



СПБГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ



Р.Р. Фаткиева

Архитектура IoT

Фрагмент конспекта

СПБГЭТУ «ЛЭТИ», 2021 г.





4. АРХИТЕКТУРА ИОТ

4.1 Обзор существующих платформ и сервисов для развертывания технологических решений с применением IoT

Переход к электронному документообороту в медицинских организациях при учете оказания медицинской помощи, сбору данных о показателях их деятельности приводит к необходимости формирования новых подходов, основными из которых являются:

- персонализированная медицина – индивидуальное сопровождение пациента с охватом всех показателей его функционирования
- медицина прецизионная – совокупность методов профилактики и оценки патологического состояния, в случае его возникновения, основанных на индивидуальных особенностях пациента;
- медицина предиктивная – подчеркивается возможность определения предрасположенности к развитию многих заболеваний и мер профилактики;
- медицина стратифицированная – стратификация пациентов на группы, лечение в которых будет различаться в зависимости от ряда критериев, в том числе генетических особенностей.

В этих условиях актуальными становятся решения, а области Internet of Medical Things (IoMT), ориентированные на получение и обработку биометрических и поведенческих данных. К задачам IoMT можно отнести:

- повышение уровня качества мониторинга состояния пациента;
- применение стандартизированных международных систем измерения и регистрации биосигналов;
- обеспечение защиты персональных данных.

К логическим уровням IoMT-системы целесообразно отнести:

Биологическую мишень, находящуюся в непосредственном контакте с датчиком и подвергающаяся измерению.

Датчик, предназначенный для получения (съема) биометрических данных, включая поиск и определение паттернов в снимаемых аналоговых и цифровых сигналах, интегрированный в сетевую инфраструктуру.

Протокол, предназначенный для предварительной обработки и передачи биометрических данных в облачное приложение.



Облачное приложение, являющее получателем биометрических данных и выполняющее основные прикладные задачи по их распознаванию, визуализации, анализу, сопоставлению, выработке рекомендаций и т.д.

Облачное хранилище биометрических данных, предназначенное для накопления и долгосрочного хранения данных.

Логическое разделение по указанным уровням позволяет сформировать общую структуру IoT, состоящую датчиков, объединенных в персональную сеть, сетей передачи данных и платформ обработки данных (Ошибка! Источник ссылки не найден.).

