УДК 330.34

КЛЮЧЕВЫЕ ФАКТОРЫ РАЗВИТИЯ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ В РОССИИ В 2020-2025 ГОДУ

Филиппов С.А.

кандидат технических наук, доцент,

Национальный исследовательский ядерный институт «МИФИ»

Москва, Россия

Титов А.Д.

магистр,

Национальный исследовательский ядерный институт «МИФИ»,

Москва, Россия

Аннотация:

Промышленный интернет вещей — система объединенных компьютерных сетей и подключенных промышленных (производственных) объектов со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме. Рынок IIoT в России пока находится в начальной стадии. Однако последние несколько лет явно заметна тенденция на успешное внедрение отечественных информационных систем интернета вещей на российских предприятиях. В ходе исследования были выявлены основные экономические и технические тенденции в развитии промышленного интернета вещей в России в ближайшие годы.

Ключевые слова: промышленный интернет вещей, кибериммунитет, сети пятого поколения, цифровая экономика, импортозамещение.

KEY FACTORS FOR THE DEVELOPMENT OF INDUSTRIAL INTERNET OF THINGS IN RUSSIA IN 2020-2025

Filippov S.A.
Candidate of Sciences in Technology, docent,
National Research Nuclear Institute MEPhI
Moscow, Russia

Titov A.D.
master
National Research Nuclear Institute MEPHI,
Moscow, Russia

Annotation:
The Industrial Internet of Things is a system of integrated computer networks and connected industrial (production) facilities with built-in sensors and software for collecting and exchanging data, with the possibility of remote monitoring and control in an automated mode. The IIoT market in Russia is still in its infancy. However, the last few years have clearly seen a trend towards the successful implementation of domestic information systems of the Internet of things in Russian enterprises. The study identified the main economic and technical trends in the development of the industrial Internet of things in Russia in the coming years.

Keywords: industrial internet of things, cyber immunity, fifth generation networks, digital economy, import substitution.

2019 год показал успешность разработки и внедрения отечественных IIoT систем. В 2019 году лауреатами премии IoT Awards в сфере промышленного Интернета вещей стали такие компании как Tibbo Systems, ANT, «УРУС», «Тингеникс». Данные компании занимаются как реализаций

решений для конкретных предприятий, так и полноценных IoT платформ (например, платформа AggreGate компании Tibbo Systems, которая включает в себя специализированную IDE и надстройки над языками программирования C и BASIC для разработки в рамках платформы для использования оборудования компании Tibbo Technologies). На данный момент фаворитом на российском рынке IoT решений является «ЭР-Телеком Холдинг». По итогам 2019 финансового года «ЭР-Телеком» выручка компании увеличилась на 13% и составила 44 873 млн. руб [8]. Показатель OIBDA вырос на 33% и составил 17 078 млн. руб. Рентабельность OIBDA - 38%. Основной драйвер роста бизнеса – сегмент B2B. Сегодня компания активно участвует в государственной программе устранения цифрового неравенства - подключает к интернету социально значимые объекты страны, в полном объеме выполняя взятые на себя обязательства. В рамках IIoT компания реализовала собственную LoRaWan сеть федерального уровня, а также имеет успешный опыт внедрения IoT решения для нефтегазовой отрасли для скважин компании «Волгодеминойл». Можно утверждать о стабильном росте и развитии компаний в технологическом и экономическом смысле.

Наравне с «ЭР-Телеком Холдинг» построением сетей федерального уровня заинтересовались и иностранные поставщики решений. Так одним из наиболее значимых событий для российского Интернета вещей является анонсированный в мае 2020 года компанией Sigfox запуск IIoT сети 0G (Zero G) на территории РФ [2]. По предварительным прогнозам, до конца лета 2020 года будут установлены и запущены более 500 станций в Москве, Санкт-Петербурге, Саранске, Казани, Екатеринбурге и Самаре. Можно утверждать, что передовые иностранные компании заинтересованы в новом рынке. С включением в международную IIoT сеть российские компании смогут масштабировать бизнес и усилить экспортный потенциал во всех странах присутствия сети, которых уже насчитывается 70. По мнению экспертов, открытый стандарт технологии 0G Sigfox обеспечит локализацию и

импортозамещение оборудования и решений Интернета вещей в России. Развертывание сети также положительно скажется на отечественном рынке производства умных устройств, разработки интеллектуальных платформ и цифровых услуг.

