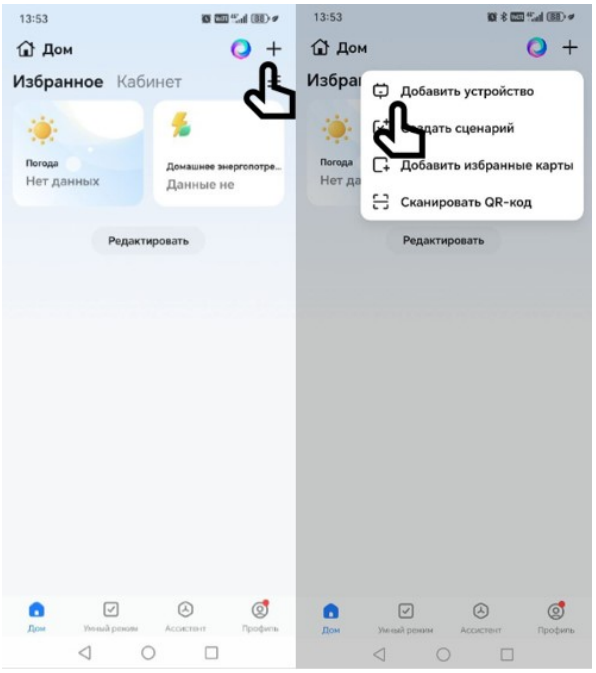
Примечание:

1. Для корректной работы необходимо правильно указать страну, в которой предполагается использовать устройство.
2. Для корректной работы приложения необходимо дать все разрешения в настройках смартфона.

4.3. Добавление устройства в Приложение

ШАГ 1

Перед добавлением устройства в приложение нужно сбросить настройки Wi-Fi модуля к заводским. Для этого нужно ввести следующего комбинацию с помощью комплектного пульта дистанционного управления (ПДУ): **✱ (Мастер-пароль) # 9 (Мастер-пароль) #**, где мастер-пароль по умолчанию – 123456.

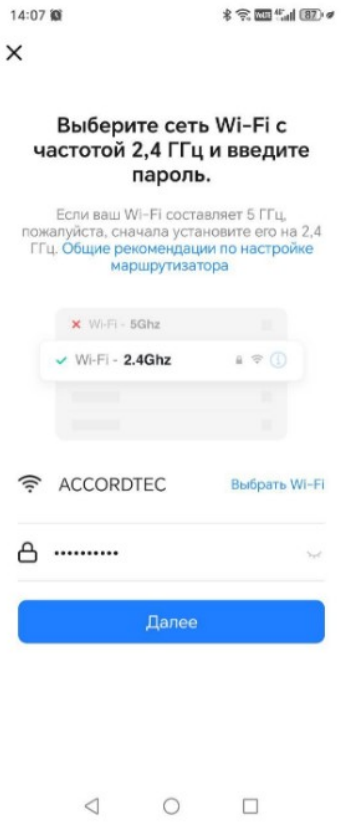


ШАГ 2

Откройте приложение Smart Life/Tuya Smart на смартфоне и убедитесь, что Вы авторизованы. Для добавления устройства нажмите соответствующую кнопку в центре экрана или иконку + в верхнем правом углу.

ШАГ 3

Если контроллер не обнаружен автоматически, то выберите раздел **Камера** и **замок**, и тип устройства **Замок (Wi-Fi).**

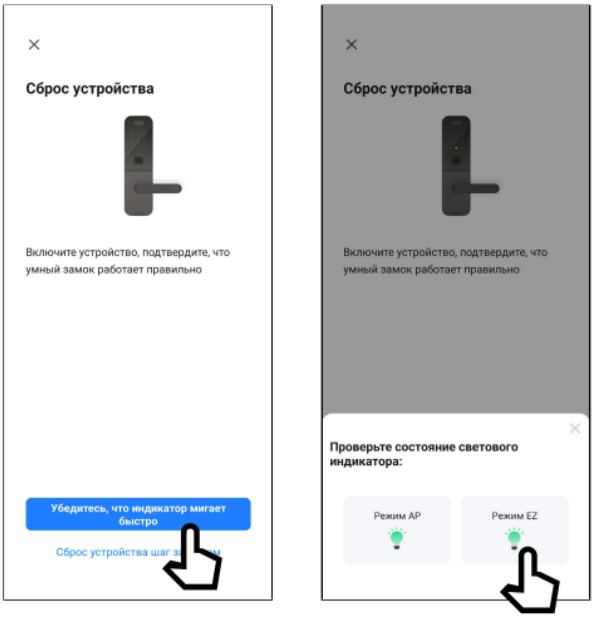


Примечание:

1. Убедитесь, что смартфон подключен к той же Wi-Fi точке доступа, к которой планируется подключить контроллер.
2. Для более быстрого добавления включите Bluetooth на смартфоне.
3. Для ввода комбинаций используйте комплектный ПДУ, предварительно удалив пластиковый язычок, защищающий его от разряда батарейки.

ШАГ 4

Выберите Wi-Fi сеть, к которой планируется подключить контроллер. После выбора сети введите пароль для подключения к ней и нажмите Далее.



