

Система контроля и управления
доступом Sigur

Считыватель Sigur MR1

Описание и инструкция по эксплуатации

Оглавление	
1. Введение	3
2. Технические характеристики	4
3. Комплект поставки	5
4. Общие функции считывателя в СКУД Sigur	6
5. Монтаж считывателя	7
5.1. Назначение проводов считывателя	7
5.2. Общие рекомендации к монтажу	8
5.3. Рекомендации по выбору кабелей	8
6. Индикация считывателя	9
6.1. Настройка управления индикацией считывателя по двум линиям	11
6.2. Настройка пользовательской индикации считывателя	13
6.2.1. Добавление звука реакции считывателя. Вкладка «Звуки»	14
6.2.2. Создание реакции считывателя. Вкладка «Реакции»	15
6.2.3. Создание профиля индикации считывателя. Вкладка «Профили»	17
7. Настройка реакции на вскрытие корпуса считывателя	19
8. Программирование считывателя	21
8.1. Программирование считывателя мастер-картой	22
8.2. Программирование считывателя конфигурационным файлом	23
9. Сброс параметров считывателя к заводским настройкам	24
9.1. Аппаратный сброс	24
9.2. Сброс параметров считывателя через приложение «Настройки»	25
10. Настройка доступа ПО Sigur к почтовым серверам	26
10.1. Настройка параметров сервера исходящей почты	26
10.2. Настройка параметров сервера входящей почты	27
11. Работа с картами Mifare и банковскими картами	29
11.1. Работа в незащищённом режиме, чтение UID	29
11.2. Работа в защищённом режиме. Эмуляция Mifare банковской картой	30
11.2.1. Настройка работы с картами Mifare Classic 1K/4K	30
11.2.2. Настройка работы с картами Mifare Plus	31
11.2.3. Настройка работы с банковскими картами	32
11.2.4. Правила заполнения служебных полей настроек карт Mifare	33
11.3. Занесение карт в ПО	35
12. Работа со смартфонами	36
12.1. Общие требования к смартфонам и ПО	37
12.2. Настройка системы на работу со смартфонами	38
12.3. Добавление мобильных идентификаторов в ПО	41
12.3.1. Отправка приглашительного письма	42
12.3.2. Отправка ответного письма	43
12.4. Работа с приложением «Доступ»	45
13. Приложение «Настройки»	46
13.1. Обновление внутреннего ПО считывателя	46
13.2. Установка специального внутреннего ПО считывателя	48
13.3. Загрузка профиля конфигурации на считыватель	50
13.4. Программный сброс параметров считывателя	53
13.5. Загрузка профиля индикации на считыватель	54
13.6. Сброс конфигурации индикации считывателя	56
14. Логика обработки идентификаторов	57
14.1. Чтение карты	57

14.2. Чтение смартфона.....59

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), в том числе, защищенный режим для семейства Mifare Classic, защищенные режимы SL1 и SL3 для семейства Mifare Plus, а также банковские бесконтактные карты МИР, Visa и MasterCard.¹

Модификация считывателя Sigur MR1 BLE дополнительно позволяет:

- проходить идентификацию по смартфону, используя технологию BLE (Bluetooth Low Energy). Поддерживаются смартфоны с ОС Android и iOS;
- запрограммировать считыватель конфигурационным файлом с помощью смартфона;
- гибко настраивать световую и звуковую индикацию считывателя.

1 Для использования банковской карты в качестве идентификатора должно быть выполнено одно из следующих условий:

1) наличие статического UID (для использования карты в режиме чтения UID);
2) наличие эмуляции карт Mifare Classic или Plus, соответствующей документу "AN10833 MIFARE Type Identification" компании NXP (для работы с картами в защищенном режиме).

2. Технические характеристики

Формат поддерживаемых идентификаторов	
Mifare (Ultralight, Classic, Mini, ID, DESFire, Plus), включая защищенные режимы SL1 и SL3 семейства Mifare Plus, защищенный режим семейства Mifare Classic.	
Бесконтактные банковские карты MasterCard, Visa, МИР в режиме чтения UID при наличии статического UID/в защищенном режиме при наличии эмуляции Mifare Classic или Plus, соответствующей документу "AN10833 MIFARE Type Identification" компании NXP.	
Смартфоны (Android, iOS) по технологии BLE (при наличии Bluetooth 4.0 и выше).	
Все идентификаторы стандарта ISO14443-A в режиме чтения UID.	
Технические параметры	
Дальность чтения карт	До 9 см (в зависимости от карты, режима работы и места установки)
Дальность чтения смартфонов	До 10 метров при прямой видимости (в зависимости от модели смартфона, режима работы и места установки)
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 °С
Класс защиты	IP65
Напряжение питания	12 В (9...15 В)
Потребляемый ток	90 мА в режиме ожидания, 130 мА при чтении карты
Индикация	
Световая	Многоцветный светодиодный индикатор
Звуковая	Широкополосный акустический динамик, PCM 16 бит 44.1 кГц моно.
Поддерживаемые звуковые форматы	.wav, .aiff, .au
Длительность 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 Classic (в том числе Mini и ID), Ultralight, DESFire, Plus в режиме чтения их уникального идентификатора – UID. Поддерживается защищённый режим работы Mifare Classic 1K/4K, а также режим 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 и датчиком температуры.

5. Монтаж считывателя

Процедура монтажа считывателя описана в [«Руководстве по монтажу считывателя Sigur MR1»](#).

5.1. Назначение проводов считывателя

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

Ниже представлена таблица, описывающая назначение проводов считывателя Sigur MR1.

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/GREEN	Первый цифровой вход управления индикацией считывателя. Если считыватель находится в заводской конфигурации, то при активации входа следует включение звукового и светового сигнала разрешения доступа.
Коричневый	IN2/RED	Второй цифровой вход управления индикацией считывателя. Если считыватель находится в заводской конфигурации, то при активации данного следует включение звукового и светового сигнала запрета доступа .
Жёлтый	IN3/SOUND	Третий цифровой вход управления индикацией считывателя. Если считыватель находится в заводской конфигурации, то при активации входа следует включение монотонного звукового сигнала. Вход используется также для аппаратного сброса считывателя к заводским настройкам.

Таблица 3. Назначение проводов считывателя Sigur MR1

5.2. Общие рекомендации к монтажу

Располагать считыватели лучше всего на некотором расстоянии друг от друга, чтобы один и тот же идентификатор не попадал в зону действия сразу нескольких считывателей:

- для карт расстояние между считывателями должно быть не меньше 15 см;
- для смартфонов расстояние определяется настроенным уровнем сигнала.

Не рекомендуется устанавливать считыватель на металлических плоскостях, вблизи источников радиопомех и силовых линий - это снижает дальность чтения идентификаторов, в том числе дальность чтения мобильных телефонов.

5.3. Рекомендации по выбору кабелей

На небольшом удалении считывателей от контроллера (до 50м) рекомендуется выполнять кабелем сечением 0,22-0,5 мм².

Допустимо использование любых типов сигнальных кабелей, например, КСПВ 8x0,5.

При большей удалённости (50-100 м) необходим кабель большего сечения (0,75-1,0 мм²), как минимум, на линиях питания считывателей.

Также при подключении ознакомьтесь с рекомендациями от производителя контроллера, к которому будет выполняться подключение.

6. Индикация считывателя

После включения считыватель ожидает управление индикацией по какому-либо из трех его цифровых входов «IN1/GREEN», «IN2/RED» или «IN3/SOUND».

Активный уровень линий управления – ноль вольт.

Независимо от конфигурации индикации, считыватель воспроизводит особые звуковые сигналы при включении, аппаратном сбросе и при программировании мастер-картой.

Также при установлении связи со считывателем и обменом данными через приложение «Настройки» или «Доступ» загорается желтый светодиод.

Логика управления индикацией отличается для случаев, когда на считывателе загружена стандартная индикация и когда загружена пользовательская конфигурация индикации.

Если на считыватель загружена **стандартная** конфигурация индикации:

- Если ни на один из управляющих входов «IN1/GREEN», «IN2/RED» или «IN3/BEEP» не было подано сигнала, то при чтении любого идентификатора считыватель реагирует звуковым сигналом «Разрешение доступа» и кратковременно моргает зеленым.
- Если на одну из управляющих линий «IN1/GREEN» или «IN2/RED» подаётся сигнал, то считыватель переводится в режим работы «[Управление индикацией по двум линиям](#)». Считыватель перестаёт сопровождать индикацией чтение любого идентификатора, ожидая управление по какой-либо из линий «IN1/GREEN» или «IN2/RED».

В случае подачи сигнала на линию «IN1/GREEN» один раз воспроизводится звук «Разрешение доступа» и загорается зеленый светодиод на время, совпадающее с временем действия управляющего сигнала.

В случае подачи сигнала на линию «IN2/RED» один раз воспроизводится звук «Запрет доступа» и загорается красный светодиод на время, совпадающее с временем действия управляющего сигнала.

- Если на управляющую линию «IN3/SOUND» подаётся сигнал, то воспроизводится монотонный звуковой сигнал. Продолжительность звукового сигнала совпадает со временем управляющего сигнала. Другие звуковые сигналы больше не воспроизводятся.

Если на считыватель загружена **пользовательская** конфигурация индикации, то от считывателя может последовать соответствующая, заранее установленная реакция (если на текущий момент нет более приоритетной реакции):

- К считывателю был поднесен и успешно прочитан идентификатор – воспроизводится реакция, установленная на событие «Прочитан идентификатор».
- Считыватель закреплён на настенной панели – воспроизводится реакция, установленная на событие «Считыватель на стене».
- Считыватель извлечен из настенной панели – воспроизводится реакция, установленная на событие «Считыватель оторван».
- Если температура считывателя вышла за пределы нормы – воспроизводится реакция, установленная на событие «Температура вне нормы».
- Если линия «IN1/GREEN» замкнута на GND (не замкнута на GND) – воспроизводится реакция, установленная на событие IN1/GREEN активно (IN1/GREEN не активно).
- Если линия «IN2/RED» замкнута на GND (не замкнута на GND) – воспроизводится реакция, установленная на событие IN2/RED активно (IN2/RED не активно).
- Если линия «IN3/Beep» замкнута на GND (не замкнута на GND) – воспроизводится реакция, установленная на событие IN3/Beep активно (IN3/Beep не активно).

