11. Решение Верховного Суда РФ от 18.06.1998 // Бюллетень Верховного Суда Российской Федерации. 1998. № 12. С. 7.

12. Ульихин В. С. Особые законы субъектов Российской Федерации: возможная конституционно-правовая трактовка // Сибирский юридический вестник. 2014. № 2. С. 32–38.

13. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 06.04.2015, с изм. от 02.05.2015) // Российская газета. 2001. № 256.

14. Петренко, Д. С. О принципе верховенства закона: противоречия между законами и подзаконными нормативными актами на примере норм, регулирующих оборот биологически активных добавок // Вестник Международного института экономики и права. 2011. № 2 (3). С. 111–120.

15. Решение Судебной коллегии по гражданским делам Московского городского суда от 5 июня 2002 г. URL: http://www.alppp.ru/law/trud-i-zanjatost-naselenija/trud/90/reshenie-moskovskogo-gorodskogo-suda-ot-05–06–2002–3–2502002.pdf (дата обращения: 23.06.2015).

16. О мерах по социальной поддержке многодетных семей: Указ Президента РФ от 05.05.1992 № 431 (ред. от 25.02.2003) // СПС «КонсультантПлюс».

17. Закон Алтайского края от 29.12.2006 № 148-ЗС «О дополнительных мерах социальной поддержки многодетных семей в Алтайском крае» (ред. от 31.12.2013) // Алтайская правда. 2007. № 8–9.

УДК 34.096
ББК 67.404.33

ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ ДЛЯ ДОСТИЖЕНИЯ ЦЕЛЕЙ УСТОЙЧИВОГО РАЗВИТИЯ

А. А. Горохов
АНО «Лаборатория гуманитарных проектов» (Москва, Россия)

И. М. Щербаков
МГУ имени М. В. Ломоносова (Москва, Россия)

Е. А. Дибров
МГУ имени М. В. Ломоносова (Москва, Россия)

В современном мире одним из важных направлений цифровой трансформации является развитие технологий Интернета вещей (IoT). На сегодняшний день несмотря на то, что технология является инновационной на территории Российской Федерации, в общемировой практике она применяется для интенсификации процессов: от природоохранной деятельности, до промышленных и трудовых процессов. В контексте достижения и реализации на практике Целей устойчивого развития, принятых ООН, технологии Интернета вещей способствуют их осуществлению в таких сферах, как экология и защита окружающей среды, социальная интеграция и ликвидация неравенства. В России применение технологий Интернета вещей происходит двойственно: с одной стороны, существуют правовые коллизии имплементации новых регуляторных норм в текущее законодательство нашей страны. С другой стороны, в области практики проявляется проблема опережения технологии и ее применения законодательных инструментов, которые должны регулировать данную сферу деятельности. Тем не менее применение подобных технических усовершенствований влечет за собой возникновение проблем морально-нравственного содержания, связанных с гарантией основных прав и свобод человека и гражданина, принятых также на уровне ООН и вносящих важные коррективы в базовые социально-гуманитарные сферы жизни.

Ключевые слова: технологии Интернета вещей, Цели устойчивого развития, цифровые технологии, природоохранная деятельность, промышленные технологии IoT

INTERNET OF THINGS TECHNOLOGIES FOR ACHIEVING SUSTAINABLE DEVELOPMENT GOALS

A. A. Gorokhov
ANO "Laboratory of Humanitarian Projects" (Moscow, Russia)
I. M. Shcherbakov
Lomonosov Moscow State University (Moscow, Russia)
E. A. Dibrov
Lomonosov Moscow State University (Moscow, Russia)

In the modern world, one of the important directions of digital transformation is the development of Internet of Things (IoT) technologies. Today, despite the fact that the technology is innovative on the territory of the Russian Federation, it is used in global practice to intensify processes: from environmental protection activities to industrial and labor processes. In the context of achieving and putting into practice the Sustainable Development Goals adopted by the UN, Internet of Things technologies contribute to their implementation in such areas as ecology and environmental protection, social integration and the elimination of inequality. In Russia, the use of Internet of Things technologies is twofold: on the one hand, there are legal conflicts of implementation of new regulatory norms in the current legislation of our country. On the other hand, in the field of practice, the problem of advancing technology and its application of legislative instruments that should regulate this field of activity is manifested. Nevertheless, the application of such technical improvements entails the emergence of moral problems related to the guarantee of fundamental human and civil rights and freedoms, also adopted at the UN level and making important adjustments to the basic socio-humanitarian spheres of life.

Keywords: Internet of Things technologies, Sustainable Development Goals, digital technologies, environmental protection, industrial IoT technologies

Doi: https://doi.org/10.14258/ralj(2022)1.2

Можно по-разному относиться к концепции четвертой промышленной революции [1], но сегодня мы объективно наблюдаем синтез трех миров: физического, информационного (или цифрового) и биологического. Ключевой технологией в этом процессе выступает «Интернет вещей» (Internet of Things, IoT).

В докладе Всемирного экономического форума IoT определяется следующим образом: это измерение и дистанционное управление ранее не связанными «вещами». Технология достигает людей и объектов, до которых ранее не могла добраться [2]. Есть и другие определения, например, Международный союз электросвязи (МСЭ), ведущая международная организация, занимающаяся проблематикой IoT, совместно с корпорацией Cisco в 2016 г. выпустила доклад на тему «Использование Интернета вещей в интересах глобального развития» [3]. Коллектив авторов определяет IoT как «растущее количество устройств — от компьютеров и смартфонов до простых датчиков (например, регистрирующих чипов RFID*) — которые подключены к Интернету и способны взаимодействовать с другими устройствами, нередко без необходимости вмешательства человека» [3].

IoT все больше рассматривается не только как способ цифровой трансформации экономики, но и как технология достижения Целей программы устойчивого развития ООН (ЦУР) [4]. Это признают многие эксперты. Например, в 2017 г. в Женеве была принята Международная декларация «Интернет вещей для устойчивого развития» [5]. Авторы декларации определили десять направлений, в которых IoT может быть эффективно применима. Назовем несколько направлений из данной декларации: во-первых, внедрение новых и инновационных приложений Интернета вещей

* RFID (англ. Radio Frequency IDentification, радиочастотная идентификация) — способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках.

для решения проблем, связанных с голодом, водоснабжением и продовольственной безопасностью; во-вторых, использование IoT для снижения рисков и смягчения последствий изменения климата с учетом разнообразия и сложности географии Земли и уязвимых групп населения, в-третьих, применение и использование Интернета вещей для сохранения биоразнообразия и экологического мониторинга с целью защиты живой природы и ее разнообразия на суше, в воздухе и под водой [5]. Также необходимо отметить, что в 2018 г. эксперты World Economic Forum пришли к выводу, что из 640 проектов, в которых применялся Интернет вещей, 84% отвечают потребностям решения проблем в области ЦУР [2].

Нельзя забывать и о параллельно развивающейся IoT технологии IIoT. IIoT (англ. Industrial Internet of Things, IIoT — промышленный интернет вещей, индустриальный интернет) — это «интернет вещей для корпоративного / отраслевого применения — 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, без участия человека» [6]. Если объяснить более просто, то применение Интернета вещей здесь переводится на следующую степень функционирования в рамках государства: отраслевые системы использования (медицина, транспорт, здравоохранение, финансы, энергетика, добыча полезных ископаемых и т. д.). Принципиально важной характеристикой данной модели является то, что эти отраслевые системы связываются между собой в своеобразную экосистему [6]. Перспективность IIoT отмечается в исследовании аналитической компании Gartner «Magic Quadrant for Industrial IoT» [7]. Коллектив авторов (Eric Goodness, Scot Kim, Ted Friedman, Alfonso Velosa, Emil Berthelsen, Amitesh Shrivastava) проанализировал мировой рынок платформ IIoT. В отчете Gartner отмечается, что число промышленных предприятий с локальными платформами IIoT вырастет на 30% к 2023 году. Лидерами являются такие компании как Software AG [8], PTC [9], Hitachi [10], Accenture [11], Atos [12], GE Digital [13], IBM [14].

