УДК 004.056.5

Коваленко Максим Алексеевич, студент (бакалавр), департамент информационной безопасности
Дальневосточный федеральный университет (г. Владивосток, Россия)
Баранов Денис Борисович, студент (бакалавр), департамент информационной безопасности
Дальневосточный федеральный университет (г. Владивосток, Россия)
Максимов Артём Евгеньевич, студент (бакалавр), департамент информационной безопасности
Дальневосточный федеральный университет (г. Владивосток, Россия)
Бледных Эдуард Данилович, студент (бакалавр), департамент истории и археологии
Дальневосточный федеральный университет (г. Владивосток, Россия)

ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА ВЕЩЕЙ В ЗДРАВООХРАНЕНИИ: ВЛИЯНИЕ НА МОНИТОРИНГ ЗДОРОВЬЯ И БЕЗОПАСНОСТЬ ДАННЫХ

Аннотация: *В данной статье рассматривается использование технологий Интернета вещей (IoT) для мониторинга состояния здоровья, а также актуальные угрозы и риски информационной безопасности, связанные с такими устройствами. Описаны примеры медицинских IoT-устройств и ключевые проблемы безопасности, включая угрозы конфиденциальности данных, кибератаки и уязвимости сетей. Анализируются современные методы защиты информации, такие как шифрование, аутентификация и управление доступом. Статья подчеркивает необходимость стандартизации и внедрения комплексных решений для обеспечения безопасности в области медицинских IoT.*

Annotation: *The article explores the use of Internet of Things (IoT) technologies for health monitoring, as well as current threats and information security risks associated with such devices. It describes examples of medical IoT devices and key*

security issues, including data privacy threats, cyberattacks, and network vulnerabilities. The paper analyzes modern information protection methods such as encryption, authentication, and access control. It emphasizes the need for standardization and the implementation of comprehensive solutions to ensure security in the field of medical IoT.

Ключевые слова: *Интернет вещей, медицинские устройства, информационная безопасность, защита данных, персональные медицинские данные, риски утечки информации.*

Keywords: *web applications, web application firewall, application-level threats, information security, injection attacks.*

Применение Интернета вещей (IoT) в здравоохранении становится все более масштабным и многообразным, охватывая широкий спектр процессов — от диагностики и мониторинга до управления медицинскими учреждениями и ресурсами. IoT представляет собой совокупность взаимосвязанных устройств, обладающих возможностью сбора, обработки и передачи данных в автоматическом режиме. В контексте медицины это означает более точное, непрерывное и персонализированное наблюдение за состоянием пациентов, что, в свою очередь, способствует улучшению качества медицинской помощи, снижению затрат и повышению эффективности клинических решений.

Одним из наиболее распространенных примеров внедрения IoT в здравоохранение являются носимые устройства. Это умные браслеты, часы, трекеры и другие портативные сенсоры, которые способны измерять жизненно важные параметры организма, такие как частота сердечных сокращений, уровень кислорода в крови, температура тела, пульс, артериальное давление, качество сна и уровень физической активности. Сбор и анализ этих данных в режиме реального времени позволяют как пациентам, так и врачам отслеживать состояние здоровья и быстро реагировать на возникающие отклонения. Особенно актуальны такие устройства для людей с хроническими

заболеваниями, включая сахарный диабет, гипертонию, ишемическую болезнь сердца и бронхиальную астму. Использование носимых IoT-устройств способствует снижению количества визитов к врачу и позволяет проводить профилактику осложнений, предотвращая развитие критических состояний(рисунок 1).

Помимо носимых, всё более активно применяются имплантируемые устройства, такие как современные кардиостимуляторы, дефибрилляторы, нейростимуляторы и инсулиновые помпы. Эти устройства не только выполняют свои базовые функции, но и оснащаются беспроводными модулями, которые передают информацию в облачные системы или напрямую в медицинские базы данных. Таким образом, обеспечивается возможность постоянного контроля за функционированием оборудования и состоянием пациента. В случае выявления сбоев или критических изменений система может оперативно оповестить врача или даже активировать экстренные протоколы помощи. Это значительно повышает безопасность и снижает риски, связанные с отказом оборудования.

