Новые приборы семейства iButton:

расширение возможностей по защите информации

Микросхемы семейства iButton компании Dallas Semiconductor традиционно применяются специалистами в области информационной безопасности в качестве электронных идентификаторов персонала. Успех iButton у разработчиков и потребителей обусловлен простотой сопряжения с компьютером, невысокой стоимостью самих приборов и средств подключения. Приборы iButton имеют защищенный корпус, легко крепятся на пластиковом брелке, могут одновременно служить ключом для нескольких приложений.

Андрей Лютько

chip@rainbow.by

Евгений Левин

lev@rainbow.by

Обычно в комплексах защиты информации используется серийный номер прибора, уникальный в каждом изделии, а также энергонезависимая память, позволяющая сохранять ключевую информацию. Из всей гаммы микросхем iButton наибольшее применение нашли устройства DS1990 без энергонезависимой памяти и DS1992 с перезаписываемой памятью 1 кбит. В случае потребности в большем объеме памяти специалисты могут использовать приборы DS1993 (4 кбит), DS1995 (8 кбит), DS1996 (16 кбит).

Открытая память перечисленных выше приборов создает определенные неудобства для разработчиков, которые они, впрочем, научились успешно преодолевать. Неудобства следующие: теоретическая возможность эмуляции идентификационного кода приборов и возможность несанкционированного считывания или изменения хранящихся в их памяти данных. Для противодействия эмуляции номера традиционно пытаются проверить личность владельца электронного ключа, запрашивая у него пароль, который должен быть введен с клавиатуры. Для защиты памяти от изменения ее содержимое шифруют.

По непонятным причинам в поле зрения разработчиков до сих пор не попали такие приборы Dallas Semiconductor, как DS1961S и DS1963S. Эти приборы специально созданы для приложений, требующих повышенной защищенности, и уже успешно применяются за рубежом.

Безопасность

Принципиальным отличием приборов iButton серии DS196xS является то, что они разработаны специально для противостояния попыткам изменения данных в памяти устройства или попыткам эмуляции поведения устройства. Безопасность устройств основана на SHA-1 (Secure Hash Algorithm) [1] — аппаратно реализованном алгоритме цифровой подписи данных (вычисления хэш-кода).

Механизм безопасности основан на преобразовании входного потока данных при помощи хэш-алгоритма с применением некоторых начальных установок. И хост (ведущий компьютер или контроллер), и прибор могут либо подписать поток передаваемых данных, либо проверить подпись другого устройства. Подписать данные означает вычислить хэш-функцию от этих данных и состояния соответствующих регистров устройства. Проверить подпись означает самостоятельно вычислить хэш-функцию для входящего потока данных и состояния соответствующих регистров и параметров, и сравнить ее со значением, полученным от передающего устройства. Существенно, что вычисление и проверка подписи хоста выполняются внутри приборов DS1961S, DS1963S на основании недоступных извне секретных кодов. Таким образом, гарантируется невозможность эмуляции приборов и подмены данных.

Для параметризации вычисления хэш-функции применяется несколько цифровых кодов. Один из них называется «секретным кодом». Секретный код заносится в память микросхемы ведущим устройством и не может быть прочитан ни этим, ни другим устройством ни при каких условиях. Мастер может записать новый секретный код в память или вычислить новый секретный код, зная старый. Секретный код в памяти мастера используется только для вычисления хэш-кода и не передается в микросхему при обмене данными. Для параметризации вычисления хэш-функции применяется также состояние идентификационного регистра микросхемы, известное и хосту, а также открытые коды, например, пин-код.

Для первого подписания данных в память прибора необходимо записать секретный код. То же значение секретного кода должно быть записано в базу данных хоста. Обязательным условием правильной работы алгоритма цифровой подписи является идентичность секретных кодов в памяти хоста и устройства. Для систем повышенной секретности может быть применен режим вычисления нового секретного кода на основе старого секретного кода, данных идентификационного регистра и дополнительной информации, указанной хостом. На основе этих данных новый секретный код будет вычислен и записан вместо старого. В этом режиме хост должен вычислить секретный код по тому же алгоритму и изменить его в своей базе данных.

