

Группа компаний «ТвинПро»

ООО «ЕС-пром»

**Система контроля и управления доступом большой ёмкости
с функциями охранной сигнализации Elsys**

**ПРИЛОЖЕНИЕ ДЛЯ НАСТРОЙКИ МУЛЬТИФОРМАТНЫХ
СЧИТЫВАТЕЛЕЙ
ELSYS-SW CONFIG
РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**

СОДЕРЖАНИЕ

1	Описание и работа приложения.....	3
1.1	Назначение приложения	3
1.2	Функциональные возможности.....	3
1.3	Особенности версий	4
1.3.1	Версия 1.06.....	4
1.3.2	Версия 1.08.....	5
1.4	Работа приложения.....	5
1.4.1	Главный экран.....	5
1.4.2	Экран поиска считывателей	6
1.4.3	Экран меню считывателя.....	8
1.4.4	Экран настроек считывателя.....	9
1.4.5	Экран ручного ввода параметров безопасности	20
1.4.6	Экран обновления прошивки	28
1.4.7	Экран списка шаблонов	29
1.4.8	Экран редактирования параметров безопасности.....	32
1.5	Требования приложения	34
ПРИЛОЖЕНИЕ А Пример настройки выходной последовательности байт		35

Настоящее руководство пользователя распространяется на приложение Elsys-SW Config (далее – приложение) версии 1.06 и старше, предназначенное для настройки считывателей Elsys-SW с поддержкой BLE.

В настоящем руководстве приняты следующие сокращения и обозначения:

BLE – Bluetooth Low Energy.

Версия настоящего документа – 1.6 (07.2025).

1 Описание и работа приложения

1.1 Назначение приложения

Приложение используется для настройки считывателей Elsys-SW18-MF, Elsys-SW-USB-Multi, Elsys-SW78-Multi, Elsys-SW78-KP-Multi и других совместимых устройств по интерфейсу Bluetooth Low Energy.

Elsys-SW Config доступно для установки из RuStore, HUAWEI AppGallery, Google Play на мобильные устройства под управлением Android версии 5.0 и старше с поддержкой BLE.

1.2 Функциональные возможности

Приложение обеспечивает следующие функциональные возможности:

- поиск считывателей Elsys-SW с поддержкой BLE;
- подключение к считывателю с использованием PIN-кода;
- вычитывание и редактирование конфигурации считывателя;
- перезагрузку считывателя;
- сброс считывателя к заводским настройкам;
- обновление прошивки считывателя;
- автономное создание, редактирование, хранение шаблонов конфигураций и загрузку их в считыватели.

1.3 Особенности версий

1.3.1 *Версия 1.06*

Новые функции приложения версии 1.06 доступны при подключении к считывателям версий:

- Elsys-SW18-MF с версией прошивки 1.15 и старше;
- Elsys-SW78-Multi с версией прошивки 1.10 и старше;
- Elsys-SW-USB-Multi с версией прошивки 1.06 и старше;
- Elsys-SW78-KP-Multi с версией прошивки 1.01 и старше.

Для повышения безопасности при использовании защищенных режимов карт Mifare и для повышения общей безопасности СКУД Elsys конфигурация мультиформатных считывателей была разделена на две части: общие настройки и параметры безопасности. В указанных выше версиях прошивок считывателей выгрузка и редактирование параметров безопасности невозможна. Доступна только запись параметров безопасностей, таких как PIN-код и настройки защищенных режимов Mifare. Для этого добавлен новый экран «Параметры безопасности» для ручного ввода настроек при подключении к считывателю, и для создания и редактирования файлов с параметрами с шифрованием AES-256 с ключом на основе пароля. Так же была добавлена функция сохранения настроек из шаблона в файл.

Таким образом, чтобы повысить уровень безопасности хранения ключей mifare, необходимо обновить приложение до версии 1.06 и прошивки считывателей до версий, указанных выше. Так же необходимо сохранить настройки и параметры безопасности в файлы из пользовательских шаблонов (два отдельных действия), после чего их следует удалить.

Как упомянуто выше, в версии 1.06 добавлена возможность создания файла с настройками. Можно создать файл с настройками из шаблона и добавить в него параметры безопасности с одним паролем, либо создать отдельный файл с параметрами безопасности с другим паролем. На каждый параметр безопасности может быть создан отдельный файл либо они могут быть объединены в один. При подключении к считывателю в него можно загрузить настройки из файла.

ВНИМАНИЕ! Если в системе используется защищенный режим *mifare*, то после обновления прошивок считывателей до актуальных, извлечь параметры безопасности из устройства будет невозможно. Перед переходом на новые версии убедитесь, что параметры безопасности системы сохранены. Либо заранее создайте новый шаблон при подключении к считывателю, из которого в дальнейшем можно будет выгрузить в файл параметры безопасности.

1.3.2 Версия 1.08

Новые функции приложения версии 1.08 доступны при подключении к считывателям версий:

- Elsys-SW18-MF с версией прошивки 1.17 и старше;
- Elsys-SW78-Multi с версией прошивки 1.12 и старше;
- Elsys-SW-USB-Multi с версией прошивки 1.08 и старше;
- Elsys-SW78-KP-Multi с версией прошивки 1.02 и старше.

В данной версии были добавлены настройки отключения способов конфигурирования и времени ожидания ответов от карт Mifare Plus и DESFire. Правильное использование этих настроек повышает безопасность системы.

Добавлены дополнительные параметры для профилей безопасности карт Mifare Classic и Mifare Plus, в том числе тип ключа.

Добавлено отображение доступности конфигурации при поиске.

Добавлено скрывание недоступных функций при подключении к считывателю после авторизации с помощью мастер-карты.

Добавлена возможность сохранения параметров в файле в формате для загрузки в мастер-карту.

1.4 Работа приложения

1.4.1 Главный экран

При запуске приложения отображается экран со списком доступных операций (Рисунок 1).

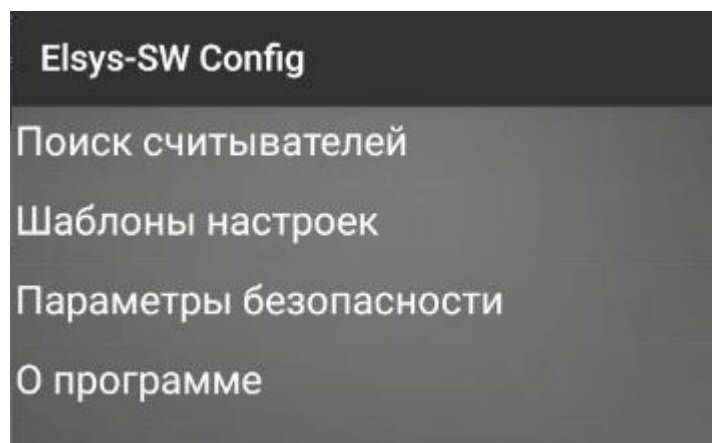


Рисунок 1 – Экран выбора функции.

На экране меню доступны следующие функции:

- «Поиск считывателей» - открывает экран поиска считывателей;
- «Шаблоны настроек» - открывает список шаблонов конфигураций;
- «Параметры безопасности» - открывает окно редактирования файлов параметров безопасности;
- «О программе» - открывает экран с версией программы.

1.4.2 Экран поиска считывателей

При открытии экрана поиска считывателей автоматически начинается поиск и найденные устройства будут отображаться в виде списка (Рисунок 2). Элемент списка содержит имя найденного считывателя (1) и заводской номер (2).

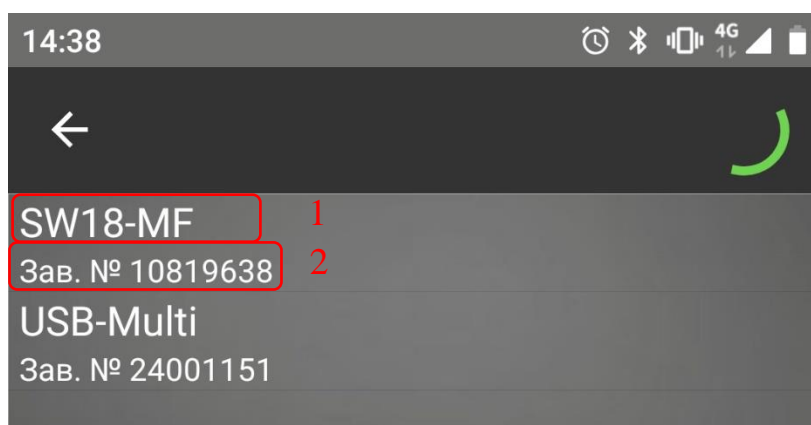


Рисунок 2 – Экран поиска считывателей.

Если у считывателя активен металлодетектор, то он будет выделяться в списке найденных устройств (Рисунок 3).

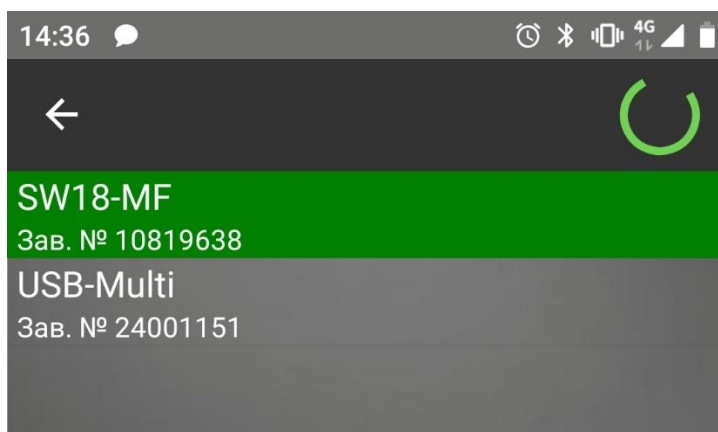


Рисунок 3 – Список найденных устройств со считывателем, у которого активен металлодетектор.