Принципы развития IoT

Коллектив исследователей организаций Cisco и МСЭ (Филиппа Биггз, Джон Гэррити, Кони ЛаСель, Анна Поломска) заявляют, что реализация технологий в развивающихся государствах является приемлемой, поскольку «во многих случаях более сложная инфраструктура, характерная для развитых стран, не требуется для развивающихся рынков», в ней нет необходимости — базовый Интернет вещей уже доступен и «обеспечивает цифровую магистраль в качестве основы для дальнейшего развития» [3].

Первым принципом развития IoT является ***приемлемость цены.*** В целом сегодня, в эпоху доминирования «законов» глобального рынка и принципов эффективности и выгоды, фактор экономической умеренности создания/поддержания инфраструктуры ИКТ в сфере Интернета вещей является одним из важнейших. Специалисты МСЭ отмечают: «Затраты на исследования и разработки в области Интернета вещей и далее будут покрываться за счет большого спроса на рынках развитых стран» [3].

Вторым принципом мы должны отметить ***доступность.*** Она выражается в дешевизне и гибкости замены комплектующих для компаний-поставщиков. Прежде всего, данное замечание касается развивающихся государств. Уместно сказать, что базисом для конструирования сетей является связанность и функциональный потенциал интернет-сетей в рамках распространения мобильных сетей, особенно сети пятого поколения (5G). Как отмечают эксперты, сеть 5G «способна передавать данные со скоростью от 1 до 20 гигабит в секунду (в 100 раз быстрее, чем 4G), с низкой задержкой между приемом и передачей сигнала и возможностью подключения к огромному количеству устройств. Это один из важнейших технологических прорывов последнего времени, часть четвертой промышленной революции» [15]. Мы можем назвать неполный перечень технический новаций, которые могут быть внедрены с 5G с позиции IoT: широкий ассортимент использования IoT-устройств на производстве и при формировании своеобразных экосистем «умных домов», резкий скачок роботизации, завязанный на «Интернете вещей», автономный транспорт и т. д. Доступность сетей 5G в мире может быть охарактеризована нами как «ближайшая перспектива». Согласно отче-

ту «Mobile Economy» [16] компании GSMA*, лидерами по внедрению являются Южная Корея, США, Китай, Австралия, Япония, Швейцария, Австрия, Италия и Великобритания. По темпам тестирования/испытания сетей в первых рядах находятся страны Евросоюза, Северной и Южной Америки и Юго-Восточной Азии.

Что касается России, то нам следует сослаться на два аспекта при характеристике распространения 5G-сетей: применимый диапазон радиочастот и важность их покрытия как качественно-количественный показатель реализации нацпрограммы «Цифровая экономика Российской Федерации» [17]. Согласно приказу Министерства цифрового развития РФ, «Высвобождение диапазона радиочастот 694–790 МГц для сетей 5G/IMT-2020 является наиболее предпочтительным вариантом обеспечения сетей 5G/IMT-2020 радиочастотным ресурсом» [18]. Проблема заключается в том, что на данных радиочастотах пока продолжает использоваться цифровое телевизионное вещание (ЦТВ), а использование аналогового телевизионного вещания в полосе 470–790 МГц определено до 19 августа 2019 г. [18]. Следующий диапазон частот (4500–4800 МГц) также теоретически может быть использован для 5G, но, как отмечается в приказе, частота «относится к категории правительственного назначения и не доступна для сетей 5G/IMT-2020» [18]. Последующие радиочастоты (4800–5000 МГц) задействованы преимущественно гражданскими радиорелейными станциями. Мы можем заметить заполненность диапазонов радиочастот различными объектами общественного назначения, что мешает форсированному внедрению 5G/IMT-2020. Следует параллельно сказать, что в рамках нацпрограммы «Цифровая экономика РФ» именно покрытие 5G-сетями крупных городов встроено в качестве показателя для достижения характеристик национальной программы цифровизации страны [17]. Описанные параметры на сегодня очерчивают круг вопросов, которые в ближайшем будущем придется решить российским властям в рамках реализации IoT.

Стоит сказать несколько слов о работе мобильных операторов в направлении Интернета вещей и внедрения 5G. Мы должны отметить несколько моментов. Во-первых, МТС стала первой из всей линейки мобильных операторов, кто в июле 2020 г. получил лицензию на использование 5G/IMT-2020 по России [19]. Правда, следует оговориться, что 5G было доступно для крупных предприятий и бизнес-компаний. Во-вторых, «Мегафон» стал первым оператором по РФ, кто в феврале 2020 г. «предложил своим абонентам международный 5Gроуминг» [20]. Как отмечает вице-президент по развитию бизнеса партнерской с «Мегафоном» организации QUALCOMM Europe Inc. Ю. Клебанова, «5G сеть МегаФона позволит обеспечить практически безграничную емкость сети в самых загруженных местах, таких как бизнес-центры, стадионы, основные улицы, конгресс-холлы, ж/д станции, аэропорты» [20]. В-третьих, следует сказать, что в конкуренции между собой мобильные операторы пытаются реализовывать проекты 5G/IMT-2020 на предельных радиочастотах. Мы уже ранее отмечали, что в диапазоне 1–6 ГГц сети 5G на данный момент могут быть использованы. Как отмечается в заметке, МТС при тестировании использовал «Модуль производства компании Telit, оснащенный модемом Qualcomm® Snapdragon™ X55 5G, испытанный *в диапазоне 4,9 ГГц* (sub-6 ГГц) на оборудовании радиодоступа Huawei» [21]. В-четвертых, многие представители других мобильных операторов и телекоммуникационных компаний отмечают (пресс-секретарь «ВымпелКома» (бренд «Билайн») Анна Айбашева, представитель «Ростелекома» Валерий Костарев), что даже для крупных предприятий сохраняется проблема точечного покрытия сетями 5G регионов на радиочастотах около 2 ГГц. При этом оптимальным, они утверждают, являются ниши на уровне 3,4–3,8 ГГц [19]. В-пятых, интернет-решения мобильных операторов на фоне пандемии в 2020 г. стали реализовываться в некоторых важных, с точки зрения общественного развития, сферах. В частности, «Мегафон» успешно предложил свою программу «Контроль кадров», в рамках которой эффективно осуществлялся контроль за посещением медицинскими и торговыми работниками закрепленных территориальных зон [22]. Это дало широкий объем данных фармацевтическим компаниям по правильному выстраиванию стратегии по продвижению собственных товаров.

---

* Ассоциация GSM (обычно называемая «Ассоциация GSMA») — это торговая организация, которая представляет интересы операторов мобильной связи по всему миру. Около 800 операторов мобильной связи являются полными членами GSMA и более 400 компаний являются ассоциированными членами. Ассоциация GSMA представляет интересы своих членов посредством отраслевых программ, рабочих групп и отраслевых информационно-пропагандистских инициатив. Она также организует конференции компаний мобильной индустрии, Всемирный Конгресс ассоциации GSM, а также ряд других мероприятий.

