



Считыватель Sigur МК100. Описание и инструкция по эксплуатации

Редакция от 19.08.2026

«Промавтоматика», г. Н. Новгород, 2026 г.

Оглавление

1.	Введение	5
2.	Версии документа	7
3.	Технические характеристики	8
4.	Комплект поставки	11
5.	Общие функции считывателя	12
6.	Монтаж считывателя	14
6.1.	Назначение клемм считывателя	14
6.2.	Общие рекомендации по монтажу считывателя	15
6.3.	Рекомендации по выбору кабелей	16
7.	Подключение кнопок и датчиков к считывателю	18
8.	Режимы работы и функции считывателя	21
8.1.	Описание режимов работы считывателя	21
8.2.	Дополнительный режим работы считывателя	21
8.3.	Функция предоставления доступа	22
8.4.	Функция управления охранными зонами	23
8.5.	Функция изменения режима точки доступа	24
8.6.	Параметры работы считывателя по умолчанию	25
8.7.	Процесс настройки считывателя	25
9.	Программирование считывателя	26
9.1.	Программирование считывателя через ПО «Клиент»	26
9.1.1.	Программирование считывателя мастер-картой	28
9.1.2.	Программирование считывателя конфигурационным файлом	29
9.1.3.	Программирование считывателя через протокол SSDP	32
9.2.	Программирование считывателя через приложение «Sigur Настройки»	34
10.	Настройка режимов работы считывателя	35
10.1.	Настройка режимов с помощью «Sigur Настройки»	35
10.2.	Настройка режимов через SSDP	37
11.	Настройка расширенных функций считывателя	38
11.1.	Настройка функции управления охранными зонами	38
11.2.	Настройка функции изменения режима точки доступа	40
11.2.1.	Настройка функции изменения режима точки доступа для нескольких объектов доступа	45
11.3.	Конфигурация длины PIN-кода для расширенных функций	47
12.	Сброс параметров считывателя к заводским настройкам	49
12.1.	Аппаратный сброс	49
12.2.	Сброс параметров считывателя через приложение «Sigur Настройки»	49
13.	Работа с PIN-кодами в качестве идентификаторов	50
14.	Работа с картами Mifare	51
14.1.	Работа в незащищённом режиме, чтение UID	51
14.2.	Работа в защищённом режиме	51
14.2.1.	Настройка работы с картами Mifare Classic 1K/4K	51
14.2.2.	Настройка работы с картами Mifare Plus	52
14.2.3.	Правила заполнения служебных полей настроек карт	

	Mifare	53
15.	Работа с банковскими картами	55
15.1.	Чтение UID или эмуляция Mifare банковской картой	55
15.2.	Чтение PAN-номера банковской карты	56
16.	Работа с картами EM Marine и HID ProxCard II	57
17.	Работа со смартфонами в качестве идентификатора	58
17.1.	Идентификация по смартфону, общие сведения	58
17.2.	Общие требования к смартфонам и ПО	58
17.3.	Настройка системы на работу со смартфонами	60
17.4.	Работа с приложением «Sigur Доступ»	62
18.	Занесение идентификаторов в ПО Sigur	65
18.1.	Занесение PIN-кодов	65
18.2.	Занесение карт	67
18.3.	Занесение мобильных идентификаторов	68
18.3.1.	Добавление мобильных идентификаторов в ПО	68
18.3.2.	Отправка приглашительного письма	69
18.3.3.	Групповая выдача мобильных идентификаторов	70
18.3.4.	Отправка ответного письма	70
19.	Настройка реакции на событие «Считыватель оторван от стены»	73
20.	Приложение «Sigur Настройки»	74
20.1.	Назначение приложения «Sigur Настройки»	74
20.2.	Настройка темы интерфейса	74
20.3.	Поиск считывателей в радиусе действия BLE смартфона	76
20.4.	Смена пароля считывателей	77
20.5.	Обновление внутреннего ПО считывателя	78
20.6.	Добавление лицензии на считыватель	80
20.7.	Работа с файлом конфигурации чтения	83
20.8.	Сброс конфигурации чтения считывателя	87
20.9.	Загрузка профиля индикации на считыватель	88
20.10.	Сброс конфигурации индикации считывателя	91
20.11.	Настройка выходного интерфейса считывателя	91
21.	Шифрование данных, передаваемых по OSDP	93
21.1.	Создание профиля шифрования OSDP	93
21.2.	Применение профиля шифрования OSDP	94
21.3.	Сброс профиля шифрования	96
21.4.	Изменение профиля шифрования	98
22.	Обновление внутреннего ПО считывателя через программу «Клиент»	100
23.	Индикация считывателя	102
23.1.	Сигналы управления индикацией	102
23.1.1.	Управление индикацией при подключении по Wiegand	102
23.1.2.	Настройка режима внешнего управления индикацией считывателя	103
23.1.3.	Управление индикацией при подключении по OSDP	104
23.1.4.	Стандартные профили индикации считывателя	107
23.2.	Настройка пользовательской индикации считывателя	109
23.2.1.	Создание профиля индикации считывателя	110
23.2.2.	Создание реакции считывателя	117
23.2.3.	Добавление звука реакции считывателя	118
23.2.4.	Способы загрузки пользовательского профиля	

	индикации на считыватель	120
24.	Журнал системных событий	122
25.	Логика обработки идентификаторов	128
25.1.	Чтение карты	128
25.2.	Чтение смартфона	128
25.3.	Чтение PIN-кода	130
26.	Логика работы системы Sigur при выполнении расширенных функций считывателя	133
26.1.	Логика работы системы при постановке зоны на охрану с помощью PIN-кода	133
26.2.	Логика работы системы при снятии зоны с охраны при проходе через точку доступа	136
26.3.	Логика работы системы при изменении режима точки доступа	137
27.	Настройка доступа ПО Sigur к почтовым серверам	140
27.1.	Настройка параметров сервера исходящей почты	140
27.2.	Настройка параметров сервера входящей почты	141
28.	Контакты	142

1. Введение

Данный документ содержит описание и инструкцию по эксплуатации считывателя Sigur MK100. Считыватель представлен в двух модификациях MK100 и MK100 Pro.

Считыватели Sigur MK100 — это настенные считыватели с сенсорной клавиатурой для ввода персонального идентификационного номера (PIN-кода), предназначенные для использования в составе систем контроля доступа.

Все модификации считывателя MK100 поддерживают идентификаторы стандарта Mifare (Ultralight, Classic, Mini, ID, DESFire, Plus), включая защищённый режим для Mifare DESFire EV1 и семейства Mifare Classic, а также защищённые режимы SL1 и SL3 для семейства Mifare Plus. Кроме того, поддерживаются банковские бесконтактные карты МИР, Visa и MasterCard. Использование банковской карты в качестве идентификатора возможно при выполнении одного из условий:

1. Поддержка технологии EMV.
2. Наличие статического UID (для использования карты в режиме чтения UID).
3. Наличие эмуляции карт Mifare Classic или Plus, соответствующей документу «AN10833 MIFARE Type Identification» компании NXP (для работы с картами в защищённом режиме).

Дополнительно считыватели Sigur MK100 и MK100 Pro поддерживают идентификацию по смартфону с использованием технологий BLE (Bluetooth Low Energy) и/или HCE (Host-based Card Emulation). Поддерживаются смартфоны под управлением ОС Android, РЕД ОС М (BLE, HCE) и iOS (BLE). Возможна идентификация по PAN-номеру банковской карты.

Все модификации считывателя MK100 также позволяют использовать карты стандартов Em-Marine и HID ProxCard II (125kHz) в качестве идентификатора.

Сенсорная кодонаборная панель позволяет выполнять следующие функции:

- предоставление доступа;
- управление охранными зонами;
- изменение режима точки доступа.

Модификация считывателя Sigur MK100 Pro дополнительно поддерживает загрузку лицензий, расширяющих базовую функциональность устройства.

Считыватели Sigur MK100 рассчитаны на круглосуточный режим работы, не должны использоваться в условиях воздействия агрессивных сред и во взрывоопасных помещениях.

Предприятие-изготовитель несёт ответственность за точность предоставляемой документации, и при существенных модификациях элементов системы обязуется предоставлять обновлённую редакцию данной документации.

Данный документ соответствует версии ПО Sigur 1.8.4.35 и версии микропрограммы считывателя 56.

2. Версии документа

Данный документ имеет следующую историю ревизий.

Ревизия	Дата публикации	Что изменилось
0001	11 ноября 2025 г.	Первая публикация.
0002	19 января 2026 г.	Добавлена информация о поддержке РЕД ОС М для мобильных приложений «Sigur Доступ» и «Sigur Настройки».
0003	24 марта 2026 г.	Добавлена информация о поддержке функции изменения режима точки доступа.
0004	20 апреля 2026 г.	Добавлена информация о пакетах и лицензиях, поддерживающих функцию групповой выдачи мобильных идентификаторов.
0005	10 июня 2026 г.	Добавлен раздел с описанием подключения OSDP кнопок и датчиков к считывателям MK100 Pro. Добавлена информация о длительности световой индикации. Добавлена информация о допустимых средствах очистки.
0006	19 августа 2026 г.	Добавлена информация о классе защиты IK08. Актуализирована информация о работе приложения «Sigur Настройки» в связи с выходом версии 2.0.0. Обновлена информация о минимальной версии ОС Android для работы приложения «Sigur Настройки».

3. Технические характеристики

Технические характеристики.

Модификация считывателя:	MK100	MK100 Pro
Формат поддерживаемых идентификаторов	- Mifare (Ultralight, Classic, Mini, ID, DESFire, Plus), включая защищённые режимы SL1 и SL3 семейства Mifare Plus, защищённый режим Mifare DESFire EV1 и семейства Mifare Classic. - Бесконтактные банковские карты MasterCard, Visa, МИР в режиме чтения UID при наличии статического UID/в защищённом режиме при наличии эмуляции Mifare Classic или Plus, соответствующей документу «AN10833 MIFARE Type Identification» компании NXP. - Все идентификаторы стандарта ISO14443-A в режиме чтения UID. - Смартфоны (Android, РЕД ОС М) по технологиям HCE и BLE. - Смартфоны (iOS) по технологии BLE. - PAN-номер банковской карты по технологии EMV (MasterCard, Visa, МИР, в т. ч. добавленные в электронные кошельки: МИР Pay, Google Pay, Apple Wallet, Samsung Pay). - Em-Marine. - HID ProxCard II (125 kHz). - Цифровой код.	
Интерфейс связи с контроллером	- Wiegand настраиваемой битности (6, 26, 34, 58); - OSDP (RS-485).	
Поддержка подключения OSDP кнопок и датчиков (совместно с контроллерами E2 Pro / E4 Pro).	Нет	Да
Поддержка лицензируемых функций	Нет	Да

Модификация считывателя:	МК100	МК100 Pro
Средства диагностики	- Встроенные средства самопроверки; - Датчик снятия считывателя с настенной панели; - Датчик температуры; - Оцифровка напряжения питания.	
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).	
Напряжение питания	12 В (9...28 В)	
Потребляемый ток в режиме ожидания	Не более 130 мА	
Потребляемый ток при чтении идентификатора	Не более 230 мА	
Мощность передатчика BLE	Не более 6,3 мВт	
Мощность передатчика RFID	Не более 2,5 Вт	
Класс защиты	IP66, IK08	
Температурный режим	От -40 °С до +60 °С	
Габариты	90x90x12 мм	
Масса нетто	Не более 0,3 кг	
Масса брутто	Не более 0,4 кг	
Индикация		
Световая	- Многоцветный светодиодный индикатор; - Подсветка сенсорной клавиатуры.	
Звуковая	Широкополосный акустический динамик, РСМ 16 бит, 44.1 кГц, моно.	
Поддерживаемые звуковые форматы	.wav, .aiff, .au	

Модификация считывателя:	MK100	MK100 Pro
Длительность загружаемых звуков	Не более 45 секунд.	

4. Комплект поставки

Комплект поставки.

Номер	Позиция	Количество
1	Считыватель Sigur	1 шт.
2	Настенная панель	1 шт.
3	Ключ для снятия с настенной панели	1 шт.
4	Комплект крепежа	1 шт.
5	Монтажный шаблон	1 шт.
6	Паспорт или гарантийный талон	1 шт.

5. Общие функции считывателя

Считыватели Sigur MK100 и MK100 Pro совместимы со СКУД Sigur, а также с большинством других систем контроля доступа.

Устройства оснащены сенсорной кодонаборной панелью, предназначенной для ввода персонального идентификационного номера (PIN-кода) и выполнения ряда функций без использования карты.

Кодонаборная панель включает:

- цифры от 0 до 9;
- кнопку «Ввод» (✓);
- кнопку «Отмена» (X).

Считыватели поддерживают 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. Поддерживаются защищённые режимы SL1 и SL3 семейства Mifare Plus, защищённый режим семейства Mifare DESFire EV1 и семейства Mifare Classic 1K/4K;
- любыми другими идентификаторами стандарта ISO 14443-A в режиме чтения UID;
- бесконтактными банковскими картами МИР, Visa и MasterCard в режиме эмуляции карт Mifare;
- бесконтактными банковскими картами в режиме чтения PAN-номера карты;
- смартфонами с ОС Android, РЕД ОС М или iOS по технологии BLE (Bluetooth Low Energy) при установленном мобильном приложении «Sigur Доступ»;
- смартфонами с ОС Android или РЕД ОС М по технологии HCE (Host Card Emulation) при установленном мобильном приложении «Sigur Доступ»;
- картами формата EM Marine;
- картами формата HID ProxCard II (125 kHz);
- цифровыми PIN-кодами различной длины.

Устройства Sigur MK100 и MK100 Pro оснащены:

- OSDP-выходом. Считыватели MK100 и MK100 Pro можно подключить по OSDP к контроллерам любых производителей, поддерживающим стандарт OSDP версии 2.2. Если считыватели подключаются по интерфейсу OSDP к контроллеру Sigur (E2, E4), то взаимодействие происходит по протоколу SSDP (Sigur Supervised Device Protocol), который имеет расширенную функциональность, характерную только для оборудования Sigur;
- Wiegand-выходом настраиваемой битности;

- многоцветным световым индикатором и подсветкой сенсорной клавиатуры;
- широкополосным акустическим динамиком;
- тремя цифровыми входами для управления индикацией считывателя (активны при работе контроллера со считывателем по Wiegand);
- средствами самодиагностики, в том числе датчиком снятия с настенной панели, датчиком температуры и датчиком замера питающего напряжения.

С помощью кодонаборной панели считыватели позволяют реализовать следующий функционал:

- доступ по PIN-коду;
- двухфакторная аутентификация (PIN + пропуск).

Считыватели Sigur MK100 и MK100 Pro также поддерживают расширенный функционал, а именно:

- управление охранными зонами;
- изменение режима точки доступа.

Расширенный функционал доступен только при подключении считывателей MK100 и MK100 Pro к контроллерам Sigur.

6. Монтаж считывателя

Процедура монтажа считывателя подробно описана в прилагаемом к считывателю руководстве по монтажу. Актуальная версия документа также доступна на нашем сайте по [ссылке](#).

6.1. Назначение клемм считывателя



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

Назначение клемм считывателя Sigur.

Название	Назначение
PWR	«Плюс» напряжения питания.
GND	«Общий» напряжения питания, линий данных и управления.
D0/A	Линия данных Wiegand 0 или A (RS-485).
D1/B	Линия данных Wiegand 1 или B (RS-485).
LEDR	Первый цифровой вход управления индикацией считывателя. Если считыватель находится в заводской конфигурации, то при активации входа следует включение звукового и светового сигнала запрета доступа.
LEDG	Второй цифровой вход управления индикацией считывателя. Если считыватель находится в заводской конфигурации, то при активации входа следует включение звукового и светового сигнала разрешения доступа.

Название	Назначение
БЕЕР	Третий цифровой вход управления индикацией считывателя. Если считыватель находится в заводской конфигурации, то при активации входа следует включение звукового и светового сигнала ожидания дополнительного действия. Вход используется также для аппаратного сброса считывателя к заводским настройкам.

6.2. Общие рекомендации по монтажу считывателя

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;
- в местах, подвергающихся длительному воздействию прямых солнечных лучей — это повышает вероятность перегрева устройства, сопровождающееся отключением звукового динамика.



Для очистки корпуса и лицевой панели считывателя используйте только чистящие средства, предназначенные для акриловых поверхностей (ПММА). Использование иных средств может привести к повреждению поверхности изделия.

6.3. Рекомендации по выбору кабелей

При подключении также ознакомьтесь с рекомендациями от производителя контроллера, к которому будет выполняться подключение.

Подключение по Wiegand.

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

Допустимо использование любых типов сигнальных кабелей, например, КСПВ 8х0,5.

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

Подключение по OSDP.

Рекомендуется выполнять кабелем типа UTP 5 категории, либо специальными кабелями (например, для внутренней проводки – КИПЭВ, КИПвЭВ, для наружной – КИПЭП, КИПвЭП).

Допускается использование свободных линий связи, проложенных на объекте, выполненных кабелем не ниже третьей категории (ЛВС, телефония). Не допускается прокладка линии связи рядом с силовыми кабелями переменного тока и кабелями управления мощными устройствами.

Электрические характеристики интерфейса RS-485 позволяют при соблюдении правил монтажа создавать сегменты линии связи до 1200 метров.

7. Подключение кнопок и датчиков к считывателю

Считыватель Sigur в модификации Pro оснащён встроенными дискретными входами LEDG, LEDR и BEEP, к которым можно напрямую подключать кнопки и датчики — например, кнопку запроса на выход или датчик положения двери.

Поддерживаются нормально разомкнутые и нормально замкнутые устройства — нормальное состояние каждого входа задаётся при настройке в ПО «Клиент». Для работы функции считыватель должен быть подключён к контроллеру по интерфейсу OSDP.

Это позволяет:

- сократить длину кабельных трасс за счёт подключения кнопок и датчиков к ближайшему считывателю;
- расширить количество управляющих элементов на точке доступа без использования дополнительных входов контроллера.



Возможность подключения кнопок и датчиков доступна только при совместном использовании считывателя Sigur в модификации Pro с контроллерами Sigur E2 Pro или E4 Pro.

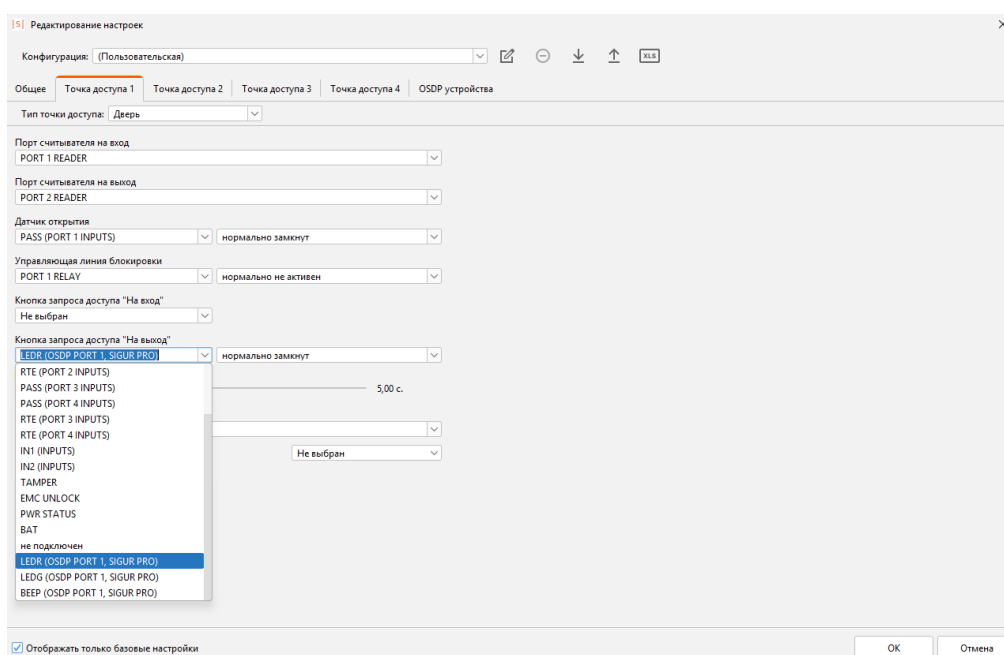
Для работы данного функционала должны выполняться следующие технические требования:

- версия микропрограммы контроллера Sigur E2 Pro / E4 Pro должна быть не ниже 1.24.1.

Для настройки данного функционала выполните следующие шаги:

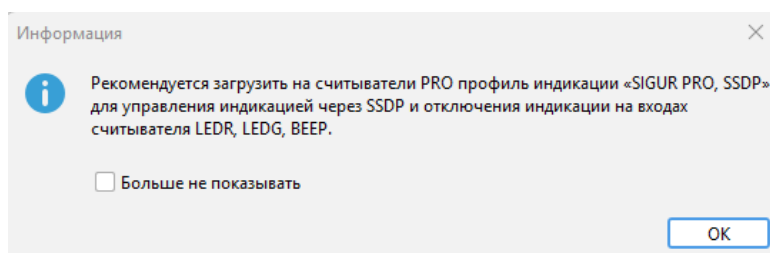
1. Подключите считыватель к контроллеру E2 Pro / E4 Pro по интерфейсу OSDP и настройте параметры связи в ПО «Клиент» на вкладке «OSDP-устройства». Порядок подключения и настройки описан в разделе «Считыватели с интерфейсом OSDP» инструкции по эксплуатации контроллера соответствующей модели.
2. В ПО «Клиент» перейдите на вкладку «Точка доступа N». Для функции «Порт считывателя» (в соответствующем направлении) укажите логический порт контроллера, настроенный для взаимодействия со считывателем, подключённым по интерфейсу OSDP.

3. Настройте необходимую логическую функцию: укажите вход считывателя, к которому подключена кнопка или датчик, и задайте нормальное состояние входа. В качестве примера рассмотрим подключение кнопки запроса доступа «На выход».



Пример настройки функции «Кнопка запроса доступа "На выход"».

4. После настройки всех необходимых параметров нажмите «ОК». При сохранении конфигурации появится информационное окно с напоминанием о необходимости загрузить профиль индикации. Нажмите «ОК» и загрузите на считыватель рекомендуемый профиль индикации Sigur PRO, SSDP. Это необходимо, так как в стандартном профиле входы считывателя LEDG, LEDR и BEEP используются для управления световой и звуковой индикацией — при назначении этих входов на функции необходимо переключить их в режим «Без реакции». Порядок загрузки описан в разделе «Загрузка профиля индикации на считыватель».



Информационное окно.

После завершения настройки при нажатии кнопки, подключённой к входу считывателя в системе зафиксировывается соответствующее событие — так же, как при нажатии кнопки, подключённой непосредственно к контроллеру.

Список событий:		
Время	Точка	Событие
2026-06-04 17:35:37		Зарегистрирован проход при открытой двери. Объект: Попов О. Р. . Напр.: вход.
2026-06-04 17:35:43		Зарегистрирован проход, санкционированный с кнопки. Напр.: выход.

Пример отображения события прохода по кнопке, подключённой к считывателю.

8. Режимы работы и функции считывателя

8.1. Описание режимов работы считывателя

Считыватели MK100 и MK100 Pro поддерживают два режима работы кодонаборной панели: основной и дополнительный.

По умолчанию считыватель находится в основном режиме работы, на который назначена функция прохода через точку доступа по PIN-коду.

Опционально может быть настроен дополнительный режим для выполнения следующих функций:

- управление охранными зонами;
- изменение режима точки доступа.

8.2. Дополнительный режим работы считывателя

Активация дополнительного режима.

Для активации дополнительного режима считывателя выполните следующие действия:

1. Назначьте необходимую функцию на дополнительный режим считывателя в приложении «Sigur Настройки» или в ПО «Клиент», если считыватель подключён по протоколу SSDP к контроллеру Sigur.
2. Настройте выбранную функцию в ПО «Клиент». Подробная информация о настройке в разделе «Настройка расширенных функций считывателя».

Переход в дополнительный режим.

Чтобы воспользоваться функцией, назначенной на дополнительный режим, переведите считыватель в этот режим — нажмите и удерживайте кнопку «Ввод» на кодонаборной панели.

При успешном переходе:

- будет проигран звуковой сигнал;
- подсветка клавиатуры изменится на красный цвет;
- цвет основного светодиодного индикатора при этом не изменится.

Если на дополнительный режим не назначена ни одна функция, при удержании кнопки «Ввод» считыватель продолжит работать в основном режиме.

Работа в дополнительном режиме.

После перехода в дополнительный режим считыватель ожидает ввод PIN-кода функции, назначенной на этот режим. После ввода PIN-кода устройство подаст световую и звуковую индикацию, подтверждающую успешное выполнение команды или отказ. Затем считыватель вернётся в основной режим работы, индикация изменится на индикацию по умолчанию.

Возврат в основной режим.

Считыватель автоматически выходит из дополнительного режима и возвращается в основной в одном из следующих случаев:

- введён 7-значный PIN-код;
- введён PIN-код длиной менее 7 символов и нажата кнопка «Ввод»;
- введён PIN-код длиной менее 7 символов и истёк тайм-аут в 5 секунд после получения последнего символа PIN-кода;
- нажата кнопка «Ввод» без ввода PIN-кода;
- истёк тайм-аут в 5 секунд без ввода PIN-кода.

Считыватель возвращается в основной режим независимо от того, верно введён PIN-код или нет.

8.3. Функция предоставления доступа

Считыватель позволяет осуществлять проход через точку доступа, используя:

1. **Только PIN-код** (PIN идентификации) – пользователь вводит заранее назначенный PIN-код на сенсорной панели устройства. После подтверждения система проверяет код и, при совпадении, разрешает проход.
2. **Карту + PIN-код** (PIN верификации) – пользователь прикладывает карту к считывателю, после чего система запрашивает ввод PIN-кода. Доступ предоставляется только при правильном сочетании карты и PIN-кода.
3. **Только карту** – пользователь прикладывает карту к считывателю, система проверяет её подлинность и права доступа. При успешной проверке доступ разрешается без дополнительной аутентификации.

Таким образом, PIN-код может использоваться как основной идентификатор или как дополнительный фактор проверки.

8.4. Функция управления охранными зонами



Функция доступна только при подключении считывателей MK100 и MK100 Pro к контроллерам Sigur E2 и E4.

Функция управления охранными зонами позволяет ставить зону на охрану с помощью ввода специального PIN-кода функции или снимать зону с охраны при разрешении доступа с использованием различных идентификаторов. Пользователь вводит PIN-код функции, после чего система проверяет права доступа и выполняет соответствующее действие. Индикация на панели отображает результат — успешную операцию, отказ или ошибку. Данная функция позволяет осуществлять активацию/деактивацию охранного шлейфа, находясь непосредственно у точки доступа.

Для управления охранными зонами необходимо:

1. Назначить функцию «Постановка на охрану» на основной или дополнительный режим считывателя. Подробнее о настройке режимов — в разделе «Настройка режимов работы считывателя».
2. Сконфигурировать параметры управления охранными зонами в ПО «Клиент», где можно выбрать способ постановки зоны на охрану, задать PIN-код и настроить функцию снятия с охраны при разрешении входа. Подробная информация — в разделе «Настройка функции управления охранными зонами».

Кодонаборная панель предоставляет следующий функционал управления охранными зонами:

1. Постановка на охрану: удержание карты перед считывателем. Активация охранного шлейфа осуществляется с помощью карты сотрудника. Подробнее в разделе «Удержание карты перед считывателем» Руководства пользователя ПО Sigur.
2. Постановка на охрану: PIN-код. Зона ставится на охрану после ввода специального PIN-кода.
3. Постановка на охрану: PIN-код + пропуск. В этом случае вводится спец. код и подтверждается пропуском сотрудника.
4. Снятие с охраны: зона снимается с охраны по факту разрешения доступа конкретному сотруднику.

Также пользователь может управлять охранными зонами вручную через ПО «Клиент» или использовать автоматическое управление зонами по расписанию. Подробнее в [Руководстве пользователя ПО Sigur](#).

8.5. Функция изменения режима точки доступа



Функция доступна только при подключении считывателей MK100 и MK100 Pro к контроллерам Sigur.

Данная функция позволяет переключать режим точки доступа между следующими состояниями:

- нормальный;
- разблокированный;
- заблокированный.

Изменять режим можно с помощью специального PIN-кода или двухфакторной аутентификации (спец. PIN + пропуск). Объект доступа вводит PIN-код функции и при необходимости подтверждает действие пропуском. После этого система проверяет права доступа и выполняет соответствующее действие. Индикация на панели отображает результат — успешную операцию, отказ или ошибку.

Для изменения режима точки доступа необходимо:

1. Назначить функцию «Изменение режима ТД» на основной или дополнительный режим считывателя. Подробнее о настройке режимов — в разделе [«Настройка режимов работы считывателя»](#).
2. Сконфигурировать параметры функции в ПО «Клиент» для конкретного объекта доступа или отдела. Подробная информация — в разделе [«Настройка функции изменения режима точки доступа»](#).

Также пользователь может изменять режимы точек доступа вручную через ПО «Клиент». Подробнее в [Руководстве пользователя ПО Sigur](#).

8.6. Параметры работы считывателя по умолчанию

При первом включении, а также после сброса конфигурации чтения считыватель имеет следующие настройки:

Параметры работы считывателя по умолчанию.