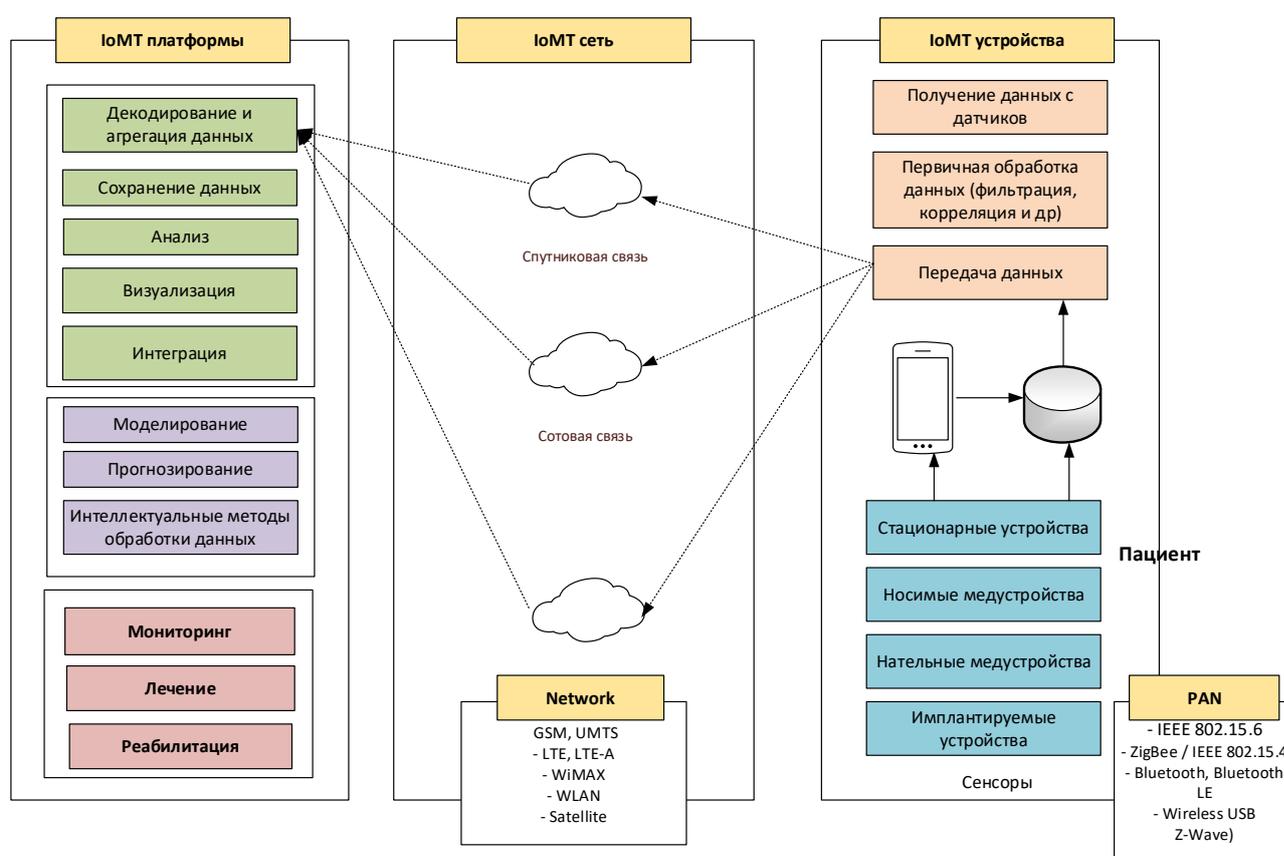


Рис. 1

Представленная сервисно-организованная архитектура организации IoT, основанная на выборе диагностических, лечебных и профилактических средств, развернутых на IoT платформах позволяет сформировать индивидуальные траектории мониторинга и лечения, которые являются оптимальными для конкретного пациента, с учётом его генетических, физиологических, биохимических, поведенческих и других особенностей.



Построение сервисно-организованной архитектуры IoT зависит от самых разных технологий, от датчиков и систем передачи данных, до приложений искусственного интеллекта и машинного обучения, которые применяются на базе различных платформ, представленных на Рис. 2.

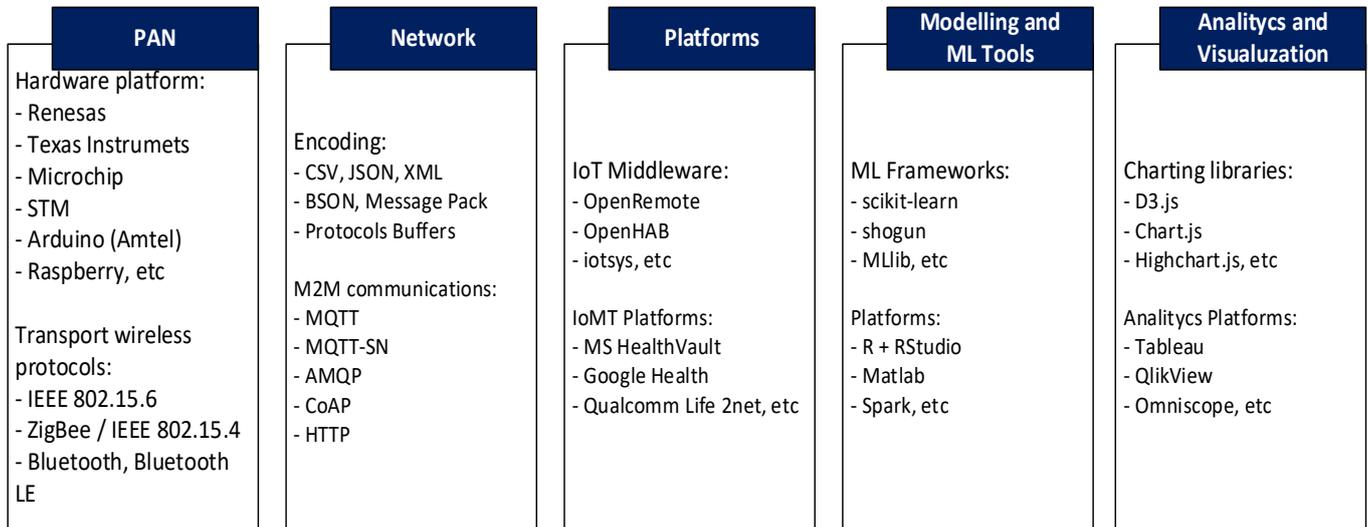


Рис. 2

При построении сервисно-организованной архитектуры IoT возникает необходимость учета угроз безопасности персональных данных в системах и сетях, функционирующих на базе облачной инфраструктуры. В этом случае объекты воздействия определяются с учетом состава и содержания услуг, предоставляемых поставщиком услуг (например, инфраструктура как услуга, платформа как сервис, программное обеспечение как сервис [7]).

Арендуемые или используемые программно-аппаратные средства и их интерфейсы, каналы связи, программное обеспечение относятся к объектам воздействия, находящимся в границе оценки угроз безопасности информации оператора. В отношении остальной информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры угрозы безопасности информации оцениваются поставщиком услуг.

Пример распределения границ при оценке угроз безопасности информации между оператором и поставщиком услуг представлена Рис. 3





Рис. 3 [7]

Поставщики услуг поддерживают целый ряд продуктов. Рассмотрим основные компоненты:

NaaS - сеть как услуга, описывает услуги для подключения к сетевому транспорту. Предполагает оптимизацию распределения ресурсов путем рассмотрения сетевых и вычислительных ресурсов как единого целого (SDN) и программно-определенного периметра (SDP).

