Считыватели бесконтактные контроля доступа UEM Mifare/NFC SKD reader, UEM Mifare/NFC SKD BT reader

Руководство по конфигурированию карт

Версия 1.4.2

Москва

Содержание

1 Принцип работы считывателя контроля доступа

После подачи питания считыватель излучает вблизи себя высокочастотное электромагнитное поле, частотой 13.56 МГц. Пассивная бесконтактная карта получает от него энергию, достаточную для работы внутренней электронной схемы, и в ответ на специфическую команду считывателя передает свой уникальный идентификационный номер. В автономном режиме работы считывателя, получение ответа от карты сопровождается индикацией светодиодом и кратковременным звуковым сигналом.

Далее считыватель преобразует принятый уникальный идентификатор карты в формат Wiegand / Touch Memory.

1.1 Настройки по умолчанию

Считыватель поставляется с настройками по умолчанию:

- автономный режим работы;

- связь с контроллером СКУД осуществляется по протоколу Wiegand-26;

- идентификатором пропуска является UID карты (или данные от смартфона);

- младший байт UID карты игнорируется;

- входные сигналы управления индикацией включают ее низким уровнем;

- при обнаружении карты считыватель независимо от контроллера издает короткий звуковой сигнал и кратковременно зажигает зеленый светодиод.

1.2 Режимы

Считыватель предназначен для работы в двух режимах.

1.2.1 Автономный режим

В автономном режиме считыватель самостоятельно определяет наличие транспондера (смарт-карты) в непосредственной близости от антенны и передает прочитанный идентификатор по интерфейсу Wiegand или 1-Wire.

При работе в формате Wiegand-26 длительность одного бита равна 2000 мкс, длительность импульса - 200 мкс.

Новый считыватель изначально настроен выдавать UID карты, без младшего байта, в формате Wiegand-26 в автономном режиме.

1.2.2 Подчиненный режим

В подчиненном режиме считыватель не производит никаких самостоятельных действий, а выполняет только команды от управляющего устройства.

Формат команд для работы в подчиненном режиме, а также описание библиотеки разработчика находятся в отдельном документе - PgmGuide_SAM.pdf

Для работы со считывателем в подчиненном режиме используйте специализированное проверочное программное обеспечение - CLESCAR_SAM.EXE, документация по которому размещена в файле Test_UEM_SAM.pdf

1.3 Индикация

Считыватель снабжен звукоизлучателем, а также красным и зеленым светодиодами.

По умолчанию при обнаружении карты считыватель издает короткий звуковой сигнал и кратковременно зажигает зеленый светодиод.

Данная индикация никак не связана с правами карты в системе, в которой установлен считыватель.

2 Виды бесконтактных карт

Система контроля доступа на основе считывателей МикроЭМ построена на следующих компонентах:

- устройства ограничения доступа (двери в помещениях, турникеты);
- контроллеры управления устройствами ограничения доступа;
- бесконтактные считыватели рабочих мест администраторов системы контроля доступа;
- бесконтактные считыватели пунктов пропуска;

- бесконтактные карты для настройки параметров считывателей (мастер-карта);
- бесконтактные карты для авторизации выпуска мастер-карт (карта-ключ);
- бесконтактные карты для пропусков (карта-пропуск).

В работе системы контроля доступа участвуют 3 типа бесконтактных карт стандарта ISO14443A, работающих на частоте 13.56МГц:

- Mifare Classic (для карты-ключа, мастер-карты и карты-пропуска);
- Mifare Plus (для карты-ключа, мастер-карты и карты-пропуска);
- Mifare Ultralight C (для карты-ключа и карты-пропуска).

Кроме того в качестве карт-пропусков, работающих в открытом режиме, можно использовать карты стандартов ISO14443B и ISO15693.

В поле считывателя всегда следует подносить только одну карту любого из поддерживаемых типов.

2.1 Карта-ключ

Карта-ключ применяется для доступа администратора к конфигурированию мастер-карт.

Хранит 128-битные мастер-ключи A и B для доступа к Мастер-карте, которые генерит администратор СКУД.

Мастер-ключи для доступа к этой карте известны считывателю.

Эта карта хранится у администратора СКУД и никому не передается.

Администратор СКУД лично проводит персонализацию каждого нового считывателя.

2.2 Мастер-карта

Мастер карта предназначена для бесконтактной настройки конфигурации считывателей контроля доступа, а также для настройки параметров рабочего места администратора системы контроля доступа с целью серийного выпуска карт-пропусков.

Хранит 128-битные мастер-ключи A и B для доступа к Карте-пропуску, а также параметры конфигурации считывателя, которые создает администратор СКУД.

Мастер-ключи для доступа к этой карте считывателю изначально не известны, они хранятся в карте-ключе и записываются в защищенную память считывателя в процессе его персонализации.

Эта карта хранится у администратора СКУД и выдается работникам службы установки для конфигурации считывателя.

2.3 Карта-пропуск

Хранит идентификатор, который создает администратор СКУД, и который передается по интерфейсу Wiegand или 1-Wire при поднесении карты к считывателю.

Мастер-ключи для доступа к этой карте считывателю изначально не известны, они хранятся в мастер-карте и записываются в защищенную память считывателя в процессе его конфигурации.

Для карт и считывателей, используемых в общей инфраструктуре, должны быть заданы одинаковые номера сектора и блока для хранения защищенного идентификатора в картах-пропусках.

2.4 Смартфоны NFC и Bluetooth

В настоящий момент система поддерживает смартфоны на базе Android 4.4 и выше с поддержкой технологий бесконтактного обмена Near Field Communication (NFC) в режиме Host Card Emulation (HCE)* и Bluetooth Low Energy (BLE)**, а также смартфоны iPhone.

Смартфон может быть использован в качестве карты-пропуска: для этого в приложении для смартфонов реализован механизм "виртуальных карт".

Уникальный открытый идентификатор для виртуальных карт создается случайным образом и сохраняется в памяти смартфона.

Закрытый идентификатор может быть добавлен к виртуальной карте и сохраняется в памяти смартфона в зашифрованном виде.

Открытый или закрытый идентификаторы передаются по радиоканалу считывателю и далее - по интерфейсу Wiegand или 1-Wire отправляются на контроллер (хост).

Для работы требуется установленное на смартфон специализированное приложение MicroEM Virtual Card.

* Интерфейс NFC (HCE - Host Card Emulation) поддерживают обе модельные линейки считывателей СКД: UEM Mifare/NFC SKD reader и UEM Mifare/NFC SKD BT reader.

** Интерфейс Bluetooth (BLE - Bluetooth Low Energy) поддерживает только модельная линейка UEM Mifare/NFC SKD BT reader.

3 Конфигурирование бесконтактных карт

В случае, если для хранения уникального идентификатора карты-пропуска система подразумевает использование ее защищенной области памяти, требуется предварительно сконфигурировать (изготовить) такие карты.

Если же в качестве идентификатора будет использоваться собственный публичный UID карты (согласно стандарта ISO14443A), то использование карт-ключей, мастер-карт и дополнительного программного обеспечения для их конфигурирования не обязательно, а настройки считывателей могут быть выполнены при помощи переключателей, согласно документации Wiegand-Installation-Guide.pdf, и раздел "Конфигурирование" можно проигнорировать.

Если возможность смены настроек считывателей при помощи переключателей не удобна, то можно использовать карты-ключи и мастер-карты без персонализации карт-пропусков.

Для изготовления карты-ключа подходят следующие типы карт:

- MIFARE Classic (EV1) 1K/4K
- MIFARE Ultralight C
- MIFARE Plus (EV1) 2K/4K

Для изготовления мастер-карты подходят следующие типы карт:

- MIFARE Classic (EV1) 1K/4K
- MIFARE Plus (EV1) 2K/4K

3.1 Считыватель настольный рабочего места администратора

Для конфигурирования карт администратором системы контродя доступа могут применяться настольные считыватели компании "МикроЭМ":

- UEM Mifare/ICode/NFC USB reader
- UEM Mifare/ICode/NFC RS reader
- UEM MifareNFC SKD reader V4.0 (в подчиненном режиме)

Настольный считыватель подключается к персональному компьютеру (ноутбуку) посредством интерфейса USB/RS.

Управляется при помощи специализированного программного обеспечения рабочего места администратора СКУД (приложение WiegandTool.exe).

3.2 Конфигурирование

Приложение WiegandTool.exe предназначено для обслуживания смарт-карт системы контроля и управления доступом (СКУД), в которой уникальный идентификатор пропуска хранится в защищенной области памяти карты, а обмен данными осуществляется с помощью считывателей производства АО "МикроЭМ" UEM Mifare/ NFC SKD reader.

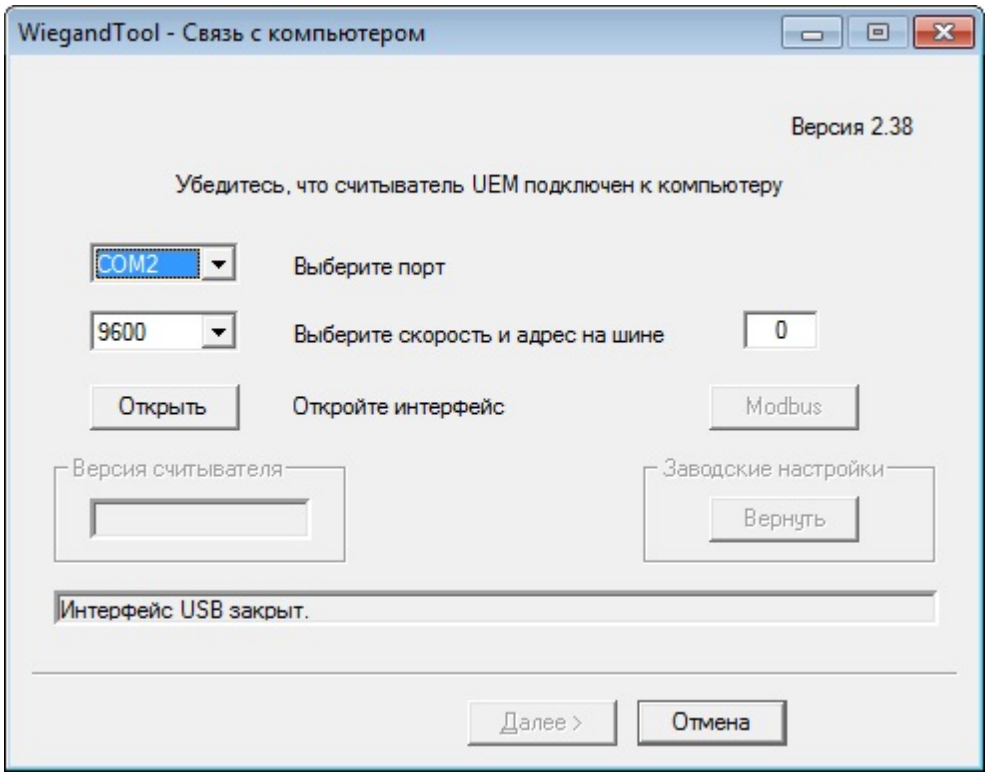
Для подготовки и обслуживания смарт-карт СКУД утилита поддерживает любые считыватели производства АО "МикроЭМ" (в том числе и UEM Mifare/NFC SKD reader) с версией микропрограммы 0x80 и выше.

Работа с утилитой построена в стиле слайд-шоу (мастера).

В любой момент работу с утилитой можно прервать, нажав кнопку "Отмена" или с помощью комбинации клавиш Alt-F4.

3.2.1 Подключение к считывателю

Внешний вид стартового окна утилиты приведен на рисунке ниже.



