Руководство пользователя
ЭНТ Контроль Доступа - RFID

Москва, 2020

Оглавление

1. Введение

Программа «ЭНТ контроль доступа RFID» предназначена для конфигурирования и работы со считывателями ЭРА-MF USB **(***настольное исполнение)* и ЭРА-MF **(***настенное исполнение***).** Оба считывателя оборудованы интерфейсом USB для быстрого и удобного подключения к ПК.

Считыватель ЭРА-MF USB используется для считывания и передачи в компьютер серийных номеров бесконтактных идентификаторов по интерфейсу USB, считыватель ЭРА-MF подключается к контроллеру СКД по интерфейсу Wiegand. Поддерживается работа с идентификаторами с рабочей частотой 13,56 МГц.

Программа позволяет выполнять следующие действия:

1) Читать ID карты;
2) Помещать ID карты в буфер обмена;
3) Осуществлять имитацию набора на клавиатуре;
4) Конфигурировать считыватель;
   a) выключить проверку контрольной суммы Wiegand;
   b) изменить разрядность интерфейса Wiegand (от 4 до 64);
   c) выбрать формат считываемых карт считывателем;
   d) включить обратный порядок байт;
   e) включить битовый сдвиг;
   f) включить «*хеш-функцию*».
5) Обновлять микропрограмму считывателя.

2. Работа с программой

2.1. Системные требования:

- ОС: Windows® 7/8/10 (32- или 64- битная версия)
- Один USB-порт
- Место на жестком диске: 10 Мб
- В ряде случаев необходимо установить **драйвер** для подключения считывателя к ПК. Драйвер находится в архиве с программой.

2.2. Запуск программы

Для запуска программы необходимо извлечь содержимое архива в папку c:\Program Files (x86)\ENT\usbreader\ после чего запустить файл Usbreader. После запуска на экране появится главное окно программы.

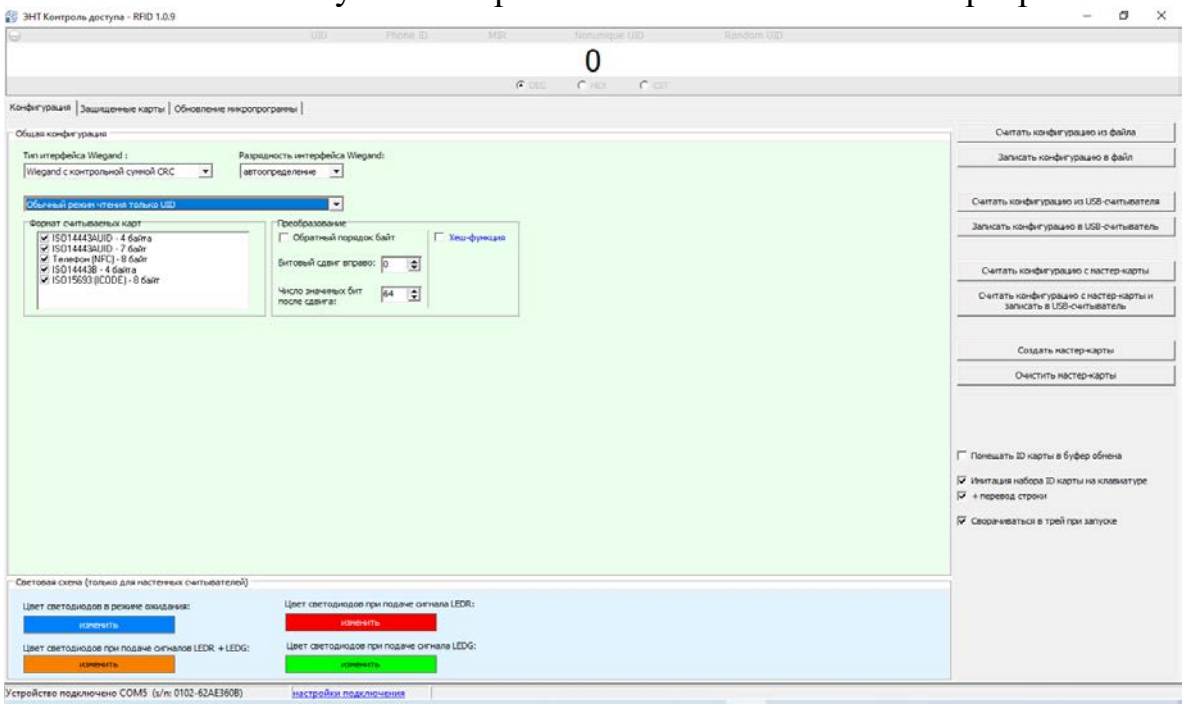

Рис. 1 (Внешний вид программы)