6.1. Настройка управления индикацией считывателя по двум линиям

В заводской конфигурации считывателя линии IN1/GREEN и IN2/RED используются для управления индикацией разрешения или запрета доступа. При активации той или иной линии включается зелёный или красный светодиод на установленный интервал времени, а также проигрывается предустановленный звуковой сигнал «Разрешение доступа» или «Запрет доступа».

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). Установите её значение равным LED1(PORTN)/LNA/LED(PORTN), 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). Установите её значение равным LED2(PORTN)/LNA/LED(PORTN), 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 порядка 1 сек. (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 порядка 1 сек. (или иное время включения световой индикации разрешения/запрета доступа).

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

Параметры первой:

- 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(PORTN)/LNA/LED(PORTN), где **N** – номер порта на контроллере, к которому подключён считыватель.

Параметры второй:

- 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(PORTN)/LNA/LED(PORTN), где **N** – номер порта на контроллере, к которому подключён считыватель.

6.2. Настройка пользовательской индикации считывателя

Световая и звуковая индикация считывателя Sigur MR1 BLE может быть гибко настроена только средствами ПО Sigur. Для настройки подойдёт также [Бесплатная версия ПО](#).

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 из списка](#). После окончательной настройки профиль прикрепляется к письму и отправляется на указываемый вами e-mail средствами ПО Sigur.
2. Полученный по электронной 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 «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 событие из списка.

- [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 звук из файла, а также прослушать ту или иную запись из списка.

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 нужный вам 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.

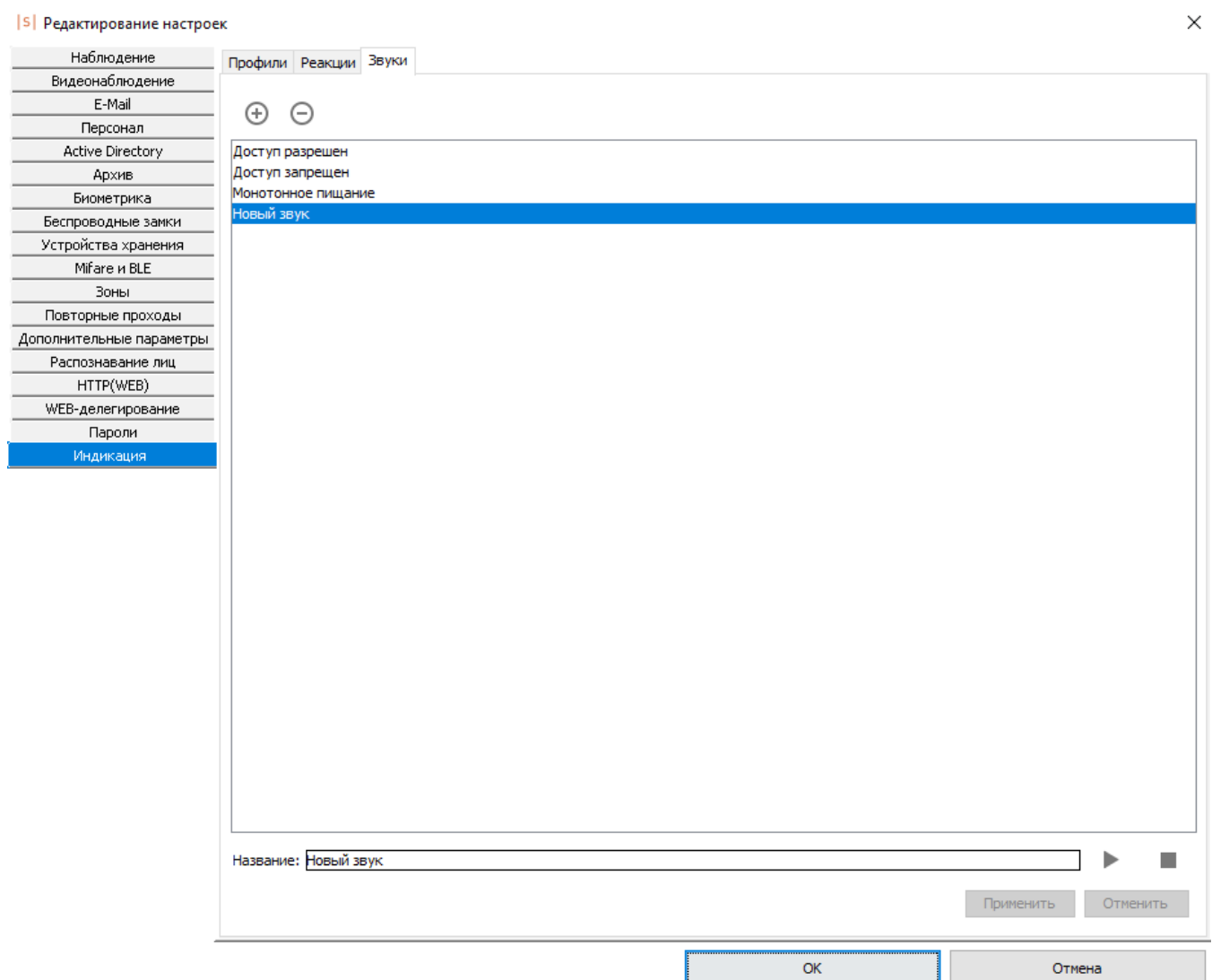


Рисунок 1. Вкладка «Звуки»

6.2.2. Создание реакции считывателя. Вкладка «Реакции»

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

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

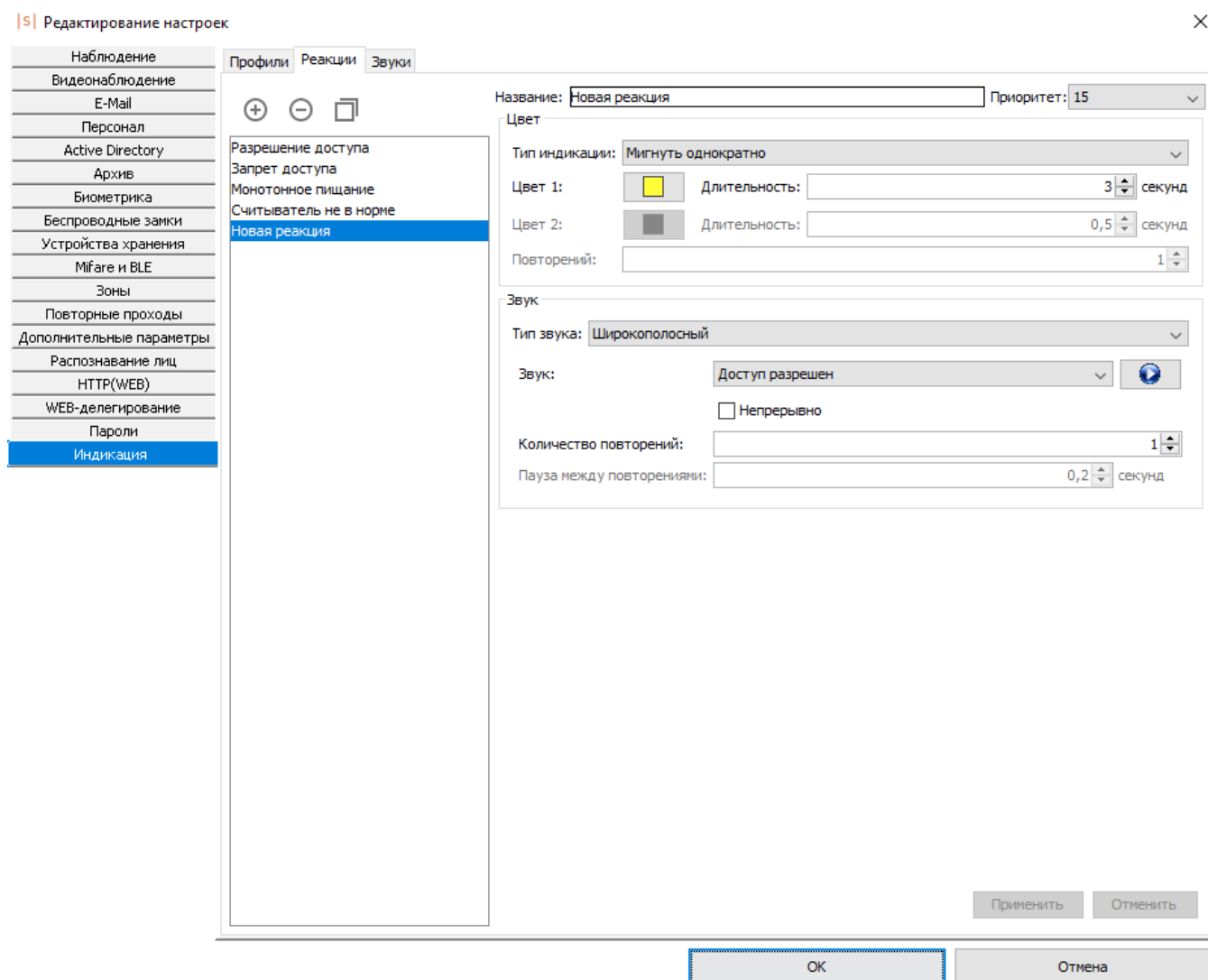


Рисунок 2. Вкладка «Реакции»

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 меняет цвет светодиода на «Цвет 1» на указанное время.

- «Мигание несколько раз»² – считыватель периодически изменяет цвет светодиода: сначала включается «Цвет 1» на указанное время, затем включается «Цвет 2» на соответствующее настройке время. Последовательность повторяется установленное количество раз.
- «Сменить цвет»¹ – считыватель изменяет цвет светодиода на «Цвет 1».
- «Мигание непрерывно»¹ – считыватель периодически изменяет цвет светодиода: сначала включается «Цвет 1» на указанное время, затем включается «Цвет 2» на соответствующее настройке время.

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 раз², либо непрерывно¹. 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».

