

Руководство пользователя

Программное обеспечение «Конфигуратор считывателей «ЭРА»»

Сделано в России

Редакция от 19.09.2025 г.

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ.....	2
1.1. Общие сведения о программе.....	2
1.2. Системные требования.....	3
2. РАБОТА С ПРОГРАММОЙ.....	3
2.1. Запуск программы.....	3
2.2. Подключение и настройка считывателя.....	3
2.2.1. Опция «хеш-функция».....	5
2.3. Запись настроек в считыватель.....	6
2.4. Дополнительные возможности программы.....	6
3. РЕЖИМ РАБОТЫ ЧТЕНИЯ КАРТ.....	8
3.1. Обычный режим чтения только UID.....	8
3.1.1. Описание.....	8
3.1.2. Работа программы в «Обычном режиме».....	8
3.2. Защищенный режим «Код объекта».....	8
3.2.1. Описание.....	8
3.2.2. Настройка системы в режиме «Код объекта».....	11
3.2.2.1. Создание мастер-карт для режима «Код объекта».....	11
3.2.2.2. Перевод считывателя в режим «Код объекта».....	12
3.2.2.3. Создание карт пользователей, работающих в режиме «Код объекта».....	14
3.3. Защищенный режим «Чтение кода из блока».....	15
3.3.1. Описание.....	15
3.4. Защищенный режим «Зоны прохода».....	16
3.4.1. Описание.....	16
3.4.2. Настройка системы в режиме «Зоны прохода».....	17
3.4.2.1. Создание мастер-карт для режима «Зоны прохода».....	17
3.4.2.2. Перевод считывателя в режим «Зоны прохода».....	19
3.4.2.3. Создание карт пользователей, работающих в режиме «Зоны прохода».....	21
4. ОБНОВЛЕНИЕ МИКРОПРОГРАММЫ СЧИТЫВАТЕЛЯ.....	22
5. ОБОЗНАЧЕНИЯ, ТЕРМИНЫ И СОКРАЩЕНИЯ.....	23
5.1. Условные обозначения, принятые в руководстве.....	23
5.2. Список принятых сокращений.....	23

1. ВВЕДЕНИЕ

Уважаемый клиент!

ООО «Эра новых технологий» выражает признательность за выбор нашей продукции. Мы придаем первостепенное значение обеспечению высокого уровня надежности и удобства эксплуатации. Надеемся, что наше решение в полной мере соответствует вашим техническим требованиям и ожиданиям.

Для оптимального использования функциональных возможностей программы настоятельно рекомендуем детально ознакомиться с настоящим руководством пользователя.

Данное руководство содержит полный спектр информации, касающейся настройки и эксплуатации считывателей «ЭРА» с использованием программного обеспечения «Конфигуратор считывателей «ЭРА».

Мы высоко ценим доверие к нашей компании и готовы предоставить комплексную техническую поддержку на всех стадиях жизненного цикла продукта. Контактная информация службы поддержки представлена в конце каждой страницы руководства пользователя.

1.1. Общие сведения о программе

Программа «Конфигуратор считывателей «ЭРА» разработана для настройки и эксплуатации считывателей «ЭРА-USB» (настольного типа) и «ЭРА-MF» (настенного типа). Оба устройства оснащены интерфейсом USB, что обеспечивает быстрое и удобное подключение к персональному компьютеру. Для конфигурирования считывателя «ЭРА-MF» также предусмотрена возможность использования мобильного телефона с установленным программным обеспечением «ЭНТ Сервис» при условии поддержки технологии USB OTG.

USB OTG (On-The-Go) — это технология, которая позволяет смартфону или планшету выступать в роли USB-хоста и поддерживать прямые соединения с другими USB-устройствами. Дословно означает «на ходу».

Считыватель «ЭРА-USB (MF/EM)» используется для считывания и передачи в программное обеспечение серийных номеров бесконтактных идентификаторов по интерфейсу USB, считыватель «ЭРА-MF» подключается к контроллеру СКУД по проводному интерфейсу связи Wiegand. Поддерживается работа с идентификаторами с рабочей частотой 13,56 МГц.

Программа позволяет выполнять следующие действия:

- Читать ID-карты;
- Помещать ID-карты в буфер обмена;
- Осуществлять имитацию набора на клавиатуре;
- Конфигурировать считыватель:
 - Выключить проверку контрольной суммы Wiegand;
 - Изменить разрядность интерфейса Wiegand (от 4 до 64);
 - Выбрать формат считываемых карт считывателем;
 - Включить обратный порядок байт;
 - Включить битовый сдвиг;
 - Включить «хеш-функцию»;

- Обновлять микропрограмму считывателя.

1.2. Системные требования

- ОС: Windows® 7/8/10 (32- или 64-разрядная версия)
- Один USB-порт
- Место на жестком диске: 10 Мб
- В ряде случаев необходимо установить драйвер для корректного подключения считывателя к ПК.

2. РАБОТА С ПРОГРАММОЙ

2.1. Запуск программы

Чтобы запустить программу, распакуйте архив в папку *C:\Program Files (x86)\ENT\usbreader*. Затем откройте файл *Usbreader.exe*. После запуска на экране отобразится главное окно программы.

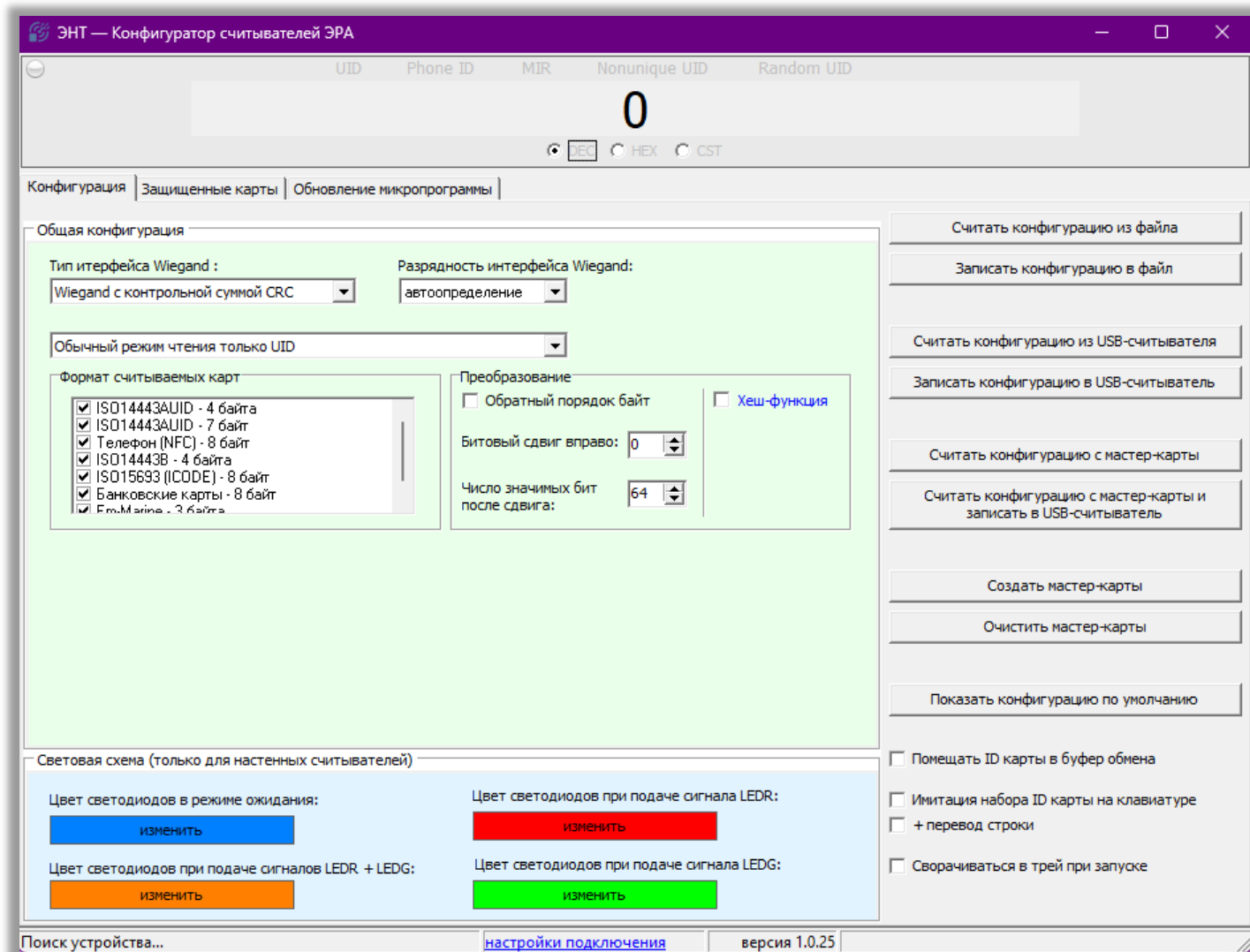


Рисунок 1.1 Внешний вид программы на вкладке «Конфигурация»

2.2. Подключение и настройка считывателя

Подключите считыватель к компьютеру по кабелю через USB-порт. В диспетчере

устройств Windows считыватель должен отображаться в разделе «Порты (COM и LPT)» как «Устройство с последовательным интерфейсом USB (COM#)».

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 быть недоступно в некоторых пакетах обновлений на определенных версиях Windows.

