ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.621.61

ОБЗОР УГРОЗ БЕЗОПАСНОСТИ, УЯЗВИМОСТЕЙ И МЕР ПРОТИВОДЕЙСТВИЯ ИНТЕРНЕТА МЕДИЦИНСКИХ ВЕЩЕЙ В СЕТЯХ С ПОДДЕРЖКОЙ 5G

Акбарова Адиля Нурлановна,
аспирант, akbarovaa94@gmail.com,

Ахунжанов Ислам Бахадырович,
аспирант, islam.ahunjanov@gmail.com.

Кыргызский государственный технический университет имени Исхак Раззакова

Аннотация

Здесь рассматриваются последние достижения встроенных систем Интернета вещей (IoT), беспроводных сетей и биосенсоров, которые помогли в быстрой разработке имплантируемых носимых датчиков. Здесь также рассматриваются приложения Интернета медицинских вещей (IoMT), которые привлекли большое внимание как экосистема подключенных клинических систем, вычислительных систем и медицинских датчиков, направленных на повышение качества медицинских услуг. Технология искусственного интеллекта на основе 5G может изменить представление о здравоохранении и образе жизни. В свете важности платформ IoT и сетей 5G цель этой предлагаемой исследовательской работы состоит в том, чтобы выявить угрозы, которые могут подорвать целостность, конфиденциальность и безопасность систем IoT. Кроме того, новые подходы на основе блокчейна, которые могут помочь в повышении конфиденциальности сети IoMT. Было обнаружено, что IoT уязвим для различных типов атак, включая отказ в обслуживании (DoS), вредоносное ПО и атаки с прослушиванием. Кроме того, IoT подвержен различным уязвимостям, таким как безопасность, конфиденциальность и конфиденциальность. Несмотря на многочисленные угрозы безопасности, существуют новые криптографические методы, такие как контроль доступа, проверка подлинности и шифрование данных, которые могут помочь повысить безопасность и надежность устройств IoMT.

Ключевые слова: IoMT, DoS, IoT, сеть 5G

OVERVIEW OF SECURITY THREATS, VULNERABILITIES AND COUNTERMEASURES OF THE INTERNET OF MEDICAL THINGS ON 5G NETWORKS

Adilya N. Akbarova,
graduate student, akbarovaa94@gmail.com,

Islam B. Ahunjanov,

graduate student, islam.ahunjanov@gmail.com.

Kyrgyz State Technical University named after Iskhak Razzakov

ABSTRACT

It reviews the latest advances in embedded Internet of Things (IoT), wireless networks, and biosensors that have helped drive the rapid development of implantable wearable sensors. It also looks at the applications of the Internet of Medical Things (IoMT), which have received a lot of attention as an ecosystem of connected clinical systems, computing systems, and medical sensors aimed at improving the quality of medical services. 5G artificial intelligence technology could change the way we think about healthcare and lifestyle. In light of the importance of IoT platforms and 5G networks, the goal of this proposed research work is to identify threats that could undermine the integrity, privacy, and security of IoT systems. In addition, new blockchain-based approaches that can help improve the privacy of the IoMT network. The IoT has been found to be vulnerable to various types of attacks, including denial of service (DoS), malware, and eavesdropping attacks. In addition, the IoT is subject to various vulnerabilities such as security, privacy and confidentiality. Despite numerous security threats, there are new cryptographic techniques such as access control, authentication, and data encryption that can help improve the security and reliability of IoMT devices.

Keywords: IoMT, DoS, IoT, 5G.

Развитие науки и техники в различных областях жизнедеятельности человека приводит к тому, что все большее число рутинных операций автоматизируется. Не исключением является и строительная отрасль, активное развитие которой сегодня происходит с комплексным внедрением цифровых технологий. Данный подход заложен в концепции Строительство 4.0, непосредственно связанной с Индустрией 4.0.

Развитие человечества неразрывно связано с изменением методов и подходов в различных областях его жизнедеятельности, что подтверждается историей. Так, например, первая промышленная революция произошла в ведущих государствах мира в XVIII—XIX веках. Характерной чертой этого промышленного переворота стал массовый переход от ручного труда к машинному, от мануфактурного производства к фабричному. И этот пример не один.