Название параметра	MK100	MK100 Pro
Выходной интерфейс	Wiegand-26	
Чтение карт Mifare (Ultralight, Classic, Mini, ID, DESFire, Plus)	UID (прямой порядок байт)	
Чтение прочих карт стандарта ISO14443-A	UID	
Чтение карт EM Marine и HID ProxCard II	Включено, фиксированный facility – не используется	
Чтение PAN-номера банковской карты	Отключено	
Работа считывателя со смартфонами	«Базовый» режим работы, дальность чтения – «Близко» и режим работы – «Когда приложение на экране»	
Функции кодонаборной панели	Основной режим – Проход через точку доступа по PIN-коду; Дополнительный режим – не используется.	
Сервисный пароль считывателя	sigur	

8.7. Процесс настройки считывателя

Настройка считывателя выполняется последовательно и включает несколько взаимосвязанных этапов. В процессе настройки производится программирование считывателя, выбор режимов его работы, а также конфигурирование дополнительных функций.

Подробное описание каждого этапа приведено в соответствующих разделах настоящего руководства:

1. [Программирование считывателя](#);
2. [Настройка режимов работы считывателя](#);
3. [Настройка расширенных функций считывателя](#) (при необходимости).

9. Программирование считывателя

В данном разделе под программированием считывателя понимается настройка параметров чтения идентификаторов и запись заданных параметров одним из способов в память устройства. Программирование не включает полную конфигурацию устройств.

Для модификаций считывателя Sigur MK100 возможны следующие варианты программирования:

- Программирование считывателя через ПО «Клиент». Параметры считывателя настраиваются непосредственно в ПО, после чего конфигурация записывается в считыватель одним из доступных способов.
- Программирование считывателя через приложение «Sigur Настройки». Конфигурация создаётся и передаётся на считыватель с помощью мобильного приложения. Настройка таким способом возможна только при использовании ОС Android.



Настройки считывателя должны соответствовать параметрам системы, используемой для выдачи идентификаторов. Если в качестве основного программного обеспечения используется ПО Sigur, рекомендуется настраивать считыватели через ПО «Клиент».

9.1. Программирование считывателя через ПО «Клиент»

Один из возможных вариантов программирования считывателей – через ПО «Клиент». Для работы можно использовать любую актуальную версию ПО, включая бесплатную. Дистрибутив доступен для скачивания на нашем официальном сайте.

Передать созданную конфигурацию на считыватель возможно одним из способов:

- Программирование мастер-картой – запись конфигурации на считыватель с помощью специальной карты.
- Программирование конфигурационным файлом – загрузка конфигурации на считыватель с помощью мобильного приложения «Sigur Настройки».
- Программирование через протокол SSDP – передача конфигурации на считыватель по интерфейсу OSDP. Доступно только при подключении считывателя к контроллеру по OSDP.



Вне зависимости от выбранного способа передачи файла конфигурации необходимо предварительно установить следующие параметры работы считывателя в ПО «Клиент».

Настройки параметров в ПО «Клиент».

Чтобы приступить к настройке, откройте ПО «Клиент» и перейдите в меню «Файл» – «Настройки» – «Бесконтактная идентификация».

Файл конфигурации считывателя включает **все настройки со всех подвкладок** раздела «Бесконтактная идентификация». Например, если вы настроили защищённый режим работы только для Mifare Plus, считыватель будет обращаться к защищённой области этих карт, а для других типов карт Mifare будет использоваться режим, заданный на соответствующих подвкладках (например, чтение UID).

Настраиваемые параметры считывателя:

- Формат Wiegand-выхода. Поддерживаются форматы Wiegand-26, 34 и 58.
- Работа считывателя с картами Mifare Classic, Mifare Plus и Mifare Desfire. Настройте режим чтения (UID или защищённый режим), порядок чтения байт (только для Mifare Classic 1K/4K и Mifare Plus).
- Работа с мобильными идентификаторами. Настройте режим («Базовый» или «Пользовательский»), секретный ключ, дальность срабатывания и политику чтения смартфонов.
- Сервисный пароль считывателя.
- Работа с картами EM-Marine и HID ProxCard II. Дополнительно можно активировать фиксированный Facility Code.
- Работа с банковскими картами (EMV).
- Функция «Удержание карты перед считывателем».
- Порядок чтения остальных идентификаторов стандарта ISO 14443-A, не указанных в данном разделе (например, Mifare Ultralight), настраивается на подкладке «Прочие».

ISO 14443-A – это распространённый стандарт бесконтактной идентификации, поддерживаемый большинством карт Mifare, NFC-модулями смартфонов и другими идентификаторами. По умолчанию считыватели Sigur обрабатывают UID всех идентификаторов этого стандарта.

Если вы работаете с картами в защищённом режиме, отключите чекбокс «Использовать UID карты в качестве идентификатора пропуска» на подкладке «Прочие». Это исключит считывание UID других идентификаторов ISO 14443-A, не указанных в разделе «Бесконтактная идентификация». Чекбокс также необходимо отключить при работе с банковскими картами по EMV и/или со смартфонами по HCE.

Подробности о работе с конкретными типами идентификаторов и требованиях к настройке можно найти в отдельных разделах:

- [Работа с PIN-кодами в качестве идентификатора.](#)
- [Работа с картами Mifare.](#)
- [Работа с банковскими картами.](#)
- [Работа с картами EM Marine и HID ProxCard II.](#)
- [Работа со смартфонами в качестве идентификатора.](#)

Информация по настройке режимов работы кодонаборной панели представлена в соответствующем [разделе](#).

9.1.1. Программирование считывателя мастер-картой



Данный способ доступен для всех считывателей Sigur независимо от используемого интерфейса для подключения к контроллеру.

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

- Карта Mifare Classic 1K/4K или Mifare Plus в транспортной конфигурации, т. е. «чистая».
- Настольный USB-считыватель Sigur MR100 USB, ACR1252U или ESMART DUAL USB. Для ESMART DUAL USB требуется драйвер производителя и соответствующий модуль лицензии.
- ПО Sigur с официального сайта. Для настройки подойдёт [бесплатная версия](#).

Необходимо выполнить следующие действия:

1. В меню «Файл» – «Настройки» – «Бесконтактная идентификация» ПО «Клиент» настройте необходимые параметры считывателя. Перечень доступных для программирования параметров и порядок их настройки представлен в разделе [«Программирование считывателя через ПО «Клиент»](#).
2. После установки всех параметров работы считывателя 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 Mifare Plus мастер-карты Sigur с иными параметрами потребуется новая «чистая» карта. Мастер-карты Mifare Plus не подлежат очистке.

3. Если считыватель МК100 был запрограммирован ранее, то сначала нужно произвести его аппаратный сброс. Процесс описан в разделе «Аппаратный сброс».
4. Если считыватель МК100 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.

9.1.2. Программирование считывателя конфигурационным файлом



Данный способ доступен для всех считывателей Sigur независимо от используемого интерфейса для подключения к контроллеру.

Для программирования считывателя конфигурационным файлом вам потребуется:

- Смартфон с поддержкой функции BLE под управлением ОС Android или РЕД ОС М с установленным приложением «Sigur Настройки».
- Опционально: доступ к почтовому ящику, с которого будет отправлен файл конфигурации средствами ПО Sigur. Файл конфигурации может быть передан на смартфон альтернативными способами (через мессенджеры, флеш-накопитель и пр.).
- ПО Sigur с официального сайта. Для настройки подойдёт бесплатная версия.

Необходимо выполнить следующие действия:

1. В меню «Файл» – «Настройки» – «Бесконтактная идентификация» ПО «Клиент» настройте необходимые параметры считывателя. Перечень доступных для программирования параметров и порядок их настройки представлен в разделе «Программирование считывателя через ПО «Клиент»». Когда все необходимые параметры будут настроены, нажмите на кнопку «ОК», чтобы все внесённые изменения применились.

2. Передайте созданную конфигурацию на смартфон и добавьте её в приложение «Sigur Настройки». Доступны два способа: сохранение файла конфигурации на диск и отправка файла конфигурации по e-mail.
3. Загрузите добавленный профиль конфигурации из приложения на считыватель.

Способ 1. Сохранение файла конфигурации на диск.

1. В ПО «Клиент» в меню «Файл» – «Настройки» – «Бесконтактная идентификация» нажмите кнопку «Сохранить на диск».

Кнопка «Сохранить на диск» в меню «Файл» – «Настройки» – «Бесконтактная идентификация».

2. В открывшемся окне выберите директорию для сохранения файла и при необходимости измените название файла.
3. Передайте сохранённый файл на смартфон любым удобным способом, например через мессенджер (Telegram, Viber и пр.).
4. Откройте полученный файл на смартфоне с помощью приложения «Sigur Настройки» или добавьте его в приложение через раздел «Конфигуратор» с помощью кнопки «Загрузить файл». Приложение отобразит уведомление об успешном добавлении конфигурации.

Способ 2. Отправка файла конфигурации по e-mail.



Этот способ предпочтителен для пользователей, у которых уже настроен доступ к серверу исходящей почты.

Файл конфигурации считывателя можно отправить на e-mail непосредственно из ПО Sigur. Для отправки письма с конфигурационным файлом серверу Sigur потребуется доступ к серверу исходящей почты. Подробная инструкция по настройке реквизитов сервера исходящей почты представлена в разделе «[Настройка параметров сервера исходящей почты](#)».

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

Отправка конфигурации по email ×

Название конфигурации

E-mail адреса получателей

Окно отправки конфигурации по email.

3. Откройте на смартфоне полученное письмо с прикрепленным файлом профиля конфигурации считывателя.
4. Нажмите на прикрепленный к письму файл: откроется приложение «Sigur Настройки» с уведомлением об успешном добавлении профиля конфигурации. Данный профиль сохранится в приложении.



Пример письма, содержащего файл конфигурации считывателя.

Загрузка профиля конфигурации на считыватель.

Дальнейший порядок действий одинаков для обоих способов передачи файла.

1. Включите функции Bluetooth и «Определение местоположения» на вашем смартфоне.
2. Запустите приложение «Sigur Настройки».
3. Выберите из списка устройств один или несколько считывателей, настройки которых требуется изменить. В открывшемся списке действий выберите пункт «Чтение карт».
4. Выберите из списка доступных конфигураций нужный файл и в панели действий нажмите кнопку «Загрузка файла конфигурации чтения на считыватель» (оранжевая стрелка). При необходимости введите сервисный пароль считывателя.
5. Новый профиль конфигурации будет загружен на выбранные считыватели автоматически. Конфигурация применится по окончании загрузки, перезагрузка устройств не требуется. После применения новых параметров считыватель издаст характерный звук, и приложение уведомит вас об успешности выполнения операции.

9.1.3. Программирование считывателя через протокол SSDP



Этот способ актуален только для тех случаев, когда считыватель Sigur подключён к контроллеру Sigur по интерфейсу OSDP.

Данная возможность — отличительная особенность протокола SSDP, позволяющая централизованно с рабочего места обновить конфигурацию чтения на считывателях. Настройка режимов работы устройств через SSDP приведена в отдельном разделе.

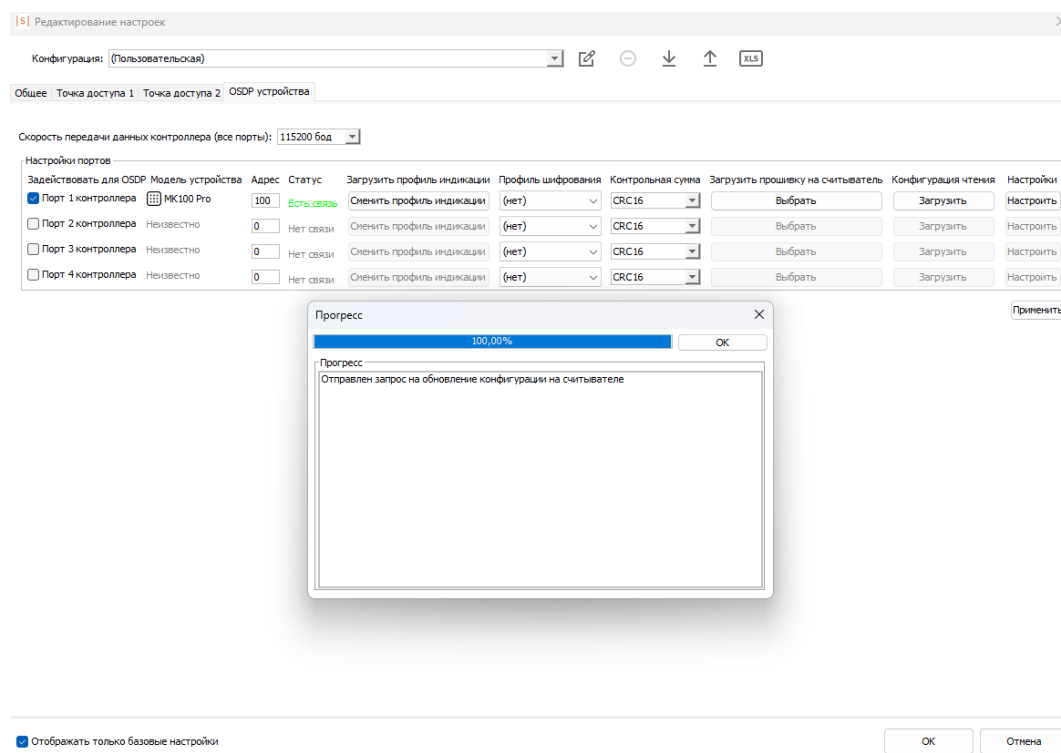
Необходимо соблюсти следующие технические требования:

- версия микропрограммы считывателя Sigur должна быть не ниже 53;
- версия микропрограммы контроллера Sigur должна быть не ниже 1.23.X;
- версия ПО Sigur должна быть не ниже 1.6.7.60.

Для программирования считывателей потребуется ПО Sigur, подойдёт бесплатная версия.

Загрузка конфигурации чтения на считыватель будет осуществляться через ПО «Клиент». Процесс состоит из нескольких шагов:

1. В меню «Файл» – «Настройки» – «Бесконтактная идентификация» настроить необходимые параметры считывателя. Более подробно про настройку параметров можно посмотреть в разделе [«Программирование считывателя через ПО «Клиент»](#). Когда все необходимые параметры будут настроены, нажать на кнопку «ОК», чтобы все внесённые изменения применились.
2. На вкладке «Оборудование» необходимо установить связь с контроллером Sigur (E2 или E4), к которому по интерфейсу OSDP подключён считыватель.
3. В меню настроек точки доступа на вкладке «OSDP устройства» для конкретного порта контроллера нажать кнопку «Загрузить» в блоке «Конфигурация чтения». Начнётся процесс загрузки конфигурации чтения на считыватель.
4. По окончании процесса загрузки конфигурации на считыватель необходимо нажать на кнопку «ОК» в окне прогресса обновления. Результат загрузки конфигурации чтения на считыватель протоколируется в журнале системных событий, подробнее о котором можно прочитать в соответствующем [разделе](#).



Окно прогресса обновления конфигурации чтения на считывателе.

9.2. Программирование считывателя через приложение «Sigur Настройки»

Данный способ доступен для смартфонов под управлением ОС Android или РЕД ОС М.

В отличие от программирования через ПО «Клиент», конфигурация чтения создаётся непосредственно на смартфоне — компьютер и подключение к серверу Sigur не требуются. Способ удобен, когда доступа к рабочему месту с ПО Sigur нет.

В приложении задаются только параметры чтения идентификаторов. Сервисный пароль в файл конфигурации не входит и настраивается отдельно — см. раздел «Смена пароля считывателей».

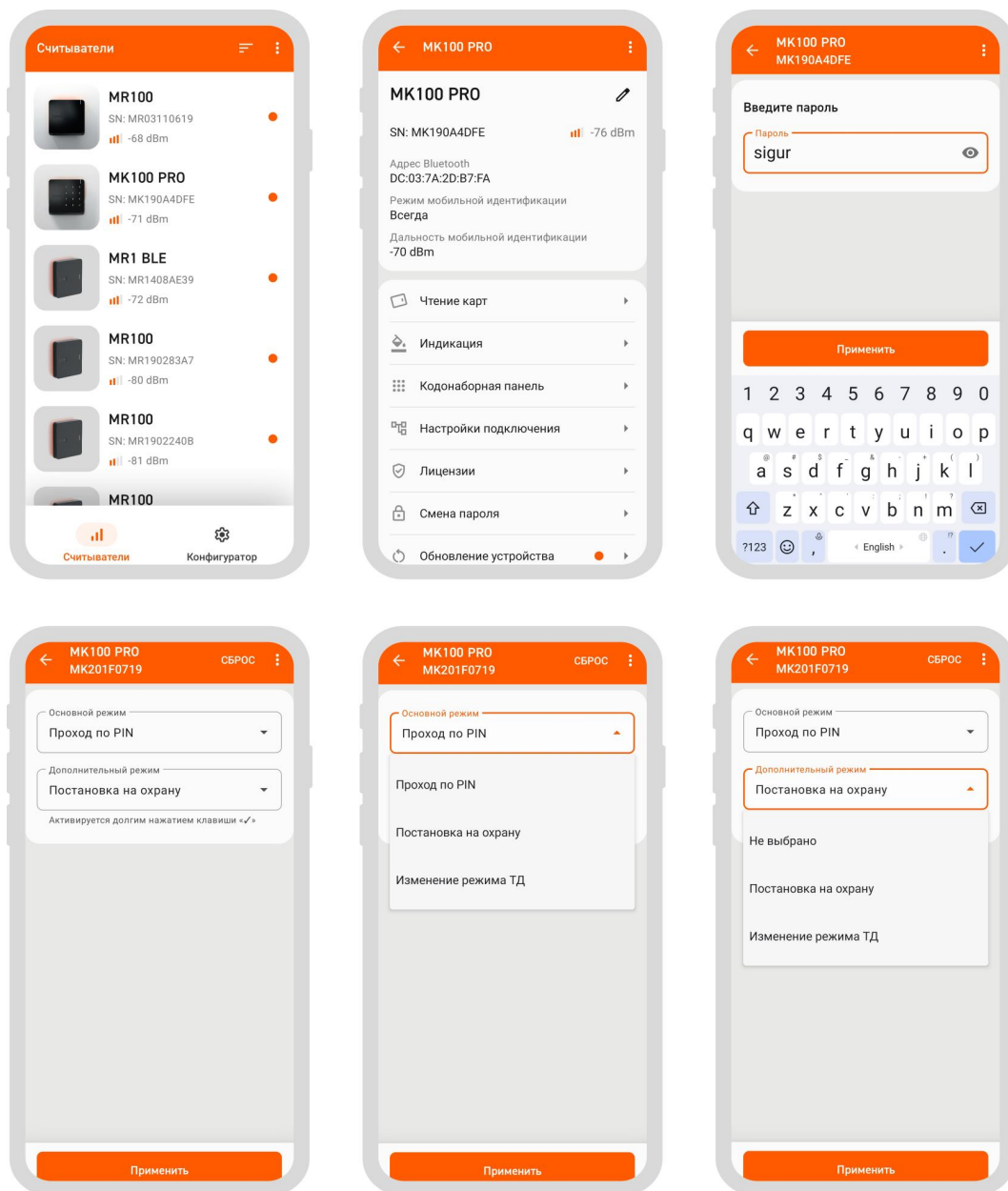
Порядок создания файла конфигурации, перечень доступных настроек и порядок загрузки готового файла на считыватели описаны в разделе «Работа с файлом конфигурации чтения».

10. Настройка режимов работы считывателя

10.1. Настройка режимов с помощью «Sigur Настройки»

Для настройки функций основного и дополнительного режима кодонаборной панели:

1. Убедитесь, что версия установленного приложения «Sigur Настройки» 1.0.29 или выше, версия микропрограммы считывателя — 53 или выше.
2. Откройте приложение «Sigur Настройки» и выберите считыватель из списка.
3. Из открывшегося списка действий выберите пункт «Кодонаборная панель».
4. При необходимости введите сервисный пароль считывателя (пароль по умолчанию – **sigur**).
5. Выберите нужный режим работы и назначьте ему функцию. Для основного режима доступны: «Проход по PIN», «Постановка на охрану» и «Изменение режима ТД». Для дополнительного режима можно выбрать только «Постановку на охрану» или «Изменение режима ТД». По умолчанию для основного режима установлена функция «Проход по PIN», для дополнительного — значение «Не выбрано». Это означает, что в дополнительном режиме выполнение каких-либо действий с помощью считывателя невозможно. Одну и ту же функцию нельзя назначить одновременно на оба режима.
6. Подтвердите операцию.
7. Дождитесь окончания загрузки настроек на считыватель. Настройки применятся автоматически, перезагрузка считывателя не требуется.

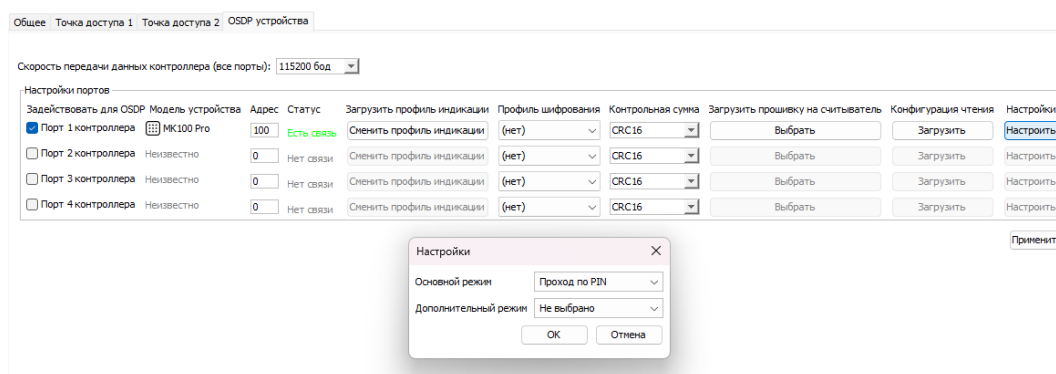


Настройка режимов кодоначборной панели.

10.2. Настройка режимов через SSDP

Для настройки функций основного и дополнительного режима кодаборной панели:

1. Убедитесь, что версия установленного ПО «Клиент» 1.6.7.60 или выше, версия микропрограммы считывателя — 53 или выше.
2. Откройте ПО в «Клиент» вкладку «Оборудование».
3. Выберите точку доступа контроллера, к которому подключён настраиваемый считыватель.
4. Перейдите на вкладку «Настройки» — «OSDP устройства».
5. Выберите нужный считыватель и в столбце «Настройки» нажмите кнопку «Настроить». Для основного режима по умолчанию выбрана функция «Проход по PIN». Для дополнительного значение «Не выбрано». Это означает, что в дополнительном режиме выполнение каких-либо действий с помощью считывателя невозможно. Настройка одной функции для двух режимов невозможна.
6. Подтвердите операцию, нажав кнопку «ОК».
7. Дождитесь окончания загрузки настроек на считыватель. Настройки применятся автоматически, перезагрузка считывателя не требуется.



Окно редактирования настроек OSDP устройств.

11. Настройка расширенных функций считывателя

11.1. Настройка функции управления охранными зонами



Данный функционал доступен при подключении считывателей MK100 и MK100 Pro к контроллерам Sigur E2 и E4.

Для настройки данного функционала выполните следующие шаги:

1. Убедитесь, что версия установленного ПО «Клиент» 1.6.7.60 или выше, версия микропрограммы считывателя — 53 или выше, версия микропрограммы контроллера — 1.23.2 или выше.
2. Убедитесь, что функция управления охранными зонами настроена на один из режимов считывателя — основной или дополнительный. Подробная информация о настройке режимов работы считывателя приведена в [этом разделе](#).
3. Откройте ПО в «Клиент» вкладку «Оборудование».
4. Выберите точку доступа контроллера, к которому подключён настраиваемый считыватель, нажмите кнопку «Настройки». В открывшемся окне редактирования настроек на вкладке «Точка доступа» настройте охранный шлейф. Нажмите «ОК».
5. На вкладке «Оборудование» перейдите в раздел «Настройки» — «Охрана».
6. Установите нужный способ постановки зоны на охрану, при необходимости сгенерируйте или введите ручную PIN-код.
7. Подтвердите операцию, нажав кнопку «Применить». При нажатии кнопки «Отменить» изменения не сохраняются.

Настройки:

Основные | Профиль шифрования | Биометрика | Охрана | Видеонаблюдение

Охранный шлейф 1

Способ постановки зоны на охрану: Не выбрано

☐ Снимать с охраны при разрешении входа

Применить Отменить

Вкладка «Охрана».

Настройки:

Основные | Профиль шифрования | Биометрика | Охрана | Видеонаблюдение

Охранный шлейф 1

Способ постановки зоны на охрану: PIN

? PIN: 1234 Сгенерировать

☐ Снимать с охраны при разрешении входа

Применить Отменить

Назначение PIN-кода на вкладке «Охрана».

Подробное описание работы системы при постановке зоны на охрану и снятии зоны с охраны приведено в данном разделе.

Настройка функции для нескольких точек доступа.

На вкладке «Оборудование» можно выбрать несколько точек доступа или целый каталог для одновременной настройки.

Если среди выбранных точек доступа есть хотя бы одна, которой назначен охранный шлейф, в перечне вкладок настроек становится доступна вкладка «Охрана».

Изменения параметров, задаваемых на вкладке «Охрана», применяются только к тем выбранным точкам доступа, для которых назначен охранный шлейф.

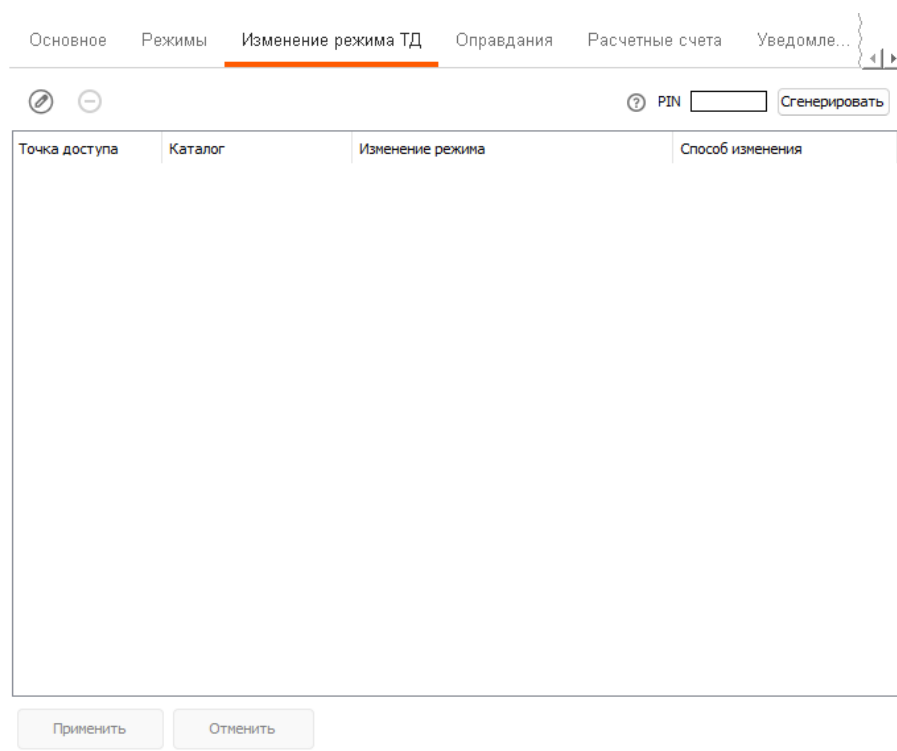
11.2. Настройка функции изменения режима точки доступа



Данный функционал доступен при подключении считывателей MK100 и MK100 Pro к контроллерам Sigur.

Для настройки данного функционала выполните следующие шаги:

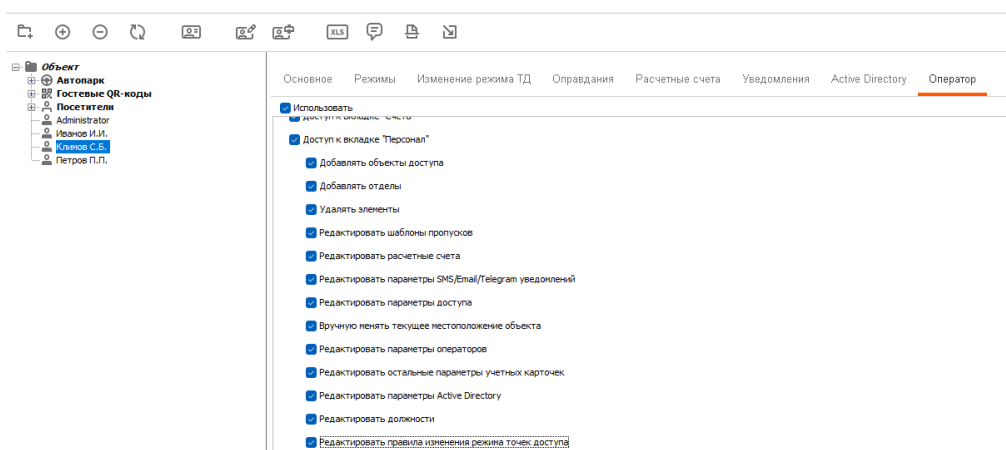
1. Убедитесь, что версия установленного ПО «Клиент» 1.6.8.101 или выше, версия микропрограммы считывателя — 53 или выше, версия микропрограммы контроллера — 1.24.0 или выше.
2. Убедитесь, что функция изменения режима ТД настроена на один из режимов считывателя — основной или дополнительный. Подробная информация о настройке режимов работы считывателя приведена в [этом разделе](#).
3. Откройте в ПО «Клиент» вкладку «Персонал».
4. Выберите объект доступа, которому необходимо назначить функцию изменения режима ТД. Конфигурирование функции осуществляется в разделе «Изменение режима ТД». Раздел отображается только при выборе объекта доступа с типом «Сотрудник», либо при выборе отдела с типом «Регулярный отдел».



