ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕМЕДИЦИНСКИХ СИСТЕМАХ НА ОСНОВЕ МОДЕЛЬНОГО ПОДХОДА

***Булдакова Татьяна Ивановна**, доктор технических наук, профессор, г. Москва*
***Суятинов Сергей Игоревич**, кандидат технических наук, доцент, г. Москва*
***Кривошеева Дарина Александровна**, г. Москва*

В статье рассмотрена проблема обеспечения защиты данных в телемедицинских системах. Построена модель возможных угроз для мобильной системы, обеспечивающей непрерывный мониторинг состояния человека по регистрируемым биосигналам. Показано, что соответствующая их обработка позволяет получить необходимую информацию для построения криптографических ключей. Обработка основывается на реконструкции математической модели, генерирующей временные ряды, которые диагностически эквивалентны исходным биосигналам.

***Ключевые слова**: защита информации, телемедицина, мобильная измерительная система, биосигналы, реконструкция моделей систем.*

ENSURING INFORMATION SECURITY IN TELEMEDICINE SYSTEMS ON THE BASIS OF MODEL APPROACH

***Tatyana Buldakova**, Doctor of Technical Sciences, Professor*
***Sergey Suyatinov**, Ph.D, Associate Professor*
Darina Krivoscheeva

The article considers the problem of ensuring data security in telemedicine systems. The model of possible threats to mobile systems, providing continuous monitoring of a person on basis of registered biosignals is received. It is shown that the corresponding processing allows to obtain the necessary information for constructing cryptographic keys. Processing is based on the reconstruction of a mathematical model that generates time series, which are diagnostically equivalent to the original biosignals.

***Keywords**: protection of information, telemedicine, mobile measuring system, biosignals, reconstruction of system model.*

Введение

В настоящее время активно создаются виртуальные инфраструктуры здравоохранения, объединяющие на базе единого информационного пространства (ЕИП) все составляющие элементы системы охраны здоровья населения [1-3]. Внедрение информационно-коммуникационных технологий обеспечивает формирование каналов устойчивых коммуникаций между специалистами разных лечебно-профилактических учреждений (ЛПУ), удаленный доступ к медицинским информационным системам (МИС), облегчение и ускорение записи пациентов на прием к врачам. В России крупные медицинские информационно-аналитические центры развертывают площадки своих центров обработки данных, используя различные платформы виртуализации (например, VMware vSphere), и создают инфраструктуру виртуальных рабочих мест для работников ЛПУ, предоставляя им прямой доступ к МИС. В первую очередь в виртуальную среду переносятся приложения и инфраструктурные сервисы, используемые при обработке биомедицинской информации.

Создаваемые виртуальные инфраструктуры позволяют решить актуальную задачу дистанционного мониторинга состояния здоровья населения. При этом остро стоит вопрос с обеспечением информационной безопасности передаваемых физиологических данных.

1. Проблема защиты данных в системах мониторинга

Развитие микроэлектроники и телекоммуникаций позволяют включить человека в единое информационное пространство системы здравоохранения, независимо от его местоположения [1]. Сделать это можно, например, путём регистрации биосигналов сердечно-сосудистой системы с помощью датчиков, вмонтированных в нательную одежду [4-6]. Биосигналы должны передаваться по каналам связи в медицинские центры мониторинга и обработки информации (рис. 1), где посредством математических моделей элементов и подсистем организма создаётся виртуальный физиологический образ пациента, описывающий физиологическую деятельность подсистем человека [7, 8].

Хранение, вычисление и визуализация огромного количества данных, собранных системой мониторинга, требует значительных вычислительных ресурсов, предоставляемых виртуальной инфраструктурой с помощью облачных технологий [9, 10]. Датчики могут отправлять данные на облако напрямую, либо через промежуточные базовые станции. Обслуживающий персонал и пользователь могут просматривать собранную медицинскую информацию непосредственно из облака с помощью смартфона или через Интернет в режиме реального времени и принимать решения в соответствии с текущим функциональным состоянием человека (рис. 2).

Рассмотрим возможные угрозы информационной безопасности применительно ко всем составляющим системы мониторинга:

- датчики: все датчики в системе изначально должны быть надежны, тогда злоумышленник не сможет получить доступ к датчику и остаться незамеченным;

- коммуникации: коммуникационная связь в системе является ненадежной. Злоумышленники могут подслушивать все виды разговоров и могут исказить сигналы. Однако не должно быть никаких помех и отказов в обслуживании и взаимодействии авторизованных устройств;

- базовая станция: даже если злоумышленник не может физически воздействовать на датчик, он может повлиять на базовую станцию. Например, если базовая станция установ-

