# Система контроля и управления доступом Sigur.

# Считыватель «Sigur MR1».

## Описание и инструкция по эксплуатации

«Промавтоматика», г. Н. Новгород, 2019 г.

Оглавление

# 1. Введение.

Данный документ содержит описание и инструкцию по эксплуатации считывателя «Sigur MR1».

Считыватель «Sigur MR1» предназначен для защищённой идентификации в системах контроля доступа с помощью карт Mifare (Ultralight, Mini, ID, Classic, DESFire, Plus), а также банковских карт: МИР, Visa и MasterCard.

Модификация считывателя «Sigur MR1 BLE» позволяет проходить идентификацию также по смартфону с операционной системой Android или iOS, используя технологию BLE (Bluetooth Low Energy). Модификация позволяет гибко настраивать световую и звуковую индикацию считывателя.

# 2. Технические характеристики.

| | |
|---|---|
| Формат поддерживаемых идентификаторов | |
| Карты Mifare Ultralight, Mini, ID, Plus, DESFire, включая защищённый режим Mifare Classic и Mifare Plus SL3 | |
| Бесконтактные банковские карты в режиме эмуляции карт Mifare. Поддерживаются карты MasterCard, Visa и МИР | |
| Смартфон (Android, iOS) с использованием технологии BLE | |
| Любые идентификаторы стандарта ISO 14443-A | |
| Технические параметры | |
| Дальность чтения карт | 4-9 см (в зависимости от карты и режима работы) |
| Дальность чтения смартфонов | До 10 метров при прямой видимости |
| Интерфейс для связи с контроллером | Wiegand настраиваемой битности (26, 34, 58) |
| Габариты | 90x90x12 мм |
| Вес | Вес брутто – 285 г; Вес нетто – 170 г |
| Температурный режим | от -25 до +55 °C |
| Класс защиты | IP65 |
| Напряжение питания | 12 В (9…15В) |
| Потребляемый ток | 90 мА в режиме ожидания, 130 мА при чтении карты |
| **Индикация** | |
| Световая | Многоцветный светодиодный индикатор |
| Звуковая | Широкополосный акустический динамик,<br>PCM 16 бит 44.1 кГц моно. |
| Поддерживаемые звуковые форматы | .wav, .aiff, .au |
| Емкость загружаемых звуков | Не более 45 секунд. |
| **Средства диагностики** | |
| Датчик открытия корпуса | |
| Датчик температуры | |

**Таблица 1. Технические характеристики «Sigur MR1».**

# 3. Комплект поставки.

| Номер | Позиция | Количество |
|---|---|---|
| 1 | Считыватель «Sigur MR1» | 1 шт. |
| 2 | Настенная панель | 1 шт. |
| 3 | Ключ | 1 шт. |
| 4 | Комплект крепежа | 1 шт. |
| 5 | Набор соединителей ScotchLock | 1 шт. |
| 6 | Инструкция по монтажу | 1 шт. |

**Таблица 2. Комплект поставки «Sigur MR1».**

# 4. Общие функции считывателя в СКУД «Sigur».

Считыватель «Sigur MR1» совместим со СКУД «Sigur», а также с большинством других систем контроля доступа.

Считыватель поддерживает работу со следующими типами идентификаторов:

- картами формата Mifare Ultralight, Mini, ID, Classic, DESFire, Plus в режиме чтения их уникального идентификатора – UID, и в защищённом режиме работы Mifare Classic и в режиме SL3 карт Mifare Plus;
- любыми другими идентификаторами стандарта ISO 14443-A в режиме чтения UID;
- бесконтактными банковскими картами МИР, Visa и MasterCard в режиме эмуляции карт Mifare;
- смартфонами с ОС Android или iOS по технологии BLE (Bluetooth Low Energy) при установленном мобильном приложении «Доступ».

Считыватель оснащён:

- Wiegand–выходом настраиваемой битности;
- многоцветным световым индикатором;
- широкополосным акустическим динамиком;
- тремя цифровыми входами для управления индикацией считывателя;
- средствами самодиагностики, в том числе датчиком вскрытия корпуса.

# 5. Подключение считывателя и аппаратный сброс.

*Для подключения считывателя к контроллеру СКУД обратитесь к документации контроллера данной СКУД.*

Ниже следует описание проводов считывателя, а также процесса проведения аппаратного сброса считывателя к заводским параметрам.

## 5.1. Назначение проводов считывателя.

| Цвет | Название | назначение |
|---|---|---|
| Красный | +12 V | «Плюс» напряжения питания |
| Чёрный | GND | «Общий» напряжения питания, линий данных и управления |
| Зелёный | Data 0 | Линия данных Wiegand 0 |
| Белый | Data 1 | Линия данных Wiegand 1 |
| Синий | IN1/Allow/Green | Включение звукового и светового сигнала разрешения доступа |
| Коричневый | IN2/Deny/Red | Включение звукового и светового сигнала запрета доступа |
| Жёлтый | IN3/Beep | Включение монотонного звукового сигнала. Используется также для аппаратного сброса считывателя к заводским настройкам |

**Таблица 3. Назначение проводов считывателя «Sigur MR1».**

## 5.2. Сброс параметров считывателя к заводским настройкам.

Считыватель поддерживает функцию аппаратного сброса настроек на заводские. Для сброса настроек необходимо:

1. Отключить питание считывателя.
2. Замкнуть между собой зеленый (Data 0) и жёлтый (Beep) провода.
3. Подать питание на считыватель и разъединить провода.

При успешном сбросе считыватель издаст характерный звуковой сигнал.

# 6. Общие настройки считывателя.

## 6.1. Управление звуковой и световой индикацией считывателя по двум линиям.

Линии Allow/Green и Deny/Red используются для управления индикацией разрешения или запрета доступа: включается зелёный или красный светодиод на установленный интервал времени, а также проигрывается предустановленный звуковой сигнал «Разрешение доступа» или «Запрет доступа».

Активный уровень линий управления – ноль вольт.

*Если считыватель подключён к контроллеру «Sigur», то следуйте приведённому ниже примеру настроек. Если считыватель подключён к стороннему контроллеру, то обратитесь к документации данной СКУД.*

В программе «Клиент» перейдите во вкладку «Оборудование», выберите первую точку доступа на данном контроллере и нажмите кнопку «Настройки».

Для контроллеров E(R)500U, E(R)900U выполните следующие настройки:

- Отключите опцию «Отображать только базовые настройки»;
- Найдите функцию «Импульс разрешения доступа на «Вход»» (или «Выход», в зависимости от того, в каком направлении подключён данный считыватель) и установите её значение равным LED1(PORT**N**)/L**N**A/LED(PORT**N**), где **N** – номер порта на контроллере, куда подключен считыватель. В выпадающем меню справа оставьте «Нормально не активен».
- Найдите функцию «Импульс запрета доступа на «Вход»» (или «Выход», в зависимости от того, в каком направлении подключён данный считыватель) и установите её значение равным LED2(PORT**N**)/L**N**A/LED(PORT**N**), где **N** – номер порта на контроллере, куда подключен считыватель. В выпадающем меню справа оставьте «Нормально не активен».
- Найдите в списке параметр «Длина импульса разрешения/запрета доступа» и установите его равным порядка 1 с. (или иное время включения световой индикации разрешения/запрета доступа).

Для контроллеров E(R)500, E(R)500D4, E(R)900I, E300(H) включите опцию «Общее» и выключите опцию «Отображать только базовые настройки».

Найдите в списке параметр «Длина импульса разрешения/запрета доступа» и установите его равным порядка 1 с. (или иное время включения световой индикации разрешения/запрета доступа).

Затем перейдите на вкладку «Переназначение клемм» и добавьте две строки:

- Функция: «Импульс разрешения доступа на «Вход»» (или «Выход», в зависимости от того, в каком направлении подключён данный считыватель).
- Точка доступа: номер ТД контроллера, которую обслуживает считыватель.
- Клемма: LED1(PORT**N**)/L**N**A/LED(PORT**N**), где **N** – номер порта на контроллере, к которому подключён считыватель.

и

- Функция: «Импульс запрета доступа на «Вход»» (или «Выход», в зависимости от того, в каком направлении подключён данный считыватель).
- Точка доступа: номер ТД контроллера, которую обслуживает считыватель.
- Клемма: LED2(PORT**N**)/L**N**A/LED(PORT**N**), где **N** – номер порта на контроллере, к которому подключён считыватель.

## 6.2. Настраиваемая индикация считывателя.

*Световая и звуковая индикация считывателя «Sigur MR1 BLE» может быть гибко настроена только средствами ПО «Sigur». Для настройки подойдёт также Бесплатная версия.*

Настройка производится в два этапа:

1. С помощью клиентского ПО «Sigur» создаётся профиль индикации. В окне настроек загружаются звуки и создаются реакции считывателя на какое-либо событие. После окончательной настройки профиль прикрепляется к письму и отправляется на указанный e-mail средствами ПО «Sigur».
2. Полученный по почте профиль индикации открывается на смартфоне в приложении «Настройки», после чего загружается на считыватель по беспроводной технологии BLE.

Для настройки индикации считывателя откройте программу «Клиент» и перейдите в меню «Файл — Настройки — Индикация».

Данное окно имеет 3 вкладки:

- Профили – содержит список профилей индикации. По умолчанию в нём создан один «Стандартный профиль», индикация которого совпадает с заводской индикацией считывателя.

  В данной вкладке создаются новые профили индикации: в профиле назначается индикация считывателя в «ждущем режиме», а также указывается реакция на какое-либо внешнее воздействие.

- Реакции – содержит список ранее настроенных реакций, а также стандартные реакции считывателя.

  В данной вкладке создаются новые реакции считывателя: указывается тип световой и звуковой индикации.

- Звуки – содержит список ранее загруженных звуков и стандартные звуки.

  В данной вкладке можно загрузить звуки из файла, а также прослушать ту или иную запись в списке.

### 6.2.1. Добавление звука реакции считывателя. Вкладка «Звуки».

Для загрузки нового звукового файла в ПО перейдите во вкладку «Файл — Настройки — Индикация — Звуки». Нажмите на кнопку «+» сверху. В открывшемся окне выберите желаемый файл формата .wav, .aiff или .au.