ШАГ 5

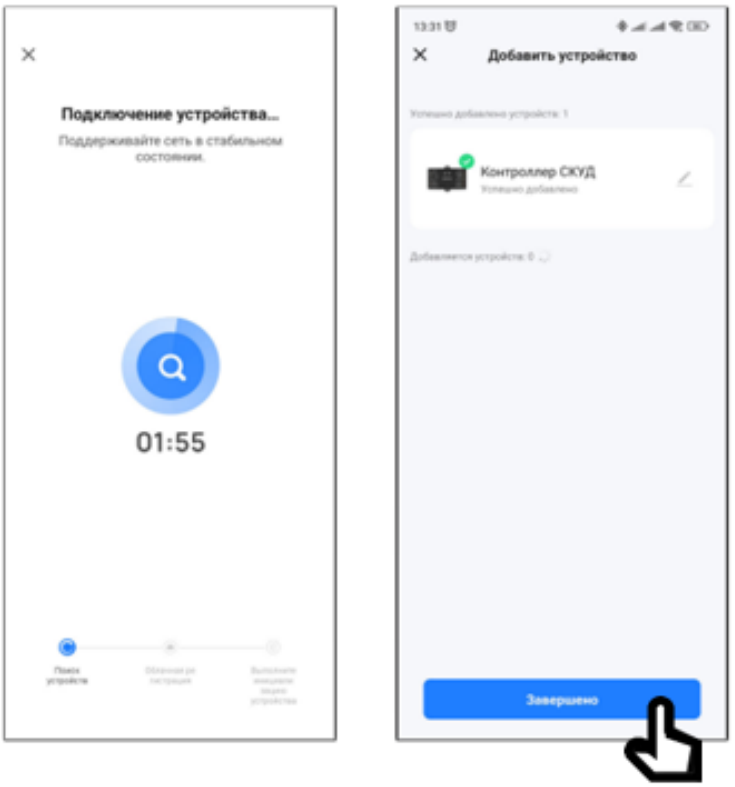
Сбросьте устройство к заводским настройкам нажав кнопку «**Убедитесь, что индикатор мигает быстро»**.

ШАГ 6

В появившемся снизу меню выберите иконку **Режим EZ**.

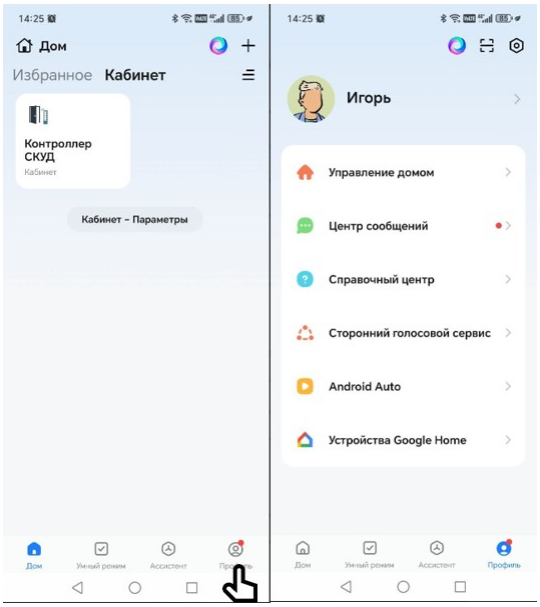
ШАГ 7

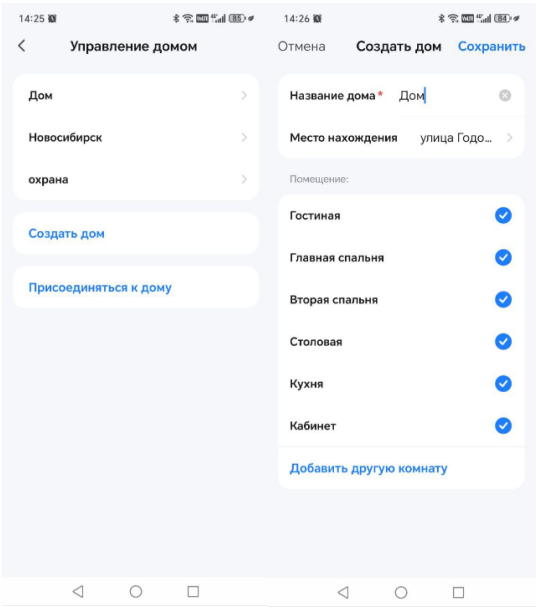
На экране появится диаграмма статуса процесса подключения. Дождитесь его завершения.



ШАГ 8

Перед началом эксплуатации для структурирования всех устройств в приложении, а также для предоставления общего доступа другим пользователям к функциям системы рекомендуется создать ДОМ. Для этого зайдите в **Профиль** →**Управление домом** → **Создать дом**. Далее нужно задать имя нового дома и нажать Сохранить.





5. Работа в приложении

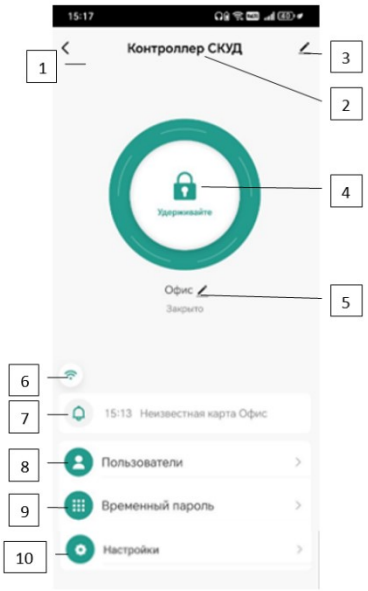
После добавления контроллера в список устройств, станет доступным следующий функционал:

- Удаленное управление запирающим механизмом
- Управление пользователями
- Выдача временных паролей
- Удаленная настройка

5.1. Описание главного меню устройства

Для просмотра главного меню контроллера выберите его из списка устройств. Описание элементов **Главного меню**:

1. Кнопка для возврата к списку устройств **Назад**
2. Имя устройства (Можно изменить)
3. Вызов меню настроек устройства
4. Кнопка для ручной разблокировки запирающего механизма
5. Имя помещения/объекта (Можно изменить)
6. Индикатор сети
7. Последнее действие в системе и кнопка перехода в журнал событий
8. Кнопка для перехода в меню **Пользователи**
9. Кнопка для перехода в меню **Временный пароль**
10. Кнопка для перехода в меню **Настройки**



Примечание:

1. После добавления устройства для управления запирающим механизмом необходимо активировать пункт **Разблокировка** из **Приложения** в **Настройках** устройства.
2. Для разблокировки запирающего механизма необходимо удерживать кнопку.
3. Если датчик двери (геркон) не используется, то для правильного отображения состояния двери в приложении рекомендуется сделать перемычку между контактами **ДАТЧИК** и **ОБЩИЙ**.

