ЖУРНАЛ CHIP NEWS НОВОСТИ О МИКРОСХЕМАХ

Н. Ракович

Приборы хранения информации в сети MicroLAN

В статье рассматриваются приборы хранения данных в сети MicroLAN. Ранее [1,2] отмечалось, что для работы в составе сети все микросхемы должны поддерживать 1-проводной протокол MicroLAN и иметь уникальный регистрационный номер. Приборы памяти, выпускаемые фирмой DALLAS SEMICONDUCTOR и предназначенные для работы в сети, отвечают этим требованиям.

Кроме традиционных пластмассовых корпусов (типа TO-92, TSOC и SOIC), эти микросхемы выпускаются также в корпусах MicroCAN. Такой корпус изготовлен из нержавеющей стали и имеет диаметр 16,3 мм. Существуют два стандартных варианта F3 и F5 толщиной, соответственно, 3,1 и 5,9 мм. На рис. 1 приведены размеры обоих типов корпусов. Именно герметичный стальной корпус в сочетании с простым двухпроводным интерфейсом стал одной из главных причин массового распространения этих микросхем.

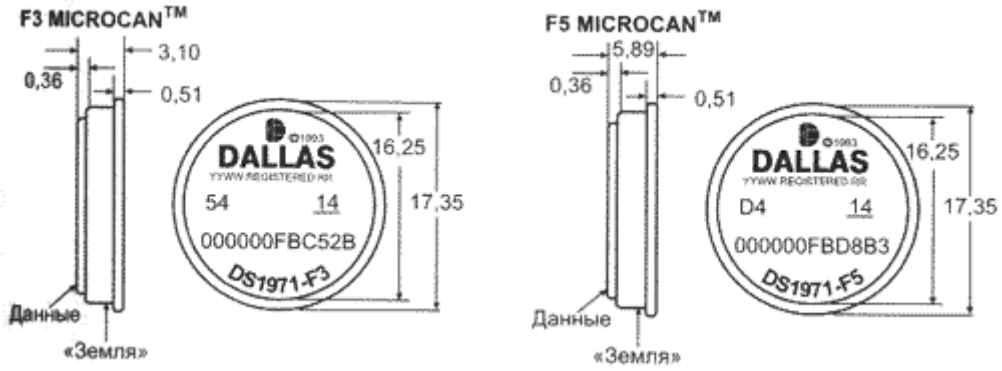

Рис. 1. Габаритные размеры корпусов MicroCAN

Приборы в металлическом корпусе имеют общее название iButton. Все приборы iButton содержат 64-бит ПЗУ с лазерным программированием. Полный номер состоит из уникального 48-бит последовательного кода, 8-бит контрольной суммы этого кода и 8-бит группового кода (рис. 2).

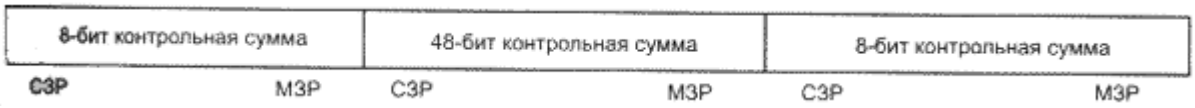

Рис. 2. Карта памяти приборов iButton (СЗР - старший значащий разряд, МЗР - младший значащий разряд)

48-бит серийный номер отражает последовательные номера производимых приборов в пределах одного группового кода.

Код контрольной суммы позволяет гарантировать правильное считывание серийного номера ведущим контроллером. Считанный групповой код и 48-бит серийный номер должны быть преобразованы по описанному циклическому алгоритму, а результат свёртки должен совпадать с контрольным кодом.

8-бит групповой код отражает функциональное назначение прибора. Младшие 7 бит обозначают тип прибора, старший бит - указатель заказных версий. Если старший бит группового кода

установлен, то функциональное назначение прибора остаётся тем же, однако формирование серийного номера выполняется по специальным правилам.