Для исключения несанкционированного изменения памяти данных подлинность хоста проверяется при записи новых данных в память устройства. После записи данных устройство вычисляет хэш-код,

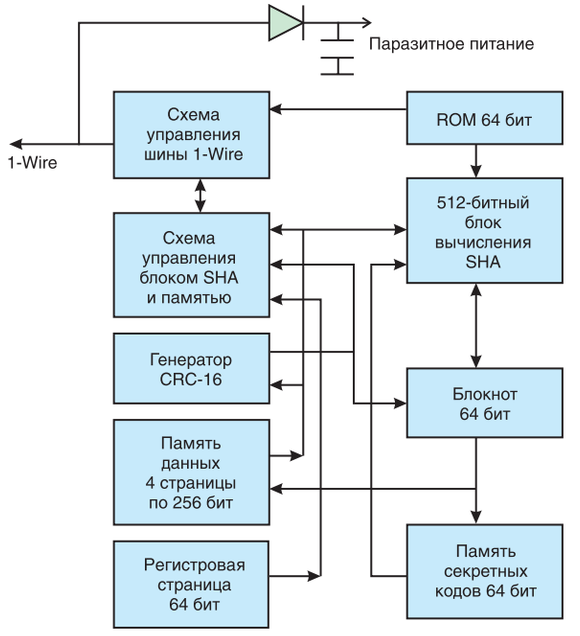

Рис. 1. Структурная схема DS1961S

используя данные страницы памяти, куда предполагается запись, частично данные блокнота, секретного кода и данных идентификационного регистра. То же самое должен сделать мастер и передать результат в устройство. При совпадении обоих хэш-кодов, данные переписываются в требуемую страницу памяти. Если же хэш-коды не совпали, то новые данные игнорируются.

Чтобы быть уверенным в подлинности прибора, хост должен прочитать для начала его серийный номер. Если серийный номер числится в базе данных хоста, то прибор считается подлинным. После признания прибора подлинным хост должен проверить цифровую подпись хранимых данных для исключения подделки устройства путем его эмуляции или копирования.

Основную роль при определении подделанных данных играет секретный код. Он никогда не может быть считан из памяти устройства, а высокая разрядность (64 бит) практически исключает его подбор. Поэтому даже при полной эмуляции микросхемы используя любые технические средства, ошибка подписи данных будет обнаружена. Точно так же, при возможном копировании данных в другое устройство, кроме ошибки подписи будет обнаружено несоответствие серийного номера.

Прибор DS 1961S для проведения электронных платежей

Кроме стандартного для всех приборов семейства iButton уникального 64-битного номера (код этого семейства — 33H), микросхемы серии DS1961S имеют энергонезависимую память (EEPROM) объемом 1128 бит, разделенную на 4 страницы по 256 бит для записи данных пользователя. Дополнительно существует 64-битная память секретного кода, доступная только для записи, при чтении из нее читается код FFh, а также 8-байтная страница регистров управления, в которую пользователь может записать до пяти собственных байт. Запись данных в микросхему возможна только при условии знания секретного кода, возможности вычисления на его основе и передачи вычисленного 160-битного MAC (Message authentication code) кода для авторизации. Исключением является область секретного кода. Страницы секретного кода и страницы памяти данных могут быть защищены от последующей записи или переведены в режим эмуляции EPROM. Прибор имеет встроенное ядро SHA-1 для вычисления хэш-кода (или MAC-кода в терминах DS1961S). Как и прочие устройства семейства iButton, DS1961S содержит буферную область памяти, называемую блокнотной, для промежуточной верификации данных. Информация сначала записывается в блокнотную память, откуда может быть считана для проверки. После проверки данные переписываются в прибор по определенному адресу, используя команду копирования блокнота, если был принят правильный 128-битный проверочный MAC-код. Для вычисления MAC-кода используется секретный код и дополнительные данные, записанные в память DS1961S, включая данные идентификационного регистра. Новый секретный код может быть перезаписан без вычисления MAC-кода.

