ЭРА НОВЫХ ТЕХНОЛОГИЙ

ДОСТУП ПОД КОНТРОЛЕМ

www.entpro.ru

Руководство по эксплуатации

Считыватель бесконтактных карт «ЭРА-MF»

Сделано в России

Редакция от 03.12.2024 г.

EAC

SEC.RU | Короткий путь к информации

Скачано с sec.ru

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ 2
2. ОБЩЕЕ ОПИСАНИЕ СЧИТЫВАТЕЛЯ 2
2.1. Настенные считыватели «ЭРА» 2
2.1.1. Считыватель «ЭРА-MF» 2
2.1.2. Считыватель «ЭРА-MF+» 3
2.1.3. Основные компоненты 3
2.1.4. Комплектация 3
2.1.5. Принцип работы 3
2.1.6. Формат идентификаторов 4
2.1.7. Режимы работы считывателя 4
2.1.8. Световая и звуковая индикация считывателя 4
3. ОПИСАНИЕ РЕЖИМОВ РАБОТЫ СЧИТЫВАТЕЛЯ 5
3.1. Защищенный режим: код объекта 5
3.2. Защищенный режим: чтение кода из блока 7
3.3. Защищенный режим: зоны прохода 8
4. ДОПОЛНИТЕЛЬНО 9
4.1. Руководство пользователя «Конфигуратор считывателей «ЭРА» 9
4.2. Программа «Конфигуратор считывателей «ЭРА» 9
4.3. Программа «ЭНТ Сервис» для ОС Android 9
4.4. Программа «ЭНТ Доступ» для ОС Android 9
5. ОБОЗНАЧЕНИЯ, ТЕРМИНЫ И СОКРАЩЕНИЯ 10
5.1. Условные обозначения, принятые в руководстве 10
5.2. Список принятых сокращений 10

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1. ВВЕДЕНИЕ

Уважаемый покупатель!

Компания «Эра новых технологий» благодарит вас за выбор нашего изделия. Мы стремимся обеспечивать высокий уровень безопасности и удобства эксплуатации — надеемся, что наше решение оправдает ваши ожидания. Мы ценим ваше доверие и готовы оказать техническую поддержку на всех этапах эксплуатации. Контактная информация службы поддержки представлена в конце каждой страницы руководства пользователя.

2. ОБЩЕЕ ОПИСАНИЕ СЧИТЫВАТЕЛЯ

RFID-считыватель, используемый в системах контроля и управления доступом (СКУД), является наиболее распространённым в Российской Федерации типом считывающих устройств. Это обусловлено тем, что данный протокол поддерживается большинством выпускаемых и реализуемых в стране proximity-карт и брелоков.

RFID-считыватель — это техническое устройство, предназначенное для считывания уникальных идентификационных данных с RFID-ключей (карт, брелоков, браслетов и других носителей информации) с использованием технологии радиочастотной идентификации. В зависимости от подключения считывателя, считываемые данные передаются в контроллер или программное обеспечение для последующей обработки.

Технология радиочастотной идентификации (RFID) обеспечивает дистанционный доступ к информации без необходимости физического контакта, что значительно упрощает процесс контроля прохода в помещения, на охраняемые территории и авторизацию в компьютерных системах.

Считыватель карт стал, пожалуй, самым популярным и известным компонентом СКУД. Именно с ним пользователи взаимодействуют чаще всего.

2.1. Настенные считыватели «ЭРА»

Как правило, они устанавливаются непосредственно на точках прохода — возле дверей, ворот, на турникетах и т. д.

Настенные считыватели «ЭРА» поставляются в двух вариантах: «ЭРА-MF» и «ЭРА-MF+».

2.1.1. Считыватель «ЭРА-MF»

Считыватели подключаются к контроллеру по проводному интерфейсу связи Wiegand. Принцип работы считывателей предусматривает считывание информации, закодированной в RFID-ключе, с последующей передачей полученных данных на контроллер, который осуществляет поиск и сравнение информации с базой данных. В результате выдается решение о разрешении либо запрете прохода.

