Андрей Никитин (г. Минск)

ДЛЯ ЗАМЕНЫ «ТАБЛЕТОК»: СИСТЕМЫ РЧ-ИДЕНТИФИКАЦИИ НА БАЗЕ КОМПОНЕНТОВ RFID КОМПАНИИ MAXIM INTEGRATED

*В статье рассматриваются новые **RFID-компоненты Maxim:** изделия **MAX66040** и **MAX66140**, в которых реализован алгоритм **криптографического хеширования SHA-1**, и отладочные наборы, предлагаемые производителем для упрощения разработки систем контроля доступом.*

Система контроля доступа (СКД) – комплекс аппаратно-программных средств безопасности, предназначенный для контроля (ограничения, регистрации) входа-выхода людей и/или транспортных средств на определенные территории через так называемые «точки прохода» (двери, ворота, проходные). Кроме того, задачами СКД могут быть также учет рабочего времени персонала и контроль прав доступа работающих к конкретному оборудованию компании (компьютеры, ксероксы, принтеры).

Ключевыми элементами любой СКД являются идентификатор и считыватель. Идентификатор (ключ) – это то, что хранит некий код, служащий для идентификации владельца и, следовательно, определяющий права его предъявителя. Считыватель – устройство, которое этот код считывает. Строго говоря, идентификатором может являться и сам человек. Существуют достаточно надежные системы доступа, основанные на биометрической идентификации. Это, например, анализ отпечатка пальца, анализ радужной оболочки или сетчатки глаза субъекта. Однако, системы, основанные на биометрической идентификации, имеют в настоящее время еще довольно ограниченное применение. Поэтому в качестве идентификатора в большинстве систем используется предмет, принципиально небольшого веса и габаритов, хранящий некий код, используемый для принятия решения о разрешении доступа. Отметим, что идентификаторы-устройства являются пропуском «на предъявителя», то есть они никаким образом не гарантируют, что идентификатор предъявит для доступа именно его законный владелец, а не постороннее лицо, владеющее «пропуском» в данный момент времени.

Наиболее распространенные устройства, выполняющие функции идентификатора:

1. Магнитные карты или карты с магнитной полосой. Позволяют считывать и записывать ограниченный объем информации. Надежность и защищенность магнитных карт в настоящее время оценивается как недопустимо низкая. В новых разработках эти карты практически не применяются, хотя в старых, масштабных проектах используются до сих пор. Например, в некоторых городах магнитные карты продолжают использоваться как проездные билеты в метрополитене.

2. Контактная память или «таблетка». В различных публикациях называется также Touch Memory или iButton . Это электронные компоненты с однопроводным протоколом обмена информацией (1-Wire), размещенные в стандартном металлическом корпусе (действительно похожем на таблетку). В наиболее простом варианте электронного ключа при считывании выдавался длинный номер, записываемый в устройство при изготовлении. Более сложные варианты изделий содержали энергонезависимую перезаписываемую память, контроллеры, таймеры, датчики температуры. Обмен данными производился при контакте со специальными считывателями, причем сама «таблетка» активизировалась для чтения-записи только в момент контакта. В странах бывшего СССР появились в самом начале 90-х годов, но и в настоящее время продолжают широко использоваться в бюджетных приложениях. Например, как ключи к домофонам в подъездах жилых домов.

3. Контактные смарт-карты представляют собой пластиковую карту со встроенной микросхемой (часто микропроцессор средней вычислительной мощности). С функциональной точки зрения – аналог «таблеток». Различие заключается исключительно в конструктивном исполнении. Контактные смарт-карты имеют небольшую зону, содержащую несколько металлических