SaaS - модель обслуживания, при которой подписчикам предоставляется готовое прикладное программное обеспечение, полностью обслуживаемое поставщиком услуг. Виртуальный SaaS фактически работает на клиенте пользователя. Сервисы SaaS работают для таких устройств, как Google Apps, Salesforce и Microsoft Office.

PaaS - модель предоставления облачных вычислений, при которой потребитель получает доступ к использованию информационно-технологических платформ. Конечный пользователь использует аппаратное обеспечение центра обработки данных, операционную систему, промежуточное ПО и различные базы данных поставщиком услуг для





размещения своего частного приложения или сервисов. Примерами публичных поставщиков PaaS являются IBM Bluemix, Google App Engine и Microsoft Azure.

IaaS - модель обслуживания, по которой потребителю предоставляются фундаментальные информационно-технологические ресурсы – виртуальные серверы с заданной вычислительной мощностью, операционной системой и доступом к сети. Это обеспечивает максимальную гибкость при развертывании, но требует больших усилий со стороны клиент.

Рассмотрим основные модели обслуживания представленных на рынке в настоящее время.

Платформа Intel использует модель обслуживания IaaS. Корпорация Intel предоставляет полный спектр технологий для перемещения, хранения и обработки массивных объемов данных с необходимой производительностью для сложной аналитики, высокопроизводительных вычислений и моделей искусственного интеллекта. Для выполнения задач точной медицины используются ЦОД на распределенных кластерах HPC или на периферийных серверах, которые хранят данные на местах, с целью соблюдения требований к локальному размещению данных.

Платформа Cisco использует модель обслуживания NaaS, обеспечивая построение систем передачи данных от датчиков к облачным вычислениям. В настоящее время активно развивается направление DevNet, в виде песочницы, позволяющее разрабатывать приложения IoT для разработчиков и программистов.

Платформа Thingworx использует модель обслуживания SaaS. Платформа позволяет организовывать централизованную передачу данных между объектами Интернета вещей. Платформа объединяет системы и сетевое оборудование, а интерактивные сеансы совместной работы помогают отдельным специалистам и рабочим группам ускорять решение совместных задач, поскольку хранилище данных лежит в основе контекстного взаимодействия и совместной работы пользователей систем.

Платформа Azure – использует модель обслуживания PaaS. Платформа, которая помогает повысить результативность лечения, упростить клинические операции, а также оптимизировать изготовление и цепочку





поставок медицинских средств. В основе платформы лежит эффективная и интеллектуальная технология Интернета.

4.2 Основные характеристики программно-аппаратных платформ. Средства и инструменты обработки данных

Мониторинг— система наблюдения за явлениями и процессами, проходящими в окружающей среде, результаты которого служат для обоснования управленческих решений по обеспечению безопасности наблюдаемого объекта.

Система мониторинга IoT базируется на съеме и преобразовании информации с датчиков в систему показателей, для последующей обработки и принятия управленческих решений с формированием управляющих воздействий через актуаторы. Для выработки управляющих воздействий в IoT анализируется такая информация:

-структурированные данные предсказуемого формата (информация из БД);

-неструктурированные данные высокой степени случайности и вариативности;

-частично структурированные данные с некоторой степенью случайности вариативности [1].

В подобных условиях возникает необходимость построения систем обнаружения и управления отклонениями от плановых показателей функционирования наблюдаемого объекта. Особенностью подобных систем является наличие компонентов в виде сенсоров/датчиков, блока мониторинга ситуации, базы происходящих событий, модуля принятия решения. В некоторых системах предусмотрен блок моделирования и прогнозирования ситуации (Рис. 4). Рассмотрим каждый блок отдельно.

Компонент съема информации с датчиков содержит следующие методы, которые могут быть реализованы как на контроллере датчика, либо в виде программного модуля в информационной системе:

- предварительная обработка - отбрасывание незначительных событий, извлечение свойств, сегментация, перевод данных в более подходящий формат;
- анализ данных - проверка данных; если они не соответствуют каким-то пограничным значениям, отправляется предупреждение.