Для настройки понадобится программа «Конфигуратор считывателей «ЭРА» или приложение «ЭНТ Сервис». Чтобы вместо ключа использовать телефон с технологией NFC, установите на него приложение «ЭНТ Доступ» для генерации уникального идентификатора.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.1.2. Считыватель «ЭРА-MF+»

Считыватель «ЭРА-MF+» выделяется среди классических решений для контроля доступа. Он сохраняет все технические характеристики и преимущества модели «ЭРА-MF», но дополнительно укомплектован отдельной миниатюрной платой для управления электромагнитным или электромеханическим замком. Плата разработана для работы считывателя в защищенном режиме «Зоны прохода». В этом режиме устройство самостоятельно решает, предоставлять доступ на территорию объекта или нет, без необходимости загружать ключи для разрешения прохода, в отличие от традиционных контроллеров. Это решение идеально для обеспечения доступа большого числа людей, например, на территорию жилого комплекса, с защитой от копирования ключей.

Система контроля доступа на базе считывателя «ЭРА-MF+» выделяется своей надежностью и простотой в обслуживании. Она не требует контроллеров, локальной сети или ведения базы данных. Новые ключи легко программируются за рабочим столом в офисе. Для этого понадобится компьютер, настольный считыватель «ЭРА-USB (MF/EM)» и программа «Конфигуратор считывателей «ЭРА». Также можно подключить устройство напрямую через USB-интерфейс к телефону с установленным приложением «ЭНТ Сервис».

2.1.3. Основные компоненты

Считыватель включает в себя следующие компоненты:

- Антенна: для приема и передачи радиосигналов.
- Микропроцессор: для обработки данных и выполнения команд.
- Память: для хранения данных и настроек.
- Интерфейсы связи: для подключения к другим компонентам системы (Wiegand, USB).
- Светодиод и бипер: для подачи светозвуковой индикации.
- Корпус

2.1.4. Комплектация

- Считыватель «ЭРА-MF»
- Паспорт изделия
- Плата управления замком LBRD 1.0 (комплектация «ЭРА-MF+»)

2.1.5. Принцип работы

Принцип работы заключается в следующем:

Считыватель постоянно генерирует электромагнитное поле.

Ключ (карта, брелок, метка), попадая в зону действия этого поля, получает энергию и активируется. Активировавшись, он передает считывателю свой уникальный идентификационный номер (UID).

Считыватель передает этот номер контроллеру, который сверяет его с базой данных и принимает решение: «открыть/не открыть».

Таким образом, существует два независимых канала для передачи данных:

Идентификатор — Считыватель: считывание данных с бесконтактной карты происходит по радиоканалу. Используется частота 13,56 МГц и формат карт Mifare.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Расстояние считывания до 10 метров при оптимальных условиях. Для обеспечения совместимости идентификатора со считывателем они должны поддерживать работу на одной частоте и совместимый протокол обмена данными (битность).

Считыватель — Контроллер: для связи считывателя с контроллером применяется проводной интерфейс Wiegand (от 8 до 66 бит). Для обеспечения совместимости считывателя с контроллером они должны иметь одинаковый проводной интерфейс связи и совместимый протокол обмена данными (битность). Максимальное расстояние для передачи данных по проводному интерфейсу связи Wiegand составляет до 100 метров при оптимальных условиях эксплуатации.

