

Оглавление

1. НАЗНАЧЕНИЕ ПРОГРАММЫ	2
2. РАБОТА С КОНТРОЛЛЕРОМ/ЗАМКОМ.....	2
2.1. Пароли доступа	2
2.2. Подключение к контроллеру/замку.....	2
2.3. Изменение состояния замка из приложения	2
2.4. Изменение состояния замка из уведомления.....	3
2.5. Изменение состояния замка с использованием виджета	4
2.6. Изменение настроек контроллера/замка	5
2.7. Сохранение «Снимка» контроллера/замка	5
2.8. Просмотр/добавление/изменение/удаление паролей.....	6
2.9. Триггерный режим работы контроллера/замка	6
2.10. Автогенерация паролей доступа	7
2.11. Настройка времени на контроллере/замке	7
3. НАСТРОЙКИ ПРИЛОЖЕНИЯ.....	8
3.1. Настройка ввода PIN-кода приложения	8
4. БАЗЫ ДАННЫХ ПРИЛОЖЕНИЯ	8
4.1. Добавление контроллера/замка в базу устройств.....	8
4.2. База устройств	9
4.3. База записей контроллеров/замков	10

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа предназначена для управления контроллерами Promix-CR.BT.01 (<https://www.promix-center.ru/kontrollery-upravleniya/radiokanalnye/promix-cr-bt-01/>).

2. РАБОТА С КОНТРОЛЛЕРОМ/ЗАМКОМ

2.1. Пароли доступа

Пароль администратора.

Содержится в контроллере/замке в единственном экземпляре, служит для настройки контроллера и редактирования паролей (см. пп. 2.6-2.12).

Постоянный пароль.

Постоянный пароль позволяет открывать/закрывать замок в любое время. При подключении к контроллеру с использованием постоянного пароля пользователю предоставляется возможность открывать/закрывать замок и просматривать текущее время на контроллере/замке.

Одноразовый пароль.

Одноразовый пароль позволяет один раз открыть замок и один раз закрыть замок (только в такой последовательности). При подключении к контроллеру/замку с использованием одноразового пароля пользователю предоставляется возможность открывать/закрывать замок и просматривать текущее время на контроллере/замке и текущий статус пароля («Открытие+Заккрытие» или «Только для закрытия»).

Временный пароль.

Временный пароль позволяет управлять замком в заданный промежуток времени. При подключении к контроллеру с использованием временного пароля пользователю предоставляется возможность открывать/закрывать замок и просматривать текущее время на контроллере/замке и промежуток времени, в котором пароль будет активен.

Коды типов паролей:

- 1 – пароль администратора;
- 2 – постоянный пароль;
- 3 – одноразовый пароль;
- 4 – временный пароль.

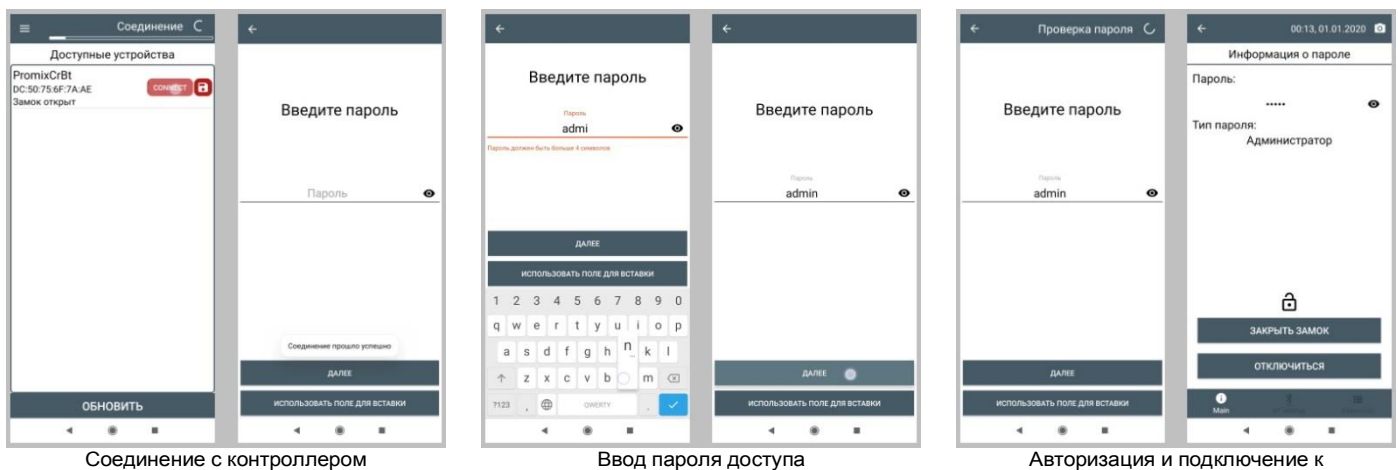
2.2. Подключение к контроллеру/замку

Для подключения необходимо войти в зону действия контроллера/замка, убедиться, что Bluetooth и GPS (Местоположение) на смартфоне включены (включить, если не включены). Запустить приложение, ввести pin-код при необходимости, после того, как нужный контроллер/замок будет найден, нажать «CONNECT» напротив его имени.

Если смартфон не находит контроллер/замок достаточно долгое время, то рекомендуется повторно нажать на кнопку «Обновить» или перезапустить приложение

ВНИМАНИЕ! С контроллером в один момент времени может быть соединен только один пользователь.

Откроется форма ввода пароля, где необходимо ввести пароль и нажать на кнопку «ДАЛЕЕ».



2.3. Изменение состояния замка из приложения

Есть два способа управления замком из приложения:

- Управления замком после подключения к контроллеру/замку.