Компонент мониторинга и хранения (сбора информации о событиях) позволяет агрегировать потоки информации и выявить отклонения от пороговых значений используя методы:

- окна событий - создается подвижный диапазон набора данных, который может быть ограничен по времени, длине. Эта функция хорошо подходит для создания правил и событий, занимающихся подсчетом;

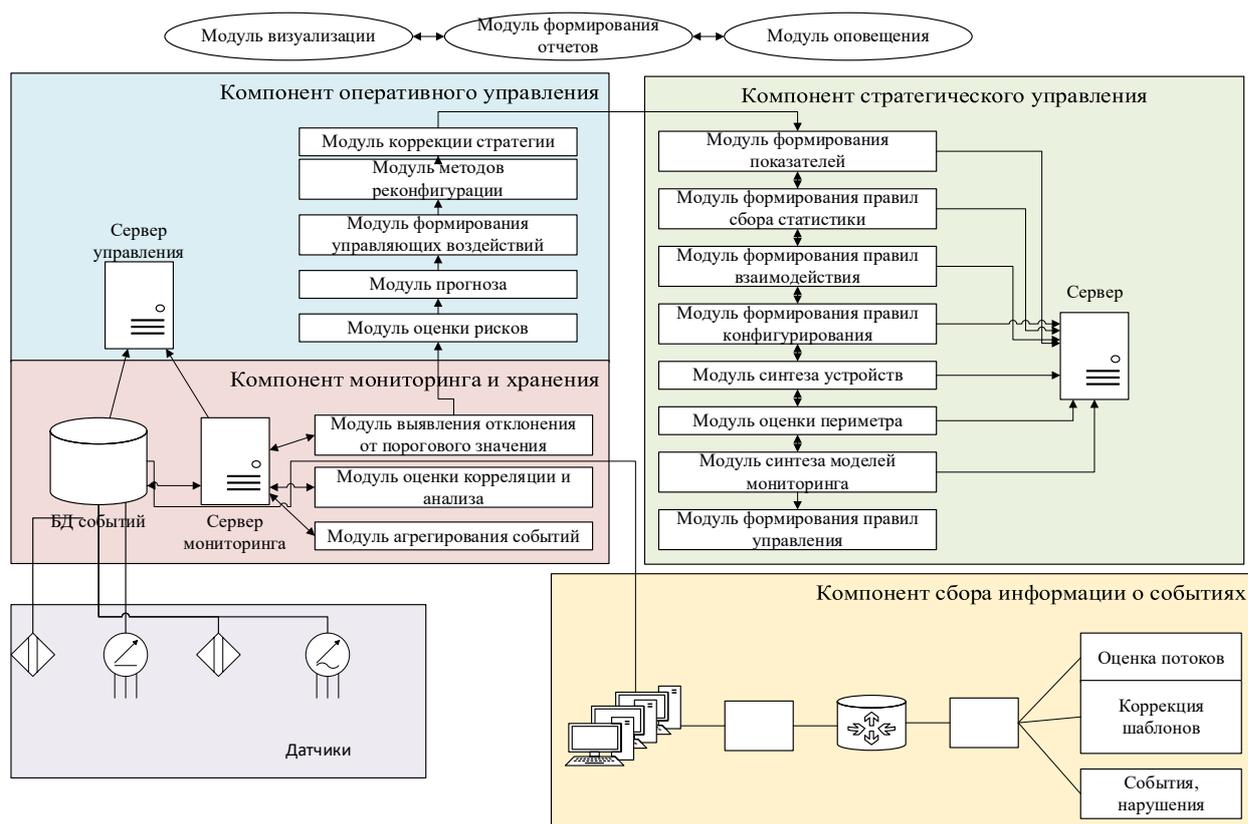


Рис. 4

- агрегация данных - объединение несколько потоков данных в один для их дальнейшей обработки;
- обработка результатов измерений- оценка полноты и наличие ошибок при потере данных, их искажении или неправильным порядком следования, оценка корреляции, выявление отклонений от пороговых значений;
- коррекция шаблонов- позволят скорректировать набор показателей, необходимым для отслеживания тех или иных состояний наблюдаемого объекта.



Компоненты оперативного управления позволяют формировать наборы управляющие воздействия пересылаемых актуатору и содержать методы:

- оценки рисков- необязательный компонент, позволяющий получить определение величины ущерба от возникшей рискованной ситуации и несвоевременного принятия мер по предотвращению риска.
- прогноза - необязательный компонент, позволяющий спрогнозировать набор показателей в заданном окне событий;
- управления - позволяют сформировать комплекс управляющих воздействий и/или мероприятий для достижения целевой функции;
- реконфигурации- изменение состава и способа взаимодействия программных и аппаратных средств объекта с целью исключения отказавших программных или аппаратных компонентов или протекающих процессов;
- коррекции стратегии - исправление операционного процесса достижения целевой функции.

Компоненты стратегического управления позволяют создавать наборы управляющих воздействий для достижения целевой функции и содержат методы формирования:

- показателей- наборов данных, характеризующих количественные, качественные или интегральные свойства объекта;
- правил взаимодействия-правил, по которым осуществляется совместный доступ к ресурсу;
- правил конфигурирования и синтеза устройств- правил соединения элементарных единиц, операционных процессов;
- оценки периметра и моделей мониторинга- нахождения границ, в пределах которых осуществляется мониторинг за объектами управления.
- правил управления- набора связей ответных реакций на входное воздействие, отраженное показателями, считанными с датчика.