Энергонезависимая память (приборы серии DS199X)

"Серийный номер" DS1990A

Этот простейший прибор в семействе iButton представляет собой программируемое при производстве ПЗУ. DS1990A применяется как электронный регистрационный номер для автоматической идентификации. Поскольку информация в приборе хранится как конфигурация поликремниевых проводников, а не в виде заряда на затворе полевого транзистора или состояния триггера, то энергия в режиме хранения не потребляется. При работе в сети MicroLAN DS1990A использует "паразитное" питание.

При идентификации прибора первым передаётся групповой код, затем - уникальный серийный номер. Последним передаётся байт контрольной суммы (CRC). Передача любого байта начинается с младшего бита. Использование контроля на основе циклического избыточного кода (функция полинома CRC = $x^8 + x^5 + x^4 + 1$) позволяет надежно читать даже в условиях нестабильного электрического контакта.

Конструктивные особенности позволяют использовать DS1990A в качестве уникального электронного идентификатора, который практически невозможно подделать.

Мультиключ DS1991

Этот прибор является энергонезависимой памятью ёмкостью 1152 бит с защитой от несанкционированного доступа, разделённой на три отдельных электронных ключа. Как и DS1990A, мультиключ содержит ПЗУ серийного номера с групповым кодом и 1-байт контрольной суммой. Каждый ключ (48 байт) защищён своим собственным паролем (8 байт) и содержит 8-байт доступное поле идентификации. Карта памяти DS1991 представлена на рис. 3.

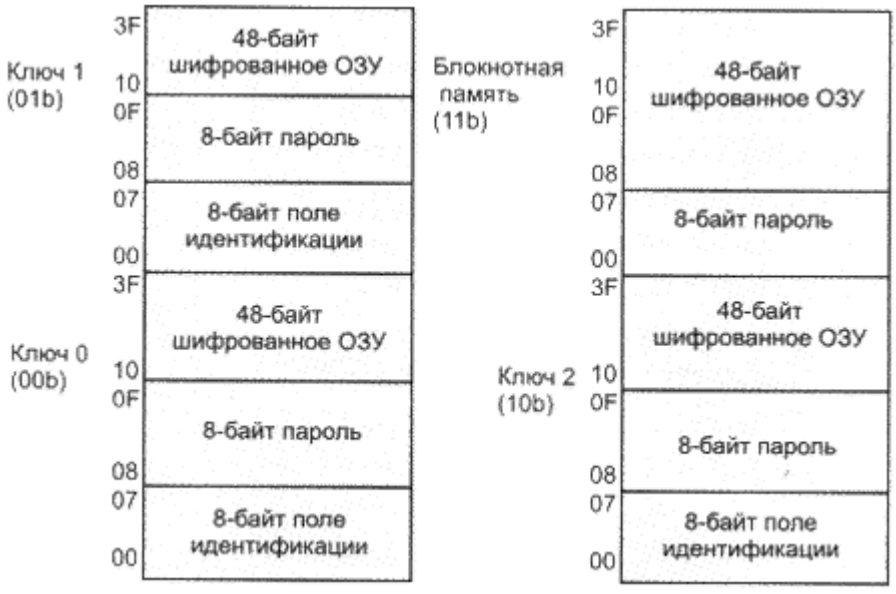

Рис. 3. Карта памяти DS1991. Каждый ключ и блокнотная память имеют свой собственный уникальный адрес

Микросхема DS1991 предназначена для приложений с высоким уровнем секретности и позволяет обеспечивать доступ к различным объектам с помощью одного физического устройства. Каждый ключ может рассматриваться как защищённый файл пользователя. Поле идентификации может содержать имя файла, а зашифрованная область данных - код доступа. Таким образом, несколько человек могут иметь доступ на один и тот же объект, используя разные экземпляры DS1991.

При попытке вскрытия пароля методом перебора автоматически включается встроенный генератор случайных чисел, который начинает подставлять выходные данные. При задании нового пароля все данные в шифрованном ОЗУ автоматически стираются.

