

novicam

КОНТРОЛЛЕРЫ СКУД  
SB310 WIFI

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Пользователь системы ответственен за соблюдение всех положений действующего законодательства в отношении мониторинга и записи видео- и аудиосигнала. Novicam™ не несет ответственности за нарушение требований закона и иных правовых актов в процессе эксплуатации системы.

## МЕРЫ ПРЕДОСТОРОЖНОСТИ

- Прежде чем начать работу с устройством, внимательно ознакомьтесь с Руководством Пользователя.
- Не разбирайте устройство, это может привести к его неправильному функционированию или поломке и сделает гарантию недействительной.
- Все электрические контакты соединяйте в полном соответствии с бирками и инструкциями, указанными в данном Руководстве.
- В противном случае Вы можете нанести изделию непоправимый ущерб и, тем самым, также сделать гарантию недействительной.
- Не эксплуатируйте устройство в условиях, если температура, показатели влажности и технические характеристики источника питания превышают установленные значения для данного прибора.
- Не используйте для протирки изделия бензин, спирт или другие растворители, т.к. они могут повредить поверхность. Для чистки используйте мягкую сухую ткань.



### ВНИМАНИЕ!

Производитель оставляет за собой право без уведомления Потребителя вносить изменения в конструкцию изделия, технические характеристики и комплектацию для улучшения их технологических и эксплуатационных параметров.

## **УВАЖАЕМЫЙ ПОКУПАТЕЛЬ!**

Поздравляем Вас с покупкой! Мы делаем все возможное, чтобы наша продукция удовлетворяла Вашим запросам.

Перед началом эксплуатации изделия ознакомьтесь внимательно с Руководством Пользователя и с Условиями гарантийного обслуживания.

**Контроллеры СКУД**  
**Модели: SB310 WIFI**

<b>ОПИСАНИЕ</b>	<b>5</b>	2.3. Добавление гостевых Пользователей	30	<b>ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ</b>	<b>64</b>
Контроллер СКУД SB310 WIFI	5	2.4. Добавление блокирующего Пользователя	31	Транспортировка и хранение	64
Описание контактов	7	2.5. Удаление Пользователей	32	Утилизация	65
Индикация	8	2.6. Добавление   Удаление Пользователей Мастер-картой	33	<b>ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА</b>	<b>66</b>
<b>ОСНОВНЫЕ ОСОБЕННОСТИ</b>	<b>9</b>	2.7. Режим АССЕРТ	34	Гарантийные обязательства	66
<b>КОМПЛЕКТАЦИЯ</b>	<b>10</b>	2.8. Передача Базы данных на другое устройство	35	Условия гарантийного обслуживания	67
<b>УСТАНОВКА И ПОДКЛЮЧЕНИЕ</b>	<b>11</b>	3. Типовые операции	36		
Общие рекомендации по установке	11	4. Начало работы с Приложением	37		
Установка контроллера	12	4.1. Установка Приложения	37		
Схемы подключения	13	4.2. Регистрация аккаунта	38		
<b>ПРОГРАММИРОВАНИЕ И ЭКСПЛУАТАЦИЯ</b>	<b>17</b>	4.3. Добавление устройства в Приложение	39		
1. Базовые настройки	17	5. Работа в Приложении	44		
1.1. Режим программирования (РП)	17	5.1. Описание Главного меню устройства	45		
1.2. Изменение Мастер-пароля	17	5.2. Подменю Пользователи	46		
1.3. Выбор режима работы	18	5.2.1. Добавление Пользователей	47		
1.4. Настройка параметров реле	19	5.2.2. Добавление RFID-ключа	49		
1.5. Настройка параметров входа Wiegand	20	5.2.3. Добавление Пароля	50		
1.6. Настройка индикации	21	5.2.4. Удаление Пользователя	51		
1.7. Функция предотвращения несанкционированного доступа	22	5.2.5. Удаление RFID-ключей и Паролей	52		
1.8. Детекция открытия силой	23	5.3. Временный Пароль	53		
1.9. Режим шлюза	24	5.4. Настройки	55		
1.10. Возврат к заводским настройкам и добавление Мастер-карты	25	5.5. Журнал	56		
1.11. Удаление устройства из аккаунта Приложения	26	5.6. PUSH-уведомление при звонке	58		
2. Работа с Пользователями	27	5.7. Общий доступ к устройству	59		
2.1. Добавление обычных Пользователей	28	5.8. Сервис и удаление устройства	61		
2.2. Добавление тревожных Пользователей	29	<b>СПЕЦИФИКАЦИИ</b>	<b>62</b>		

# ОПИСАНИЕ

## КОНТРОЛЛЕР СКУД SB310 WIFI

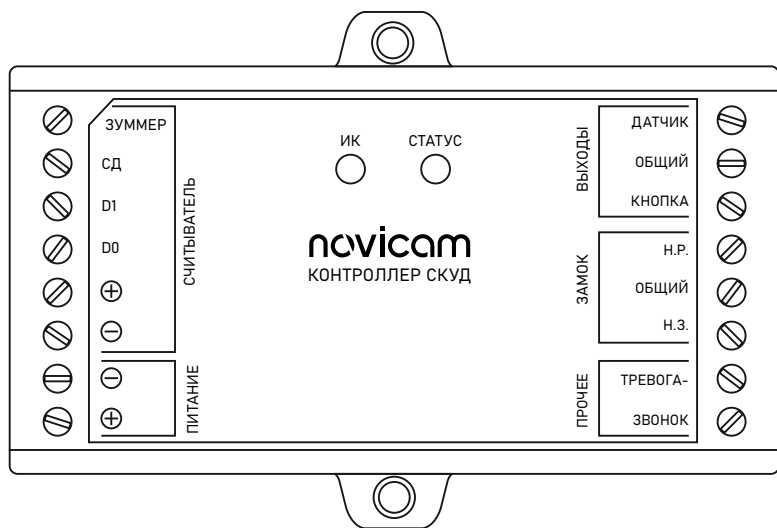


Рис. 1 Внешний вид контроллера

Программируемый контроллер **Novicam™ SB310 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.

Контроллер **SB310 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 недоступных местах.

# ОПИСАНИЕ

## КОНТРОЛЛЕР СКУД SB310 WIFI

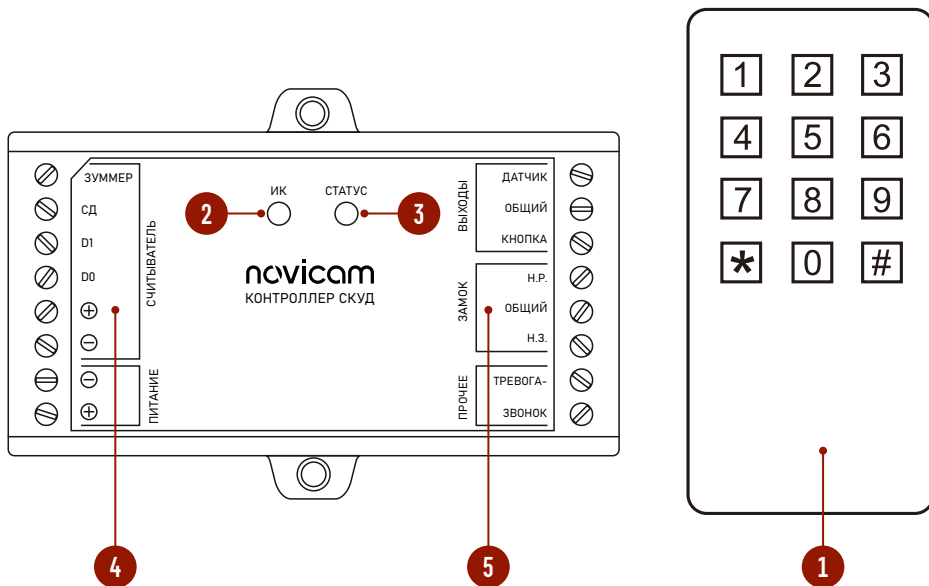


Рис. 2 Контроллер SB310 WIFI и ПДУ

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

Обозначение	Описание	
<b>ЛЕВАЯ КЛЕММНАЯ КОЛОДКА</b>		
Считыватель	Зуммер	Управление зуммером на подключенных считывателях
	СД	Управление светодиодом на подключенных считывателях
	D1	Интерфейс Wiegand (вход) для подключения считывателей
	D0	
	⊕	«+» для питания считывателей
	⊖	Общий контакт «-» для считывателей
Питание	⊖	Общий контакт. «-» контакт для подключения блока питания
	⊕	«+» для подключения блок питания
<b>ПРАВАЯ КЛЕММНАЯ КОЛОДКА</b>		
Входы	Датчик	Н.З. контакт для подключения датчика двери (геркона)
	Общий	Общий контакт для подключения датчика двери и кнопки выхода
	Кнопка	Контакт для подключения кнопки выхода с Н.Р. контактами
Замок	Н.Р.	Нормально-разомкнутый контакт реле («мокрый»/«сухой») для подключения электромеханического замка
	Общий	Общий контакт реле для подключения замка
	Н.З.	Нормально-замкнутый контакт реле («мокрый»/«сухой») для подключения электромагнитного замка
Прочее	Тревога	Контакт для подключения исполнительного устройства (сирены)
	Звонок	Контакт для подключения кнопки звонка

Состояние	Светодиод	Зуммер
Режим ожидания	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

- Поддержка до 1000 Пользователей
- Поддержка до 2 считывателей с интерфейсом Wiegand
- Настройка, управление, администрирование, выдача временных паролей в Приложении **Smart Life | Tuya Smart**
- Поддержка всех типов электрозамков
- Работа в режиме шлюза
- Тревожные вход/выход
- Корпус из ABS-пластика

- Контроллер – 1 шт.
- Пульт дистанционного управления (ПДУ) – 1 шт.
- Защитный диод 1N4004– 1 шт.
- Крепежный комплект – 1 шт.
- EM-Margin Мастер-карта – 1 шт.
- Паспорт и гарантийный талон – 1 шт.



#### **ВНИМАНИЕ!**

Перед подключением внимательно ознакомьтесь с Руководством Пользователя.

# УСТАНОВКА И ПОДКЛЮЧЕНИЕ

## ОБЩИЕ 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 Н.Р./Н.З. подаётся/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 "ДАТЧИК" и "ОБЩИЙ".
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.

# УСТАНОВКА КОНТРОЛЛЕРА

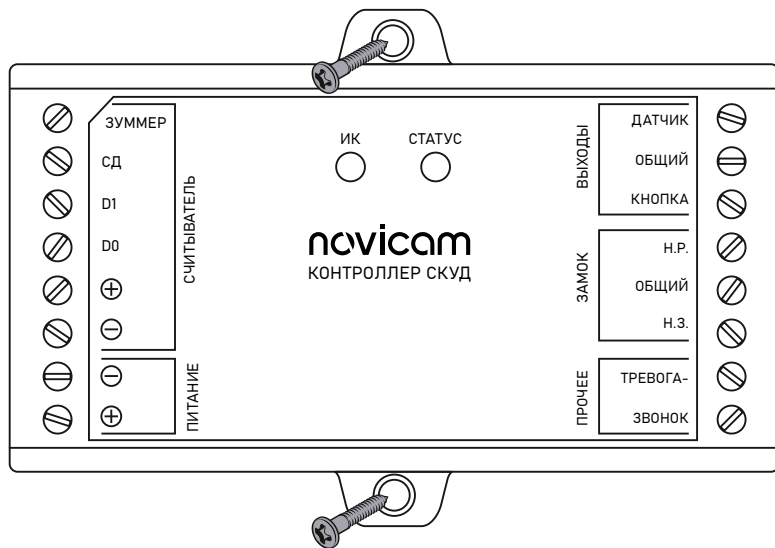


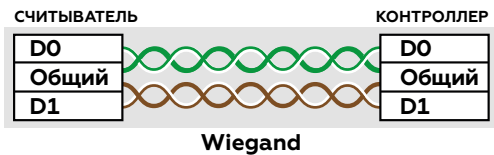
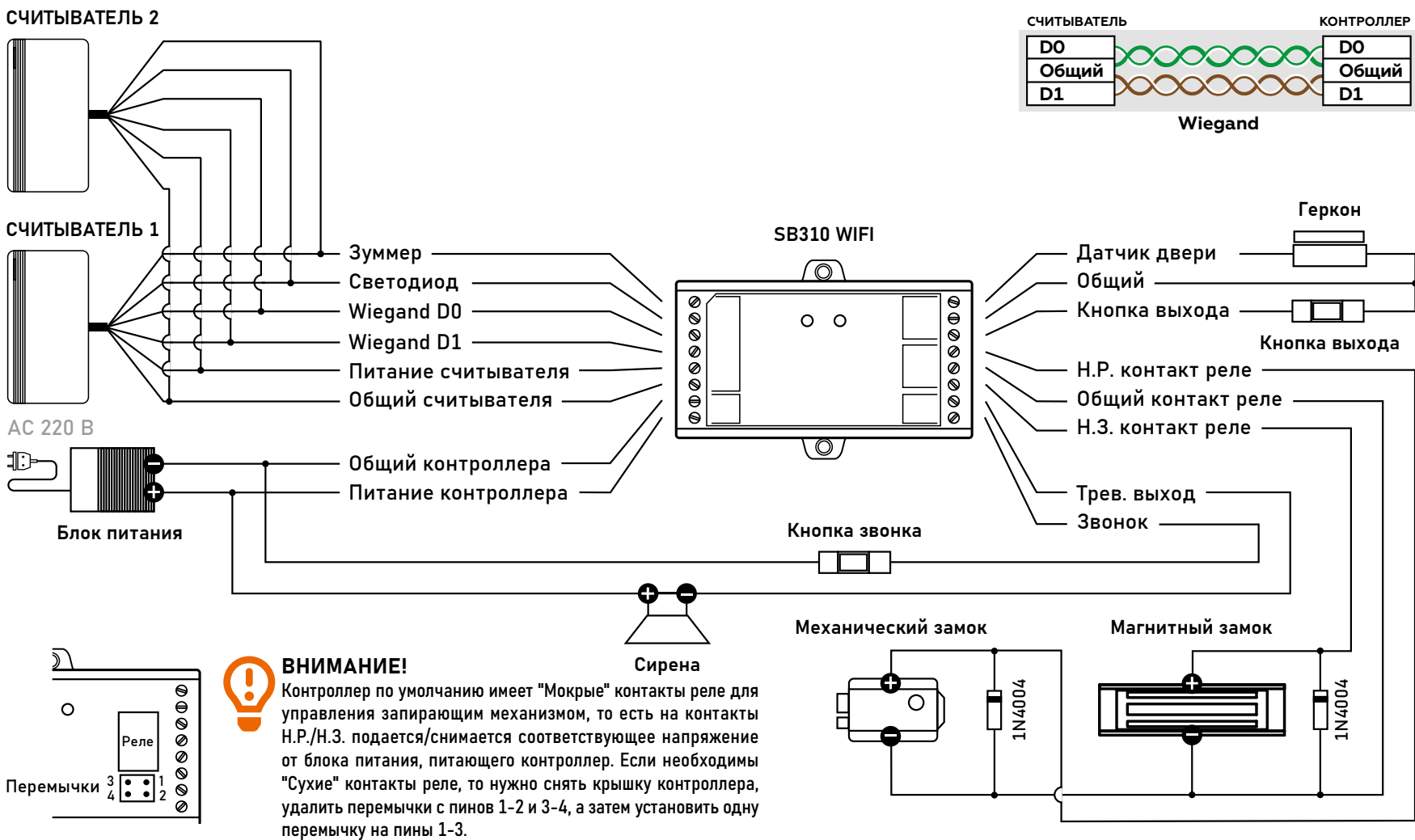
Рис. 3 Монтаж контроллера

1. В соответствии с рисунком слева 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 отвёртки.
4. Если это необходимо, поменяйте тип контактов реле для управления запирающим механизмом. Контроллер по умолчанию имеет "мокрые" контакты реле, то есть на контакты Н.Р./Н.З. подаётся/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



## ВНИМАНИЕ!

1. Контакты **Светодиод** и **Зуммер** являются опциональными. Подключать их необязательно.
2. При использовании витой пары для подключения считывателя к контроллеру по интерфейсу Wiegand правильное подключение предполагает использование 2 витых пар: одной для D0/Общий, второй для D1/Общий. При других подключениях считыватель может не передавать корректно данные на контроллер.



