КБ5004РР1

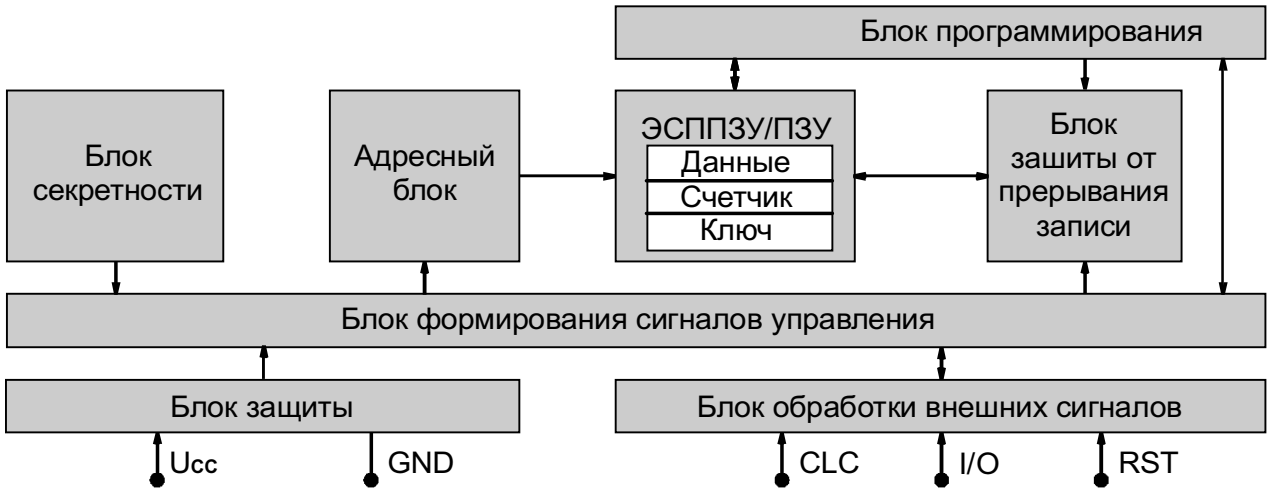
СЧЕТЧИК НА ЭСППЗУ 616 БИТ С ВЫСОКОЙ КРИПТОСТОЙКОСТЬЮ ДЛЯ ТАКСОФОННЫХ КАРТ ВТОРОГО ПОКОЛЕНИЯ

КБ5004РР1 (Аn5001) - ИС памяти 632 бит (16 бит - ПЗУ и 616 бит ЭСППЗУ) для таксофонных карт с встроенными средствами для аутентификации с высокой криптостойкостью.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

- ЭСППЗУ – 616 бит
- ПЗУ – 16 бит
- Граница счета счетчика – 29160
- Защита от прерывания записи
- Ключ модуля секретности – 256 бит
- Циклов программирования – 100 000
- Время программирования – 5 мс
- Время хранения информации – 10 лет
- Защита от статического электричества – 4000 V
- Порт по ISO 7816-3
- Питание – 5 В ± 10 %, < 5 мА
- Технология КМОП
- Рабочая температура – -65 ÷ +85°С

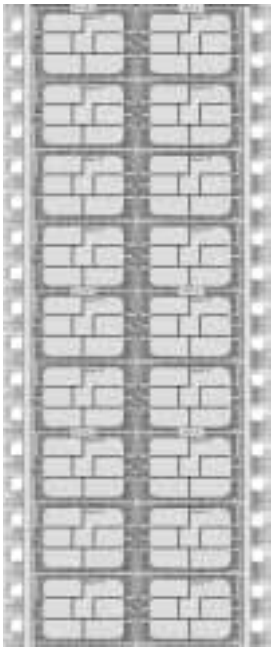
СТРУКТУРНАЯ СХЕМА



- **Блок ЭСППЗУ/ПЗУ** – организация счетчика, хранение идентификационных данных, ключей и данных пользователя.
- **Адресный блок –** формирование адресов для проведения операций с накопителем.
- **Блок программирования –** формирование напряжения для программирования ЭСППЗУ.
- **Блок защиты от прерывания записи –** восстановление правильного значения счетчика в случае прерванной операции “запись-восстановление”.
- **Блок секретности** – обработка данных, передаваемых между карточкой и ридером в процессе проведения процедуры аутентификации .