Имя звука задаётся в поле «Название». После изменения имени необходимо нажать «Применить».

В этой же вкладке вы можете прослушать любой звук из списка, нажав соответствующие кнопки воспроизведения в нижнем правом углу.

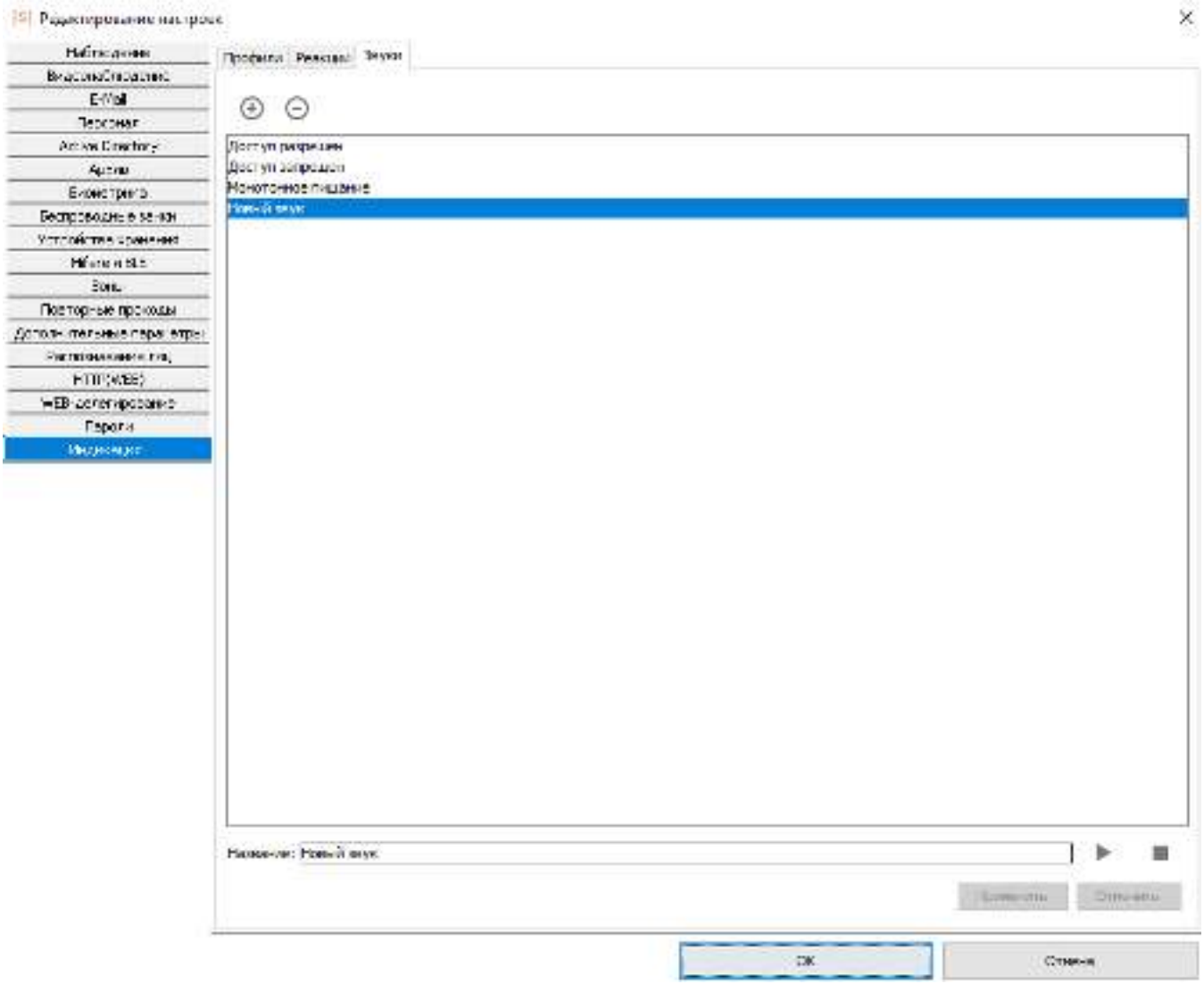


***Рисунок 1. Вкладка «Звуки».***

### 6.2.2. Создание реакции считывателя. Вкладка «Реакции».

Для добавления новой реакции считывателя на какое-либо событие перейдите во вкладку «Файл — Настройки — Индикация — Реакции». Новая реакция создаётся путём нажатия кнопки «+» или копированием другой реакции соответствующей кнопкой.

Имя реакции задаётся в поле «Название». После изменения имени необходимо нажать «Применить».

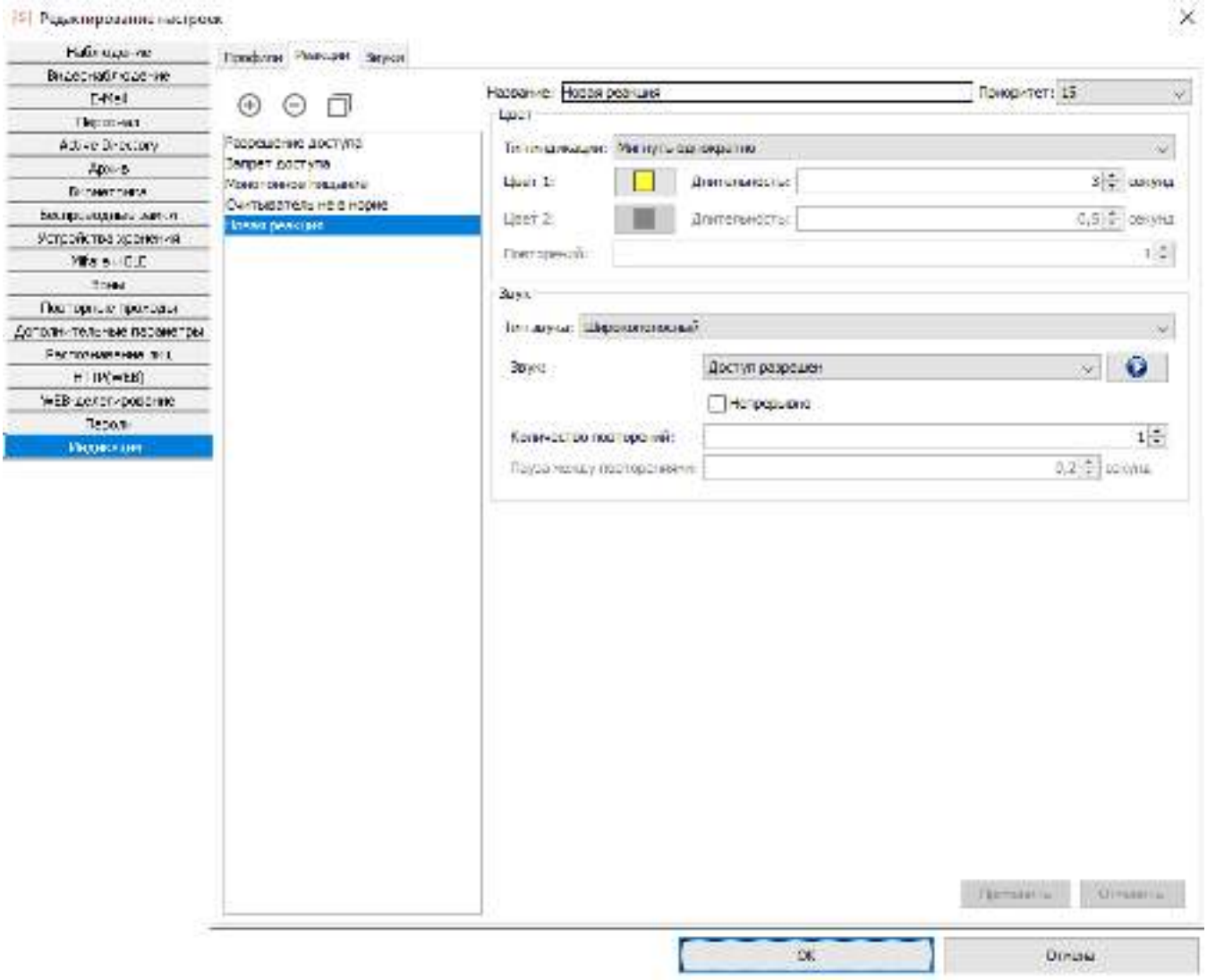



***Рисунок 2. Вкладка «Реакции».***

Реакция содержит следующие основные элементы:

1. **Тип индикации** — определяет тип световой индикации считывателя на событие. Тип световой индикации может быть:

   - *«Без реакции»* – световая индикация на событие отсутствует. Цвет светодиода не будет изменён.
   - *«Мигнуть однократно»*[2] – считыватель мигает 1 раз установленным цветом на установленное вами время.

- *«Мигание несколько раз»*[2] – считыватель мигает установленное количество раз двумя цветами с установленной длительностью.
- *«Сменить цвет»*[1] – считыватель меняет цвет светодиода на установленный.
- *«Мигание непрерывно»*[1] – считыватель мигает непрерывно двумя цветами с установленной длительностью.

**2.** **Тип звука** — определяет тип звуковой индикации считывателя на событие. Типы звуковой индикации могут быть следующими:

- *«Без реакции»* – звуковая индикация на событие отсутствует.
- *«Широкополосный»* – воспроизводится один из пользовательских звуков вкладки «Звуки».
  Звук воспроизводится либо установленное число раз[2], либо непрерывно[1]. В обоих случаях может быть установлен интервал пауз.

(1) – Длительность реакции определяется длительностью события.

(2) – Фиксированная длительность реакции.

.

**3.** **Приоритет** – параметр, определяющий, сменится ли индикация реакции при наступлении другой реакции.

| Тип реакции | | Приоритет текущей реакции | Результат. Наступающая реакция: |
|---|---|---|---|
| Текущей | Наступающей | | |
| 1 | 1 | Меньше или равен | Перекроет текущую |
| | | Больше | Не перекроет текущую |
| 1 | 2 | Меньше или равен | Перекроет текущую |
| | | Больше | Не перекроет текущую |
| 2 | 1 | Меньше | Перекроет текущую |
| | | Больше или равен | Не перекроет текущую |
| 2 | 2 | Любой | Перекроет текущую |

**Таблица 4. Смена реакций в зависимости от их приоритетов и типов.**

После внесения изменений в настройки реакции необходимо нажать «Применить».