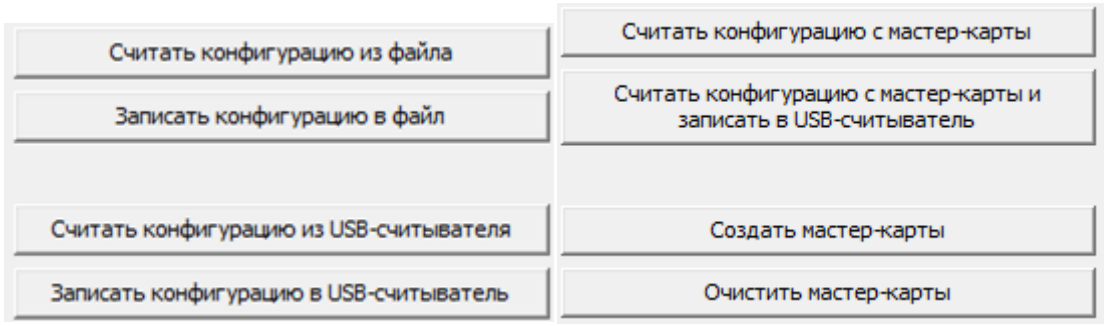

Рис. 2 (Опции, доступные во вкладке «Конфигурация»)

2.3. Подключение и настройка считывателя

Для выбора считывателя в программе предусмотрен автоматический поиск подключенного устройства, выбор номера COM-порта из списка и ручной ввод номера COM-порта.

Если ваш считыватель не определился автоматически, то настройка подключения осуществляется по нажатию на соответствующую кнопку (выделена синим) в нижней части программы. Автоматическое подключение может не работать в некоторых версиях Windows с последними пакетами обновлений.

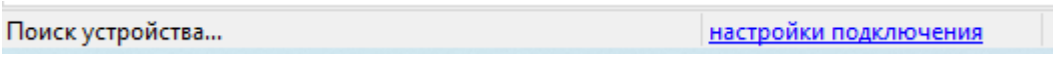

Рис. 3 (Строка состояния подключения)

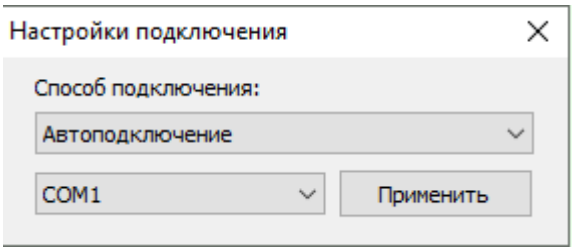

Рис. 4 (Настройки подключения)

По умолчанию считыватель работает со следующими настройками:

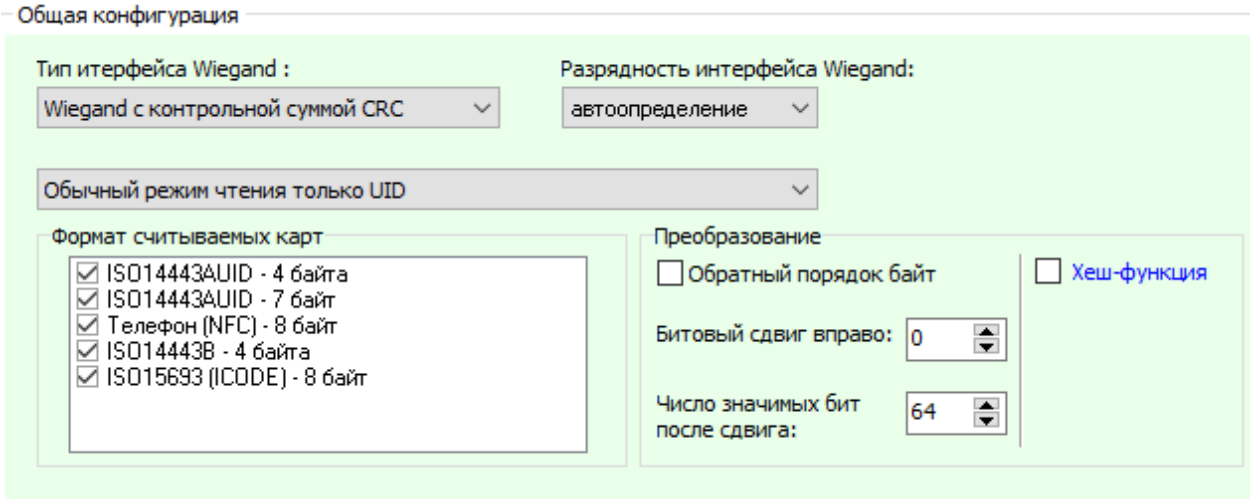

Рис. 5 (Настройки по умолчанию)

Описание опции «*хеш-функция*».

Когда длина идентификатора (карты доступа) больше разрядности протокола Wiegand можно использовать хеш-функцию для формирования итогового кода карты.

В программе приведено два примера реализации опции «*хеш-функция*».

2.4. Запись настроек в считыватель

Для записи нужной конфигурации в считыватель нужно нажать кнопку «Записать конфигурацию в USB-считыватель». Для просмотра ранее записанной конфигурации считывателя - нажмите кнопку «считать конфигурацию из считывателя». Для конфигурирования нескольких считывателей можно записать настройки в файл и считывать их при необходимости восстановления.

Для этого в правой части программы есть соответствующие кнопки.

При работе с считывателем необходимо в правой части программы выбрать «*помещать ID карты в буфер обмена*» либо «*имитация набора на клавиатуре*». Опционально, можно включить «*сворачивание программы в трей*».