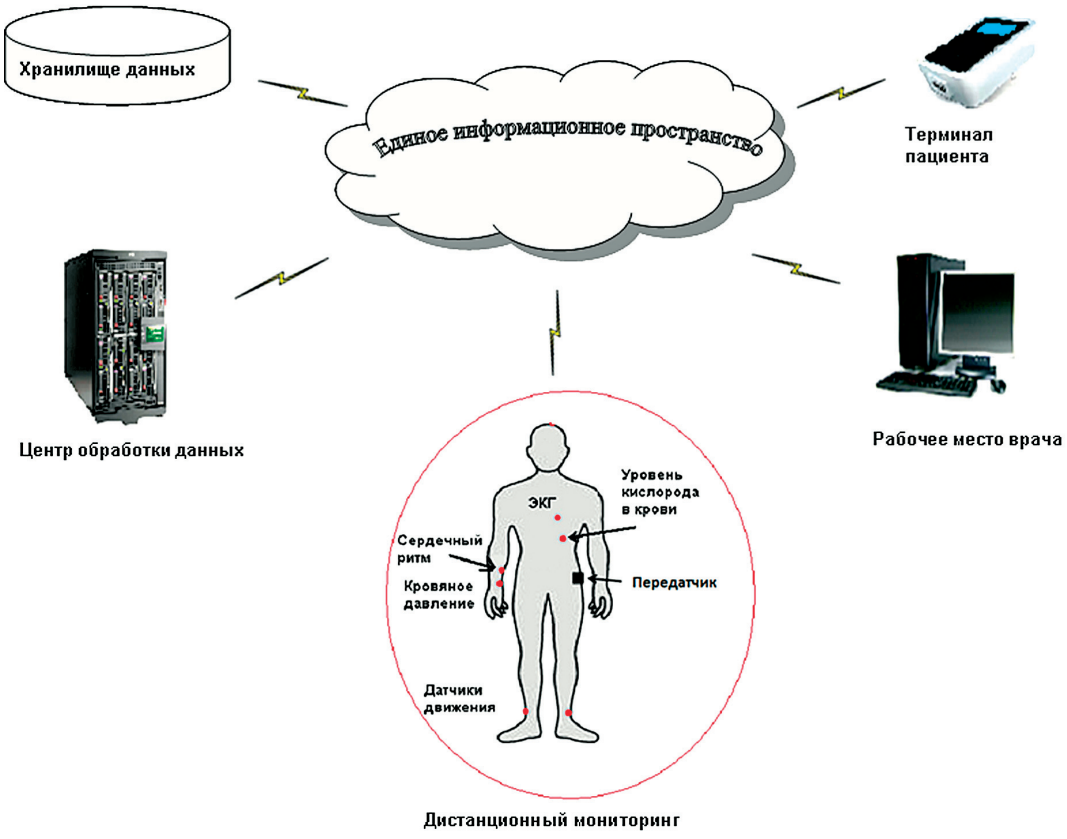

Рис. 1. *Дистанционный мониторинг состояния человека на основе ЕИП*

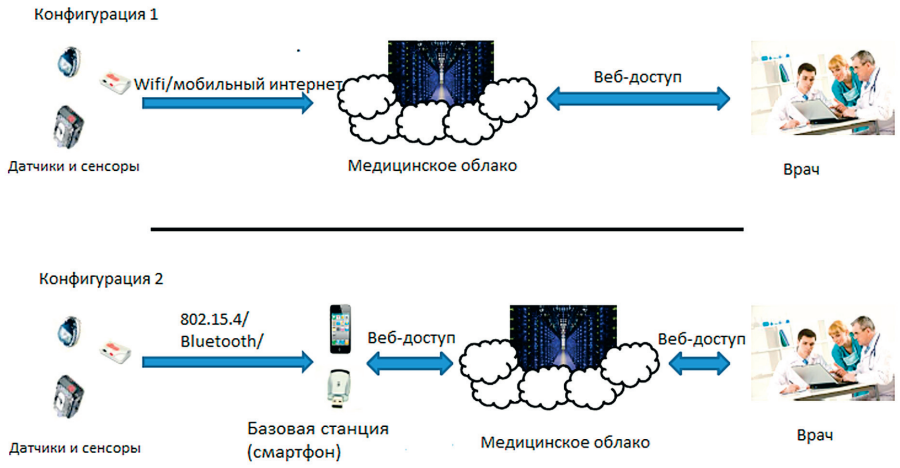

Рис. 2. *Конфигурации мобильной системы дистанционного мониторинга*

лена на смартфоне, то злоумышленники могут взломать приложение на нем;

- облако: предполагается, что медицинское облако является надежным. Обслуживающий персонал может получить доступ к информации о пациенте только после успешной авторизации;

- обслуживающий персонал или пациент: предполагается, что они не откроют доступ к информации под влиянием злоумышленников;

- тело пациента: предполагается, что злоумышленник может иметь физический контакт с пользователем мобильной системы (например, пожать руку пациента), поэтому электрические сигналы пользователя могут быть искажены сигналами злоумышленника. Однако злоумышленник не может внедрить вредоносные датчики в систему. Кроме того, предполагается, что информация о состоянии здоровья пациента в прошлом неизвестна злоумышленнику.

Таким образом, модель угроз показала, что существует проблема обеспечения конфиденциальности и целостности данных пациентов, передаваемых от датчика в облако. Более того, в мобильной измерительной системе обеспечение безопасности личных медицинских данных при передаче через коммуникационный канал от датчиков к облачной медицинской базе данных имеет решающее значение. Поэтому для защиты передаваемых данных необходимо выбрать способ распределения криптографических ключей между датчиком и облаком для обеспечения зашифрованности и целостности данных.

2. Традиционные подходы к обеспечению безопасности систем здравоохранения

С точки зрения защиты информации наиболее уязвимым является канал связи «датчик-облако». Часто используемый в таких случаях протокол защиты *E2E (end-to-end)* работает путем задания и последующего распределения криптографических ключей между датчиками и облаком. Этот протокол обеспечивает скрытность и целостность данных. В дальнейшем ключ также можно использовать для взаимной проверки подлинности сообщения. Основная проблема здесь заключается в возможности конфиденциального распределения (доставки) ключей их пользователям. Для пациента эта процедура должна быть понятна и не обременительна. В наиболее благоприятном случае пациент вообще не должен заботиться о ключе.