### 6.2.3. Создание профиля индикации считывателя. Вкладка «Профили».

Для добавления нового профиля индикации считывателя перейдите во вкладку «Файл — Настройки — Индикация — Профили». Новый профиль индикации создаётся путём нажатия кнопки «+» или копированием другого профиля соответствующей кнопкой.

Имя профиля индикации может быть изменено в поле «Название». После изменения имени необходимо нажать «Применить».

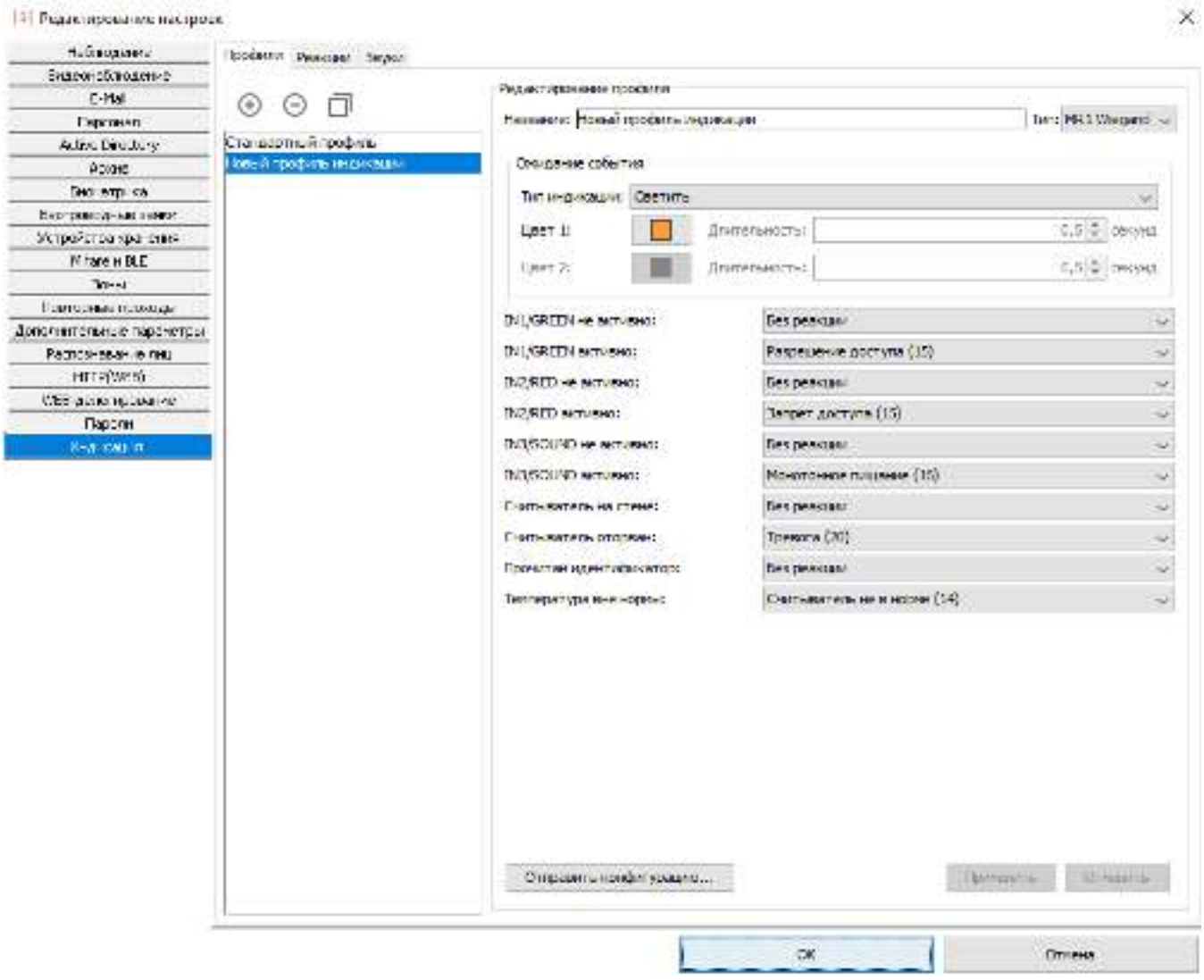



***Рисунок 3. Вкладка «Профили».***

Профиль индикации позволяет настроить:

1. **Световую индикацию считывателя ожидания наступления какого-либо события.**

   Параметр «Тип индикации» может иметь следующие значения:

   - «Светить» - цвет светодиода не меняется до наступления какого-либо события.
   - «Мигать» - считыватель мигает одним или двумя цветами с установленным интервалом до наступления какого-либо события.

**2. Реакцию считывателя на наступление какого-либо события.**

Считыватель имеет три линии управления индикацией: IN1/GREEN; IN2/RED и IN3/SOUND.

Активный уровень линий управления – ноль вольт.

Какая-либо реакция из вкладки «Реакции» может быть назначена на одну из представленных ниже функций.

| **Название функции** | **Описание. Реакция активируется при:** |
|---|---|
| IN1/GREEN не активно | линия GREEN не подключена на GND. |
| IN1/GREEN активно | линия GREEN подключена на GND. |
| IN2/RED не активно | линия RED не подключена на GND. |
| IN2/RED активно | линия RED подключена на GND. |
| IN3/SOUND не активно | линия Beep не подключена на GND. |
| IN3/SOUND активно | линия Beep подключена на GND. |
| Считыватель на стене | задняя крышка считывателя находится в закрытом положении (на считывателе). |
| Считыватель оторван | задняя крышка считывателя находится в открытом положении (не на считывателе). |
| Прочитан идентификатор | чтении идентификатора считывателем (карта или смартфон). |
| Температура вне нормы | выходе температуры считывателя из пределов нормы. |

**Таблица 5. Функции вкладки «Профили».**

После настройки профиля индикации необходимо нажать «Применить».

Для загрузки профиля индикации на считыватель нажмите кнопку «Отправить конфигурацию» и введите e-mail. На указанный e-mail придёт письмо с прикреплённым файлом конфигурации.

Для дальнейшей работы на смартфоне должно быть установлено приложение «Настройки» (его можно будет скачать по ссылке из письма). Для загрузки профиля индикации на считыватель следуйте пункту Загрузка профиля индикации на считыватель.

## 6.3. Настройка реакции на вскрытие корпуса считывателя.

При открытии и закрытии корпуса считывателя на управляющий контроллер отправляются специальные Wiegand-посылки.

По приходу на сервер данных Wiegand-посылок можно настроить какую-либо реакцию системы.

*Если считыватель подключён к стороннему контроллеру, то для настройки обратитесь к документации данной системы.*

При подключении считывателя к контроллерам «Sigur» можно настроить реакцию системы, используя дополнительный модуль «Реакция на события». В качестве данной реакции могут выступать: отправка уведомления, блокировка точек доступа и т.п.

Пример настроек:

- В программе «Клиент» создайте две новых учётных карточки пользователя с любыми именами, например: «Открытие корпуса считывателя» и «Закрытие корпуса считывателя».
- У пользователя «Открытие корпуса считывателя» в поле «Пропуск» установите W58 и значение, равное «FFFFFFFFFFFF00» (без кавычек). У учётной записи «Закрытие корпуса считывателя» сделайте аналогично со значением, равным «FFFFFFFFFFFF01».
- Удалите все точки доступа у данных пользователей на вкладке «Общее».
- Перейдите во вкладку «События», создайте новое событие кнопкой «Добавить событие».
- В пункте «Редактирование события» установите тип события: «По факту запрета доступа».
- Объект доступа – «Открытие корпуса считывателя» и/или «Закрытие корпуса считывателя».
- Выберите точки доступа из списка, к которым подключены считыватели «Sigur MR1». Укажите фиксируемые направления («Вход», «Выход»).
- В пункте «Редактирование реакции на событие» выберите необходимую вам реакцию:
    - установить режим точек доступа;
    - уведомить оператора;
    - отправлять SMS/PUSH/Telegram сообщение;
    - отправлять e-mail;
    - осуществлять HTTP-запрос;
    - выполнить команду ОС.

Пример настройки того или иного типа реакции на событие приведён в документе «Руководство пользователя ПО «Sigur».

# 7. Программирование считывателя.

*Программирование считывателя на текущий момент производится только средствами ПО «Sigur». Для настройки считывателя необходимо создать мастер-карту. Вам потребуется:*

- *Карта Mifare Classic или Mifare Plus в транспортной конфигурации, т.е. «чистая».*
- *Настольный USB-считыватель модели ACR 1252U.*
- *ПО «Sigur» с официального сайта. Для настройки подойдёт также Бесплатная версия.*

Мастер-карта Sigur необходима для программирования считывателя «Sigur MR1». С помощью мастер-карты можно задать следующие параметры считывателя:

- разрядность Wiegand-выхода;
- режим работы с картами Mifare Classic и Plus (UID или защищённый). Для защищённого режима указываются реквизиты доступа к памяти карты;
- сервисный пароль считывателя;
- ключ для идентификации по смартфону;
- дальность срабатывания считывателя при идентификации по смартфону;
- политика срабатывания считывателя при идентификации по смартфону.

После установки или изменения данных параметров в программном обеспечении необходимо создать мастер-карту Sigur.

Для этого в меню «Файл – Настройки – Mifare и BLE» нажмите на кнопку «Эмиссия мастер-карты Sigur». Поднесите любую чистую карту (Mifare Classic или Mifare Plus) к настольному считывателю. При успешной (или неуспешной) записи данных на карту программа уведомит вас.

**Для создания мастер-карты Sigur с иными параметрами понадобится другая чистая карта.**

Запрограммировать считыватель «Sigur MR1» можно, произведя его аппаратный сброс. Процесс описан в разделе «Сброс параметров считывателя к заводским настройкам».

После сброса к заводским настройкам необходимо поднести мастер-карту к считывателю в течение 25 секунд.