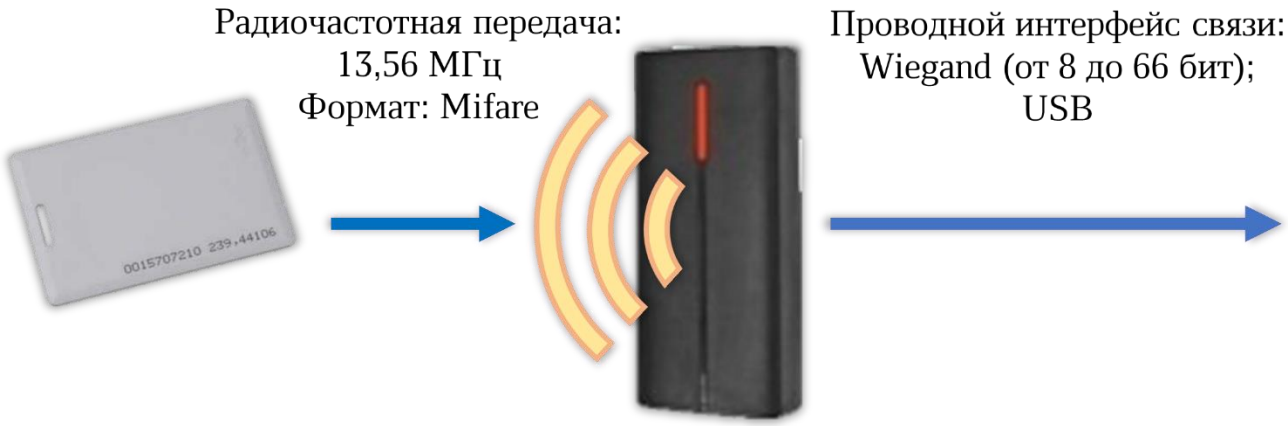

Рисунок 1 Принцип работы RFID-считывателя

2.1.6. Формат идентификаторов

- ISO 14443AUID – 4 байта;
- ISO 14443AUID – 7 байта;
- UID 8 байт телефона по технологии NFC (ОС Android);
- ISO 14443B – 4 байта;
- ISO 15693 ICODE – 8 байт;
- Чтение закрытых областей карт Mifare Classic, Mifare Plus S, Mifare Plus SE и Mifare Plus X;
- Банковские карты – 8 байт.

2.1.7. Режимы работы считывателя

- Незащищенный режим (без шифрования) — чтение UID ключа и/или телефона (только для ОС Android);
- Защищенный режим (с шифрованием):
  - Режим «Код объекта»;
  - Режим «Чтение кода из блока»;
  - Режим «Зоны прохода».

2.1.8. Световая и звуковая индикация считывателя

Индикация может работать по внутренней или внешней логике. При включении считыватель работает по внутренней логике. В случае, если был подан управляющий сигнал на контакты *LedG*, *LedR* или *Beep*, то считыватель переходит в режим управления внешними сигналами.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Работа индикации при управлении внешними сигналами предусматривает 4 цветовых режима:

1) Отсутствие управляющих сигналов на *LedG* и *LedR* (по умолчанию «синий»);
2) Присутствует только сигнал *LedG* (по умолчанию «зеленый»);
3) Присутствует только сигнал *LedR* (по умолчанию «красный»);
4) Присутствуют оба сигнала *LedG* и *LedR* (по умолчанию «оранжевый»);

Цвета по умолчанию могут быть изменены с помощью ПО. Возможно как поменять цвет, так и отключить индикацию в данном режиме вообще, выбрав черный. Данные изменения коснутся работы индикации как по внутренней, так и по внешней логике. Например, при работе по внутренней логике в режиме ожидания горит индикация «Режим 3». При успешном чтении включается «Режим 2» и т. д.

3. ОПИСАНИЕ РЕЖИМОВ РАБОТЫ СЧИТЫВАТЕЛЯ

3.1. Защищенный режим: код объекта

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

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

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

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

Рисунок 2 Таблица сравнения форматов

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

Для данного режима следует использовать карты, нигде ранее не использованные и находящиеся в так называемом «транспортном состоянии» (в этом состоянии находятся карты при выходе с завода-изготовителя). Этот момент важен, так как система конфигурирует карты самостоятельно и переводит их из «транспортного состояния» в режим SL3. Карты, переведенные в режим SL1, SL2, SL3 считывателями другого производителя, использоваться в данном режиме уже НЕ смогут (т. к. при этом будут использованы неизвестные системе коды доступа, а перевод обратно в

SEC.RU | Короткий путь к информации Скачано с sec.ru

транспортный режим невозможен)! Также следует отметить, что при переводе считывателем карт в режим SL3 устанавливается Random UID. Т. е. карта будет выдавать каждый раз разный UID размером 4 байта при поднесении к считывателям, работающим только по UID. Это позволяет «обезличить» бесконтактные карты для любых сторонних систем. Как в случае Mifare Classic, так и в случае Mifare Plus используется механизм диверсификации ключей. Это означает, что в каждой бесконтактной карте будут свои ключи для доступа к закрытым областям, что также положительно сказывается на защищенности системы. Подбор ключа для одной карты позволит скопировать только данную карту и не будет действителен для других карт.