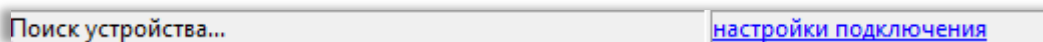


Рисунок 1.2 Строка состояния подключения

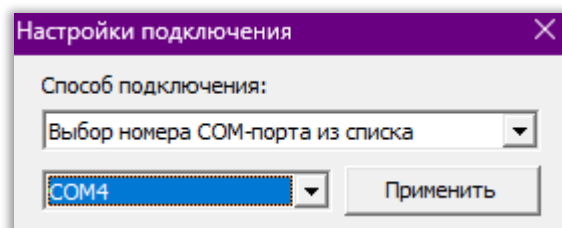


Рисунок 1.3 Окно настройки подключения

При обнаружении считывателя программа считывает конфигурацию из считывателя и откроется окно с соответствующим уведомлением.

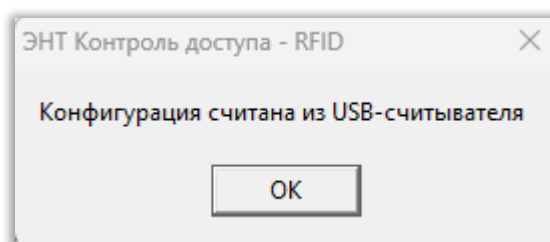


Рисунок 1.4 Окно с уведомлением при обнаружении считывателя

По умолчанию считыватель работает с настройками как изображено на *Рисунок 1.5*.

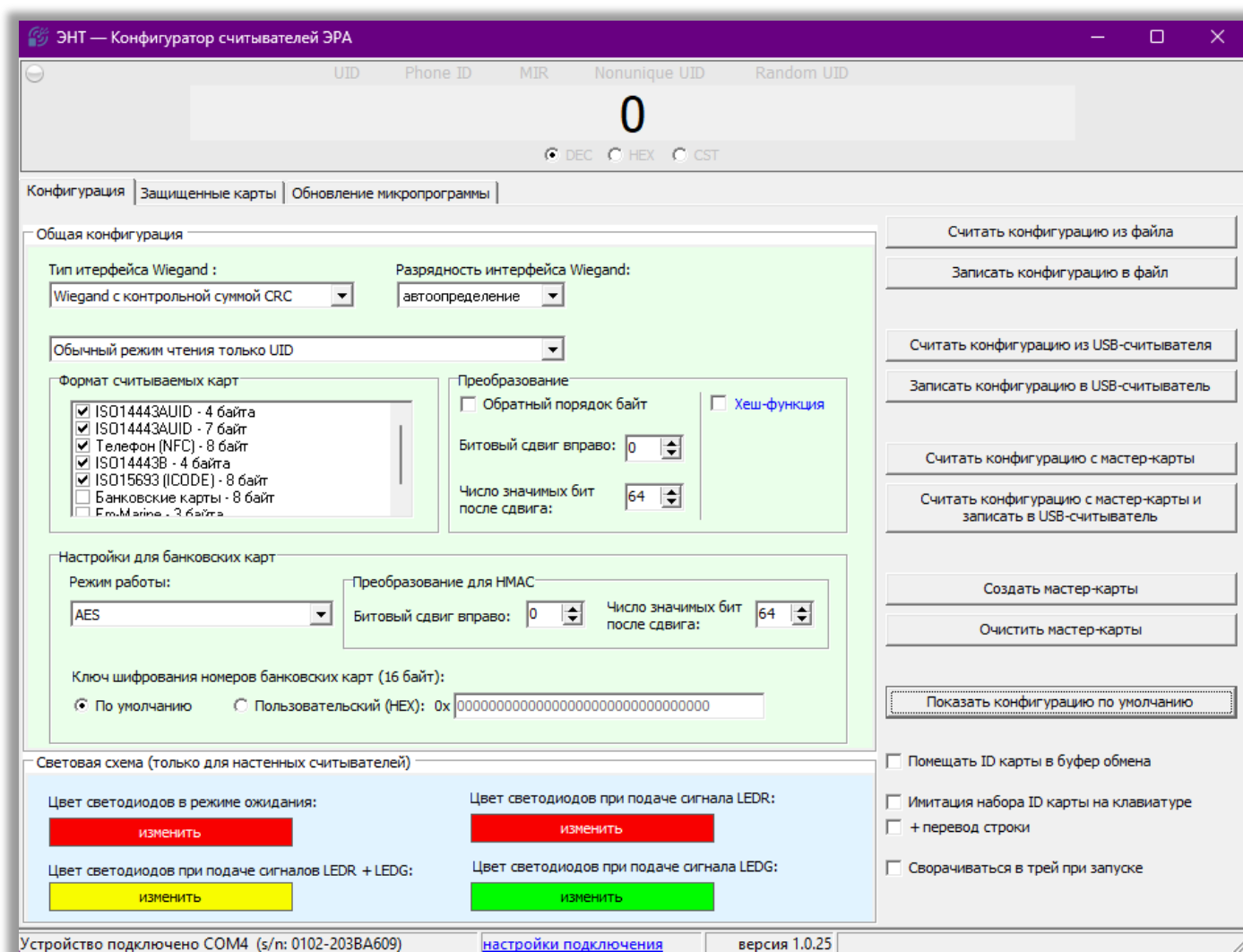


Рисунок 1.5 Заводские настройки считывателя

2.2.1. Опция «хеш-функция»

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

Ниже приведен пример использования опции «хеш-функция»:

UID карты – 56 бит. Разрядность Wiegand – 26 бит. Если нет понимания, в какой части UID карты будут происходить изменения при прикладывании карты, то имеет смысл выбрать режим преобразования «хеш-функция». В этом случае у вас будет посчитан хеш по всему UID карты. Эта опция дает возможность иметь различные коды на выходе считывателя для различных карт, даже если у вас низкая разрядность Wiegand, так как изменение в любом месте UID приведет к изменению выдаваемого считывателем кода. Рассмотрим ситуацию более подробно.

Есть три карты с UID 7 байт, а именно (красным отмечены изменяемые части UID):

0x01 00 00 00 00 03 04

0x01 00 00 00 00 05 06

0x01 07 00 00 00 05 06

Контроллер работает в режиме Wiegand 26, таким образом, считыватель мы вынуждены перевести в режим Wiegand 26. В данном случае невозможно выбрать «битовый сдвиг» и «число значимых бит» так, чтобы был разный код Wiegand для всех трех карт. В случае же использования хеш-функции все три карты будут различаться автоматически.

2.3. Запись настроек в считыватель

Для записи нужной конфигурации в считыватель можно:

1. Использовать ранее созданную мастер-карту;
2. Подключить считыватель к компьютеру через USB и воспользоваться программой.

Рассмотрим второй вариант:

Для записи конфигурации в считыватель необходимо нажать кнопку «**Записать конфигурацию в USB-считыватель**» (см. Рисунок 1.6 — 1). Для просмотра ранее записанной конфигурации считывателя нажмите кнопку «**Считать конфигурацию из считывателя**» (см. Рисунок 1.6 — 2). Для конфигурирования нескольких считывателей можно записать настройки в файл и считывать их при необходимости восстановления. Для этого в правой части программы есть соответствующие кнопки (см. Рисунок 1.6 — 3).

2.4. Дополнительные возможности программы

Для передачи идентификатора в программное обеспечение при работе со считывателем в правой части программного интерфейса «RFID» выберите опцию «**Помещать ID карты в буфер обмена**» или «**Имитация набора ID карты на клавиатуре**» (см. Рисунок 1.6 — 4).

В случае выбора опции «**Помещать ID карты в буфер обмена**» код карты будет скопирован в системный буфер обмена операционной системы Windows. Затем следует выбрать поле, в которое должен быть введен идентификатор карты, и вставить его из буфера системы, например одновременным нажатием на клавиатуре клавиш «Ctrl+V».

При выборе опции «**Имитация набора ID карты на клавиатуре**» код карты будет введен в программу посредством эмуляции нажатий клавиш на клавиатуре. Данный метод обеспечивает удобное введение кода карты в целевое программное обеспечение, например, «ЭНТ Контроль Доступа — Клиент». Для этого следует выбрать поле, в которое должен быть введен идентификатор карты, и затем поднести карту к считывающему

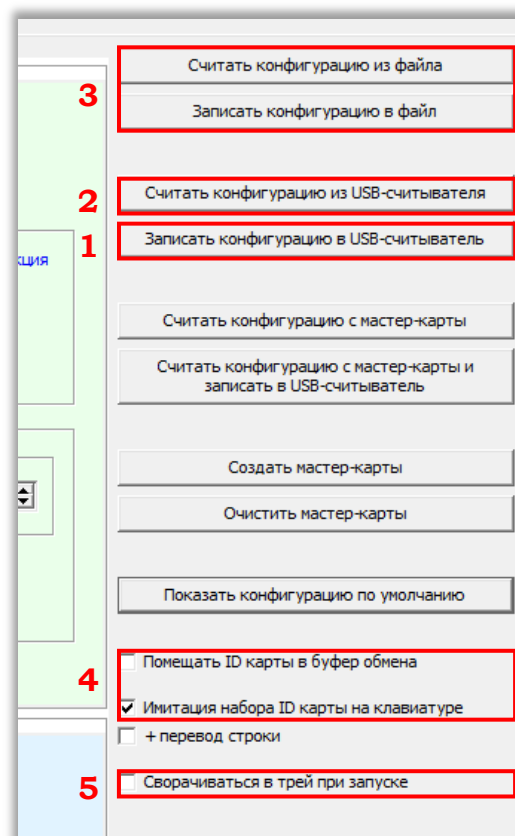


Рисунок 1.6 Опции, доступные на вкладке «Конфигурация»

устройству. Код карты автоматически будет введен в выбранное поле (см. Рисунок 1.8 — 1).