При этом одним из ключевых аспектов совершенствования промышленности при развитии концепции «Индустрия 4.0» объявляется применение в заводских процессах киберфизических систем (КФС), внедрение которых обеспечивает полную интеграцию вычислительных ресурсов в физические процессы. При этом внедрение КФС предполагается как в промышленность, так и на транспорте, в энергетику и даже системы жизнеобеспечения. Вместе с тем связующим звеном между физической, биологической и цифровой реальностями становятся информационные технологии. [11]

Последние разработки в области полупроводников и связанных с ними технологий, включая датчики и системы. Умные устройства используют искусственный интеллект (ИИ) для составления интеллектуальных прогнозов. Однако, как упоминалось, чтобы гарантировать, что эти устройства эффективно используют федеративное обучение — идеальное совместное обучение для устройств IoMT, они должны быть подключены к сети

беспроводной связи для выполнения различных сложных вычислительных задач. Для этого необходимая поддержка интеллектуальных медицинских устройств возможна только с помощью 5G или других коммуникационных технологий. использование этих технологий, как уже упоминалось, не ограничивается смартфонами, но и различным разнообразием. В то время как использование дизайна сети 5G может значительно улучшить стоимость, гибкость и возможности сети IoMT. Несмотря на высокий спрос сети 5G использует для передачи терагерцовые сигналы, со скоростью передачи более 1 Тбит/с и основан на трехмерной структуре связи (частота, пространство и время), а не на двумерной структуре, как в сети 5G. Медицинские устройства интернета вещей IoT с широким и глубоким охватом.(https://tallinn.mhealth.events/article/iot-v-meditsine-kak-internet-veshchey-sovershenstvuet-sferu-zdravoohraneniya-97414)

Селективный блокчейн соединяет Интернет вещей, умные объекты, а затем миллиарды умных городов, умных фабрик, умного здравоохранения, сетей умных автомобилей, таких как умные сети, умные дома и экосистемы умных технологий, которые приводят к созданию новой парадигмы. Одной из наиболее важных областей внедрения технологий в секторе здравоохранения является повсеместное предоставление услуг в режиме реального времени. Под эгидой Интернета вещей IoT разнообразные объекты, такие как машины, люди и вещи, взаимосвязаны везде и в любое время в пространстве данных. Рост и развитие Интернета вещей динамично меняет индустрию здравоохранения с внедрением Интернета вещей, в котором медицинские устройства доступны каждому через глобальную сеть, в любом месте и в любое время (рис. 1).