Блокнотная память ёмкостью 512 бит применяется для записи и проверки данных, которые затем заносятся в шифрованное ОЗУ. Такой способ записи данных, используемый в приборах iButton, гарантирует запись достоверных данных даже в случае нарушения электрического контакта в процессе передачи. Помимо этого, блокнотная память используется как незащищённая область данных общего применения.

Энергонезависимые ОЗУ DS1992-DS1996

Эти микросхемы памяти, как и все приборы iButton, содержат уникальный серийный номер, групповой код и байт контрольной суммы. Встроенный в микросхему литиевый источник питания позволяет сохранять данные в ОЗУ в течение 10 лет. ПЗУ и интерфейс могут питаться как от литиевой батареи, так и от шины данных ("паразитное питание"). Это обеспечивает доступ к постоянной памяти даже при полном истощении внутреннего источника, а также позволяет экономить энергию этого источника при напряжении питания на шине данных свыше 3 В.

Внутреннее ОЗУ каждой микросхемы организовано в виде страниц объёмом 256 бит. Содержимое памяти может быть прочитано с любого байта любой страницы. Кроме оперативной памяти, каждый прибор содержит область блокнотной памяти объёмом 256 бит, которая является буфером при записи данных в ОЗУ. Данные записываются в блокнотную память и, после проверки по команде копирования, заносятся в оперативное ОЗУ. Блок-схема приборов DS199X приведена на рис. 4.

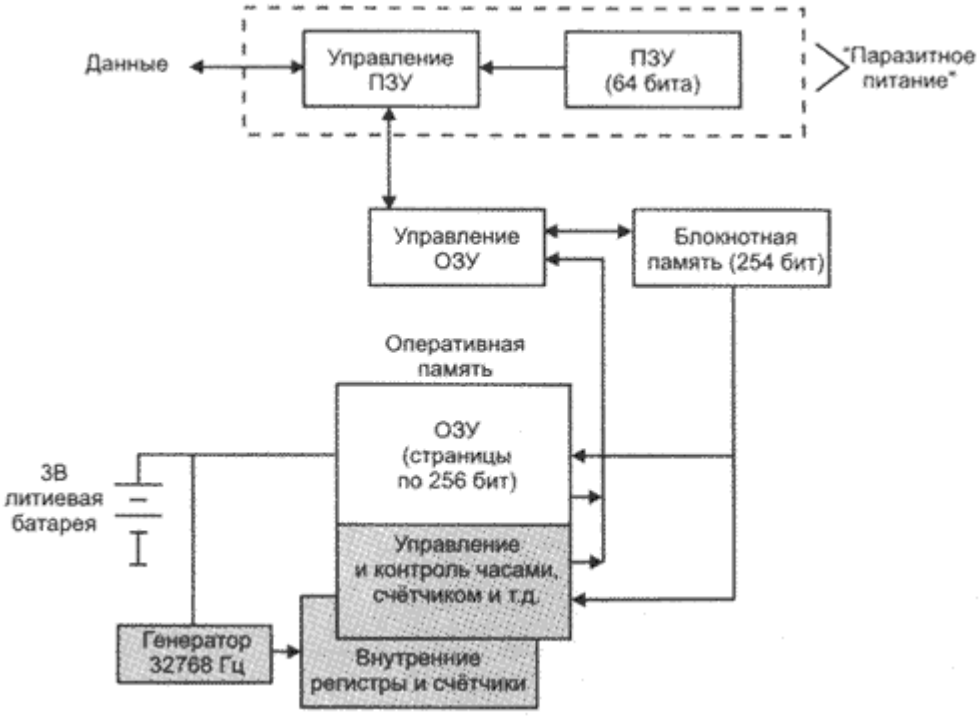

Рис. 4. Блок-схема микросхем памяти DS199X. Заштрихованные области входят в состав только DS1994

Как видно из блок-схемы, структура всех микросхем одинакова, отличие состоит только в объёме памяти и идентификаторе группового кода.

Структура прибора DS1994, отличающаяся дополнительными блоками, будет рассмотрена ниже.

Объём памяти каждой микросхемы и групповой код приведены в табл. 1.