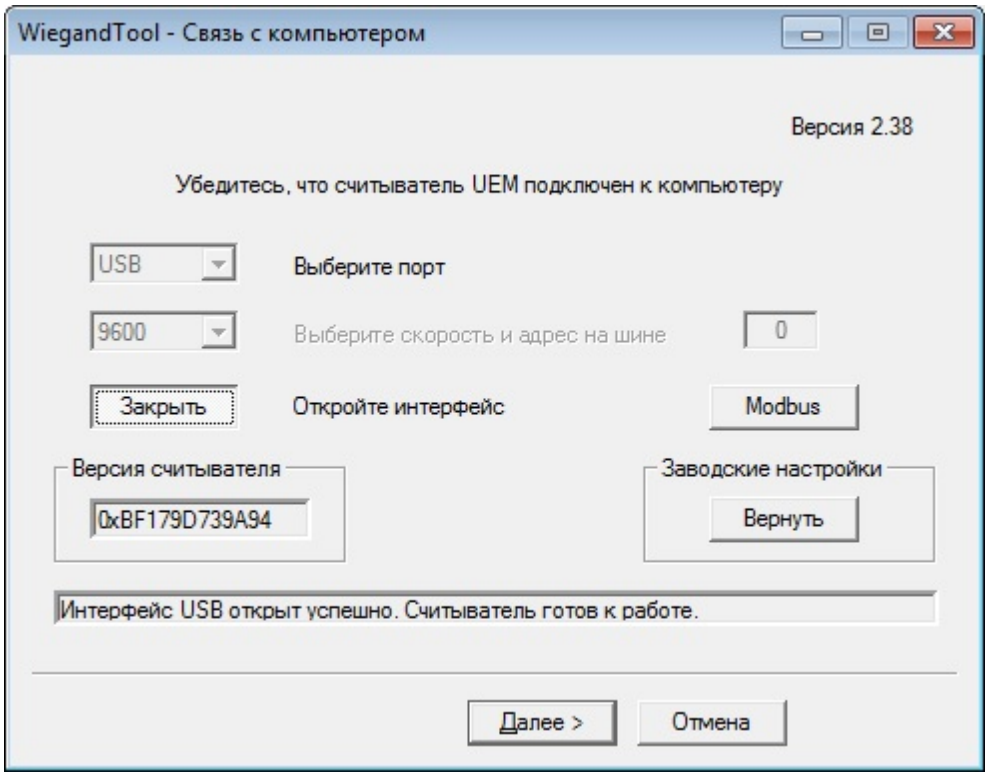
Здесь можно выбрать интерфейс, с помощью которого считыватель подключен к компьютеру. Это может быть USB или COM-порт (RS232 или RS485).

Для COM-порта можно выбрать скорость обмена (в том в случае, если считыватель работает на скорости, отличной от 9600 Кбод).

Для порта RS485 укажите адрес на шине (укажите 0, если на шине всего один считыватель).

Далее необходимо нажать кнопку "Открыть".

Если операция прошла без ошибок, необходимо нажать кнопку "Далее".

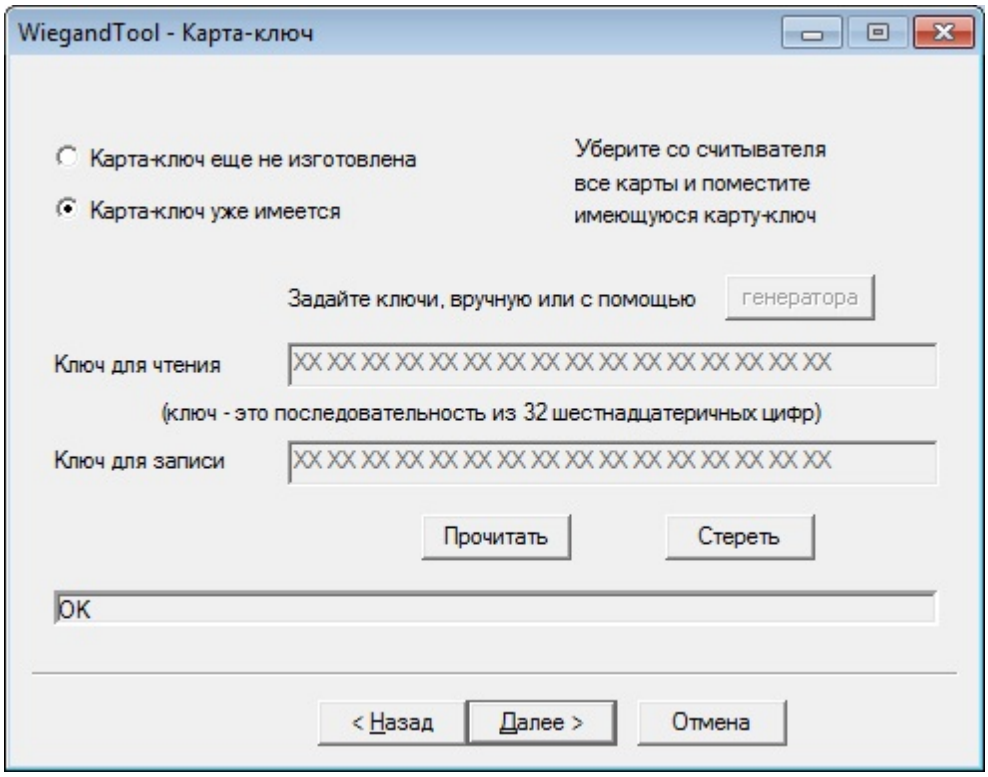


3.2.2 Работа с картой-ключом

Карта-ключ хранит ключи для доступа к мастер-карте, которые должны быть предварительно записаны в считыватель путем обнаружения карты-ключа считывателем.

Для работы с этой картой, после запуска программы выполните действия, описанные в разделе "Подключение к считывателю".

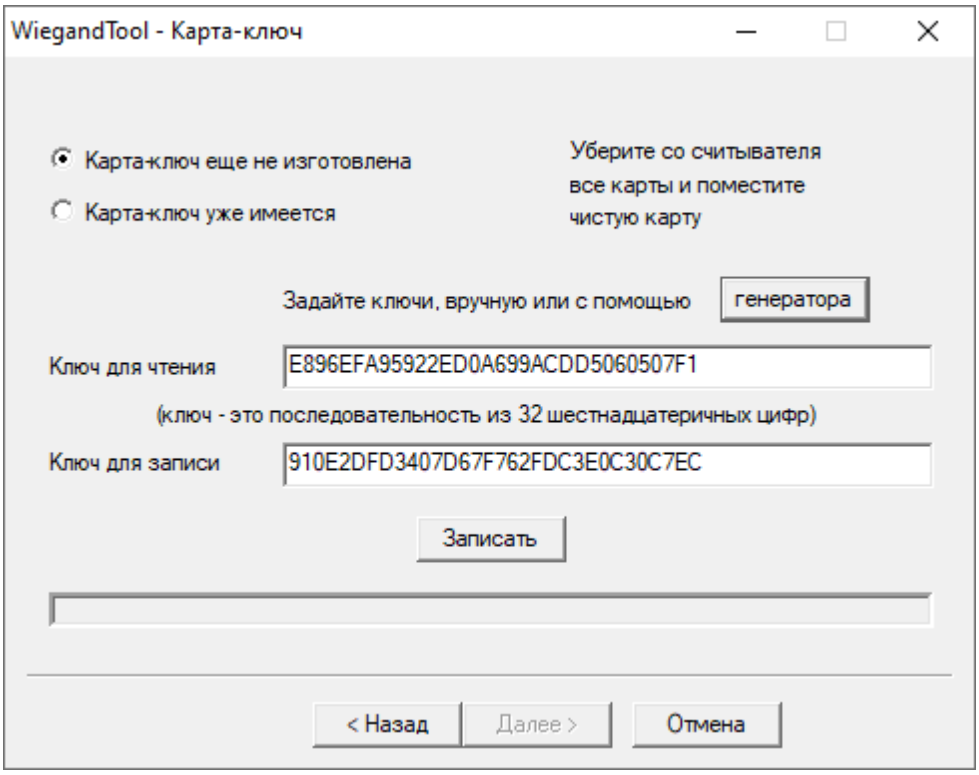
После чего откроется окно, предназначеное для работы с картой-ключом.



3.2.2.1 Изготовление карты-ключа

Если карта-ключ еще не изготовлена, необходимо:

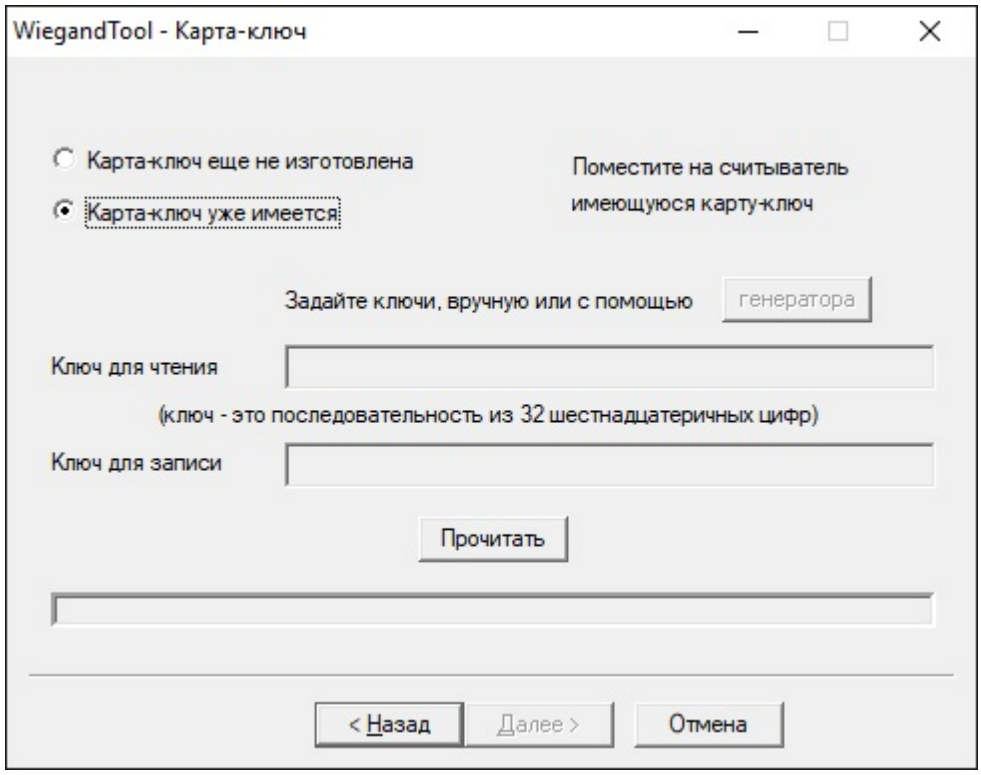
- поместить на считыватель чистую карту типа MIFARE Plus, MIFARE Ultralight C или MIFARE Classic;
- задать два ключа (ключи можно задать вручную, набрав для каждого из них 32 шестнадцатеричных цифры, или автоматически, нажав кнопку "генератора");
- нажать кнопку "Записать".



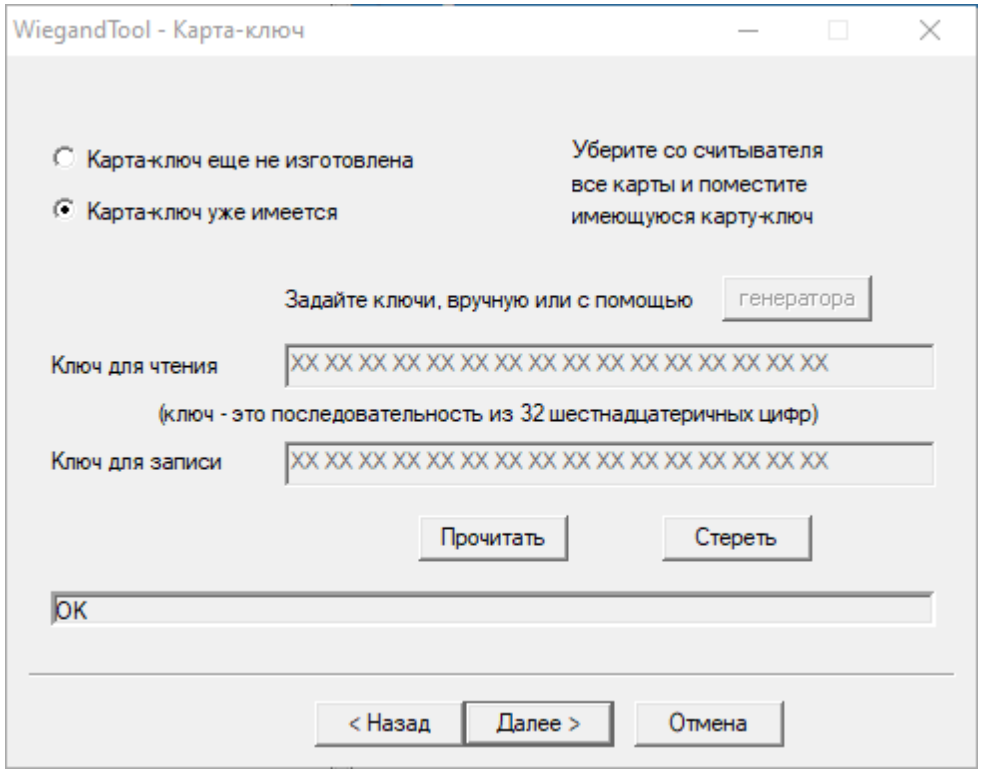
3.2.2.2 Применение карты-ключа

Если карта-ключ уже существует, то для работы с мастер-картами и картами-пропусками необходимо ее прочитать программой:

- поместить ее на считыватель;
- нажать радио-кнопку "Карта-ключ уже имеется";
- нажать кнопку "Прочитать".