Раздел «Изменение режима ТД».



По умолчанию раздел «Изменение режима ТД» недоступен. Для его отображения у оператора должны быть права на доступ к вкладке «Персонал» и на редактирование правил изменения режима точек доступа. Подробнее о настройке прав операторов см. в соответствующем разделе [Руководства пользователя ПО Sigur](#).

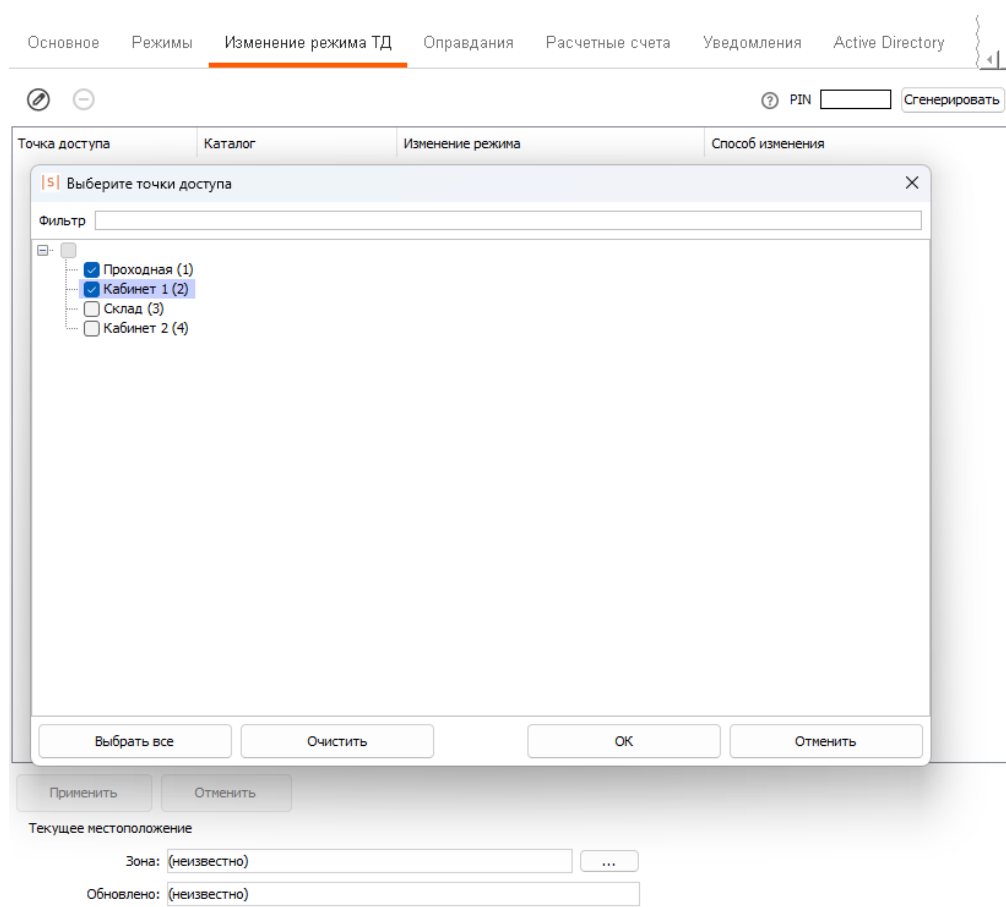


Пример настройки прав оператора.

5. В разделе «Изменение режима ТД» нажмите на кнопку редактирования в левом верхнем углу. В открывшемся окне выберите точки доступа, режим которых необходимо изменять. Нажмите «ОК».



В окне выбора точек доступа отображается список ТД, назначенных объекту доступа на вкладке «Персонал» в разделе «Основное».



Раздел «Изменение режима ТД».

6. Для выбранной ТД настройте параметр «Изменение режима». Возможные значения параметра:
- нормальный <-> разблокированный (значение по умолчанию);
 - нормальный <-> заблокированный;
 - разблокированный <-> заблокированный.

Основное Режимы **Изменение режима ТД** Оправдания Расчетные счета

Точка доступа	Каталог	Изменение режима	Способ изменения
Кабинет 1	Оборудование	нормальный <-> разблокированный	PIN
Проходная	Оборудование	нормальный <-> разблокированный	PIN
		нормальный <-> заблокированный	
		разблокированный <-> заблокированный	

Текущее местоположение

Зона:

Обновлено:

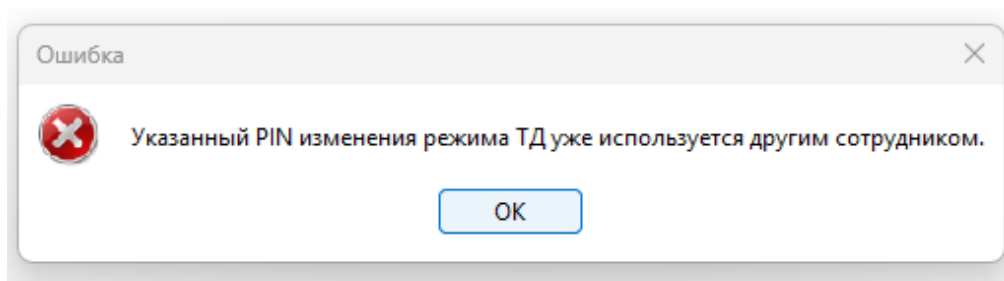
Настройка параметра «Изменение режима».

7. Для выбранной ТД настройте параметр «Способ изменения». Возможные значения параметра:

- PIN — используется специальный PIN-код для изменения режима (значение по умолчанию);
- PIN + пропуск — используется тот же специальный PIN-код, после ввода которого необходимо предъявить пропуск сотрудника.

Настройка параметра «Способ изменения».

8. Сгенерируйте или введите вручную специальный PIN-код. PIN должен быть уникальным для сотрудника в рамках функции «Изменение режима ТД». Если введенный PIN-код уже назначен другому сотруднику, система отобразит соответствующее предупреждение.



Предупреждение об ошибке.

9. Подтвердите операцию, нажав кнопку «Применить». При нажатии кнопки «Отменить» изменения не сохраняются.

В программном обеспечении допускается назначение одинаковых параметров «Изменение режима» (например, «нормальный <-> разблокированный») и «Способ изменения» (например, «PIN») для одной и той же точки доступа различным объектам доступа. При этом у каждого объекта доступа должен быть уникальный PIN-код.

Подробное описание работы системы при изменении режима точки доступа приведено в данном разделе.

11.2.1. **Настройка функции изменения режима точки доступа для нескольких объектов доступа**

На вкладке «Персонал» можно выбрать несколько объектов доступа или целый отдел для одновременной настройки функции изменения режима точки доступа.

Отображение раздела «Изменение режима ТД».

Раздел отображается, если выполняется хотя бы одно из условий:

- среди выбранных объектов доступа есть хотя бы один с типом «Сотрудник»;
- выбран хотя бы один отдел типа «Регулярный отдел». В этом случае изменения применяются ко всем сотрудникам отдела. Если в выбранном отделе отсутствуют сотрудники, настройка правил изменения режима будет недоступна.

В разделе отображается список правил изменения режима точек доступа, добавленных хотя бы одному из выбранных сотрудников.

Создание правил изменения режима точки доступа.

Создание правил изменения режима точки доступа осуществляется с помощью кнопки «+». При её нажатии открывается модальное окно «Выберите разрешённые точки доступа» в котором можно отметить ТД, для которых будет действовать правило. В окне отображаются только точки доступа, назначенные всем выбранным объектам доступа. Если общих ТД нет, кнопка «+» недоступна.

Если при массовом выборе сотрудников правило изменения режима уже есть в списке, его изменения применяются ко всем выбранным объектам доступа.

Основное Режимы **Изменение режима ТД** Оправдания Расчетные счета

+ −
? Сгенерировать PIN

Точка доступа	Каталог	Изменение режима	Способ изменения
Кабинет 1	Оборудование	(не менять) ▾	(не менять) ▾
Кабинет 2	Оборудование	нормальный <-> разблокирова... ▾	PIN ▾
Проходная	Оборудование	(не менять) ▾	(не менять) ▾
Склад	Оборудование	(не менять) ▾	(не менять) ▾

Добавление правил изменения режима ТД при выборе нескольких объектов доступа.

По нажатию на кнопку «Сгенерировать PIN» для каждого объекта доступа генерируется уникальный PIN-код. Данное действие перезаписывает текущие PIN-коды сотрудников.

По умолчанию в столбцах «Изменение режима» и «Способ изменения» установлено значение «(не менять)». Это означает, что при применении настроек соответствующие параметры останутся без изменений.

Основное Режимы **Изменение режима ТД** Оправдания Расчетные счета

+ −
? Сгенерировать PIN

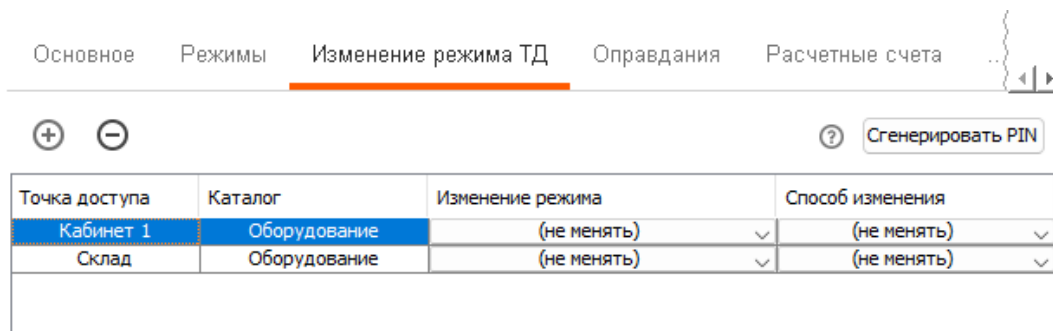
Точка доступа	Каталог	Изменение режима	Способ изменения
Кабинет 1	Оборудование	(не менять) ▾	(не менять) ▾
Склад	Оборудование	(не менять) ▾	(не менять) ▾

Вид раздела «Изменение режима ТД» при выборе нескольких объектов доступа.

Изменения значений в этих столбцах применяются только к объектам доступа, для которых правило изменения режима уже добавлено в разделе «Изменения режима ТД». Для остальных выбранных объектов такие изменения применяться не будут.

Удаление правил изменения режима точки доступа.

При выборе одного или нескольких правил становится доступна кнопка «–», предназначенная для удаления.



Удаление правил изменения режима ТД при выборе нескольких объектов доступа.

Правило изменения режима удаляется только у сотрудников, для которых оно было добавлено в разделе «Изменения режима ТД». Перед удалением отображается запрос подтверждения.

11.3. Конфигурация длины PIN-кода для расширенных функций

ПО Sigur также позволяет сконфигурировать длину PIN-кодов, для этого выполните следующие шаги:

1. В программе «Клиент» перейдите в меню «Файл» – «Настройки» – «PIN и QR-коды».
2. Установите необходимое количество символов PIN-кода. Допустимое количество символов: от 4 до 7, по умолчанию установлено 4. Вновь заданное количество символов распространяется на генерацию и на ручной ввод для новых PIN-кодов и никак не затрагивает существующие PIN-коды.
3. Нажмите «ОК».

Редактирование настроек

Наблюдение	PIN Количество символов в PIN для функций: Идентификация 4 Постановка на охрану 4 Изменение режима ТД 4 QR-коды 4 Wiegand формат W2 Система счисления DEC
IC:Предприятие	
Видеонаблюдение	
Печать пропусков	
Платежная система	
SMS	
Telegram	
E-Mail	
Персонал	
Бесконтактная идентификация	
Биометрика	6
Распознавание лиц	
Active Directory	
Оправдательные документы	
Пропуска посетителей	
Архив	
Синхронизация данных	
Распознавание документов	
Устройства хранения	
Зоны	
Повторные проходы	7
Дополнительные параметры	
HTTP(WEB)	
Заявки	
WEB-делегирование	
Права операторов	
BAS-IP	
True IP	
Профили шифрования OSDP	
Индикация	
Карантин	?
Профили шифрования	
OAuth2.0 Device Auth Grant	
Документы	
Контроллеры	
PIN и QR-коды	
Утилиты	

OK Отмена

Окно конфигурации длины PIN-кодов.

12. Сброс параметров считывателя к заводским настройкам

Для считывателей доступно 2 способа сброса параметров к заводским настройкам:

1. Аппаратный сброс.
2. Сброс параметров через приложение «Sigur Настройки».

Оба способа позволяют сбросить следующие параметры считывателя:

- режим работы и функции кодонаборной панели считывателя;
- разрядность Wiegand;
- параметры работы считывателя с картами;
- параметры работы считывателя со смартфонами;
- сервисный пароль считывателя.

Далее представлены способы сброса параметров считывателя к заводским настройкам.

12.1. Аппаратный сброс

Для аппаратного сброса настроек считывателя необходимо:

1. Отключить питание считывателя.
2. Соединить перемычкой клеммы D0 и ВЕЕР.
3. Подать питание на считыватель, после чего разъединить провода.

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

12.2. Сброс параметров считывателя через приложение «Sigur Настройки»

Для сброса параметров чтения карт и смартфонов, а также разрядности Wiegand следуйте пунктам раздела «Сброс конфигурации чтения считывателя».

Для сброса параметров индикации следуйте пунктам раздела «Сброс конфигурации индикации считывателя».

Для изменения пароля следуйте пунктам раздела «Смена пароля считывателей».

13. Работа с PIN-кодами в качестве идентификаторов

Считыватель поддерживает использование PIN-кодов как основного идентификатора доступа (PIN-код идентификации) или как дополнительного фактора аутентификации (PIN-код верификации).

При использовании только PIN-кода идентификации пользователь вводит свой код на сенсорной панели и подтверждает ввод кнопкой «Ввод». В режиме двухфакторной аутентификации пользователь сначала прикладывает карту, затем вводит PIN-код верификации для подтверждения личности и подтверждает ввод кнопкой «Ввод».

Считыватель должен быть предварительно сконфигурирован для работы с PIN-кодами. Подробная информация представлена в разделе «Настройка режимов работы считывателя».

Считыватель автоматически передаёт введённые данные контроллеру, который, в свою очередь, выполняет проверку прав доступа и принимает решение о предоставлении доступа. Подробнее о чтении PIN-кодов в соответствующем разделе.

14. Работа с картами Mifare

14.1. Работа в незащищённом режиме, чтение UID

Для карт Mifare поддерживается функция считывания их открытого уникального идентификатора – UID.

По умолчанию считыватель настроен на чтение UID карты и выдаёт его в прямом порядке байт в формате Wiegand-26. Вы можете изменить выходной формат Wiegand на другой. Для этого:

1. В программе «Клиент» перейдите в меню «Файл» – «Настройки». Выберите пункт «Бесконтактная идентификация».
2. Установите пункт «Формат идентификатора пропуска» равным одному из следующих вариантов: Wiegand-26 (3 байта), 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.
3. Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя».

14.2. Работа в защищённом режиме

Считывателем поддерживается защищённый режим работы для карт Mifare Classic 1K/4K, Mifare Plus SL3, Mifare DESFire EV1, 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.

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

1. В программе «Клиент» перейдите в меню «Файл» – «Настройки».
2. Выберите пункт «Бесконтактная идентификация», вкладку «Classic».
3. 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.

4. «Номер блока памяти» (в шестнадцатеричном формате). В большинстве случаев значение достаточно оставить равным по умолчанию.
5. «Ключ для доступа к памяти». Как правило, достаточно нажать кнопку «Сгенерировать ключ».
6. «В память карты записывать». Выберите либо «Автосгенерированное значение», либо «UID карты». В большинстве случаев достаточно оставить значение равным по умолчанию.
7. Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя».

14.2.2. Настройка работы с картами Mifare Plus

1. В программе «Клиент» перейдите в меню «Файл» — «Настройки».
2. Выберите пункт «Бесконтактная идентификация», вкладку «PLUS».
3. Выберите ваш тип карты: PLUS S или PLUS X.
4. 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.

5. «Номер блока памяти» (в шестнадцатеричном формате). В большинстве случаев значение достаточно оставить равным по умолчанию.
6. «Ключ для доступа к памяти». Как правило, достаточно нажать кнопку «Сгенерировать ключ». Остальные поля заполнятся автоматически.
7. «В память карты записывать». Выберите либо «Автосгенерированное значение», либо «UID карты». В большинстве случаев достаточно оставить значение равным по умолчанию.
8. Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя».

14.2.3. Правила заполнения служебных полей настроек карт Mifare

Заполняя служебные поля вручную, необходимо соблюдать следующие условия:

Для карт Mifare Classic 1K/4K:

- «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.

- «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».

- «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».

- «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:

- **«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.

- **«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.

- **«Мастер-ключ карты».**
- **«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).

- **«Ключ для переключения в SL2».**

Поле для ввода AES ключа, переключающего карту на более высокий уровень безопасности – Security Level 2. Используется системой в процессе персонализации карты. Значение задаётся в шестнадцатеричном формате и должно состоять из 16 байт (32 символов).

- **«Ключ для переключения в SL3».**

Поле для ввода AES ключа, переключающего карту на более высокий уровень безопасности – Security Level 3. Используется системой в процессе персонализации карты. Значение задаётся в шестнадцатеричном формате и должно состоять из 16 байт (32 символов).

- **«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».

15. Работа с банковскими картами

15.1. Чтение UID или эмуляция Mifare банковской картой

Все модификации считывателей Sigur позволяют использовать в качестве идентификаторов бесконтактные банковские карты MasterCard, Visa, МИР в режиме чтения UID (при наличии статического UID), либо аналогично картам Mifare, если банковская карта умеет эмулировать Mifare.



Эмулирует ли банковская карта Mifare, и какой именно формат — необходимо уточнить напрямую у банка, выпустившего карту.

Для настройки считывателей на работу в данном режиме:

1. В программе «Клиент» перейдите в меню «Файл» — «Настройки». Выберите пункт «Бесконтактная идентификация». Установите сверху пункт «Формат идентификатора пропуска» равным одному из следующих вариантов: Wiegand-26 (3 байта), 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.
2. Если 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».
3. Если банковская карта эмулирует какую-либо карту из семейства Mifare:
 - Для чтения UID эмулируемой карты в этом же меню выберите вкладку, на которой указан формат ваших карт (Classic или Plus). Установите пункт «В качестве идентификатора пропуска использовать» равным «UID».
 - Для работы в защищённом режиме выполните настройки, описанные в разделе «Работа в защищённом режиме». У банка, выпустившего карту, необходимо уточнить номер блока памяти, который можно использовать для нужд СКУД, а также ключ от данного блока памяти, если он есть.
4. Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя».

15.2. Чтение PAN-номера банковской карты

Модификации считывателей Sigur MK100 и Sigur MK100 Pro позволяют использовать в качестве идентификатора PAN-номер банковской карты, используя технологию EMV (**E**uropay + **M**asterCard + **V**ISA). Может использоваться как физическая карта, так и добавленная в электронный кошелек на смартфоне (МИР Pay, Google Pay, Apple Wallet, Samsung Pay).

По факту чтения карты считыватели Sigur передают в сторону контроллера хэш от считанного PAN-номера, что позволяет избежать компрометации данного номера карты.

Для настройки:

1. В программе «Клиент» перейдите в меню «Файл» — «Настройки». Выберите пункт «Бесконтактная идентификация». Установите сверху пункт «Формат идентификатора пропуска» равным одному из следующих вариантов: Wiegand-26 (3 байта), 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.
2. Перейдите на вкладку «EMV PAN» и установите галочку для опции «Использовать». Тип шифрования на текущий момент не настраивается.
3. Рекомендуем отключить использование UID карты в качестве идентификатора пропуска. Для этого перейдите на вкладку «Прочие» и снимите галочку напротив одноимённой опции.
4. Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя».

При чтении PAN-номера карты из банковского мобильного приложения (например, МИР Pay) рекомендуется отключить идентификацию по BLE и NFC в мобильном приложении «Sigur Доступ», если оно у вас установлено.

16. Работа с картами EM Marine и HID ProxCard II

Все считыватели линейки Sigur MK100 поддерживают использование карт EM Marine и HID ProxCard II (125 kHz) для идентификации.

Для считанных карт всегда возвращается считанный код в формате Wiegand-26. При необходимости можно установить передачу фиксированного facility кода карты или отключить чтение данного типа карт.

Для настройки:

1. В программе «Клиент» перейдите в меню «Файл» – «Настройки».
2. Выберите пункт «Бесконтактная идентификация», вкладку «EM Marine» или «HID».
3. Установите галку «Включить чтение карт EM Marine» и/или «Включить чтение карт HID ProxCard II» если необходимо читать карты соответствующего формата, либо снимите её, если какой-либо из форматов карт читать не нужно.
4. При необходимости можно включить опцию «Использовать фиксированный facility code» и установить необходимое значение (от 0 до 255).
5. Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «Программирование считывателя».

17. Работа со смартфонами в качестве идентификатора

17.1. Идентификация по смартфону, общие сведения

Считыватели Sigur модификации MK100 и MK100 Pro позволяют использовать смартфоны (с установленным приложением «Sigur Доступ») в качестве идентификатора. В случае смартфонов на базе iOS, Android или РЕД ОС М это может быть реализовано с помощью технологии BLE (Bluetooth Low Energy). Также для смартфонов с ОС Android или РЕД ОС М может использоваться альтернативный вариант – технология HCE (Host-based Card Emulation).

BLE-идентификация может происходить в режиме «hands-free» на расстоянии до 10 метров при прямой видимости считывателя. Дальность HCE-идентификации ограничена 9 см.

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».

Общие требования к смартфонам, а также некоторые комментарии приведены в разделе «Общие требования к смартфонам и ПО».

Модификации считывателей Sigur MK100 и MK100 Pro также позволяют использовать в качестве идентификатора PAN-номер банковской карты, добавленной в электронный кошелек (МИР Pay, Google Pay, Apple Wallet, Samsung Pay и т. п.). Данный способ не требует установки приложения «Sigur Доступ». Для получения более подробной информации по данному режиму работы обратитесь к разделу «Чтение PAN-номера банковской карты».

17.2. Общие требования к смартфонам и ПО

Для полноценной работы функций приложений «Sigur Доступ» и «Sigur Настройки» должны соблюдаться следующие требования:

- ОС Android: 5.0 и выше (для «Sigur Доступ»), 6.0 и выше (для «Sigur Настройки») / РЕД ОС М (для обоих приложений) / iOS 9.0 и выше (только для «Sigur Доступ»).
- Поддержка технологии BLE (Bluetooth Low Energy).



Производителем не гарантируется полная функциональность приложений на смартфонах с ОС Android. 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.



В силу стандартных ограничений мобильных платформ идентификация в фоновом режиме или на заблокированном экране может переставать работать спустя некоторое время.



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.



При установке приложений на смартфоны под управлением ОС Android рекомендуется отключить для приложений контроль фоновой активности. Наличие такого контроля и возможность его отключения зависит от конкретного производителя, например: зайти в «Настройки» ОС – выбрать раздел «Приложения» – «Все приложения» – выбрать приложение Sigur в списке – найти опцию «Контроль активности» и установить её в значение «Нет ограничений».

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

Доступ к геолокации, в свою очередь, приложениями Sigur не используется: это описано в политике конфиденциальности к приложениям производителя [здесь](#) и [здесь](#). Таким образом, приложения Sigur не используют и не собирают информацию о физических координатах устройств.

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

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

17.3. Настройка системы на работу со смартфонами

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

1. Указание параметров конфигурации работы считывателя в ПО «Клиент» (значение параметров конфигурации описываются в данном пункте).
2. Заполнение реквизитов подключения к серверам исходящей и входящей почты.
3. Программирование считывателя.
4. Добавление мобильных идентификаторов в ПО.

В программе «Клиент» перейдите в меню «Файл» – «Настройки» – «Бесконтактная идентификация». Выберите пункт «Мобильная идентификация» и включите «Использовать». Здесь нужно настроить следующие поля:

1. Сервисный пароль – используется для доступа к считывателю через мобильное приложение «Sigur Настройки». Настоятельно не рекомендуется оставлять данное поле в состоянии по умолчанию.

Сервисный пароль считывателя, установленный по умолчанию – **sigur** (с маленькой буквы).

2. Мобильная идентификация MR – режим работы считывателя. Доступно три варианта:

- **«Не использовать»** – в данном режиме ни один смартфон с запущенным приложением «Sigur Доступ» не будет считан.
- **«Базовый»** – в этом режиме считыватель будет реагировать на любой смартфон, на котором установлено и запущено приложение «Sigur 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 BLE — ориентировочная дальность, на которой будет осуществляться BLE-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. Успешная идентификация будет осуществляться при превышении данного уровня. Вы можете выяснить необходимый уровень сигнала для идентификации с помощью мобильного приложения «[Sigur 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 PIN-код/графический ключ/производя считывание отпечатка пальца и т. п.

Если дальнейших настроек считывателя не требуется, то следуйте пунктам раздела «[Программирование считывателя](#)».

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

Редактирование настроек

Наблюдение
1С:Предприятие
Видеонаблюдение
Печать пропусков
Платежная система
SMS
Telegram
E-Mail
Персонал
Бесконтактная идентификация
Биометрика
Распознавание лиц
Active Directory
Оправдательные документы
Пропуска посетителей
Архив
Синхронизация данных
Распознавание документов
Беспроводные замки
Устройства хранения
Зоны
Повторные проходы
Дополнительные параметры
HTTP(WEB)
Заявки
WEB-делегирование
Права операторов
BAS-IP
True IP
Профили шифрования OSDP
Индикация
Профили шифрования

Формат идентификатора пропуска: Wiegand 34 (4 байта)

Classic Desfire EV1 PLUS PLUS BY Прочие Мобильная идентификация Em-Marine HID® EMV Pan

Сервисный пароль MR: sigur

Мобильная идентификация MR
Использовать в пользовательском режиме

Ключ: 086725B5A84279764386A77092C9C9AD

Расстояние срабатывания BLE: близкое

Политика срабатывания: когда приложение на экране

BLE идентификация ESMART
☐ Использовать

☐ Использовать функцию "удержание карты перед считывателем"

COM-порт настольного считывателя Z-2: COM13

Окно настроек мобильной идентификации по смартфону.

17.4. Работа с приложением «Sigur Доступ»

Мобильное приложение «Sigur Доступ» может быть установлено на смартфоны под управлением ОС Android, РЕД ОС М или iOS.

В зависимости от ОС смартфона функциональность приложения немного различается. Ключевые отличия: на смартфонах под управлением ОС Android или РЕД ОС М доступна идентификация с использованием встроенного NFC-модуля (по технологии HCE) и, в случае использования в ОС «тёмной темы», немного отличается внешний вид приложения.

Функция идентификации по BLE доступна для смартфонов с ОС Android, РЕД ОС М или iOS.

Для идентификации по BLE через приложение «Sigur Доступ» включите на смартфоне функцию Bluetooth. В случае некоторых моделей смартфонов на базе Android дополнительно может потребоваться включение функции определения местоположения.

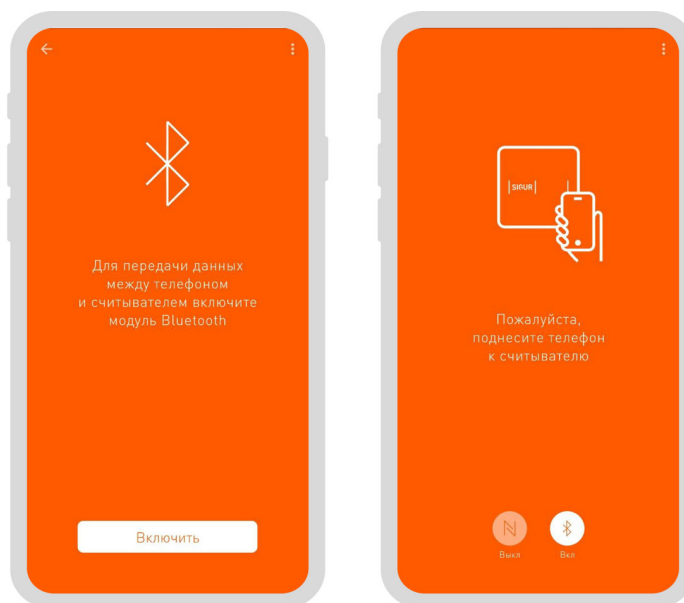
Идентификация по HCE через приложение «Sigur Доступ» доступна только для смартфонов с ОС Android или РЕД ОС М. Для этого включите на смартфоне функцию NFC.



Для успешной идентификации по HCE необходимо, чтобы в конфигурации чтения считывателя была отключена функция «Использовать UID карты в качестве идентификатора пропуска» для прочих карт.

Данная функция настраивается в ПО «Клиент» при редактировании конфигурации чтения в меню «Файл» – «Настройки» – «Бесконтактная идентификация», вкладка «Прочие».

После запуска мобильного приложения будут запрошены дополнительные разрешения, предоставьте их приложению. Приложение «Sigur Доступ» может работать в фоновом режиме (см. далее таблицу с описанием политик срабатывания считывателя).



Разрешения приложения «Sigur Доступ».

В зависимости от установленной политики идентификация требует следующих действий:

Описание выполнения необходимых условий при действии той или иной политики идентификации.

