

Руководство пользователя

Программное обеспечение «Конфигуратор считывателей «ЭРА»

Сделано в России

Редакция от 21.04.2026 г.

Версия 1.0.31

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ.....	4
1.1. Общие сведения о программе.....	4
1.2. Системные требования	6
1.3. Контактная информация службы поддержки.....	6
1.4. Условные обозначения, принятые в руководстве.....	6
1.5. Список принятых сокращений.....	7
1.6. Краткое резюме по разделу	7
2. РАБОТА С ПРОГРАММОЙ.....	8
2.1. Запуск программы и подключение считывателя	8
2.1.1. Запуск программы	8
2.1.2. Подключение считывателя к компьютеру.....	8
2.1.3. Выбор СОМ-порта в программе	9
2.1.4. Автоматическое обнаружение считывателя.....	9
2.1.5. Ручная настройка подключения	9
2.1.6. Диагностика подключения.....	10
2.1.7. Важные замечания.....	10
2.2. «Поле вывода UID»	11
2.3. Вкладка «Конфигурация»	12
2.3.1. Блок «Общая конфигурация».....	14
2.3.1.1. Параметр «Тип интерфейса Wiegand».....	14
2.3.1.2. Параметр «Разрядность интерфейса Wiegand».....	17
2.3.1.3. Параметр с выбором режима работы считывателя.....	20
2.3.1.4. Параметр «Формат считываемых карт»	21
2.3.1.5. Параметры раздела «Преобразование».....	26
2.3.1.6. Параметры раздела «Настройки для банковских карт».....	34
2.3.1.7. Параметры раздела «Чтение кода из блока»	43
2.3.1.8. Параметры раздела «Зоны прохода»	45
2.3.2. Боковая панель действий.....	50
2.3.2.1. Кнопка «Считать конфигурацию из файла».....	51
2.3.2.2. Кнопка «Записать конфигурацию в файл»	51
2.3.2.3. Кнопка «Считать конфигурацию из USB-считывателя»	51
2.3.2.4. Кнопка «Записать конфигурацию в USB-считыватель».....	52
2.3.2.5. Кнопка «Считать конфигурацию с мастер-карты»	52
2.3.2.6. Кнопка «Считать конфигурацию с мастер-карты и записать в USB-считыватель»	53
2.3.2.7. Кнопка «Создать мастер-карты»	54
2.3.2.8. Кнопка «Очистить мастер-карты»	55
2.3.2.9. Кнопка «Показать конфигурацию по умолчанию»	56

2.3.2.10.	Чекбокс «Помещать ID карты в буфер обмена»	57
2.3.2.11.	Чекбокс «Имитация набора ID карты на клавиатуре».....	57
2.3.2.12.	Чекбокс «+ перевод строки».....	58
2.3.2.13.	Чекбокс «Сворачиваться в трей при запуске».....	59
2.3.3.	Блок «Световая схема».....	59
2.4.	Вкладка «Защищенные карты»	60
2.4.1.	Кнопка «Создать защищенные карты»	62
2.4.2.	Кнопка «Очистить защищенные карты - удалить код объекта/зоны прохода)»	62
2.4.3.	Кнопка «Очистить защищенные карты - удалить все коды объектов/зоны прохода).....	63
2.4.4.	Таблица зон прохода и вспомогательные кнопки	64
2.4.5.	Важные замечания.....	65
2.5.	Вкладка «Обновление микропрограммы»	65
2.6.	Вкладка «Журнал»	66
2.6.1.	Просмотр событий.....	67
2.6.2.	Сохранение журнала в файл	67
3.	НАСТРОЙКА РЕЖИМОВ РАБОТЫ.....	70
3.1.	Обычный режим: «Чтение только UID»	70
3.1.1.	Описание.....	70
3.1.2.	Доступные параметры конфигурации	70
3.1.3.	Настройка считывателя:	71
3.1.4.	Создание мастер-карт для режима «Чтение только UID»	72
3.2.	Защищенный режим «Код объекта».....	72
3.2.1.	Описание режима	72
3.2.2.	Доступные параметры конфигурации	73
3.2.3.	Порядок настройки системы.....	74
3.2.3.1.	Создание мастер-карт для режима «Код объекта»	74
3.2.3.2.	Настройка считывателя в режим «Код объекта».....	75
3.2.3.3.	Запись карт пользователей	76
3.2.4.	Важные замечания.....	76
3.2.5.	Краткое резюме	77
3.3.	Защищенный режим «Чтение кода из блока»	78
3.3.1.	Описание режима	78
3.3.2.	Доступные параметры конфигурации	79
3.3.3.	Порядок настройки системы.....	80
3.3.3.1.	Вариант А: Настройка считывателя для чтения существующих защищенных карт	80
3.3.3.2.	Вариант Б: Настройка считывателя для нового объекта	81

3.3.3.3. <i>Вариант В: Настройка для интеграции с внешними системами</i>	83
3.3.4. Важные замечания.....	88
3.3.5. Краткое резюме	89
3.4. Защищенный режим «Зоны прохода».....	89
3.4.1. Описание режима	89
3.4.2. Доступные параметры конфигурации	90
3.4.3. Порядок настройки системы.....	91
3.4.3.1. <i>Создание мастер-карт для режима «Зоны прохода»</i>	91
3.4.3.2. <i>Перевод считывателя в режим «Зоны прохода»</i>	91
3.4.3.3. <i>Запись карт пользователей</i>	92
3.4.4. Примеры использования	93
3.4.5. Важные замечания.....	94
3.4.6. Краткое резюме	94

1. ВВЕДЕНИЕ

Назначение документа

Настоящий документ представляет собой руководство пользователя по работе с программным обеспечением «Конфигуратор считывателей «ЭРА».


Руководство содержит полный спектр информации, касающейся установки, настройки и эксплуатации считывателей «ЭРА» с использованием указанного программного обеспечения.

Аудитория

Документ предназначен для:

Категория пользователей	Описание
Инженеры по установке СКУД	Выполняют монтаж, настройку и пусконаладку считывателей на объектах
Администраторы безопасности	Управляют системой контроля доступа, выдают и обслуживают карты пользователей
Технические специалисты	Производят диагностику, обновление микропрограммы и решение нештатных ситуаций

Рекомендация:

 Для оптимального использования функциональных возможностей программы настоятельно рекомендуется детально ознакомиться с настоящим руководством перед началом работы.

1.1. Общие сведения о программе

Назначение

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.

Поддерживаемые считыватели

Модель	Тип	Назначение
«ЭРА-USB (MF/EM)»	Настольный	Считывание и передача в программное обеспечение серийных номеров бесконтактных идентификаторов по интерфейсу USB
«ЭРА-MF»	Настенный	Подключение к контроллеру СКУД по проводному интерфейсу связи Wiegand или автономное управление

замком (только в комплектации «ЭРА-MF+»)

«ЭРА-MF v2» Настенный Подключение к контроллеру СКУД по проводному интерфейсу связи Wiegand или автономное управление замком

Мобильная версия

Для конфигурирования считывателя «ЭРА-MF» также предусмотрена возможность использования мобильного устройства на операционной системе (ОС) Android с установленным программным обеспечением «[ЭНТ Сервис](#)» при условии поддержки технологии USB OTG.

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

Функциональные возможности

Программа позволяет выполнять следующие действия:

Категория	Функции
Чтение карт	Отображение ID карты, копирование в буфер обмена, имитация набора на клавиатуре
Конфигурирование	Настройка интерфейса Wiegand (тип, разрядность, преобразования данных), выбор форматов считываемых карт, шифрование банковских карт
Режимы работы	Обычный режим (только UID) и три защищенных режима: «Код объекта», «Чтение кода из блока», «Зоны прохода»
Управление картами	Создание и очистка мастер-карт, запись и очистка защищенных карт пользователей
Обслуживание	Обновление микропрограммы, просмотр и сохранение журнала событий

Подробное описание всех функций приведено в соответствующих разделах настоящего руководства.

Краткое резюме

Программа предназначена для настройки считывателей «ЭРА-USB» и «ЭРА-MF», позволяет читать ID-карты, конфигурировать интерфейс Wiegand, настраивать форматы считываемых карт, работать в защищенных режимах и обновлять микропрограмму.

1.2. Системные требования


Для корректной работы программы «Конфигуратор считывателей «ЭРА» необходимо обеспечить соответствие компьютера следующим требованиям:

Минимальные требования

Компонент	Требование
Операционная система	Windows® 7 / 8 / 10 (32- или 64-разрядная версия)
USB-порт	1 свободный порт
Свободное место на диске	10 МБ
Дополнительно	В некоторых случаях необходима ручная установка драйвера для корректной работы считывателя с ПК

Рекомендации по установке драйвера

Ситуация	Рекомендация
Считыватель не определяется автоматически	Установите драйвер вручную из папки с программой или скачайте с сайта производителя
Считыватель отображается в диспетчере устройств с восклицательным знаком	Обновите драйвер через диспетчер устройств Windows


 При подключении считывателя к компьютеру он должен отображаться в диспетчере устройств Windows в разделе «Порты (COM и LPT)» как «Устройство с последовательным интерфейсом USB (COM#)».

1.3. Контактная информация службы поддержки

Канал связи	Информация
Сайт	www.entpro.ru
Телефон	+7 495 984-76-64, 8 800 777-76-58
Электронная почта	support@entpro.ru

Мы высоко ценим доверие к нашей компании и готовы предоставить комплексную техническую поддержку на всех стадиях жизненного цикла продукта.

1.4. Условные обозначения, принятые в руководстве

Обозначение	Значение
	Критически важная информация. Если не соблюдать правила и условия, описанные в разделах, помеченных

этой меткой, система не будет работать.



Важная информация. Абзацы, выделенные данным знаком, содержат информацию, которая облегчит работу с системой.



Справочная информация. Разъясняет некоторые понятия системы.

Текст, выделенный голубым цветом и с нижним подчёркиванием

Ссылка. Ведёт к определённом месту в данном документе или на внешнюю интернет-страницу.

1.5. Список принятых сокращений

Сокращение Полное наименование

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 идентификационный номер ключа (карты)
PAN	Primary Account Number — номер банковской карты
AES	Advanced Encryption Standard — алгоритм симметричного шифрования
HMAC	Hash-based Message Authentication Code — код аутентификации сообщения
CRC	Cyclic Redundancy Check — циклическая контрольная сумма (в контексте Wiegand — биты четности)

1.6. Краткое резюме по разделу

Раздел 1. «ВВЕДЕНИЕ» содержит общие сведения о программе «Конфигуратор считывателей «ЭРА», системные требования, контактную информацию службы поддержки, условные обозначения и список сокращений.

Программа предназначена для настройки считывателей «ЭРА-USB» и «ЭРА-MF», позволяет читать ID-карты, конфигурировать интерфейс Wiegand, настраивать форматы считываемых карт и обновлять микропрограмму.

Системные требования: Windows 7/8/10, USB-порт, 10 МБ свободного места.

2. РАБОТА С ПРОГРАММОЙ

2.1. Запуск программы и подключение считывателя

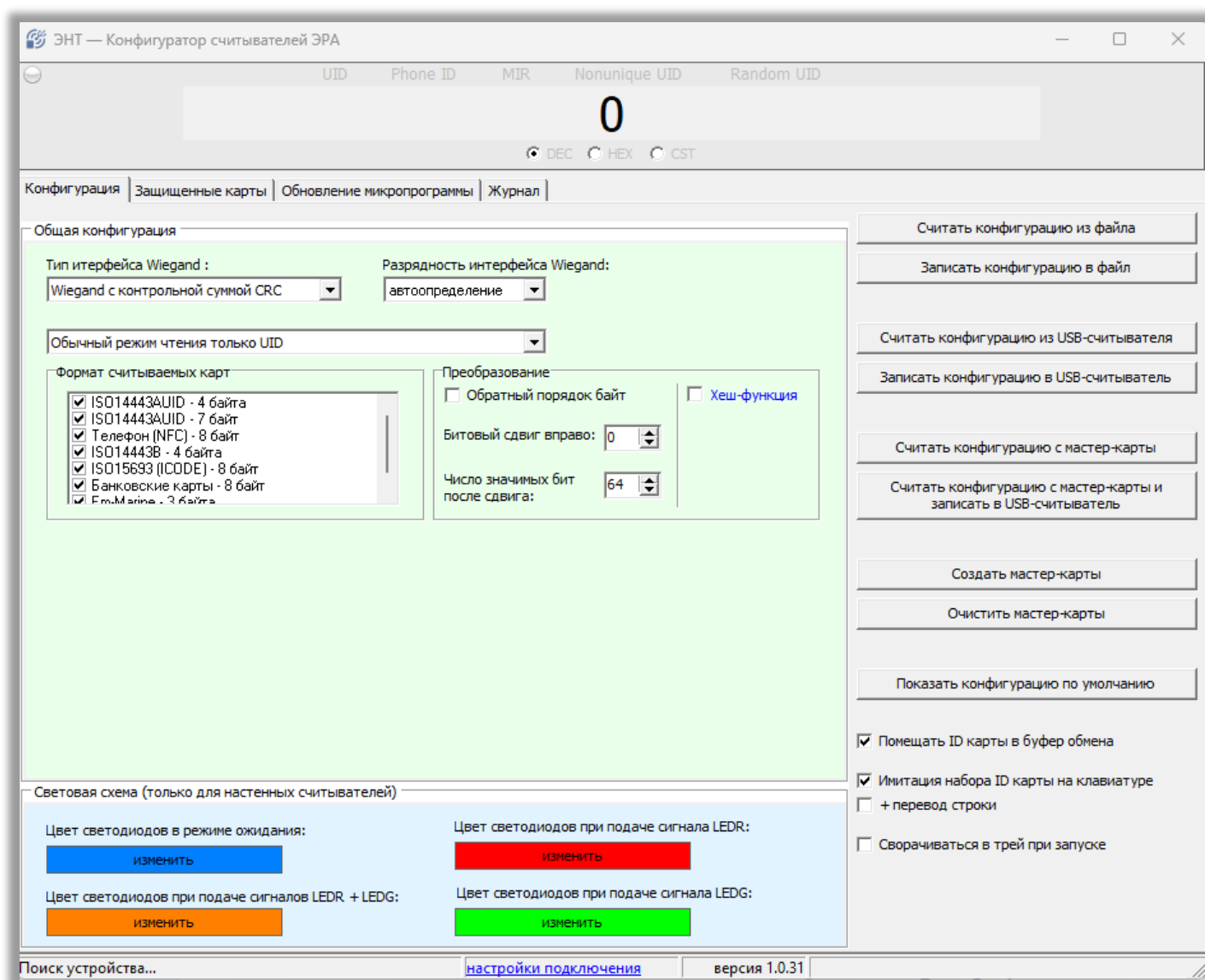
2.1.1. Запуск программы

Для запуска программы выполните следующие действия:

- Распакуйте архив в любую удобную папку (например, C:\ENT\Configurator) и запустите Usbreader.exe.


После запуска на экране отобразится главное окно программы (Рисунок 1). Внешний вид окна может отличаться в зависимости от версии программы.

Рисунок 1. Интерфейс программы без подключённого считывателя



2.1.2. Подключение считывателя к компьютеру

- Подключите считыватель к компьютеру по кабелю через USB-порт.
- Дождитесь, пока операционная система определит устройство.

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

2.1.3. Выбор COM-порта в программе

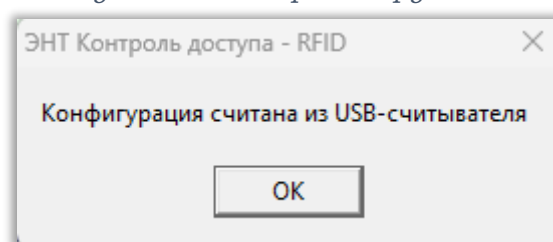
Для выбора считывателя в программе предусмотрены следующие способы:

Способ	Описание
Автоматический поиск	Программа самостоятельно обнаруживает подключенный считыватель
Выбор из списка	Ручной выбор номера COM-порта из выпадающего списка
Ручной ввод	Ввод номера COM-порта вручную (для опытных пользователей)

2.1.4. Автоматическое обнаружение считывателя

При обнаружении считывателя программа автоматически считывает из него текущую конфигурацию. На экране появится окно с соответствующим уведомлением (Рисунок 2).

Рисунок 2. Окно уведомления при обнаружении считывателя



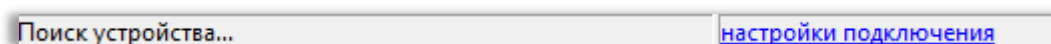
Порядок действий:

- Дождитесь появления окна с уведомлением.
- Нажмите кнопку «**ОК**».
- Программа отобразит считанную конфигурацию в интерфейсе программы.

2.1.5. Ручная настройка подключения

Если считыватель не определился автоматически, настройка подключения осуществляется по нажатию на соответствующую кнопку в нижней части программы (Рисунок 3).

Рисунок 3. Строка состояния подключения



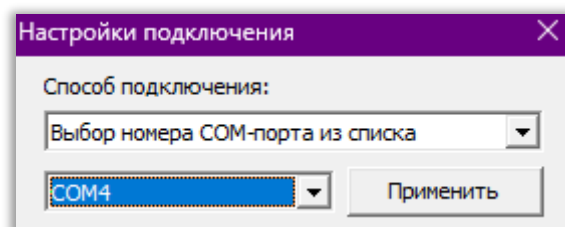
Примечание:

Автоматическое подключение может быть недоступно в некоторых пакетах обновлений на определенных версиях Windows.

Порядок ручной настройки подключения:

- Нажмите на кнопку настройки подключения (выделена синим) в нижней части программы (Рисунок 3).
- В открывшемся окне выберите из списка номер COM-порта, соответствующий подключенному считывателю.
- Нажмите кнопку «**Применить**» (Рисунок 4).

Рисунок 4. Окно настройки подключения



- После успешного подключения программа считывает конфигурацию из считывателя.

2.1.6. Диагностика подключения

<i>Симптом</i>	<i>Возможная причина</i>	<i>Рекомендация</i>
Считыватель не отображается в списке COM-портов	Не установлен драйвер	Установите драйвер вручную из папки с программой
Считыватель отображается с восклицательным знаком	Конфликт драйверов	Переустановите драйвер через диспетчер устройств
Программа не видит считыватель	Неверный COM-порт	Проверьте номер COM-порта в диспетчере устройств
Ошибка при считывании конфигурации	Считыватель не отвечает	Отключите и снова подключите считыватель, повторите попытку

2.1.7. Важные замечания

- Драйвер устройства: для корректной работы считывателя в некоторых случаях требуется ручная установка драйвера. Драйвер поставляется в комплекте с программой.
- Права администратора: при установке драйвера и запуске программы на некоторых версиях Windows могут потребоваться права администратора.
- Автоматическое определение: программа запоминает последний использованный COM-порт и при следующем запуске пытается подключиться к нему автоматически.
- Подключение и отключение считывателя: Считыватель можно подключать и отключать от компьютера во время работы программы. Перезапуск

программы, компьютера или считывателя при этом не требуются.

- Не рекомендуется отключать считыватель во время выполнения следующих операций:
 - Запись конфигурации в считыватель;
 - Обновление микропрограммы считывателя;
 - Запись мастер-карт или карт пользователей;
 - Очистка мастер-карт.

Прерывание связи в этих процессах может привести к некорректной работе считывателя или повреждению данных.

2.2. «Поле вывода UID»

Назначение:

Отображает идентификационные номера, полученные от карты или мобильного устройства через считыватель и переданные в интерфейс программы.

Расположение:

Верхняя область основного окна программы (Рисунок 1).

Отображаемые типы идентификаторов

В поле выводятся следующие идентификаторы:

Тип	Описание
UID	Уникальный идентификатор карты (производителя. Рисунок 5).
Phone ID	Идентификатор мобильного устройства (NFC).
MIR	Идентификатор банковской карты платёжной системы «Мир» (только для спец. проекта).
Nonunique UID	Неуникальный идентификатор (может повторяться на разных картах).
Random UID	Случайный идентификатор (меняется при каждом считывании. Рисунок 6).

Примеры отображения:

Рисунок 5. Вывод UID Mifare Classic

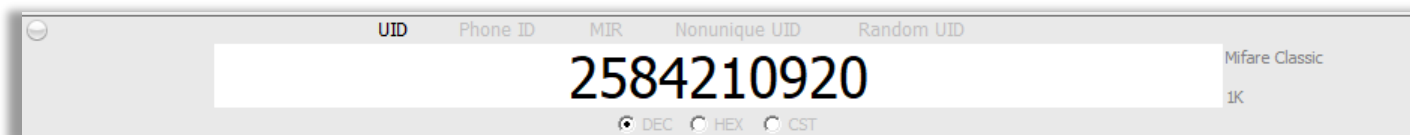
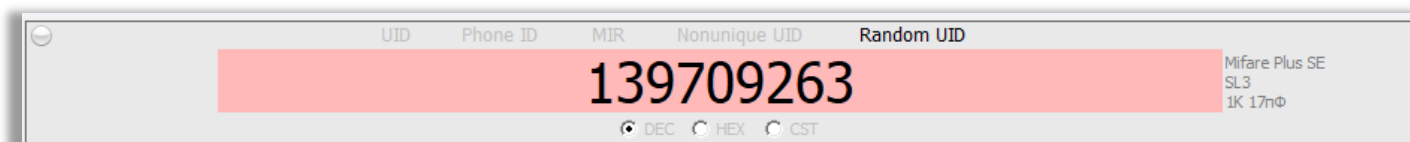
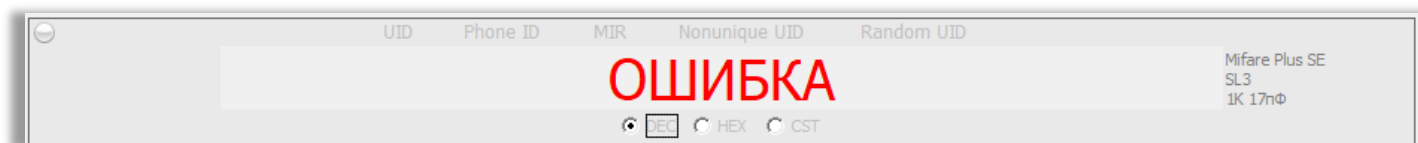


Рисунок 6. Вывод случайного идентификатора Mifare Plus



Случайная генерация UID может быть вызвана переводом карты в защищенный режим без соответствующей активации считывающего устройства в аналогичном режиме.

Рисунок 7. Вывод ошибки при получении UID



Ошибка может возникнуть в случае:

- Если считывающее устройство функционирует в защищённом режиме, а используемая карта — нет.
- Также проблема может быть обусловлена тем, что считывающее устройство и карта находятся в различных защищённых режимах.
- Дополнительно следует учитывать, что подобная ситуация может наблюдаться при попытке считать UID мастер-карты.