Стационарные IoT-системы, применяемые в клиниках и госпиталях, также играют ключевую роль в цифровизации здравоохранения. К ним относятся интеллектуальные кроватные мониторы, инфузионные насосы, аппараты искусственной вентиляции легких, термоконтрольные устройства, а также системы наблюдения и климат-контроля в стерильных помещениях. Все эти элементы могут быть объединены в единую информационную инфраструктуру, которая позволяет медицинскому персоналу централизованно отслеживать состояние пациентов, автоматически настраивать параметры оборудования и вести медицинскую документацию. Такие интеграции особенно эффективны в палатах интенсивной терапии и при лечении пациентов с множественными хроническими заболеваниями.

Еще одной важной сферой применения IoT является телемедицина. IoT-устройства, интегрированные с онлайн-платформами, позволяют врачам контролировать параметры пациента на расстоянии, проводить дистанционные консультации, корректировать схемы лечения и отслеживать результаты терапии.

Это особенно актуально в условиях пандемий, ограниченной мобильности пациентов и удаленности от медицинских центров. Более того, появление технологий цифровых двойников пациента — виртуальных моделей организма, созданных на основе данных, собранных IoT-устройствами — позволяет прогнозировать реакцию на лечение и моделировать развитие заболеваний без риска для самого пациента.

Применение IoT также повышает эффективность системы экстренного реагирования. Например, если пациент теряет сознание или показатели его здоровья резко ухудшаются, устройство автоматически отправляет сигнал тревоги медицинскому персоналу или напрямую в службу скорой помощи. Это особенно важно для пожилых людей, людей с эпилепсией, сердечно-сосудистыми патологиями и другими состояниями, требующими немедленного вмешательства. В некоторых случаях такие системы могут предотвратить смертельные исходы, обеспечивая своевременное реагирование.

Рисунок 1 - Пример умных медицинских устройств и систем мониторинга

Внедрение технологий Интернета вещей (IoT) в здравоохранение открывает широкие перспективы для развития отрасли, оптимизации

медицинских процессов и повышения качества обслуживания пациентов. Благодаря способности устройств IoT собирать и передавать данные в режиме реального времени, медицина становится более точной, предиктивной и ориентированной на пациента. Рассмотрим основные преимущества и возможности применения этих технологий.

Одним из ключевых преимуществ IoT в медицине является возможность круглосуточного мониторинга состояния здоровья пациентов. Устройства, такие как носимые трекеры, глюкометры, пульсометры и тонометры, обеспечивают непрерывное отслеживание жизненно важных показателей. Это особенно важно для пациентов с хроническими заболеваниями, пожилых людей и пациентов, находящихся в реабилитации после операций.

Постоянное наблюдение позволяет выявлять даже незначительные отклонения от нормы, что способствует раннему диагностированию заболеваний и предотвращению острых состояний. Например, резкое повышение артериального давления может быть немедленно зафиксировано и передано врачу для принятия решения, не дожидаясь визита в клинику.

IoT способствует развитию персонализированной медицины. Собранные данные о физиологических показателях, образе жизни, режиме сна и активности пациента позволяют врачам строить более точные индивидуальные схемы лечения. Вместо стандартных терапевтических протоколов можно применять адаптивные подходы, которые учитывают уникальные особенности конкретного организма.

Кроме того, системы искусственного интеллекта, работающие в связке с IoT-устройствами, могут анализировать большие объемы данных и предлагать персонализированные рекомендации. Это может касаться, например, корректировки дозировки лекарств, выбора диеты или оптимального графика физических нагрузок.

Постоянный мониторинг и оперативная обработка данных позволяют заранее выявлять состояния, требующие вмешательства. В результате

сокращается количество экстренных госпитализаций, вызовов скорой помощи и других критических ситуаций.

Автоматизированные системы оповещения могут в реальном времени сообщать врачу или родственникам пациента о рисках. Например, при падении пожилого человека с носимым датчиком система может немедленно отправить сигнал тревоги. Это позволяет среагировать быстрее и минимизировать последствия.

IoT-технологии создают основу для эффективного дистанционного наблюдения. Врач может получать актуальные данные о состоянии пациента, находясь за сотни километров от него. Это особенно важно в сельских или труднодоступных регионах, где доступ к медицинским учреждениям ограничен.