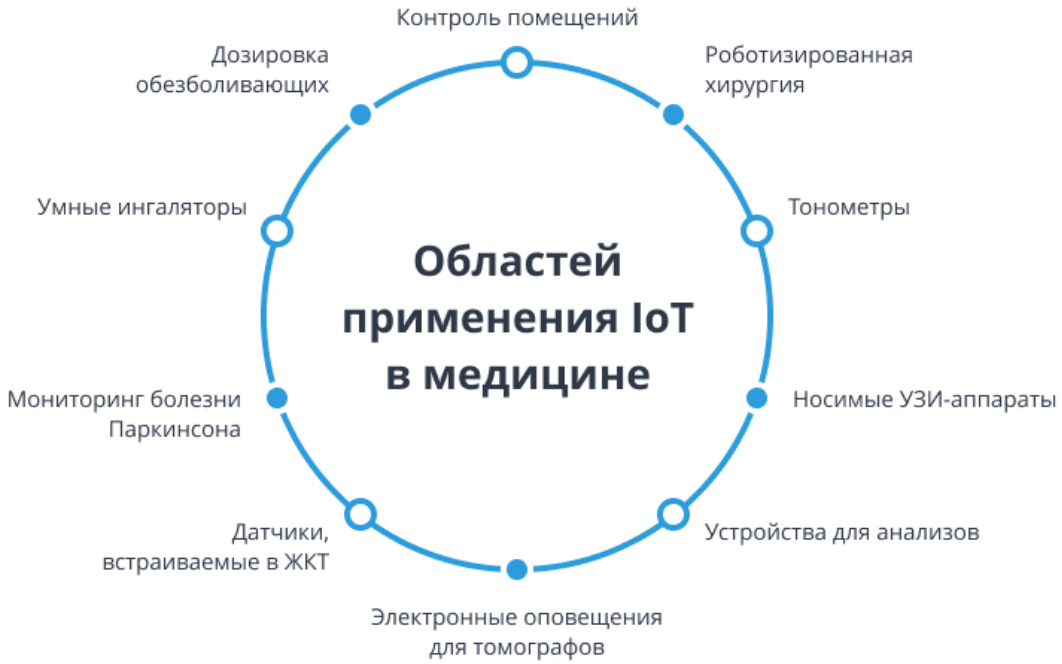

Рисунок 1. Применение медицинского интернета вещей для медицинских услуг [1]

Это делает IoT следующим шагом в мировом технологическом развитии с темпом расширения более 270%. Но хотя это играет большую роль в изменении будущего умных городов, повсеместный, плотный и невидимый сбор, а также передача и обработка информации в личной жизни людей вызывают серьезные опасения по поводу конфиденциальности. В частности, устройства IoMT, имплантируемые датчики и медицинские носимые устройства, которые составляют основные компоненты пограничной сети IoMT, подвергаются риску из-за различных угроз кибербезопасности и, таким образом, представляют серьезную угрозу безопасности пользователей и конфиденциальности пациентов [6]. Динамичный и универсальный характер устройств

Интернета вещей значительно увеличивает вероятность киберэксплуатации, которая может привести к атакам доступа к данным, отказу в обслуживании (dos), атакам распределенных сетевых ботов, нарушению целостности и существующих процессов, компрометации данных или разрушению всей экосистемы. Несанкционированный доступ к медицинской информации пациента может нанести потенциальный вред при назначении неправильных медицинских рецептов, что приведет к риску для здоровья или даже смерти. Следовательно, в дополнение к большим преимуществам, Интернет вещей уязвим для киберугроз, таких как распространение вредоносных ботов, кража личных данных, фишинг и кейлоггинг, что делает область биомедицины важной областью исследований. В дополнение к потенциальным угрозам кибербезопасности цифровой ландшафт IoMT требует методов взлома, которые подрывают физическую безопасность. Поскольку безопасность зависит от надежности медицинского устройства, успешная интеграция технологии IoMT в здравоохранение требует наличия механизма безопасности, обеспечивающего безопасность сети IoMT [10]. Важным шагом в этом отношении является выявление потенциальных и существующих угроз для сети IoMT. Поскольку устройства IoMT обладают теми же техническими характеристиками и функциями, что и возможности, и функции устройств Интернета вещей, существующие атаки можно рассматривать как угрозу повреждения устройств IoT.

Одна из ключевых проблем в терапии диабета — недостаточная и поздняя выявляемость диабета 2 типа. По данным Минздрава России, в 2019 г. было 5 110 090 больных всеми типами сахарного диабета, что дает 3,5% от всего населения, или 4,7% от населения 20–79 лет, если вести расчет по методике IDF, хотя в регистре учитываются также дети и подростки. (https://expertnw.com/tekhnologii/)

Для лечения больных, страдающих сахарным диабетом II типа с нарушенной секрецией инсулина, но с отсутствием инсулинорезистентности тканей.

В чем суть. Технология позволяет избежать регулярных инъекций инсулина пациентам с сахарным диабетом. Вместо них — одна щадящая операция и инъекция. В основе нового подхода к лечению лежит технология, которая помогает управлять активностью органов и тканей с помощью термогенетики. Методика не имеет мировых аналогов, утверждают авторы проекта.

В бета-клетки пациентов вводятся ионные каналы, пропускающие кальций в ответ на стимуляцию инфракрасным светом. В тело больного имплантируется крошечный аппарат, который постоянно измеряет уровень глюкозы и при его повышении подает инфракрасный сигнал бета-клеткам. При росте уровня глюкозы внутри бета-клеток будет создаваться повышенная концентрация ионов кальция, что послужит сигналом для выброса инсулина. Этот механизм максимально близок к естественному и замедлит развитие патологии, улучшит самочувствие больных [12].