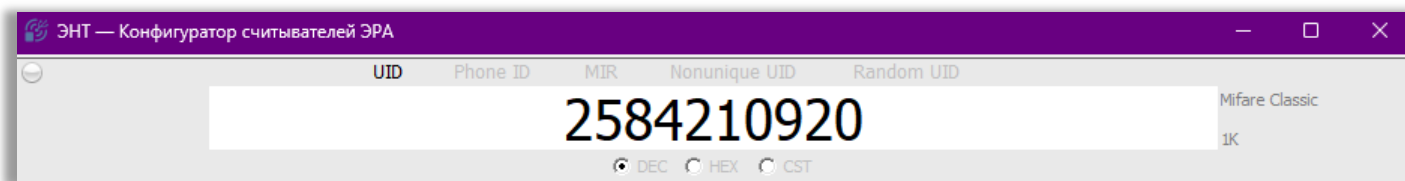


Рисунок 1.7 Идентификатор ключа, полученный программой «RFID»

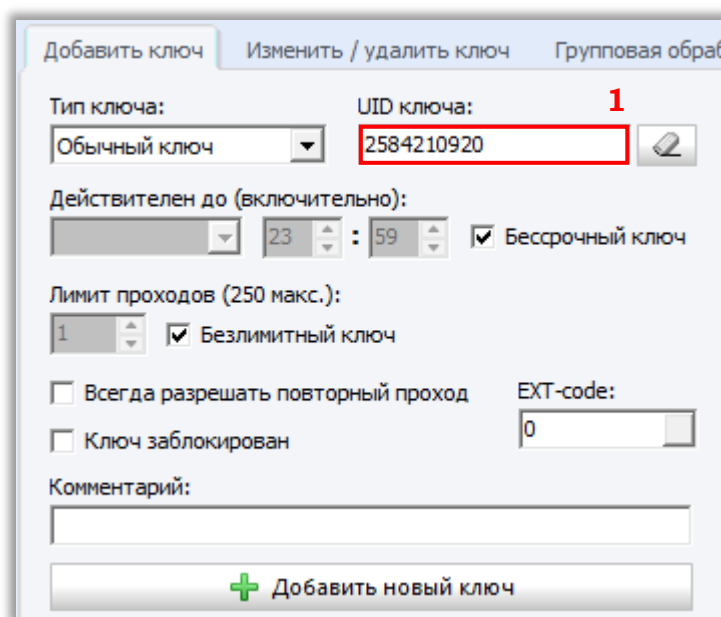



Рисунок 1.8 Идентификатор ключа, переданный в программу «Клиент»

 Для работы данного функционала программа «ЭНТ – Конфигуратор считывателей «ЭРА» должна быть запущена.

Чтобы она не мешала на рабочем столе после запуска, можно активировать функцию «Сворачиваться в трей при запуске» (область уведомлений Windows) (см. рис. 1.6 — 5). Программа останется работать в свернутом режиме.

Чтобы открыть окно, наведите курсор на значок в панели уведомлений Windows. Щелкните правой кнопкой и выберите «Развернуть».

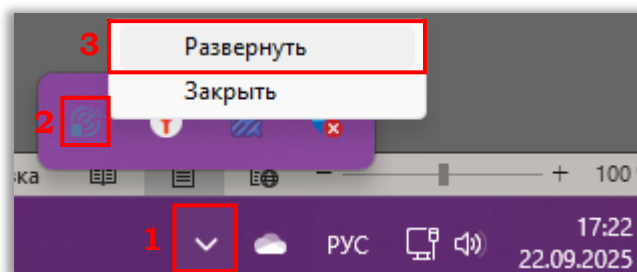


Рисунок 1.9 Разворот программы из области уведомлений панели задач

3. РЕЖИМ 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 13,56 МГц (различные вариации Mifare, I-Code 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.

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 байт (например, к данному варианту можно отнести карты Mifare Ultralite и др.);
3. Телефон с NFC;
4. ISO14443B – 4 байта;
5. ISO15693 (ICODE) – 8 байт;
6. Банковские карты – 8 байт;
7. Em-Marine – 3 байта (для считывателей ЭРА-USB-MF/EM).

3.1.2. Работа программы в «Обычном режиме»

Для работы в данном режиме считыватель должен быть сконфигурирован «по умолчанию» — см. *Рисунок 1.5*.

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	Crypto 1	AES
Длина ключа, бит	48	128


Таблица 1


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 позволит скопировать только данную карту и не будет действителен для других карт.

Чтобы начать использовать этот режим, вам необходимо создать мастер-карты с кодом объекта.


 *Настоятельно рекомендуем использовать карты формата Mifare Plus для решения этой задачи. Эти карты оснащены более современным и криптостойким алгоритмом шифрования, что делает их невосприимчивыми к попыткам копирования злоумышленниками.*


 *Если вы используете защищенный режим код-объекта с Mifare Classic, обратите внимание на следующие важные моменты:*


1. Если вы используете считыватель с микропрограммой 1.2.7 и ниже для создания мастер-карты Mifare Classic, её функциональность будет ограничена.

 *В частности, с такими мастер-картами вы не сможете снять защиту со считывателя, если эта опция была активирована при их создании. Также не*


будет доступна функция «Считать конфигурацию с мастер-карты и записать её в считыватель».

 *Поэтому мы рекомендуем использовать хотя бы одну мастер-карту на основе Mifare Plus для обеспечения более широких возможностей в работе с системой и возможности снять защищённый режим со считывателя.*

 *2. Если у вас считыватель с микропрограммой 1.2.8, вы можете воспользоваться полным функционалом мастер-карты формата Mifare Classic. Однако стоит учесть, что Mifare Classic не является не копируемой, а значит, существует риск её копирования злоумышленниками.*

 *Если вы используете защищённый режим код-объекта на основе Mifare Plus, применение мастер-карт Mifare Classic становится невозможным.*

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 одновременно (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. 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 ту же 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. Также 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»

Для перевода системы в режим «Код объекта» необходимо сделать три основополагающие настройки, а именно:

1. Создание мастер-карт соответствующего режима;
2. Перевод считывателей в режим;
3. Создание карт пользователей, работающих в режиме «Код объекта».

Рассмотрим их подробнее.

3.2.2.1. Создание мастер-карт для режима «Код объекта»

1. В программе «ЭНТ контроль доступа RFID» выберите соответствующий режим работы.
2. Выберите используемый тип карт;
3. В случае необходимости последующего дублирования конфигурации на считыватели с применением мастер-карты, предоставьте необходимые параметры, включая тип и разрешение интерфейса Wiegand, а также параметры преобразования данных.
4. Нажмите кнопку «Создать мастер-карты».
5. Укажите количество создаваемых мастер-карт (Рисунок 1.10);

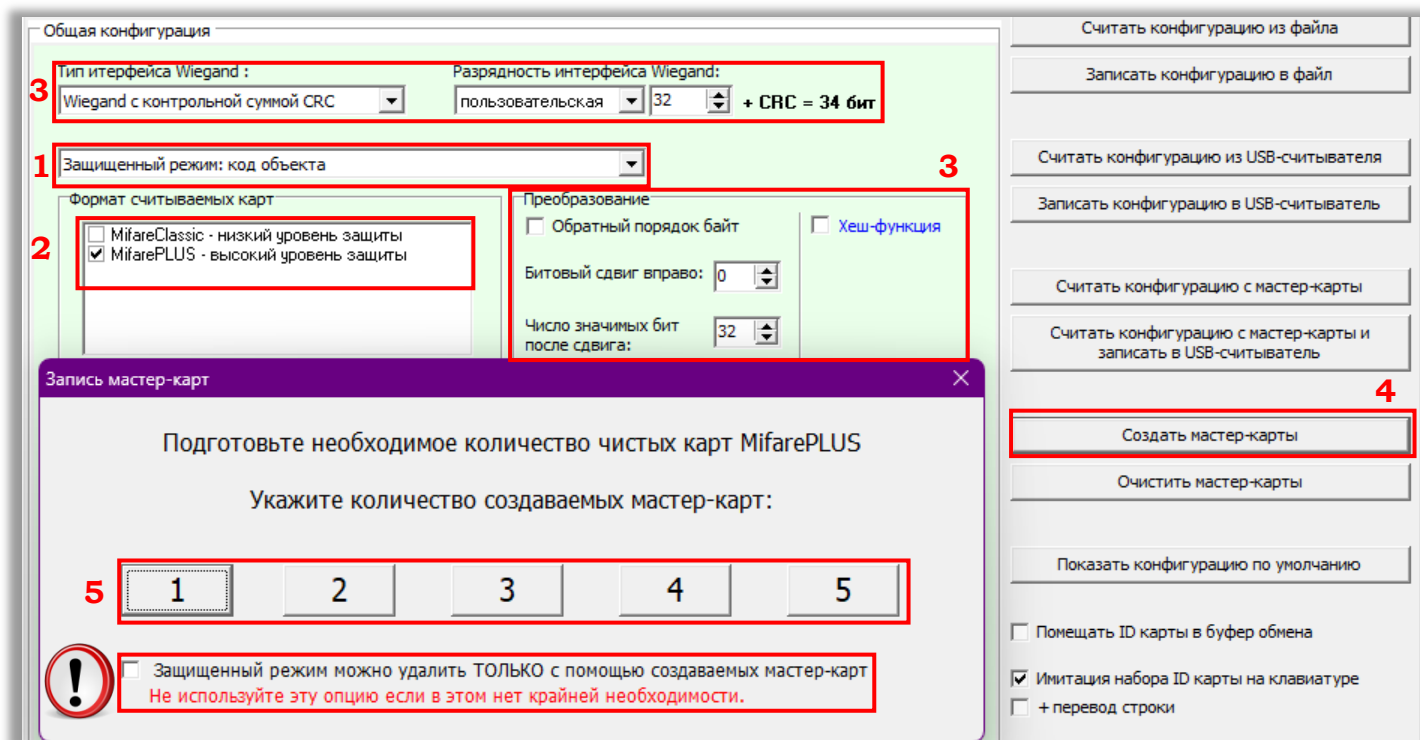



Рисунок 1.10 Запись мастер-карт «Код объекта»

6. Поочередно приложите карты к считывателю

 При установке галочки в соответствующем поле (см. Рисунок 1.10) 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!