3. Режимы работы чтения карт

3.1 Обычный режим чтения только UID

3.1.1 Описание

Данный режим используется для чтения исключительно идентификационного номера карты, запрограммированного на заводе-изготовителе. Данный режим сделан для случаев, когда на объекте уже используются бесконтактные карты, работающие на частоте 13,56МГц (различные вариации *Mifare, Icode* и другие). Данный режим **не является** защищенным, т.к. UID карты может быть легко скопирован. Для совместимости со считывателями других производителей возможно менять порядок байт, делать битовый сдвиг и устанавливать число значащих бит после сдвига кода карты, перед передачей по интерфейсу Wiegand или USB. Например, если в вашей системе используются считыватели с Wiegand 34, то вам нужно будет обозначить число значащих бит – 32, выбрать обратный порядок байт (если требуется), тип интерфейса – Wiegand с CRC, разрядность Wiegand – 32+CRC. Таким образом данный считыватель может **заменить любой считыватель** другого производителя для случаев работы с UID бесконтактных карт.

В данном режиме работы возможно выбирать какие типы карт должны быть прочитаны в системе:

1. *ISO14443A* с UID размером 4 байта (например, к данному варианту можно отнести карты *Mifare Classic* и др.)
2. *ISO14443A* с UID размером 7 байта (например, к данному варианту можно отнести карты *Mifare Ultralite* и др.)
3. Телефон с *NFC*
4. I*SO14443B*
5. *ISO15693* (ICODE)

3.1.2 Работа программы в «Обычном режиме»

Для работы в данном режиме считыватель должен быть сконфигурирован «по умолчанию».

При прикладывании карты к считывателю код этой карты отобразится в программе. Если был выбран вариант «*помещать ID карты в буфер обмена*», то код карты будет скопирован в буфер. Если был выбран пункт «*имитация набора для клавиатуре*», то код карты будет скопирован в

необходимую программу, например в «ЭНТ Контроль Доступа Клиент». Для этого необходимо выбрать то поле, куда должен быть помещен идентификатор карты. После этого поднести карту к считывателю. Код карты будет введен в выбранное поле.

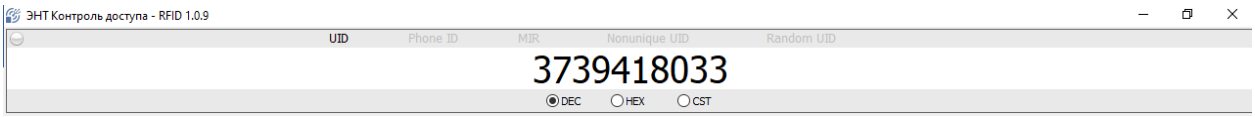

Рис. 6 (Код карты, считанный программой «RFID»)

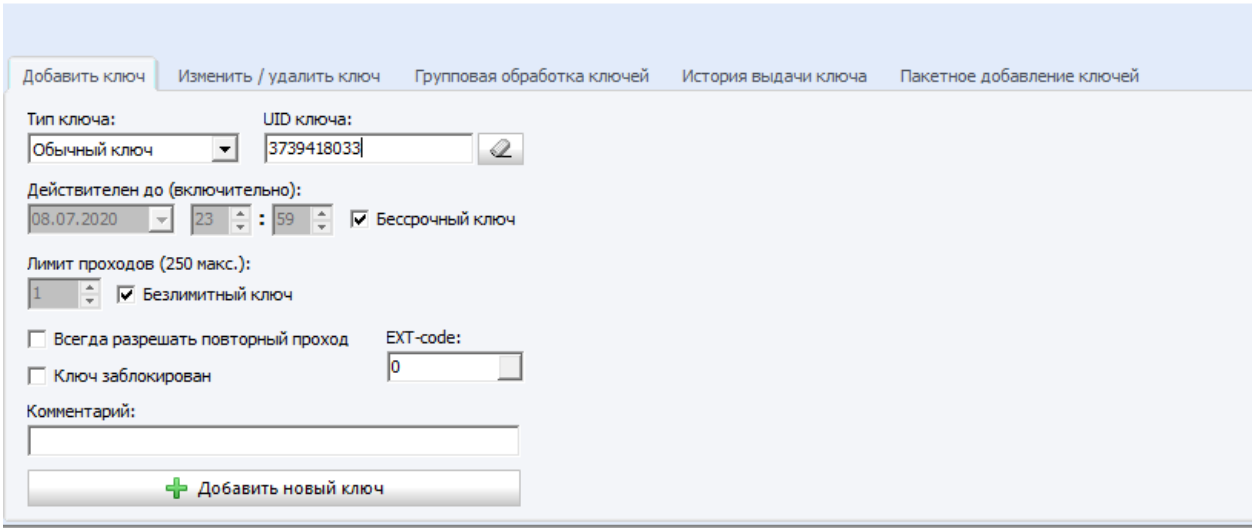

Рис. 7 (Код карты, переданный в программу «Клиент»)

3.2. Защищенный режим: код объекта

3.2.1 Описание

Данный режим является защищенным. Это означает, что идентификация карт будет происходить не по UID карты, а по информации, содержащейся в определенной области, закрытой от чтения секретным ключом. В данном режиме возможно использование **одного из двух** типов карт:

1. *Mifare Classic 1K* или *4K, (Mifare ID* не подойдет)
2. *Mifare Plus (SE, S, X)*

Поддержка *Mifare Classic* сделана исключительно для возможности использования в существующих системах, где уже имеется определенное количество карт в обороте и требуется повысить уровень безопасности. Следует понимать, что на текущий момент карты *Mifare Classic* нельзя считать безопасными, так как их можно копировать. Однако сделать это сложнее (дороже хоть и незначительно) чем скопировать UID. Для сравнения *Mifare Classic* и *Mifare Plus* можно привести следующую таблицу:

	Mifare Classic	Mifare Plus
Алгоритм шифрования	Crypto1	AES
Длинна ключа, бит	48	128

Для исключения возможности копирования карт, особенно при проектировании новых объектов, следует использовать карты стандарта *Mifare Plus*. Самые простые и, как следствие, доступные по цене – это карты *Mifare Plus SE 2K*. Карты большей емкости и стандартов *Plus S* и *Plus X* также могут быть успешно использованы в данном режиме.