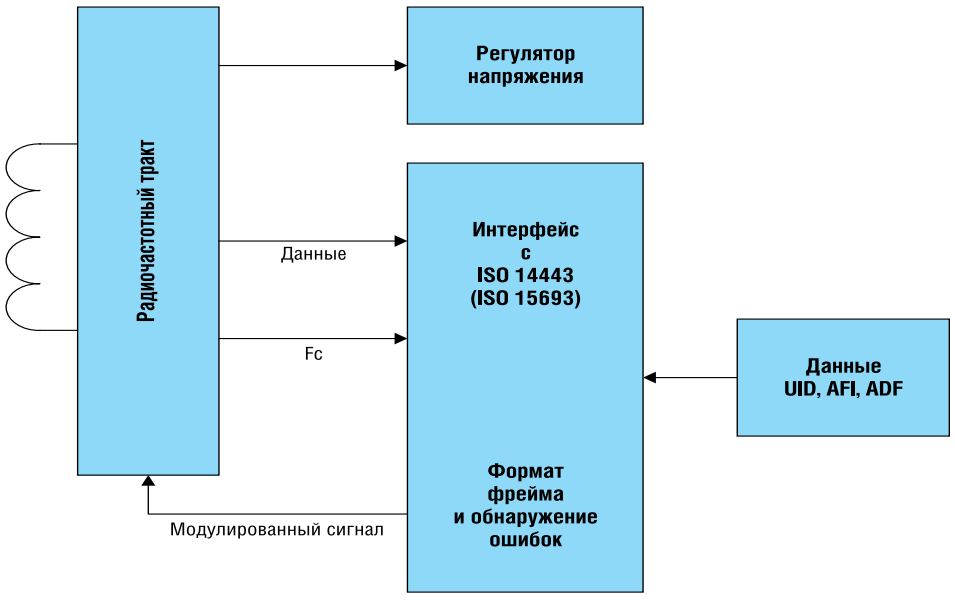

Рис. 1. **Структурная схема идентификаторов MAX66000 и MAX66100**

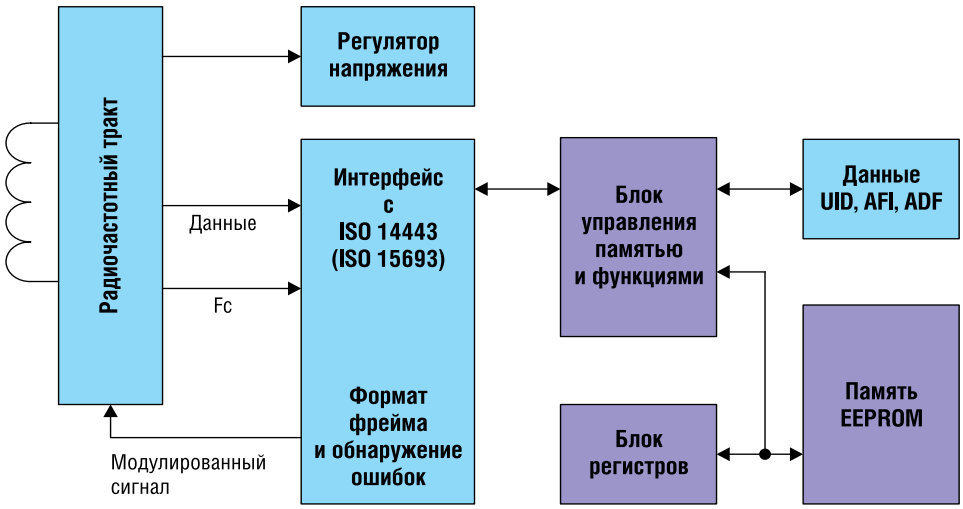

Рис. 2. **Структурная схема идентификаторов MAX66020 и MAX66120**

контактных лепестков. Когда карта вставлена в считыватель, то чип карты соприкасается с электрическими контактами считывателя, и последний получает доступ к информации с чипа. Вычислительная мощность микропроцессора позволяет не только считать и записать данные в энергонезависимую память, но, в ряде приложений, поддерживать выполнение специфических криптографических функций. Основная сфера применения: банковские карты, проездные билеты, второстепенные документы (например, студенческие и читательские билеты), ключи для систем доступа.

4. Бесконтактные смарт-карты – это смарт-карты, использующие технологию RFID (*Radio Frequency IDentification*). Для проведения необходимых операций требуется поднести карточку достаточно близко к считывателю. Однако непосредственное касание не требуется, так как обмен данными происходит по радиоканалу. Бесконтактные смарт-карты подразделяются на два класса: так называемый proximity card, соответствующий стандарту ISO/IEC 14443 и vicinity card, соответствующий стандарту ISO/IEC 15693. Основное отличие: в первом случае расстояние от карты до считывателя не превышает 15 сантиметров, а во втором увеличено до 100 сантиметров. То есть, в первом случае карту следует все же поднести к считывателю достаточно близко, а во втором она может оставаться в кармане пальто. Рабочая частота в обоих случаях составляет 13,56 МГц, однако скорости обмена данными в первом случае заметно выше: 106…848 кбит/с против 1,6…26 кбит/с.