Традиционные подходы к обеспечению безопасности систем здравоохранения [11, 12] основываются на асимметричных криптосистемах.

Асимметричное шифрование использует два разных ключа: один для шифрования (который также называется открытым), другой для дешифрования (называется закрытым или секретным). Такой подход является достаточно надежным для обеспечения конфиденциальности и целостности передаваемых данных, но оказывается дорогим для регулярного обмена данными в системе реального времени, поскольку требует больших затрат ресурсов и времени. Кроме того, асимметричная криптография плохо противостоит некоторым видам атак и для ее использования необходимы дополнительные механизмы аутентификации. Поэтому в системах дистанционного мониторинга нецелесообразно использовать асимметричное шифрование.

Альтернативным является подход к защите передаваемых данных путем создания парных симметричных ключей для датчика и приемника.

В симметричной криптосистеме для шифрования и дешифрования применяется один и тот же криптографический ключ, который должен сохраняться в секрете обеими сторонами. В результате алгоритмы с закрытым ключом работают на три порядка быстрее алгоритмов с открытым ключом, что очень важно для телемедицинских систем реального времени. Однако недостатком симметричных шифров является невозможность их использования для подтверждения авторства, так как ключ известен каждой стороне.

Для повышения надежности симметричных криптографических ключей и уменьшения нагрузки на пациента в ряде работ предложено использовать регистрируемые датчиками биосигналы, которые отражают физиологические особенности пациента и могут использоваться для сокрытия информации [13, 14].

Такой подход основывается на следующих положениях:

физиологические сигналы сложны, изменчивы, достаточно уникальны. Вместе с тем существуют характеристики, отражающие морфологию сигнала, которые относительно стабильны (рис. 3). Например, исследования [15] показали, что для сигналов ЭКГ (электрокардиограммы) и ФПК (фотоплетизмограммы) морфологические параметры (в отличие от временных параметров) меняются очень медленно на протяжении жизни человека и, следовательно, могут интерпретироваться как «физиологическая» подпись;

физиологические сигналы могут быть искусственно сгенерированы с помощью генератора модельного сигнала при условии, что данная модель верно построена на основе информации о состоянии человека.

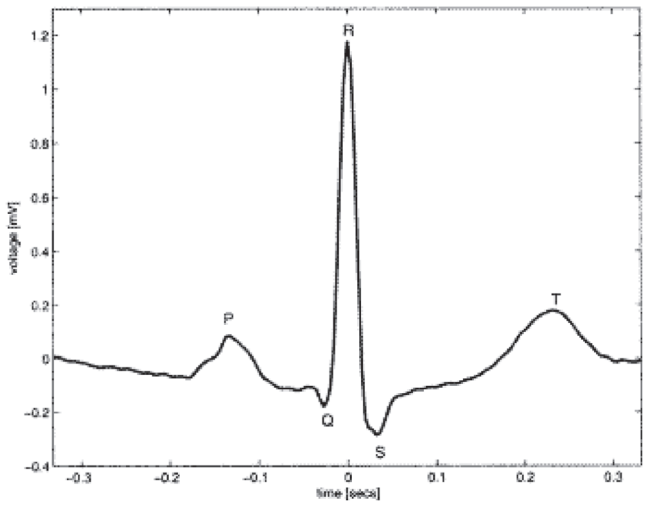

Рис. 3. *Морфологические PQRST-параметры сигнала ЭКГ здорового человека*

Отмеченные свойства биосигналов позволяют использовать их для создания ключей.

Необходимая информация (морфологические особенности биосигналов конкретного человека) извлекается при первой регистрации сигналов. Далее необходимо выбрать метод построения модели для генерации искусственных физиологических сигналов.

Рассмотрим реализацию данного подхода к защите канала связи от датчика к облаку на примере протокола *PEES (Physiology-based End-to-End Security)* [10]. Для защиты данных будут использоваться ЭКГ и ФПГ.

Генератор искусственной ЭКГ описывается выражением

$$\frac{dECG(t)}{dt} = -\sum_{i\in P,Q,R,S,T} a_i\left(2\pi hr_{mean}t-\theta_i\right)e^{\left(\frac{-\left(2\pi hr_{mean}t-\theta_i\right)^2}{2b_i^2}\right)},$$

где hr_{mean} – средняя частота сердечных сокращений человека.

Для получения морфологических параметров каждый вид волн P, Q, R, S и T на ЭКГ представляется кривой Гаусса. Каждая кривая имеет три параметра, и, следовательно, существует 15 морфологических параметров (a_P, a_Q, a_R, a_S, a_T, b_P, b_Q, b_R, b_S, b_T, θ_P, θ_Q, θ_R, θ_S, θ_T).

Кривая фотоплетизмограммы ФПГ получается в результате решения дифференциальных уравнений, основанных на простой модели сосудистой системы человека - модели Виндкесселя [16]. ФПГ разделена на две части – систолу и диастолу. Диастола моделируется с помощью уравнения:

$$PPG_{dias}(t) = a_1 + a_2e^{(-a_3t)} + \frac{1}{a_4+e^{(-a_5t-a_6)}}\cdot\cos(a_7t+a_8). \quad (1)$$

Для систолы аналитическое выражение формы сигнала имеет вид:

$$PPG_{sys}(t) = \frac{1}{a_9+e^{(-a_{10}t-a_{11})}}. \quad (2)$$

Коэффициенты [a_1, a_2, …, a_{11}] в уравнениях (1) и (2) являются морфологическими параметрами.