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

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

Если вы используете защищённый режим код-объекта с картами формата Mifare Classic, обратите внимание на следующие важные моменты:

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

В частности, с такими мастер-картами вы не сможете снять защиту со считывателя, если эта опция была активирована при их создании. Также не будет доступна функция «Считать конфигурацию с мастер-карты и записать её в считыватель».

Поэтому мы рекомендуем использовать как минимум одну мастер-карту на основе Mifare Plus. Это позволит вам иметь больше возможностей при работе с системой и, при необходимости, снять защиту со считывателя.

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

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

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

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

создать другую мастер-карту (кроме уже созданных) с таким кодом невозможно!

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

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

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

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

Подробное описание настройки системы в режиме «код объекта» указано в «Руководстве пользователя «Конфигуратор считывателей «ЭРА»

3.2. Защищенный режим: чтение кода из блока

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

При чтении настроек с мастер-карты пользователю будет выводиться контрольная

SEC.RU | Короткий путь к информации Скачано с sec.ru

сумма кода доступа к блоку, чтобы исключить его несанкционированное копирование.

Подробное описание настройки системы в режиме «чтение кода из блока» указано в «Руководстве пользователя «Конфигуратор считывателей «ЭРА».

3.3. Защищенный режим: зоны прохода

В этом режиме считыватель «ЭРА-MF» выполняет функцию контроля доступа. Отличительной особенностью такого режима является отсутствие необходимости в базе бесконтактных карт, что в некоторых случаях может быть весьма удобно. Например, этот режим прекрасно подходит для больших жилых комплексов, где ведение БД затруднительно, и часто используются контроллеры в режиме автозаписи. Давайте более подробно рассмотрим особенности этого режима.

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

Данный режим так же, как и первый защищенный режим, использует понятие кода объекта. Код объекта генерируется при создании мастер-карт (от 1 до 5 штук). На этапе конфигурирования системы в считыватели записывается код объекта и соответствующие данному объекту зоны прохода. Таким образом, в нашем примере получится, что у каждого подъезда будут стоять считыватели, у которых будет прописана одна зона, соответствующая конкретному подъезду (например, с 1 по 20). Считыватели на калитках будут иметь разрешенную зону 21.

При формировании карт пользователей оператор может выбрать, в какие зоны будет разрешен доступ обладателю этой карты. В данном примере каждому жителю будет разрешен доступ в две зоны – в его подъезд и калитки. Работникам коммунальных служб можно разрешить доступ во все зоны. При поднесении карты считыватель смотрит, какие зоны записаны на карте, и если хотя бы одна совпадает с зонами, прописанными в нем, то он разрешает проход.

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

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

Внимание! Данный режим работы считывателя «ЭРА-MF» возможен только при наличии платы LBRD 1.0 (входит в состав «ЭРА-MF+»).

Подробное описание настройки системы в режиме «Зоны прохода» указано в «Руководстве пользователя «Конфигуратор считывателей «ЭРА».

SEC.RU | Короткий путь к информации Скачано с sec.ru

4. ДОПОЛНИТЕЛЬНО

4.1. Руководство пользователя «Конфигуратор считывателей «ЭРА»

4.2. Программа «Конфигуратор считывателей «ЭРА»

4.3. Программа «ЭНТ Сервис» для ОС Android

4.4. Программа «ЭНТ Доступ» для ОС Android

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5. Обозначения, термины и сокращения

5.1. Условные обозначения, принятые в руководстве

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

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

– справочная информация, разъясняющая некоторые понятия системы.

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

5.2. Список принятых сокращений

СКУД – Система контроля и управления доступом.
ОС – Операционная система.
ПО – Программное обеспечение.
ПК – Персональный компьютер.
UID ключа – Уникальный идентификатор ключа.

SEC.RU | Короткий путь к информации Скачано с sec.ru