Если в считывателе отключена возможность конфигурирования с помощью Elsys-SW Config, то он будет отображаться в поиске с соответствующей пометкой (Рисунок 4).

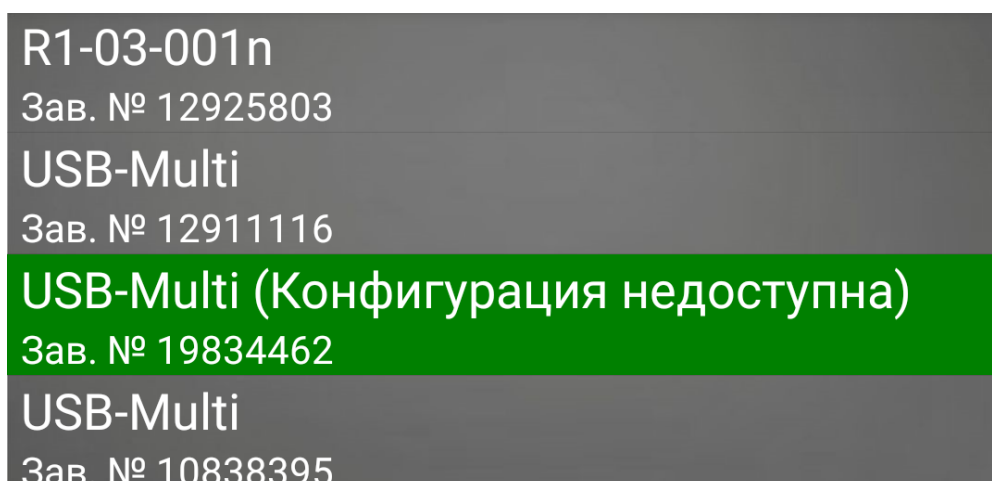


Рисунок 4 – Считыватель с недоступной конфигурацией.

Для подключения к считывателю необходимо нажать на найденное устройство. Во время установки подключения появляется системное окно сопряжения с устройством (Рисунок 5), после успешного ввода PIN-кода (по умолчанию «123456») отобразится экран функций считывателя (пункт 1.4.3). Вид системного окна может отличаться в зависимости от версии Android.

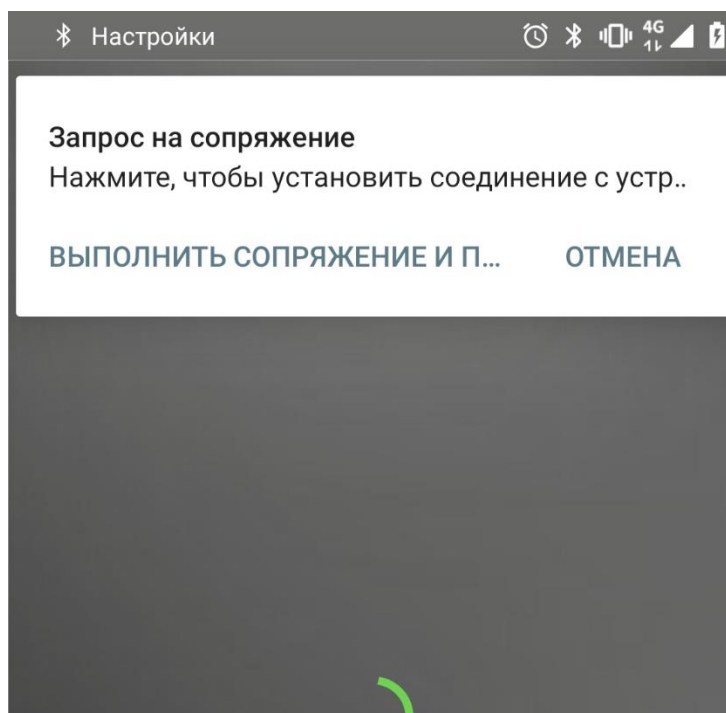


Рисунок 5 – Системное окно запроса на сопряжение с устройством.

Обновить список найденных считывателей можно выполнив жест «свайп сверху» или, если поиск устройств остановлен, то нажатием кнопки «Поиск», расположенной в правом верхнем углу экрана.

1.4.3 Экран меню считывателя

Меню считывателя (Рисунок 6) отображается после успешного подключения к устройству. На странице отображаются следующие опции:

- «Настройки считывателя» - открывает экран с вычитанной конфигурацией считывателя с возможностью редактирования и сохранения;
- «Параметры безопасности» - открывается экран для ввода параметров безопасности вручную;
- «Загрузить настройки из шаблона» - открывает страницу с выбором шаблона конфигурации, который будет загружен в считыватель;
- «Сохранить настройки как шаблон» - создаёт новый шаблон на основе конфигурации подключенного считывателя;
- «Загрузить настройки из файла» - применяет к считывателю настройки из файла;
- «Перезагрузить считыватель» - выполняет программный сброс считывателя, при этом соединение разрывается;

- «Очистить конфигурацию» - устанавливает заводские настройки считывателя, при этом соединение сохраняется;
- «Обновить прошивку» - открывает экран обновления прошивки.

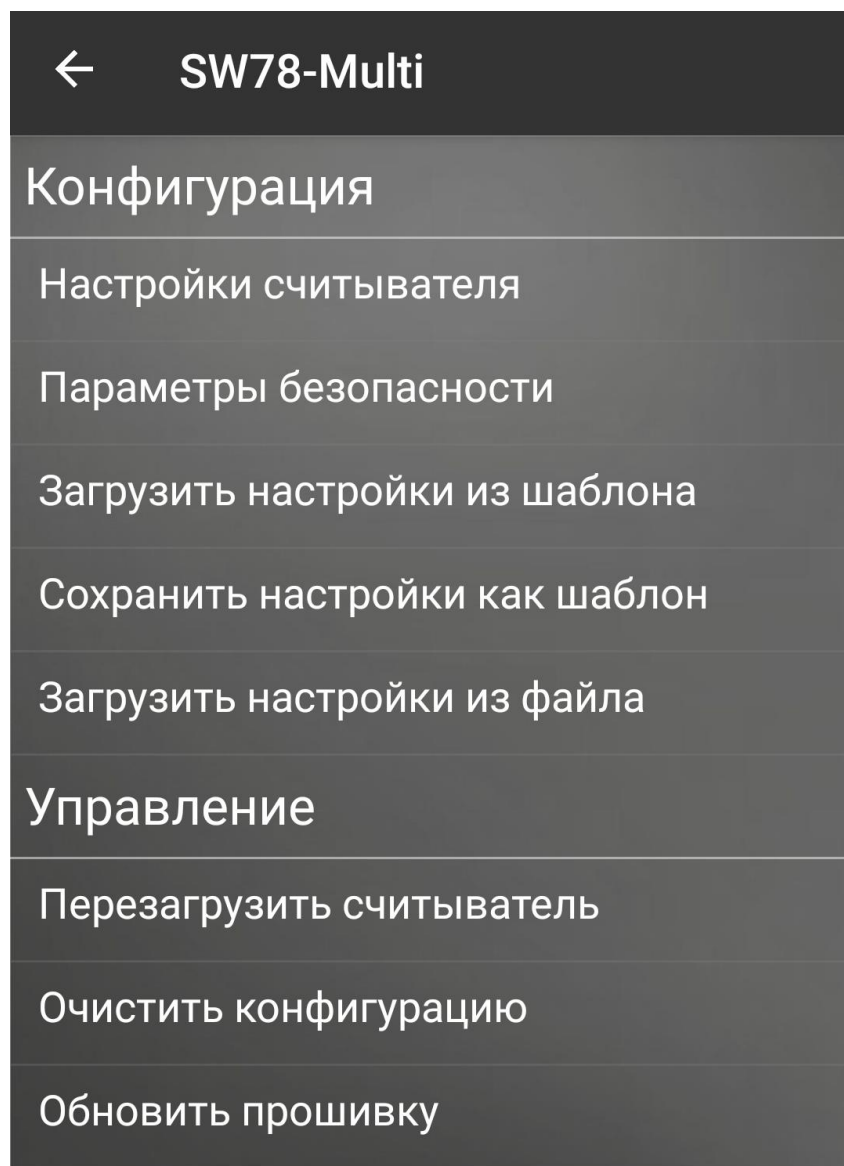


Рисунок 6 – Меню считывателя.

Если была выполнена авторизация доступа с помощью мастер-карты, то будут отображаться только разрешенные мастер-картой опции.

1.4.4 Экран настроек считывателя

Страница отображается при выборе функции «Настройка считывателя» и содержит вычитанную конфигурацию с возможностью редактирования. Для сохранения изменений необходимо нажать на «Сохранить».

Настройки, помеченные как «параметр безопасности», не отображаются в настройках считывателя с актуальными прошивками. В последних версиях

прошивок они не могут быть вычитаны из считывателя и должны применяться к считывателю на экране «Параметры безопасности» при подключении или загружаться в считыватель из файла функцией «Загрузить настройки из файла».