Параметры модели должны быть изначально отправлены на облако. Параметризация – это важнейший фактор в использовании моделей. Например, генераторы модельных сигналов ЭКГ и ФПК используют временные и морфологические свойства биосигналов. Они могут быть вычислены в режиме «off-line» и переданы на облако, когда модель перейдет в режим «on-line», или можно отправить образец биосигнала на облако, который затем поможет вычислить морфологические значения сигнала.

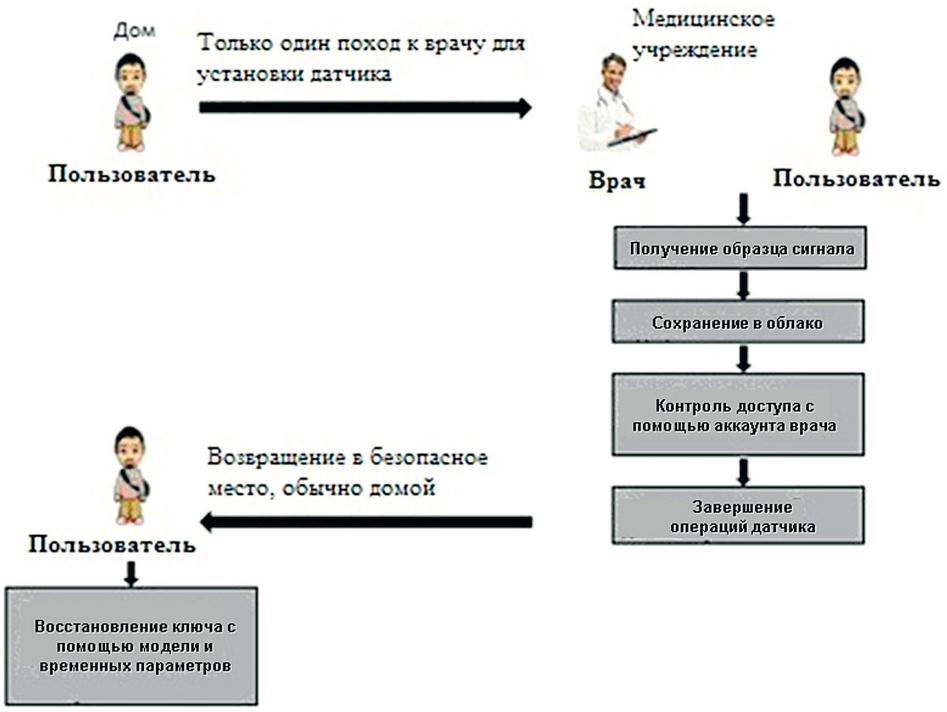

Рис. 4. *Процесс инициализации*

Произвести инициализацию модели генератора для пользователя необходимо будет только один раз, независимо от того, как эта инициализация будет сделана: дома у пользователя или в специальном учреждении. Предполагается, что исходные биосигналы безопасно передадутся в облако. После первоначальной передачи любое будущее распространение *E2E* ключей будет происходить прозрачно. Для иллюстрации процесса инициализации на рис. 4 рассмотрена ситуация, когда пользователь обращается к врачу для установки датчиков ЭКГ. Предполагается, что врач имеет аккаунт в облаке в момент инициализации электронной медицинской записи пользователя.

Разные датчики, регистрируя биосигналы (например, ФПГ и ЭКГ), могут использовать общие физиологические особенности, чтобы скрыть и отобразить секретный ключ. В рассматриваемой системе один датчик (отправитель) генерирует случайный ключ и скрывает его в криптографической конструкции, называемой хранилищем, с помощью частотных сигналов, полученных на основе зарегистрированных биосигналов. В свою очередь хранилище передает данные в другой датчик (приемник), который использует свой собственный набор частотных сигналов. Данный набор частотных сигналов получается в результате одновременного измерения биосигналов «приемника» вместе с «отправителем» с целью сокрытия случайного ключа.

Протокол *PEES* не требует априорного распределения ключей. Для создания безопасной *E2E* связи достаточно простой установки датчиков на пользователе. В облаке, внутри хранилища, находится диагностический эквивалент биосигналов в форме временных рядов, созданных с помощью модельного генератора [16], который должен быть настроен согласно физиологическим данным пользователя (рис. 5).

Отметим, что по существу в приведенном примере применялся подбор функциональных зависимостей по виду регистрируемых биосигналов. Ниже предлагается подход на основе реконструкции моделей систем в форме дифференциальных уравнений, решением которых являются искомые функциональные зависимости.

3. Предлагаемый подход к решению задачи

Основным недостатком рассмотренного выше примера является большое количество морфологических параметров, которые надо рассматривать как многомерный характеристический вектор. Назовем его морфологическим вектором, поскольку морфология представлена именно совокупностью параметров, а не каждым параметром в отдельности. Изменение даже одного параметра описывает уже другую морфологическую форму. Если учесть, что расчет указанных морфологических параметров с использованием метода наименьших квадратов является плохо обусловленной задачей, то приходим к выводу, что на практике морфологический вектор не отличается необходимой стабильностью.