Если операция прошла без ошибок, необходимо нажать кнопку "Далее".



3.2.2.3 Стирание карты-ключа

Если требуется полностью очистить карту-ключ, то после ее чтения, нажмите на

кнопку "Стереть".

Внимание! Данная операция приведет к утрате основного ключа вашей системы доступа, построенной на стираемой карте-ключе. После стирания основного ключа, вы утратите возможность обновлять существующие и создавать новые мастер-карты. Вы также не сможете стереть ключи из считывателя без необходимости отправки устройств производителю.

3.2.3 Работа с мастер-картой

Мастер-карта хранит ключи для доступа к карте-пропуску и настройки считывателя UEM Mifare NFC SKD reader.

В системе контроля доступа должны быть единые ключи доступа для всех карт-пропусков. В связи с этим дополнительные мастер-карты с новыми мастер-ключами могут быть созданы только с целью образования подгрупп доступа в организации. Допускается также копирование созданных мастер-карт с последующим изменением параметров - тогда копии можно будет использовать в отдельных подгруппах доступа.

Для работы с мастер-картой предварительно требуется использовать карту-ключ.

Если карты-ключа у вас нет, сперва ее нужно создать, выполнив действия из раздела "Изготовление карты-ключа".

Если карта-ключ у вас имеется, ее нужно прочитать, выполнив действия из раздела "Применение карты-ключа".

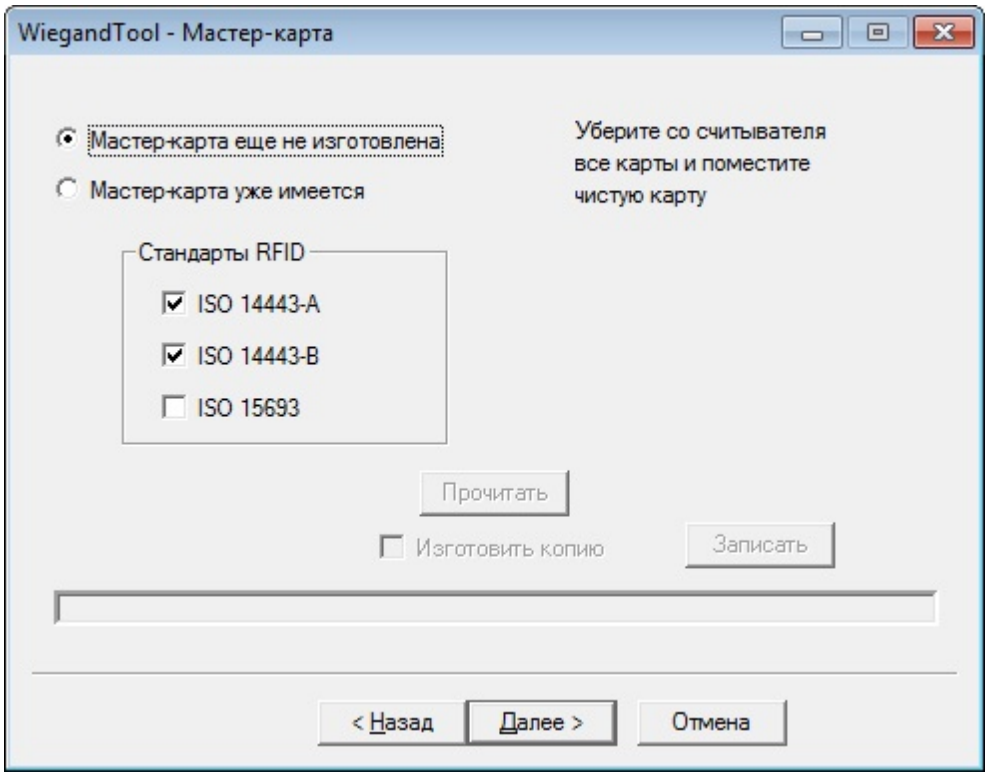
После выполнения этих действий уберите карту-ключ со считывателя.

Следующие три окна предназначены для работы с мастер-картой.

3.2.3.1 Изготовление мастер-карты

Если мастер-карта еще не изготовлена, необходимо:

- поместить на считыватель чистую карту типа MIFARE Plus или MIFARE Classic;
- установить стандарты карт, с которыми должны будут работать настраиваемые мастер-картой считыватели;
- нажмите на кнопку "Далее".



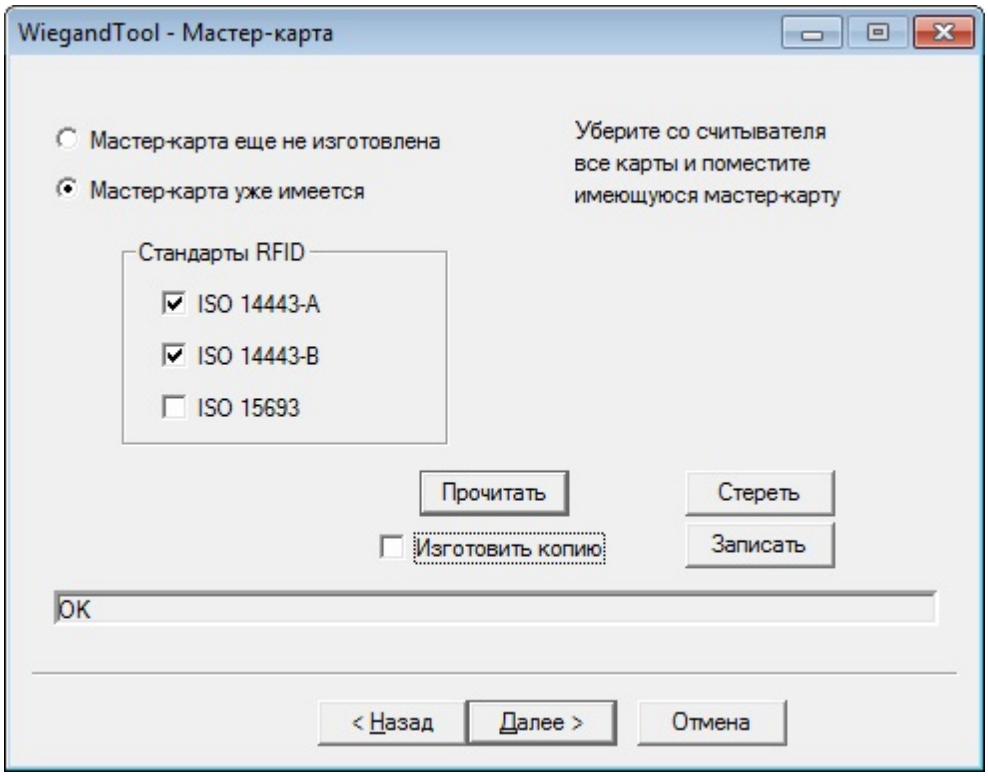
Дальнейшие шаги описаны в разделе "Изменение настроек мастер-карты".

3.2.3.2 Применение мастер-карты

Если мастер-карта уже существует, необходимо:

- поместить ее на считыватель;
- нажать радио-кнопку "Мастер-карта уже имеется";
- нажать кнопку "Прочитать".

Если операция прошла без ошибок, вы увидите следующее окно:



Теперь можно при необходимости изменить настройки стандартов и типов карт, сохраненные в этой мастер-карте, изготовить копию карты или нажать кнопку "Далее" для уточнения параметров.

Дальнейшие шаги описаны в разделе "Изменение настроек мастер-карты" (или "Копирование мастер-карты", если также нужно изготовить ее копии).

3.2.3.3 Стирание мастер-карты

Если требуется полностью очистить мастер-карту, то после ее чтения нажмите на кнопку "Стереть".

Внимание! Данная операция приведет к утрате мастер-ключей вашей системы доступа, построенной на стираемой мастер-карте. После стирания ключей мастер-карты вы утратите возможность обновлять существующие и создавать новые карты-пропуска, если у вас нет дополнительных копий стираемой мастер-карты.

3.2.3.4 Копирование мастер-карты

Для копирования мастер-карты необходимо:

- пройти операции в пункте "Изготовление мастер-карты" или "Применение мастер-карты", если мастер-карта уже изготовлена;

- установить флаг "Изготовить копию";
- нажать кнопку "Записать".

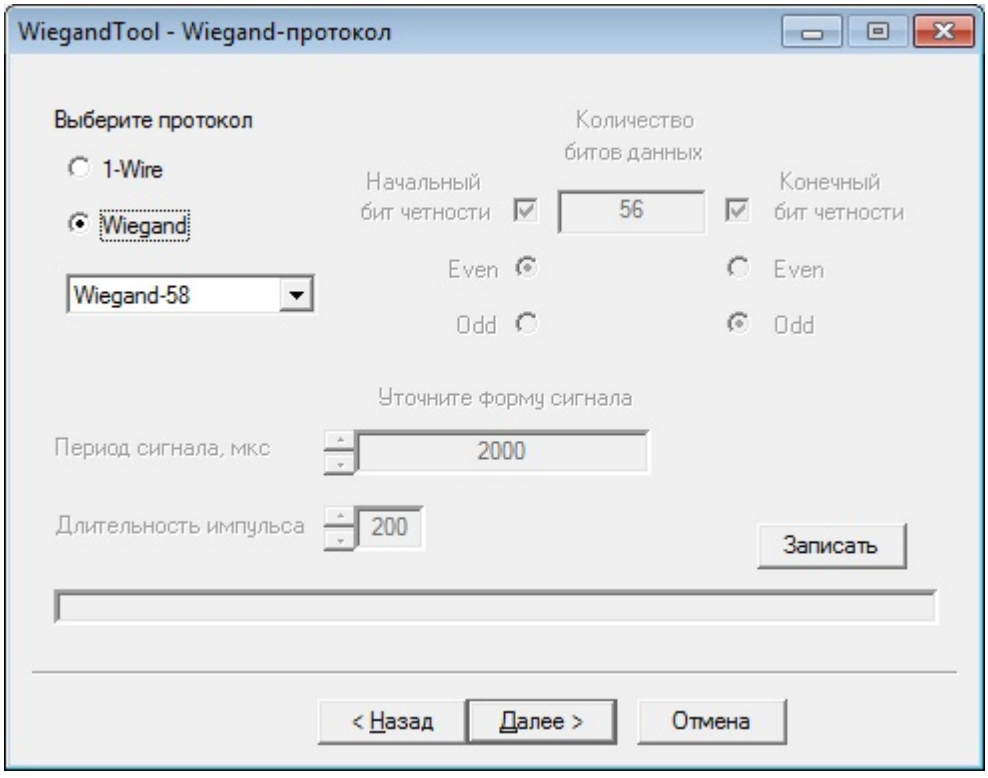
Если операция прошла без ошибок, то в только что изготовленном дубликате мастер-карты можно изменить настройки. Для этого необходимо нажать на кнопку "Далее".

Дальнейшие шаги описаны в разделе "Изменение настроек мастер-карты".

3.2.3.5 Изменение настроек мастер-карты

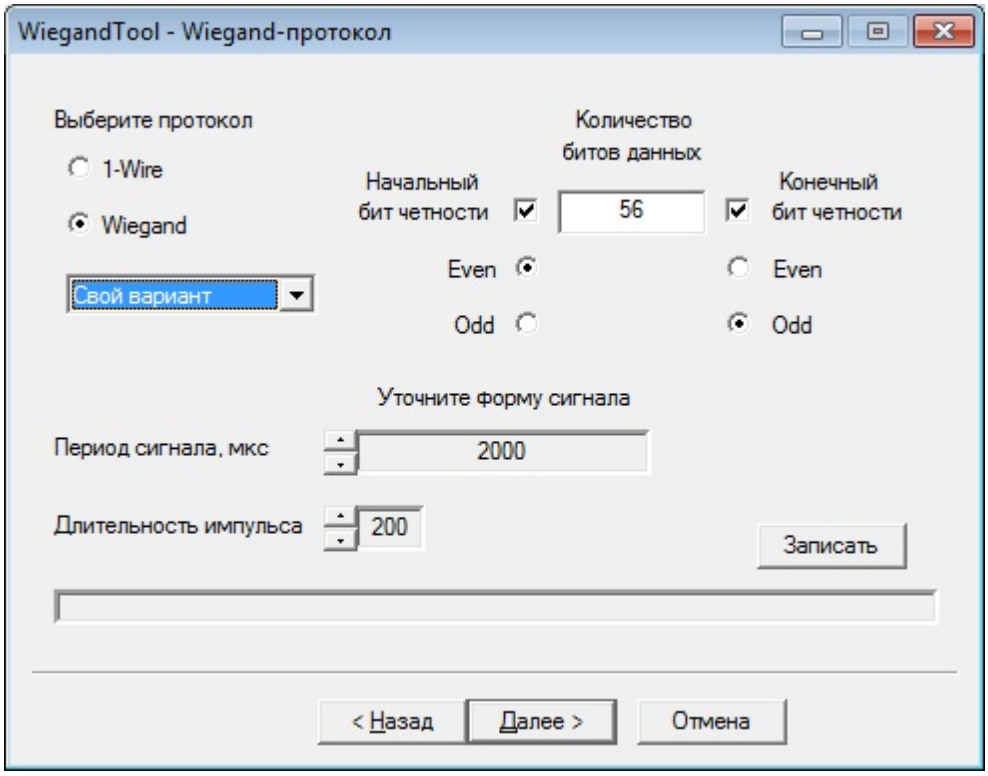
Перед изменением настроек мастер-карту нужно создать согласно разделу "Изготовление мастер-карты", либо применить уже созданную, согласно разделу "Применение мастер-карты".

