МИКРОКОНТРОЛЛЕР ДЛЯ ЭЛЕКТРОННЫХ БИЛЕТОВ С СЕКТОРНЫМ ДЕЛЕНИЕМ ПАМЯТИ

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

РЧ-ИНТЕРФЕЙС В СООТВЕТСТВИИ С ISO/IEC 14443A

- Бесконтактная передача данных.
- Рабочее расстояние между картой и антенной считывающего-записывающего устройства: до 100 мм (в зависимости от геометрии антенны и мощности считывающего-записывающего устройства).
- Рабочая частота: 13.56 МГц ±7 КГц.
- Скорость передачи данных: 106 кбит/с.
- Проверка целостности данных при передаче: 16-битовая контрольная сумма (CRC), проверка на четность.
- Алгоритм антиколлизии.
- Уникальный 7-байтовый серийный номер (каскадный уровень 2, соответствующий ISO/IEC 14443-3).

ЭСППЗУ

- 1 Кбайт ЭСППЗУ для хранения данных, организованных в виде 16 секторов по 4 страницы. Каждая страница содержит 16 байт данных.
- Задаваемые пользователем права доступа для каждой страницы данных.
- Сохранность данных: 5 лет.
- Не менее 10000 циклов перезаписи.

БЕЗОПАСНОСТЬ

- 7-байтовый уникальный серийный номер, записанный в каждый контроллер при поставке с возможностью перехода к 4-байтному серийному номеру, случайному или полученному на основе 7-байтового.
- Трехэтапная аутентификация для доступа к сектору (в соответствии с ISO/IEC DIS 9798-2).
- Отдельная пара ключей для каждого сектора, обеспечивающая возможность использования одной карты сразу для нескольких областей применения.

ОБЩЕЕ ОПИСАНИЕ

Контроллер разработан в соответствии с ISO/IEC 14443A. Уровни протокола обмена соответствуют частям 2 и 3 стандарта ISO/IEC 14443A. Контроллер представляет собой специализированную ИС, в основном предназначенную для использования в бесконтактном проездном билете для проезда в общественной транспортной системе.

БЕСКОНТАКТНЫЙ ПЕРЕНОС ЭНЕРГИИ И ДАННЫХ

Контроллер не нуждается во внешнем или батарейном источнике питания. Подача энергии и передача данных на высокой скорости 106 кбит/с осуществляется посредством радиочастотного обмена, когда антенну контроллера помещают вблизи антенны считывающего устройства.

АЛГОРИТМ АНТИКОЛЛИЗИИ

Интеллектуальная функция антиколлизии позволяет считывающему устройству мгновенно обрабатывать более одной карты. Алгоритм антиколлизии позволяет осуществлять выбор каждой карты в отдельности. Он позволяет произвести транзакцию с одной выбранной картой таким образом, чтобы избежать помех, создаваемых другой картой, находящейся в поле.

Функция антиколлизии основывается на уникальном идентификационном (серийном) номере (UID) контроллера. Этот уникальный идентификатор (UID) контроллера имеет длину 7 байтов (возможен также выбор длины идентификатора 4 байта) и поддерживает каскадный уровень 2 в соответствии с ISO/IEC 14443-3.

ПРОЦЕДУРА ТРЕХЭТАПНОЙ АУТЕНТИФИКАЦИИ

Процедура трехэтапной аутентификации требует прохождения следующих этапов:

1) Считывающее устройство указывает сектор, к которому необходимо осуществить доступ и выбирает тип ключа, используемого при аутентификации (A или B). В ответ кристалл, если к сектору возможен доступ, посылает случайное число.

2) Считывающее устройство производит операцию шифрования, используя в качестве входных значений случайное число кристалла, собственное случайное число и ключ и посылает результат кристаллу.

3) Кристалл проверяет ответ считывающего устройства, производит операцию шифрования, используя в качестве входных значений случайное число считывающего устройства и ключ, и посылает результат считывающему устройству. Считывающее устройство проверяет ответ кристалла.

Везде входным значением также является серийный номер кристалла.

ФУНКЦИОНАЛЬНОЕ ОПИСАНИЕ

БЛОК-СХЕМА КОНТРОЛЛЕРА

Микросхема состоит из ЭСППЗУ, РЧ-интерфейса, ГСЧ и цифровых блоков. На Рис.1 представлена блок-схема контроллера. Энергия и данные передаются посредством антенны, содержащей в себе катушку с несколькими витками, напрямую подсоединенными к кристаллу. Необходимость во внешних компонентах отсутствует.