Для данного режима следует использовать карты нигде ранее не использованные и находящиеся в так называемом «транспортном состоянии» (в этом состоянии находятся карты при выходе с завода-изготовителя). Этот момент важен, т.к. система конфигурирует карты самостоятельно и переводит их из «транспортного состояния» в режим *SL3*. Карты, переведенные в режим *SL1, SL2, SL3* считывателями другого производителя использоваться в данном режиме уже **НЕ смогут** (т.к. при этом будут использованы неизвестные системе коды доступа, а **перевод обратно в транспортный режим невозможен**)! Также следует отметить, что при переводе считывателем карт в режим *SL3* устанавливается *Random UID*. Т.е. карта будет выдавать каждый раз разный UID размером 4 байта при поднесении к считывателям, работающим только по UID. Это позволяет «обезличить» бесконтактные карты для любых сторонних систем.

Как в случае *Mifare Classic*, так и в случае *Mifare Plus* используется механизм диверсификации ключей. Это означает, что в каждой бесконтактной карте будут свои ключи для доступа к закрытым областям, что также положительно сказывается на защищенности системы. Подбор ключа для одной карты позволить скопировать только данную карту и не будет действителен для других карт.

Использование данного режима начинается с создания мастер-карт с кодом объекта. Всего мастер-карт с одинаковым кодом можно создать не более 5 штук. Все они создаются за один раз и нумеруются. Т.е. на каждой карте содержится информация сколько таких карт было создано и какой номер по порядку у данной карты. При чтении конфигурации с мастер-карты в заголовке всплывающего окна вы можете получить информацию о том, сколько было создано карт с такими настройками. Это важно если, после развертывания системы, заказчики захотят убедиться, что им были отданы все карты с кодом именно их объекта.

Код объекта формируется как случайное число при создании мастер-карты и содержится **только на мастер-картах, созданных единовременно** (до 5-ти мастер-карт). Посмотреть код объекта, переписать его куда либо,

принудительно создать другую мастер-карту (кроме уже созданных) с таким кодом невозможно! Помимо кода объекта мастер-карта содержит и другие настройки, которые фигурируют на вкладке данного режима. Мастер-карты могут быть использованы для дальнейшего конфигурирования считывателей с одинаковыми настройками на объекте без использования программы для ПК. С мастер-карты возможно считать настройки, кроме закрытых. Например, вместо кода объекта вы получите контрольную сумму кода объекта. Это позволит вам в случае необходимости определить какие мастер-карты содержат одинаковый код объекта (у них будут одинаковые контрольные суммы), но **в оригинальном виде код объекта вы посмотреть не сможете**.

В защищенном режиме «*код объекта*» на каждую карту пользователя записывается код объекта. Аналогичный код объекта записывается и в считыватели на этапе конфигурации. При прикладывании карты, считыватель, обращаясь к закрытой области, ищет там соответствующий код объекта. Если код найден, то считыватель выдает ID карты. Если код не найден или не соответствует, то ничего не происходит. Каждая карта пользователя может содержать более 10 различных кодов объектов, что позволяет использовать одну и туже карту на разных объектах.

Карты, которые были отформатированы данной системой могут быть использованы повторно, т.е. с карты можно удалить всю информацию с конфигурацией (стереть мастер-карту) и использовать ее как карту пользователя записав туда код объекта и наоборот. Так же с карты пользователя можно удалить конкретный код объекта (при наличии мастер-карты с этим кодом) или все коды объектов сразу. Данные возможности позволяют повторно использовать карты или даже менять коды объекта системы в процессе эксплуатации, если это необходимо.

На этапе создания мастер-карт можно использовать опцию настроек, при которой вы не сможете переконфигурировать считыватель другой мастер-картой (картой, у которой другой код объекта). Это возможно сделать только той картой (картами с одинаковым кодом объекта), с помощью которой он был переведен в данный защищенный режим. Эта функция позволяет избежать несанкционированного переконфигурирования системы.