В частном случае, архитектура ряда IoT может состоять из набора агентов различных типов, специализированных для решения подзадач обнаружения отклонений от заданных параметров функционирования.

При применении указанной архитектуры зачастую возникают трудности при определении типа отклонений и степени ее опасности. Отклонения могут иметь различные причины и быть связаны как с деятельностью наблюдаемого объекта, так и с неисправностью аппаратуры и дефектами программного обеспечения. Отклонения могут быть видимыми и проявляться непосредственно в некорректной работе датчика, информационно-вычислительной системы, а могут не иметь видимых признаков, но привести к сбоям через длительное время.

Однако разнообразие аномалий, протекающих в IoT приводит к трудностям формализации показателей функционирования и как следствие, ошибкам при построении эффективной системы управления, которая включает в себя механизмы предупреждения, обнаружения, определения источника и противодействия.

Проблема построения показателей идентификации аномалий заключается в том, что гомеостаз в организме человека не постоянен и зависит от пола, возраста, различных видов цикла и др. В связи с этим обнаружение аномалий и борьба с ними осложняется следующими обстоятельствами: сложностью разделения потоков; необходимостью обработки больших объёмов данных в сжатые сроки; трудностью идентификации аномалии и нахождения местоположения источника.

В этом случае возникает необходимость встраивания в систему мониторинга различных методов оценки функционирования и обнаружений аномалий и отклонений. Однако данный способ не предусматривает контроль содержания информации, полученной с датчиков. Сигнатурные методы позволяют описать данные, полученные с сенсора набором правил или с помощью формальной модели, в качестве которой может применяться символьная строка, семантическое выражение на специальном языке и т.п. Однако для сложных распределенных систем сбора информации проверка на соответствие сценарию является нетривиальной задачей. Системы поиска аномалий идентифицируют необычное поведение («аномалии») в функционировании контролируемого объекта. Методы, обычно применяемые





для обнаружения аномалии, включают использование: пороговых значений; профилей; нейронных сетей; генетических алгоритмов.

4.3 Методы обработки данных

Исторически сложилось, что методы обнаружения аномалий можно разделить на два основных класса, которые могут пересекаться:

Статистические методы предполагают количественный анализ измеряемых характеристик. Системы, реализующие этот метод, производят мониторинг поведения объекта наблюдений и контролируют значения характеристических величин, а также отклонения от порогового значения. Характеристики метода: низкая достоверность, не всегда высокая производительность, но существует способность к обнаружению новых аномалий.

Из методов статистического анализа наиболее часто применяются модели сглаживания, автокорреляции, спектрального анализа, авторегрессии и др. Построение процедуры сглаживания на основе метода скользящего среднего позволяет оценить тренд и построить упрощенную модель прогноза (Рис. 5). Однако необходимо помнить, что данная модель линейна и не может использоваться для критических условий. При подборе модели анализа статистическими методами возникает необходимость построения набора параметров для обнаружения идентификации возникновения аномалии. Это в свою очередь приводит к необходимости сопоставления тех или иных параметров и формирования требований к метрическим показателям, в частности:

- воспроизводимости;
- отсутствию субъективной оценки;
- простоте в сборе и снятии с датчиков;
- возможности выразить измеряемую характеристику числом;
- специфичностью и понятностью.



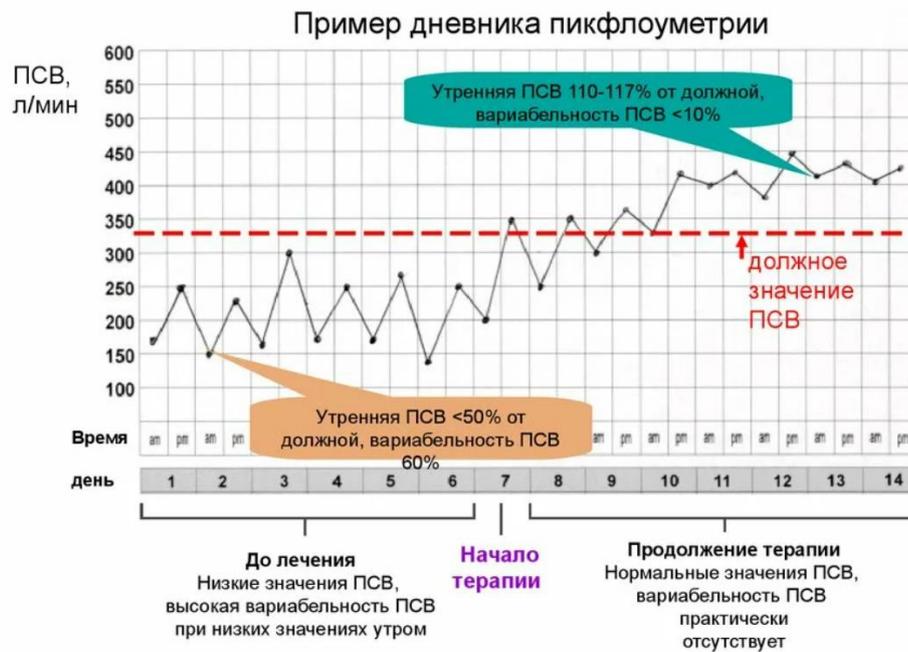


Рис. 5 [2]

Проблема построения параметров наблюдаемого объекта напрямую связана с необходимостью описания классификации воздействий, так как идентификация того или иного отклонения от нормы требует поиска тех характеристик воздействия, которые однозначно смогли бы обнаружить с заданной точностью его тип или совокупность типов в случае множественности воздействий.