Удалённый контроль позволяет не только отслеживать эффективность терапии, но и вносить в нее коррективы без необходимости личного посещения врача. Это экономит время как пациентов, так и медицинских работников, снижает нагрузку на поликлиники и больницы, способствует оптимизации медицинского процесса.

IoT-устройства собирают большие объемы данных с высокой частотой, что позволяет получать более полную клиническую картину состояния пациента. В отличие от традиционных методов, при которых измерения проводятся эпизодически, IoT обеспечивает непрерывный поток информации, что снижает риск ошибок и недоучтённых факторов.

Анализ трендов и отклонений во времени даёт возможность предсказать развитие заболевания, оценить влияние лечения и повысить точность диагностики. Например, при использовании IoT-систем в кардиологии врачи могут анализировать не только факт аритмии, но и частоту, длительность и условия её возникновения.

Благодаря автоматическому сбору данных, медицинские сотрудники освобождаются от части рутинных задач. Это позволяет сконцентрироваться на клиническом принятии решений и индивидуальной работе с пациентами. Кроме

того, IoT-системы упрощают документооборот, снижая количество ручного ввода информации и исключая ошибки, связанные с человеческим фактором.

Например, автоматическая регистрация показателей пациента напрямую в электронной медицинской карте экономит время и повышает точность учёта. Такие решения особенно востребованы в стационарах и отделениях интенсивной терапии. Схема взаимодействия IoT-устройств продемонстрирована на рисунке 2.

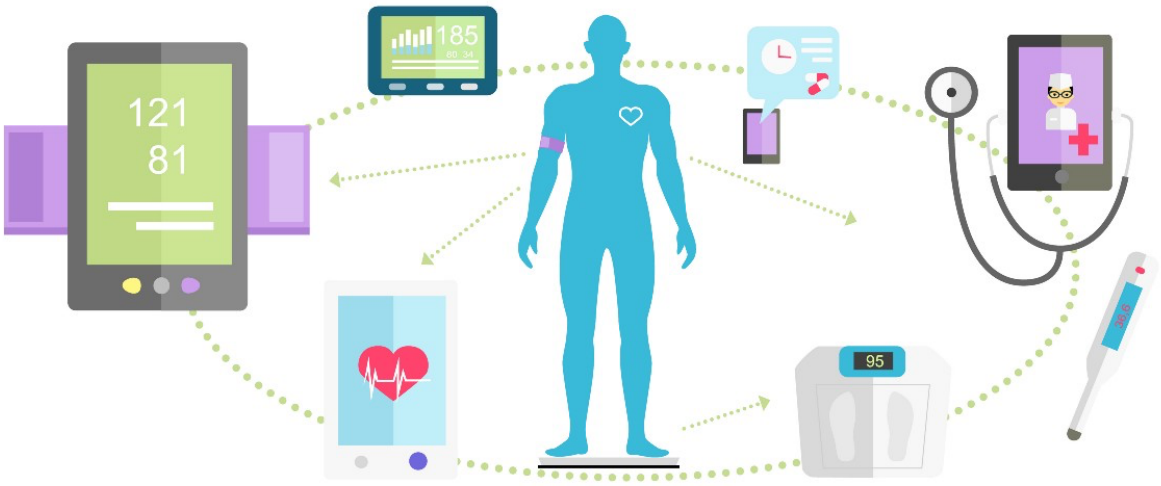

Рисунок 2. Схема взаимодействия умных устройств

Хотя внедрение IoT требует определённых вложений, в долгосрочной перспективе это позволяет значительно сократить затраты. Превентивная диагностика и своевременное вмешательство уменьшают расходы на лечение осложнений. Удалённое наблюдение снижает количество госпитализаций и визитов к врачу, а автоматизация процессов сокращает потребность в ручной работе персонала.

Более того, IoT позволяет повысить эффективность распределения ресурсов. Например, умные системы мониторинга запасов медикаментов и расходных материалов предотвращают их дефицит и снижают избыточные закупки.

Несмотря на очевидные преимущества и широкий спектр применения технологий Интернета вещей в здравоохранении, их использование сопряжено с целым рядом серьезных угроз информационной безопасности. Учитывая, что медицинские IoT-устройства обрабатывают чувствительные персональные данные, любые сбои или уязвимости в системе могут привести к утечкам информации, вмешательству в работу оборудования и даже рискам для жизни пациента.