Все больше и больше организаций осознают, что угрозы информационной безопасности могут негативно сказаться на непрерывности бизнеса и общественном имидже, вызывая проблемы с юридическими органами в плане соблюдения этих требований. Эти риски также могут привести к финансовым потерям и негативно повлиять на отношения с клиентами и партнерами и сделать эти отношения удовлетворительными.

«Информационная безопасность защищает данные и их ключевые компоненты.» Информационная безопасность характеризуется тремя основными характеристиками: безопасностью, конфиденциальностью и доступностью. Сохранение конфиденциальности важно, поскольку это ограничивает число людей, имеющих доступ к информации. Целостность информации подразумевает, насколько она полна и неизменяема. Атрибуты доступности делают данные доступными для пользователей или других систем [2].

Внутренние угрозы были горячей темой в области информационной безопасности в течение многих лет, однако имеющиеся данные по этому поводу разочаровывают 50 процентов респондентов заявили, что в 2012 году они ожидали финансовых потерь только из-за внешних атак, а не из-за внутренних злоупотреблений. Однако 44% респондентов признали, что в 2015 году они были жертвами инсайдерской торговлей, что сделало их второй по распространенности формой мошенничества в сфере информационной безопасности после вирусов. Последнее исследование Ernst & Young (2015) также показывает, что внутренний риск выше: 25% респондентов сообщают об увеличении числа внутренних атак и 13% сообщают об увеличении числа мошенников, совершивших внутри компании.(https://cyberleninka.ru/article/n/vnutrennie-ugrozy-vs-vneshnie-ugrozy-dlya-rossii-dinamika-obschestvennyh-nastroeniy/viewer)

Сотрудники, бывшие сотрудники, партнеры или клиенты, которые разрешают доступ к корпоративным активам, будут использовать этот доступ таким образом, который ухудшит безопасность корпоративной информации, что называется "внутренними угрозами". Внутренний риск является проблемой для всех организаций из-за ряда негативных слухов или рисков. по мнению некоторых исследователей, внутренний риск может быть важнее внешних угроз, но не каждая компания рассматривает своих сотрудников как серьезный фактор угрозы [4].

Наш страх перед хакерами может привести к тому, что мы неадекватно отреагируем на решение проблем информационной безопасности, потому что у тех, кого мы знаем и кому доверяем (например, у сотрудников ИТ-поддержки), нет причин бояться. В отличие от сотрудников, у которых нет физического или надлежащего доступа, инсайдеры с большей вероятностью поставят под угрозу информационную безопасность компании.

Если менеджеры с подозрением относятся к своим сотрудникам и считают их преступниками, слишком строгие требования могут привести к культуре невежества, которая позволяет обходить правила и способствовать недовольству. Важно соблюдать баланс между безопасностью и простотой использования, но организация должна принимать во внимание различные аспекты угроз, рисков, контрмер и людей. На самом деле многие компании сталкиваются с проблемой защиты информации, которой необходимо делиться с сотрудниками для выполнения или поддержки бизнес-процесса.

В исследовательской работе могут использоваться качественные, количественные и смешанные подходы. При качественном подходе исследования фокусируются на глубоком и детальном изучении теоретических данных, которые обычно собираются для описания или определения явления с использованием открытых инструментов. Однако, когда выбирается количественный подход, исследование фокусируется на числовых или статистических данных, собранных для подтверждения гипотезы или оценки корреляций между выбранными переменными. Исследовательские подходы должны выбираться на основе заранее поставленных целей. Таким образом, для достижения целей данного исследования использовался количественный подход.