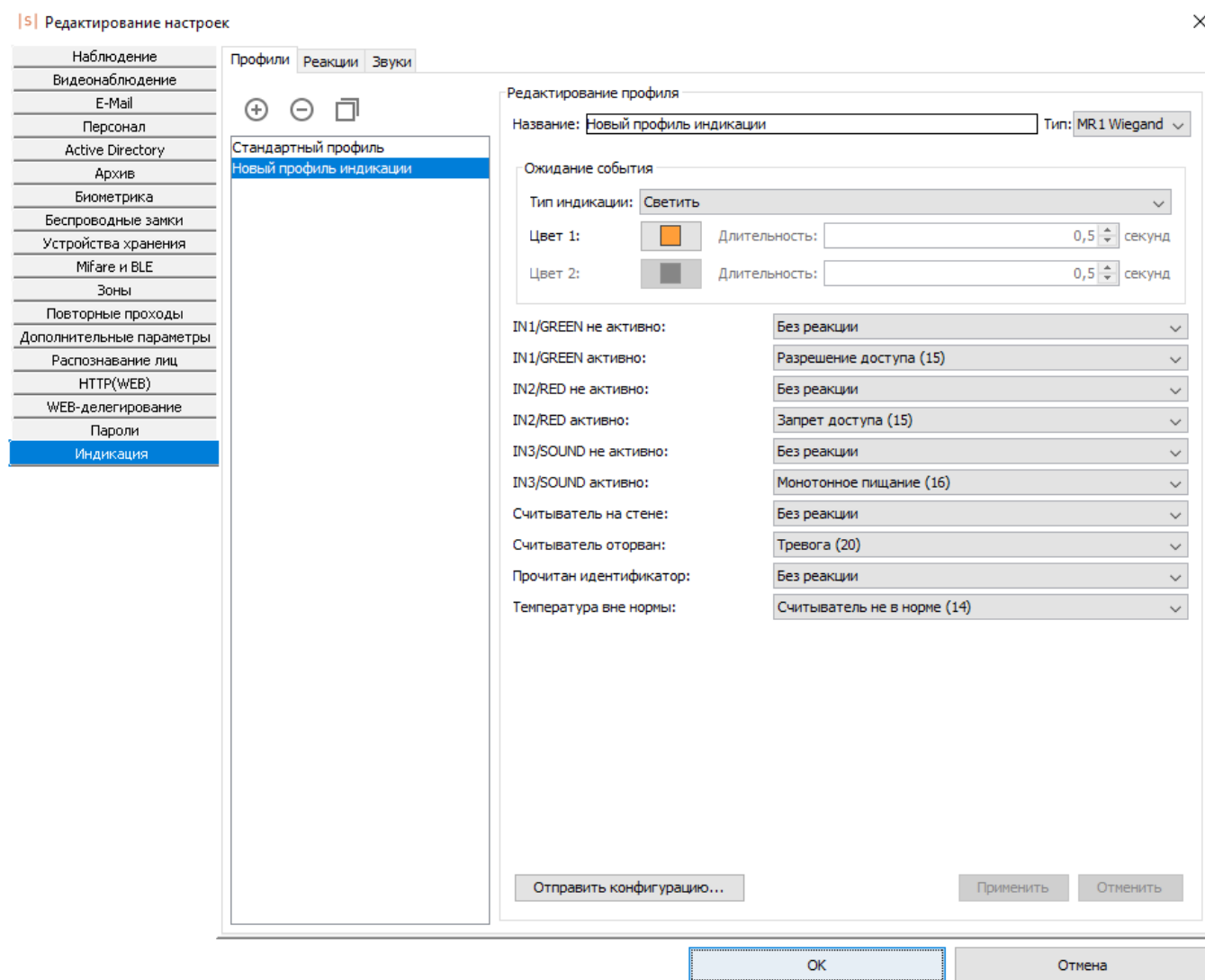


Рисунок 3. Вкладка «Профили»

Профиль индикации позволяет настроить:

1. Световую индикацию ожидания считывателем наступления какого-либо события.

Параметр «Тип индикации» может иметь следующие значения:

- «Светить» - цвет светодиода не меняется до наступления какого-либо события.
- «Мигать» - считыватель периодически изменяет цвет светодиода: сначала включается «Цвет 1» на указанное время, затем включается «Цвет 2» на соответствующее настройке время.

2. Реакцию считывателя на какое-либо событие.

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 IN1/GREEN не подключена на GND
IN1/GREEN активно	линия IN1/GREEN подключена на GND
IN2/RED не активно	линия IN2/RED не подключена на GND
IN2/RED активно	линия IN2/RED подключена на GND
IN3/SOUND не активно	линия IN3/SOUND не подключена на GND
IN3/SOUND активно	линия IN3/SOUND подключена на GND
Считыватель на стене	считыватель закреплен на настенной панели
Считыватель оторван	считыватель извлечен из настенной панели
Прочитан идентификатор	чтение идентификатора считывателем (карта или смартфон)
Температура вне нормы	выход температуры считывателя из пределов нормы

Таблица 5. Функции вкладки «Профили»

После настройки профиля индикации необходимо нажать «Применить».

Для отправки письма с конфигурационным файлом индикации ПО Sigur потребуется доступ к серверу исходящей почты. Подробная инструкция по настройке реквизитов доступа сервера исходящей почты представлена в разделе «[Настройка параметров сервера исходящей почты](#)».

Для загрузки профиля индикации на считыватель нажмите кнопку «Отправить конфигурацию» и введите e-mail. На указанный e-mail придёт письмо с прикрепленным 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](#)».

7. 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 выступить: 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 «FFFFFFFFF00» (без кавычек). У учётной записи «Закрытие корпуса считывателя» сделайте аналогично со значением, равным «FFFFFFFFF01».
- 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»](#).

8. Программирование считывателя

Программирование считывателя на текущий момент производится только средствами ПО Sigur. Вы можете воспользоваться любой актуальной версией нашего ПО, в том числе бесплатной. Дистрибутив доступен на нашем [официальном сайте по ссылке](#).

Программирование считывателя осуществляется в 3 этапа:

- настройка параметров считывателя через ПО «Клиент»;
- запись данных конфигурации на карту или в файл;
- непосредственное программирование считывателя на настроенную конфигурацию.

После установки ПО откройте программу «Клиент» и перейдите во вкладку «Файл – Настройки – Mifare и BLE».

В этой вкладке возможно изменение следующих параметров считывателя:

- Разрядность Wiegand-выхода. Поддерживаются форматы Wiegand-26, 34 и 58;
- Параметры работы считывателя с картами (чтение UID или защищенный режим работы для карт Mifare Classic 1K/4K и Mifare Plus). Для защищённого режима указываются реквизиты доступа к памяти карты;
- Параметры работы считывателя Sigur MR1 BLE со смартфонами: «Базовый» или «Пользовательский» режим, секретный ключ доступа, дальность срабатывания и политика чтения смартфонов;
- Сервисный пароль считывателя.

Подробное описание каждого пункта настройки представлено в следующих разделах:

- [Работа с картами Mifare и банковскими картами](#);
- [Работа со смартфонами](#).

После того, как вы примените данные параметры, конфигурацию необходимо будет записать на считыватели вручную. Для считывателей Sigur MR1 доступно 2 способа, как это сделать:

- [Программирование считывателя мастер-картой](#). Данный способ доступен для всех модификаций считывателя Sigur MR1.
- [Программирование считывателя конфигурационным файлом](#). Данный способ доступен только для модификации считывателей Sigur MR1 BLE.

8.1. Программирование считывателя мастер-картой

Данный способ доступен для всех модификаций считывателя Sigur MR1.

Для настройки считывателя необходимо создать мастер-карту. Вам потребуется:

- Карта Mifare Classic 1K/4K 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](#).

Перечень доступных для программирования параметров и порядок их настройки представлен в разделе «[Программирование считывателя](#)».

После установки всех параметров работы считывателя в ПО «Клиент», в разделе «Файл – Настройки – Mifare и BLE» нажмите на кнопку «Эмиссия мастер-карты Sigur».

Поднесите любую чистую карту (Mifare Classic 1K/4K или Mifare Plus) к настольному считывателю. Программа уведомит вас о результате операции.



Для создания мастер-карты Sigur с иными параметрами понадобится другая «чистая» карта!

Если считыватель был запрограммирован ранее, то сначала нужно произвести его аппаратный сброс. Процесс описан в разделе «[Аппаратный сброс](#)».

Если считыватель Sigur MR1 не был запрограммирован ранее, или вы уже произвели его аппаратный сброс, то:

- выключите и включите считыватель;
- поднесите мастер-карту к считывателю (время ожидания считывателем мастер-карты равно 25 секундам).

После поднесения мастер-карты считыватель издаст характерный звук.

8.2. Программирование считывателя конфигурационным файлом

В настоящий момент программирование считывателя конфигурационным файлом возможно только для модификации Sigur MR1 BLE. Для программирования считывателя другой модификации следуйте пунктам раздела «[Программирование считывателя мастер-картой](#)».

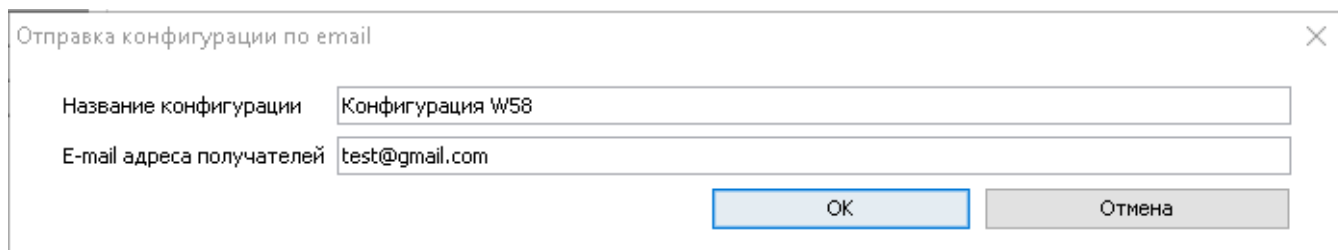
Для программирования считывателя конфигурационным файлом вам потребуется:

- Смартфон с ОС Android с установленным приложением «[Настройки](#)», с доступом к какому-либо почтовому ящику и с поддержкой функции BLE;
- Доступ к почтовому ящику, с которого будет отправлен файл конфигурации средствами ПО Sigur;
- ПО Sigur с официального сайта. Для настройки подойдет также [Бесплатная версия](#).