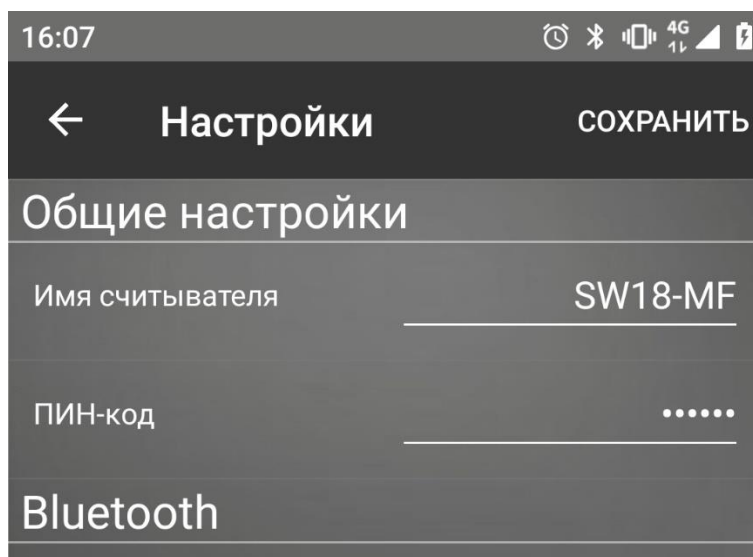


Рисунок 7 – Настройки считывателя.

В зависимости от типа считывателя настенный (Elsys-SW18-MF, Elsys-SW78-Multi) или настольный (Elsys-SW-USB-Multi) будет отличаться набор доступных настроек. Для настенных считывателей доступны: основные настройки, расширенные настройки. Для настольных считывателей доступны: основные настройки за исключением настроек индикации, расширенные настройки, настройка выдачи карт.

1.4.4.1 Основные настройки

1. «Общие настройки» (Рисунок 8):

- «Имя считывателя» - задаёт название считывателя, которое будет отображаться при поиске.

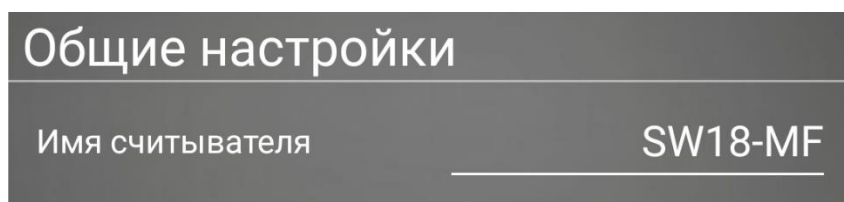


Рисунок 8 – Общие настройки.

2. «Bluetooth» (Рисунок 9):

- «Мощность передатчика» – задаёт значение мощности передатчика считывателя, выбираемого из списка 0 – 6дБм, при

больших значениях увеличивается дальность работы, но при этом повышается ток потребления (по умолчанию 4дБм);

- «Детектор приближения» – при включении настройки считыватель будет использовать детектор металлических объектов, и идентификация приложением Elsys-SW ID в фоновом режиме будет возможна только при попадании телефона в зону его обнаружения (по умолчанию включена).

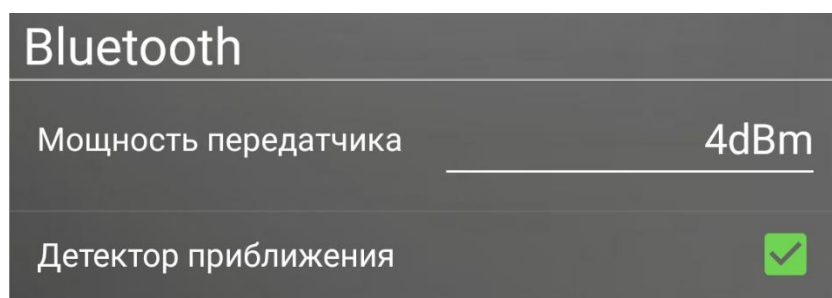


Рисунок 9 – Настройки Bluetooth.

3. «Выходной интерфейс» (Рисунок 10):

- «Интерфейс Wiegand» – выбор формата Wiegand из предустановленного списка: Wiegand-26, Wiegand-32, Wiegand-33, Wiegand-34, Wiegand-34 HID, Wiegand-37, Wiegand-40, Wiegand-42, Wiegand-44, Wiegand-48, Wiegand-56, Wiegand-58, Wiegand-64 (по умолчанию Wiegand-26), для настольных считывателей задаёт длину выдаваемого кода;
- «Формат Touch Memory» – выбор длины кода 3, 5 или 6 байт, передаваемого по TouchMemory (по умолчанию 6 байт);
- «Адрес ESDP» (только для настенных считывателей) – настройка адреса для протокола ESDP. По умолчанию «Аппаратный», при котором адрес задаётся с помощью выводов считывателя. Адрес соответствует номеру считывателя в контроллере;
- «Скорость обмена» (только для настенных считывателей) – настройка скорости для протокола ESDP. По умолчанию 9600;
- «Формат PIN-кода WG» (только для клавиатурных считывателей) – настройка, задающая формат передачи кода при

подключении считывателя по Wiegand. С установленными настройками «Wiegand-4», «Wiegand-6», «Wiegand-8» считыватель будет передавать код посимвольно. Если установлена настройка «Как карта ...», то считыватель будет передавать введенный код целиком в выбранном формате Wiegand или Touch Memory. По умолчанию «Wiegand-4»;

- «Формат PIN-кода ESDP» (только для клавиатурных считывателей) – настройка, задающая тип передачи кода при подключении считывателя по ESDP. По умолчанию «Одним пакетом».



Рисунок 10 – Настройки выходного интерфейса.

4. «Поддерживаемые идентификаторы» (Рисунок 11) – включает или выключает считывание идентификаторов конкретного типа. По умолчанию все интерфейсы включены для проверки считывания предполагаемых идентификаторов. Отключение неиспользуемых интерфейсов идентификации позволяет уменьшить электропотребление считывателя и защититься от совпадения номеров карт разного типа. Для конфигурирования доступны следующие настройки:

- «EM-Marine» – настройка включает считывание карт EM-Marine;
- «HID ProxCard II» – настройка включает считывание карт HID ProxCard II и ISOProx II;
- «Mifare» – настройка включает считывание UID карт Mifare Classic, Plus, DESfire, Ultralight банковских карт с эмуляцией Mifare;
- «Elsys-SW ID (BLE)» – настройка включает считывание мобильных идентификаторов Elsys-SW ID по интерфейсу Bluetooth;
- «Apple Wallet\Банковские карты» – настройка включает считывание номеров банковских карт, добавленных в платежное приложение Apple Wallet, или банковских карт, которые не имеют статичный UID;
- «Elsys-SW ID (NFC)» – настройка включает считывание мобильного идентификатора Elsys-SW ID по интерфейсу NFC.

Поддерживаемые идентификаторы	
EM-Marine	✓
HID ProxCard II	✓
Mifare	✓
Elsys-SW ID (BLE)	✓
Apple Wallet\Банковские карты	✓
Elsys-SW ID (NFC)	✓

Рисунок 11 – Поддерживаемые идентификаторы.

5. «Настройка индикации» (Рисунок 12) – позволяет выбрать один из девяти цветов (Рисунок 13) свечения многоцветного светодиода при замыкании соответствующих управляющих входов.


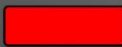

Индикация	
Активен вход LED Green	
Активен вход LED Red	
Активны входы LED Green+LED Red	

Рисунок 12 – Настройка индикации.



Рисунок 13 – Выбор цвета.

1.4.4.2 Расширенные настройки считывателя

1. «Bluetooth» (Рисунок 14):

- «Только из приложения» – при включении настройки, отправка идентификатора будет возможна только при ручном управлении из приложения Elsys-SW ID (по умолчанию выключена);
- «Ограничивать дальность» – при включении настройки, считыватель будет игнорировать запросы подключения устройств, вычисленное расстояние до которых дальше установленного значения, в том числе от приложений Elsys-SW ID, Elsys-SW Config (по умолчанию выключена);
- «Максимальная дальность» – порог ограничения дальности подключения при выключенной настройке «Ограничивать дальность» (измеряется в м, по умолчанию 1м, максимальное значение 15м);

- «Дальность считывания» – регулировка дальности считывания мобильного идентификатора по BLE (по умолчанию в среднем положении).

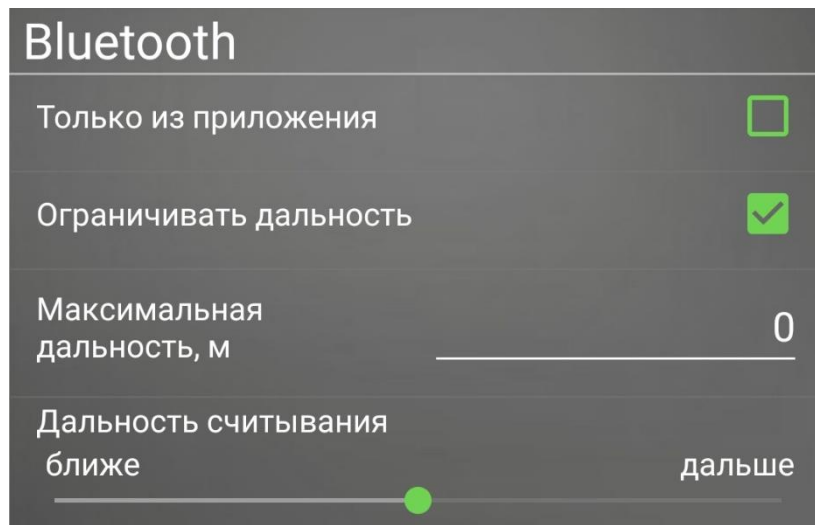


Рисунок 14 – Расширенные настройки Bluetooth.

