4. Качество на первом месте. Все чаще наблюдается тенденция отказа от брендов с высокими ценами, но не всегда гарантирующих качество, в пользу товаров с высоким качеством локальных производителей. Как раз таки, такие товары заслуживают внимания и имеют все шансы для успешной реализации именно через маркетплейсы, так как смешиваются со всеми остальными товарами.

5. Наличие уникальной продукции. Все больше покупателей привлекает внимание узкоспециализированных магазинов с уникальными предложениями и профессионалами своего дела.

6. Ориентация на желания потребителя. В ситуации, когда продавец тщательно изучил портреты потенциальных покупателей и точно понимает его характеристики, в таком случае, может легко регулировать наполняемость собственного магазина, подбирая ассортимент, пользующийся спросом.

Учитывая текущую ориентированность продавцов и владельцев интернет-магазинов и маркетплейсов на удобство и быстроту совершения покупок онлайн, можно сказать, что интернет-торговля в России продолжит набирать популярность.

Обезлюдение торговых центров, уменьшение потока людей и, как следствие, очередей в магазинах, и снижение нагрузки на транспортную инфраструктуру – те самые последствия распространения онлайн-коммерции, которые могут привести и к изменению городской среды. Более того, пункты выдачи заказов могут располагаться не только в центре города, но и в шаговой доступности для жителей периферийных территорий, тем самым заполняя «пробелы» размещения торговых помещений в регионах. Поэтому потенциал прироста новых покупателей достаточно большой, но для его реализации необходимы как усилия игроков рынка, так и решение ряда экономических и законодательных проблем. Можно предположить, что поколение next уже не будет смотреть на процесс покупки, как на непременную транспортировку куда-либо в пространстве.

УДК 339.564

А.Г. Дупленко, А.Е. Ширкин
A.G. Duplenko, A.E. Shirkin
Балтийский федеральный университет им. И. Канта
Калининград, Россия
Baltic Federal University. I. Kant
Kaliningrad, Russia
aduplenko@kantiana.ru

ОСНОВНЫЕ ТРЕНДЫ И РИСКИ РАЗВИТИЯ «ИНТЕРНЕТА ВЕЩЕЙ»
THE MAIN TRENDS AND RISKS OF THE DEVELOPMENT OF THE "INTERNET OF THINGS"

Аннотация. В статье рассмотрены основные тенденции развития «Интернета вещей» — рост количества «умных устройств», использование искусственного интеллекта для поступающих от них данных, развитие граничных вычислений и др., а также связанные с этим риски и угрозы.

Annotation. The article discusses the main trends in the development of the "Internet of Things" - the growth in the number of "smart devices", the use of artificial intelligence for data coming from them, the development of edge computing, etc., as well as the associated risks and threats.

Ключевые слова: AI–аналитика, граничные вычисления, интернет вещей, искусственный интеллект, умные вещи, IT.

Keywords: AI analytics, edge computing, internet of things, artificial intelligence, smart things, IT.

«Интернет-вещей» — это концепция сети передачи данных между устройствами, которая предполагает не только коммуникации людей с «умными вещами», но и коммуникации «вещей» между собой. Это новая реальность, которая активно проникает практически во все сферы жизни и оказывает на них влияние, значение которого сейчас сложно себе представить. Скорость развития «Интернета вещей» настолько высока, что осмысление его значения и последствий отстает от развития соответствующих ИТ-технологий, и это несет серьезные риски. Поэтому

задача исследования тенденций и рисков развития «Интернета вещей» представляется не только очень важной, но и чрезвычайно актуальной.

Первый из трендов развития «Интернета вещей» связан с продолжающимся лавинообразным ростом количества «умных устройств». По прогнозу Gartner, их количество в мире к концу 2021 года должно было вырасти до 5,8 млрд [5]. В сочетании с недостаточным уровнем защищенности данных устройств все большую опасность представляет их несанкционированное использование для проведения DDoS-атак, для майнинга криптовалют, превращения в скрытые прокси-серверы и т.д. Одним из способов минимизации угроз такого рода является разработка инструментов, которые упрощают сегментацию локальной сети, позволяя изолировать безопасные области на основе технологии «нулевого доверия» и использовать их только для правомерных действий. В качестве второго тренда можно назвать все более активное использование искусственного интеллекта для анализа данных с устройств «Интернета вещей» (так называемая AI-аналитика).

К настоящему времени количество устройств, подключенных к «Интернету вещей», достигло огромных масштабов — уже в 2021 году их насчитывалось 46 миллиардов, а сейчас еще больше. Соответственно, гигантских масштабов достиг и сбор данных с помощью устройств «Интернета вещей». На наших глазах происходит интеграция «Интернета вещей», формируемых с помощью «умных устройств» больших данных и самообучающегося искусственного интеллекта, занимающегося их обработкой и анализом. Исследования показывают, что искусственный интеллект повышает эффективность обработки данных «Интернета вещей» на 25%, при этом качество прогнозной аналитики, которая используется в процессе принятия решений, улучшается на 42% [5].

Использование искусственного интеллекта для анализа данных с устройств «Интернета вещей» также несет свои риски. К ним можно отнести, в частности, неэффективное выполнение задачи в случае недостаточно четкой ее формулировки. Причем в этом случае выполнение задачи может быть не только неэффективным, но и иметь серьезные негативные последствия.