Чтобы перевести в этот режим после создания мастер-карт, вам потребуется нажать кнопку «Считать конфигурацию с мастер-карты и записать в USB-считыватель», после чего перезапустить считыватель по питанию.

3.2.2.2. Перевод считывателя в режим «Код объекта»

Перевод считывателя в данный режим возможен несколькими способами: с ручным вводом конфигурации для считывателя или копированием предустановленных конфигураций с мастер-карты.

Подключите считыватель через USB-порт и запустите программу «[Конфигуратор считывателей «ЭРА»](#)». Для считывателей «ЭРА-MF» можно использовать мобильную версию программы «[ЭНТ Сервис](#)»;

Вариант 1. Ручной ввод конфигурации для считывателя

1. После определения считывателя в программе выберите **защищенный режим «Код объекта»**.
2. Выберите требуемые настройки интерфейса Wiegand.
3. Укажите преобразование для исходящего идентификатора.
4. Выберите нужные параметры цветовой схемы;
5. Нажмите кнопку «**Записать конфигурацию в USB-считыватель**».

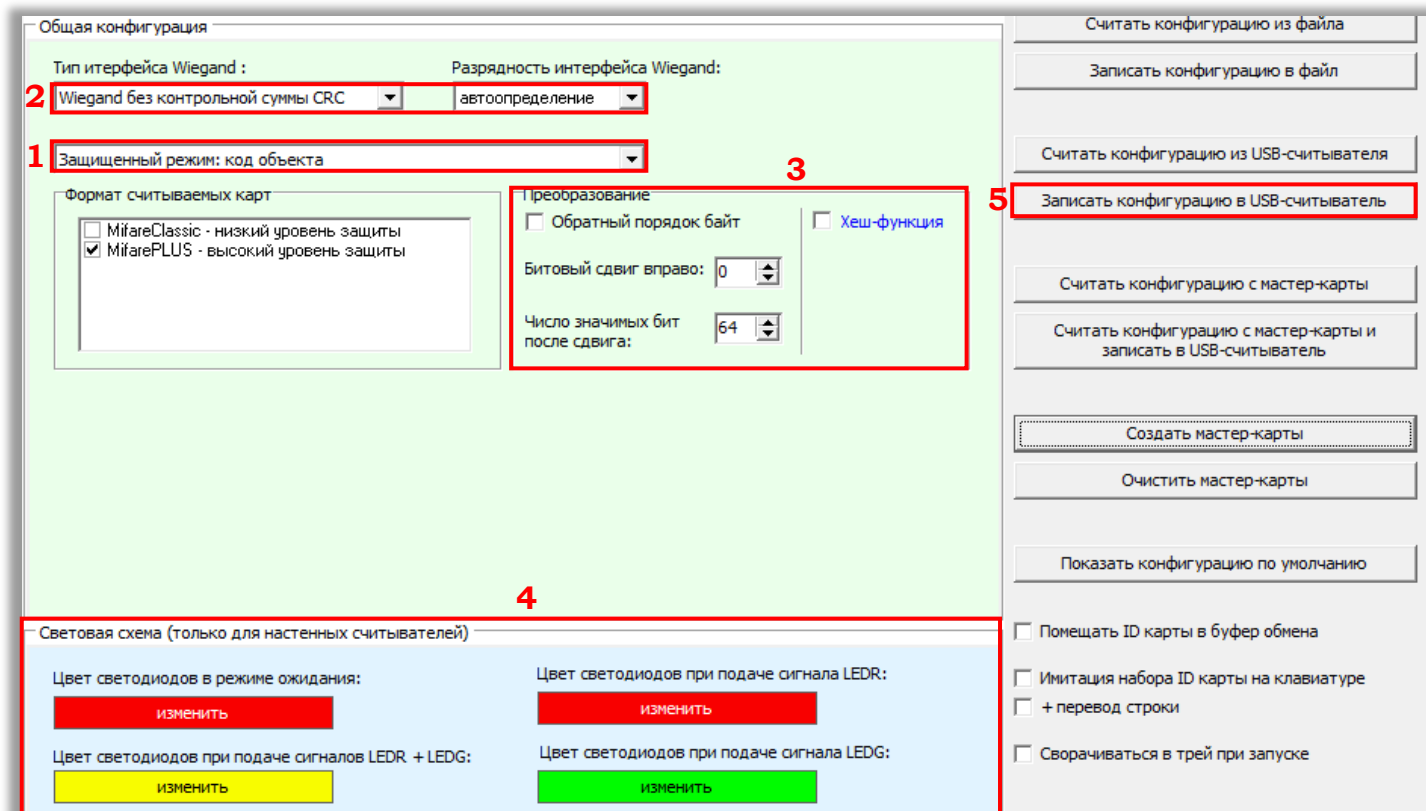


Рисунок 1.11 Перевод считывателя в режим «Код объекта» с ручной конфигурацией

6. На экране появиться диалоговое окно. Нажмите «Да», чтобы скопировать код объекта в считыватель. Нажмите «Нет», чтобы отменить действие.

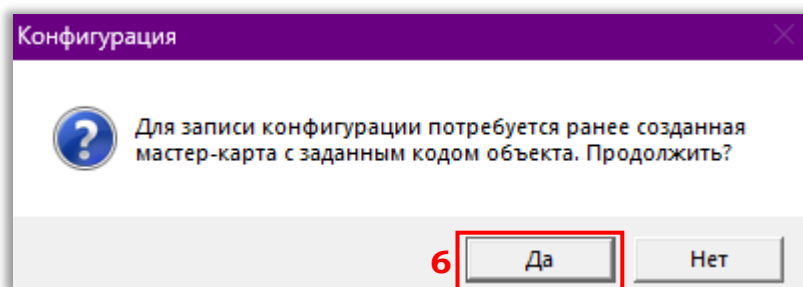


Рисунок 1.12 Запись конфигурации в считыватель

7. Приложите ранее созданную мастер-карту к считывателю для копирования кода объекта в считыватель;
8. Считыватель переведен в режим «Код объекта». Все настройки, кроме кода, установлены из программы.

Вариант 2. Копирование конфигурации из мастер-карты

1. После определения считывателя в программе выберите **защищенный режим «Код объекта»**.
2. Нажмите кнопку **«Считать конфигурацию с мастер-карты и записать конфигурацию в USB-считыватель»**.

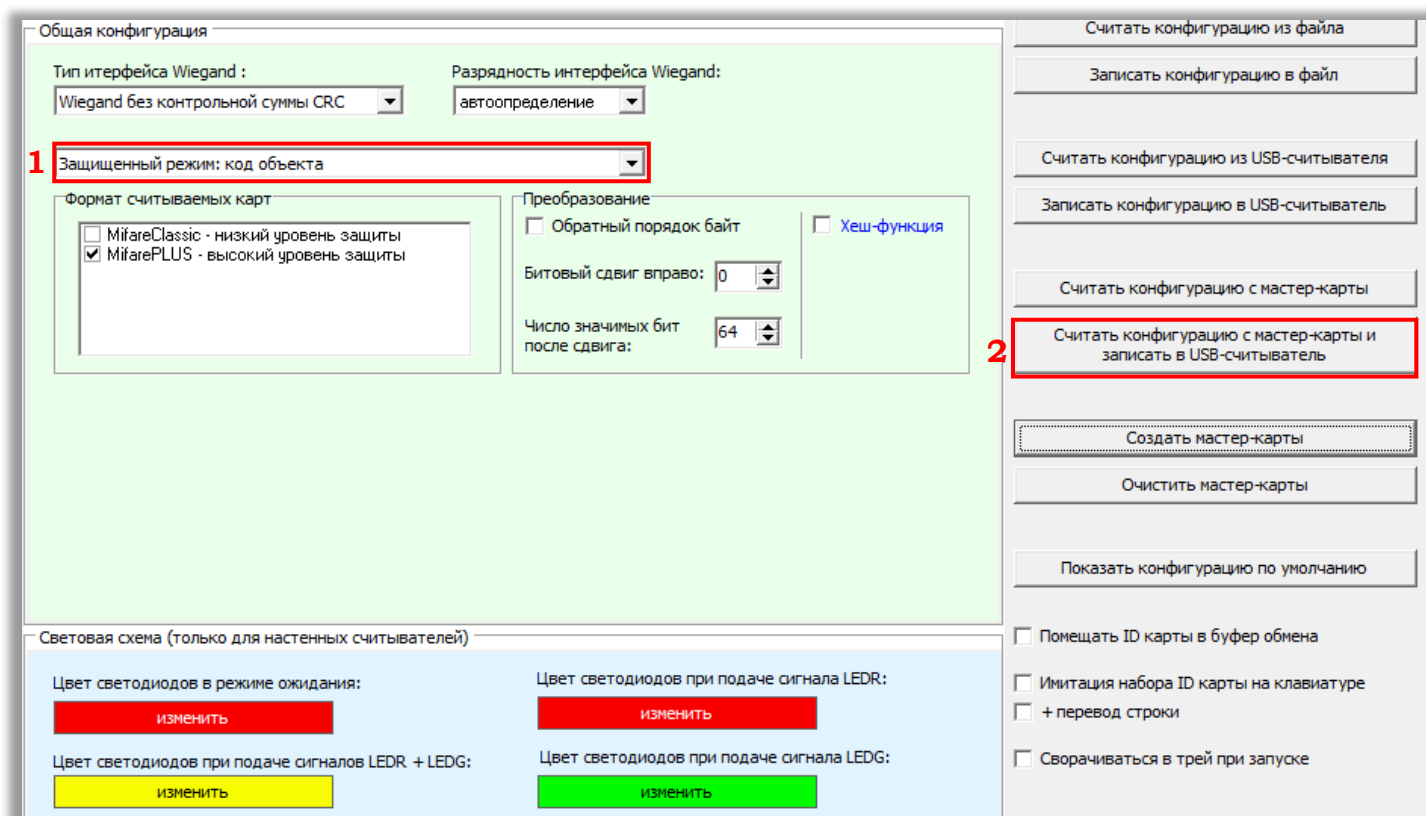


Рисунок 1.13 Перевод считывателя в режим «Код объекта» с копированием конфигурации из мастер-карты

3. На экране появится диалоговое окно. Нажмите «Да», чтобы продолжить. Нажмите «Нет», чтобы отменить действие.