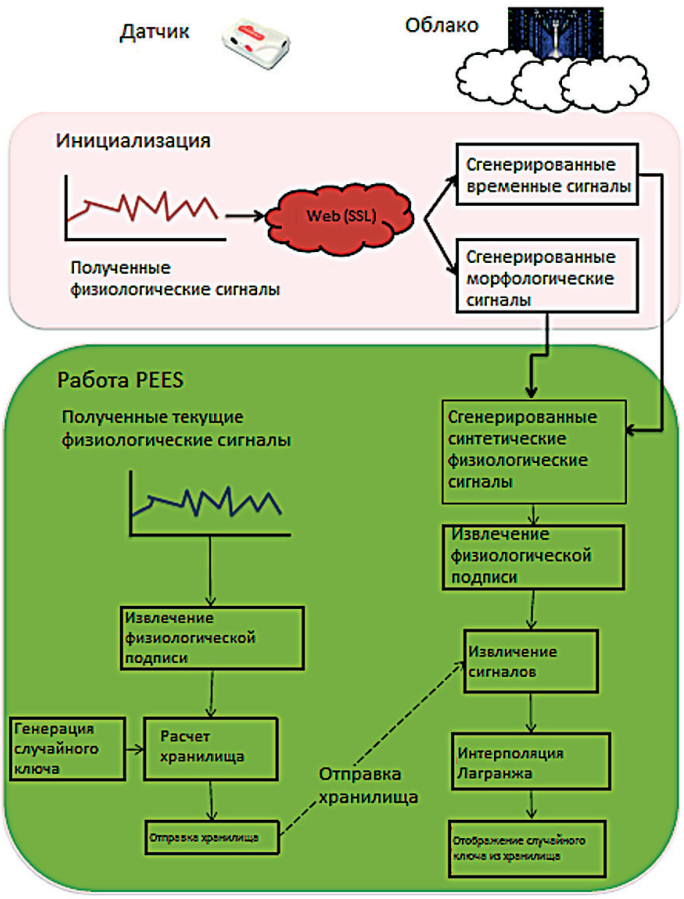

Рис. 5. *Обеспечение информационной безопасности с использованием протокола PEES [10]*

Предлагается в качестве морфологических признаков использовать не отдельные параметры временной кривой, а математическую модель генератора биосигнала в форме системы дифференциальных уравнений. Морфологическими признаками в этом случае является как сама структура модели, так и ее параметры. Задача определения морфологических признаков в этом случае сводится к задаче реконструкции модели системы, которая генерирует временные ряды, диагностически эквивалентные исходным сигналам.

Реконструкция модели сложной системы по наблюдаемому временному ряду (обратная задача динамики) успешно применяется для решения различных задач. В условиях неполных данных метод реконструкции позволяет оценить состояние системы, выявить особенности поведения, прогнозировать ее развитие. Эти задачи являются очень важными при дистанционном мониторинге состояния сложных систем. Модельный подход к анализу систем с использованием реконструкции хорошо зарекомендовал себя при обработке биосигналов человека.

Рассмотрим применение указанного подхода на примере использования сфигмограммы, которая регистрирует колебания артериальной стенки сосуда, обусловленные выбросом ударного объема крови в артериальное русло. Используя принцип базовых моделей колебательных систем с учетом биомеханики сосуда, в работах [6, 8] описаны динамические свойства сосудистой стенки автономным уравнением Ван-дер-Поля – Релея:

$$\ddot{x} + \left[\varepsilon_1\left(x^2 - r_0^2\right) + \varepsilon_2\left(\dot{x}^2 - \omega_0^2 \cdot r_0^2\right)\right] \cdot \dot{x} + ax = 0.$$

Здесь x – это перемещение стенки кровеносного сосуда, регистрируемое датчиком.

Очевидно, что параметры уравнения, отражающие такие свойства сосуда, как податливость, диссипацию, свойственны любым сосудам и вместе с тем уникальны для отдельного индивидуума.

Поскольку стенки сосуда перемещаются под действием давления тока крови, то учет влияния сердечной подсистемы приводит к следующему уравнению

$$\ddot{x} + \left[\varepsilon_1\left(x^2 - r^2\right) + \varepsilon_2\left(\dot{x}^2 - \omega_0^2 \cdot r^2\right)\right] \cdot \dot{x} + ax = P(\omega_0 t). \quad (3)$$

Исходной информацией для определения неизвестных параметров управления является временной ряд пульсаций стенки сосуда (сфиг-

мограмма). Данные временного ряда предварительно обрабатываются с целью удаления тренда, стабилизации частоты, уменьшения шума.

Учитывая, что система функционирует в режиме предельного цикла, неизвестные параметры ω_0 и r уравнения (3) находятся из экспериментальных данных. После их определения, используя измеренные значения $x_u(t)$ и вычисленные значения $\dot{x}(t)$ и $\ddot{x}(t)$, методом наименьших квадратов находятся значения p_i, a, ε_1 и ε_2. Здесь p_i – это коэффициенты разложения функции P в ряд Фурье, $i = 1, \ldots, N$.

Однако проведенные исследования показали, что данная модель не всегда соответствует регистрируемому биосигналу. Поэтому в зависимости от состояния сосудов, пациенты были разделены на несколько групп, каждой из которых ставится в соответствие определенная структура модельного уравнения. Таким образом, был создан банк данных моделей. Например, для пожилых пациентов вместо уравнения (3) использовалась модель Ван-дер-Поля – Дуффинга [17].