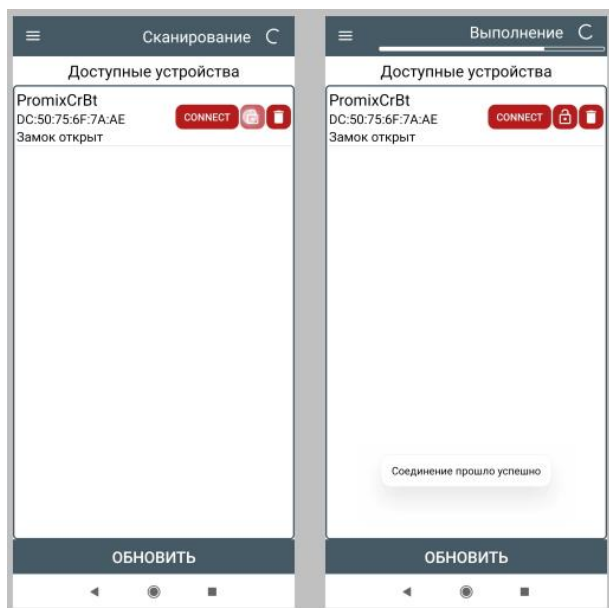
Для изменения состояния замка необходимо подключиться к контроллеру/замку (см. п. 2.2). После подключения в открывшемся окне будет предоставлена возможность изменять состояние замка.

- Управление замком из главного окна приложения.

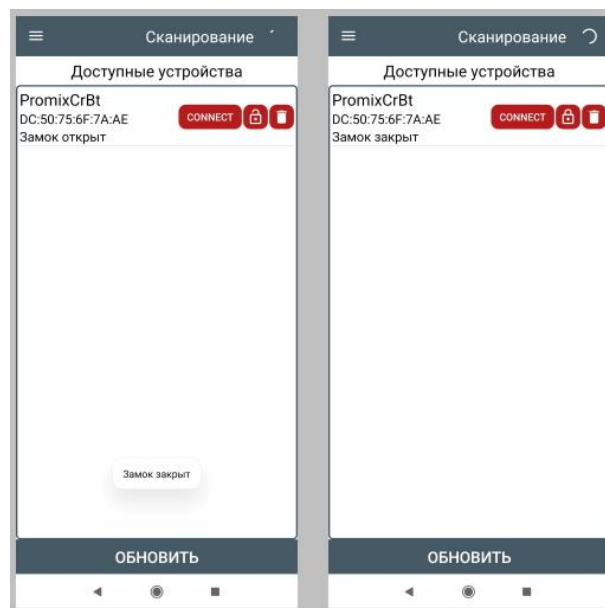
Данный способ позволяет изменять состояние замка из главного окна приложения, не вводя пароль доступа. Для использования этого способа необходимо сохранить контроллер/замок в базе устройств и задать ему действующий пароль (см. п. 4.1). После того как

При использовании данного способа рекомендуется включить в настройках пункт «Ввод pin-кода при входе в приложения».

контроллер/замок был добавлен в базу, изменять состояние замка можно из главного окна приложения, выбирая пункт «Открыть/Закрыть».



Инициирование изменения состояния замка из главного окна приложения



Успешное изменение состояния замка из главного окна приложения

2.4. Изменение состояния замка из уведомления

Данный способ позволяет управлять замком через уведомление, не заходя в само приложение.

Управление состоянием замка через уведомление рекомендуется использовать при ВКЛЮЧЕННОМ встроенного в смартфон средству защиты от несанкционированного доступа к устройству (графический ключ, пароль, отпечаток пальца).

Через уведомление управлять можно только одним контроллером/замком.

Если управление состоянием замка через уведомление включено, то управление с помощью виджета не доступно.

Для успешной настройки уведомления, управляющего состоянием замка, нужно проделать следующие действия:

- Добавить замок, которым требуется управлять (контроллер, состояние замка которого нужно изменить), в базу устройств и задать ему пароль, который будет использоваться при изменении состояния замка (см. п. 4.1).

При управлении состоянием замка через уведомление рекомендуется использовать постоянные пароли (пароли, которые не будут удалены из контроллера/замка без ведома администратора).

- Перейти в настройки приложения
- Включить пункт «Управление состоянием замка через уведомления»
- Выбрать замок, которым требуется управлять (контроллер, состояние замка которого нужно менять), нажав на пункт «Устройство управления» и в открывшемся списке выбрав нужный контроллер/замок.
- Выбрать режим управления замком, нажав на пункт «Режим управления» и в открывшемся списке выбрав нужный режим.

Описание режимов управления представлено далее.

Режим 1. Когда смартфон с запущенным уведомлением находится в зоне действия контроллера/замка, он автоматически подключится к нему и откроет замок. Далее пользователь вручную может изменять состояние замка из уведомления. Когда смартфон с запущенным уведомлением покинет зону действия контроллера/замка, он отключится от него.

ВНИМАНИЕ! С контроллером в один момент времени может быть соединен только один пользователь.

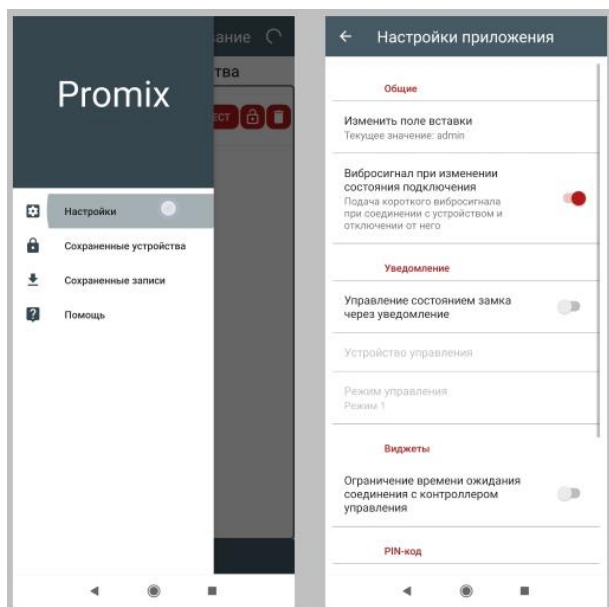
Режим 2. Пользователю предоставляется возможность вручную управлять подключением к контроллеру/замку, состоянием замка и отключением от контроллера/замка.