Таблица 1. Основные параметры приборов DS199X

Тип прибора	Объём памяти, Кбит	Организация памяти, Кбит	Групповой код
DS1992	1	4x32	08H
DS1993	4	16x32	06H
DS1994	4	16x32	04H
DS1995	16	64x32	0AH
DS1996	64	256x32	0CH

По структуре памяти микросхема DS1994 аналогична прибору DS1993. Вместе с тем, она дополнена часами/календарём реального времени, таймером, счётчиком событий и программируемыми сигнальными устройствами. Дополнительные регистры (часы, таймер и так далее) расположены на отдельной странице в верхней области памяти.

Отличительной особенностью часов прибора DS1994 является способ представления времени. Сами часы - двоичный счётчик с разрешением 1/256 с. Минуты, часы,..., годы вычисляются из числа секунд, прошедших от условно выбранной даты. Это позволяет значительно упростить вычисление временных интервалов между различными событиями. Таймер может использоваться как секундомер или для контроля интервалов времени работы оборудования, так как в его состав входит схема генерации прерываний. Часы реального времени совместно с сигнальным регистром можно использовать для организации доступа по времени, например, дя ограничения доступа персонаа в помещение на опредеенное время.

Возможность установки защиты от записи в счетчик времени и сигнальные регистры позволяет превратить DS1994 в необнуляемый контроллер окончания срока действия. Описаны применения микросхемы DS1994 в качестве датчика фиксации времени определенных событий, например, вскрытия охраняемых помещений или емкостей.

Семейство ЭППЗУ DS1982 (DS2502), DS1985 (DS2505), DS1986 (DS2506)

Микросхемы этого семейства выпускаются в корпусах типов MicroCAN (DS198x) и TO-92, TSOC, SOIC (DS250x). Для хранения записанной информации источника питания не требуется. В качестве него для работы и программирования используется 1-проводная линия ("паразитное питание"). Как и все приборы для 1-проводной сетия, ЭППЗУ содержат ПЗУ с серийным номером, групповым кодом и байтом контрольной суммы. Рабочая область памяти организована в виде страниц объемом по 32 байт каждая. Основные параметры приборов приведены в табл. 2.

Таблица 2. Основные параметры приборов DS198x (DS250x)

Тип прибора	Объем памяти, Кбит	Организация памяти, Кбит	Групповой код
DS1982 (2502)	1	4x32	09H
DS1985 (2505)	16	64x32	0BH
DS1986 (2506)	64	256x32	0FH

Чтение данных из DS198x (DS250x) аналогично чтению из других микросхем DS, однако запись выполняется иначе. Первоначально данные заносятся в 1-байт блокнотную память. Затем выполняется проверка команды записи, адреса и записываемых данных с использованием 8-бит

контрольного кода. При положительном результате проверки импульс длительностью 1 мс и амплитудой 12 В записывает данные в память. Важность такого контроля очевидна, так как если даные будут записаны неправильно, то их уже невозможно будет изменить. После этого любая страница памяти может быть индивидуально защищена от последующих попыток записи. Необходимо отметить, что возможно многократное программирование, но не перезапись данных, поскольку бит может быть изменен только из "1" в "0", но не наоборот.

Флаги защиты данных или переадресации хранятся в старшей области памяти и называются памятью состояния ЭППЗУ (рис. 5). Запись в нее выполняется так же, как и в память данных. При чтении как данных, так и состояния прибора для проверки правильности передачи используется встроенный генератор контрольной суммы.

