

На процедуру проверки возлагаются такие обязанности, как расшифрование защищенного исполнимого кода, проверка целостности некоторых участков или всей программы, инициализация ряда важных для работы переменных и т.п. Именно по вышеперечисленным причинам изъять процедуру проверки не получится.

ЗАКЛЮЧЕНИЕ

Одним из наиболее качественных методов защиты программ является криптографическое преобразование информации. Согласно правилу Кирхгофа, стойкость криптозащит определяется исключительно стойкостью секретного ключа. Даже если алгоритм работы такой защиты известен, это не сильно упрощает его взлом. При условии правильного выбора длины ключа, криптозащиты не ломаемы в принципе.

При реализации процедуры проверки серийного номера наиболее уязвимые места – это операция сравнения и передача управления на определенную ветвь кода. Однако операцию сравнения нужно использовать для предварительной проверки введенного ключа, так что ее результат является лишь защитой от ошибочного набора номера. Чтобы исключить возможность передачи управления на участок кода, отвечающий за последствия правильного ввода номера, необходимо использовать шифрование этого кода на основе ключа, генерируемого из введенного серийного номера.

УСТРОЙСТВО КАРДИОМОНИТОРИНГА НА ОСНОВЕ МОБИЛЬНОГО ТЕЛЕФОНА КЛАССА «SMARTPHONE»

А. В. Столяров

На протяжении многих лет различные заболевания, связанные с сердечно-сосудистой системой, держат печальную пальму первенства в списке болезней человека и приводят к существенному сокращению продолжительности его жизни. Всем хорошо известно, что для любых болезней, наряду с профилактикой, исключительно важным является их раннее обнаружение и диагностика. Это обуславливает значительное внимание, уделяемое вопросам создания и развития современных средств автоматизированного инструментального исследования сердечно-сосудистой системы человека.

Наиболее распространенным и доступным для широкого круга людей методом инструментального исследования сердечно-сосудистой системы была и остается электрокардиография, основу которой составляет реги-

страция биопотенциалов, возникающих в сердце, точнее – электрических потенциалов, возникающих при сокращении сердечной мышцы. Имеется зависимость между электрической активностью сердца и его функциональным состоянием, что открывает возможности для диагностики заболеваний сердца. Анализируя направление и скорость распространения волн поляризации в сердце, оказывается возможным определять не только его функциональное состояние, но и выявлять очаги повреждений миокарда.

Несмотря на достаточную сложность интерпретации информации, получаемой с помощью электрокардиографии, имеются относительно простые методики, позволяющие с ее помощью оценить состояние сердечно-сосудистой системы, а также организма в целом.

В настоящее время существует много разновидностей и моделей электрокардиографов. Однако до сих пор эти приборы не преодолели некоторый рубеж по своей стоимости и удобству применения, когда они могли бы стать массовыми приборами медицинского назначения, используемыми человеком в его повседневной жизни. А это весьма актуально, поскольку даже не очень занятые люди могут позволить себе регулярные, лучше ежедневные, посещения врача для снятия и анализа кардиограммы. Более того, даже если удастся такие процедуры делать регулярно, далеко не все нарушения сердечной деятельности могут быть выявлены, поскольку многие сбои в работе сердца происходят в период напряженной физической нагрузки или высокого психоэмоционального напряжения человека, а не в расслабленном состоянии на приеме у врача.

Не так давно появились и получили активное развитие так называемые «Холтеровские кардиографы». Эти устройства достаточно малогабаритны, автономно работают от встроенного аккумулятора и способны производить регистрацию кардиограммы в буферной памяти, например, в течение суток. Однако для расшифровки полученных результатов необходимо подключение в стационарных условиях к компьютеру врача.