Третьим принципом технологий следует назвать ***масштабируемость***. Стоит сразу отметить, что данный принцип не является явным на данный момент, но перспективным, при условии реализации сетей 5G на основе модели взаимодействия M2M*. По прогнозам GSMA «в ближайшие годы стоит ждать настоящего бума IoT-устройств. Так, по прогнозам GSMA, в период с 2019 по 2025 год число IoT-устройств увеличится более чем в два раза, а глобальный доход от этого сектора вырастет в три раза — до $1.1 трлн» [15]. Исследователь В. Сикирин предполагает, что «по мере распространения IoT-устройств — от смартфонов и домашней техники до самоуправляемых автомобилей — они будут объединяться в сети. Устройства смогут обмениваться друг с другом данными, в том числе проводить микротранзакции без участия человека» [15]. Конечно, некоторые моменты сейчас, связанные с технологиями IoT, с позиции обыденного сознания (например, самоуправляющиеся автомобили, которые расплачиваются автоматически на бензозаправках) выглядят немного футуристично и предполагают под собой ряд проблем, решение которых позволит улучшить работу данных технологий.

В то же время необходимо заметить, что сегодня помимо внедрения сетей G5 активно ведутся фундаментальные исследования нового поколения связи 6G. Если 5G предполагает скорость от 1 гигабайта в секунду, то 6G будет обеспечивать передачу данных со скоростью 1 терабайт в секунду. Такой уровень связи обеспечит ускоренное развитие IoT во всех областях человеческой деятельности. Поэтому мы считаем, что уровень развития технологий передачи данных — это одно из ключевых условий развития IoT. Что касается сроков разработки и внедрения технологии нового поколения связи, то один из прогнозов изложен компанией Samsung Electronics в своем докладе «6 G. Технология гиперсвязи следующего поколения для всех» [6]. В этом документе утверждается, что завершение разработки стандарта 6G может произойти уже в 2028 г., а массовый коммерческий запуск — около 2030 г. Тем самым мы можем прогнозировать, что к 2030 г. развитие IoT может выйти на совершенно новый уровень. Что касается России, то пока исследование сетей 6G находится на стадии «определения „облика 6G", то есть какой будет сама технология, а также технологических подходов к организации устройств» [23]. Принципиально важным остается вопрос о качественном прогнозировании реализации данных сетей без повтора проблем, касающихся сетей 5G. В сентябре 2020 г. Сколковский институт науки и технологий заявил о разработке сверхвысокочастотного интегрального электрооптического модулятора для 6G [24]. Данное устройство позволяет модулировать оптическое излучение с длиной волны 1.5 мкм электрическим сигналом с частотой до 10 ГГц, которое является подходящим для 6G-систем. Если обратиться к опыту зарубежных стран, например Китая и США, то стоит сказать, что в КНР в ноябре 2019 г. министерство науки и технологий официально объявило о начале работ по созданию сетей 6G [25]. В рамках двух исследовательских групп, в которые входят различные участники, от чиновников профильных министерств до университетов, проводится работа по продвижению и техническому оснащению технологий сетей шестого поколения. В некоторых новостных источниках проходила информация о запуске Китаем в космос первого в мире спутника с целью развития 6G [26]. В свою очередь, в США компания Apple начала искать инженеров для разработки беспроводной сети 6G [27]. Ранее, в 2019 г. Федеральная комиссия по связи США (FCC) начала подготовку к исследованиям и разработкам в области сетей шестого поколения и единогласно проголосовала за открытие нового частотного сегмента для услуг 6G [6]. Все эти факты красноречиво говорят о том, что сети шестого поколения являются не футуристической концепцией, а разрабатываемым перспективным проектом.

При этом России необходимо более активно включиться в разработку стандартов 6G, чтобы избежать проблем, которые возникли с частотами для поколения связи 5G.

Проблемы применения IoT

Сначала нам следует рассмотреть влияние технологии Интернета вещей в контексте реализации ЦУР. В контексте реализации 11-й ЦУР: ***устойчивые города и населенные пункты*** — стоит обратить внимание на такую проблему IoT, как уязвимость от мошеннических кибератак. Обратимся к заметке И. Куксова, сотрудника kaspersky daily. Он замечает, что, например, в рамках «умного дома» возможны бесконтрольное скачивание и загрузка со стороны на облачный сервер резервных

* Machine-to-machine, или M2M-устройства, — технологии, в основу которых положены принципы взаимодействия объединенных устройств при помощи проводных или беспроводных связей. Используются при обмене данными в двух— или одностороннем направлении, предусматривая допустимость отслеживать объединенные в систему элементы.

копий программной начинки контроллера [28]. По результатам проведенного сотрудниками «Лаборатории Касперского» исследования [29] было доказано, что технология «умного дома» компании Fibaro [12] имела техническую неполадку в программной начинке контроллера. Эта начинка отвечает за управление такими приборами, как термостаты, кофеварки, охранная система. Кроме того, в данной резервной копии хранятся и персональные данные владельца в нешифрованном виде: местоположение дома, смартфон владельца, электронный адрес аккаунта хозяина, список подключенных устройств и пароли — словом, все то, что для хакеров представляет «основной товар» для мошенничества. Еще один пример технической слабости продуктов IoT — незащищенность единого хранилища данных для автоматизированной работы устройств «умного дома». Американская группа исследователей (Каушал Кафле, Кевин Моран, Сунил Манандхар, Адвайт Надкарни и Денис Пошиваник) заметили [30], что в рамках платформы Nest [31] производства компании Nest Labs существует дефект в процедуре авторизации пользователя: между приложением и сервером происходит обмен данными через зашифрованный канал и специализированный, подтверждающий SSL-сертификат. В статье приводится следующий алгоритм внедрения злоумышленника в дом [31]:

1. Преступник выслеживает хозяина приглянувшегося дома и ждет, когда тот подключится к публичному Wi-Fi, например в кафе или метро.

2. Приложение Kasa (отвечает за включение/выключение электричества) пытается соединиться с сервером.

3. Войдя в ту же сеть, злоумышленник перехватывает соединение и показывает приложению свой SSL-сертификат.

4. Приложение принимает преступника за сервер и передает ему токен, необходимый для аутентификации.

5. Преступник, в свою очередь, демонстрирует этот токен настоящему серверу, и тот принимает его за приложение.

6. Взломщик сообщает выключателю прямо из кафе, что хозяин вернулся.

7. Параметр, отвечающий за присутствие хозяина, получает значение «дома».

8. Цель достигнута — камера считывает параметр и прекращает запись, после чего преступник или его сообщники могут незамеченными проникнуть в дом.

На основании проанализированных данных нам следует отметить, что проблема киберуязвимости продуктов IoT важна при испытании и использовании их для реализации ЦУР.

Кроме того, еще одной важной проблемой применения Интернета вещей является автономная работа организаций, которые, используя IoT, могут обходить трудовое законодательное регулирование. Как правило, собственники подобных организаций выстраивают удобную модель для встройки их интересов между позициями государства (заказчика общественных услуг) и «сотрудников» (низший уровень реализации этих услуг). В частности, Филипп Говард ссылается на ситуацию с агрегатором такси Uber в Китае. Так, в городе Ханчжоу во время протестов местных таксистов против водителей Uber агрегатор «призвал своих водителей не выезжать на место происшествия и поручил тем, кто уже там, немедленно уехать. Uber заявила, что будет использовать GPS для идентификации водителей, которые отказались покинуть это место, и расторгнет с ними свои контракты. В сообщениях говорилось, что действия Uber были направлены на „поддержание социального порядка”»[32]. Иными словами, функция контроля, заложенная в технологию IoT, не направляется, на примере данной ситуации, на решение как минимум двух ЦУР: «**достойная работа и экономический рост**» и «***уменьшение неравенства*».

Если говорить о нашей стране, то сегодня в Москве, например, начинала реализовываться инициатива мэрии Москвы по внедрению «системы, запрещающей агрегаторам передавать заказы водителям такси, злостно нарушающим ПДД и не соблюдающим нормы режима труда и отдыха. Это одна из мер, направленных на снижение аварийности с участием таксомоторов» [33]. Создание таких профилей, с одной стороны, дает возможность властям и агрегаторам такси отслеживать состояние и здоровье водителей, с другой — может быть использована в качестве платформы для кражи персональных данных покупателей и кибератак извне, поскольку компьютерные системы могут иметь уязвимости в безопасности [34]. Поэтому защита от кибератак и информационная безопасность является очень важным элементом для устойчивого развития.

