



Интернет вещей

ЦИФРОВАЯ

ЭКО
НОМИ
КА

D-ECONOMY.RU

Развитие технологий и оценка
возможностей перехода на
отечественные решения

Интернет вещей

Развитие технологий и оценка
возможностей перехода
на отечественные решения

Содержание

3	Глоссарий
7	Введение
9	1 Развитие технологий и рынка IoT
10	Развитие концепции и определение рынка IoT
14	Развитие глобального рынка и влияние IoT на макроэкономические показатели
23	Развитие беспроводных технологий связи для IoT
68	2 Национальные стратегии развития интернета вещей
69	Мировые лидеры
79	Региональные примеры
88	Развитие IoT в России: возможности и барьеры для перехода на отечественные решения
99	Основные международные тренды и особенности российского подхода
104	Выводы: ключевые тренды и рекомендации
112	Редакционная коллегия
113	Приложения
114	Приложение № 1: Примеры и характеристики основных технологий беспроводной связи для IoT
116	Приложение № 2: Справочная информация о государственных и государственно-частных инициативах развития технологической области IoT в России в 2018–2021 гг.
134	Источники

Глоссарий

1. Общие понятия

AIoT – Artificial Intelligence/Internet of Things, концепция, описывающая интегрированные применения технологий искусственного интеллекта и интернета вещей

ARPU – Average Revenue per User, среднемесячная выручка на одного абонента услуг связи

B2B – Business to Business, рыночная ниша «бизнес для бизнеса»

B2C – Business to Customers, рыночная ниша «бизнес для конечного пользователя»

B2G – Business to Government, рыночная ниша «бизнес для государства»

IoT – Internet of Things, интернет вещей

IoMT – Internet of Medical Things, «интернет медицинских вещей» (технологическая и рыночная ниша, описывающая применение интернета вещей в медицине и здравоохранении)

IIoT – Industrial Internet of Things, промышленный или индустриальный интернет вещей (примечание: описывает применение интернета вещей не в конкретном секторе промышленного производства, а в целом в промышленном масштабе)

Ка-диапазон – диапазон частот сантиметровых и миллиметровых длин волн, используемых в основном для спутниковой радиосвязи и радиолокации (от 26,5 до 40 ГГц)

Ku-диапазон – диапазон частот сантиметровых длин волн, используемых в основном в спутниковом телевидении (от 12 до 18 ГГц)

M2M – Machine-to-Machine, межмашинные коммуникации (взаимодействия между подключенными устройствами без участия человека)

R&D – Research&Development, в российской практике рассматривается как аналог научно-исследовательских и опытно-конструкторских работ (НИОКР)

RT-IoT – Real Time Internet of Things, системы интернета вещей реального времени (примечание: в отчете используется в определении Проекта национального стандарта ПНСТ 419-2020; система RT-IoT – система интернета вещей, корректность работы которой зависит не только от логической точности, но и от соответствия временным ограничениям)

АПК – агропромышленный комплекс

АПК – аппаратно-программный комплекс (в контексте ведомственного проекта «Безопасный город» Министерства чрезвычайных ситуаций РФ)

БПЛА – беспилотные летательные аппараты

ВГК/АС ВГК – весогабаритный контроль / автоматизированная система весогабаритного контроля

ВТО – высокотехнологичные области (в контексте государственных программ и соглашений)

ГИС – государственная информационная система

ГПСД – государственная платформа сбора данных

ИБ – информационная безопасность

ИИ – искусственный интеллект

ИКТ – информационно-коммуникационные технологии

ИТС – интеллектуальные транспортные системы

КИИ – критическая информационная инфраструктура

НПА – нормативно-правовые акты

НТИ – Национальная технологическая инициатива

ПНСТ – предварительный национальный стандарт

СЦТ – сквозные цифровые технологии

ТК/ПТК – технический комитет / проектно-технический комитет (типовые рабочие структуры в составе организаций и органов технической стандартизации)

ФОИВ – федеральные органы исполнительной власти

ФСТТ – федеральная сеть транспортной телематики

2. Технологии связи

2G – 2nd generation, технологии второго поколения беспроводной мобильной связи

3G – 3rd generation, технологии третьего поколения беспроводной мобильной связи

4G/LTE – 4th generation/Long-Term Evolution, технологии четвертого поколения беспроводной мобильной связи, включающие стандарты «долговременного развития» LTE

5G – 5th generation, технологии пятого поколения беспроводной мобильной связи, в том числе соответствующие требованиям к Международным мобильным телекоммуникациям-2020 (см. IMT-2020)

5GC – 5G Core, ядро сети связи пятого поколения

CPS – Cyber-Physical Systems, киберфизические системы

DSTIoT – Direct-to-Satellite Internet of Things, сервис прямой спутниковой связи для устройств интернета вещей

eMBB – extended Mobile Broadband, усовершенствованный мобильный широкополосный доступ (одно из требований к сценариям применения сетей связи пятого поколения – IMT-2020)

EPC – Evolved Packet Core, ядро сети связи четвертого поколения (4G/LTE)

FSS – Fixed-Satellite Service, услуги фиксированной спутниковой связи

IMT-2020 – International Mobile Telecommunications-2020, Международные мобильные телекоммуникации-2020 (набор технических требований Международного союза электросвязи к сетям, устройствам и сервисам мобильной связи пятого поколения)

LAN – Local Area Networks, локальные сети

LPWAN – Low Power Wide Area Networks, узкополосные энергоэффективные беспроводные сети дальнего радиуса действия

mMTC – massive Machine-Type Communication, массовые межмашинные взаимодействия (одно из требований к сценариям применения сетей связи пятого поколения – IMT-2020)

MVNO – Mobile Virtual Network Operator, оператор мобильной виртуальной сети связи

NFC – Near Field Communication, коммуникации ближнего поля

PAN – Personal Area Networks, сети персонального доступа

QoS – Quality of Service, качество обслуживания (технология предоставления различным классам сетевого трафика различных приоритетов в обслуживании)

RFID – Radio Frequency Identification, технология радиочастотной идентификации

TWT – Target Wake Time, функция экономии расхода энергии подключенных устройств в технологиях беспроводной связи

URLLC – Ultra-Reliable Low Latency Communication, сверхнадежная передача данных с малой задержкой (одно из требований к сценариям применения сетей связи пятого поколения – IMT-2020)

V2X – Vehicle-to-Everything, технологическая концепция универсального взаимодействия транспортных средств с подключенными объектами внешнего окружения

WAN – Wide Area Networks, беспроводные сети связи дальнего радиуса действия

WSN – Wireless Sensor Networks, беспроводные сенсорные сети

3. Организации

3GPP – 3rd Generation Partnership Project, Проект партнерства третьего поколения мобильной связи

GSMA – GSM Association, Ассоциация GSM

IEEE – Institute of Electrical and Electronics Engineers, Институт инженеров электроники и электротехники

АИВ – Ассоциация участников рынка интернета вещей (сокращенное название – Ассоциация интернета вещей)

ГКРЧ – Государственная комиссия по радиочастотам

МСЭ – Международный союз электросвязи (International Telecommunication Union, ITU)

Введение



Развитие интернета вещей уже много лет задает вектор и во многом определяет ход процессов глобальной технологической трансформации общества, включая развитие цифровой экономики, построение индустрии 4.0, переход на управление на основе данных и пересборку логики бизнес-процессов в частном секторе, государственном секторе и отдельных отраслях.

Глобальные информационные сети, связывающие государства, общества и рынки, являются в первую очередь интернетом вещей: число межмашинных соединений в мире на 2021 г. втрое превышало число интернет-пользователей (14,6 млрд¹ против 4,9 млрд²). К 2030 г. интернет людей окончательно превратится в остров в океане межмашинных взаимодействий.

На этом временном горизонте вклад интернета вещей в мировую экономику будет измеряться уже не сотнями миллиардов, а триллионами долларов, внося существенный вклад в глобальный ВВП. Применения интернета вещей позволяют существенно ускорять товарооборот, обеспечивать общественную безопасность и снижать смертность от дорожно-транспортных происшествий, увеличивать урожайность, сокращать издержки в промышленности и многих других отраслях. Эффекты от внедрения интернета вещей во всех отраслях и нишах применения усиливает его конвергенция с технологиями 5G, искусственного интеллекта и обработки больших данных, облачных и граничных вычислений, распределенных реестров.

Россия является частью мирового рынка и активным участником развития технологической ниши интернета вещей. Важность этого направления в том числе отражена в национальной программе «Цифровая экономика» и входящих в ее состав федеральных проектах. АНО «Цифровая экономика» также определяет развитие интернета вещей в качестве одного из ключевых приоритетов своей деятельности.