Для определения параметров модели и оценки адекватности используется расширенный фильтр Калмана. Регистрируемый биосигнал обрабатывается с использованием алгоритма фильтра Калмана. Алгоритм использует определенную структуру модели. На каждой итерации анализируется ковариационная матрица ошибок. Если значения погрешностей превышают заданные допустимые пределы, то выбирается другая структура модели. В противном случае выбранная модель используется для формирования ключей в системе защиты информации. В отличие от ранее рассмотренных подходов, в нашем случае необходимо анализировать не более трех физиологически значимых параметров, например эластичность сосудов, степень диссипации, время релаксации.

Предложенный метод можно улучшить, синхронно регистрируя несколько сигналов. Для примера рассмотрим систему «сердце-сосуды».

В основе метода моделирования биосистемы «сердце-сосуды» лежит парадигма о колебательно-волновой общности кажущихся непохожими явлений самой разной природы, которая составляет сущность современного научного мировоззрения. Теоретической базой этой парадигмы является нелинейная теория колебаний и волн, которая вмещает науку о сложности, синергетику, нелинейную динамику.

В соответствии с указанной парадигмой, предлагается строить динамические модели подсистем и всей системы «сердце-сосуды» на принципах синергетики, подразумевающих наличие сравнительно простых базовых моделей, описывающих колебательные процессы в различных областях знаний. Это позволяет строить модели рассматриваемой биосистемы в форме дифференциальных уравнений с сосредоточенными параметрами, а также в форме кибернетических моделей типа «вход-выход». Обоснование структуры базовых моделей осуществляется на основе известных физических законов, положенных в основу функционирования рассматриваемого элемента динамической биосистемы. Определение параметров полученных таким образом структурно-функциональных моделей осуществляется на основе зарегистрированных биосигналов.

Предлагаемая динамическая модель биосистемы «сердце-сосуды» (рис. 6) использует три биосигнала (электрокардиограмму, сейсмокардиограмму, сфигмограмму) и более полно отражает ее состояние.

Ввиду сложного характера взаимосвязей между рассматриваемыми подсистемами, ограниченных возможностей неинвазивных методов их исследования, предлагается строить функциональную модель взаимодействия подсистем на основе обучаемых динамических сетей оригинальной структуры [18]. В отличие от используемых в настоящее время упрощенных моделей пропорци-

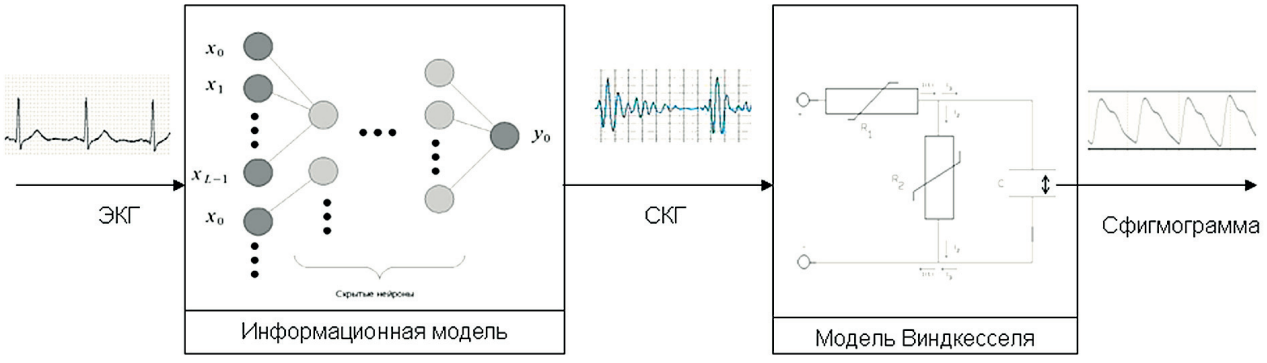

Рис. 6. *Предлагаемая динамическая модель биосистемы «сердце-сосуды»*

онального взаимодействия, использование динамических сетей позволяет эффективно использовать большой объем экспериментальных данных при обучении сети и отобразить в модели сложные механизмы взаимодействия подсистем.

Для идентификации биосистемы «сердце-сосуды» предлагается локализовать частотный спектр регистрируемых сигналов в области частот, обусловленных преимущественно сократительной деятельностью миокарда. Модель сердца представляется в виде динамической сети, на вход которой подается сигнал ЭКГ, а выходом является сейсмокардиосигнал, зарегистрированный в прекардиальной области. Этот же сигнал является входом сосудистой подсистемы. В качестве базовой модели здесь выбрана модель Виндкесселя, которая модифицирована на случай регистрируемого выходного сигнала в виде пульсаций сонной артерии. Такой, впервые предложенный подход позволит идентифицировать физиологически обусловленные параметры модели Виндкесселя по неинвазивно зарегистрированным сигналам «вход-выход».

Функционирование сердечно-сосудистой системы является результатом сложного взаимодействия различных подсистем. Это взаимодействие отражается в регистрируемых биосигналах, но с разной степенью выраженности. Накладываясь, эти эффекты взаимодействия создают своеобразный шумовой фон, который приводит к большой вариабельности как числа, так и параметров модели биосигнала. Это, как было отмечено выше, создает проблемы при распределении ключей защиты информации.