Выбор формата отображения

Под полем вывода расположены элементы управления форматом отображения идентификатора:

Элемент *Назначение*

DEC	Отображает UID в десятичной системе счисления
HEX	Отображает UID в шестнадцатеричной системе счисления
CST	Открывает редактор для создания собственного пользовательского шаблона отображения UID

Порядок выбора формата:

- Установите кружок (переключатель) в нужном чекбоксе: DEC или HEX.
- Формат отображения UID изменится.

Создание пользовательского шаблона (CST):

- Установите кружок в чекбоксе CST.
- Откроется редактор для создания собственного шаблона отображения UID.
- Настройте шаблон в соответствии с требуемым форматом вывода.
- Сохраните настройки шаблона.

Результат:

UID отображается в выбранном формате (DEC, HEX или пользовательском CST).

2.3. Вкладка «Конфигурация»

Назначение вкладки

Вкладка «Конфигурация» является основным рабочим пространством программы

«Конфигуратор считывателей «ЭРА». Здесь выполняется полная настройка параметров считывателя: от выбора формата передачи данных до настройки цветовой индикации и сохранения конфигурации (Рисунок 8).

Все изменения, внесенные на этой вкладке, применяются к считывателю после нажатия соответствующих кнопок в панели «Действия».


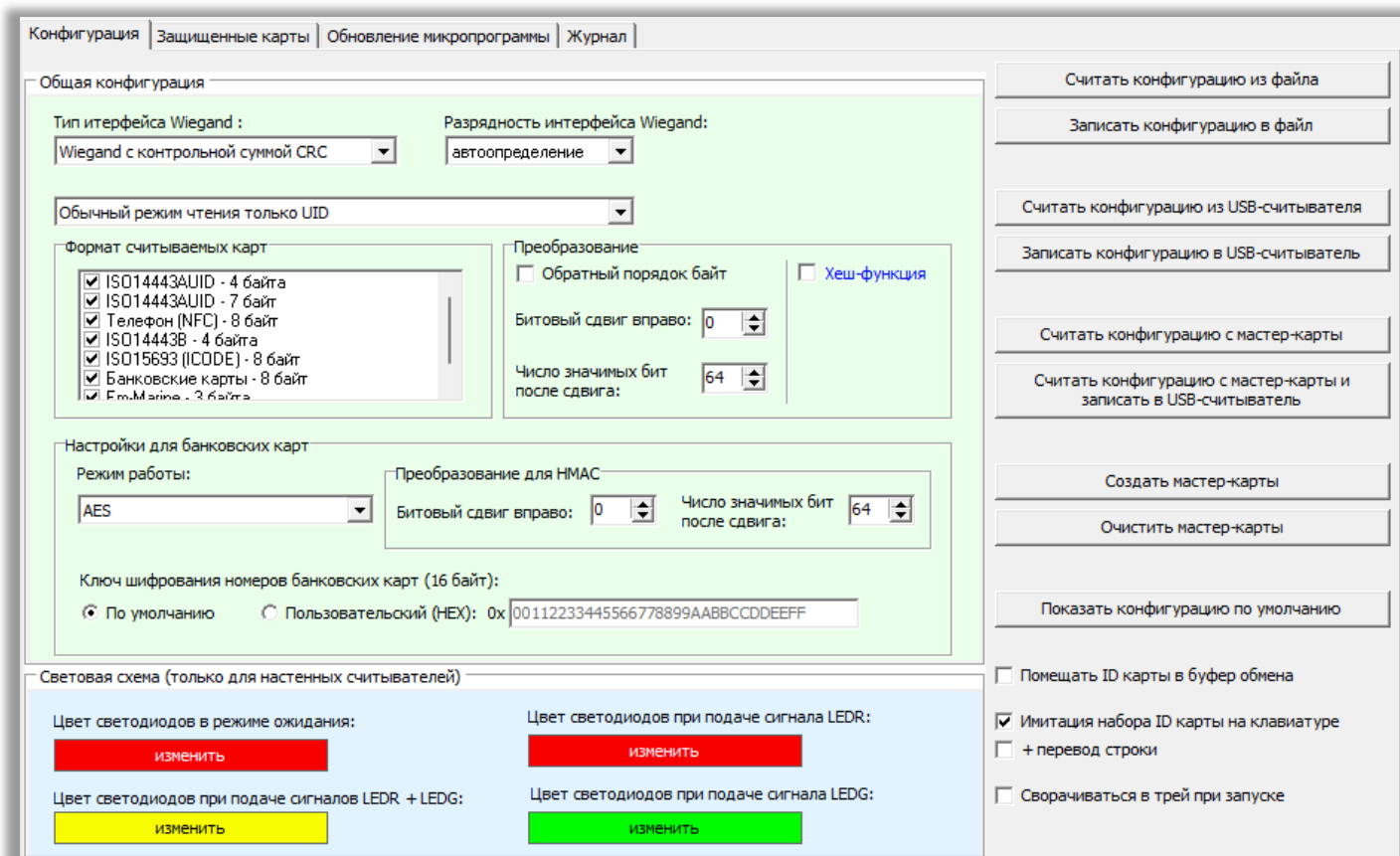
 Для записи указанных настроек в память считывателя нажмите кнопку «Записать конфигурацию в USB-считыватель».

Рисунок 8. Интерфейс программы с конфигурацией по умолчанию (от производителя)



Состав вкладки

Вкладка «Конфигурация» включает три основных блока:

Блок	Расположение	Назначение
<u>Блок «Общая конфигурация»</u>	Центральная область	Основные параметры работы считывателя: формат Wiegand, режим идентификации, поддерживаемые типы карт, преобразования данных и настройки для банковских карт
<u>Световая схема</u>	Нижняя часть	Настройка цветов светодиодной индикации (только для настенных считывателей серии «MF»)
<u>Панель действий</u>	Правая боковая панель	Кнопки для чтения, записи, сохранения конфигурации, работы с мастер-картами, а

также чекбоксы для вывода ID карты в сторонние приложения

2.3.1. Блок «Общая конфигурация»

Основной блок, определяющий поведение считывателя при идентификации карт и передаче данных на контроллер.

Рисунок 9. Общая конфигурация в обычном режиме чтения UID

i Отображение параметров в блоке «Общая конфигурация» меняется в зависимости от выбранного режима работы для считывателя.

2.3.1.1. Параметр «Тип интерфейса Wiegand»

Назначение параметра

Представляет собой раскрывающийся список. Параметр определяет формат данных, которые считыватель передает на контроллер по интерфейсу Wiegand. От выбранного значения зависит структура передаваемого пакета и наличие в нем контрольных битов четности.

Доступные значения

Значение


Краткое описание

«Wiegand без контрольной суммы CRC»

Считыватель передает на контроллер весь считанный UID (уникальный идентификатор карты) «как есть», в виде последовательности битов. Контрольные биты четности не добавляются.

«Wiegand с контрольной суммой CRC»

Считыватель добавляет к передаваемым данным 2 бита четности (Parity Bits) для контроля целостности передачи. Фактически в данном режиме включается стандартный механизм четности, предусмотренный протоколом Wiegand.

 Название параметра использует термин «CRC» для обозначения режима с проверкой целостности, однако технически в данном случае применяются биты четности (Parity), а не циклическая контрольная сумма (CRC). Это следует учитывать при интерпретации документации сторонних устройств.

Подробное описание значений

1. «Wiegand без контрольной суммы CRC»

В этом режиме считыватель работает в максимально простом и совместимом варианте.

Принцип работы:

- Считыватель извлекает UID (уникальный идентификатор) с карты или метки.
- Полученный UID передается на контроллер последовательностью импульсов по линиям Data0 и Data1.
- Передаваемая последовательность соответствует всем битам UID без каких-либо изменений, дополнений или служебных битов.

Особенности:

- Длина передаваемого пакета полностью определяется битностью UID считанной карты (например, 32 бита, 40 бит, 56 бит и т.д.).
- Контроллер принимает данные в «сыром» виде и сам интерпретирует их в соответствии со своими настройками.
- Контроль целостности передачи (обнаружение ошибок из-за помех) в этом режиме не осуществляется.

Рекомендуется использовать:

- При подключении к контроллерам, которые требуют приема UID в полном объеме без дополнительной обработки.
- Для обеспечения максимальной совместимости с различными моделями контроллеров.

2. «Wiegand с контрольной суммой CRC»

В этом режиме считыватель формирует пакет данных в соответствии со стандартным протоколом Wiegand, добавляя биты четности для контроля целостности передачи.

Принцип работы:

- Считыватель извлекает UID с карты или метки.
- К полученным битам UID считыватель добавляет 2 бита четности:
 - **Первый бит четности** (старший) контролирует четность одной половины битов.
 - **Второй бит четности** (младший) контролирует четность второй половины битов.
- Итоговый пакет передается на контроллер в формате: [бит четности] + [биты UID] + [бит четности].

Особенности:

- Общая длина передаваемого пакета увеличивается на 2 бита по сравнению с исходным UID.
- Контроллер на принимающей стороне проверяет биты четности. Если четность не сходится, пакет считается поврежденным и отбрасывается.
- Данный режим соответствует классической реализации протокола Wiegand (например, в формате Wiegand-26, где 2 бита отводятся под четность, а 24 бита — под данные).

Рекомендуется использовать:

- При подключении к контроллерам, которые ожидают стандартный Wiegand-формат с битами четности.
- В условиях возможных электромагнитных помех, когда требуется базовый контроль целостности передачи.
- Для обеспечения совместимости с оборудованием, где включение битов четности является обязательным требованием.

Сравнительная таблица

<i>Характеристика</i>	<i>Без CRC (без четности)</i>	<i>С CRC (с четностью)</i>
Передаваемые данные	Только UID карты	UID карты + 2 бита четности
Длина пакета	Равна битности UID	Битность UID + 2 бита
Контроль целостности	Отсутствует	Базовый (проверка четности)
Совместимость	Универсальная (любые контроллеры)	Контроллеры, поддерживающие стандартный Wiegand с четностью
Помехозащищенность	Низкая (ошибки не отслеживаются)	Средняя (ошибки обнаруживаются)

Рекомендации по выбору

Сценарий подключения

Рекомендуемое значение

Контроллер настроен на прием «сырого» UID (Raw Mode)	Wiegand без контрольной суммы CRC
Контроллер ожидает стандартный Wiegand-формат (например, Wiegand-26, Wiegand-34)	Wiegand с контрольной суммой CRC
Требуется максимальная совместимость с неизвестным контроллером	Начать с режима без CRC, при необходимости переключить на с CRC
Система работает в условиях электромагнитных помех, и контроллер поддерживает четность	Wiegand с контрольной суммой CRC



Важные замечания:

- **Согласованность настроек:** Считыватель и контроллер должны быть настроены на одинаковый режим работы. Если считыватель передает пакет с битами четности, а контроллер ожидает данные без них (или наоборот), идентификация карты происходить не будет.
- **Длина пакета:** при включении режима «с CRC» общая длина передаваемых данных увеличивается на 2 бита. Убедитесь, что контроллер поддерживает прием пакетов соответствующей длины.
- **Диагностика неисправностей:** если после изменения параметра считыватель перестал передавать данные на контроллер:
 - Верните настройку в исходное положение;
 - Проверьте, какой режим ожидает контроллер;
 - Убедитесь, что длина пакета (битность UID + 2 при включенной четности) поддерживается контроллером.

2.3.1.2. Параметр «Разрядность интерфейса Wiegand»

Назначение параметра

Представляет собой раскрывающийся список. Параметр определяет, каким образом считыватель определяет длину (разрядность) передаваемого Wiegand-пакета. От выбранного значения зависит, будет ли считыватель автоматически подстраиваться под формат считанной карты или использовать фиксированную длину, заданную вручную.

Доступные значения

Значение	Краткое описание
«Автоопределение»	Считыватель автоматически анализирует данные, полученные от карты или метки, сопоставляет их со стандартными Wiegand-форматами и формирует пакет соответствующей длины.

Считыватель использует фиксированную длину пакета, «Пользовательская» заданную пользователем в дополнительном поле. Диапазон настройки — от 8 до 64 бит.

Подробное описание

1. «Автоопределение»

В этом режиме считыватель самостоятельно определяет, какой формат данных был считан с карты или метки, и формирует исходящий Wiegand-пакет соответствующей длины.

Принцип работы:

- Считыватель получает от карты (метки) уникальный идентификатор (UID) и служебные данные.
- Считыватель анализирует полученную структуру и сопоставляет ее с известными стандартными форматами Wiegand (например, Wiegand-26, Wiegand-34, Wiegand-37 и другими).
- На основе этого сопоставления считыватель определяет, сколько бит должно быть передано на контроллер.
- Формируется и отправляется пакет соответствующей длины (с учетом настроек битов четности, если они включены).

Особенности:

- Считыватель автоматически адаптируется под различные типы карт и меток без необходимости ручной настройки.
- Длина передаваемого пакета может меняться в зависимости от того, какая карта приложена к считывателю.
- Режим обеспечивает максимальную совместимость при работе с разными типами идентификаторов в рамках одной системы.

Рекомендуется использовать:

- В системах, где используются карты и метки различных типов и форматов.
- При подключении к контроллерам, поддерживающим автоматическое определение длины Wiegand-пакета.
- Для упрощения настройки и обслуживания системы.

2. «Пользовательская»

В этом режиме считыватель использует фиксированную длину Wiegand-пакета, заданную пользователем вручную. При выборе данного значения становится доступным дополнительное поле для указания количества бит.

Параметры настройки:

- Диапазон значений: от 8 до 64 бит.
- Шаг изменения: 1 бит.

Принцип работы:

- Считыватель получает UID от карты или метки.
- Из полученных данных извлекается количество бит, соответствующее заданному пользователем значению (как правило, это младшие биты UID или биты, начиная с определенной позиции, в зависимости от внутренней логики считывателя).
- Формируется и отправляется пакет строго заданной длины (с учетом настроек битов четности, если они включены).

Особенности:

- Позволяет жестко зафиксировать длину пакета, что необходимо при работе с контроллерами, не поддерживающими автоматическое определение формата.
- Дает возможность обрезать или расширять передаваемые данные до требуемой длины.
- Обеспечивает предсказуемое поведение системы: все карты передаются в едином формате независимо от их исходной битности.

Рекомендуется использовать:

- При подключении к контроллерам, которые ожидают пакет строго определенной длины (например, только Wiegand-26 или только Wiegand-34).
- В системах, где используются карты одного типа с одинаковой битностью.
- Когда требуется стандартизировать передаваемые данные для упрощения интеграции с верхним программным обеспечением.

Рекомендации по выбору

<i>Сценарий использования</i>	<i>Рекомендуемое значение</i>	<i>Уточнение</i>
Используются карты разных форматов	Автоопределение	Считыватель сам подберет корректный формат для каждой карты
Контроллер поддерживает автоопределение Wiegand-форматов	Автоопределение	Наиболее простой и универсальный вариант
Контроллер настроен на прием строго определенного формата	Пользовательская	Укажите длину, соответствующую

(например, только 26 бит)		настройкам контроллера
Требуется унифицировать данные от всех карт в единый формат	Пользовательская	Задайте фиксированную длину, подходящую для вашей системы
Возникают проблемы с идентификацией карт в режиме автоопределения	Пользовательская	Фиксация длины поможет устранить несовместимость



Важные замечания:

- Взаимосвязь с битами четности: Заданная разрядность влияет на итоговую длину пакета с учетом настроек параметра «**Тип интерфейса Wiegand**»:
 - Если выбран режим «**без CRC**» (без битов четности), пакет будет иметь длину, равную указанной разрядности.
 - Если выбран режим «**с CRC**» (с битами четности), к указанной разрядности будут добавлены 2 бита четности. Итоговая длина пакета составит $N + 2$ бита.
- Ограничения автоопределения: при значении «**Автоопределение**» распознаются только стандартные Wiegand-форматы. Если карта имеет нестандартную структуру данных или используется специфический формат, может потребоваться ручная настройка разрядности.
- Обрезание данных: при использовании «**Пользовательской**» разрядности с длиной, меньшей, чем исходная битность UID карты, часть данных будет обрезана. Убедитесь, что это не приводит к потере уникальности идентификатора (коллизиям, когда разные карты начинают передавать одинаковый номер).
- Диагностика неисправностей: если после изменения разрядности считыватель перестал передавать данные на контроллер:
 - Проверьте, какую длину пакета ожидает контроллер;
 - Убедитесь, что выбранная разрядность соответствует настройкам контроллера (с учетом добавления битов четности);
 - Временно верните режим «Автоопределение» для проверки работоспособности считывателя.

2.3.1.3. Параметр с выбором режима работы считывателя

Представляет собой раскрывающийся список. Параметр определяет режим взаимодействия считывателя с картами (метками) и способ обработки считанных данных. От выбранного режима зависит, какая информация извлекается из карты и передается на контроллер, а также доступный набор настроек в интерфейсе программы.

Доступные значения

Значение

Краткое описание

Обычный режим чтения
«Только UID»

Считыватель извлекает только уникальный идентификатор (UID) карты и передает его на контроллер. Наиболее простой и универсальный режим.

Защищенный режим
«Код объекта»

Идентификация карт происходит не по UID, а по информации, содержащейся в определенной области памяти карты, закрытой от чтения секретным ключом.

Защищенный режим
«Чтение кода из блока»

Считыватель обращается к защищенной области памяти карты (сектор/блок), где хранится пользовательский идентификатор, и передает его на контроллер. Повышает уровень защиты от клонирования.


Защищенный режим
«Зоны прохода»

В данном режиме считыватель работает в роли контроллера доступа. Идентификация происходит не по UID карты, а по записанным в память карты зонам прохода. Аналогично режиму «Код объекта», основывается на использовании уникального идентификатора объекта.



Важные замечания:

- Совместимость карт: не все режимы поддерживаются всеми типами карт. Убедитесь, что используемые карты поддерживают выбранный режим работы.
- Предварительная подготовка: режимы «код объекта», «чтение кода из блока» и «зоны прохода» требуют предварительной записи данных на карты с использованием соответствующе настроенного программного обеспечения и оборудования.
- Изменение режима: смена режима работы считывателя после того, как карты уже выданы пользователям, может привести к невозможности идентификации ранее выданных карт.
- Обратная совместимость: карты, подготовленные для защищенных режимов, не будут корректно работать в считывателях, настроенных на обычный режим чтения UID (и наоборот).
- Взаимосвязь с другими параметрами: доступные значения параметров в интерфейсе программы зависят от выбранного режима работы.

 С подробным описанием каждого режима можно ознакомиться в соответствующем разделе данного руководства.

2.3.1.4. Параметр «Формат считываемых карт»

Назначение параметра

Представляет собой список с чекбоксами. Параметр позволяет гибко настраивать

поддержку различных типов карт и меток, которые может распознавать считыватель. Доступные форматы зависят от выбранного режима работы считывателя (параметр «Режим работы считывателя»).

С помощью чекбоксов (флажков) можно включать или отключать поддержку определенных стандартов.

В зависимости от выбранного режима работы для считывателя меняются доступные форматы считываемых карт.

Краткое описание доступных форматов с учетом режимов работы

Режим чтения	Идентификаторы	Стандарт
<u>Обычный режим чтения</u> <u>«Только UID»</u>	Mifare Classic, Ultralight, Plus, DESFire и т.п.	ISO14443A – 4 и 7 байт ISO14443B – 4 байта
	Em-Marine	Em-Marine – 3 байта
	Мобильные устройства	NFC – 8 байт
	Банковские карты С чипом ICODE	EMV – 8 байт ISO15693 – 8 байт
<u>Защищенный режим «Код объекта»</u>	Mifare Classic 1K и 4K, Mifare Plus SE, S, X	ISO14443A – 4 и 7 байт
<u>Защищенный режим «Чтение кода из блока»</u>	Mifare Plus SE, S, X	ISO14443A – 4 и 7 байт
<u>Защищенный режим «Зоны прохода»</u>	Mifare Plus SE, S, X	ISO14443A – 4 и 7 байт

Включение только необходимых форматов позволяет:

- Ускорить обработку карт за счет сокращения времени перебора форматов;
- Исключить ложное срабатывание на неиспользуемые типы карт;
- Повысить безопасность, ограничивая допустимые типы идентификаторов.

Описание форматов с учетом режимов работы

1. ISO14443A с UID размером 4 байта

Этот формат является наиболее распространенным в системах контроля доступа. Стандарт карт Mifare Classic, Mifare Ultralight, Mifare Plus (в режиме совместимости) и т.п. Длина идентификационного номера ключе не превышает 4 байт.

Доступность:

- Обычный режим чтения только UID: ✓ Доступен;
- Защищенный режим: код объекта: ✓ Доступен (используется для чтения кода объекта из защищенной области карт Mifare Classic);
- Защищенные режимы: чтение кода из блока / зоны прохода: – Недоступен.

Примечание:

В защищенном режиме «код объекта» используются карты Mifare Classic, работающие на стандарте ISO14443A с 4-байтным UID.

2. ISO14443A с UID размером 7 байт

Формат используется для карт с расширенным уникальным идентификатором.

Описание: Карты и метки стандарта ISO/IEC 14443A с расширенным UID (например, Mifare Plus, Mifare Desfire и т.п.). Длина идентификационного номера ключе не превышает 7 байт.

Доступность:

- Обычный режим чтения только UID: ✓ Доступен;
- Защищенные режимы (все): – ✓ Доступен (используется для чтения кода объекта из защищенной области карт Mifare Plus).

Особенности:

Обеспечивает большую уникальность идентификаторов за счет увеличенной разрядности.

Примечание:

Данный формат используется только для чтения UID в обычном режиме. Для защищенных режимов применяются карты на базе Mifare Plus (описаны ниже).

3. Телефон с NFC (мобильное устройство на базе ОС Android)

Данный формат позволяет использовать смартфоны на базе Android в качестве идентификаторов доступа. Длина идентификационного номера ключе не превышает 8 байт.

Доступность:

- Обычный режим чтения только UID: ✓ Доступен;
- Защищенные режимы (все): – Недоступен.

Важные условия работы:

- Для корректной работы на мобильном устройстве должна быть предустановлена и запущена программа «ЭНТ Доступ»;
- Приложение генерирует уникальный идентификатор каждого мобильного устройства, который считывается и передается на контроллер;
- Без запущенного приложения смартфон не будет распознаваться считывателем.

Примечание:

Использование смартфонов в качестве идентификаторов требует предварительной

установки и настройки программного обеспечения на каждом устройстве.

4. ISO14443B – 4 байта

Стандарт карт ISO/IEC 14443B который отличается от более распространенного типа А протоколом обмена (например, некоторые типы транспортных карт, идентификационные карты). Длина идентификационного номера ключе не превышает 4 байт.

Области применения:

- Некоторые транспортные системы;
- Национальные идентификационные карты;
- Специализированные карты доступа.

Доступность:

- Обычный режим чтения только UID: ✓ Доступен;
- Защищенные режимы (все): – Недоступен.

Примечание:

Данный формат не используется в защищенных режимах работы считывателя.