3.2.2 Настройка системы в режиме «Код объекта»

1. В программе «ЭНТ контроль доступа RFID» выберите соответствующий режим работы и используемый тип карт;

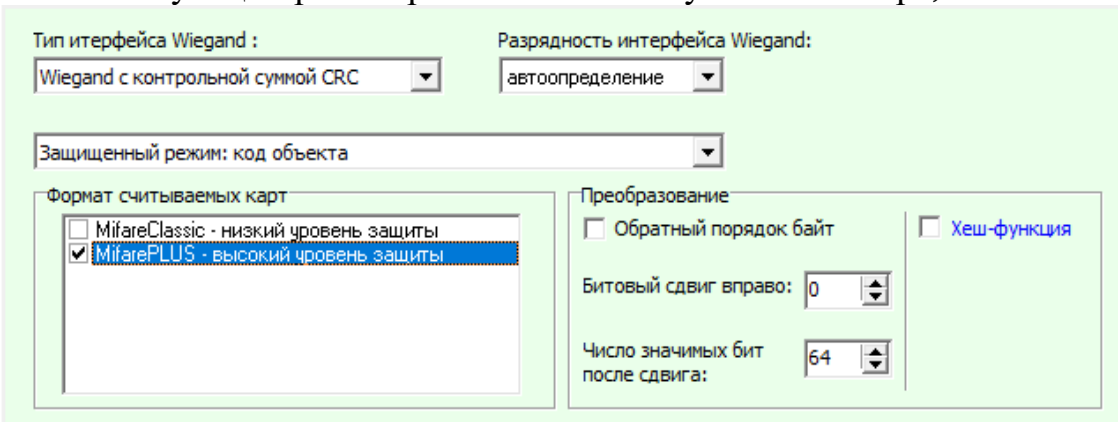

Рис. 8 (Режим работы «*код объекта*»)

2. Нажмите кнопку «*создать мастер-карты*» и указать количество создаваемых мастер карт;

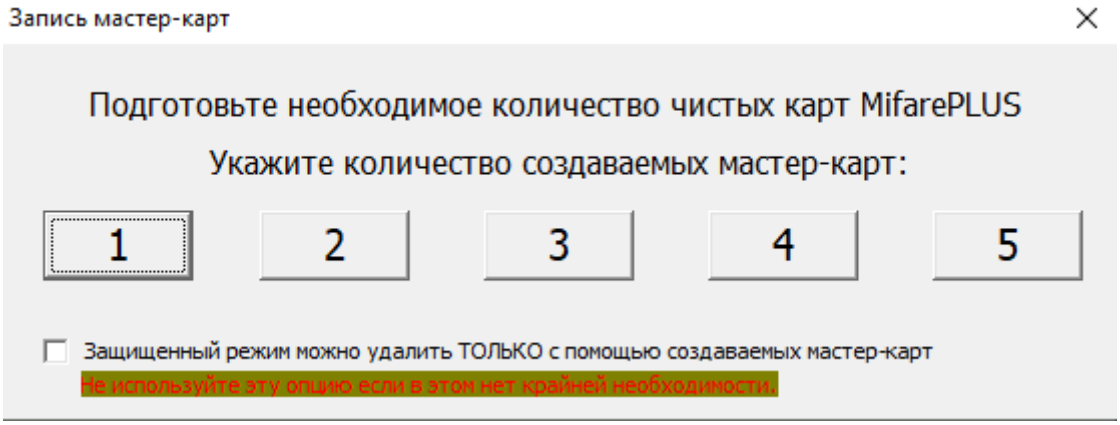

Рис. 9 (Запись мастер-карт)

При нажатии на соответствующую галочку защищенный режим работы считывателя можно будет удалить **только с помощью мастер-карт с таким же кодом объекта**. Т.е. если мастер-карта будет утеряна или стёрта, то переконфигурировать считыватель будет невозможно!!!

3. Нажмите кнопку «*записать конфигурацию в USB-считыватель*»;

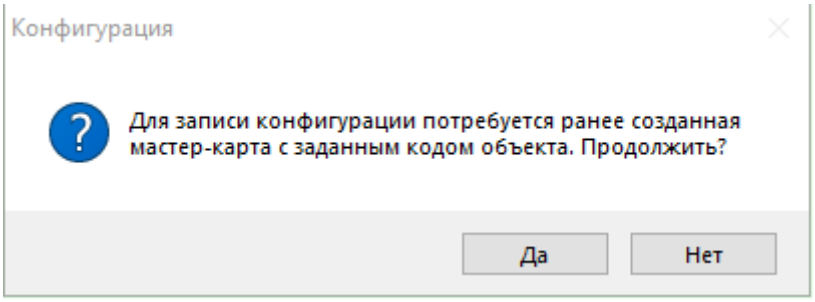

Рис. 10 (Запись конфигурации в считыватель)

4. Приложить ранее созданную мастер карту к USB-считывателю для подтверждения записи настроек;
5. Перейти во вкладку «*защищенные карты*», нажать кнопку «*создать защищенные карты*»;
6. Приложить ранее созданную мастер карту, после чего приложить; необходимое количество карт для доступа на объект;
7. Теперь в режим «*Код объекта*» необходимо перевести считыватели *ЭРА-MF*. Сделать это можно как при подключении к ПК, так и с помощью мастер-карты. Для конфигурации мастер-картой необходимо:
   a) При выключенном считывателе, перевести 4-ый дип-переключатель в положение On;
   b) Включить питание;
   c) Приложить ранее созданную мастер-карту с настройками;
   d) Перевести 4-ый дип-переключатель в положение Off;
   e) Выключить считыватель, после чего включить к его.
8. Осуществить добавление ключей в «ЭНТ контроль доступа Клиент» через считыватель *ЭРА-MF* или *ЭРА-MF USB*, либо с помощью меню **«пакетное добавление ключей»** и считыватель *ЭРА-MF* подключенный к контроллеру СКД.

