КБ5004ХК3

БЕСКОНТАКТНОЕ РАДИОЧАСТОТНОЕ КРИПТОЗАЩИЩЕННОЕ ЭППЗУ 8К БИТ

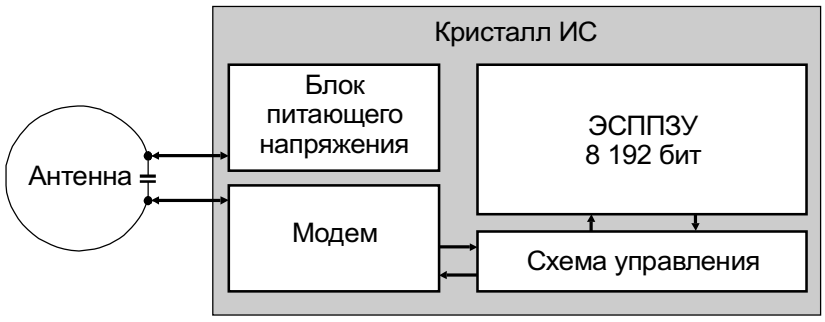
КБ5004ХК3 (**An5505**) – ИС бесконтактного **криптозащищенного** пассивного ответчика-идентификатора представляет собой электрически перепрограммируемое ПЗУ (ЭСППЗУ), считывание информации из которого и электропитание производятся по встроенному радиоканалу. Она является основой идентификатороа **КИБИК**, работающего на частоте 13,56 МГц. На ее основе могут быть построены идентификаторы в иных конструктивных исполнениях.

КБ5004ХК3 содержит 8 192 бит электрически перепрограммируемого ПЗУ. Встроенный радиоканал получает наведенный в антенне внешним излучением сигнал, который используется блоком питания для получения напряжения питания микросхемы и блоком управления как синхронизирующий сигнал. Шифратор преобразует информацию из ЭСППЗУ в соответствующие коды, а модулятор формирует и выдает ответный сигнал в антенну.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

- Состав:
  - ЭСППЗУ – 8 192 (16×512) бит
  - Блок управления
  - Блок питающего напряжения
  - Блок радиоканала (модем)
- 16 секторов, размером в 512 разрядов каждый, с индивидуальными правами доступа к сектору
- 2 ключа шифрования, размером в 48 разрядов, для доступа к каждому из 16 секторов
- Наличие процедуры антиколлизии
- Аутентификация с последующей шифрацией канала обмена
- Частота радиоканала – 13,56 МГц
- Скорость обмена – 106 кбод
- Циклов программирования – 100 000
- Дальность считывания (зависит от считывателя и условий его установки) – 0÷100 мм и более
- Электропитание при эксплуатации не требуется
- Обмен информацией по ISO 14443-2, тип А

СТРУКТУРНАЯ СХЕМА ИС



КОНСТРУКЦИЯ

ИС **КБ5004ХК3** изготовлена по КМОП технологии в виде кристалла. Поставляется ИС потребителю исключительно в составе бесконтактных идентификаторов.

ФУНКЦИОНИРОВАНИЕ

Обмен информацией со считывающим устройством производится согласно стандарту на бесконтактные карты ISO 14443-2 тип А.

Передача информации от считывающего устройства идентификатору осуществляется 100 % амплитудной модуляцией напряженности электромагнитного поля. Уменьшение амплитуды напряженности электромагнитного поля, излучаемого антенной считывающего устройства, до 5% от начального его значения на время, равное 2.34 мкс, формирует “паузу”. Для представления информации используется модифицированное кодирование Миллера.

Информация от считывающего устройства к карте посылается в виде команд, состоящих из последовательности разрядов, передаваемых младшим разрядом вперед. Каждый передаваемый байт сопровождается контрольным разрядом, в котором посылается результат проверки байта на четность. Для четного числа передаваемых единиц значение контрольного разряда равняется единице. В конце команды, как правило, передается циклический код, для проверки правильности передаваемой информации. Образующий полином – $X^{16} + X^{12} + X^5 + 1$. **КБ5004ХК3** при приеме осуществляет контроль правильности принятой команды. В случае несовпадения циклического кода выдается сообщение об ошибке. Аналогично, информация, передаваемая от **КБ5004ХК3** к считывающему устройству, сопровождается контрольными разрядами проверки на четность и таким же циклическим кодом. Считывающее устройство также производит контроль правильности полученной информации по совпадению циклического кода и проверки на четность каждого байта.

Организация памяти

Память **КБ5004ХК3** организованна в виде 16 секторов размером в 512 разрядов каждый. Нумерация секторов производится от нулевого сектора до пятнадцатого. Обращение к сектору возможно только после правильно исполненной команды аутентификации по одному из ключей данного сектора. Для доступа к сектору имеются два ключа: ключ А и ключ В, которые записываются при персонализации идентификатора.

Сектор состоит из четырех блоков, размером в 128 разрядов. Нумерация блоков производится от нулевого блока до третьего. Команды чтения, записи и работы со счетчиком работают с одним блоком. Последний третий блок в секторе имеет специальное назначение и называется служебным блоком сектора. В служебном блоке сектора размещаются две ключа аутентификации и разряды управления доступом к блокам сектора. Нулевой блок нулевого сектора доступен только по чтению и является блоком изготовителя. В блоке изготовителя записан серийный номер микросхемы, который уникален для каждой микросхемы, а также дополнительная информация изготовителя микросхемы.