5.2. Подменю Пользователи

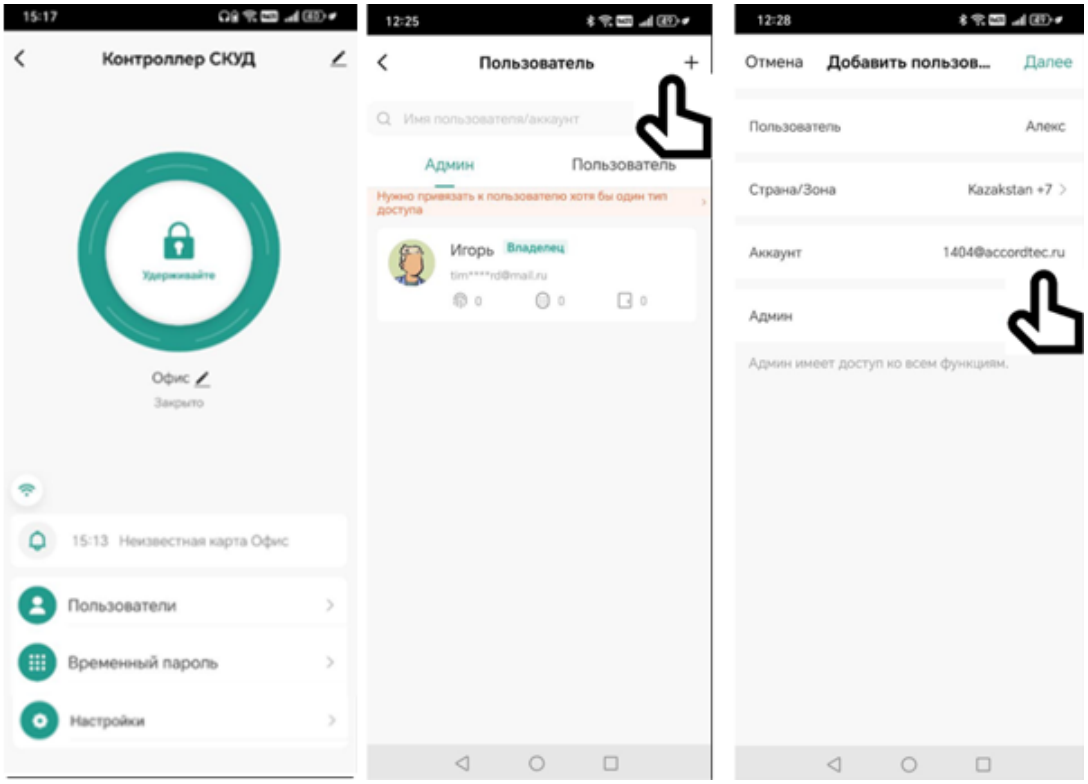
Для управления пользователями зайдите в соответствующее подменю. В системе предусмотрено 3 категории Пользователей с разными правами, описание которых представлено в таблице.

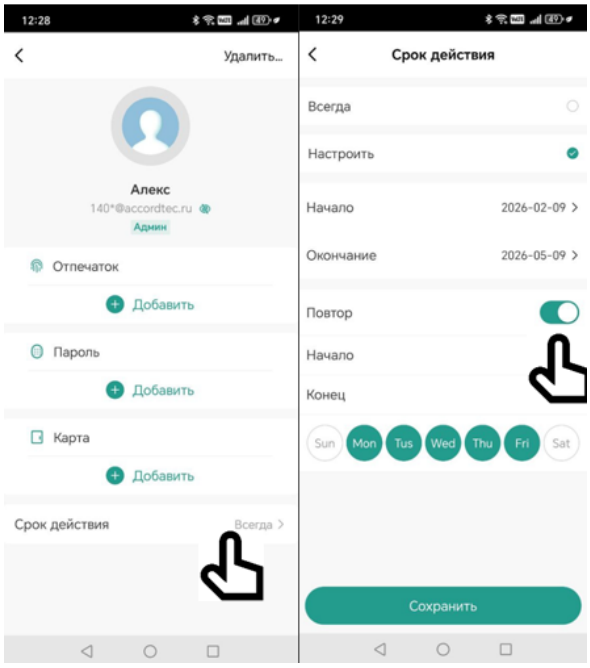
	Владелец	Администратор	Обычный пользователь
Разблокировка запирающего механизма	ν	ν	ν
Управление обычными пользователями	ν	ν	×
Назначение администраторов	ν	×	×
Просмотр журнала	ν	ν	×
Настройка времени задержки реле	ν	ν	×

Примечание: Владельцем устройства автоматически считается **Пользователь**, который добавил устройство в **Приложение**.

5.2.1. Добавление пользователей

Для добавления нового пользователя нажмите «**+**» в правом верхнем углу дисплея. Далее укажите имя, страну и электронную почту. По умолчанию пользователь имеет постоянный доступ, то есть имеет неограниченный срок действия всех идентификаторов.