5. ISO15693 (ICODE) – 8 байт

Стандарт карт дальнего радиуса действия ISO/IEC 15693 (например, ICODE SLI, TI Tag-it). Длина идентификационного номера ключе не превышает 8 байт. Они оптимальны для сценариев, где важны дальность, устойчивость к помехам и массовое считывание (антиколлизия), но не требуется высокий уровень криптографической защиты.

Области применения:

- Системы логистики (учет товаров, складские системы);
- Библиотечные системы (учет книг);
- СКУД (реже, но используется для парковочных систем, где требуется увеличенная дистанция чтения).

Доступность:

- Обычный режим чтения только UID: ✓ Доступен;
- Защищенные режимы (все): – Недоступен.

Примечание:

Формат применяется в системах логистики, библиотечных системах и некоторых СКУД, но не используется в защищенных режимах.

6. Банковские карты – 8 байт

Поддержка технологии чтения банковских (платежных) карт в соответствии с

международным стандартом EMV. Длина идентификационного номера ключе не превышает 8 байт. В процессе чтения происходит сканирование номера карты, который представляет собой 16-значный идентификатор, расположенный на лицевой стороне карты. Данный номер подвергается криптографическому преобразованию с использованием установленного алгоритма шифрования.

Доступность:

- Обычный режим чтения только UID: ✓ Доступен;
- Защищенные режимы (все): – Недоступен.

Особенности настройки:

Для работы с банковскими картами предусмотрены специальные настройки, связанные с шифрованием UID. Данные настройки направлены на обеспечение безопасности при использовании банковских карт в системах контроля доступа.

Передача идентификационного номера карты с устройства считывания на контроллер осуществляется в зашифрованном формате. Подробное описание настроек шифрования банковских карт в разделе [2.3.1.6. «Параметры раздела «Настройки для банковских карт»»](#).

7. Em-Marine – 3 байта

Карты и метки стандарта Em-Marine (EM4100, EM4102). Длина идентификационного номера ключе не превышает 3 байт.

Доступность:

- Обычный режим чтения только UID: ✓ Доступен (только для считывателей «ЭРА-USB-MF/EM»);
- Защищенные режимы (все): – Недоступен.

Примечание:

Формат доступен исключительно для считывателей модели «ЭРА-USB-MF/EM», поддерживающих работу на частоте 125 кГц.



Важные замечания:

- При выборе «Обычный режим чтения только UID». Чем больше форматов включено, тем больше времени требуется считывателю на опрос и идентификацию карты. Для повышения быстродействия рекомендуется включать только необходимые форматы.
- Совместимость оборудования: формат Em-Marine доступен только для моделей считывателей, поддерживающих частоту 125 кГц (например, «ЭРА-USB-MF/EM»). Для считывателей, работающих только на 13.56 МГц (например, «ЭРА-MF»), этот формат недоступен.

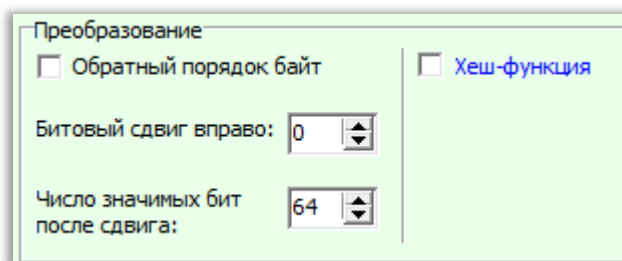
- При выборе защищенного режима «Код объекта» автоматически доступны только карты формата ISO14443A с максимальным размером UID 8 байт (Mifare Classic, Mifare Plus). Остальные форматы недоступны для выбора.
- При выборе защищенного режима «Чтение кода из блока» или «Зоны прохода» автоматически доступны только карты Mifare Plus. Форматы, не поддерживающие работу с защищенными блоками памяти, недоступны.

2.3.1.5. Параметры раздела «Преобразование»

Назначение раздела

Параметры блока «Преобразование» позволяют изменять формат передаваемых данных (UID) перед отправкой на контроллер. Эти настройки дают возможность адаптировать выходной сигнал считывателя под требования конкретного контроллера или системы, которые могут ожидать данные в определенном порядке байт, со сдвигом битов или ограниченной разрядностью.

Рисунок 10. Параметры раздела "Преобразование"



Доступные параметры

Параметр	Описание	Диапазон значений
<u>Параметр «Обратный порядок байт»</u>	Инвертирует порядок следования байт в UID	Вкл. / Выкл. (чекбокс)
<u>Параметр «Битовый сдвиг вправо»</u>	Сдвигает битовое представление UID вправо на указанное количество позиций	0 (по умолчанию) или от 1 до 63
<u>Параметр «Число значимых бит после сдвига»</u>	Ограничивает количество бит, передаваемых на контроллер	64 (по умолчанию) или от 1 до 64
<u>Опция «Хеш-функция»</u>	Преобразует исходный UID карты в хеш-значение фиксированной длины	Вкл. / Выкл. (чекбокс)

Подробное описание параметров

2.3.1.5.1. Параметр «Обратный порядок байт»

Принцип работы:

Представляет собой чекбокс (квадратик), в который можно поставить или убрать

галочку. При включении данной опции считыватель изменяет порядок следования байт в UID на обратный (little-endian вместо big-endian или наоборот, в зависимости от исходного формата). При этом порядок битов внутри каждого байта сохраняется.

Пример преобразования:

Исходный UID (DEC): 3881151482

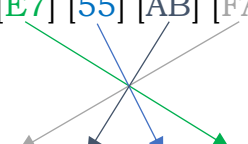
Представление	Значение
HEX	E7 55 AB FA
BIN	11100111 01010101 10101011 11111010
Порядок байт	1-й байт: E7, 2-й байт: 55, 3-й байт: AB, 4-й байт: FA

После включения «Обратный порядок байт»:

Представление	Значение
HEX	FA AB 55 E7
BIN	11111010 10101011 01010101 11100111
DEC	4205532647

Визуальное представление:

Исходный UID (побайтно): [E7] [55] [AB] [FA]



После обратного порядка: [FA] [AB] [55] [E7]

Рекомендации:

- Включайте, если необходима передача данных в формате little-endian (младший байт первым).
- Отключайте, если используется стандартный порядок байт (старший байт первым).

2.3.1.5.2. Параметр «Битовый сдвиг вправо»

Принцип работы:

Представляет собой поле с цифровым выбором. Параметр позволяет сдвинуть битовое представление UID вправо на указанное количество позиций. При каждом сдвиге на одну позицию:

- С левой стороны (старшие биты) добавляется нулевой бит;
- С правой стороны (младшие биты) один бит отбрасывается.

Пример преобразования:

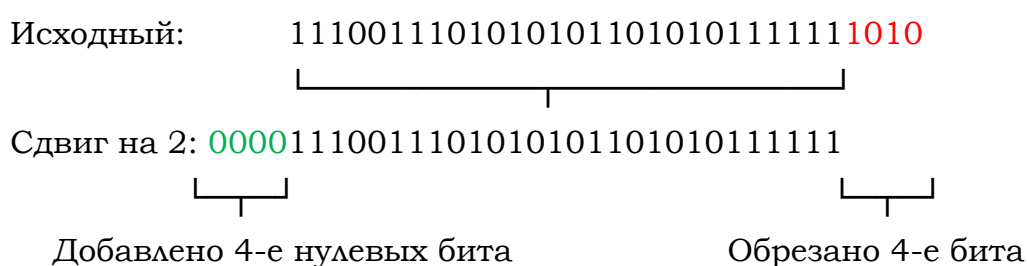
- Исходный UID (DEC): 3881151482, (DEX) E755ABFA;

- Бинарное представление (32 бита): 11100111010101011010101111111010.

При сдвиге вправо на 2 бита:

Этап	Описание
Исходный UID (32 бита)	11100111 01010101 10101011 11111010
Сдвиг вправо на 4 бита	Отбрасываются 4 младших бита (1010), добавляются 4 нулевых бита слева
Результат (32 бита)	00001110 01110101 01011010 10111111
DEC	242571967
HEX	E755ABF

Визуальное представление:




Рекомендации:

- Используйте для обеспечения корректного согласования разрядности при передаче данных с изменённым битовым сдвигом относительно исходного уникального идентификатора (UID);
- Поле пустое (значение 0) означает отсутствие сдвига.

2.3.1.5.3. Параметр «Число значимых бит после сдвига»

Принцип работы:

Представляет собой поле с цифровым выбором. Параметр ограничивает количество бит, которое будет передано на контроллер. Если указанное значение меньше фактической длины UID (после применения сдвига), лишние биты обрезаются с левого конца (старшие биты).

 При увеличении значения параметра «Битовый сдвиг вправо» максимально доступное значение для параметра «Число значимых бит после сдвига» уменьшается, так как сдвиг сокращает общее количество значимых бит в данных.

Пример преобразования:

- Исходный UID (DEC): 7774984, (HEX) 76A308;
- Бинарное представление (24 бита): 01110110 10100011 00001000.

Параметр

Значение

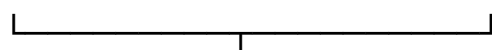
Число значимых бит после сдвига	20
---------------------------------	----

Результат:

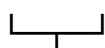
Этап	Описание
Исходный UID (24 бита)	011101101010001100001000
Обрезание до 20 бит	Обрезаются 4 старших бита (0111)
Результат (20 бит)	01101010001100001000
DEC	434952
HEX	6A308

Визуальное представление:

Исходный (24 бита): 011101101010001100001000



Обрезание до 20 бит: 01101010001100001000



Обрезано 4-е бита (0111)

Рекомендации:


- Устанавливайте значение, соответствующее ожидаемой разрядности контроллера.
- По умолчанию установлено значение 64, что позволяет передавать UID без обрезания (при условии, что исходный UID не превышает 64 бит).

Взаимосвязь параметров «Битовый сдвиг вправо» и «Число значимых бит после сдвига»

При увеличении значения параметра «Битовый сдвиг вправо» фактическая длина значимых бит в данных уменьшается. Это влияет на максимально доступное значение параметра «Число значимых бит после сдвига».

Пример:

Исходная длина UID	Сдвиг вправо	Максимальное число значимых бит
64 бита	0	64
64 бита	4	60
64 бита	10	54
64 бита	63	1

 Параметр «Число значимых бит после сдвига» не может быть больше, чем (исходная длина UID - битовый сдвиг). При попытке установить некорректное значение программа автоматически скорректирует его до допустимого максимума.



Важные замечания:

- Потеря уникальности: при использовании сдвига или обрезания бит возможно возникновение коллизий, когда два разных UID после преобразований дают одинаковый результат. Убедитесь, что выбранные параметры не приводят к потере уникальности идентификаторов.
- Совместимость: перед настройкой убедитесь, что выбранные параметры соответствуют требованиям системы. Несовпадение может привести к невозможности идентификации карт.
- Проверка результата: при изменении параметров рекомендуется протестировать работу считывателя с несколькими картами, чтобы убедиться в корректности преобразований.

2.3.1.5.4. Опция «Хеш-функция»

Назначение опции

Представляет собой чекбокс (квадратик), в который можно поставить или убрать галочку. Опция включает механизм хеширования (преобразования) уникального идентификатора карты (UID) для формирования выходного кода, передаваемого на контроллер. Предназначена для ситуаций, когда длина UID карты превышает разрядность протокола Wiegand, используемого для передачи данных.

При включении хеш-функции считыватель вычисляет хеш-значение по всему UID карты. Это позволяет получить уникальный выходной код для каждой карты даже при ограниченной разрядности Wiegand, поскольку изменение любого бита исходного UID приводит к изменению всего результирующего хеш-значения.

Активация опции «Хеш-функция» деактивирует остальные параметры в блоке «Преобразование».

Принцип работы

Хеш-функция преобразует исходный UID карты (который может иметь длину до 8 байт / 64 бит) в хеш-значение фиксированной длины (8 байт). Далее из этого хеш-значения формируется выходной пакет с учетом настроек разрядности и битов четности.

Ключевое свойство хеш-функции:

Изменение любого бита в исходном UID карты приводит к изменению всех байт результирующего хеш-значения.

Это свойство позволяет гарантировать уникальность выходных кодов для разных карт даже в тех случаях, когда стандартными методами (сдвиг, обрезание) невозможно добиться отсутствия коллизий.

Когда целесообразно использовать хеш-функцию

Опция «Хеш-функция» рекомендуется к использованию в следующих случаях:

<i>Ситуация</i>	<i>Пояснение</i>
Длина UID превышает разрядность Wiegand	Например, карта имеет 56-битный UID, а система работает в режиме Wiegand 26 (26 бит). Прямая передача всего UID невозможна.
Различия в UID карт находятся в разных позициях	У разных карт изменяемые части UID могут находиться как в старших, так и в младших байтах. Выбрать единый сдвиг или обрезание, чтобы все карты имели уникальные номера, невозможно.
Требуется гарантированная уникальность выходных кодов	Хеш-функция обеспечивает, что любые два различных UID дадут различные выходные коды (с высокой вероятностью).

Пример использования.

Рассмотрим ситуацию, когда:

- Система работает в режиме Wiegand 26 (26 бит);
- Используются карты с 7-байтным UID (56 бит);
- Невозможно подобрать параметры «битовый сдвиг» и «число значимых бит» так, чтобы все карты имели разные выходные коды.

Исходные данные (три карты):

<i>Карта</i>	<i>UID (HEX)</i>	<i>Изменяемая часть</i>
Карта 1	01 00 00 00 00 03 04	03 04 (младшие байты)
Карта 2	01 00 00 00 00 05 06	05 06 (младшие байты)
Карта 3	01 02 00 00 00 05 06	01 02 (старшие байты)

Проблема без хеш-функции:

При использовании стандартных методов (сдвиг, обрезание) невозможно выбрать единые параметры, которые обеспечат уникальные выходные коды для всех трех карт, так как изменения в UID происходят в разных позициях.

Решение с использованием хеш-функции:

При включении опции «Хеш-функция» считыватель вычисляет хеш по всему 56-битному UID каждой карты. Поскольку изменение любого бита исходного UID приводит к изменению всех байт хеш-значения, все три карты получают различные выходные коды автоматически, без необходимости подбора параметров сдвига и обрезания.

Особенности работы с хеш-функцией

Особенность	Описание
Длина хеш-значения	Хеш-функция формирует выходное значение длиной 8 байт (64 бита).
Взаимодействие с другими преобразованиями	Хеш-функция применяется к исходному UID, при ее включении применение других преобразований (обратный порядок байт, битовый сдвиг, число значимых бит) невозможно.
Совместимость с Wiegand	После вычисления хеш-значения к нему применяются настройки разрядности и битов четности (аналогично обычному UID).
Гарантия уникальности	Хеш-функция обеспечивает высокую вероятность уникальности выходных кодов для различных входных UID.

Сравнение подходов: стандартные преобразования vs хеш-функция

Критерий	Стандартные преобразования (сдвиг, обрезание)	Хеш-функция
Принцип	Выбор части UID (старшие/младшие биты)	Преобразование всего UID в хеш-значение
Зависимость от позиции изменений	Критична: изменения в невывбранной части игнорируются	Не критична: изменение любого бита влияет на результат
Риск коллизий	Высокий при неоптимальном выборе параметров	Низкий (разные UID дают разный хеш)
Сложность настройки	Требует анализа структуры UID и подбора параметров	Минимальная (достаточно включить опцию)
Совместимость с контроллерами	Универсальная	Универсальная



Важные замечания

- Когда не требуется: если длина UID карты не превышает разрядность Wiegand и различия в UID находятся в предсказуемой позиции, можно использовать стандартные преобразования (сдвиг, обрезание) без включения хеш-функции.
- Совместимость с другими считывателями: хеш-функция реализована в оборудовании «ЭРА» и может использоваться для подготовки карт, которые впоследствии будут применяться с другими считывателями. Однако для

корректной работы на стороннем оборудовании карты должны быть предварительно подготовлены с использованием хеш-функции.

- Активация «Хеш-функции» деактивирует возможность применения иных настроек в блоке «Преобразование».

2.3.1.5.5. Рекомендации по настройке преобразования

Сценарий	Рекомендации
Система ожидает стандартный порядок байт	«Обратный порядок байт» — выключен
Система ожидает обратный порядок байт (little-endian)	«Обратный порядок байт» — включен
Система ожидает данные со сдвигом	Установите необходимое значение в поле «Битовый сдвиг вправо»
Система ожидает определенное число значимых бит	Установите «Число значимых бит после сдвига» равным ожидаемой разрядности
Требуется передать UID без изменений	Оставьте значения по умолчанию: «Обратный порядок байт» — выключен, «Битовый сдвиг вправо» — 0, «Число значимых бит после сдвига» — 64 или согласно установленной разрядности Wiegand
Длина UID превышает разрядность Wiegand	Включить хеш-функцию.
UID карт отличаются в разных позициях (старшие/младшие байты)	Включить хеш-функцию
Разрядность Wiegand достаточна для передачи всего UID	Хеш-функцию можно отключить
Подготовка карт для использования на стороннем оборудовании	Включите хеш-функцию при записи карт, чтобы обеспечить совместимость

2.3.1.5.6. Краткое резюме по разделу «Преобразование»

«Параметр «Обратный порядок байт» — самостоятельный параметр, меняющий местами байты в UID. Используйте, если контроллер ожидает данные в другом порядке следования байт.

«Параметр «Битовый сдвиг вправо» — сдвигает биты вправо, отбрасывая младшие биты и добавляя нули слева. Позволяет согласовать разрядность данных.

«Параметр «Число значимых бит после сдвига» — ограничивает длину передаваемых данных, обрезая лишние старшие биты. Используйте для приведения к требуемой разрядности контроллера.

Взаимосвязь параметров «Битовый сдвиг вправо» и «Число значимых бит после сдвига» — при увеличении значения параметра «Битовый сдвиг вправо» фактическая длина значимых бит в данных уменьшается. Это влияет на максимально доступное значение параметра «Число значимых бит после сдвига».

«Опция «Хеш-функция» — опция, которая преобразует весь UID карты в хеш-значение. Используйте ее, когда длина UID превышает разрядность Wiegand или когда различия в UID карт находятся в разных позициях (нельзя подобрать единый сдвиг). Хеш-функция гарантирует, что любые две разные карты будут иметь разные выходные коды, даже при ограниченной разрядности Wiegand.

Если длина UID не превышает разрядность Wiegand и изменения в UID происходят в предсказуемой позиции, хеш-функцию можно не включать, используя стандартные преобразования (сдвиг, обрезание).

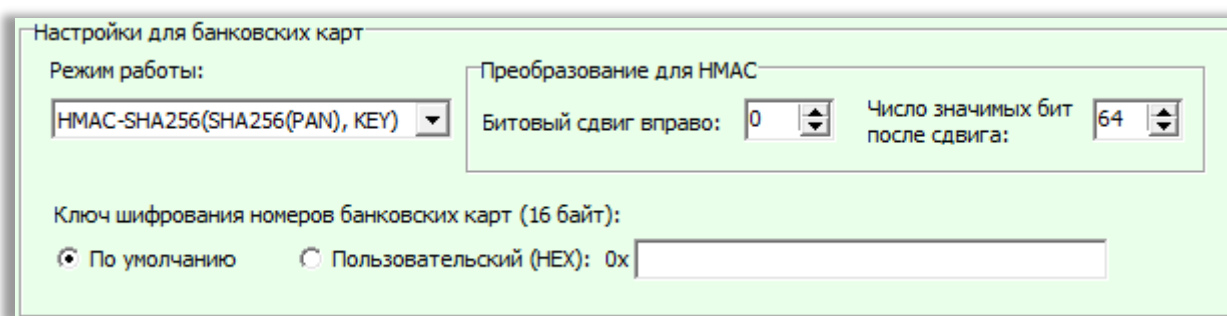
2.3.1.6. Параметры раздела «Настройки для банковских карт»

Назначение блока

Блок **«Настройки для банковских карт»** становится доступным, когда в параметре **«Формат считываемых карт»** выбран вариант **«Банковские карты – 8 байт»**.

Данный раздел позволяет настроить параметры шифрования и преобразования номера банковской карты (PAN — Primary Account Number) перед передачей на контроллер. Использование шифрования обеспечивает дополнительную защиту идентификационных данных банковской карты, исключая возможность несанкционированного перехвата или клонирования номера карты в процессе передачи по интерфейсу Wiegand.

Рисунок 11. Параметры раздела "Настройка для банковских карт"



Контроллеру, принимающему данные от считывателя, не требуется специальной настройки. Для него полученный номер является обычным UID ключа (карты). Вся логика шифрования и преобразования выполняется исключительно в считывателе.

Доступные параметры

Параметр	Описание
<u>Параметр «Режим работы</u>	Определяет алгоритм шифрования для передачи преобразования номера банковской карты
<u>Раздел «Преобразование для НМАС</u>	Настройки битового сдвига и обрезания для зашифрованного номера карты.
<u>Раздел «Ключ шифрования номеров банковских карт (16 байт)</u>	Выбор используемого ключа шифрования: стандартный (по умолчанию) или пользовательский

Подробное описание параметров

2.3.1.6.1. Параметр «Режим работы»

Представляет собой поле с раскрывающимся списком для выбора значения. Параметр определяет алгоритм шифрования, который применяется к номеру банковской карты (PAN) для формирования выходного идентификатора, передаваемого на контроллер.

Доступные варианты:

Режим	Описание	Длина выходных данных
AES	Шифрование номера банковской карты с использованием алгоритма AES (Advanced Encryption Standard) с 16-байтным ключом	128 бит
НМАС-SHA256(PAN, KEY)	Вычисление НМАС (Hash-based Message Authentication Code) на основе номера банковской карты (PAN) и ключа шифрования с использованием алгоритма SHA-256	256 бит
НМАС-SHA256(SHA256(PAN), KEY)	Вычисление НМАС на основе хеша SHA-256 от номера банковской карты (PAN) и ключа шифрования. Обеспечивает дополнительный уровень защиты за счет предварительного хеширования PAN	256 бит

2.3.1.6.2. Раздел «Преобразование для НМАС»

Данный раздел параметров доступен для любого из режимов шифрования банковских карт. Он позволяет выбрать необходимый участок из всего зашифрованного номера карты для передачи на контроллер.

При шифровании PAN карты образуется номер длиной:

- 128 бит для режима AES;

- 256 бит для режимов HMAC.

Считыватель может передать на контроллер максимум 64 бита (ограничение протокола Wiegand). С настройками от производителя передаются 64 младших бита зашифрованного номера.

Параметры преобразования позволяют выбрать, какой именно участок и какой длины из всего зашифрованного номера будет передан.

Доступные параметры:

Параметр	Описание	Диапазон значений
Битовый сдвиг вправо	Определяет начальную позицию выборки в зашифрованном номере (считая от младших битов)	0–255 (для HMAC)
Число значимых бит после сдвига	Определяет длину итогового номера, передаваемого на контроллер	от 1 до 64

Принцип работы:



Параметр «Битовый сдвиг вправо» работает только с шифрованием HMAC.