Перечень доступных для программирования параметров и порядок их настройки представлен в разделе «[Программирование считывателя](#)».

Для отправки письма с конфигурационным файлом ПО Sigur потребуется доступ к серверу исходящей почты. Подробная инструкция по настройке реквизитов доступа сервера исходящей почты представлена в разделе «[Настройка параметров сервера исходящей почты](#)».

После установки всех параметров работы считывателя в ПО «Клиент», в разделе «Файл – Настройки – Mifare и BLE» нажмите кнопку «Отправить по e-mail». В открывшемся меню введите название любое конфигурации и укажите почтовый ящик, на который будет выслан файл конфигурации. Нажмите «ОК».



Отправка конфигурации по email

Название конфигурации: Конфигурация W58

E-mail адреса получателей: test@gmail.com

ОК Отмена

Рисунок 4. Диалог отправки конфигурации по e-mail

После получения файла конфигурации для дальнейшего программирования считывателя следуйте пунктам раздела «[Загрузка профиля конфигурации на считыватель](#)».

9. Сброс параметров считывателя к заводским настройкам

Ниже следует описание способов сброса параметров считывателя. Для считывателей Sigur MR1 доступно 2 способа сброса параметров считывателя к заводским настройкам:

- [Аппаратный сброс](#). Поддерживается всеми модификациями считывателей Sigur MR1.
- [Сброс параметров через приложение «Настройки»](#). Поддерживается только модификацией Sigur MR1 BLE.

Оба способа позволяют сбросить следующие параметры считывателя:

- Разрядность Wiegand (по умолчанию – Wiegand-26).
- Параметры работы считывателя в защищенном режиме с картами Mifare Classic 1K/4K и Mifare Plus (по умолчанию – чтение UID карты).
- Параметры чтения «Прочих» карт (по умолчанию – чтение UID карты).
- Параметры работы считывателя со смартфонами для считывателей Sigur MR1 BLE. По умолчанию используется «Базовый» режим работы, дальность чтения – «Близко» и режим работы – «Когда приложение на экране».
- Сервисный пароль считывателя.

Далее представлены способы сброса параметров считывателя к заводским настройкам.

9.1. Аппаратный сброс

Любая ревизия считывателя Sigur MR1 поддерживает функцию аппаратного сброса на заводские настройки.

Для аппаратного сброса настроек считывателя необходимо:

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

Если считыватель был ранее запрограммирован, то при успешном сбросе он издаст характерный звуковой сигнал.

9.2. Сброс параметров считывателя через приложение «Настройки»

Данный способ сброса настроек поддерживается только модификацией считывателя Sigur MR1 BLE. Для сброса параметров считывателя другой модификации воспользуйтесь способом, описанным в разделе [«Аппаратный сброс»](#).

Для сброса параметров чтения карт и смартфонов, а также разрядности Wiegand следуйте пунктам раздела [«Программный сброс параметров считывателя»](#).

Для сброса параметров индикации следуйте пунктам раздела [«Сброс конфигурации индикации считывателя»](#).

10. Настройка доступа ПО Sigur к почтовым серверам

Настройка доступа ПО Sigur к почтовым серверам может понадобиться, если вы используете какую-либо из данных функций:

- доступ по смартфону: отправка приглашающих писем и регистрация идентификаторов смартфонов в системе;
- отправка файла конфигурации считывателя;
- отправка файла конфигурации индикации считывателя.

10.1. Настройка параметров сервера исходящей почты

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 ОК.

Если всё введено верно, вы увидите сообщение «Письмо успешно отправлено». Убедитесь в факте его получения на указанном вами почтовом ящике.

10.2. Настройка параметров 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.

[S] Редактирование настроек

×

Наблюдение	Почтовый сервер для отправки исходящих писем:
Видеонаблюдение	Адрес SMTP сервера: <input type="text" value="smtp.gmail.com"/>
E-Mail	Порт SMTP сервера: <input type="text" value="465"/>
Персонал	От кого: <input type="text" value="test.sigur.stand@gmail.com"/>
Active Directory	<input checked="" type="checkbox"/> Использовать аутентификацию:
Архив	SMTP логин: <input type="text" value="test.sigur.stand@gmail.com"/>
Биометрика	SMTP пароль: <input type="password" value="....."/>
Беспроводные замки	<input checked="" type="checkbox"/> Использовать SSL
Устройства хранения	<input type="button" value="Сохранить параметры отправки e-mail и протестировать"/>
Mifare и BLE	
Зоны	
Повторные проходы	
Дополнительные параметры	Почтовый сервер для получения входящих писем:
Распознавание лиц	Сервер: <input type="text" value="imap.gmail.com"/>
HTTP(WEB)	Порт: <input type="text" value="993"/>
WEB-делегирование	Протокол: <input type="text" value="IMAP"/>
Пароли	Логин: <input type="text" value="test.sigur.stand@gmail.com"/>
Индикация	Пароль: <input type="password" value="....."/>
	E-mail: <input type="text" value="test.sigur.stand@gmail.com"/>
	<input checked="" type="checkbox"/> Использовать SSL

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

11. Работа с картами Mifare и банковскими картами

11.1. Работа в незащищённом режиме, чтение UID

Для карт Mifare и бесконтактных банковских карт МИР, Visa и MasterCard 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.
- Если ваша бесконтактная банковская карта не эмулирует какую-либо карту из семейства Mifare, то в этом же меню перейдите на вкладку «Прочие» и поставьте галку «Использовать UID в качестве идентификатора пропуска».
- Если ваша бесконтактная банковская карта эмулирует какую-либо карту из семейства Mifare, то в этом же меню выберите вкладку, на которой указан формат ваших карт (Classic или Plus). Установите пункт «В качестве идентификатора пропуска использовать» равным «UID».

Какой формат карт Mifare эмулирует ваша банковская карта вам необходимо уточнить напрямую у банка, выпустившего карту.

- Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела [«Программирование считывателя мастер-картой»](#) или [«Программирование конфигурационным файлом»](#).

11.2. Работа в защищённом режиме. Эмуляция Mifare банковской картой

Считывателем поддерживается защищённый режим работы для карт Mifare Classic 1K/4K и Mifare Plus SL3, а также банковских карт МИР, Visa и MasterCard в режиме эмуляции карты Mifare Classic 1K/4K или Plus.

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

11.2.1. Настройка работы с картами Mifare Classic 1K/4K

- 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 следуйте пунктам раздела [«Программирование считывателя мастер-картой»](#) или [«Программирование конфигурационным файлом»](#).

11.2.2. 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 заполняются 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 следуйте пунктам раздела [«Программирование считывателя мастер-картой»](#) или [«Программирование конфигурационным файлом»](#).

11.2.3. Настройка работы с банковскими картами

!	<p>Возможность работы банковских карт со СКУД напрямую зависит от банка, который выпустил вашу карту.</p> <p>Режим, в котором сейчас находится карта, необходимо уточнять напрямую у банка. Если карты находятся в режиме эмуляции карт Mifare Classic 1K/4K 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.</p>
----------	---

Произведите настройки согласно предыдущим пунктам инструкции, соответствующим картам [Classic](#) и [Plus](#).

Если у вас используются банковские карты в режиме эмуляции карт Mifare Classic 1K/4K, 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.

11.2.4. Правила заполнения служебных полей настроек карт Mifare

Заполняя служебные поля вручную, необходимо соблюдать следующие условия:

Для карт Mifare Classic 1K/4K:

1. «Номер блока памяти».

В этой строке в шестнадцатеричном формате указывается номер блока памяти для хранения идентификатора пропуска. Указываемый блок не должен быть равен «0» (нулевой блок нулевого сектора) и не должен быть последним блоком сектора:

– Для карт Mifare Classic 1K значение может быть 01h до 3Fh. Остаток от деления указываемого значения на 4 не должен равняться 3).

– Для карт Mifare Classic 4K значение может быть 01h до FFh. Остаток от деления указываемого значения на 4 не должен равняться 3) для значений, меньших 80h. Остаток от деления на 16 не должен быть равен 15 для значений, начиная с 80h.

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».

Данный параметр не используется считывателем и его значение должно оставаться равным по умолчанию, то есть отключено.

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».

11.3. 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».

12. 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.

Трафик между смартфоном и считывателем шифруется AES-алгоритмом шифрования.

Дальность и режим чтения считывателя настраивается конфигурационным файлом или мастер-картой Sigur. Последовательность настройки считывателя подробно описана в разделе «[Программирование считывателя](#)».

12.1. 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 1.0.60.59.s [и выше](#).

!	<p>Производителем не гарантируется полная функциональность приложений на смартфонах с ОС Android.</p> <p>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.</p>
----------	--

!	<p>В силу стандартных ограничений мобильных платформ идентификация в фоновом режиме или на заблокированном экране может переставать работать спустя некоторое время.</p>
----------	---

!	<p>Приложения «Sigur Доступ» и «Sigur Настройки» используют сервис «Определение местоположения» смартфона. Включите данную функцию на вашем смартфоне и предоставьте соответствующие права на её использование приложениям.</p>
----------	--

Сервис «Определение местоположения» используется нашими приложениями для сканирования BLE-устройств вокруг. Такими устройствами являются считыватели Sigur MR1.

Доступ к геолокации, в свою очередь, нашими приложениями не используется: это написано в нашей политике конфиденциальности к приложениям [здесь](#) и [здесь](#). Таким образом, наши приложения не используют и не собирают информацию о Ваших физических координатах.

Необходимость включения службы «Определение местоположения» для поиска BLE-устройств вокруг – часть архитектуры систем Android и iOS и является политикой компаний-разработчиков этих операционных систем.

- На устройствах с ОС Android версии 6.0 и выше сканирование BLE-устройств не работает без включенного модуля и предоставленных прав к функции «Определение местоположения».
- На устройствах с iOS не работает идентификация в фоновом режиме без включенной функции «Определение местоположения».