Считается, что бесконтактные карты по сравнению с контактными ключами имеют существенный плюс: такую карту не требуется вставлять в считыватель – достаточно подержать ее в непосредственной близости от него. Предполагается, что такой способ повышает пропускную способность «точки прохода». Но применительно к СКД это, скорее всего, несущественно: если алгоритм допуска на режимную территорию (помещение) предполагает проход через турникет по одному человеку, то пропускная способность будет определяться именно турникетом. Реальный выигрыш будет в других факторах. Во-первых, отсутствие механических частей и контактов существенно повышает срок работы и самих ключей, и считывателей. Во-вторых, подделка бесконтактной карты, в принципе, возможна, но трудозатраты на эту процедуру будут на порядок выше, чем при использовании «таблетки» или контактной смарт-карты. Фактор стоимости в настоящее время не представляется существенным: разница в цене контактного и бесконтактного исполнений скажется только в СКД с числом пропусков от десятков тысяч и более.

Алгоритмы защиты информации

Рекомендуемые к применению в новых разработках RFID-ключи компании Maxim предполагают наличие встроенного блока, реализующего алгоритм SHA-1. SHA-1 (*Secure Hash Algorithm*) – алгоритм криптографического хеширования, то есть вычисления хеш-суммы – значения какой-то конкретной для данного алгоритма хеш-функции, вычисленной на принятой последовательности данных. Для входного сообщения произвольной длины алгоритм SHA-1 генерирует 160-битную хеш-сумму, которая также называется дайджестом. Строго говоря, любая контрольная сумма, например, CRC32, которая используется во многих программах – это тот же дайджест, только вычисленный по другому алгоритму. В криптографии применяемая хеш-функция должна удовлетворять трем требованиям. Во-первых, необратимость, то есть по дайджесту должно быть невозможным восстановить входное сообщение. Во-вторых, по заданному дайджесту должно быть вычислительно невозможно (то есть, невозможно за разумное время) подобрать сообщение, которое будет иметь этот же дайджест. В-третьих, по исходному сообщению вычислительно невозможно подобрать другое сообщение, имеющее аналогичный дайджест.

Что на практике дает применение алгоритма криптографического хеширования? Если криптографическая защита в СКД не используется, то для того, чтобы инициировать некую операцию (например, открыть дверь в помещение) с карты-идентификатора клиента, необходимо отослать на сервер некоторый код, выполняющий функцию пароля. Сервер сравнит полученный пароль со списком допустимых вариантов и, если в этом списке найдется полученный пароль, разрешит доступ к запрошенной операции. Заполучив каким-то образом этот список, злоумышленник может сымитировать отсылку требуемого пароля и получить право на доступ. При использовании криптографической защиты на сервере хранятся не сами пароли, а только их дайджесты. В этом случае ситуация для злоумышленника становится практически неразрешимой. Чтобы получить доступ, надо отослать пароль, но сервер хранит не пароли, а дайджесты от пароля и, только получив сообщение-пароль, рассчитывает дайджест. Причем само принятое сообщение на сервере принципиально не запоминается. Если полученный дайджест есть в списке разрешенных, то сервер дает право на запрашиваемую операцию. Злоумышленник, получив доступ к серверу, может узнать только разрешенные дайджесты, но не сам список паролей. А зная только дайджест, он не может за разумное время подобрать допустимый пароль и, таким образом, даже обладание файлом дайджестов не дает возможность получить право на требуемую операцию. Примерно аналогичным образом процессор на карте клиента может проверять право сервера изменить (записать) некую информацию в свою пользовательскую и системную память (когда это возможно в принципе).

Иными словами, речь идет не о шифровании или дешифровании самих передаваемых сообщений – предполагается, что злоумышленник не имеет возможность «прослушивать» канал обмена. Если это не так, то теряется смысл применения алгоритмов криптозащиты. Речь идет только лишь о невозможности за разумное время подобрать допустимые сообщения-пароли, имея в распоряжении список разрешенных дайджестов. Отметим, однако, что алгоритм SHA-1 не является какой-то обязательной или даже желательной частью стандарта на

бесконтактные карты. Существует, как минимум, десятка два алгоритмов, подобных SHA-1, разной степени популярности, которые различаются конкретной процедурой формирования дайджеста и теоретически оцененным временем подбора входного сообщения с заданным дайджестом (причем во всех случаях избыточным). Все обязательные требования к бесконтактным proximity- (или vicinity-) картам определяются стандартами ISO/IEC 14443B (или ISO/IEC 15693) и только ими. Все остальное, в частности – алгоритмы хеширования, является надстройкой, которая может присутствовать, а может и отсутствовать в конкретном приложении.