Следующее окно предназначено для изменения параметров интерфейса передачи идентификатора.



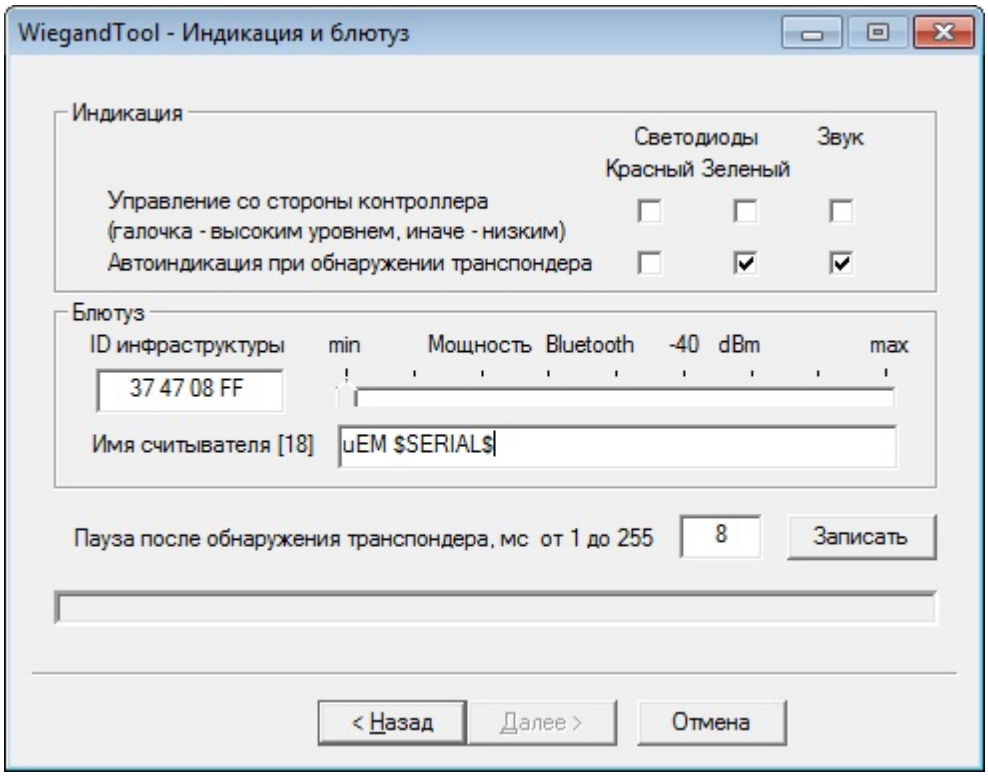
Для интерфейса Wiegand возможен выбор из популярных вариантов: Wiegand-26, 33, 34, 37, 40, 42 или 58.

Кроме того, предоставлена возможность реализовать свой собственный вариант, задавая такие параметры, как количество битов данных, наличие и тип битов четности, период сигнала и длительность импульса.



У интерфейса 1-Wire (по-другому он еще называется "Touch memory" или Dallas) все параметры фиксированы.

В следующем окне уточняются параметры индикации, блютуза и задержки.



Считыватель снабжен двумя светодиодами (красным и зеленым) и звукоизлучателем.

Если контроллер СКУД имеет возможность управлять этими средствами, то необходимо задать уровень сигнала (низкий или высокий), которым включается то или иное средство индикации.

Кроме того, надо уточнить, для каких средств индикации включено автоматическое сопровождение прикладывания карты к считывателю.

В группе управления "Блютуз" задаются идентификатор (ID) инфраструктуры, символьное имя считывателя, мощность передатчика Bluetooth.

ID инфраструктуры используется для того, чтобы приложения на смартфонах могли подобрать нужную виртуальную карту для работы с конкретным считывателем, он генерируется на основе главного ключа, хранящегося в ключ-карте. Однако вы можете задать свой идентификатор в формате HEX, 4 байта.

Мощность передатчика Bluetooth в считывателе может быть установлена вручную в диапазоне от -40 дБм (наименьшая мощность, самое короткое расстояние срабатывания приложения на смартфонах, примерно 10-30 см.) до 4 дБм (наибольшая мощность, позволяющая активировать считыватель на максимальном

расстоянии в несколько метров, зависящем также от модели смартфона). Установка мощности считывателей позволяет конфигурировать их либо для контроля доступа к двери в помещение, либо для проезда транспорта через ворота.

Имя считывателя позволяет идентифицировать считыватель в приложении на смартфонах, что нужно как для ручной, так и для автоматической активации считывателя смартфоном и может применяться совместно с активацией считывателей по идентификатору инфраструктуры. Длина Имени считывателя не должна превышать 18 символов.

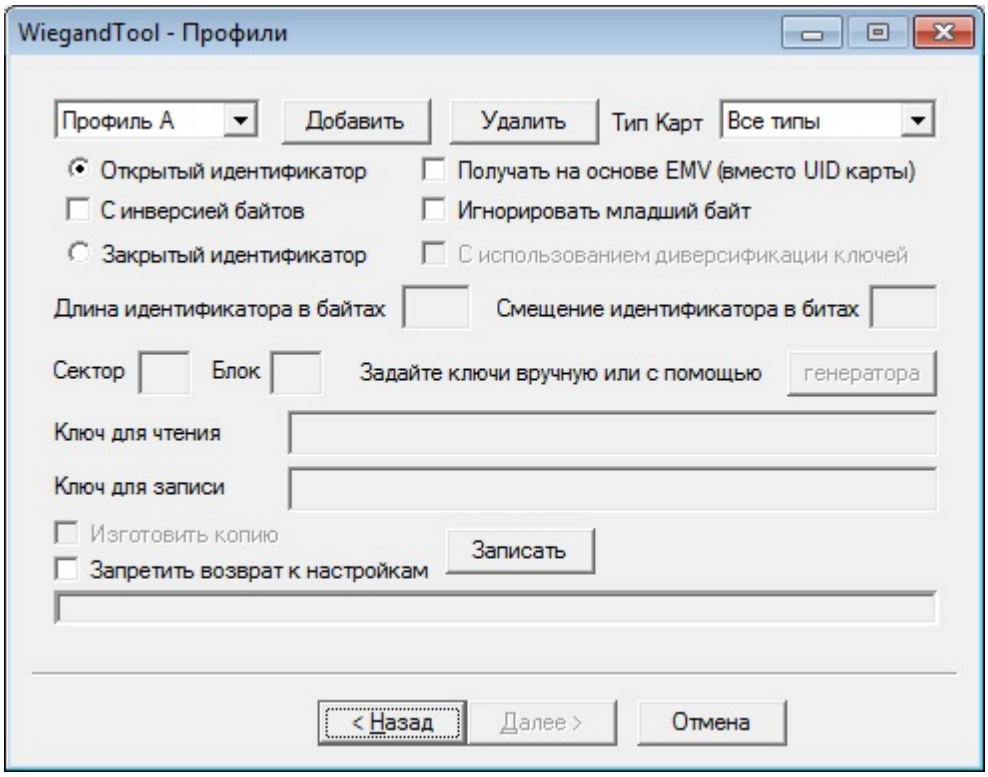
Пауза после обнаружения карты Mifare Plus требуется для запитывания карты энергией.

Далее открывается окно для работы с профилями.

В новом окне можно задать до 12 профилей, которые представляют собой различные конфигурации способов получения уникального идентификатора из карты пропуска.

При поднесении карты-пропуска, считыватель перебирает запрограммированные в нем профили до тех пор, пока с одним из них карточка не аутентифицируется успешно и не вернет свой уникальный номер.

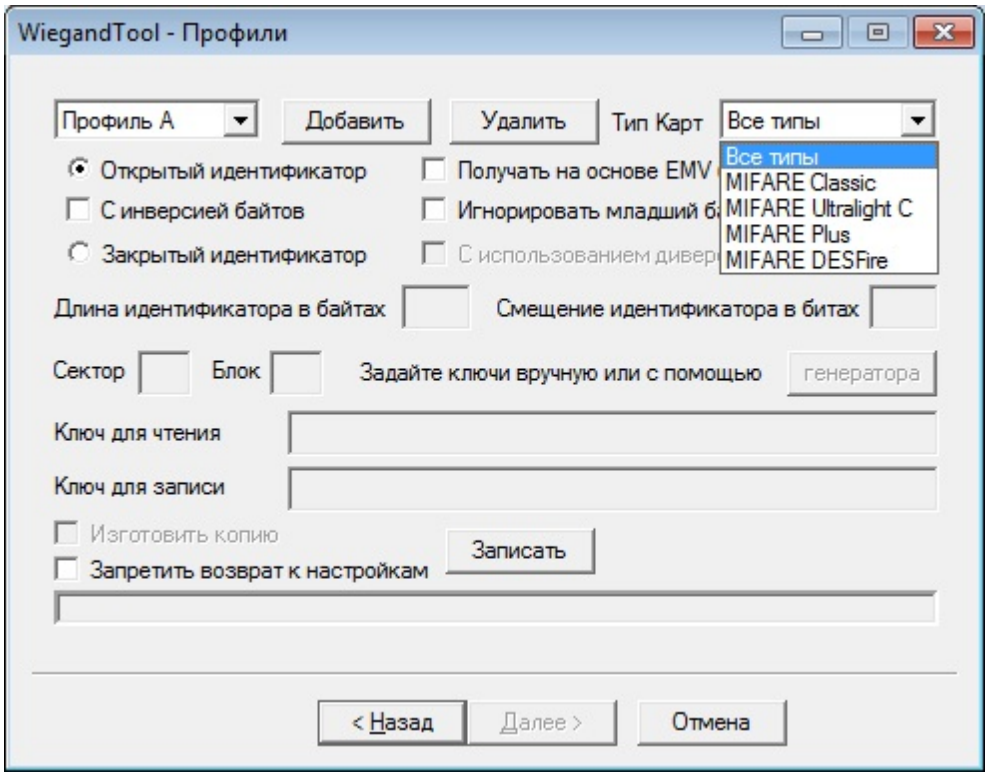
Для каждого профиля необходимо уточнить, что именно будет являться идентификатором пропуска СКУД: UID карты ("Открытый идентификатор") или данные, расположенные в ее защищенной области памяти ("Закрытый/защищенный идентификатор").



Допустимо использование только одного профиля с открытым идентификатором.

При создании мастер-карты, в ней автоматически прописывается всего один профиль - открытый идентификатор. Этот профиль позволяет вычитывать заводские уникальные идентификаторы чипов бесконтактных карт для любого типа карт.