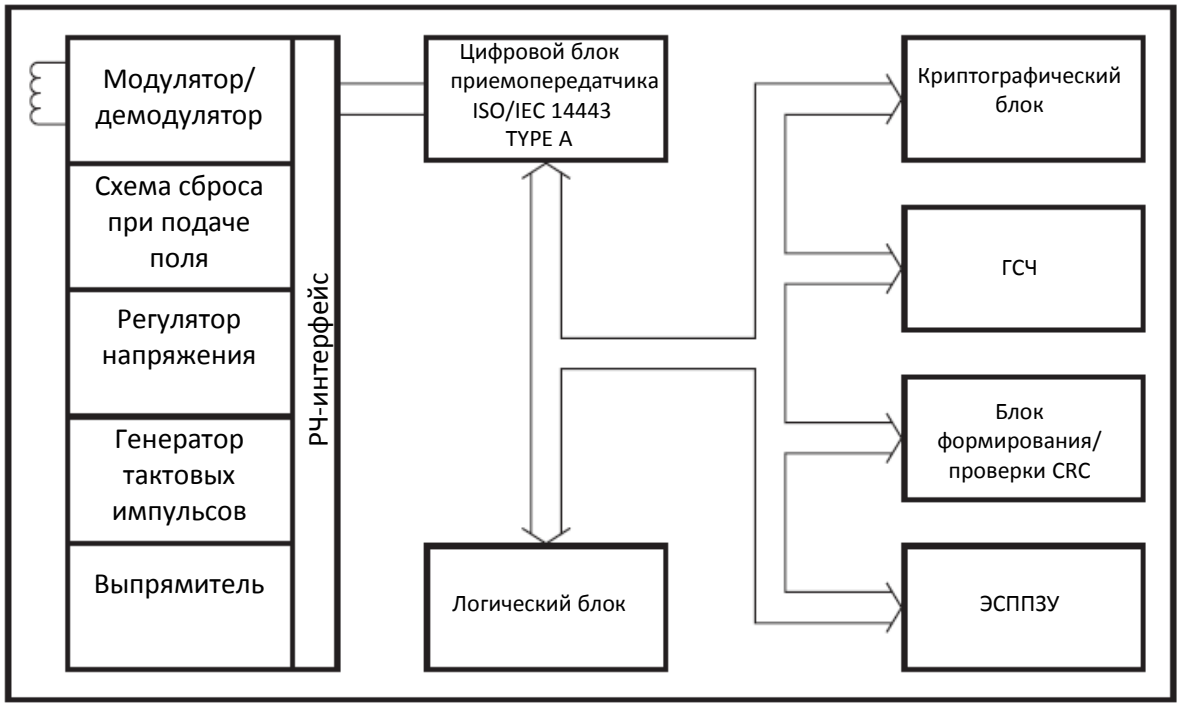


Рис. 1. Блок-схема контроллера

РЧ-ИНТЕРФЕЙС включает в себя:

- Модулятор/демодулятор
- Схему сброса при подаче поля
- Регулятор напряжения
- Схему генерации тактовых импульсов
- Выпрямитель

ЦИФРОВОЙ БЛОК ПРИЕМОПЕРЕДАТЧИКА ISO/IEC 14443 TYPE A служит для обработки команд и формирования ответа карты в соответствии с протоколом ISO/IEC 14443 TYPE A. В частности, данный блок обеспечивает возможность взаимодействия считывающего устройства с каждым кристаллом, внесенным в поле, в отдельности благодаря алгоритму антиколлизии.

КРИПТОГРАФИЧЕСКИЙ БЛОК служит для обеспечения процедуры трехэтапной аутентификации к выбранному сектору и последующего шифрования данных в ходе обмена считывающего устройства с кристаллом.

ЛОГИЧЕСКИЙ БЛОК обеспечивает проверку прав доступа и позволяет производить логические операции с целыми числами, хранимыми в ЭСППЗУ в специальном формате.

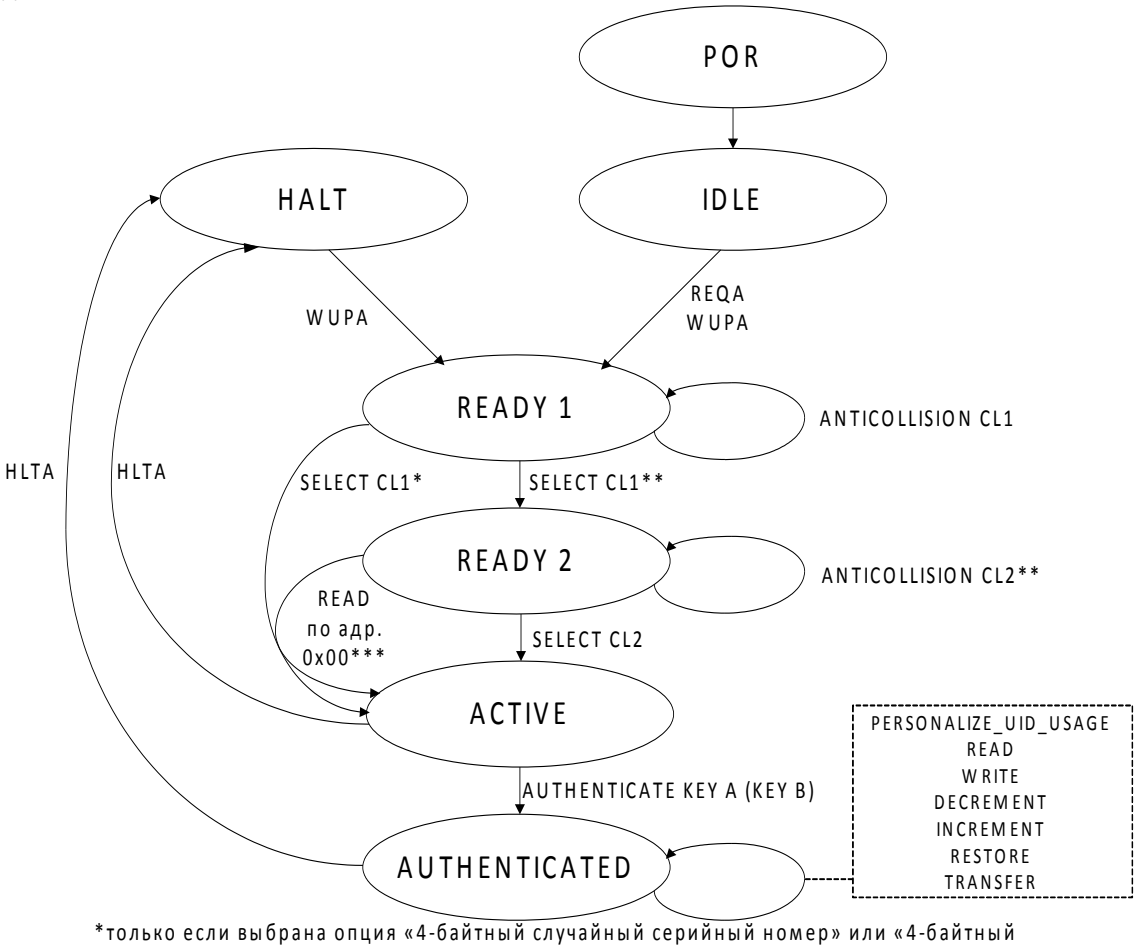
БЛОК ФОРМИРОВАНИЯ/ПРОВЕРКИ CRC служит для формирования и проверки циклического избыточного кода (Cyclic Redundancy Check, CRC), посылаемого вместе с кадрами данных и служащего для проверки их целостности.

ГСЧ (ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ) служит для генерации случайных чисел, используемых в процедуре аутентификации и для формирования случайного серийного номера.

ЭСППЗУ имеет объем 1 Кбайт и организован в виде 16 секторов по 4 страницы. Каждая страница содержит 16 байт. Последняя страница каждого сектора называется «заголовком» сектора и содержит два ключа и биты прав доступа для каждой страницы сектора, которые могут быть изменены пользователем после успешного прохождения процедуры аутентификации.