Сигнатурные методы используют как качественный, так и количественный анализ характеристик и позволяют обнаружить аномалию по характерным для неё параметрам. Характеристики метода: обнаружение только известных отклонений, но с более высокой точностью.

Метод обнаружения аномалий, основанный на анализе поведения пациента и мониторинге отклонения текущего поведения от нормального профиля, при котором превышение пороговой величины расценивается как аномалия. Метод позволяет обнаруживать известные и неизвестные ранее аномалии поведения, но обладает низкой достоверностью принимаемых решений. Это связано с нестационарностью процессов, протекающих в человеческом организме, и эволюцией поведенческих механизмов [5].

Модели Маркова позволяют вычислить неизвестные характеристики моделей и осуществить прогноз развития [4].

Обнаружение аномалий, основанное на использовании многоагентного моделирования механизмов распространения вирусов, базируется на моделях



команд агентов и их взаимодействия, особенностью которых является учет ключевых параметров исследуемых процессов - параметров вирусов, параметров и механизмов распространения, параметров и механизмов защиты, что позволяет исследовать эффективность разнообразных механизмов защиты [3].

Применение машинного обучения и нейросетевых методов показывает возможность повышения качества обнаружения отклонений от тех или иных параметров, а также повышения быстродействия системы за счет сокращения анализируемых данных. Поскольку нейросетевой подход достаточно терпим к приемлемому количеству ошибочных обучающих примеров, то имеет и слабые стороны: в частности, относительность выдаваемых ответов, высокая вычислительная стоимость обучения, что приводит к отсутствию гарантий приемлемости результата применения метода [6].

4.4 Понятие цифрового двойника

Цифровой двойник (Digital Twin) – цифровая копия физического объекта или процесса, помогающая оптимизировать эффективность процесса принятия решений или функционирования объекта.

Предпосылкой для создания направления послужило:

- развитие теории оптимизации процессов и автоматизации методов принятия решений;
- развитие теории устойчивости нелинейных систем;
- возможность создания цифрового профиля или цифровой модели за счет удешевления базы микроэлектроники и программного обеспечения (возможность повторного использование кода).

Область применения (Рис. 6):

- персонализированная медицина (лечение хронических больных, мониторинг пациентов, прогнозирование);
- реабилитация (уход за новорожденными, лежачими больными...);
- спорт и фитнес (трекинг показателей, хронометраж тренировок...);
- здоровый образ жизни (хронометраж сна, контроль храпа...);
- интенсивные производственные процессы (мониторинг работоспособности операторов, диспетчеров, бойцов...).



В здравоохранении цифровые двойники чаще всего используются при создании технологий мониторинга состояния здоровья пациентов с возможностью анализа данных и передачи их врачам для принятия решений.

Кроме того, цифровой двойник может быть создан не только для физического лица, но и для всей медицинской клиники с целью повышения эффективности на разных этапах операционного управления.