Считыватель формирует 64-битное окно, начиная с бита, указанного в параметре «Битовый сдвиг вправо». Затем параметр «Число значимых бит после сдвига» определяет, сколько бит из этого окна будет фактически передано.

Базовое правило: Сумма значений параметров «Битовый сдвиг вправо» и «Число значимых бит после сдвига» не может превышать длину зашифрованного номера (256 бит для HMAC).

Битовый сдвиг вправо + Число значимых бит после сдвига ≤ Длина хеша

Параметры взаимозависимы: при изменении одного параметра максимально доступное значение другого автоматически корректируется.

Правило определения отбрасываемых битов:

Поскольку считыватель всегда работает с 64-битным окном (номер банковской карты 8 байт), при установке «Числа значимых бит» меньше 64 необходимо отбросить 64 - N бит. Направление отбрасывания зависит от того, выходит ли окно за пределы зашифрованного номера.

Условие	Что отбрасывается	Пояснение
Сдвиг + Число бит < Длина хеша	Отбрасываются старшие биты 64-битного окна	Окно полностью находится в пределах хеша. Отбрасываются старшие биты, остаются младшие
Сдвиг + Число бит = Длина хеша	Отбрасываются младшие биты 64-битного окна	Окно выходит за пределы хеша на 64 - N бит. Эти «вышедшие» биты

хеша (младшие в окне) отбрасываются

Визуальный пример преобразования (режим HMAC, 256 бит):

Исходный card_hashpan (256 бит, для наглядности разделен на 4 группы):

```
101100001011000101110000010110001110010110111101000100100101011110
0001100111010000101111100111011110110111011110101101101110011001
100110010000011110010110011010101101111010000100011011100000
01010001011100101000010100101110001010101000100101011110110111000001
```

Считыватель передаст в систему только младшие 64 бита:

Ситуация 1: Сдвиг на 4 бита (выборка младших битов со смещением)

При смещении вправо на 4 бита отбрасываются 4 самых младших бита, и берутся следующие 64 бита:

Параметр	Значение
Битовый сдвиг вправо	4
Число значимых бит после сдвига	64

Результат (card_hashpan_short 64 бита):

```
0101000101110010100001010010111000101010100010010101111011011100
```

Смещено на 4-е бита

Обрезано 4-е младших бита (0001)

Ситуация 2: Сдвиг на 200 бит и число значимых бит 56 (выборка старших битов)

При смещении вправо на 200 бита мы «перемещаемся» к старшим битам исходного числа и выбираем 56 бит из старшей области:

Параметр	Значение
Битовый сдвиг вправо	200
Число значимых бит после сдвига	56

Результат (card_hashpan_short 56 бита из старшей части):

```
10110000101100010111000001011000111001011011110100010010
```

Обрезано 8 младших бит (01011110)

Ситуация 3: Сдвиг 68 бит и число значимых бит 48

Результат (card_hashpan_short 48 бита из младшей части):

```
011110010110011010101101111010000100011011100000
```

Обрезано 16 старших бит (100110010000)

Таблицы взаимозависимости параметров

Для HMAC (длина хеша = 256 бит)

Сценарий	Битовый сдвиг вправо	Число значимых бит	Сумма	Отбрасываются
Младшие 64 бита	0	64	64	Никакие
Младшие 56 бит	0	56	56	Старшие 8 бит
Младшие 48 бит	0	48	48	Старшие 16 бит
Произвольный участок (64 бита)	100	64	164	Никакие
Произвольный участок (48 бит)	100	48	148	Старшие 16 бит
Старшие 64 бита	192	64	256	Никакие
Старшие 56 бит	200	56	256	Младшие 8 бит
Старшие 48 бит	208	48	256	Младшие 16 бит
Старшие 32 бита	224	32	256	Младшие 32 бита
Только старший бит (бит 255)	255	1	256	Младшие 63 бита

Примеры настройки

Пример 1: Получение младших 64 бит (стандартный режим)

Параметр	Значение
Битовый сдвиг вправо	0
Число значимых бит после сдвига	64

Результат: передаются младшие 64 бита (биты 0–63) 256-битного хеша.

Пример 2: Получение младших 48 бит

Параметр	Значение
Битовый сдвиг вправо	0
Число значимых бит после сдвига	48

Результат: передаются младшие 48 бит (биты 0–47). Старшие 16 бит младшего 64-битного окна отбрасываются.

Пример 3: Получение старших 64 бит

Параметр	Значение
----------	----------

Битовый сдвиг вправо	192
Число значимых бит после сдвига	64

Результат: передаются старшие 64 бита (биты 192–255) 256-битного хеша.

Пример 4: Получение старших 56 бит (без потери первого байта)

<i>Параметр</i>	<i>Значение</i>
Битовый сдвиг вправо	200
Число значимых бит после сдвига	56

Результат: передаются старшие 56 бит (биты 200–255) 256-битного хеша.

Что происходит:

- Считыватель формирует 64-битное окно, начиная с бита 200.
- Биты 200–255 (56 бит) попадают в окно.
- Биты 256–263 (8 бит) выходят за пределы хеша.
- Поскольку сумма сдвига и числа бит равна 256, отбрасываются младшие 8 бит окна (выход за пределы).
- В результате передаются биты 200–255 — старшие 56 бит исходного хеша.

Пример 5: Получение старших 32 бит

<i>Параметр</i>	<i>Значение</i>
Битовый сдвиг вправо	224
Число значимых бит после сдвига	32

Результат: передаются старшие 32 бита (биты 224–255) 256-битного хеша.

Пример 6: Получение только самого старшего бита

<i>Параметр</i>	<i>Значение</i>
Битовый сдвиг вправо	255
Число значимых бит после сдвига	1

Результат: передается только бит 255 (самый старший бит хеша).

Общая формула для получения старших битов

Если требуется получить N старших битов исходного 256-битного хеша (где N от 1 до 64), необходимо установить:

<i>Параметр</i>	<i>Формула</i>	<i>Пример (N = 56)</i>
Битовый сдвиг вправо	$256 - N$	$256 - 56 = 200$

Число значимых бит после сдвига	N	56
---------------------------------	---	----

Проверка: $(256 - N) + N = 256$ (сумма равна 256, отбрасываются младшие биты окна).

Рекомендации:

Задача	Рекомендация
Передать младшие биты зашифрованного номера	Установите «Битовый сдвиг вправо» = 0
Передать старшие биты зашифрованного номера	Установите «Битовый сдвиг вправо» = 192 (для НМАС)
Требуется выбрать произвольный участок	Рассчитайте сдвиг, исходя из позиции нужного участка (для НМАС)



Важные замечания

- Взаимозависимость параметров: Изменение одного параметра автоматически корректирует максимально допустимое значение другого, чтобы сумма не превышала 256.
- Направление отбрасывания:
 - Если сдвиг + число бит < 256 — отбрасываются старшие биты 64-битного окна.
 - Если сдвиг + число бит = 256 — отбрасываются младшие биты 64-битного окна (выход за пределы хеша).
- По умолчанию: «Битовый сдвиг вправо» = 0, «Число значимых бит после сдвига» = 64 (передаются младшие 64 бита).
- Независимость порядка установки: Параметры можно изменять в любом порядке. Программа автоматически отслеживает их взаимозависимость и корректирует значения при превышении лимита 256.

2.3.1.6.3. Раздел «Ключ шифрования номеров банковских карт (16 байт)»

Представляет собой две радио-кнопки и поле для ввода данных с клавиатуры. Параметр определяет, какой ключ шифрования будет использоваться для защиты номера банковской карты.

Доступные варианты:

Вариант	Описание
По умолчанию	Используется стандартный ключ, заданный в программе. Подходит для большинства систем, не требующих индивидуальной настройки шифрования.
Пользовательский (HEX)	Позволяет ввести собственный ключ шифрования в шестнадцатеричном формате. Длина ключа должна

составлять 16 байт (32 символа в HEX).

При выборе «Пользовательский (HEX)»:

- Становится доступно поле для ввода ключа.
- Ключ должен быть указан в шестнадцатеричном формате (HEX).
- Длина ключа — 16 байт, что соответствует 32 шестнадцатеричным символам.
- Пример корректного ключа: A1B2C3D4E5F60718293A4B5C6D7E8F90

Рекомендации:

Сценарий	Рекомендация
Стандартная инсталляция, отсутствие специальных требований к безопасности	По умолчанию
Требуется индивидуальный ключ для конкретной системы	Пользовательский (HEX)
Использование нескольких считывателей в одной системе	На всех считывателях должен быть установлен одинаковый ключ шифрования

2.3.1.6.4. Пример схемы обработки данных банковской карты

Банковская карта (PAN).

↓

Считывание PAN (обычно 8 байт / 64 бита).

↓

Применение выбранного режима шифрования:

- AES → 128 бит;
- HMAC-SHA256(PAN, KEY) → 256 бит;
- HMAC-SHA256(SHA256(PAN), KEY) → 256 бит.

↓

Преобразование для HMAC (только для HMAC-режимов):

- Формирование 64-битного окна, начиная с бита = «Битовый сдвиг вправо»;
- Отбрасывание битов согласно правилу:
 - * Если сдвиг + число_бит < 256: отбрасываются СТАРШИЕ биты окна;
 - * Если сдвиг + число_бит = 256: отбрасываются МЛАДШИЕ биты окна.

Для режимов AES и HMAC:

- Формирование результата длиной = «Число значимых бит после сдвига».

↓

Основные преобразования (раздел «Преобразование», опционально):

- Обратный порядок байт;

- Битовый сдвиг вправо (стандартный, с добавлением нулей слева);
- Число значимых бит после сдвига (обрезание старших битов).



Формирование Wiegand-пакета (с битами четности или без).



Передача на контроллер (как обычный UID).



Важные замечания

- Активация раздела: настройки для банковских карт становятся доступны только после выбора формата «**Банковские карты – 8 байт**» в параметре «**Формат считываемых карт**».
- Длина зашифрованного номера: при шифровании PAN образуется число длиной 128 бит (AES) или 256 бит (HMAC). Считыватель может передать максимум 64 бита, поэтому всегда передается выбранный участок длиной не более 64 бит.
- Преобразование для AES: В блоке «**Преобразование для HMAC**» параметр «**Битовый сдвиг вправо**» работает только для HMAC. Параметр «**Число значимых бит после сдвига**» работает для обоих режимов шифрования. Для AES максимальная длина зашифрованного номера составляет 128 бит, что необходимо учитывать при расчете сдвига.
- Единообразие ключей: В системе, использующей несколько считывателей, на всех устройствах должен быть установлен одинаковый ключ шифрования. В противном случае карты, инициализированные с одним ключом, не будут корректно обрабатываться считывателями с другим ключом.
- Стойкость шифрования: Использование AES и HMAC-SHA256 обеспечивает высокий уровень защиты номера банковской карты при передаче по интерфейсу Wiegand.

2.3.1.6.5. Краткое резюме по разделу «Настройки для банковских карт»

- «**Режим работы**» — выбирает алгоритм шифрования номера банковской карты: AES (128 бит) или HMAC (256 бит).
- «**Преобразование для HMAC**» — позволяет выбрать участок из зашифрованного номера для передачи на контроллер.
 - «**Битовый сдвиг вправо**» определяет начальную позицию (от младших битов к старшим).
 - «**Число значимых бит после сдвига**» определяет длину результата (1–64 бита).
 - Если сумма параметров меньше длины хеша — отбрасываются старшие биты окна.
 - Если сумма равна длине хеша — отбрасываются младшие биты окна (выход за пределы).

- Для AES можно установить только число значимых бит.
- «**Ключ шифрования**» — определяет, какой ключ используется для шифрования.
- Раздел активируется только при выборе формата «**Банковские карты**».
- Контроллеру не требуется специальной настройки — он воспринимает результат как обычный UID карты.

2.3.1.7. Параметры раздела «Чтение кода из блока»

Данный раздел появляется в блоке «Общая конфигурация» только при выборе режима «**Чтение кода из блока**». Он позволяет указать, из какого именно места памяти карты считыватель должен извлекать идентификационные данные.

При активации параметра «Тип замка» предоставляется доступ к дополнительному разделу с параметрами «**Зоны прохода**» (см. [раздел 2.3.1.8](#)).

Рисунок 12. Параметры раздела "Чтение кода из блока"

Параметр	Описание	Диапазон значений
Номер блока	Абсолютный номер блока в памяти карты, с которого начинается чтение	0–127
Смещение байт в блоке	Указывает, с какого байта в блоке начать чтение	0–15
Количество байт для передачи	Объем данных (длина UID), который считыватель передаст на контроллер	1–8
Код доступа к требуемому блоку (16 байт)	Ключ доступа к защищенному блоку памяти	16 байт (HEX)

2.3.1.7.1. Параметр «Номер блока»

Назначение:


Представляет собой поле с цифровым выбором. Определяет абсолютный номер блока в памяти карты, из которого считыватель будет извлекать данные.

Доступные значения: от 0 до 127.

Пояснение:

Абсолютный номер блока — это порядковый номер блока во всей памяти карты. Например:

- Сектор 0: блоки с 0 по 3
- Сектор 1: блоки с 4 по 7
- Сектор 2: блоки с 8 по 11
- Сектор N: блоки с $N \times 4$ по $N \times 4 + 3$

 Программа автоматически рассчитывает номер сектора и относительного блока на основе указанного абсолютного номера. Пользователю не нужно самостоятельно вычислять сектор.

2.3.1.7.2. Параметр «Смещение байт в блоке»

Назначение:

Представляет собой поле с цифровым выбором. Указывает, с какого байта внутри выбранного блока считыватель начнет чтение данных. Каждый блок памяти карты содержит 16 байт (от 0 до 15).

Доступные значения: от 0 до 15.

Взаимосвязь с «Количеством байт для передачи»:

Доступное смещение	Количество байт для передачи
0–8	8
0–9	7
0–10	6
0–11	5
0–12	4
0–13	3
0–14	2
0–15	1

Принцип работы:

- Если смещение = 0, передаются байты с 0 по (N-1) из блока.
- Если смещение = 8, передаются байты с 8 по (8+N-1) из блока.
- Сумма смещения и количества байт не должна превышать 16.

2.3.1.7.3. Параметр «Количество байт для передачи»

Назначение:

Представляет собой поле с цифровым выбором. Определяет объем данных (длину UID), который считыватель передаст на контроллер.

Доступные значения: от 1 до 8 байт.

Рекомендации:

Задача	Рекомендуемое значение
Стандартная передача UID (4 байта)	4
Передача полного 8-байтового идентификатора	8
Минимальная длина (для тестирования)	1

2.3.1.7.4. Параметр «Код доступа к требуемому блоку (16 байт)»**Назначение:**

Представляет собой поле для ввода данных с клавиатуры. Задает ключ доступа к защищенному блоку памяти карты. Без правильного кода доступа считыватель не сможет прочитать данные из указанного блока.

Формат ввода:

HEX (шестнадцатеричный), 16 байт (32 символа).

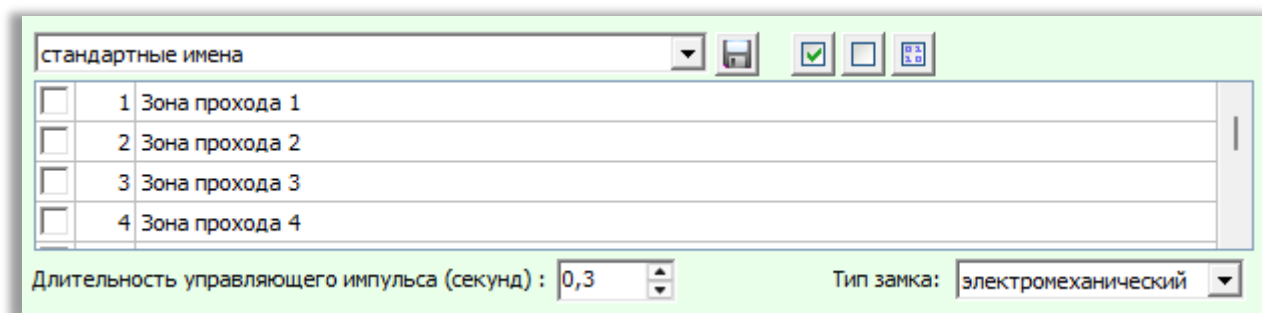
**Важные замечания:**

- Код доступа вводится в открытом виде. Берегите его от несанкционированного доступа.
- При чтении конфигурации с мастер-карты или считывателя отображается контрольная сумма кода доступа, а не сам код.
- Защита действует на уровне сектора, а не блока. Все блоки внутри одного сектора защищены одним и тем же ключом.


2.3.1.8. Параметры раздела «Зоны прохода»

Раздел «**Зоны прохода**» появляется в блоке «**Общая конфигурация**» только при выборе защищенного режима «**Зоны прохода**». Он позволяет настроить считыватель для самостоятельного управления запирающим устройством (замком) без участия внешнего контроллера СКУД.

Рисунок 13. Параметры раздела «Зоны прохода»



Считыватель, работающий в этом режиме, принимает решение о доступе на основе информации о разрешенных зонах, записанной в память карты пользователя. Если хотя бы одна зона, указанная в настройках считывателя, совпадает с зонами, записанными на карте, считыватель разблокирует замок на заданное время.

 Функционал программного изменения типа замка предусмотрен исключительно для считывателей модели «ЭРА-MF v2», оснащённых микросхемой версии 0.95. Для считывателей модели «ЭРА-MF» предыдущих версий необходимо использование специализированной платы для управления запирающим устройством.

Доступные параметры

Параметр	Описание
Выбор шаблона имен зон	Поле с всплывающим списком, где отображаются сохраненные шаблоны с пользовательскими именами зон прохода. По умолчанию выбрано значение «Стандартные имена».
Таблица зон прохода	Список зон (от 1 до 64) с чекбоксами напротив каждой. Для активации зоны установите соответствующий флажок.
«Сохранить имена зон прохода»	Сохраняет текущие пользовательские имена зон в файл-шаблон для последующего использования.
«Выбрать все зоны прохода»	Активирует все чекбоксы в таблице зон одновременно.
«Снять выбор со всех зон прохода»	Деактивирует все чекбоксы в таблице зон одновременно.
«Битовая строка»	Открывает окно для ввода маски разрешенных зон в виде 64-битной последовательности (0 и 1). Удобно для быстрой настройки при известной битовой маске.
«Длительность управляющего импульса (секунд)»	Устанавливает время, на которое считыватель подает напряжение на замок (для электромеханического замка) или снимает напряжение (для электромагнитного замка).
«Тип замка»	Выпадающий список для выбора типа запирающего устройства: «Электромеханический» или «Электромагнитный».

2.3.1.8.1. Параметр для выбора шаблона имен зон

Поле с раскрывающимся списком, расположенное в верхней части раздела. По умолчанию выбрано значение «Стандартные имена» (зона прохода 1, 2, 3...). Если ранее были созданы и сохранены пользовательские шаблоны с именами зон (например, «Подъезд 1», «Калитка», «Офис»), они отображаются в этом списке для быстрого выбора по названию файла.

2.3.1.8.2. Таблица зон прохода

Представляет собой список зон с 1 по 64. Напротив каждой зоны расположен чекбокс.

Назначение:

Для настройки считывателя необходимо выбрать те зоны, которые он будет обслуживать. Например, считыватель на входе в подъезд №5 должен иметь активной только зону «Подъезд 5». Считыватель на калитке может иметь активной зону «Калитка».

Принцип работы:

При поднесении карты считыватель проверяет маску зон, записанную на карте. Если хотя бы одна зона из настроек считывателя присутствует в маске зон карты, доступ разрешается.

2.3.1.8.3. Кнопка «Сохранить имена зон прохода»

Назначение:

Позволяет сохранить переименованные зоны (например, вместо «Зона прохода 1» указать «Цокольный этаж») и сохранить набор имен в файл-шаблон для последующего использования.

Порядок работы:

- Дважды кликните левой кнопкой мыши по названию зоны в таблице.
- Введите новое имя зоны.
- Повторите для всех зон, которые требуется переименовать.
- Нажмите кнопку «**Сохранить имена зон прохода**».
- В открывшемся диалоговом окне выберите папку с программой «Конфигуратор считывателей «ЭРА» для сохранения.
- Введите имя файла и нажмите «**Сохранить**».

После сохранения созданный шаблон появится в списке выбора шаблонов. При выборе этого шаблона пользовательские имена зон отобразятся в таблице.

2.3.1.8.4. Кнопка «Выбрать все зоны прохода»

Назначение:

Быстро активирует все чекбоксы в таблице зон прохода.

Применение:

Полезна, если считыватель должен обслуживать все зоны (например, для администратора или мастера).

2.3.1.8.5. Кнопка «Снять выбор со всех зон прохода»

Назначение:

Быстро деактивирует все чекбоксы в таблице зон прохода.

Применение:

Полезна для сброса ранее выбранных зон перед новой настройкой.

Программный параметр функционирует исключительно в считывателях модели «ЭРА-MF v2», оснащенных микросхемой версии 0.95 и программным обеспечением не ниже 1.5.1. Для устройств модели «ЭРА-MF» предыдущих версий предусмотрена специализированная плата для управления запорным механизмом.

2.3.1.8.8. Параметр «Тип замка»

Назначение:

Представляет собой поле с раскрывающимся списком. Определяет тип запирающего устройства, подключенного к считывателю.

Доступные значения:

Значение	Описание
Электромеханический	Замок, который открывается при подаче напряжения (защелочные, ригельные замки).
Электромагнитный	Замок, который удерживается под напряжением и открывается при снятии напряжения.

Влияние на работу:

В зависимости от выбранного типа считыватель меняет логику работы с «Длительностью управляющего импульса» (подает или снимает напряжение).



Важные замечания

- Совместимость оборудования: программное управление замком поддерживается только для считывателей «ЭРА-MF v2» с микросхемой версии 0.95. Для более ранних версий требуется специальная плата.
- Максимальное количество зон: не более 64 зон.
- Отсутствие преобразований: параметры раздела «Преобразование» (обратный порядок байт, битовый сдвиг, число значимых бит, хеш-функция) в данном режиме недоступны, так как считыватель не передает UID.
- Совместимость с другими считывателями: карты, подготовленные для режима «Зоны прохода», не будут корректно работать в считывателях, настроенных на обычный режим чтения UID (и наоборот).
- Шаблоны имен: сохраненные шаблоны с пользовательскими именами зон необходимо хранить в папке с программой «Конфигуратор считывателей «ЭРА».

2.3.1.8.9. Краткое резюме по разделу «Зоны прохода»

Режим «Зоны прохода» позволяет считывателю самостоятельно управлять замком, проверяя права доступа по маске зон, записанной на карте пользователя.

