

15. Галин Р.Р. Эффективная модель государственного управления на примере муниципального образования г. Томск. Всероссийская научно-техническая конференция «Научная сессия ТУСУР 2013». Автоматизация технологических процессов. Сборник докладов. Т., 2013.
16. Галин Р.Р. Тезисы «Эффективное государственное управление в социальном воспроизводстве общества». Изд. - Наука, образование, общество: тенденции и перспективы: сборник научных трудов по материалам Международной научно-практической конференции 31 января 2013 г., АР-Консалт, Москва, 2013. С 132, 133.

### МОДЕЛИРОВАНИЕ ЭЛЕКТРИЧЕСКОЙ АКТИВНОСТИ СЕРДЦА

*М.Г. Григорьев, аспирант, Н.В. Турушев, аспирант,  
Национальный исследовательский Томский политехнический университет  
634050, г. Томск, пр. Ленина, 30, тел. +7(913)-824-83-97  
E-mail: Mishatpu@sibmail.com*

По данным всемирной организации здравоохранения (ВОЗ) от болезней сердца и сосудов каждый год в мире погибают более 17 миллионов человек. Более того, согласно прогнозу ВОЗ к 2030 году умрет ещё около 23,6 миллионов человек. В России, в 2012 году от сердечно-сосудистых заболеваний (ССЗ) погибли 1 млн. 232 тыс. 182 человека (рис. 1)[1].

Основным наиболее распространенным в медицинских учреждениях различного уровня является электрокардиографический (ЭКГ) метод исследования состояния сердечно-сосудистой системы человека. ЭКГ метод является методом функциональной диагностики с количественной оценкой результатов исследования. Впервые кардиографические исследования были проведены в конце 19-го века шотландским ученым Александром Мьюхедом [2]. Тело представляет собой объемный проводник. Активная работа сердца приводит к генерации электромагнитного поля, которое может быть измерено на поверхности тела. Это поле в ходе возбуждения сердца постоянно меняется и характеристики этого поля в каждый момент времени зависят от того, в каком направлении движется по сердцу волна возбуждения. Изучение этого поля позволяет судить о последовательности возбуждения предсердий и желудочков.

Решением данной проблемы занимается множество предприятий, но особого успеха добились лишь единицы.



Рис. 1. Отчет ВОЗ по ССЗ за 2012 г.

Проведенный анализ показал, что в настоящее время отсутствуют аппаратно-программные комплексы (АПК) для массового применения (в отделениях функциональной диагностики и кардиологии, в стационарах, в поликлиниках и медико-санитарных частях, в машинах скорой помощи, а также в частной медицинской практике, в домашних условиях, в постоянно носимых аппаратах) с целью неинвазивного углубленного исследования сердца путем регистрации низкоамплитудных потенциалов сердца с поверхности тела человека без процедуры осреднения кардиоциклов и фильтрации. Подобные аппараты представлены в таблице 1.

Таблица 1

## Краткий обзор по фирмам – производителям

Название фирмы	Кол-во отведений	Уровень сигнала, мкВ	Частотный диапазон, Гц	Цена, тыс. руб.
Геолинк-Электроникс (Россия)	3	6	0,03-10,0	270
Rozinn (США)	3	8	0.05-70	385
OXFORD (Англия)	3	5	0,05-100	400
ФГБОУ ВПО НИ ТПУ (Россия)	3-12	0,3	0-10000	<50
Davis Medical Electronics Inc. (США)	3-12	2	0.05-60	227
HELLIGE (США)	3-12	5	0,05 -100	417
CardioMem CM 3000 (Германия)	3	8	0,03-70	160
Scan Tech Medical, LLC (США)	3	6	0.05-100	163

Как видно из таблицы, рыночная стоимость кардиографов известных компаний непомерно велика по сравнению с предложенным нами продуктом. Это связано с тем, что в устройстве используются разработанные нами наносенсоры, позволяющие без использования фильтров и осреднения получать сигналы нановольтового уровня.

Актуальным для совершенствования диагностики сердечно-сосудистых заболеваний, в том числе и для ранней диагностики сердца взрослых, детей, младенцев и плода, является разработка нового поколения наносенсоров и компьютеризированной ЭКГ-аппаратуры высокого разрешения для применения в поликлиниках и в домашних условиях.

Для решения данной задачи необходимо исследование численной модели распространения возбуждения в сердечной мышце.

Возбуждение распространяется по сердечной ткани с определенной скоростью, различной для разных отделов сердца (рис. 2).