Важной проблемой является правовое регулирование IoT и стандартизация протоколов. Если говорить о регулировании государством стандартов интернет-протоколов, то некоторые шаги руководством нашей страны уже предпринимаются в этом направлении. Росстандарт совместно с Техническим комитетом 194 «Кибер-физические системы» на базе РВК и экспертами Ассоциации Интернета вещей, участвовавших в рабочей группе АИВ LoRaWAN, утвердил стандарт протокола LoRaWan, который является одним из наиболее востребованных на рынке протоколов Интернета вещей. Стандарт для протокола LoRaWAN (Long Range Wide Area Networks) утвержден в форме предварительного национального стандарта (ПНСТ) Интернета вещей для управления коммунальным хозяйством и транспортной инфраструктурой, в сельском хозяйстве, добывающей и нефтехимической промышленности и других отраслях. В 2019 г. стандарт получил поддержку международных экспертов LoRa Alliance и был одобрен к использованию в качестве региональной модели, адаптированной для российского рынка LoRaWAN RU [35]. Более того, Министерство цифрового развития РФ на законодательном уровне утвердило в 2019 г. дорожную карту по реализации Концепции построения и развития узкополосных беспроводных сетей связи Интернета вещей на территории Российской Федерации [36]. ГК «Ростех» также предлагала свои планы по «распределенному реестру и технологиям беспроводной связи, а также… в разработке дорожных карт по искусственному интеллекту, компонентам робототехники и сенсорики» [37]. Правда, стоит отметить, что в 2020 г. правительственная комиссия по цифровому развитию пересмотрела и частично приняла [38] предложения ГК «Ростех», поскольку ряд положений планов корпорации слабо согласованы с направлениями нацпрограммы «Цифровая экономика», отсутствует обоснование финансово-экономических деталей планов, а также не учтены мнения других государственных ведомств и министерств (ФСБ, Минэкономики, ФНС, Роспатента, Министерства финансов, Минпромторга и т. д.).

Что касается правового регулирования IoT в России, то отметим мнение менеджера по интеллектуальной собственности компании Parallels Л. Кулаковой. Она отмечает, ссылаясь на данные International Data Cooperation (IDC), что «рост объема рынка Интернета вещей будет составлять 16,9% в год, что может потребовать четкого регуляторного вмешательства» [39]. Тем не менее мы должны заметить, что в России система нормативно-правовых актов (НПА) опосредованно касается системы IoT. Следует вспомнить уже упоминавшуюся ранее национальную программу «Цифровая экономика» [17], которая, по сути, является «ядерным» НПА, вокруг которого выстраиваются другие, менее императивные по характеру реализации нормативно-правовые акты. В качестве «ответвленных» НПА следует назвать Приказ Минкомсвязи России № 923 «Об утверждении Концепции создания и развития сетей 5G/IMT-2020 в Российской Федерации» [18], Приказ Минкомсвязи России № 637 «Об утверждении Плана (дорожной карты) реализации Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации» [36]. Следует также обратить особое внимание на процесс масштабного пересмотра нормативно-правовой базы РФ с 1 января 2021 г. [40, 41] в рамках механизма «регуляторной гильотины». Минкомсвязи за несколько лет до этой даты собирало предложения и представления профильных компаний и организаций по поводу изменения НПА. Как отмечает журналистка А. Устинова, «опубликованный Минкомсвязи перечень состоит из 30 нормативных правовых актов, которые были приняты в период с 2005 по 2017 гг. 28 из них — это приказы Минкомсвязи (Мининформсвязи), одно — постановление Правительства РФ, и еще одно — изменение в отдельные положения ПП РФ» [42]. Все равно следует еще раз отметить, что нормативно-правовая база на данном этапе находится на стадии активной разработки и технической встройки в национальное законодательство.

Все эти факты, события и проблемы должны учитываться экспертным сообществом при анализе проблем IoT, которые могут возникать при соприкосновении с национальным коммуникационным пространством различных государств.

Необходимо обратить внимание и на зарубежный опыт правового регулирования IoT. Например, в 2018 г. в штате США Калифорния был принят закон SB-327 о безопасности IoT-устройств — «Information privacy: connected devices»*. Закон вступил в силу 1 января 2020 г. Данный закон устанавливает норму: все производители IoT в Калифорнии должны создавать для каждого устройства уникальную пару логин — пароль. Но и на федеральном уровне в США осуществляется попытка

* Текст закона см.: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

нормативного регулирования IoT. Особенно в части защиты от киберугроз. С этой целью в 2017 г. в Конгресс были внесены следующие законопроекты: Securing IoT Act of 2017** и Internet of Things Cybersecurity Improvement Act of 2017***. В 2019 г. в США происходили слушания в одном из подкомитетов Сената по вопросу кибербезопасности Интернета вещей: рассмотрение самих проблем уязвимости IoT и способы стимулирования создания большей кибербезопасности путем проектирования подключенных устройств и сетей, которые их поддерживают [43]. Особенно стоит отметить, что в слушаниях также обсуждался вопрос о сетевой безопасности 5G для устройств и инструментальных возможностей правительства, бизнеса и общества в целом продвигать кибербезопасность IoT. До этого в Конгресс США был внесен и в апреле 2020 г. принят законопроект о повышении роли федерального правительства в сфере технологий Интернета вещей [44]. Ключевой характеристикой этого закона является то, что правительство США совместно с IT-специалистами и экспертами устанавливает перечень уязвимостей, которые могут возникнуть при использовании IoT. Также, согласно закону, разработчики подобных устройств обязуются предоставлять доступ государственных органов к «прошивке» и сообщать данные о киберпроблемах этих устройств с полным анализом данных о способах противодействия им.

Мировая практика применения IoT

Мы уже отметили выше, что технологии Интернета вещей могут быть использованы для решения глобальных ЦУР ООН. На прошедшем в мае 2016 г. Глобальном симпозиуме для регуляторных органов в Шарм-эль-Шейхе (Египет) по теме «ИМЕТЬ расширенные права и возможности, БЫТЬ охваченным: составляющие „умных" обществ в соединенном мире» генеральный секретарь МСЭ Хоулинь Чжао отметил, что «Все три основы устойчивого развития — экономический рост, социальная интеграция и экологическая устойчивость — нуждаются в ИКТ как в важнейшем катализаторе, и ИКТ будут, безусловно, играть решающую роль в достижении ЦУР» [45, с. 5].

Из всего перечня 17 ЦУР три являются определяющими: ***экологическая устойчивость, экономический рост*** (в рамках ликвидации неравенства) и ***социальная интеграция***. Следует обратиться к накопленному небольшому опыту реализации IoT некоторыми промышленными компаниями.

Если говорить о конкретных примерах, то сегодня в сфере экологии успешно действует, например, «Система мониторинга микроклимата Bosch Micro-Climate Monitoring System (MCMS)» на базе технологий Intel. Данная система в пространстве города позволяет «правительствам, отраслям промышленности и сообществам измерять, просматривать, логически связывать и анализировать данные из нескольких пространственно распределенных устройств, устанавливать пороговые значения для критических измерений и эффективно передавать информацию нескольким заинтересованным сторонам для принятия решений о качестве воздуха в режиме реального времени» [46]. Основной принцип работы данной системы заключается в том, что программное обеспечение и датчики, встроенные в нее, позволяют быстро и точно определять параметры загрязнения воздуха. В перспективе мы можем предположить, что эта система мониторинга (при сохранении изначальных целей) поможет городским властям других государств принимать подходящие меры против загрязнения окружающей среды и впоследствии решать одну из ЦУР на своем уровне.