Обзор

Структурная схема DS1961S приведена на рис. 1.

Микросхема включает шесть основных компонентов:

1) 64-битное ПЗУ кода семейства, используемое для общей идентификации микросхемы.
2) 64-битный блокнот.
3) Четыре 32-байтных страницы EEPROM.
4) 64-битная регистровая страница.
5) 64-битная память секретного кода.
6) 512-битное ядро SHA-1 (Secure Hash Algorithm).

При считывании и записи данных первым передается или принимается младший бит.

Как и в других устройствах семейства iButton, для чтения информации ведущее устройство должно сначала послать одну из команд функций ПЗУ:

1) Чтение ПЗУ.
2) Сравнение ПЗУ.
3) Поиск ПЗУ.
4) Пропуск ПЗУ.
5) Продолжение обмена.
6) Поиск ПЗУ в ускоренном режиме.
7) Сравнение ПЗУ в ускоренном режиме.

По окончании приема команд ускоренного режима, посланных на стандартной скорости, DS1961S переходит в ускоренный режим, и обмен данными осуществляется на повышенной

Таблица 1. Карта памяти DS1961S

Диапазон адресов	Описание	Примечания
0000h-001Fh	Страница 0 памяти данных	Доступ для записи невозможен без знания секретного кода
0020h-003Fh	Страница 1 памяти данных	Доступ для записи невозможен без знания секретного кода
0040h-005Fh	Страница 2 памяти данных	Доступ для записи невозможен без знания секретного кода
0060h-007Fh	Страница 3 памяти данных	Доступ для записи невозможен без знания секретного кода
0080h-0087h	Память секретного кода	Только для записи, знания секретного кода не требуется
0088h[1]	Защита от записи секретного кода	Активизируется кодом 55h или AAh
0089h[1]	Защита от записи страниц 0–3	Активизируется кодом 55h или AAh
008Ah[1]	Байт пользователя, защита от записи самого себя	Активизируется кодом 55h или AAh
008Bh[1]	Байт производителя, только для чтения	Считывается AAh или 55h
008Ch[1]	Байт пользователя/управление режимом EPROM для страницы 1[2]	Активизируется кодом 55h или AAh
008Dh[1]	Байт пользователя/защита от записи только страницы 0	Активизируется кодом 55h или AAh
008Eh-008Fh	Байт пользователя/код производителя	Функция зависит от значения байта производителя
0090h-0097h	64-битный идентификационный регистр	Только для чтения

[1] Будучи однажды запрограммированными значением 55h или AAh, эти адреса становятся доступными только для чтения. Любые другие коды не приводят к включению защиты от записи.

[2] При включенном режиме EPROM состояние битов в странице 1 может быть изменено только с '1' в '0', если память не защищена от записи.