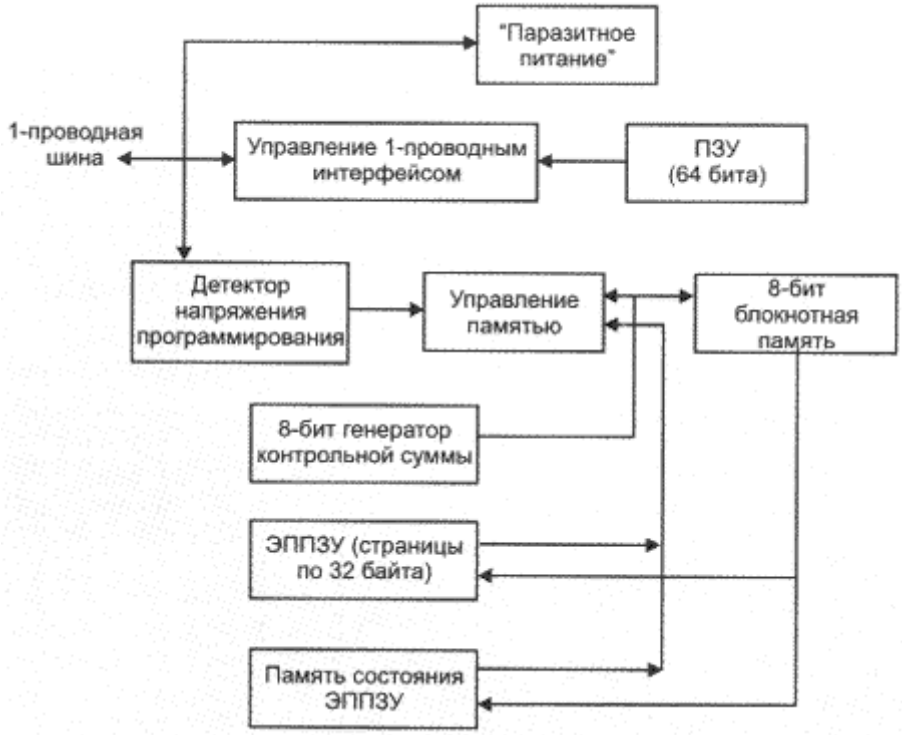

Рис. 5. Блок-схема ЭППЗУ семейства DS198x (DS250x)

Важнейшим свойством микросхем ЭППЗУ семейства DS198x (DS250x) является невозможность удаления записанных данных (принцип "Add-only"). При необходимости обновления данных, это выполняется размещением новых данных на другой странице памяти. Прежние данные при этом сохраняются, и при необходимости к ним можно вернуться. Благодаря аппаратной защите от записи при установке бита защиты от записи невозможно изменить ни одного бита памяти данных или состояния памяти.

Семейство ЭСППЗУ DS1971 (DS2430A), DS1973 (DS2433A)

Микросхемы этого семейства, как и ЭППЗУ DS198x (DS250x), выпускаются в корпусах MicroCAN (DS197x) и корпусах типа TO-92, TSOC (DS2430A), PR-35, SOIC (DS2433A). Для хранения записанной информации в ЭСППЗУ также не требуется источника питания, а вместо него для работы и программирования используется 1-проводная линия ("паразитное питание"). Аналогично всем приборам для 1-проводной сети, ЭСППЗУ содержат ПЗУ с серийным номером, групповым кодом и байтом контрольной суммы. Рабочая область памяти организована в виде страниц объемом по 32 байт каждая. Основные параметры приборов приведены в табл. 3, блок-схема - на рис. 6.

Таблица 3. Основные параметры приборов DS197x (DS243x)

Тип прибора	Объем памяти, бит	Организация памяти, Кбит	Групповой код
DS1971 (2430A)	256x64	1x32	14H
DS1973 (2433A)	4096	16x32	23H