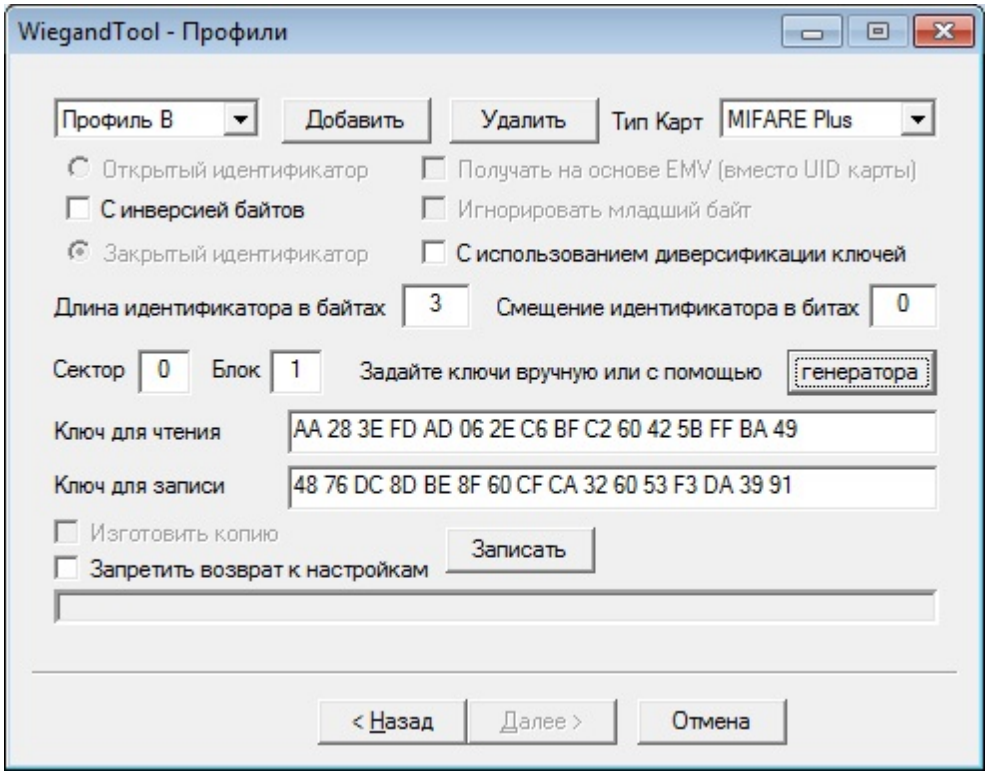
Чтобы задать конкретный тип карты, используете выкидной список с перечнем поддерживаемых типов.



Если вы при автономном режиме работы считывателя используете открытый идентификатор (открытый режим), то вы можете выбрать опцию получения идентификатора на основе EMV. Если эта опция активна, то при поднесении к считывателю смартфона с включенным NFC или банковской карты, считыватель будет создавать уникальный открытый идентификатор (UID) карты/смартфона на основании статических уникальных данных карты/смартфона в поле, которые считыватель получит автоматически. И только при неудачной попытке такого считывания, будет использоваться обычный открытый идентификатор согласно используемому протоколу. *На начало 2021 года это единственная возможность использовать iPhone в качестве NFC пропуска, без нашего мобильного приложения, использующего на iPhone только Bluetooth.* **Важно: полученный таким образом *открытый идентификатор не несет в себе никаких персональных, в том числе платежных, данных пользователя системы: идентификатор обезличивается программно, а считыватель и система в целом не сохраняют и не передают такие данные.*** **Тем не менее, если вы планируете использовать данный метод создания открытого идентификатора в своей системе доступа, то вы как организатор/владелец системы доступа обязаны предварительно получить согласие всех ее пользователей на обработку их персональной информации, поскольку *считыватель будет обращаться к системным приложеням на картах/ смартфонах, но только для чтения статической информации, находящейся***

там в открытом доступе: **никаких финансовых операций, никаких операций записи/изменений в банковских картах или платежных приложениях на смартфонах считыватель самостоятельно не выполняет.**

Если вы измените/добавите профиль на использование закрытого (защищенного) идентификата/режима, то для такого вида профиля нужно будет задать номер сектора и блока карты-пропуска для хранения уникального идентификатора пропуска, тип используемой карты, а также ключ доступа к сектору.



Для карт Ultralight C абсолютный номер блока переводится в адрес следующим образом:

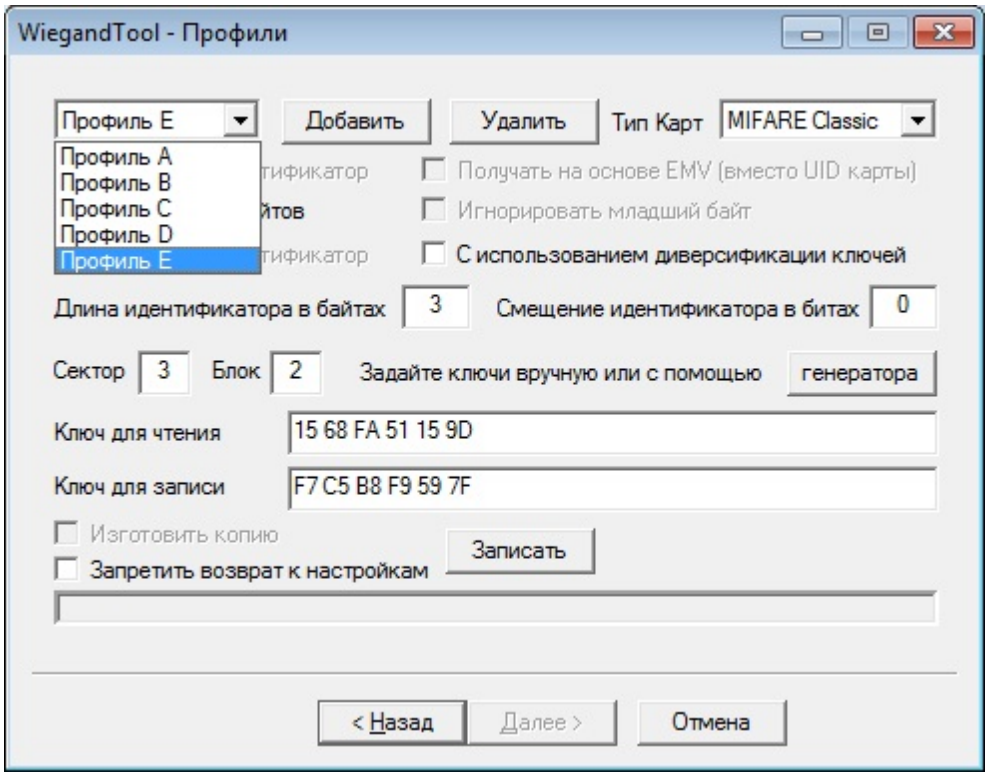
Mf_Ul_Page = (AbsBlockNo % 9 + 1) << 2.

Кроме того, в настройках профиля вы можете выбрать диверсифицировать или нет ключи карт-пропусков. Если выбрана диверсификация, то ключи доступа к секторам карт-пропусков будут разными для каждой отдельной карты-пропуска, и будут вычисляться на основании общего мастер-ключа и уникальных открытых идентификаторов пропусков.

Профили можно добавлять (до 12 штук) при помощи кнопки "Добавить". При этом новый профиль получит свободную латинскую букву обозначения и будет добавлен

в конец выкидного списка.

Удаление профилей производится при помощи кнопки "Удалить". Для удаления предварительно выберите ненужный профиль в выкидном списке.



Если все параметры протокола заданы, необходимо нажать кнопку "Записать" - общие параметры, а также обновленный список профилей доступа к картам-пропускам будут сохранены в мастер-карту.

При последующем нажатии на кнопку "Далее", откроется окно работы с картами-пропусками.

3.2.4 Работа с картой-пропуском

Карта-пропуск используется при непосредственном проходе через двери.

В качестве карты-пропуска также может быть использован смартфон, поддерживающий технологию NFC HCE (эмуляция карт NFC), либо BLE (Bluetooth Low Energy)

Для работы с картой-пропуском предварительно требуется использовать карту-ключ и мастер-карту.

Если карты-ключа у вас нет, сперва ее нужно создать, выполнив действия из раздела "Изготовление карты-ключа".

Если карта-ключ у вас имеется, ее нужно прочитать, выполнив действия из раздела "Применение карты-ключа".

После выполнения этих действий уберите карту-ключ со считывателя.

Если мастер-карты у вас нет, сперва ее нужно создать, выполнив действия из раздела "Изготовление мастер-карты".

Если мастер-карта у вас имеется, ее нужно прочитать, выполнив действия из раздела "Применение мастер-карты".

После выполнения этих действий уберите мастер-карту со считывателя.

В следующем окне можно изготовить бесконтактную карту-пропуск, либо виртуальную карту-пропуск на смартфоне, а также прочитать или изменить идентификатор в уже имеющейся карте-пропуске.

Если ранее в настройках мастер-карты в качестве идентификатора пропуска был выбран UID карты, то данное окно не используется.

3.2.4.1 Пропуска в виде бесконтактных карт

3.2.4.1.1 Изготовление карты-пропуска

Для изготовления карты-пропуска на основе карт типа MIFARE Plus и MIFARE Classic допускается использование бывшей в употреблении карты со свободным сектором, имеющим ключи по умолчанию (все единички), при этом единственное ограничение - все карты-пропуска в данной системе контроля доступа должны иметь один и тот же номер сектора для хранения уникального идентификатора.

Ограничения в использовании б/у карт MIFARE Plus SL3 и MIFARE Classic:

- необходимо наличие свободного сектора с единичными ключами и чтением/записью по ключу A;

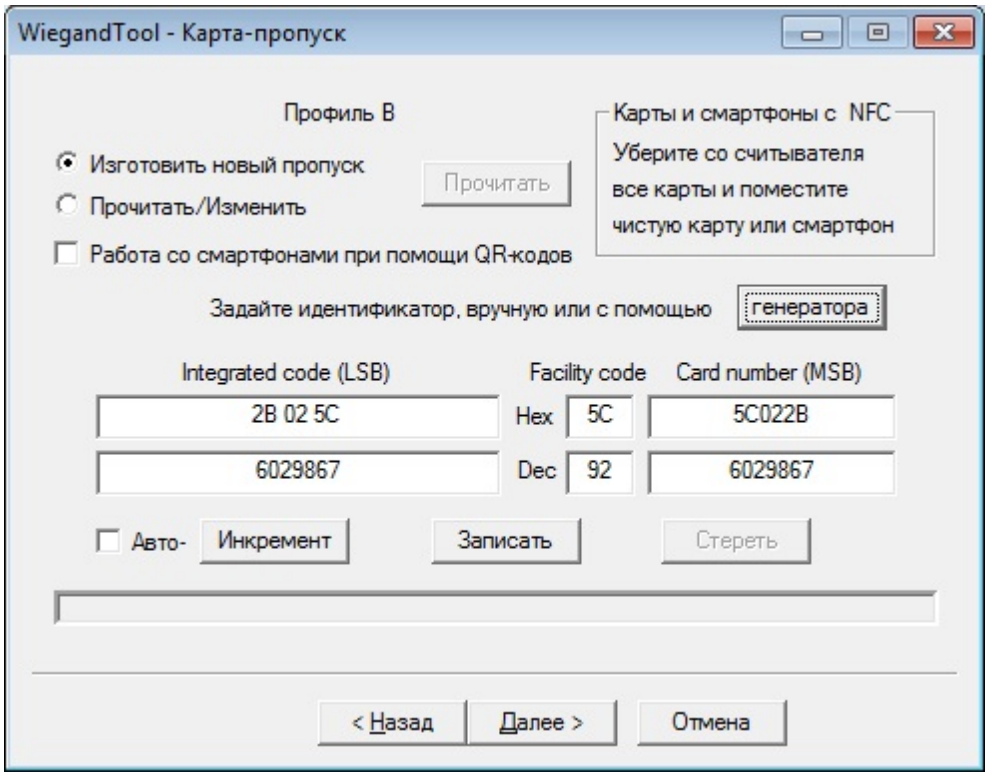
- номер свободного сектора должен совпадать с номером сектора в пропусках данной СКУД.

Дополнительно для карт MIFARE Plus:

- после перевода карты в T=CL аутентификация используемого сектора должна быть доступна без каких-либо дополнительных операций.

Дополнительно для карт MIFARE Plus EV1:

- карта должна иметь ATS, где T0 = 0x78.



Для изготовления карты-пропуска с UID, хранящимся в защищенной области памяти карты:

- поместите на считыватель чистую карту типа MIFARE Plus, MIFARE Ultralight C или MIFARE Classic;
- выберите пункт "Изготовить новый пропуск";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" НЕ установлена;
- в поле "Integrated code" слева от слова "Hex" укажите уникальный идентификатор карты в формате HEX:

- для Wiegand-26: 3 байта;

- для Wiegand-33: 4 байта;

- для Wiegand-34: 4 байта;

- для Wiegand-37: 5 байт;

- для Wiegand-40: 5 байт;

- для Wiegand-42: 5 байт;

- для Wiegand-58: 7 байт;

- для 1-Wire: 6 байт.

Вы также можете задать идентификатор путем вписывания по отдельности значений Facility Code (код подразделения) и Card number (номер карты).

Как альтернатива, вы можете задать значения полей в десятичном формате, воспользовавшись дублирующими полями ввода, расположенными под полями ввода значения в шестнадцатеричном формате Hex.