Этот отчет является первым в серии аналитических материалов, общая цель которых – выявить возможности развития и более эффективного использования технологий интернета вещей для российской экономики, рынка и государства. Задача отчета – определить главные тенденции развития технологий и рынка IoT, а также возможности и инструменты государства как участника и бенефициара этих процессов.

- Первый раздел доклада отражает развитие концепции интернета вещей, структуру, ключевые направления и тренды развития рынка IoT. В том числе оценивается макроэкономический эффект от развития технологий интернета вещей, рассматривается развитие технологий связи и фиксируются основные тенденции и факторы, влияющие на рынок.
- Второй раздел включает в себя анализ национальных стратегий развития технологий и национальных рынков. В разделе рассмотрены три мировых лидера по размеру рынка интернета вещей (Европейский союз, КНР, США) и выборка стран, представляющих различные регионы (Австралия, Бразилия, Великобритания, Республика Корея). Отдельно рассматривается развитие государственной повестки в отношении интернета вещей в России.

В дополнение к функции обзорного аналитического материала отчет содержит предварительные рекомендации по приоритетным направлениям и механизмам поддержки развития интернета вещей в России. Продвижение этих рекомендаций и основанных на них проектных инициативах входит в задачи дальнейшей аналитической работы АНО «Цифровая экономика». Мы надеемся, что этот материал позволит привлечь внимание к насущным вопросам развития технологий и рынка IoT и будет полезен представителям отрасли, технического сообщества и государственных органов.

1 Развитие технологий и рынка IoT



Развитие концепции и определение рынка IoT

Понятие и концепция IoT

К настоящему моменту понятие IoT зафиксировано во множестве документов международных организаций. В 2012 г. Международный союз электросвязи (МСЭ) принял рекомендацию МСЭ-Т Y.2060³, в которой были предложены эталонная модель архитектуры и определение интернета вещей: *глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально информационно-коммуникационных технологий (ИКТ).*

Подход МСЭ во многом заложил исходную систему координат для концепции IoT, но не изменил ее зонтичный, обобщающий характер. С тех пор и по сей день подходы к пониманию и структурированию IoT развиваются и множатся как на национальном, так и на международном уровне. Только в российских источниках можно обнаружить не менее 15 различных определений интернета вещей⁴. Еще большее разнообразие определений, структурных схем и функциональных моделей существует в международных технических стандартах, нормативно-правовых актах, обзорах рынка и иных материалах.

Такая ситуация продиктована развитием технологии: интернет вещей изначально не был структурирован как единый технологический стек или консолидированный рынок. Удачный собирательный термин, придуманный в конце прошлого столетия, фактически вмещает в себя технологическую парадигму: *«киберфизические системы + межмашинное взаимодействие (M2M) + передача межмашинных данных по сетям связи + интеллектуальная обработка и аналитика данных».*

Критерии IoT: определяя границы между интернетом вещей и интернетом людей

Один из главных парадоксов интернета вещей «зашит» в его названии: на практике данные в межмашинной коммуникации не всегда передаются через глобальный интернет, даже если используется стек протоколов TCP/IP:

- Промышленные и корпоративные сервисы IoT часто развертываются на базе частных сетей связи, в которых доступ в интернет не используется для большинства бизнес-процессов.
- Многие технологии связи, применяемые для передачи данных между устройствами IoT, используют собственные протоколы транспортного и сетевого уровня и не ориентированы на TCP/IP как стандартный способ организации соединения. Например, большинство узкополосных энергоэффективных сетей (LPWAN) и такие протоколы, как Bluetooth, Zigbee, имеют собственные системы адресации и по умолчанию не используют IP-адреса.
- То же можно сказать и о технологии радиочастотной идентификации (RFID): меткам RFID может быть присвоен IP-адрес, но по умолчанию для сервисов на базе этой технологии не требуется интернет-соединение.

- Во многих случаях M2M-данные не передаются дальше локального контура информационной системы, к которой подключены генерирующие их устройства. Например, в эту категорию попадает большая часть объема данных видеокамер, радаров и лидаров подключенных автомобилей.

С каждым годом передача данных по TCP/IP все более широко используется в сервисах и приложениях IoT – так, почти вся аналитика M2M-данных сегодня организована на базе облачных сервисов, доступных через интернет. И тем не менее передача данных по IP-протоколу не может считаться строгим критерием, позволяющим отделить IoT от других ИКТ-сервисов.

- Единственным таким критерием служит сама межмашинная коммуникация, то есть формирование и передача данных подключенных устройств без участия человека, как ее определяют Международный союз электросвязи и Институт инженеров электроники и электротехники (IEEE)⁵.
- На сегодняшний день, с учетом развития технологий граничных вычислений, к этому списку можно добавить еще один необязательный критерий «умного» устройства IoT: наличие у устройства собственной вычислительной мощности и/или блока памяти для перезаписи M2M-данных, а также их обработки.

Таким образом, основу интернета вещей полностью определяют M2M-коммуникации. Сегодня к ним добавляется обширный уровень аналитики и обработки межмашинных данных через различные сервисы – централизованные и распределенные, развернутые в интернете, в локальных сетях или на периферии вплоть до самого устройства.

Структура продуктов и технологий IoT: из чего складывается IoT?

Каждый участник рынка, системы государственного управления, отраслевого и технического сообщества рассматривает интернет вещей исходя из своей позиции, зоны ответственности, задач развития и сферы компетенций.

С учетом такой картины нет смысла пытаться уложить интернет вещей в единую жесткую модель или структуру для анализа. Чтобы понять, куда движется рынок IoT, какие факторы способствуют его расширению и формированию спроса, целесообразнее «распаковать» понятие IoT в несколько основных проекций или срезов технологии и ее применений:

1. **Стек протоколов и спецификаций технологий IoT:** включает протоколы сетей связи, по которым передаются межмашинные данные; протоколы, схемы и форматы M2M-данных; протоколы идентификации и управления подключенными устройствами; базовые инфраструктурные технологии и протоколы, «поверх» которых выстраивается M2M-взаимодействие и работа сервисов IoT, и прочее. В настоящем отчете стек протоколов IoT привязан не к эталонной модели взаимодействия открытых систем (ISO/OSI), а к модели TCP/IP, которая применяется для описания сетевых взаимодействий через интернет.

2. **Инфраструктурно-продуктовая экосистема IoT:** в этом разрезе интернет вещей представлен с точки зрения самого рынка, тех продуктов и решений, которые на нем представлены, – условных «кирпичиков», из которых выстраиваются современные сервисы и бизнес-модели. С этой точки зрения экосистема IoT включает в себя:

- a. оборудование и аппаратные решения для «умных вещей»;
- b. ПО и оборудование для средств связи и передачи M2M-данных по сетям;
- c. инфраструктуру и сервисы хранения, обработки и аналитики данных;
- d. пользовательские сервисы.

Сквозные элементы в этой схеме – интегрированные платформы IoT и средства обеспечения кибербезопасности.

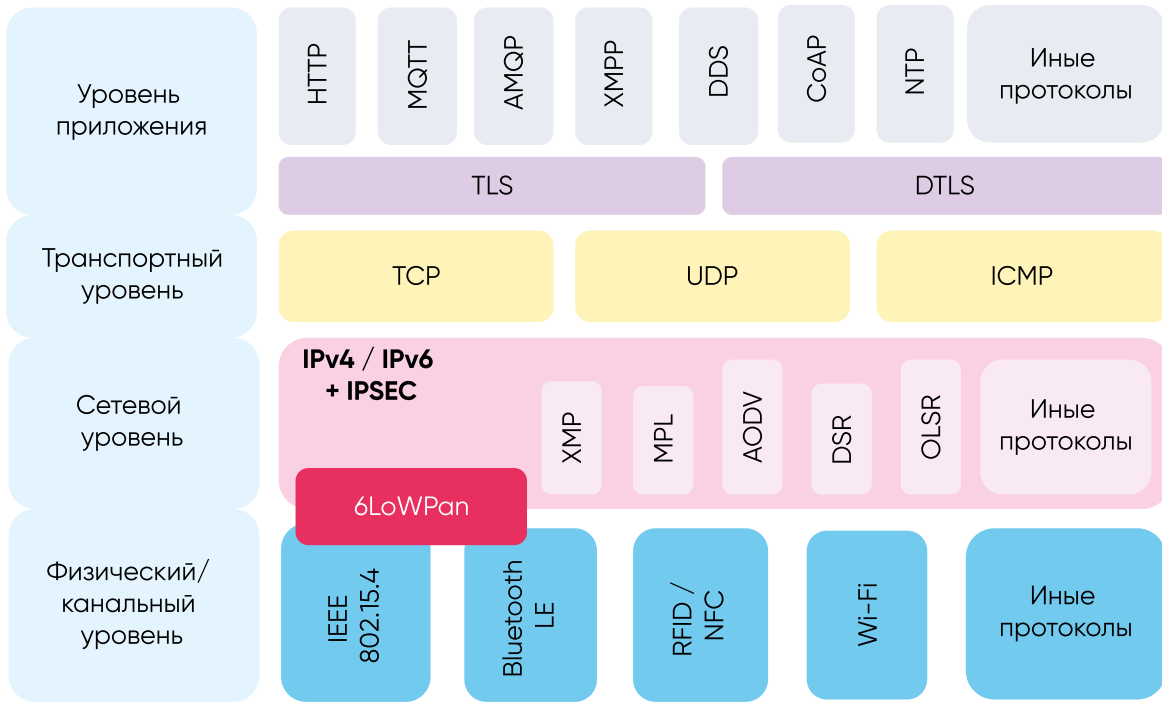
3. Наконец, третий срез IoT – **спектр нишевых и отраслевых применений** в экономике, хозяйстве и управлении. Примеры включают применения интернета вещей в агропромышленном комплексе, обрабатывающей промышленности, медицине, транспортном и логистическом секторе, энергетике и так далее. В отдельных случаях возникают комплексные многоуровневые отрасли применения интернета вещей, такие как умный город (Smart City). Нишу умного города формируют применения межмашинной передачи и обработки данных в рамках индивидуального домохозяйства (умный дом, Smart Home), многоквартирных домов и офисных зданий (умное здание, Smart Building), а также в городских интеллектуальных транспортных системах и «умных» общественных пространствах.