АЛГОРИТМ ФУНКЦИОНИРОВАНИЯ КОНТРОЛЛЕРА

Команды подаются считывающим устройством, затем они обрабатываются интерпретатором команд контроллера в соответствии с текущим состоянием, генерирующим необходимые сигналы ответа. На рис. 2 представлена диаграмма состояний контроллера. Все команды, требующие указания адреса страницы, подаваемые кристаллу в состоянии **[AUTHENTICATED]**, должны, для успешного их выполнения, содержать адреса страниц, относящихся к сектору, к которому произведена аутентификация. О выборе функциональных опций кристалла будет сказано далее.



*только если выбрана опция «4-байтный случайный серийный номер» или «4-байтный серийный номер, полученный на основе 7-байтного серийного номера»
**только если выбрана опция «7-байтный серийный номер номер» или «7-байтный серийный номер с дополнительным переходом между состояниями»
***только если выбрана опция «7-байтный серийный номер с дополнительным переходом между состояниями»

Рис. 2. Диаграмма состояний контроллера

Примечание: *во всех состояниях происходит переход кристалла в состояние IDLE или HALT, если принята любая другая команда, кроме указанной. Если кристалл ранее уже находился в состоянии HALT, в этом случае он перейдет в состояние HALT.*

СОСТОЯНИЯ КОНТРОЛЛЕРА

IDLE

Из состояния **[POR]** в результате сброса после подачи поля контроллер переходит в состояние **[IDLE]**. Контроллер выходит из этого состояния только после получения от считывающего устройства команды ***REQA*** или ***WUPA***. Любые другие данные, полученные в этом состоянии, интерпретируются как ошибка и контроллер остается в режиме **[IDLE]**.

Если ранее команда ***HLTA*** (“*Остановка*”) была выполнена правильно, то контроллер, при приеме неверной команды, переходит в состояние ожидания **[HALT]**, из которого он может быть выведен только командой ***WUPA***. Впоследствии, при получении неправильной команды в любом из состояний, контроллер будет переходить в состояние ожидания **[HALT]**, а не в состояние **[IDLE]**. Ответ на команду ***REQA*** или ***WUPA*** , выдаваемый картой, 2 байта 0x0044.

READY1

В этом состоянии контроллер позволяет считывающему устройству проводить первую стадию идентификации и получать 3 байта серийного номера идентификации контроллера по команде ***ANTICOLLISION CL1*** (“*Антиколлизия*”, каскадный уровень 1). Контроллер переходит из этого состояния в состояние **[READY2]** или **[ACTIVE]** (если выбран 4-байтный серийный номер) при получении команды ***SELECT*** (“*Выбрать*”) каскадного уровня 1 (SELECT Cascade Level 1, ***SELECT CL1***).

Любые другие команды, полученные в состоянии **[READY1]** (“*Готовность 1*”), интерпретируются как ошибка и контроллер переходит в состояние ожидания (**[IDLE]** или **[HALT]** в зависимости от его предыдущего состояния).

Ответ на команду ***SELECT CL1,*** выдаваемый картой, - байт 0x04 с 2 байтами CRC, если в кристалле выбрана функциональная опция «семибайтный серийный номер» и байт 0x08 с 2 байтами CRC, если в кристалле выбрана опция «четырехбайтный серийный номер». О том, как производить выбор функциональной опции кристалла, будет сказано далее.

READY2

Это состояние позволяет проводить вторую стадию идентификации контроллера и получать остальные 4 байта серийного номера идентификатора контроллера по команде ***ANTICOLLISION*** каскадного уровня 2. Переход из этого состояния в состояние **[ACTIVE]** происходит только в результате приема контроллером команды ***SELECT*** каскадного уровня 2 (SELECT Cascade Level 2, ***SELECT CL2***) или по команде ***READ*** (по адресу 0, переход возможен, только если выбрана функциональная опция «7-байтный серийный номер с дополнительным переходом между состояниями»).

Примечание*: При нахождении более чем одного контроллера в поле считывающего устройства, выполнение команды* ***READ*** *(по адресу 0) будет вызывать коллизию из-за различных серийных номеров контроллеров, но, несмотря на это, выбраны будут все контроллеры в поле.*

После выполнения команды ***SELECT*** каскадного уровня 2 единственно выбранным является контроллер, который прошел все стадии процедуры антиколлизии, и только этот контроллер будет продолжать поддерживать обмен данными со считывающим устройством, даже если другие бесконтактные устройства пребывают в поле считывающего устройства.

Любые другие команды, полученные в состоянии **[READY2]**, интерпретируются как ошибка, и контроллер переходит в состояние ожидания (**[IDLE]** или **[HALT]** в зависимости от предыдущего состояния).

Ответ на команду ***SELECT CL2,*** выдаваемый картой, - байт 0x08 с 2 байтами CRC.

ACTIVE

Над кристаллом, находящимся в активном **[ACTIVE]** состоянии, возможно проведение процедуры аутентификации. Правильный способ выведения контроллера из этого состояния – исполнение команды ***HLTA, AUTHENTICATE KEY A, AUTHENTICATE KEY B***. Любые другие команды, принятые в этом состоянии, интерпретируются как ошибка и контроллер переходит обратно в состояние ожидания (**[IDLE]** или **[HALT]** в зависимости от предыдущего состояния).

HALT

Состояние **[HALT]**, как и состояние **[IDLE]**, - это другое состояние ожидания, реализованное в контроллере. Контроллер, с которым считывающее устройство уже завершило обмен данными, может быть введен в это состояние командой ***HLTA***. Это состояние помогает считывающему устройству обнаруживать находящиеся в поле устройства, с которыми еще не производился обмен данными. Единственный путь выведения контроллера из состояния **[HALT]** – передача ему команды ***WUPA***.

Любые другие данные, полученные в этом состоянии, интерпретируются как ошибка, что оставляет контроллер в этом состоянии.

AUTHENTICATED

В этом состоянии возможен доступ ко всем страницам ЭСППЗУ, находящихся в секторе, к которому произведена аутентификация, с правами доступа, заданными для текущего сектора.

Выход из данного состояния может быть осуществлен путем подачи команды ***HLTA,*** или любой другой команды, кроме команд, указанных на диаграмме состояний контроллера на рис. 2 для данного состояния, или команды, содержащей ошибку.