Одной из ключевых проблем является недостаточный уровень защищённости самих устройств. Многие медицинские IoT-системы проектируются с упором на функциональность, тогда как вопросы безопасности остаются на второстепенном уровне. Это делает их уязвимыми к внешнему вмешательству. Часто устройства используют устаревшие протоколы передачи данных, слабую аутентификацию и отсутствующие или плохо реализованные механизмы обновления программного обеспечения.

Также стоит отметить недостаточную защиту каналов передачи данных. В большинстве случаев устройства IoT обмениваются информацией с облачными хранилищами или локальными серверами по беспроводным сетям (Wi-Fi, Bluetooth, LTE и др.). Если передача данных не шифруется должным образом, злоумышленники могут перехватить информацию и получить доступ к медицинским показателям, истории болезней, или даже личной информации пациента — ФИО, адресам, паспортным данным.

Особую опасность представляет возможность удаленного вмешательства в работу устройств. В ряде случаев хакеры могут получить контроль над функционированием медицинского оборудования. Так, в 2017 году исследователи из США продемонстрировали возможность взлома кардиостимулятора и отправки вредоносной команды, способной повлиять на сердечный ритм пациента. В подобной ситуации ошибка может привести к летальному исходу. Аналогичные угрозы касаются и других критически важных систем — инсулиновых помп, аппаратов ИВЛ, нейростимуляторов.

Еще одна уязвимость — централизованные системы хранения данных, которые становятся объектом интереса для киберпреступников. В случае взлома сервера, на котором хранятся медицинские данные тысяч пациентов, утечка информации может носить массовый характер. Так, в 2018 году в одной из клиник США произошла компрометация IoT-системы, в результате чего были украдены конфиденциальные данные более 100 000 пациентов.

Также следует учитывать риски, связанные с человеческим фактором. Низкая цифровая грамотность медицинского персонала, слабые пароли, отсутствие политики обновления устройств и программного обеспечения — всё это создает уязвимости, которые могут быть использованы злоумышленниками.

Таким образом, с расширением использования IoT в медицинской практике значительно возрастает поверхность атаки и потенциальный ущерб от киберинцидентов. Это требует выработки целостной стратегии обеспечения кибербезопасности в здравоохранении.

Современные методы защиты IoT в медицине

Для эффективного противодействия угрозам, связанным с использованием IoT в здравоохранении, необходимо внедрение многоуровневых систем информационной безопасности. Эти меры должны охватывать как технические, так и организационные аспекты, начиная от уровня отдельных устройств и заканчивая политиками всего медицинского учреждения.

Один из наиболее базовых и одновременно критически важных методов — это применение надежных алгоритмов шифрования для защиты данных при их передаче и хранении. Рекомендуется использовать современные стандарты, такие как AES-256 для хранения данных и TLS 1.3 для защищенного соединения. Это позволяет минимизировать риски перехвата и подмены информации.

Обязательным элементом является двухфакторная или многофакторная аутентификация как для пользователей, так и для устройств. Это предотвращает несанкционированный доступ к данным и оборудованию. Применение ролевой модели доступа (RBAC) ограничивает действия пользователей в зависимости от

их должностных полномочий. Например, медсестра может просматривать показатели пациента, но не вносить изменения в протокол лечения.

Многие инциденты в области кибербезопасности связаны с использованием устаревшего ПО или незакрытых уязвимостей. Поэтому жизненно важно обеспечить возможность регулярного обновления прошивок и программного обеспечения устройств, а также автоматическое уведомление о наличии обновлений. Следует также внедрять процессы управления уязвимостями (vulnerability management) и регулярно проводить тестирование на проникновение.

Для минимизации последствий возможного взлома применяется сегментация сетевой инфраструктуры, при которой IoT-устройства изолируются от основной корпоративной сети. Это позволяет локализовать потенциальные атаки. Дополнительно используются системы обнаружения вторжений (IDS/IPS) и мониторинга сетевого трафика, что помогает своевременно выявить аномальную активность.

Эффективная защита невозможна без системы аудита и ведения журналов событий, позволяющих отслеживать действия пользователей, изменения в настройках, попытки доступа и другие ключевые события. Эти журналы должны храниться в защищенном виде и периодически анализироваться специалистами по безопасности.