Как показано на схеме ниже, все эти срезы IoT взаимосвязаны друг с другом и развитие одного из них изменяет содержание остальных. В рамках отчета проводится верхнеуровневый анализ рынка IoT по технологиям связи и по основным нишам продуктовой и инфраструктурной экосистемы.

Инфраструктурно-продуктовая экосистема IoT



Протоколы IoT по уровням модели TCP/IP



Развитие глобального рынка и влияние IoT на макроэкономические показатели

Рост подключений и данных IoT: оставляя интернет людей позади

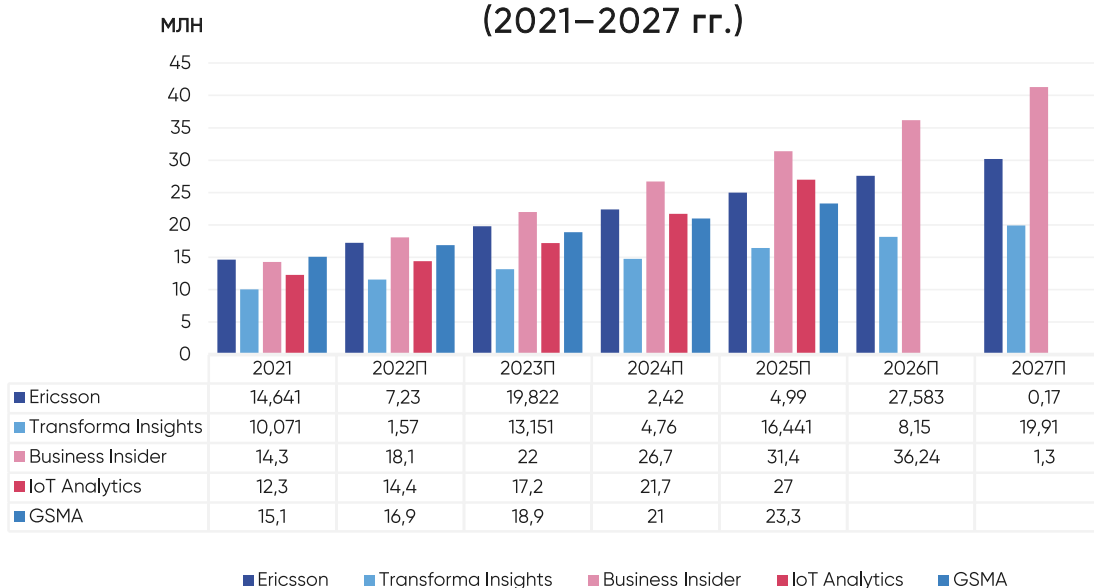
Предварительные оценки числа подключенных устройств в мире на 2022 г. находятся в диапазоне от 11,57 до 18,3 млрд⁶. Несмотря на разброс в количестве подключений, различные источники анализа рынка сходятся в том, что глобальная индустрия IoT преодолела последствия пандемии COVID-19 и почти вернулась к прежним темпам роста. Все оценки числа подключений на текущий год показывают рост от 15 до 20 % по отношению к 2021 г., который носит восстановительный характер и компенсирует замедление в 2020–2021 гг.

В 2020 г. интернет вещей преодолел ключевой рубеж в своем развитии – число подключенных устройств IoT впервые превысило подключения всех других типов устройств (персональные компьютеры, смартфоны, планшеты и прочее)⁷. В дальнейшем этот разрыв будет только расти – к 2025 г. на одно устройство интернета людей придется 4 устройства для M2M-взаимодействий⁸.

Впрочем, прогнозы роста числа устройств IoT на среднесрочную перспективу серьезно расходятся (от 19,91 до 41,3 млрд подключений на 2027 г.).

- Наиболее близкие друг к другу оценки дают крупные мобильные операторы, плотно вовлеченные в развитие инфраструктуры связи для IoT. Прогноз GSMA предполагает 23,3 млрд подключений к 2025 г., данные Ericsson – 24,99 млрд⁹.
- Аналитические компании, специализирующиеся на рынке IoT, дают оценки с разбросом почти в два раза – от 16,44 до 31,4 млн подключений к 2025 г.¹⁰

Динамика общего числа подключенных устройств IoT (2021–2027 гг.)



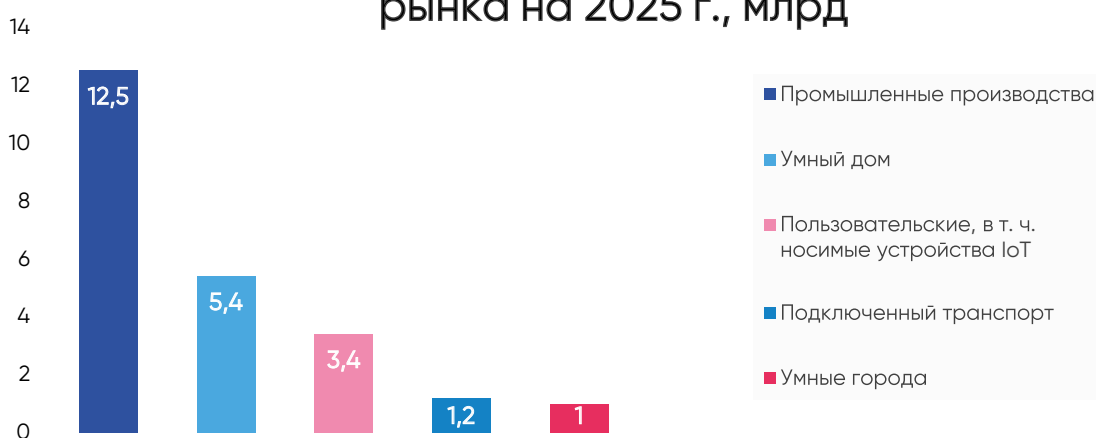
- В долгосрочной перспективе ожидается взрывообразный рост подключений: к 2030 г. McKinsey ожидает более 59,5 млрд подключенных устройств IoT¹¹, Huawei к этому же году ориентируется на 100 млрд¹².

Еще один важный тренд в структуре подключений связан с ростом удельного веса индустриального IoT.

- До сих пор пользовательский сегмент неизменно обеспечивал основную долю подключений устройств: 7 млн против 6 млн промышленных подключений в 2020 г., 9 млн против 8 млн в 2022 г.
- В 2023 г. оба сегмента сравниваются по числу подключений, а с 2024 г. промышленный IoT будет устойчиво лидировать: прогноз на 2025 г. – 14 млрд промышленных подключений IoT против 11 млрд пользовательских¹³.

Преобладание применений IoT индустриального уровня, в первую очередь собственно в промышленных производствах, отражается в разбивке подключений по нишам.

Подключения устройств IoT по сегментам рынка на 2025 г., млрд



Промышленный сегмент IoT формирует среда, обеспечивающая управление технологическим циклом, включая конкретное производственное оборудование, с помощью различных исполнительных устройств, датчиков и сенсоров. IIoT-решения позволяют предприятиям сокращать простои, снижать затраты на техническое обслуживание, усовершенствовать процедуры прогнозирования и предотвращения отказов оборудования, а также обеспечивать безопасность производственного персонала.