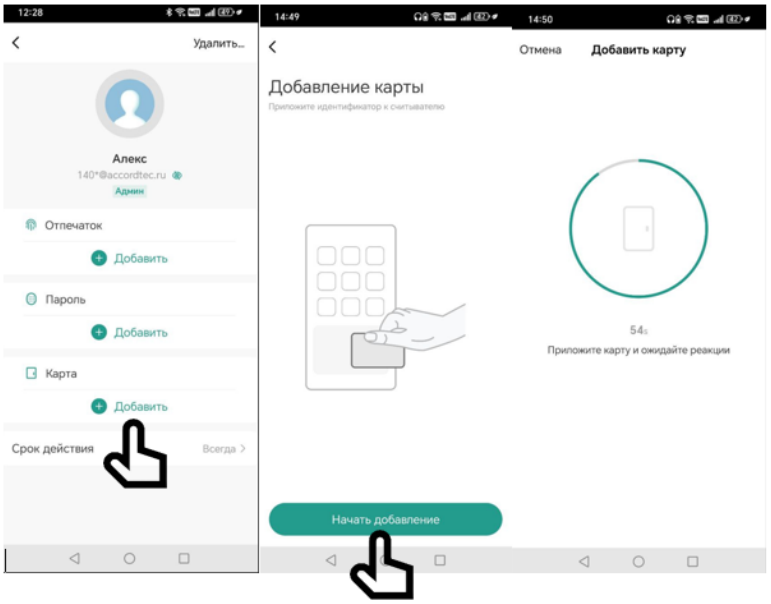
При необходимости можно ограничить время действия идентификаторов для каждого пользователя индивидуально. Для этого необходимо выбрать пользователя и далее нажать на поле Срок действия. После этого выбрать Настроить. Далее необходимо выбрать даты начала и окончания действия идентификаторов. Также опционально можно ограничить действие идентификаторов по времени, активировав функцию Повтор, указав время начала и окончания по определенным дням недели.

Sun – Воскресенье
Mon – Понедельник
Tus – Вторник
Wed – Среда
Thu – Четверг
Fri – Пятница
Sat – Суббота

Примечание: Функция добавления/удаления отпечатков через приложение не доступана для данного устройства.

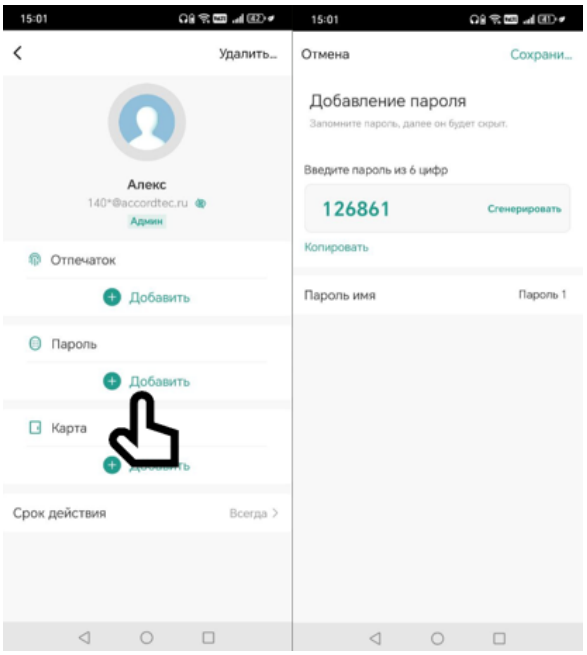
5.2.2. Добавление RFID-ключа

Для добавления RFID-ключа выберите или создайте **Пользователя**, которому будет присвоен идентификатор. Далее нажмите **Начать добавление** и приложите RFID-ключ к считывателю.



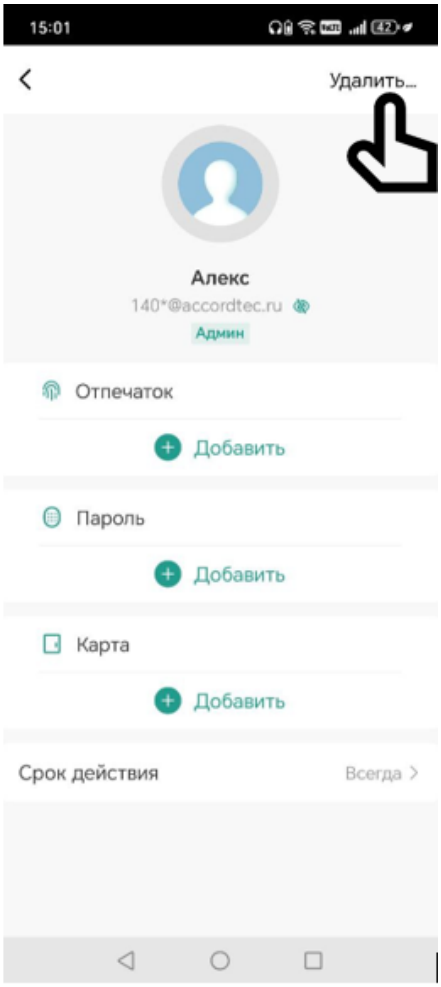
5.2.3. Добавление пароля

Для добавления пароля выберите или создайте **Пользователя**, которому он будет присвоен. Далее введите или сгенерируйте пароль и задайте ему имя. По окончании нажмите **Сохранить**.