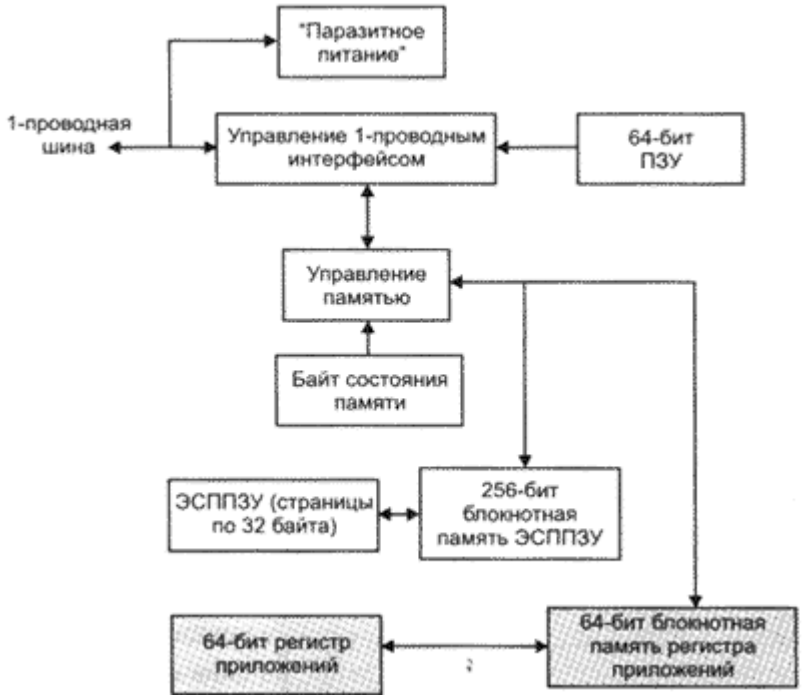

Рис. 6. Блок-схема ЭСППЗУ семейства DS197x (DS243x). Заштрихованные области относятся к DS1971 (DS2430A)

Использование перепрограммируемой памяти значительно расширяет возможности пользователя по хранению изменяющихся данных: калибровочные постоянные, идентификация плат, модифицированные параметры изделий или товаров.

Запись в память осуществляется через блокнотную память объемом 256 бит аналогично записи в ЭППЗУ.

Как видно из блок-схемы, микросхемы DS1971 (DS2430A) имеет дополнительный регистр приложений и соответствующую блокнотную память. В отличие от основной памяти, в которую данные могут многократно перезаписываться, регистр приложений программируется всего один раз, причем сразу после записи его содержимое автоматически защищается. Это позволяет однозначно связать микросхему с приложением. Состояние регистра приложений содержится в регистре состояния. Если данные не были занесены в регистр приложений, то в регистре состояния хранится FFh. При записи данных из блокнотной памяти регистра в регистр приложений, в регистре состояний очищаются два последних значащих бита (FCh).

Энергонезависимое "денежное" ОЗУ DS1963L

Эта микросхема памяти ёмкостью 4 Кбит в корпусе iButton отличается от других ОЗУ структурой, напрямую связанной с её назначением. DS1963L может хранить зашифрованные данные, которые представляют собой денежные средства.

Уникальный регистрационный номер, счётчики количества циклов записи данных на страницу и биты определения попыток взлома предотвращают несанкционированное вторжение в ваш электронный кошелёк. Считается, что в финансовых приложениях зашифрованная память ключа

содержит управляемый программно счётчик транзакций. В этом случае перезапись памяти с целью мошенничества приведёт к рассогласованию аппаратного и программного счётчиков транзакций и будет немедленно обнаружена. Высокая скорость выполнения перевода денег (изменение содержимого кошелька происходит менее, чем за 100 мс) позволяет избежать каких-либо неприятностей в людных местах.

Состав DS1963L приведён на рис. 7. В основном структура прибора совпадает с микросхемами серии DS199x, за исключением счётчиков количества циклов записи данных на страницу. Каждый из этих счётчиков связан с одной из страниц памяти размером 265 бит (страницы 12-15). Содержимое счётчика считывается одновременно с данными из соответствующей страницы памяти специальной командой.