Еще один пример из области экологии. Совместный консорциум компаний Intel, Accenture и экологического фонда Sulubaaï в апреле 2020 г. объявили о старте проекта «Project: CORaiL» по использованию роботизированных устройств для спасения коралловых рифов на побережье Филиппинских островов. Во-первых, они (участники проекта) построили бетонную подводную платформу «Сулу-риф», разработанную компанией Sulubaaï для обеспечения прочной поддержки нестабильных фрагментов кораллов. «Сулу-риф включает в себя фрагменты живых кораллов, которые будут расти и расширяться, обеспечивая гибридную среду обитания для рыб и морских обитателей. Затем они стратегически разместили интеллектуальные подводные видеокамеры, оснащенные Accenture Applied Intelligence Video Analytics Services Platform (VASP) для обнаружения и фотографирования

** Законопроектом предлагается внести поправки в Закон о связи 1934 года, предусматривающие установление стандартов кибербезопасности для определенного радиочастотного оборудования. Текст законопроекта см.: https://www.congress.gov/bill/115th-congress/house-bill/1324/text

*** Законопроект устанавливает минимальные оперативные стандарты кибербезопасности для подключенных к Интернету устройств, приобретаемых федеральными агентствами. Текст законопроекта см: https://www.congress.gov/bill/115th-congress/senate-bill/1691/text

рыб по мере их прохождения. VASP использует ИИ для подсчета и классификации морских обитателей, а затем данные отправляются информационную панель, где они предоставляют аналитику и количественные тренды исследователям в режиме реального времени, что позволяет им принимать решения на их основе для защиты кораллового рифа» [47].

Следующий пример. В Малайзии технологии IoT применяются местными фермерами для контроля работы оросительных систем на рисовых полях. Малайзия, как «азиатский тигр» в Юго-Восточной Азии, в сфере производства риса на 70% зависит от своих водных ресурсов. Компания Abbaco Control реализует свои проектные инициативы в этой области, в частности, «Проектирование и разработка SCADA-мониторинга для системы очистки воды. Эта водоочистная установка состоит из очистной станции и водораспределительной станции (насосной станции). Этот проект использует Siemens S7–1500 PLC для программирования контроллера и VijeoCitectfor SCADA-системы мониторинга» [48]. Принцип работы мониторинговой модели базируется на системе датчиков и маячков, установленных на шлюзовых отсеках водоемов, которые отслеживают уровень воды в водоеме в режиме реального времени, направление течения стока, кислотность воды, ее температуру. Весь этот массив данных отправляется автоматически в облачные хранилища, где уже сама компьютерная система преобразует их в вид, наиболее удобный для восприятия фермерами на своих ПК или мобильных устройствах. Весь этот проект по своим целевым представлениям также направлен на решение проблемы загрязнения окружающей среды как структурного компонента ЦУР в национальных рамках государства Малайзии.

На Ближнем Востоке также используется IoT и IIoT для экономии водных ресурсов. Например, в Катаре на основе программы Qatar National Vision 2030 program построены очистные сооружения для использования в системах кондиционирования воздуха и орошения земель. Для управления системами используются технологии IoT и IIoT [49], встроенные в платформу NEXUS Integra [50].

Еще несколько примеров практического применения устройств на базе Интернета вещей в области экологии. Во-первых, стоит вспомнить использование разработанного группой исследователей Квинслендского технологического университета робота LarvalBot для восстановления Большого барьерного рифа [51]. Основная функциональная задача внедрения этого устройства чем-то схожа с описанным выше нами примером Project: CORaiL на Филиппинах. Исследователи хотят «заселить поврежденные участки австралийского Большого барьерного рифа устойчивыми к перегреву зародышами коралловых полипов, чтобы помочь в борьбе с последствиями нашествия хищников и изменения климата» [51]. Во-вторых, обратим внимание на проект «Океан вещей» (Ocean of Things) компании Xerox [52]. По данным источника, авторы проекта из Управления перспективных исследовательских проектов Министерства обороны США (DARPA) предполагают запуск в бухтах Южной Калифорнии и на юге Мексиканского залива около 15 000 плавучих буев (на первом этапе проекта), в которые внедрена система датчиков, собирающая данные о «температуре, солености, загрязнении океана и маршрутах судов в течение года» [52]. Все эти приспособления (при истинном целеполагании проекта, а не для военных нужд) в перспективе могут способствовать исследованию экосистемы Мирового океана.

Примеров в мировой практике существует достаточно много, тем не менее все они в основной массе сводятся к попыткам общества/государства проконтролировать выполнение процессов для эффективной работы компаний и организаций в области ЦУР.

Российская практика

В нашей стране также предпринимаются меры для внедрения и использования технологии Интернета вещей. В данной части обзора мы обратимся к аналитическим наработкам исследовательской компании PwC, специализирующейся на распространении и популяризации IoT. Коллектив авторов под руководством Юрия Пуха, руководителя практики по оказанию услуг компаниям в области связи, информационных технологий и СМИ, выпустил тематическое исследование по Интернету вещей в России. В нем отмечается, что в перспективе в РФ будут находиться «в центре внимания — шесть направлений: электроэнергетика, здравоохранение, сельское хозяйство и животноводство, транспортировка и хранение грузов, „умный город", „умный дом"»[53]. Кроме того, в докладе, выпущенном консорциумом организаций под эгидой Агентства промышленного развития Москвы, отмечаются тренды российского рынка IoT: IT-сектор (отвечает за программную составляющую всех физических объектов), услуги связи с применением новейших технических решений сетей 5G, внедрение преди-

кативной (прогностической) диагностики в тяжелой промышленности, smart city, smart house, научные разработки в сфере ИИ, робототехника [6].

Обратимся к применению модели «интеллектуальной сети» [54], принятой на вооружение Министерством энергетики РФ в 2017 г. в области контроля за работой электрических систем генерации энергии холдингом «Россети». Мы не будем вдаваться в сложную инженерную терминологию системы, но лишь обозначим, что реализация подобных «интеллектуальных сетей» позволяет их авторам (в лице холдингов и государственных энергетических корпораций) объединять разрозненные энергетические элементы (потребительские домохозяйства, «умные» трансформаторы, электрические подстанции и т. д.) в единую «экосистему», которой легко управлять. Все эти описанные примеры из жизни укладываются в популяризирующуюся концепцию «Умного города» и ее применения на практике [55].

Еще несколько примеров. Авторы доклада PwC заявляют, что сегодня также в области электроэнергетики российские власти реализуют некоторые проекты. Во-первых, «в генерации элементы „Интернета вещей" также используются — это системы управления активами класса АСУТП (автоматизированные системы управления технологическими процессами)» [53]. Через эти автоматизированные системы регулятор может получать сведения о работе ключевых систем и в перспективе менять свою стратегию поведения. В другом проекте «с целью развития IoT в генерации Минэнерго совместно с РОСНАНО и Ростелекомом формирует национальный проект по „Индустриальному интернету" на основе пилотного проекта развития системы удаленного мониторинга и диагностики парогазовых установок» [53]. На данный момент мы с уверенностью можем сказать, что в 2019 г. «Индустриальный интернет» успешно прошел стадию тестирования на Кировском заводе в Санкт-Петербурге [56]. По мысли операторов проекта, их инициатива «обеспечивает программно-аппаратный сбор данных с измерительных приборов, установленных на тепломагистралях и водопроводных трубах» [56]. Все эти проекты так или иначе направлены на удаленный контроль за работой промышленных систем и организаций и отвечает целям ЦУР в области реализации ***экономического роста*** и в перспективе ***ликвидации проблем с неравенством***.