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 «Sigur Доступ» должно быть запущено на экране смартфона.

На разные считыватели могут быть загружены разные конфигурации настроек, поэтому дальность и политика идентификации могут отличаться.

18. Занесение идентификаторов в ПО Sigur

18.1. Занесение PIN-кодов



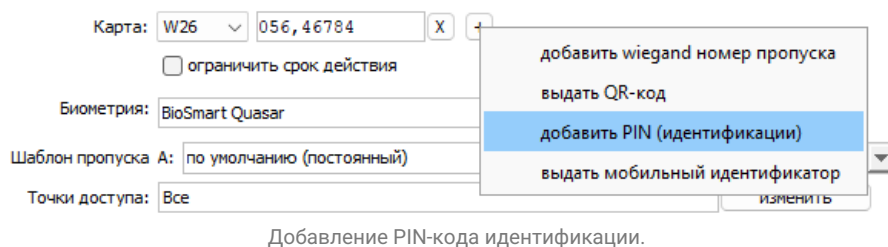
Ниже приведена информация по занесению PIN-кодов в ПО Sigur. Для добавления PIN-кодов в другие СКУД обратитесь к их документации.

В системе используются два типа PIN-кодов:

- **PIN идентификации** — используется как самостоятельный идентификатор доступа, аналог карты. Сотрудник может входить по PIN-коду без предъявления карты.
- **PIN верификации** — применяется вместе с картой как дополнительный фактор аутентификации (например, «карта + PIN»).

Добавление PIN идентификации в базу ПО Sigur.

1. Убедитесь, что версия установленного ПО «Клиент» 1.6.7.60 или выше, версия микропрограммы считывателя — 53 или выше, версия микропрограммы контроллера — 1.23.X или выше.
2. Убедитесь, что функция «Проход по PIN» настроена на основной режим считывателя. Подробная информация о настройке режимов работы считывателя приведена в [этом разделе](#).
3. В программе «Клиент» перейдите на вкладку «Персонал».
4. Выберите нужного сотрудника либо создайте нового кнопкой «Добавить сотрудника в выбранный отдел».
5. На вкладке «Общее» нажмите кнопку «+» (добавить ключ) напротив поля «Карта». Выберите вариант «Добавить PIN (идентификации)». PIN-код может быть сгенерирован автоматически или задан вручную. При вводе вручную система проверяет, чтобы PIN-код был уникален и не совпадал с уже существующими в базе.
6. Сохраните внесённые изменения кнопкой «Применить».



ПО Sigur также позволяет сконфигурировать длину PIN-кодов, для этого выполните следующие шаги:

1. В программе «Клиент» перейдите в меню «Файл» — «Настройки» — «PIN и QR-коды».
2. Установите необходимое количество символов PIN-кода. Допустимое количество символов: от 4 до 7, по умолчанию установлено 4. Вновь заданное количество символов распространяется на генерацию и на ручной ввод для новых PIN-кодов и никак не затрагивает существующие PIN-коды.
3. Нажмите «ОК».

При изменении длины PIN-кодов идентификации также необходимо настроить размер буфера накопления нажатий. Размер буфера определяет количество набранных цифр, по достижении которого автоматически начинается обработка введенной последовательности (в посимвольном режиме работы кодонаборных панелей). Допустимые значения размера буфера: 4, 5, 6 или 7 символов. Рекомендуется устанавливать размер буфера равным длине PIN-кода — в этом случае обработка начинается сразу после ввода последнего символа, без необходимости нажимать кнопку «Ввод» или ждать истечения тайм-аута. Настройка распространяется только на обработку PIN-идентификации и PIN-верификации.

Процесс настройки размера буфера накопления нажатий:

1. В программе «Клиент» на вкладке «Оборудование» выберите точку доступа, на которой используются считыватели с кодонаборной панелью. Нажмите кнопку «Настройки».
2. В открывшемся окне редактирования настроек перейдите на вкладку «Общее» и отключите чекбокс «Отображать только базовые настройки».
3. Настройте параметр «Размер буфера накопления нажатий». Установите значение, равное или больше заданной длины PIN-идентификации.
4. Нажмите «ОК».

Подробная информация о работе с PIN идентификации представлена в разделе «Тип пропуска» [Руководства пользователя ПО Sigur](#).

Добавление PIN верификации в базу ПО Sigur.

1. Убедитесь, что версия установленного ПО «Клиент» 1.6.7.60 или выше, версия микропрограммы считывателя — 53 или выше, версия микропрограммы контроллера — 1.23.X или выше.
2. Убедитесь, что функция «Проход по PIN» настроена на основной режим считывателя. Подробная информация о настройке режимов работы считывателя приведена в [этом разделе](#).
3. Откройте ПО в «Клиент» вкладку «Режимы».
4. Выберите нужный режим и на вкладке «Специальные правила» включите опцию «Дополнительно запрашивать PIN (верификации)».
5. Нажмите «Применить». PIN-код верификации автоматически создаётся для каждого сотрудника и отображается в его параметрах на вкладке «Персонал». При необходимости PIN-код верификации можно задать вручную (фиксированная длина кода – 4 символа).

Подробная информация о работе с PIN верификации представлена в разделе «Доступ с PIN-кодом» [Руководства пользователя ПО Sigur](#).

18.2. Занесение карт



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

Занесение карт Mifare и бесконтактных банковских карт в базу ПО Sigur производится с помощью контрольных USB-считывателей Sigur MR100 USB, ACR1252U и ESMART DUAL USB. Для работы с идентификаторами Mifare также может использоваться считыватель IronLogic Z-2 USB, но только в режиме чтения UID.

Добавление карт EM Marine и HID ProxCard II может выполняться вручную либо с использованием контрольных USB-считывателей Sigur MR100 USB, Sigur Reader-EH и IronLogic Z-2 USB.

Для считывателей Sigur MR100 USB, Sigur Reader EH и ACR1252U не требуется предварительная настройка. Для использования ESMART DUAL USB требуется драйвер производителя и соответствующий модуль лицензии. Настройка ПО для работы со считывателем Z-2 USB описана в [«Руководстве пользователя ПО Sigur»](#).

Для добавления карты в базу ПО Sigur через подключённый USB-считыватель:

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

При чтении PAN-номера карты из банковского мобильного приложения (например, МИР Pay) рекомендуется отключить идентификацию по BLE и NFC в мобильном приложении «Sigur Доступ», если оно у вас установлено.

18.3. Занесение мобильных идентификаторов

18.3.1. 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.

В «Базовом» режиме работы считывателей добавить мобильные идентификаторы можно следующими способами:

- Использовать функцию «Захватывать коды с точки доступа» (см. «Руководство пользователя ПО Sigur»).
- С помощью настольного считывателя Sigur MR100 USB.
- Вручную, скопировав ID в мобильном приложении «Sigur Доступ» (нажать кнопку в правом верхнем углу, далее «О программе») и указав его в поле «Пропуск» в программе «Клиент», предварительно укоротив до нужной битности Wiegand.

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

При переходе по данной ссылке приложение «Sigur Доступ» автоматически формирует письмо, которое должно быть отправлено в ответ.

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

18.3.2. Отправка пригласительного письма

Для добавления смартфона в систему СКУД Sigur сначала необходимо задать настройки SMTP-сервера для отправки пригласительных 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 кнопку «+» (добавить ключ) напротив поля «Ключ». Выберите вариант «Выдать мобильный идентификатор».

Выдача мобильного идентификатора.

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.

Окно ввода Email для отправки пригласительного письма.

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

18.3.3. Групповая выдача мобильных идентификаторов

Во всех пакетах лицензий, специальном модуле ПО «Школа» или при наличии дополнительного модуля ПО «Реакция на события» доступна отправка пригласительных сразу группе сотрудников. Для этого необходимо перейти в раздел «Файл» – «Настройки» – «Персонал» и в области «Выдать мобильные идентификаторы Sigur» выбрать нужных сотрудников.

Выдать мобильные идентификаторы Sigur:

Выбрать

Выдать



Окно для отправки группы пригласительных писем.

Затем требуется нажать кнопку «Выдать», после чего выбранным сотрудникам будут отправлены пригласительные письма. В качестве email, на которые отправляются письма, система использует значения параметра из учётных карточек сотрудников (на вкладке «Персонал» – «Уведомления» выбран «Тип уведомлений» – Email).



Область «Выдать мобильные идентификаторы Sigur» отображается только в случае, если есть хотя бы один сотрудник, у которого указан Email на вкладке «Персонал» – «Уведомления».

18.3.4. 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](#).

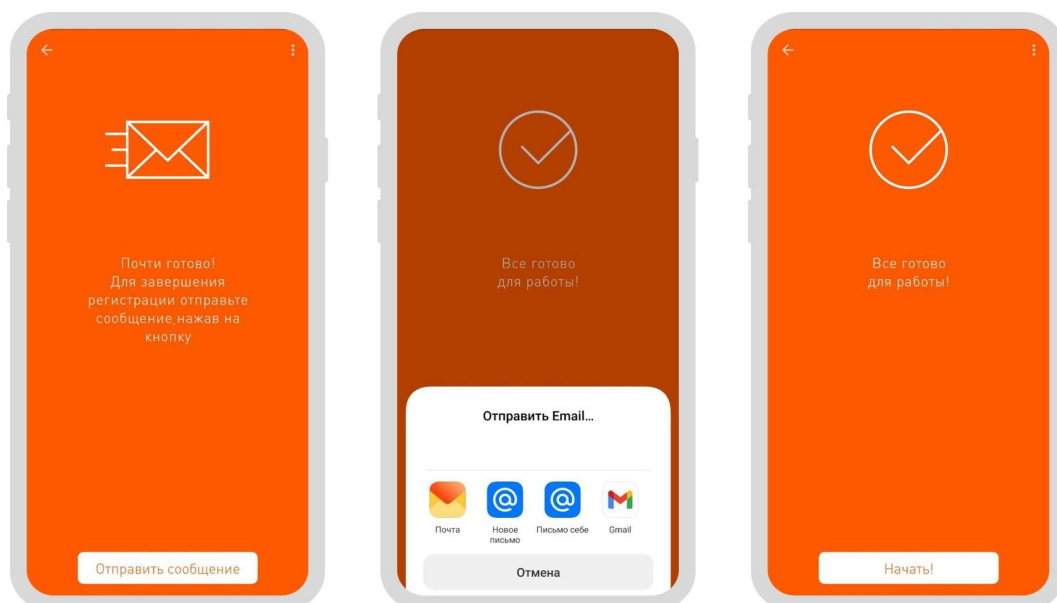
Инструкция в приложении поможет настроить устройство. В случае проблем обратитесь к администратору объекта.

Пример приглашительного письма.

1. Установите мобильное приложение «Sigur Доступ» на смартфон по ссылкам из письма или из [Google Play](#), [App Store](#), [AppGallery](#), [RuStore](#).
2. Перейдите по специальной ссылке из письма, отправленного сервером СКУД Sigur. Вы также можете скопировать ссылку в любой стандартный веб-браузер.
3. После перехода по ссылке откроется приложение «Sigur Доступ», которое сформирует ответное письмо. В нём содержится идентификатор, связанный с устройством.
4. 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 приглашительное письмо.

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



Отправка ответного письма.

19. Настройка реакции на событие «Считыватель оторван от стены»

При открытии и закрытии корпуса считывателя на управляющий контроллер отправляются специальные послышки в формате Wiegand-58. По приходу на сервер данных 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. 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 «Руководстве пользователя ПО Sigur».

20. Приложение «Sigur Настройки»

20.1. Назначение приложения «Sigur Настройки»

Мобильное приложение «Sigur Настройки» доступно для установки на смартфоны под управлением ОС Android или РЕД ОС М. Приложение предназначено для:

- поиска считывателей в радиусе действия BLE смартфона;
- смены пароля считывателей;
- обновления внутреннего ПО считывателей;
- добавления лицензий на считыватели;
- работы с файлом конфигурации чтения;
- загрузки профиля индикации на считыватель;
- сброса конфигурации чтения считывателя к заводским настройкам;
- сброса конфигурации индикации считывателя к заводским параметрам;
- настройки выходного интерфейса считывателя.

Общие требования к устройствам, а также некоторые комментарии приведены в разделе «Общие требования к смартфонам и ПО».

Скачать приложение «Sigur Настройки» можно из [Google Play](#), [RuStore](#) или [AppGallery](#).

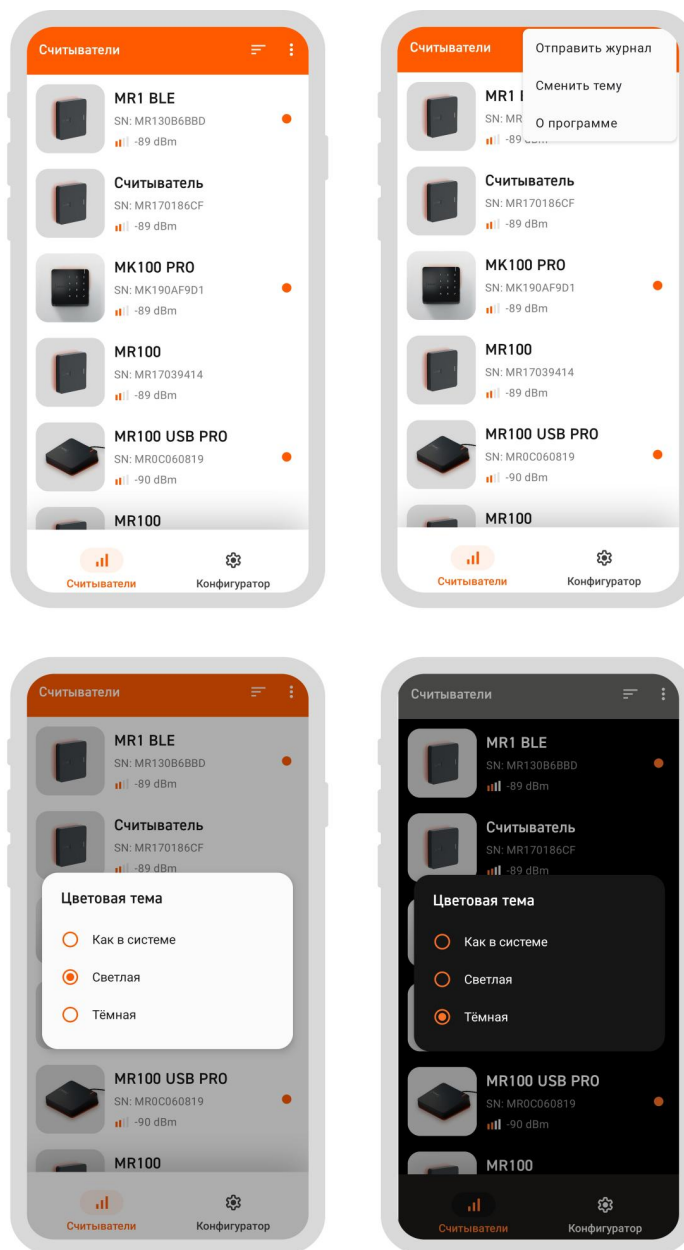
При первом запуске приложения предоставьте ему все запрашиваемые разрешения.

20.2. Настройка темы интерфейса

Для изменения темы приложения «Sigur Настройки» необходимо нажать на три точки в правом верхнем углу экрана и выбрать действие «Сменить тему». Для выбора будут доступны следующие опции:

- как в системе – интерфейс приложения будет соответствовать теме системы устройства;
- светлая;
- тёмная.

Изменение темы произойдёт сразу, перезагрузка приложения не требуется.



Смена темы приложения «Sigur Настройки».

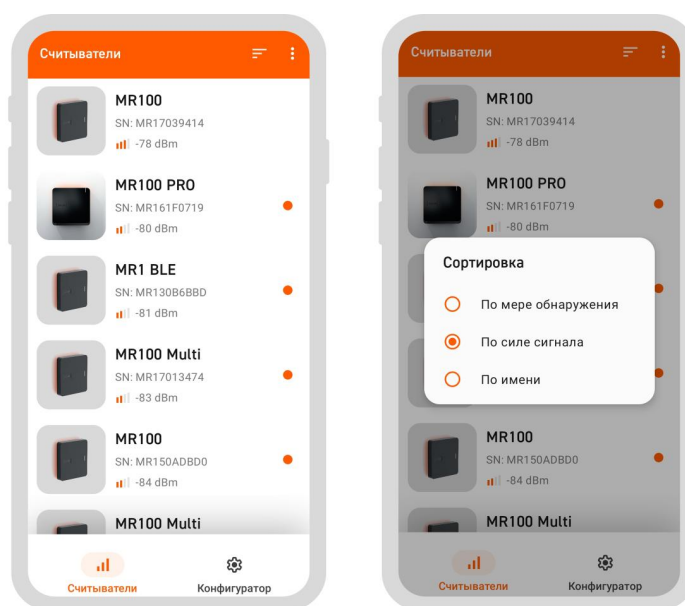
20.3. Поиск считывателей в радиусе действия BLE смартфона

Для работы приложения необходимо включить функцию Bluetooth на смартфоне. При первом запуске приложения необходимо предоставить все запрашиваемые разрешения.

В разделе «Считыватели» будет отображаться список обнаруженных считывателей. Для каждого считывателя доступна следующая информация:

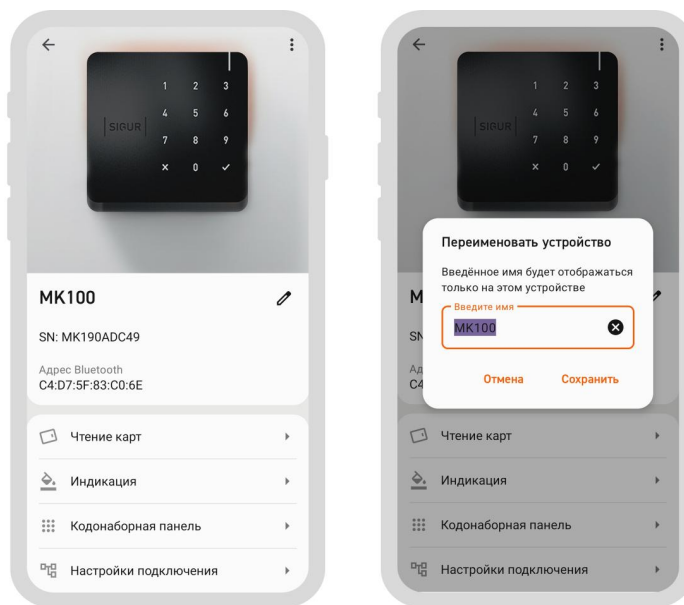
- название или модель считывателя;
- серийный номер;
- уровень принимаемого сигнала.

По умолчанию считыватели в списке сортируются по мере обнаружения. При необходимости можно настроить сортировку, нажав на соответствующую кнопку в правом верхнем углу главного окна приложения и выбрав признак сортировки (по мере обнаружения, по силе сигнала или по имени устройств).



Раздел «Считыватели» приложения «Sigur Настройки» и сортировка списка устройств.

Считыватели можно переименовать для удобства их поиска и конфигурирования. Для этого нажмите на считыватель в списке, а затем нажмите на иконку с изображением карандаша рядом с названием считывателя. Введите новое имя считывателя и нажмите «Сохранить». Введённые наименования устройств сохраняются только на текущем смартфоне.



Редактирование названия считывателя.

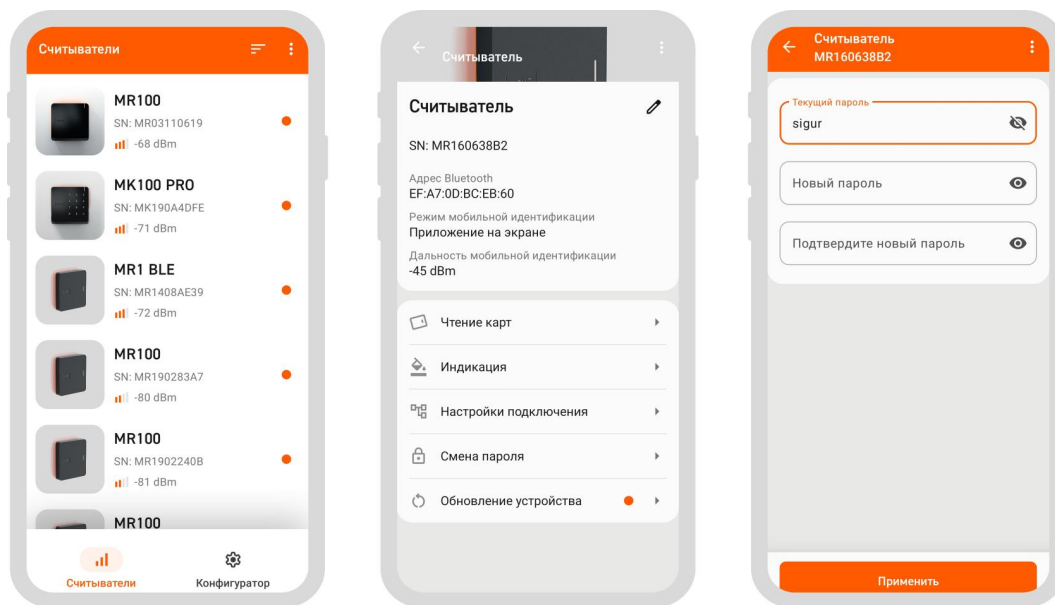
20.4. Смена пароля считывателей

Некоторые действия в приложении требуют ввода сервисного пароля. Рекомендуется изменить пароль, установленный по умолчанию, при первом подключении к считывателю для обеспечения безопасности.

Чтобы сменить пароль через мобильное приложение, выполните следующее:

1. Включите функции Bluetooth и «Определение местоположения» на вашем смартфоне и запустите приложение «Sigur Настройки».
2. Подойдите к считывателю(-ям). На вкладке «Настройки считывателя» отобразится список доступных устройств.
3. Выберите нужный считыватель из списка и нажмите «Смена пароля».
4. Введите текущий пароль считывателя (по умолчанию – **sigur**), затем дважды укажите новый и нажмите «Применить».
5. Дождитесь завершения отправки и применения нового пароля. Индикация считывателя будет изменяться в соответствии с таблицей.

Минимальная длина нового пароля — 6 символов.



Окно изменения сервисного пароля считывателя.

Приложение поддерживает работу с несколькими считывателями:

1. Выберите один из считывателей в списке долгим нажатием, затем добавьте ещё несколько устройств короткими нажатиями. В верхней части окна отобразится количество выбранных считывателей.
2. Нажмите кнопку «Далее», затем – «Смена пароля». Алгоритм действий для каждого устройства будет таким же, как при индивидуальной настройке.
3. При необходимости можно пропустить изменение пароля на отдельных считывателях, нажав «Пропустить». Переход к следующему устройству выполняется кнопкой «Далее».
4. После ввода паролей и нажатия «Применить» приложение последовательно обновит их на всех выбранных считывателях. Прогресс обновления отображается в интерфейсе приложения.

20.5. Обновление внутреннего ПО считывателя

Новые микропрограммы могут исправлять некоторые ошибки предыдущих версий и расширять функции считывателя. Обновление внутреннего ПО считывателя производится с помощью мобильного приложения «[Sigur Настройки](#)».

Также обновить внутреннее ПО считывателя можно централизованно с рабочего места, но этот способ актуален только для считывателей, подключённых к контроллеру Sigur по интерфейсу OSDP. Данная процедура описана в соответствующем [разделе](#).

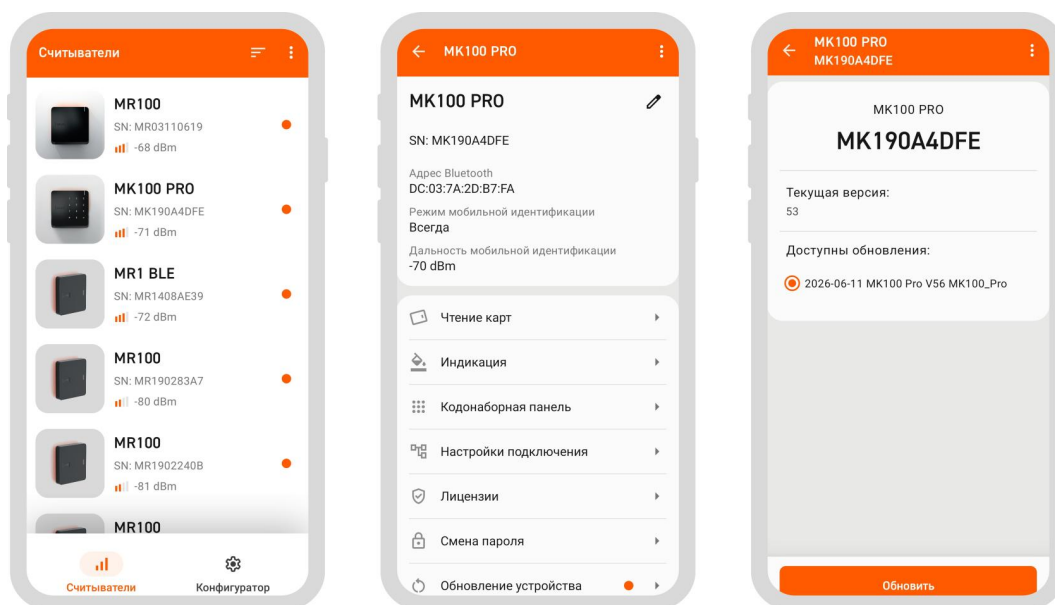
Для проведения операции обновления внутреннего ПО считывателя:

1. Включите функции: Bluetooth, «Определение местоположения» и Wi-Fi (или мобильный интернет) на вашем смартфоне и запустите приложение «Sigur Настройки». Приложение само будет загружать новые версии микропрограмм считывателя через интернет при первой возможности.
2. Подойдите к считывателю(-ям) и откройте приложение «Sigur Настройки». В разделе «Считыватели» отобразится список доступных считывателей.
3. Выберите из данного списка один из считывателей для обновления микропрограммы, после чего нажмите «Обновление устройства». При наличии доступных обновлений рядом с опцией «Обновление устройства» отображается оранжевый индикатор.
4. Программа отобразит текущую версию внутреннего ПО считывателя, а также наличие обновления. Выберите одну из доступных микропрограмм и нажмите кнопку «Обновить».
5. 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).
6. Дождитесь окончания отправки файла микропрограммы и обновления считывателя. Во время загрузки микропрограммы считыватель изменит свою индикацию: светодиод будет гореть жёлтым. После успешной загрузки считыватель перейдёт к применению микропрограммы, изменив свою индикацию: светодиод будет моргать жёлтым и белым цветами.
7. 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:

1. Для начала выберите один из считывателей долгим нажатием, после чего можно будет выбрать ещё несколько считывателей короткими нажатиями. В верхней части окна отображается количество выбранных устройств.
2. После завершения выбора нажмите кнопку «Действия с устройствами». 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 «Пропустить». 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.



Обновление внутреннего ПО считывателя.

При каждом обновлении версии микропрограммы считывателя через приложение «Sigur Настройки» также происходит попытка обновить лицензию.

20.6. Добавление лицензии на считыватель

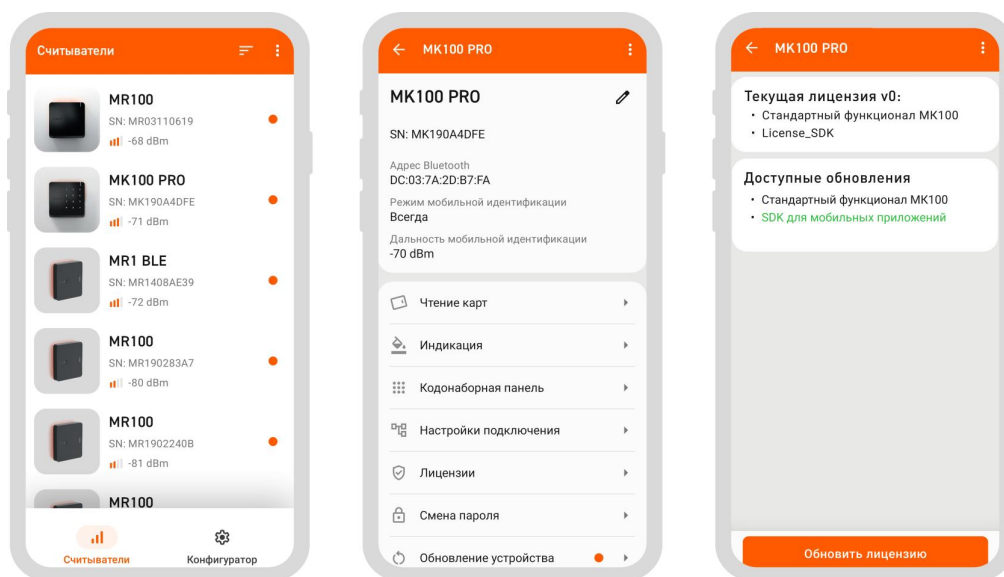
На считывателях Sigur MK100 Pro можно активировать специальное внутреннее ПО, расширяющее стандартную функциональность. Использование специальных функций лицензируется отдельно. Подробности можно уточнить в отделе продаж Sigur.

С помощью приложения «Sigur Настройки» вы можете самостоятельно добавить на считыватель приобретённую лицензию — специальные функции станут доступны автоматически. Для этого убедитесь, что у вас установлена версия «Sigur Настройки» 1.0.29 или выше.