Основные параметры настройки:

- **Таблица зон** — выберите зоны, которые будет обслуживать считыватель.
- **«Длительность управляющего импульса»** — время открытия замка (в секундах).
- **«Тип замка»** — электромеханический или электромагнитный.

Вспомогательные функции:

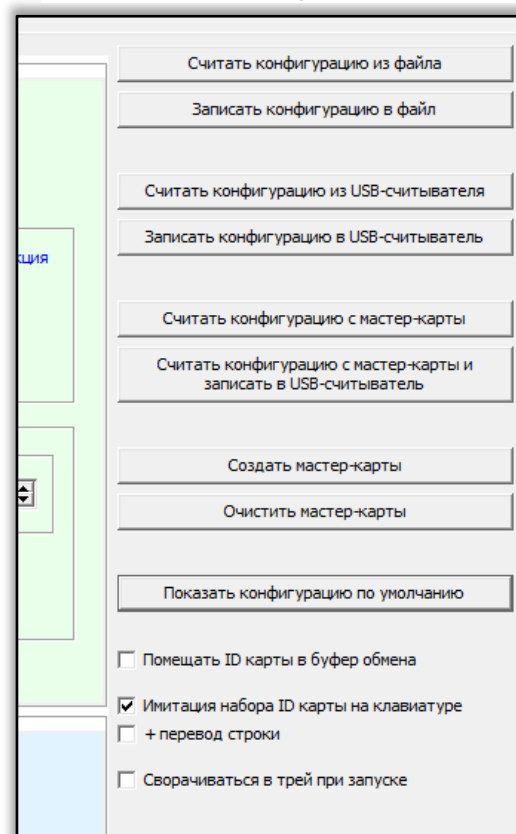
- **«Сохранить имена зон прохода»** — создание шаблонов с пользовательскими именами зон.
- **«Битовая строка»** — быстрый ввод маски зон в виде 64-битной последовательности.

 Программное управление замком доступно только для считывателей «ЭРА-MF v2».

2.3.2. Боковая панель действий

Представляет собой список кнопок и чекбоксов. Данная панель расположена справа от основных настроек и содержит кнопки для работы с конфигурацией считывателя, а также чекбоксы для активации вывода ID карты в сторонний программный интерфейс.

Рисунок 14. Боковая панель действий на вкладке «Конфигурация»



Кнопки:

- Считать конфигурацию из файла;
- Записать конфигурацию в файл;
- Считать конфигурацию из USB-считывателя;
- Записать конфигурацию в USB-считыватель;
- Считать конфигурацию с мастер-карты;
- Считать конфигурацию с мастер-карты и записать в USB-считыватель;
- Создать мастер-карты;
- Очистить мастер-карты;
- Показать конфигурацию по умолчанию.

Чекбоксы:

- Помещать ID карты в буфер обмена;
- Имитация набора ID карты на клавиатуре;
- + перевод строки;
- Сворачиваться в трей при запуске.

2.3.2.1. Кнопка «Считать конфигурацию из файла»

Назначение:


Загружает ранее сохранённую конфигурацию считывателя из файла в интерфейс программы, заменяя текущие настройки.

Порядок действий:

- Нажмите кнопку «Считать конфигурацию из файла».
- В открывшемся диалоговом окне выберите файл конфигурации (формат .rcf).
- Нажмите «Открыть».

Результат:

Настройки в интерфейсе программы обновляются в соответствии с загруженным файлом. Появляется окно с уведомлением «Конфигурация считана из файла». Нажмите «ОК» для продолжения работы.

 Если файл повреждён, программа отобразит сообщение об ошибке. Конфигурация останется без изменений. Программа работает только с файлами формата .rcf.

2.3.2.2. Кнопка «Записать конфигурацию в файл»

Назначение:

Сохраняет текущие настройки конфигурации, отображаемые в интерфейсе программы, в файл на компьютере для последующего использования или переноса на другой считыватель.

Порядок действий:

- Нажмите кнопку «Записать конфигурацию в файл».
- В открывшемся диалоговом окне выберите папку для сохранения.
- Укажите имя файла (расширение .rcf добавляется автоматически).
- Нажмите «Сохранить».

Результат:

Файл с конфигурацией создаётся в указанном месте. Появляется окно с уведомлением «Выполнено». Нажмите «ОК» для продолжения работы.

 При сохранении файла с существующим именем программа перезапишет файл с существующими настройками.

2.3.2.3. Кнопка «Считать конфигурацию из USB-считывателя»

Назначение:

Загружает ранее сохранённую конфигурацию из подключённого USB-считывателя в интерфейс программы, заменяя текущие настройки.

Порядок действий:

- Подключите USB-считыватель к компьютеру.
- Убедитесь, что считыватель определяется системой.
- Нажмите кнопку «Считать конфигурацию из USB-считывателя».

Результат:

Настройки в интерфейсе программы обновляются в соответствии с конфигурацией, считанной из считывателя. Появляется окно с уведомлением об успешном завершении операции. Нажмите «ОК» для продолжения работы.

Примечание:

Если считыватель не подключен или не отвечает, программа будет неактивной. Убедитесь, что соединение установлено, и повторите попытку.

2.3.2.4. Кнопка «Записать конфигурацию в USB-считыватель»

Назначение:

Сохраняет текущие настройки конфигурации, отображаемые в интерфейсе программы, в подключённый USB-считыватель.

Порядок действий:

- Подключите USB-считыватель к компьютеру.
- Убедитесь, что считыватель определяется системой.
- Нажмите кнопку «Записать конфигурацию в USB-считыватель».

Результат:

Конфигурация из интерфейса программы записывается в память считывателя. Появляется окно с уведомлением «Выполнено». Нажмите «ОК» для продолжения работы.

Во время записи конфигурации не отключайте считыватель от компьютера и не закрывайте программу. Прерывание процесса записи может привести к некорректной работе считывателя.

Примечание:

При записи предыдущая конфигурация в считывателе будет заменена новой.

2.3.2.5. Кнопка «Считать конфигурацию с мастер-карты»

Назначение:

Загружает конфигурацию, сохранённую в памяти ранее созданной мастер-карты, в интерфейс программы, заменяя текущие настройки.

Порядок действий:

- Нажмите кнопку «Считать конфигурацию с мастер-карты».
- На экране появится модальное окно с временным лимитом (индикатором

обратного отсчёта).

- В течение указанного времени поднесите мастер-карту к считывающему устройству.
- Дождитесь завершения процесса считывания.

Результат:

Модальное окно с индикатором будет заменено на диалоговое окно, подтверждающее успешное считывание конфигурации. Нажмите «ОК». Параметры, сохранённые в мастер-карте, отобразятся в интерфейсе программы.

Примечание:

- Если мастер-карта не будет поднесена в течение отведённого времени, операция прервётся. В этом случае повторите попытку.
- В случае использования идентификатора, не являющейся мастер-картой, в поле вывода UID появится сообщение об ошибке.
- Считывающее устройство должно быть подключено и исправно.

2.3.2.6. Кнопка «Считать конфигурацию с мастер-карты и записать в USB-считыватель»

Назначение:

Копирует конфигурацию, хранящуюся в памяти мастер-карты, непосредственно в память USB-считывателя (без предварительного отображения в интерфейсе программы).

Порядок действий:

- Подключите USB-считыватель к компьютеру.
- Нажмите кнопку «Считать конфигурацию с мастер-карты и записать в USB-считыватель».
- На экране появится модальное окно с временным лимитом (индикатором обратного отсчёта).
- В течение указанного времени поднесите мастер-карту к считывающему устройству.
- Дождитесь завершения процесса.

Результат:

Модальное окно с индикатором будет заменено на диалоговое окно с надписью «Выполнено», подтверждающее успешное считывание конфигурации с мастер-карты и её запись в USB-считыватель. Нажмите «ОК». Параметры, сохранённые в мастер-карте, скопируются в память считывателя.

Примечание:

- При выполнении записи предыдущая конфигурация, сохранённая в USB-

считывателе, будет замещена. Исключение составляют случаи, когда при предыдущей конфигурации считывателя была активирована опция защиты от реконфигурации в защищенном режиме (Рисунок 15 – 2).

- Данная операция не изменяет настройки в интерфейсе программы. Чтобы отобразить скопированную конфигурацию из памяти считывателя в программном интерфейсе, дополнительно нажмите кнопку «**Считать конфигурацию из USB-считывателя**».
- Если мастер-карта не будет поднесена в течение отведённого времени, операция прервётся. Повторите попытку.

2.3.2.7. Кнопка «Создать мастер-карты»

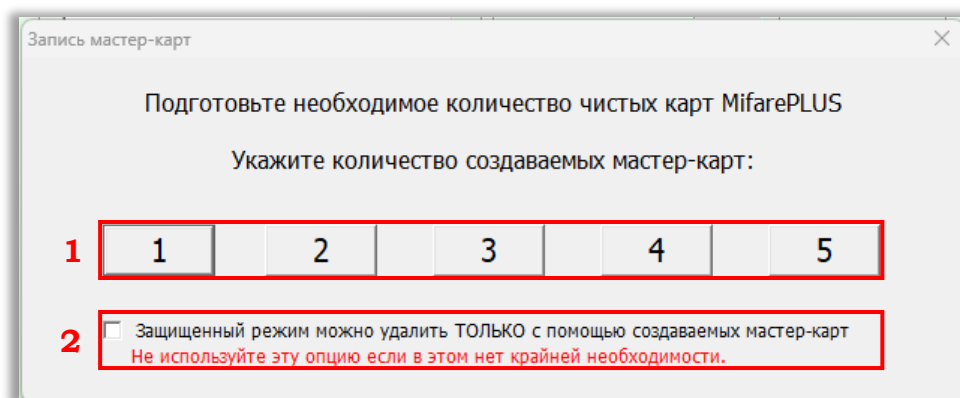
Назначение:


Записывает текущую конфигурацию, указанную в интерфейсе программы (включая параметры из разделов «Общая конфигурация» и «Световая схема») и необходимую информацию (в том числе код объекта или доступа) на одну или несколько мастер-карт. В дальнейшем эти мастер-карты можно использовать для быстрого копирования конфигурации на другие считыватели или для восстановления доступа в защищённом режиме.

Порядок действий:

- В программе выберите необходимый режим работы для считывающего устройства.
- При необходимости укажите тип используемых карт.
- Настройте требуемые параметры в разделах «**Общая конфигурация**» и «**Световая схема**» (доступность параметров зависит от выбранного режима работы).
- Нажмите кнопку «**Создать мастер-карты**».
- Выберите количество мастер-карт, подлежащих созданию (Рисунок 15 – 1).

Рисунок 15. Окно записи мастер-карт



 При активации функции защиты от реконфигурации (**Ошибка! Источник ссылки не найден.** – 2), доступной исключительно в защищенных режимах,

сохранение конфигурации в памяти мастер-карты и настройка считывателя с её использованием делают дальнейшее изменение режима без применения мастер-карт с идентичным кодом объекта невозможным. В случае утраты такой мастер-карты, процесс реконфигурации считывателя становится неосуществимым.

- Последовательно приложите карты к считывающему устройству.

Результат:

После успешного выполнения операции отобразится окно с уведомлением «Мастер-карта(ы) успешно создана(ы)». Нажмите кнопку «ОК». Созданные мастер-карты готовы к использованию.

Примечание:

- Для записи мастер-карт необходимо использовать чистые карты, находящиеся на заводском уровне безопасности – SL0 (Security Level 0), и поддерживаемого формата, например Mifare PLUS.
- Особенности применения мастер-карт в различных режимах работы подробно описаны в соответствующих разделах настоящего руководства.

2.3.2.8. Кнопка «Очистить мастер-карты»

Удаляет конфигурацию из памяти одной или нескольких мастер-карт, что приводит к прекращению их функционирования в качестве мастер-карт.


Порядок действий:

- Нажмите кнопку «Очистить мастер-карты».
- Откроется диалоговое окно с предупреждением.
 - Нажмите «Да» для продолжения операции.
 - Нажмите «Нет» для отмены действия.
- После подтверждения откроется окно «Очистка мастер-карт».
- Последовательно подносите каждую мастер-карту к USB-считывающему устройству.
- В процессе выполнения операции в окне будет отображаться количество успешно очищенных карт.
- Для завершения процесса нажмите кнопку «Закончить очистку мастер-карт».

Результат:

Выбранные мастер-карты очищены от конфигурации и более не могут использоваться для копирования настроек на считыватели.

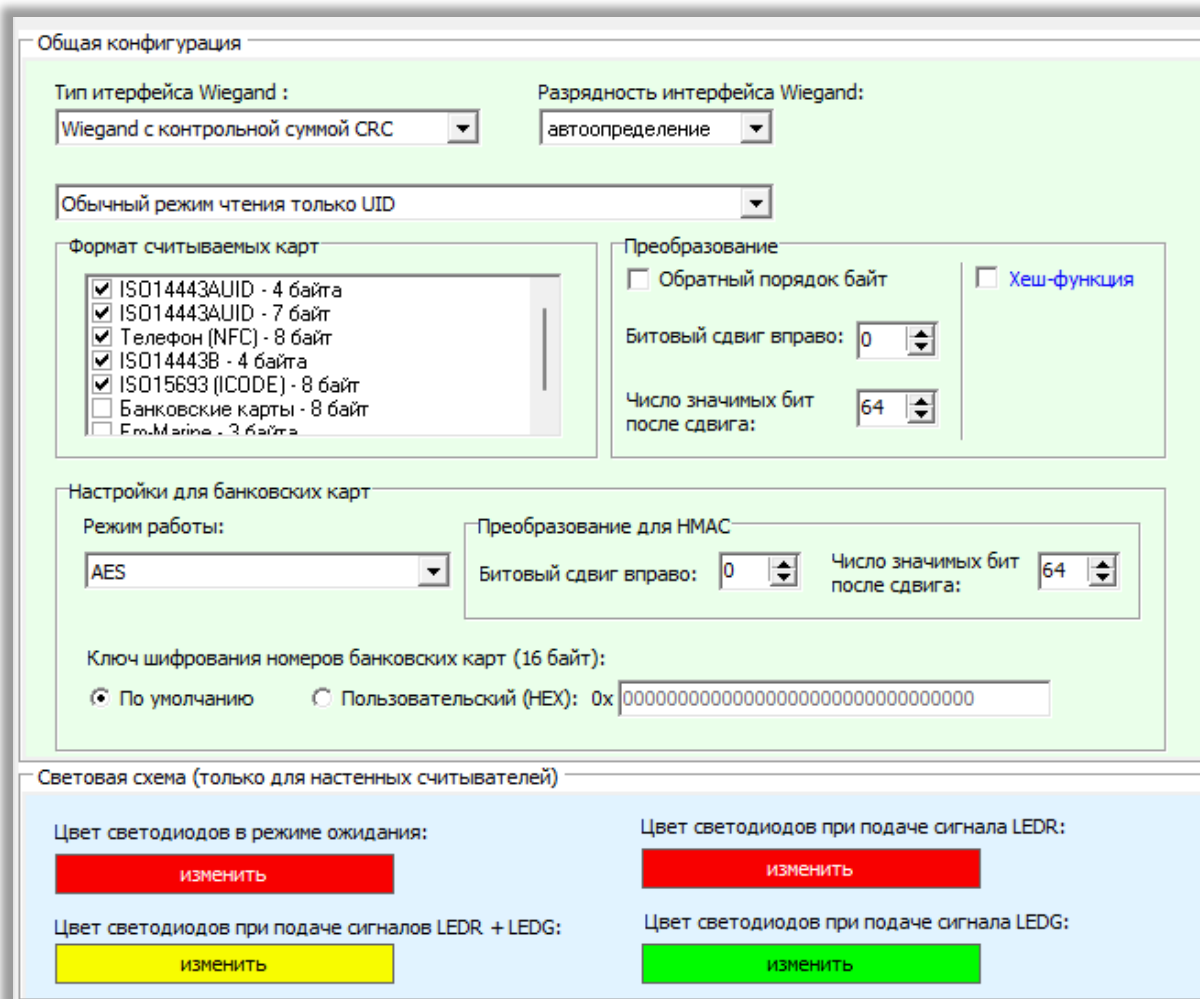
Примечание:

 *Будьте внимательны: если при конфигурации считывателей в защищенном режиме была активирована опция защиты от реконфигурации, удаление всех мастер-карт приведёт к невозможности перенастройки считывателя.*

2.3.2.9. Кнопка «Показать конфигурацию по умолчанию»**Назначение:**

Восстанавливает заводские настройки считывателя в интерфейсе программы, заменяя все текущие параметры на значения, установленные производителем.

Рисунок 16. Интерфейс программы на вкладке "Конфигурация" с настройками от производителя



Общая конфигурация

Тип интерфейса Wiegand :
Wiegand с контрольной суммой CRC

Разрядность интерфейса Wiegand:
автоопределение

Обычный режим чтения только UID

Формат считываемых карт

- ISO14443AUID - 4 байта
- ISO14443AUID - 7 байт
- Телефон (NFC) - 8 байт
- ISO14443B - 4 байта
- ISO15693 (ICODE) - 8 байт
- Банковские карты - 8 байт
- Em.Marine - 3 байта

Преобразование

Обратный порядок байт

Хеш-функция

Битовый сдвиг вправо: 0

Число значимых бит после сдвига: 64

Настройки для банковских карт

Режим работы:
AES

Преобразование для HMAC

Битовый сдвиг вправо: 0

Число значимых бит после сдвига: 64

Ключ шифрования номеров банковских карт (16 байт):

По умолчанию Пользовательский (HEX): 0x 00000000000000000000000000000000

Световая схема (только для настенных считывателей)

Цвет светодиодов в режиме ожидания:
ИЗМЕНИТЬ

Цвет светодиодов при подаче сигнала LEDR:
ИЗМЕНИТЬ

Цвет светодиодов при подаче сигналов LEDR + LEDG:
ИЗМЕНИТЬ

Цвет светодиодов при подаче сигнала LEDG:
ИЗМЕНИТЬ

Порядок действий:

- Нажмите кнопку «Показать конфигурацию по умолчанию».
- Откроется модальное окно с сообщением «Показана конфигурация по умолчанию».
- Нажмите «ОК» для завершения процесса.

Результат:

Все настройки в разделах «Общая конфигурация», «Световая схема» и прочие

параметры приводятся к заводским значениям по умолчанию (от производителя).

Примечание:

- Данная операция изменяет только отображаемую в интерфейсе конфигурацию, но не записывает её автоматически в считыватель или на мастер-карты.
- Чтобы применить заводские настройки к оборудованию, после нажатия этой кнопки выполните запись конфигурации в USB-считыватель или на мастер-карты.
- Операция полезна для быстрого сброса настроек перед началом новой настройки или при возникновении ошибок в текущей конфигурации.

2.3.2.10. Чекбокс «Помещать ID карты в буфер обмена»

Назначение:

Копирует считанный идентификатор карты в системный буфер обмена Windows для последующей ручной вставки в любое поле ввода.

Порядок действий:

- Установите флажок «Помещать ID карты в буфер обмена».
- Поднесите карту к считывающему устройству.
- Установите курсор мыши в поле, предназначенное для ввода номера карты.
- Вставьте скопированное значение из буфера обмена (например, одновременным нажатием клавиш **Ctrl+V**).

Результат:

Идентификатор карты вставлен в выбранное поле ввода.

Примечание:

- В буфер обмена копируется только последний считанный ID.
- Опция работает независимо от других способов передачи.

2.3.2.11. Чекбокс «Имитация набора ID карты на клавиатуре»

Назначение:

Автоматически вводит считанный идентификатор карты в активное поле ввода целевого программного обеспечения посредством эмуляции нажатий клавиш клавиатуры.

Порядок действий:

- Установите флажок «Имитация набора ID карты на клавиатуре».
- Программа «ЭНТ – Конфигуратор считывателей «ЭРА» должна оставаться запущена.
- Установите курсор мыши в поле для ввода ID карты в целевом ПО.

- Поднесите карту к считывающему устройству.

Результат:

Идентификатор карты автоматически вводится в выбранное поле (Рисунок 17— 1).

Рисунок 17. Идентификатор ключа, переданный в программу «Клиент»

Добавить ключ | Изменить / удалить ключ | Групповая обработка

Тип ключа: Обычный ключ | UID ключа: 2584210920

Действителен до (включительно): 23 : 59 Бессрочный ключ

Лимит проходов (250 макс.): 1 Безлимитный ключ

Всегда разрешать повторный проход | EXT-code: 0


Ключ заблокирован

Комментарий:

+ Добавить новый ключ

Примечание:

- Метод удобен для быстрого ввода ID в системы контроля доступа и другие приложения.

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

2.3.2.12. Чекбокс «+ перевод строки»

Назначение:

Автоматически перемещает курсор в начало следующей строки после ввода идентификатора карты.

Условия работы:

Опция функционирует только совместно с опцией «Имитация набора ID карты на клавиатуре».

Порядок действий:

- Установите оба флажка: «Имитация набора ID карты на клавиатуре» и «+ перевод строки».
- Установите курсор в поле ввода.
- Поднесите карту к считывающему устройству.

Результат:

После автоматического ввода ID карты курсор мыши перемещается в начало следующей строки (например, для последовательного ввода нескольких карт).

2.3.2.13. Чекбокс «Сворачиваться в трей при запуске»

Назначение:

Автоматически сворачивает окно программы в скрытую область уведомлений Windows (трей) при каждом запуске, чтобы оно не занимало место на рабочем столе (Рисунок 18 – 1).

Порядок действий:

- Установите флажок «Сворачиваться в трей при запуске».
- Закройте или перезапустите программу (при следующем запуске окно будет сразу свёрнуто).

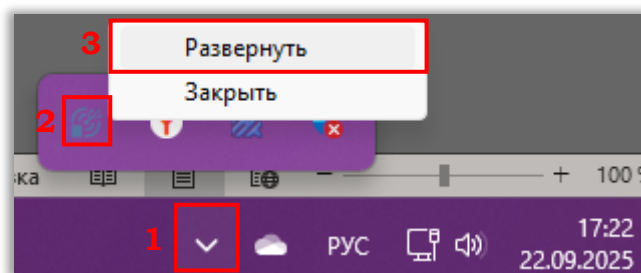
Результат:

Программа работает в свернутом режиме, отображаясь только значком в панели уведомлений (Рисунок 18 – 2).

Как развернуть окно:

- Наведите курсор на значок программы в панели уведомлений Windows.
- Щелкните правой кнопкой мыши.
- Выберите «Развернуть» (Рисунок 18 – 3).