Режим 3. Пользователь предоставляется возможность изменять состояние замка, при которой не будет поддерживаться постоянное соединение с контроллером/замком. После получения команды на изменение состояния замка от пользователя запускается следующая последовательность действий:

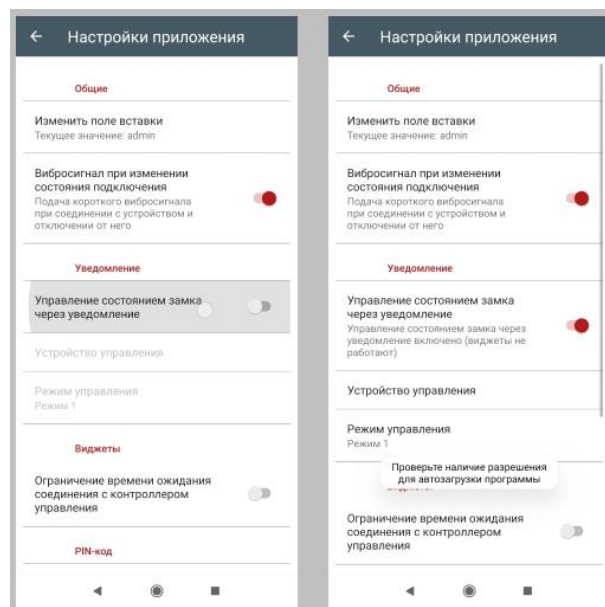
- подключение к контроллеру/замку (если подключиться не удастся, то происходит возврат в исходное состояние);
- изменение состояния замка;
- отключение от контроллера/замка.

Уведомление, работающее в режиме 2 или в режиме 3, появляется, когда на смартфоне включен Bluetooth и приложение «BT_CON» не запущено. Уведомление, работающее в режиме 1, появляется, когда на смартфоне включен Bluetooth, включен GPS (Местоположение) и приложение «Promix CrBt» не запущено.

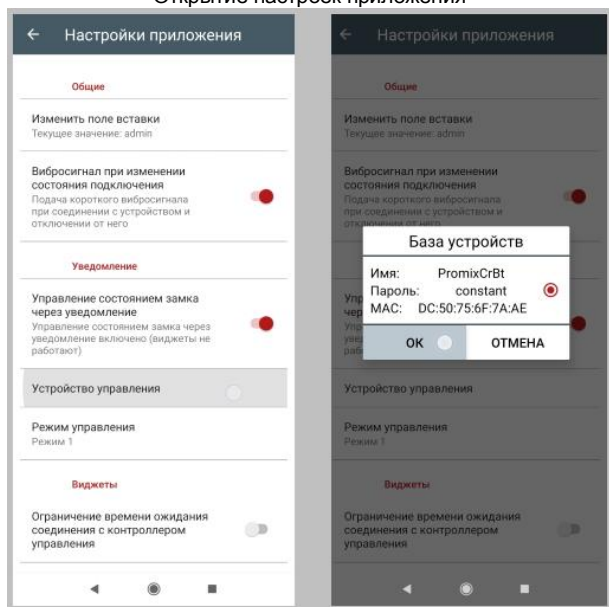
Если уведомление не появляется при описанных условиях, то нужно разрешить автозапуск приложению «Promix CrBt»



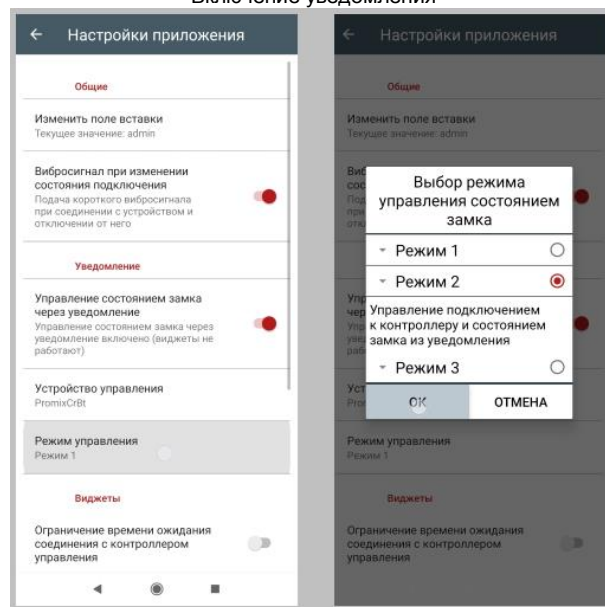
Открытие настроек приложения



Включение уведомления



Выбор устройства для управления из уведомления



Выбор режима управления

2.5. Изменение состояния замка с использованием виджета

Данный способ позволяет управлять замками через виджеты, не заходя в само приложение.

Управление состоянием замков через виджеты рекомендуется использовать при ВКЛЮЧЕННОМ встроенном в смартфон средстве защиты от несанкционированного доступа к устройству (графический ключ, пароль, отпечаток пальца).

Количество создаваемых виджетов не ограничено.