Помимо промышленного сегмента, в этой выборке интересна большая доля умного дома, в 5,4 раза опережающего другие сегменты умного города по числу подключений. К применениям IoT в умном доме относятся:

- индивидуальные квартирные счетчики потребления коммунальных ресурсов;
- системы домашней автоматизации и контроля освещения;
- домашние системы кондиционирования;
- системы безопасности и управления подключенной бытовой техникой;
- в загородных домах растет применение IoT для управления автономными системами теплоснабжения и энергоснабжения (например, частными котельными и солнечными батареями).

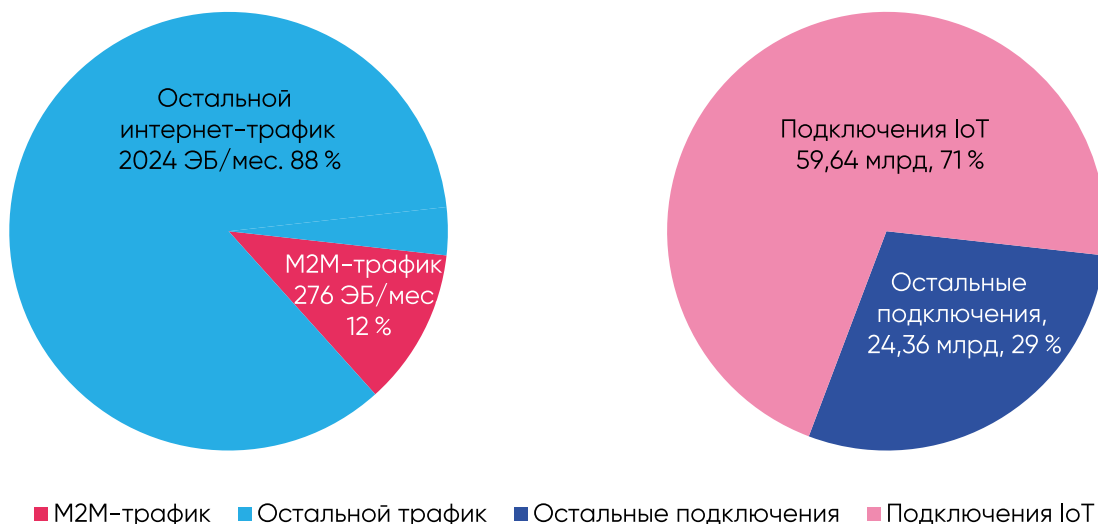
Как отмечалось выше, умный дом образует лишь один из элементов комплексной ниши умного города, наряду с умным зданием (Smart Building) и другими видами «умной» городской инфраструктуры на базе технологий IoT. Ключевые составляющие умного города представлены на схеме ниже.



Приведенная выше статистика говорит о том, что вторым после промышленного сегмента драйвером роста подключений устройств IoT в среднесрочной перспективе останется ниша умного дома. Несмотря на масштабные государственные и частные инвестиции в развитие умных городов, динамика общего числа подключений IoT будет в большей степени определяться сценариями применения недорогих и сравнительно простых устройств в масштабах отдельного домохозяйства.

Несмотря на рост числа подключений, IoT в обозримой перспективе так и не сравняется с интернетом людей по объему генерируемых данных. По оценке McKinsey, к 2030 г. объем M2M-трафика вырастет в 44 раза (до 276 ЭБ/мес.), но его доля в общем интернет-трафике составит лишь 12 %.

Доля устройств IoT и M2M-трафика от общего числа подключений и объема интернет-трафика на 2030 г. ¹⁴



Но этот прогноз учитывает только M2M-данные, которые передаются через интернет, то есть по IP-протоколу. Общий объем данных, генерируемых в процессе M2M-коммуникаций, многократно выше и включает в себя данные в частных сетях, сетях общего доступа, не использующих IP-соединение, и данные, передаваемые и обрабатываемые в локальном контуре информационных систем.

С учетом этих видов данных объем датасферы IoT измеряется зеттабайтами¹⁵. По оценке IDC, ежегодный объем M2M-данных в 2019 г. достиг 18,3 ЗБ, а к 2025 г. вырастет в 4 раза и составит порядка 80 ЗБ/год¹⁶. Основную долю в этом объеме будут обеспечивать системы умного видеонаблюдения, применения интернета вещей в автоиндустрии и сервисы индустриального IoT.

Рыночный объем IoT: ускоренный рост после COVID-19

Мировой рынок IoT серьезно замедлился в развитии в 2020–2021 гг. под влиянием пандемии COVID-19. В первом квартале 2022 г. рынок начал постепенно возвращаться к прежней траектории роста. Однако начиная с марта 2022 г. дальнейшие события, включая обострение международно-политической обстановки, затянувшийся глобальный дефицит предложения полупроводниковой продукции и кризисы на энергетических рынках, вновь затормозили развитие интернета вещей. Новые оценки по итогам года только формируются, однако они могут отставать от приведенных ниже данных на начало года на 5–10 % по темпам роста и на 8–15 % по объемам рынков IoT:

- На 2021 г. объем рынка, подсчитываемый по совокупным расходам на внедрение решений IoT, оценивался в 381–385 млрд долл. США¹⁷.
- На текущий год оценки составляли уже порядка 478 млрд долл. США, а к 2028 г. прогнозируется рост рынка до 1,84–2,46 трлн долл. США¹⁸.
- Ежегодный темп роста оценивался в 24–31 %, что практически не отличается от прогнозов, которые формировались до пандемии.
- На краткосрочную перспективу (2022–2024 гг.) отдельные источники прогнозировали более низкий темп роста рынка (11,3 %), связанный с замедленным восстановлением спроса после пандемии¹⁹.

Развитие рынка IoT по расходам остается крайне неравномерным в региональном разрезе, и в среднесрочной перспективе ситуация не поменяется.

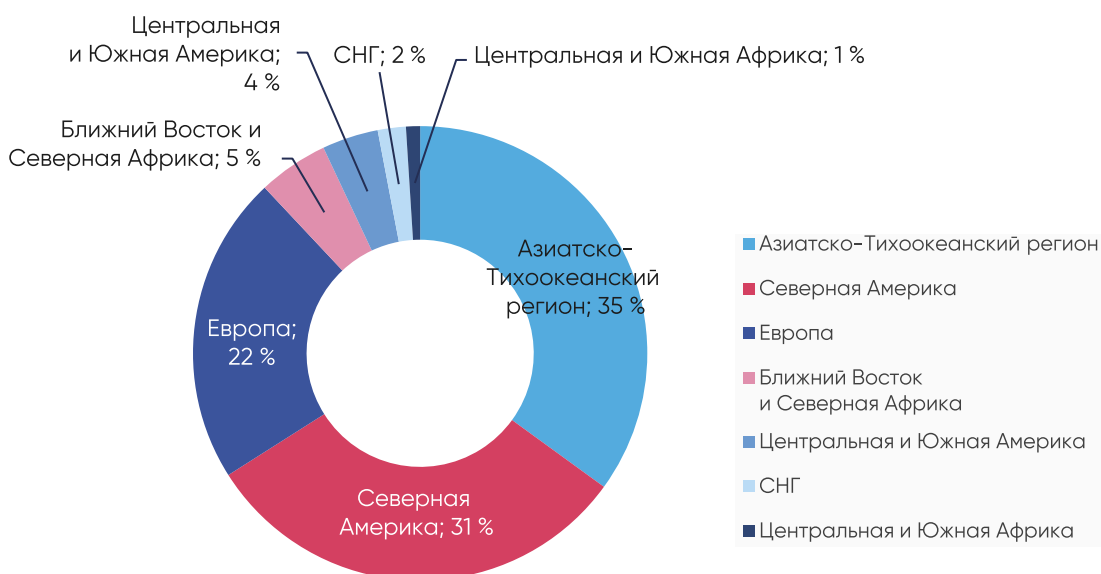
- КНР, США и ЕС продолжают формировать основу рынка: в сумме на три страны/региона приходилось более 75 % всех затрат на внедрения IoT в 2021 г.²⁰ Рыночная картина практически в точности соответствует тому, как эти страны представлены в статистике подключений IoT: в сумме на них приходится три четверти подключенных устройств, и такая пропорция сохранится до 2027 г.
- При этом, даже среди трех рыночных лидеров, КНР выделяется превосходящими темпами роста – 13,4 % ежегодно против 9–11,4 % в США и ЕС. По оценке IDC, к 2024 г. на КНР придется более четверти от общих мировых расходов на внедрения IoT (26,7 %), что сделает страну лидером по вложениям в эту технологическую нишу²¹.

