

## **ИССЛЕДОВАНИЕ ПОТЕНЦИАЛА РАЗВИТИЯ ИНДУСТРИИ ИКТ В СОВРЕМЕННОМ МИРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ**

**Алламурат Абылай Қошқарбайұлы, Жандосова Дина Жандосқызы**

**Abylai9802@mail.ru**

**Магистранты ФТФ кафедры РЭТ ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан**

**Научный руководитель –Жакатаев Т.А.**

В ходе проведения комплекса исследований, были определены основные перспективы развития процессов автоматизации в сфере информационно-коммуникационных технологий (ИКТ) на отечественном рынке. Процессы автоматизации на сегодняшний день вклиниваются во все сферы деятельности человека, начиная от простой оцифровки документов и заканчивая полной роботизацией жизненных процессов [1].

С развитием инновационных технологий все большее предпочтение уделяется роботизации, автоматизации и тем процессам, которые могут улучшить или же упростить обыденную жизнь человека. По результатам многочисленных исследований одним из глобальных технологических переворотов в сфере ИКТ является внедрение IoT.

Глобальная арена ИВ является массивной и растет в геометрической прогрессии. Те, кто находится в развивающемся цифровом мире, недавно стали свидетелями распространения и воздействия устройств с поддержкой IoT. IoT предоставил новые возможности на технологической арене, одновременно поставив ряд проблем на более высокий уровень [2].

Проведенное исследование имеет как практический, так и теоретический импульс, поскольку IoT все еще находится в зачаточном состоянии, и все же многие инженеры считают его самой важной технологической инициативой сегодня. Исследование включает систематический обзор и синтез литературы, связанной с IoT, а также разработку теоретической основы и концептуальной модели, изученные и собранные данные, имеют достаточно большую актуальность в сфере ИКТ.

Обзор литературы показывает, что количество приложений, которые используют IoT, резко возросло и охватывает области от бизнеса и производства до дома, здравоохранения и так далее. Хотя IoT может создавать бесценные данные в каждой отрасли, это не происходит без проблем, одной из масштабных проблем можно назвать стандартизацию так называемых вещей «устройств». Разработанная теоретическая база в определяет приоритетные области и проблемы IoT, обеспечивая руководством ведущих инициатив IoT и раскрывая возможности для будущих исследований IoT.

На данный момент именно процессы стандартизации тормозят темпы развития IoT, в связи с этим множество мировых компаний занимаются разработкой и формированием комплекса решений для продвижения единых функций управления ИВ [3].

На рынок Казахстана понятие ИВ было заведено не так давно, что позволяет нам, одними из первых на постсоветском пространстве сформировать стандарт управления и продвижения ИВ, в связи с отсутствием единого стандарта управления IoT. Потенциальные выгоды IoT для экономического роста и социального обеспечения кажутся неоспоримыми, IoT сталкивается с рядом технологических, социальных, правовых и нормативных проблем

стандартизации, начиная от совместимости и доступности спектра до кибер безопасности и конфиденциальности [2].

Эти проблемы могут и должны решаться совместными усилиями широкого круга заинтересованных сторон из государственного и частного секторов. Продвижение IoT частично зависит от того, как специалисты реагируют на связанные с ним возможности и проблемы.

Сегодня имеющиеся телекоммуникационные компании на рынке занимаются активным продвижением идеологии ИВ, тем самым суля незаурядное будущее рынку ИКТ. Результаты проведенного исследования показали, что темп развития ИВ затрудняет именно отсутствие единого стандарта управления и внедрения [4].

Именно по этой причине стандартизация ИВ является на данный момент первостепенным блоком в продвижении ИВ, так как большинство услуг предлагаемых благодаря этой технологии не обременены как для телекоммуникационных компаний, так и для самих пользователей, к примеру, это может быть беспилотное управление ТС или дистанционный мониторинг показаний. На самом деле таких процессов автоматизации большое множество, поэтому стандартизация вещей «устройств» и процессов это новый этап в развитии ИВ, как на отечественном рынке, так и мировом.