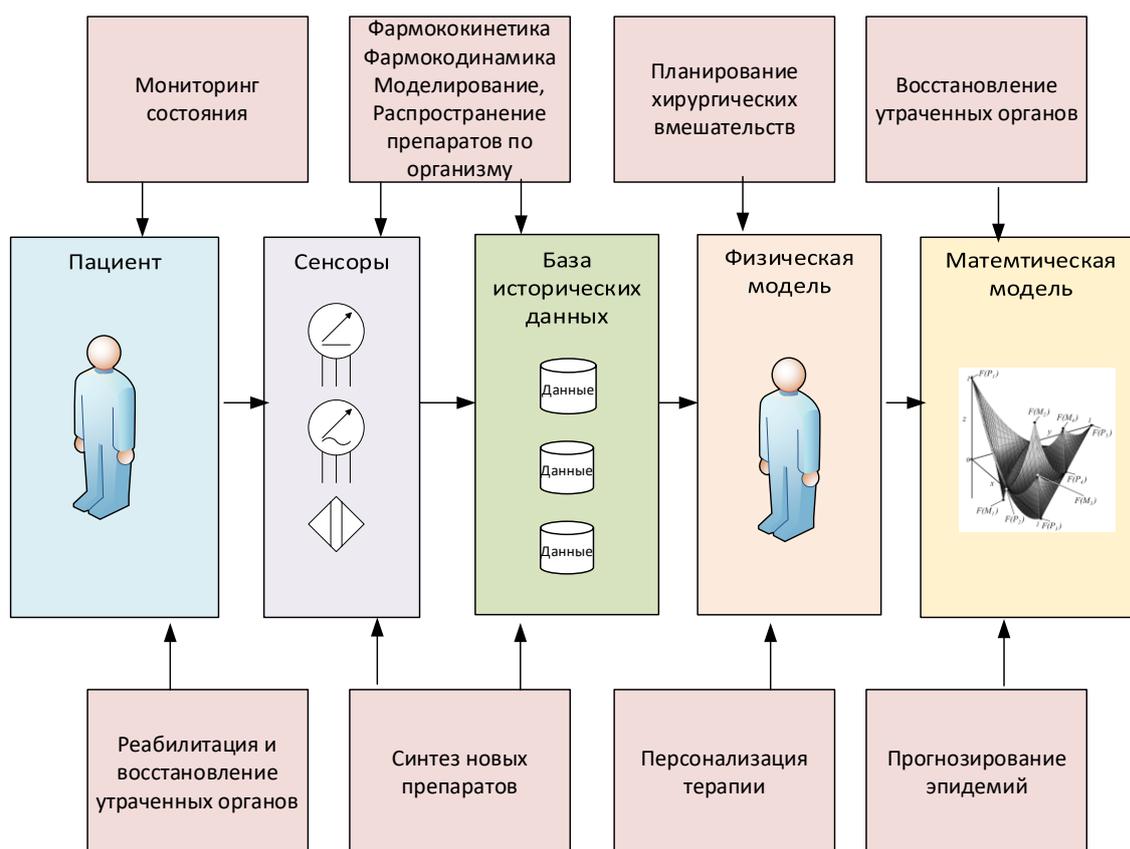


Рис. 6

Классификация цифровых двойников по уровням сложности [8]:

Доцифровой двойник – виртуальный прототип, создаваемый на этапе предварительного проектирования, с целью уменьшения технических рисков и выявления проблемы функционирования на стадии предварительного проектирования.

Цифровой двойник - виртуальная модель физического объекта или процесса. Изучение поведения физического близнеца осуществляется на основе сбора данных от физических датчиков и вычислительных элементов для различных вероятных сценариев.

Адаптивный цифровой двойник - виртуальная модель располагает адаптивным пользовательским интерфейсом с учетом предпочтений и



приоритетов пользователя/оператора. Модели, используемые в двойнике, обновляются на основе данных, получаемых от физического близнеца в режиме реального времени.

Умный цифровой двойник- обладает всеми возможностями адаптивного цифрового двойника, но наряду с этим наделен способностью машинного неконтролируемого обучения, благодаря чему распознает объекты и шаблоны, встречающиеся в рабочей среде и тем самым- обладает высокой степенью автономии.

Рассмотрим основные этапы построения цифрового двойника:

1. Поиск множества сбалансированных показателей модели цифрового двойника позволяет построить математическую модель исследуемого объекта, а также сформировать пространство системы мониторинга за поведением исследуемого объекта.
2. Построение математической или имитационной модели цифрового двойника.
3. Верификация модели позволяет оценить степень соответствия модели близнецу и, в случае необходимости, скорректировать модель и соответствующие ей показатели функционирования.
4. Моделирование функционирования цифрового двойника для различных вероятных сценариев развития исследуемых ситуаций. Этап позволяет сформировать поиск решений для различных жизненных ситуаций.
5. Мониторинг поведения близнеца для распознавания и коррекции траектории развития и/или достижения целевой функции
6. Реконфигурация объекта и/или модели в целях коррекции траектории развития и/или достижения целевой функции.

Использование всех этапов на протяжении требуемого времени необходимо для сбора различных данных об организме человека (результаты обследований, измерения жизненных показателей). Это дает возможность построения цифровой копии любого органа, с выходом на полную виртуальную модель человека, что позволит внедрить технологии персонализированной медицины в полном объеме.





4.5 Методы синтеза и реконфигурации устройств

Для оптимизации построения исследуемого устройства или процесса в условиях необходимости применения синтезирующих функций или в случае возникновения отказов возникает необходимость реконфигурации.

Реконфигурация - изменение состава и способа взаимодействия программных и аппаратных средств системы с целью исключения отказавших программных или аппаратных компонентов.

Реконфигурации имеется три варианта решения:

Слепая реконфигурация - осуществляется перенаправления задач, необходимых для решения близлежащим функциональным элементам, загруженными задачами, имеющими низкий приоритет выполнения.

Структурная реконфигурация - множеству заданных функций ставится в соответствие порядок выполнения и множество алгоритмов выполнения функций. Множеству структурных единиц ставится в соответствие выполнение одной или множества функций.