- В относительном выражении на первое место по темпам роста расходов выходят Ближний Восток и Северная Африка (19,0 %), Центральная и Восточная Европа (17,6 %) и Латинская Америка (15,8 %) ²². Ускорение развития IoT в этих регионах любопытно и определяется такими факторами, как:
 - рост зрелости технологий и бизнес-моделей IoT в сельском хозяйстве, что повышает привлекательность интернета вещей для развивающихся стран с высоким удельным весом аграрного сектора;
 - растущий потенциал IoT для сокращения издержек в управлении и промышленном секторе, что создает возможности для резкого повышения эффективности в указанных регионах за счет эффекта низкой базы;
 - растущая доступность решений IoT, основанных на облачных сервисах и платформенных моделях.

Что касается доходов участников рынка IoT, влияние пандемии здесь сохранится в краткосрочной перспективе.

- К 2025 г. совокупные доходы рынка утроятся по сравнению с 2021 г. и достигнут 900 млрд долл. США, однако этот объем на 20 % меньше прогнозируемого из-за влияния COVID-19 ²³.
- По другим оценкам, совокупный доход рынка к 2025 г. все же успеет вернуться к допандемийным темпам роста и достигнет 1,1 трлн долл. США ²⁴.
- Распределение доходов участников отрасли IoT по регионам почти в точности отражает картину рынка по расходам, но еще более неравномерно. На Европу, Северную Америку и Азиатско-Тихоокеанский регион в сумме приходится 88 % доходов, доля остальных регионов незначительна.

Региональное распределение рынка IoT в 2021 г. (по доходам), %



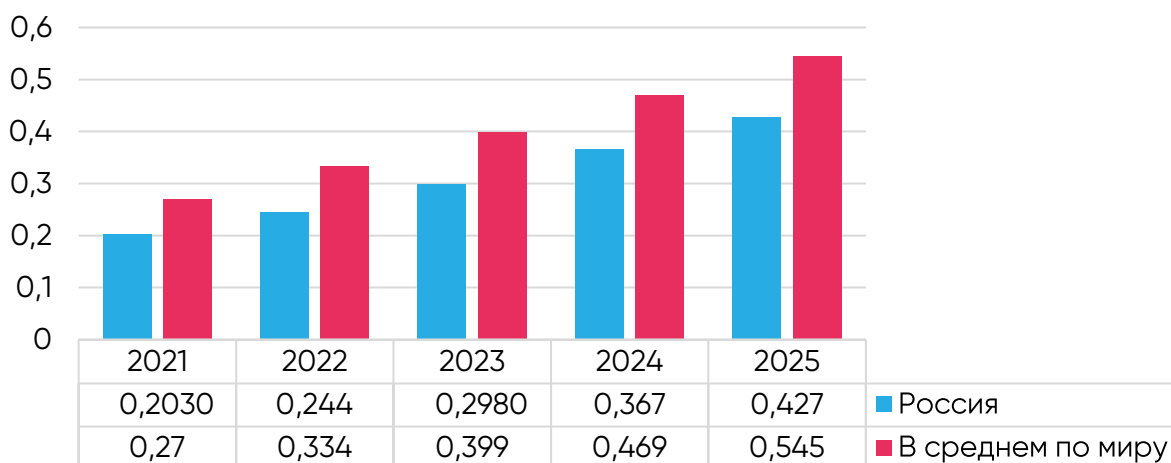
Россия на фоне общемировых тенденций находится в когорте отстающих стран по числу подключенных устройств IoT на душу населения и темпам роста рынка.

Еще до февраля 2022 г. число подключений IoT в сетях дальнего радиуса действия (WAN) на душу населения в России было ниже среднего по миру. По прогнозам, отставание на 25–30 % должно было сохраниться как минимум до 2025 г.

С учетом нынешней ситуации и ее последствий российские темпы роста числа подключений на душу населения в краткосрочной перспективе будут еще ниже, а отставание от среднемирового уровня может достичь 35–45 %.

По оценке J’son&Partners Consulting, даже без учета нынешней ситуации доля России в подключениях IoT по сетям WAN к 2025 г. должна была упасть ниже 1 % от общего числа подключений в мире²⁵.

Число подключений IoT в сетях дальнего радиуса действия (WAN) на душу населения (подключения/чел.)



Макроэкономические эффекты: IoT как фактор роста ВВП

Влияние IoT на экономику гораздо шире, чем сумма расходов на внедрение и доходов поставщиков решений. Экономическая ценность интернета вещей определяется прямыми и косвенными эффектами от внедрения и использования его решений и включает в себя следующее:

1. Повышение производительности, прежде всего в промышленности, снижение доли производственного брака и, как следствие, общих издержек.
2. Снижение потерь электроэнергии, воды, тепла, аварийности в распределительных сетях, оптимизация распределения коммунальных ресурсов.
3. Повышение урожайности и иных основных показателей в сельском хозяйстве, повышение качества переработки и хранения продовольствия, снижение расходов топлива и темпов амортизации сельхозтехники.
4. Ускорение логистического цикла, сокращение потерь от задержек в цепочках поставок и повышение эффективности использования складских помещений.

5. Оптимизация грузового, товарного и пассажирского трафика, снижение расходов топлива, высвобождение времени водителей подключенного автотранспорта.
6. Повышение качества, ускорение процесса и рост результативности медицинской помощи, сокращение смертности населения за счет использования технологий IoT в здравоохранении, повышение удельной эффективности применения медицинского оборудования и медтехники.
7. Снижение уровня преступности, аварийности и смертности на дорогах, расширение возможностей информирования населения о чрезвычайных ситуациях.
8. Повышение качества, расширение охвата и спектра экологического мониторинга, минимизация последствий экологических инцидентов.

Измерение этих эффектов от внедрения сервисов интернета вещей не всегда может быть полным и точным, однако текущие оценки показывают их уверенный рост.

- Суммарный накопленный вклад IoT в глобальную экономику на конец 2020 г. достиг 1,6 трлн долл. США (для сравнения, это соответствует 1,89 % глобального ВВП за тот же год)²⁶.
- К 2030 г. этот показатель может достичь в разных сценариях от 5,5 до 12,6 трлн долл. США²⁷.
- К 2025 г. ежегодный вклад IoT в рост мировой экономики за счет повышения производительности достигнет 370 млрд долл. США, или 0,34 % от прогнозируемого объема глобального ВВП²⁸.
- В эти оценки включается в том числе выгода, получаемая клиентами и потребителями сервисов IoT.

Фактические данные за прошедшие периоды в целом подтверждают такие оценки:

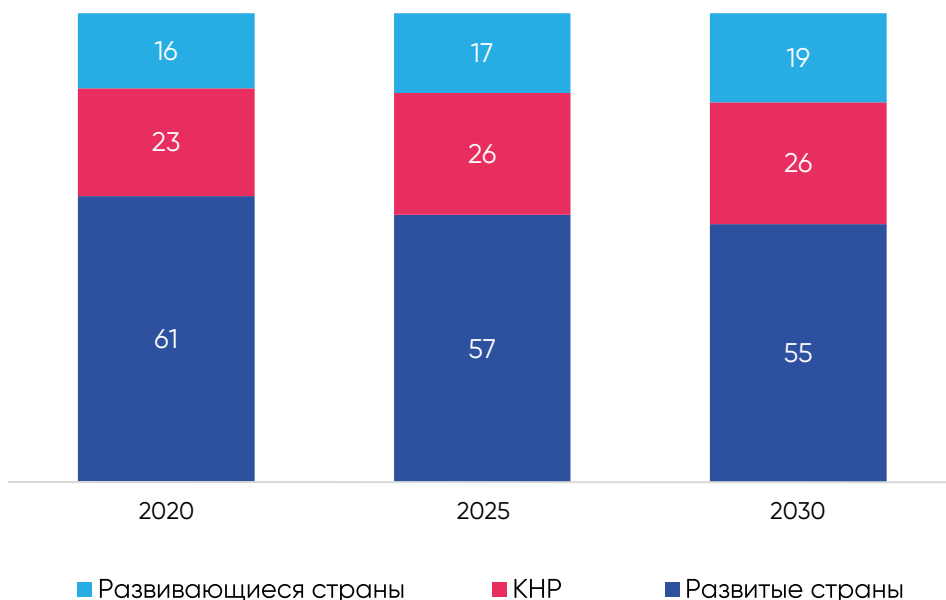
- Исследования ежегодного вклада IoT в экономический рост, проведенные в 2021 г., дают верхнюю оценку от 0,69 до 0,8 % глобального ВВП на ближайшие годы²⁹.
- Вклад применений IoT в рост производительности, снижение издержки и иную экономическую выгоду для бизнес-клиентов за 2018 г. оценивается в 175 млрд долл. США, или 0,2 % глобального ВВП³⁰.
- Для выхода на прогнозные значения к 2025 году обеспечиваемый интернетом вещей вклад в глобальную экономику должен увеличиваться ежегодно на 11,5 %. Такие темпы роста вполне соответствуют текущим и прогнозным данным по темпам роста самого рынка IoT. Вопрос лишь в том, будет ли расширение рынка линейно конвертироваться в прирост накопленного вклада IoT в экономику.