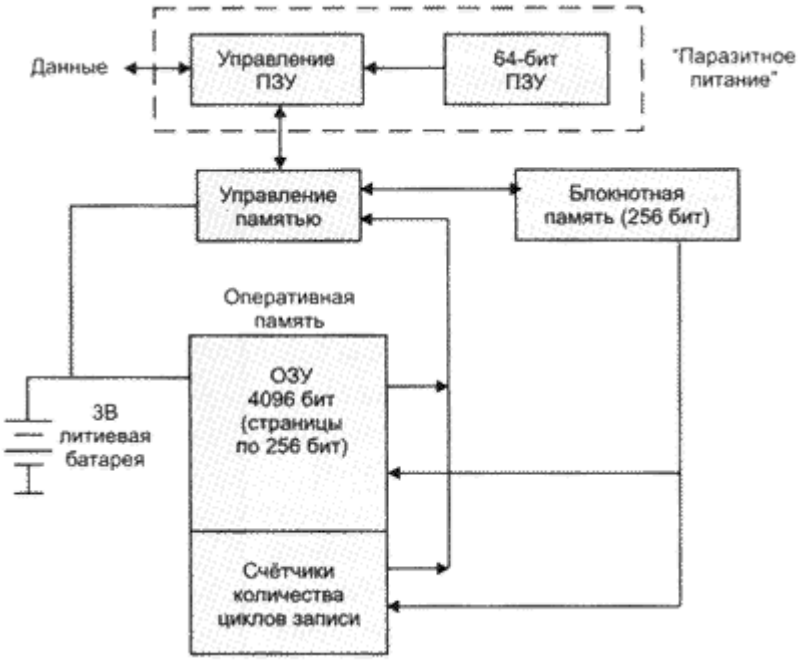

Рис. 7. Блок-схема DS1963L

Энергонезависимая SHA-память DS1963S

Эта микросхема с объёмом памяти 4 Кбит занимает особое место среди приборов памяти. Особенность прибора заключается не только в том, что он функционирует как локальная база данных с открытым доступом к информации и защищёнными данными владельца, но и в наличии встроенного 512-бит SHA-процессора для вычисления 160-бит хэш-функций (кодов идентификации). Более подробную информацию по системам безопасности на базе стандарта SHA-1 (Secure Hash Standard) можно найти в Интернете по адресу http://www.itl.nist.gov/div897/pubs/fip180-1.htm. Применение формата TMEX позволяет использовать отдельную микросхему в четырёх независимых приложениях: безопасный "кошелёк" для электронных расчётов, оплата телефонных разговоров, парковки автомобиля или покупки в торговых автоматах. Кроме этого, DS1963S может работать как сопроцессор ведущего шины при вычислении сигнатур.

Блок-схема микросхемы приведена на рис. 8. В состав DS1963S входят:

- 64-бит ПЗУ с уникальным номером;
- блокнотная память объёмом 256 бит;
- ОЗУ общего назначения в виде 8 32-байт страниц;
- защищённое ОЗУ объёмом 8 страниц по 32 байта;

- две 32-байт страницы для хранения 8 64-бит ключей с индивидуальными счётчиками количества циклов записи;
- 512-бит SHA-процессор.