## ВНИМАНИЕ!

Контроллер по умолчанию имеет "Мокрые" контакты реле для управления запирающим механизмом, то есть на контакты Н.Р./Н.З. подается/снимается соответствующее напряжение от блока питания, питающего контроллер. Если необходимы "Сухие" контакты реле, то нужно снять крышку контроллера, удалить переключки с пинов 1-2 и 3-4, а затем установить одну переключку на пины 1-3.

Рис. 4 Схема подключения контроллера по умолчанию с "мокрыми" контактами реле

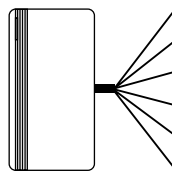


## ВНИМАНИЕ!

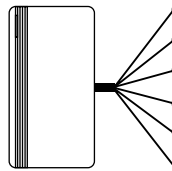
1. Параллельно замку в обратной полярности рекомендуется установить защитный диод 1N4004 (входит в комплект поставки), если конструкцией замка он не предусмотрен.
2. Если датчик двери (геркон) не используется, то для правильного отображения состояния двери в Приложении рекомендуется сделать переключку между контактами **ДАТЧИК** и **ОБЩИЙ**.

# СХЕМЫ ПОДКЛЮЧЕНИЯ

СЧИТЫВАТЕЛЬ 2

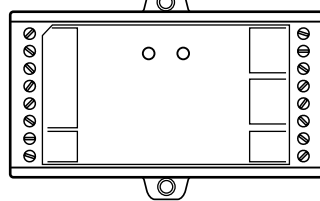


СЧИТЫВАТЕЛЬ 1



Зуммер  
Светодиод  
Wiegand D0  
Wiegand D1  
Питание считывателя  
Общий считывателя

SB310 WIFI



Датчик двери  
Общий  
Кнопка выхода  
Н.Р. контакт реле  
Общий контакт реле  
Н.З. контакт реле  
Трев. выход  
Звонок

Геркон

Кнопка выхода

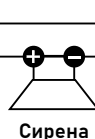
АС 220 В



Блок питания

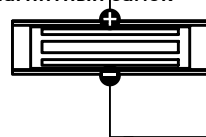
Общий контроллера  
Питание контроллера

Кнопка звонка

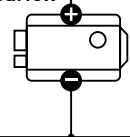


Сирена

Магнитный замок

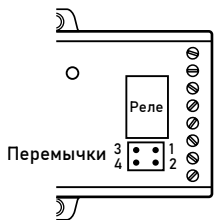


Мех.замок



АС 220 В

Блок питания замка



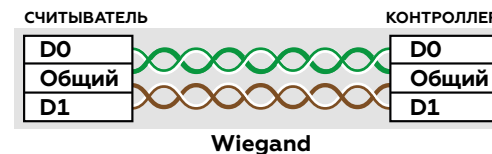
## ВНИМАНИЕ!

Для работы контроллера по данной схеме необходимы "Сухие" контакты реле. Для этого нужно снять перемычки с пинов 1-2 и 3-4, а затем установить на пины 1-3.



## ВНИМАНИЕ!

1. Контакты Светодиод и Зуммер являются опциональными. Подключать их необязательно.
2. При использовании витой пары для подключения считывателя к контроллеру по интерфейсу Wiegand правильное подключение предполагает использование 2 витых пар: одной для D0/Общий, второй для D1/Общий. При других подключениях считыватель может не передавать корректно данные на контроллер.



## ВНИМАНИЕ!

1. Параллельно замку в обратной полярности рекомендуется установить защитный диод 1N4004 (входит в комплект поставки), если конструкцией замка он не предусмотрен.
2. После подключения по данной схеме убедитесь, что перемычка установлена на пины 1-3.
3. Если датчик двери (геркон) не используется, то для правильного отображения состояния двери в Приложении рекомендуется сделать перемычку между контактами ДАТЧИК и ОБЩИЙ.

Рис. 5 Схема подключения контроллера с "сухими" контактами реле

# УСТАНОВКА И ПОДКЛЮЧЕНИЕ

## СХЕМЫ ПОДКЛЮЧЕНИЯ

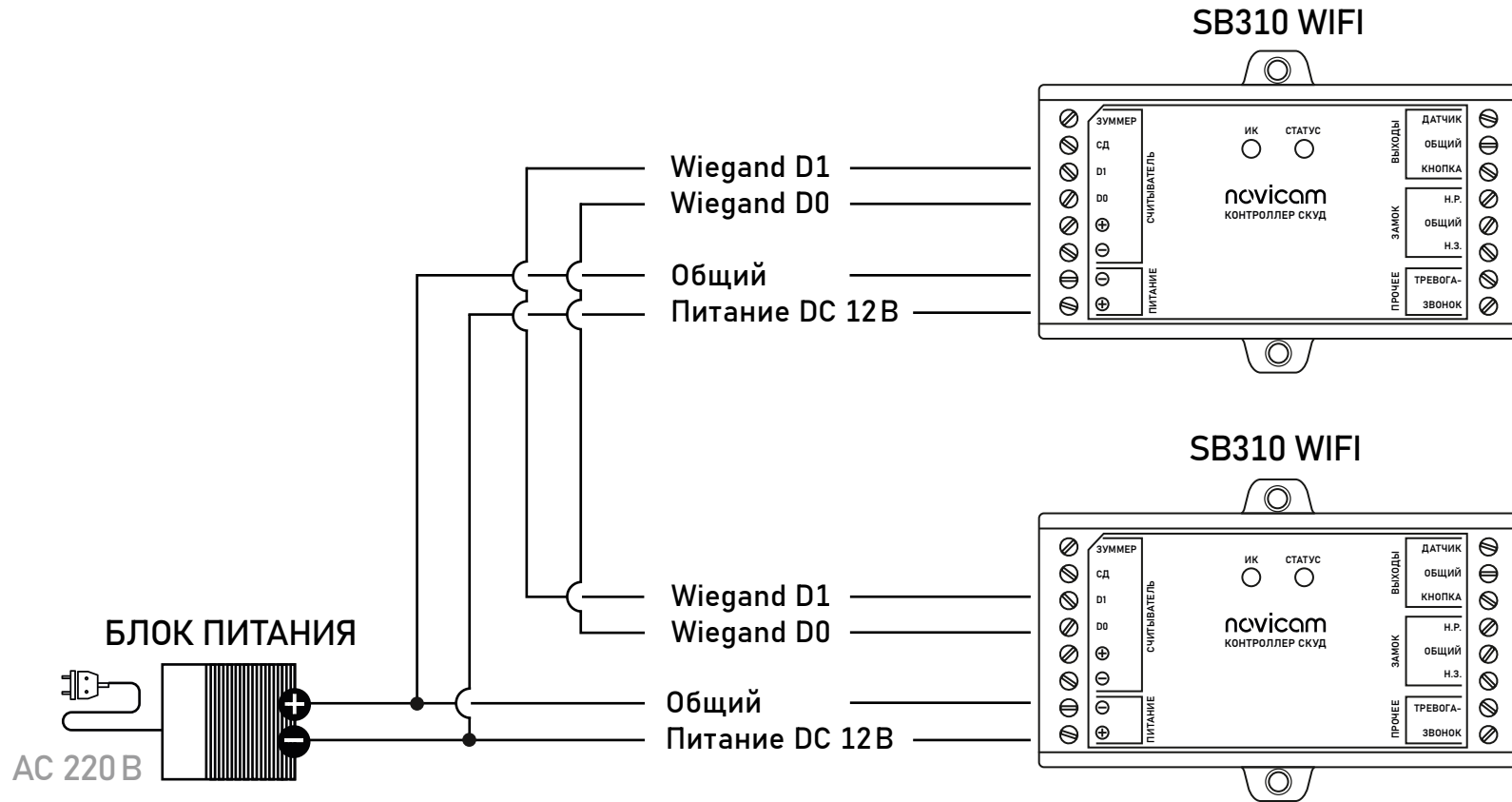


Рис. 6 Схема подключения контроллеров для передачи данных

# УСТАНОВКА И ПОДКЛЮЧЕНИЕ

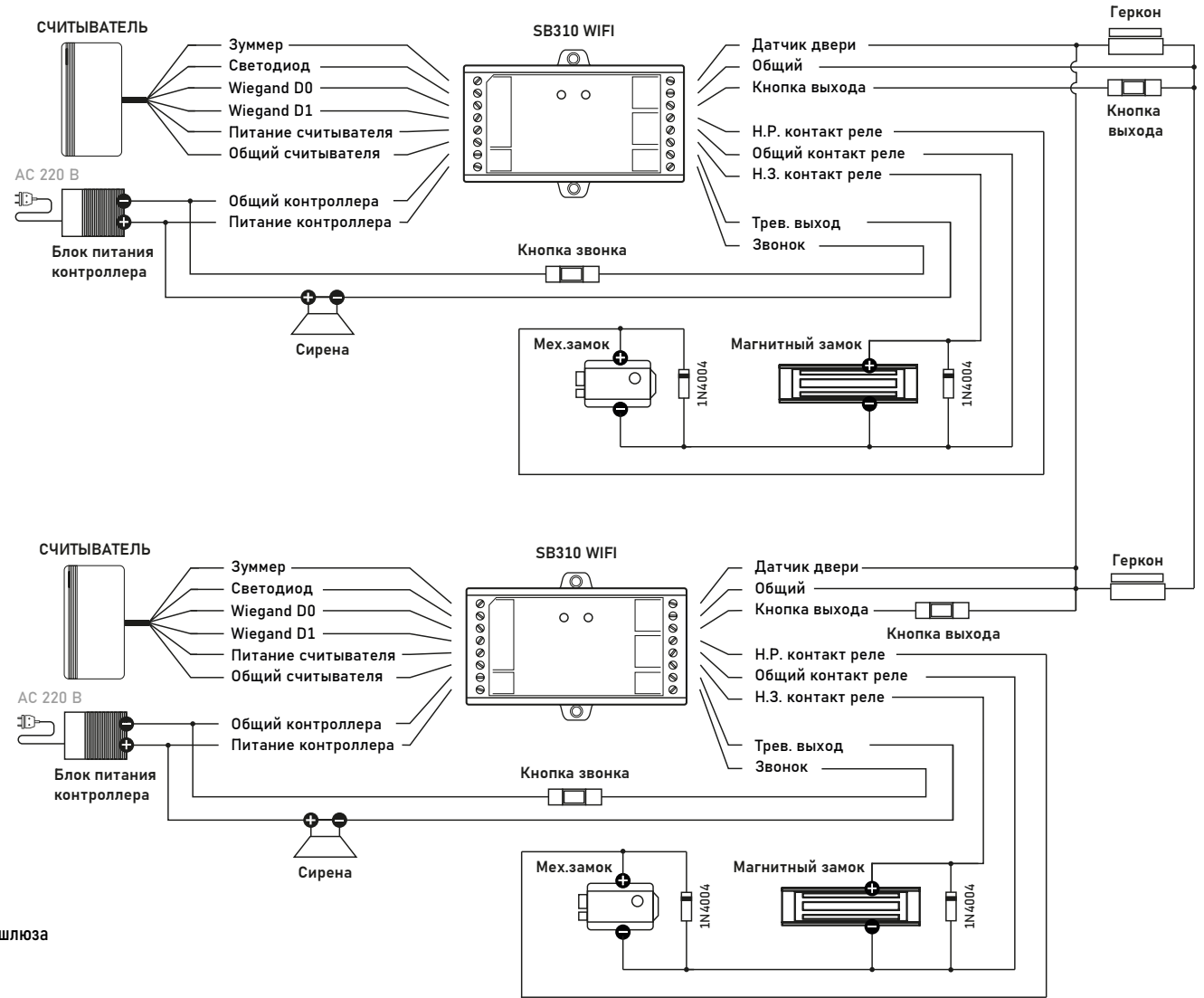


Рис. 7 Схема подключения для работы в режиме шлюза

## 1. БАЗОВЫЕ НАСТРОЙКИ

### 1.1. РЕЖИМ ПРОГРАММИРОВАНИЯ

	Операция	Комбинация
1	Вход в РП	* <b>(Мастер-пароль)</b> # по умолчанию – 123456
2	Выход из РП	*

### 1.2. ИЗМЕНЕНИЕ МАСТЕР-ПАРОЛЯ

	Операция	Комбинация
1	Вход в РП	* <b>(Мастер-пароль)</b> # по умолчанию – 123456
2	Изменение Мастер-пароля	* <b>(Новый Мастер-пароль)</b> # <b>(Повтор нового Мастер-пароля)</b> # Мастер-пароль должен состоять из 6 цифр
3	Выход из РП	*



#### ВНИМАНИЕ!

1. 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.
2. 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.

## 1. БАЗОВЫЕ НАСТРОЙКИ

### 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 груп-

повой доступ по нескольким ключам и/или паролям. То есть доступ будет разрешен при считывании нескольких действительных RFID-ключей и/или паролей в любой комбинации.