ЦЕЛОСТНОСТЬ ДАННЫХ

Для обеспечения надежной передачи данных между считывающим устройством и контроллером по каналу бесконтактного сообщения, используются следующие механизмы:

- 16-битовый циклический избыточный код (Cyclic Redundancy Check, CRC) для каждого передаваемого блока
- Контрольные биты четности для каждого байта
- Проверка количества битов
- Побитовое кодирование для различения “единиц”, “нулей” и “отсутствия информации”
- Мониторинг канала передачи (анализ принимаемых команд протокола, анализ принимаемого битового потока)

РЧ-ИНТЕРФЕЙС

РЧ-интерфейс контроллера соответствует ISO/IEC 14443A.

Радиочастотное поле от считывающего устройства должно присутствовать постоянно (с короткими паузами в ходе передачи) поскольку оно служит в качестве источника питания контроллера.

Как в случае передачи данных от считывающего устройства контроллеру, так и в обратном направлении, требуется передача стартового бита в начале каждого кадра передачи. После каждого байта контроллером и считывающим устройством передается бит четности (инверсия операции «исключающее ИЛИ» над всеми битами одного байта). Максимальная длина кадра, передаваемого в любом из направлений, - 163 бита (16 байт данных + 2 байта CRC = 16*9 + 2*9 + 1 стартовый бит).

Первым всегда передается младший значащий бит байта. Если осуществляется подача контроллером нескольких байт страницы памяти, первым всегда подается младший значащий байт.

ОРГАНИЗАЦИЯ ЭСППЗУ

1024x8 бит ЭСППЗУ организованы в виде 16 секторов по 4 страницы в каждом. Каждая страница содержит 16 байт данных. Структура ЭСППЗУ приведена на рисунке 3.

Сектор	Номер страницы в секторе	Номер байта в странице																Адрес страницы
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
15	3	Ключ А						Биты доступа				Ключ В						0x3F
	2																	0x3E
	1																	0x3D
	0																	0x3C
14	3	Ключ А						Биты доступа				Ключ В						0x3B
	2																	0x3A
	1																	0x39
	0																	0x38
⋮	⋮																	⋮
1	3	Ключ А						Биты доступа				Ключ В						0x07
	2																	0x06
	1																	0x05
	0																	0x04
0	3	Ключ А						Биты доступа				Ключ В						0x03
	2																	0x02
	1																	0x01
	0	Серийный номер, данные производителя																0x00

Рис. 3. Структура памяти микроконтроллера

СЕРИЙНЫЙ НОМЕР ИДЕНТИФИКАЦИИ (UID)

Уникальный 7-байтный серийный номер (UID) и два байта его контрольной суммы запрограммированы в нулевой странице памяти контроллера (см. рис. 4). Если кристалл переведен в функциональный режим, предполагающий использование 4-байтного серийного номера для выбора кристалла, 4-байтный серийный номер либо формируется случайно, либо формируется кристаллом на основе 7-байтного серийного номера.

Также в нулевой странице запрограммированы данные производителя, используемые в качестве служебных данных. Нулевая страница ЭСППЗУ программируется в процессе производства и ее изменение невозможно в пользовательском режиме.

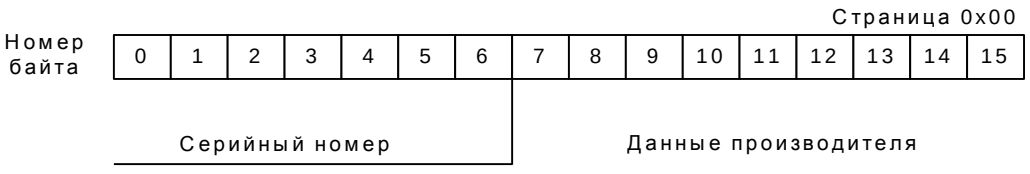


Рис. 4. Содержимое нулевой страницы ЭСППЗУ (нулевой сектор ЭСППЗУ)

В соответствии с ISO/IEC 14443-3 байт 0 (BCC0) контрольной суммы вычисляется как сумма по модулю 2 байта 0x88, байт 0, 1, 2 серийного номера. Байт 1 (BCC1) контрольной суммы вычисляется как сумма по модулю 2 байт 3-6 серийного номера. Байт 0 серийного номера используется для записи кода производителя в соответствии с ISO/IEC 14443-3 и ISO/IEC 7816-6 AMD.1.

СТРАНИЦЫ С ДАННЫМИ

Каждый сектор содержит 3 страницы для хранения данных пользователя, каждая из которых содержит 16 байт данных. Последняя страница сектора является заголовком сектора.

Страницы данных могут использоваться для хранения информации как в произвольном формате, так и в формате «целое число». Формат «целое число» может использоваться для приложения «электронный кошелек», в котором выполняются такие операции над данными, хранимыми в памяти, как «увеличить на заданное значение», «уменьшить на заданное значение».

Для любой операции с ЭСППЗУ требуется успешное прохождение процедуры аутентификации.

СТРАНИЦЫ В ФОРМАТЕ ЦЕЛОГО ЧИСЛА

Со страницами в формате целого числа можно выполнять следующие операции, выполняемые приложением «электронный кошелек»: чтение, запись, увеличение целого числа с загрузкой во внутренний регистр, уменьшение целого числа с загрузкой во внутренний регистр, загрузка целого числа во внутренний регистр, запись значения из внутреннего регистра в ЭСППЗУ.

Формат целого числа предполагает хранение целых чисел в формате, приведенном на рис. 5.

	Номер байта в странице															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Хранимое значение	V				$\overline{V}$				V				A	$\overline{A}$	A	$\overline{A}$

Рис. 5. Формат целого числа.

На рис. 5 V и A – произвольные 4-байтное и 1-байтное значения соответственно. $\overline{V}$ и $\overline{A}$ - побитная операция инверсии над V и A соответственно. V изменяется в арифметических операциях как целое число в формате дополнительного кода. Для обеспечения выявления нарушений целостности хранимого целого числа из-за сбоев при обмене информацией с кристаллом в ЭСППЗУ требуется сохранение двух дубликатов целого числа:

1) идентичного исходному числу
2) являющегося результатом побитной инверсии исходного числа.