Государство так же не остается в стороне, осознавая перспективность и темпы развития направления. Решением президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24 декабря 2018 года был утвержден паспорт национальной программы «Цифровая экономика Российской Федерации». В рамках программы будут решены вопросы правового регулирования цифровых платформ, их учета и контроля, реализации программ поддержки отечественных производителей решений IoT и внедрения различных государственных цифровых платформ. Согласно прописанному плану, в 2020 году «будет создана система отраслевого регулирования использования киберфизических систем, включая «Интернет вещей»» [6]. И действительно, на сайте госзакупок в октябре 2019 года Министерство цифрового развития, связи и массовых коммуникаций российской федерации опубликовало конкурс на создание Единой государственной платформы сбора данных, промышленного интернета вещей и инструментов анализа объективных данных о наблюдаемых объектах в составе платформы исполнения государственных функций (ЕГПСД) в составе платформы исполнения государственных функций [4]. Реализацией платформ, по итогам тендера, будет выступать государственное НИИ «Восход».

Непростая сложившаяся мировая ситуация, связанная с пандемией COVID-19, показала, насколько востребован удаленный доступ к производственным ресурсам. В связи с этим Министерство промышленности и торговли анонсировало Витрину технических решений для организаций – портал для дистрибуции программных комплексов, позволяющих решить проблему удаленной работы для производств с производственными циклами

различной степени сложности [3]. К маю 2020 года платформа получила уже более 200 заявок для рассмотрения и представления потребителям. Таким образом, государство выступает не только регулятором для отрасли, но и представляет площадки для дистрибуции IIoT решений на внутреннем рынке.

Для промышленного интернета вещей двумя наиболее важными составляющими являются скорость и безопасность передачи данных, так как нагрузка на сеть в подобных системах исчисляется сотнями гигабайт в минуту, а любое устройство в рамках киберфизической системы, которое было подвержено воздействию нежелательного или вредоносного программного обеспечения, несет в себе опасность не только по отношению к данным предприятия или сотрудников, но и по отношению к объектам материального мира, в том числе, человеку.

На прошедшем в апреле 2020 года заседании рабочей группы «Индустриальный интернет» Ассоциации IoT Андрей Духвалов, руководитель управления перспективных технологий АО «Лаборатория Касперского», подробно рассмотрел основные тренды кибербезопасности. Сотрудники «Лаборатории» пришли к выводу, что индустрия информационной безопасности не справляется с постоянно растущим потоком угроз. По собственной статистике компании, если в 1998 году в день обнаруживалось порядка 50 угроз в день, то в 2018 году эта величина достигла значения в 380 000 новых угроз в день. Появление новых типов устройств способствует появлению не только новых видов, но и типов потенциальных атак. Специалистами компании была предложена концепция кибериммунитета (CyberImmunity) – замена текущей модели кибербезопасности (CyberSecurity), отвечающая современным реалиям [7]. В основе концепции лежит идея, что любая информационная система должна быть защищена от любого типа негативного воздействия без дополнительных наложенных средств. Стоимость кибератаки на подобную систему должна

быть заведомо больше возможного нанесенного ущерба. Ключевыми принципами кибериммунитета являются:

- Immunity – информационная система включает в себя все необходимые средства для самозащиты;
- Separation kernel – изоляция доменов безопасности;
- Complete mediation – наблюдения и контроль всех взаимодействий в системе;
- Корень доверия – наличие в системе самой надежной точки, от которой идет контроль наследования доверия;
- Контролируемый жизненный цикл – системы должны разрабатываться по методологиям жизненного цикла безопасных систем.

Компания не остановилась лишь на формулировке концепции и реализовала собственную защищенную операционную систему KasperskyOS, которая разработана в соответствии со всеми принципами кибериммунитета. На текущий момент работа по внедрению операционной системы идет в нескольких направлениях, в том числе и в промышленном интернете вещей. Примером готовой реализации является совместная разработка НПО «Адаптивные Промышленные Технологии» и Siemens AG - промышленный шлюз данных IKS 1000 GP под управлением KasperskyOS. Шлюз выполняет прямое подключение промышленного оборудования для быстрой передачи данных в Mind Sphere - IoT платформу компания Siemens. За счет использования разработки «Лаборатории Касперского» подключенное оборудование и передаваемые данные полностью защищены за счёт встроенных механизмов на уровне операционной системы. Новое решение уже применяется в совместном инновационном проекте НПО «Адаптивные промышленные технологии» и группы ЧТПЗ по применению технологий промышленного интернета вещей в области цифровой трансформации работы предприятия [5].