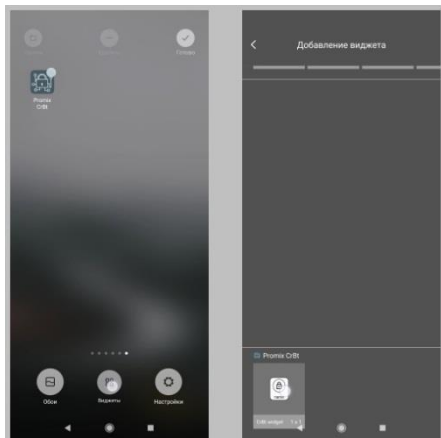
Для успешной настройки виджета нужно проделать следующие действия:

- Добавить замок, которым требуется управлять (контроллер, состояние замка которого нужно изменять), в базу устройств и задать ему пароль, который будет использоваться при изменении состояния замка (см. п. 4.1).

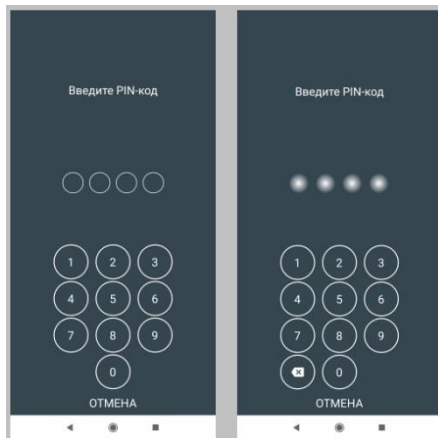
Если управление состоянием замка через уведомление включено, то управление с помощью виджета не доступно.

- Переместить виджет приложения на рабочий стол из меню доступных виджетов.
- В открывшемся окне конфигурации выбрать замок, которым требуется управлять (контроллер, состояние замка которого нужно изменять) и нажать на кнопку «Создать виджет».

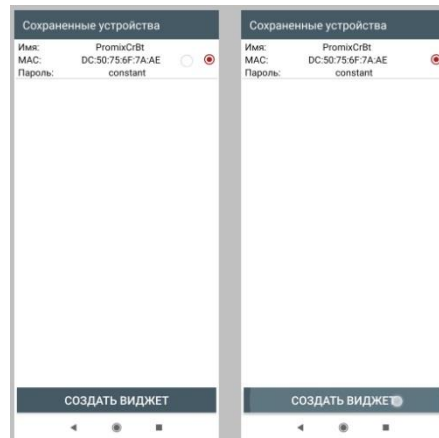
Принцип функционирования виджета аналогичен принципу работы уведомления в режиме 3 (см. п. 2.4).



Добавление виджета на рабочий стол



Ввод PIN-кода приложения



Выбор контроллера управления

2.6. Изменение настроек контроллера/замка

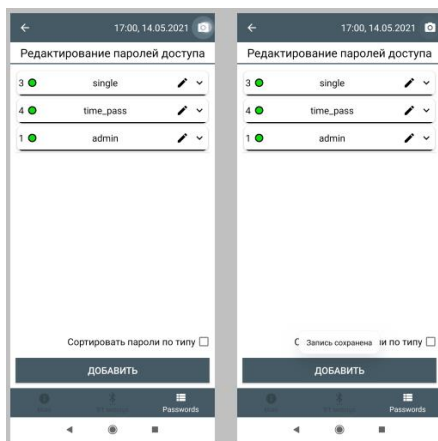
Для изменения настроек контроллера/замка необходимо подключиться к контроллеру (см. п. 2.2), используя пароль администратора, и в открывшемся окне перейти на вторую вкладку (вкладку настройки).

Настройки у разных контроллеров/замков могут отличаться. К общим для всех типов контроллеров/замков относятся Возможны следующие настройки:

- Имя контроллера.
- Тип замка:
 - нормально-открытый (замок, который открыт, когда на нем нет напряжения, и закрыт, когда на нем есть напряжение);
 - нормально закрытый (замок, который закрыт, когда на нем нет напряжения, и открыт, когда на нем есть напряжение).
- Включение/выключение звуковой индикации изменения состояния замка.
- Включение/выключение и настройка триггерного режима работы (см п. 2.9).
- Настройка параметров автогенерации паролей (см п. 2.10).
- Настройка времени на контроллере/замке (см. п. 2.11).

2.7. Сохранение «Снимка» контроллера/замка

Во время подключения к контроллеру/замку администратор может сохранять в память смартфона «Снимок» контроллера, в который входят текущие пароли и их характеристики (тип, статус, время функционирования), текущее время на контроллере, текущее имя контроллера и текущие параметры автогенерации паролей.



Сохранение «снимка» контроллера управления

После сохранения «Снимка» на смартфон, он может быть просмотрен в любое время. «Снимки» сохраняются в приложении в разделе «Сохраненные записи» (см. п.4.3).

2.8. Просмотр/добавление/изменение/удаление паролей

Пароли доступа задаются администратором. Под администратором понимается пользователь, который получил доступ к контроллеру, используя пароль администратора. Длина паролей может варьироваться от 5 до 15 символов включительно. Максимальное количество паролей доступа – 10.

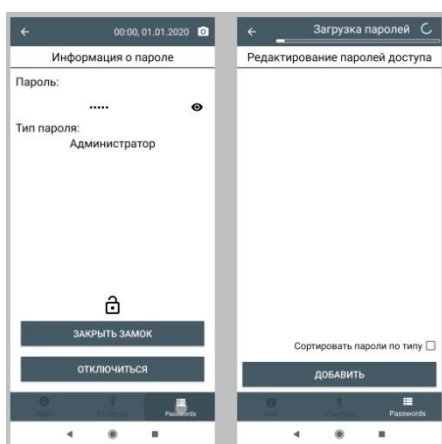
Изначально контроллер/замок содержит только один пароль – пароль администратора по умолчанию: admin. После первого подключения к контроллеру необходимо изменить пароль администратора!

Для добавления паролей необходимо подключиться к контроллеру, используя пароль администратора (см. п. 2.2) и перейти на вкладку «Passwords» в открывшемся окне.