При записи, считывании и выполнении операций увеличения и уменьшения значения целого числа, первым передается младший байт целого числа.

Поля A и $\overline{A}$ могут быть использованы для хранения однобайтного адреса. Адрес, хранимый в ЭСППЗУ, может быть использован для последующего восстановления данных в случае выявления нарушений целостности.

Значение 1234567 в десятичном формате, хранимое в странице с десятичным адресом 17, в формате целого числа имеет следующий вид:

0x 84D612007829EDFF84D6120011EE11EE

ЗАГОЛОВОК СЕКТОРА

Заголовок сектора – это страница с номером 3 внутри каждого сектора (страницы внутри сектора имеют номера с 0 по 3 включительно), т.е. каждая четвертая страница ЭСППЗУ (страницы с адресами 0x03, 0x07, …, 0x3F). Заголовок сектора содержит:

1) Ключи A (обязательный) и B (дополнительный)
2) Биты прав доступа для каждой страницы внутри сектора, к которому относится заголовок.

Если ключ B не используется, последние 6 байт могут быть использованы для хранения других данных. Байты 6 – 9 служат для хранения бит доступа для каждой страницы сектора. При чтении заголовка сектора вместо бит ключа A

кристалл всегда выдает нулевые биты. Ключ B также может быть скрыт от пользователя. Для этого необходимо задать право доступа к ключу B для операции чтения «никогда».

При поставке кристалла во все байты ключей A и B записывается значение 0xFF.

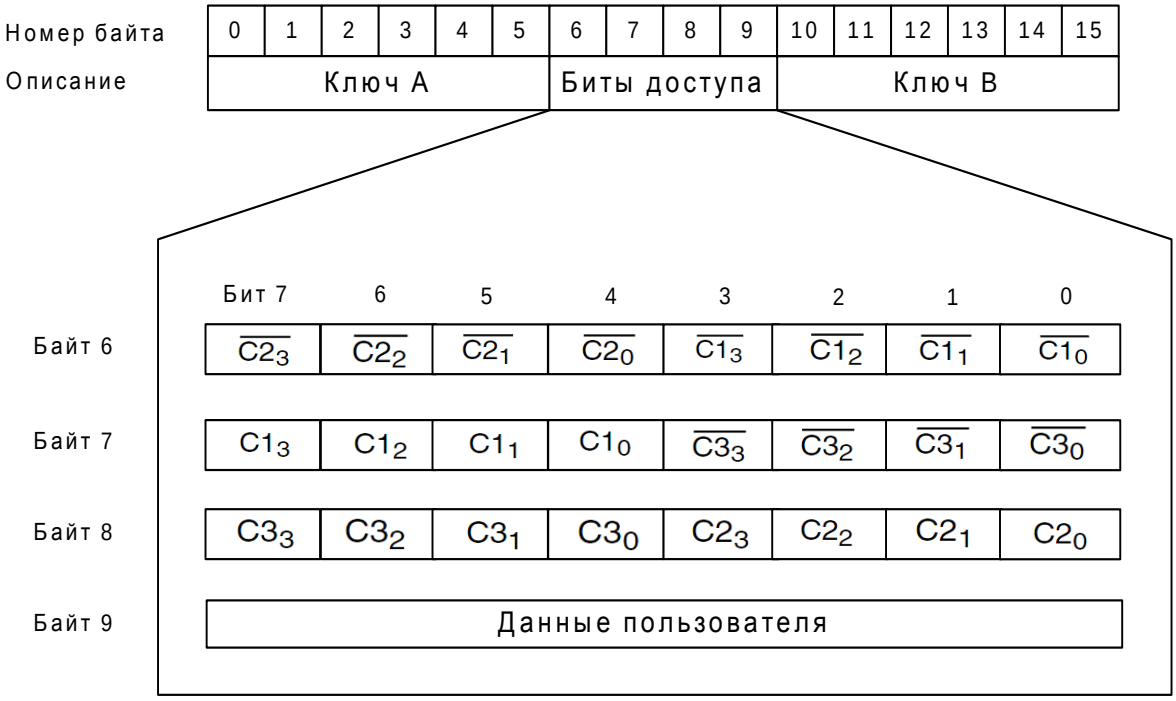


Рис. 6. Содержимое заголовка сектора

На рисунке 6 C1, C2, C3 – биты доступа для одной из страниц сектора. Индекс при C1, C2 или C3 – номер страницы сектора, для которой биты доступа задают права доступа. Если в заголовок сектора преднамеренно или в результате помех на линии связи биты доступа будут записаны в формате, отличном от приведенного на рисунке 6, это приведет к необратимой блокировке сектора, в результате которой аутентификация в сектор станет невозможна ни по одному из ключей.

В зависимости от значений бит доступа, хранимых в байтах 6-9 заголовка сектора, пользователю могут быть обеспечены различные варианты прав доступа, приведенные в таблицах 1 (права доступа для заголовка сектора) и 2 (права доступа для остальных страниц внутри сектора).

Таблица 1

Биты доступа			Тип и права доступа для области заголовка сектора						Примечание
			Ключ A		Биты доступа		Ключ B		
C1	C2	C3	READ	WRITE	READ	WRITE	READ	WRITE	
0	0	0	никогда	ключ A	ключ A	никогда	ключ A	ключ A	Ключ B может быть прочитан
0	1	0	никогда	никогда	ключ A	никогда	ключ A	никогда	Ключ B может быть прочитан
1	0	0	никогда	ключ B	ключ A|B	никогда	никогда	ключ B	
1	1	0	никогда	никогда	ключ A|B	никогда	никогда	никогда	
0	1	1	никогда	ключ A	ключ A	ключ A	ключ A	ключ A	Ключ B может быть прочитан
0	1	1	никогда	ключ B	ключ A|B	ключ B	никогда	ключ B	
1	0	1	никогда	никогда	ключ A|B	ключ B	никогда	никогда	
1	1	1	никогда	никогда	ключ A|B	никогда	никогда	никогда	

Таблица 2

Биты доступа			Тип обращения к карте и права доступа			
C1	C2	C3	READ	WRITE	INCREMENT	DECREMENT TRANSFER RESTORE
0	0	0	ключ A|B	ключ A|B	ключ A|B	ключ A|B
0	1	0	ключ A|B	никогда	никогда	никогда
1	0	0	ключ A|B	ключ B	никогда	никогда
1	1	0	ключ A|B	ключ B	ключ B	ключ A|B
0	0	1	ключ A|B	никогда	никогда	ключ A|B
0	1	1	ключ B	ключ B	никогда	никогда
1	0	1	ключ B	никогда	никогда	никогда
1	1	1	никогда	никогда	никогда	никогда

В таблицах 1 и 2 ***READ*** – операция чтения, ***WRITE*** – операция записи, ***INCREMENT*** – увеличение хранимого в странице целого числа на указанное значение с последующей записью результата во внутренний регистр, ***DECREMENT*** – уменьшение хранимого в странице целого числа на указанное значение с последующей записью результата во внутренний регистр, ***RESTORE*** – загрузка хранимого в странице целого числа во внутренний регистр, ***TRANSFER*** – запись хранимого во внутреннем регистре целого числа в страницу данных.