12.2. Настройка системы на работу со смартфонами

Ниже приведена информация по настройке системы Sigur для работы со смартфонами.

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

- Указание параметров конфигурации работы считывателя в ПО «Клиент» (значение параметров конфигурации описываются в данном пункте);
- [Заполнение реквизитов подключения к серверам исходящей и входящей почты;](#)
- [Программирование считывателя мастер-картой или конфигурационным файлом;](#)
- [Добавление мобильных идентификаторов в ПО.](#)

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

Здесь нужно 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, с маленькой буквы).

2. BLE идентификация MR1 – режим работы считывателя. Доступно два режима работы:

- **Не использовать** – в данном режиме ни один смартфон с запущенным приложением «Доступ» не будет считан.
- **Базовый** – в этом режиме считыватель будет реагировать на любой смартфон, на котором установлено и запущено приложение «Доступ».
- **Пользовательский** – в данном режиме работы считыватель будет реагировать только на смартфоны, которым было выслано приглашительное письмо с данного сервера.

3. Ключ — используется только в пользовательском режиме работы, и в большинстве случаев достаточно нажать «сгенерировать ключ». Этот ключ не должен меняться в дальнейшем. При его изменении всем сотрудникам потребуется выдать идентификаторы смартфонов повторно.

4. 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»](#).

5. 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.

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 дальнейших настроек считывателя не требуется, то следуйте пунктам раздела [«Программирование считывателя мастер-картой»](#) или [«Программирование конфигурационным файлом»](#).

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 или файл конфигурации. **Изменять поле «Ключ» не нужно!**

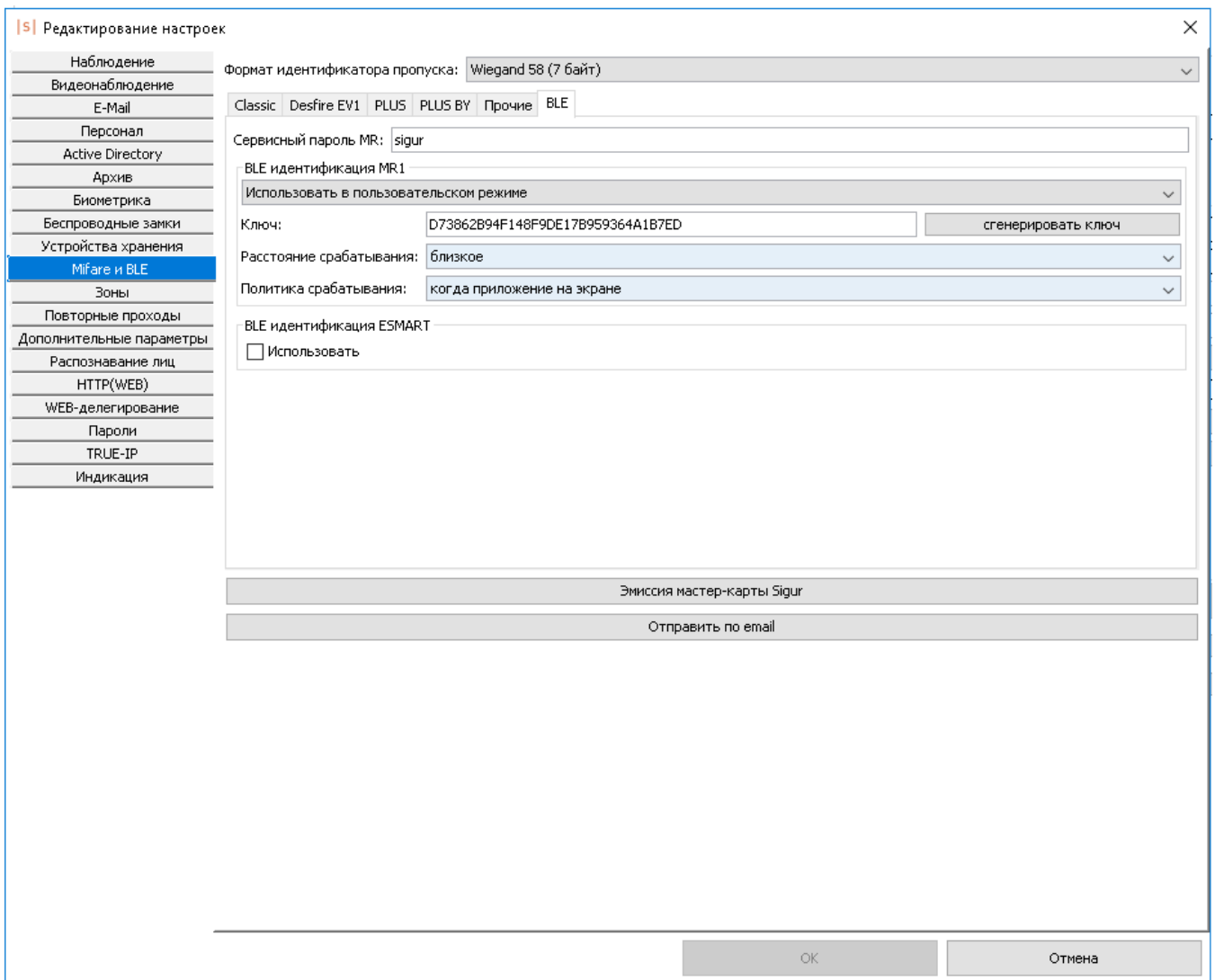


Рисунок 6. Окно настроек BLE – идентификации по смартфону

12.3. Добавление мобильных 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 приглашающих e-mail уведомлений с сервера СКУД Sigur, в которых будет содержаться специальная ссылка для мобильного приложения «Доступ». Приглашающие письма отправляются только в «Пользовательском» режиме работы.

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



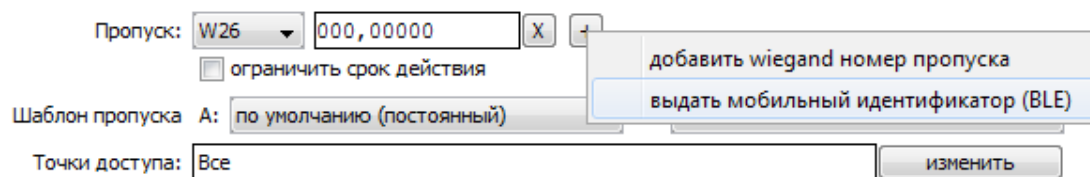
Выполнение пользователем каких-либо нестандартных действий со смартфоном (например, hard reset или переустановка приложения) может повлечь за собой необходимость повторной выдачи мобильного идентификатора. Так же известны случаи, когда мобильный идентификатор изменялся при обновлении ОС Android.

12.3.1. Отправка приглашительного письма

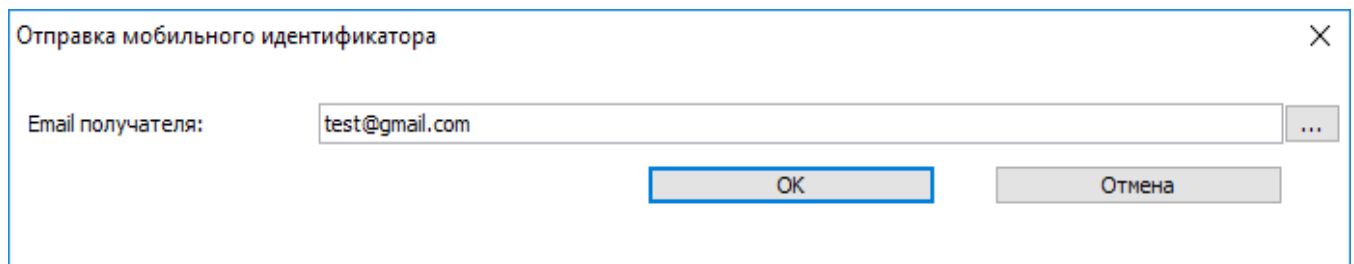
Для добавления смартфона в систему СКУД Sigur сначала необходимо задать настройки SMTP-сервера для отправки приглашительных e-mail сообщений. Если этого не было сделано ранее, следуйте пунктам раздела «[Настройка доступа к почтовым серверам](#)».

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, в которой хранится адрес электронной почты. 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.

12.3.2. Отправка ответного письма

После получения пригласительного письма:



ДОСТУП ПО ТЕЛЕФОНУ



Здравствуйте!

Вам предоставлен доступ по мобильному идентификатору. Это позволит использовать обычный смартфон как карту доступа. Для начала работы установите приложение «Sigur Доступ»:



После установки приложения перейдите по [ссылке](#).

Инструкция в приложении поможет настроить устройство. В случае проблем обратитесь к администратору объекта.

Рисунок 7. 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 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.