2. «Выходной интерфейс» (Рисунок 15):

- «Обрезать первый байт Mifare» – если настройка включена, то для карт с длиной UID 7, 10 байт будет происходить обрезка первого байта с кодом производителя (по умолчанию включена);
- «Инверсный порядок байт» – если настройка включена, то направленность последовательности байт выходной посылки изменится на обратную той, что используется в системе Elsys, (по умолчанию выключена), например, с установленной настройкой код 0x665544332211 будет передан: при Wiegand-42 как 0x1122334455, при Wiegand-26 как 0x112233;
- «Выходная последовательность байт» (Рисунок 16) – расширенная настройка формата выходного кода с выбором типа идентификатора к которому применяется (по умолчанию не используется), пример см. приложение А, обрезка первого байта Mifare происходит до применения этой настройки, а обрезка кода под формат Wiegand или TouchMemory и инвертирование порядка байт – после. Настройка рассчитана на опытных пользователей.

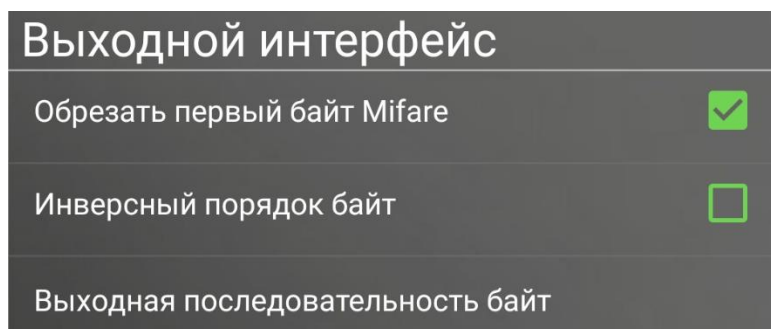


Рисунок 15 – Расширенные настройки выходного интерфейса.

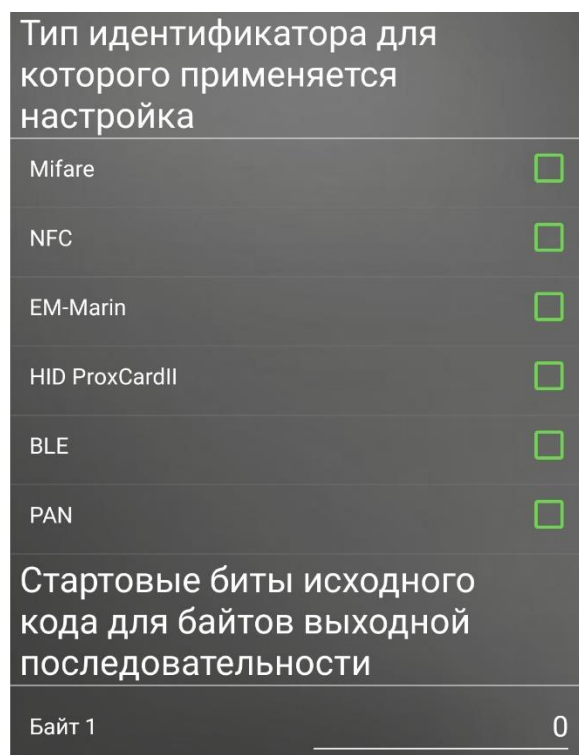


Рисунок 16 – Выходная последовательность байт.

3. «Считывание» (Рисунок 17):

- «Антиклон EM-Marine» – при включении данной настройки считыватель не воспринимает перезаписываемые карты и выдаёт специальный код в контроллер (по умолчанию выключена). Этот режим позволяет выявить предъявление клона (дубликата) карты в большинстве случаев, но не гарантирует 100% вероятность выявления дубликатов;
- «Коэффициент усиления приёмника mifare» – служебная функция, влияющая на чтение карт Mifare разных типов и производителей. По умолчанию «20dB».

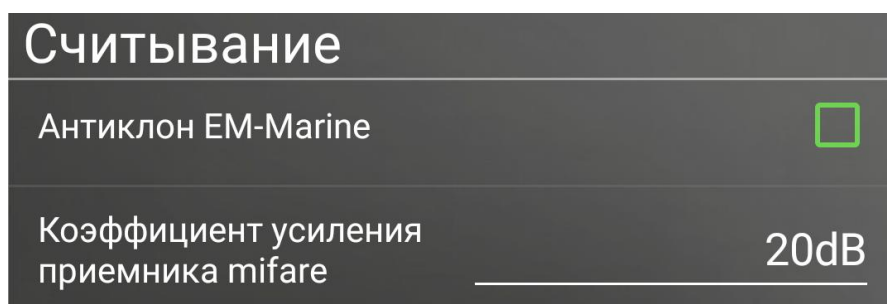


Рисунок 17 – Расширенные настройки считывания.

4. «Клавиатура» (Рисунок 18):

- «Режим» - настройка устанавливает последовательность ввода идентификаторов. Может принимать значения: «Сначала PIN-код» (сначала вводится ПИН-код, потом предъявляется идентификатор), «Сначала карта» (сначала предъявляется идентификатор, потом вводится ПИН-код), «Только PIN-код», «Только карта». По умолчанию «Сначала PIN-код»;
- «PIN тайм-аут, с» - настройка времени до сброса пароля. При начале ввода PIN-кода в считывателе запускается таймер, по окончании работы которого, если не был нажат символ завершения ввода, очистится текущий код и в контроллер отправится символ отмены ввода. По умолчанию 5с;
- «Тайм-аут второго признака, с» - настройка устанавливает время, отводимое на ввод второго идентификатора. После ввода первого идентификатора в считывателе запускается таймер, по истечению которого, если не был предъявлен второй идентификатор, считыватель перейдет к ожиданию первого. По умолчанию 5с;
- «Символ ввода» - настройка устанавливает какой спец символ отвечает за ввод ПИН-кода, а какой за сброс. По умолчанию # - символ ввода, * - символ сброса;
- «Защита от перебора» - настройка включает специальный режим, в котором усложняется подбор ПИН-кода перебором. Если эта опция включена, то при вводе трёх ПИН-кодов подряд в течение 10 секунд, считыватель перестанет реагировать на ввод в течение 30 секунд. Важно, что считыватель не

анализирует корректность ПИН-кода, т.е. если были введены три штатных кода подряд, то ввод заблокируется. По умолчанию опция выключена.

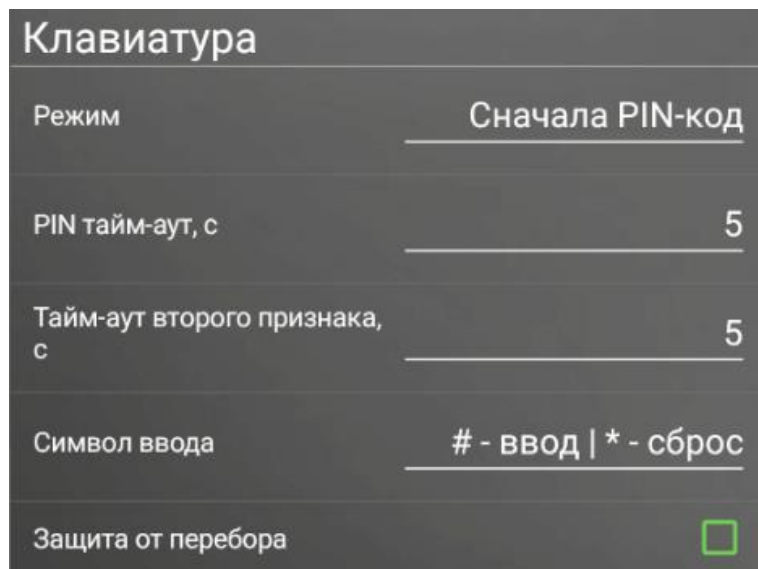


Рисунок 18 – Настройки клавиатуры.

1.4.4.3 Настройка выдачи карт

1. «Выдача карт» (Рисунок 19):

- «Шифровать неиспользуемые сектора» – настройка включает шифрование неиспользуемых секторов при выпуске карт в защищенном режиме;
- «Заданный номер» – настройка включает последовательную запись кодов при выпуске карты в защищенном режиме из диапазона, задаваемого параметрами «Минимальное значение» и «Максимальное значение»;
- «Минимальное значение» - параметр устанавливающий код, начиная с которого будет происходить запись в карту при выпуске в защищенном режиме, доступен только при включенной настройке «Заданный номер»;
- «Максимальное значение» - параметр устанавливающий код, до которого будет происходить выпуск карт в защищенном режиме, доступен только при включенной настройке «Заданный номер»;
- «Следующий номер» - значение, отображающее код, который будет записан в карту при следующем выпуске в защищенном режиме, доступен только при включенной настройке «Заданный номер».