При поднесении мастер-карты считыватель издаст характерный звук (такой же, как при аппаратном сбросе). Удерживайте карту у считывателя несколько секунд до появления звука разрешения  или запрета доступа (светодиод загорится зелёным/красным).

# 8. Работа с картами Mifare и банковскими картами.

## 8.1. Работа в незащищённом режиме, чтение UID.

Для карт Mifare и бесконтактных банковских карт МИР, Visa и MasterCard в режиме эмуляции карт Mifare поддерживается функция считывания их открытого уникального идентификатора – UID.

По умолчанию считыватель настроен на чтение UID карты и выдаёт его в формате Wiegand-26. Вы можете изменить выходной формат Wiegand на другой.

Для настройки:

- В программе «Клиент» перейдите в меню «Файл - Настройки». Выберите пункт «Mifare и BLE». Установите сверху пункт «Формат идентификатора пропуска» равным одному из следующих вариантов: Wiegand-26 (3 байта UID), Wiegand-34 (4 байта) или Wiegand-58 (7 байт). Эта настройка предназначена как для конфигурации выходного формата считывателя, так и для настройки формата получаемых номеров карт с настольного считывателя.
- В этом же меню выберите вкладку, на которой указан формат ваших карт (Classic, DESFire или Plus). Какой формат карт Mifare эмулирует ваша банковская карта вам необходимо уточнить напрямую у банка.
- Установите пункт «В качестве идентификатора пропуска использовать» равным «UID».
- Если дальнейших настроек считывателя не требуется, то нажмите «Эмиссия мастер-карты Sigur» и приложите любую чистую карту к контрольному USB-считывателю. Далее следуйте разделу п.7 «Программирование считывателя».

## 8.2. Работа в защищённом режиме. Эмуляция Mifare банковской картой.

Считывателем поддерживается защищённый режим работы для карт Mifare Classic и Mifare Plus SL3, а также банковских карт МИР, Visa и MasterCard в режиме эмуляции карты Mifare Classic или Plus.

Другие режимы эмуляции карт Mifare не могут быть использованы для реализации защищённого режима работы и подойдут только для чтения их UID.

### 8.2.1. Настройка работы с картами Mifare Classic.

- В программе «Клиент» перейдите в меню «Файл — Настройки».
- Выберите пункт «Mifare и BLE», вкладку «Classic».
- Установите значение «В качестве идентификатора пропуска использовать» равным «Данные из памяти (защищённый режим)».

| | |
|---|---|
| **!** | **Если у вас уже был выбран данный режим и использовались карты Mifare, то ни в коем случае не изменяйте реквизиты доступа системы к памяти карт. Это приведёт к тому, что новые карты не будут иметь доступ к старым считывателям, а старые — к новым. Придётся перезаписать все старые карты, используя новые реквизиты и перепрограммировать все остальные считыватели.** |

- «Номер блока памяти» (в шестнадцатеричном формате) в большинстве случаев значение достаточно оставить равным по умолчанию.
- «Ключ для доступа к памяти». Как правило, достаточно нажать кнопку «Сгенерировать ключ».
- «В память карты записывать» - выберите либо «Автосгенерированное значение», либо «UID карты». В большинстве случаев достаточно оставить равным по умолчанию.
- Если дальнейших настроек считывателя не требуется, то нажмите «Эмиссия мастер-карты Sigur» и приложите любую чистую карту к контрольному USB-считывателю. Далее следуйте пунктам работы с мастер-картой Sigur.

### 8.2.2. Настройка работы с картами Mifare Plus.

- В программе «Клиент» перейдите в меню «Файл — Настройки».
- Выберите пункт «Mifare и BLE», вкладку «PLUS».
- Выберите ваш тип карты: PLUS S или PLUS X.
- Установите значение «В качестве идентификатора пропуска использовать» равным «Данные из памяти (защищённый режим)».

| | |
|---|---|
| **!** | **Если у вас уже был выбран данный режим и использовались эти карты Mifare, то ни в коем случае не изменяйте реквизиты доступа системы к памяти карт. Это приведёт к тому, что новые карты не будут иметь доступ к старым считывателям, а старые — к новым. Придётся перезаписать все старые карты, используя новые реквизиты и перепрограммировать все остальные считыватели.** |

- «Номер блока памяти» в шестнадцатеричном формате. В большинстве случаев значение достаточно оставить равным по умолчанию.
- «Ключ для доступа к памяти». Как правило, достаточно нажать кнопку «Сгенерировать ключ». Остальные поля заполнятся автоматически.
- «В память карты записывать» - выберите либо «Автосгенерированное значение», либо «UID карты». В большинстве случаев достаточно оставить равным по умолчанию.
- Если дальнейших настроек считывателя не требуется, то нажмите «Эмиссия мастер-карты Sigur» и приложите любую чистую карту к контрольному USB-считывателю. Далее следуйте пунктам работы с мастер-картой Sigur.

### 8.2.3. Настройка работы с банковскими картами.

| | |
|---|---|
| ! | **Возможность работы банковских карт со СКУД напрямую зависит от банка, производящего эмиссию карт.**<br><br>**Режим, в котором сейчас находится карта, необходимо уточнять напрямую у банка. Если карты находятся в режиме эмуляции карт Mifare Classic или Mifare Plus, то вам необходимо уточнить номер их блока памяти, который можно использовать для нужд СКУД, а также ключ от данного блока памяти, если он есть.** |

Произведите настройки согласно предыдущим пунктам инструкции, соответствующим картам Classic и Plus.

Если у вас используются банковские карты в режиме эмуляции карт Mifare Classic, то заполните полученные от банка реквизиты в поля:

- «Номер блока памяти» (в шестнадцатеричном формате);
- «Ключ для доступа к памяти».

Если у вас используются банковские карты в режиме эмуляции карт Mifare Plus, то заполните полученные от банка реквизиты в поля:

- «Номер блока памяти» (в шестнадцатеричном формате);
- «Ключ для доступа к блоку памяти». Если блок закрыт ключом, то укажите его. Если нет — используйте автоматически сгенерированное значение;
- Остальные пункты («Мастер-ключ карты», «Конфиг-ключ карты», «Ключ для переключения в SL2», «Ключ для переключения в SL3») поставьте равным предыдущему.

### 8.2.4. Правила заполнения служебных полей настроек карт Mifare.

Заполняя служебные поля вручную, необходимо соблюдать следующие условия:

Для карт Mifare Classic:

1. **«Номер блока памяти».**
   В этой строке в шестнадцатеричном формате указывается номер блока памяти для хранения идентификатора пропуска. Указываемый блок не должен быть последним блоком сектора (остаток от деления указываемого значения на 4 не должен равняться 3) или «0» (нулевой блок нулевого сектора).
2. **«Ключ для доступа к памяти».**
   Поле для указания значения секретного ключа (KEY-A), используемого для доступа к указанному блоку памяти карты, в шестнадцатеричном формате.
   **Значение ключа для доступа к памяти по умолчанию («FFFFFFFFFFFF») не должно использоваться в защищённом режиме!**
   Можно ввести собственное значение вручную или воспользоваться кнопкой «Сгенерировать ключ».
3. **«В память карты записывать».**
   Позволяет выбрать из выпадающего списка, что будет записано в память карты в качестве идентификатора. Доступно два варианта: UID карты или автоматически созданное значение. Формат записываемого значения будет соответствовать выбранному в верхней части окна «Формату идентификатора пропуска».
4. **«Биты чётности Wiegand хранятся на карте».**
   Позволяет выбрать, будут ли биты чётности Wiegand храниться в памяти карты. Как правило, должна быть отключена. Устанавливается при использовании старых моделей считывателей PROX.

Для карт Mifare Plus:

1. **«Номер блока памяти».**
   Значение данного поля указывается в шестнадцатеричном формате, нумерация блоков начинается с 00h (недоступен и не может быть использован).
   Для карт Mifare Plus 2K значение должно быть от 01h до 79h. Остаток от деления значения на 4 не должен быть равен трём.
   Для карт Mifare Plus 4K значение должно быть от 01h до FFh. Остаток от деления значения на 4 не должен быть равен трём для значений, меньших 80h. Начиная с 80h остаток от деления значения на 16 не должен равняться 15.
2. **«Ключ для доступа к блоку памяти».**
   Поле для ввода AES ключа, используемого для доступа к указанному выше блоку памяти. Значение задаётся в шестнадцатеричном формате и должно состоять из 16 байт (32 символов). По умолчанию состоит из всех нулей и не должен использоваться в защищённом режиме с таким значением.

3. **«Мастер-ключ карты».**
4. **«Конфиг-ключ карты».**

   Два поля для ввода AES ключей, используемых системой для персонализации карты. Значения задаются в шестнадцатеричном формате и должны состоять из 16 байт (32 символов).
5. **«Ключ для переключения в SL2».**

   Поле для ввода AES ключа, переключающего карту на более высокий уровень безопасности - Secure Level 2. Используется системой в процессе персонализации карты. Значение задаётся в шестнадцатеричном формате и должно состоять из 16 байт (32 символов).
6. **«Ключ для переключения в SL3».**

   Поле для ввода AES ключа, переключающего карту на более высокий уровень безопасности - Secure Level 3. Используется системой в процессе персонализации карты. Значение задаётся в шестнадцатеричном формате и должно состоять из 16 байт (32 символов).
7. **«В память карты записывать:».**

   Позволяет выбрать из выпадающего списка, что будет записано в память карты в качестве идентификатора. Доступно два варианта: UID карты или автосгенерированное значение. Формат записываемого значения будет соответствовать выбранному в верхней части окна «Формату идентификатора пропуска».

## 8.3. Занесение карт в ПО.

*Ниже приведена информация по занесению карт в ПО «Sigur». Для добавления карт в другие СКУД обратитесь к их документации.*

Занесение карт Mifare и банковских карт в базу ПО «Sigur» производится с помощью контрольного USB-считывателя ACR 1252U.