В области транспорта в России активно реализуются технологии IoT. Прежде всего это выражается в направлении дистанционного мониторинга за работой такси и их эффективной работы на всех этапах: от заказа услуги до прибытия в пункт назначения. С этой целью уже внедрены специализированные агрегаторы, работающие на платформах крупных отечественных и основных зарубежных IT-корпораций и использующие определенные данные о потребителе (местоположение заказчика, данные «личного кабинета» пользователя, генерация таргетированной рекламы на основе потребительских предпочтений). «Вокруг смартфонов в автомобиле — целые экосистемы программных решений (например, Uber, Яндекс Такси, Get Taxi и др.). Данные решения полностью изменили рынок такси в крупных городах. Такие сервисы уже не ограничиваются только сферой такси и проникают в сферу логистики» [56, с. 8]. Мы уже ранее по ходу данного обзора описывали ситуацию, связанную с протестами в городе Хуанчжоу и ролью агрегатора такси Uber в их разрешении. Логистические новации заключаются в том, что руководство агрегатора посредством технической поддержки разработчиков и использующихся устройств может отслеживать состояние водителя и впоследствии ограничивать его в своей деятельности по различным причинам (например, медицинским или трудовым).

Из российских наработок в области транспортной логистики можно выделить также еще некоторые проекты. Например, компания «Северсталь» использует платформу SAP TM для отслеживания перемещения своих грузов и форсированного решения гипотетических проблем, которые могут возникнуть на любом из этапов цепочки поставок. Как отмечается в докладе Международного горно-металлургического саммита SAP, «… использование платформы SAP TM в транспортной логистике „Северсталь", эта система контроля является мультимодальной и, если мы не будем вдаваться в детали проектной документации, позволяет отслеживать передвижение грузов по трем направлениям: ж/д перевозки, автоперевозки, судовые партии» [50]. Для наглядности продемонстрируем характерные черты выполняющихся надзорных операций в сфере автоперевозок. На всей системе транспортной цепочки поставок введены компьютеризированные устройства: «взаимодействие с перевозчиком через Collaboration Portal, автоматизация оценки уровня сервиса перевозчиков, автоматизация (централизованная) обработки счетов, Новый клиентский сервис в интернет магазине SAP Hybris» [57] для отображения статуса транспортировки и отгрузочных документов.

Кроме того, еще одним проектом в сфере реализации национального IoT является внедрение с ноября 2020 г. «Единой государственной платформы сбора данных промышленного интернета вещей» — системы, которая создается в рамках федерального проекта «Цифровое государственное управление». Платформа будет использоваться как облачное решение контрольно-надзорными органами для дистанционного контроля (надзора), анализа потоковых и структурированных данных, прогнозирования рисков [58]. По сути, на практике данная система позволит посредством встроенных датчиков отслеживать сохранность и безопасное использование объектов культурного наследия, а также экологическую ситуацию в российских регионах. Платформа в онлайн-режиме фиксирует концентрацию вредных веществ в атмосфере и передает информацию в государственную информационную систему «Типовое облачное решение по автоматизации контрольно-надзорной деятельности». Это дает государственным органам возможность получать актуальные сведения по состоянию окружающей среды в субъектах РФ без проведения контрольно-выездных мероприятий. «В основу платформы легла технология интернета вещей Mail.ru IoT Platform, которая обеспечивает сбор, обработку и хранение данных» [58]. К 2022 г. Минцифры в рамках развития этой же платформы внедрит не менее 15 решений дистанционного контроля, на что выделяется порядка 588 млн рублей из федерального бюджета [59].

Скажем несколько слов о развитии природоохранной деятельности в России на базе IoT систем. Примерами могут послужить участие IT-компании WaveAcess в уже описанной нами выше разработке платформы «Единая государственная платформа сбора данных промышленного интернета вещей»; Система «Лесной Дозор» от «ДиСиКон»; Система оперативного мониторинга лесоизменений «КЕДР»; «Цифровое лесное хозяйство» — инициатива от Группы компаний «Элемент» (совместная компания «Ростеха» и АФК «Система»); Умные контейнеры для утилизации мусора SmartCity Bin от компании «Бинолоджи» [60, с. 22]. Отдельно скажем о программных решениях в области IoT компании WaveAcess. Применительно к ЦУР в сфере медицины специалисты этой компании «разрабатывают программные решения для повышения эффективности работы медицинских учреждений. Разработанные приложения направлены на повышение качества обслуживания и обеспечение оперативной связи пациентов с их лечащим врачом» [61].

Последний пример в этой части — внедрение системы «Платон». Один из авторов доклада Ю. Пуха отмечает, что «на базе IoT построена система взимания платы за проезд грузовых автомобилей массой 12 тонн и более по автодорогам „Платон”, в которой на конец 2016 г. было зарегистрировано около 700 тыс. автомобилей» [53]. Логистически данная система позволит разгрузить транспортную загруженность столицы РФ и увеличить приток денег для их перенаправления на благоустройство национальной транспортной сферы. При этом нельзя забывать о проблемах, которые вызвал «Платон»: проблемы при замене бортовых устройств и сложности в оформлении маршрутных карт во время пандемии [62].

На основе проанализированных примеров мы можем выделить совпадение основной цели внедрения систем IoT в России — контроль и мониторинг выполнения рутинных технологических процессов в разных общественных сферах. Эти системы вписываются в рамки ЦУР в сфере решения следующих проблем: контроль за развитием окружающей среды, продовольственная безопасность, экономический рост и ликвидация социального неравенства — и позволяют их разрешать на своем уровне.

Выводы

Если переходить к выводам по использованию технологий Интернета вещей для реализации ЦУР и не только, то нужно отметить несколько важных тезисов.

Во-первых, технологические изменения — Индустрия 4.0, процессы которой неизбывно разворачиваются вокруг нас, приносит достаточно много ***«цивилизационных удобств» человеку.*** Благодаря достижениям в данной области он может оперировать большим массивом данных, которые могут быть полезны для исследовательской работы в различных сферах: экономическая аналитика, политический анализ и прогнозирование, энергетика и т. д.

Во-вторых, технологическая сфера позволяет предложить эффективные решения, если обобщать по ЦУР, в ***сфере экологии и защиты окружающей среды***. Рассмотренные выше проекты позволяют нам в этом убедиться. При этом по таким целям устойчивого развития, как ***социальная интеграция***

и ***ликвидация неравенства*** как компонент экономического роста, остается много вопросов относительно морального контроля применяющихся устройств и их киберуязвимости, которые требуют дальнейшего исследования.

В-третьих, повышается важность ***морально-нравственного контроля*** над технологиями. Мы могли заметить на примерах, что процесс реализации Интернета вещей на практике различными компаниями или государственными регуляторами сопряжен с функцией контроля за выполнением какой-либо одной, узкоспециализированной работы. Тем не менее нельзя распространять прямо или опосредованно данные технологические новации для контроля за ***человеком***, его поведением в частной жизни. В противном случае это косвенно может привести к так называемому феномену «чрезвычайного положения» [63] (терминология Дж. Агамбена) как авторитарного режима политического правления на «временной основе». Иными словами, нельзя использовать в неразумных объемах в угоду своим политическим желаниям те средства и методы, которые изначально придумывались для пользы человека и улучшения его жизни.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Шваб К. Четвертая промышленная революция. М.: Эксмо, 2020.

2. Internet of Things: Guidelines for Sustainability. Geneva: World Economic Forum, 2018.

3. Harnessing the Internet of Things for Global Development URL: https://d-russia.ru/wp-content/uploads/2016/01/Harnessing-IoT-Global-Development.pdf (дата обращения: 17.02.2021).

4. Резолюция ГА ООН A/RES/70/1. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года. 25.09.2015. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=R (дата обращения: 26.02.2021).