Выдача карт	
Шифровать неиспользуемые сектора	<input type="checkbox"/>
Заданный номер	<input checked="" type="checkbox"/>
Минимальное значение	1
Максимальное значение	F4240
Следующий номер	1

Рисунок 19 – Настройка выдачи карт.

1.4.5 Экран ручного ввода параметров безопасности

Экран «Параметры безопасности» (Рисунок 20) открывается при выборе функции «Параметры безопасности» на экране меню считывателя. Предназначен для ручного ввода параметров безопасности. В актуальных версиях прошивок считывателей текущие параметры безопасности невозможно выгрузить и невозможно их отредактировать.

На экране «Параметры безопасности» можно вручную ввести требуемые настройки и применить их к считывателю. Каждый параметр безопасности загружается в считыватель отдельно.

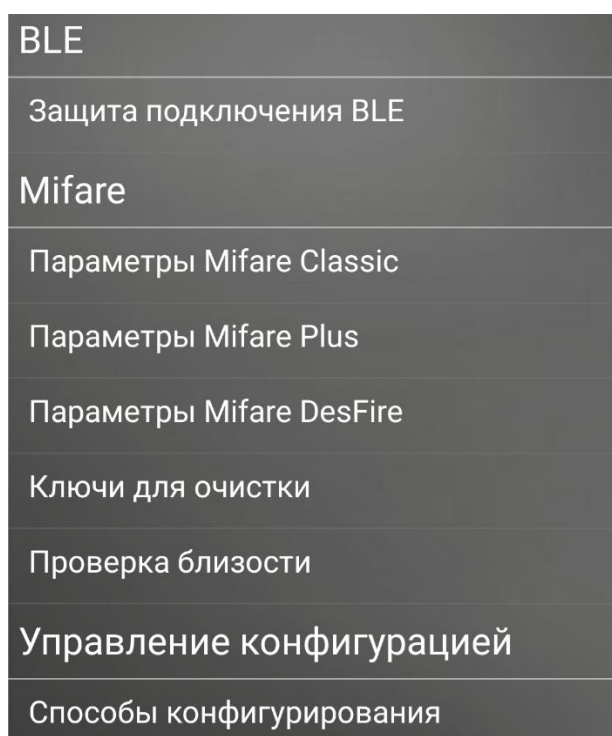


Рисунок 20 – Параметры безопасности.

1. «Защита подключения BLE» (Рисунок 21).

- «ПИН-код» – PIN-код для сопряжения со считывателем (по умолчанию «123456»), должен содержать 6 символов. Для защиты от доступа посторонних лиц к настройкам считывателя PIN-код необходимо сменить в обязательном порядке, с дублированием его на безопасном носителе информации. В случае утраты PIN-кода, для аппаратного сброса настроек к заводским, обратитесь к документации считывателя.
- «Защищать каналы NFC, BLE» (параметр безопасности) – настройка включает защиту каналов передачи идентификатора

NFC и BLE от свободного чтения, случайной посылки, повторной отправки посылки (по умолчанию выключена), при включении настройки возможны задержки в чтении идентификатора по данным каналам.

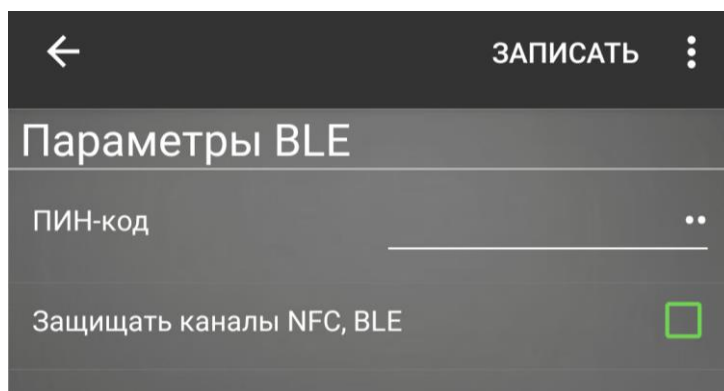


Рисунок 21 – Защита подключения BLE.

2. «Параметры Mifare Classic» (Рисунок 22, Рисунок 23).

- «Защищенный режим Mifare Classic» – опция включает соответствующий защищенный режим (по умолчанию выключена). При подключении к считывателю эта опция вычитывается из считывателя, параметры Mifare Classic служат только для записи.
- «Рабочий ключ» - ключ для доступа к защищенному сектору в режиме SL1. Длина 6 байт (12 символов), записывается старшим байтом вперед.
- «№ сектора» - номер сектора, который используется для хранения идентификатора. Может принимать значения 0 – 15.
- «№ блока в секторе» - номер блока в секторе, который используется для хранения идентификатора. В актуальных версиях прошивки используется 8 первых байт блока, идентификатор записывается младшим байтом вперед. Может принимать значения 0 – 3. Нулевой блок нулевого сектора не может использоваться для хранения пользовательского идентификатора, т.к. там расположен UID карты.
- «Стартовый байт в блоке» – номер байта в блоке начиная с которого считыватель будет вычитывать данные (по умолчанию 0, максимальное значение 15).

- «Число байт для чтения» – количество байт, которое прочитает считыватель начиная с «Стартовый байт в блоке» (по умолчанию 8, максимальное значение = 16 - «Стартовый байт в блоке»).
- «Тип ключа» – настройка определяет какой тип ключа указан в поле «Рабочий ключ» (по умолчанию A).

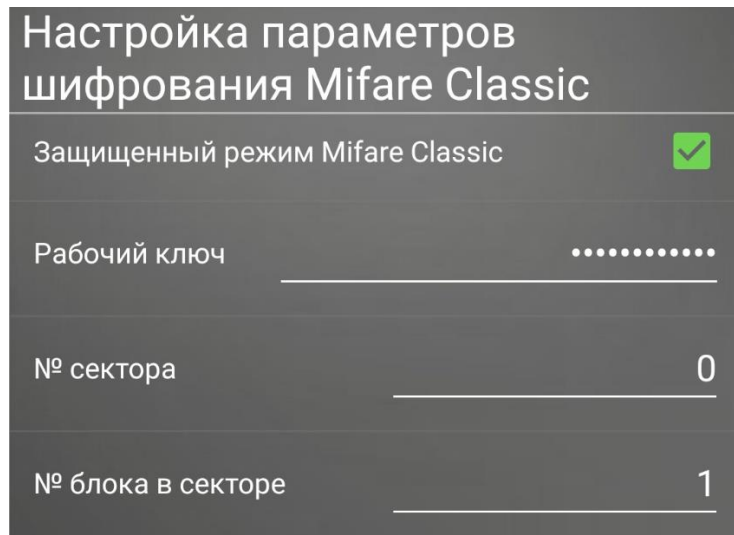


Рисунок 22 – Настройка параметров шифрования Mifare Classic.

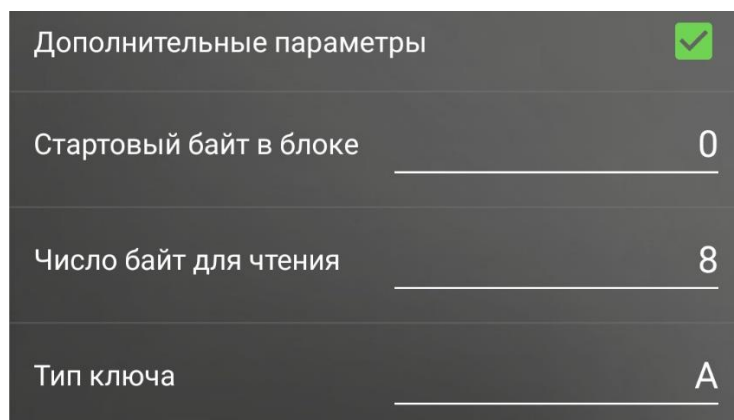


Рисунок 23 – Дополнительные параметры профиля Mifare Classic.

3. «Параметры Mifare Plus» (Рисунок 24).

- «Защищенный режим Mifare Plus» – опция включает соответствующий защищенный режим (по умолчанию выключена). При подключении к считывателю эта опция вычитывается из считывателя, параметры Mifare Plus служат только для записи.
- «Рабочий ключ» - ключ для доступа к защищенному сектору в режиме SL3. Длина 16 байт (32 символа), записывается старшим байтом вперед.

- «№ сектора» - номер сектора, который используется для хранения идентификатора. Может принимать значения 0 – 15.
- «№ блока в секторе» - номер блока в секторе, который используется для хранения идентификатора. В актуальных версиях прошивки используется 8 первых байт блока, идентификатор записывается младшим байтом вперёд. Может принимать значения 0 – 3. Нулевой блок нулевого сектора не может использоваться для хранения пользовательского идентификатора, т.к. там расположен UID карты.
- «Стартовый байт в блоке» – номер байта в блоке начиная с которого считыватель будет вычитывать данные (по умолчанию 0, максимальное значение 15).
- «Число байт для чтения» – количество байт, которое прочтает считыватель начиная с «Стартовый байт в блоке» (по умолчанию 8, максимальное значение = 16 - «Стартовый байт в блоке»).
- «Тип ключа» – настройка определяет какой тип ключа указан в поле «Рабочий ключ» (по умолчанию А).