Рисунок 18. Отображение значка программы в области уведомлений панели задач



Примечание:

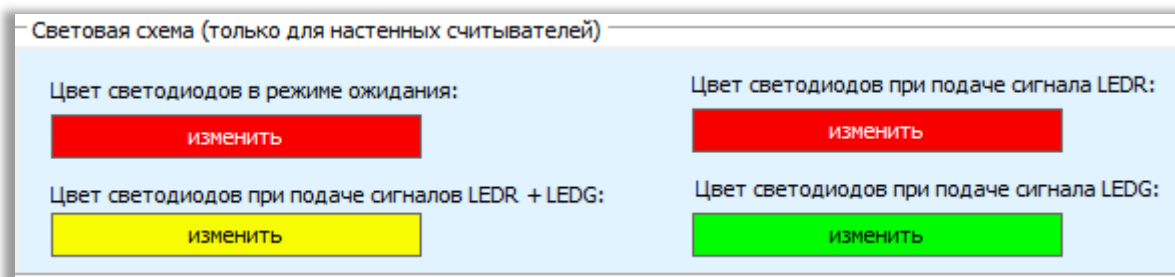
- Программа продолжает работать в фоновом режиме и выполнять свои функции.
- Чтобы окончательно закрыть программу, нажмите «Заккрыть» или разверните окно и закройте его стандартным способом.

2.3.3. Блок «Световая схема»

Этот блок предназначен исключительно для конфигурирования настенных считывателей серии «МФ». Он предоставляет возможность модификации заранее установленных цветовых параметров светодиодных индикаторов считывателя в

различных сценариях подачи сигнала на его контакты LEDR и LEDG, а также в режиме ожидания.

Рисунок 19. Внешний вид блока конфигураций "Световая схема"



Для изменения цвета необходимо нажать на кнопку с предустановленным цветом и подписью «Изменить». После этого выбрать требуемый цвет и подтвердить выбор, нажав кнопку «ОК».

Для записи настроек в память считывателя нажмите кнопку «Записать конфигурацию в USB-считыватель».

2.4. Вкладка «Защищенные карты»

Назначение вкладки

Вкладка «Защищенные карты» предназначена для управления картами пользователей в защищенных режимах работы считывателя. Здесь можно создавать новые защищенные карты, а также очищать (удалять) коды объектов или зоны прохода с существующих карт (Рисунок 20).

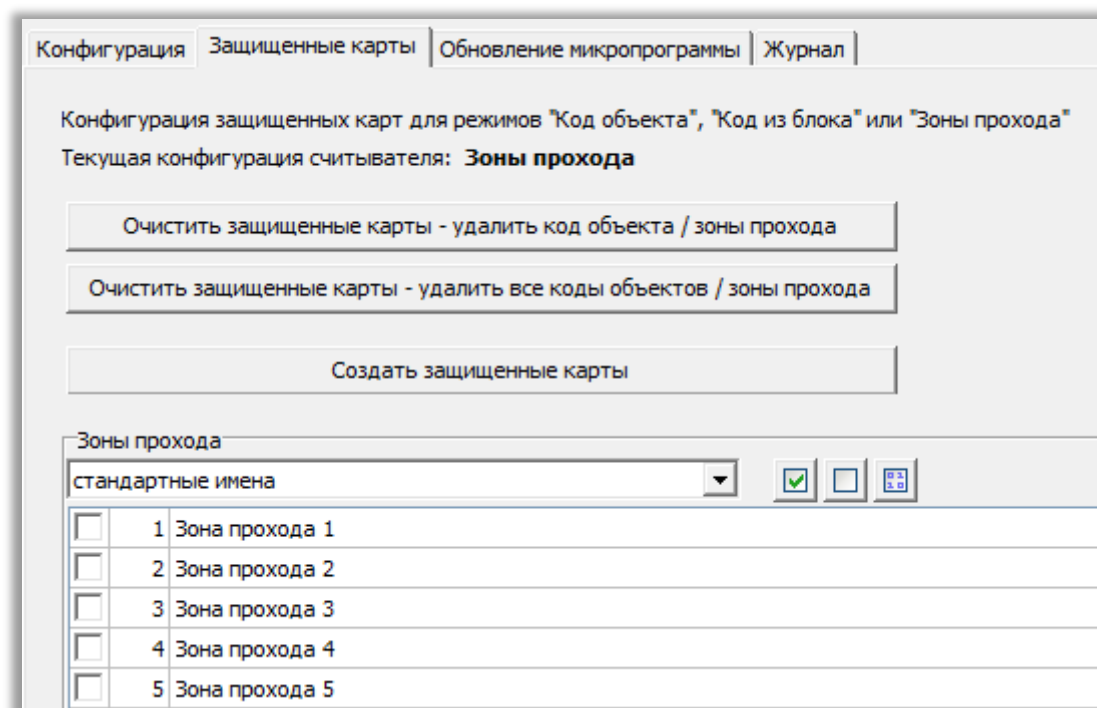
Параметры на данной вкладке активны только тогда, когда подключенный считыватель переведен в один из защищенных режимов:

- «Код объекта» ([раздел 3.2](#))
- «Чтение кода из блока» ([раздел 3.3](#))
- «Зоны прохода» ([раздел 3.4](#))



Состав доступных элементов управления зависит от выбранного защищенного режима.

Рисунок 20. Вкладка "Защищенные карты" в режиме "Зоны прохода"



Элементы управления

Элемент

Назначение

[«Создать защищенные карты»](#)

Осуществляется перевод пользовательских карт в защищенный режим, а также запись специфических данных в заранее определенные области памяти карты, в соответствии с конфигурационными параметрами считывающего устройства.

[«Очистить защищенные карты — удалить код объекта/зоны прохода»](#)

Удаляет с карты пользователя только тот код объекта (или зону прохода), который соответствует мастер-карте, приложенной в процессе очистки.

[«Очистить защищенные карты — удалить все коды объектов/зоны прохода»](#)

Удаляет с карты пользователя все коды объектов (или все зоны прохода) без необходимости прикладывать мастер-карту.

[Таблица зон прохода](#)

Список зон (от 1 до 64) с чекбоксами. Позволяет выбрать, какие зоны будут записаны на карту пользователя при создании.

«Выбрать все зоны»

Активирует все чекбоксы в таблице зон прохода.

«Снять выбор со всех зон»

Деактивирует все чекбоксы в таблице зон прохода.

«Битовая строка»

Открывает окно для ввода маски разрешенных зон в виде 64-битной последовательности (0 и 1). Позволяет быстро задать зоны при известной битовой маске.

2.4.1. Кнопка «Создать защищенные карты»

Назначение:

Создает одну или несколько защищенных карт пользователей. В зависимости от выбранного режима на карту записывается следующая информация:

В режиме «**Код объекта**»:

- В определенной области памяти, защищенной от несанкционированного доступа с помощью секретного ключа, сохраняется зашифрованный уникальный идентификатор (UID) карты и код объекта.

В режиме «**Чтение кода из блока**»:


- В указанную область памяти (сектор) записываются следующие данные:
 - UID карты (блок 0 относительно сектора);
 - Хеш UID карты (блок 1 относительно сектора);
 - Битовая маска зон (блок 2 относительно сектора) в соответствии с таблицей, указанной в [разделе 3.3.3.2.5](#);
 - Код доступа к блоку.

В режиме «**Зоны прохода**»:

- В определенной области памяти, защищенной от несанкционированного доступа с помощью секретного ключа, сохраняются битовая маска зон прохода и код объекта.

Порядок действий:

- Убедитесь, что считыватель находится в защищенном режиме.
- Если выбран режим «**Чтение кода из блока**» или «**Зоны прохода**», отметьте флажками в таблице зоны прохода, которые будут разрешены для создаваемых карт.
- Нажмите кнопку «**Создать защищенные карты**».
- При необходимости (в зависимости от режима) приложите мастер-карту.
- Последовательно прикладывайте карты пользователей, которые требуется записать.
- Нажмите кнопку «**Закончить создание защищенных карт**».

 *Карты, не сконфигурированные как «защищенные» в программе «Конфигуратор считывателей «ЭРА», не будут восприниматься считывателями, работающими в защищенном режиме.*

2.4.2. Кнопка «Очистить защищенные карты - удалить код объекта/зоны прохода»

Назначение:

Удаляет с карты пользователя только тот код объекта (или зону прохода), который соответствует мастер-карте, приложенной в процессе очистки. Операция доступна в

режимах «Код объекта» и «Зоны прохода».

Порядок действий:

- Нажмите кнопку «Очистить защищенные карты — удалить код объекта/зоны прохода».
- В появившемся диалоговом окне с надписью «Для очистки защищенных карт потребуется ранее созданная мастер-карта с заданным кодом объекта. Продолжить?» нажмите «Да».
- Появится окно с таймером обратного отсчета и надписью приложить мастер-карту к считывателю. Приложите мастер-карту.
- Поочередно подносите карты пользователей, которые требуется очистить.
- Нажмите кнопку «Закончить очистку защищенных карт».

Результат:

С каждой приложенной карты пользователя удаляется код объекта (или зона прохода), соответствующий приложенной мастер-карте. Другие коды объектов (если они были записаны на карту) остаются без изменений.

2.4.3. Кнопка «Очистить защищенные карты - удалить все коды объектов/зоны прохода»

Назначение:

Удаляет с карты пользователя все коды объектов (или все зоны прохода). Операция доступна в режимах «Код объекта» и «Зоны прохода».

Порядок действий:

- Нажмите кнопку «Очистить защищенные карты — удалить все коды объектов/зоны прохода».
- В появившемся диалоговом окне с надписью «Для очистки защищенных карт потребуется ранее созданная мастер-карта с заданным кодом объекта. Продолжить?» нажмите «Да».
- Появится окно с таймером обратного отсчета и надписью приложить мастер-карту к считывателю. Примечание: В данной операции мастер-карта не требуется, окно с таймером может быть пропущено или закрыто.
- Поочередно подносите карты пользователей, которые требуется очистить.
- Нажмите кнопку «Закончить очистку защищенных карт».

Результат:

С каждой приложенной карты пользователя удаляются все коды объектов (или все зоны прохода). Карта становится «чистой» и может быть использована для записи новых данных.

Отличие от предыдущей операции: при удалении всех кодов объектов мастер-карта

не требуется, и с карты удаляется вся информация, связанная с защищенными режимами.

2.4.4. Таблица зон прохода и вспомогательные кнопки

В режимах «Чтение кода из блока» и «Зоны прохода» на вкладке «Защищенные карты» отображается таблица зон прохода.

<i>Элемент</i>	<i>Описание</i>
Таблица зон прохода	Список зон с 1 по 64. Напротив каждой зоны расположен чекбокс. Для записи на карту пользователя необходимо отметить флажками те зоны, которые будут разрешены.
«Выбрать все зоны»	Активирует все чекбоксы в таблице зон прохода одновременно.
«Снять выбор со всех зон»	Деактивирует все чекбоксы в таблице зон прохода одновременно.
«Битовая строка»	Открывает окно для ввода маски разрешенных зон в виде 64-битной последовательности (0 и 1). После ввода и нажатия «Применить» соответствующие чекбоксы в таблице будут автоматически установлены. Подробное описание в разделе 2.3.1.8.6 «Битовая строка» .

Принцип формирования идентификатора при выводе битовой маски зон прохода:

При записи карт пользователя программа формирует 64-битную битовую маску на основе отмеченных зон. Каждая зона соответствует определенному биту:

<i>Зона</i>	<i>Бит</i>	<i>Вес</i>
Зона 1	бит 0	1 (2^0)
Зона 2	бит 1	2 (2^1)
Зона 3	бит 2	4 (2^2)
...
Зона 64	бит 63	2^{63}

Полученная маска записывается в память карты. При поднесении карты к считывателю, работающему в режиме «Чтение кода из блока» или «Зоны прохода», считыватель передает на контроллер/ПО это 64-битное число, интерпретированное как десятичное значение.

Примеры:

<i>Отмеченные зоны</i>	<i>Двоичная маска (младшие биты)</i>	<i>Десятичное значение</i>
Зона 1	000...0001	1

Зоны 1 и 2	000...0011	3
Зоны 1, 2 и 3	000...0111	7
Все 64 зоны	111...1111	18 446 744 073 709 551 615

Примечание: В режиме «Зоны прохода» считыватель работает автономно и может не передавать номер карты на контроллер. Однако при необходимости (например, для отладки или интеграции) полученное число можно увидеть в поле вывода UID.

2.4.5. Важные замечания

- Активность вкладки: параметры на вкладке «Защищенные карты» активны только при подключении считывателя, переведенного в один из защищенных режимов.
- Мастер-карта: для операций создания и очистки защищенных карт в режимах «Код объекта» и «Зоны прохода» требуется мастер-карта с соответствующим кодом объекта.
- Битовая строка: при использовании функции ввода маски через кнопку «Битовая строка» пользователь имеет возможность ввести последовательность символов (0 или 1) в количестве, соответствующем числу обозначаемых зон. Не введенные биты, после применения маски, автоматически заполняются символом 0. Ввод осуществляется в порядке возрастания значимости битов: от младшего (бит 0) к старшему (бит 64).

2.5. Вкладка «Обновление микропрограммы»

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

Файлы с микропрограммой предоставляются службой технической поддержки по запросу на электронную почту support@entpro.ru.

Нажав соответствующую кнопку, можно узнать текущую версию микропрограммы.

Для обновления микропрограммы нужно:

- Нажать кнопку «**Обзор**» и выбрать файл с микропрограммой.
- Нажать кнопку «**Начать обновление микропрограммы**».
- Дождаться окончания операции.

Во время обновления микропрограммы категорически запрещается:



- *Отключать считыватель от компьютера;*
- *Закрывать программу;*
- *Выключать или перезагружать компьютер.*

Прерывание процесса обновления может привести к выходу считывателя из строя.

2.6. Вкладка «Журнал»

Назначение вкладки

Вкладка «Журнал» предназначена для отображения и сохранения событий, происходящих в программе «Конфигуратор считывателей «ЭРА». Журнал позволяет отслеживать действия пользователя, события подключения и отключения считывателя, операции чтения и записи конфигурации, а также результаты считывания карт.

Журнал полезен для:

- Диагностики проблем при настройке считывателя;
- Аудита действий при работе с защищенными картами;
- Контроля процесса записи и очистки мастер-карт и карт пользователей;
- Анализа ошибок при считывании карт.

Внешний вид вкладки

Вкладка «Журнал» содержит:

Элемент	Описание
Таблица событий	Список событий с указанием времени, типа события и описания.
Кнопка «Сохранить журнал в файл»	Позволяет сохранить текущее содержимое журнала в текстовый файл для последующего анализа или отправки в службу технической поддержки.

Типы событий:

События в журнале классифицируются по типам:

Тип события	Описание	Примеры
Система	События, связанные с запуском программы и подключением оборудования	«Программа запущена», «Устройство и подключено COM4 (s/n: 0102-6C44F246)», «Устройство отключено»
Конфигурация	События, связанные с чтением и записью конфигурации считывателя	«Конфигурация считана из USB-считывателя», «Конфигурация записана в USB-считыватель»
Чтение карты	События, возникающие при поднесении карты к считывателю	«Тип карты: Mifare Plus X», «Мастер-карта не пуста», «Тип карты: Mifare Plus SE»
Ошибка	События, связанные с возникновением ошибок (при наличии)	«Ошибка чтения конфигурации», «Не удалось определить тип карты»

2.6.1. Просмотр событий

Все события отображаются в таблице в хронологическом порядке (от более ранних к более поздним). Каждая строка таблицы содержит:

Колонка *Описание*

Время	Время возникновения события в формате «ЧЧ:ММ:СС»
Тип	Категория события (Система, Конфигурация, Чтение карты, Ошибка)
Описание	Подробное текстовое описание события

Пример отображения событий:

Рисунок 21. Пример отображения событий на вкладке "Журнал"

Время	Тип	Описание
12:04:47	Система	Программа запущена
12:04:52	Система	Устройство подключено COM4 (s/n: 0202-B29698CD)
12:04:52	Конфигурация	Конфигурация считана из USB-считывателя
14:05:31	Чтение карты	Тип карты: Mifare Plus SE
14:05:52	Чтение карты	Тип карты: Mifare Plus SE
14:05:52	Конфигурация	Конфигурация считана с мастер-карты и записана в USB-считыватель
14:06:03	Чтение карты	Тип карты: Mifare Plus SE
14:06:04	Чтение карты	Ошибка аутентификации MFP.
14:06:04	Чтение карты	Тип карты: Mifare Plus SE
14:06:04	Чтение карты	ID карты: 9492280448472199760

2.6.2. Сохранение журнала в файл

Назначение:

Позволяет сохранить текущее содержимое журнала в текстовый файл для последующего анализа, печати или отправки в службу технической поддержки.

Порядок действий:

- Перейдите на вкладку «Журнал».
- Нажмите кнопку «Сохранить журнал в файл».
- В открывшемся диалоговом окне выберите папку для сохранения.
- Укажите имя файла (расширение .txt).
- Нажмите «Сохранить».

Результат:

Текущее содержимое журнала сохраняется в текстовый файл в выбранном месте.

Формат сохраненного файла:

Текстовый файл с расширением `.txt`, в котором каждая запись журнала выводится в виде строки с разделителями (например, табуляцией или пробелами). Файл может быть открыт любым текстовым редактором (Блокнот, WordPad и т.д.) или импортирован в электронные таблицы.

Особенности работы журнала

Особенность	Описание
Автоматическое добавление	Все события добавляются в журнал автоматически без участия пользователя.
Хронологический порядок	События отображаются в порядке их возникновения.
Очистка журнала	При закрытии программы журнал очищается. Для долговременного хранения используйте кнопку «Сохранить журнал в файл».
Максимальный размер	Журнал не имеет ограничения по количеству записей в рамках одного сеанса работы программы.
Время событий	Время берется из системных часов компьютера.



Важные замечания:

- Журнал не сохраняется автоматически: при закрытии программы все записи журнала теряются. Для сохранения истории используйте кнопку «Сохранить журнал в файл» перед закрытием программы.
- Отображение только текущего сеанса: журнал показывает события только текущего сеанса работы программы. При перезапуске программы журнал начинает заполняться заново.
- Полезен для диагностики: при возникновении проблем с настройкой считывателя сохраните журнал и передайте его в службу технической поддержки для анализа.
- Конфиденциальность: сохраненный журнал может содержать серийные номера считывателей и другую служебную информацию. Учитывайте это при передаче файла третьим лицам.

Краткое резюме:

Вкладка «Журнал» отображает хронологию событий программы: запуски, подключения считывателей, операции с конфигурацией, результаты считывания карт. Все события автоматически записываются с указанием времени и типа.

Основные возможности:

- Просмотр событий в таблице.

-
- Сохранение журнала в текстовый файл (кнопка «Сохранить журнал в файл»).
 - Диагностика проблем и аудит действий.

Важно: Журнал не сохраняется автоматически. Для долговременного хранения используйте сохранение в файл перед закрытием программы.

3. НАСТРОЙКА РЕЖИМОВ РАБОТЫ

3.1. Обычный режим: «Чтение только UID»

3.1.1. Описание

Данный режим, предназначенный для считывания исключительно идентификационного номера карты (UID) или (PAN) в случае банковских карт при выборе соответствующего формата, запрограммированного на заводе-изготовителе. Данный режим используется в случаях, когда на объекте уже применяются бесконтактные карты. Следует подчеркнуть, что данный режим не обладает уровнем защиты, поскольку уникальный идентификационный номер (UID) карты может быть легко скопирован. Исключение составляет чтение PAN-номера у банковских карт, который защищен от relay-атак и не может быть скопирован и эмулирован.

Для предотвращения возможности копирования карт, особенно на этапе проектирования новых объектов, рекомендуется настраивать систему для работы в защищенном режиме.

Заводские настройки параметров представлены на **Ошибка! Источник ссылки не найден.** В соответствии с этими настройками, считыватель будет принимать уникальный идентификационный код, запрограммированный на заводе-изготовителе, от карт, соответствующих стандартам, указанным в параметре «**Формат считываемых карт**». Устройство поддерживает все стандартные форматы Wiegand длиной до 64 битов включительно, а также осуществляет контроль чётности.

Для адаптации считывателя к необходимым требованиям необходимо установить соответствующие значения параметров в блоке «Общая конфигурация» и нажать кнопку «Записать конфигурацию в считыватель».

3.1.2. Доступные параметры конфигурации

При выборе обычного режима «Чтение только UID» в блоке программного интерфейса «Общая конфигурация» становятся доступными следующие параметры. Подробное описание каждого параметра приведено в разделе 2.3.1.

<i>Параметр / Раздел</i>	<i>Краткое описание для настройки</i>
«Тип интерфейса Wiegand»	Выберите формат передачи данных на контроллер: с битами четности (Wiegand с CRC) или без них (Wiegand без CRC).
«Разрядность интерфейса Wiegand»	Укажите длину пакета вручную (от 8 до 64 бит) или выберите «Автоопределение» для автоматического подбора под стандартные форматы.
«Формат считываемых карт»	Отметьте флажками те типы карт, которые будут использоваться (Mifare, банковские карты, телефон

с NFC, Em-Marine и др.). Включение только нужных форматов ускоряет работу считывателя.

«Преобразование»

Настройте изменение формата UID перед отправкой на контроллер, если это требуется:

↳ «Обратный порядок байт»

Включите, если контроллер ожидает данные в формате little-endian (младший байт первым).

↳ «Битовый сдвиг вправо»

Сдвигает биты UID вправо. Позволяет отбросить младшие биты и добавить нули слева.

↳ «Число значимых бит после сдвига»

Ограничивает длину передаваемых данных, обрезая лишние старшие биты. Используйте для приведения к требуемой разрядности контроллера.

↳ «Хеш-функция»

Включите, если длина UID превышает разрядность Wiegand или различия в UID карт находятся в разных позициях. Преобразует весь UID в хеш-значение, гарантируя уникальность выходных кодов. При включении остальные параметры преобразования становятся недоступны.

«Настройки для банковских карт»

Доступен только при выборе формата «Банковские карты – 8 байт». Позволяет настроить шифрование PAN банковской карты:

↳ «Режим работы»

Выберите алгоритм шифрования: AES (128 бит) или HMAC-SHA256 (256 бит).

↳ «Преобразование для HMAC»

Настройте битовый сдвиг и число значимых бит для выбора участка из зашифрованного номера (доступно для HMAC).

↳ «Ключ шифрования (16 байт)»

Выберите ключ по умолчанию или укажите пользовательский (HEX). На всех считывателях системы ключ должен быть одинаковым.

3.1.3. Настройка считывателя:


Пример порядка для настройки считывателя:

- Подключите считыватель к компьютеру.
- Перейдите на вкладку «Конфигурация».
- В блоке «Общая конфигурация»:
 - Выберите тип интерфейса Wiegand.
 - Настройте разрядность.
 - Выберите режим работы считывателя.
 - Отметьте необходимые форматы считываемых карт.

- При необходимости настройте преобразования и параметры для банковских карт.
- При работе с настенным считывателем «ЭРА-MF» настройте цвета в блоке «Световая схема».
- При необходимости включите чекбоксы для вывода ID карты (буфер обмена, имитация набора).
- В боковой панели действий нажмите **«Записать конфигурацию в USB-считыватель»**.
- Для проверки поднесите карту к считывателю — ID должен отобразиться в боковой панели вкладки «Отладка».