5.2.4. Удаление пользователя

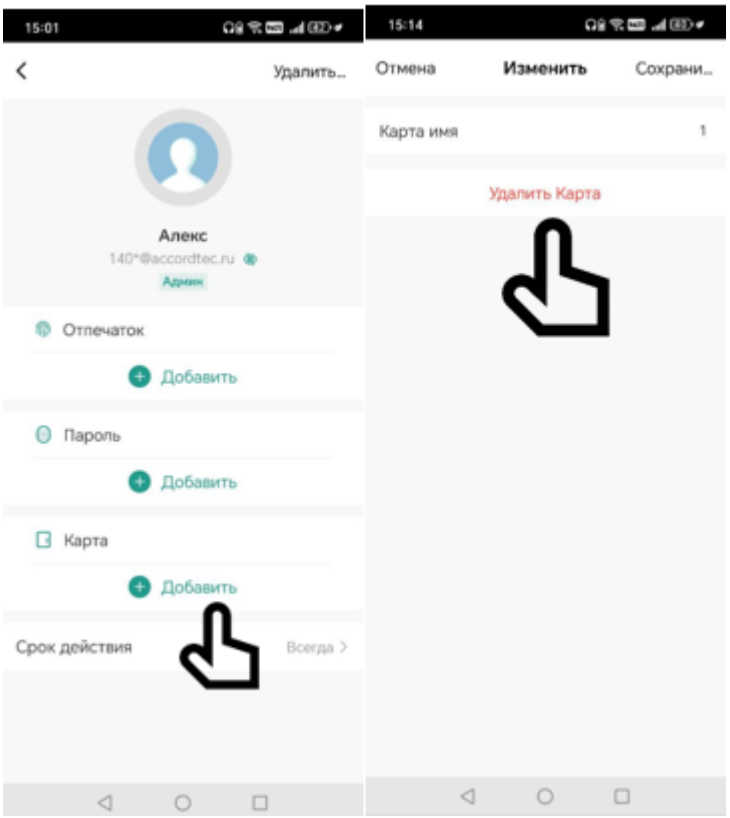
Для удаления **Пользователя** выберите его из списка и нажмите **Удалить** в правом верхнем углу.



Примечание: при удалении определенного **Пользователя** будут удалены все присвоенные ему идентификаторы и пароли.

5.2.5. Удаление RFID -ключей и паролей

Для удаления RFID-ключа/пароля выберите его в карточке **Пользователя**, а затем нажмите **Удалить** в правом верхнем углу дисплея.



Примечание: Функция добавления/удаления отпечатков через **Приложение** недоступно для данного устройства.

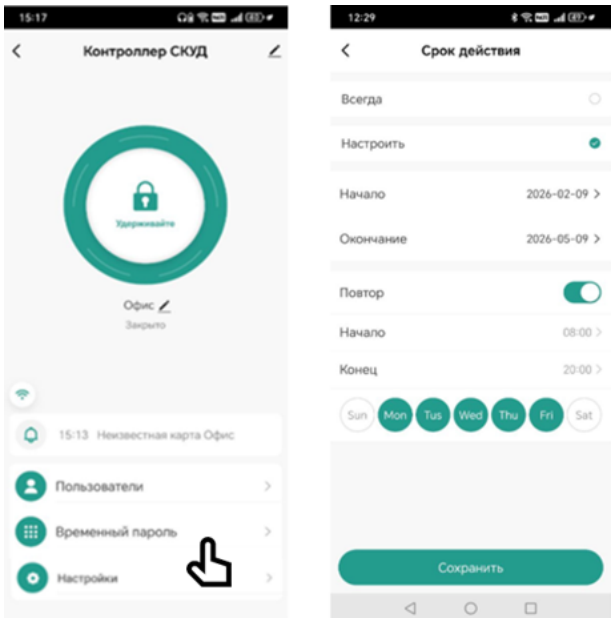
5.3. Временный пароль

Временный пароль используется для разового или многоразового гостевого доступа. Существует два типа временных паролей:

Регулярный – пароль, время действия которого может быть ограничено по дате, времени и дням недели.

Одноразовый – пароль, который можно использовать только один раз.

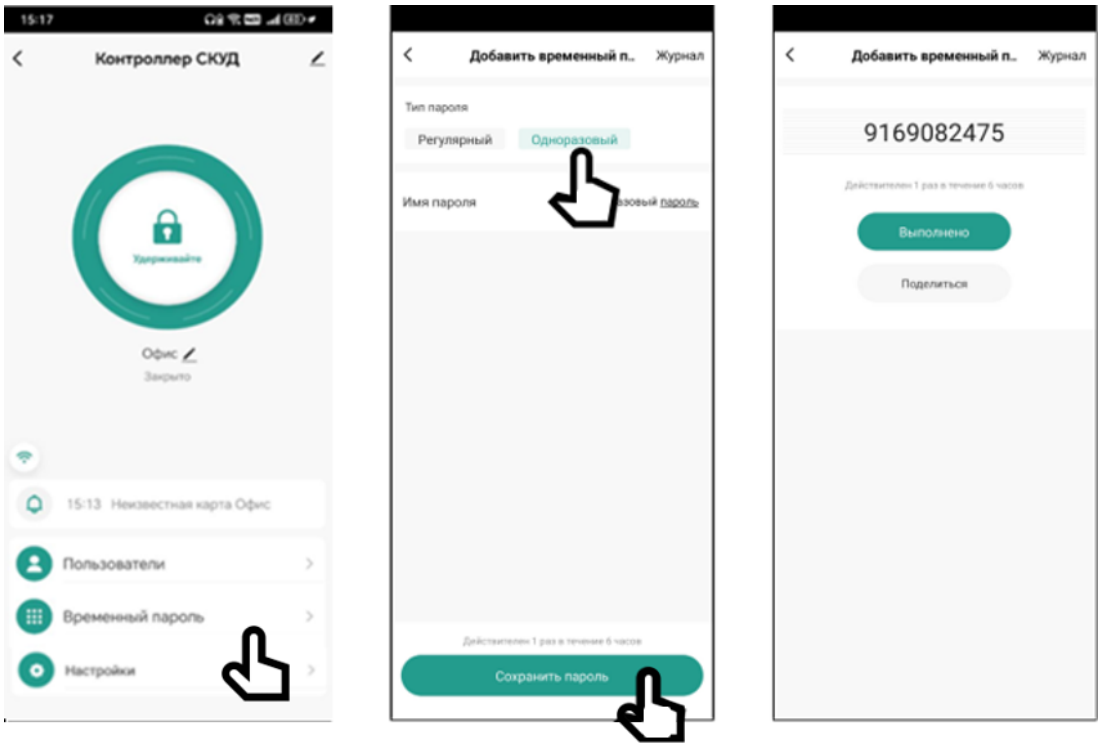
1. Для активации регулярного пароля сначала выберите его тип. Далее введите или сгенерируйте сам пароль и задайте сроки его действия. Также опционально можно ограничить действие регулярного пароля по времени, активировав функцию Повтор, указав время начала и окончания по определенным дням недели.