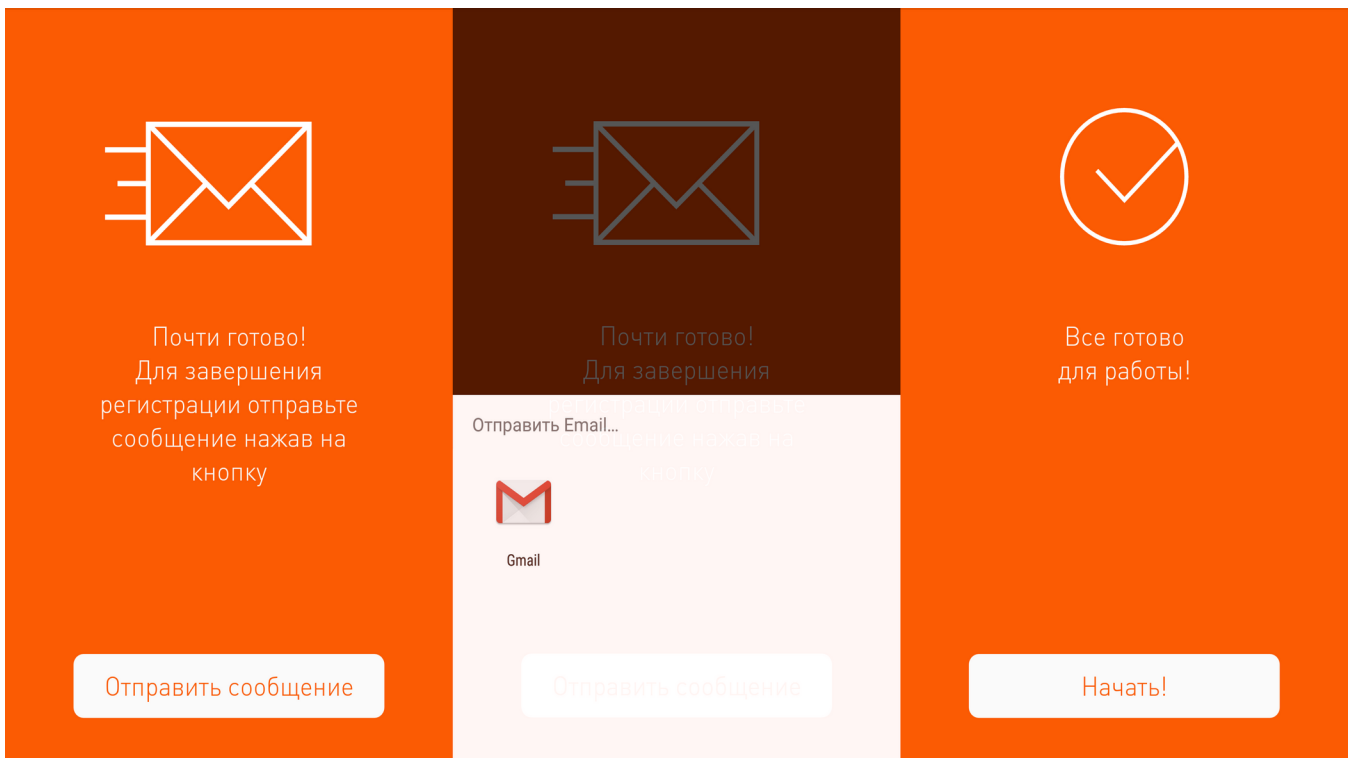


Рисунок 8. Отправка ответного письма

12.4. 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.

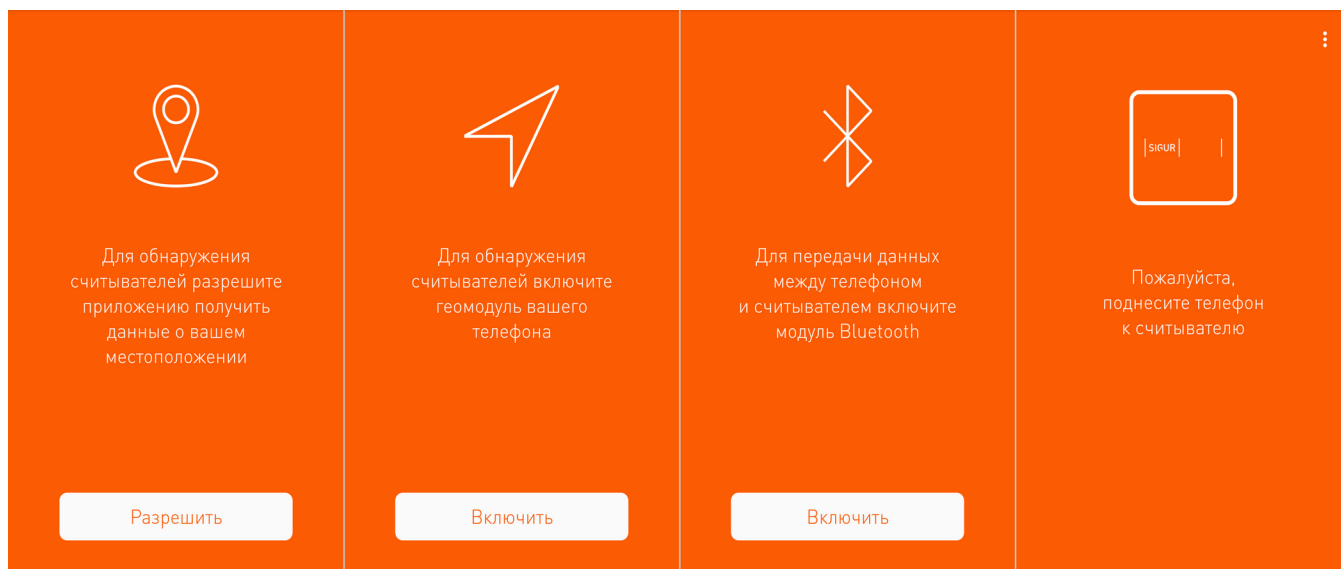


Рисунок 9. Разрешения приложения «Доступ»

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

13. Приложение «Настройки»

Приложение «Настройки» предназначено для:

- [Обновления внутреннего ПО считывателей;](#)
- [Загрузки профиля конфигурации на считыватель;](#)
- [Загрузки профиля индикации на считыватель;](#)
- [Сброса конфигурации считывателя к заводским настройкам;](#)
- [Сброса конфигурации индикации считывателя к заводским параметрам.](#)

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.

13.1. Обновление внутреннего ПО считывателя

Данная функция доступна для любой модификации считывателя Sigur MR1. Новые микропрограммы могут исправлять некоторые ошибки предыдущих версий и расширять функции считывателя.

Обновление внутреннего ПО считывателя производится с помощью приложения «[Настройки](#)».

Для проведения операции обновления внутреннего ПО считывателя:

- Включите функции: «Bluetooth», «Определение 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.
- Подойдите к считывателю(ям) 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 [сброса параметров считывателя к заводским настройкам](#). Сервисный пароль считывателя, установленный по умолчанию - «sigur» (без кавычек, с маленькой буквы).

- Дождитесь окончания отправки файла микропрограммы и обновления считывателя. Во время загрузки микропрограммы считыватель изменит свою индикацию: светодиод будет гореть желтым. После успешной загрузки считыватель перейдет к применению микропрограммы, изменив свою индикацию: светодиод будет моргать желтым и белым цветами.
- Приложение оповестит вас о результате операции, а считыватель издаст характерный звук. После обновления считыватель сразу готов к работе, все прежние настройки сохраняются.

Приложение поддерживает работу сразу с несколькими считывателями.

- Для начала выберите один из считывателей долгим нажатием, после чего можно будет выбрать еще 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.

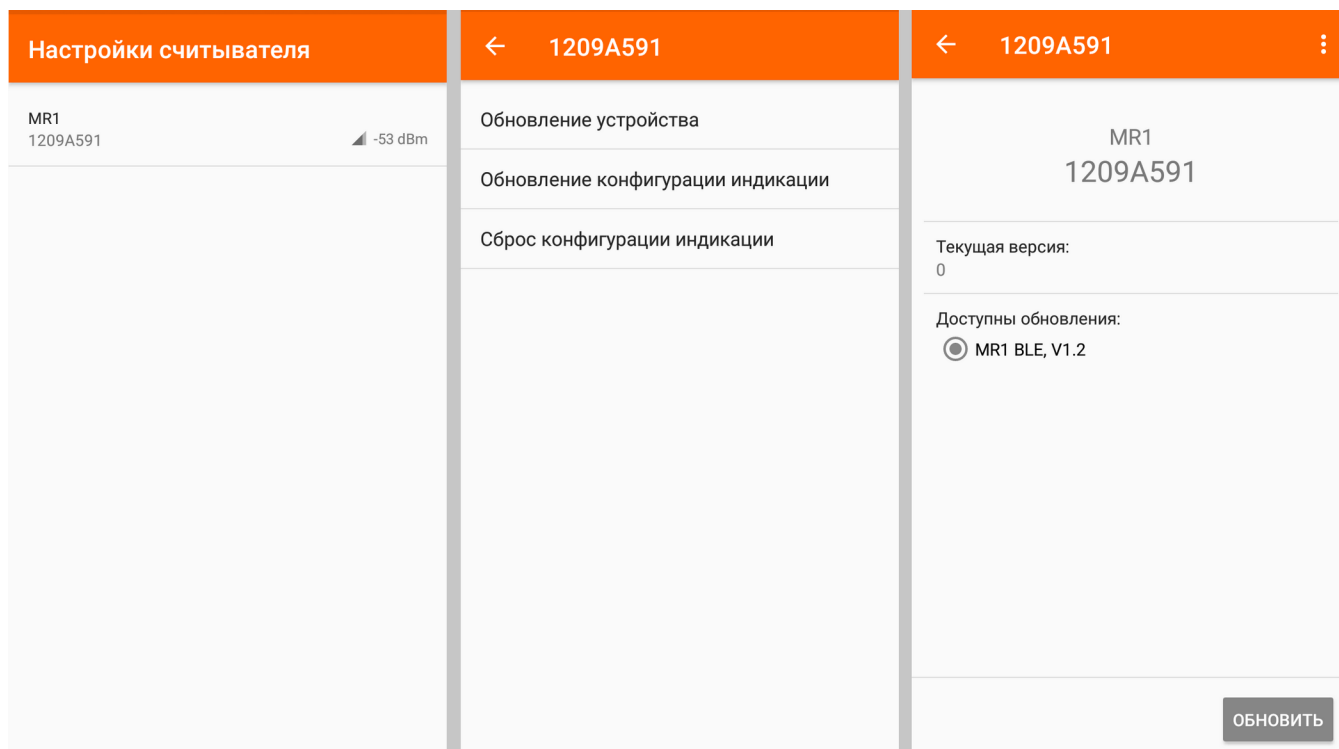


Рисунок 10. Обновление внутреннего ПО считывателя

13.2. Установка специального внутреннего ПО считывателя

Данная функция доступна для любой модификации считывателя Sigur MR1.

Обновление внутреннего ПО считывателя производится с помощью приложения «Настройки».

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

Для проведения операции обновления внутреннего ПО считывателя:

- Включите функции: «Bluetooth», «Определение местоположения» и «Wi-Fi» (или 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 попытается 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».