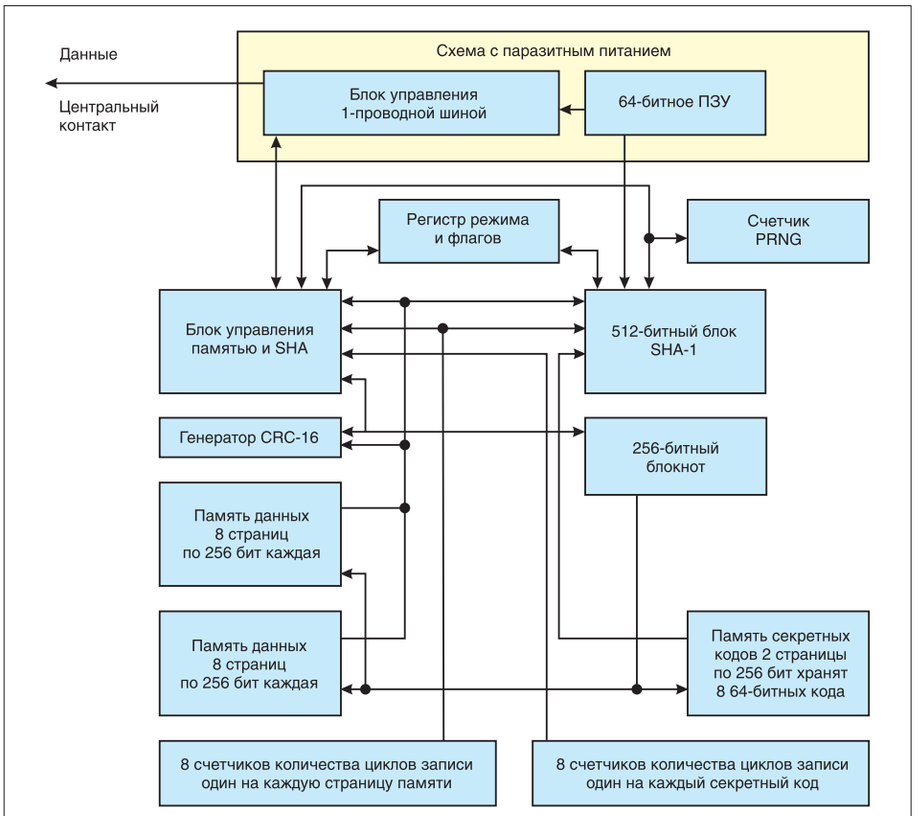

Рис. 2

скорости. После исполнения одной из команд функций ПЗУ DS1961S ожидает одну из команд работы с памятью или команду блока SHA:

1) Запись блокнота.
2) Чтение блокнота.
3) Загрузка первого секретного кода.
4) Вычисление нового секретного кода.
5) Копирование блокнота.
6) Чтение аутентифицированной страницы.
7) Обновление блокнота.
8) Чтение памяти.

Как и все микросхемы iButton, каждый экземпляр DS1961S содержит уникальный запрограммированный лазером номер длиной 64 бит. Первые 8 бит являются кодом семейства (33H), следующие 48 бит являются уникальным серийным номером, и последние 8 бит — контрольная сумма CRC-8 первых 56 бит. Информацию о контрольной сумме и методе ее вычисления можно найти в таблице 1.

Карта памяти

Как уже отмечалось, DS1961S имеет четыре области памяти — память данных, память секретного кода, блокнот и страница регистров с байтами пользователя и регистрами специальных функций. Блокнот используется как буфер при записи памяти и страницы регистров. Память данных и страница регистров размещены в линейном адресном пространстве (табл. 1) и имеют неограниченный доступ для чтения, но запись данных в эти области памяти требует знания секретного кода и правильного вычисления кода авторизации ведущим устройством.

Секретный код может быть запрограммирован путем копирования данных из блокнота в соответствующую область памяти. Второй механизм состоит в вычислении нового секретного кода на базе данных блокнота и прежнего секретного кода. Секретный код ни при каких обстоятельствах не может быть прочитан из памяти, доступ к нему для чтения имеет только блок SHA для вычисления кодов аутентификации сообщений.