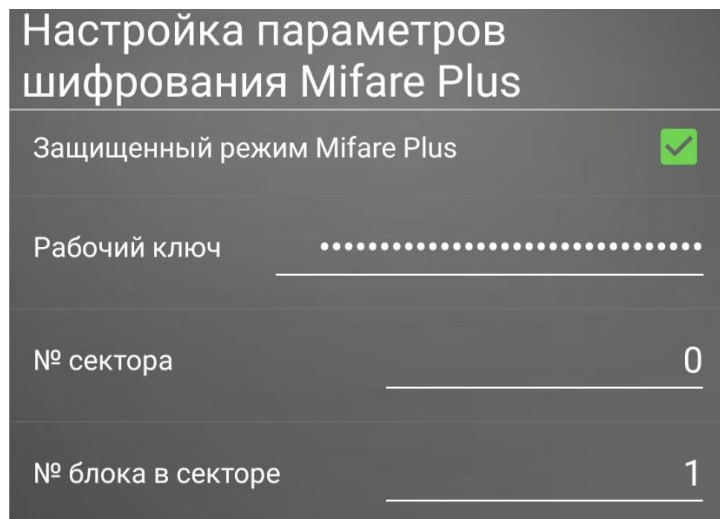


Рисунок 24 – Настройка параметров шифрования Mifare Plus.

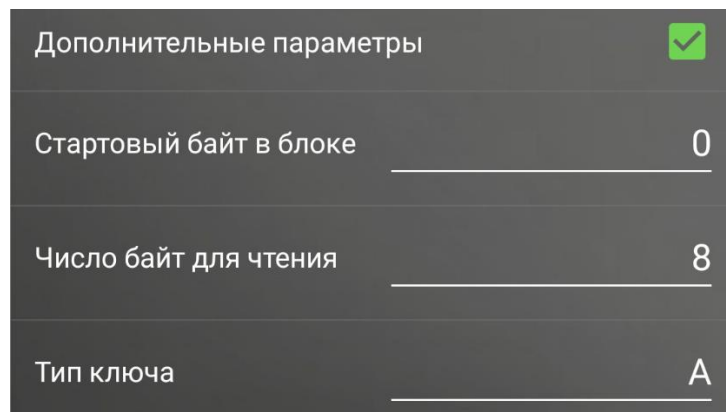


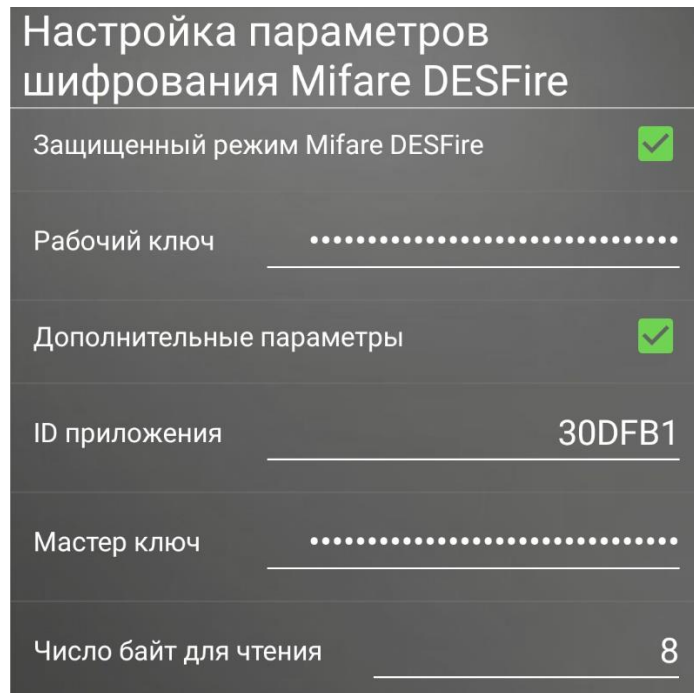
Рисунок 25 – Дополнительные параметры профиля Mifare Plus.

4. «Настройка Mifare DESFire» (Рисунок 26).

- «Защищенный режим Mifare DESFire» – опция включает соответствующий защищенный режим (по умолчанию выключена). При подключении к считывателю эта опция вычитывается из считывателя, параметры Mifare DESFire служат только для записи.
- «Рабочий ключ» - ключ для доступа к защищенному сектору с шифрованием AES-128. Длина 16 байт (32 символа), записывается старшим байтом вперед.
- «Дополнительные параметры» - настройка раскрывает расширенные параметры (Рисунок 27).
- «ID приложения» – идентификатор приложения, которое будет создано при эмиссии карты, и которое будет использоваться настольным считывателем при чтении. Содержит 6 шестнадцатеричных символов (3 байта), по умолчанию 0x30DFB1.
- «Мастер ключ» – ключ, содержащий 16 байт (32 символа) старшим байтом вперед, который доступен только для настольного считывателя. Если карта используется в нескольких системах, то настольный считыватель должен знать используемый мастер ключ для создания приложения, в котором будет храниться идентификатор. Если карта используется только в системе Elsys, то настольный считыватель использует мастер ключ по умолчанию для защиты приложения от удаления. При

создании шаблона необходимо обязательно указать мастер ключ, т.к. ключ по умолчанию хранится в настольном считывателе.

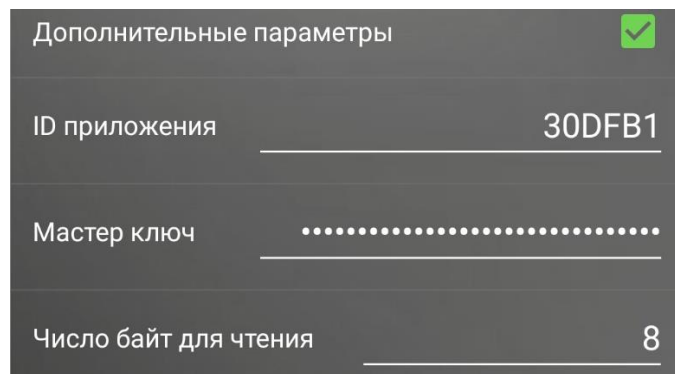
- «Число байт для чтения» – количество байт, которое прочитает считыватель из файла 0 приложения DES Fire (по умолчанию 8, максимальное значение 16).



Настройка параметров шифрования Mifare DESFire

Защищенный режим Mifare DESFire	<input checked="" type="checkbox"/>
Рабочий ключ
Дополнительные параметры	<input checked="" type="checkbox"/>
ID приложения	30DFB1
Мастер ключ
Число байт для чтения	8

Рисунок 26 – Настройка параметров шифрования Mifare DESFire.



Дополнительные параметры

ID приложения	30DFB1
Мастер ключ
Число байт для чтения	8

Рисунок 27 – Расширенные настройки параметров шифрования Mifare DESFire.

5. «Ключи для очистки карт» (параметр безопасности) (Рисунок 28) задают ключи шифрования для соответствующих типов карт, используемые считывателем при очистке пропуска, в случае смены рабочего ключа системы, необходимо указать старый ключ для возможности обновления старых карт доступа, формат – массив шестнадцатеричных символов. В поле Mifare DESFire указывается старый мастер ключ карты.

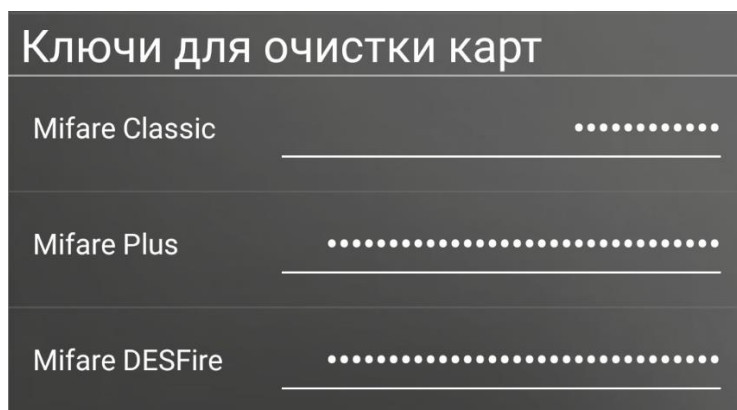


Рисунок 28 – Настройка ключей для очистки карт.

- б. «Проверка близости» – настройка функции защиты от relay-attack (Рисунок 29). Проверка близости осуществляется путём ограничения времени ожидания ответа от карты при аутентификации. Следует учитывать, что на данный момент нет 100% защиты от relay-attack, т.к. современные средства позволяют минимизировать задержку передачи данных, а время ответа карт можно уменьшить путём увеличения частоты поля. Теоретически считыватель может отклонить авторизацию карты, если задержка ответа, вызванная каналом передачи данных злоумышленника, превышает 100мкс. Время ответа карты на команду аутентификации может отличаться в зависимости от типа, версии и производителя микросхемы. Настройка параметра таймаута выполняется следующим образом: включается защищенный режим карты Mifare; проверяется чтение эмитированной карты; значение таймаута уменьшается в два раза до тех пор, пока карта не перестанет читаться считывателем; после чего таймаут увеличивается с шагом 1мс до тех пор, пока карта не начнет читаться; далее происходит тонкая подстройка таймаута с точностью до 10мкс. Настройку необходимо производить с несколькими картами. Если в системе применяются карты с разным временем ответа на команду аутентификации, то настройка происходит по самому большому времени, но при этом уменьшается избирательность этой функции.

Проверка близости	
Максимальное ожидание ответа от карты Mifare DESFire, мс	100,00
Максимальное ожидание ответа от карты Mifare Plus, мс	100,00

Рисунок 29 – Настройка «Проверка близости».