При поставке биты доступа C1, C2, C3 для заголовка каждого сектора имеют значения «001» (в двоичном формате), для всех страниц данных – значения «000» (в двоичном формате).

Если ключ B может быть прочитан (выделенные серым строки таблицы 1), то для всех страниц с данными сектора действуют права доступа, соответствующие значениям бит доступа C1, C2, C3 «111» в двоичном формате.

Если для страниц сектора заданы условия доступа «001» - такой кристалл может быть использован как билет с ограниченным числом поездок, поскольку возможно только уменьшение значения целого числа или его чтение.

Если для страниц сектора заданы условия доступа «110» - такой кристалл может быть использован как билет с ограниченным числом поездок, но с возможностью увеличения числа поездок после аутентификации только по ключу B.

ВРЕМЕННЫЕ ПАРАМЕТРЫ КРИСТАЛЛА

В зависимости от последнего бита, поданного считывающим устройством, время ответа кристалла может иметь либо одно, либо другое значение, также зависящее от команды, поданной кристаллу, как показано на рис. 8. На приведенном рисунке fc = 13,56 МГц.

Зависимость времени ответа от команды определяется значением n. Значение n для команд, не требующих выполнения операции записи в кристалл, равно 9. В этом случае время ответа (Frame Delay Time, FDT) составит ~91 мкс или ~87 мкс. Если в результате приема команды производится запись данных в ЭСППЗУ кристалла, n будет равно 400, что соответствует FDT = ~3,8 мс.

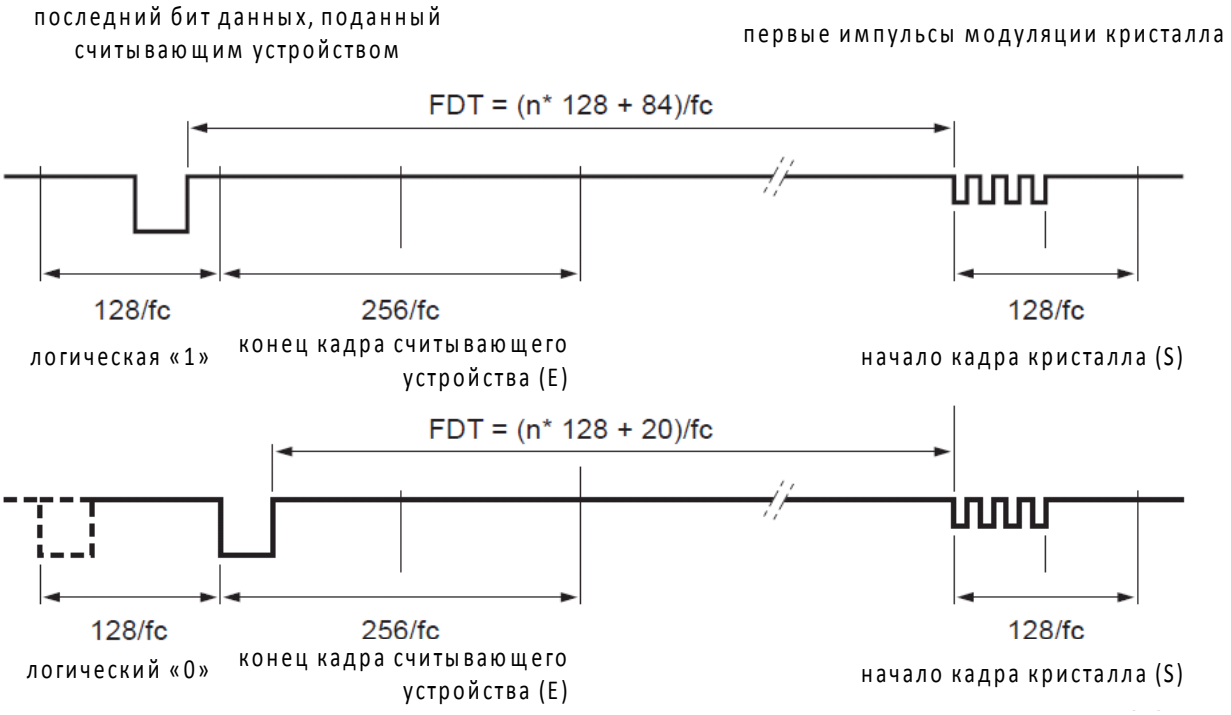


Рис. 8. Время ответа кристалла.

ОТРИЦАТЕЛЬНЫЕ И ПОЛОЖИТЕЛЬНОЕ ПОДТВЕРЖДЕНИЯ

Если кристаллом принят кадр, в котором обнаружена ошибка четности или ошибка CRC, кристалл отвечает четырехбитным отрицательным подтверждением 0x1. Кристалл ответит четырехбитным отрицательным подтверждением 0x2, если кристаллом принят кадр:

- содержащий не существующий в кристалле адрес;
- запроса на операцию, которая не выполнима при заданных правах доступа;
- команды ***INCREMENT***, ***DECREMENT***, ***RESTORE***, ***TRANSFER*** или ***WRITE***, содержащей в поле адреса нулевой адрес ЭСППЗУ;
- команды ***INCREMENT***, ***DECREMENT***, ***RESTORE***, ***TRANSFER*** или ***WRITE***, содержащей в поле адреса адрес страницы, расположенной вне сектора, к которому произведена аутентификация;
- запроса на операцию, которая приводит к результату арифметической операции, который не может быть сохранен в 4 байтах памяти;
- команды ***INCREMENT***, ***DECREMENT***, ***RESTORE*** с адресом страницы, в которой информация представлена не в формате целого числа.
- команды ***INCREMENT***, ***DECREMENT***, ***RESTORE***, ***TRANSFER*** или ***WRITE*** после аутентификации к сектору, заголовок которого представлен в неправильном формате (см. рис. 6)

Положительное подтверждение, выдаваемое кристаллом, 4 бита 0xA. Выдается кристаллом в ответ на любую команду, если не указано иное.