В региональном и страновом разрезе распределение этого вклада примерно соответствует долям крупнейших участников рынка.

- На 2020 г. более 50 % всего экономического эффекта от внедрения IoT было сконцентрировано в США и КНР.

- К 2025 г. доля КНР в общемировом вкладе IoT в экономику достигнет 26 % и закрепится на этом уровне до 2030 г. Внедрение интернета вещей в КНР продолжит обеспечивать больший экономический эффект, чем во всех развивающихся странах, вместе взятых³¹. Этот показатель заметно превысит общую прогнозируемую долю КНР в мировой экономике (20 %).

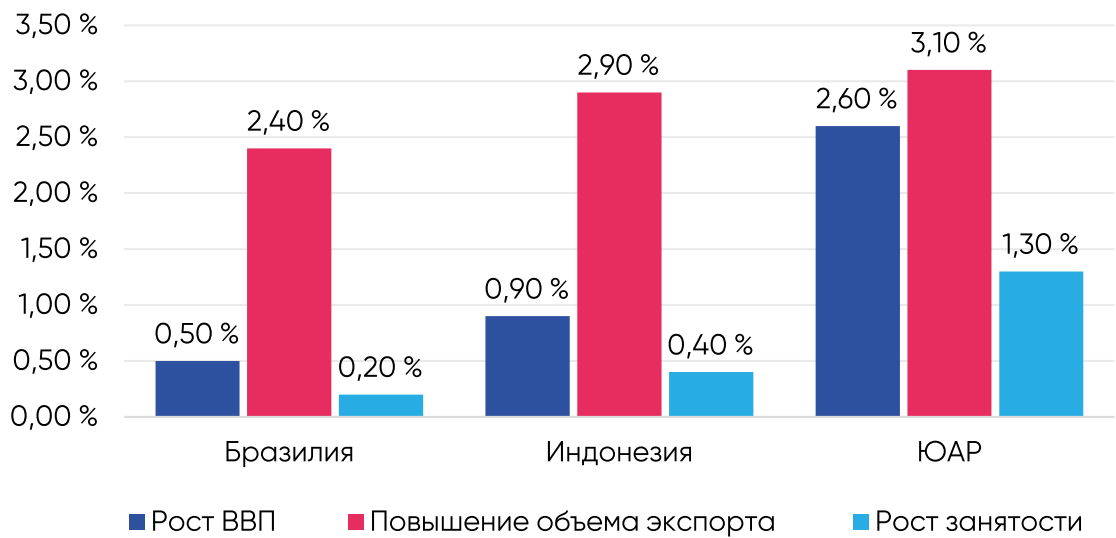
Экономический вклад IoT в региональном разрезе, %



В разрезе сегментов рынка и отраслевых ниш основную долю (65 %) добавленного объема для мировой экономики обеспечит сектор B2B. Ключевым генератором экономического вклада будут применения IoT в промышленном производстве (более 50 % от суммарного накопленного вклада в экономику).

Помимо общего вклада в глобальный ВВП, технологии интернета вещей способны существенно ускорить экономическое развитие отдельных государств. В значительной степени макроэкономический эффект от внедрений IoT зависит от того, насколько существующее регулирование не препятствует трансграничным потокам M2M-данных. Выборочные исследования за 2021 г. показывают, что при отсутствии барьеров для трансграничной передачи и обработки M2M-данных опережающее внедрение IoT может обеспечить отдельным развивающимся странам рост национального ВВП на 0,5–2,6 %, рост объема национального экспорта на 2,4–3,1 % и повышение уровня занятости на 0,2–1,3 %.

Потенциальные эффекты опережающего внедрения IoT для развивающихся стран



При этом для ряда рынков нарушение свободного трансграничного обмена M2M-данными сократит все перечисленные эффекты более чем наполовину. Это свидетельствует о том, что развитие интернета вещей все больше зависит не только от инфраструктуры связи, но и от технологий, бизнес-моделей и регуляторной среды обработки данных.

Исключениями являются те рынки, где бизнес-модели и сценарии потребления сервисов IoT по разным причинам замкнуты прежде всего на внутристрановую аудиторию. Ключевым примером такого рынка является КНР: объем внутреннего рынка делает его экономически самодостаточным и радикально снижает необходимость в развитии сервисов и бизнес-моделей IoT на базе трансграничного обмена данными. Другим примером может выступить Россия, где снижение зависимости от трансграничных сервисов IoT диктуется прежде всего стремлением к технологической независимости и суверенитету над данными и инфраструктурой их обработки.

В случае России и КНР фактор трансграничного обмена данными при развитии сервисов и инфраструктуры IoT уже весьма далек от 50 % и не оказывает существенного влияния на развитие индустрии.

Развитие беспроводных технологий связи для IoT

Развитие спектра технологий связи для IoT

Несмотря на то, что каждый уровень в технологическом стеке IoT представляет собой отдельную нишу, развитие глобального рынка в первую очередь определяют технологии связи. Кроме того, подключенные к сетям связи устройства интернета вещей поддаются объективному подсчету, что дает возможность оценить и измерить рынок.

На сегодняшний день на рынке IoT присутствуют как беспроводные, так и проводные технологии связи. Прямые проводные подключения устройств используются преимущественно в промышленном IoT.

- Основные достоинства проводной связи на промышленных объектах – надежность соединения, возможность обеспечить качество обслуживания, простота управления сетью, контроля и обеспечения безопасности.
- Но эта технология оказывает все меньшее влияние на рынок по причине худшей масштабируемости, особенно если нужно обеспечить массовые подключения на большом количестве распределенных объектов.

Развитие IoT и его будущее, за исключением специфических производств, определяет беспроводная связь.

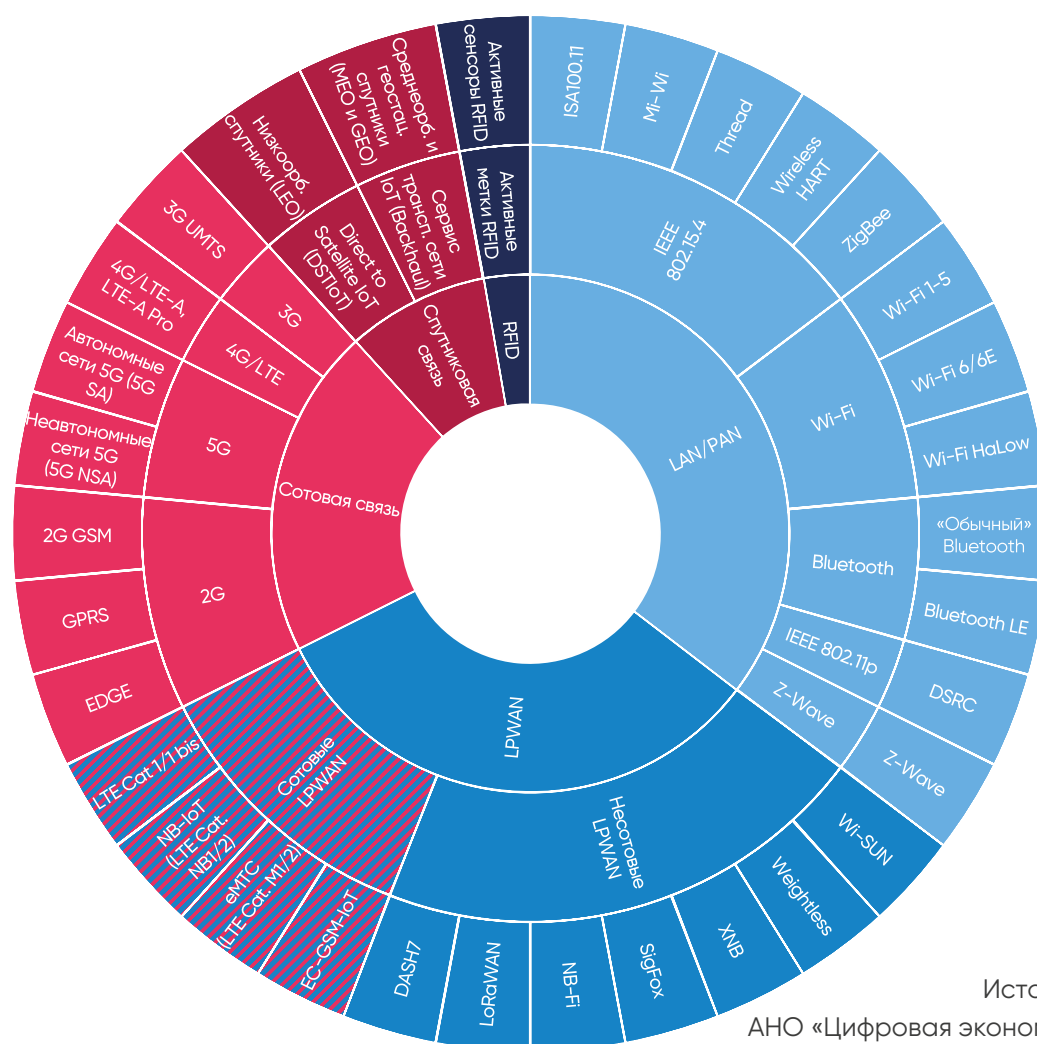
На 2022 г. к основным технологиям беспроводной связи для подключения устройств IoT относятся:

1. Спутниковая связь, использующая для подключений устройств IoT ряд частотных диапазонов (Ku-, K-, Ka-диапазоны и прочие) и спутниковых группировок на орбитах разной высоты (от низкоорбитальных до геостационарных).
2. Технологии сотовой связи, которые охватывают поколения 2G/GSM, 3G, 4G/LTE и активно развивающийся сегмент связи 5G.
3. Энергоэффективные узкополосные сети дальнего радиуса действия (Low Power Wide Area Networks, LPWAN) – группа технологий связи, развитие которой было изначально ориентировано на M2M-взаимодействия. Включает в себя две категории:
 - LPWAN на базе сотовой связи (*cellular LPWAN*). Такие узкополосные сети используют модифицированные протоколы сотовой связи и, как правило, развертываются поверх сотовых сетей, представляя собой разновидность «наложенной» сети. В настоящее время наиболее широко распространенные на рынке решения этой категории – стандартизированные консорциумом 3GPP технологии NB-IoT (LTE Cat-NB), EC-GSM-IoT, eMTC (LTE Cat M1/M2) и LTE Cat 1 / Cat 1 bis.

- Вторая группа LPWAN, напротив, не основана на технологиях сотовой связи и использует собственные протоколы для узкополосной энергоэффективной передачи данных. Несотовые LPWAN развертываются на полосах частот в нелицензируемых диапазонах, в отличие от сетей сотовой связи. На рынке эта категория представлена международными стандартами LoRaWAN, SigFox, Weightless, RPMA, DASH7, а также российскими NB-Fi, GoodWan/OpenUNB, XNB, LoRaWAN RU.
4. Беспроводные технологии ближнего радиуса действия, которые составляют основу локальных и персональных беспроводных сетей (Local Area Networks, LAN и Personal Area Networks, PAN). К этой группе относится большое количество протоколов и технологий, включая Wi-Fi, Bluetooth, протоколы на базе стандарта IEEE 802.15.4, Z-Wave, DSRC и прочие.
 5. Отдельную группу составляют технологии радиочастотной идентификации – RFID и ее подвид NFC. Эти способы беспроводного взаимодействия по своим характеристикам находятся «на границе» IoT, несмотря на то что в 1990-е гг. сам термин «интернет вещей» появился благодаря RFID-меткам.

Наполнение этих групп технологий более подробно представлено на схеме ниже. Стоит отметить, что в ней представлен не исчерпывающий перечень: общее число протоколов и стандартов беспроводной связи, применяемых в IoT, слишком велико и постоянно растет в связи с бурным развитием рынка.

Спектр основных технологий беспроводной связи для IoT

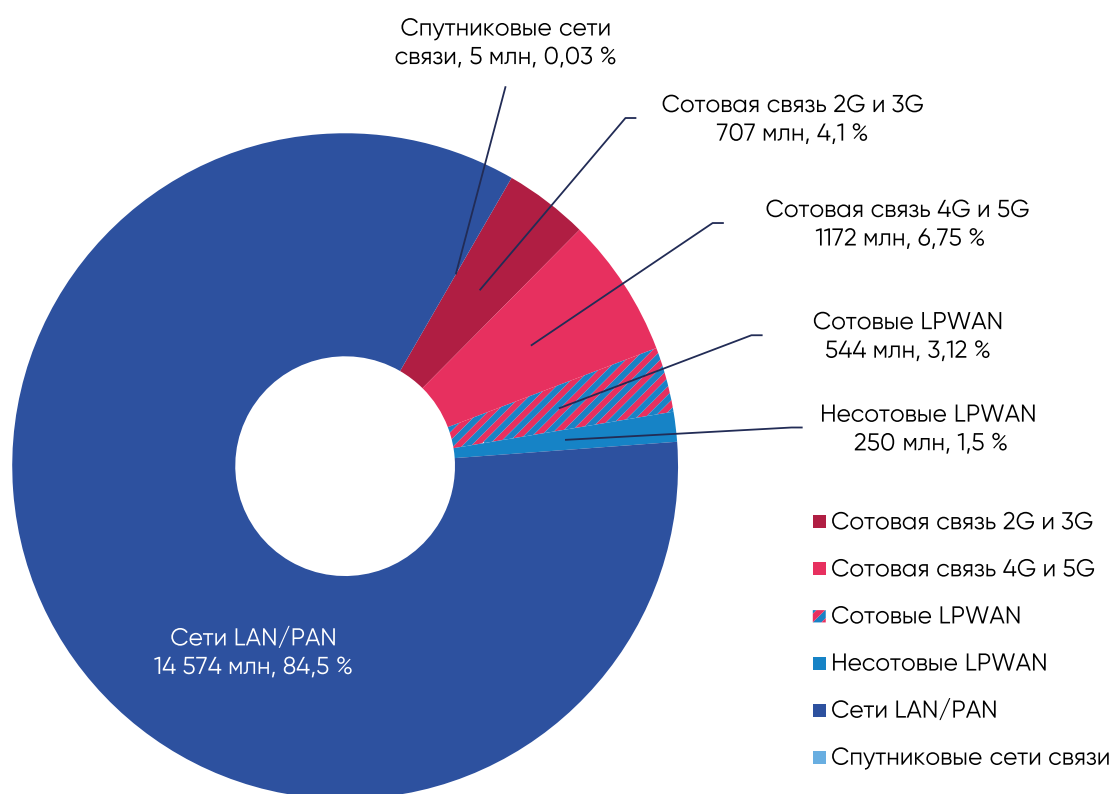


Источник:
АНО «Цифровая экономика»

Структура подключений устройств IoT по технологиям принципиально не изменилась за последние 3 года.

- На 2022 г. основную долю подключений устройств IoT в мире (84,5 %) ³² обеспечивают беспроводные технологии малого радиуса действия (сети локального и персонального доступа, LAN/PAN), такие как Wi-Fi, Bluetooth, Zigbee и прочие.
- На втором месте – беспроводные сети с дальним радиусом действия (Wide Area Networks, WAN), которые на 2022 г. обеспечивают 15,4–16,3 % от всех подключений устройств IoT, или порядка 2,66–2,8 млрд подключенных устройств. К 2027 г. эти показатели возрастут до 5,913 млрд и 19,5 % соответственно.
- Среди технологий WAN крупнейшим сегментом пока остается широкополосная сотовая связь всех поколений (порядка 6,75 % от общего числа подключений устройств IoT), оставшуюся долю делят между собой сотовые и несотовые узкополосные сети (3,12 и 1,5 % соответственно).
- Другие технологии, такие как спутниковая связь и проводные коммуникации, обеспечивают незначительную долю от общего числа подключений.

Доля подключений устройств IoT по беспроводным технологиям связи на 2022 г., %



Сети широкополосной сотовой связи: миграция IoT с 2G на 5G

Широкополосная сотовая связь является одним из ключевых технологических драйверов роста и расширения рынка IoT.

- По разным оценкам, общее количество подключенных устройств IoT на базе широкополосной сотовой связи всех поколений (от 2G до 5G) в 2022 г. достигнет от 1,21 до 1,88 млрд³³. Расчеты крупных операторов и ассоциаций сотовой связи (Ericsson, GSMA) находятся у верхней границы этих оценок.
- По прогнозам, эти показатели будут плавно расти в среднесрочной перспективе. Так, общее число подключений устройств IoT по всем поколениям широкополосной сотовой связи достигнет 1,96–2,69 млрд к 2027 г.³⁴ Среднегодовые темпы роста количества подключений составят порядка 10 %.
- Одним из важнейших факторов, стимулирующих участников рынка к переходу на новые поколения связи, является растущая эффективность использования радиочастотного ресурса. LTE и 5G позволяют использовать полосы радиочастотного спектра с большей удельной эффективностью, что является ключевым преимуществом в условиях постоянно растущего дефицита радиочастотного ресурса и доступных для коммерческих операторов участков спектра.