Если вы добавляете лицензию впервые или хотите загрузить обновлённую версию, выполните следующие шаги:

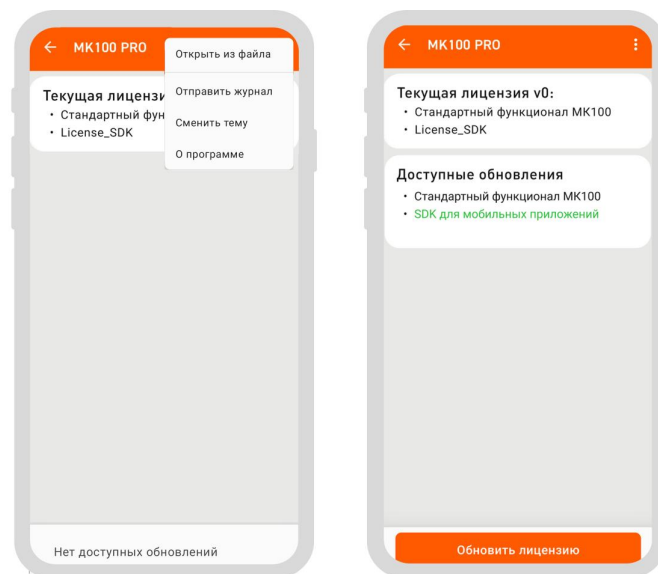
- Включите функции: Bluetooth, «Определение местоположения» и Wi-Fi (или мобильный интернет) на вашем смартфоне.
- Откройте приложение «Sigur Настройки» и выберите считыватель из списка.

3. Перейдите в блок «Лицензии».
4. При необходимости введите сервисный пароль считывателя (пароль по умолчанию – **sigur**).
5. Приложение отобразит текущую версию лицензии считывателя и доступное обновление.



Обновление лицензии считывателя.

6. Приложение «Sigur Настройки» автоматически загружает все доступные лицензии при наличии подключения к интернету. Если доступ к сети отсутствует, архив лицензий можно добавить в приложение вручную. Для получения архива обратитесь в [техническую поддержку Sigur](#). Далее нажмите на три точки в правом верхнем углу экрана, выберите пункт «Открыть из файла» и загрузите архив из файловой системы устройства.



Обновление лицензии считывателя при отсутствии доступа к сети.

7. Нажмите кнопку «Обновить лицензию».
8. Дождитесь окончания обновления лицензии. Приложение оповестит вас о результате операции, а считыватель издаст характерный звук.
9. После обновления в приложении появится информация о текущем составе лицензии на устройстве. Считыватель готов к работе.

При наличии большого количества устройств можно воспользоваться функцией массового обновления лицензий. Для этого:

1. В общем списке выделите один из считывателей долгим нажатием, а затем выделите остальные короткими нажатиями. В верхней части окна отобразится количество выбранных устройств.
2. По завершении выбора нажмите кнопку «Действия с устройствами» и в списке действий «Лицензии».
3. Нажмите «Обновить» для каждого из выбранных считывателей. При необходимости укажите сервисные пароли устройств (пароль по умолчанию – **sigur**). Вы также можете пропустить обновление лицензий отдельных считывателей, нажав «Пропустить».

Попытка обновить лицензию также происходит при каждом обновлении версии микропрограммы считывателя через приложение «Sigur Настройки».

20.7. Работа с файлом конфигурации чтения

В приложении «Sigur Настройки» доступны два раздела: «Считыватели» и «Конфигуратор». Создать и отредактировать файл конфигурации чтения идентификаторов можно в любом из разделов.

Создание и редактирование файла конфигурации чтения.

Чтобы создать новый файл, выполните следующие шаги:

1. Откройте приложение, включите функцию Bluetooth и перейдите в раздел «Конфигуратор».



Для создания и редактирования настроек чтения на вкладке «Считыватели» предварительно выберите необходимый считыватель – действие «Чтение карт». Далее станет доступно окно создания конфигурации, как при открытии раздела «Конфигуратор».

2. В списке действий выберите «Создать конфигурацию». При выборе опции откроется окно с доступными функциями считывателя.
3. Заполните обязательные поля на вкладке «Общее»: введите название файла конфигурации и формат идентификатора пропуска (доступны Wiegand-26, 34, 58). Дополнительно можно включить опцию «Удержание карты перед считывателем».
4. Задайте необходимые настройки чтения идентификаторов. Чтобы включить, переведите переключатель в активное положение.

Для выбора доступны следующие настройки чтения:

- **Mifare Classic.** Выберите тип идентификатора: UID или данные из памяти (защищённый режим). При необходимости включите использование обратного порядка байт. При выборе опции «Данные из памяти» становятся доступны для заполнения поля:
 - Номер блока памяти. Ограничение – число от 1 до 255.
 - Ключ доступа к памяти. Ограничение – 12 символов. Доступна кнопка автоматической генерации значения.
- **Mifare Plus.** Выберите тип идентификатора: UID или данные из памяти (защищённый режим). При необходимости включите использование обратного порядка байт. При выборе опции «Данные из памяти» становятся доступны для заполнения поля:

- Номер блока памяти. Ограничение – число от 1 до 255.
- Ключ доступа к памяти. Ограничение – 32 символа. Доступна кнопка автоматической генерации значения.
- **Mifare DESFire.** Выберите тип идентификатора: UID или данные из памяти (защищённый режим). При необходимости включите использование обратного порядка байт.
При выборе опции «Данные из памяти» становятся доступны для заполнения поля:
Идентификатор приложения (карты). Ограничение – 6 символов.
 - Алгоритм шифрования данных: DES или AES. По умолчанию – DES.
 - Идентификатор файла. Ограничение – от 0 до 31.
 - Позиция в файле. Ограничение – 6 символов. Идентификатор пропуска хранится, начиная с данного значения.
 - Номер ключа для доступа к файлу. Ограничение – целое число от 0 до 14.
 - Ключ доступа к файлу. Ограничение – 32 символа.
- **Мобильная идентификация.** При включении доступны следующие опции:
 - Как использовать. Выберите один из вариантов: «Использовать в базовом режиме» или «Использовать в пользовательском режиме».
 - Идентификатор сервера. Обязательное поле. Для получения идентификатора запустите клиентское рабочее место, подключённое к серверу объекта, на котором планируется производить проходы, и перейдите в ПО «Клиент», меню «Файл» – «Настройки» – «Бесконтактная идентификация» – «Мобильная идентификация».
 - Расстояние срабатывания BLE: близкое, среднее, далёкое, указать RSSI. При выборе последней опции введите соответствующее число в появившемся ниже поле.
 - Политика срабатывания: когда приложение на экране, когда экран заблокирован, всегда.
- **EM-Marine.** При активации чекбокса «Использовать фиксированный facility code» необходимо ввести соответствующее значение. Ограничение – число от 0 до 255.
- **HID ProxCard II.** При активации чекбокса «Использовать фиксированный facility code» необходимо ввести соответствующее значение. Ограничение – число от 0 до 255.
- **EMV Pan.** Необходимо указать тип шифрования: по умолчанию – хэш-функция MD5.

- **Прочие.** Использование карт Mifare Ultralight, Felica и прочих идентификаторов стандарта ISO14443-A в режиме чтения UID.

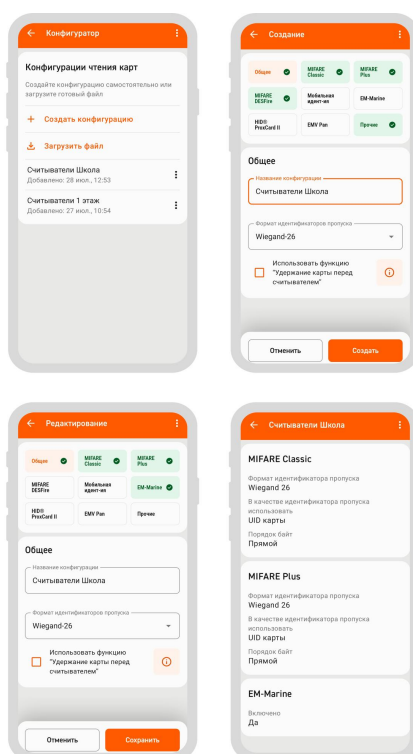


Переведите переключатель «Прочие» в неактивное состояние, если вы работаете с картами в защищённом режиме, с банковскими картами по EMV или со смартфонами по HCE.



По умолчанию в файле конфигурации выбраны следующие настройки: «Mifare (Classic, Plus, DESFire)» – чтение UID, и «Прочие».

5. После выбора настроек и заполнения обязательных полей станет активна кнопка «Создать» – при нажатии на неё файл с настройками будет автоматически сохранён и появится в списке доступных конфигураций в приложении.

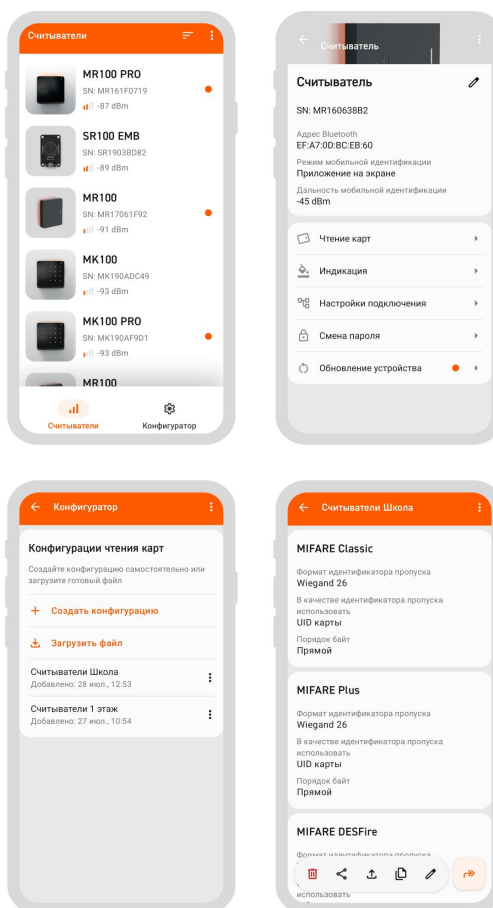


Создание, редактирование и просмотр файла конфигурации чтения.

Загрузка файла конфигурации чтения на считыватель.

По завершении создания и редактирования настроек файл готов к загрузке на считыватели. Для этого:

1. Выберите из списка устройств считыватель (несколько считывателей), для которого планируется изменить настройки, действие «Чтение карт».
2. Выберите из списка доступных конфигураций нужный файл и в панели действий нажмите кнопку «Загрузка файла конфигурации чтения на считыватель» (оранжевая стрелка). При необходимости введите сервисный пароль считывателя.
3. Новый профиль конфигурации будет загружен на выбранные считыватели автоматически. Конфигурация применится по окончании загрузки, перезагрузка устройств не требуется. После применения новых параметров считыватель издаст характерный звук, и приложение уведомит вас об успешности выполнения операции.



Загрузка профиля конфигурации чтения на считыватель.

Возможные действия с файлом конфигурации.

Для работы с готовым файлом необходимо нажать на три точки справа от его названия. Будут доступны следующие действия:

- Просмотреть. Показать конфигурацию чтения выбранного файла.
- Редактировать. Изменить настройки чтения карт в файле.
- Копировать. Скопировать файл с настройками чтения считывателей.
- Поделиться. Поделиться файлом одним из способов, доступных на устройстве.
- Скачать. Скачать и сохранить файл в памяти устройства.
- Удалить. Удаление файла конфигурации из памяти приложения.



При удалении файла конфигурации доступна отмена данного действия – для этого нажмите кнопку «Отмена» в появившемся окне предупреждения.

20.8. Сброс конфигурации чтения считывателя

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

Для возврата конфигурации чтения считывателя к заводским настройкам:

1. Включите функции Bluetooth и «Определение местоположения» на вашем смартфоне и запустите приложение «Sigur Настройки».
2. Выберите считыватель (несколько считывателей), конфигурацию чтения которого необходимо сбросить к заводским параметрам.
3. Из открывшегося списка действий выберите пункт «Чтение карт». Если данный пункт отсутствует в списке действий, то обновите внутреннее ПО считывателя до последней доступной версии.
4. В окне «Текущая конфигурация» введите сервисный пароль считывателя (по умолчанию – **sigur**), после чего станут доступны просмотр и сброс текущей конфигурации.
5. Выберите опцию «Сбросить конфигурацию».
6. Подтвердите операцию нажатием кнопки «Сбросить», после чего произойдёт сброс текущих настроек чтения считывателя и возврат к заводским.

7. По окончании процесса сброса считыватель издаст характерный звук, а приложение уведомит об успешности операции. Заводская конфигурация применится по окончании сброса, перезагрузка считывателя не требуется.

20.9. Загрузка профиля индикации на считыватель



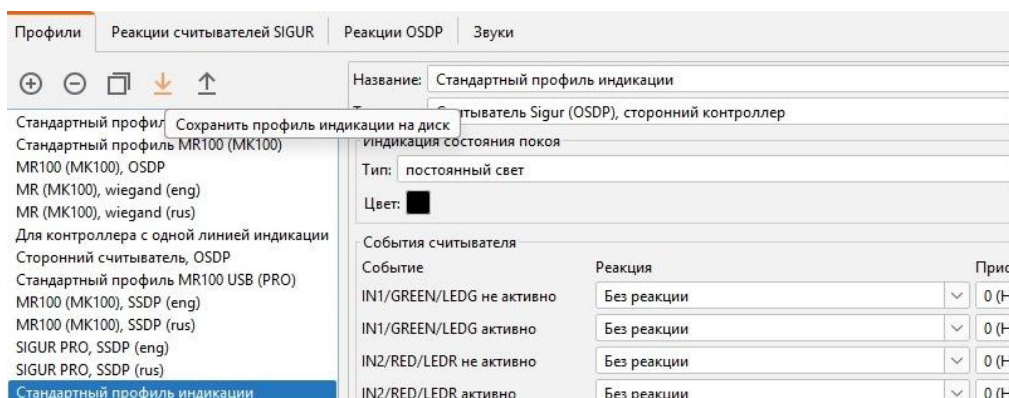
Загрузка профиля индикации через мобильное приложение возможна для любой модификации считывателя Sigur MK100 и не зависит от интерфейса, по которому считыватель подключён к контроллеру.

Перед загрузкой профиля индикации необходимо создать новый профиль или выбрать один из стандартных. Стандартные профили, а также порядок создания нового профиля рассмотрены в разделе [«Индикация считывателя»](#).

Для загрузки профиля индикации на считыватель на смартфоне должно быть установлено приложение [«Sigur Настройки»](#). Вы можете установить его по ссылке из письма с прикреплённым профилем индикации (в том случае, если файл с настройками был отправлен на email из ПО Sigur), либо самостоятельно найти его в магазинах мобильных приложений.

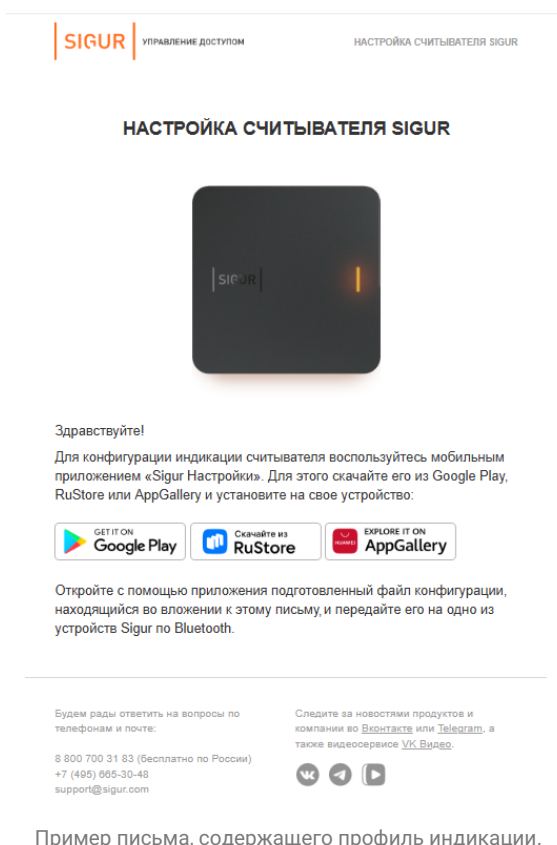
Передать файл профиля индикации на смартфон можно двумя способами:

- Сохранить файл на компьютер, а затем передать на смартфон (отправить через мессенджер, использовать внешний накопитель и пр.). Чтобы сохранить файл на диск, необходимо в меню «Файл» – «Настройки» – «Индикация» – «Профили» выбрать нужный профиль и нажать на соответствующую кнопку. После этого система предложит ввести произвольное название файла профиля индикации и выбрать каталог для сохранения.



Сохранение файла профиля индикации на диск.

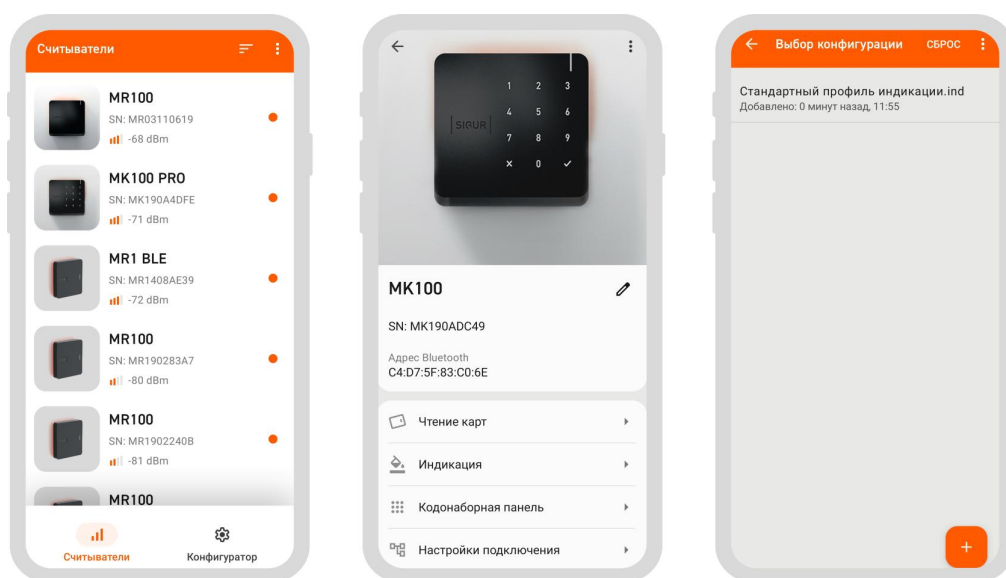
- Отправить файл на email средствами ПО Sigur. Для отправки письма с файлом профиля индикации ПО Sigur потребуется доступ к серверу исходящей почты. Подробная инструкция по настройке реквизитов сервера исходящей почты представлена в разделе «Настройка параметров сервера исходящей почты». Для отправки файла в меню «Файл» – «Настройки» – «Индикация» нажмите кнопку «Отправить email» и введите адрес электронной почты. На указанный email придёт письмо с прикрепленным файлом конфигурации.



Для загрузки профиля индикации на считыватель:

- Откройте полученный файл профиля индикации с помощью мобильного приложения «Sigur Настройки». После этого автоматически запустится приложение «Sigur Настройки» с уведомлением об успешном добавлении профиля индикации. Данный профиль сохранится в приложении. Файл можно загрузить в приложение вручную. Для этого необходимо включить функции Bluetooth и «Определение местоположения», запустить приложение «Sigur Настройки», в главном окне выбрать произвольный считыватель, в меню действий нажать «Индикация», после этого откроется хранилище конфигураций. В правом нижнем углу необходимо нажать на кнопку «+» и добавить профиль индикации, выбрав файл из памяти смартфона.

2. Включите функции Bluetooth и «Определение местоположения» на вашем смартфоне.
3. Запустите приложение «Sigur Настройки». Выберите нужный считыватель в списке долгим нажатием, затем короткими нажатиями добавьте остальные считыватели, на которые необходимо загрузить профиль индикации.
4. Из открывшегося списка действий выберите пункт «Индикация».
5. В списке профилей индикации выберите желаемый и при необходимости введите сервисный пароль считывателя.
6. Дождитесь окончания загрузки конфигурации на считыватель. Конфигурация индикации применится по окончании загрузки, перезагрузка считывателя не требуется.



Добавление нового профиля индикации.

7. Для удаления профиля индикации в списке необходимо смахнуть файл в сторону: влево или вправо. После этого файл будет удалён из списка.

20.10. Сброс конфигурации индикации считывателя



Данная функция доступна для любой модификации считывателя.

Для сброса конфигурации индикации считывателя на смартфоне должно быть установлено приложение «Sigur Настройки».

Для возврата индикации считывателя к заводским настройкам:

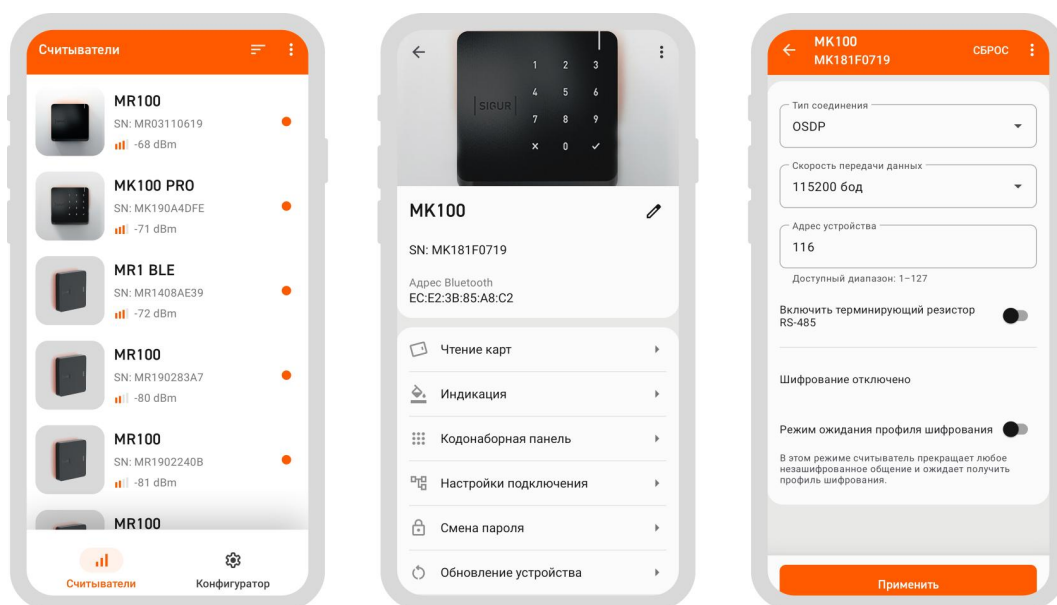
1. Включите функции Bluetooth и «Определение местоположения» на вашем смартфоне и запустите приложение «Sigur Настройки».
2. В разделе «Считыватели» выберите считыватель (один или несколько), индикацию которого необходимо сбросить.
3. Из открывшегося списка действий выберите пункт «Индикация» и нажмите кнопку «Сброс» в верхней части экрана.
4. Подтвердите действие нажатием кнопки «Продолжить» и введите сервисный пароль считывателя (пароль по умолчанию – **sigur**).
5. Дождитесь окончания сброса конфигурации индикации. После этого будет применена заводская конфигурация, перезагрузка считывателя не требуется.

20.11. Настройка выходного интерфейса считывателя

Для установки выходного интерфейса считывателя:

1. Откройте приложение «Sigur Настройки» и выберите считыватель из списка.
2. Из открывшегося списка действий выберите пункт «Настройки подключения».
3. Введите сервисный пароль считывателя (по умолчанию – **sigur**).
4. Выберите нужный режим работы: Wiegand или OSDP. Если считыватель подключается к контроллеру по OSDP, необходимо также настроить:
 - Скорость передачи данных – скорость обмена на RS-485-шлейфе между контроллером и подключёнными к нему считывателями. Возможные скорости: 9600, 19200, 38400, 57600, 115200 бод.
 - Адрес устройства – уникальный адрес считывателя на RS-485-

- шлейфе. Целое число от 1 до 127.
- Включение терминирующего резистора RS-485 – требуется, если устройство является первым или последним на шлейфе.
 - Установочный режим шифрования – требуется установить, если считыватель необходимо перевести в режим шифрования данных, передаваемых по OSDP, и загрузить профиль шифрования.
5. Нажмите кнопку «Применить» и дождитесь окончания загрузки настроек на считыватель. Настройки применяются автоматически, перезагрузка считывателя не требуется.



Установка выходного интерфейса считывателя.

21. Шифрование данных, передаваемых по OSDP

При работе считывателей по интерфейсу OSDP в целях повышения уровня безопасности опционально может быть включено шифрование передаваемых данных между считывателем и контроллером.

Для использования функциональности шифрования данных считыватель Sigur может быть подключён по интерфейсу OSDP как к контроллеру Sigur, так и к контроллеру стороннего производителя.

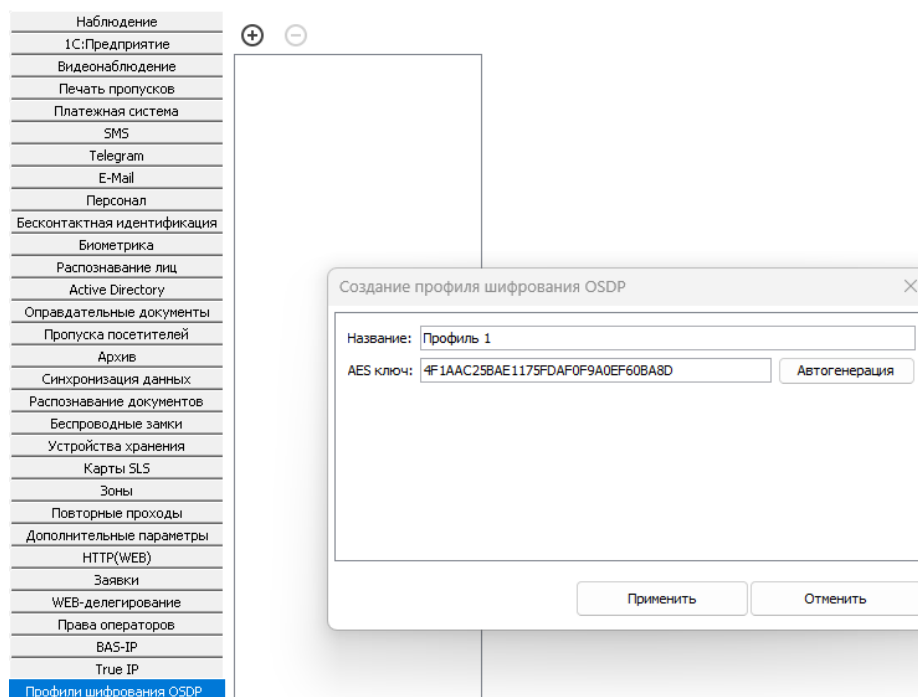
Настройка такого режима работы состоит из следующих этапов:

1. Создание профиля шифрования.
2. Применение профиля шифрования.

21.1. Создание профиля шифрования OSDP

Создание и управление профилями шифрования осуществляется в программе «Клиент».

1. Чтобы создать новый профиль шифрования OSDP, перейдите в меню «Файл» – «Настройки» – «Профили шифрования OSDP» и нажмите кнопку «+».
2. В открывшемся окне задайте название профиля и укажите AES ключ (введите вручную или сгенерируйте автоматически с помощью кнопки «Автогенерация»).
3. После ввода всех данных нажмите кнопку «Применить» – созданный профиль шифрования появится в списке.

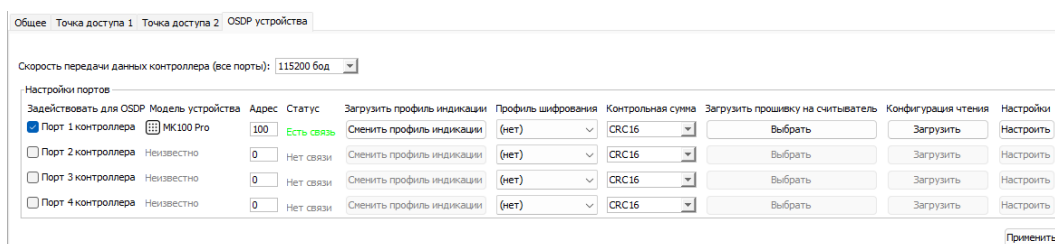


Окно редактирования настроек профилей шифрования OSDP.