Структурно-функциональная реконфигурация - учитывает динамически изменяющиеся условия внешней среды и осуществляет переналадивание системы за счет оценки показателей функционирования качества таких как:

- перераспределение потоков;
- динамическое изменение управляющих воздействий в случае изменения карты потока.

Структурно-динамическая реконфигурация, при которой возникает необходимость исследования как структурных, функциональных, так и качественных характеристик системы. На структурном уровне ключевым является выявление критичных элементов, играющих важную роль в обеспечении отказоустойчивости и резервировании системы. На функциональном уровне возникает необходимость выявления сценариев выполнения функций (оптимистичный, пессимистичный, прогнозный). Все это приводит к необходимости формализации системы показателей качества функционирования как системы в целом, так и выполнения целевой функции.

Рассмотрим основные этапы реконфигурации:

Шаг 1. Декомпозиция множества структурно функциональных элементов с возможностью их ранжирования по значимости выполнения целевой функции.





Для этого определяются множества показателей значимости всех элементов при выполнении целевой функции и показатель значимости каждого элемента.

Шаг 2. Формируется множество нарушений функционирования объекта, характеризующее изменения его структурных и функциональных характеристик и состоящее из подмножества нарушений операционного цикла.

Шаг 3. Генерация вариантов множества – вариантов реконфигурации структурно функциональной организации объекта.

3.1. Определение вероятностного пространства нарушений функционирования объекта (из шага 1).

3.2. Определение подмножества элементов (из шага 1), которые могут участвовать в перестроении критически важных процессов при нарушении функционирования объекта. При этом подмножество элементов должно позволять осуществить выбор минимум из двух вариантов структурных элементов с учетом их значимости и интенсивности отказа элемента.

3.3. Формирование множества согласующих правил, позволяющих задавать отношения предпочтения в условиях протекания элементарных событий.

3.4. Построение множества сценариев реконфигурации для каждого варианта нарушения функционирования.

Шаг 4. Коррекция целевых функций, путем построения множества оптимальных решений достижения цели с помощью:

4.1. мониторинга показателей качества функционирования и определения момента времени и структурного элемента, требующего оптимизации;

4.2. исключения структурного элемента, требующего оптимизации процесса из структурно функциональной схемы;

4.3. исключения межструктурных связей, требующих оптимизации и запрета доступа к ним;

4.4. расчета возможных путей реконфигурации с требуемыми структурно функциональными показателями качества, с учетом сценариев реконфигурации.





Шаг 5. Поиск оптимального варианта реконфигурации из множества, полученного на шаге 4 с целью сохранения наиболее приоритетной функции выполнения целевой задачи.

Шаг 6. Коррекция стратегических целей путём построения множества оптимальных решений достижения цели при отклонении показателей качества функционирования объекта (повторение п.п 4.1- 4.4 для стратегических задач, показателей мониторинга, пространства проблемных ситуаций).

При использовании данного подхода формируется новая топологическая структура из элементов, логических каналов, процессов и т. п. При этом остается возможность достижения заданных показателей качества функционирования объекта, с показателями качества до реконфигурации.

СПИСОК ЛИТЕРАТУРЫ

1. Ли П. Архитектура интернета вещей/ пер. с англ. М. А. Райтмана. - М.: ДМК Пресс, 2019. - 454 с.: ил.
2. Цели и правила проведения пикфлоуметрии при бронхиальной астме, нормы ПСВ. <https://bronhialnaya-astma.com/diagnostika/tseli-i-pravila-provedeniya-pikfloumetrii-pri-bronhialnoj-astme-normy-psv>
3. Кондратьев, М. А. Имитационное моделирование в медицине: многоагентная модель распространения гриппа / М. А. Кондратьев // Компьютерные инструменты в образовании. - 2011. - № 4. - С. 32-36.
4. Жукова, О. В. Модель формирования бронхиальной астмы у детей, страдающих острым и рецидивирующим обструктивным бронхитом / О. В. Жукова, С. В. Кононова, Т. М. Конышкина // Сибирский медицинский журнал (Иркутск). - 2016. - Т. 145. - № 6. - С. 22-27.
5. Демченко, М. В. Разработка медицинской информационной системы с элементами поддержки принятия решений в кардиологии / М. В. Демченко, М. А. Фирюлина, И. Л. Каширина // Международный научно-исследовательский журнал. - 2021. - № 8-1(110). - С. 69-76. - DOI 10.23670/IRJ.2021.110.8.010





6. Глубокое машинное обучение (искусственный интеллект) в ультразвуковой диагностике / Г. С. Лебедев, А. П. Маслюков, И. А. Шадеркин, А. И. Шадеркина // Журнал телемедицины и электронного здравоохранения. - 2020. - Т. 6. - № 2. - С. 22-29. - DOI 10.29188/2542-2413-2020-6-2-22-29.
7. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)
8. Денис Хитрых. Цифровой двойник: концепция, уровни, связь с Интернетом вещей и роль численного и системного моделирования. <https://sapr.ru/article/26079>