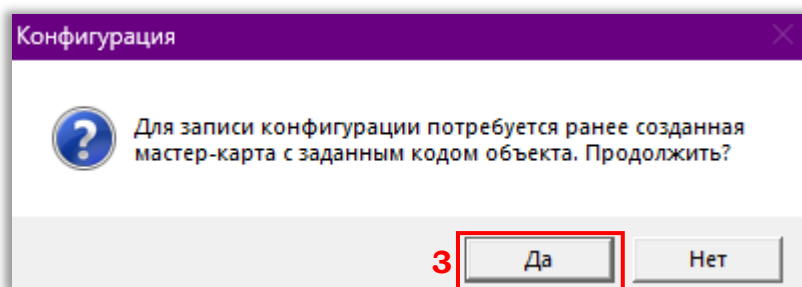


Рисунок 1.14 Запись конфигурации в считыватель

4. Приложите ранее созданную мастер-карту к считывателю для копирования кода объекта и ранее сохраненной конфигурации в считыватель;
5. Считыватель переведен в режим «Код объекта» с предустановленными настройками.

3.2.2.3. Создание карт пользователей, работающих в режиме «Код объекта»

Для создания карт необходимо:

1. Откройте вкладку «Защищенные карты».
2. Нажмите кнопку «Создать защищенные карты – записать код объекта/зоны прохода»;

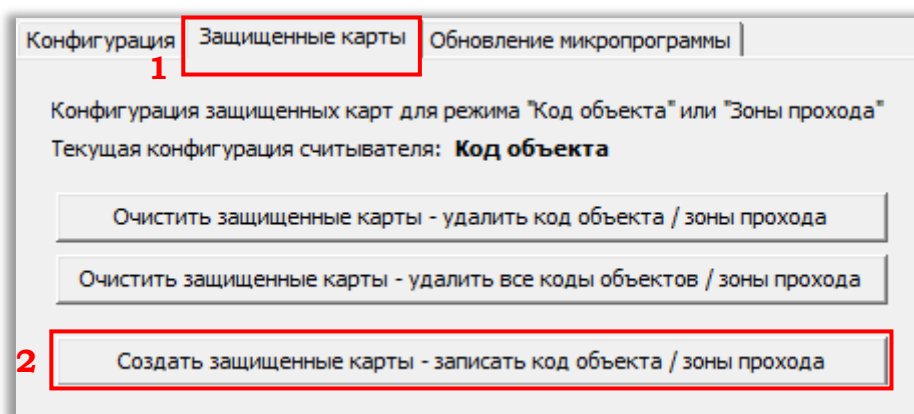



Рисунок 1.15 Создание защищенной карты

3. Приложите ранее созданную мастер-карту к считывателю, а затем приложите необходимое количество карт для доступа на объект;
4. Нажмите кнопку «Закончить создание защищенных карт»;
5. Внесите данные карт пользователей в программу «ЭНТ контроль доступа – Клиент». Это можно сделать с помощью считывателя «ЭРА-MF» или «ЭРА-USB». Также можно воспользоваться функцией «Пакетное добавление ключей» в программе «Клиент» вместе со считывателем «ЭРА-MF», который подключен к контроллеру СКУД. Подробные инструкции можно найти в разделе 4.2.2.1 «Добавление нового ключа» в [Руководстве пользователя – Клиент](#).

 Карты, которые не были сделаны «защищенными» в программе «ЭНТ – Конфигуратор считывателей «ЭРА», не будут восприниматься считывателями ЭРА-MF и ЭРА-USB, работающими в «защищенном» режиме.

Пример отображения идентификатора карты:

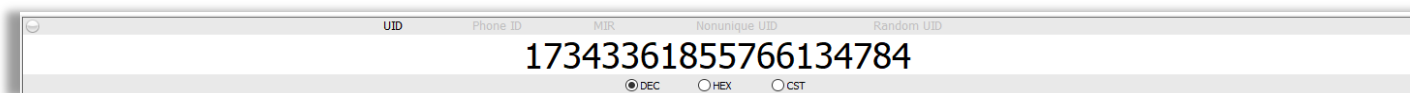


Рисунок 1.16 Уникальный идентификатор карты, считанный программой

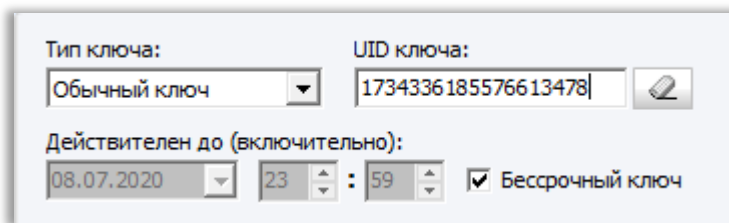


Рисунок 1.17 Уникальный идентификатор карты, переданный в программу «Клиент»

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 укажите номер блока, смещение в данном блоке и количество байт для передачи. Также укажите код доступа к данному блоку.

i Максимальное количество байт для передачи – 8. Размер кода доступа 16 байт.

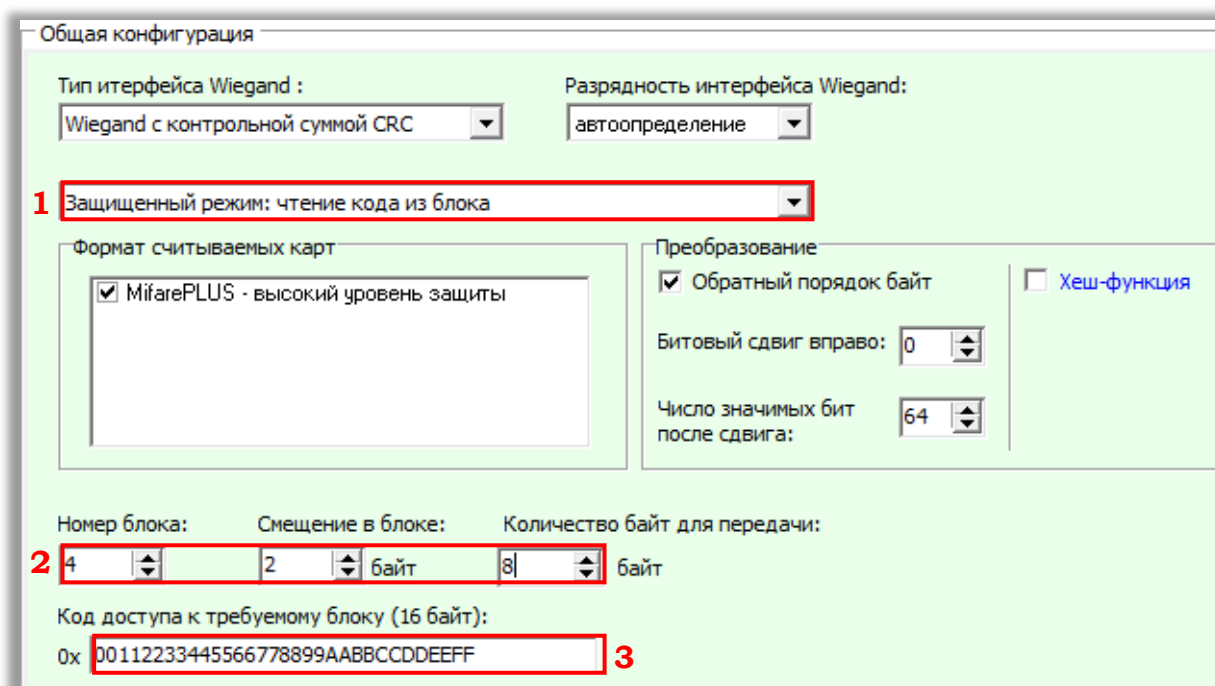


Рисунок 1.18 Режим «Чтение кода из блока»

i В данном режиме код доступа вводится 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.

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.

В качестве примера можно рассмотреть жилой комплекс, состоящий из двадцати подъездов, огражденный забором с калитками. Каждый из подъездов может быть выделен в отдельную зону, а все калитки объединены в одну общую зону. Таким образом, в данном примере будет задействовано двадцать одна зона.

Данный режим, аналогичный режиму «Код объекта», основывается на использовании уникального идентификатора объекта. Идентификатор объекта формируется при создании мастер-карты. На этапе конфигурации системы в считыватели вводятся идентификатор объекта и соответствующие зоны прохода. В нашем примере это означает, что на каждом подъезде будут установлены считыватели, настроенные на одну конкретную зону, соответствующую данному подъезду (например, с 1 по 20). Считыватели, установленные на калитках, будут настроены на зону прохода 21.

При создании защищенных карт пользователей администратор может выбрать, в какие зоны будет разрешен доступ владельцу 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 этом режиме передача данных осуществляется также по протоколам *Wiegand* и *USB*. Однако вместо идентификационного номера карты система отправляет битовую строку с информацией о разрешенных зонах.

Чтобы упростить работу администраторов, программа позволяет переименовывать зоны и сохранять настройки в виде готовых шаблонов.