Карты, которые не были сделаны «*защищенными*» в программе ЭНТ контроль доступа RFID не будут восприниматься считывателями *ЭРА-MF и ЭРА-MF USB*, работающими в «*защищенном*» режиме.

Пример:

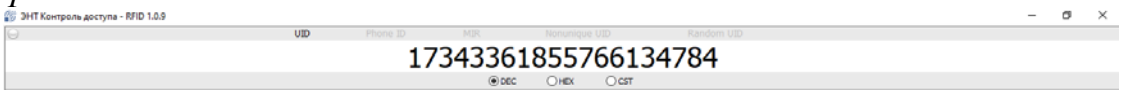

Рис. 11 (Код карты, считанный программой «RFID»)

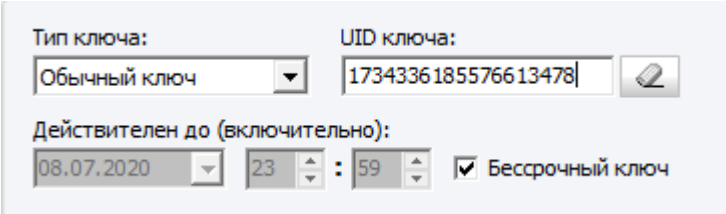

Рис. 12 (Код карты, переданный в программу «Клиент»)

3.3 Защищенный режим: чтение кода из блока

3.3.1 Описание

Данный режим предусмотрен для случаев, когда на объекте уже существует своя система с картами *Mifare Plus* в режиме *SL3*. В этом случае вы можете использовать как идентификатор информацию в закрытой области памяти карты. Для этого вам нужно указать номер блока, смещение в данном блоке и количество байт для передачи. Максимальное количество байт для передачи – *8*. Также вам требуется указать код доступа к данному блоку. Размер кода доступа *16* байт. В данном режиме код доступа вводиться в **открытом виде** и его следует беречь от «чужих глаз», так как он может быть легко скопирован для создания дубликатов карт и других нарушений. Как и в предыдущем защищенном режиме возможно создать до *5 мастер-карт* с настройками. При чтении настроек с мастер-карты пользователю будет выводиться *контрольная сумма* кода доступа к блоку, чтобы исключить его несанкционированное копирование.

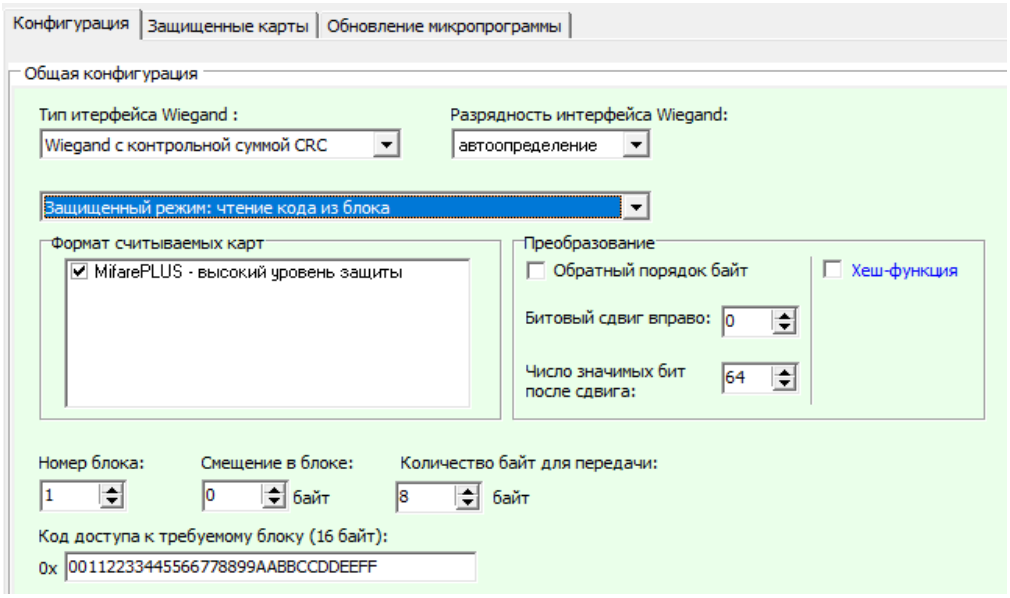

Рис. 13 (Режим «*чтение кода из блока*»)

3.4 Защищенный режим: зоны прохода

3.4.1 Описание

В данном режиме считыватель *ЭРА-MF* работает в роли контроля доступа. Отличительной чертой данного режима является тот факт, что **нет необходимости содержать базу** бесконтактных карт что в ряде случаев бывает исключительно удобно. Например, данный режим идеально подходит для больших жилых комплексов, где нет возможности вести базу и очень часто ставятся контроллеры в режиме автозаписи. Рассмотрим данный режим более подробно.

При использовании данного режима, объект следует разделить на несколько зон, доступ к которым требуется разграничить. Максимальное количество зон – **64**. Как пример, можно рассмотреть жилой комплекс из 20 подъездов, огороженный забором с калитками. Каждый подъезд можно выделить как одну зону и все калитки также выделить в одну общую зону. Итого в данном примере будет использоваться 21 зона.