Проведя исследование, было определено, что большинство экспертов в области IoT прогнозируют, что к 2025 году в мире будет предположительно 100 млрд. устройств, которые смогут взаимодействовать друг с другом. Но также на пути развития IoT стоят проблемы, которые, безусловно, могут затормозить процесс развития этой технологии [2].

Если рассматривать идеальную картину, когда на пути развития IoT нет затруднений, то все технологические процессы улучшат и упростят жизнь человека, в качестве примера, где может быть использована технология IoT, рассмотрим несколько вариантов. К примеру, использование технологии IoT в здравоохранении позволит повысить качество жизни человека в несколько раз. Для контроля, за состоянием здоровья пациентов находящихся в зоне риска, будут устанавливаться специальные устройства, которые позволят дистанционно контролировать, давление, уровень сахара в крови и так далее, а также сигнализировать о надвигающейся угрозе. Это позволит специалистам в нужный момент связаться с пациентом и прописать ему курс лечения или проинформировать, как избавиться от надвигающейся проблемы.

Такой же процесс можно рассмотреть, к примеру, в логистике, сегодня мы часто начинаем сталкиваться с такой ситуацией, заказав какой либо товар из-за рубежа нам предоставляется возможность контролировать его перемещение от склада к покупателю. Но как показала практика, не всегда эта система работает так, мы можем только в виде сообщения понимать пришла посылка или нет. Благодаря внедрению ИВ появится возможность в режиме реального времени вести постоянный контроль передвижения заказа, кроме того у компаний также появится возможность функционально распределять процессы чтобы на конечной точке выдачи заказа время ожидания было самым минимальным.

Описанный процесс мы сможем наблюдать абсолютно во всех сферах деятельности человека, и, безусловно, можно прогнозировать, что это улучшит множество быденных операций.

Интернет вещей это не просто устройства, которые будут общаться между собой по воздуху, для разработки и функционирования определенных направлений потребуется организация своей сети взаимодействия, к примеру, если потребуется организовать умный дом, то это, безусловно, организация сети в доме. То есть формируется своеобразная сеть, которая позволит устройствам общаться между собой в одном помещении и выводить данные в виде определенного стандарта для пользователя [5].

Если рассматривается более масштабная организация как умный город, то это заведомо говорит о масштабах сети, так как в городской среде может быть задействовано до

миллиарда устройств, которые будут общаться и передавать данные, это весьма трудоемкий процесс, который требует стандартизации всех этапов при организации.

Интернет позволяет человеку поддерживать связь, с физическим миром используя персональные гаджеты, устройства для умного дома и сети автоматизации. Следует отметить, все новые технологические процессы в своей основе кроют не только огромные возможности, но и колоссальные риски.

Интернет вещей позволяет ощутить и контролировать объекты, создавая тем самым возможности для более прямого взаимодействия между физическим миром и компьютерными системами.

Развертывание существующих решений безопасности, в IoT не так просто из-за неоднородности устройств, высоко динамичности больших масштабов развертывания.

Технология Интернета вещей обеспечивает доступ к реальному миру физических объектов через Интернет [3].

Мы наблюдаем смену парадигмы, в рамках которой повседневные объекты становятся взаимозависимыми и умными [5].

Однако человеческое понимание и опыт в области использования взаимосвязанных интеллектуальных вещей и интеллектуальных систем не развиваются одинаковыми темпами, что порождает проблемы с огромными технологическими трудностями, а также проблемами безопасности, конфиденциальности и доверия.

В перспективе акцент будет сделан на реализации искусственного интеллекта во всех сферах Интернета вещей, включая организацию дорожного движения, энергоснабжение, мониторинг, производство промышленной продукции, строительную отрасль, сельское хозяйство, охрану окружающей среды и так далее, для формирования интеллектуального сетевого общества, в котором должны быть задействованы ресурсы.

Все эти инновационные разработки IoT создают новые вызовы для обеспечения безопасности и открытые исследовательские области, требующие решения. Безопасность Интернета вещей должна обеспечиваться на основе характеристик среды Интернета вещей, в которой она применяется.