Представленная трехэлементная модель биосистемы «сердце-сосуды» позволяет осуществить оригинальную селекцию информации, заключенной в совместно зарегистрированных трех биосигналах. Выделив подсистемы, функционирование которых имеет физическое обоснование на основе законов биомеханики, мы выделяем главные движения системы, обусловленные их внутренней динамикой. При этом осуществляется определенное разделение воздействий других подсистем и их привязка к элементам рассматриваемой модели. В целом это приводит к своеобразному эффекту фильтрации и позволяет уменьшить вариацию параметров модели.

Заключение

Предложен подход, в котором для построения криптографических ключей используется реконструированная математическая модель генератора биосигнала. Метод защиты данных на основе этого подхода продемонстрирован на примере биосистемы «сердце-сосуды». Его реализация в системах мониторинга позволит не только повысить адекватность оценки состояния целостного организма человека на основе множественных неинвазивных измерений, но и сформировать морфологические признаки для формирования «физиологической» подписи. Эти признаки включают структуру модели, используемой для оценки состояния человека, и ее физиологически значимые параметры.

Литература:

1. Вопросы создания Единого информационного пространства в системе здравоохранения РАН / Н. Г. Гончаров, Я. И. Гулиев, Ю. В. Гуляев и др. // Информационные технологии и вычислительные системы. 2006. № 4. С. 83-94.
2. Концептуальная модель виртуального центра охраны здоровья населения / В. С. Анищенко, Т. И. Булдакова, П. Я. Довгалевский и др. // Информационные технологии. 2009. №12. С. 59-64.
3. Развитие системы электронных услуг муниципальной поликлиники (на основе анализа зарубежных web-ресурсов) / А. В. Ланцберг, К. Тройч, Т. И. Булдакова // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2011. № 4. С. 1-7.
4. Winters J., Wang Y. Wearable Sensors and Telerehabilitation // IEEE Engineering in Medicine and Biology Magazine. 2003. No. 3. Pp. 56-65.
5. Paradiso R., Loriga G., Taccini N. A Wearable Health Care System Based on Knitted Integrated Sensors // IEEE Transactions on Information Technology in Biomedicine. 2005. V. 9, No. 3. Pp. 337-344.

References:

1. Voprosy sozdania Edinogo informacionnogo prostranstva v systeme zdravoohranenia RAN / N. G. Goncharov, Ya. I. Guliev, Ya. V. Gulyaev i dr. // Informacionnye tehnologii i vychislitel'nye sistemy. 2006. № 4. S. 83-94 (Questions of common information space in the health system of the RAS / N.G. Goncharov, Ya. I. Guliev, Ya. V. Gulyaev et al. // Information technology and computing. 2006. No. 4. Pp. 83-94).
2. Konceptual'naya model virtual'nogo centra ohrany zdorov'ya naseleniya / V. S. Anitchenko, T. I. Buldakova, P. Ya. Dovgalevsky i dr. // Informacionnye tehnologii. 2009. № 12. S. 59-64. (Conceptual model of the virtual center of public health / V. S. Anitchenko, T. I. Buldakova, P. Ya. Dovgalevsky et al. // Information technology. 2009. No. 12. Pp. 59-64.)
3. Development of the electronic service system of a municipal clinic (based on the analysis of foreign web resources) / A. V. Lantsberg, K. Treusch, T. I. Buldakova // Automatic Documentation and Mathematical Linguistics. 2011. No. 2. Vol. 45. Pp. 74-80.
4. Winters J., Wang Y. Wearable Sensors and Telerehabilitation // IEEE Engineering in Medicine and Biology Magazine. 2003. No. 3. Pp. 56-65.

6. Информационно-измерительный комплекс совместной регистрации и обработки биосигналов/ Т. И. Булдакова, А. В. Коблов, С. И. Суятинов // Приборы и системы. Управление, контроль, диагностика. 2008. № 6. С. 41-46.
7. Prado M., Roa L., Reina-Tosina J. Virtual Center for Renal Support: Technological Approach to Patient Physiological Image // IEEE Transaction on biomedical engineering. 2002. V. 49, No. 12. Pp. 1420-1430.
8. Программно-аналитический комплекс модельной обработки биосигналов / Т. И. Булдакова, В. И. Гриднев, К. И. Кириллов и др. // Биомедицинская радиоэлектроника. 2009. № 1. С. 71-77.
9. Применение облачных технологий в медицинских дистанционных диагностических устройствах / В. И. Кузнецов, С. А. Тараканов, Н. И. Рыжаков, А. А. Рассадина // Врач и информационные технологии. 2012. № 5. С. 68-72.
10. Banerjee A., Gupta S. K. S., Venkatasubramanian K. K. PEES: Physiology-based End-to-End Security for mHealth // Proceedings of the 4th Conference on Wireless Health. 2013. Article No. 2.
11. Malhotra K., Gardner S., Patz R. Implementation of elliptic-curve cryptography on mobile healthcare devices // Networking, Sensing and Control. 2007. Pp. 239-244.
12. Liu A., Ning P. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks // Information Processing in Sensor Networks. 2008. Pp. 245-256.
13. Venkatasubramanian K. K., Banerjee A., Gupta S. K. S. PSKA: Usable and secure key agreement scheme for body area networks // IEEE Transactions on Information Technology in Biomedicine. 2010. Vol. 14, No 1. Pp. 60-68.
14. Cherukuri S., Venkatasubramanian K., Gupta S. K. S. BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body // Proceedings of Workshop on Wireless Security and Privacy. 2003. Pp. 432-439.
15. McSharry P. E., Clifford G. D., Tarassenko L., Smith L. A. A dynamical model for generating synthetic electrocardiogram signals // IEEE Transactions on Biomedical Engineering. 2003. Vol. 50, No 3. Pp. 289-294.
16. Nabar S., Banerjee A., Gupta S. K. S., and Poovendran R. GeM-REM: Generative Model-Driven Resource Efficient ECG Monitoring in Body Sensor Networks // International Conference on Body Sensor Networks (BSN). 2011. Pp. 1-6.
17. Выявление групп риска у людей с высоким уровнем холестерина: статистический и модельный подходы / Т. И. Булдакова, В. Б. Лифшиц, С. И. Суятинов // Информационные технологии моделирования и управления. 2008. №4 (47). С. 363-368.
18. Моделирование связей в системе «сердце-сосуды» / Н. С. Самочетова, А. С. Ситников, С. И. Суятинов // Наука и образование: электронное научно-техническое издание. 2013. № 1. С. 123-134.