21.2. Применение профиля шифрования OSDP

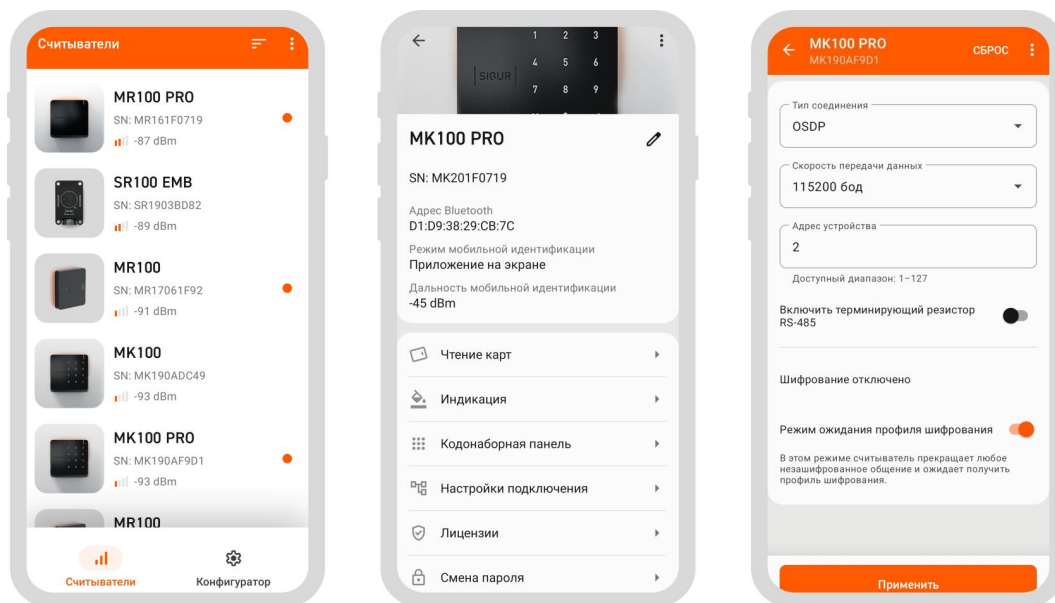
Чтобы применить профиль шифрования, необходимо:

1. Убедиться, что между считывателем и контроллером установлена связь. Если считыватель подключён к контроллеру Sigur, то для этого в программе «Клиент» на вкладке «Оборудование» нужно выделить точку доступа контроллера и нажать кнопку «Настройки». На вкладке «OSDP устройства» считыватель должен быть назначен на конкретный порт контроллера, статус которого «Есть связь».



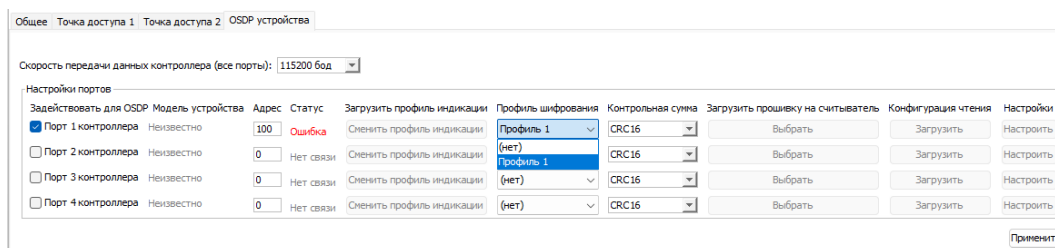
Проверка состояния связи по OSDP между считывателем и контроллером через ПО «Клиент».

2. В мобильном приложении «Sigur Настройки» выбрать интересующий считыватель и в списке действий для него перейти в «Настройки подключения», активировать опцию «Режим ожидания профиля шифрования» и нажать кнопку «Применить».



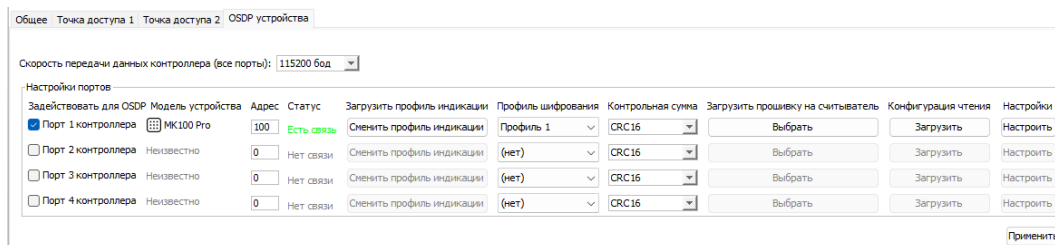
Активация режима ожидания профиля шифрования на считывателе.

3. Загрузить профиль шифрования с контроллера на считыватель. Если считыватель подключён к контроллеру Sigur, то в программе «Клиент» в меню настроек точки доступа на вкладке «OSDP устройства» для конкретного порта контроллера назначить ранее созданный профиль шифрования, нажать кнопку «Применить».



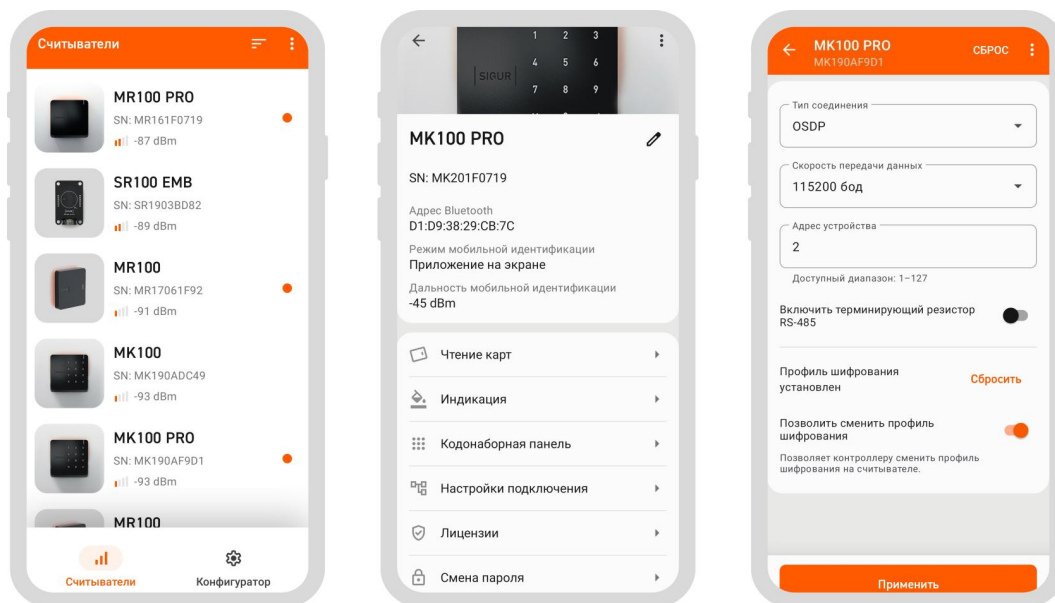
Назначение профиля шифрования OSDP.

4. Далее необходимо убедиться, что статус связи после применения профиля шифрования OSDP отображается как «Есть связь».



Проверка состояния связи по OSDP после применения профиля шифрования.

5. В мобильном приложении также можно увидеть, что профиль шифрования был успешно установлен.



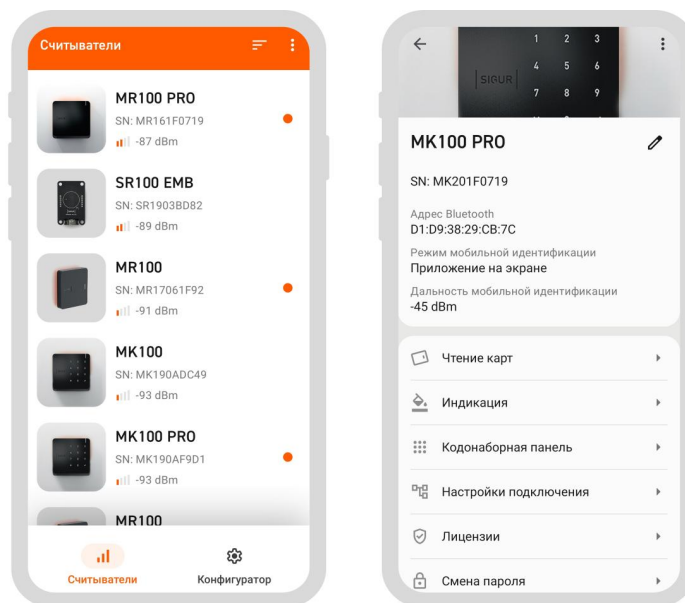
Меню настроек подключения считывателя при установленном профиле шифрования.

21.3. Сброс профиля шифрования

При необходимости профиль шифрования OSDP можно сбросить. Сброс профиля шифрования OSDP необходим в случае, если по каким-то причинам (удалена база данных, сервер вышел из строя, человеческий фактор) был удалён профиль шифрования OSDP в программе «Клиент», а восстановить значение AES-ключа не представляется возможным.

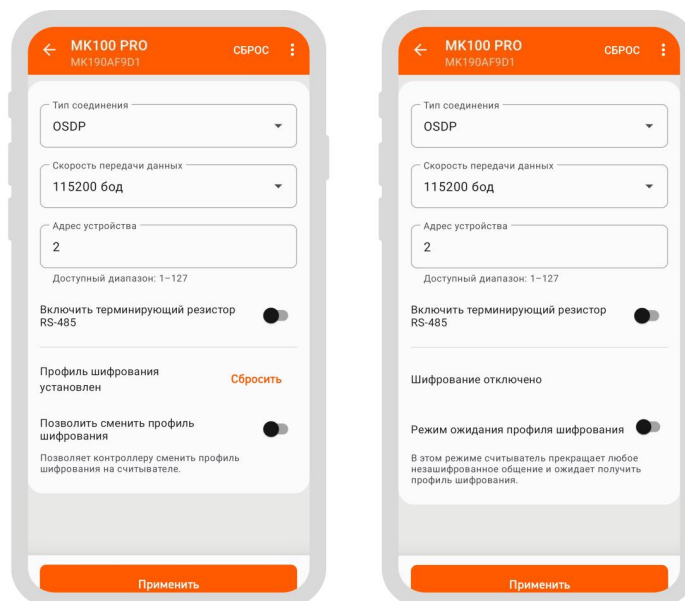
Чтобы сбросить профиль шифрования, необходимо выполнить следующие действия:

1. В мобильном приложении «Sigur Настройки» выбрать интересующий считыватель и в списке действий для него перейти в «Настройки подключения».



Список доступных действий.

2. Нажать на кнопку «Сбросить» напротив пункта «Профиль шифрования установлен» и нажать кнопку «Применить», чтобы внесённые изменения применились на считыватель.



Процедура сброса профиля шифрования OSDP на считывателе.

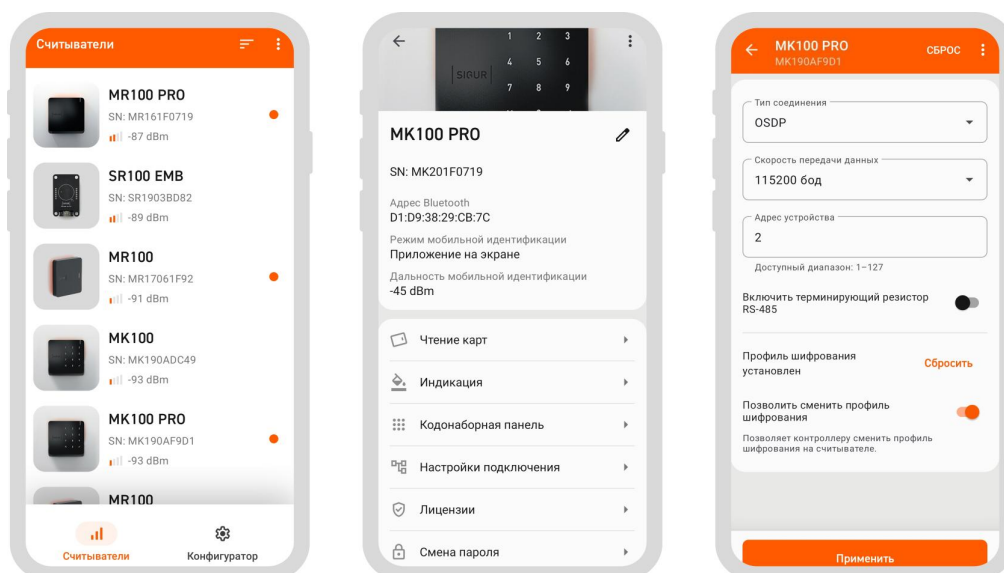
21.4. Изменение профиля шифрования

Если на считывателе уже установлен профиль шифрования, то опционально на считывателе можно активировать функцию, позволяющую изменить текущий профиль на другой с помощью команды протокола OSDP со стандартным AES-ключом.

В частности, если контроллеру не будет известен ранее установленный на считывателе профиль шифрования OSDP с определенным AES-ключом, то он сможет установить на считыватель новый профиль шифрования (с новым AES-ключом), и этот профиль будет передан на считыватель с помощью команды OSDP-протокола со стандартным AES-ключом.

Для активации опции «Позволить сменить профиль шифрования» необходимо выполнить следующие действия:

1. В мобильном приложении «Sigur Настройки» выбрать интересующий считыватель и в списке действий для него перейти в «Настройки подключения».
2. Активировать опцию «Позволить сменить профиль шифрования» и нажать кнопку «Применить», чтобы внесённые изменения применились на считыватель.
3. Если считыватель подключён к контроллеру Sigur, то далее можно выбрать новый профиль шифрования в настройках точки доступа в программе «Клиент».



Процесс активации опции «Позволить сменить профиль шифрования».

Если данная опция не будет активирована, то считыватель будет игнорировать попытки изменения текущего профиля шифрования с помощью команд со стандартным AES-ключом, полученных по OSDP. В таком случае профиль шифрования можно будет изменить только при условии, что между контроллером и считывателем уже установлено шифрованное соединение или после сброса профиля шифрования на считывателе.

22. Обновление внутреннего ПО считывателя через программу «Клиент»

Новые микропрограммы могут исправлять некоторые ошибки предыдущих версий и расширять функции считывателя.



Этот способ актуален только для тех случаев, когда считыватель подключён к контроллеру Sigur по интерфейсу OSDP.

Данная возможность – отличительная особенность протокола SSDP, позволяющая централизованно с рабочего места обновить микропрограмму считывателя до актуальной версии.

Если используется иная конфигурация системы, воспользуйтесь альтернативным способом – обновите микропрограмму считывателя с помощью мобильного приложения. Процедура подробно описана в соответствующем [разделе](#).

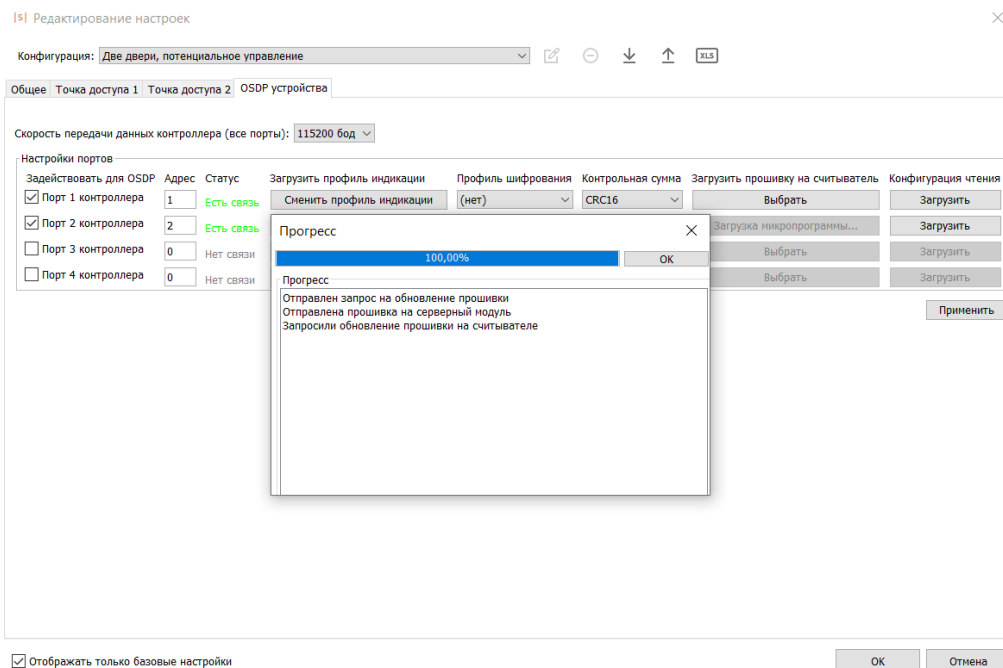
Для обновления микропрограммы считывателя через ПО «Клиент» должны выполняться следующие технические требования:

- версия микропрограммы считывателя должна быть не ниже 53;
- версия микропрограммы контроллера должна быть не ниже 1.23.X;
- версия ПО должна быть не ниже 1.6.7.60 (подойдёт [бесплатная версия](#)).

Для проведения операции обновления микропрограммы считывателя необходимо выполнить следующие действия:

1. Скачать файл программного обеспечения считывателя Sigur с [сайта](#) (раздел «Прочее»).
2. Перейти на вкладку «Оборудование» программы «Клиент», выбрать в списке оборудования точку доступа и нажать кнопку «Настройки».
3. В открывшемся окне нужно перейти на вкладку «OSDP устройства» и нажать кнопку «Выбрать» в колонке «Загрузить прошивку на считыватель» для конкретного порта контроллера.
4. После этого откроется окно с выбором файла микропрограммы считывателя, где необходимо выбрать файл и нажать на кнопку «Открыть». Начнётся процесс загрузки микропрограммы на считыватель.

5. Во время загрузки кнопка «Выбрать» будет изменена на «Загрузка микропрограммы» и будет неактивна, а в журнале системных событий появится событие «Начало применения микропрограммы на считыватель».



Процесс загрузки микропрограммы на считыватель через программу «Клиент».

6. При успешном окончании загрузки кнопка «Выбрать» примет свое стандартное состояние, а в журнале системных событий (подробнее можно ознакомиться в разделе «Журнал системных событий») появится событие «Микропрограмма считывателя успешно обновлена».

23. Индикация считывателя

23.1. Сигналы управления индикацией

Независимо от конфигурации индикации считыватель воспроизводит особые звуковые сигналы при включении, аппаратном сбросе, переходе в дополнительный режим работы, нажатии кнопок сенсорной клавиатуры и при программировании мастер-картой.

В состоянии покоя клавиатура и основной индикатор светятся белым. При нажатии кнопок подсветка клавиатуры становится оранжевой, при переходе в дополнительный режим – красной, индикатор при этом не меняет цвет. При установлении связи со считывателем и во время обмена данными через мобильные приложения «Sigur Настройки» или «Sigur Доступ» загорается оранжевый светодиод индикатора, клавиатура остаётся белой.

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

23.1.1. Управление индикацией при подключении по Wiegand

При подключении по протоколу Wiegand считыватель Sigur ожидает управление индикацией по какому-либо из трёх его цифровых входов «IN1/GREEN/LEDG», «IN2/RED/LEDR» или «IN3/BEEP».

Активный уровень линий управления – ноль вольт.

Подключение по Wiegand, стандартная конфигурация индикации

- Если ни на один из управляющих входов «IN1/GREEN/LEDG», «IN2/RED/LEDR» или «IN3/BEEP» не было подано сигнала, то при чтении любого идентификатора считыватель реагирует звуковым сигналом «Разрешение доступа» и кратковременно моргает зелёным.
- Если на одну из управляющих линий «IN1/GREEN/LEDG» или «IN2/RED/LEDR» подаётся сигнал, то считыватель переводится в режим внешнего управления индикацией. Считыватель перестаёт сопровождать индикацией чтение любого идентификатора, ожидая управление по какой-либо из линий «IN1/GREEN/LEDG» или «IN2/RED/LEDR».

В случае подачи сигнала на линию «IN1/GREEN/LEDG» один раз воспроизводится звук «Разрешение доступа» и светодиод светится зелёным на время, совпадающее с временем действия управляющего сигнала. В случае подачи сигнала на линию «IN2/RED/LEDR» один раз воспроизводится звук «Запрет доступа» и светодиод светится красным на время, совпадающее с временем действия управляющего сигнала.

- Если на управляющую линию «IN3/BEEP» подаётся сигнал, то периодически воспроизводится звуковой сигнал «Ожидание действия» и светодиод мигает оранжевым (0,2 с – оранжевый, 0,2 с – отсутствие цвета). Продолжительность воспроизведения звукосветовой последовательности совпадает со временем управляющего сигнала.

Подключение по Wiegand, пользовательская конфигурация индикации.

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 поднесён 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 извлечён 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/LEDG» замкнута на GND (не замкнута на GND) – воспроизводится реакция, установленная на событие IN1/GREEN/LEDG активно (IN1/GREEN/LEDG не активно).
- Если линия «IN2/RED/LEDR» замкнута на GND (не замкнута на GND) – воспроизводится реакция, установленная на событие IN2/RED/LEDR активно (IN2/RED/LEDR 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).

23.1.2. Настройка режима внешнего управления индикацией считывателя

В заводской конфигурации считывателя линии IN1/GREEN/LEDG и IN2/RED/LEDR 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 на вкладку «Оборудование», выберите точку доступа на данном контроллере и нажмите кнопку «Настройки».

Для контроллеров E(R)500U, E(R)900U, E2, E4, E510 и более новых выполните следующее:

1. Отключите опцию «Отображать только базовые настройки».
2. 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/LEDG(PORTN), где **N** – номер порта на контроллере, куда подключён считыватель. В выпадающем меню справа оставьте значение «Нормально не активен».
3. 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/LEDR(PORTN), где **N** – номер порта на контроллере, куда подключён считыватель. В выпадающем меню справа оставьте значение «Нормально не активен».
4. Найдите в списке параметр «Длина импульса разрешения/запрета доступа» и установите его порядка 1 с (или иное время включения световой индикации разрешения/запрета доступа).

Для контроллеров предыдущих моделей настройка идентична, за исключением того, что редактирование функции «Импульс разрешения доступа на «Вход»/«Выход» производится на вкладке «Переназначение клемм».

23.1.3. Управление индикацией при подключении по OSDP

При подключении считывателя по протоколу OSDP команды управления индикацией передаются на считыватель Sigur по линиям «А» и «В». Также индикацией можно управлять и по отдельным линиям «IN1/GREEN/LEDG», «IN2/RED/LEDR» и «IN3/BEEP».

При подключении считывателя к контроллеру Sigur по OSDP контроллер переходит в режим управления индикацией считывателя на этом порту по линиям «А» и «В». Тем не менее считыватель MK100 в данном режиме продолжает обрабатывать состояние входов IN1, IN2, IN3 и реагировать на изменение состояния соответствующей индикацией. Поэтому опционально для контроллера Sigur можно настроить управление индикацией считывателя по этим линиям.

Конфигурация управления индикацией может быть изменена пользователем.

Управление индикацией по OSDP/SSDP, стандартная конфигурация индикации.

Если на считыватель не загружена пользовательская конфигурация индикации, то при чтении любого идентификатора считыватель реагирует звуковым сигналом и кратковременно мигает зелёным.

Управление индикацией по OSDP/SSDP, пользовательская конфигурация индикации.

Если на считыватель была загружена конфигурация индикации, то от считывателя может последовать соответствующая, заранее установленная реакция на определённые события (если на текущий момент нет более приоритетной реакции).

Так как при подключении считывателя по OSDP происходит двунаправленное взаимодействие между считывателем и контроллером, соответственно, события, на которые может отреагировать считыватель, делятся на два типа: события, генерируемые самим считывателем, и события, генерируемые контроллером.

События, генерируемые считывателем MK100:

- «IN1/GREEN/LEDG активно» («IN1/GREEN/LEDG не активно») – линия «IN1/GREEN/LEDG» замкнута на GND (не замкнута на GND).
- «IN2/RED/LEDR активно» («IN2/RED/LEDR не активно») – линия «IN2/RED/LEDR» замкнута на GND (не замкнута на GND).
- «IN3/BEEP активно» («IN3/BEEP не активно») – линия «IN3/BEEP» замкнута на GND (не замкнута на GND).
- «Считыватель на стене» – считыватель закреплён на настенной панели.
- «Считыватель оторван» – считыватель извлечён из настенной панели.
- «Прочитан идентификатор» – к считывателю был поднесён и успешно прочитан идентификатор.
- «Температура вне нормы» – температура считывателя вышла за пределы нормы.
- «Напряжение питания вне нормы» – напряжение считывателя вышло за пределы нормы.

События, генерируемые контроллером Sigur:

- **«Ожидание прохода»** – объекту доступа был разрешён доступ, контроллер ожидает, когда объект доступа совершит проход.
- **«Взлом»** – было зафиксировано пересечение точки доступа несанкционированным образом.
- **«Удержание двери»** – датчик открытия двери не возвращён в нормальное состояние до истечения времени, установленного в настройках точки доступа параметром «Время до сигнала «Удержание двери».
- **«Тревога охранного шлейфа»** – от охранного шлейфа контроллера Sigur (E2, E4) поступило событие «Тревога». Считыватель будет реагировать на событие «Тревога» только от того шлейфа, который назначен точке доступа, связанной с этим считывателем.
- **«Ожидание санкции оператора»** – для идентифицированного объекта доступа применяется режим с установленной опцией «Требовать санкции оператора на проход», идёт ожидание решения оператора.
- **«Ожидание PIN-кода»** – для идентифицированного объекта доступа применяется режим с установленной опцией «Дополнительно запрашивать PIN код», контроллер ожидает получения кода от подключённой кодаборной панели.
- **«Ожидание второй карты»** – для идентифицированного объекта доступа применяется режим с установленной опцией «Доступ в сопровождении» или «Доступ только вдвоём», идёт ожидание идентификации сопровождающего или второго объекта доступа (в случае логики «Доступ только вдвоём»).
- **«Доступ разрешён»** – идентифицированному объекту доступа разрешён доступ.
- **«Доступ запрещён»** – идентифицированному объекту доступа запрещён доступ.
- **«Ожидание алкотестирования»** – для идентифицированного объекта доступа применяется режим с установленной опцией «Тестирование на алкоголь», идёт ожидание результата тестирования.
- **«Зона взята под охрану»** – от охранного шлейфа контроллера Sigur (E2, E4) поступило событие «Взят».
- **«Зона снята с охраны»** – от охранного шлейфа контроллера Sigur (E2, E4) поступило событие «Снят».
- **«Зона под охраной»** – индикация будет активна все время, пока статус у зоны «Взят». Должна воспроизводиться после реакции на событие «Зона взята на охрану» и действовать до события «Зона снята с охраны».
- **«Зона встаёт под охрану»** – воспроизводится после начала процесса постановки на охрану на протяжении времени, когда система игнорирует кратковременные срабатывания датчиков в зоне.
- **«Не удалось взять зону под охрану»** – неудачная постановка зоны на охрану по какой-либо причине.
- **«Не удалось сменить режим точки доступа»** – неудачная смена режима точки доступа по какой-либо причине.
- **«Установлен разблокированный режим»** – индикация смены режима точки доступа на «Разблокировано».

- **«Установлен заблокированный режим»** – индикация смены режима точки доступа на «Заблокировано».
- **«Установлен нормальный режим»** – индикация смены режима точки доступа на «Нормальный».
- **«Точка доступа разблокирована»** – индикация будет активна всё время, пока точка доступа находится в разблокированном режиме. Воспроизводится после реакции на событие «Установлен режим "Разблокировано"».
- **«Точка доступа заблокирована»** – индикация будет активна всё время, пока точка доступа находится в заблокированном режиме. Воспроизводится после реакции на событие «Установлен режим "Заблокировано"».
- **«Ожидание подтверждения картой»** – индикация активируется, когда для подтверждения действий постановки зоны на охрану или смены режима точки доступа, требуется предъявить дополнительный идентификатор. Актуально, когда для выполнения действия требуется PIN + карта.

23.1.4. Стандартные профили индикации считывателя

В программе «Клиент» предусмотрены стандартные профили индикации с заранее установленными реакциями на определённые события, которые можно загрузить на считыватель Sigur.

В зависимости от того, по какому интерфейсу связи подключён считыватель и к какому контроллеру (к контроллеру Sigur или к контроллеру стороннего производителя), выбирается соответствующий профиль.

Стандартные профили индикации считывателя, подключённого по Wiegand.

Если необходимо настроить индикацию на считывателе, подключённом к любому контроллеру (Sigur или стороннего производителя) **по Wiegand**, то на считыватель можно загрузить такие стандартные профили индикации, как:

- Стандартный профиль MR100 (MK100);
- MR (MK100), Wiegand (eng). Индикация сопровождается голосовой озвучкой на английском языке;
- MR (MK100), Wiegand (rus). Индикация сопровождается голосовой озвучкой на русском языке.

Стандартные профили индикации считывателя, подключённого по SSDP.

Если необходимо настроить индикацию на считывателе, подключённом к **контроллеру Sigur по OSDP (SSDP)**, то на считыватель можно загрузить такие стандартные профили индикации, как:

- MR100 (MK100), SSDP (eng). Индикация сопровождается голосовой озвучкой на английском языке.

- MR100 (MK100), SSDP (rus). Индикация сопровождается голосовой озвучкой на русском языке.
- SIGUR PRO, SSDP (eng). Индикация сопровождается голосовой озвучкой на английском языке.
- SIGUR PRO, SSDP (rus). Индикация сопровождается голосовой озвучкой на русском языке.

Профили индикации Sigur PRO, SSDP (rus) и Sigur PRO, SSDP (eng) позволяют отключить управление индикацией на отдельных входах и использовать их для подключения кнопок и датчиков. Подробная информация о данном функционале представлена в разделе «Подключение кнопок и датчиков к считывателю».