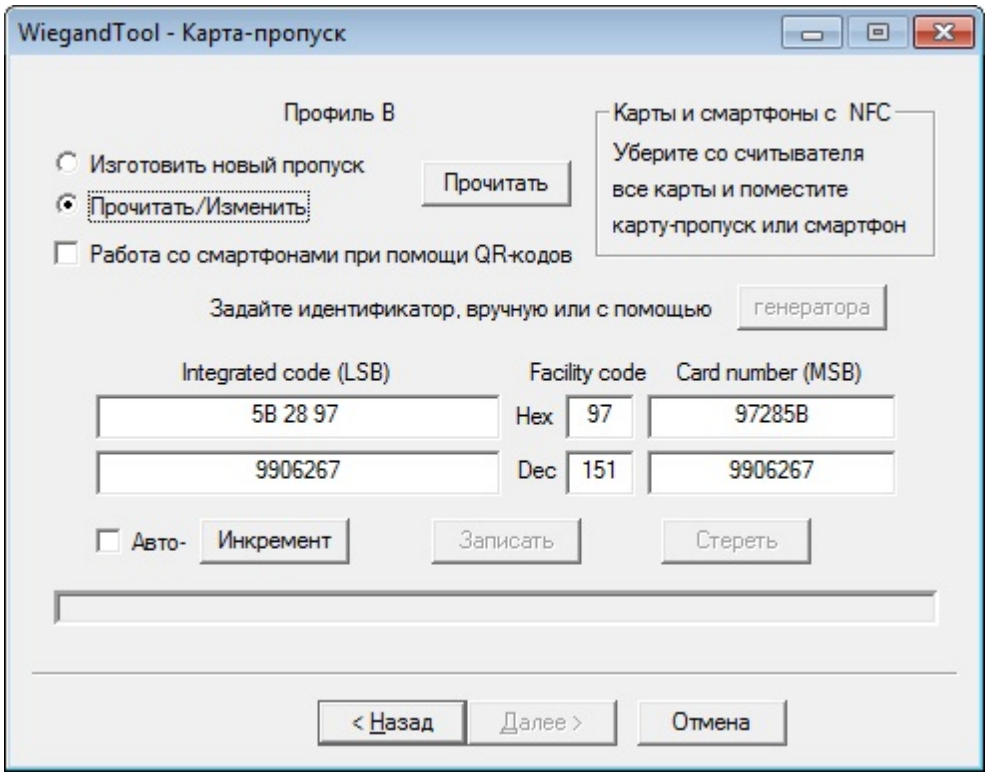
Можно разово увеличить значение на 1 при помощи кнопки "Инкремент", либо увеличивать автоматически при помощи галочки "Авто".

- нажмите на кнопку "Записать".

3.2.4.1.2 Чтение и изменение настроек карты-пропуска

Для чтения идентификатора карты-пропуска с UID, хранящимся в открытой или защищенной области памяти карты:

- поместите на считыватель карту-пропуск;
- выберите пункт "Прочитать/Изменить";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" НЕ установлена;
- нажмите на кнопку "Прочитать".



Для изменения идентификатора карты-пропуска с UID, хранящимся в защищенной области памяти карты:

- поместите на считыватель карту-пропуск;
- выберите пункт "Прочитать/Изменить";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" НЕ установлена;
- нажмите на кнопку "Прочитать";
- измените уникальный идентификатор карты (можно разово увеличить значение на 1 при помощи кнопки "Инкремент", либо увеличивать автоматически при помощи галочки "Авто");
- нажмите на кнопку "Записать".

3.2.4.2 Пропуска в виде виртуальных карт на смартфонах с интерфейсом NFC

Для работы в качестве бесконтактного пропуска в системе, на Android-смартфоне через функцию NFC:

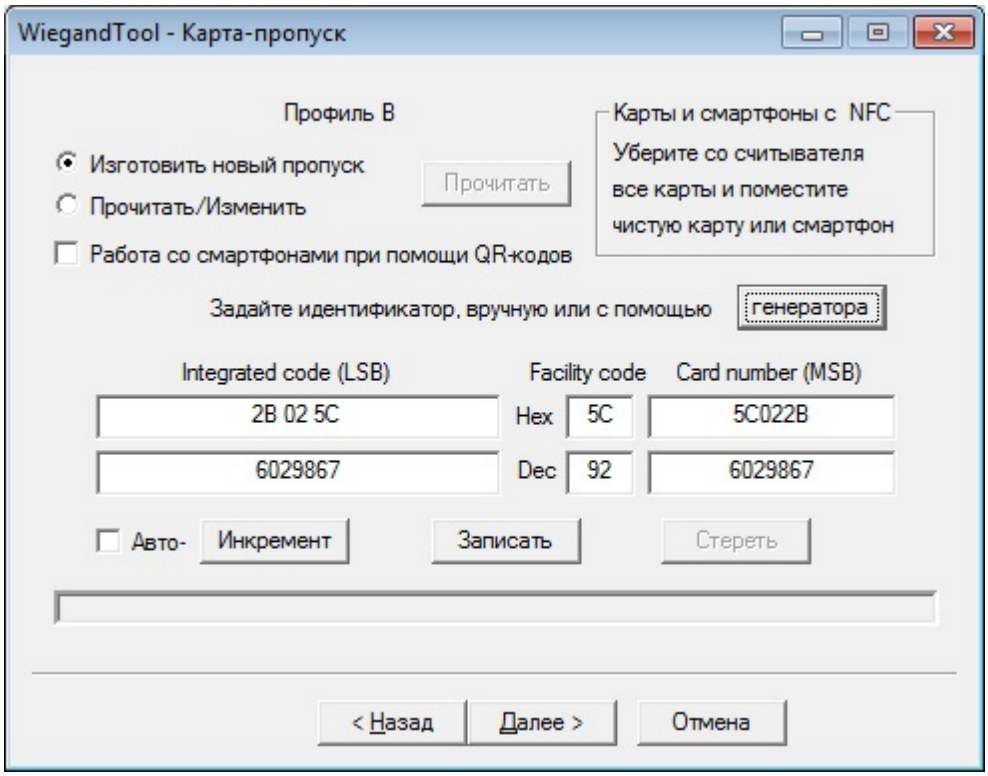
1) должно быть установлено специализированное приложение: https://

play.google.com/store/apps/details?id=ru.microem.virtualcard

2) в настройках смартфона должен быть активирован модуль NFC.

3.2.4.2.1 Изготовление виртуальной карты-пропуска

С точки зрения работы с приложением WiegandTool процедура изготовления виртуальной карты-пропуска на смартфоне, в случае применения технологии NFC, аналогична процедуре изготовления бесконтактной карты-пропуска:



Для изготовления защищенного идентификатора виртуальной карты-пропуска:

- создайте новую виртуальную карту или выберите уже существующую виртуальную карту в настройках приложения MicroEM Virtual Card на смартфоне;
- положите смартфон на считыватель;
- в WiegandTool выберите пункт "Изготовить новый пропуск";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" НЕ установлена;
- в поле "Integrated code" слева от слова "Hex" укажите уникальный идентификатор

карты в формате HEX:

- для Wiegand-26: 3 байта;
- для Wiegand-33: 4 байта;
- для Wiegand-34: 4 байта;
- для Wiegand-37: 5 байт;
- для Wiegand-40: 5 байт;
- для Wiegand-42: 5 байт;
- для Wiegand-58: 7 байт;
- для 1-Wire: 6 байт.

Вы также можете задать идентификатор путем вписывания по отдельности значений Facility Code (код подразделения) и Card number (номер карты).

Как альтернатива, вы можете задать значения полей в десятичном формате, воспользовавшись дублирующими полями ввода, расположенными под полями ввода значения в шестнадцатеричном формате Hex.

Можно разово увеличить значение на 1 при помощи кнопки "Инкремент", либо увеличивать автоматически при помощи галочки "Авто".

- нажмите на кнопку "Записать".

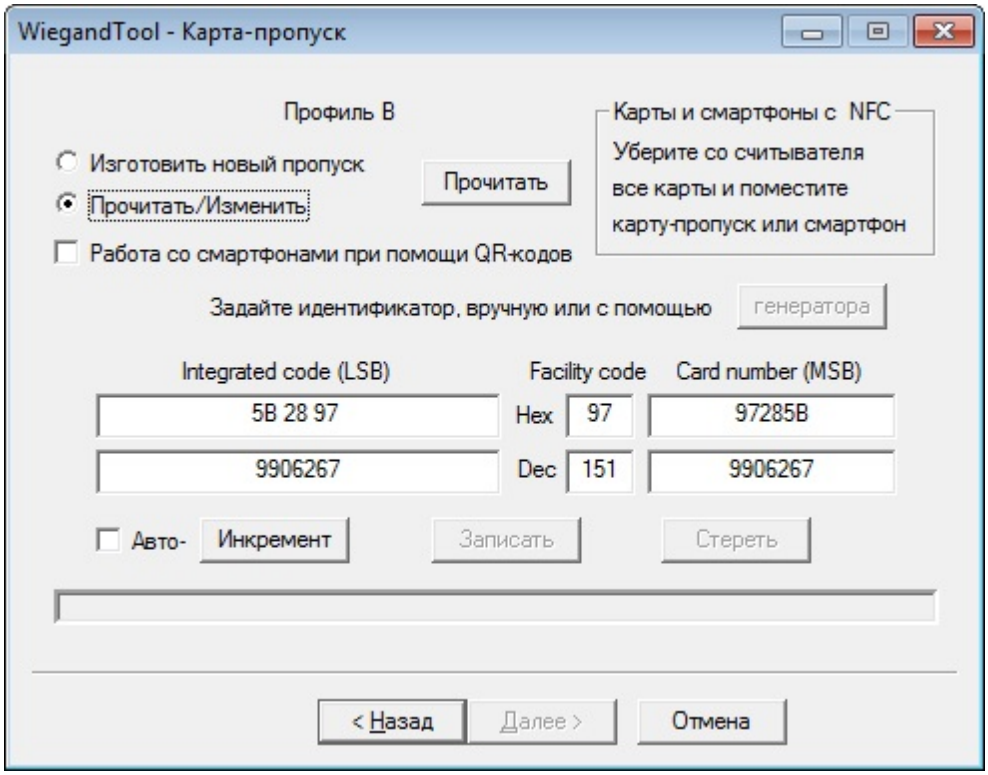
3.2.4.2.2 Чтение и изменение настроек виртуальной карты-пропуска

С точки зрения работы с приложением WiegandTool процедура чтения виртуальной карты-пропуска на смартфоне и изменения ее идентификатора, в случае применения технологии NFC, аналогична процедуре чтения и изменения бесконтактной карты-пропуска.

Для чтения открытого или защищенного идентификатора виртуальной карты-пропуска:

- выберите уже существующую виртуальную карту в настройках приложения MicroEM Virtual Card на смартфоне;
- если считывается открытый идентификатор со смартфона на базе Андроид, установите в приложении смартфона на главной странице галочку "Однократно передать открытый идентификатор";

- поместите на считыватель смартфон;
- выберите пункт "Прочитать/Изменить";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" НЕ установлена;
- нажмите на кнопку "Прочитать".



Для изменения защищенного идентификатора виртуальной карты-пропуска:

- выполните последовательность действий при чтении защищенного идентификатора виртуальной карты-пропуска, описанную выше;
- измените уникальный идентификатор карты (можно разово увеличить значение на 1 при помощи кнопки "Инкремент", либо увеличивать автоматически при помощи галочки "Авто");
- нажмите на кнопку "Записать".