В случае некорректной записи в ЭСППЗУ кристалла кристалл вместо положительного подтверждения не выдает какого-либо ответа. Это происходит в результате автоматизированной проверки успешности операции записи, выполняемой кристаллом. После записи кристалл производит чтение по адресу записи и сравнивает записанное значение со значением, полученным в составе команды записи.

ФУНКЦИОНАЛЬНЫЕ ОПЦИИ КРИСТАЛЛА, ВЫБИРАЕМЫЕ ПОЛЬЗОВАТЕЛЕМ

Хотя кристалл содержит 7-байтный уникальный серийный номер, хранимый в 0 странице ЭСППЗУ, пользователем может быть выбрана одна из 4-х функциональных опций, влияющих на процедуру выбора кристалла при помощи его серийного номера:

1) 7-байтный серийный номер
2) 7-байтный серийный номер с дополнительным переходом между состояниями
3) 4-байтный случайный серийный номер
4) 4-байтный серийный номер, полученный на основе 7-байтного серийного номера

Выбор кристалла и процедура антиколлизии для опций с 4-байтным и 7-байтным серийным номером производится в соответствии с частью 3 стандарта ISO 14443. Опция, установленная для кристалла при поставке, опция 1.

Выбор функциональной опции кристалла осуществляется путем подачи кристаллу команды ***PERSONALIZE_UID_USAGE***. Данная команда может быть подана кристаллу только один раз, и впоследствии кристалл отвечает на команду отрицательным подтверждением и не выполняет ее.

Строго рекомендуется подавать данную команду при записи первоначальных данных в кристалл, даже если планируется использовать функциональную опцию 1 (выбранную по умолчанию). Это позволит избежать нежелательного изменения опции в случае помех в РЧ-поле. Новая функциональная опция становится активна только после сброса поля вблизи кристалла (вынесения и повторного внесения кристалла в поле).

Кадр команды ***PERSONALIZE_UID_USAGE*** содержит, в порядке их подачи, следующие байты: код команды, код опции, 2 байта CRC. Код опции 0x00 – для опции 1, 0x40 для опции 2, 0x20 – для опции 3, 0x60 – для опции 4.

ИСПОЛЬЗОВАНИЕ СЕРИЙНОГО НОМЕРА В ПРОЦЕДУРЕ АУТЕНТИФИКАЦИИ К СЕКТОРУ

Для опции 1 в качестве входных данных для процедуры аутентификации используются байты 3-6 серийного номера. Для опции 2, если переход в **[ACTIVE]** произошел из состояния **[READY2]**, на вход блока шифрования также подаются байты 3-6 серийного номера. Для опции 2, если переход в **[ACTIVE]** произошел из состояния **[READY1]**, на вход блока шифрования подаются байт 0x88 и байты 0-2 серийного номера. Для опций 3 и 4 качестве входных данных для процедуры аутентификации используются байт 0x88 и байты 0-2 серийного номера (случайного или 4-байтного, полученного на основе 7-байтного).

ПРОЦЕДУРА АУТЕНТИФИКАЦИИ К СЕКТОРУ

В процедуре аутентификации к сектору, считывающее устройство инициирует аутентификацию, посылая команду ***AUTHENTICATE KEY A*** или ***AUTHENTICATE KEY B***. Кадр команды ***AUTHENTICATE*** содержит, в порядке подачи, следующие байты: код команды (в случае аутентификации по ключу B и по ключу A различен), адрес любой страницы выбранного сектора, 2 байта CRC. В ответ кристалл выдает кадр, содержащий 4-байтное случайное число и 2 байта CRC. Затем считывающее устройство посылает кристаллу свой 8-байтный шифр с 2 байтами CRC. Кристалл проверяет полученный шифр и в случае успешного результата проверки отвечает 4-байтным шифром с 2 байтами CRC. Если считывающее устройство выдает успешный результат проверки шифра кристалла, процедуру аутентификации можно считать успешно завершенной. Все данные, поданные кристаллу, находящемуся в состоянии **[AUTHENTICATED]** и выдаваемые им в ответ, шифруются ключевым потоком, сформированным в результате аутентификации.

ЧТЕНИЕ ИНФОРМАЦИИ ИЗ КРИСТАЛЛА

Чтение информации из кристалла осуществляется посредством подачи команды ***READ***. Кадр команды ***READ*** содержит, в порядке подачи, следующие байты: код команды, адрес любой страницы выбранного сектора, 2 байта CRC.

ЗАПИСЬ ИНФОРМАЦИИ В КРИСТАЛЛ

Может осуществляться путем подачи команд ***WRITE*** и ***TRANSFER.*** Если необходима запись произвольных данных, используется команда ***WRITE***, состоящая из 2-х кадров. Первый кадр команды ***WRITE*** содержит, в порядке подачи, следующие байты: код команды, адрес любой страницы выбранного сектора, 2 байта CRC. Второй кадр команды ***WRITE*** содержит, в порядке подачи, следующие байты: 16 записываемых байт, начиная с младшего значащего байта, 2 байта CRC.

Если необходим перенос целого числа, хранимого во внутреннем регистре кристалла, загруженного туда в результате выполнения кристаллом команды ***INCREMENT***, ***DECREMENT***, ***RESTORE***, необходимо использовать команду ***TRANSFER***. Кадр команды ***TRANSFER*** содержит, в порядке подачи, следующие байты: код команды, адрес любой страницы выбранного сектора, 2 байта CRC.