- В программе «Клиент» перейдите во вкладку «Персонал».
- Выберите нужного сотрудника либо создайте нового кнопкой «Добавить сотрудника в выбранный отдел».
- В том же разделе установите пункт «Действие при чтении карты» равным «Присваивать код текущему объекту».
- Поднесите карту к контрольному считывателю.
- При успешном считывании в поле «Пропуск» появится информация, связанная с данной картой.
- Сохраните внесённые изменения кнопкой «Применить».

# 9. Работа со смартфонами.

Модификация считывателя «Sigur MR1 BLE» позволяет использовать смартфоны в качестве идентификатора, используя технологию BLE (Bluetooth Low Energy).

Идентификация может происходить в режиме «hands-free» на расстоянии до 10 метров при прямой видимости считывателя. Дальность и режим чтения настраивается с помощью мастер-карты «Sigur».

Трафик между смартфоном и считывателем шифруется AES-алгоритмом шифрования.

## 9.1. Общие требования к смартфонам и ПО.

- ОС Android 5.0 и выше или iOS 9.0 и выше.
- Поддержка технологии BLE (Bluetooth Low Energy).
- Версия сервера СКУД «Sigur» 1.0.59.46.s и выше.

| | |
|---|---|
| **!** | **На текущий момент не поддерживается идентификация на смартфонах с iOS в фоновом режиме, а также на заблокированном экране.**<br><br>**Производителем не гарантируется полная функциональность приложений на смартфонах с ОС Android.**<br><br>**Например, некоторые смартфоны могут не поддерживать функцию идентификации при заблокированном экране. Это может происходить из-за физического отключения Bluetooth смартфона в силу особенностей данного устройства или его системной сборки.** |

## 9.2. Настройка считывателя.

*Ниже приведена информация о настройке считывателя в ПО «Sigur».*

Настройка считывателя и ПО на работу со смартфонами производится в несколько этапов:

- Создание мастер-карты в ПО «Sigur» и программирование считывателя данной мастер-картой.
- Заполнение реквизитов подключения к серверам исходящей и входящей почты.
- Отправка пригласительного письма из ПО «Sigur» на e-mail.
- Установка приложения «Доступ» и отправка ответного письма.

В программе «Клиент» перейдите в меню «Файл – Настройки – Mifare и BLE». Выберите пункт «BLE» и включите «Использовать».

Здесь вы должны настроить следующие поля:

1. **Сервисный пароль** — используется для доступа к считывателю через мобильное приложение «Настройки». Настоятельно не рекомендуется оставлять данное поле в состоянии по умолчанию.
   Сервисный пароль считывателя, установленный по умолчанию - «sigur», без кавычек.
2. **Ключ** — в большинстве случаев достаточно нажать «сгенерировать ключ». Этот ключ не должен меняться в дальнейшем. При его изменении всем сотрудникам потребуется выдать идентификаторы смартфонов повторно.
3. **Расстояние срабатывания** — ориентировочная дальность, на которой будет осуществляться идентификация. Доступно четыре варианта:

- близкое: - 45 dBm;
- среднее: - 75 dBm;
- далёкое: < - 75 dBm;
- пользовательское (укажите RSSI);

При настройке пользовательской дальности необходимо указать уровень принимаемого сигнала (RSSI) в dBm. При превышении данного уровня будет происходить идентификация. Вы можете выяснить необходимый уровень сигнала для идентификации с помощью мобильного приложения «Настройки».

4. **Политика срабатывания** — правило, при котором будет осуществляться идентификация. Доступно три варианта:

- когда приложение на экране – экран разблокирован и приложение было открыто;
- когда экран разблокирован – экран разблокирован и приложение работает в фоне;
- всегда – приложение запущено в фоне и идентификация происходит даже при заблокированном экране.

| | |
|---|---|
| ! | **Идентификация при заблокированном экране может повлечь произвольное открытие точек доступа при проходе рядом со считывателями.**<br>**Данный режим также понижает общую защищённость системы контроля доступом, т.к. при утере смартфона злоумышленнику не придётся разблокировать экран смартфона, вводя пин-код/графический ключ/производить считывание отпечатка пальца и т.п.** |

Если у вас будут несколько считывателей, на которых нужно задать разные дальности срабатывания или политики идентификации, — достаточно будет изменить параметры «Расстояние срабатывания» и «Политика срабатывания», после чего создать ещё одну мастер-карту Sigur. **Изменять поле «Ключ» не нужно!**

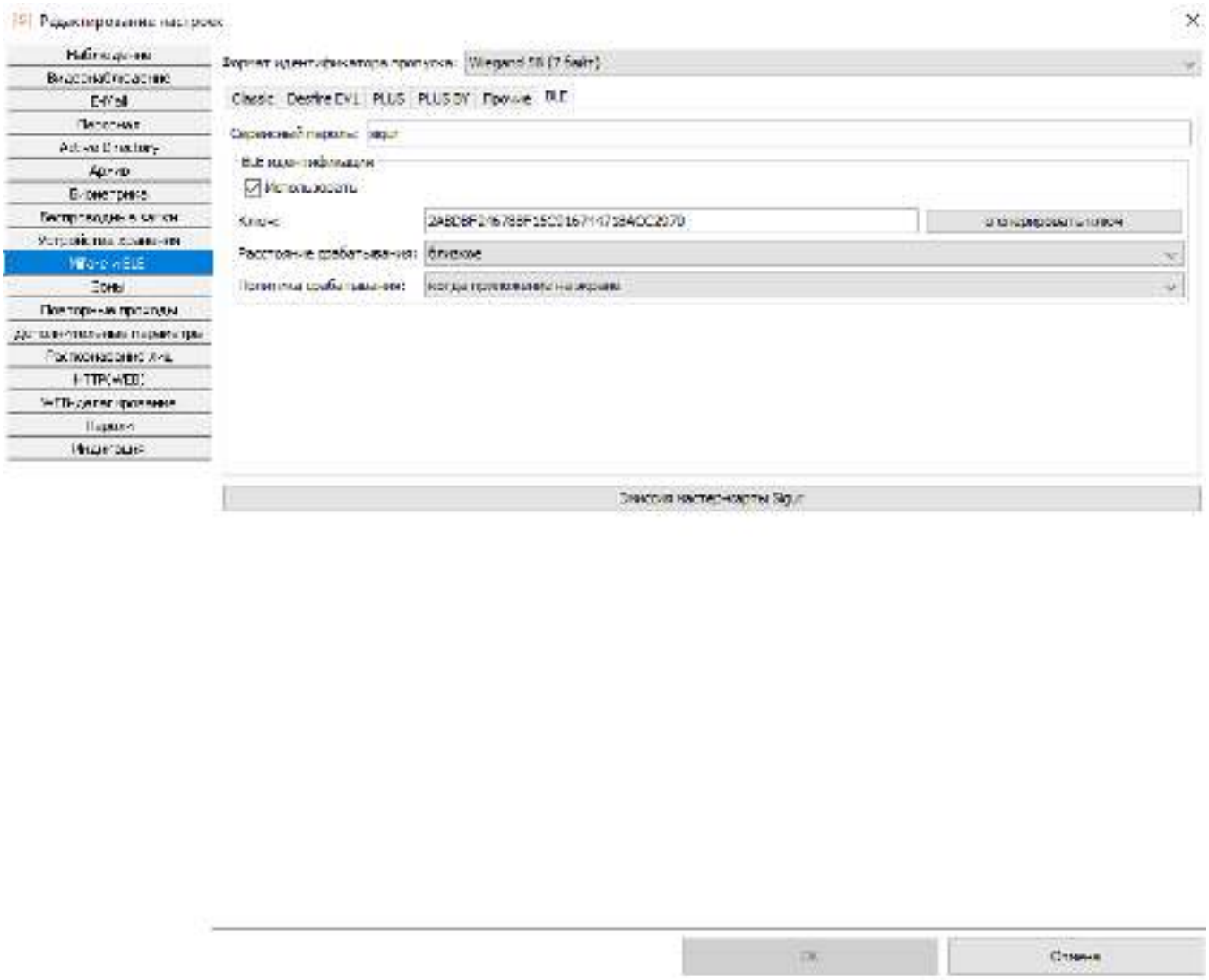



***Рисунок 4. Окно настроек BLE – идентификации по смартфону.***

## 9.3. Добавление идентификаторов в ПО.

*Ниже приведена информация о добавлении идентификаторов смартфонов в ПО «Sigur». При использовании считывателя в составе иной СКУД обратитесь к документации данной системы.*

Добавление идентификаторов смартфонов происходит путём рассылки пригласительных e-mail уведомлений с сервера СКУД «Sigur», в которых будет содержаться специальная ссылка для мобильного приложения «Доступ».

При переходе по данной ссылке приложение «Доступ» создаёт ответное письмо, которое должно быть отправлено в ответ.

### 9.3.1. Рассылка на e-mail. Настройки SMTP-сервера.

Для добавления смартфона в систему СКУД «Sigur» сначала необходимо задать настройки SMTP-сервера для отправки пригласительных e-mail сообщений.

Вы можете использовать как SMTP сервер вашей организации, так и любой другой, в том числе бесплатный.

Перейдите в программе «Клиент» в меню «Файл – Настройки – e-mail».

Заполните поля подпункта «Почтовый сервер для отправки исходящих писем»:

- «Адрес SMTP-сервера» – адрес используемого для отправки писем почтового сервера.
- «Порт SMTP сервера» – порт для подключения к почтовому серверу.
- «От кого» – e-mail адрес отправителя.
- «Использовать аутентификацию» – включает использование аутентификации на почтовом сервере.
- «SMTP логин» – логин для аутентификации на SMTP сервере.
- «SMTP пароль» – пароль для аутентификации на SMTP сервере.
- «Использовать SSL» – включает использование криптографического протокола для обеспечения более безопасной связи.

После указания реквизитов вы можете проверить правильность настройки, нажав кнопку «Сохранить параметры и протестировать». Укажите e-mail адрес получателя и нажмите OK.

Если всё верно, вы увидите сообщение «Письмо успешно отправлено». Убедитесь в факте его получения на указанный вами адрес.