Для этого необходимо:

1. Наведите курсор на название зоны прохода и дважды кликните левой клавишей мыши и напишите новое имя зоны;

2. После ввода всех имен нажмите кнопку «Сохранить имена зон прохода»

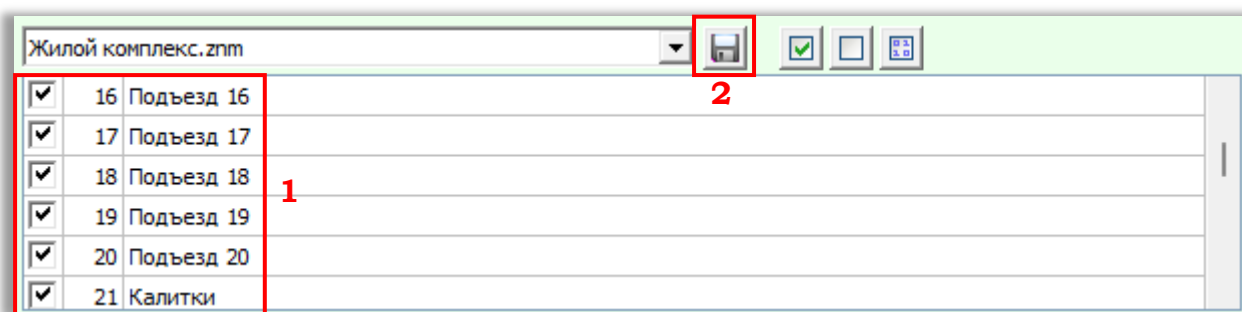


Рисунок 1.19 Переименование зон прохода и сохранение шаблона

3. Для сохранения укажите папку, где находится файл с программой «Конфигуратор считывателей «ЭРА».
4. Введите имя файла и нажмите «Сохранить».
Затем вы сможете легко выбирать сохранённые шаблоны из списка в программе по их названиям.

3.4.2. Настройка системы в режиме «Зоны прохода»

Для перевода системы в режим «Зоны прохода» необходимо сделать три основополагающие настройки точно так же, как и в режиме «Код объекта»:

1. Создать мастер-карты соответствующего режима;
2. Перевести считыватели в режим;
3. Создать карты пользователей, работающих в режиме «Зоны прохода».

3.4.2.1. Создание мастер-карт для режима «Зоны прохода»

1. В программе «Конфигуратор считывателей «ЭРА» выберите соответствующий режим работы;
2. В случае необходимости последующего дублирования конфигурации на считыватели с применением мастер-карты, предоставьте необходимые параметры, включая тип и разрешение интерфейса Wiegand, длительность управляющего импульса для подключенного замка, а также параметры цветовой схемы.

3. Нажмите кнопку «Создать мастер-карты».

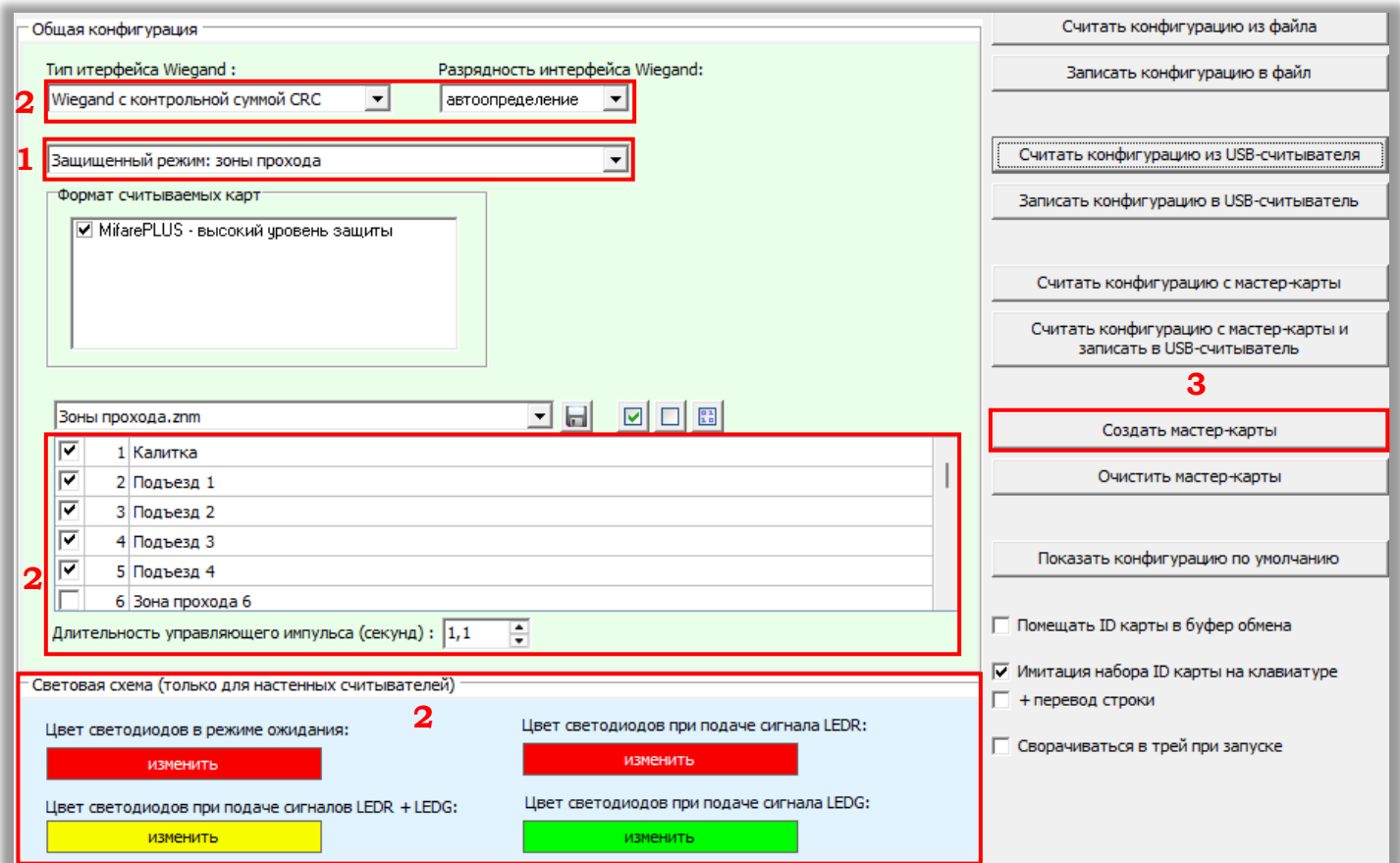


Рисунок 1.20 Запись мастер-карт «Зоны прохода»

4. Укажите количество создаваемых мастер-карт;

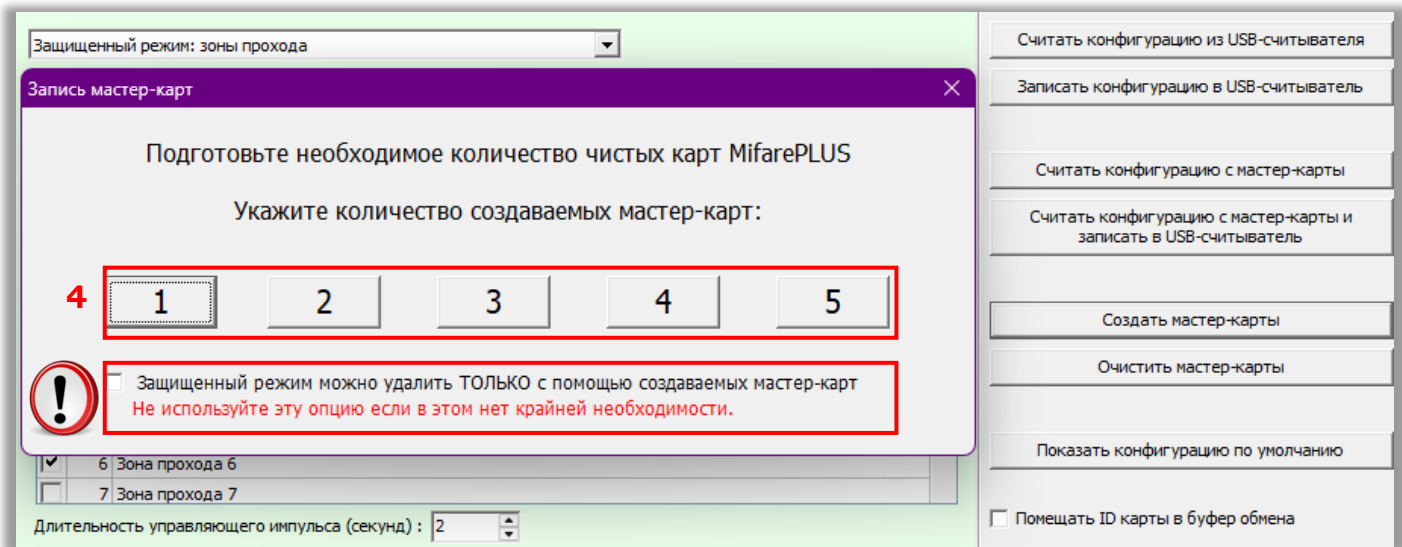


Рисунок 1.21 Выбор количества создаваемых мастер-карт

5. Поочередно приложите карты к считывателю

! При установке галочки в соответствующем поле (см. Рисунок 1.10) 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!

Чтобы перевести в этот режим после создания мастер-карт, вам потребуется

нажать кнопку «Считать конфигурацию с мастер-карты и записать в USB-считыватель», после чего перезапустить считыватель по питанию.

3.4.2.2. Перевод считывателя в режим «Зоны прохода»

Перевод считывателя в данный режим возможен несколькими способами: с ручным вводом конфигурации для считывателя или копированием предустановленных конфигураций с мастер-карты.