Для расширенных функций считывателя выполняется следующая стандартная индикация:

- **«Зона взята под охрану»** – основной индикатор 2 раза мигает зелёным и жёлтым цветом, воспроизводится звуковой сигнал «Зона взята под охрану».
- **«Зона снята с охраны»** – основной индикатор 2 раза мигает зелёным и жёлтым цветом, воспроизводится звуковой сигнал «Зона снята с охраны».
- **«Зона под охраной»** – основной индикатор непрерывно мигает красным и зелёным цветом (0,2 с – красный, 0,2 с – зелёный), звуковой сигнал отсутствует.
- **«Зона встаёт под охрану»** – основной индикатор непрерывно мигает оранжевым и белым цветом (0,2 с – оранжевый, 0,3 с – белый), воспроизводится звуковой сигнал «Зона встаёт под охрану».
- **«Не удалось взять зону под охрану»** – основной индикатор 3 раза мигает красным цветом, воспроизводится звуковой сигнал «Не удалось взять зону под охрану».
- **«Не удалось сменить режим точки доступа»** – основной индикатор 3 раза мигает красным цветом, воспроизводится звуковой сигнал «Не удалось сменить режим точки доступа».
- **«Установлен разблокированный режим»** – основной индикатор 3 раза мигает зелёным и белым цветом, воспроизводится звуковой сигнал «Установлен разблокированный режим».
- **«Установлен заблокированный режим»** – основной индикатор 1 раз мигает красным и белым цветом, воспроизводится звуковой сигнал «Установлен заблокированный режим».
- **«Установлен нормальный режим»** – основной индикатор 1 раз мигает зелёным и белым цветом, воспроизводится звуковой сигнал «Установлен нормальный режим».
- **«Точка доступа разблокирована»** – основной индикатор непрерывно мигает зелёным и белым цветом (2 с – зелёный, 0,5 с – белый), звуковой сигнал отсутствует.
- **«Точка доступа заблокирована»** – основной индикатор непрерывно мигает красным и белым цветом (2 с – красный, 0,5 с – белый), звуковой сигнал отсутствует.

- **«Ожидание подтверждения картой»** – основной индикатор на протяжении всего тайм-аута ожидания подтверждения (10 секунд) мигает жёлтым и белым цветом (0,5 с – жёлтый, 0,5 с – белый), воспроизводится звуковой сигнал «Ожидание подтверждения картой».

Стандартные профили индикации считывателя, подключённого по OSDP.

Если необходимо настроить индикацию на считывателе, подключённом к **контроллеру стороннего производителя по OSDP**, то на считыватель можно загрузить стандартный профиль – Sigur MR100 (MK100), OSDP.

Если возникает необходимость изменить стандартный профиль или создать свой собственный, то с настройкой пользовательской индикации можно ознакомиться в соответствующем разделе.

23.2. Настройка пользовательской индикации считывателя



Световая и звуковая индикация считывателей Sigur MK100 может быть гибко настроена только средствами ПО Sigur. Если считыватель настраивается на работу с контроллером СКУД стороннего производителя, то для настройки достаточно бесплатной версии ПО.

Настройка индикации считывателей, подключённых **по Wiegand к любому контроллеру** (стороннего производителя или Sigur), а также считывателей, подключённых **по OSDP к контроллеру стороннего производителя** производится следующим образом:

1. С помощью ПО Sigur «Клиент» создаётся профиль индикации. В окне настроек загружаются звуки и создаются реакции считывателя на какое-либо событие из списка. Создание профиля индикации более подробно рассматривается ниже.
2. После окончательной настройки профиль либо прикрепляется к письму и отправляется на указываемый вами e-mail средствами ПО Sigur, либо сохраняется на компьютер, а далее передаётся на смартфон альтернативными способами.
3. Полученный профиль индикации открывается на смартфоне в приложении «Sigur Настройки», после чего загружается на считыватель по беспроводной технологии BLE. Подробнее этот процесс описан в разделе «Загрузка профиля индикации на считыватель».

Настройка индикации считывателей, подключённых **по OSDP к контроллеру Sigur**, может осуществляться альтернативным способом – профиль индикации можно загружать на считыватель централизованно из программы «Клиент» по протоколу SSDP. Подробнее этот способ описан в соответствующем разделе.

Все действия, связанные с настройкой профилей индикации считывателя, производятся в меню «Файл» – «Настройки» – «Индикация».

Данное окно имеет 4 вкладки:

- Профили – содержит список профилей индикации. По умолчанию в нём созданы стандартные профили.

На данной вкладке создаются новые профили индикации: назначается индикация считывателя для режима ожидания, т.е. для «состояния покоя», а также указывается реакция на какое-либо событие из списка.

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

На данной вкладке создаются новые реакции, характерные исключительно для считывателей Sigur: настраивается логика световой и звуковой индикации. Эти реакции могут быть использованы при управлении индикацией считывателя как по какому-либо из трёх его цифровых входов, так и по протоколу SSDP.

- Реакции OSDP – содержит список ранее настроенных реакций OSDP.

На данной вкладке создаются реакции считывателя, характерные для стандартного протокола OSDP и применимые для считывателей, управление индикацией которых может выполняться с помощью команд OSDP: указывается тип световой и параметры стандартной звуковой индикации считывателя.

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

На данной вкладке можно загрузить звук из файла, а также прослушать ту или иную запись из списка. Впоследствии звуки можно использовать при настройке реакций считывателей Sigur.

23.2.1. Создание профиля индикации считывателя

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

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

Также при создании пользовательского профиля индикации необходимо выбрать его тип.

Тип показывает, как именно будет осуществляться управление индикацией (по трём цифровым входам, по протоколу OSDP или по протоколу SSDP), для какого считывателя (Sigur или стороннего производителя) и при взаимодействии с каким контроллером (Sigur или стороннего производителя) настраивается данный профиль индикации. В зависимости от того, какой тип был выбран, меняется список событий, на которые можно настроить реакции.



Если создаётся профиль индикации с типом «считыватель и контроллер Sigur», то наиболее полный функционал профиля данного типа можно будет получить, подключив считыватель к контроллеру по интерфейсу OSDP, а не Wiegand.

В частности, при подключении считывателя Sigur по интерфейсу OSDP есть возможность использовать не только реакции на события считывателя, но и реакции на события контроллера.

Если считыватель Sigur подключён к контроллеру по Wiegand, а управление индикацией происходит по трём линиям, то актуальна будет лишь часть функций, то есть можно будет настроить реакции на события считывателя, а реакции на события контроллера в таком случае не будут использоваться совсем.

При создании профиля индикации для считывателя Sigur можно выбрать один из следующих типов:

- Считыватель и контроллер Sigur – если считыватель подключён к контроллеру Sigur независимо от интерфейса подключения. В случае подключения по интерфейсу Wiegand будут использоваться только реакции на события считывателя, а в случае подключения по интерфейсу OSDP для настройки будут доступны все реакции (события считывателя и контроллера).
- Считыватель Sigur (Wiegand), сторонний контроллер – если считыватель подключён по Wiegand к контроллеру стороннего производителя и управление индикацией происходит по цифровым входам «IN1/GREEN/LEDG», «IN2/RED/LEDR» или «IN3/BEEP».

- Считыватель Sigur (OSDP), сторонний контроллер – если считыватель подключён к стороннему контроллеру по OSDP, и управление индикацией происходит посредством команд стандартного протокола OSDP.

Название: Профиль индикации

Тип: Считыватель и контроллер Sigur

Индикация состояния покоя

Тип: постоянный свет

Цвет: ■

Событие	Реакция	Приоритет
IN1/GREEN/LEDG не активно	Без реакции	0 (Наименьший)
IN1/GREEN/LEDG активно	Разрешение доступа 2	15
IN2/RED/LEDR не активно	Без реакции	0 (Наименьший)
IN2/RED/LEDR активно	Запрет доступа 2	15
IN3/BEEP не активно	Без реакции	0 (Наименьший)
IN3/BEEP активно	Считыватель не в норме	14
Считыватель на стене	Без реакции	0 (Наименьший)
Считыватель оторван	Вскрытие корпуса	14
Прочитан идентификатор	Без реакции	0 (Наименьший)
Температура вне нормы	Считыватель не в норме	14
Напряжение питания вне нормы	Считыватель не в норме	14

отправить email

применить отменить

Создание и настройка нового профиля индикации считывателя.

Профиль индикации позволяет настроить:

- Световую индикацию ожидания считывателем наступления какого-либо события.

Параметр «Тип индикации» может иметь следующие значения:

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

- Реакцию считывателя на какое-либо событие.

Реакции, созданные на вкладках «Реакции считывателей Sigur», могут быть назначены на одну из представленных ниже функций.

Полный перечень функций на вкладке «Профили».

Название функции	Описание. Реакция активируется при:
IN1/GREEN/LEDG не активно	Линия IN1/GREEN/LEDG не замкнута на GND.
IN1/GREEN/LEDG активно	Линия IN1/GREEN/LEDG замкнута на GND.
IN2/RED/LEDR не активно	Линия IN2/RED/LEDR не замкнута на GND.
IN2/RED/LEDR активно	Линия IN2/RED/LEDR замкнута на GND.
IN3/BEEP не активно	Линия IN3/BEEP не замкнута на GND.
IN3/BEEP активно	Линия IN3/BEEP замкнута на GND.
Считыватель на стене	Считыватель закреплён на настенной панели.
Считыватель оторван	Считыватель извлечён из настенной панели.
Прочитан идентификатор	Чтение идентификатора считывателем (карта или смартфон).
Температура вне нормы	Выход температуры считывателя за пределы нормы.
Напряжение питания вне нормы	Напряжение считывателя вышло за пределы нормы.
Ожидание прохода	Объекту доступа был разрешён доступ, контроллер ожидает, когда объект доступа совершит проход.
Взлом	Было зафиксировано пересечение точки доступа несанкционированным образом, например, активировался датчик открытия двери.
Удержание двери	Датчик открытия двери не возвращён в нормальное состояние до истечения времени, установленного в настройках точки доступа параметром «Время до сигнала «Удержание двери»».
Тревога охранного шлейфа	От охранного шлейфа контроллера Sigur (E2, E4) поступило событие «Тревога».

Название функции	Описание. Реакция активируется при:
Ожидание санкции оператора	Для идентифицированного объекта доступа применяется режим с установленной опцией «Требовать санкции оператора на проход», идёт ожидание решения оператора.
Ожидание PIN-кода	Для идентифицированного объекта доступа применяется режим с установленной опцией «Дополнительно запрашивать PIN код», контроллер ожидает получения кода от подключённой кодонаборной панели.
Ожидание второй карты	Для идентифицированного объекта доступа применяется режим с установленной опцией «Доступ в сопровождении» или «Доступ только вдвоём», идёт ожидание идентификации сопровождающего или второго объекта доступа (в случае с опцией «Доступ только вдвоём»).
Доступ разрешён	Идентифицированному объекту доступа разрешён доступ.
Доступ запрещён	Идентифицированному объекту доступа запрещён доступ.
Ожидание алкотестирования	Для идентифицированного объекта доступа применяется режим с установленной опцией «Тестирование на алкоголь», идёт ожидание результата тестирования.
Зона взята под охрану	От охранного шлейфа контроллера Sigur (E2, E4) поступило событие «Взят».
Зона снята с охраны	От охранного шлейфа контроллера Sigur (E2, E4) поступило событие «Снят».
Зона под охраной	Индикация активна всё время пока статус у зоны «Взят». Должна воспроизводиться после реакции на событие «Зона взята на охрану» и действовать до события «Зона снята с охраны».

Название функции	Описание. Реакция активируется при:
Зона встаёт под охрану	Индикация воспроизводится после инициации постановки на охрану на протяжении времени, когда система игнорирует кратковременные срабатывания датчиков в зоне.
Не удалось взять зону под охрану	Индикация неудачной постановки на охрану по какой-либо причине.
Не удалось сменить режим точки доступа	Индикация неудачной смены режима точки доступа по какой-либо причине.
Установлен разблокированный режим	Индикация воспроизводится в момент поступления события «Установлен режим "Разблокировано"».
Установлен заблокированный режим	Индикация воспроизводится в момент поступления события «Установлен режим "Заблокировано"».
Установлен нормальный режим	Индикация воспроизводится в момент поступления события «Установлен режим "Нормальный"».
Точка доступа разблокирована	Индикация активна всё время, пока точка доступа находится в разблокированном режиме. Воспроизводится после реакции на событие «Установлен режим "Разблокировано"».
Точка доступа заблокирована	Индикация активна всё время, пока точка доступа находится в заблокированном режиме. Воспроизводится после реакции на событие «Установлен режим "Заблокировано"».
Ожидание подтверждения картой	Индикация активируется, когда для подтверждения действий постановки зоны на охрану требуется предъявить дополнительный идентификатор. Актуально, когда для выполнения действия требуется PIN + карта.

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

Реакции могут быть двух типов:

1 – длительность реакции определяется длительностью события (сменить цвет, мигание непрерывно);

2 – фиксированная длительность реакции (мигнуть однократно, мигнуть несколько раз).

Логика смены реакций представлена в таблице ниже.

Смена реакций в зависимости от их приоритетов и типов.

Тип реакции		Приоритет текущей реакции	Результат. Наступающая реакция:
Текущей	Наступающей		
1	1	Меньше или равен	Переключает текущую
		Больше	Не переключает текущую
1	2	Меньше или равен	Переключает текущую
		Больше	Не переключает текущую
2	1	Меньше или равен	Переключает текущую
		Больше	Не переключает текущую
2	2	Любой	Переключает текущую

Опционально может быть настроен «Приоритет OSDP событий стороннего контроллера». Этот параметр будет актуален только для тех случаев, когда считыватель подключён к контроллеру по интерфейсу OSDP и управление индикацией происходит стандартными командами OSDP. В качестве системных событий выступают события, переданные контроллером на считыватель. Таким образом, настройкой данного параметра можно определить приоритет событий, генерируемых контроллером, над событиями, генерируемыми считывателем.

После настройки профиля индикации необходимо нажать «Применить».

23.2.2. Создание реакции считывателя

Для добавления новой реакции считывателя Sigur на определённое событие перейдите во вкладку «Файл» – «Настройки» – «Индикация» – «Реакции считывателей Sigur». Новая реакция создаётся путём нажатия кнопки «+» или копированием другой реакции соответствующей кнопкой.

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

Профили Реакции считывателей SIGUR Реакции OSDP Звуки

Название: Реакция

LED 1

Тип индикации: Мигание несколько раз

Цвет 1: Длительность: 0,5 секунд

Цвет 2: Длительность: 0,5 секунд

Повторений: 1

Buzzer 1

Звук: Авария

☒ Непрерывно

Количество повторений: 0 раз

Пауза между повторениями: 0,2 секунд

Применить Отменить

OK Отмена

Создание реакции для считывателя Sigur.

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.



При выборе типа индикации «Сменить цвет» длительность реакции принимает значение 0 секунд и становится недоступной для редактирования. Для остальных типов индикации автоматически применяется значение по умолчанию — 0,5 с.

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

- «Нет звука» — 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.

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

23.2.3. Добавление звука реакции считывателя

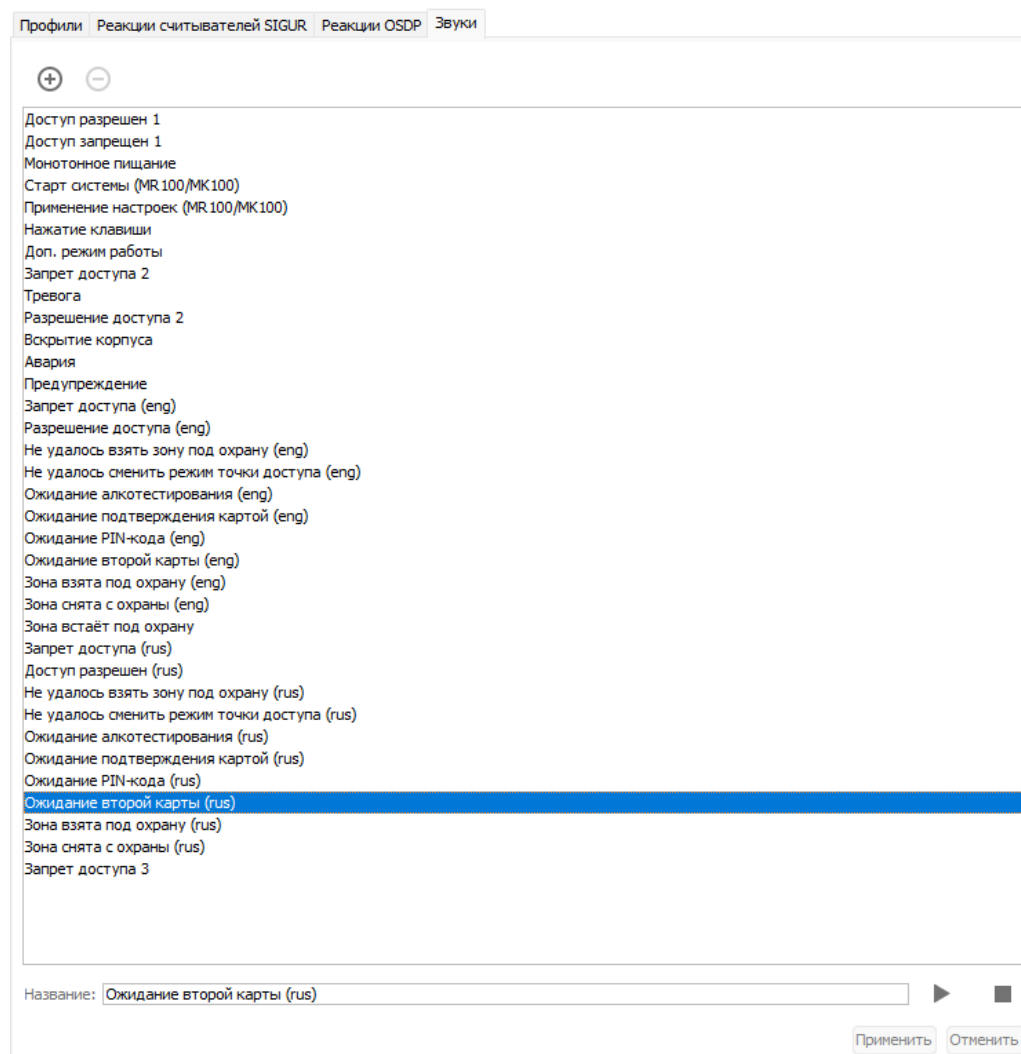
Для загрузки нового звукового файла в ПО перейдите во вкладку «Файл» — «Настройки» — «Индикация» — «Звуки». Нажмите на кнопку «+» сверху. В открывшемся окне выберите нужный аудиофайл.

Поддерживаемые звуковые форматы:

- Формат звукового файла: *.wav, *.aiff или *.au.
- Частота дискретизации: 8kHz-48kHz.
- Разрешение семпла: 8-bit, 16-bit.
- Максимальное количество каналов: 2.
- Длительность загружаемых звуков: не более 45 секунд.

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.



Вкладка «Звуки» в окне «Файл» – «Настройки» – «Индикация».

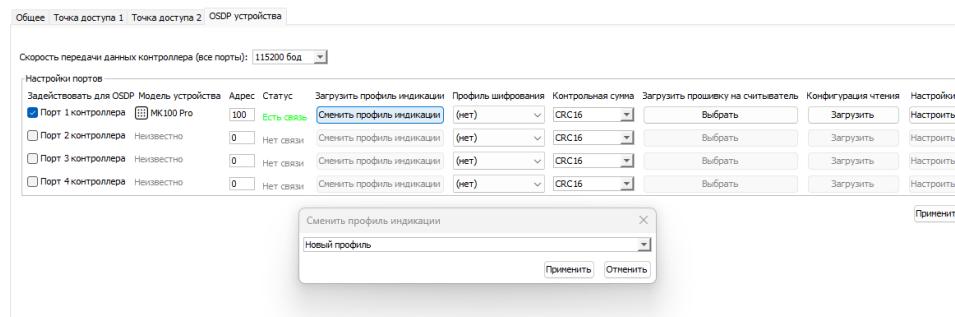
23.2.4. Способы загрузки пользовательского профиля индикации на считыватель

Пользовательский профиль индикации можно загрузить на считыватель двумя способами:

1. Загрузить конфигурационный файл индикации с помощью приложения «Sigur Настройки», установленного на смартфоне. Этот способ подробно описан в соответствующем [разделе](#).
2. Загрузить профиль индикации с помощью программы «Клиент» через OSDP-интерфейс. Этот способ актуален только для тех случаев, когда считыватель Sigur подключён к контроллеру Sigur по интерфейсу OSDP. Данная возможность – отличительная особенность протокола SSDP, позволяющая централизованно с рабочего места обновить профиль индикации на считывателях.
 - Для этого в программе «Клиент» на вкладке «Оборудование» можно перейти в меню настроек точки доступа, а далее в новом окне – на вкладку «OSDP устройства». После чего для конкретного порта контроллера нажать кнопку «Сменить профиль индикации», выбрать из выпадающего списка профиль индикации, который необходимо загрузить на считыватель, и нажать кнопку «Применить». После этих действий начнётся процесс загрузки профиля индикации на считыватель.

Загрузка профиля индикации происходит в фоновом режиме и может занимать продолжительное время.

Во время загрузки кнопка «Сменить профиль индикации» будет изменена на информационное сообщение «Профиль загружается» и будет неактивна, а в журнале системных событий (подробнее можно ознакомиться в разделе «[Журнал системных событий](#)») появится событие «Начало загрузки профиля индикации на считыватель».



Процесс загрузки профиля индикации на считыватель через программу «Клиент».

- При успешной загрузке профиля индикации кнопка «Сменить профиль индикации» снова станет активной, а в журнале системных событий появится событие «Профиль индикации успешно загружен на считыватель».
- При неуспешной загрузке профиля индикации в журнале системных событий появится событие об ошибке. Подробнее ознакомиться с возможными ошибками можно в соответствующем [разделе](#).

24. Журнал системных событий

Для отслеживания процесса выполнения процедур обновления профиля индикации, профиля чтения карт, микропрограммы считывателя, а также событий, связанных с постановкой/снятием зон на охрану через протокол SSDP в программе «Клиент» предусмотрен «Журнал системных событий».

Для отслеживания обновлений профиля индикации, профиля чтения карт, микропрограммы считывателя, а также событий постановки и снятия зон с охраны по протоколу SSDP в программе «Клиент» используется «Журнал системных событий».

События в журнале можно просмотреть, нажав на кнопку «Показать журнал системных событий», расположенную на вкладке «Оборудование».



Кнопка «Показать журнал системных событий».



Данная кнопка появляется автоматически, если есть как минимум одно событие.

В журнале указана следующая информация:

- Дата и время события.
- Параметры. Содержит такую информацию, как:
 - серийный номер контроллера;
 - порт, к которому подключён считыватель, связанный с данным событием.
 - название профиля индикации (опционально).
- Тип события.

Журнал системных событий		
Охватываемый период		
От: 23.09.2025 00:00	До: 24.09.2025 23:59	Выбор типа события Применить
Дата и время	Параметры	Событие
2025-09-23 13:02:37	Серийный номер контроллера: 15087021, порт: 1.	Запуск процесса обновления профиля чтения карт считывателя.
2025-09-23 13:02:38	Серийный номер контроллера: 15087021, порт: 1.	Начало применения профиля чтения карт на считыватель.
2025-09-23 13:02:38	Серийный номер контроллера: 15087021, порт: 1.	Профиль чтения карт считывателя успешно обновлен.
2025-09-23 14:54:18	Серийный номер контроллера: 15087021, порт: 1.	Запуск процесса обновления профиля чтения карт считывателя.
2025-09-23 14:54:19	Серийный номер контроллера: 15087021, порт: 1.	Начало применения профиля чтения карт на считыватель.
2025-09-23 14:54:19	Серийный номер контроллера: 15087021, порт: 1.	Профиль чтения карт считывателя успешно обновлен.
2025-09-23 14:54:54	Серийный номер контроллера: 15087021, порт: 1.	Запуск процесса обновления профиля чтения карт считывателя.
2025-09-23 14:54:55	Серийный номер контроллера: 15087021, порт: 1.	Профиль чтения карт считывателя успешно обновлен.
2025-09-23 14:55:34	Серийный номер контроллера: 15087021, порт: 1.	Запуск процесса обновления профиля чтения карт считывателя.
2025-09-23 14:55:35	Серийный номер контроллера: 15087021, порт: 1.	Профиль чтения карт считывателя успешно обновлен.
2025-09-24 11:37:23	Серийный номер контроллера: 15087021, порт: 1, профиль индикации: "MR100 (MK100), SS..."	Начало загрузки профиля индикации на считыватель.
2025-09-24 11:45:36	Серийный номер контроллера: 15087021, порт: 1, профиль индикации: "MR100 (MK100), SS..."	Ошибка обновления профиля индикации: Не удалось выполнить операцию при работе с файло...
2025-09-24 11:48:14	Серийный номер контроллера: 15087021, порт: 1, профиль индикации: "MR100 (MK100), SS..."	Начало загрузки профиля индикации на считыватель.
2025-09-24 12:13:22	Серийный номер контроллера: 15087021, порт: 1, профиль индикации: "MR100 (MK100), SS..."	Профиль индикации успешно загружен на считыватель.
Отфильтровать отображенные события		

Отображение событий в журнале системных событий.

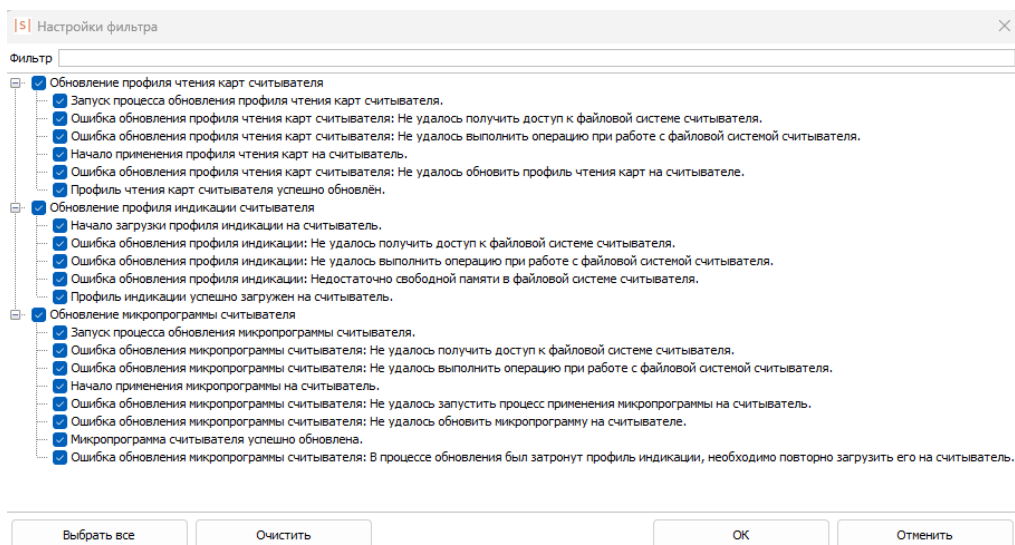
В журнале отображаются такие события, как:

- События, связанные с обновлением профиля чтения карт считывателя:
 - Запуск процесса обновления профиля чтения карт считывателя.
 - Ошибка обновления профиля чтения карт считывателя: Не удалось получить доступ к файловой системе считывателя.
 - Ошибка обновления профиля чтения карт считывателя: Не удалось выполнить операцию при работе с файловой системой считывателя.
 - Начало применения профиля чтения карт на считыватель.
 - Ошибка обновления профиля чтения карт считывателя: Не удалось обновить профиль чтения карт на считывателе.
 - Профиль чтения карт считывателя успешно обновлён.
- События, связанные с профилем индикации считывателя:
 - Начало загрузки профиля индикации на считыватель.
 - Ошибка обновления профиля индикации: Не удалось получить доступ к файловой системе считывателя.
 - Ошибка обновления профиля индикации: Не удалось выполнить операцию при работе с файловой системой считывателя.
 - Ошибка обновления профиля индикации: Недостаточно свободной памяти в файловой системе считывателя.
 - Профиль индикации успешно загружен на считыватель.
- События, связанные с обновлением микропрограммы считывателя:
 - Запуск процесса обновления микропрограммы считывателя.
 - Ошибка обновления микропрограммы считывателя: Не удалось получить доступ к файловой системе считывателя.
 - Ошибка обновления микропрограммы считывателя: Не удалось выполнить операцию при работе с файловой системой считывателя.
 - Начало применения микропрограммы на считыватель.

- Ошибка обновления микропрограммы считывателя: Не удалось запустить процесс применения микропрограммы на считыватель.
- Ошибка обновления микропрограммы считывателя: Не удалось обновить микропрограмму на считывателе.
- Микропрограмма считывателя успешно обновлена.
- Ошибка обновления микропрограммы считывателя: В процессе обновления был затронут профиль индикации, необходимо повторно загрузить его на считыватель.
- События, связанные с настройкой кодонаборной панели:
 - Режимы MK100 успешно настроены.
 - Ошибка настройки режимов MK100.
- События, связанные с управлением охранными зонами (отображаются только события от охранных шлейфов, подключенных к контроллеру E2/E4 (OC Sigur)):
 - Зона снята с охраны.
 - Зона взята под охрану.
 - Зона встаёт под охрану.
 - Тревога охранного шлейфа.
 - Ожидание подтверждения постановки на охрану.
 - Не удалось взять зону под охрану. Неверный PIN-код.
 - Не удалось взять зону под охрану. Не дождалась подтверждения пропуском.
 - Не удалось взять зону под охрану. Доступ запрещен.
 - Не удалось взять зону под охрану. Сопротивление шлейфа не в пределах нормы.
 - Не удалось взять зону под охрану. Тревога охранного шлейфа.
 - Не удалось взять зону под охрану. Дверь открыта.
 - Не удалось взять зону под охрану. Ворота открыты.
 - Не удалось взять зону под охрану. Охранный шлейф не задан.
 - Не удалось взять зону под охрану. Считыватель занят.
 - Не удалось взять зону под охрану. Зона уже встаёт под охрану.