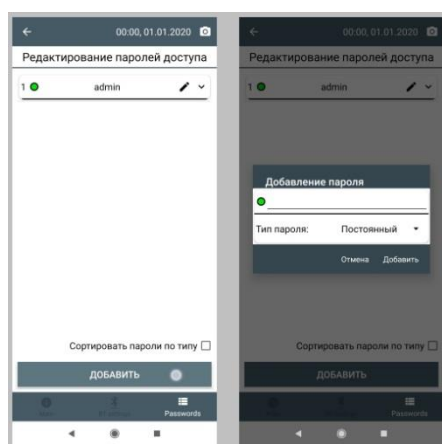
При добавлении и изменении паролей нужно учитывать следующие условия:

- длина пароля от 5 до 15 символов включительно;
- в пароле должны отсутствовать локализованные символы (русские буквы);
- для временных паролей время «От» должно быть строго меньше времени «До»;
- для временных паролей время «До» должно быть строго больше текущего времени на контроллере.

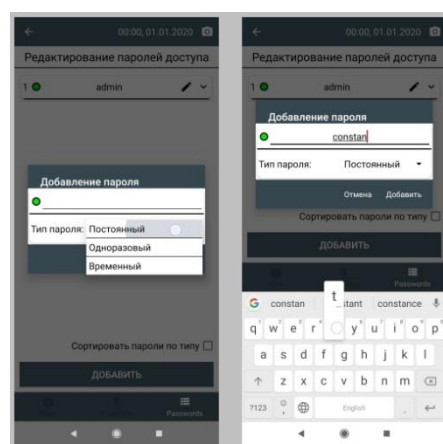
Для удаления паролей необходимо выбрать нужный пароль и нажать на кнопку «Удалить». Пароль администратора удалить нельзя.



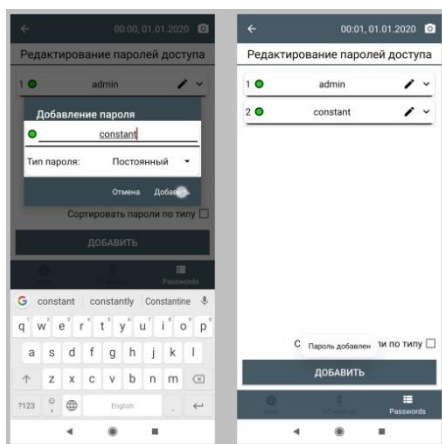
Переход на вкладку управления паролями



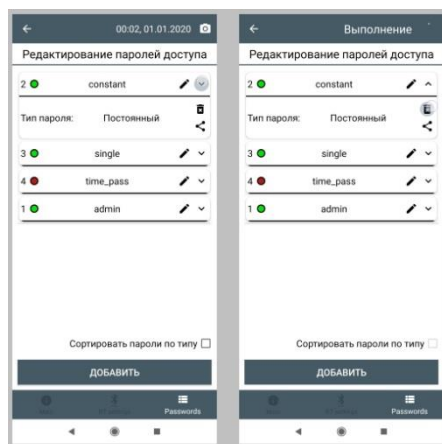
Выбор пункта добавления пароля



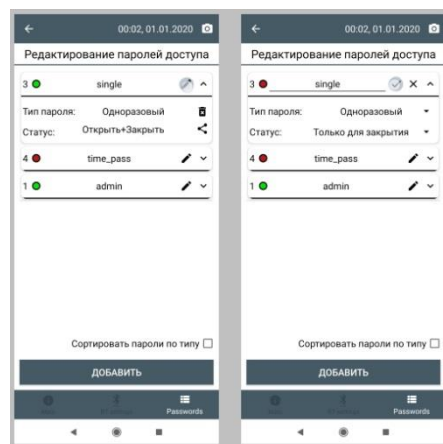
Добавление пароля (ввод/выбор параметров)



Добавление пароля



Удаление пароля



Изменение пароля

2.9. Триггерный режим работы контроллера/замка

Триггерный режим работы контроллера/замка заключается в следующем: после открытия замок автоматически закрывается через заданное количество секунд.

Для настройки триггерного режима работы на контроллере/замке необходимо подключиться к нему, используя пароль администратора (см. п. 2.2), и в открывшемся окне перейти на вторую вкладку (вкладку «BT settings»).

Для настройки триггерного режима работы доступны следующие возможности:

- Включение/выключение триггерного режима работы.
- Изменение времени открытия замка.

2.10. Автогенерация паролей доступа

Автогенерация предусмотрена для одноразовых и временных паролей. Включать, выключать автогенерацию и изменять ключ автогенерации может только пользователь, подключившийся к контроллеру, используя пароль администратора.

Автогенерация одноразовых паролей.

После того как с помощью одноразового пароля замок будет открыт и закрыт, пароль удаляется из памяти, а на его основе с помощью ключа автогенерации будет создан новый одноразовый пароль. Статус нового одноразового пароля – «Открытие+Закрытие».

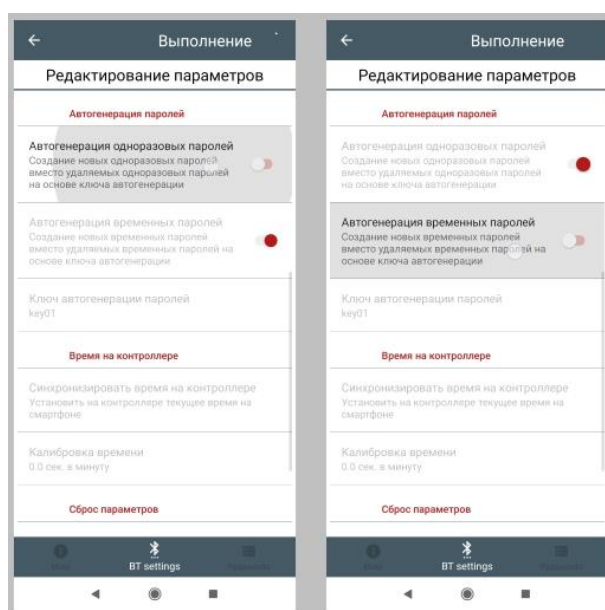
Автогенерация временных паролей.