УВЕЛИЧЕНИЕ, УМЕНЬШЕНИЕ, СЧИТЫВАНИЕ ЦЕЛОГО ЗНАЧЕНИЯ С ЗАГРУЗКОЙ ВО ВНУТРЕННИЙ РЕГИСТР

Увеличение, уменьшение, считывание целого значения с загрузкой во внутренний регистр выполняется посредством подачи команд ***INCREMENT, DECREMENT, RESTORE*** соответственно. Каждая из команд ***INCREMENT, DECREMENT, RESTORE*** состоит из 2-х кадров. Первый кадр команды ***INCREMENT, DECREMENT,*** или ***RESTORE*** содержит, в порядке подачи, следующие байты: код команды (для каждого типа команды определен свой код команды), адрес любой страницы выбранного сектора, 2 байта CRC. Второй кадр команды ***INCREMENT, DECREMENT,*** или ***RESTORE*** содержит, в порядке подачи, следующие байты: 4 байта целого числа, на которое производится изменения значения, хранимого в ЭСППЗУ (для ***RESTORE*** – произвольны, ни для одной из команд не допустимо отрицательное значение), 2 байта CRC. На второй кадр команды ***INCREMENT, DECREMENT,*** или ***RESTORE*** кристалл не должен выдавать положительного подтверждения. Попытка выполнения арифметической операции с целым числом, приводящее к получению значения меньше минимального или больше максимального, которое может быть сохранено в 4 байтах в формате дополнительного кода, приводит к выдаче кристаллом отрицательного подтверждения 0x2.

ЭЛЕКТРИЧЕСКИЕ ПАРАМЕТРЫ

ПРЕДЕЛЬНО ДОПУСТИМЫЕ ЗНАЧЕНИЯ ПАРАМЕТРОВ

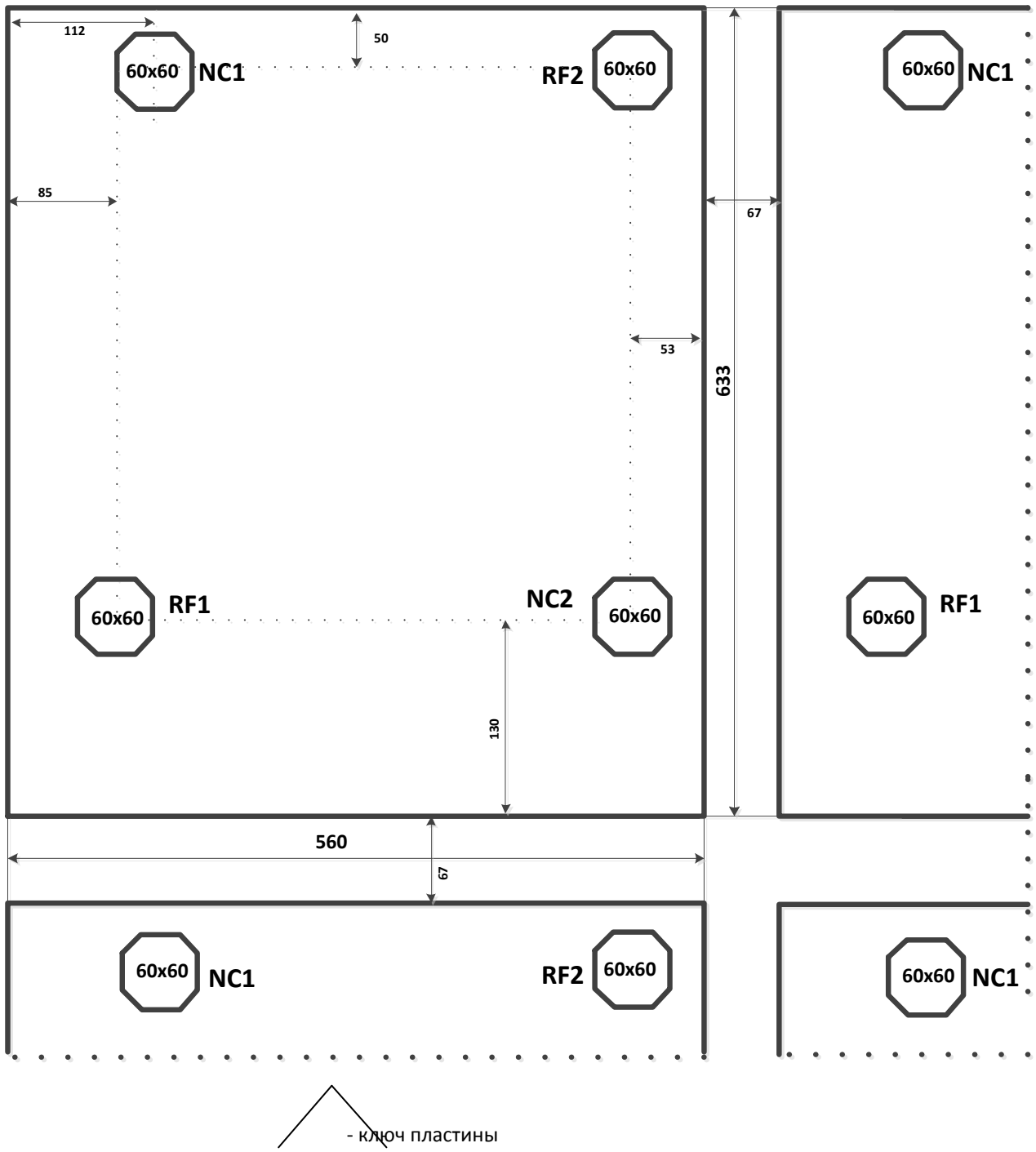
- Входной ток: не выше 30 мА
- Ток защелкивания: не ниже 100 мА
- Температура хранения: -40о до +125о С
- Защита от статического электричества: не ниже 2кВ

Таблица 3. Электрические и временные параметры

Параметр	Обозначение	Мин.	Тип.	Макс.	Единица
Рабочая частота	Fin	-	13.56 ± 7КГц	-	МГц
Входная емкость, T=22°C, Fin = 13.56 МГц, Vin = 2В	Cin	13	17.9	21	пФ
Время программирования ЭСППЗУ	Twr	-	4.0	-	мс

T = -25 до +70℃ (если не оговорено иным образом)

РАЗМЕР КРИСТАЛЛА И МЕСТОРАСПОЛОЖЕНИЕ КОНТАКТНЫХ ПЛОЩАДОК



RF1, RF2 –входы антенн
NC – не подсоединена

Рис.6. Размер кристалла и месторасположение площадок