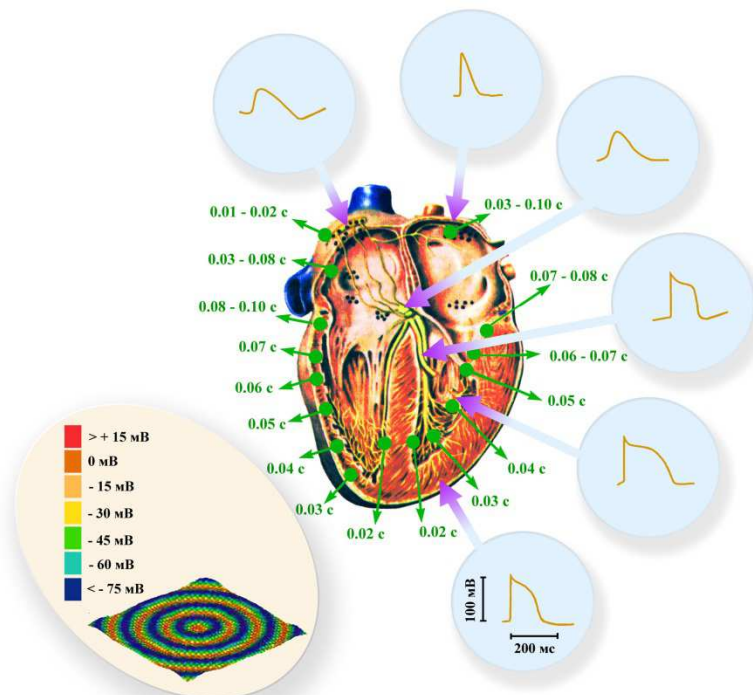


Рис. 2. Схема пространственно-временной организации нормальной работы сердца человека

Зеленые надписи и стрелки указывают время прихода волны возбуждения в данную область сердца. Голубые врезки показывают форму профиля бегущей волны (т.н. «потенциала действия») в

разных областях сердца, обусловленную различием свойств элементов возбудимой среды, которую формируют ткани сердца. Бежевая врезка — нормальное распространение бегущей волны возбуждения из пейсмекерной зоны в центре (синусового узла) в сторону краев (по рабочему миокарду) в простейшей имитационной математической модели [3].

В результате формируется пространственно-временная организация возбуждения сердца, обеспечивающая его функционирование. При моделировании процесса распространения возбуждения необходимо учитывать все особенности организации возбуждения в сердце.

Для моделирования распространения возбуждения предложена одна из простейших моделей возбудимых сред [4], двухкомпонентная модель Алиева-Панфилова. Модель реализована в виде уравнений типа «реакция – диффузия».

$$\frac{\partial u}{\partial t} = -ku \cdot (u - a) \cdot (u - 1) - uv + \Delta u, \quad (1)$$

$$\frac{\partial v}{\partial t} = -\left(\varepsilon_0 + \frac{\mu_1 v}{u + \mu_2}\right) \cdot (v + ku \cdot (u - a - 1)), \quad (2)$$

где  $u(x, y, t)$  – безразмерная функция, соответствующая трансмембранному потенциалу, и  $v(x, y, t)$  – безразмерная функция, соответствующая медленному мембранному току восстановления. При этом связи между клетками сердечной мышцы описываются диффузионными членами уравнений, а динамика отдельной клетки – реакционными нелинейными членами уравнений. Проведя ряд экспериментов, были определены параметры модели, при которых система лучше всего соответствует свойствам сердечной мышцы:  $k = 8.0$ ,  $\varepsilon_0 = 0.01$ ,  $\mu_1 = 0.2$ ,  $\mu_2 = 0.3$ ,  $a = 0.15$ .

Для реализации моделирования процесса распространения возбуждения в сердце, в рамках концепции оценки состояния сердечно-сосудистой системы (ССС), на базе лаборатории № 63 института неразрушающего контроля предполагается разработка аппаратно – программного комплекса. Алгоритм работы АПК представлен на рисунке 3.

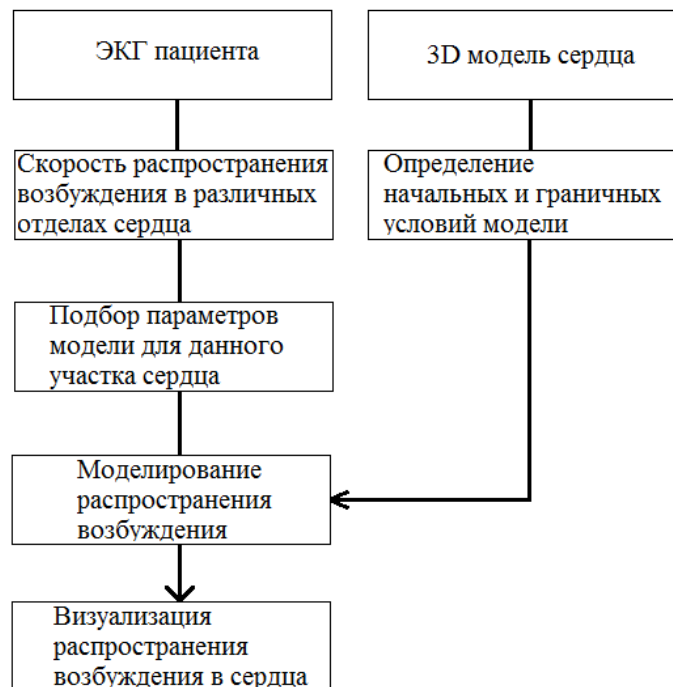


Рис. 3. Алгоритм моделирования процесса распространения возбуждения в сердце

Согласно алгоритму сначала на основе анализа кардиографической информации осуществляется задание начальных и граничных условий модели, затем определяются параметры модели для различных анатомических отделов сердца, и моделируется распространение возбуждения. По ре-

зультатам моделирования осуществляется визуализация распространения возбуждения на поверхности сердца пациента.