	Операция	Комбинация
1	Вход в РП	<b>*(Мастер-пароль)#</b> по умолчанию – 123456
2	Только по RFID-ключам	<b>40#</b> по умолчанию
	Только по паролям	<b>41#</b>
	По RFID-ключам или паролям	<b>43#</b>
	Групповой доступ	<b>43(2-9)#</b> 2-9 — Количество действительных RFID-ключей или паролей
3	Выход из РП	<b>*</b>



#### ВНИМАНИЕ!

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. БАЗОВЫЕ НАСТРОЙКИ

### 1.4. НАСТРОЙКА ПАРАМЕТРОВ РЕЛЕ

Реле имеет два 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 вво-

де 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.

	Операция	Комбинация
1	Вход в РП	<b>*(Мастер-пароль)#</b> по умолчанию - 123456
	Импульсный режим	<b>3(1-99)#</b> 1-99 – время задержки реле от 1 до 99 секунд По умолчанию установлено 5 секунд
	Триггерный режим	<b>30#</b>
2	Выход из РП	<b>*</b>

## 1. БАЗОВЫЕ НАСТРОЙКИ

### 1.5. НАСТРОЙКА ВХОДА WIEGAND

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

	Операция	Комбинация	
1	Вход в РП	<b>* (Мастер-пароль) #</b>	по умолчанию – 123456
2	Битность для EM-Marin считывателя	<b>8(26-44) #</b>	по умолчанию – 26 бит
	Битность для Mifare считывателя	<b>80(26-44, 56, 58) #</b>	по умолчанию – 34 бита
3	Выключить бит четности	<b>80 #</b>	
	Включить бит четности	<b>81 #</b>	по умолчанию
4	Выход из РП	<b>*</b>	

## 1. БАЗОВЫЕ НАСТРОЙКИ

### 1.6. НАСТРОЙКА ИНДИКАЦИИ

При необходимости у устройства можно отключить светодиод и звуковую индикацию, а также подсветку клавиатуры. По умолчанию клавиатура имеет умную подсветку сенсорных кнопок, которая

гаснет по истечении 20 секунд, а активируется при прикосновении к ней. Причем первое прикосновение только активирует подсветку клавиатуры.

	Операция	Комбинация
1	Вход в РП	<b>*(Мастер-пароль)#</b> по умолчанию – 123456
2	Выключить зуммер	<b>70#</b>
	Включить зуммер	<b>71#</b> по умолчанию
3	Выключить светодиод	<b>72#</b>
	Включить светодиод	<b>73#</b> по умолчанию
5	Выход из РП	<b>*</b>



#### ВНИМАНИЕ!

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

## 1. БАЗОВЫЕ НАСТРОЙКИ

### 1.7. ФУНКЦИЯ ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

При активной функции предотвращения несанкционированного доступа (ПНД) после 10 неудачных попыток считывания недействительного RFID-ключа

включается зуммер и на 10 минут блокируется доступ.

По умолчанию функция отключена.

	Операция	Комбинация
1	Вход в РП	<b>*(Мастер-пароль)#</b> по умолчанию – 123456
2	Выключить ПНД	<b>60#</b> по умолчанию
	Включить ПНД	<b>61#</b> Только блокировка доступа на 10 мин. Отключится автоматически по истечении этого времени
	Включить ПНД с установкой длительности тревоги	<b>62#5(0-3)#</b> 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 действительный RFID-ключ или Мастер-карту
3	Выход из РП	<b>*</b>



#### ВНИМАНИЕ!

При активированной функции ПНД разблокировка по кнопке выхода актуальна всегда.

## 1. БАЗОВЫЕ НАСТРОЙКИ

### 1.8. ДЕТЕКЦИЯ ОТКРЫТИЯ СИЛОЙ

Детекция открытия силой требует наличия подключенных к контроллеру датчика двери (геркона) и электромагнитного замка. Если дверь открывается несанкционировано силой, то автома-

тически активируются зуммер и тревожный выход.

По умолчанию функция отключена.

	Операция	Комбинация
1	Вход в РП	<b>* (Мастер-пароль) #</b> по умолчанию – 123456
2	Выключить функцию детекции открытия силой	<b>63 #</b> по умолчанию
	Включить функцию детекции открытия силой с настройкой длительности тревоги	<b>64 # 5 (0-3) #</b> где 0-3 длительность тревоги (по умолчанию 1 мин). Активация зуммера и тревожного выхода. Для отключения можно ввести действительный пароль или Мастер-пароль/считать действительный RFID-ключ или Мастер-карту.
3	Выход из РП	<b>*</b>

## 1. БАЗОВЫЕ НАСТРОЙКИ

### 1.9. РЕЖИМ ШЛЮЗА

С помощью двух 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 (Рис. 7).
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.

	Операция	Комбинация
1	Вход в РП	<b>*(Мастер-пароль)#</b> по умолчанию – 123456
2	Выключить режим шлюза	<b>90#</b> по умолчанию
	Включить режим шлюза	<b>91#</b>
3	Выход из РП	<b>*</b>

## 1. БАЗОВЫЕ НАСТРОЙКИ

### 1.10. ВОЗВРАТ К ЗАВОДСКИМ НАСТРОЙКАМ И ДОБАВЛЕНИЕ МАСТЕР-КАРТЫ

Для возврата к заводским настройкам и добавления новой Мастер-карты:

1. Отключите питание устройства.
2. Зажмите кнопку выхода (замкните контакты КНОПКА и ОБЩИЙ) и включите питание устройства.
3. После 2 звуковых сигналов отпустите кнопку выхода (разомкните контакты КНОПКА и ОБЩИЙ).
4. После того, как светодиод станет **оранжевым**, поднесите к считывателю любой RFID-ключ соответствующий формату считывателя для записи его в качестве Мастер-карты.
5. При успешном возврате к заводским настройкам и записи новой Мастер-карты светодиод станет **красным**.



#### ВНИМАНИЕ!

1. Если Мастер-карту добавлять не нужно, то удерживать кнопку выхода необходимо не менее 5 секунд после 2 звуковых сигналов.
2. Формат Мастер-карты должен соответствовать формату считывателя.
3. При возврате к заводским настройкам информация о Пользователях не удаляется.

## 1. БАЗОВЫЕ НАСТРОЙКИ

### 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 сенсорной клавиатуре.

	Операция	Комбинация
1	Вход в РП	* <b>(Мастер-пароль)</b> # по умолчанию – 123456
2	Удаление из аккаунта	<b>9(Мастер-пароль)</b> #
3	Выход из РП	*

## 2. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

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

Существуют 4 типа Пользователей:

Пользователь	Описание	UserID
<b>Обычный</b>	Разблокирует точку прохода по какому-либо RFID-ключу или паролю	<b>1-986</b>
<b>Блокирующий</b>	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	<b>987</b>
<b>Тревожный</b>	Активирует тревожный выход. Это может быть использовано для интеграции с охранно-пожарными системами	<b>988-989</b>
<b>Гость</b>	Разово или временно разблокирует точку прохода	<b>990-999</b>



### ВНИМАНИЕ!

1. UserID не должен начинаться с нулей!
2. Пароль может состоять из 4–6 цифр.

## 2. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

### 2.1. ДОБАВЛЕНИЕ ОБЫЧНЫХ ПОЛЬЗОВАТЕЛЕЙ

	Операция	Комбинация
1	Вход в РП	<b>* (Мастер-пароль) #</b> по умолчанию – 123456
2	Добавление RFID-ключа с автоматическим присвоением следующего доступного UserID	<b>1 (Чтение ключа) #</b> Можно добавлять все ключи по очереди
	Добавление RFID-ключа по номеру с автоматическим присвоением следующего доступного UserID	<b>1 (8/10/17-значный номер ключа) #</b> Можно добавлять все ключи по очереди
	Добавление RFID-ключа с присвоением определенного UserID	<b>1 (UserID) # (Чтение ключа) #</b>
	Добавление RFID-ключа по номеру с присвоением определенного UserID	<b>1 (UserID) # (8/10/17-значный номер ключа) #</b>
	Групповое добавление	<b>1 (UserID) # (Количество ключей) # (8/10/17-значный номер первого ключа) #</b> Можно добавить сразу все RFID-ключи за один шаг, если их номера последовательны. Операция может занять до 2 минут
3	Добавление пароля с автоматическим присвоением следующего доступного UserID	<b>1 (Пароль) #</b> Можно добавить все пароли по очереди
	Добавление пароля с присвоением определенного UserID	<b>1 (UserID) # (Пароль) #</b>
4	Выход из РП	<b>*</b>



#### ВНИМАНИЕ!

1. Для обычных Пользователей нужно использовать UserID 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. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

### 2.2. ДОБАВЛЕНИЕ ТРЕВОЖНЫХ ПОЛЬЗОВАТЕЛЕЙ

При считывании RFID-ключа или наборе пароля тревожного Пользователя система активирует тревожный выход.

	Операция	Комбинация
1	Вход в РП	* <b>(Мастер-пароль)</b> # по умолчанию – 123456
2	Добавление тревожного RFID-ключа	<b>1(UserID)#(Чтение ключа)#</b>
	Добавление тревожного RFID-ключа по номеру	<b>1(UserID)#(8/10/17-значный номер ключа)#</b>
	Добавление тревожного пароля	<b>1(UserID)#(Пароль)#</b>
3	Выход из РП	*



#### ВНИМАНИЕ!

1. Для тревожных Пользователей нужно использовать UserID 988 и 989.
2. Пароль для активации тревоги может содержать 4–6 цифр.

## 2. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

### 2.3. ДОБАВЛЕНИЕ ГОСТЕВЫХ ПОЛЬЗОВАТЕЛЕЙ

Для гостей предусмотрено 10 UserID, 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.

Операция	Комбинация
1 Вход в РП	<b>*(Мастер-пароль)#</b> по умолчанию – 123456
2 Добавление гостевого RFID-ключа	<b>1(UserID)#(0-9)#(Чтение ключа)#</b> 0-9 количество проходов, где 0 означает 10 проходов
Добавление гостевого RFID-ключа по номеру	<b>1(UserID)#(0-9)#(8/10/17-значный номер ключа)#</b> 0-9 количество проходов, где 0 означает 10 проходов
Добавление гостевого пароля	<b>1(UserID)#(0-9)#(Пароль)#</b> 0-9 количество проходов, где 0 означает 10 проходов
3 Выход из РП	<b>*</b>



#### ВНИМАНИЕ!

1. Для гостевых Пользователей нужно использовать UserID 990 и 999.
2. Гостевой пароль может содержать 4–6 цифр.

## 2. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

### 2.4. ДОБАВЛЕНИЕ БЛОКИРУЮЩЕГО ПОЛЬЗОВАТЕЛЯ

В системе предусмотрен блокирующий Пользователь, к UserID 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.

	Операция	Комбинация
1	Вход в РП	* <b>(Мастер-пароль)</b> # по умолчанию – 123456
2	Добавление блокирующего RFID-ключа	<b>1(UserID)#(Чтение ключа)#</b>
	Добавление RFID-ключа по номеру	<b>1(UserID)#(8/10/17-значный номер ключа)#</b>
	Добавление блокирующего пароля	<b>1(UserID)#(Пароль)#</b>
3	Выход из РП	*



#### ВНИМАНИЕ!

1. Для блокирующего Пользователя нужно использовать UserID 987.
2. Блокирующий пароль может содержать 4–6 цифр.

## 2. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

### 2.5. УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

	Операция	Комбинация
1	Вход в РП	* <b>(Мастер-пароль)#</b> по умолчанию – 123456
2	Удаление по RFID-ключу	<b>2(Чтение ключа)#</b> Можно удалять по очереди
	Удаление по номеру RFID-ключа	<b>2(8/10/17-значный номер ключа)#</b>
	Удаление по паролю	<b>2(Пароль)#</b> Можно удалять по очереди
	Удаление по UserID	<b>2(UserID)#</b>
	Удаление всех Пользователей	<b>2(Мастер-пароль)#</b>
3	Выход из РП	*

## 2. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

### 2.6. ДОБАВЛЕНИЕ | УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЕЙ МАСТЕР-КАРТОЙ

Операция	Действие
<b>Добавление Пользователей</b>	<ol style="list-style-type: none"> <li>1. Считывание Мастер-карты</li> <li>2. Чтение RFID-ключа/ввод пароля. Можно добавлять ключи и пароли по очереди</li> <li>3. Считывание Мастер-карты</li> </ol>
<b>Удаление Пользователей</b>	<ol style="list-style-type: none"> <li>1. Считывание Мастер-карты дважды с максимальным интервалом 5 сек</li> <li>2. Чтение RFID-ключа/ввод пароля Можно добавлять ключи и пароли по очереди</li> <li>3. Считывание Мастер-карты</li> </ol>



#### ВНИМАНИЕ!

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. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

### 2.7. РЕЖИМ АССЕРТ

При активации режима АССЕРТ 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 необходимо отключить.

	Операция	Комбинация
1	Вход в РП	<b>* (Мастер-пароль) #</b> по умолчанию – 123456
2	Выключить режим АССЕРТ	<b>92 #</b> по умолчанию
	Включить режим АССЕРТ	<b>93 #</b>
3	Выход из РП	<b>*</b>

## 2. РАБОТА С ПОЛЬЗОВАТЕЛЯМИ

### 2.8. ПЕРЕДАЧА БАЗЫ ДАННЫХ НА ДРУГОЕ УСТРОЙСТВО

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

	Операция	Комбинация
1	Вход в РП	* (Мастер-пароль) # по умолчанию – 123456
2	Активация передачи базы данных Пользователей	98#
3	Выход из РП	*



#### ВНИМАНИЕ!

1. Устройства, поддерживающие передачу Базу данных Пользователей, должны быть одной модели.
2. Убедитесь, что устройства подключены по соответствующей схеме для передачи Базы данных.
3. Убедитесь, что Мастер-пароли передающего и принимающего устройств совпали.
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 окончании прозвучит 1 звуковой сигнал и светодиод станет красным. Это будет означать, что передача данных успешно завершена.