В качестве примера рассмотрим конфигурацию считывателя для использования стандартного формата Wiegand 37 с обратным порядком байт. В программе «Конфигуратор считывателей «ЭРА» установите параметр «Разрядность интерфейса Wiegand» на значение «Пользовательская» и задайте 35 бит. Учитывая контрольную сумму, общая длина идентификатора составит 37 бит. Активируйте функцию «Обратный порядок байт», установив соответствующую галочку. Параметр «Число значимых бит после сдвига» должен быть установлен на значение 35. После выполнения этих настроек сохраните конфигурацию в считыватель «ЭРА». Для проверки корректности конфигурации приложите карту к считывателю и убедитесь в корректности выводимого формата UID.

Таким образом можно обеспечить совместимость с устройствами других производителей при работе с UID бесконтактных карт.

 *Параметры в блоке «Общая конфигурация» должны соответствовать настройкам подключенного контроллера (тип Wiegand, разрядность, биты четности). В противном случае контроллер может не распознавать полученный UID карты.*

3.1.4. Создание мастер-карт для режима «Чтение только UID»

Для создания мастер-карт в режиме «Чтение только UID» выполните общую процедуру, описанную в разделе [2.3.2.7 «Создание мастер-карт»](#).

Особенности для данного режима:

Допускается создание неограниченного числа мастер-карт с установленными параметрами, однако единовременная запись не может превышать пяти карт.


3.2. Защищенный режим «Код объекта»

3.2.1. Описание режима

Данный режим является защищенным. Идентификация карт происходит не по заводскому UID, а по информации, содержащейся в определенной области памяти карты, закрытой от чтения секретным ключом.


Поддерживаемые типы карт:

Тип карты	Уровень защиты	Примечание
Mifare Classic 1K / 4K	Низкий	Поддержка добавлена для использования в существующих системах. Карты можно скопировать, но сложнее, чем UID.
Mifare Plus (SE, S, X)	Высокий	Рекомендуется для новых объектов. Использует алгоритм AES с длиной ключа 128 бит.

 Для данного режима следует использовать карты, находящиеся в «транспортном состоянии» (с завода-изготовителя). Карты, уже переведенные в режим SL1/SL2/SL3 другим оборудованием, использовать НЕЛЬЗЯ. Карты Mifare ID не подходят для данного режима.

Особенности режима:

- При переводе карт в защищенный режим устанавливается Random UID — карта выдает каждый раз разный UID длиной 4 байта при поднесении к обычным считывателям. Это «обезличивает» карты для сторонних систем.
- Используется механизм диверсификации ключей — в каждой карте свои ключи доступа. Подбор ключа для одной карты позволит скопировать только её.
- Код объекта формируется как случайное число при создании мастер-карт и нигде не отображается в открытом виде (только контрольная сумма).
- Одна карта пользователя может содержать более 10 различных кодов объектов.

 При использовании считывателя с микропрограммой 1.2.7 и ниже для мастер-карт Mifare Classic функциональность ограничена: недоступна функция снятия защиты от реконфигурации и операция «Считать конфигурацию с мастер-карты и записать в USB-считыватель». Рекомендуется использовать хотя бы одну мастер-карту на основе Mifare Plus.

3.2.2. Доступные параметры конфигурации

При выборе защищенного режима «Код объекта» в блоке программного интерфейса «Общая конфигурация» становятся доступными следующие параметры. Подробное описание каждого параметра приведено в соответствующих подразделах раздела [2.3.1 «Блок «Общая конфигурация»»](#).

Параметр / Раздел

Краткое описание для настройки

«Тип интерфейса Wiegand»	Выберите формат передачи данных на контроллер: с битами четности (Wiegand с CRC) или без них (Wiegand без CRC).
«Разрядность интерфейса Wiegand»	Укажите длину пакета вручную (от 8 до 64 бит) или выберите «Автоопределение» для автоматического подбора под стандартные форматы.
«Формат считываемых карт»	Доступны только Mifare Classic (низкий уровень защиты) и Mifare Plus (высокий уровень защиты).
Раздел «Преобразование»	Настройте изменение формата UID перед отправкой на контроллер, если это требуется. Все параметры раздела доступны.
↳ «Обратный порядок байт»	Включите, если контроллер ожидает данные в формате little-endian (младший байт первым).
↳ «Битовый сдвиг вправо»	Сдвигает биты UID вправо. Позволяет отбросить младшие биты и добавить нули слева.
↳ «Число значимых бит после сдвига»	Ограничивает длину передаваемых данных, обрезая лишние старшие биты.
↳ «Хеш-функция»	Преобразует весь UID в хеш-значение. Используйте, если длина UID превышает разрядность Wiegand.

3.2.3. Порядок настройки системы

Для перевода системы в режим **«Код объекта»** необходимо выполнить три шага:

- Создать мастер-карты с кодом объекта.
- Перевести считыватель в защищенный режим.
- Записать карты пользователей.

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

Для создания мастер-карт в режиме «Код объекта» выполните общую процедуру, описанную в разделе [2.3.2.7 «Кнопка «Создать мастер-карты»](#).

Особенности для данного режима:


<i>Особенность</i>	<i>Описание</i>
Поддерживаемые карты	Mifare Classic 1K/4K и Mifare Plus (SE, S, X).
Максимальное количество	Не более 5 мастер-карт с одинаковым кодом объекта. Все создаются за один раз и нумеруются.

Код объекта


Формируется случайным образом. Посмотреть или переписать его невозможно. При чтении конфигурации отображается только контрольная сумма.

Нумерация карт

Каждая мастер-карта содержит информацию о том, сколько карт было создано и какой номер по порядку у данной карты. Это позволяет проверить, что заказчику переданы все созданные мастер-карты.

 **Защита от реконфигурации**

При активации защиты от реконфигурации (Рисунок 15 – 2) снять защиту со считывателя можно будет только с помощью мастер-карт с тем же кодом объекта. При утере всех мастер-карт перенастроить считыватель станет невозможно.

 **Совместимость версий микропрограммы**

При использовании считывателя с микропрограммой 1.2.7 и ниже для мастер-карт Mifare Classic функциональность ограничена: недоступна функция снятия защиты от реконфигурации и операция «Считать конфигурацию с мастер-карты и записать в USB-считыватель». Рекомендуется использовать хотя бы одну мастер-карту на основе Mifare Plus.

 *Если защищенный режим «Код объекта» используется на основе мастер-карт Mifare Plus, применение карт Mifare Classic становится невозможным.*

3.2.3.2. Настройка считывателя в режим «Код объекта»

Существует два способа перевода считывателя в защищенный режим. В обоих случаях необходимо наличие предварительно созданной мастер-карты с кодом объекта. В первом варианте параметры конфигурации задаются через интерфейс программного обеспечения, с мастер-карты копируется исключительно код объекта, во втором — путем извлечения всех данных из памяти мастер-карты.

Вариант 1: Ручной ввод конфигурации

- Подключите считыватель к компьютеру.
- В программе выберите режим «**Защищенный режим: код объекта**».
- Выберите «**Формат считываемых карт**».
- Настройте параметры интерфейса Wiegand, преобразования и цветовой схемы.
- Нажмите кнопку «**Записать конфигурацию в USB-считыватель**».
- В появившемся диалоговом окне нажмите «**Да**».
- Приложите ранее созданную мастер-карту к считывателю для копирования кода объекта.

Рисунок 22. Параметры для настройки считывателя на работу в режиме "Код объекта"

Вариант 2: Копирование конфигурации из мастер-карты

- Подключите считыватель к компьютеру.
- Нажмите кнопку «**Считать конфигурацию с мастер-карты и записать в USB-считыватель**».
- Приложите мастер-карту к считывателю.
- После завершения операции считыватель переведен в режим «**Код объекта**» со всеми настройками, сохраненными на мастер-карте.


3.2.3.3. Запись карт пользователей

Для записи пользовательских карт выполните общую процедуру, описанную в разделе [2.4.1 «Кнопка «Создать защищенные карт»»](#).

i *Карты, не сконфигурированные как «защищенные» в программе «Конфигуратор считывателей «ЭРА», не будут восприниматься считывателями, работающими в защищенном режиме.*

3.2.4. Важные замечания

Замечание	Пояснение
Совместимость карт	Mifare Classic поддерживаются для обратной совместимости, но не являются полностью безопасными (алгоритм шифрования Crypto-1, длина ключа 48 бит). Для новых объектов рекомендуется использовать Mifare Plus (алгоритм шифрования AES, длина ключа 128 бит).
Необходимый уровень безопасности карты	Карты должны быть исключительно на заводском уровне безопасности (SL0). Система самостоятельно переводит их из SL0 на SL3. Карты, уже переведенные на SL1/SL2/SL3 другим оборудованием, использовать НЕЛЬЗЯ — коды доступа неизвестны, а перевод обратно невозможен.
Random UID	После перевода карты в защищенный режим при поднесении к считывателям, работающим только по UID, карта будет выдавать каждый раз случайный UID размером 4 байта. Это

	нормальное поведение, позволяющее «обезличить» карты для сторонних систем.
Диверсификация ключей	В каждой карте используются свои ключи для доступа к закрытым областям. Подбор ключа для одной карты позволит скопировать только её и не будет действителен для других карт.
Изменение режима	Смена режима работы считывателя после того, как карты уже выданы пользователям, может привести к невозможности идентификации ранее выданных карт.
Обратная совместимость	Карты, подготовленные для защищенного режима, не будут корректно работать в считывателях, настроенных на обычный режим чтения UID (и наоборот).
 Хранение мастер-карт	<i>Храните мастер-карты в надежном месте. При активации опции защиты от реконфигурации утрата всех мастер-карт делает невозможным перенастройку считывателя.</i>
Код объекта не отображается	Код объекта невозможно посмотреть или скопировать. При чтении конфигурации с мастер-карты или считывателя отображается только контрольная сумма, позволяющая определить, что мастер-карты содержат одинаковый код объекта.


3.2.5. Краткое резюме

Режим «Код объекта» — защищенный режим, в котором идентификация карт происходит не по UID, а по коду объекта, хранящемуся в закрытой области памяти карты.

Поддерживаемые карты: Mifare Classic (низкий уровень, для существующих систем) и Mifare Plus (высокий уровень, рекомендуется для новых объектов).

Для настройки потребуется:

- Создать мастер-карты с кодом объекта ([раздел 2.3.2.7 «Кнопка «Создать мастер-карты»](#)).
- Записать конфигурацию в считыватель (с мастер-карты или вручную, [раздел 3.2.3.2. «Настройка считывателя в режим «Код объекта»](#)).
- Записать карты пользователей на вкладке «Защищенные карты» ([раздел 2.4.1 «Кнопка «Создать защищенные карты»](#)).

 *Код объекта невозможно посмотреть — только контрольная сумма. Мастер-карт с одинаковым кодом может быть не более 5. При активации опции защиты от реконфигурации утеря мастер-карт делает перенастройку считывателя невозможной. Для перевода карт в защищенный режим используйте карты Mifare Plus на заводском уровне защиты (SLO).*

3.3. Защищенный режим «Чтение кода из блока»

3.3.1. Описание режима

Данный режим позволяет использовать в качестве идентификационного номера карты заводской UID или другие данные, хранящиеся в определенной области (блоке) памяти карты. Каждый сектор памяти карты может быть ограничен в чтении и записи установкой соответствующего кода доступа. Отдельно задается ключ на чтение и на запись (могут быть одинаковы). Важно понимать, что доступ ограничен именно в пределах сектора (не блока).

Поддерживаемые карты: Mifare Plus (SE, S, X).

Области применения:

Сценарий	Описание
Интеграция с существующей системой	На объекте уже есть карты Mifare Plus в режиме SL3 со своими данными в защищенной области. Считыватель настраивается на чтение из той же области с тем же ключом.
Создание новой защищенной системы	Защищенные карты пользователей будут выдаваться через считыватель «ЭРА», записывая в них UID (или хеш UID) в определенный блок с определенным ключом.
Управление замками (зоны прохода)	При использовании считывателя «ЭРА», возможно реализовать систему контроля доступа без дополнительного оборудования системы контроля и управления доступом (аналогично принципу работы в режиме «Зоны прохода», раздел 3.4).

Особенности режима:

- При вводе кода доступа в открытом виде берегите его от несанкционированного доступа.
- При чтении конфигурации с мастер-карты или считывателя отображается контрольная сумма кода доступа, а не сам код.
- Защита действует на уровне сектора: все блоки внутри одного сектора защищены одним ключом.
- Для записи и чтения записанных пользовательских карт при помощи считывателя «ЭРА» используйте таблицу соответствия ([раздел 3.3.3.2.5](#)), чтобы выбрать правильный блок и смещение в зависимости от нужного формата (прямой/обратный порядок, UID/хеш, битовая маска).
- При выборе одного из трех блоков (0, 1 или 2) в контексте сектора при записи пользовательских карт, процесс записи будет охватывать весь сектор, включая блоки с номерами от 0 до 2.

3.3.2. Доступные параметры конфигурации

При выборе защищенного режима «Чтение кода из блока» в блоке программного интерфейса «Общая конфигурация» становятся доступными следующие параметры. Подробное описание каждого параметра приведено в соответствующих подразделах раздела [2.3.1. «Блок «Общая конфигурация»»](#).

<i>Параметр / Раздел</i>	<i>Краткое описание для настройки</i>
«Тип интерфейса Wiegand»	Выберите формат передачи данных на контроллер: с битами четности (Wiegand с CRC) или без них (Wiegand без CRC).
«Разрядность интерфейса Wiegand»	Укажите длину пакета вручную (от 8 до 64 бит) или выберите «Автоопределение».
«Формат считываемых карт»	Будет автоматически выбран Mifare Plus.
«Преобразование»	Настройте обратный порядок байт, битовый сдвиг или число значимых бит, если требуется изменить формат UID перед отправкой.
Раздел параметров «Чтение кода из блока»	Это главные параметры для данного режима. Укажите, откуда именно считывать код:
↳ «Номер блока»	Абсолютный номер блока в памяти карты (от 0 до 127), откуда начинать чтение.
↳ «Смещение байт в блоке»	С какого байта внутри блока начать (от 0 до 15). Зависит от «Количества байт».
↳ «Количество байт для передачи»	Длина идентификатора (от 1 до 8 байт), который будет передан на контроллер.
↳ «Код доступа к требуемому блоку»	Ключ для доступа к защищенному блоку (16 байт в HEX). Храните в безопасности.
Раздел параметров «Зоны прохода»	Позволяет настроить считыватель как самостоятельный контроллер для управления замком. Доступен только для считывателей «ЭРА-MF».
↳ «Выбор шаблона имен зон»	Выберите сохраненный шаблон с пользовательскими именами зон или оставьте «Стандартные имена».
↳ Таблица зон прохода	Отметьте флажками те зоны, которые будет обслуживать данный считыватель.

↳ «Сохранить имена зон прохода»	Сохраняет переименованные зоны в файл-шаблон для последующего использования.
↳ «Выбрать все зоны прохода»	Активирует все чекбоксы в таблице зон.
↳ «Снять выбор со всех зон прохода»	Деактивирует все чекбоксы.
↳ «Битовая строка»	Позволяет ввести маску зон в виде 64-битной последовательности (0 и 1).
↳ «Длительность управляющего импульса (секунд)»	Время, на которое считыватель подает напряжение (для электромеханического замка) или снимает напряжение (для электромагнитного).
↳ «Тип замка»	Выберите тип запирающего устройства: «Электромеханический» или «Электромагнитный».

3.3.3. Порядок настройки системы

Настройка зависит от цели использования:

Вариант А: настройка считывателя для чтения существующих защищенных карт (интеграция с уже работающей внешней системой).

Вариант Б: настройка считывателя для нового объекта (создание мастер-карт, перевод считывателя, запись карт пользователей).

Вариант В: настройка считывателя для автономной работы и интеграции пользовательских карт с внешними системами, например, домофонами Bas-IP или аналогами.


3.3.3.1. Вариант А: Настройка считывателя для чтения существующих защищенных карт

Данный вариант применяется в случае, если на объекте уже функционирует внешняя система контроля и управления доступом (СКУД), использующая карты стандарта Mifare Plus, на которых записаны данные в определенном блоке и известен код доступа.

- Подключите считыватель к компьютеру.
- В программе выберите **защищенный режим «Чтение кода из блока»**.
- В разделе настроек **«Чтение кода из блока»** укажите:
 - **«Номер блока»** — блок, где хранятся идентификационные данные.
 - **«Смещение байт в блоке»** — с какого байта начинать чтение.
 - **«Количество байт для передачи»** — длину идентификатора.
 - **«Код доступа к требуемому блоку»** — ключ доступа.
- При необходимости настройте «Тип интерфейса Wiegand», «Разрядность» и «Преобразование».

- Нажмите кнопку «**Записать конфигурацию в USB-считыватель**» на боковой панели «Действия».

Рисунок 23. Основные параметры для настройки считывателя на чтение кода из блока. Вариант А

 *Код доступа вводится в открытом виде. Берегите его от несанкционированного доступа, так как он может быть использован для создания дубликатов карт.*

3.3.3.2. Вариант Б: Настройка считывателя для нового объекта


Для настройки считывателя и последующей выдачи пользовательских карт необходимо выполнить три шага:

- Создать мастер-карты.
- Перевести считыватель в защищенный режим.
- Записать карты пользователей.

3.3.3.2.1. Создание мастер-карты для режима «Чтение кода из блока»

Для создания мастер-карт в режиме «Чтение кода из блока» выполните общую процедуру, описанную в разделе [2.3.2.7 «Создание мастер-карт»](#).

Особенности для данного режима:

Особенность	Описание
Поддерживаемые карты	Mifare Plus (SE, S, X).
Максимальное количество	Допускается создание неограниченного числа мастер-карт, но одновременно не более 5.
Контрольная сумма	При считывании настроек с мастер-карты или считывателя отображается контрольная сумма кода доступа, а не сам код. Это предотвращает его несанкционированное копирование.
 Формат записи	При создании мастер-карт и указании номера блока необходимо учитывать, в каком формате будут записываться


данные в карты пользователей (прямой/обратный порядок, хеш или UID). От этого зависит, какой идентификатор будет передаваться в систему (раздел [3.3.3.2.5 «Таблица соответствия для записи карт»](#)).


3.3.3.2.2. Перевод считывателя в режим «Чтение кода из блока»

Существует два способа перевода считывателя в защищенный режим. В первом варианте параметры конфигурации задаются через интерфейс программного обеспечения, во втором — путем извлечения данных из памяти ранее созданной мастер-карты.

Вариант 1: Ручной ввод конфигурации

- Подключите считыватель к компьютеру.
- В программе выберите **защищенный режим «Чтение кода из блока»**.
- В разделе настроек **«Чтение кода из блока»** укажите:
 - **«Номер блока»** — блок, где хранятся идентификационные данные.
 - **«Смещение байт в блоке»** — с какого байта начинать чтение.
 - **«Количество байт для передачи»** — длину идентификатора.
 - **«Код доступа к требуемому блоку»** — ключ доступа.
- При необходимости настройте «Тип интерфейса Wiegand», «Разрядность» и «Преобразование».
- Нажмите кнопку **«Записать конфигурацию в USB-считыватель»** на боковой панели «Действия».

 При последующей записи данных в блоки 0 и 1 (относительно сектора) памяти пользовательских карт будет использоваться уникальный идентификационный номер (UID), присвоенный карте на заводе. Однако, в зависимости от конкретного блока и битности данный номер преобразуется в соответствии с предварительно установленными алгоритмами. Подробнее в разделе [3.3.3.3.5. Таблица соответствия для записи карт](#).

 Код доступа вводится в открытом виде. Берегите его от несанкционированного доступа, так как он может быть использован для создания дубликатов карт.

Вариант 2: Копирование конфигурации из памяти мастер-карты

- Подключите считыватель к компьютеру.
- Нажмите кнопку **«Считать конфигурацию с мастер-карты и записать в USB-считыватель»**.
- Приложите ранее созданную мастер-карту к считывателю.
- После завершения операции считыватель переведен в режим «Чтение кода из блока» со всеми настройками, сохраненными на мастер-карте.

3.3.3.2.3. Запись карт пользователей

Для записи пользовательских карт выполните общую процедуру, описанную в разделе [2.4.1 «Кнопка «Создать защищенные карт»»](#).

3.3.3.3. Вариант В: Настройка для интеграции с внешними системами

Например, интеграция с домофонами Bas-IP или их аналогами (организация прохода на калитки).

Сценарий:

На объекте установлены домофоны Bas-IP (или другие, поддерживающие карты Mifare Plus в режиме SL3). Требуется закрыть дополнительные двери (калитки, тамбуры, служебные входы), где домофоны отсутствуют, но нет необходимости устанавливать полноценный контроллер СКУД.

Решение:

Используется режим «Чтение кода из блока» как для записи карт пользователей, так и для настройки считывателей на точках прохода как автономный контроллер. В карту пользователя в блок 2 (относительно сектора) записывается маска разрешенных зон (64 бита). Считыватель «ЭРА-MF» на калитке считывает из блока 2 маску зон и, если его зона присутствует, управляет замком.

Необходимое оборудование:

- Считыватель «ЭРА-USB» (для настройки и записи карт).
- Считыватели «ЭРА-MF» на калитках (для контроля доступа).
- Мастер-карты Mifare Plus.
- Карты пользователей Mifare Plus.

3.3.3.3.1. Настройка считывателя для интеграции пользовательских карт с внешними системами

Для создания мастер-карт в режиме «Чтение кода из блока» выполните общую процедуру, описанную в разделе [2.3.2.7 «Создание мастер-карт»](#).

Особенности для данного режима:

Особенность	Описание
Поддерживаемые карты	Mifare Plus (SE, S, X).
Максимальное количество	Допускается создание неограниченного числа мастер-карт, но одновременно не более 5.
Контрольная сумма	При считывании настроек с мастер-карты или считывателя отображается контрольная сумма кода доступа, а не сам код. Это предотвращает его несанкционированное копирование.

При создании мастер-карт необходимо указать:

- «Номер блока» — $N \times 4 + 2$, где N — сектор. Например, для сектора 2: $2 \times 4 + 2 = 10$, указать 10 блок.

- Смещение и количество байт — оставьте по умолчанию (0 и 8 соответственно).

- «Код доступа к требуемому блоку» — задайте ключ доступа (16 байт HEX).



Формат записи

(раздел [3.3.3.2.4 «Таблица соответствия для записи карт»](#)).


3.3.3.3.2. Перевод считывателя в режим «Чтение кода из блока» для управления точкой прохода


Существует два способа перевода считывателя в защищенный режим. В первом варианте параметры конфигурации задаются через интерфейс программного обеспечения, во втором — путем извлечения данных из памяти ранее созданной мастер-карты.