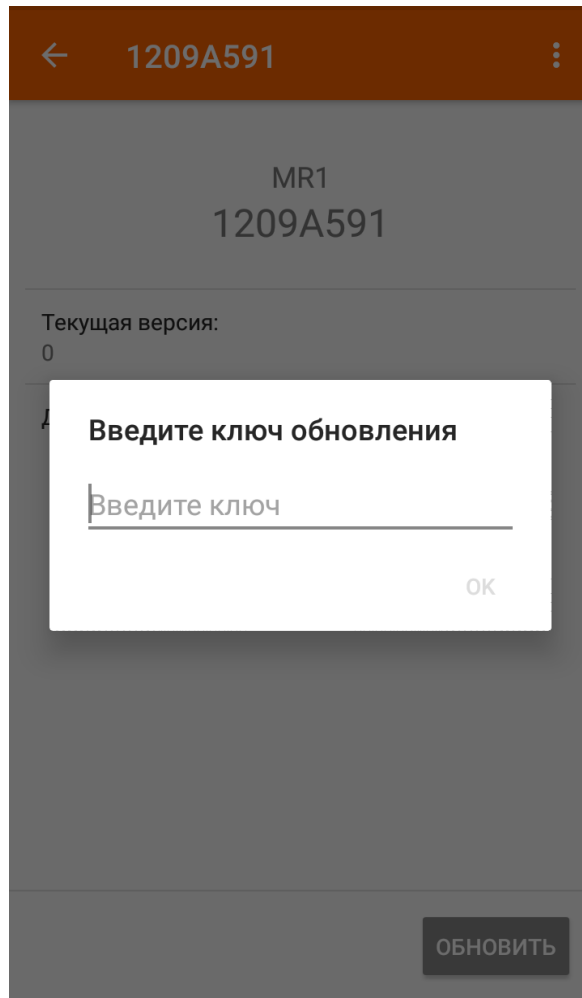


Рисунок 11. Окно ввода ключа специального ПО считывателя

13.3. Загрузка профиля конфигурации на считыватель

Данная функция доступна только для модификации считывателя Sigur MR1 BLE. Для программирования считывателя другой модификации следуйте пунктам раздела «[Программирование считывателя мастер-картой](#)».

Программирование считывателя конфигурационным файлом производится с помощью приложения «[Настройки](#)». Сам конфигурационный файл создается и отправляется на почту средствами ПО Sigur. Для получения конфигурационного файла следуйте пунктам раздела «[Программирование считывателя](#)».

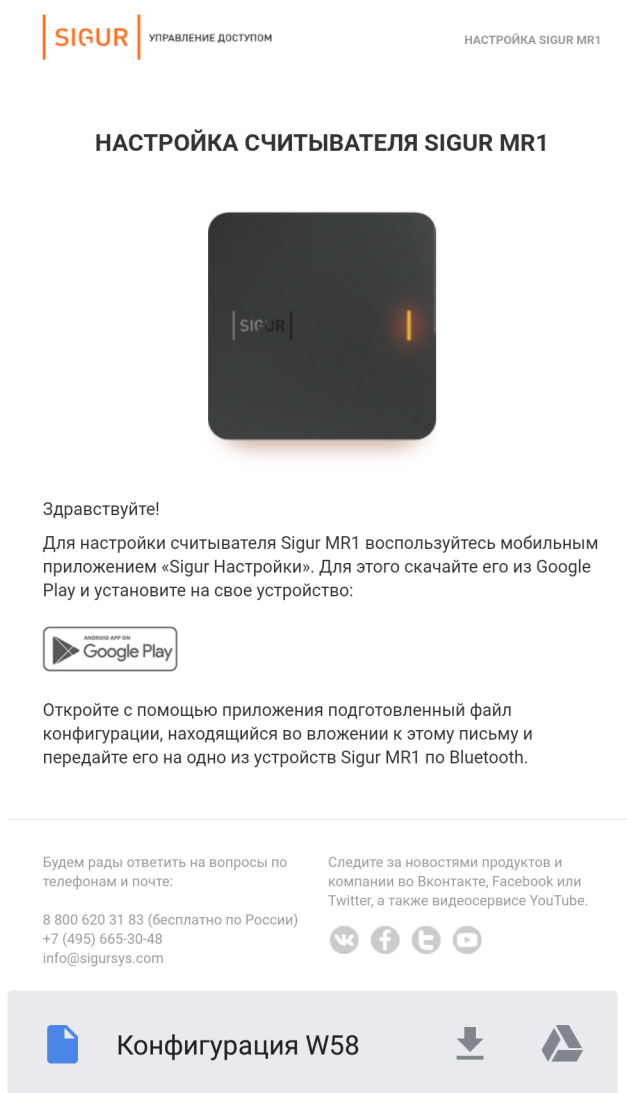


Рисунок 12. Пример письма, содержащего файл конфигурации считывателя

Для загрузки профиля конфигурации на считыватель:

- Откройте полученное письмо с прикрепленным файлом профиля конфигурации считывателя и нажмите на прикрепленный к письму файл: откроется приложение «Настройки» с уведомлением об успешном добавлении профиля конфигурации.

Данный профиль сохранится в приложении, вам не придётся нажимать на файл в письме каждый раз.

- Включите функции: «Bluetooth» и «Определение местоположения» на вашем смартфоне.
- Запустите приложение «Настройки». Выберите считыватель (несколько считывателей), на который необходимо загрузить желаемый профиль конфигурации считывателя.
- Из открывшегося списка действий выберите пункт «Обновление конфигурации».
- Если данный пункт отсутствует в списке действий, то убедитесь в том, что модель считывателя соответствует требованиям выше и обновите [внутреннее ПО считывателя](#) до последней доступной версии.
- Из открывшегося списка профилей конфигурации выберите желаемый и введите сервисный пароль считывателя.
- Дождитесь окончания загрузки конфигурации на считыватель.
- Конфигурация применится по окончании загрузки, перезагрузка считывателя не требуется. После применения новых параметров считыватель издаст характерный звук и приложение уведомит Вас об успешности операции.

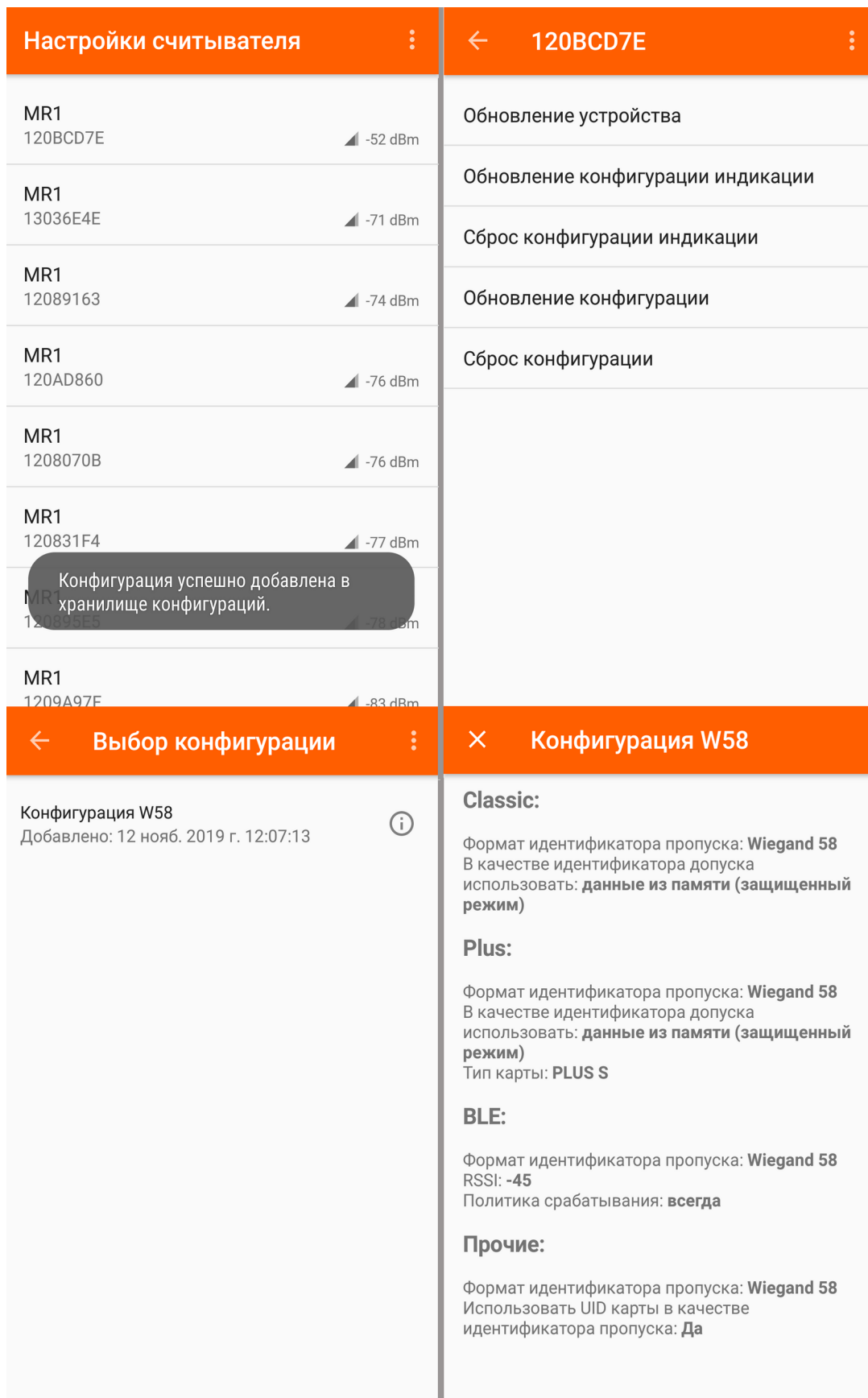


Рисунок 13. Пример добавления профиля конфигурации считывателя и просмотр информации о нем

13.4. Программный сброс параметров считывателя

Данная функция доступна только для модификации считывателя Sigur MR1 BLE. Для сброса параметров к заводским считывателя другой модификации следуйте пунктам раздела «[Аппаратный сброс](#)».

Для проведения операции программного сброса параметров считывателя на смартфоне должно быть установлено приложение «[Настройки](#)».