#### Литература

1. Сердечно – сосудистые заболевания. Информационный бюллетень №317. // Сайт Всемирной организации здравоохранения [Электронный ресурс]. – 2013. – Режим доступа: <http://www.who.int/mediacentre/factsheets/fs317/ru/index.html>. – Загл. с экрана.
2. Alexander Muirhead // Wikipedia.com: [Электронный ресурс]. – режим доступа: [http://en.wikipedia.org/wiki/Alexander\\_Muirhead](http://en.wikipedia.org/wiki/Alexander_Muirhead)(дата обращения: 11.02.2014).
3. Сердце человека // Wikipedia.ru: [Электронный ресурс]. – режим доступа: [http://ru.wikipedia.org/wiki/Сердце\\_человека](http://ru.wikipedia.org/wiki/Сердце_человека) (дата обращения: 18.02.2014)
4. Простейшие модели возбудимых сред // Mathematical Cell: [Электронный ресурс]. – режим доступа: [http://www.mathcell.ru/ru/obzors/obzor\\_Elkin2](http://www.mathcell.ru/ru/obzors/obzor_Elkin2) (дата обращения: 10.03.2014)

### АНАЛИЗ СТОЙКОСТИ КВАНТОВЫХ ПРОТОКОЛОВ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

*В.А. Эттель, доц, к.т.н., А.Н. Кайралапова, магистрант  
Карагандинский государственный технический университет  
100000, г. Караганда, Бульвар мира, 56, тел.: +7(7212)567592  
E-mail: aknur\_kan91@mail.ru*

Квантовая криптография как наука зародилась в 1984 году, когда был разработан первый квантовый протокол распределения ключей, названный BB84 [1]. В настоящее время квантовая криптография включает несколько разделов: квантовые протоколы распределения ключей (КПК), квантовые протоколы защищенной прямой связи, аутентификацию квантовых сообщения и квантовую цифровую подпись.

Квантовое распределение ключей – метод, с помощью которого между двумя абонентами (Алиса и Боб) может быть распределен секретный ключ, если они имеют доступ к квантовому каналу связи, т.е. каналу для передачи отдельных квантовых частиц, например, фотонов, и открытому обычному каналу с возможностью аутентификации отправителя сообщения. Основным преимуществом квантового распределения ключей перед обычными классическими схемами является принципиальная возможность обнаружить подслушивающего агента, который, в силу законов квантовой физики, при подслушивании вынужден возмущать состояния передаваемых квантовых частиц [2]. Таким образом, подслушивающий агент, по традиции называемый Евой, вносит в передаваемую последовательность бит определенный процент ошибок. Если уровень ошибок при передаче значительно превышает естественный уровень помех в канале, то это служит сигналом к прерыванию процедуры передачи ключа.

Целью настоящей работы является анализ стойкости двух протоколов с передачей кубитов к различным стратегиям атак подслушивающего агента.

Следует отметить, что доказательство стойкости всего протокола квантового распределения ключа является трудной теоретической задачей квантовой криптографии, которая в настоящее время не решена полностью ни для одного протокола. Однако некоторые аспекты безопасности различных КПК уже анализировались в литературе. В частности для некоторых протоколов и для некоторых конкретных стратегий атак уже получены зависимости  $I_{AE}(D)$ .

#### Стратегии атак подслушивающего агента

Простейшим видом съема информации в обычных оптических телекоммуникационных системах является разделение пучка фотонов. Однако в протоколах квантовой криптографии передача должна происходить посредством одиночных фотонов, и в таком случае Ева не может ответить часть сигнала. Поэтому данный вид атак не применим в квантово-криптографических системах в идеальных условиях однофотонных сигналов. На практике в настоящее время используют слабые когерентные импульсы, излучаемые лазерными светодиодами [3]. В настоящее время и в квантовой криптографии возможны атаки с разделением пучка фотонов.

Основные стратегии атак, которые может использовать Ева в случае, когда все сигналы содержат строго один фотон, подразделяют на два класса [2]. К первому классу относят *некогерентные* или индивидуальные атаки. При таких атаках Ева обрабатывает каждый фотон Алисы отдельно. Простейшим вариантом является атака перехвата – повторной отправки фотона. Ева перехватывает