Вариант 1: Ручной ввод конфигурации

- Подключите считыватель к компьютеру.
- В программе выберите **защищенный режим «Чтение кода из блока»**.
- В разделе настроек **«Чтение кода из блока»** укажите:
 - «**Номер блока**» — $N \times 4 + 2$, где N — сектор. Например, для сектора 2: $2 \times 4 + 2 = 10$, указать 10 блок (2 блок относительно сектора);
 - «**Смещение байт в блоке**» — 0;
 - «**Количество байт для передачи**» — длину идентификатора;
 - «**Код доступа к требуемому блоку**» — ключ доступа.
- В разделе настроек **«Зоны прохода»** укажите:
 - Выберите **«Тип замка»**, которым будет управлять считыватель.;
 - **«Длительность управляющего импульса (секунд)»**;
 - **«Зоны прохода»** - выберите точку прохода, которую будет контролировать считыватель (например, зону 1 для доступа через калитку).
- При необходимости настройте **«Тип интерфейса Wiegand»**, **«Разрядность»** и **«Преобразование»**.
- Нажмите кнопку **«Записать конфигурацию в USB-считыватель»** на боковой панели **«Действия»**.

Рисунок 24. Основные параметры для настройки считывателя на чтение кода из блока. Вариант В

 При настройке считывателя на получения данных из блока 2 (относительно сектора) памяти пользовательских карт он будет считывать битовую маску разрешенных зон (64 бита).

 Код доступа вводится в открытом виде. Берегите его от несанкционированного доступа, так как он может быть использован для создания дубликатов карт.

Вариант 2: Копирование конфигурации из мастер-карты

- Подключите считыватель к компьютеру.
- Нажмите кнопку «Считать конфигурацию с мастер-карты и записать в USB-считыватель».
- Приложите ранее созданную мастер-карту к считывателю.
- После завершения операции считыватель переведен в режим «Чтение кода из блока» со всеми настройками, сохраненными на мастер-карте


3.3.3.3.3. Запись карт пользователей

Для записи пользовательских карт выполните общую процедуру, описанную в разделе [2.4.1 «Кнопка «Создать защищенные карт»»](#).

Программа автоматически запишет в блок 10 битовую маску разрешенных зон (64 бита) в соответствии с отмеченными флажками.

Для осуществления процедуры записи карт и ввода/вывода уникального идентификационного номера карт рекомендуется использовать USB-считыватель «ЭРА-

USB MF/EM». Настройка считывателя должна быть произведена на чтение кода из блока (например, 1 блок относительно сектора для получения хеш (UID)), указанного в разделе [3.3.3.3.5 «Таблица соответствия для записи карт»](#) того же сектора, который отмечен на считывателе на точке прохода с тем же кодом доступа. Таким образом, считыватель на точке прохода функционирует в соответствии с битовой маской зон, а в офисном помещении производится запись новых карт с необходимым выводом идентификационного номера (прямой/обратный порядок, UID/хеш (UID)) для интеграции с внешней системой и выдачи пользователям.

 *Карты, не сконфигурированные как «защищенные» в программе «Конфигуратор считывателей «ЭРА», не будут восприниматься считывателями, работающими в защищенном режиме.*

3.3.3.3.4. Настройка внешней системы

Произведите настройку устройства считывания идентификационных данных внешней системы для корректного распознавания идентификационного номера, генерируемого считывателем «ЭРА», из блока 0 или 1, либо битовую маску зон прохода из блока 2 заданного сектора. Введите код доступа к блоку (используемый для настройки считывателя «ЭРА») и идентификационный номер карты, предоставленный считывателем «ЭРА», в систему управления доступом Bas-IP или аналогичную систему.

Что происходит при поднесении карты к считывателю на калитке:


- Считыватель «ЭРА-MF», функционирующий в режиме «Чтение кода из блока», осуществляет сверку кода доступа, хранящегося в памяти карты, с собственным кодом. В случае совпадения данных, считыватель обращается к блоку 10 памяти карты, следуя установленным настройкам.
- Считывает 8 байт (64 бита) — маску разрешенных зон.
- Проверяет, установлен ли бит, соответствующий его зоне (например, бит 1 для зоны 1).
- Если бит установлен в «1» — считыватель подает (или снимает) напряжение на замок на заданное время (длительность управляющего импульса настраивается в разделе «Зоны прохода», но фактически управление замком реализовано через соответствующую логику в прошивке).


Что происходит при поднесении карты к домофону Bas-IP:


- Домофон функционирует в соответствии с установленными настройками и получает уникальный идентификационный номер (UID) или его хэш-значение, или битовую маску, сохранённую в соответствующем секторе памяти идентификационной карты пользователя.
- Сравнивает его со своей базой карт (или передает на сервер).
- При совпадении разблокирует замок.

Важные замечания для данного примера:

<i>Замечание</i>	<i>Пояснение</i>
Единый код доступа	Код доступа к сектору должен быть одинаковым для мастер-карт, считывателя на калитке и процесса записи карт пользователей. Иначе считыватель не сможет прочитать маску зон из блока 2.
Выбор сектора	Не используйте нулевой сектор для записи пользовательских карт (блоки 0-3). Начиная с сектора 1 (блоки 4-6 в системе абсолютной нумерации) или выше.
Управление замком	Считыватель «ЭРА-МФ» в режиме «Чтение кода из блока» может управлять замком, анализируя маску зон из блока 2 (относительно сектора). Длительность импульса и тип замка настраиваются в разделе «Зоны прохода» (2.3.1.8).
Совместимость	Убедитесь, что считывающее устройство возможно настроить на считывание кода из блока.
Карты должны быть Mifare Plus	Данный пример работает только с картами Mifare Plus (SE, S, X) в режиме SL3.

 При осуществлении записи используется уникальный идентификационный номер (UID), присвоенный карте на заводе. В зависимости от конкретного блока, данный номер преобразуется в соответствии с предварительно установленными алгоритмами.

 Запись данных не осуществляется в нулевой сектор и в последний блок каждого сектора (сектор-трейлер). При выборе блока для записи данные записываются начиная с нулевого и заканчивая вторым блоком выбранного сектора.

 Карты, не сконфигурированные как «защищенные» в программе «Конфигуратор считывателей «ЭРА», не будут восприниматься считывателями, работающими в защищенном режиме.

3.3.3.3.5. Таблица соответствия для записи карт

<i>Сектор</i>	<i>Нумерация блоков в секторе</i>	<i>Сквозная нумерация блоков</i>	<i>Доступные байты для передачи с 0 по 7</i>	<i>Доступные байты для передачи с 8 по 15</i>
N	Блок 3	$N \times 4 + 3$	Не используется	Не используется
N	Блок 2	$N \times 4 + 2$	Зоны прохода (64 бита маски разрешенных зон прохода)	Не используется
N	Блок 1	$N \times 4 + 1$	Прямой порядок, Хеш	Обратный порядок,

			(UID)	Хеш (UID)
N	Блок 0	$N \times 4 + 0$	Прямой порядок, UID	Обратный порядок, UID

Пояснения к таблице:

Блок	Назначение
Блок 0	При считывании данных из этого блока система получает стандартный UID карты. Для прямого порядка укажите смещение 0 байт, для обратного — смещение 8 байт.
Блок 1	Рекомендуется при укороченной длине Wiegand (например, 26 бит). В этом блоке для UID применяется хеш-функция, позволяющая исключить 5 байт хеша и выпускать карты без риска дублирования идентификаторов. Подробнее о хеш-функции в разделе 2.3.1.5.4. «Опция «Хеш-функция»» .
Блок 2	Используется для организации контроля доступа с управлением замком. Аналог режима «Зоны прохода»). <i>«Подробнее о режиме «Зоны прохода» в разделе 3.4»</i> .

3.3.4. Важные замечания

Замечание	Пояснение
Код доступа	При вводе в открытом виде храните его в надежном месте. При чтении конфигурации отображается только контрольная сумма.
Совместимость карт	Режим работает только с картами Mifare Plus (SE, S, X).
Защита сектора	Код доступа действует на весь сектор. Если вы указали блок в секторе, все блоки этого сектора защищены одним ключом.
Неиспользуемые области	Блок 3 каждого сектора (сектор-трейлер) и нулевой сектор не используются для хранения пользовательских данных.
Изменение режима	Смена режима работы считывателя после того, как карты уже выданы пользователям, может привести к невозможности идентификации ранее выданных карт.
Обратная совместимость	Карты, подготовленные для защищенного режима, не будут корректно работать в считывателях, настроенных на обычный режим чтения UID (и наоборот).
UID при записи	При осуществлении записи используется уникальный идентификационный номер (UID), присвоенный карте на заводе. В зависимости от конкретного блока, данный номер преобразуется в соответствии с предварительно установленными алгоритмами.

Структура секторов Перед настройкой убедитесь, что выбранный блок и смещение соответствуют структуре данных необходимых для вывода в систему. Используйте таблицу соответствия ([раздел 3.3.3.2.5](#)).

3.3.5. Краткое резюме

Режим «Чтение кода из блока» позволяет считывать идентификационные данные не из заводского UID, а из произвольного блока памяти карты Mifare Plus.

Поддерживаемые карты: Mifare Plus (SE, S, X).

Основные параметры настройки:


- «**Номер блока**» (0–127) — указывает, из какого блока памяти читать данные.
- «**Смещение байт в блоке**» (0–15) — с какого байта начать чтение.
- «**Количество байт для передачи**» (1–8) — длина идентификатора.
- «**Код доступа (16 байт)**» — ключ для доступа к защищенному блоку.

Для настройки чтения существующих карт:

- Укажите параметры блока и код доступа.
- Нажмите «**Записать конфигурацию в USB-считыватель**».

Для создания новых защищенных карт:

- Создайте мастер-карты ([раздел 2.3.2.7. «Кнопка «Создать мастер-карты»](#)).
- Переведите считыватель в режим ([раздел 3.3.3.2.2](#) или [3.3.3.3.1](#)).
- Запишите карты пользователей на вкладке «Защищенные карты» ([раздел 2.4.1. «Кнопка «Создать защищенные карты»](#)).

 При вводе кода доступа в открытом виде — берегите его от посторонних глаз. При чтении конфигурации отображается только контрольная сумма. Для записи карт используйте таблицу соответствия ([раздел 3.3.3.2.4](#)), чтобы выбрать правильный блок и смещение в зависимости от нужного формата (прямой/обратный порядок, UID/хеш).

3.4. Защищенный режим «Зоны прохода»

3.4.1. Описание режима


В данном режиме считыватель «ЭРА-MF» работает как самостоятельное устройство контроля доступа и может управлять замком (электромеханическим или электромагнитным) без участия внешнего контроллера СКУД.

Основная идея:

Объект делится на зоны (до 64). На карту пользователя записывается маска разрешенных зон. Считыватель на точке прохода настраивается на конкретную зону (например, «Подъезд 5» или «Калитка»). При поднесении карты считыватель проверяет, есть ли его зона в маске зон карты. Если есть — доступ разрешен.

Преимущества режима:

- Не требуется центральная база карт и постоянная связь с контроллером.
- Карты можно выпускать «на лету» без синхронизации с сервером.
- Считыватель сам управляет замком (подает или снимает напряжение).

 Программное переключение типа замка поддерживается только для считывателей «ЭРА-MF v2» с микросхемой версии 0.95. Для более ранних версий требуется специальная плата.

3.4.2. Доступные параметры конфигурации

При выборе защищенного режима «Зоны прохода» в блоке программного интерфейса «Общая конфигурация» становятся доступными следующие параметры. Подробное описание каждого параметра приведено в соответствующих подразделах раздела [2.3.1. «Вкладка «Общая конфигурация»»](#).

Параметр / Раздел	Краткое описание для настройки
«Тип интерфейса Wiegand»	Выберите формат передачи данных на контроллер: с битами четности (Wiegand с CRC) или без них (Wiegand без CRC).
«Разрядность интерфейса Wiegand»	Укажите длину пакета вручную (от 8 до 64 бит) или выберите «Автоопределение».
«Формат считываемых карт»	Будет автоматически выбран Mifare Plus.
Раздел «Зоны прохода»	Главные параметры для данного режима. Позволяют выбрать зоны и настроить управление замком:
↳ Выбор шаблона имен зон»	Выберите сохраненный шаблон с пользовательскими именами зон или оставьте «Стандартные имена».
↳ Таблица зон прохода	Отметьте флажками те зоны, которые будет обслуживать данный считыватель.
↳ «Сохранить имена зон прохода»	Сохраняет переименованные зоны в файл-шаблон для последующего использования.
↳ «Выбрать все зоны прохода»	Активирует все чекбоксы в таблице зон.
↳ «Снять выбор со всех зон прохода»	Деактивирует все чекбоксы.
↳ «Битовая строка»	Позволяет ввести маску зон в виде 64-битной последовательности (0 и 1).
↳ «Длительность управляющего импульса»	Время, на которое считыватель подает напряжение (для электромеханического замка) или снимает напряжение

(секунд)»	(для электромагнитного).
↳ «Тип замка»	Выберите тип запирающего устройства: «Электромеханический» или «Электромагнитный».

3.4.3. Порядок настройки системы


Для перевода системы в режим «Зоны прохода» необходимо выполнить три шага:

- Создать мастер-карты.
- Перевести считыватель в защищенный режим.
- Записать карты пользователей.

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

Для создания мастер-карт в режиме «Зоны прохода» выполните общую процедуру, описанную в разделе [2.3.2.7 «Создание мастер-карт»](#).

Особенности для данного режима:

Особенность	Описание
Поддерживаемые карты	Mifare Plus (SE, S, X).
Максимальное количество	Не более 5 мастер-карт за один раз.
 Защита от реконфигурации	<i>При активации опции «Защита от реконфигурации» (раздел 2.3.2.7) снять защиту со считывателя можно будет только с помощью этих же мастер-карт. При утере всех мастер-карт перенастройка считывателя станет невозможна.</i>
Сохраняемые настройки	На мастер-карту записываются: код объекта, выбранные зоны прохода (битовая маска), длительность импульса, тип замка, настройки Wiegand и цветовой схемы.

3.4.3.2. Перевод считывателя в режим «Зоны прохода»

Существует два способа перевода считывателя в защищенный режим. В обоих случаях необходимо наличие предварительно созданной мастер-карты. В первом варианте параметры конфигурации задаются через интерфейс программного обеспечения, с мастер-карты копируется исключительно код объекта, во втором — путем извлечения всех данных из памяти мастер-карты.

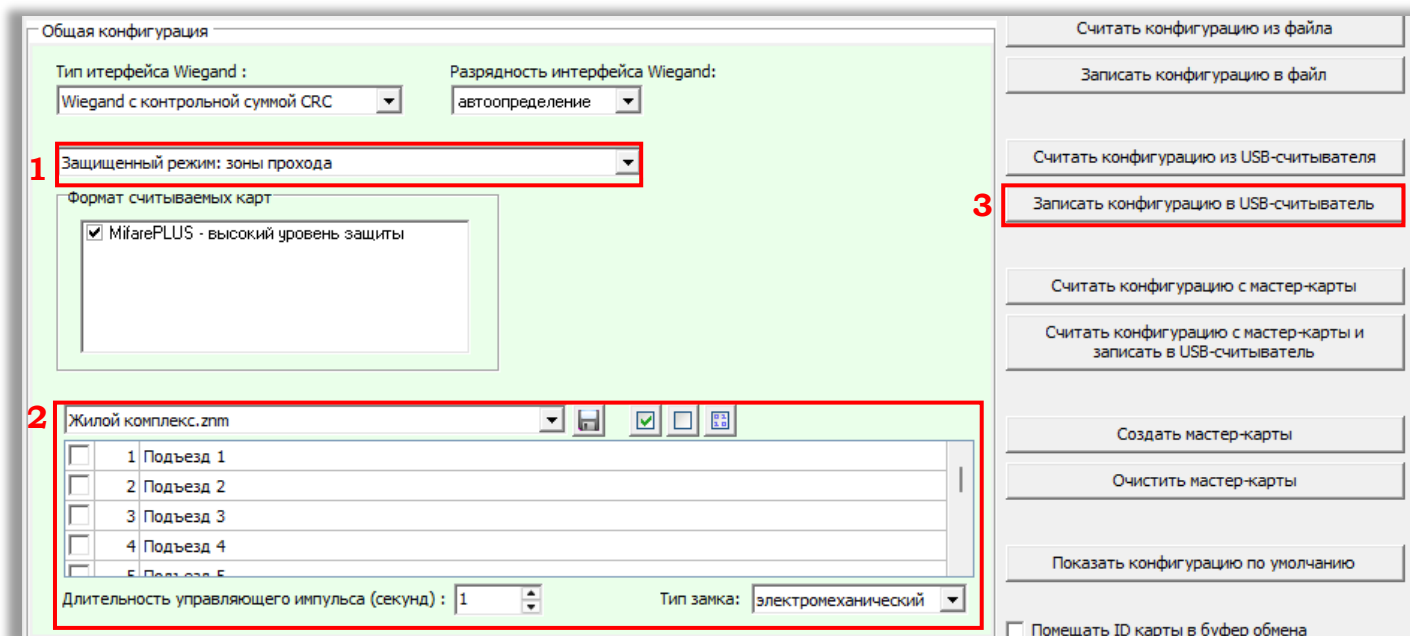
Вариант 1: Ручной ввод конфигурации

- Подключите считыватель к компьютеру.
- В программе выберите режим «**Защищенный режим: зоны прохода**».
- Настройте параметры интерфейса Wiegand.
- В параметрах раздела «**Зоны прохода**» выберите нужные зоны, настройте

длительность импульса и тип замка.

- Нажмите кнопку «**Записать конфигурацию в USB-считыватель**».
- В появившемся диалоговом окне нажмите «**Да**».
- Приложите ранее созданную мастер-карту к считывателю для копирования кода объекта.

Рисунок 25. Основные параметры для настройки считывателя на работу в режиме "Зоны прохода".




Вариант 2: Копирование конфигурации из мастер-карты

- Подключите считыватель к компьютеру.
- Нажмите кнопку «**Считать конфигурацию с мастер-карты и записать в USB-считыватель**».
- Приложите мастер-карту к считывателю.
- После завершения операции считыватель переведен в режим «Зоны прохода» со всеми настройками, сохраненными на мастер-карте.
- Если требуется изменить зоны для данного считывателя, нажмите «**Считать конфигурацию из USB-считывателя**», выберите нужные зоны и нажмите «**Записать конфигурацию в USB-считыватель**» (для записи конфигурации потребуется ранее созданная мастер-карта с заданным кодом объекта).

3.4.3.3. Запись карт пользователей

Для записи пользовательских карт выполните общую процедуру, описанную в разделе [2.4.1 «Кнопка «Создать защищенные карт»»](#).

 *Карты, не сконфигурированные как «защищенные» в программе «Конфигуратор считывателей «ЭРА», не будут восприниматься считывателями, работающими в защищенном режиме.*

3.4.4. Примеры использования

Пример организации контроля доступа в жилом комплексе.

Сценарий:

Жилой комплекс состоит из 20 подъездов, огражден забором с калитками. Необходимо разграничить доступ: жители имеют право проходить в свой подъезд и через калитки, а обслуживающий персонал — во все зоны.

Решение:

Шаг	Действие	Результат
1. Создание мастер-карт	В программе выберите режим «Зоны прохода». Настройте параметры Wiegand, длительность импульса (например, 2 сек) и тип замка. Нажмите «Создать мастер-карты». Создайте 2-3 мастер-карты.	Созданы мастер-карты с уникальным кодом объекта и конфигурацией.
2. Настройка считывателей на подъездах	Для каждого подъезда: подключите считыватель к компьютеру, выберите режим «Зоны прохода», в таблице зон отметьте только одну зону (например, для подъезда №1 — зону 1, для подъезда №2 — зону 2 и т.д.). Настройте длительность импульса и тип замка. Нажмите «Записать конфигурацию в USB-считыватель», приложите мастер-карту.	Считыватель на подъезде №1 открывает дверь только тем картам, у которых в маске зон установлен флажок зоны 1.
3. Настройка считывателей на калитках	На калитках настройте считыватели аналогично, но в таблице зон отметьте зону 21 (или любую другую, выделенную для калиток).	Считыватель на калитке открывает проход только тем картам, у которых в маске зон установлен флажок зоны 21.
4. Запись карт жителей	Перейдите на вкладку «Защищенные карты». Отметьте флажками зоны, которые будут разрешены жителю (например, зона 1 и зона 21). Нажмите «Создать защищенные карты», приложите мастер-карту, затем — карту жителя.	Карта жителя подъезда №1 открывает и его подъезд, и калитки.
5. Запись карт обслуживающего персонала	Аналогично, но отметьте флажками все зоны (от 1 до 21).	Карта сотрудника открывает все подъезды и все

КАЛИТКИ.

Результат:

Система работает автономно. Каждый считыватель сам проверяет права доступа по маске зон на карте. База карт не ведется, добавление нового жителя не требует синхронизации с считывателями.

3.4.5. Важные замечания

<i>Замечание</i>	<i>Пояснение</i>
Совместимость оборудования	Программное переключение типа замка поддерживается только для считывателей «ЭРА-MF v2» с микросхемой версии 0.95. Для более ранних версий требуется специальная плата.
Максимальное количество зон	Не более 64 зон.
Формат передачи данных	В режиме «Зоны прохода» считыватель передает в систему (по Wiegand или USB) битовую маску разрешенных зон.
Отсутствие преобразований	Параметры раздела «Преобразование» (обратный порядок байт, битовый сдвиг, число значимых бит, хеш-функция) в данном режиме недоступны.
Обратная совместимость	Карты, подготовленные для режима «Зоны прохода», не будут корректно работать в считывателях, настроенных на обычный режим чтения UID или с другим кодом объекта (и наоборот).
Изменение режима	Смена режима работы считывателя после того, как карты уже выданы пользователям, может привести к невозможности идентификации ранее выданных карт.
Шаблоны имен	Сохраненные шаблоны с пользовательскими именами зон необходимо хранить в папке с программой «Конфигуратор считывателей «ЭРА».

3.4.6. Краткое резюме

Режим «Зоны прохода» позволяет считывателю самостоятельно управлять замком, проверяя права доступа по битовой маске зон, записанной на карте пользователя.


Поддерживаемые карты: Mifare Plus (SE, S, X).

Основные параметры настройки:

- Таблица зон — выберите зоны, которые будет обслуживать считыватель (до 64).
- «Длительность управляющего импульса» — время открытия замка (0,3–30 секунд).
- «Тип замка» — электромеханический или электромагнитный.

Для настройки системы:

- Создайте мастер-карты (раздел [2.3.2.7. «Кнопка «Создать мастер-карты»](#)).
- Переведите считыватель в режим (раздел [3.4.3.2. «Перевод считывателя в режим «Зоны прохода»](#)).
- Запишите карты пользователей на вкладке «Защищенные карты», отметив нужные зоны (раздел [2.4.1. Кнопка «Создать защищенные карты»](#)).

 Программное переключение типа замка поддерживается только для считывателей «ЭРА-MF v2» с микросхемой версии 0.95. Для более ранних версий требуется специальная плата.