Бесконтактные идентификационные карты компании Maxim

В настоящее время компания Maxim в линейке RFID-компонентов для идентификации предлагает два изделия: **MAX66040** и **MAX66140**. Первое – MAX66040 – поддерживает стандарт ISO/IEC 14443B, и, соответственно, предназначено для приложений направления proximity card. Второе – MAX66140 – поддерживает ISO/IEC 15693 и приложения vicinity card. Имеет смысл начать рассмотрение с ранних изделий для понимания развития направления RFID-идентификаторов, предлагаемых компанией Maxim (в настоящее время не рекомендуются для новых разработок).

Простейшие идентификаторы **MAX66000** и **MAX66100** включали в себя 64-хразрядный уникальный номер изделия (UID), задаваемый в процессе изготовления, и радиочастотный интерфейс 13,56 МГц, удовлетворяющий требованиям ISO/IEC 14443B или ISO/IEC 15693 (для MAX66000 и MAX 66100 соответственно). Структурная схема идентификаторов **MAX66x00** представлена на рисунке 1 Данные устройства поддерживали только две команды управления: «Get System Information» (чтение системной информации) и «Get UID» (чтение UID).

Усовершенствованием этих изделий были идентификаторы MAX66020 и MAX66120, которые также включали в себя 64-разрядный уникальный номер изделия и радиочастотный интерфейс 13,56 МГц (также в двух вариантах реализации). Дополнительно изделия содержали пользовательскую память EEPROM (электрически стираемое, программируемое пользователем ПЗУ) объемом 1024 бита, организованную как 16 блоков по 8 байт. Кроме того, в пространство памяти входило два дополнительных блока для организации регистров данных и управления.

Структурная схема идентификаторов **MAX66x20** представлена на рисунке 2. Фиолетовым цветом выделены блоки,