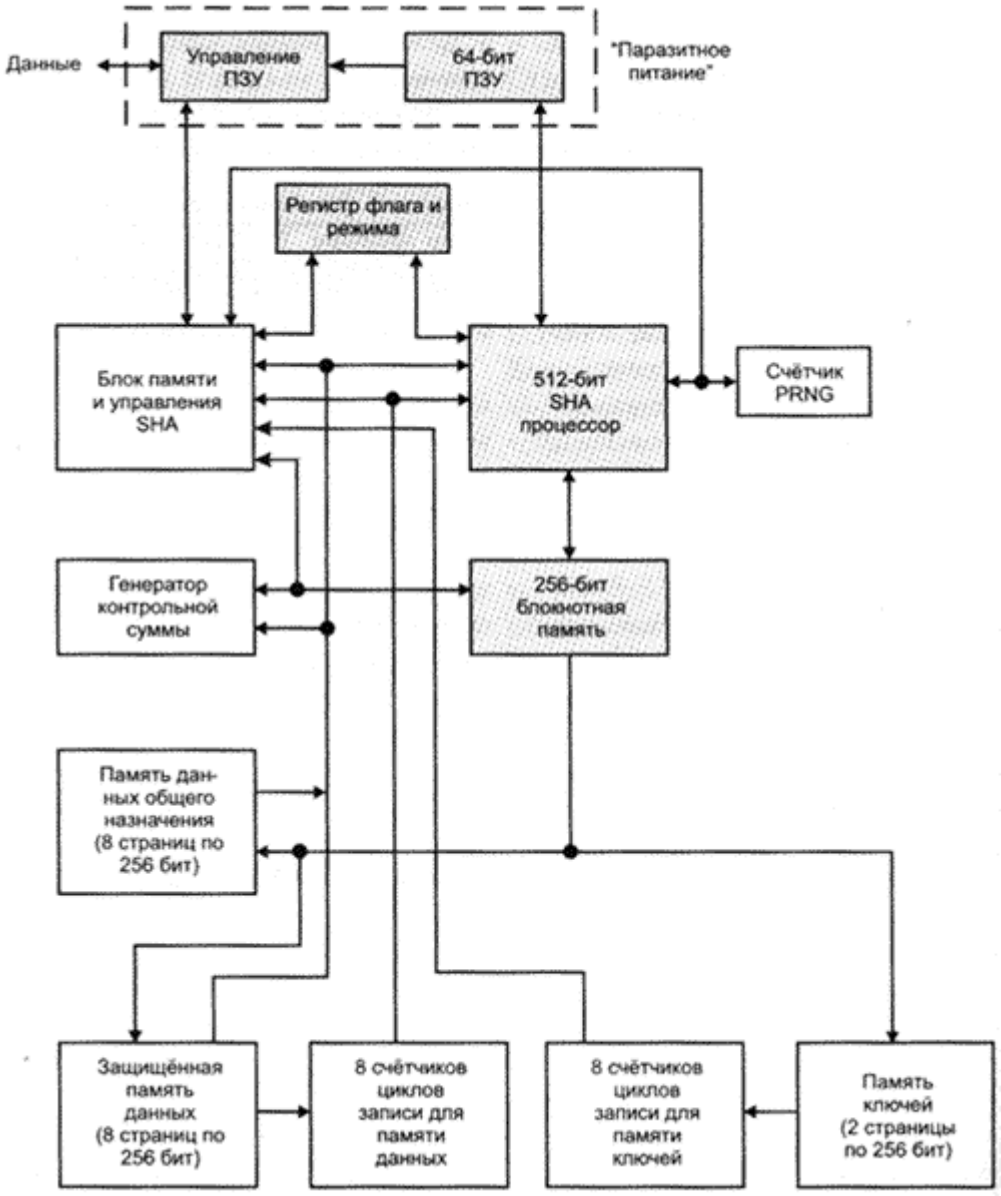

Рис. 8. Блок-схема DS1963S35

Как видно из блок-схемы, в состав прибора входит четыре области памяти: память данных, память ключей, память счётчиков и блокнотная память. Последняя работает как буфер при записи информации в память данных и в память ключей. Страницы 0-15 являются памятью с неограниченным доступом. Страницы 16 и 17 содержат 8 64-бит ключей с индивидуальными счётчиками количества циклов записи, доступ к которым возможен только при записи. Значения ключей могут быть прочитаны с помощью SHA-процессора, который использует их для вычисления кодов идентификации. 16 32-бит счётчиков циклов записи расположены на страницах 19 и 20, причём их содержимое можно считать без каких-либо ограничений. На странице 21 находится счётчик количества запусков процессора SHA. На основе содержимого этого счётчика работает генератор псевдослучайных чисел (ГПСЧ). Поскольку потребление SHA-процессора при работе в 20 раз больше, чем при копировании полного содержимого блокнотной памяти, то ГПСЧ может быть использован как индикатор ёмкости встроенного источника питания. Страница 18 представляет собой физическое расположение блокнотной памяти.

Подробную информацию о сети MicroLAN и компонентах для её построения можно получить по адресу www.rainbow.msk.ru.

Литература

1. *Ракович Н.Н. Выбор сети для коммуникации и управления // Chip News. - 2000. - № 5. - С. 25-27.*
2. *Ракович Н.Н. Основы построения сетей MicroLAN // Chip News. - 2000. - № 6. - С. 14-17.*