5. Международная декларация «Интернет вещей для устойчивого развития» URL: https://iotforum.org/wp-content/uploads/2019/10/IoT4SDG-Declaration_Russian.pdf (дата обращения: 14.02.2021).

6. Промышленный интернет вещей // Tadviser. 07.07.2019. URL: https://www.tadviser.ru/index.php/Статья: IIoT_-_Industrial_Internet_of_Things_ (Промышленный_интернет_вещей) #IIoT_.D0. B2_. D0. A0. D0. BE.D1.81. D1.81. D0. B8. D0. B8 (дата обращения: 26.02.2021).

7. Eric Goodness, Scot Kim, Ted Friedman, Alfonso Velosa, Emil Berthelsen, Amitesh Shrivastava Magic Quadrant for Industrial IoT. URL: https://b2bsalescafe.files.wordpress.com/2019/09/gartner-magic-quadrant-for-industrial-iot-platforms-june-2019.pdf (дата обращения: 26.02.2021).

8. Сайт компании Software AG. URL: https://www.softwareag.com/en_corporate.html (дата обращения: 26.02.2021).

9. Сайт компании PTC. URL: https://www.ptc.com/ru/ (дата обращения: 26.02.2021).

10. Сайт компании Hitachi. URL: https://www.hitachi.com/ (дата обращения: 26.02.2021).

11. Сайт компании Accenture. URL: https://www.accenture.com/ru-ru (дата обращения: 26.02.2021).

12. Сайт компании Atos. URL: https://atos.net/ru/russia (дата обращения: 26.02.2021).

13. Сайт компании GE Digital. URL: https://www.ge.com/digital/ (дата обращения: 26.02.2021).

14. Сайт компании IBM. URL: https://www.ibm.com/ru-ru (дата обращения: 26.02.2021).

15. Сикирин В. Как 5G и криптовалюты запустят IoT-революцию // DeCenter. URL: https://decenter.org/ru/5g-i-kriptovalyuty (дата обращения: 17.02.2021).

16. Отчет компании GSMA по профилю «The Mobile Economy». URL: https://www.gsma.com/mobileeconomy/#key_stats (дата обращения: 17.01.2021).

17. Цифровая экономика Российской Федерации: Программа. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 21.02.2021).

18. Об утверждении Концепции создания и развития сетей 5G/IMT-2020 в Российской Федерации: Приказ Минкомсвязи России № 923. URL: https://digital.gov.ru/uploaded/files/kontseptsiya-sozdaniya-i-razvitiya-setej-5g-imt-2020.pdf (дата обращения: 21.02.2021).

19. Калюков Е., Балашова А. МТС первой в России получила лицензию на создание сети 5G. URL: https://www.rbc.ru/technology_and_media/28/07/2020/5f1fefeb9a7947ae493be541 (дата обращения: 21.02.2021).

20. МегаФон достиг гигабитных скоростей в международном 5G-роуминге. 19.02.2021. URL: https://corp.megafon.ru/press/news/federalnye_novosti/20210219–1104.html (дата обращения: 21.02.2021).

21. МТС протестировала IoT-модуль в сети 5G. 30.03.2020. URL: https://moskva.mts.ru/about/media-centr/soobshheniya-kompanii/novosti-mts-v-rossii-i-mire/2020–03–30/mts-protestirovala-iot-modul-v-seti-5g (дата обращения: 21.02.2021).

22. Для чего компании из разных отраслей применяют технологии интернета вещей и как IoT-решения МегаФона помогают бизнесу успешно развиваться // «IoT-Индекс»: аналитика для принятия эффективных решений. URL: https://www.comnews.ru/projects/megafon-iot-index (дата обращения: 21.02.2021).

23. Алпатова И. Частоты без помех // Российская газета. 2020. 23 авг.

24. В Сколтехе разработали сверхвысокочастотный интегральный электрооптический модулятор для 6G. 21.09.2020. URL: https://www.skoltech.ru/2020/09/v-skoltehe-razrabotali-sverhvysokochastotnyj-integralnyj-elektroopticheskij-modulyator-dlya-6g/ (дата обращения: 26.02.2021).

25. Kharpal Arjun China starts development of 6G, having just turned on its 5G mobile network // CNBC. 7.11.2019. URL: https://www.cnbc.com/2019/11/07/china-starts-6g-development-having-just-turned-on-its-5g-mobile-network.html (дата обращения: 26.02.2021).

26. Китай запустил «первый в мире спутник 6G». Конечно, всё не так просто // 1XBT.com. 09.11.2020. URL: https://www.ixbt.com/news/2020/11/09/kitaj-zapustil-pervyj-v-mire-sputnik-6g-konechno-vsjo-ne-tak-prosto-.html (дата обращения: 26.02.2021).

27. Jobs at Apple. URL: https://jobs.apple.com/en-us/search?search=6g&sort=relevance&location=united-states-USA (дата обращения: 26.02.2021).

28. Куксов И. Умный дом, а в нем — взлом // kaspersky daily. 15.07.2019. URL: https://www.kaspersky.ru/blog/vulnerable-smart-home/23116/ (дата обращения: 21.02.2021).

29. Перекалин А. Взлом умного дома нашего босса // kaspersky daily. 01.07.2019. URL: https://www.kaspersky.ru/blog/hacking-things/23017/ (дата обращения: 21.02.2021).

30. Kaushal Kafle, Kevin Moran, Sunil Manandhar, Adwait Nadkarni, Denys Poshyvanyk. A Study of Data Store-based Home Automation // CODASPY 2019, March 2019, Dallas, TX, USA. URL: https://arxiv.org/pdf/1812.01597.pdf (дата обращения: 21.02.2021).

31. Сайт компании Nest Labs. URL: https://nest.com/ (дата обращения: 21.02.2021).

32. Murphy C. Uber Orders Drivers in China to Steer Clear of Taxi Protests // The Wall Street Journal. 13.06.2015. URL: https://www.politico.com/agenda/story/2015/06/philip-howard-on-iot-transformation-000099/ (дата обращения: 17.02.2021).

33. Буранов И. Таксистов сфотографируют в профиль // Коммерсант. 2020. 17 авг.

34. Волобуев А. Путь заказан: в популярных приложениях такси найдены уязвимости // Известия. 2019. 11 апр.

35. Росстандарт утвердил стандарт протокола LoRaWAN // Некоммерческая организация Ассоциация участников рынка Интернета вещей iotas. 03.02.2021. URL: https://iotas.ru/media/day_theme/1209/ (дата обращения: 17.02.2021).

36. Об утверждении Плана (дорожной карты) реализации Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации: Приказ Минкомсвязи России № 637. URL: https://digital.gov.ru/ru/documents/7046/ (дата обращения: 21.02.2021).

37. Разработанные Ростехом дорожные карты лягут в основу развития «сквозных» цифровых технологий: Пресс-релиз ГК «Ростех». 03.10.2019. URL: https://rostec.ru/media/pressrelease/razrabotannye-rostekhom-dorozhnye-karty-lyagut-v-osnovu-razvitiya-skvoznykh-tsifrovykh-tekhnologiy/?sphrase_id=244622 (дата обращения: 21.02.2021).

38. Тишина Ю. Интернет ненужных вещей // Коммерсант. 2020. 10 дек.

39. Кулакова Л. Необходимость регулирования интернета вещей // Хабр. 21.07.2017. URL: https://habr.com/ru/company/parallels/blog/333840/ (дата обращения: 17.02.2021).

40. Механизм «регуляторной гильотины». URL: https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/mehanizm_regulyatornoy_gilotiny/ (дата обращения: 21.02.2021).