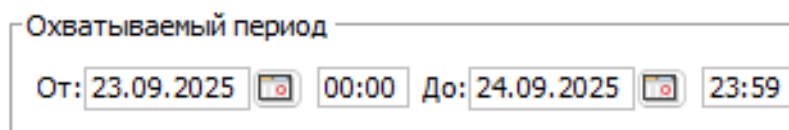
Для поиска нужных событий используются фильтры. Доступны следующие фильтры:

- «Тип события». Фильтрация отображаемых событий по типу. Данный фильтр можно настроить, нажав на кнопку «Выбор типа события».



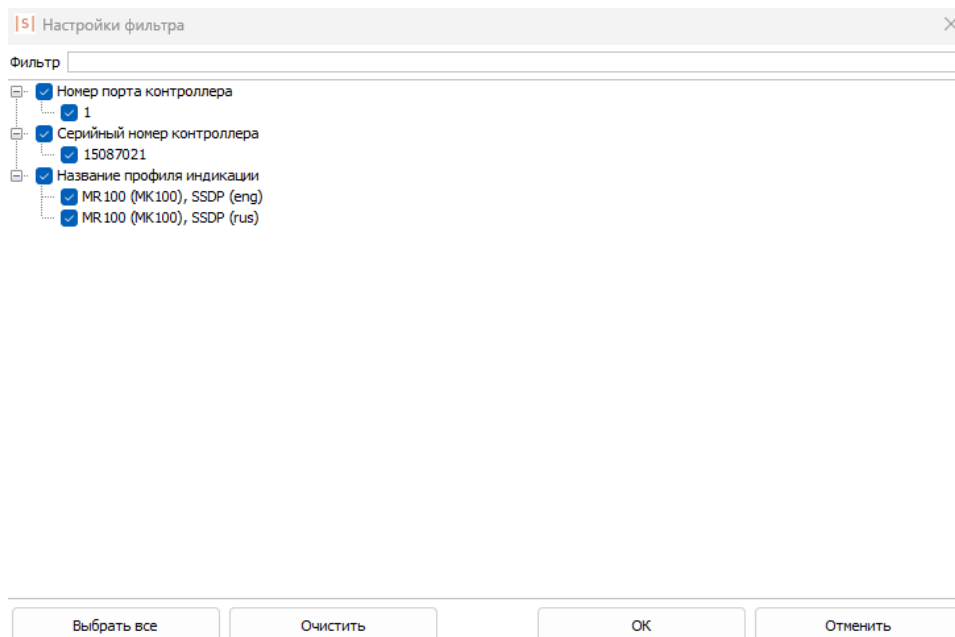
Настройки фильтра по типу события.

- «По дате и времени». С помощью данного фильтра можно отобразить события за нужный период, указав необходимые даты и время в соответствующих полях.



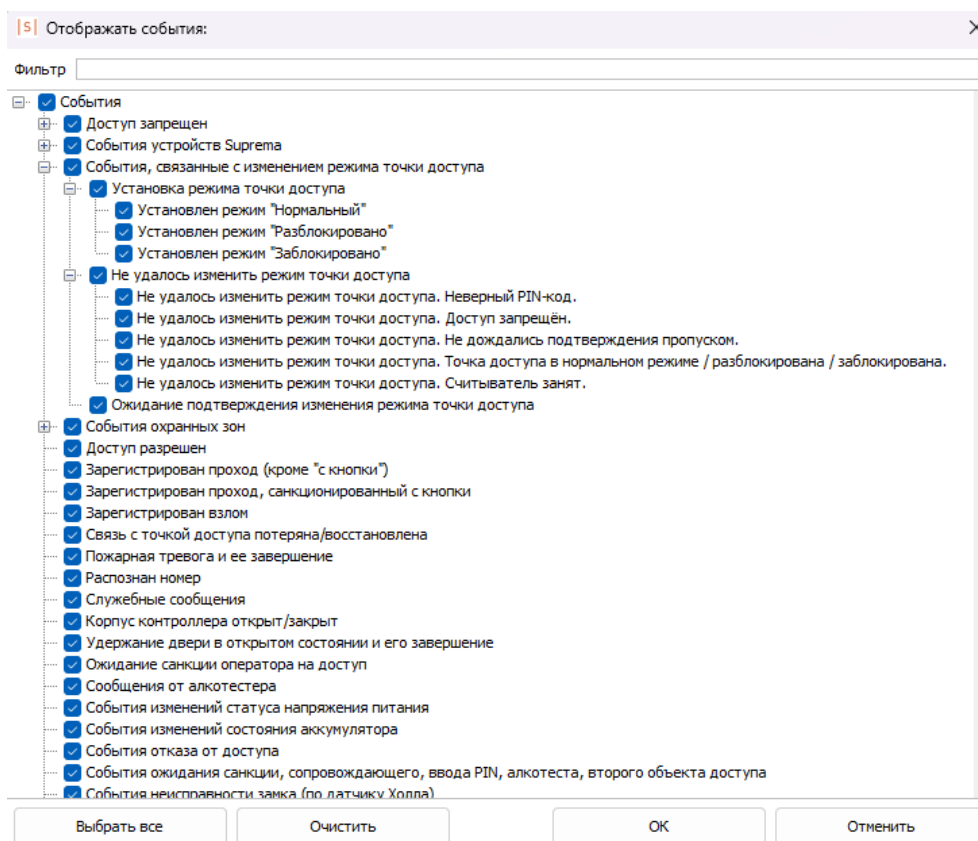
Настройки фильтра по дате и времени.

- «По параметрам». Данный фильтр можно настроить, нажав на кнопку «Отфильтровать отображённые события». С помощью фильтра можно настроить отображение событий по таким параметрам, как:
 - номер порта контроллера;
 - серийный номер контроллера;
 - название профиля индикации.



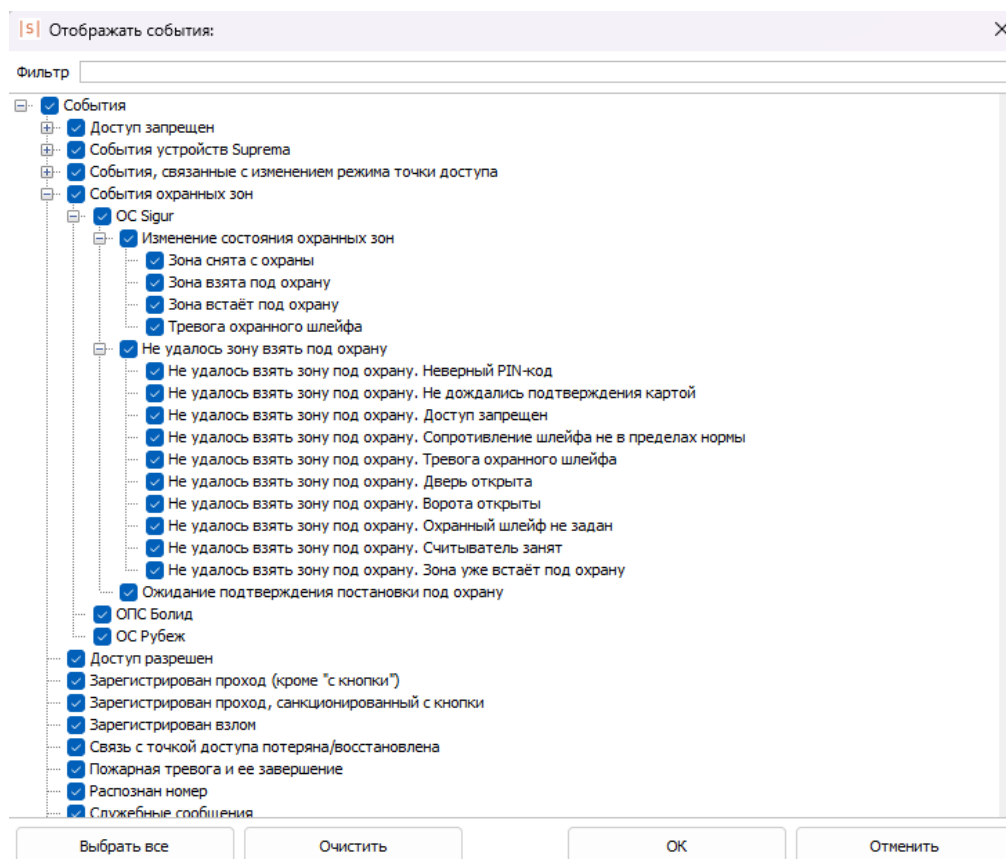
Настройки фильтра по параметрам.

- «События, связанные с изменением режима точки доступа». Фильтр позволяет отображать успешные и неуспешные изменения режима точки доступа.



События, связанные с изменением режима точки доступа.

- «События охранных зон». Фильтрация событий охраны, с помощью фильтра можно настроить отображение событий изменения состояния охранных зон или неуспешных взятий зон под охрану.



События охранных зон.

25. Логика обработки идентификаторов

25.1. Чтение карты

После поднесения карты поддерживаемого формата к включённому считывателю в область его чтения:

- Считыватель определяет формат поднесенной карты.
- В зависимости от заранее загруженной на считыватель конфигурации, определяет режим чтения карты по её типу: «Защищённый», «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 выходной интерфейс не передаются никакие данные.
- 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 защищённой 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: отсутствует какая-либо индикация считывателя, на выходной интерфейс не передаются никакие данные.
- После успешного чтения код карты передаётся на выходной интерфейс считывателя. В качестве кода передаётся:
 - Для всех карт, кроме EM Marine и HID ProxCard II – N байт, определенных конфигурацией считывателя в прямом порядке: Wiegand-26 – 3 байта, Wiegand-34 – 4 байта, Wiegand-58 – 7 байт. В случае защищённого режима – это первые N байт блока памяти карты, без смещений. Если считанный код содержит меньше информации, чем определённая разрядность Wiegand, то код дополняется ведущими нулями. В случае идентификаторов Mifare Classic и Mifare Plus порядок следования байт зависит от настроек конфигурации, загруженной на считыватель.
 - Для карт EM Marine и HID ProxCard II – 3 байта. Если конфигурацией определена передача фиксированного facility-кода, то правый байт заменяется на заданное в конфигурации значение.

25.2. Чтение смартфона

- Если приложение «Sigur Доступ» запущено, ему предоставлены соответствующие права и на смартфоне включены функции Bluetooth и «Определение местоположения», то приложение пытается обнаружить считыватели Sigur, поддерживающие данный функционал.

- Если в результате сканирования было найдено несколько считывателей, то с каждым из них последовательно выполняются следующие операции:
 - Со считывателя приложение получает данные о его настройках:
 - Включён ли на считывателе режим чтения смартфонов.
 - Установленная дальность чтения смартфонов.
 - Политика срабатывания («Когда приложение на экране», «Приложение в фоне, экран разблокирован» или «Всегда»).
 - Режим чтения смартфонов: «Не использовать», «Базовый» или «Пользовательский».
 - Уникальная информация 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».
 - Состояние приложения и смартфона соответствуют политике срабатывания, установленной настройками считывателя (приложение в фоне, экран разблокирован и т. п.).
 - В случае BLE-идентификации:
 - В приложении «Sigur Доступ» включён режим Bluetooth-идентификации.
 - Показания мощности сигнала на антенне смартфона, наводимой сигналом с данного считывателя, больше по номинальной величине значения, установленного настройками считывателя (отрицательные значения dBm).
 - 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.
 - В случае НСЕ-идентификации:
 - В приложении «Sigur Доступ» включён режим NFC-идентификации.
 - NFC-модуль устройства был обнаружен считывателем.

- 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 «Sigur Доступ». Если какое-либо условие не выполняется, код не передаётся на считыватель.
- После получения считывателем идентификатора смартфона его код передаётся на выходной интерфейс считывателя. В качестве кода передаётся N байт, определённых конфигурацией считывателя: Wiegand-26 – 3 байта, Wiegand-34 – 4 байта, Wiegand-58 – 7 байт.

25.3. Чтение PIN-кода

После начала ввода PIN-кода на кодонаборной панели включённого считывателя:

- Считыватель определяет режим в котором он находится.
- В зависимости от предварительной настройки, считыватель определяет какая функция назначена на основной и дополнительный режимы работы.
- Считыватель выбирает формат посимвольной передачи PIN-кода в зависимости от назначенной функции:
 - при подключении по интерфейсу Wiegand для прохода через точку доступа используется Wiegand-6, расшифровка данной кодировки представлена ниже. Если считыватель подключён по OSDP, используется стандартная функция osdp_KEYPAD.
 - при подключении по интерфейсу Wiegand для управления охранными зонами и режимом точки доступа формируется посылка в вендор-специфичном формате, поддерживаемом только контроллерами Sigur.
При подключении по SSDP используется вендор-специфичная функция, обеспечивающая передачу тех же команд управления через протокол SSDP.

Кодировка символов кодонаборного считывателя в формате Wiegand-6 (6 бит на нажатие кнопки).

Символ	Код	Символ	Код
0	0 0000 1	6	1 0110 0
1	0 0001 0	7	1 0111 1
2	0 0010 0	8	1 1000 1
3	0 0011 1	9	1 1001 0
4	1 0100 1	X	1 1010 0
5	1 0101 0	✓	1 1011 1

Логика работы системы Sigur при использовании PIN-кодов в качестве идентификаторов.

1. Результат проверки количества введённых символов.

Контроллер проверяет, совпадает ли введённое количество символов с размером буфера накопления нажатий PIN-кода идентификации и верификации, установленным в настройках в ПО «Клиент».

- Если количество введённых символов меньше 4, по истечению тайм-аута (5 секунд) буфер будет сброшен, индикация считывателя изменится на индикацию по умолчанию, состояние точки доступа не изменяется.
- Если количество символов меньше размера буфера, но введено не менее четырёх символов, то при нажатии кнопки «Ввод» или по истечении тайм-аута (5 секунд) считыватель передаёт код на контроллер, и тот, в свою очередь, проверяет наличие PIN-кода в автономной памяти или в базе данных сервера.
- Если количество введённых символов совпадает с размером буфера, считыватель сразу после ввода последнего символа передаёт код на контроллер, без необходимости нажимать кнопку «Ввод» или ждать истечения тайм-аута. Контроллер проверяет наличие PIN-кода в автономной памяти или в базе данных сервера.

2. Результат проверки наличия PIN-кода в базе системы.

- Если PIN-код не прошёл проверку, контроллер генерирует событие «Доступ запрещён. Введён неверный PIN-код» и активирует соответствующую индикацию считывателя, состояние точки доступа не изменяется.
- Если PIN-код прошёл проверку, система переходит к проверке валидности PIN-кода.

3. **Результат проверки валидности PIN-кода.** Валидным считается такой PIN-код, для которого не установлены причины отказа в доступе (не регистрируется событие «Доступ запрещён»), не истёк срок его действия, предоставлен доступ к нужной точке доступа, и срок этого доступа также актуален.
- Если PIN-код не прошёл проверку, контроллер генерирует событие «Доступ запрещён. [Указание причины]» и активирует соответствующую индикацию считывателя, состояние точки доступа не изменяется.
 - Если PIN-код прошёл проверку, контроллер генерирует событие «Доступ разрешён» и активирует соответствующую индикацию считывателя, точка доступа разблокируется для совершения однократного прохода.

26. Логика работы системы Sigur при выполнении расширенных функций считывателя

26.1. Логика работы системы при постановке зоны на охрану с помощью PIN-кода

1. Активация функции постановки зоны на охрану.

- Если функция назначена на основной режим работы, пользователь сразу вводит специальный PIN-код.
- Если функция управления охранными зонами настроена на дополнительный режим, необходимо активировать его удержанием кнопки «Ввод» на панели. Это сопровождается индикацией перехода в дополнительный режим.

2. Ввод специального PIN-кода.

- Если пользователь не ввёл PIN-код, по истечению тайм-аута считыватель перейдёт в основной режим работы, индикация считывателя изменится на индикацию по умолчанию.
- Если пользователь ввёл неверный PIN-код, контроллер генерирует событие «Не удалось взять зону под охрану. Неверный PIN-код» и активирует соответствующую индикацию считывателя. После этого считыватель переходит в основной режим работы.
- Если пользователь ввёл верный PIN-код, система переходит к проверке состояния зоны.

3. Результат проверки состояния зоны.

- Если состояние зоны «В тревоге» — контроллер генерирует событие «Не удалось взять зону под охрану. Тревога охранного шлейфа» и активирует соответствующую индикацию считывателя, происходит возврат в основной режим работы.
- Если состояние зоны «На охране» — контроллер генерирует событие «Зона взята под охрану» и активирует соответствующую индикацию считывателя, происходит возврат в основной режим работы.

4. Ожидание подтверждения постановки зоны на охрану. Если требуется подтверждение постановки на охрану пропуском, система переходит в режим ожидания — контроллер генерирует событие «Ожидание подтверждения постановки зоны под охрану» и активирует

соответствующую индикацию считывателя.

- Если пользователь не успел приложить пропуск в оставшийся тайм-аут (10 секунд), контроллер генерирует событие «Не удалось взять зону под охрану. Не дождался подтверждения пропуском» и активирует соответствующую индикацию считывателя. После этого считыватель переходит в основной режим работы.
- Если пользователь приложил пропуск в оставшийся тайм-аут, система переходит к проверке валидности пропуска.

5. **Результат проверки валидности пропуска.** Валидным считается такой пропуск, для которого не установлены причины отказа в доступе (не регистрируется событие «Доступ запрещён»), не истёк срок его действия, предоставлен доступ к нужной точке доступа, и срок этого доступа также актуален.

- Если пропуск не валиден, контроллер генерирует событие «Доступ запрещён. [Указание причины]» и «Не удалось взять зону под охрану. Доступ запрещён», активирует соответствующую индикацию считывателя, считыватель переходит в основной режим работы.
- Если пропуск валиден, система переходит к проверке направления считывателя, к которому приложен пропуск.

6. **Результат проверки направления считывателя, к которому приложен пропуск. Пропуск приложен к считывателю в направлении «На выход».** Иницируется проверка всех специальных правил доступа сотрудника согласно режиму (если таковые есть):

- Если проверка прошла успешно — контроллер генерирует событие «Доступ разрешён» и активирует соответствующую индикацию считывателя, происходит разблокировка точки доступа, активируется задержка постановки зоны на охрану.
- Если хотя бы одно спец. правило не прошло проверку — контроллер генерирует событие «Доступ запрещён. [Указание причины]» и «Не удалось взять зону под охрану. Доступ запрещён», активирует соответствующую индикацию считывателя. Считыватель переходит в основной режим работы.

7. **Результат проверки направления считывателя, к которому приложен пропуск. Пропуск приложен к считывателю в направлении «На вход» или «Неизвестно».** Точка доступа не разблокируется, проверка специальных правил не производится. Иницируется проверка поля «Задержка постановки зоны на охрану».

8. Результат проверки поля «Задержка постановки зоны на охрану»

- Если значение 0 мс, система предпринимает попытку поставить зону на охрану.
- Если значение больше 0 мс — контроллер генерирует событие «Зона встаёт под охрану» и активирует соответствующую индикацию считывателя. Задержка длится согласно заданному в ПО «Клиент» значению.

9. Попытка системы поставить зону на охрану. Система проверяет состояние датчиков охранного шлейфа и состояние геркона/датчика закрытого положения, если они настроены для точки доступа.

- Если датчик охранного шлейфа в состоянии тревога и/или геркон/датчик закрытого положения нормально разомкнут (т.е. дверь/ворота открыты) — контроллер генерирует событие «Не удалось взять зону под охрану. Сопротивление шлейфа не в пределах нормы» и/или «Не удалось взять зону под охрану. Дверь/ворота открыты», активирует соответствующую индикацию считывателя. После этого считыватель переходит в основной режим работы.
- Если датчик охранного шлейфа в нормальном состоянии и геркон/датчик закрытого положения нормально замкнут (т.е. дверь/ворота закрыты) — контроллер генерирует событие «Зона взята под охрану», и активирует соответствующую индикацию считывателя. После этого считыватель переходит в основной режим работы.

Проход в зону, находящуюся в процессе постановки на охрану.

1. Попытка прохода в зону, находящуюся в процессе постановки на охрану, в направлении «на вход».

- Если сотрудник подносит валидный пропуск к считывателю в направлении «на вход», постановка на охрану прерывается, контроллер генерирует событие «Доступ разрешён», активирует соответствующую индикацию считывателя, точка доступа разблокируется. Вне зависимости от того, зафиксирован факт прохода или нет, система не инициирует повторную постановку зоны на охрану.
- Если сотрудник подносит невалидный пропуск к считывателю в направлении «на вход», постановка на охрану не прерывается, контроллер генерирует событие «Доступ запрещён. Причина», активирует соответствующую индикацию считывателя, точка доступа не разблокируется.

2. **Попытка прохода в зону, находящуюся в процессе постановки на охрану, в направлении «на выход» или «неизвестно».**

- Если сотрудник подносит валидный пропуск к считывателю в направлении «на выход» или «неизвестно», постановка на охрану не прерывается, контроллер генерирует событие «Доступ разрешён», активирует соответствующую индикацию считывателя, точка доступа разблокируется.
- Если сотрудник подносит невалидный пропуск к считывателю в направлении «на выход» или «неизвестно», постановка на охрану не прерывается, контроллер генерирует событие «Доступ запрещён. Причина», активирует соответствующую индикацию считывателя, точка доступа не разблокируется.

26.2. **Логика работы системы при снятии зоны с охраны при проходе через точку доступа**

1. **Инициация снятия с охраны.** Пользователь проходит идентификацию на считывателе любым доступным способом (например, по карте, PIN-коду идентификации или карта + PIN-код верификации). После этого система начинает проверку прав доступа.
2. **Результат проверки прав доступа.**
 - Если пропуск не валиден — контроллер генерирует событие «Доступ запрещён. [Указание причины]» и активирует соответствующую индикацию считывателя. Зона с охраны не снимается.
 - Если пропуск валиден, система переходит к проверке геркона/датчика открытия точки доступа.
3. **Результат проверки геркона / датчика открытия точки доступа.**
 - Если геркон/датчик открытия не подключён и/или не настроен — контроллер генерирует событие «Зона снята с охраны» и «Зарегистрирован проход» и активирует соответствующую индикацию считывателя, происходит снятие зоны с охраны и разблокировка точки доступа.
 - Если геркон/датчик открытия подключен и настроен — контроллер генерирует событие «Зона снята с охраны» и «Доступ разрешён» и активирует соответствующую индикацию считывателя, происходит снятие зоны с охраны и разблокировка точки доступа. После этого система ожидает факт прохода через точку доступа для завершения процедуры снятия с охраны.

4. Ожидание прохода.

- Если проход совершён — контроллер генерирует событие «Зарегистрирован проход».
- Если проход не совершён — контроллер генерирует событие «Проход не совершён. Истёк тайм-аут ожидания прохода», система переходит к проверке состояния датчиков охранного шлейфа.

5. Результат проверки состояния датчиков охранного шлейфа.

- Если датчики охранного шлейфа неактивны — контроллер снова ставит зону на охрану, генерирует событие «Зона взята под охрану» и активирует соответствующую индикацию считывателя.
- Если датчики охранного шлейфа активны — контроллер генерирует событие «Тревога охранного шлейфа» и активирует соответствующую индикацию считывателя.

26.3. Логика работы системы при изменении режима точки доступа

1. Активация функции изменения режима точки доступа.

- Если функция назначена на основной режим работы, пользователь сразу вводит специальный PIN-код.
- Если функция управления охранными зонами настроена на дополнительный режим, необходимо активировать его удержанием кнопки «Ввод» на панели. Это сопровождается индикацией перехода в дополнительный режим.

2. Ввод специального PIN-кода.

- Если пользователь не ввёл PIN-код, по истечению тайм-аута считыватель перейдёт в основной режим работы, индикация считывателя изменится на индикацию по умолчанию.
- Если пользователь ввёл неверный PIN-код, контроллер генерирует событие «Не удалось сменить режим точки доступа. Неверный PIN-код» и активирует соответствующую индикацию считывателя. После этого считыватель переходит в основной режим работы.
- Если пользователь ввёл верный PIN-код, система переходит к проверке текущего режима точки доступа.

3. **Проверка текущего режима точки доступа.** Проверяется наличие у сотрудника правила на изменение текущего режима данной точки доступа.
 - Если сотрудник не может изменять текущий режим ТД — контроллер генерирует событие «Не удалось сменить режим точки доступа. Точка доступа [текущее состояние ТД]» и активирует соответствующую индикацию считывателя, происходит возврат в основной режим работы. Режим точки доступа не изменяется.
 - Если сотрудник может изменять текущий режим ТД, система переходит к проверке прав доступа пользователя на данную ТД в момент ввода PIN-кода.
4. **Проверка прав доступа пользователя.** Проверяется доступ на ТД, временные интервалы из режимов. При проверке система не учитывает специальные логики доступа (проход вдвоём, верификация лица и другие проверки согласно специальным правилам режимов).
 - Если у пользователя недостаточно прав доступа, контроллер генерирует событие «Не удалось сменить режим точки доступа. Доступ запрещён» и активирует соответствующую индикацию считывателя, происходит возврат в основной режим работы. Режим точки доступа не изменяется.
 - Если у пользователя есть права доступа на данную ТД, система переходит к проверке способа изменения режима точки доступа.
5. **Проверка способа изменения режима точки доступа.** Определяется, какой способ изменения режима (PIN или PIN+пропуск) задан в правилах изменения режима данной точки доступа.
 - Если для изменения режима требуется только специальный PIN, контроллер генерирует событие «Установлен режим [название режима] (ввод PIN-кода, был [название предыдущего режима ТД])» и активирует соответствующую индикацию считывателя. После этого считыватель переходит в основной режим работы.
 - Если для изменения режима требуется подтверждение пропуском, система переходит в режим ожидания подтверждения изменения режима.

6. Ожидание подтверждения изменения режима точки доступа.

Контроллер генерирует событие «Ожидание подтверждения смены режима точки доступа» и активирует соответствующую индикацию считывателя.

- Если пользователь не успел приложить пропуск в оставшийся тайм-аут (10 секунд), контроллер генерирует событие «Не удалось сменить режим точки доступа. Не дождался подтверждения пропуском» и активирует соответствующую индикацию считывателя. После этого считыватель переходит в основной режим работы.
- Если пользователь приложил пропуск в оставшийся тайм-аут (10 секунд), система переходит к проверке валидности пропуска.

7. Результат проверки валидности пропуска. Валидным считается такой пропуск, который принадлежит тому же объекту доступа (пользователю), который ранее вводил PIN-код. Также для пропуска не должны быть установлены причины отказа в доступе (не регистрируется событие «Доступ запрещён»), не истёк срок его действия, предоставлен доступ к нужной точке доступа, и срок этого доступа также актуален.

- Если пропуск не валиден, контроллер генерирует событие «Доступ запрещён. Ожидается подтверждение изменения режима точки доступа», активирует соответствующую индикацию считывателя. Контроллер продолжает ожидать подтверждение изменения режима точки доступа пропуском (см. пункт 5 данного раздела). Тайм-аут при этом не обновляется.
- Если пропуск валиден, контроллер генерирует событие «Установлен режим [название режима] (ввод PIN-кода с подтверждением пропуском, был [название предыдущего режима ТД])» и активирует соответствующую индикацию считывателя, происходит возврат в основной режим работы.

27. 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;
- загрузка на считыватель файла конфигурации чтения идентификаторов;
- загрузка на считыватель файла конфигурации индикации.

27.1. 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 блока «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.
- Тип защищённого соединения – позволяет выбрать тип криптографического протокола для обеспечения более безопасной связи. Соединение с SMTP-сервером шифруется для обеспечения более безопасной связи. Выберите опцию SSL для сервисов, где соединение для портов защищено изначально (Mail.ru, Gmail и др.), а опцию STARTTLS – для сервисов, где защита соединения устанавливается в процессе работы (Outlook (Hotmail), Exchange серверы и др.).

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

Если настройки были указаны верно, то вы увидите сообщение «Письмо успешно отправлено». Убедитесь в факте его получения на указанном вами почтовом ящике.

27.2. 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.

- «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.

Редктирование настроек

Наблюдение	Почтовый сервер для отправки исходящих писем:
Видеонаблюдение	Адрес SMTP сервера: smtp.gmail.com
E-Mail	Порт SMTP сервера: 465
Персонал	От кого: test.sigur.stand@gmail.com
Бесконтактная идентификация	☒ Использовать аутентификацию:
Биометрика	SMTP логин: test.sigur.stand@gmail.com
Распознавание лиц	SMTP пароль: ●●●●●●●●
Active Directory	Тип защищенного соединения: SSL
Архив	
Беспроводные замки	Сохранить параметры отправки e-mail и протестировать
Устройства хранения	
Зоны	Почтовый сервер для получения входящих писем:
Повторные проходы	Сервер: imap.gmail.com
Дополнительные параметры	Порт: 993
HTTP(WEB)	Протокол: IMAP
WEB-делегирование	Логин: test.sigur.stand@gmail.com
Права операторов	Пароль: ●●●●●●●●
Профили шифрования OSDP	E-mail: test.sigur.stand@gmail.com
Индикация	☒ Использовать SSL
Профили шифрования	
Документы	

Окно настройки параметров почтовых серверов.

28. Контакты

ООО «Промышленная автоматика – контроль доступа»
Адрес: 603001, Нижний Новгород, ул. Керченская, д. 13, 4 этаж.

Система контроля и управления доступом «Sigur»

Сайт: www.sigur.com

По общим вопросам: info@sigur.com

Техническая поддержка: support@sigur.com

Телефон: +7 (800) 700 31 83, +7 (495) 665 30 48, +7 (831) 260 12 93