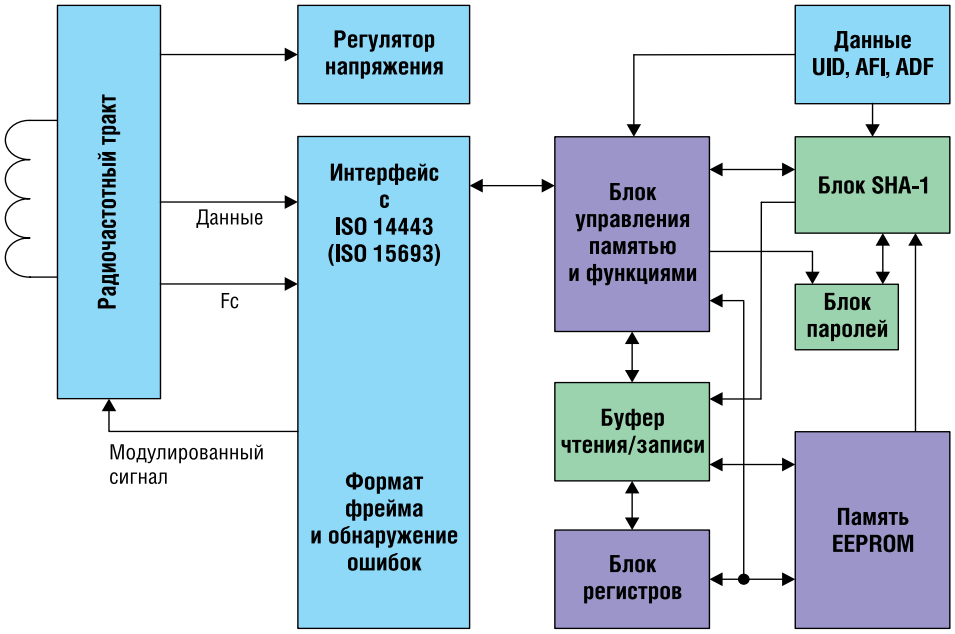

Рис. 3. **Структурная схема идентификаторов MAX66040 и MAX66140**

отсутствующие в изделиях MAX66x00. Изделия MAX66x20 могли быть использованы как прямая замена ключей MAX66x00, поскольку форматы команд управления «Get System Information» и «Get UID» были сохранены без каких либо изменений. Однако, дополнительно были добавлены команды, поддерживающие чтение отдельного блока памяти, запись в блок и его закрытие. Расширенные команды позволили содержать на карте не только постоянную информацию, записанную при изготовлении, но и небольшой объем пользовательских данных (например, ФИО и должность владельца, структурное подразделение и т.п.).

Идентификаторы MAX66040 и MAX66140 являются дальнейшим развитием этого направления. Эти изделия, как и их предшественники, включают в себя 64-разрядный уникальный номер изделия и радиочастотный интерфейс. Пользовательское EEPROM имеет объем 1024 бита, организацию «16 блоков по 8 байт» и два дополнительных блока, что соответствует архитектуре памяти изделий MAX66x20. Команды управления памятью, присутствующие в изделии MAX66x20, сохранены в идентификаторах MAX66x40 без изменений. Таким образом обеспечивается совместимость изделий MAX66x40 с более ранними компонентами MAX66x20 и, соответственно, MAX66x00. То есть, идентификаторы MAX66x40 могут быть использованы как прямая замена MAX66x20 и MAX66x00 без внесения каких-либо изменений в само приложение. Однако, в дополнение к MAX66x20, изделия MAX66x40 имеют третий дополнительный блок, предназначенный для хранения пароля, а также встроенный блок, аппаратно реализующий защиту на базе алгоритма хеширования SHA-1. Система команд расширена таким образом, что позволяет изделию работать как без использования средств защиты SHA-1 (то есть, в режиме MAX66x20), так и реализуя возможности MAX66x40 в полном объеме. Структурная схема идентификаторов MAX66x40 представлена на рисунке 3. Светло-зеленым цветом выделены новые, по сравнению с MAX66x00 и MAX66x20, блоки. Введение дополнительных средств криптографической защиты позволило значительно расширить возможную сферу применения RFID-ключей компании Maxim до современных СКД с серьезными требованиями к безопасности и защите от несанкционированных воздействий.

Отметим, что изделия MAX66x40 выпускаются в виде двух возможных форм-факторов. Исполнение в виде бесконтактной смарт-карты стандартных размеров имеет суффикс “E” (например, MAX66040E), а исполнение в виде брелка – суффикс “K”.

Несколько слов о карт-ридерах, предназначенных для работы с RFID-идентификаторами MAX66xx0. Эту продукцию разного качества выпускают многие независимые компании. Для работы с идентификаторами **MAX660x0 (MAX661x0)** достаточным требованием является соответствие карт-ридера стандарту ISO/IEC 14443B (или ISO/IEC 15693, соответственно). То есть на «стандартном» карт-ридере можно гарантированно считать с карты ее UID. Для карт с EEPROM должны быть задействованы функции доступа к другим ресурсам карты, которые оговорены в части 4 стандарта ISO/IEC 14443B, где определяется протокол обмена данными. Однако эта часть реализована далеко не

Рис. 4. **Состав отладочного комплекта MAX66901 EV Kit**

в любом карт-ридере, соответствующем ISO/IEC 14443B. Если в приложении необходим доступ к другим ресурсам карты (к той же памяти), то необходимо убедиться, что карт-ридер «понимает» именно ISO/IEC 14443B-4. Для стандарта ISO/IEC 15693 ситуация аналогична, с той лишь разницей, что протокол обмена данными регламентирован третьей частью этого стандарта – ISO/IEC 15693-3. Функции криптозащиты, заложенные в MAX66x40, в настоящее время непосредственно карт-ридерами не поддерживаются, а реализуются поверхстандартов ISO/IEC 14443B (ISO/IEC 15693) на уровне программного обеспечения сервера.