7. «Защищенный режим ESDP» (Рисунок 30) – доступен только при непосредственном подключении к настенному считывателю.

- «Режим установления нового защищенного соединения / Небезопасное соединение» - когда настройка включена, считыватель будет работать по протоколу ESDP в нешифрованном режиме или будет готов установить новое защищенное соединение. При этом интерфейс будет автоматически определяться между ESDP, Wiegand, Touch Memory. В процессе нового защищенного соединения считыватель и контроллер обмениваются информацией, которая позволит в дальнейшем идентифицировать друг друга, при этом данная настройка выключится. Когда эта опция выключена считыватель будет устанавливать только защищенное соединение по ESDP со связанным контроллером, другие интерфейсы будут недоступны (Wiegand, Touch Memory). Для подключения к другому контроллеру или смены интерфейса, необходимо включить эту настройку.

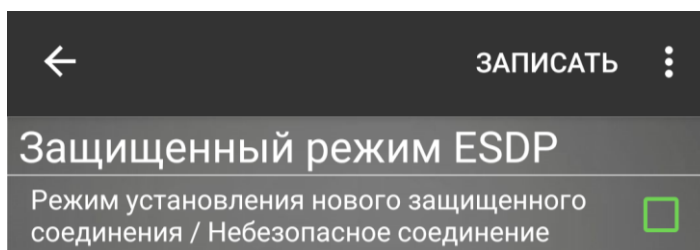


Рисунок 30 – Защищенный режим ESDP.

8. «Способы конфигурирования» – Настройка способов конфигурирования. По умолчанию все включены. При настройке рекомендуется отключать неиспользуемые способы конфигурации.

Если доступ к настройкам через Elsys-SW Config разрешается с помощью мастер-карты, то эти настройки недоступны.

- «Мастер-карта» – опция включает или выключает конфигурирование считывателя с помощью мастер-карты (по умолчанию – включена). Если мастер карта не используется, то эту опцию необходимо выключить.
- «ESDP» – опция включает или выключает конфигурирование считывателя по ESDP (по умолчанию – включена). Если считыватель не подключено по ESDP, то эту опцию необходимо выключить.
- «Выводы считывателя» – опция включает или выключает очистку конфигурации и смену параметров с помощью проводов считывателя (по умолчанию – включена). Рекомендуется не отключать эту опцию в процессе настройки настройки.

Способы конфигурирования	
Мастер карта	<input checked="" type="checkbox"/>
ESDP	<input checked="" type="checkbox"/>
Выводы считывателя	<input checked="" type="checkbox"/>

Рисунок 31 – Способы конфигурирования считывателя.

1.4.6 Экран обновления прошивки

Экран обновления прошивки открывается при выборе функции «Обновить прошивку».

Для загрузки прошивки необходимо выбрать файл обновления с расширением `mcg` из файловой системы телефона, нажать «Обновить» и дождаться окончания обновления (примерно 30 секунд). После завершения загрузки считыватель перезагрузится и соединение разорвется.

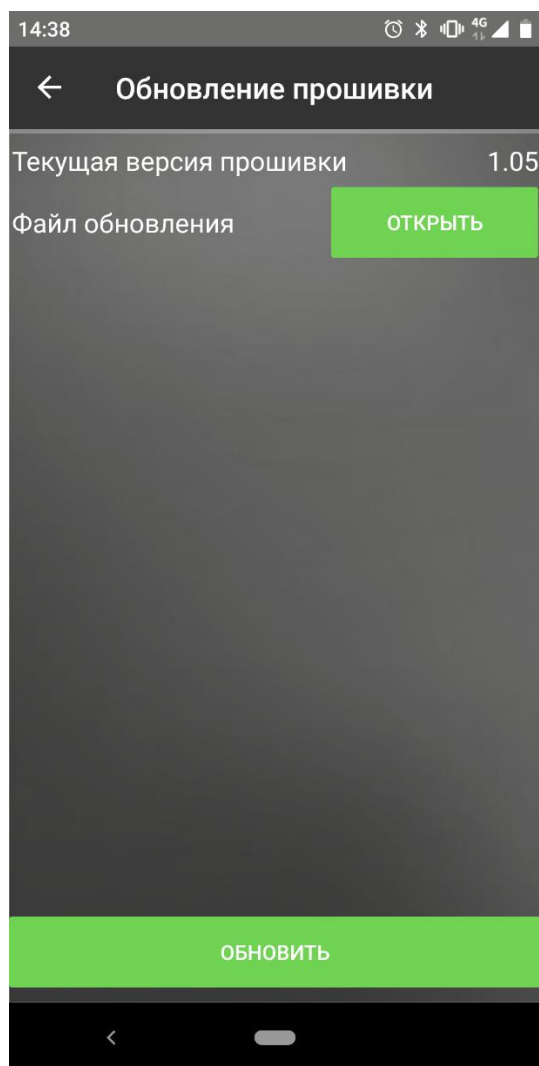


Рисунок 32 – Экран обновления прошивки.

1.4.7 Экран списка шаблонов

Экран со списком шаблонов (Рисунок 33) отображается при выборе «Шаблоны настроек» на главном экране. Предназначен для создания, хранения и редактирования конфигураций в автономном режиме. После установки приложение будет содержать настройки по умолчанию для считывателя.

Для создания нового шаблона необходимо нажать «Новый», после ввода названия добавится конфигурация с настройками по умолчанию. Чтобы переименовать шаблон, копировать или удалить его, необходимо нажать и удерживать требуемый элемент списка до появления контекстного меню, и в нём выбрать необходимую функцию (Рисунок 34).

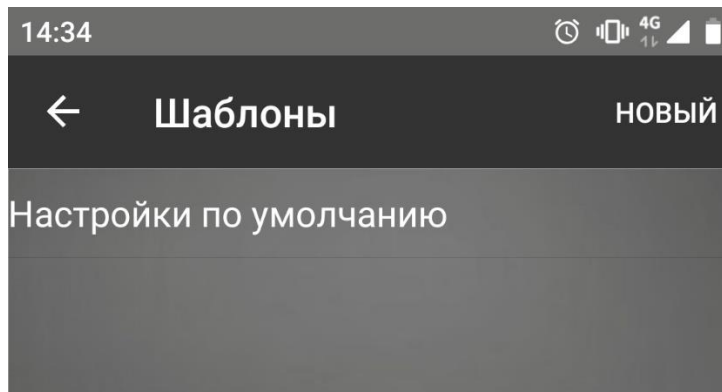


Рисунок 33 – Экран списка шаблонов.

Для редактирования шаблона, необходимо нажать на него. После выбора откроется экран настроек считывателя (пункт 1.4.4), с полной конфигурацией, включающей в себя настройки для настенного и настольного считывателя, за исключением поля имени устройства. Сохранение шаблона происходит при нажатии на кнопку «Сохранить». Шаблоны хранятся в защищенном хранилище системы Android с невозможностью прочитать скрытые поля (PIN-код, ключ шифрования Mifare Classic).

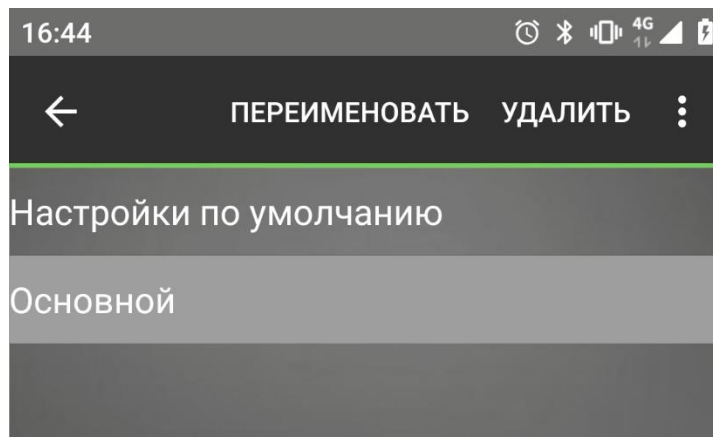


Рисунок 34 – Контекстное меню списка шаблонов.

Шаблон можно загрузить в считыватель любого типа, при этом применяются только доступные для него настройки. При сохранении конфигурации считывателя как шаблона, шаблон дополняется до полного набора настроек с параметрами по умолчанию, которые можно будет сменить.

Начиная с версии приложения 1.06 из шаблона можно сохранить настройки и параметры безопасности в отдельности в файл. При сохранении параметров их можно зашифровать с использованием пароля. Из файла с настройками можно создать новый шаблон или применить его при

подключении к считывателю, при этом будет запрошен пароль, если параметры были зашифрованы.

Настройки параметров безопасности из шаблона не будут применяться к считывателям актуальных версий прошивки. Чтобы загрузить параметры безопасности из ранее созданного шаблона, необходимо сохранить параметры безопасности в файл, после чего их можно будет применить при подключении к считывателю. Для редактирования файла с параметрами безопасности необходимо использовать экран «Параметры безопасности».

Для создания нового шаблона с применением настроек из файла необходимо раскрыть дополнительное меню в верхней части экрана и выбрать «Загрузить настройки из файла», после чего ввести имя нового шаблона и пароль, если настройки были зашифрованы при сохранении.