Для проведения операции программного сброса считывателя:

- Включите функции: «Bluetooth» и «Определение местоположения» на вашем смартфоне и запустите приложение «Настройки».
- Выберите считыватель (несколько считывателей), конфигурацию которого необходимо сбросить к заводским параметрам.
- Из открывшегося списка действий выберите пункт «Сброс конфигурации».

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

- Дождитесь окончания операции конфигурации на считыватель. По окончании операции считыватель издаст характерный звук и приложение уведомит Вас об успешности операции.
- Заводская конфигурация применится по окончании загрузки, перезагрузка считывателя не требуется.

13.5. Загрузка профиля индикации на считыватель

Загрузка профиля индикации возможна только на считывателях модификации 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 прикрепленным профилем индикации.

Сам профиль индикации создаётся и отправляется на почту средствами ПО Sigur. Для его получения следуйте пунктам раздела «[Настраиваемая индикация считывателя](#)».



Рисунок 14. Пример письма, содержащего профиль индикации

Для загрузки профиля индикации на считыватель:

- Откройте полученное письмо с прикрепленным файлом профиля индикации и нажмите на прикрепленный к письму файл: откроется приложение «Настройки» с уведомлением об успешном добавлении профиля индикации. Данный профиль сохранится в приложении, вам не придется нажимать на файл в письме каждый раз.
- Включите функции: «Bluetooth» и «Определение местоположения» на вашем смартфоне.
- Запустите приложение «Настройки». Выберите считыватель или несколько считывателей, 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 доступной 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.

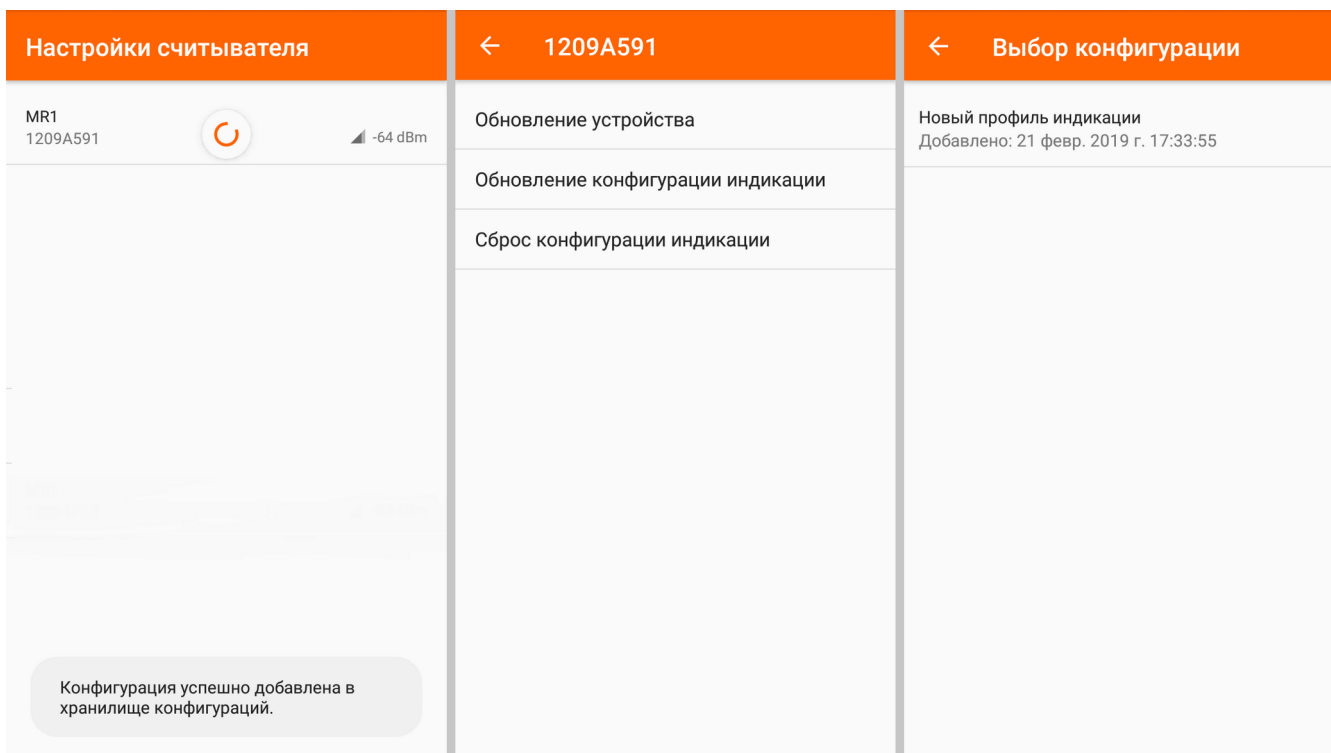


Рисунок 15. Добавление нового профиля индикации

13.6. Сброс конфигурации индикации считывателя

Данная функция доступна только для модификации считывателя Sigur MR1 BLE.

Для сброса конфигурации индикации считывателя на смартфоне должно быть установлено приложение «[Настройки](#)».

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.

14. Логика обработки идентификаторов

В данном разделе описаны основные моменты логики работы считывателя с разными типами идентификаторов.

14.1. Чтение карты

После поднесения карты формата Mifare или любого другого идентификатора, удовлетворяющего стандарту ISO 14443-A к включенному считывателю в область его чтения:

- Считыватель определяет формат поднесенной карты: Mifare Classic, Mifare Plus или «Прочая»;
- В зависимости от заранее загруженной на считыватель конфигурации, определяет режим чтения карты по её типу: «Защищенный», «UID» или «Нет»;
- Если настройка для данного типа карты не предусматривает её чтение, то считыватель не реагирует на карту: отсутствует какая-либо индикация считывателя, на Wiegand-выход не передаётся никаких данных.
- Если настройка для данного типа карты предусматривает чтение UID, то считыватель пытается прочитать уникальный открытый код карты.
- Если настройка для данного типа карты предусматривает работу с защищенной областью памяти карты, то считыватель пытается авторизоваться в блоке памяти карты. Номер блока памяти и ключ указаны в конфигурации считывателя.

В случае успешной авторизации считывается информация из данного блока памяти. В случае неуспешной авторизации никакой реакции от считывателя не последует: в данном случае отсутствует какая-либо индикация считывателя, на Wiegand-выход не передаётся никаких данных.

- После успешного чтения код карты передаётся на Wiegand-выход считывателя. В качестве кода передаётся N байт, определенных конфигурацией Wiegand-выхода считывателя: Wiegand-26 — 3 байта, Wiegand-34 – 4 байта, Wiegand-58 – 7 байт.

В случае защищенного режима — это первые N байт блока памяти карты, без смещений.

Если считанный код содержит меньше информации, чем разрядность Wiegand-выхода, то код дополняется ведущими нулями.

- Второй раз одна и та же карта может быть прочитана только спустя 1 секунду. Если та же карта подносится повторно к считывателю раньше, то интервал ожидания обновляется и считыватель не реагирует на эту карту.

- Другая карта может быть поднесена сразу же, задержек при чтении в этом случае не возникает.

14.2. Чтение смартфона

- Если приложение «Доступ» запущено, ему предоставлены соответствующие права и на смартфоне включены функции «Bluetooth» и «Определение местоположения», то приложение пытается обнаружить считыватели Sigur MR1 BLE.
- Если в результате сканирования было найден один или более считывателей Sigur MR1 BLE, то с каждым из них последовательно выполняются следующие операции:
- Со считывателя приложение получает данные о его настройках:
 - Включен ли на считывателе режим чтения смартфонов;
 - Установленная дальность чтения смартфонов;
 - Режим срабатывания («Когда приложение на экране», «Приложение в фоне, экран разблокирован» или «Всегда»);
 - Режим чтения смартфонов: «не использовать», «базовый» или в «пользовательский»;
 - Уникальную информацию о сервере, на котором создавался конфигурационный файл или мастер-карта для считывателя.
- Идентификация будет произведена (смартфон «считается») в случае, если выполнены следующие условия:
 - Режим чтения смартфонов «Базовый» или «Пользовательский».
 - Показания мощности сигнала на антенне смартфона, наводимой сигналом с данного считывателя, больше по номинальной величине значения, установленного настройками считывателя (отрицательные значения dBm).
 - Состояние приложения и смартфона соответствует политике срабатывания, установленной настройками считывателя (приложение в фоне, экран разблокирован и т.п.);
 - Данный смартфон «не появлялся» в области чтения данного считывателя дольше 5 секунд.

Под «появлением» стоит понимать не только физическое положение смартфона относительно считывателя, но и выполнение политики срабатывания в текущий момент на смартфоне. Например, если политика срабатывания на считывателе «Приложение на экране», то перевод приложения в фоновый режим работы аналогичен выходу из зоны чтения считывателя.

Таким образом, если смартфон «появлялся», то каждое его «появление» увеличивает это ожидание ещё на 5 секунд. Если смартфон совсем не покидает область чтения, то идентификация произойдёт лишь один раз;

– Сравнивается информация о сервере СКУД, с которого был запрограммирован считыватель с информацией о сервере СКУД, указанном в одном из загруженных «пригласительных» писем. Если считыватель работает в «базовом» режиме, этот шаг пропускается.

- После выполнения всех вышеуказанных условий, на считыватель передаётся идентификатор смартфона, который можно посмотреть в разделе «О программе» приложения «Доступ». Если какое-либо условие не выполняется, код не передаётся на считыватель.
- После получения считывателем идентификатора смартфона, его код передаётся на Wiegand-выход считывателя. В качестве кода передаётся N байт, определенных конфигурацией считывателя: Wiegand-26 — 3 байта, Wiegand-34 – 4 байта, Wiegand-58 – 7 байт.

ООО «Промышленная автоматика – контроль доступа»
603002, г. Нижний Новгород, ул. Советская, д. 18 Б, 1 этаж
Техническая поддержка: 8 (800) 700 31 83, +7 (495) 665 30 48, +7 (831) 260-12-93

Система контроля и управления доступом Sigur

Сайт: sigur.com

Электронная почта: info@sigur.com