Sun – Воскресенье
Mon – Понедельник
Tus – Вторник
Wed – Среда
Thu – Четверг
Fri – Пятница
Sat – Суббота

Примечание: Регулярный пароль может быть изменен или удален в период времени своего действия из списка всех паролей.

2. Для выдачи одноразового пароля выберите его тип, задайте имя и нажмите **Сохранить пароль.** Затем автоматически будет сгенерирован пароль, который можно будет использовать только один раз в течение 6 часов.



5.4. Настройки

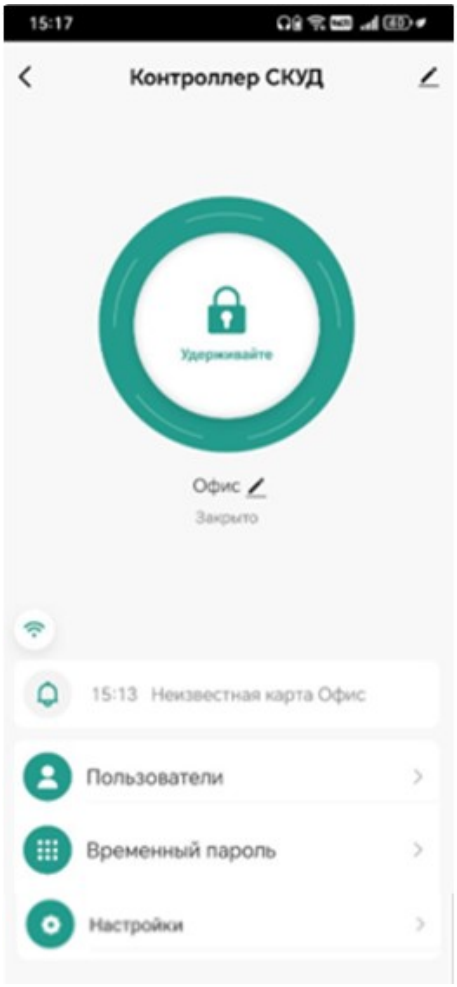
Разблокировка из Приложения – включение/отключение управления запирающим механизмом через приложение. По умолчанию отключено. При активации удаленного управления предоставляется возможность выбора группы пользователей для управления запирающим механизмом (Администратор/ Пользователь).

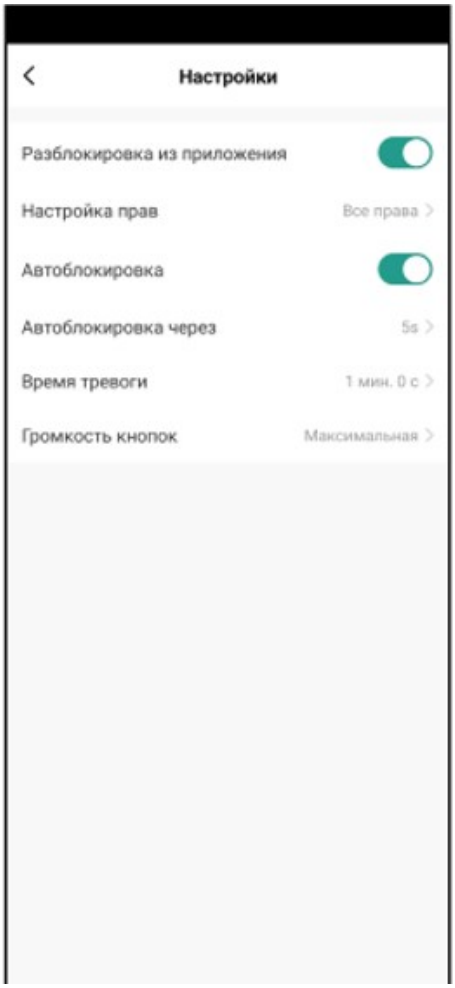
Автоблокировка – настройка режима работы реле для управления запирающим механизмом. По умолчанию автоблокировка включена, то есть реле работает в импульсном режиме и меняет положение якоря на заданное ниже время. При отключенной настройке, реле работает в триггерном режиме и меняет свое положение при каждом проходе.

Автоблокировка через – настройка времени работы реле от 0 до 100 сек. для импульсного режима. По умолчанию 5 сек. При отключении импульсного режима настройка скрывается.

Время тревоги–время, в течение которого будет активирована тревога от 1 до 3 мин. По умолчанию установлена 1 мин.