5. Paradiso R., Loriga G., Taccini N. A Wearable Health Care System Based on Knitted Integrated Sensors // IEEE Transactions on Information Technology in Biomedicine. 2005. V. 9, No. 3. Pp. 337-344.
6. Informacionno-izmeritel'ny complex sovmestnoy registracii i obrabotki biosignalov / T. I. Buldakova, A. V. Koblov, S. I. Suyatinov // Pribory i sistemy. Upravlenie, kontrol, diagnostika. 2008. № 6. S. 41-46. (Information-measuring complex of joint registration and processing of biosignals / T. I. Buldakova, A. V. Koblov, S. I. Suyatinov // Devices and systems. Management, monitoring, diagnostics. 2008. No. 6. Pp. 41-46.)
7. Prado M., Roa L., Reina-Tosina J. Virtual Center for Renal Support: Technological Approach to Patient Physiological Image // IEEE Transaction on biomedical engineering. 2002. V. 49, No. 12. Pp. 1420-1430.
8. Programmno-analitichesky komplex model'noy obrabotki biosignalov / T. I. Buldakova, V. I. Gridnev, K. I. Kirillov et al. // Biomedicinskaya radioelektronika. 2009. № 1. C. 71-77. (Software-analytical complex of model processing of biosignals / T. I. Buldakova, V. I. Gridnev, K.I. Kirillov et al. // Biomedical electronics. 2009. No. 1. Pp. 71-77.)
9. Primenenie oblachnyh tehnology v medicinskih distancionnyh diagnosticheskih ustroistvah / V. I. Kuznetsov, S. A. Cockroaches, N. I. Ryzhakov, A. A. Rassadina // Vrach i informacionnie tehnologii. 2012. № 5. S. 68-72. (The use of cloud technologies in remote medical diagnostic device / V. I. Kuznetsov, S. A. Cockroaches, N. I. Ryzhakov, A. A. Rassadina // Doctor and information technology. 2012. No. 5. Pp. 68-72.)
10. Banerjee A., Gupta S.K.S., Venkatasubramanian K.K. PEES: Physiology-based End-to-End Security for mHealth // Proceedings of the 4th Conference on Wireless Health. 2013. Article No. 2.
11. Malhotra K., Gardner S., Patz R. Implementation of elliptic-curve cryptography on mobile healthcare devices // Networking, Sensing and Control. 2007. Pp. 239-244.
12. Liu A., Ning P. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks // Information Processing in Sensor Networks. 2008. Pp. 245-256.
13. Venkatasubramanian K. K., Banerjee A., Gupta S. K. S. PSKA: Usable and secure key agreement scheme for body area networks // IEEE Transactions on Information Technology in Biomedicine. 2010. Vol. 14, No 1. Pp. 60-68.
14. Cherukuri S., Venkatasubramanian K., Gupta S. K. S. BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body // Proceedings of Workshop on Wireless Security and Privacy. 2003. Pp. 432-439.
15. McSharry P. E., Clifford G. D., Tarassenko L., Smith L. A. A dynamical model for generating synthetic electrocardiogram signals // IEEE Transactions on Biomedical Engineering. 2003. Vol. 50, No 3. Pp. 289-294.
16. Nabar S., Banerjee A., Gupta S. K. S., and Poovendran R. GeM-REM: Generative Model-Driven Resource Efficient ECG Monitoring in Body Sensor Networks // International Conference on Body Sensor Networks (BSN). 2011. Pp. 1-6.
17. Vyyavlenie grupp riska u lyudei s vysokim urovnem holesterina: statistichesky i model'ny podhody / T. I. Buldakova, V. B. Lifshitz, S. I. Suyatinov // Informacionnye tehnologii modelirovaniya i upravleniya. 2008. №4 (47). S. 363-368. (Identification of risk groups for people with high cholesterol levels: statistical and modeling approaches / T. I. Buldakova, V. B. Lifshitz, S. I. Suyatinov // Information Technology of Modeling and Control. 2008. No.4 (47). Pp. 363-368.)
18. Modelirovanie svyazey v sisteme «serdtze-sosudy» / N. S. Samochetova, A. S. Sitnikov, S. I. Suyatinov // Nauka i obrazovanie: elektronnoe nauchno-tehnicheskoe izdanie. 2013. № 1. S. 123-134. (Modeling relationships in the «heart-vessels» system / N. S. Samochetova, A. S. Sitnikov, S. I. Suyatinov // Science and education: electronic scientific and technical publication. 2013. No. 1. Pp. 123-134.)