### 9.3.2. Настройка сервера входящей почты.

Сервер входящей почты необходим для приёма сервером СКУД писем, отправленных со смартфонов, для их автоматического внесения в список идентификаторов пользователя. Вы можете использовать как сервер вашей организации, так и любой бесплатный. Адреса серверов исходящей и входящей почты могут отличаться.

| | |
|---|---|
| ! | **Для нужд СКУД требуется завести отдельный почтовый ящик. Письма в почтовом ящике будут УДАЛЕНЫ сервером СКУД.** |

В программе «Клиент» перейдите в меню «Файл – Настройки – e-mail».

Заполните поля «Почтовый сервер для получения входящих писем»:

- «Сервер» – адрес почтового сервера.
- «Порт» – входящий порт почтового сервера.
- «Протокол» – протокол работы сервера входящей почты. Доступны варианты «IMAP» и «POP».
- «Логин» – логин для аутентификации на сервере входящей почты.
- «Пароль» – пароль для аутентификации на сервере входящей почты.
- «E-mail» – укажите адрес электронной почты. На указанный вами адрес будут приходить ответные письма от пользователей.
- «Использовать SSL» – включает использование криптографического протокола для обеспечения более безопасной связи.

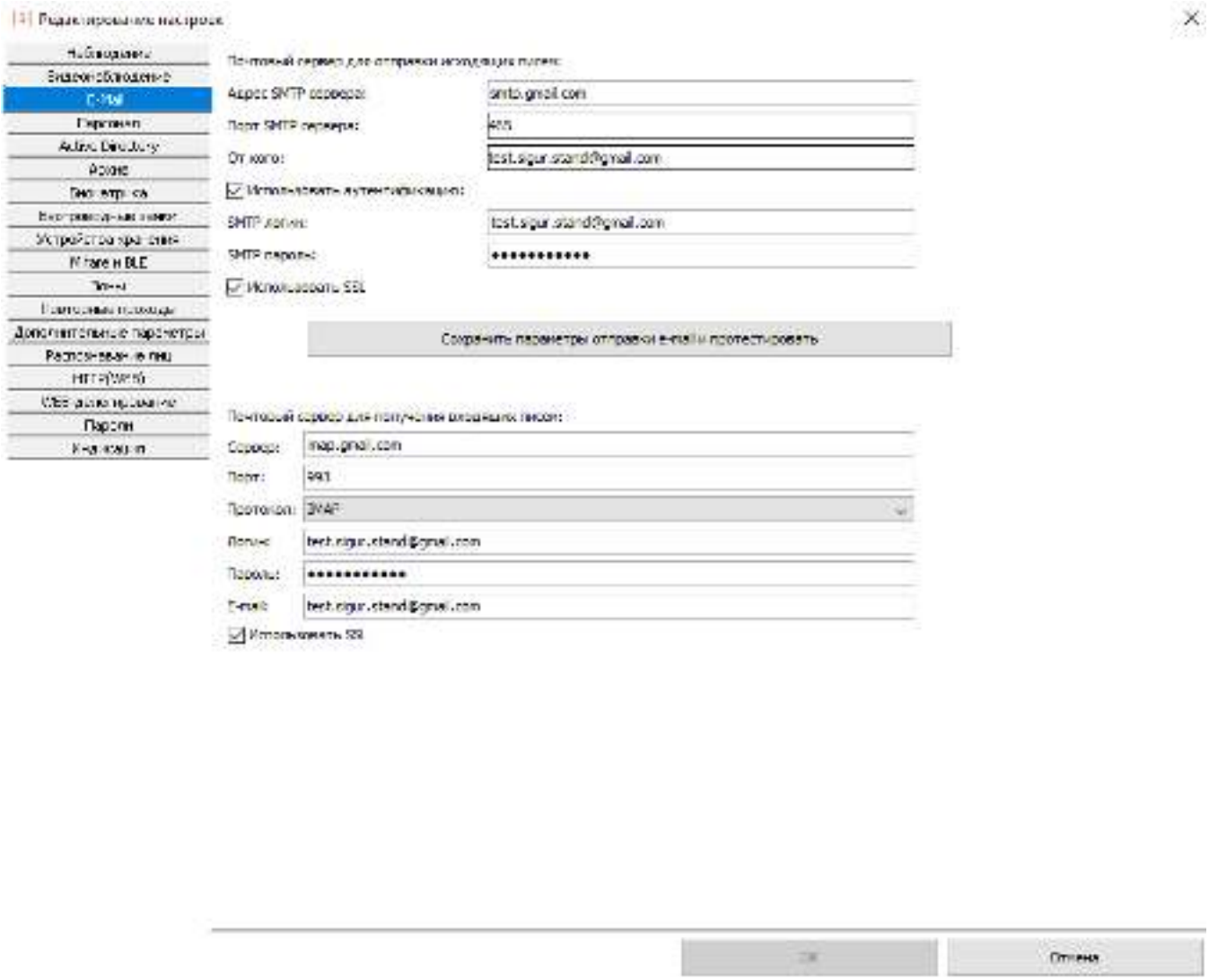
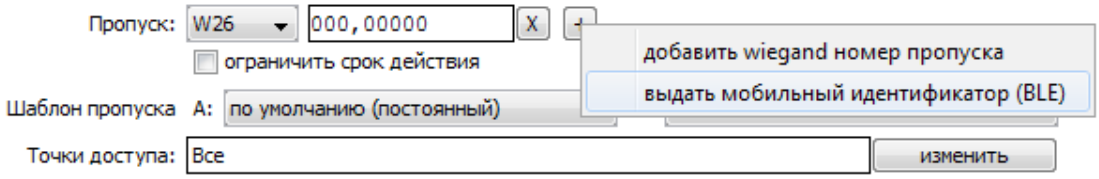



***Рисунок 5. Окно настроек E-mail. Пример настроек реквизитов подключения к серверу исходящей и входящей почты.***

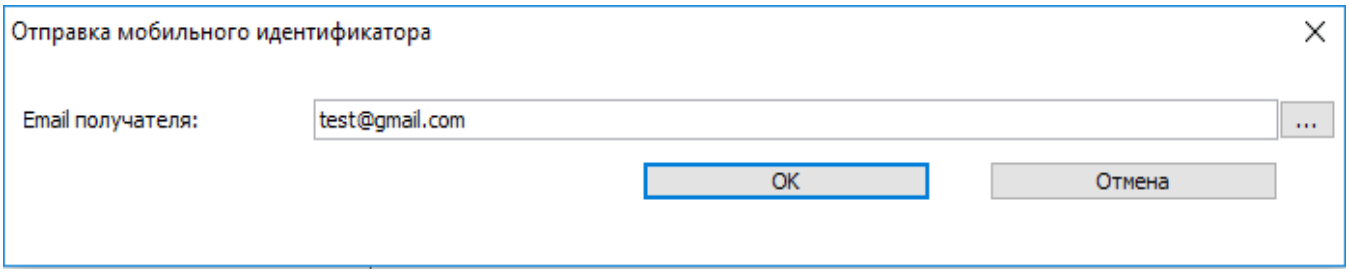
### 9.3.3. Отправка пригласительного письма.

Перейдите во вкладку «Персонал». Выберите нужного сотрудника либо создайте нового кнопкой «Добавить сотрудника в выбранный отдел».

На вкладке «Общее» нажмите «добавить ключ» напротив поля пропуск. Выберите вариант «Выдать мобильный идентификатор (BLE)»:




В появившемся поле введите e-mail адрес получателя либо укажите одну из доступных переменных. Нажмите «ОК» и дождитесь окончания отправки.




Данное письмо будет содержать служебную ссылку для приложения «Доступ», также в нём будут присутствовать ссылки на скачивание данного приложения из Google Play или App Store.

## 9.4. Отправка ответного письма.

После получения пригласительного письма:


***Рисунок 6. Пример пригласительного письма.***

- Установите приложение «Sigur Доступ» на смартфон по ссылкам из письма или из Google Play, App Store.
- Перейдите по специальной ссылке из письма, отправленного сервером СКУД Sigur. Вы также можете не переходить по ней непосредственно из письма, а скопировать ссылку в любой стандартный веб-браузер.
- После перехода по ссылке откроется приложение «Доступ», которое сгенерирует ответное письмо, содержащее идентификатор, связанный с устройством.

  Данное письмо будет передано в стандартное почтовое приложение устройства, но не будет отправлено. Вам необходимо отправить его вручную.

  Если у вас нет возможности отправить письмо с того же устройства, вы можете скопировать и отправить содержимое письма с любого другого устройства на указанный e-mail адрес. Необязательно отправлять его с того же адреса, на которое пришло пригласительное письмо.

- После отправки ответного письма в программе «Клиент» у данного сотрудника автоматически добавится дополнительный идентификатор в поле «Пропуск». Это будет означать удачную привязку идентификатора. С этого момента сотрудник может пользоваться приложением «Доступ».
- Один смартфон может быть зарегистрирован на нескольких серверах СКУД «Sigur». Для этого потребуется повторить указанные выше пункты на каждом из объектов.