Третий тренд развития «Интернета вещей» — использование граничных (периферийных) вычислений, под которыми понимаются вычисления, связанные со сбором и анализом данных не в «облачном» центре обработки данных, а максимально близко к месту генерации потоков данных, т.е. к датчикам устройств «Интернета вещей». Граничные вычисления позволяют в десятки раз сократить объем данных, отправляемых от этих устройств в центр обработки данных, что значительно уменьшает потребность в пропускной способности, предотвращает задержку передачи данных и повышает скорость реагирования на события, особенно когда принятие решений должно происходить в режиме реального времени. К основным рискам, связанным с использованием граничных вычислений, можно отнести недостаточную безопасность граничных серверов, которая может привести к сбоям в их работе или физическому отключению; проблемы с обеспечением безопасности граничных сетей, а также граничных устройств [4].

Четвертым трендом развития «Интернета вещей» является опережающее развитие данных технологий в здравоохранении. До пандемии COVID-19 реализация проектов «Интернета вещей» в данной сфере тормозилась из-за жесткого регулирования и общей пассивной позиции отрасли. По оценке некоторых экспертов, воздействие пандемии на использование информационно-телекоммуникационных технологий в больницах можно было сравнить с «цифровым взрывом» [5].

На государственном уровне стимулируется использование цифровых технологий в медицинских учреждениях; разрабатываются цифровые приложения для лечения определенных заболеваний; с помощью технологий мониторинга с искусственным интеллектом оптимизируется транспортировка, хранение и распределение вакцин; активно развивается телемедицина. Использование «Интернета вещей» в медицинских целях сдерживается очень опасными последствиями в случае нарушения работы «умных устройств» злоумышленниками. Еще в 2012 году были общественности были продемонстрированы компьютерные программы, позволяющие в радиусе 100 метров автоматически взламывать систему защиты устройств для постоянной подкожной инфузии инсулина и заставлять их впрыскивать все содержимое в кровь, что приводит к мгновенной гибели человека, а также с расстояния 50 метров заставлять кардиостимуляторы генерировать смертельный электрический разряд напряжением 830 вольт [1, с. 74].

Еще одним трендом является активное развитие промышленного «Интернета вещей», который стал одним из факторов «Четвертой промышленной революции» («Индустрии 4.0»), создание индустриальных киберфизических систем, в том числе «интеллектуальных фабрик». В числе основных направлений развития промышленного «Интернета вещей» можно назвать оптимизацию взаимодействия многодоменных систем, повышение эффективности визуализации и интеграции персонала, а также удешевление инженерных информационных систем до уровня, который бы позволил их использование малыми и средними предприятиями [2, с. 52].

Развитие интеллектуальных производственных систем актуализировало задачи по исследованию проблем их информационной безопасности. На практике это может выражаться в разработке и внедрении так называемых профилей информационной безопасности (Cybersecurity Framework). Особенно высок риск использования «Интернета вещей» в ядерной энергетики, на крупных химических производствах и т.п. По оценке компании Hewlett-Packard, более 70 процентов устройств, входящих в «Интернет вещей», имеют уязвимости. Острота данной проблемы для промышленного «Интернета вещей» во многом объясняется тем, что многие производственные сети не предназначались для подключения к сети Интернет и имели защиту только от физических угроз своей безопасности [3, с. 168].

Помимо проблем межсетевого взаимодействия, могут возникнуть трудности и с основными промышленными устройствами, такими как программируемые логические контроллеры. Они имеют базовые коммуникационные протоколы, которые могут давать сбой в случае получения каких-либо непредусмотренных данных. Можно сделать вывод о том, что «Интернет вещей» будет активно развиваться, меняя жизнь и отдельных людей, и предприятий, и общества в целом. Как и любая сложная технология, при своем использовании он создает множество угроз и рисков, однако это должно рассматриваться не как препятствие для его развития, а как задачи, требующие своего решения.

Список литературы

1. *Актуальные* экономические исследования калининградских вузов: сборник научных трудов / Союз землячеств приморских регионов; Балтийский федеральный университет им. И. Канта, Институт экономики и менеджмента. Казань : Общество с ограниченной ответственностью "Бук", 2017. 266 с.

2. Андреев Ю.С., Третьяков С.Д. Промышленный интернет вещей. СПб: Университет ИТМО, 2019. 54 с.

3. *Кривонос Д.А.* Современные тенденции обеспечения экономической безопасности предприятия / Д.А. Кривонос, Н.Г. Дупленко // Экономическая безопасность: проблемы, перспективы, тенденции развития: Материалы IV Международной научно-практической конференции. Пермь: Пермский государственный национальный исследовательский университет, 2017. С. 164-172.

4. *Рябоконь В.В., Кузькин А.А., Тутов С.Ю., Махов А.С.* Обзор угроз информационной безопасности в концепции граничных вычислений // Вестник Евразийской науки. 2018. № 3. Режим доступа: https://esj.today/PDF/79ITVN318.pdf

5. *Тренды* на 2021 год в сфере IT. Режим доступа: https://superhome.pro/trendy-na-2021-god-v-sfere-iot-i-ne-tolko/.

УДК 659

В.В. Карпова, А.И. Балдынюк
V.V. Karpova, A.I. Baldynyuk
Донецкий национальный университет
Донецк, Россия
Donetsk National University
Donetsk, Russia
vladlena_karpova00@mail.ru

ИНФОРМАЦИОННЫЕ СИСТЕМЫ ТОРГОВОГО ПРЕДПРИЯТИЯ
INFORMATION SYSTEMS OF A TRADING ENTERPRISE

Аннотация. В статье рассматривается роль информационных систем в развитии торговых предприятий. Приводится классификация информационных ресурсов, задействованных в бизнес-процессах торговых предприятий. Проводится характеристика угроз, влияющих на безопасность информации деятельности торгового предприятия. Выделяется политика безопасности как один из