Разработка и внедрение отраслевых стандартов безопасности является важным направлением. Международные и национальные регламенты, такие как ISO/IEC 27001, ISO/IEC 80001, HIPAA, GDPR, а также российский 152-ФЗ о персональных данных, определяют требования к защите информации и должны соблюдаться всеми участниками медицинского процесса.

Также растёт актуальность обязательной сертификации медицинских IoT-устройств, включающей тестирование на безопасность, проверку механизмов шифрования, устойчивости к DDoS-атакам и другим угрозам.

Одной из основных проблем является отсутствие единых международных стандартов, регламентирующих разработку, внедрение и эксплуатацию

медицинских IoT-устройств. В то время как некоторые аспекты охвачены стандартами по информационной безопасности и защите персональных данных (например, ISO/IEC 27001, ISO/IEC 27701, HIPAA в США, GDPR в ЕС), они не учитывают специфики именно IoT-устройств: постоянную передачу данных, беспроводное взаимодействие, ограниченные вычислительные ресурсы и низкий уровень автономной защиты на устройствах.

В большинстве случаев производители самостоятельно определяют архитектуру безопасности, шифрования и политику обновлений, что приводит к значительной неоднородности решений. Это, в свою очередь, затрудняет интеграцию устройств в единую медицинскую инфраструктуру, снижает уровень совместимости и увеличивает вероятность уязвимостей.

Правовое регулирование в сфере персональных медицинских данных

Одним из наиболее чувствительных вопросов является обращение с персональными медицинскими данными. В большинстве стран такие данные отнесены к категории конфиденциальных и подлежат особой защите. В Российской Федерации это регулируется федеральным законом № 152-ФЗ «О персональных данных», а также законом № 323-ФЗ «Об основах охраны здоровья граждан». Согласно этим нормативам, обработка медицинских данных возможна только с письменного согласия пациента, и должна сопровождаться мерами по защите конфиденциальности и целостности информации.

Однако практика показывает, что многие IoT-устройства не соответствуют требованиям законодательства, особенно если речь идет об устройствах иностранного производства, работающих через зарубежные облачные сервисы. Это порождает юридические коллизии и риски нарушения закона.

Необходимость сертификации и проверки на соответствие

В условиях растущих рисков и отсутствия должного контроля остро стоит задача введения обязательной сертификации IoT-устройств медицинского назначения. Такая сертификация должна включать:

- проверку механизма шифрования данных;
- устойчивость к кибератакам;

- возможность безопасного обновления ПО;
- систему журналирования и мониторинга событий;
- соответствие требованиям по сбору и хранению персональных данных.

На международном уровне данная задача решается, в частности, через стандарты ISO/IEC 80001 (управление рисками ИТ-сетей, включающих медицинские устройства), а также документы Международной электротехнической комиссии (IEC), такие как IEC 60601 (безопасность электрооборудования медицинского назначения).

В России важную роль играет Минздрав РФ, который должен выступать инициатором внедрения обязательных технических регламентов и процедур аккредитации IoT-устройств, применяемых в здравоохранении.

СПИСОК ЛИТЕРАТУРЫ:

1. Essential Guide to IoT Monitoring - Benefits and Best Practices. — Текст : электронный // SigNoz : [сайт]. — URL: https://signoz.io/guides/iot-monitoring/ (дата обращения: 29.03.2025).
2. The Growth of Internet of Things (IoT) In The Management of Healthcare Issues and Healthcare Policy Development. — Текст : электронный // ResearchGate : [сайт]. — URL: https://www.researchgate.net/publication/355685356_The_Growth_of_Internet_of_Things_IoT_In_The_Management_of_Healthcare_Issues_and_Healthcare_Policy_Development (дата обращения: 29.03.2025).
3. The Dangers of Medical IoT Devices: Risks and Challenges. — Текст : электронный // ResearchGate : [сайт]. — URL: https://www.researchgate.net/publication/370403682_The_Dangers_of_Medical_IoT_Devices_Risks_and_Challenges (дата обращения: 29.03.2025).
4. Аксенова, Е. И. Интернет медицинских вещей (IoMT): новые возможности для здравоохранения / Е. И. Аксенова. — Текст : электронный // niioz : [сайт]. — URL:

https://niioz.ru/upload/iblock/8e2/8e2ecff098ac4476c2142d8b7e450be7.pdf (дата обращения: 29.03.2025).