Выбор подходящего исследовательского подхода обеспечивает основу для исследования; однако этап сбора данных необходим для сбора необходимых данных из источников, которые могут быть проанализированы для интерпретации и получения статистических результатов [3]. Как правило, есть два источника данных, которые предоставляют данные для исследования, то есть первичные и вторичные источники данных. Источники первичных данных обычно основаны на участниках, выбранных для получения исходных и исходных данных, специально предназначенных для достижения цели исследования. Однако компании обычно передают такие исследования на аутсорсинг исследовательским агентствам из-за ограничений по времени и стоимости. С другой стороны, вторичные источники данных могут быть в форме литературных источников,

таких как журнальные статьи, статьи на веб-сайтах, книги, материалы конференций или годовые отчеты организаций. Установлено, что эта информация содержит риск быть либо неактуальной, либо устаревшей. Однако вторичное исследование обычно считается эффективным с точки зрения затрат и времени и сводит к минимуму этические риски. В связи с этим данные собираются из таких источников, как журналы IEEE, Springer и Elsevier.

Безопасность данных

Из-за зависимости от открытой беспроводной связи устройства IoMT уязвимы для сетевых/беспроводных атак. Злоумышленник может перехватывать и прослушивать исходящие и входящие данные из-за отсутствия мер безопасности, от которых страдают устройства IoMT из-за конструкции или слабых мер безопасности аутентификации. Более того, поскольку большинство устройств IoMT не способны обнаруживать и предотвращать атаки, опытные злоумышленники могут обойти систему безопасности и получить несанкционированный доступ к данным пациента. Как следствие, злоумышленники могут использовать повышенные привилегии при заражении устройств вредоносными кодами или вредоносными программами. Это видно из исследования, где авторы продемонстрировали, насколько медицинские устройства уязвимы для атак зомби или ботнетов. Например, приступ может логически изменить или манипулировать дозой препарата, что может привести к серьезным последствиям для здоровья или смерти пациента. Следовательно, поскольку большинство устройств IoMT используют технологию блокчейна, злоумышленник может идентифицировать запись пациента в сети блокчейна. Более того, в системах здравоохранения медицинские данные склонны к фабрикации, что может привести к неправильному назначению лекарств и прогнозу пациента, что в дальнейшем может привести к аллергической реакции. Из-за уязвимостей в системе безопасности злоумышленники также могут отправлять фальшивые медицинские предупреждения и причинять значительные финансовые потери [5].

Медицинские учреждения, с другой стороны, теперь должны рассматривать кибербезопасность как стратегическую проблему. Медицинские учреждения являются главной целью для хакеров из-за устаревшего почтения, некачественных информационных систем и общего отсутствия управления ИТ в больницах. Они используют программы-вымогатели, чтобы вывести из строя системы, продать данные о пациентах тому, кто предложит самую высокую цену, угрожать обнародованием частной информации и отключить электроснабжение больниц.

В исследователи рассмотрели классификацию SVM, помня о безопасности. Раньше можно было обезопасить обучающую выборку многими другими способами. Один подход показывает установленную скорость другим пользователям, а другой подход скрывает ее от пользователей. Оба подхода предполагают, что окончательный классификатор надежно хранится надежной третьей стороной, и не обращаются к защите SVM после обучения.

Конфиденциальность данных

Типы атаки в IoMT

- Вредоносная атака
- Подслушивающая атака
- DOS атаки

Данные, собранные с помощью устройств для химиотерапии, могут раскрыть конфиденциальную информацию о привычках пациента. Например, как описано, сигналы, передаваемые датчиками, используемыми для сообщения о состоянии пациента, могут раскрывать медицинские функции устройства. Аналогичным образом, при пассивных атаках, таких как анализ трафика, злоумышленники могут разгадывать или

собирать идентификационную информацию пациента в дополнение к чувствительной и конфиденциальной информации [7]. И самое главное, как обсуждалось, такие атаки, как "человек посередине" (MitM), могут саботировать целостность и конфиденциальность сетей IoMT, вмешиваясь в коммуникации, чтобы явно изменить обмен данными между сторонами. Например, собранные медицинские данные могут быть отправлены на удаленный сервер, где злоумышленники могут изменять и перехватывать медицинские данные, чтобы нарушить их конфиденциальность. Кроме того, поскольку несанкционированное хранение информации уязвимо для атак на целостность данных, конфиденциальность и безопасность, исследователи превратили такие проблемы конфиденциальности и безопасности в серьезную угрозу конфиденциальности пользователей и конфиденциальности данных. Это совершенно очевидно для устройств IoMT, поскольку у них отсутствует надежный механизм аутентификации. Таким образом, отсутствие контроля доступа к сети и шифрования данных позволяет злоумышленникам нарушать конфиденциальность пользователей путем прослушивания.