Подключите считыватель через USB-порт и запустите программу «Конфигуратор считывателей «ЭРА». Для считывателей «ЭРА-MF» можно использовать мобильную версию программы «ЭНТ – Сервис»;

Вариант 1. Ручной ввод конфигурации для считывателя

1. После определения считывателя в программе выберите **защищенный режим «Зоны прохода»**;
2. Выберите требуемые настройки интерфейса Wiegand;
3. Выберите зоны прохода, соответствующие данному считывателю;
4. Укажите длительность управляющего импульса для подключенного замка;
5. Выберите нужные параметры цветовой схемы;
6. Нажмите кнопку «Записать конфигурацию в USB-считыватель».

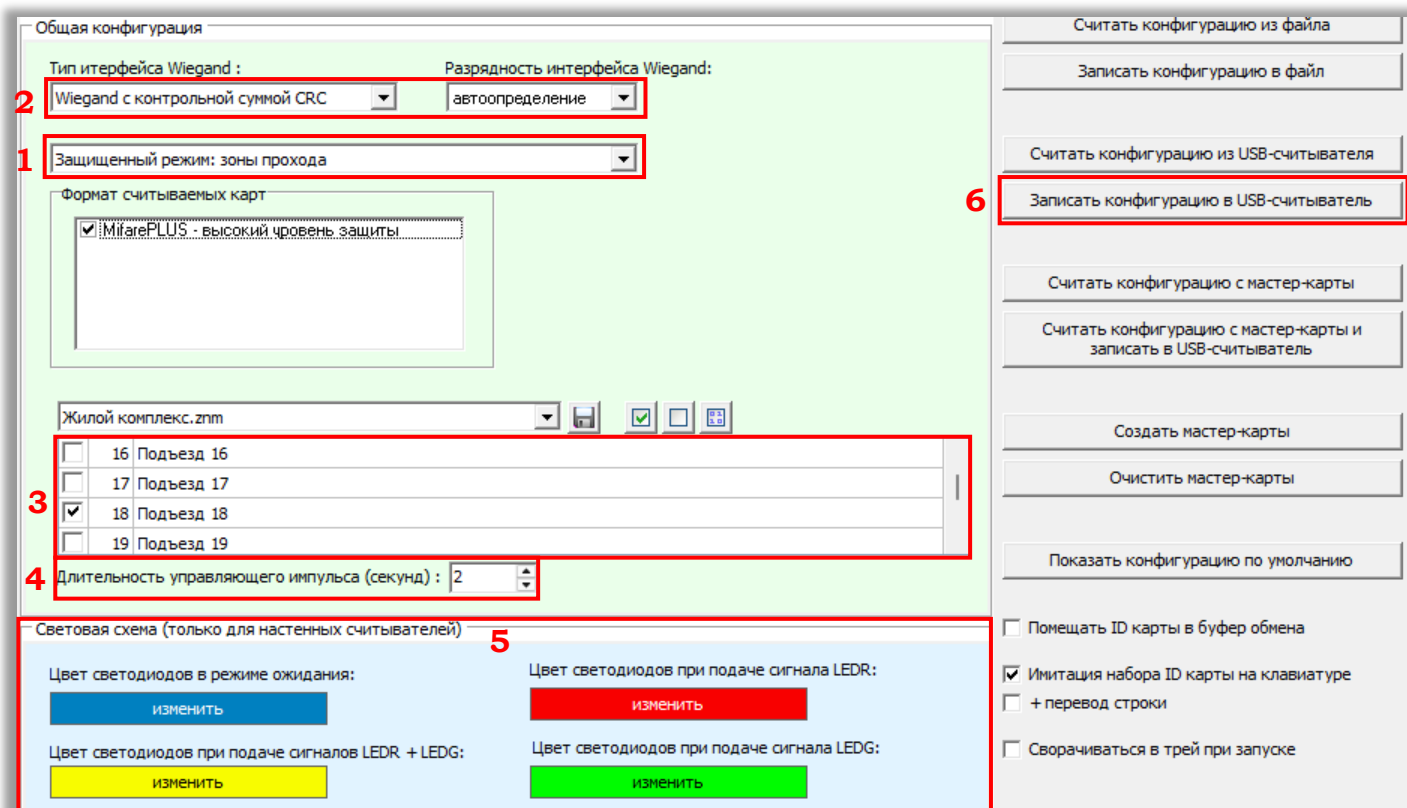


Рисунок 1.22 Перевод считывателя в режим «Зоны прохода» с ручной конфигурацией

- На экране появиться диалоговое окно. Нажмите «Да», чтобы скопировать код объекта в считыватель. Нажмите «Нет», чтобы отменить действие.

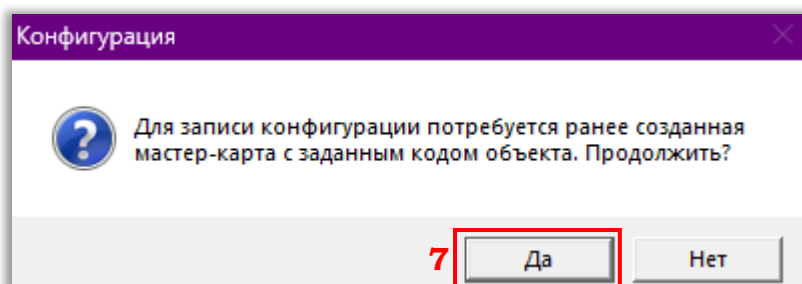


Рисунок 1.23 Запись конфигурации в считыватель

- Приложите ранее созданную мастер-карту к считывателю для копирования кода объекта в считыватель;
- Считыватель переведен в режим «Зоны прохода». Все настройки, кроме кода, установлены из программы.

Вариант 2. Копирование конфигурации из мастер-карты

- После определения считывателя в программе выберите **защищенный режим «Зоны прохода»**.
- Нажмите кнопку **«Считать конфигурацию с мастер-карты и записать конфигурацию в USB-считыватель»**.
- Приложите ранее созданную мастер-карту к считывателю для копирования кода объекта и ранее сохраненной конфигурации в считыватель;

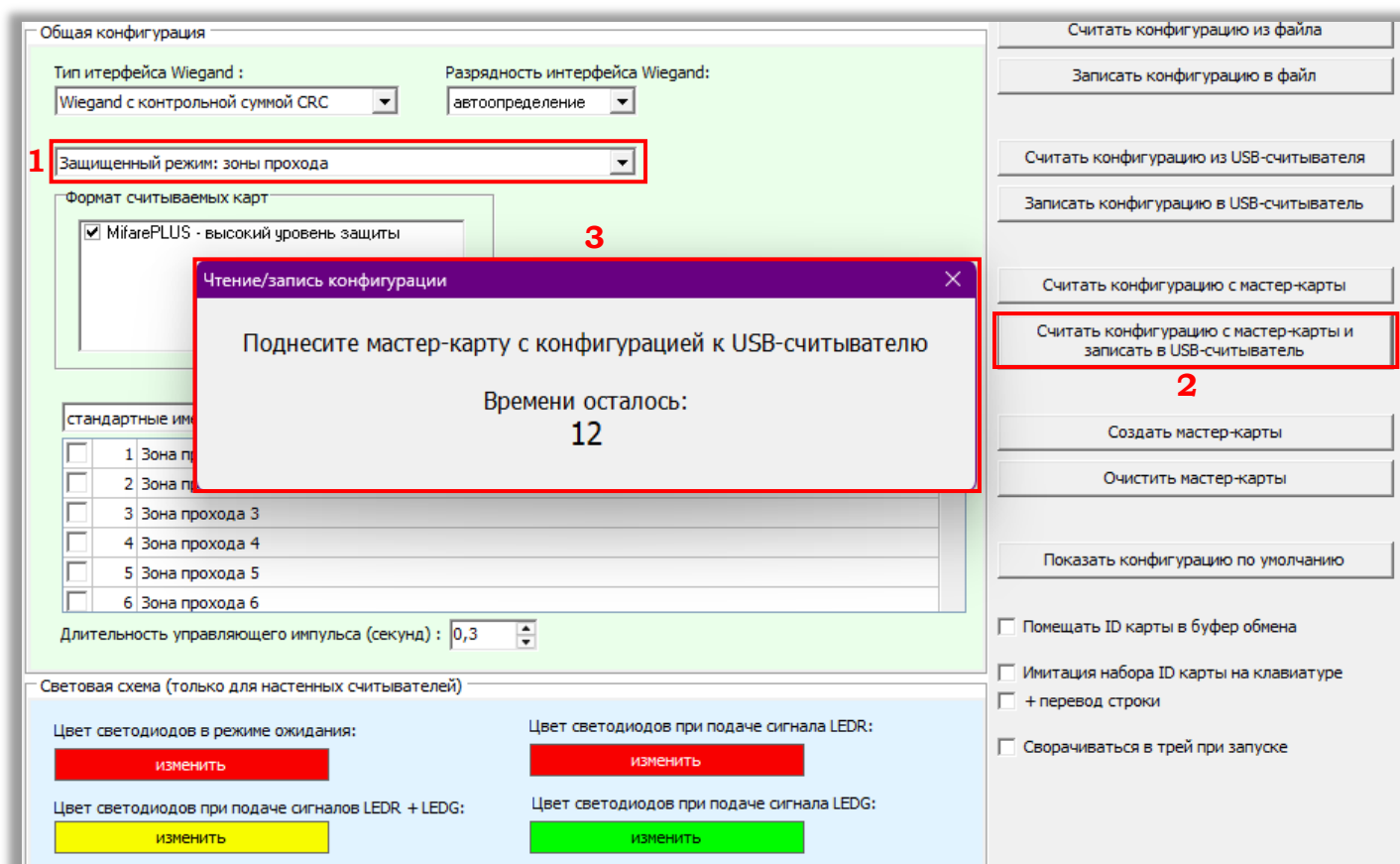


Рисунок 1.24 Перевод считывателя в режим «Зоны прохода» с копированием конфигурации из мастер-карты

- Нажмите «ОК». Считыватель переведен в режим «Зоны прохода» с

- предустановленными настройками;
5. Нажмите кнопку «**Считать конфигурацию из USB-считывателя**». В программе отобразятся настройки считывателя;
 6. Выберите зоны прохода, соответствующие данному считывателю;
 7. Нажмите кнопку «**Записать конфигурацию в USB-считыватель**».

