заключается в подборе того коэффициента, на который умножали базовую точку. Именно этот коэффициент является закрытым ключом.

На рисунке 1 представлена структурная схема устройства для генерации цифровой подписи. В случае использования стандартной эллиптической кривой схему можно упростить, убрав генератор параметров эллиптической кривой и подавая на вход блоков электронной подписи соответствующие параметры.

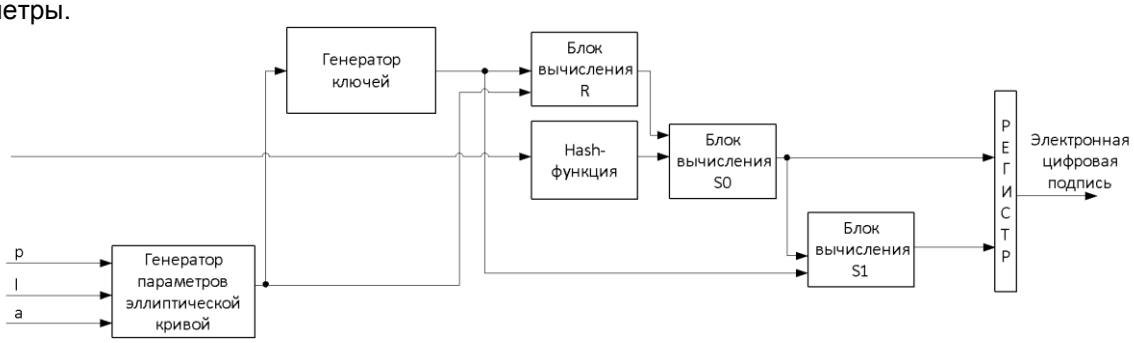

Рисунок 1 – Структурная схема устройства для выработки электронной цифровой подписи

$R = k * G$, где G – базовая точка, являющаяся выходом генератора параметров эллиптической кривой. Блоки S0 и S1 являются частями итоговой подписи и выражаются следующими формулами:

$S_0 =< belt - hash(OID(h)|| < R >_{2l} ||H) >_l$,

$S_1 =< (k - \underline{H} - \left(\underline{S_0} + 2^l\right) d \ mod \ q) >_{2l}$, где belt-hash – функция хэширования, H – выход блока хэш-функции, OID – идентификатор функции($06092A7000020022651F51_{16}$), R – выход блока вычисления R, d – личный ключ, q – порядок группы точек из поля Fp.

Уровень стойкости равен 128. Длина итоговой подписи равна 384 бита.

Одним из блоков алгоритма электронной цифровой подписи является блок вычисления функции хэширования. В качестве функции хэширования выбрана функция из стандарта СТБ 34.101.31-2011, в основе вычисления которой лежит алгоритм блочного шифрования из того же стандарта. При использовании данной хэш-функции в алгоритме электронной цифровой подписи на ее вход подается сообщение фиксированной длины. На выходе функции получается хэш-значение длиной 256 бит.

Приведенное устройство реализуется на базе FPGA семейства Virtex 7 фирмы Xilinx.

Аппаратную реализацию цифровой подписи можно использовать для проверки транзакций криптовалют, цифровых операций с валютами (платежами), подписи на электронные документы и любые другие файлы.

Список использованных источников:

1. Информационные технологии. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых : СТБ 34.101.45–2013. – Введ. 30.08.201. – Минск : Госстандарт, 2013. – 41 с.

УСТРОЙСТВО ДЛЯ НЕПРЕРЫВНОГО НЕИНВАЗИВНОГО ИЗМЕНЕНИЯ АРТЕРИАЛЬНОГО ДАВЛЕНИЯ

Крылов Н.Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Азаров И.С. – д.т.н.,доцент

Развитие микроэлектроники и элементной базы позволило выйти носимой электронике на новый уровень. Однако ряд актуальных задач остается нерешенным. Одной из таких задач является непрерывное неинвазивное измерение артериального давления. Решить данную задачу призваны алгоритмы машинного обучения.

На сегодняшний день измерение артериального давления вне реанимации производится методом Короткова, что доставляет дискомфорт пациенту и не позволяет производить непрерывное измерение. Решение данной проблемы возможно при измерении давления по косвенным признакам. Наиболее точным методом является измерение методом допплерографии, однако такой подход является технически сложным, дорогим и менее исследованным. Альтернативным подходом является анализ кривой фотоплетизмограммы (далее PPG). Существуют исследования[1-3],

показывающие эффективность такого подхода, однако исследования проводились с использованием данных, полученных в лабораторных условиях. В реальных условиях появляется множество артефактов из-за различных причин: двигательная активность, измерения во внешней среде. Избавиться от данных артефактов и повысить точность измерений возможно с применение технических и программных средств.