После завершения периода функционирования временного пароля, пароль удаляется из памяти, а на его основе с помощью ключа автогенерации будет создан новый временный пароль. Время функционирования нового пароля – такой же интервал времени, как у старого пароля, начиная с момента удаления старого пароля. Например, если старый пароль был активен с 00:00 01.01.2020 до 01:00 05.01.2020, то созданный вместо него новый пароль будет функционировать с 01:00 05.01.2020 до 02:00 09.01.2020.

Сгенерированные пароли доступа базируются на ключе автогенерации и предыдущем значении пароля. Сгенерированные пароли состоят из цифр.

Ключ автогенерации – слово, длиной от 5 до 15 символов.

Для включения/выключения автогенерации паролей и изменения ключа автогенерации необходимо подключиться к контроллеру/замку (см. п. 2.2), используя пароль администратора, и перейти на вторую вкладку (вкладку «BT settings»).



2.11. Настройка времени на контроллере/замке

Для настройки времени на контроллере/замке необходимо подключиться к нему, используя пароль администратора (см. п. 2.2), и в открывшемся окне перейти на вторую вкладку (вкладку настройки).

Для настройки времени доступны следующие возможности:

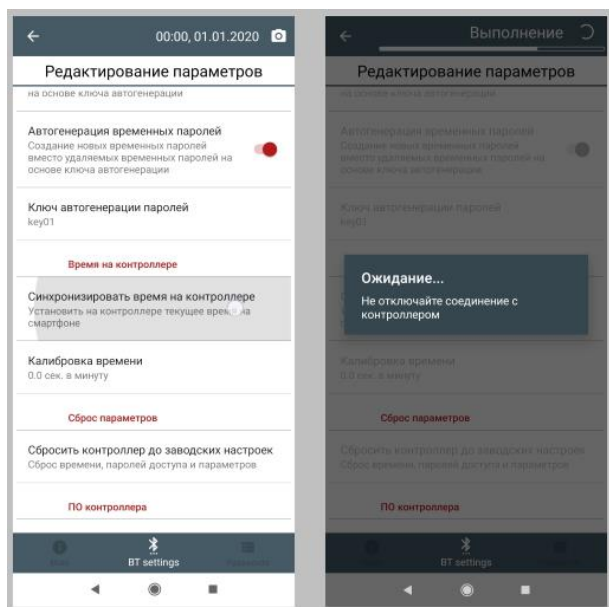
- «Синхронизировать время на контроллере».

Данная функция устанавливает на контроллере/замке текущее на смартфоне время. Первый раз вызов этой функции продолжается 10 секунд, следующие вызовы занимают время меньше 1 секунды.

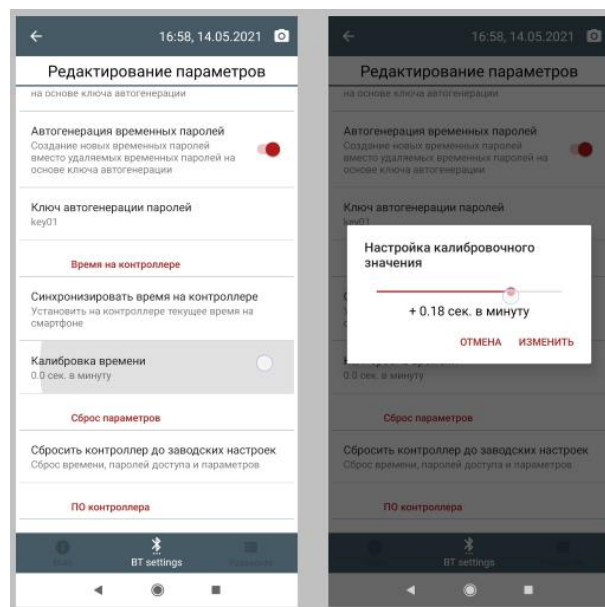
- «Калибровка времени».

Подстройка параметров часов на контроллере/замке. Необходимо, если отсчет времени на контроллере/замке спешит или отстает.

После первой синхронизации времени на контроллере/замке необходимо через несколько дней подстроить время. Калибровка времени проводится из следующего расчета: отличие времени на контроллере/замке через 1-2 минуты спустя 24 часа после синхронизации времени требует калибровки на $\pm 0,02$ единицы («плюс» в случае, если время на контроллере/замке спешит, «минус» - если отстает).



Синхронизация времени на контроллере/замке с смартфоном



Калибровка времени на контроллере/замке

3. НАСТРОЙКИ ПРИЛОЖЕНИЯ

3.1. Настройка ввода PIN-кода приложения

Для настройки параметров ввода PIN-кода необходимо перейти в настройки приложения. Для изменения доступны следующие пункты:

- «Использовать PIN-код при запуске».

Включение и выключение запроса внутреннего PIN-кода при запуске приложения.

Ввод PIN-кода рекомендуется включить при выключенной встроенной в смартфон защите от несанкционированного доступа к устройству (графический ключ, пароль, отпечаток пальца) и сохранении контроллеров/замков в базе устройств (см. п. 4.1), так как это дает возможность управлять состоянием замка из главного окна приложения (см п. 2.3) без ввода паролей доступа.

- «Разблокировка с использованием биометрии».

Включение и отключение возможности использования вместо ввода внутреннего PIN-кода разблокировку по отпечатку пальца, разблокировку по лицу и т. п. Данный пункт меню может отсутствовать, если на устройстве нет возможности использования биометрических параметров.