## 3. ТИПОВЫЕ ОПЕРАЦИИ

	Операция	Действие
1	Проход по RFID-ключу	Чтение действительного RFID-ключа
2	Проход по паролю	Пароль#
3	Отключение тревоги	<ul style="list-style-type: none"><li>▪ Чтение действительного RFID-ключа</li><li>▪ Чтение Мастер-карты</li><li>▪ Мастер-пароль#</li><li>▪ Действительный пароль#</li></ul>

## 4. НАЧАЛО РАБОТЫ С ПРИЛОЖЕНИЕМ

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



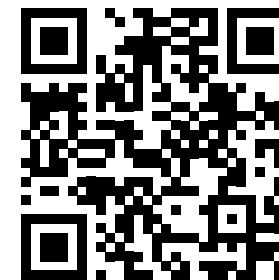
Smart Life

### 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.



Tuya Smart



Приложение  
Smart Life – Smart Living  
для Android & iOS

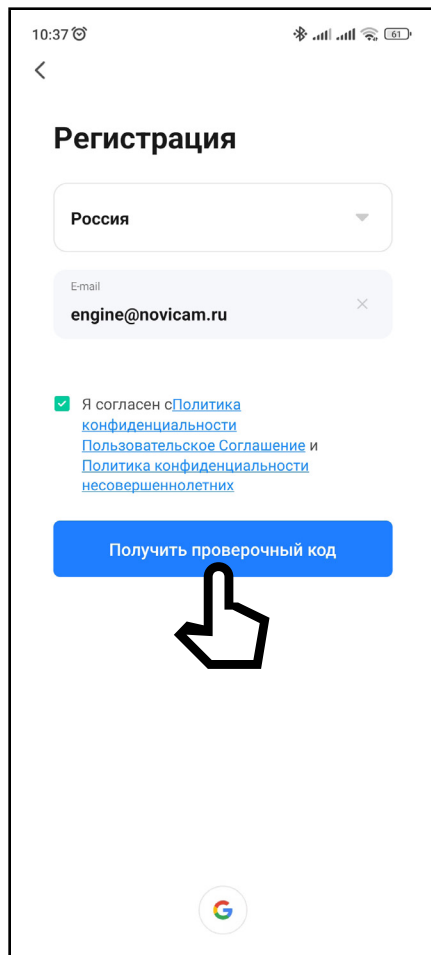
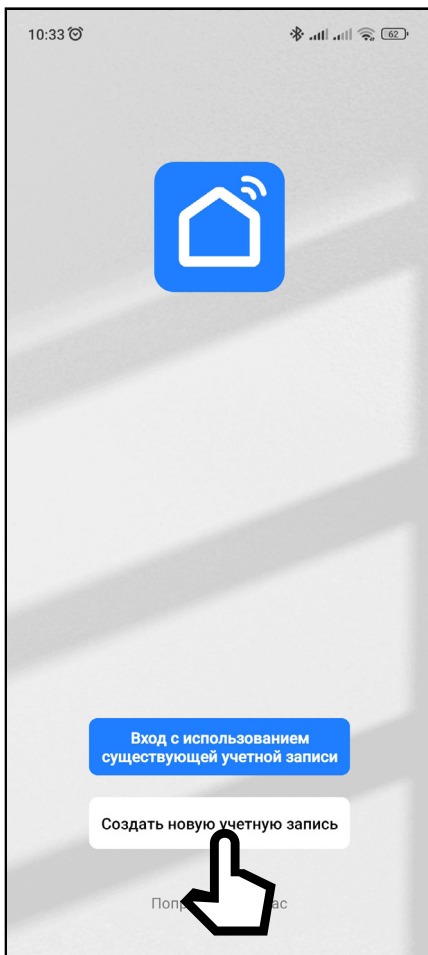


#### ВНИМАНИЕ!

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

# 4. НАЧАЛО РАБОТЫ С ПРИЛОЖЕНИЕМ

## 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.



### ВНИМАНИЕ!

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.

Рис. 8 Регистрация новой учетной записи

## 4. НАЧАЛО РАБОТЫ С ПРИЛОЖЕНИЕМ



Рис. 9 Список устройств

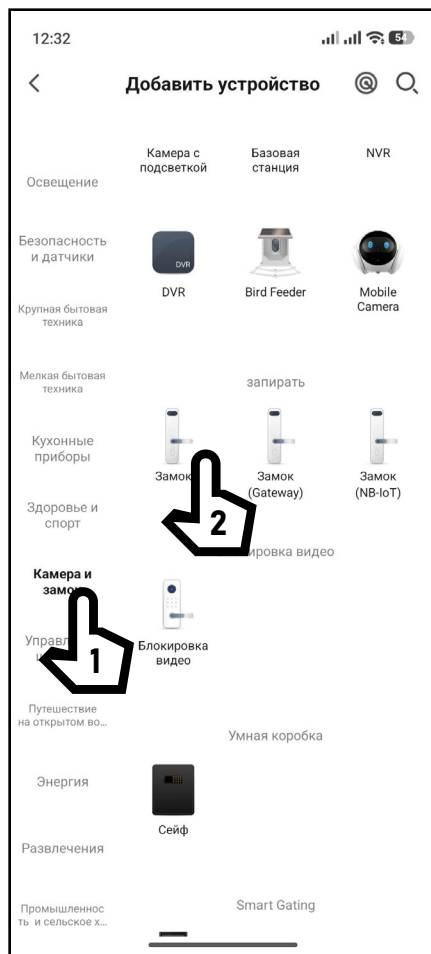


Рис. 10 Выбор типа устройства

### 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 следующую комбинацию с помощью комплектного пульта дистанционного управления (ПДУ):

**\*(Мастер-пароль)#9(Мастер-пароль)#,**  
где Мастер-пароль по умолчанию – 123456.

#### ШАГ 2 (Рис. 9)

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 (Рис. 10)

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



#### ВНИМАНИЕ!

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.

## 4. НАЧАЛО РАБОТЫ С ПРИЛОЖЕНИЕМ

### 4.3. ДОБАВЛЕНИЕ УСТРОЙСТВА В ПРИЛОЖЕНИЕ

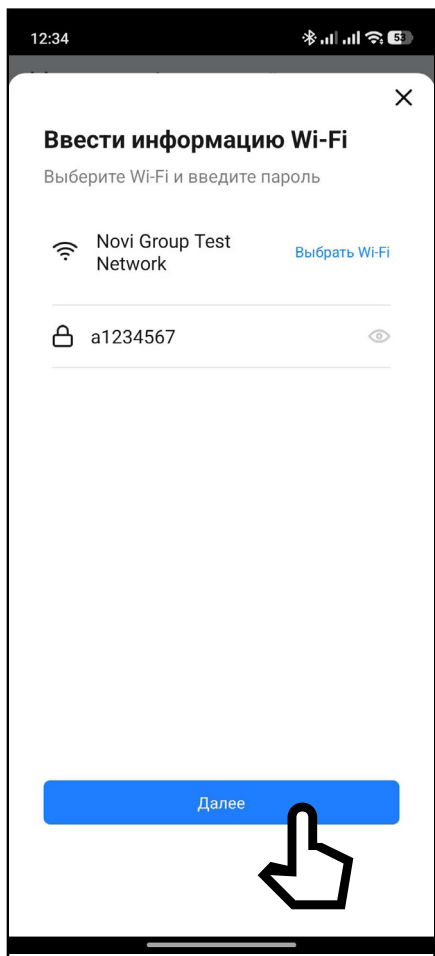


Рис. 11 Выбор Wi-Fi сети

#### ШАГ 4 (Рис. 11)

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



#### ВНИМАНИЕ!

Контроллеры Novisat™ поддерживают работу только с Wi-Fi сетями, функционирующими на частоте 2.4 ГГц.

## 4. НАЧАЛО РАБОТЫ С ПРИЛОЖЕНИЕМ

### 4.3. ДОБАВЛЕНИЕ УСТРОЙСТВА В ПРИЛОЖЕНИЕ

#### ШАГ 5 (Рис. 12)

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

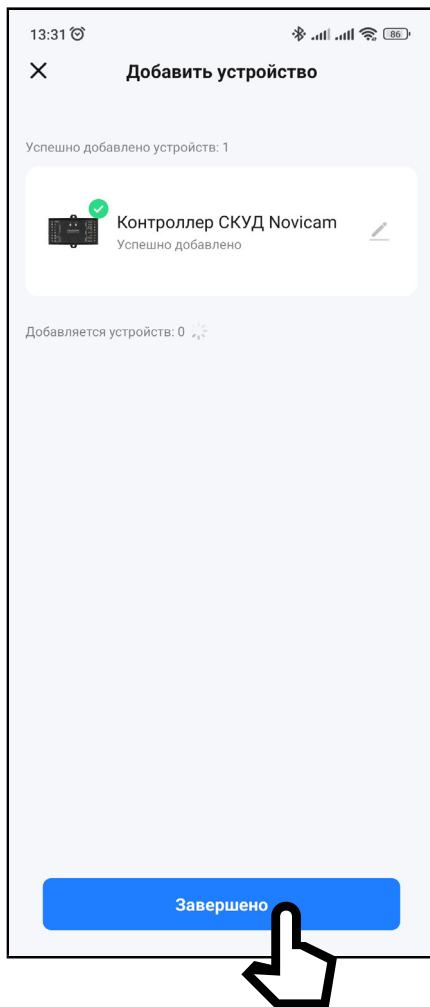


Рис. 12 Подключение завершено

## 4. НАЧАЛО РАБОТЫ С ПРИЛОЖЕНИЕМ

### 4.3. ДОБАВЛЕНИЕ УСТРОЙСТВА В ПРИЛОЖЕНИЕ

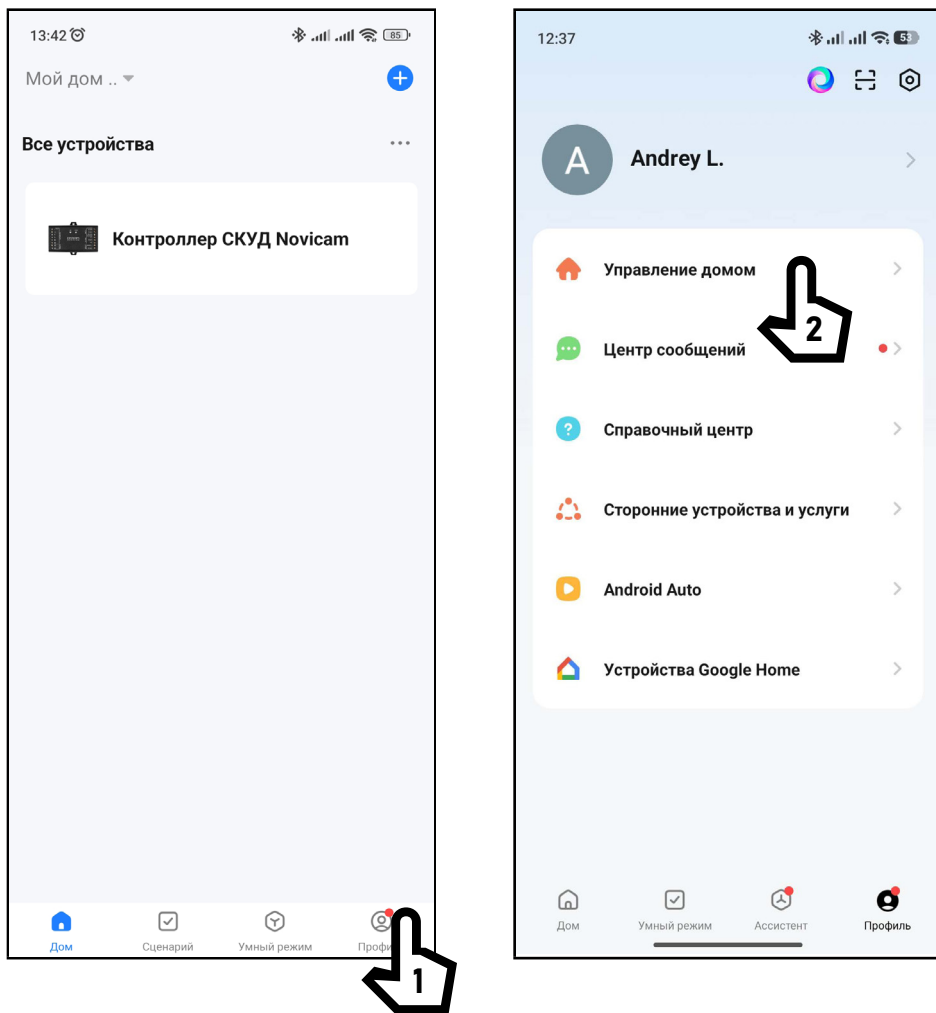


Рис. 13 Создание дома

#### ШАГ 6 (Рис. 13-14)

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**.

## 4. НАЧАЛО РАБОТЫ С ПРИЛОЖЕНИЕМ

### 4.3. ДОБАВЛЕНИЕ УСТРОЙСТВА В ПРИЛОЖЕНИЕ

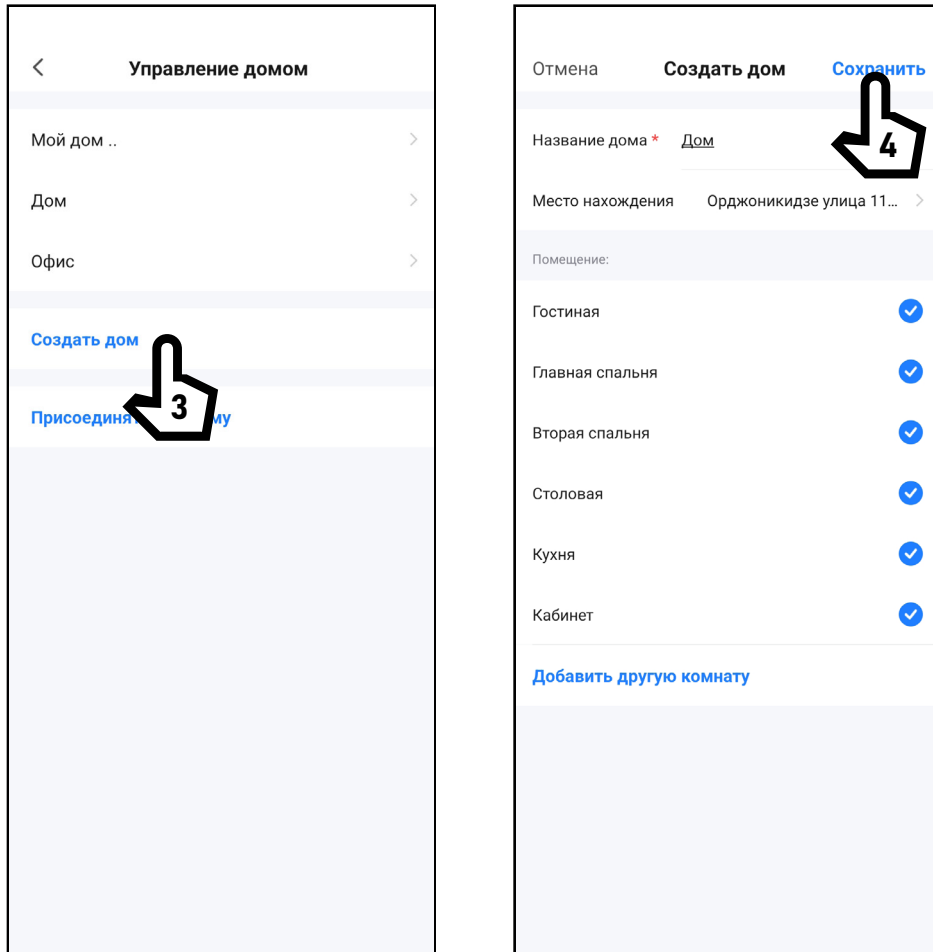


Рис. 14 Создание дома

## 5. РАБОТА В ПРИЛОЖЕНИИ

После добавления контроллера в список устройств станет доступным следующий функционал:

- Удаленное управления запирающим механизмом
- Управление Пользователями
- Выдача временных паролей
- Удаленная настройка
- Просмотр и экспорт Журнала событий

# 5. РАБОТА В ПРИЛОЖЕНИИ

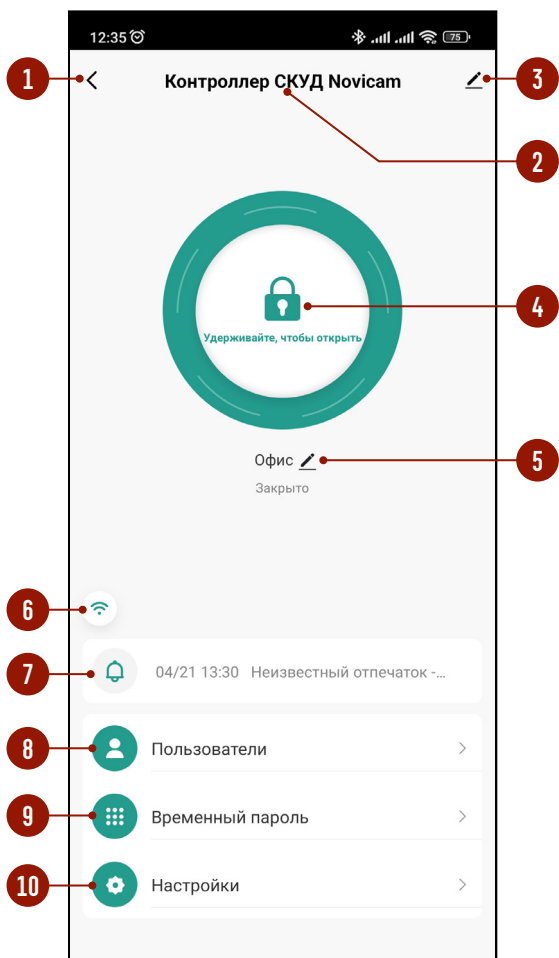


Рис. 15 Главное меню устройства

## 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**



### ВНИМАНИЕ!

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 переключку между контактами Датчик и Общий.

# ПРОГРАММИРОВАНИЕ И ЭКСПЛУАТАЦИЯ

## 5. РАБОТА В ПРИЛОЖЕНИИ

### 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	✓	✓	✓
Управление обычными Пользователями	✓	✓	✗
Назначение администраторов	✓	✗	✗
Просмотр журнала	✓	✓	✗
Настройка времени задержки реле	✓	✓	✗

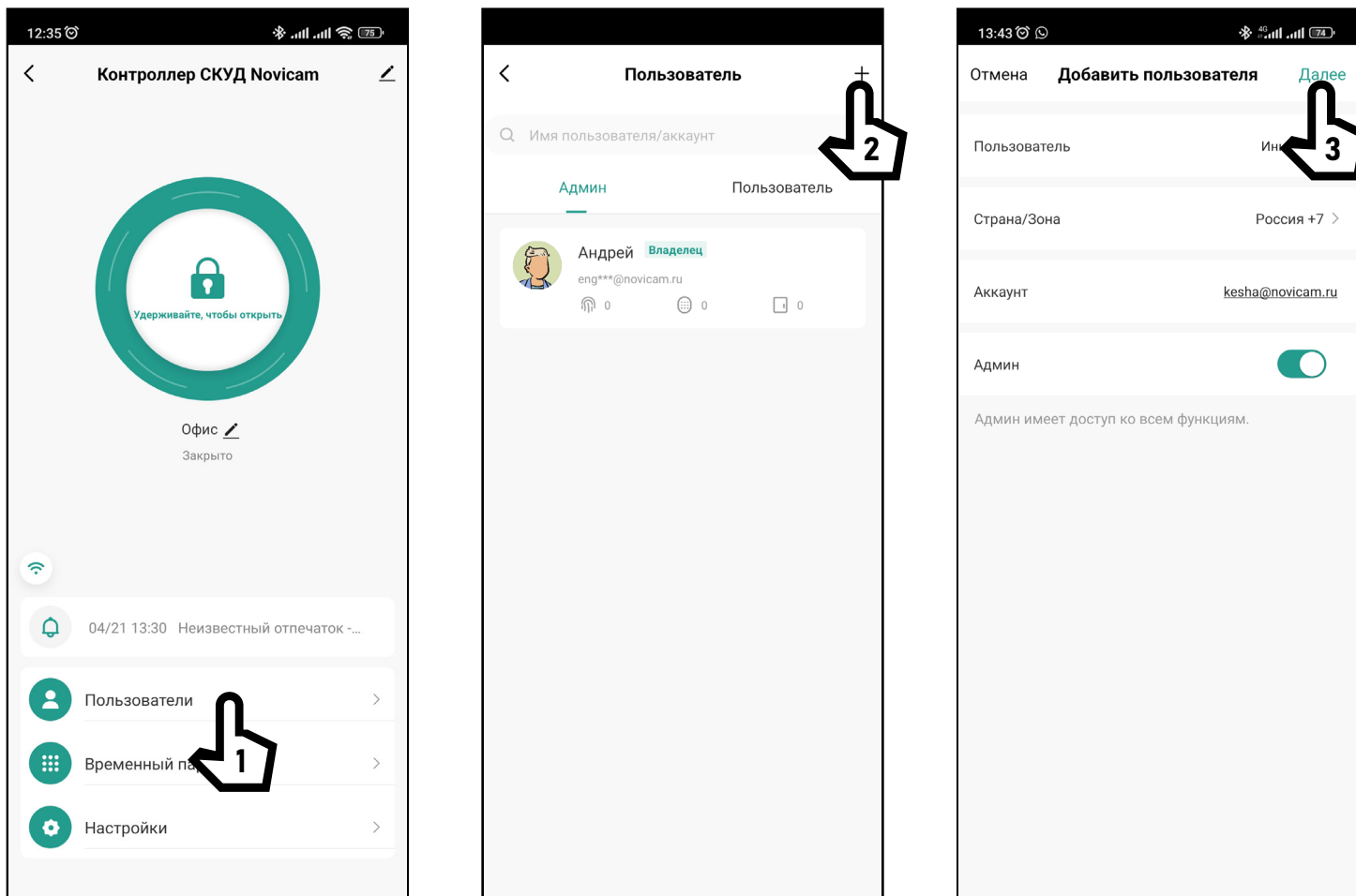


#### ВНИМАНИЕ!

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

# 5. РАБОТА В ПРИЛОЖЕНИИ

## 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.

Рис. 16 Добавление Пользователя

## 5. РАБОТА В ПРИЛОЖЕНИИ

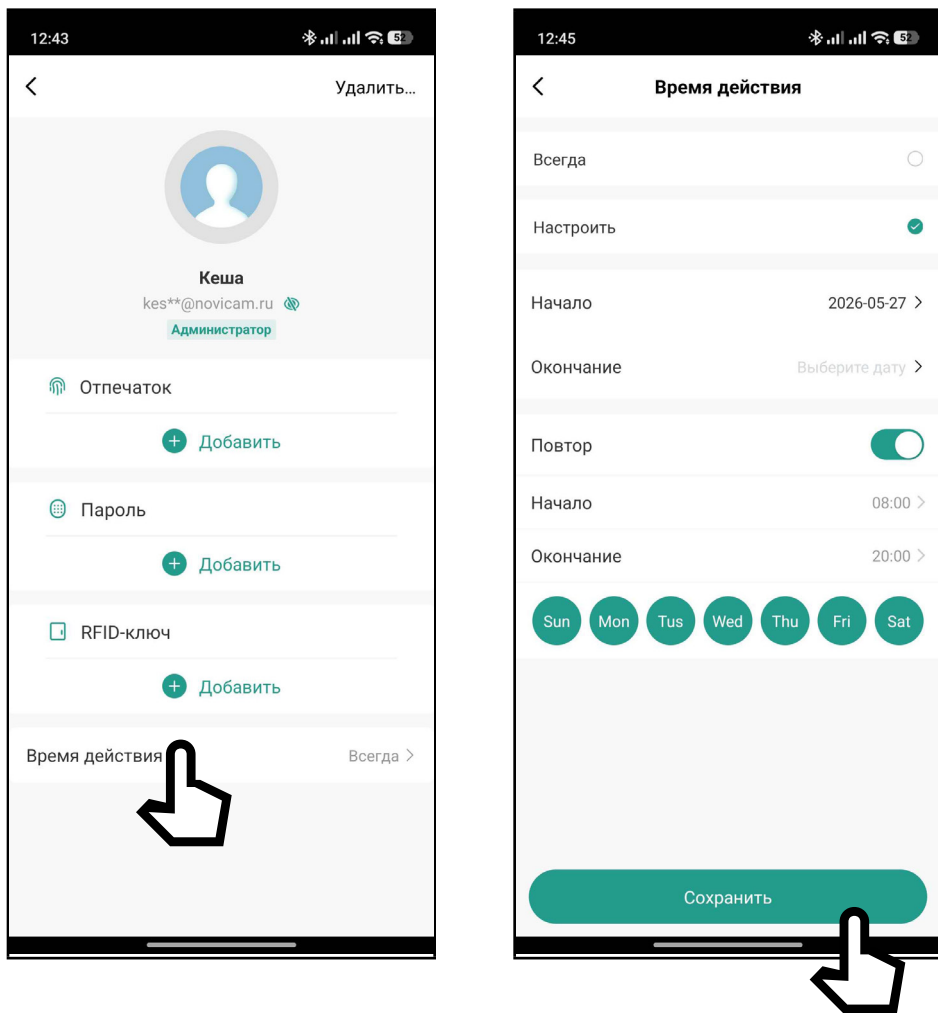


Рис. 17 Настройка сроков действия идентификаторов для Пользователя

### 5.2.1. ДОБАВЛЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

При необходимости можно ограничить время действия идентификаторов для каждого Пользователя индивидуально. Для этого необходимо выбрать Пользователя и далее нажать на поле **Время 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  
Tue – Вторник  
Wed – Среда  
Thu – Четверг  
Fri – Пятница  
Sat – Суббота



#### ВНИМАНИЕ!

Функция Добавления/Удаления отпечатков через Приложение недоступна для данного устройства.