В типовой архитектуре Интернета вещей есть три базовых уровня: уровень зондирования/восприятия, уровень транспорта/сети и прикладной уровень. Каждый из этих уровней имеет свои специфические проблемы безопасности [1]. Уровень восприятия/чувствительности контролирует физические устройства IoT, которые имеют разные значения параметров в соответствующей среде. Если хакеры получают доступ к этим приборам, они смогут извлекать из них секретную информацию [5].

Исследования свидетельствуют о том, что эти технологии также уязвимы. По результатам был оценен алгоритм сквозной безопасности для IoT с использованием технологии IPSec, которая повышает безопасность для 6LoWPAN [1].

Мы проанализировали сорок аналитических документов по безопасности Интернета вещей, основанных на семи параметрах: безопасность, конфиденциальность, доверие и учет распределенного интеллекта, используемого в приложении, использование программно-определяемой сети, сети виртуализации функций (NFV), технологии блокчейн и машинного обучения.

Из результатов стало очевидно, что ни в одном из этих документов не были обсуждены принципы использования концепций машинного обучения для повышения безопасности Интернета вещей.

Из полученных результатов мы также можем сделать вывод, что некоторые исследователи не обсуждали доверие к инфраструктуре Интернета вещей и доверие между различными организациями, представленными в разных странах, кроме того большинство специалистов утверждают, что именно стандартизация приведет к обеспечению безопасности ИВ.

Любое решение по обеспечению безопасности должно учитывать три основных свойства: конфиденциальность, целостность.

Конфиденциальность данных означает, что доступ к ним неуполномоченных лиц ограничен. Целостность гарантирует оригинальность данных. Это означает, что данные не могут быть изменены посторонними лицами. IoT движется вперед каждый день с его быстрым внедрением во всех секторах, включая «умный город», «умное сельское хозяйство», интеллектуальное управление дорожным движением, самоуправляемые автомобили, интеллектуальную логистику.

Любое типичное приложение IoT может быть заменено на вышеуказанную многоуровневую модель. Но IoT движется вперед, технология нацелена на то, чтобы принимать решения в режиме реального времени, например, автомобиль должен немедленно решить проявившуюся проблему, кроме того автомобиль сам должен контролировать дистанцию при передвижении ТС.

В лабораторных условиях был протестирован подход на основе нейро сетевой безопасности [2], собраны и проанализированы данные сети.

Интернет вещей – это многопрофильная область, где технологии встречаются с людьми, чтобы обогатить качество жизни за счет улучшения условий труда и повышения производительности.

Для защиты узлов Интернета вещей от несанкционированного доступа необходима надежная инфраструктура Интернета вещей. Массивный объем конфиденциальных данных должен быть получен из будущих систем Интернета вещей [1].

Для обеспечения безопасности, конфиденциальности и доверия к будущим сетям IoT и данным IoT будет увеличиваться использование алгоритмов машинного обучения, распределенного интеллекта, виртуализации сетевых функций, программно-определенных сетей, технологий блокчейн и беспроводной сети 5G. Использование всех этих новых технологий создает открытые проблемы безопасности и стандартизации устройств. Стоит отметить, что игнорирование описанных проблем может полностью застопорить развитие технологии ИВ.

#### **Список использованных источников**

- 1 Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации, книжное издание. – Москва: Связь. 2005. – С. 45-53.
- 2 Дрожжинов В.И. Умный город, и принципы его создания. Экономическая политика. – Москва: Техносфера. 2013. – С. 78-91.
- 3 Егоров П.М. Метрология, стандартизация и сертификация в инфокоммуникациях. – Москва: Академия. 2018 – С. 256-283.
- 4 Лихтенштейн В.Е. Стандартизация и разработка программных систем. – Москва: Связь. 2010. – С. 23-27.
- 5 СТ РК 2192-2012 «Информационные технологии. Интернет-ресурс, интернет-портал, интернет-портал. Общие описания».