Диапазон адресов 88h-8Fh, называемый страницей регистров, содержит регистры специальных функций, байты пользователя и байт производителя. Единожды запрограммированные кодом 55h или AAh, большинство этих байтов становятся доступными только для чтения и не могут быть изменены в дальнейшем. Любые другие коды не приводят к активизации защиты этих байтов от записи. Байт производителя может иметь значение 55H или AAh. Обычно он имеет значение 55h, указывая на то, что адреса 008Eh и 008Fh доступны пользователю для записи и чтения и не имеют никакой защиты. Значение AAh указывает на то, что эти два адреса защищены от записи и содержат запрограммированный производителем идентификатор. Этот идентификатор может использоваться программным обеспечением для упрощения опознавания микросхемы и быстрее выбирать подходящий секретный код. Идентификаторы назначаются и регистрируются изготовителем. Диапазон адресов 0090h-0097h — идентификационный регистр. Обычно он содержит копию регистрационного номера, записанного в ПЗУ, в том же формате. В заказных версиях в идентификационном регистре может находиться любая указанная пользователем последовательность.

Адресные регистры и состояние пересылки

DS1961S использует три адресных регистра: TA1, TA2 и E/S. Такие регистры имеются во многих других однопроводных устройствах, но работают они по-иному. Регистры TA1 и TA2 загружаются соответственно младшим и старшим байтами адреса назначения и указывают, куда должны быть записаны или откуда считаны данные. Регистр E/S является регистром состояния пересылки и доступен только для чтения. Он используется для проверки целостности данных при выполнении команд записи. Так как блокнот DS1961S способен принимать данные только в виде блоков по 8 байт, младшие 3 бита регистра TA1 всегда равны нулю, а три младших бита регистра E/S (конечное смещение) всегда считываются как единицы. Это означает, что все данные блокнота используются для последующего копирования в основную память секретного кода. Бит 5 регистра E/S, называемый PF или флагом неполного байта, устанавливается в 1, если число бит данных, переданных мастером не кратно 8, или если данные в блокноте недействительны из-за пропадания питания. Успешная запись данных в блокнот очищает бит PF. Старший бит регистра E/S называется AA или битом принятия авторизации. Он указывает на то, что данные, сохраненные в блокноте, уже были скопированы в память по адресу назначения. При записи данных в блокнот этот флаг автоматически очищается.

Подробное техническое описание DS1961S можно найти на сайте w www.maxim-ic.com.

Прибор DS 1963S с блоком SHA и встроенным ОЗУ

Отличия DS1963S от DS1961S: увеличенный до 4096 бит объем памяти, наличие на кристалле ОЗУ вместо EEPROM, счетчики числа записи страниц, а также возможность использования микросхемы как сопроцессора для вычисления MAC-кодов. Счетчики числа записи страниц являются дополнительным механизмом безопасности. Они позволяют мгновенно выявить попытки несанкционированной записи в память, для чего необходимо вести программный счет количества циклов записи и сравнивать его с показаниями аппаратного счетчика циклов записи. Применение устройства в качестве сопроцессора безопасности хоста позволяет разгрузить процессор хоста и повысить уровень секретности системы за счет хранения секретного кода в памяти DS1963S, откуда он не может быть считан ни при каких условиях.

Энергонезависимая память прибора объемом 4096 бит, разделена на 16 страниц по 256 бит с возможностью записи-чтения. Восемь страниц памяти имеют индивидуальные 64-битные секретные коды и 32-битные «только для чтения» счетчики количества циклов записи без переполнения. Секретные коды имеют индивидуальные 32-битные счетчики количества циклов записи. Чтение содержимого секретных кодов невозможно. Так же, как и в других приборах семейства iButton, DS1963S содержит область блокнота, предназначенную для проверки записываемых данных до их окончательного занесения в память.

DS1963S имеет свой собственный уникальный 64-битный регистрационный номер, который записан в ПЗУ лазером в процессе изготовления, что обеспечивает гарантированную

идентификацию и позволяет осуществлять абсолютный контроль.

Область применения микросхемы — системы оплаты и идентификации, требующие высокой степени секретности.

Обзор

Структурная схема устройства показана на рис. 2.