# 5. РАБОТА В ПРИЛОЖЕНИИ

## 5.2.2. ДОБАВЛЕНИЕ RFID-КЛЮЧА

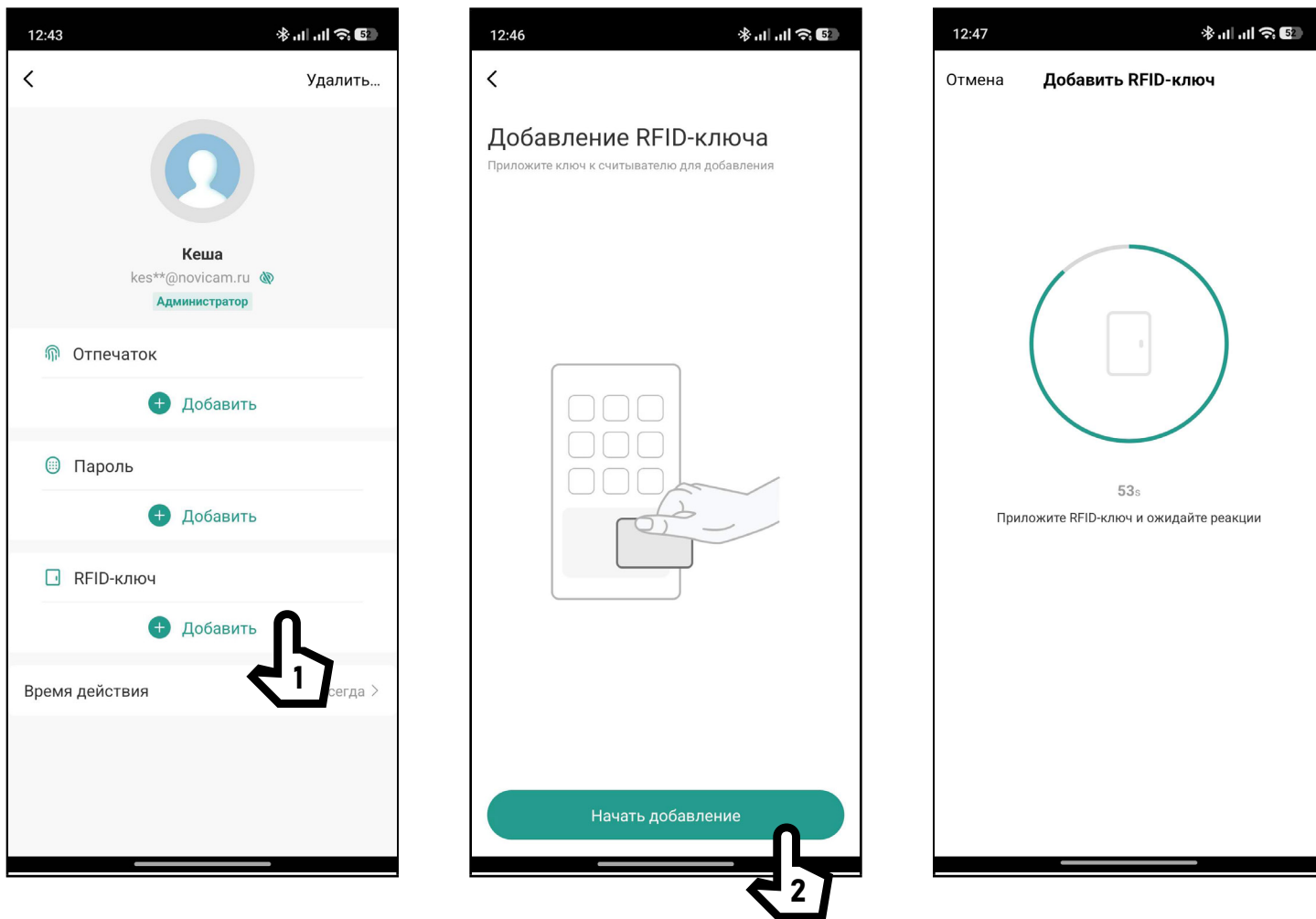


Рис. 18 Добавление RFID-ключа

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

## 5. РАБОТА В ПРИЛОЖЕНИИ

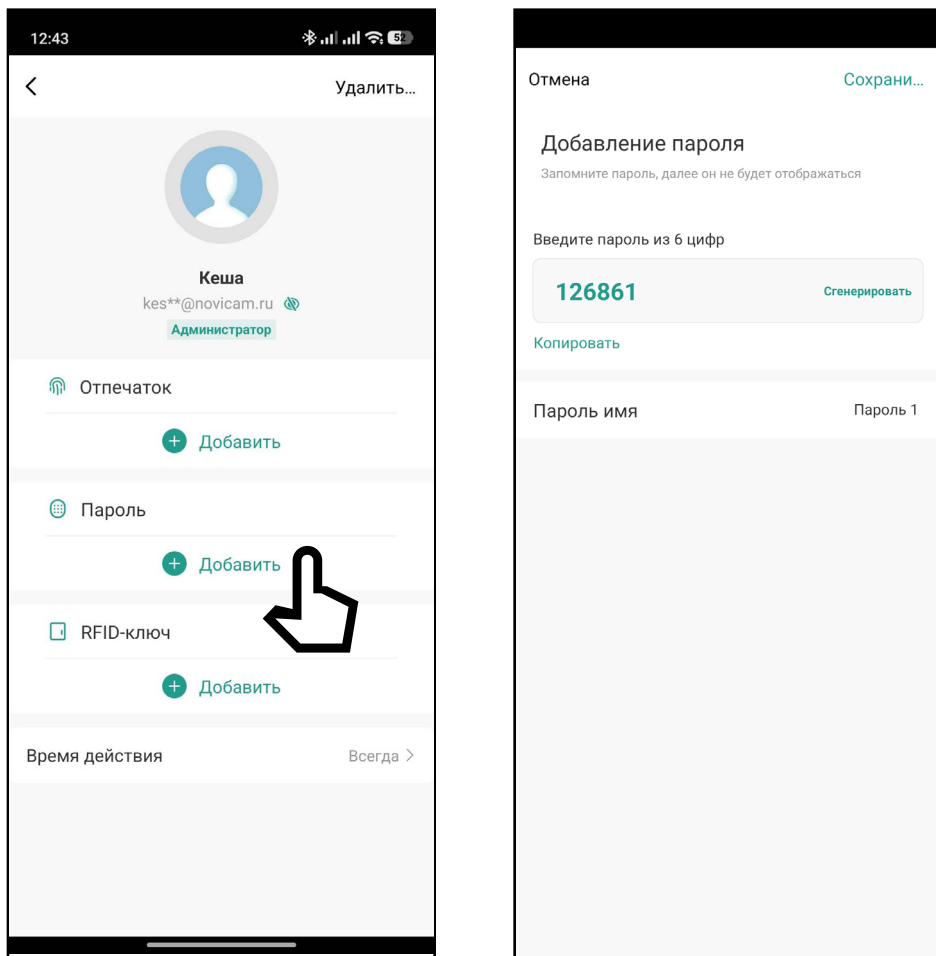


Рис. 19 Добавление пароля

### 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. РАБОТА В ПРИЛОЖЕНИИ

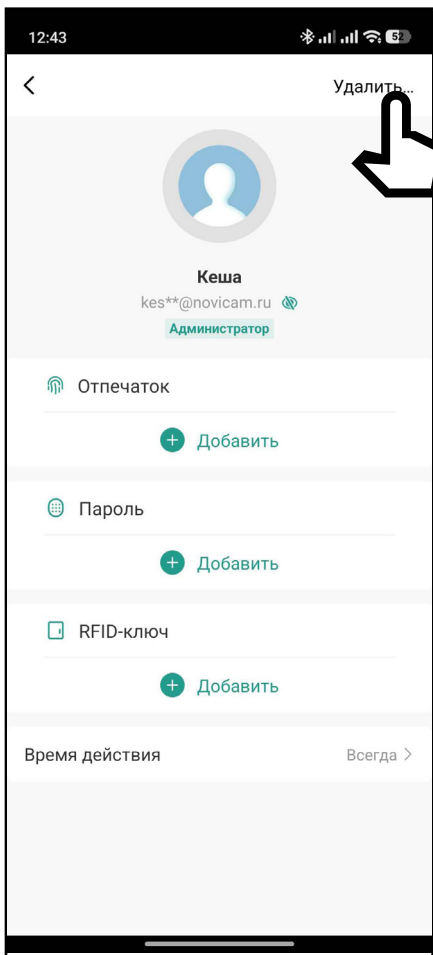


Рис. 20 Удаление Пользователя

### 5.2.4. УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЯ

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



#### **ВНИМАНИЕ!**

При удалении определенного Пользователя будут удалены все присвоенные ему идентификаторы и пароли.

## 5. РАБОТА В ПРИЛОЖЕНИИ

### 5.2.5. УДАЛЕНИЕ RFID-КЛЮЧЕЙ И ПАРОЛЕЙ

Для удаления RFID-ключа/Пароля выберите его в карточке Пользователя, а затем нажмите **Удалить**.

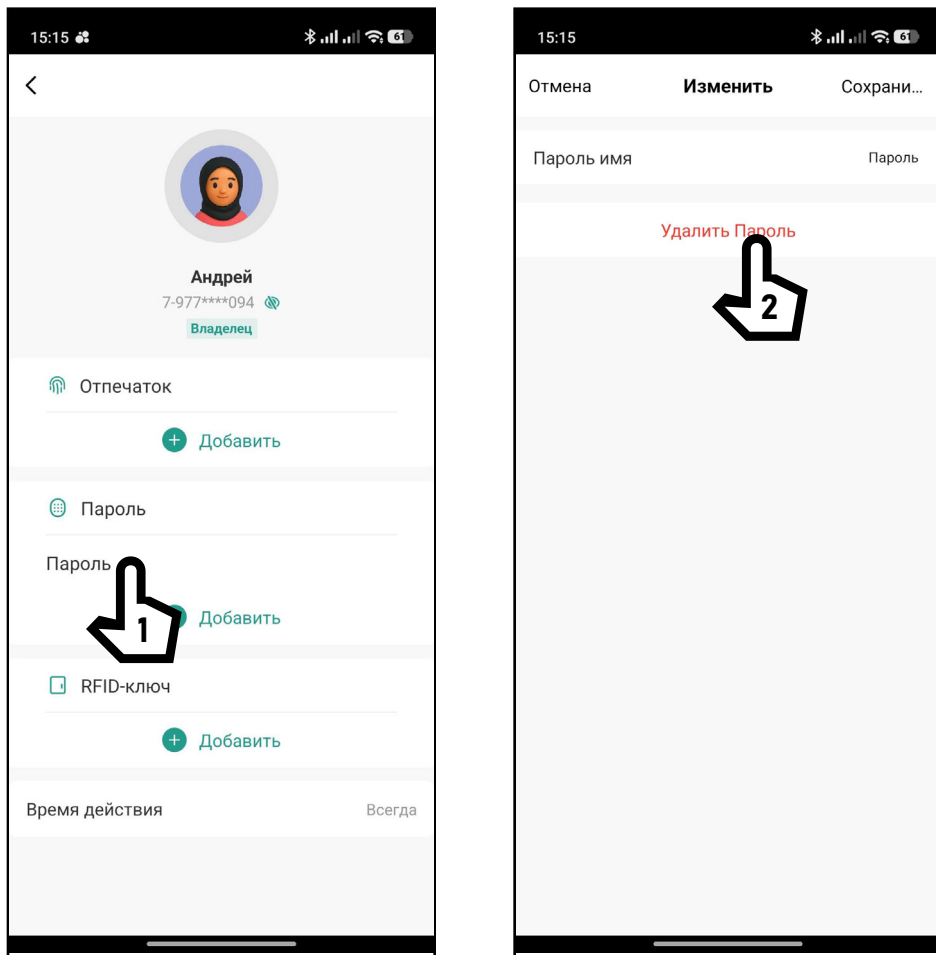


Рис. 21. Удаление RFID-ключа или Пароля

## 5. РАБОТА В ПРИЛОЖЕНИИ

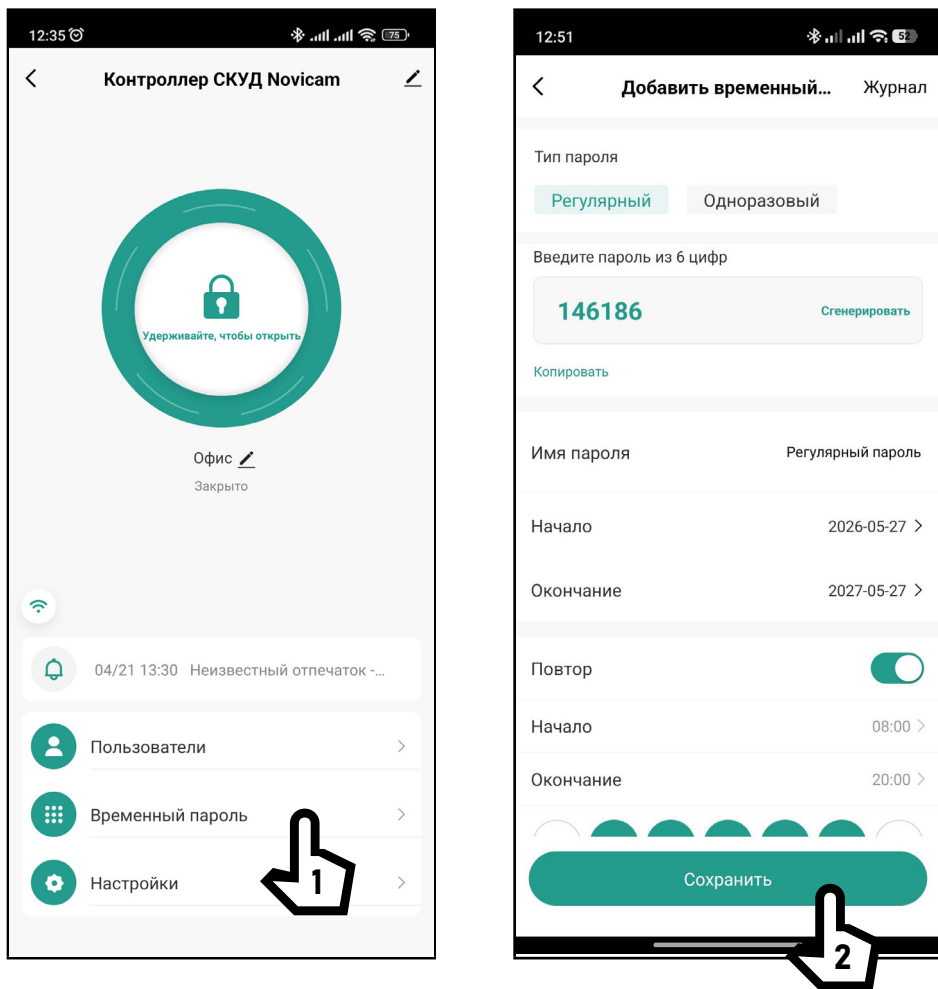


Рис. 22 Активация регулярного пароля

### 5.3. ВРЕМЕННЫЙ ПАРОЛЬ

Временный пароль используется для разового или многократного 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



#### ВНИМАНИЕ!

Регулярный пароль может быть Изменен или Удален в период времени своего действия из списка всех паролей.