КОНСТРУКЦИЯ

ИС ЭСППЗУ выполнена по КМОП двухметальной технологии и содержит 5 выводов, соответствующих требованиям стандарта ISO 7816. ИС выпускается в трех конструктивных исполнениях: в виде неразделенных кристаллов в кремниевой пластине диаметром 150 мм (КБ5004РР1-4), в виде отдельных некорпусированных кристаллов (КБ5004РР1-5) и в виде электронного модуля для вклеивания в пластиковые карты согласно ISO 7816 (КБ5004РР1Х). Потребителю ИС поставляются в виде модумя в 35 мм транспортно-технологической ленте.



Модули в ленте

Исполнения

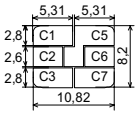
Вариант исполнения	ТУ	Конструктивное исполнение
КБ5004РР1-4	АДБК.431210.601 ТУ	Неразделенные кристаллы в пластине 150 мм
КБ5004РР1-4		Кристаллы
К5004РР1Х	АДБК.431210.774 ТУ	Модуль в ленте для вклеивания в карты по ISO 7816

Описание выводов

Контакт	Символ	Назначение	Контакт	Символ	Назначение
C1	U_{CC}	Питание	C5	GND	GND
C2	RST	Сброс	C6	-	Не используется
C3	CLC	Тактовая частота	C7	I/O	Порт по ISO 7816-3

Контакты модуля

по ISO 7816-2



ФУНКЦИОНИРОВАНИЕ

Память в кристалле организована как 632 x 1 и состоит из 16 ячеек ПЗУ и 616 ячеек ЭСППЗУ.

Во время операции ‘стирание’ в ячейку ЭСППЗУ заносится заряд и она переходит в состояние логической ‘1’. Во время операции ‘запись’ ячейка переходит в нейтральное состояние и читается как логический ‘0’. Это же состояние ячейка приобретает при несанкционированном внешнем воздействии (облучение, перегрев и т.п.)

Телефонная карточка имеет две фазы существования , отличающиеся режимами доступа к области памяти кристалла:

Фаза «Распространителя»

В этой фазе кристалл защищен транспортным ключом, запрещающим несанкционированное использование карточки.

Используя транспортный ключ пользователь должен записать индивидуальный ключ карточки и, после успешно проведенной аутентификации, становится возможным записать флаг персонализации и рабочие области кристалла.

Фаза «Пользователя»

После записи флага персонализации становится возможной работа с областями счетчика и пользовательскими данными.

Распределение памяти

Память в КБ5004РР1 распределена следующим образом:

Код производителя	16 БИТ
Область персонализации 1	48 БИТ
Бит персонализации	1 БИТ
Счетчик + биты защиты от прерванной записи	40 БИТ
Область персонализации 2	80 БИТ
Данные пользователя	192 БИТ
Ключ аутентификации	256 БИТ

Счетчик

Организация счетчика:

- пять стадий счетчика с возможностью декремента от 29160 единиц со стиранием и переносом по всем стадиям счетчика;
- четыре разряда защиты от прерванной записи предохраняющие от возможной потери счетчиком своего значения в результате прерывания контакта со считывающим устройством.

Организация счетчика

Стадия	Значение	Количество битов	Биты защиты
I	1	8	1
II	8	8	1
III	72	8	1
IV	648	8	1
V	5832	8	Счетчик

Операция перезагрузки

Уменьшение счетчика происходит путем стирания бита в соответствующей стадии. Если в стадии нет свободных битов , то используется операция перезагрузки.

Перезагрузка состоит из двух последовательных операций со счетчиком:

- стирание бита в старшей стадии;
- запись битов во всех младших стадиях.

Биты резервной копии

Прерывание операции перезагрузки может служить причиной потери данных счетчика, содержащихся в младших стадиях. Для устранения этой потери каждой из четырех старших стадий счетчика соответствует свой бит резервной копии.

Внимание ! Последовательность восстановления счетчика должна предшествовать любой штатной операции перезагрузки.

Аутентификация

КБ5004РР1 содержит блок секретности, который позволяет проводить защищенную операцию аутентификациии между карточкой и ридером, используя индивидуальный секретный ключ карты.

AN5301

МОДУЛЬ БЕЗОПАСНОСТИ

ИС модуля безопасности **An5301** размещается в контроллере ридера таксофона и в аппаратуре персонализакации. В совокупности с ИС карточки КР5004РР1 модуль безопасности обеспечивает высокий уровень защиты от несанкционированных действий.