Отладочные комплекты для работы с RFID-идентификаторами компании Maxim

Основным отладочным комплектом, предлагаемым компанией Maxim для работы с RFID-ключами MAX660x0 и MAX661x0, является **MAX66901 EV Kit.** В комплект входит карт-ридер **INfinity-110** американской компании **Sirit** с соответствующим программным обеспечением, источник питания, необходимые кабели и переходники, а также RFID-брелки MAX660xxK (всех шести типов ключей, выпускаемых компанией Maxim). Непосредственно карт-ридер INfinity-110 поддерживает работу с картами стандартов ISO/IEC 14443B и ISO/IEC 15693 в полном объеме, то есть позволяет считывать UID устройств, обеспечивает возможность работы со всем пространством памяти ключей MAX66x20 и MAX66x40 и работу с функциями криптозащиты SHA-1, которые реализованы в MAX66x40. Отладочный комплект позволяет выполнить следующие процедуры работы с пространством памяти: чтение системной информации, чтение UID, чтение, запись и закрытие блоков памяти, запись и закрытие байта AFI. В режиме работы с использованием функций SHA-1 комплект позволяет записать блок паролей, произвести чтение-запись в блок дайджестов, выполнить расчет дайджеста и провести проверку аутентификации. Отметим, что программное обеспечение, входящее в состав отладочного комплекта, несколько отличается от фирменного ПО, поставляемого компанией Sirit с модулем INfinity-110. Программа для работы с комплектом MAX66901 EV Kit не содержит операций для работы с RFID-ключами тех типов, которые не входят в номенклатуру компании Maxim (например, ключи **Mifare** компании **NXP**), что позволяет в наибольшей степени сконцентрироваться на особенностях именно изделий Maxim. Фотография отладочного комплекта MAX66901 EV Kit представлена на рисунке 4. Для работы только с изделиями MAX661x0 (категория vicinity card) существует также отладочный комплект MAX66903 EV Kit. Однако существенных дополнительных возможностей (по сравнению с MAX66901 EV Kit) он не предоставляет.

Отличительные особенности RFID-идентификаторов MAX66x40 компании Maxim

Бесконтактные ключи MAX66040 и MAX66140 – это конечные изделия для вполне конкретных приложений. Основная отличительная особенность новых изделий – наличие встроенных функций криптозащиты SHA-1. Сам по себе алгоритм SHA-1 не лучше и не хуже других, подобных ему. Тот или иной алгоритм применяют различные производители, поскольку выбор алгоритма криптозащиты на данный момент не регламентирован каким-то глобальным стандартом, а является исторически сложившейся практикой конкретной компании. Применение SHA-1 в приложениях контроля доступа – это своеобразная визитная карточка компании Maxim, отработанная на множестве «таблеток» iButton, например, на изделиях **DS1961S** или **DS1963S,** которые нашли применение не только в системах контроля доступа, но и в различных приложениях eCash (электронные деньги) в качестве носителей информации. С этой точки зрения MAX66x40 являются хорошей функциональной заменой для DS1961S. Поэтому появление RFID-идентификаторов MAX66040 и MAX66140 позволяет с минимальными усилиями перевести хорошо зарекомендовавшие себя СКД-приложения, реализованные на «таблетках», на более современный, более удобный в использовании и просто более эстетичный форм-фактор носителя информации. Именно с этим связан параллельный выпуск двух модификаций: под стандарты ISO/IEC 14443B (proximity card) и ISO/IEC 15693 (vicinity card). Применение «таблеток» требовало непосредственного контакта со считывателем. Причем, поскольку и ключи, и считыватели создавались одной компанией и появились одновременно, то вопрос о различных стандартах просто не возникал. Для RFID-приложений уже сложилось два направления: высокоскоростной обмен данными в непосредственной близости от считывателя, или малая скорость на большем расстоянии. У разных разработчиков могут быть разные условия или предпочтения, поэтому предложены оба варианта функциональной замены.

Заключение

Отметим, что компания Maxim в линейке RFID-продуктов не предлагает чипы. Предлагаются только брелки и бесконтактные карты, то есть законченные изделия-идентификаторы. Как законченные изделия ключи компании Maxim не имеет смысла сравнивать с простейшими бесконтактными ключами множества производителей Юго-Восточной Азии и других регионов. Основное предназначение моделей MAX66040 и MAX66140 – замена контактных «таблеток» с реализованным алгоритмом хеширования SHA-1 на бесконтактные proximity- и vicinity-решения в тех системах контроля доступа, где компоненты Maxim успешно зарекомендовали себя в исполнении iButton.

Получение технической информации, заказ образцов, поставка – *e-mail: analog.vesti@compel.ru*