Данный режим также, как и первый защищенный режим, использует понятие кода объекта. Код объекта генерируется при создании мастер-карт (от 1 до 5 штук). На этапе конфигурирования системы в считыватели записывается код объекта и соответствующие данному объекту зоны прохода. Таким образом в нашем примере получится, что у каждого подъезда, будут стоять считыватели, у которых будет прописана одна зона, соответствующая конкретному подъезду (например, с 1 по 20). Считыватели на калитках будут иметь разрешенную зону 21. При формировании карт пользователей оператор может выбрать в какие зоны будет разрешен доступ обладателю этой карты. В данном примере, каждому жителю будет разрешен доступ в две зоны – в его подъезд и калитки. Работникам коммунальных служб можно разрешить доступ во все зоны. При поднесении карты – считыватель смотрит какие зоны записаны на карте и если хотя бы одна совпадает с зонами, прописанными в нем, то он разрешает проход.

В данном режиме передача данных по протоколу *Wiegand, USB* и *RS485* не прекращается. Однако передается не идентификационный номер карты, а битовая строка разрешенных зон.

Для удобства администраторов системы, в ПО можно переименовать зоны в удобные для использования названия и сохранить эти настройки в шаблонах.

3.4.2 Настройка системы в режиме «Зоны прохода»

1. В программе «ЭНТ контроль доступа RFID» выберите соответствующий режим работы;

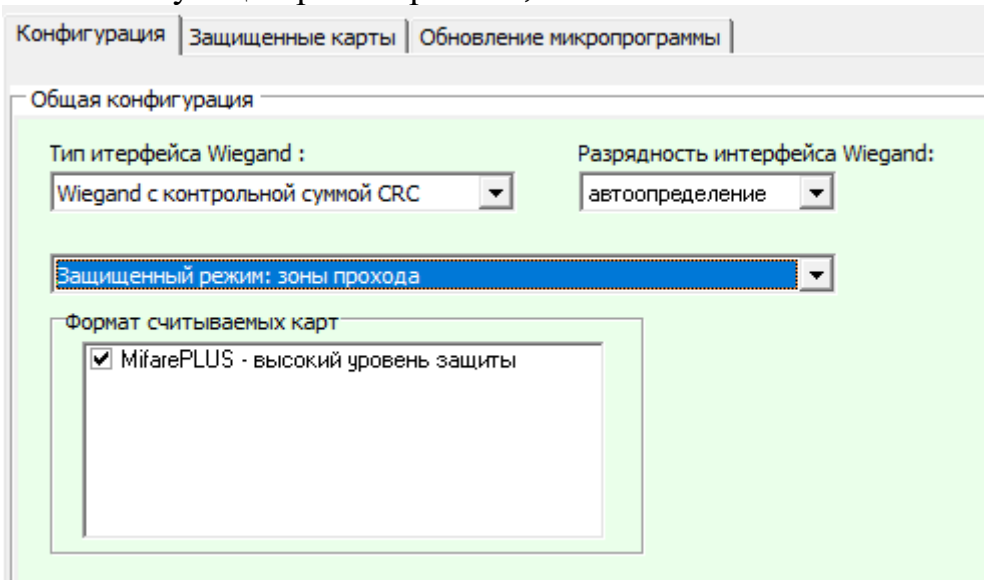

Рис. 14 (Режим работы «*зоны прохода*»)

2. Укажите необходимые зоны прохода и длительность управляющего импульса для подключенного замка.

3. Нажмите кнопку «*создать мастер-карты*» и укажите количество создаваемых мастер карт;

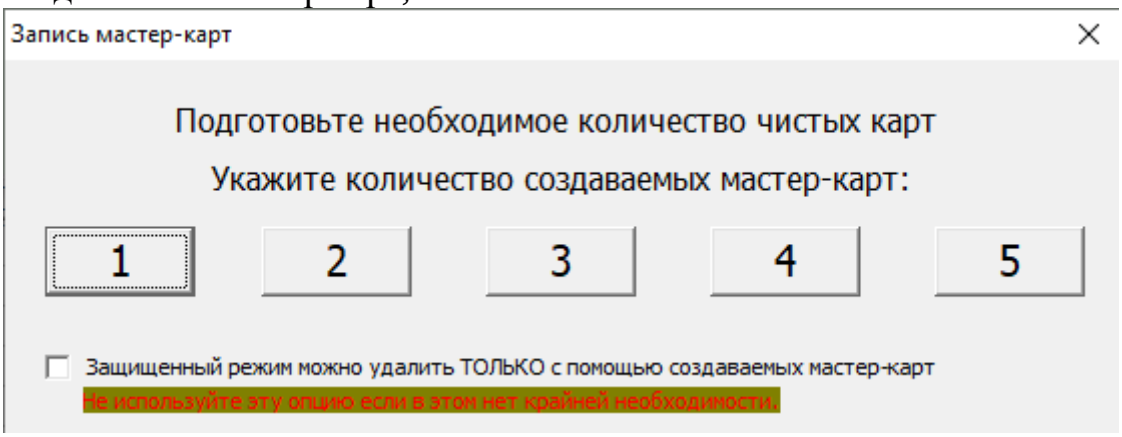

Рис. 15 (Запись мастер-карт)

При нажатии на соответствующую кнопку защищенный режим работы считывателя можно будет удалить **только с помощью мастер-карт с таким же кодом объекта**. Т.е. если мастер-карта будет утеряна или стёрта, то переконфигурировать считыватель будет невозможно!!!