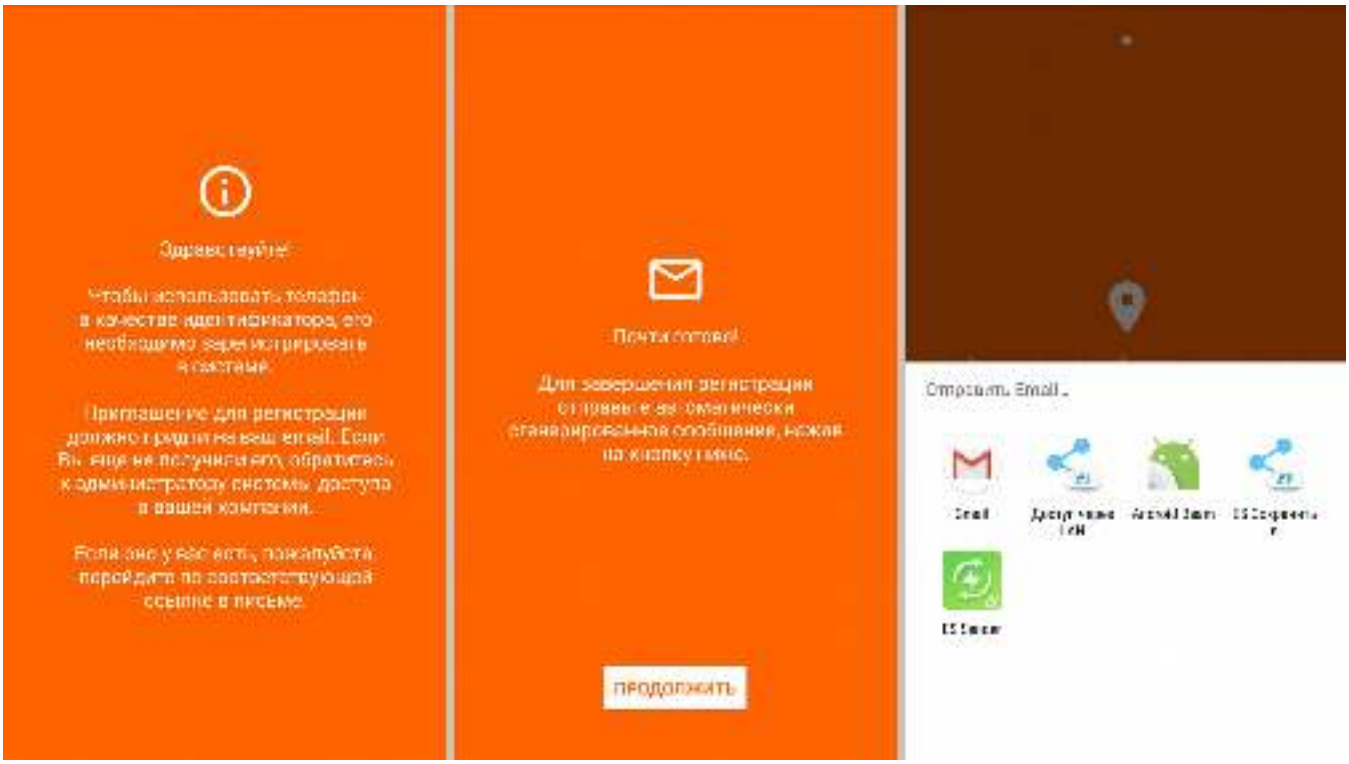



***Рисунок 7. Отправка ответного письма.***

## 9.5. Работа с приложением «Доступ».

Для функционирования приложения «Доступ» включите функции Bluetooth и определения местоположения. Держите их включёнными при необходимости прохождения идентификации. Предоставьте запрашиваемые разрешения приложению. Приложение «Доступ» может работать в фоновом режиме.

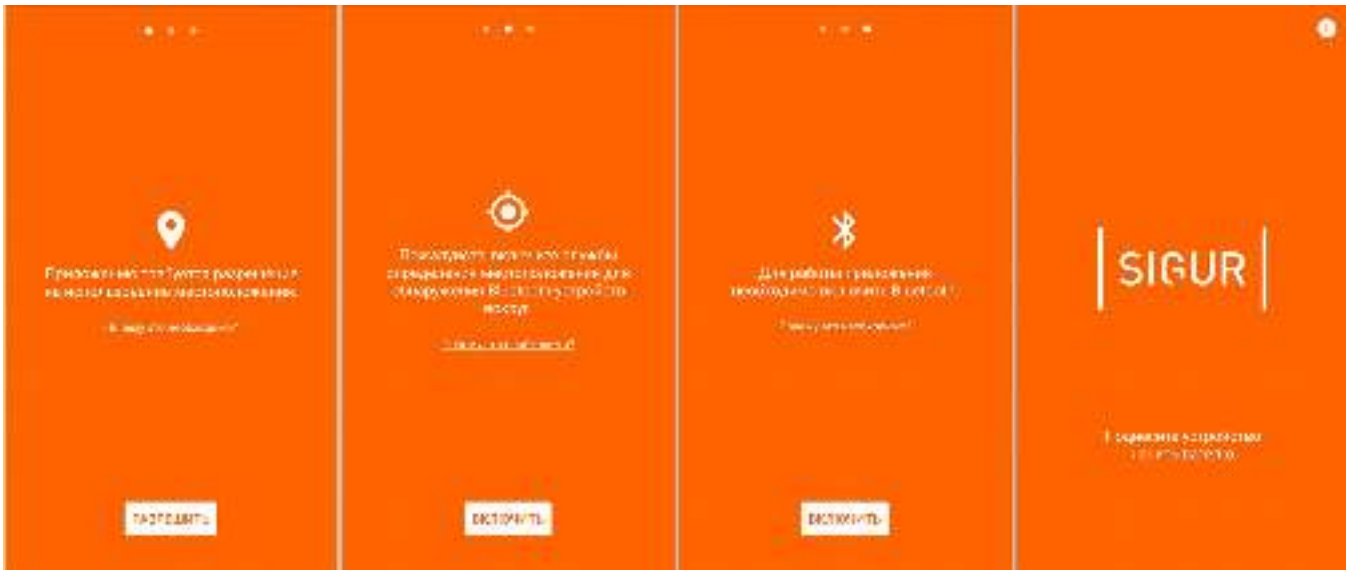



***Рисунок 8. Разрешения приложения «Доступ».***

В зависимости от установленных на считывателе настроек дальность считывания может быть разной – как и сама политика прохождения идентификации.

Какая именно политика и какая дальность срабатывания установлена на том или ином считывателе — уточните у вашего системного администратора.

В зависимости от установленной политики идентификация требует следующих действий:

| Политика срабатывания считывателя | Необходимые условия |
|---|---|
| Всегда | Смартфону достаточно попасть в область действия считывателя. Идентификация работает даже на заблокированном экране. |
| Когда экран разблокирован | Смартфон должен находиться в поле действия считывателя, и его экран должен быть разблокирован. |
| Когда приложение на экране | Смартфон должен находиться в поле действия считывателя, его экран должен быть разблокирован и приложение «Доступ» должно быть запущено на экране смартфона. |

**Таблица 6. Описание выполнения необходимых условий при действии той или иной политики считывателя.**

# 10. Приложение «Настройки».

Приложение «Настройки» предназначено для обновления внутреннего ПО считывателей. Новые микропрограммы могут исправлять некоторые ошибки предыдущих версий и расширять функции считывателя.

Скачать данное приложение можно только из Google Play: «Sigur Настройки», а также по ссылкам на нашем сайте.

При первом запуске приложения предоставьте ему все запрашиваемые разрешения.

## 10.1. Обновление внутреннего ПО считывателя.

- Включите функции: Bluetooth, определения местоположения и Wi-Fi (или мобильный интернет) на вашем смартфоне и запустите приложение «Настройки». Приложение само будет загружать новые версии микропрограмм считывателя через интернет при первой возможности. Объём трафика при первом включении будет составлять менее 1 МБ.
- Подойдите к считывателю или их группе и откройте приложение «Настройки». Во вкладке «Настройки считывателя» перед вами отобразится список доступных считывателей. В данном списке отображается модель считывателя, его серийный номер и уровень принимаемого сигнала.
- Выберите из данного списка один из считывателей для обновления микропрограммы, после чего нажмите «Обновление устройства».
- Программа отобразит текущую версию внутреннего ПО считывателя, а также наличие обновления. Выберите одну из доступных микропрограмм и нажмите кнопку «Обновить».
- Введите сервисный пароль устройства. При повторных действиях со считывателем вводить этот пароль не потребуется. Для сброса пароля к стандартному воспользуйтесь функцией аппаратного сброса. Сервисный пароль считывателя, установленный по умолчанию - «sigur», без кавычек.
- Дождитесь окончания отправки файла микропрограммы и обновления считывателя. Во время обновления микропрограммы считыватель изменит свою индикацию (светодиод моргает оранжевым).
- Приложение оповестит вас о результате операции, а считыватель при успешном обновлении издаст характерный звук. После обновления он сразу готов к работе, все прежние настройки сохранятся.

Приложение поддерживает работу сразу с несколькими считывателями.

- Для начала выберите один из считывателей долгим нажатием, после чего можно будет выбрать ещё несколько считывателей короткими нажатиями. Вверху отображается количество выбранных считывателей.
- После завершения выбора нажмите кнопку «Далее» и «Обновление устройства». В данном случае возможны все те же варианты, что и в случае одного считывателя. Если будут какие-то неоднозначности в действиях, приложение отобразит информацию об

этом. Вы можете пропустить и не обновлять считыватель нажатием кнопки «Пропуск». Переход к следующему считывателю осуществляется кнопкой «Следующий».

- После выбора нужных микропрограмм и нажатия кнопки «Обновить» приложение последовательно обновит внутреннее ПО считывателей, прогресс операции вы сможете увидеть в приложении.