DS1961S имеет шесть основных компонентов:

1) 64-битное ПЗУ, запрограммированное лазером.
2) 256-битный блокнот.
3) Восемь 32-байтных страниц ОЗУ общего назначения.
4) Восемь 32-байтных страниц ОЗУ, защищенных счетчиками циклов записи.
5) Две 32-байтных страницы, хранящие восемь 64-битных секретных кодов с индивидуальными счетчиками количества циклов записи.
6) 512-битное ядро SHA-1.

Для чтения информации мастер шины вначале должен послать одну из команд функций ПЗУ:

1) Чтение ПЗУ.
2) Сравнение ПЗУ.
3) Поиск ПЗУ.
4) Пропуск ПЗУ.
5) Продолжение обмена.
6) Поиск ПЗУ в ускоренном режиме.
7) Сравнение ПЗУ в ускоренном режиме.

По окончании команд ускоренного режима, посланных на стандартной скорости, устройство переходит в ускоренный режим, когда обмен данными осуществляется на повышенной скорости. После того как команда ПЗУ успешно выполнена, становятся доступными функции памяти, и мастер может передавать одну из 8 команд функций памяти. При считывании и записи данных первым передается младший бит.

Карта памяти

Как уже отмечалось выше, DS1963S имеет четыре области памяти: память данных, память секретных кодов, счетчики и блокнот. Каждая из этих областей организована в виде страниц по 32 байт, как показано в таблице 2. Блокнот используется как буфер при записи в память данных или в память секретных кодов. Страницы 0–15 имеют неограниченный доступ для записи-чтения. Страницы 16 и 17 содержат восемь 64-битных секретных кодов, и их содержимое не может быть считано. Шестнадцать 32-битных счетчиков подсчитывают количество циклов записи в страницы 8–16 и в область каждого из восьми секретных кодов. Счетчики расположены в страницах 19–20 и могут быть только считаны. Страница 21 содержит счетчик, который инкрементируется при каждом запуске блока SHA (счетчик PRNG). Его значение может быть использовано для генерации псевдослучайных чисел, а также как измеритель ресурса встроенной батареи. Блокнот расположен в блоке № 18.

Адресные регистры

DS1963S использует три адресных регистра: TA1, TA2 и E/S. Регистры TA1 и TA2 загружаются адресом назначения, указывающим, куда должны быть записаны или откуда считаны данные. Регистр E/S является счетчиком байт и регистром состояния пересылки. Он доступен только для чтения. Пять младших битов этого регистра содержат адрес последнего байта, скопированного в блокнот (конечное смещение). Бит 5 — флаг неполного байта. Он устанавливается, когда число принятых битов не кратно 8. Бит 6 не несет никаких функций и всегда читается как 0.

Старший бит регистра E/S является флагом принятия авторизации, если он установлен в 1, то это значит, что данные были успешно скопированы в память. Запись данных в блокнот очищает этот флаг.

Одно из отличий DS1963S от DS1961S заключается в том, что блокнот также может быть защищен от несанкционированного чтения. Защита блокнота автоматически включается после обнаружения сигнала «сброс», и снимается и устанавливается в дальнейшем блоком SHA или командой очистки блокнота. Это позволяет обеспечить защиту секретных данных, которые, возможно, остались в блокноте от предыдущего обмена от несанкционированного чтения.

Высокая защищенность описанных приборов позволяет применять их для хранения данных и аутентификации в системах, требующих повышенной безопасности. Такими приложениями являются платежные системы, в том числе и на АЗС, на транспорте, системы удаленного доступа к ресурсам, системы защиты ПЭВМ от несанкционированного доступа. Известны приложения, в которых устройства использованы в составе электронных счетчиков с предоплатой в качестве индивидуальных ключей, а также в качестве персональных электронных кошельков в глобальной платежной системе.

Авторы надеются, что полученная информация позволит специалистам в области создания платежных приложений, систем информационной и объектовой безопасности по-новому взглянуть на возможности хорошо известных им устройств семейства iButton.