Громкость кнопок – настройка громкости зуммера при нажатии кнопок на ПДУ (Без звука/Тихий/Нормальный/Громкий).

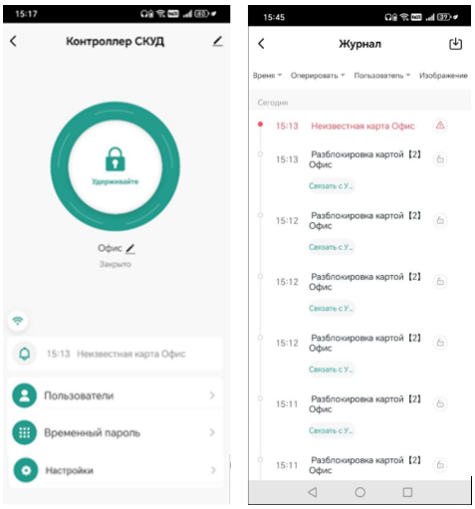




Примечание: Приложении необходимо активировать настройку **Разблокировка** из приложения для управления запирающим механизмом.

5.5. Журнал

В журнале отображаются все события, происходящие в системе. В верхней части журнала расположены фильтры, с помощью которых можно отфильтровать события по времени, типу операций и пользователям. Благодаря фильтру по пользователям можно проследить, когда человек первый и последний раз использовал устройство, то есть сделать примитивный учет рабочего времени.

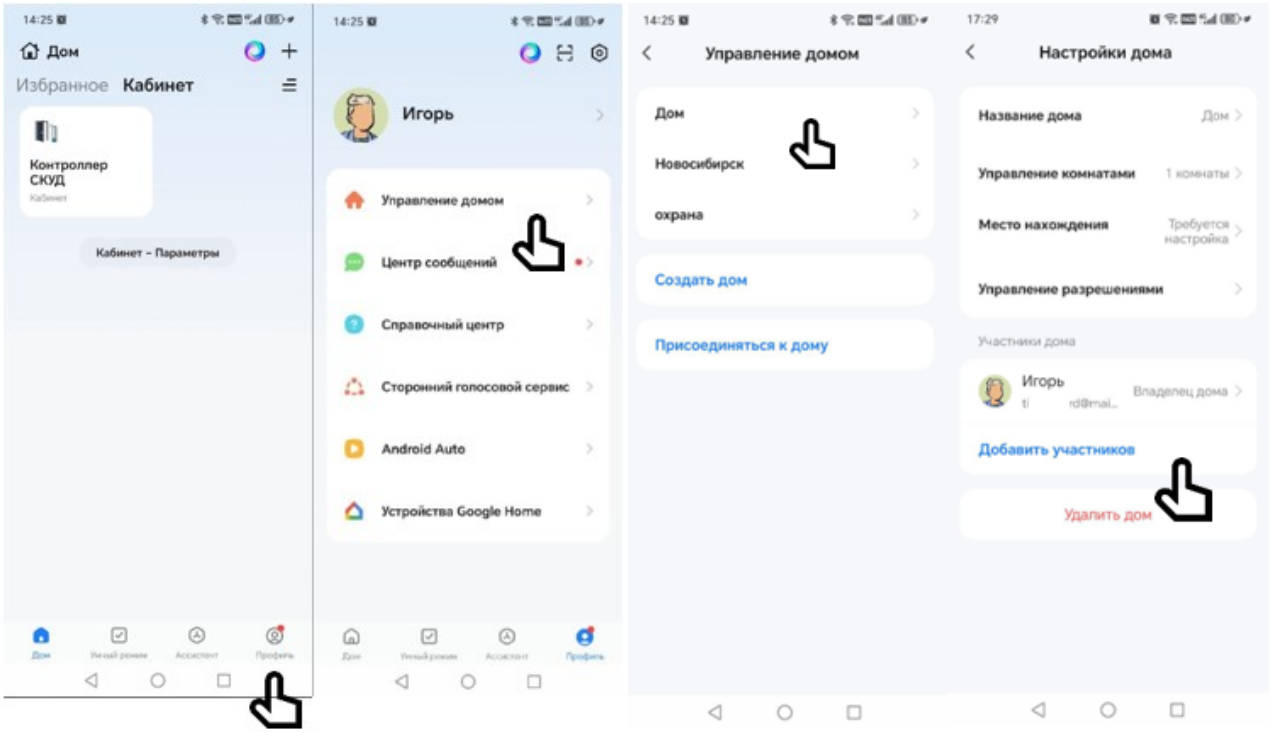


5.6. PUSH-уведомления при звонке

На контроллере AT-AC1000 WIFI реализована возможность подключения кнопки (см. схему подключения), при нажатии на которую приложение получит PUSH-уведомление, с помощью которого можно перейти в главное меню устройства и разблокировать запирающий механизм. Информация о нажатии кнопки также будет отображаться в списке устройств под названием соответствующего контроллера.