Для удобства организации платежных приложений в **КБ5004ХК3** имеется 32-разрядный счетчик. Счетчик представляет собой регистр, который загружается содержимым специально сконфигурированного блока по команде загрузки счетчика. Для гарантии целостности данных информация для загрузки счетчика размещается в блоке три раза: в прямом виде, затем в инверсном виде и затем обратно в прямом виде. Оставшиеся разряды в блоке используются для хранения байта произвольной информации. Для гарантии целостности байт произвольной информации повторяется четыре раза: в прямом виде, в инверсном виде, в прямом виде и снова в инверсном.

Система команд

Как только идентификатор попадает в электромагнитное поле, излучаемое считывающим устройством, она переходит к ожиданию команды ЗАПРОС КАРТЫ (REQUEST). Все остальные команды, принятые **КБ5004ХК3**, игнорируются. Приняв команду ЗАПРОС КАРТЫ (REQUEST), **КБ5004ХК3** переходит к ожиданию приема следующей команды - АНТИКОЛЛИЗИЯ (ANTICOLLISION). Аналогично команде ЗАПРОС действует команда ЗАПРОС ВСЕХ (REQUEST ALL), но если на команду ЗАПРОС не реагируют идентификаторы, приведенные в состояние останова командой ОСТАНОВ (HALT), то на команду ЗАПРОС ВСЕХ (REQUEST ALL) реагируют все **КБ5004ХК3**, находящиеся в электромагнитном поле считывающего устройства.

Система команд

Команд	Время выполнения, мсек
ЗАПРОС КАРТЫ (REQUEST)	0.354
ЗАПРОС ВСЕХ (REQUEST ALL)	0.354
АНТИКОЛЛИЗИЯ (ANTICOLLISION)	0.713
ВЫБОР КАРТЫ (SELECT)	1.14
АУТЕНТИФИКАЦИЯ (AUTHENTICATION)	2
ЧТЕНИЕ БЛОКА (READ BLOCK)	2
ЗАПИСЬ БЛОКА (WRITE BLOCK)	6.2
ЗАГРУЗКА СЧЕТЧИКА (RESTORE)	1.3
УВЕЛИЧЕНИЕ СЧЕТЧИКА (INCREMENT)	1.3
УМЕНЬШЕНИЕ СЧЕТЧИКА (DECREMENT)	1.3
СОХРАНЕНИЕ СЧЕТЧИКА (TRANSFER)	4.63
ЗАВЕРШЕНИЕ РАБОТЫ (HALT)	0.5

Следует отметить, что в электромагнитном поле, излучаемом антенной считывающего устройства, может находиться несколько идентификаторов одновременно. В связи с этим возникает необходимость работы только с одним из них, выбранным для работы. Остальные **КБ5004ХК3**, которые не были выбраны, находятся в состоянии ожидания. Каждая **КБ5004ХК3** обладает уникальным серийным номером, присвоенным ей на этапе изготовления. Серийный номер размещается в блоке изготовителя и не может быть модифицирован. Для определения **КБ5004ХК3**, с которой можно начать сеанс работы, предназначена команда АНТИКОЛЛИЗИЯ (ANTICOLLISION). В результате проведения процедуры антиколлизии считывающее устройство будет знать серийный номер **КБ5004ХК3**, с которой можно начать работу. После определения этой **КБ5004ХК3** считывающее устройство подает команду ВЫБОР КАРТЫ (SELECT), и только та ИС, которая была выбрана в этой команде, будет воспринимать все последующие команды.

Секторы **КБ5004ХК3** защищены криптографически. Все команды чтения, записи и работы со счетчиком будут восприниматься **КБ5004ХК3** только после того как будет подана команда АУТЕНТИФИКАЦИЯ (AUTHENTICATION). После подачи команды аутентификации канал обмена информацией между считывающим устройством и **КБ5004ХК3** шифруется шифровальной последовательностью, выработанной в процессе выполнения команды АУТЕНТИФИКАЦИЯ (AUTHENTICATION).

Основные команды работы с идентификатором предназначены для работы с одним блоком. В каждой команде указывается адрес блока, с которым будет работать данная команда. Основные команды работы с блоком – это команды ЧТЕНИЕ БЛОКА (READ BLOCK) и ЗАПИСЬ БЛОКА (WRITE BLOCK).

Для работы со счетчиком введены специальные команды работы со счетчиком. Команда ЗАГРУЗКА СЧЕТЧИКА (RESTORE) загружает регистр счетчика содержимым блока, указанного в команде. Команды УВЕЛИЧЕНИЕ СЧЕТЧИКА (INCREMENT) и УМЕНЬШЕНИЕ СЧЕТЧИКА (DECREMENT) меняют содержимое регистра счетчика в сторону увеличения или уменьшения на величину, указанную в этих командах. Счетчик можно сохранить командой СОХРАНЕНИЕ СЧЕТЧИКА (TRANSFER) как в блоке, из которого было считано начальное значение счетчика, так и любом другом блоке сектора.

Для прекращения работы с идентификатором считывающее устройство должно подать команду ЗАВЕРШЕНИЕ РАБОТЫ (HALT). После приема этой команды **КБ5004ХК3** на все время нахождения идентификатора в зоне действия антенны считывателя переходит в состояние останова и не реагирует на команды, подаваемые считывающим устройством.

Апрель 2001 г.

103460, **МОСКВА,** Зеленоград, ОАО **АНГСТРЕМ**
т. (095) 531-49-06, т/ф. 532-96-21 • E-mail: market@angstrem.ru • http://www.angstrem.ru