# 5. РАБОТА В ПРИЛОЖЕНИИ

## 5.3. ВРЕМЕННЫЙ ПАРОЛЬ

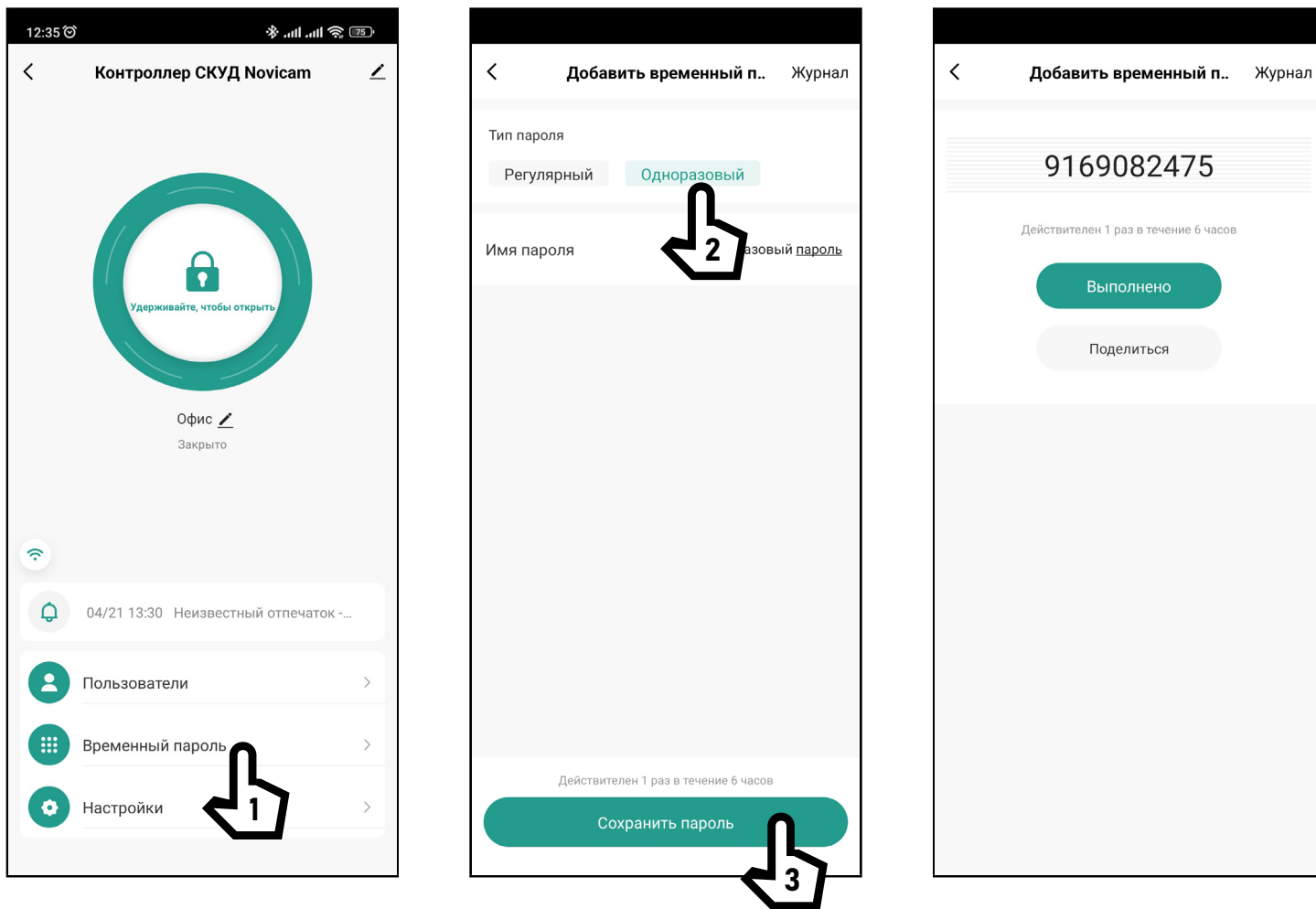


Рис. 23 Выдача одноразового пароля

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. РАБОТА В ПРИЛОЖЕНИИ

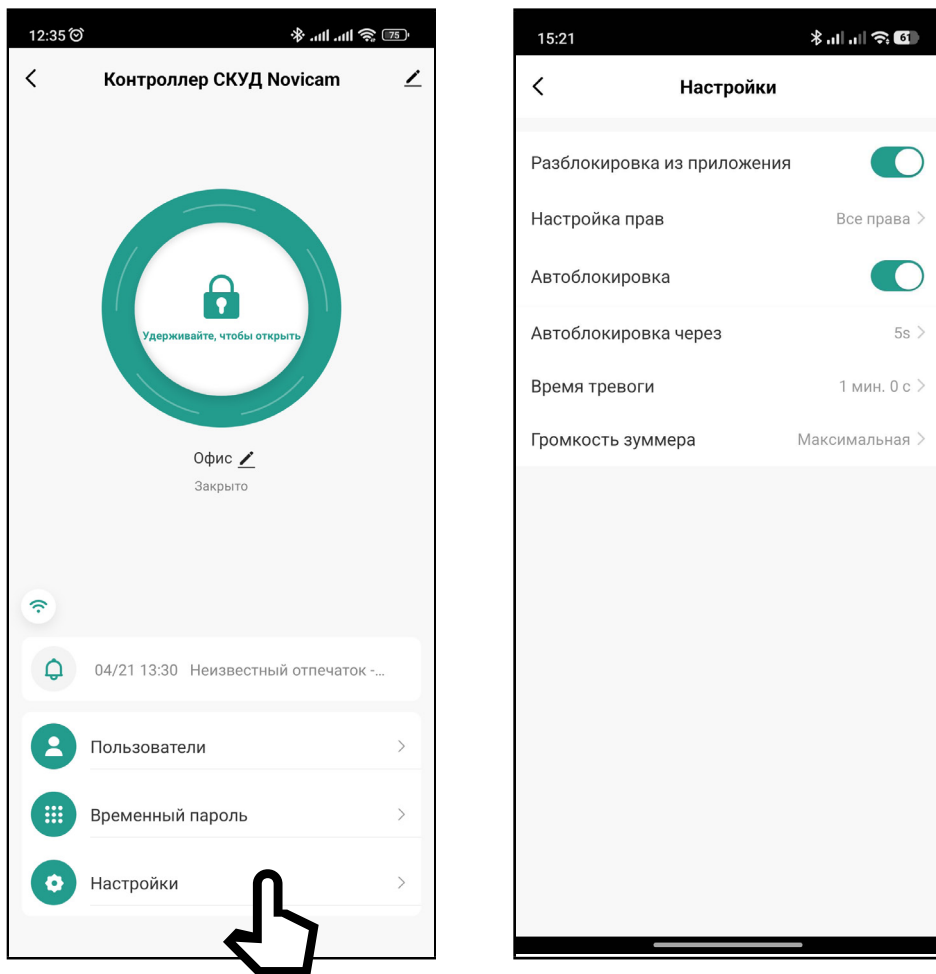


Рис. 24 Настройки

## 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.



### ВНИМАНИЕ!

Необходимо активировать настройку Разблокировка из Приложения для управления запирающим механизмом.

**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 зуммера** – настройка громкости зуммера (Без звука / Минимальная / Средняя / Максимальная).

# 5. РАБОТА В ПРИЛОЖЕНИИ

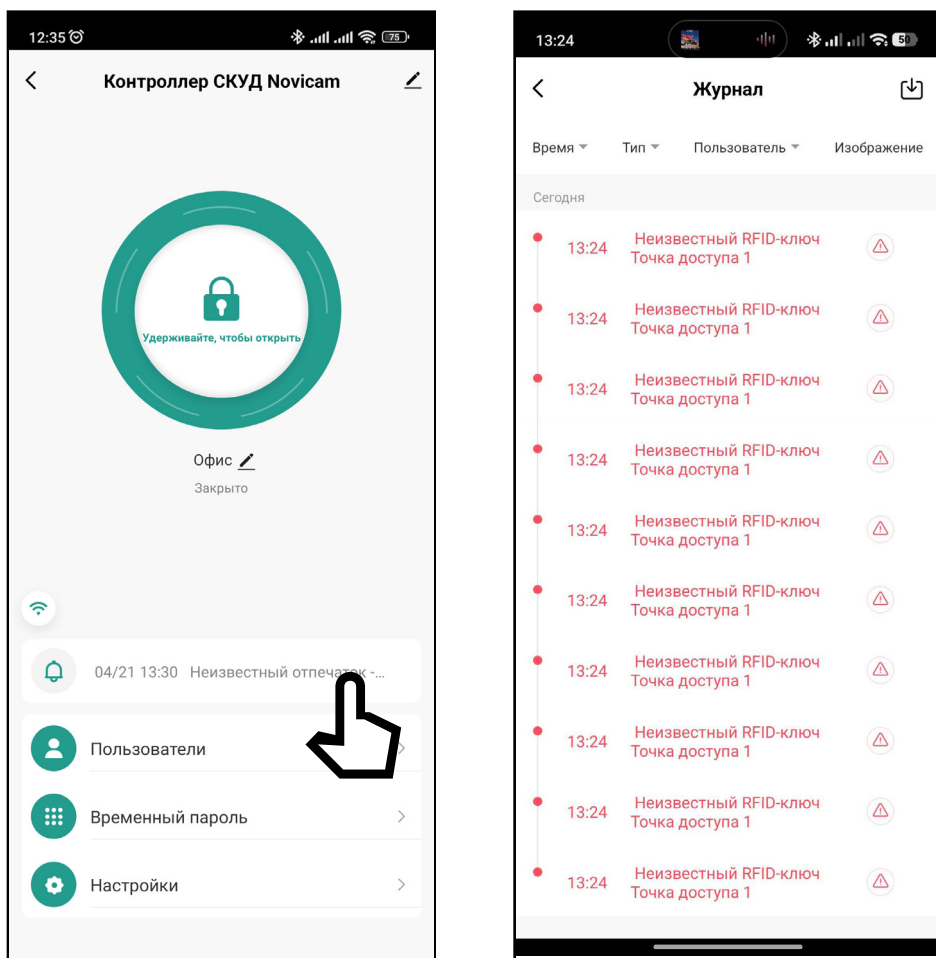


Рис. 25 Журнал событий

## 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.

Нажав в верхнем правом углу на значок, можно экспортировать данные на почту в формате xls.

# 5. РАБОТА В ПРИЛОЖЕНИИ

## 5.5. ЖУРНАЛ

Журнал событий можно экспортировать на указанную электронную почту в формате xls для дальнейшего анализа и обработки. Предварительно для этого нужно выбрать период событий и нажать кнопку **Экспорт**.

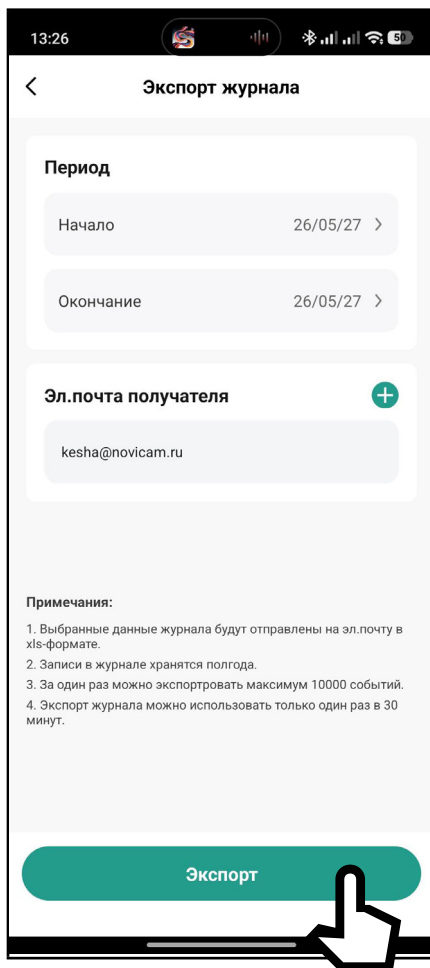


Рис. 26 Экспорт Журнала



### ВНИМАНИЕ!

1. Данные Журнала событий хранятся в облаке экосистемы полгода.
2. За один раз можно экспортировать максимум 10000 событий.
3. Экспорт Журнала можно использовать один раз в 30 минут.

## 5. РАБОТА В ПРИЛОЖЕНИИ

### 5.6. PUSH-УВЕДОМЛЕНИЯ ПРИ ЗВОНКЕ

На контроллере Novicam SB310 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. РАБОТА В ПРИЛОЖЕНИИ