3.2.4.3 Пропуска в виде виртуальных карт на смартфонах с интерфейсом Bluetooth

Для работы в качестве бесконтактного пропуска в системе, на Android-смартфоне

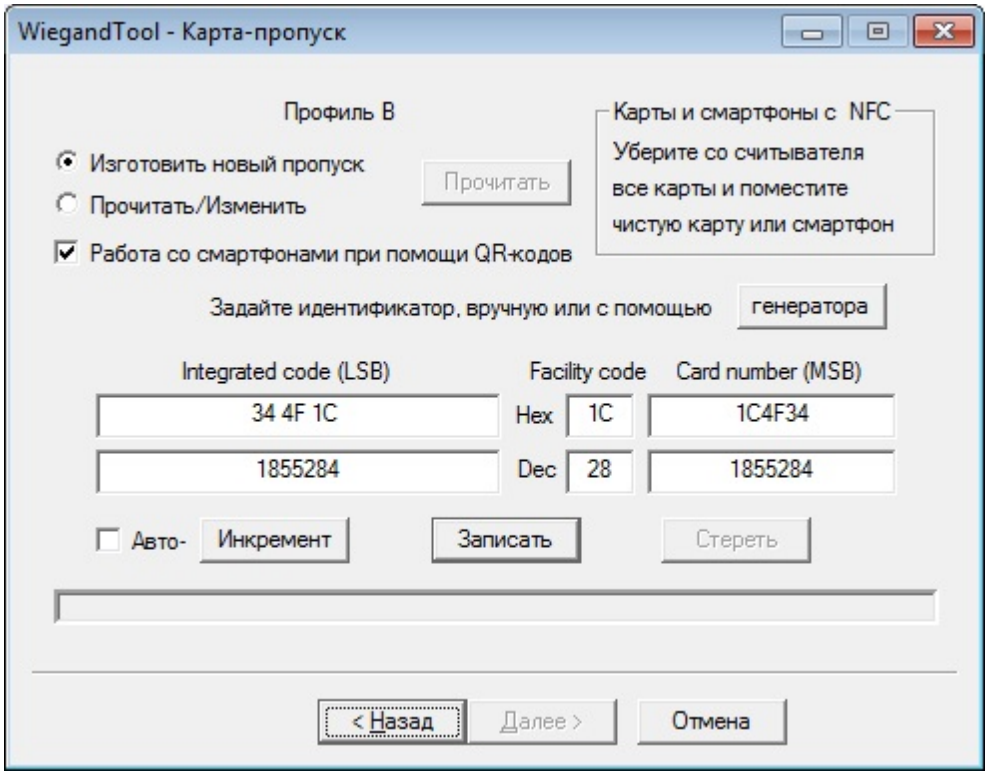
посредством Bluetooth:

1) должно быть установлено специализированное приложение: https://play.google.com/store/apps/details?id=ru.microem.virtualcard

2) в настройках должен быть активирован модуль Bluetooth.

3.2.4.3.1 Изготовление виртуальной карты-пропуска

С точки зрения работы с приложением WiegandTool процедура изготовления виртуальной карты-пропуска на смартфоне, в случае применения технологии Bluetooth, аналогична процедуре изготовления бесконтактной карты-пропуска, однако передача информации от WiegandTool в приложение на смартфоне осуществляется при помощи графических QR-кодов.



Для изготовления виртуальной карты-пропуска с защищенным идентификатором:

- создайте новую виртуальную карту или выберите уже существующую виртуальную карту в списке карт в настройках приложения MicroEM Virtual Card на смартфоне;
- откройте настройки виртуальной карты на смартфоне, перейдите по ссылке

"Добавить/изменить защищенный идентификатор"; при необходимости разрешите приложению на смартфоне пользоваться камерой;

- в WiegandTool выберите пункт "Изготовить новый пропуск";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" установлена;
- в поле "Integrated code" слева от слова "Hex" укажите уникальный идентификатор карты в формате HEX:

- для Wiegand-26: 3 байта;

- для Wiegand-33: 4 байта;

- для Wiegand-34: 4 байта;

- для Wiegand-37: 5 байт;

- для Wiegand-40: 5 байт;

- для Wiegand-42: 5 байт;

- для Wiegand-58: 7 байт;

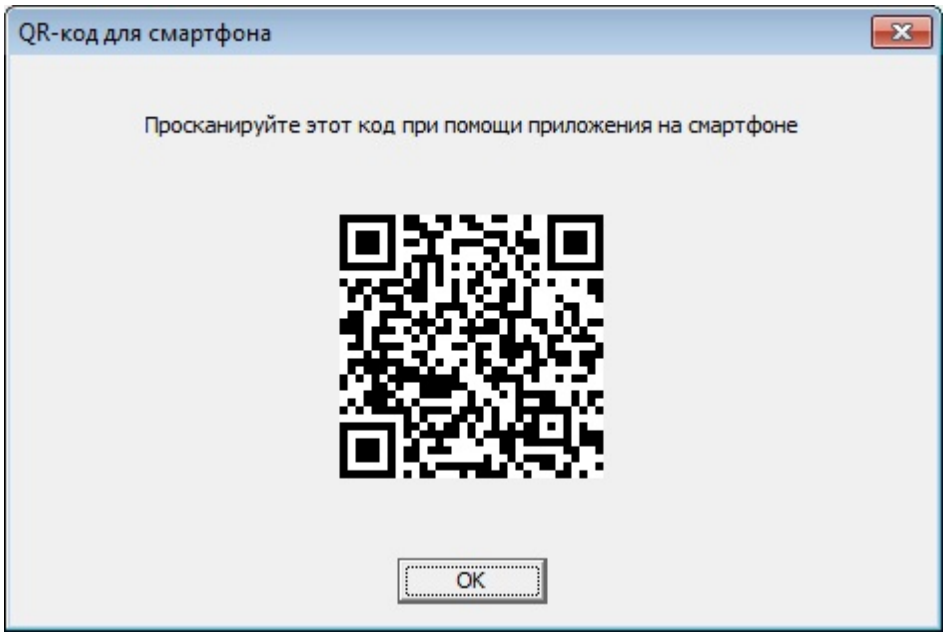
- для 1-Wire: 6 байт.

Вы также можете задать идентификатор путем вписывания по отдельности значений Facility Code (код подразделения) и Card number (номер карты).

Как альтернатива, вы можете задать значения полей в десятичном формате, воспользовавшись дублирующими полями ввода, расположенными под полями ввода значения в шестнадцатеричном формате Hex.

Можно разово увеличить значение на 1 при помощи кнопки "Инкремент", либо увеличивать автоматически при помощи галочки "Авто".

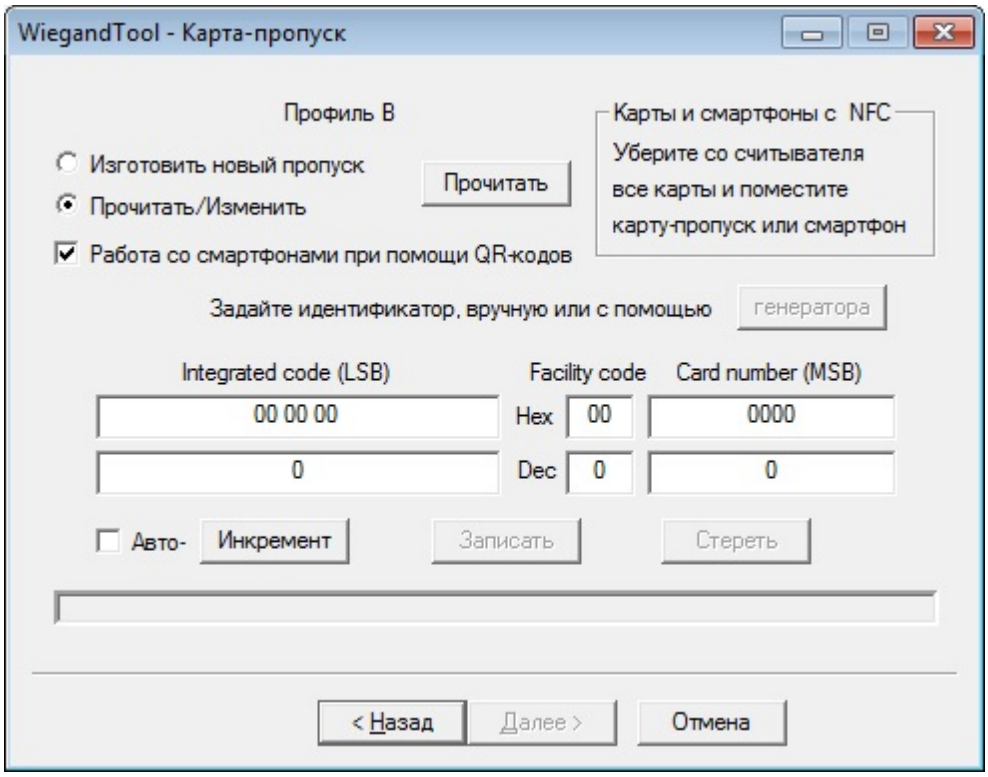
- нажмите на кнопку "Записать";



- в открывшемся окне нажмите на кнопку "Нажмите и прочитайте QR-код справа", подождите, пока на диалоговом окне отрисуется код;
- поднесите смартфон к экрану ПК и просканируйте QR-код;
- при успешном прохождении процедуры приложение на смартфоне уведомит вас об этом, и вы можете закрыть диалоговое окно с кодом в WiegandTool;
- при ошибке вы можете повторить попытку считывания кода или прекратить процедуру на смартфоне, вернувшись в настройки виртуальной карты.

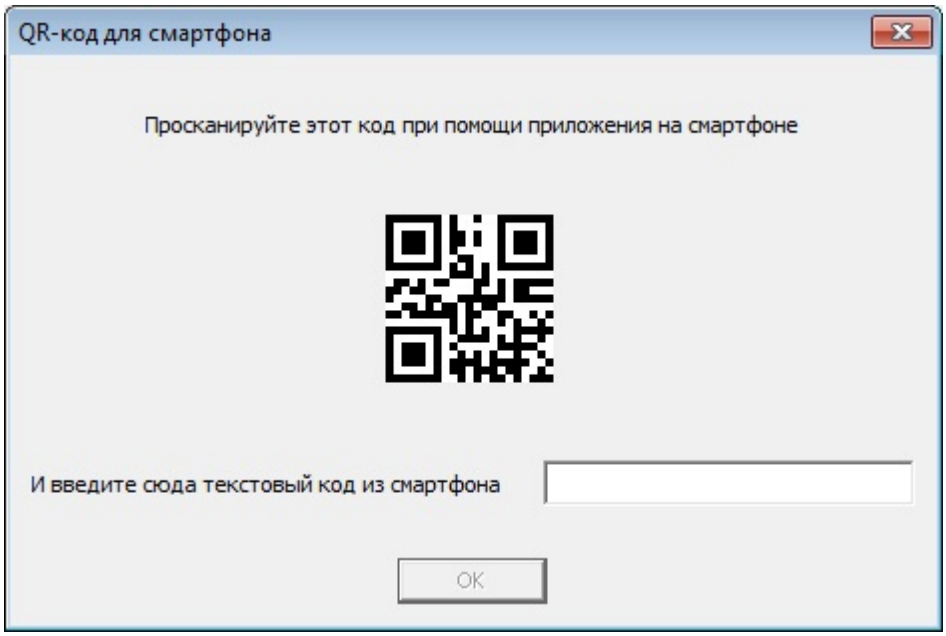
3.2.4.3.2 Чтение и изменение настроек виртуальной карты-пропуска

С точки зрения работы с приложением WiegandTool процедура чтения защищенного идентификатора виртуальной карты-пропуска на смартфоне и его изменения, в случае применения технологии Bluetooth, аналогична процедуре чтения и изменения бесконтактной карты-пропуска, однако передача информации от WiegandTool в приложение на смартфоне осуществляется при помощи графических QR-кодов, а в обратную сторону - путем копирования специальной символьной строки.



Для чтения защищенного идентификатора виртуальной карты-пропуска:

- выберите уже существующую виртуальную карту в списке карт в настройках приложения MicroEM Virtual Card на смартфоне;
- откройте настройки виртуальной карты на смартфоне, перейдите по ссылке "Добавить/изменить защищенный идентификатор"; при необходимости разрешите приложению на смартфоне пользоваться камерой;
- в WiegandTool выберите пункт "Прочитать/Изменить";
- убедитесь, что галочка "Работа со смартфонами при помощи QR-кодов" установлена;
- нажмите на кнопку "Прочитать".



- поднесите смартфон к экрану ПК и просканируйте QR-код;
- при ошибке вы можете повторить попытку считывания кода или прекратить процедуру на смартфоне и в программе, вернувшись в настройки виртуальной карты.
- при успешном прохождении процедуры приложение на смартфоне уведомит вас об этом и отобразит символьную строку;
- скопируйте эту строку в поле ввода WiegandTool; вы можете копировать визуально, либо воспользоваться средствами электронной связи между устройствами;
- при успешной проверке кода программой WiegandTool, активируется кнопка "OK";
- после этого вы можете нажать на "OK" и закрыть диалоговое окно с кодом в WiegandTool;
- прочитанный из приложения на смартфоне защищенный идентификатор виртуальной карты отобразится в WiegandTool.