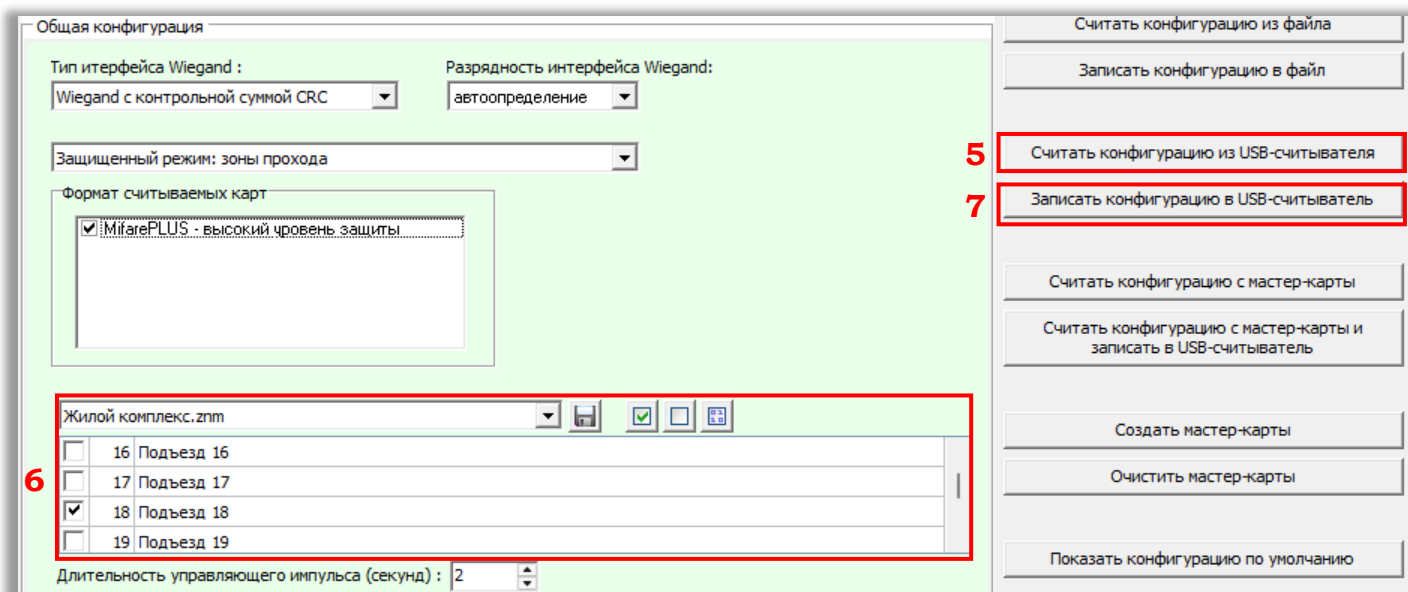


Рисунок 1.25 Выбор зоны прохода, соответствующей данному считывателю

8. На экране появится диалоговое окно. Нажмите «**Да**», чтобы подтвердить запись конфигурации. Нажмите «**Нет**», чтобы отменить действие.

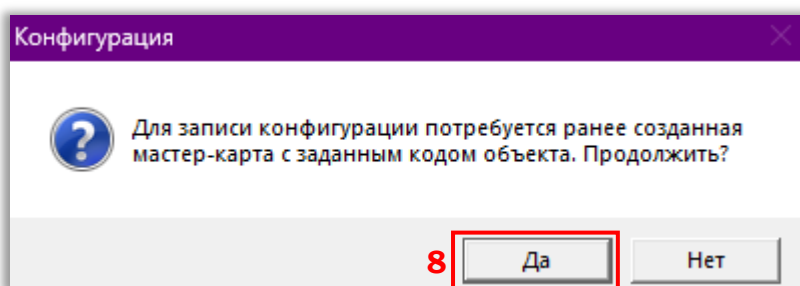


Рисунок 1.26 Запись конфигурации в считыватель

9. Приложите ранее созданную мастер-карту к считывателю для записи зон прохода в считыватель;
10. Считыватель закреплен за соответствующей зоной прохода.

3.4.2.3. Создание карт пользователей, работающих в режиме «Зоны прохода»

Для создания карт необходимо:

1. Откройте вкладку «**Защищенные карты**».

2. Нажмите кнопку «Создать защищенные карты – записать код объекта/зоны прохода»;

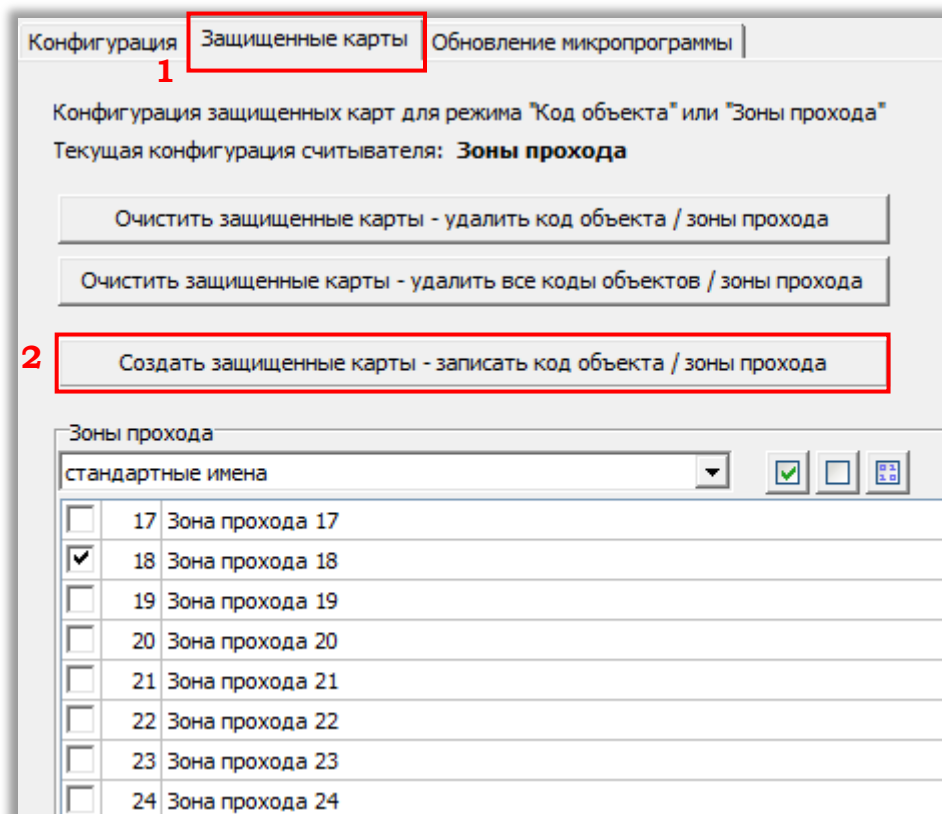



Рисунок 1.27 Создание защищенной карты

3. Приложите ранее созданную мастер-карту к считывателю, а затем приложите необходимое количество карт для доступа на объект;
4. Нажмите кнопку «Закончить создание защищенных карт»;

 Карты, которые не были сделаны «защищенными» в программе «ЭНТ – Конфигуратор считывателей «ЭРА», не будут восприниматься считывателями ЭРА-MF и ЭРА-USB, работающими в «защищенном» режиме.

Пример отображения идентификатора карты:

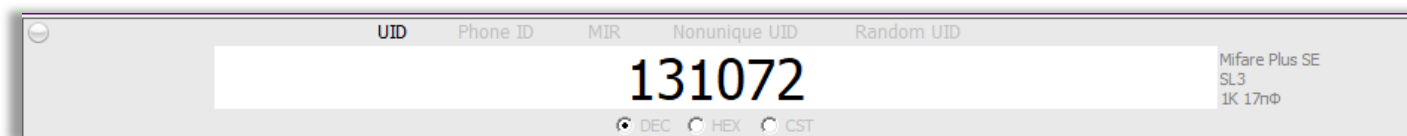


Рисунок 1.28 Идентификатор карты, считанный программой

4. ОБНОВЛЕНИЕ МИКРОПРОГРАММЫ СЧИТЫВАТЕЛЯ


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


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.

5. ОБОЗНАЧЕНИЯ, ТЕРМИНЫ И СОКРАЩЕНИЯ

5.1. Условные обозначения, принятые в руководстве

 – этой меткой будет обозначена критически важная информация. Если не соблюдать правила и условия, описанные в разделах, помеченных этой меткой, система не будет работать.

 – абзацы, выделенные данным знаком, составляют важную информацию о системе, которая облегчит работу с ней.

 – справочная информация, разъясняющая некоторые понятия системы.

Текст, выделенный голубым цветом и с нижним подчёркиванием, представляет собой ссылку, которая ведёт к определённому месту в данном документе или на внешнюю интернет-страницу.

5.2. Список принятых сокращений

БД – База данных.

СКУД – Система контроля и управления доступом.

ОС – Операционная система.

ПО – Программное обеспечение.

ПК – Персональный компьютер.

Клиент – ПО «ЭНТ Контроль доступа – Клиент».

Сервер – ПО «ЭНТ Контроль доступа – Сервер».

UID ключа – Уникальный идентификатор ключа