41. План мероприятий по реализации механизма «регуляторной гильотины». URL: https://www.economy.gov.ru/material/file/4f4528d323c83ffd075de7ebcc0f0cd9/dorozhnaya_karta.pdf (дата обращения: 21.02.2021).

42. Устинова А. Минкомсвязи выбрало жертв для «регуляторной гильотины» // Comnews. 17.09.2019. URL: https://www.comnews.ru/content/122040/2019–09–17/minkomsvyaz-vybrala-zhertv-dlya-regulyatornoy-gilotiny (дата обращения: 21.02.2021).

43. Strengthening the Cybersecurity of the Internet of Things. Слушания в подкомитете Сената по коммерции, науке и транспорту. 30.04.2019. URL: https://www.commerce.senate.gov/2019/4/strengthening-the-cybersecurity-of-the-internet-of-things (дата обращения: 26.02.2021).

44. IoT Cybersecurity Improvement Act of 2020. — URL: https://www.congress.gov/bill/116th-congress/house-bill/1668/text?q=%257B%2522search%2522%253A%255B%2522internet%2522%255D%257D&r=15&s=1 (дата обращения: 26.02.2021).

45. Отчет Председателя 16-го Глобального симпозиума для регуляторных органов (ГСР-16) «ИМЕТЬ расширенные права и возможности, БЫТЬ охваченным: составляющие «умных» обществ в соединенном мире». 11–14 мая 2016. URL: https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2016/Meeting-Report_Russian.pdf (дата обращения: 17.01.2021)

46. Intel & Bosch: A Breath of Fresh Air. URL: https://www.intel.ru/content/www/ru/ru/internet-of-things/bosch-smart-city.html (дата обращения: 18.02.2021).

47. Using Artificial Intelligence to Save Coral Reefs. URL: https://newsroom.intel.com/news/using-artificial-intelligence-save-coral-reefs/#gs.tu71e8 (дата обращения: 18.02.2021).

48. Abbaco Controls. URL: http://www.abbacocontrols.com.my/new/webpage2.php?mainp=1642592&subpg=28334712&sub_third_pg=34083784 (дата обращения: 18.02.2021).

49. A more water-efficient Qatar. URL: https://www.iot-now.com/2019/01/21/92286-nexus-in-qatar/ (дата обращения: 26.02.2021).

50. Nexus Integra, IoT for the integration of water cycle management. URL: https://smartwatermagazine.com/news/nexus-integra/nexus-integra-iot-integration-water-cycle-management (дата обращения: 26.02.2021).

51. Подводный робот LarvalBot доставляет первую партию коралловых личинок на Большой барьерный риф. 18.12.2018. URL: https://robogeek.ru/podvodnye-i-nadvodnye-roboty/larvalbot-dostavlyaet-pervuyu-partiyu-korallovyh-lichinok-na-bolshoi-barernyi-rif (дата обращения: 21.02.2021).

52. Проект «Океан вещей» позволит больше узнать о состоянии Мирового океана // Натур Продукт. 26.10.2020. URL: https://np-mag.ru/dela/proekty/proekt-okean-veshchej-datchiki-rasskazhut-o-mirovom-okeane-bolshe/ (дата обращения: 21.02.2021).

53. Пуха Ю. Перспективы развития «Интернета вещей» в России // Доклад PwC. URL: https://www.pwc.ru/ru/communications/assets/the-internet-of-things/2019-internet-of-things-russian.pdf (дата обращения: 18.02.2021).

54. Интернет вещей (IoT) в России // PwC. URL: https://www.pwc.ru/ru/publications/IoT.html (дата обращения: 18.02.2021).

55. Формирование социально-политической концепции «умный город»: мировой и российский опыт: материалы научной конференции кафедры российской политики факультета политологии МГУ имени М. В. Ломоносова 26 ноября 2019 г. / под ред. И. А. Василенко. М.: РУСАЙНС, 2019.

56. Tele2, «Ростелеком» и Ericsson разработали IoT-решение для промышленности. URL: https://iot.ru/promyshlennost/tele2-rostelekom-i-ericsson-razrabotali-iot-reshenie-dlya-promyshlennosti (дата обращения: 21.02.2021).

57. Стежко О. Использование платформы SAP TM в транспортной логистике «Северсталь». URL: https://docplayer.ru/58536810-Ispolzovanie-platformy-sap-tm-v-transportnoy-logistike-severstal.html (дата обращения: 18.02.2021).

58. В России запущена госплатформа для дистанционного контроля охраняемых законом объектов. URL: https://www.tadviser.ru/index.php/Проект: ЕГПСД_ (Единая_государственная_платформа_сбора_данных_промышленного_интернета_вещей) (дата обращения: 18.02.2021).

59. Михайлов К. Типовое и облачное. URL: https://www.kommersant.ru/doc/4593824 (дата обращения: 18.02.2021).

60. Горохов А. А. Технология «Интернет вещей» (IoT и IIoT) для защиты окружающей среды и развития экономики: роль университетов и научной дипломатии // Сборник тезисов докладов участников Научно-практического форума о продвижении принципов «зеленой» экономики в целях ускорения научно-технологического прогресса 29–30 октября 2020. М.: Знание-М, 2020.

61. Сайт IT-компании WaveAcess. URL: https://www.waveaccess.ru/ (дата обращения: 18.02.2021).
62. «Мы не знаем, как работать». Пандемия отразилась на системе «Платон» // BFM.RU. 10.06.2020. URL: https://www.bfm.ru/news/445723 (дата обращения: 18.02.2021).
63. Агамбен Дж. Homo sacer. Чрезвычайное положение. М.: Европа, 2011.
64. G. The Next Hyper Connected Experience for All // Codeground. URL: https://cdn.codeground.org/nsr/downloads/researchareas/6G%20Vision.pdf (дата обращения: 26.02.2021).

УДК 342.56
ББК 67.75

ПРАВОВЫЕ ПОЗИЦИИ КОНСТИТУЦИОННОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ ОРГАНОВ МЕСТНОГО САМОУПРАВЛЕНИЯ И ИХ ДОЛЖНОСТНЫХ ЛИЦ

О. Л. Казанцева
Алтайский государственный университет (Барнаул, Россия)

В научной статье анализируются правовые позиции Конституционного Суда Российской Федерации в сфере юридической ответственности органов местного самоуправления и их должностных лиц, отмечаются важная роль Конституционного Суда Российской Федерации как высшего органа конституционной юстиции и его влияние на правовую основу в сфере местного самоуправления, в том числе по вопросам юридической ответственности органов и должностных лиц местного самоуправления. Особое внимание обращается на правовые позиции, в которых Конституционный Суд Российской Федерации анализирует понятия «органы местного самоуправления» и «должностные лица местного самоуправления», определяет формы ответственности главы муниципального образования, депутата, члена выборного органа местного самоуправления, выборного должностного лица местного самоуправления, а также муниципальных служащих.

Ключевые слова: местное самоуправление, органы местного самоуправления, Конституционный Суд Российской Федерации, правовые позиции Конституционного Суда Российской Федерации, юридическая ответственность

LEGAL POSITIONS OF THE CONSTITUTIONAL COURT OF THE RUSSIAN FEDERATION IN THE SPHERE OF LEGAL RESPONSIBILITY OF LOCAL SELF-GOVERNMENT BODIES AND THEIR OFFICIALS

O. L. Kazantseva
Altai State University (Barnaul, Russia)

The scientific article analyzes the legal positions of the Constitutional Court of the Russian Federation in the field of legal responsibility of local governments and their officials, notes the important role of the Constitutional Court of the Russian Federation as the highest body of constitutional justice and its influence on the legal framework in the field of local government, including legal liability of bodies and officials of local self-government. Particular attention is drawn to the legal positions in which the Constitutional Court of the Russian Federation analyzes the concepts of "local self-government bodies' and "local self-government