- «Изменить PIN-код».

Возможность изменения внутреннего PIN-кода приложения.

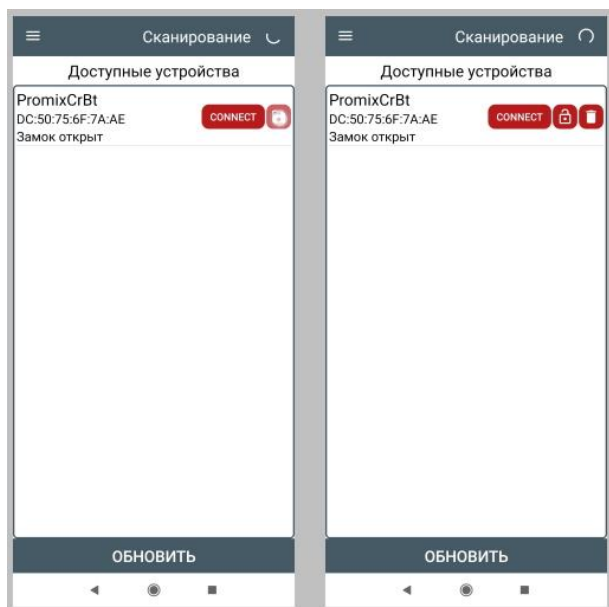
- «Поле для вставки».

Служит для упрощения ввода пароля доступа при подключении к устройству (см. п. 2.2). Для изменения поля для вставки необходимо перейти в настройки приложения выбрать пункт «Изменить поле для вставки».

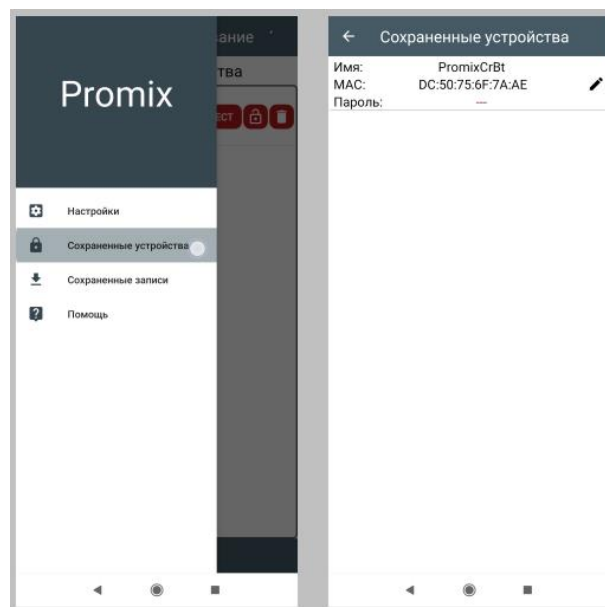
4. БАЗЫ ДАННЫХ ПРИЛОЖЕНИЯ

4.1. Добавление контроллера/замка в базу устройств

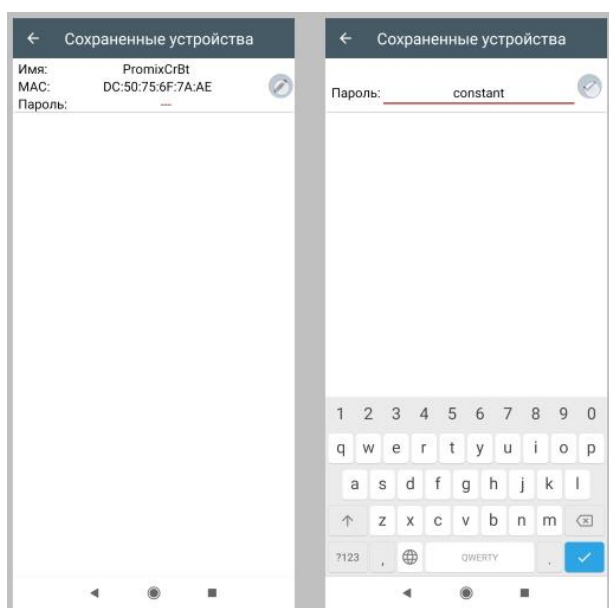
Для добавления контроллера/замка в базу устройств нужно войти в зону действия контроллера, включить Bluetooth и GPS (Местоположение). Запустить приложение, ввести PIN-код при необходимости, после того, как нужный контроллер/замок будет найден, нажать на кнопку сохранения устройства (кнопка, справа от кнопки CONNECT) и выбрать пункт «Добавить в базу». После этого необходимо зайти в раздел «Сохраненные устройства» и задать пароль по умолчанию для сохраненного контроллера/замка.