Процесс сохранения конфиденциальности в обученной SVM также может быть описан с помощью, которого является другим методом. Хотя этот подход не берет на себя роль функции Гаусса, его можно использовать только с ядром Гаусса, конечная SVM может привести к утечке информации о типах окончательной классификации, даже если это гарантирует конфиденциальность. В связи с этим данный метод обладает низкой точностью. Когда на самом деле главной целью было выпустить готовую рабочую тетрадь, сохранив при этом конфиденциальность векторов поддержки пациентов, большинство решений было сосредоточено на медицинских рабочих тетрадях. Если они создадут рабочую книгу SVM, они смогут создавать опорные векторы, необходимые для практического извлечения биометрических данных субъекта [8,9]. Так что эти системы не работают. Система сопоставления аутентификации SvM должна быть разработана с акцентом на предотвращение раскрытия конфиденциальных данных из стандартной классификации.

Заключение

Динамика медицинских процедур была изменена современными технологическими инновациями с появлением сетевых медицинских устройств. В результате интерес к сетевой безопасности медицинских устройств привлек внимание. Кроме того, было отмечено, что с внедрением новых коммуникационных технологий, таких как сети 5G, будет проведена полная реструктуризация отрасли здравоохранения. Мы увидим прекрасные изменения в секторе здравоохранения благодаря ускоренному развитию коммуникационных технологий. Из-за проблем со связью он не может выполнить операцию удаленно. Благодаря инфраструктуре 5G службы скорой помощи будут заменены службами скорой помощи, а оборудование перевозчика будет пересмотрено. Однако из-за технологических достижений эта платформа подвержена различным угрозам безопасности и, следовательно, может представлять большую угрозу для конфиденциальности и безопасности пациентов. Таким образом, современные проблемы безопасности вынуждают исследователей анализировать различные преимущества медицинских устройств. Кроме того, поскольку безопасность является важным элементом для обеспечения надежности международных онкологических лечебных учреждений и успешной интеграции этой технологии в систему здравоохранения, необходимы новые защитные планы, которые могут обеспечить целостность и безопасность международных систем лечения онкологии. В связи с этим текущее исследование выявляет существующие угрозы и атаки, которые угрожают: открытости, авторизации, аутентификации, неотторжению, целостности и конфиденциальности устройств внутреннего контроля. Кроме того, в исследовании рассматривались аномалии, заимствованные из литературы, и новая защита от угрозы

международных схем химиотерапии. Наконец, были предложены различные методы и планы для более надежного выявления и улучшения IoMT, которые могут помочь в дальнейшем улучшении качества медицинской помощи и здоровья пациентов.

Список литературы:

1. IoT в медицине: Будущее уже наступило [https://www.azoft.ru/blog/iot-in-healthcare/]
2. Ван, Л., Али, Ю., Назир, С., Ниази, М. Система оценки ISA для безопасности системы интернета медицинских вещей с использованием методов AHP-TOPSIS. IEEE Access 8, 152316–152332 (2020).
3. Наяк, С., Патгири, Р. Видение интеллектуальной медицинской службы для неотложной помощи в эпоху связи 5G и 6G. Одобренный EAI Trans. Интернет-вещи 6 (22), 1–13 (2020)
4. Обзор угроз безопасности интернета вещей [https://cyberleninka.ru/article/n/obzor-ugroz-bezopasnosti-interneta-veschey]
5. Информационная безопасность интернета вещей [https://www.tadviser.ru/index.php/]
6. Папайоанну М., Карагеоргу М., Мантас Г., Сукасас В., Эссоп И. и др. Исследование угроз безопасности и мер противодействия в Интернете медицинских вещей (IoMT). Транс. Новые Телекоммуникации. Технол. e4049 (2020).
7. Атамли А.В., Мартин А. Анализ безопасности Интернета вещей на основе угроз. Международный семинар по безопасному Интернету вещей, 2014 г., Вроцлав, Польша, стр. 35–43 (2014 г.).
8. Ахтаруззаман, М., Хасан, М.К., Кабир, С.Р., Абдулла, SNHS, Садек, М.Дж. и др. Распределенная модель глубокого обучения на основе узких мест HSIC для прогнозирования нагрузки в интеллектуальных сетях с всесторонним обзором. IEEE Access 8, 222977–223008 (2020).
9. Проблемы безопасности Интернета вещей [https://izd-mn.com/PDF/20MNNPU21.pdf]
10. Рани, С., Ахмед, С.Х., Талвар, Р., Малхотра, Дж., Сонг, Х. IoMT: надежный межуровневый протокол для Интернета мультимедийных вещей. IEEE IoT J. 4 (3) , 832–839 (2017).
11. Ацето, Г., Персико, В., Пескейп, А. Обзор информационных и коммуникационных технологий для Индустрии 4.0: современное состояние, таксономии, перспективы и проблемы. Сообщество IEEE. Surv. Учебники 21 (4) , 3467–3501 (2019).
12. Джоши А.М., Джейн П., Моханти С.П. Secure-iGLU: безопасное устройство для неинвазивного измерения уровня глюкозы и автоматической доставки инсулина в рамках IoMT . В: Ежегодный симпозиум IEEE Computer Society по СБИС (ISVLSI) 2020 г. Лимассол, Кипр , стр. 440–445 (2020.).

References:

1. IoT in medicine: The future is here [https://www.azoft.ru/blog/iot-in-healthcare/]
2. Wang, L., Ali, Y., Nazir, S., Niazi, M. ISA scoring system for IoT system security using AHP-TOPSIS methods. IEEE Access 8, 152316–152332 (2020).

3. Nyack, S., Patgiri, R.: The vision of an intelligent medical service for emergency care in the era of 5G and 6G communications. Approved by EAI Trans. Internet Things 6 (22), 1–13 (2020)
4. Overview of threats to the security of the Internet of things [https://cyberleninka.ru/article/n/obzor-ugroz-bezopasnosti-interneta-veschey]
5. Information security of the Internet of things [https://www.tadviser.ru/index.php/]
6. Papaioannou M, Karageorgu M, Mantas G, Sukasas V, Essop I, et al. Exploring Security Threats and Countermeasures in the Internet of Medical Things (IoMT). Trance. New Telecommunications. Technol. e4049 (2020).
7. Atamli A.V., Martin A. Security analysis of the Internet of things based on threats. In: International Seminar on the Secure Internet of Things 2014, Wroclaw, Poland, pp. 35–43 (2014).
8. Akhtaruzzaman, M., Hassan, M.K., Kabir, S.R., Abdullah, SNHS, Sadeq, M.J. et al. A Distributed Deep Learning Model Based on HSIC Bottlenecks for Load Prediction in Smart Grids with a Comprehensive View. IEEE Access 8, 222977–223008 (2020).
9. Internet of Things Security Issues [https://izd-mn.com/PDF/20MNNPU21.pdf]
10. Rani, S., Ahmed, S.H., Talwar, R., Malhotra, J., Song, H. IoMT: A reliable cross-layer protocol for the Internet of multimedia things. IEEE IoT J. 4(3), 832–839 (2017).
11. Aceto, G., Persico, V., Pesscape, A. Overview of Information and Communication Technologies for Industry 4.0: State of the Art, Taxonomies, Perspectives, and Challenges IEEE Community. Surv. Textbooks 21(4), 3467–3501 (2019).
12. Joshi A.M., Jane P., Mohanty S.P. Secure-iGLU: A secure device for non-invasive glucose measurement and automated insulin delivery within the IoMT. In: IEEE Computer Society VLSI Annual Symposium (ISVLSI) 2020, Limassol, Cyprus, pp. 440–445 (2020.).