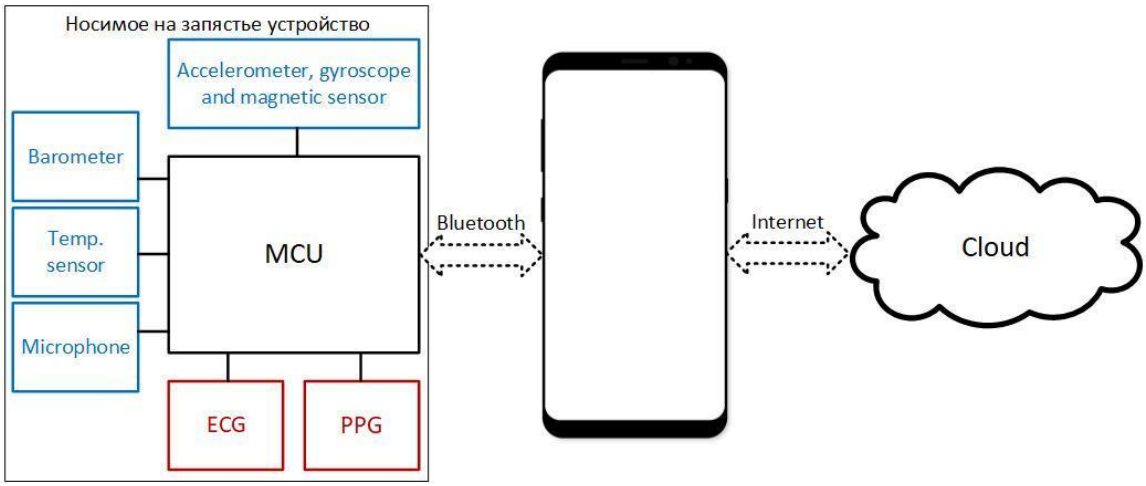

Рисунок 1 – Схема носимого устройства и системы взаимодействия

Применение современных комбинированных датчиков фотоплетизмографии, использующих свет с различной длинной волны, позволяет снимать с большей точностью кривую PPG и уровень сатурации кислородом крови.

Использование алгоритмов машинного обучения позволяет измерять давление с большей точностью. Для этого используется FFT кривой PPG и значение PWTT (Pulse Wave Transit Time – время распространения пульсовой волны)[3]. Использование данных о физической активности, данных о внешней среде и нескольких каналов PPG совместно с нейронной сетью позволяет дополнительно повысить точность измерения.

Вся система включает в себя носимое устройство, мобильное приложение и серверную часть. Серверная часть состоит из веб-сервиса, базы данных и модели сверочной и рекуррентной нейронной сети для определения артериального давления. Программное обеспечение носимого устройства включает модель машинного обучения для классификации активности.

Список использованных источников:

1. Xia Tan, Zhong Ji, Yadan Zhang, “Non-invasive continuous blood pressure measurement based on mean impact value method, BP neural network, and genetic algorithm”, Technol Health Care, 26(Suppl 1): 87–101, 2018.

2. Peng Su, Xiao-Rong Ding, Yuan-Ting Zhang, Jing Liu, Fen Miao, Ni Zhao, Long-term Blood Pressure Prediction with Deep Recurrent Neural Networks, arXiv preprint:1705.04524v3 [cs.LG], 2018.

3. Xiaoman Xing, Mingshan Sun, “Optical blood pressure estimation with photoplethysmography and FFT-based neural networks”, Biomed Opt Express, 7(8): 3007–3020, 2016.

ПРИМЕНЕНИЕ ДЕТЕКТОРА ГОЛОСА В СЛУХОВОМ АППАРАТЕ

Лайша А.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Вашкевич М.И. – к.т.н.,доцент

Слуховые аппараты — это электронные устройства, которые усиливают звуки выше порога слышимости пользователя с нарушениями слуха. Многие из пользователей слуховых аппаратов жалуются на дискомфорт восприятия их собственного голоса. При закрытии слухового канала слуховым аппаратом усиливаются низкочастотные компоненты голоса, а высокочастотные компоненты ослабляются ввиду звуковой проводимости костей. Это явление называется «эффект окклюзии» и является одной из критических проблем при ношении слуховых аппаратов.

Эффект окклюзии – причина, по которой пользователи жалуются на раздражающие или неестественные звуки. Проблема заключается в том, что из-за звуковой проводимости костей