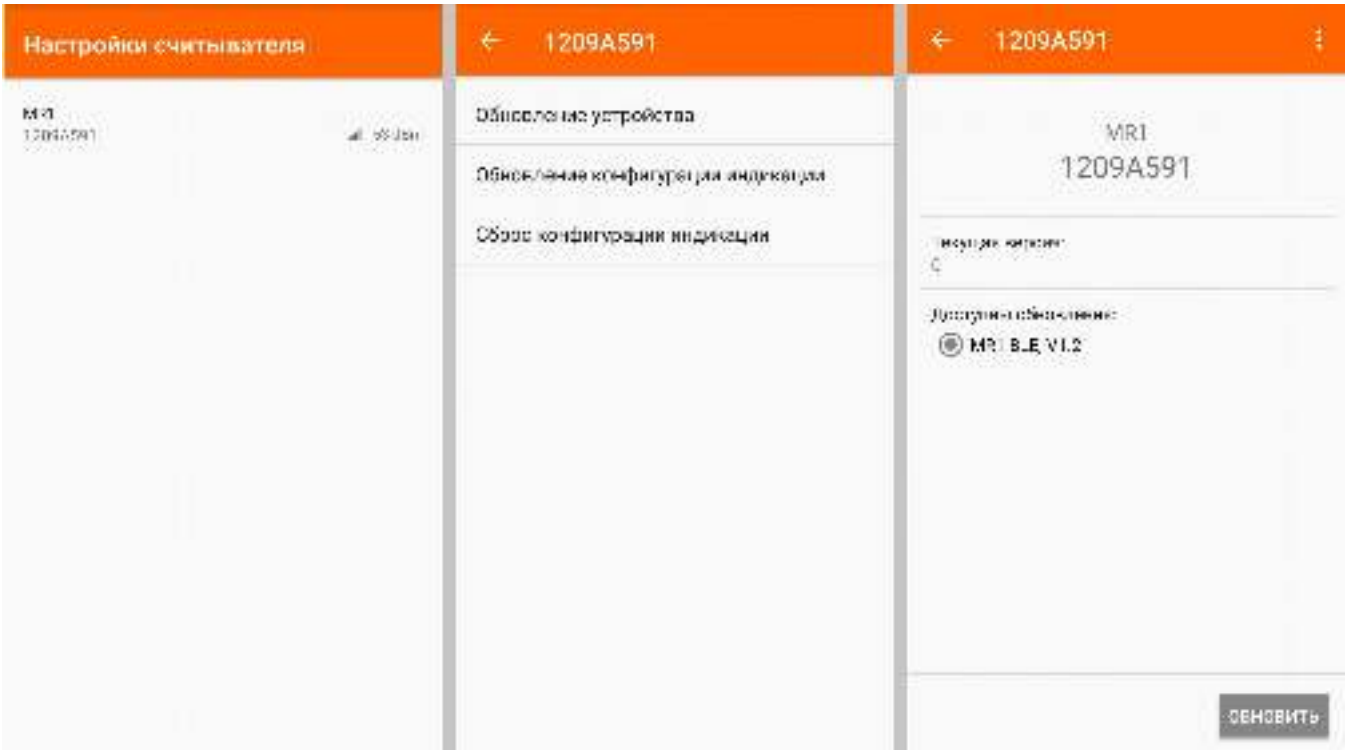



***Рисунок 9. Обновление внутреннего ПО считывателя.***

## 10.2. Установка специального внутреннего ПО считывателя.

Специальное внутреннее ПО считывателя становится доступно при введении лицензионного ключа. Оно позволяет расширять функционал считывателей и решать другие задачи.

- Включите функции Bluetooth, определения местоположения и Wi-Fi (мобильный интернет) на вашем смартфоне и запустите приложение «Настройки». Выберите считыватель или несколько считывателей.
- Нажмите кнопку «Обновление устройства».
- В открывшемся окне нажмите на кнопку «Меню» справа сверху.
- Нажмите «Ввести ключ».
- Если у вас есть лицензионный ключ для считывателя, введите его.

Приложение попробует найти микропрограмму считывателя, относящуюся к данному лицензионному ключу. Лицензионный ключ может расширять возможности стандартного ПО считывателей.

Если микропрограмма считывателя будет найдена приложением, то она попадёт в список доступных – вам не придётся вводить лицензионный ключ снова.

После этого обновите выбранные считыватели, нажав кнопку «Обновить».

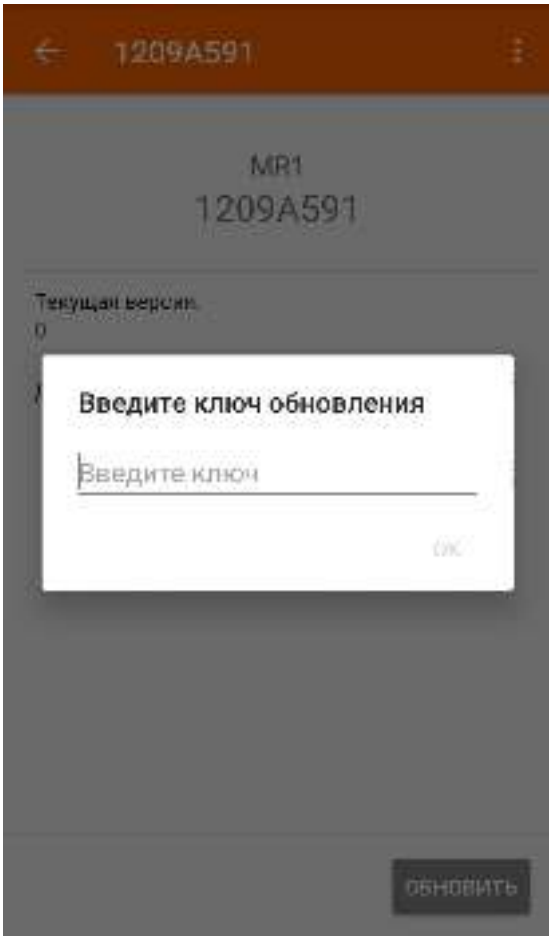



***Рисунок 10. Окно ввода ключа для специального ПО считывателя.***

## 10.3. Загрузка профиля индикации на считыватель.

*Загрузка профиля индикации возможна только на считывателях модели Sigur MR1 BLE. Для загрузки профиля индикации на считыватель на смартфоне должно быть установлено приложение «Настройки». Вы можете установить его по ссылке из письма с прикреплённым профилем индикации.*

Для загрузки профиля индикации на считыватель:


***Рисунок 11. Пример письма, содержащего профиль индикации.***

- Откройте полученное письмо с прикреплённым файлом профиля индикации и нажмите на прикреплённый к письму файл: откроется приложение «Настройки» с уведомлением об успешном добавлении профиля индикации.
  Данный профиль сохранится в приложении, вам не придётся нажимать на файл в письме каждый раз.
- В приложении «Настройки» выберете считыватель, на который необходимо загрузить желаемый профиль индикации.

- Из открывшегося списка действий выберите пункт «Обновление конфигурации индикации».

  Если данный пункт отсутствует в списке действий, то убедитесь в том, что модель считывателя соответствует требованиям выше и обновите внутреннее ПО считывателя до последней версии.

- Из открывшегося списка профилей индикации выберите желаемый и введите сервисный пароль считывателя.
- Дождитесь окончания загрузки конфигурации на считыватель. Конфигурация индикации применится по окончании загрузки, перезагрузка считывателя не требуется.

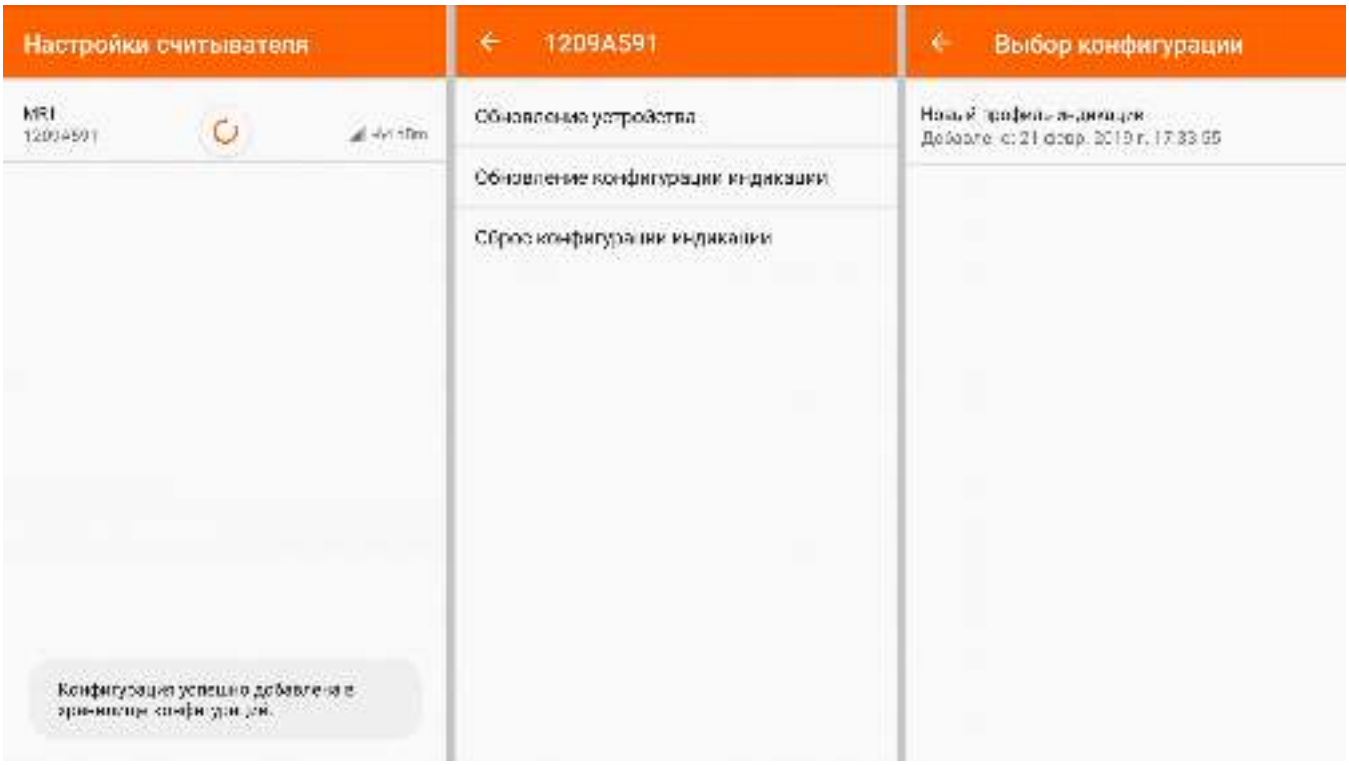



***Рисунок 12. Добавление нового профиля индикации.***

## 10.4. Сброс конфигурации индикации считывателя.

Для сброса индикации считывателя к заводским настройкам:

- Откройте приложение «Настройки» и выберите считыватель из списка.
- Из открывшегося списка действий выберите пункт «Сброс конфигурации индикации».
- Подтвердите операцию и введите сервисный пароль считывателя.
- Дождитесь окончания загрузки конфигурации на считыватель. Конфигурация индикации применится по окончании загрузки, перезагрузка считывателя не требуется.

ООО «Промышленная автоматика – контроль доступа»
603002, г. Нижний Новгород, ул. Советская, д. 18б
Техническая поддержка: 8 (800) 700 31 83, +7 (495) 665 30 48, +7 (831) 260-12-93

Система контроля и управления доступом «Sigur»
Сайт: http://www.sigursys.com
Электронная почта: info@sigursys.com
Skype: spnx.support