В отношении технологии передачи данных наибольший интерес вызывает применение сетей 5G. Release 16 3GPP привнес важные для промышленного интернета новшества в стандарт 5G сетей такие, как реализация сверхнадежной межмашинная связи с низкими задержками (URLLC), поддержку чувствительного ко времени сетевого обмена данными (TSN) и использование нелицензированных спектров частот (5G NR-U). Многие зарубежные компании видят в 5G безусловную замену проводному соединению. Так в 2019 году компания Qualcomm представило свое видение того, как сети пятого поколения найдут свое применение в промышленном интернете вещей. По их мнению, внедрение 5G в IIoT приведет к глобальному экономическому росту более чем на 5 трлн. долларов к 2035 году [1]. Однако российские эксперты Ассоциации IoT убеждены, что несмотря на всю перспективность направления, на промышленных комплексах в ближайшее время будет применяться обычное проводное соединение, как наиболее безопасное в плане передачи данных и проверенное временем. Сети 5G могут найти ограниченное применение на предприятиях там, где отсутствует прямое воздействие аппаратно-программного комплекса на технологические процессы (например, считывание информации о местоположении и действиях сотрудников).

Таким образом можно выделить несколько основных тенденций развития рынка промышленного интернета вещей в России в ближайшие годы:

1) Рост количества внедрения отечественных разработок на промышленных предприятиях России
2) Выход российских компаний на международный экспорт IIoT решений на базе глобальной сети Sigfox 0G;
3) Вовлеченность государства в отрасли (построению собственных сетей федерального уровня и увеличение объёма госзаказов в рамках IIoT), реализация в срок плана программы «Цифровая экономика РФ»;

К техническим тенденциям развития можно отнести:

1) Интенсивное развитие в сфере безопасности применимо к киберфизическим системам и построение разработки комплексов по модели кибериммунитета;
2) Сети 5G могут найти ограниченное применение на отечественных предприятиях, однако как основной стандарт взаимодействия с аппаратным обеспечением промышленных комплексов в ближайшее время рассматривается проводное соединение и связанные с ним промышленные протоколы.

Библиографический список

1. How will 5G Transform Industrial IoT [Электронный ресурс] // Qualcomm: Wireless Technology & Innovation, URL: https://www.qualcomm.com/media/documents/files/how-5g-will-transform-industrial-iot.pdf (дата обращения: 25.04.2020)
2. Sigfox Россия. Пресс-релиз. [Электронный ресурс] // Sigfox Россия, URL: https://sigfoxrussia.com/pressrelease (дата обращения: 21.05.2020)
3. Витрина технических решений для организации процесса удаленной работы [Электронный ресурс] // Минпромторг России, URL: https://gisp.gov.ru/remote/ (дата обращения: 02.05.2020)
4. Выполнение работ по созданию Единой государственной платформы сбора данных, промышленного интернета вещей и инструментов анализа объективных данных о наблюдаемых объектах в составе платформы исполнения государственных функций [Электронный ресурс] // Единая информационная система в сфере закупок, URL: https://zakupki.gov.ru/epz/order/notice/ok504/view/common-info.html?regNumber=0173100007519000136 (дата обращения: 17.04.2020)

5. Доверенные промышленные данные [Электронный ресурс] // Kaspersky Daily, URL: https://www.kaspersky.ru/blog/aprotech-chelyabinsk/27907/ (дата обращения: 23.04.2020)
6. Национальный проект «Цифровая экономика». [Электронный ресурс] // Правительство России, URL: http://static.government.ru/media/files/3b1AsVA1v3VziZip5VzAY8RTcLEbdCct.pdf (дата обращения: 29.04.2020)
7. Открытое заседание рабочей группы АИВ «Промышленный интернет вещей» [Электронный ресурс] // Некоммерческая организация Ассоциация участников рынка интернета вещей, URL: https://iotas.ru/media/day_theme/996/ (дата обращения: 29.04.2020)
8. Пресс-релиз по итогам 2019 года. [Электронный ресурс] // ЭР-Телеком, URL: https://ertelecom.ru/ru/investors/activity-results (дата обращения: 19.04.2020)

Оригинальность 91%