Для сохранения настроек или параметров безопасности в файл из шаблона необходимо нажать на элемент списка и удерживать до появления контекстного меню, где необходимо раскрыть дополнительные функции и выбрать «Сохранить как файл параметров» или «Сохранить параметры безопасности», появится поле ввода пароля для шифрования параметров (если оставить поле пустым, то данные сохранятся в открытом виде), после ввода пароля выбрать место сохранения и ввести имя файла.

Для сохранения настроек в файл для загрузки в мастер-карту необходимо нажать на элемент списка и удерживать до появления контекстного меню, где необходимо раскрыть дополнительные функции и выбрать «Сохранить для мастер-карты», после чего выбрать место сохранения и ввести имя файла.

Для совместимости с предыдущими версиями приложений и прошивок считывателей в шаблонах осталась возможность редактирования параметров безопасности. При этом обратите внимание, что в актуальные прошивки считывателей, при применении шаблона к нему, не загрузятся параметры безопасности. Их необходимо вводить вручную, либо загружать из файла, защищенного паролем.

1.4.8 Экран редактирования параметров безопасности

Экран создания и редактирования параметров безопасности (Рисунок 35) отображается при выборе «Параметры безопасности» на главном экране. Предназначен для создания и редактирования файлов с параметрами безопасности.

Описание параметров безопасности см. в п. 1.4.5.

Параметры безопасности — это настройки для конфигурирования защиты доступа к считывателю и защиты чтения идентификаторов из карт доступа. Параметры безопасности невозможно вычитать из считывателей с актуальной прошивкой.

Каждый параметр безопасности редактируется по отдельности. При этом несколько параметров безопасности можно сохранить в один файл. Например, для инициализации нового считывателя можно создать файл с настройками из шаблона и добавить в него параметры «Защита подключения BLE», где указан PIN код, а для конфигурирования защищенного режима Mifare создать новый файл с параметрами «Защищенные режимы Mifare», где включен Mifare Plus, и добавить в него «Параметры Mifare Plus». Таки образом параметры безопасности для чтения карт Mifare будут отделены от общих настроек и так же могут иметь различный пароль шифрования данных.

Для создания нового файла с параметрами безопасности, необходимо открыть страницу требуемого типа, внести изменения и, раскрыв дополнительные функции в верхней части, выбрать пункт «Создать новый файл параметров», после чего ввести пароль (если поле пароля оставить пустым, то данные сохранятся в открытом виде), выбрать место хранения и ввести имя файла. При этом в файле параметров будет содержаться только конкретный тип параметров безопасности, далее можно к нему добавить другие типы параметров безопасности.

Для добавления параметров безопасности к существующему файлу необходимо на экране с конкретным типом, раскрыв дополнительные функции в верхней части экрана, выбрать пункт «Добавить к файлу параметров», появится окно ввода пароля (если поле пароля оставить пустым, то данные сохранятся в открытом виде), пароль должен совпадать с используемым в файле. После его ввода, необходимо выбрать файл параметров к которому

необходимо добавить настройки. Если этот тип параметров безопасности уже был в файле, то он переписывается. Параметры безопасности можно добавить к другим параметрам безопасности или к настройкам, выгруженным из шаблона.

Для сохранения параметров безопасности для загрузки в мастер-карту необходимо на экране с конкретным типом, раскрыв дополнительные функции в верхней части экрана, выбрать пункт «Сохранить для мастер-карты», после чего выбрать место сохранения и ввести имя файла.

Для редактирования параметров безопасности в файле, необходимо выбрать конкретный тип и нажать на пункт в верхней части экрана «Загрузить настройки из файла». После выбора файла, если параметры были зашифрованы с использованием пароля, то появится окно с полем для его ввода. После успешной загрузки параметров, они будут доступны для редактирования в текущем окне, для их сохранения необходимо создать новый файл или добавить к существующему (см. выше).

Файл с параметрами безопасности можно применить к считывателю при подключении к нему см. п. 1.4.3.

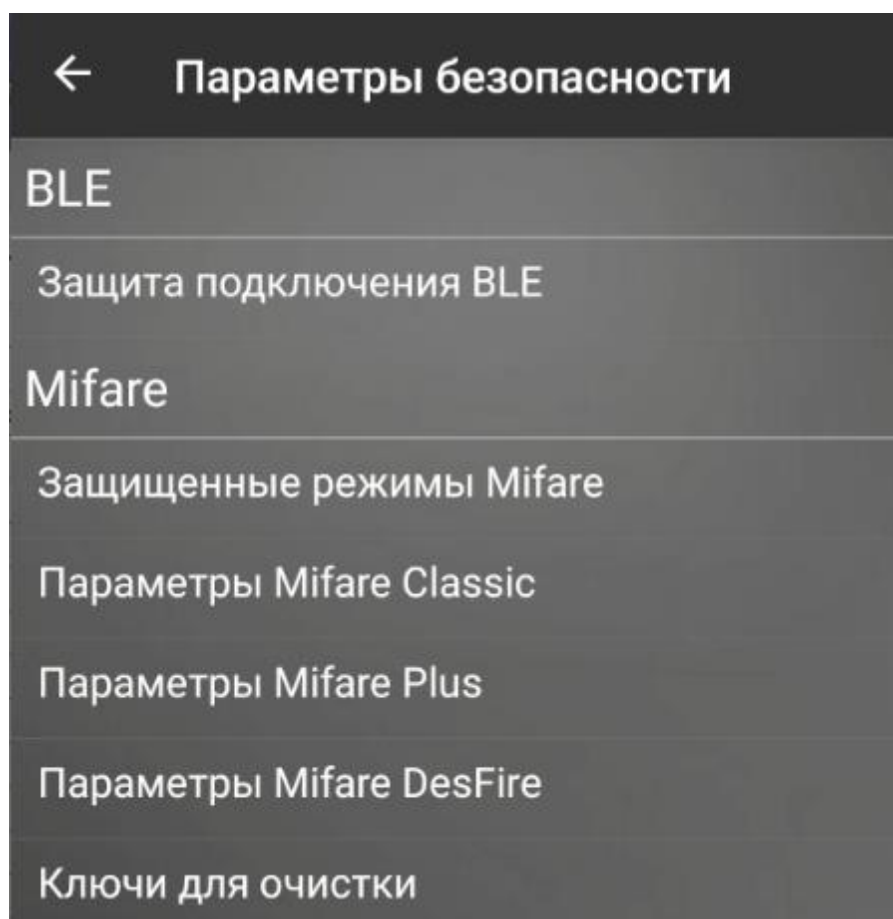


Рисунок 35 – Параметры безопасности.

1.5 Требования приложения

Для выполнения поиска считывателей необходимо включить Bluetooth и предоставить приложению разрешение на определение местоположения на Android версии 11 и ниже или разрешение на устройства поблизости на Android версии 12 и старше.

Для обновления прошивки приложению необходимо предоставить разрешение на использование локального хранилища для выбора файла обновления на файловой системе телефона.

ПРИЛОЖЕНИЕ А

Пример настройки выходной последовательности байт

Для примера настроим считыватель так, чтобы код карты EM-Marine 0x5544332211 передавался по Wiegand-42 в виде 0x6355004321, где старший байт 0x63 постоянный, а число 0x55004321 составлено из кода карты.

Для этого необходимо выполнить настройку как показано на рисунках: Рисунок 36; Рисунок 37; Рисунок 38.

В настройке «Стартовые биты исходного кода для байтов выходной последовательности» для каждого байта выходной последовательности Байт 1 ... Байт 8 задаётся значение стартового бита исходной последовательности. Для получения первого байта 0x21 берутся 8 бит начиная с 4-го, для получения второго байта 0x43 берутся 8 бит начиная с 20-го, для получения третьего байта 0x00 берутся 8 бит начиная с 40-го (больше общего количества байт исходной последовательности, поэтому будет 0x00), для получения четвертого байта 0x55 берутся 8 бит начиная с 32-го.

Число 0x5544332211 можно представить в двоичном виде, из которого и составляется выходная последовательность:

0b000000000101010101000100001100110010001000010001
 Байт 3 Байт 4 Байт 2 Байт 1

В настройке «Постоянные значения байт выходной последовательности» для каждого байта выходной последовательности Байт 1 ... Байт 8 задаётся постоянное десятичное значение отличное от 0x00. Для того, чтобы старшим байтом всегда передавалось число 0x63, необходимо задать «Байт 5» равным 99.

При такой конфигурации коды карт EM-Marine 0x0011223344, 0xFEDCBA9876, будут передаваться как 0x6300001234, 0x63FE00CB87 соответственно.

Тип идентификатора для которого применяется настройка	
Mifare	<input type="checkbox"/>
NFC	<input type="checkbox"/>
EM-Marin	<input checked="" type="checkbox"/>
HID ProxCardII	<input type="checkbox"/>
BLE	<input type="checkbox"/>
PAN	<input type="checkbox"/>

Рисунок 36 – Настройка типов идентификатора для изменения выходной последовательности байт.

Стартовые биты исходного кода для байтов выходной последовательности	
Байт 1	4
Байт 2	20
Байт 3	40
Байт 4	32
Байт 5	0
Байт 6	0
Байт 7	0
Байт 8	0

Рисунок 37 – Настройка стартовых бит выходной последовательности байт.

Постоянные значения байт выходной последовательности	
Байт 1	0
Байт 2	0
Байт 3	0
Байт 4	0
Байт 5	99
Байт 6	0
Байт 7	0
Байт 8	0

Рисунок 38 – Настройка постоянных значений байтов выходной последовательности.