Для изменения защищенного идентификатора виртуальной карты-пропуска:

- выполните последовательность действий при чтении защищенного

идентификатора виртуальной карты-пропуска, описанную выше;

- в поле "Integrated code" слева от слова "Hex" измените уникальный идентификатор карты в формате HEX:

- для Wiegand-26: 3 байта;

- для Wiegand-33: 4 байта;

- для Wiegand-34: 4 байта;

- для Wiegand-37: 5 байт;

- для Wiegand-40: 5 байт;

- для Wiegand-42: 5 байт;

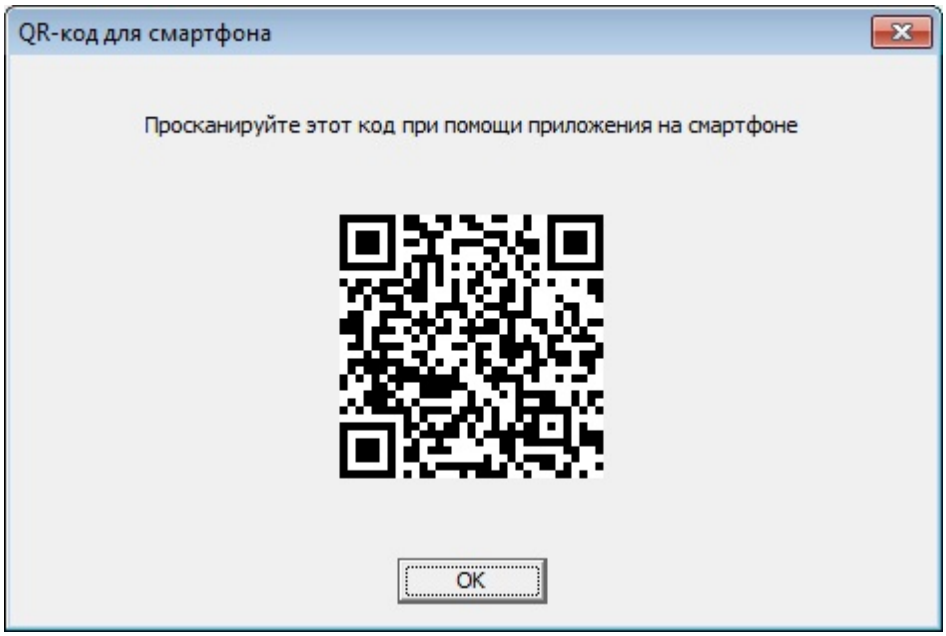
- для Wiegand-58: 7 байт;

- для 1-Wire: 6 байт.

Вы также можете задать идентификатор путем вписывания по отдельности значений Facility Code (код подразделения) и Card number (номер карты).

Как альтернатива, вы можете задать значения полей в десятичном формате, воспользовавшись дублирующими полями ввода, расположенными под полями ввода значения в шестнадцатеричном формате Hex.

- нажмите на кнопку "Записать";



- поднесите смартфон к экрану ПК и просканируйте QR-код;
- при успешном прохождении процедуры приложение на смартфоне уведомит вас

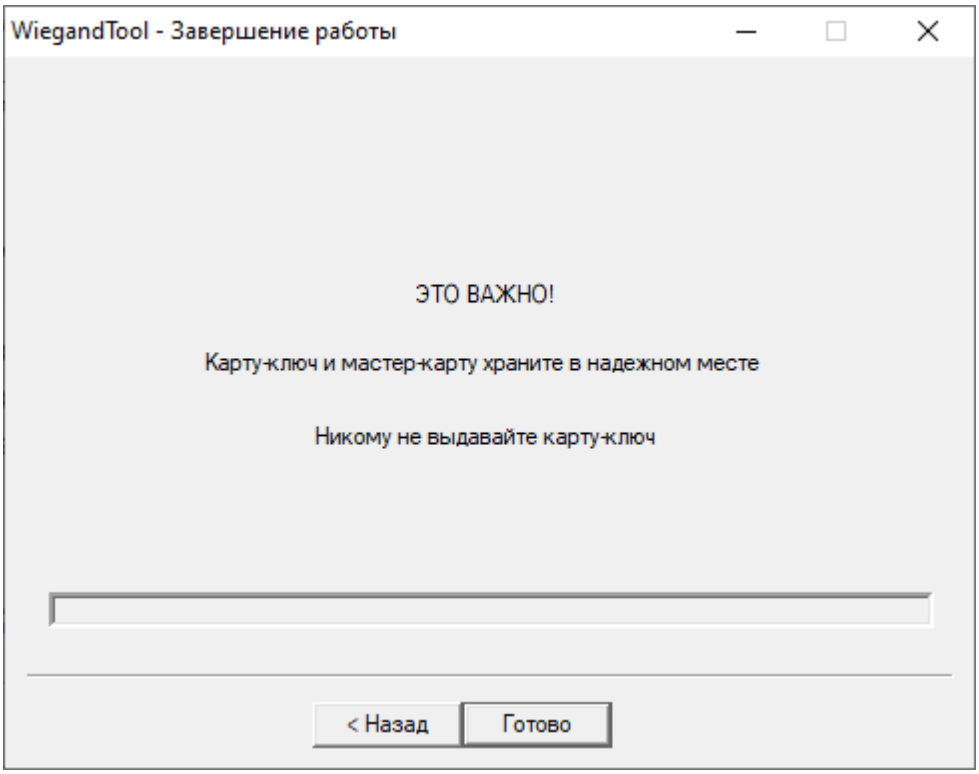
об этом, и вы можете закрыть диалоговое окно с кодом в WiegandTool;

- при ошибке вы можете повторить попытку считывания кода или прекратить процедуру на смартфоне, вернувшись в настройки виртуальной карты.

3.2.5 Завершение работы с программой

Вы можете выполнять операции по работе с картами-пропусками столько раз, сколько понадобится: пока приложение запущено, оно "помнит" необходимые настройки, вычитанные из ключ- и мастер-карт.

При необходимости приложение можно закрыть, нажав на "крестик" в правом верхнем углу. Также вы можете при помощи кнопок "Далее" дойти до конца программы и завершить ее там, нажав "Готово":



4 Доступ по картам-пропускам и смартфонам

Для доступа по карте-пропуску, поднесите карту к считывателю, дождитесь звукового сигнала.

В зависимости от выбранного интерфейса (1-Wire или Wiegand), при успешном считывании карты-пропуска или смартфона, идентификатор будет отсылаться по соответствующему интерфейсу.

Для доступа по смартфону Android:

1) активируйте на смартфоне в настройках модуль NFC, либо Bluetooth (в зависимости от предпочитаемого вами интерфейса активации считывателей);

2) запустите приложение Virtual Card MicroEM, убедитесь, что в настройках приложения включен нужный вам интерфейс, и приложению дано разрешение на использование этого интерфейса;

3) при использовании интерфейса NFC, поднесите смартфон к считывателю, дождитесь звукового сигнала считывателя;

4) при использовании интерфейса Bluetooth, поднесите смартфон к считывателю, убедитесь, что считыватель появился в списке на главной странице приложения, нажмите на кнопку "Активаровать", дождитесь звукового сигнала считывателя;

5) в целях экономии энергии, при желании деактивируйте модуль NFC или Bluetooth в смартфоне;

6) более подробную инструкцию по работе с приложением на смартфоне читайте в документе **Wiegand - Mobile.pdf**

Для получения максимального расстояния считывания бесконтактных карт или при использовании интерфейса NFC на смартфоне, подносите карту следующим образом: держите карту параллельно к поверхности считывателя, придвигайте карту медленно по направлению к считывателю до тех пор, пока не появится световая и/или звуковая индикация. Чтобы прочитать карту еще раз необходимо убрать ее из поля считывателя и поднести снова.

Для доступа по смартфону iPhone:

1) запустите приложение Virtual Card MicroEM;

2) поднесите смартфон к считывателю, убедитесь, что считыватель появился в списке на главной странице приложения, нажмите на кнопку "Активаровать", дождитесь звукового сигнала считывателя;

3) в целях экономии энергии, при желании деактивируйте модуль Bluetooth в смартфоне;

4) более подробную инструкцию по работе с приложением на смартфоне читайте в документе **Wiegand - Mobile.pdf**

4.1 Вычитывание идентификатора по интерфейсу RS-485

Дополнительно почитать последний считанный идентификатор можно по интерфейсу RS-485 в течение 3 секунд, по истечении которых он будет удален из памяти считывателя. Для этого нужно отправить команду 58 98 01 по нашему протоколу, описанному в документации на настольные считыватели здесь. Ответ на команду придет также в соответствии с протоколом, описанным в документации по ссылке выше. Краткое описание команды:

// Запрос 0x58 0x98 0x01

// Ответ: ACK[1], TotalSize[1], Standard[1], ID[TotalSize-2]

// TotalSize[1] – Общая длина элемента (включая TotalSize)

// Standard[1] :

// 0x01 - ISO14443A

// 0x02 - ISO14443B

// 0x04 - ISO15693

// 0x10 - EMV

// 0x20 - Bluetooth

// 0x40 - Защищенный режим

// 0x80 - Смартфон

Примеры:

Mifare 4 byte UID

58 98 01

00 06 01 94 C8 A6 03

Mifare 7 byte UID

58 98 01

00 09 01 04 82 6F F2 04 3E 80

ISO14443B

58 98 01

00 06 02 6F 33 24 02

4.2 Использование протокола MOD BUS

Считыватель поддерживает стандартную команду протокола MODBUS RTU (интерфейс RS-485).

0x03 Read Holding Registers

Считыватель имеет 11 регистров:

- Reg[0] - Size
- Reg[1] - UID0
- Reg[2] - UID1
- Reg[3] - UID2
- Reg[4] - UID3
- Reg[5] - UID4
- Reg[6] - UID5
- Reg[7] - UID6
- Reg[8] - UID7
- Reg[9] - UID8
- Reg[10] - UID9

В регистре Reg[0] располагается длина идентификатора UID, который в простейшем случае является номером карты.

Длина может принимать следующие значения:

- 0x0000 - нет карты,
- 0x0004 - MIFARE Classic 1K/4K, либо NTAG
- 0x0007 - MIFARE Ultralight, либо Classic 1K/4K, либо Plus (EV1) 2K/4K, либо NTAG

- 0x0008 - NTAG
- 0x000A - защищенный идентификатор или открытый идентификатор на основе EMV.

Идентификатор располагается в буфере, который представляет собой совокупность из 10 последовательных регистров, начиная с Reg[1].

В буфере располагается UID, по одному байту в регистре.

Если карты нет, все регистры содержат нули.

Очередной байт UID располагается в младших 8 битах регистра, старшие 8 битов регистра равны 0. Лишние регистры содержат нули.

UID хранится в буфере все время, пока карта находится в поле действия считывателя, плюс 1 секунду после ее изъятия.

Обработка ошибок производится следующим образом.

Считыватель не отвечает, если вычисленный CRC не совпадает с CRC, полученным в команде, или адрес считывателя не совпадает с адресом в команде, а также если считыватель неисправен или не подключен к питанию. В остальных случаях, когда считыватель не может выполнить команду, он отвечает кодом ошибки:

- 0x01 - принятый код команды не поддерживается;
- 0x02 - адрес данных, указанный в команде, недоступен.

Примеры

05 04 00 00 00 01 30 4E

05 84 01 C3 01

код команды не поддерживается

05 03 00 01 00 0C 15 8B

05 83 02 81 30

регистр недоступен

05 03 00 00 00 01 85 8E

05 03 02 00 00 49 84

нет карты

05 03 00 00 00 01 85 8E

05 03 02 00 07 08 46

длина UID 7 байтов

05 03 00 01 00 07 54 4C

05 03 0E 00 04 00 D2 00 FC 00 F2 00 EF 00 56 00 80 B6 87

UID = (LSB) 04 D2 FC F2 EF 56 80

05 03 00 00 00 01 85 8E

05 03 02 00 04 48 47

длина UID 4 байта

05 03 00 01 00 04 14 4D

05 03 08 00 CC 00 D6 00 A6 00 3C 25 0B

UID = (LSB) CC D6 A6 3C

05 03 00 00 00 0B 05 89

05 03 16 00 07 00 04 00 D2 00 FC 00 F2 00 EF 00 56 00 80 00 00 00 00 00 00 04 16

чтение всех регистров одновременно

Конфигурация

При изготовлении считыватель получает адрес на шине RS485, равный 0, и производит обмен данными на скорости 9600 бод.

Есть возможность переключить скорость на 19200, 38400, 57600 или 115200 бод.

Для работы по протоколу MODBUS RTU адрес считывателя должен быть в пределах от 1 до 247.

Требуемые адрес и скорость устанавливаются с помощью утилиты CLeSCaR:

1. На вкладке "Интерфейс" слева открыть интерфейс.
2. На вкладке "Считыватель" слева вверху выбрать требуемую скорость.
3. На вкладке "Интерфейс" справа вверху записать новый адрес.
4. Закрыть интерфейс.