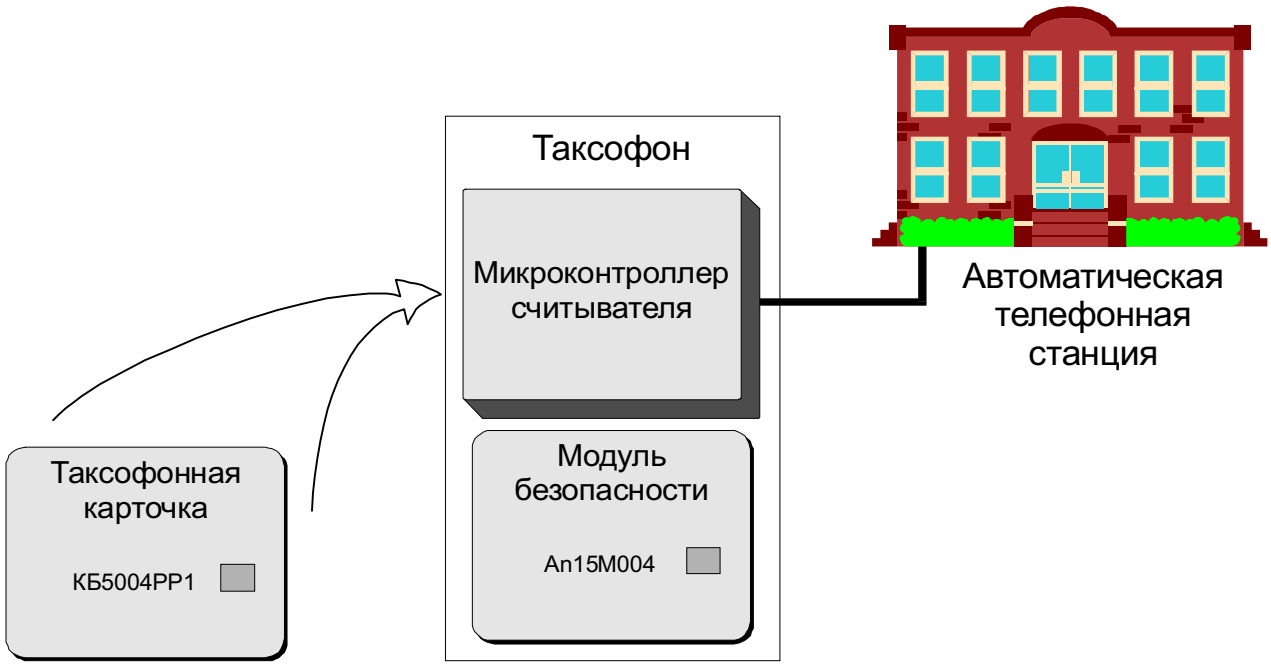
Модуль безопасности **An5301** выполняет следующие функции:

В таксофоне:

- проверка подлинности телефонной карты;
- хранение и защита ключей для работы с телефонной картой и компьютером телефонной станции;
- проведение двухсторонней аутентификации и обмен криптографически защищенными данными между модулем безопасности и компьютером центральной станции. Поддержка возможности смены ключей в модуле безопасности компьютером центральной станции;
- хранение данных совокупной длительности телефонных звонков, обслуженных оператором. Учет длительности может вестись для каждого оператора (телефонной компании) отдельно.

В аппаратуре персонализаации:

- проверка подлинности карт с использованием транспортного ключа;
- выработка индивидуального ключа телефонной карты.



ПОКАЗАТЕЛИ УСТОЙЧИВОСТИ

Микросхема устойчива к механическим и климатическим воздействиям по ГОСТ 18 725 и ГОСТ 15150 (исполнение В категории 4), в том числе:

- линейным ускорениям – 5 000м/с^2 (500g)
- пониженной рабочей температуре – -10°С
- повышенной рабочей температуре – +70°С
- пониженной предельной температуре – -60°С
- повышенной предельной температуре – +85°С
- изменениям температуры среды – -60÷+85°С

ПОКАЗАТЕЛИ НАДЕЖНОСТИ

Наработка на отказ:

- в полном диапазоне условий – 50 000 ч
- в режиме (U_{CC}= 3 В ±5%) – 60 000 ч

Интенсивность отказов – $\leqslant 1\times10^{-6}$ 1/ч

Гамма процентный срок сохраняемости – 10 лет

ГАРАНТИИ ИЗГОТОВИТЕЛЯ

Гарантии изготовителя – по ГОСТ 18 725

Гарантийный срок хранения – 10 лет

Гарантийная наработка – 50 000 ч

•

Обозначение микросхемы при заказе и в конструкторской документации другой продукции:

Микросхема К5004РР1Х АДБК.431210.774ТУ

•

Май 2001

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