4. Нажмите кнопку «*записать конфигурацию в USB-считыватель*»;

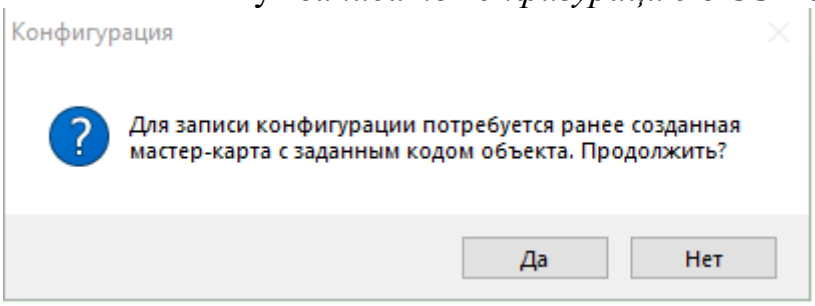

Рис. 16 (Запись конфигурации в считыватель)

5. Приложить ранее созданную мастер карту к USB-считывателю для подтверждения записи настроек;
6. Перейти во вкладку «*защищенные карты*», выберите необходимые зоны прохода;
7. Нажмите кнопку «*создать защищенные карты*»;
8. Приложить ранее созданную «*мастер карту*», отвечающую за эти зоны прохода;
9. Приложите необходимое количество карт для доступа на объект;
10. Нажмите кнопку «*закончить создание защищенных карт*»
11. Теперь в режим «*Зоны прохода*» необходимо перевести считыватели *ЭРА-MF*. Сделать это можно как при подключении к ПК, так и с помощью мастер-карты. Для конфигурации мастер-картой необходимо:
    f) При выключенном считывателе, перевести 4-ый дип-переключатель в положение On;
    g) Включить питание;
    h) Приложить ранее созданную мастер-карту с настройками;
    i) Перевести 4-ый дип-переключатель в положение Off;
    j) Выключить считыватель, после чего включить к его.
12. Теперь считыватель *ЭРА-MF* будет воспринимать защищенные карты доступа, работающие с ним в одной зоне.

Карты, которые не были сделаны «*защищенными*» в программе ЭНТ контроль доступа RFID не будут восприниматься считывателями *ЭРА-MF и ЭРА-MF USB*, работающими в «*защищенном*» режиме.

Пример:

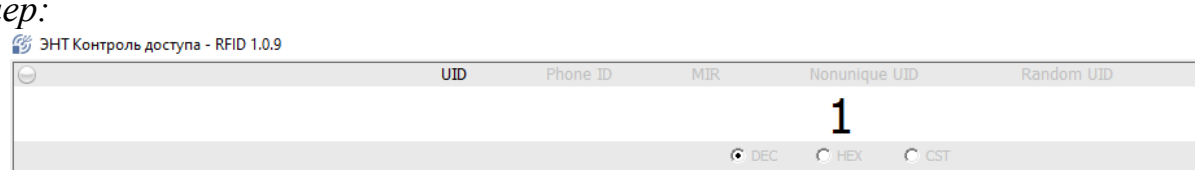

Рис. 17 (Номер зоны прохода, считанный с карты программой «RFID»)

4. Обновление микропрограммы считывателя

При переходе на вкладку «Обновление микропрограммы» пользователю доступна возможность обновить микропрограмму подключенного к ПК считывателя.

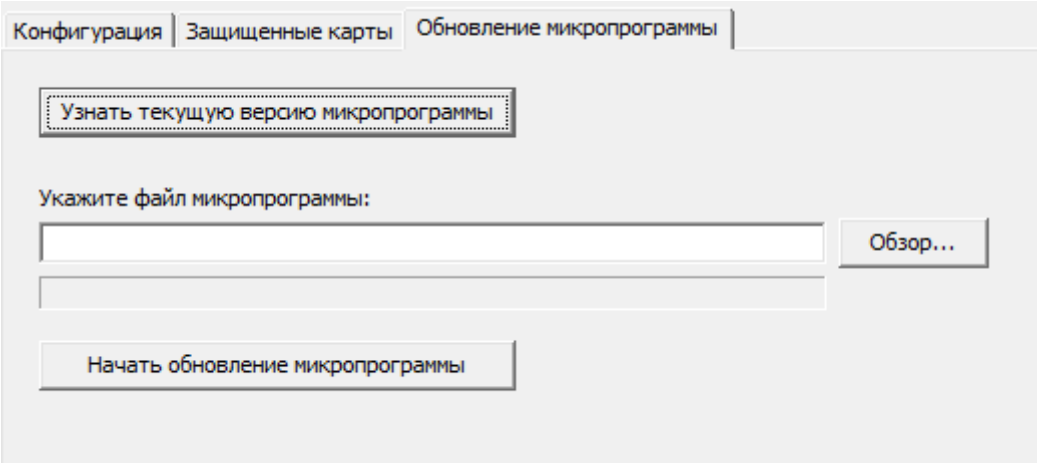

Рис. 18 (Меню обновления микропрограммы)

Нажав соответствующую кнопку, можно узнать текущую версию микропрограммы.

Для обновления микропрограммы нужно:

1. Нажать кнопку «*Обзор*» и выбрать файл микропрограммы.
2. Нажать кнопку «*Начать обновление микропрограммы*»
3. Дождаться окончания операции.