Литература

1. FIPS PUB 180-1 «SECURE HASH STANDARD». Department of commerce. Technology administration. **h ttp://w ww.i tl.nist.gov/div897/pubs/fip180-1.htm.**
2. Book of DS19xx iButton standards.
3. App Note 152: SHA iButton Secrets and Challenges. **ht tp://w ww. maxim-ic.com/appnotes.cfm/appnote_number/835**.
4. Securing Electronic Transactions Using SHA-1 Secure Hash Algorithm. ht tp://w ww. maxim-ic.com/appnotes.cfm/appnote_number/1770.
5. App Note 154: Passwords in SHA Authentication. **h ttp://w ww .maxim-ic.com/appnotes.cfm/appnote_number/974**.
6. White Paper 3: Why are 1-Wire SHA-1 Devices Secure? **h ttp://w ww.maxim-ic.com/appnotes.cfm/appnote_number/1098**.
7. White Paper 4: Glossary of 1-Wire SHA-1 Terms. **h ttp://w ww. maxim-ic.com/appnotes.cfm/appnote_number/1099**.
8. App Note 157: SHA iButton API Overview. **ht tp://ww w. maxim-ic.com/appnotes.cfm/appnote_number/1016**.

Таблица 2. Карта памяти DS1963S

№ страницы	Диапазон адресов	№ секретного кода	№ счетчика	Инкремент счетчика
0	0000h–001Fh	0	0	Нет
1	0020h–003Fh	1	1	Нет
2	0040h–005Fh	2	2	Нет
3	0060h–007Fh	3	3	Нет
4	0080h–009Fh	4	4	Нет
5	00A0h–00BFh	5	5	Нет
6	00C0h–00DFh	6	6	Нет
7	00E0h–00FFh	7	7	Нет
8	0100h–011Fh	0	0	При записи
9	0120h–013Fh	1	1	При записи
10	0140h–015Fh	2	2	При записи
11	0160h–017Fh	3	3	При записи
12	0180h–019Fh	4	4	При записи
13	01A0h–01BFh	5	5	При записи
14	01C0h–01DFh	6	6	При записи
15	01E0h–01FFh	7	7	При записи

Таблица 2. Карта памяти DS1963S (продолжение)

№ страницы	Диапазон адресов	Описание
Память секретных кодов с доступом пользователя только по записи		
16	0200h–0207h	Секретный код 0
	0208h–020Fh	Секретный код 1
	0210h–0217h	Секретный код 2
	0218h–021Fh	Секретный код 3
17	0220h–0227h	Секретный код 4
	0228h–022Fh	Секретный код 5
	0230h–0237h	Секретный код 6
	0238h–023Fh	Секретный код 7
Память счетчиков с доступом пользователя только для чтения		
19	0260h–0263h	Счетчик 0 (циклы записи для страницы 8)
	0264h–0267h	Счетчик 1 (циклы записи для страницы 9)
	0268h–026Bh	Счетчик 2 (циклы записи для страницы 10)
	026Ch–026Fh	Счетчик 3 (циклы записи для страницы 11)
	0270h–0273h	Счетчик 4 (циклы записи для страницы 12)
	0274h–0277h	Счетчик 5 (циклы записи для страницы 13)
	0278h–027Bh	Счетчик 6 (циклы записи для страницы 14)
	027Ch–027Fh	Счетчик 7 (циклы записи для страницы 15)
20	0280h–0283h	Счетчик циклов записи секретного кода 0
	0284h–0287h	Счетчик циклов записи секретного кода 1
	0288h–028Bh	Счетчик циклов записи секретного кода 2
	028Ch–028Fh	Счетчик циклов записи секретного кода 3
	0290h–0293h	Счетчик циклов записи секретного кода 4
	0294h–0297h	Счетчик циклов записи секретного кода 5
	0298h–029Bh	Счетчик циклов записи секретного кода 6
	029Ch–029Fh	Счетчик циклов записи секретного кода 7
21	02A0h–02A3h	PRNG-счетчик