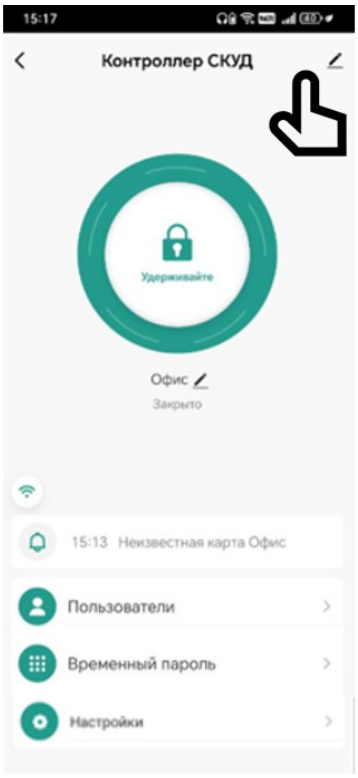
5.7. Общий доступ к устройству

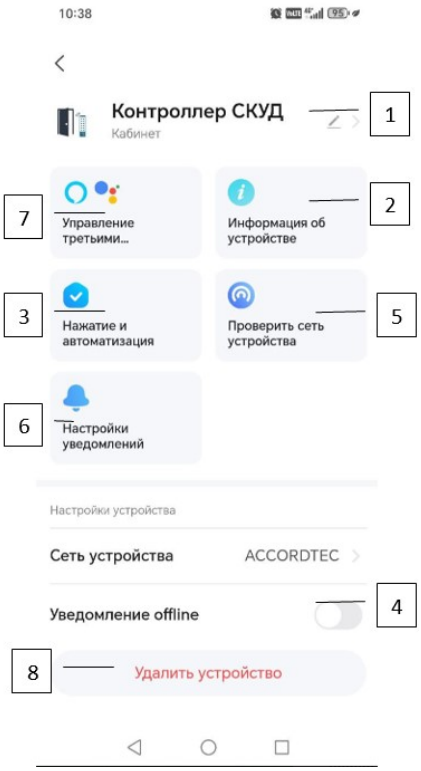
Для предоставления доступа к устройству другим пользователям зайдите в свой **Профиль** и выберите пункт **Управление домом**. Выберите предварительно созданный дом и добавьте нового участника. Следует отметить, что новый участник должен иметь свой зарегистрированный аккаунт в приложении, а также должен быть добавлен в меню Пользователи для устройства, к которому предполагается предоставить общий доступ.



5.8. Сервис и удаление устройства

Для просмотра информации об устройстве, доступа к некоторым сервисным функциям, а также удаления устройства из аккаунта выберите значок карандаша в правом верхнем углу главного меню устройства.





1. Изменение имени устройства и его расположения.
2. В данном пункте содержится информация: Виртуальный ID (он же Cloud ID, Product ID) IP-адрес MAC-адрес Часовой пояс
3. Сценарии автоматизации.
4. Активация уведомлений, если устройство отключено от сети более чем на 30 мин.
5. Проверка качества беспроводного соединения с Wi- Fi точкой доступа.
6. Настройка уведомлений.
7. Создание группы
8. Удаление устройства из аккаунта.

Сведения о сертификации

Изделие соответствует требованиям технических регламентов Таможенного союза ТР ТС 020/2011 и ТР ТС 004/2011

Правила хранения и транспортировки

Хранение изделия в потребительской таре должно соответствовать условиям хранения 1 по ГОСТ. В помещениях для хранения изделия не должно быть паров кислот, щёлочи, агрессивных газов и других вредных примесей, вызывающих коррозию. Устройства в транспортной таре перевозятся любым видом крытых транспортных средств (в железнодорожных вагонах, закрытых автомашинах, трюмах и отсеках судов, герметизированных отапливаемых отсеках самолетов и т.д.) в соответствии с требованиями действующих нормативных документов.

Утилизация

Изделие утилизировать как бытовую технику без принятия специальных мер защиты окружающей среды.

Техническое обслуживание

Техническое обслуживание изделия должно проводиться не реже одного раза в год электромонтерами, имеющими группу по электробезопасности не ниже 3.

Ежегодные работы по техническому обслуживанию включают:

а) проверку работоспособности изделия, согласно инструкции по монтажу;

б) проверку целостности корпуса изделия, надёжности креплений, контактных соединений;

в) очистку корпуса изделия от пыли и грязи.

Гарантийные обязательства и техническая поддержка

Изготовитель гарантирует соответствие изделия требованиям эксплуатационной документации при соблюдении потребителем правил транспортирования, хранения, монтажа и эксплуатации. Средний срок службы изделия – не менее 5 лет.

Предприятие-изготовитель гарантирует работу изделия в течение 38 месяцев с момента продажи.

При отсутствии документа, подтверждающего факт приобретения, гарантийный срок исчисляется от даты производства.

Гарантийные обязательства считаются недействительными, если причиной выхода изделия из строя явились:

механическое повреждение корпуса; электрический пробой входного/выходного каскада; ошибка при установке.

В случае появления неисправности или некорректной работы изделия свяжитесь с нашей службой техподдержки по телефонам 8(495)-223-01-00, 8(800)7700415 или по электронной почте support@accordsb.ru .

Сервисный отдел компании АккордТек находится по адресу: 127410, г. Москва, Алтуфьевское шоссе, дом 41А, стр. 2, пом.22.

Производитель не гарантирует, что изделие будут работать должным образом с оборудованием других производителей, и не дает гарантий и представлений, подразумеваемых или выраженных, относительно качества, рабочих характеристик, или работоспособности изделия при использовании его для целей, не предусмотренных производителем. Производитель старался сделать этот документ наиболее точным и полным, и, тем не менее, он отказывается от ответственности за любые опечатки или пропуски, которые, возможно, произошли. Информация в любой части данного документа изменяется без предварительного уведомления. Производитель не берет на себя никакой ответственности за любые неточности, которые могут содержаться в этом документе и не берет на себя ответственности и не гарантирует выпуска обновлений или сохранения без изменений, какой-либо информации в настоящем документе, и оставляет за собой право производить изменения в этом документе и/или в изделиях, описанных в данном документе, в любое время без уведомления. При обнаружении ошибок, опечаток или неточностей в данном документе, пожалуйста, сообщите об этом в службу технической поддержки.