Для обеспечения удобной непрерывной регистрации и экспресс-анализа электрокардиограмм (ЭКГ) автором разработано автономное устройство, работающее под управлением мобильного телефона с расширенными возможностями класса Smartphone, представляющим собой гибрид портативного компьютера (PDA) и мобильного телефона. Для улучшения комфортности применения устройства в качестве интерфейса его электронной измерительной части с управляющим телефоном использована технология беспроводной передачи данных Bluetooth. Это обеспечивает работу устройства в режиме непрерывного кардиомониторинга пользователя при отсутствии жесткой привязки измерительного

блока к телефону – последний может находиться на расстоянии до 100 м (на открытой местности) от пользователя – и сохранении обычной функциональности телефона. Кроме того, в роли управляющего компьютера для устройства может выступать любой другой переносной (типа «ноутбук») либо стационарный (офисный) компьютер с подключенным к нему Bluetooth адаптером.

Устройство состоит из двух основных компонент: блока регистрации и блок управления на основе компьютера (телефона «Smartphone»). Блок регистрации выполнен в виде малогабаритного автономного электронного модуля, носимого на поясе. Он имеет встроенный источник питания, использующий Li-Ion аккумулятор, в котором реализована возможность контроля потребления и отключения аналогового входного тракта блока регистрации во время ожидания команд. Блок регистрации имеет на входе пять электродов, используя четыре из шести грудных отведений Вильсона (Рис. 1) и пятый опорный электрод [1, 2]. Так как сигнал, поступающий с электродов, достаточно слабый (2–8 мВ), то для усиления его применяются инструментальные усилители. Схема на усилителях реализована таким образом, что с помощью пятого опорного электрода удастся практически избавиться от синфазной помехи в 50 Гц. Для борьбы с шумами, возникающими при сокращении мышц, и иными, то есть получить максимально «чистый» электрокардиосигнал (рис. 2), использовались три стадии фильтрации:

- 1) аналоговый фильтр собранный после усилителей;
- 2) цифровые фильтры встроенные в АЦП и способные самостоятельно определять верхнюю граничную частоту входного сигнала;
- 3) цифровой полосовой фильтр низких частот, реализованный в процессоре блока регистрации (полосовой фильтр Баттерворта) с частотами среза 0,05 Гц снизу и 100 Гц [3].

Для оцифровки сигнала использовалось 22-разрядное Σ - Δ АЦП фирмы Analog Devices, специально разработанное для применения в биомедицинских системах, имеющее встроенный цифровой ФНЧ, выполненное по LC^2MOS технологии и потребляющее 35 мВт. Блок регистрации содержит также цифровой процессор с архитектурой ARM7, общей производительностью 54 MIPS при тактовой частоте 60 МГц, который осуществляет приём данных от АЦП, их сохранение в кольцевом буфере и

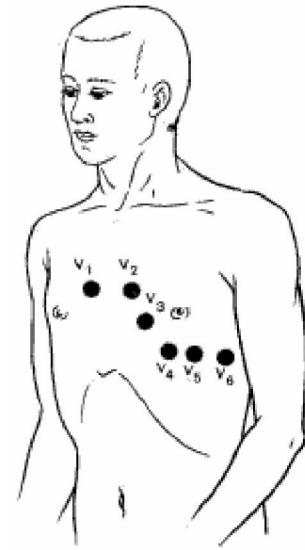


Рис. 1. 6 грудных отведений Вильсона

предварительный анализ электрокардиосигнала, например, на предмет наличия последнего в случае плохого контакта электродов с поверхностью кожи. Кроме того, процессор производит сжатие данных с помощью аудиокодека, реализованного программно, и поддерживает передачу сжатого потока данных с помощью модуля беспроводного интерфейса Bluetooth класса 1.