### 5.7. ОБЩИЙ ДОСТУП К УСТРОЙСТВУ

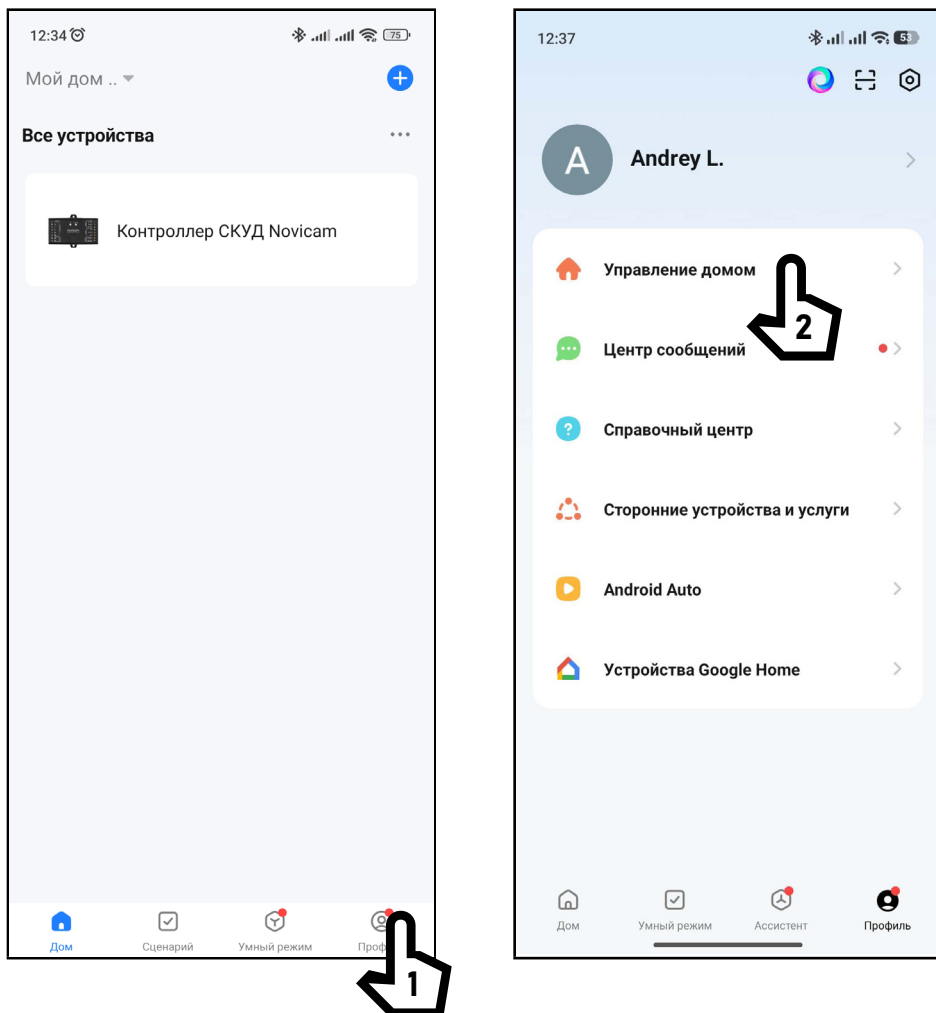


Рис. 27 Предоставление Общего доступа к устройству

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. РАБОТА В ПРИЛОЖЕНИИ

### 5.7. ОБЩИЙ ДОСТУП К УСТРОЙСТВУ

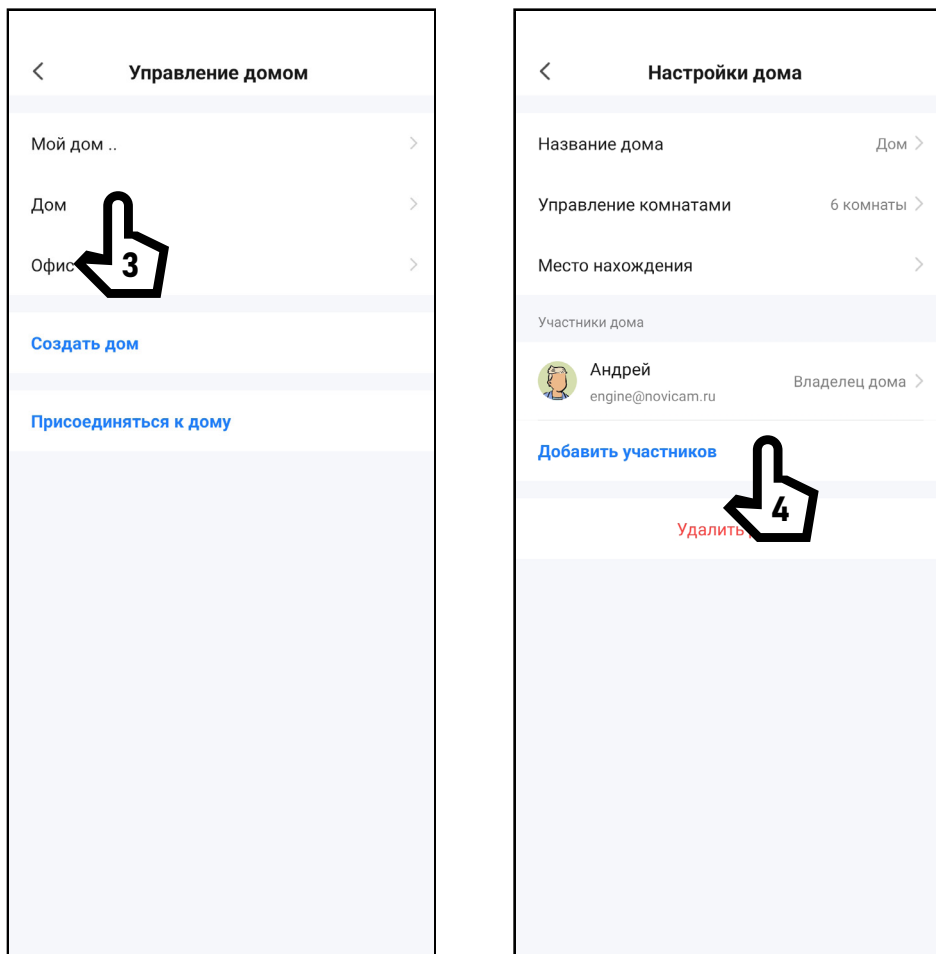


Рис. 28 Предоставление Общего доступа к устройству

# 5. РАБОТА В ПРИЛОЖЕНИИ

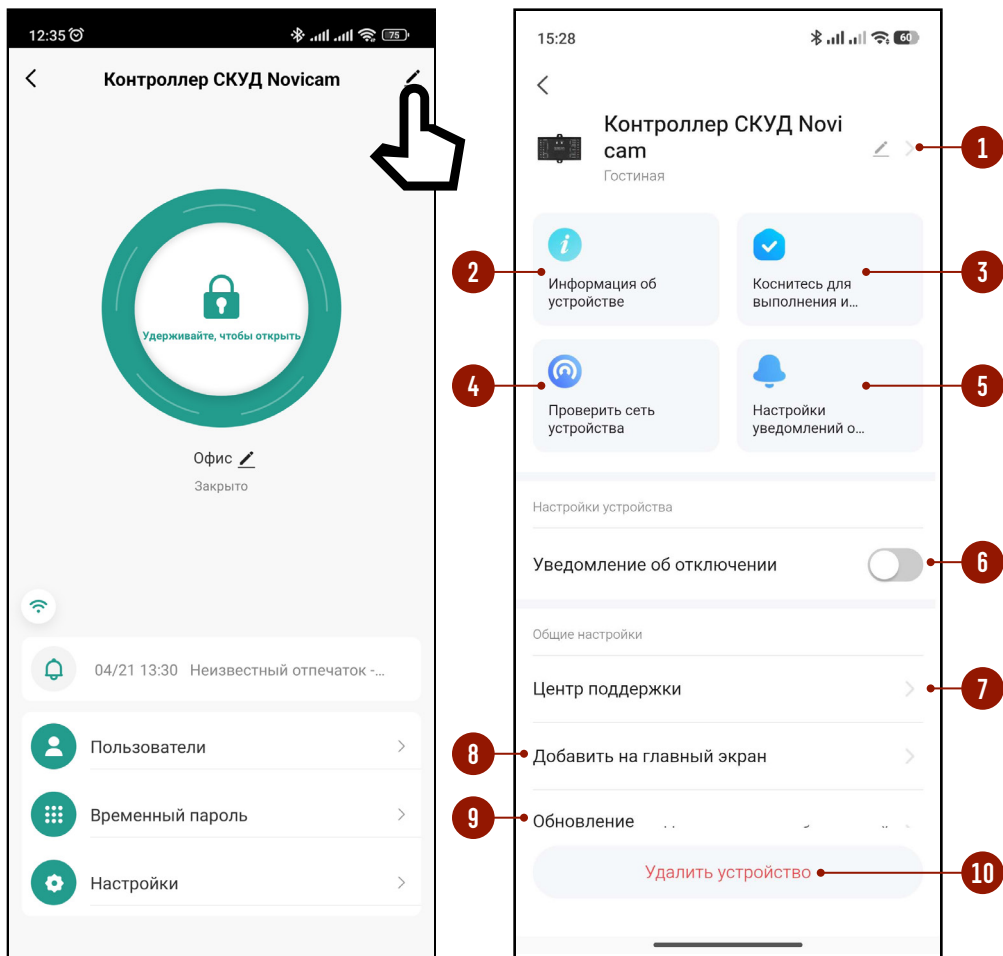


Рис. 29 Меню Сервис

## 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 в Приложении.

1. Изменение имени устройства и его расположения.
2. В данном пункте содержится информация:
  - Виртуальный ID (он же UUID)
  - IP-адрес
  - MAC-адрес
  - Часовой пояс
  - Уровень сигнала

3. Сценарии автоматизации.
4. Проверка качества сетевого соединения, а также просмотр IP- и MAC-адреса устройства.
5. Настройка уведомлений (неактуально)
6. Активация уведомлений, если устройство отключено от сети более чем на 30 минут.
7. Часто задаваемые вопросы и обратная связь с разработчиками.
8. Добавление иконки устройства на главный экран смартфона для удобства доступа.
9. Информация о текущей прошивке устройства, ее обновление в ручном и автоматическом режимах.
10. Удаление устройства из аккаунта.



### ВНИМАНИЕ!

1. При удалении устройства из Приложения предлагается два варианта – Удаление только из аккаунта (с сохранением данных Пользователя и настроек) и Удаление с полной очисткой данных из памяти устройства.
2. Если доступ к аккаунту в Приложении, по каким-либо причинам, утерян, то отвязать устройство можно с помощью следующей комбинации, набранной на ПДУ: \*(Мастер-пароль)#9(Мастер-пароль)#, где Мастер-пароль по умолчанию – 123456.

<b>Модель</b>	<b>SB310 WIFI</b>
Версия	4242
<b>СИСТЕМА</b>	
Режимы работы	Только RFID-ключ, Только отпечаток, RFID-ключ или Отпечаток или Пароль, Групповой
Емкость памяти	до 1000 RFID-ключей/паролей
Количество Пользователей в Приложении	до 500
Индикация	Световая и звуковая
Программирование	Кодовое ПДУ, Мастер-картой, Через Приложение
Временный пароль	Задается через Приложение
Учет рабочего времени	Журнал событий с возможностью экспорта в xls
Коммутация	Клеммные колодки
<b>ПОДКЛЮЧЕНИЕ</b>	
Тип реле	Электромеханическое, "мокрый" или "сухой" контакт Н.Р./Н.З, Импульсный и триггерный режимы
Ком. параметры реле	2 А, АС 250 В 2 А, DC 30 В
Задержка реле	от 0 до 99 с
Кнопка выхода	Н.Р.
Кнопка звонка	Зависит от кнопки (вход с Н.Р. контактами)
Датчик двери	Н.З.
Тревожные входы/выходы	1/1 (макс. нагрузка 5 А)
Считыватель	Вход: Wiegand-26...44, 56, 58 бит Макс. расстояние для интерфейса Wiegand – 100 м

<b>Модель</b>	<b>SB310 WIFI</b>
Версия	4242
<b>СЕТЬ</b>	
Беспроводной интерфейс	Wi-Fi: 802.11b/g/n Протокол <b>WEP</b> с алгоритмом шифрования RC4 и длиной ключа 64/128 бит Протокол <b>WPA-PSK</b> с алгоритмом шифрования RC4/TKIP и длиной ключа 128 бит Протокол <b>WPA2-PSK</b> с алгоритмом шифрования AES и длиной ключа 128 бит
Программное обеспечение	Smart Life, Tuya Smart (iOS & Android)
<b>ФИЗИЧЕСКИЕ ПАРАМЕТРЫ</b>	
Материал	ABS-пластик
Монтаж	Накладной
Температурный режим	-40°C...+60°C
Размер (Ш×В×Г)	91×48×20 мм
Питание	DC 12 В, 0.15 А, 1.8 Вт

## ТРАНСПОРТИРОВКА И ХРАНЕНИЕ

1. Оборудование в транспортной таре перевозится любым видом крытых транспортных средств согласно действующим нормативам.
2. Условия транспортирования оборудования должны соответствовать условиям хранения 5 по ГОСТ 15150-69.
3. Хранение оборудования устройства в транспортной таре на складах изготовителя регламентируется условиями 1 по ГОСТ 15150-69.

## УТИЛИЗАЦИЯ

Утилизацию продукции, содержащей электронные компоненты, необходимо производить в соответствии с местными законами и нормативными актами. Для подробной информации о правилах утилизации обратитесь к местным органам власти.

Производитель гарантирует исправность изделия и его нормальную работу в течение 3 (трех) лет с даты производства или 1 (одного) года с даты продажи/передачи потребителю (в зависимости от того, какой срок наступит позднее) при соблюдении условий, изложенных в Руководстве Пользователя.

Дата производства указана на этикетке устройства и в паспорте изделия, либо зашифрована в серийном номере.

Определение даты производства с использованием серийного номера осуществляется в разделе «Проверка гарантийного срока оборудования» на веб-странице: [www.novicam.ru/tech-support](http://www.novicam.ru/tech-support):

Серийный номер состоит из латинских букв и цифр. Например: 2033:325d38878c.

Дата продажи подтверждается документами о покупке (товарный чек, товарная

накладная, пр.). Для подтверждения даты продажи просим вас сохранять документы о покупке изделия на весь период гарантийного срока. Дата передачи потребителю подтверждается документами передачи товара.

Если в течение гарантийного срока в изделии обнаружится недостаток, Производитель по настоящей гарантии безвозмездно произведет ремонт/замену изделия ненадлежащего качества или его дефектных деталей в соответствии с приведенными ниже Условиями гарантийного обслуживания. Ремонт/замена изделия или его дефектных деталей может производиться с использованием новых и/или восстановленных деталей по решению Производителя.

При выявлении недостатков в работе изделия потребителю следует обратиться в Единую службу поддержки.

# УСЛОВИЯ ГАРАНТИЙНОГО ОБСЛУЖИВАНИЯ

1. В соответствии с данной гарантией Производитель дает обязательства в течение гарантийного срока устранить недостаток в изделии или осуществить замену изделия, на которое распространяются условия настоящей гарантии.
2. Производитель не несет ответственности за любой ущерб, убытки или расходы, прямые, косвенные или случайные, последовательные или особые, связанные с использованием изделия.
3. Услуги по гарантийному обслуживанию могут быть оказаны при обращении потребителя к Производителю по гарантийному случаю в период до истечения гарантийного срока.
4. Настоящая гарантия не распространяется на изделия с измененным, неразборчивым или отсутствующим на изделии серийным номером.
5. Производитель принимает на обслуживание изделия без установленных дополнительных элементов, в том числе носителей информации, декоративных и защитных элементов. До передачи изделия Производителю на обслуживание, необходимо отделить все элементы, не входящие в комплектацию поставки изделия. Производитель не несет ответственности за детали/элементы, не входящие в комплект поставки изделия, переданные вместе с изделием на обслуживание.
6. Все дефектные изделия/детали изделия, которые подверглись замене на новые, переходят в собственность Производителя.

\* Под естественным износом понимается ожидаемое уменьшение пригодности детали в результате износа или обычного воздействия окружающей среды. Интенсивность износа и долговечность детали, зависит от условий ее работы (характера нагрузки, величины удельного давления, температуры и т.д.), а также материала детали, регулировки, смазки, своевременности и тщательности выполнения работ по техническому обслуживанию, соблюдения правил и условий эксплуатации изделия, изложенных в Руководстве Пользователя.

# ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

## УСЛОВИЯ ГАРАНТИЙНОГО ОБСЛУЖИВАНИЯ

- 7.** Настоящая гарантия не распространяется на:
- 7.1.** Периодическое обслуживание, ремонт или замену частей в связи с их естественным износом\*;
  - 7.2.** Расходные материалы (компоненты), которые требуют периодической замены на протяжении срока службы изделия. Например: элементы питания, карты памяти.
  - 7.3.** Риски, связанные с транспортировкой изделия для обслуживания;
  - 7.4.** Недостатки изделия, вызванные неправильной эксплуатацией изделия:
    - 7.4.1.** Неправильное обращение, повлекшее физические, косметические повреждения или повреждения поверхности, деформацию изделия или повреждение сенсорных панелей;
    - 7.4.2.** Нарушение правил и условий установки, эксплуатации и обслуживания изделия, изложенных в Руководстве Пользователя и другой документации, передаваемой Потребителю в комплекте с изделием;
    - 7.4.3.** Установку или использование изделия с нарушением технических стандартов и норм безопасности, действующих в стране установки или эксплуатации.
    - 7.4.4.** Использования программного обеспечения, не входящего в комплект поставки изделия или в результате неправильной установки, настройки, изменения (вмешательства в программный код) программного обеспечения, входящего в комплект поставки изделия;
    - 7.4.5.** Использования изделия с аксессуарами, периферийным оборудованием и другими устройствами, тип, состояние и стандарт которых не соответствует рекомендациям Производителя;
    - 7.4.6.** Несанкционированного вмешательства в конструкцию изделия, в том числе попытка осуществления самостоятельного ремонта;

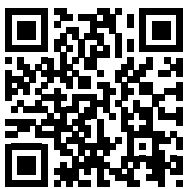
# ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

## УСЛОВИЯ ГАРАНТИЙНОГО ОБСЛУЖИВАНИЯ

7.4.7. Несчастных случаев, пожаров, попадания насекомых, инородных жидкостей, химических веществ, других веществ, затопления, вибрации, высокой температуры, неправильной вентиляции, колебания напряжения, использования повышенного или недопустимого питания, облучения, электростатических разрядов, включая разряд молнии, и иных видов внешнего воздействия или влияния.

8. Настоящая гарантия распространяется исключительно на аппаратные компоненты изделия. Гарантия не распространяется на программное обеспечение.

9. Срок службы изделия составляет 7 лет от даты производства изделия. Использование товара по истечении срока службы может представлять опасность для здоровья или имущества потребителя. Ответственность за любые последствия эксплуатации изделия после истечения срока службы в полном объеме возлагается на лицо, осуществляющее эту эксплуатацию.



ТЕХНИЧЕСКАЯ  
ПОДДЕРЖКА

Произведено в Китае  
по заказу и под контролем ООО "НОВИ ГРУПП" РОССИЯ

Все торговые марки являются собственностью их законных владельцев.  
Настоящий документ и содержащаяся в нем информация защищены авторским правом.  
Copyright © 2026 ООО "НОВИ ГРУПП" (Novicam™) Все права защищены. v.1.4