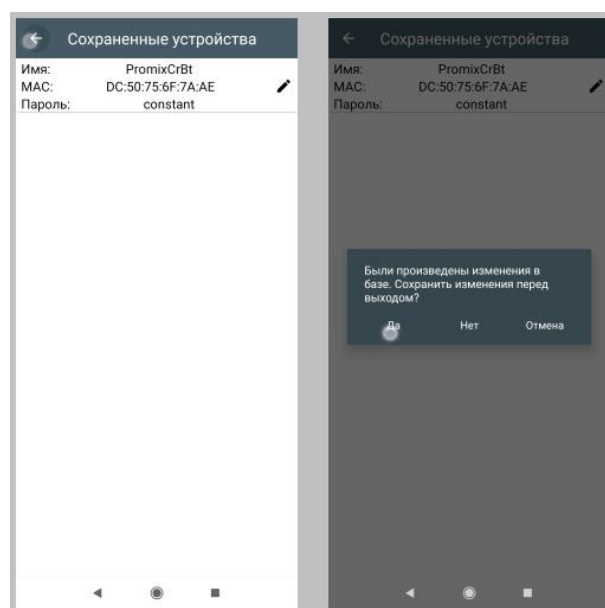
Добавление контроллера в базу устройств



Открытие базы сохраненных устройств



Задание пароля доступа по умолчанию для контроллера/замка



Сохранение изменений в базе устройств

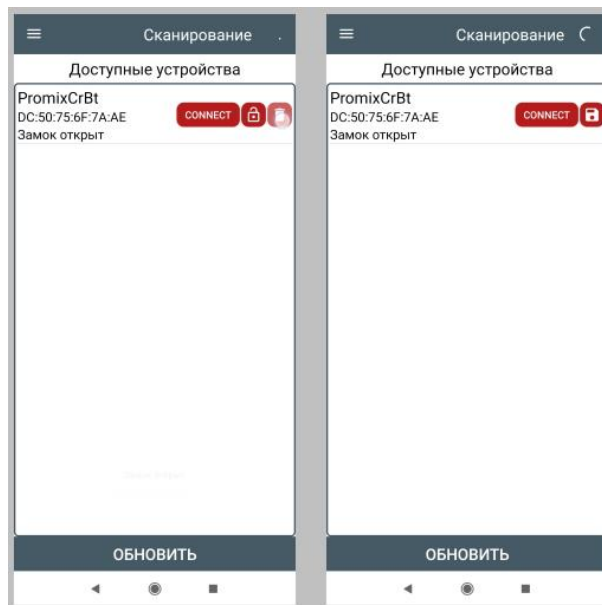
4.2. База устройств

В базе устройств можно просмотреть сохраненные контроллеры/замки и задать им пароли для использования по умолчанию при управлении состоянием замка из главного окна приложения (см. п. 2.3), из уведомления (см. п. 2.4) и из виджетов (см. п. 2.5).

Добавление устройств описано в п. 4.1.

Для удаления контроллера/замка из базы устройств нужно войти в зону действия контроллера, включить Bluetooth и GPS (Местоположение). Запустить приложение, ввести PIN-код при необходимости, после того, как нужный контроллер/замок будет найден, нажать на кнопку удаления из базы устройств (кнопка, справа от кнопки CONNECT и быстрого изменения состояния замка).

Запись сохраненного контроллера/замка (имя сохраненного устройства) автоматически обновляется при появлении записи при поиске устройств (в главном окне приложения).



Удаление контроллера/замка из базы устройств

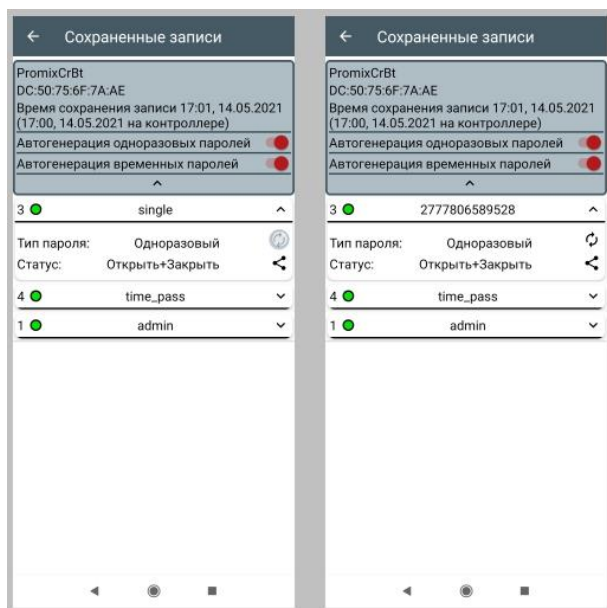
4.3. База записей контроллеров/замков

База записей хранит «Снимки» контроллеров/замков.

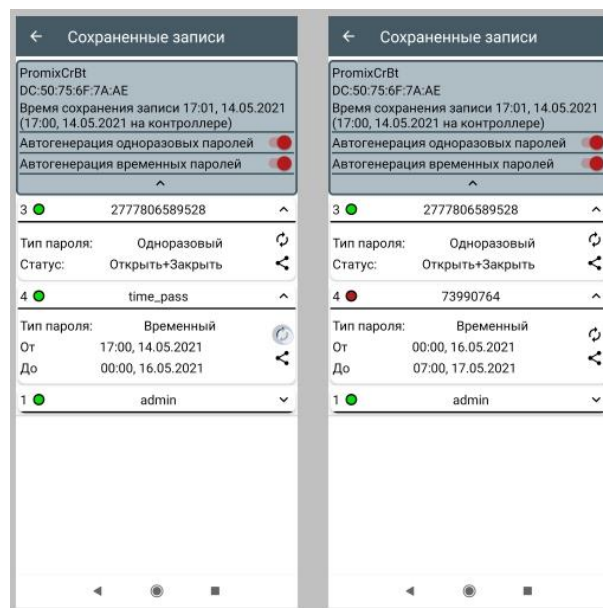
«Снимок» контроллера содержит:

- Пароли, содержащиеся в контроллере/замке, на момент сохранения «Снимка», и их характеристики (тип, статус, время функционирования);
- Время сохранения записи;
- Время на контроллере в момент сохранения записи.

«Снимок» дает возможность пользователю просматривать пароли доступа без соединения с контроллером/замком и делиться ими с другими пользователями, просматривать результат автогенерации временных и одноразовых паролей (см. п. 2.10).



Автогенерация одноразового пароля без подключения к контроллеру/замку



Автогенерация временного пароля без подключения к контроллеру/замку

Создание «Снимка» описано в п. 2.7.

Для удаления «Снимка» (или пароля из «Снимка») необходимо смахнуть запись «Снимка» (или запись пароля из «Снимка») вправо. Все изменения – удаление и автогенерация паролей – могут быть сохранены перед выходом из базы записей.