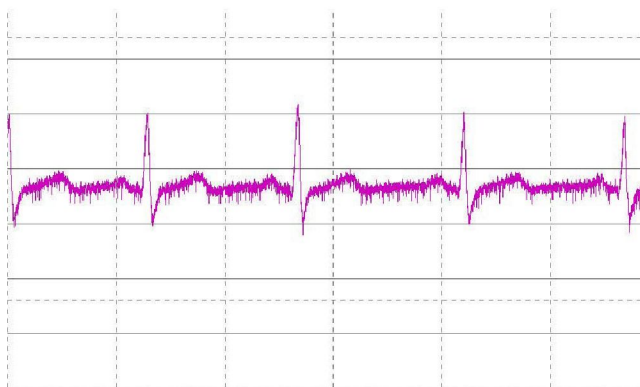


Рис. 2. Усиленный и оцифрованный сигнал

Блок управления на основе мобильного телефона класса «Smartphone» осуществляет общее управление устройством, прием, оперативное и долговременное хранение и экспресс-анализ электрокардиосигнала. Телефон имеет встроенный процессор архитектуры ARM9, имеющий общую производительность 220 MIPS при тактовой частоте 200 МГц. Он работает под управлением операционной системы (ОС) Windows Mobile, являющейся 32-битной ОС реального времени, позволяющей, используя предоставляемый пользовательский интерфейс WinAPI, создать достаточно сложное приложение.

Работа и структура приложений в Windows Mobile схожа с настольными версиями Windows, в частности, каждому процессу выделяется четырех гигабайтное адресное пространство виртуальное адресное пространство, определяются приоритеты процесса и т.д. Но есть и отличия, которые свойственны только мобильным устройствам. Windows Mobile имеет двухуровневую архитектуру. Верхний уровень – это ядро системы, включающее модули, обслуживающие аппаратную часть, так называемые драйвера, и процессы, занимающиеся высокоприоритетными задачами. Нижний уровень – это прикладные программы, интерфейсная и пользовательская часть.

В Windows Mobile, как и в настольной версии Windows, ядро выполняет основной цикл и обработку всех запросов, приходящих от драйверов и процессов верхнего уровня, либо от активных процессов нижнего уровня. Аппаратная часть Windows Mobile не доступна для пользователя с нижнего уровня напрямую, с ней можно работать через драйвера посредством интерфейса WinAPI.

Использование Windows Mobile и учет вышеописанных нюансов позволили разработать достаточно эффективную программу кардиоанализа

«Cardio». Программа состоит из основного модуля анализа и обработки данных, модуля сбора данных, графического модуля и блока, работающего с радиомодулем телефона. Кроме того, в программе реализованы модули управления питанием блока регистрации, блока формирования сигнальных данных отправляемых через службу коротких сообщений SMS, блока формирования ЭКГ передаваемой через Internet с помощью услуги GPRS и другие. Результат анализа выводится непосредственно на экран мобильного телефона «Smartphone», либо сохраняются на карту памяти.

Следует отметить также, в качестве существенного достоинства разработанной программы, реализацию в ней алгоритма определения местоположения пользователя с помощью технологии GSM, что очень важно для пользователя, оказавшегося в критической ситуации.

Литература

1. *Суворов А. В.* Клиническая электрокардиография.- НГМИ. Нижний Новгород, 1993.- с 5.-34
2. *Ripley K. L., Bump T. E., and Arzbaecher R. C.* Evaluation of techniques for recognition of ventricular arrhythmias by implanted devices. / *IEEE Trans. Biomed. Eng.* – Vol. 36, 1989/ – p. 618–624
3. *Крекрафт Д., Джерджли С.* Аналоговая электроника. Схемы, системы, обработка сигнала. – М., 2005. с. 34–101

СПОСОБЫ И АЛГОРИТМЫ ЭФФЕКТИВНОЙ ПРОГРАММНОЙ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

В. А. Трофимчук

В процессе интенсивного развития беспроводных коммуникационных технологий возникает необходимость обеспечения безопасности при передаче данных. Одним из методов реализации конфиденциального трафика является применение криптографических преобразований. При реализации криптопреобразований, особенно несимметричных, возникают проблемы, связанные малым быстродействием используемых алгоритмов. В данной работе рассматриваются несколько способов вычисления произведения kP , где k – большое целое число, P – точка на плоскости. Данная операция является основной при реализации криптосистем на основе эллиптических кривых [1].

При создании криптографических систем нужно учитывать, что все вычисления производятся по модулю некоторого целого числа p . В частности, это означает, что используются не произведения и суммы чисел, а остатки от деления этих произведений и сумм на данный модуль. При