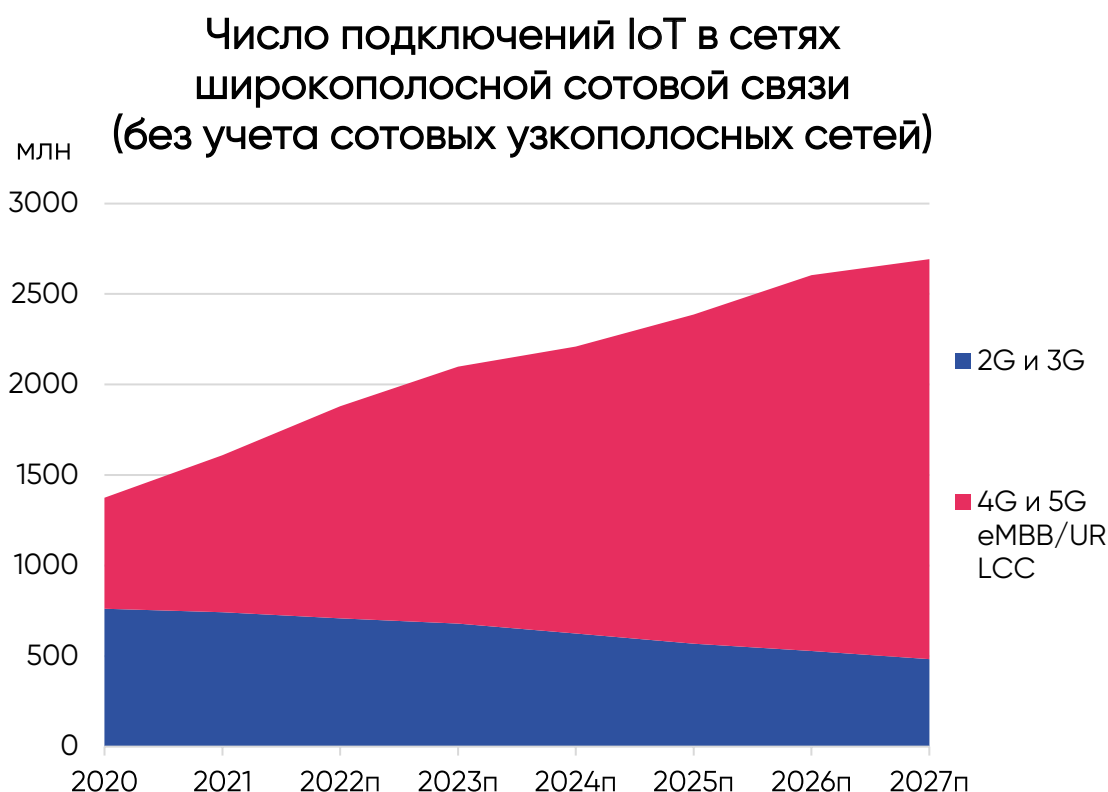
Эта статистика не включает в себя развитие узкополосных сетей на базе сотовой связи (сотовые LPWAN), которые обеспечат основной прирост числа подключений на базе сотовой связи в среднесрочной и долгосрочной перспективе. Развитие этой ниши технологий сотовой связи и ее применений в IoT подробно рассматривается в следующем разделе.

Ключевой тренд, который определяет динамику применений широкополосной сотовой связи для интернета вещей, – растущий спрос промышленного сектора на IoT для критически важных процессов (critical IoT):

- «Критический» IoT необходим в тех нишах, где максимально важны очень высокая скорость передачи M2M-данных (от 50 Мбит/с и выше), минимальная задержка сигнала (порядка 10 мс, а в некоторых применениях не более 1–2 мс) и надежность соединения.
- Большая часть сценариев «критического» IoT – это управление системами передачи M2M-данных в режиме реального времени (Real Time IoT, RT-IoT). В таких системах поток данных с подключенных устройств идет практически непрерывно, а технология должна гарантировать двустороннюю связь, обработку больших объемов данных и качество сервиса.
- Примеры таких применений IoT включают в себя управление подключенными автомобилями и поддержку их взаимодействия с окружающими объектами (V2X); эксплуатацию медицинской, логистической и промышленной робототехники; мониторинг и управление производственными процессами; управление комплексными системами мониторинга, включая видеонаблюдение в высоком разрешении, в умном городе; поддержку взаимодействий с использованием технологий виртуальной, дополненной и расширенной реальности (VR, AR, XR); управление группировками гражданских и военных БПЛА и прочее.

Параллельно ускоряется другой процесс – неуклонное снижение доли подключений устройств IoT на базе «старых» поколений мобильной связи (2G и 3G).

- В 2021 г. был пройден важный рубеж – число подключений устройств IoT на базе 2G и 3G впервые составило менее 50 % от общего числа подключений на базе широкополосной сотовой связи, уступив 4G и 5G.
- По оценке на 2022 г., 2G и 3G обеспечат лишь 37,7 % подключений (708 млн).
- Этот разрыв необратим и будет быстро углубляться – уже к 2027 г. доля подключений устройств IoT на базе 2G и 3G снизится всего до 18 %, а в абсолютном выражении сократится до 484 млн.



Основная причина такой динамики – «глобальный закат» 2G и 3G, который определяется общими закономерностями развития технологий сотовой связи.

- Сети связи на базе «старых» поколений не могут конкурировать по своим характеристикам с 4G и 5G как для пользователей, так и для самих операторов, и выводятся из эксплуатации по всему миру.
- Для 2G этот процесс уже наполовину пройден: за последние 4 года крупнейшие сотовые операторы США прекратили поддержку сетей второго поколения либо планируют сделать это до конца 2022 г.; похожая ситуация наблюдается в КНР и большей части стран Юго-Восточной Азии³⁵.
- В Европе прекращение поддержки 2G запланировано на 2025 г., 3G – на 2030 г.³⁶

«Высвободившиеся» подключения устройств IoT перераспределяются по различным технологиям связи. Для многих устройств, подключенных к сетям 2G и 3G, таких как датчики потребления коммунальных ресурсов, датчики и сенсоры в точном земледелии, умном доме и прочее, не нужна высокая скорость и малая задержка сигнала, а тарифы

4G и 5G для M2M слишком дороги. В результате уход 2G и 3G с технологической сцены также влечет за собой ускоренную миграцию сервисов IoT на технологии узкополосных энергоэффективных сетей LPWAN и дает дополнительный толчок к развитию этой ниши.

Кроме того, «глобальный закат» 2G и 3G в IoT в сочетании с растущим спросом на «критический» IoT укрепляет позиции сетей сотовой связи следующих поколений – 4G/LTE и 5G.

- На начало 2022 г. на 4G приходится наибольшая доля подключений устройств IoT среди всех поколений широкополосной сотовой связи (от 61 до 68,5 %, или от 0,83 до 1,15 млрд подключений)³⁷.
- В будущем количество подключений на базе 4G заметно вырастет и составит от 1,58 до 2,0 млрд к 2027 г., а их доля в широкополосных сотовых подключениях устройств IoT увеличится до 74–81 %.
- Таким образом, в среднесрочной перспективе 4G/LTE будет обеспечивать подавляющее большинство широкополосных сотовых подключений устройств IoT.

На сегодняшний день технические характеристики связи 4G/LTE (скорость до 500 Мб/с, задержка сигнала порядка 50 мс, радиус действия до 15 км на открытой местности для LTE-Advanced Pro) закрывают потребности большинства применений IoT. В сочетании с широким проникновением и охватом сетей 4G почти во всем мире это делает связь четвертого поколения наиболее востребованной технологией для широкополосных M2M-подключений.

- При этом даже обновленные стандарты LTE-A Pro в полной мере не закрывают потребности применений промышленного IoT для критически важных процессов по допустимой задержке сигнала и качеству обслуживания.
- Возможности LTE для промышленного IoT могут быть использованы по максимуму в частных сетях, где территория и количество подключений ограничены, а конфигурация сети может быть упрощена.
- Наконец, при всех своих достоинствах широкополосная связь LTE для IoT не отличается экономичностью в энергопотреблении и тарифах.

В результате основную конкуренцию для IoT на базе широкополосной связи 4G/LTE сегодня составляют две технологии:

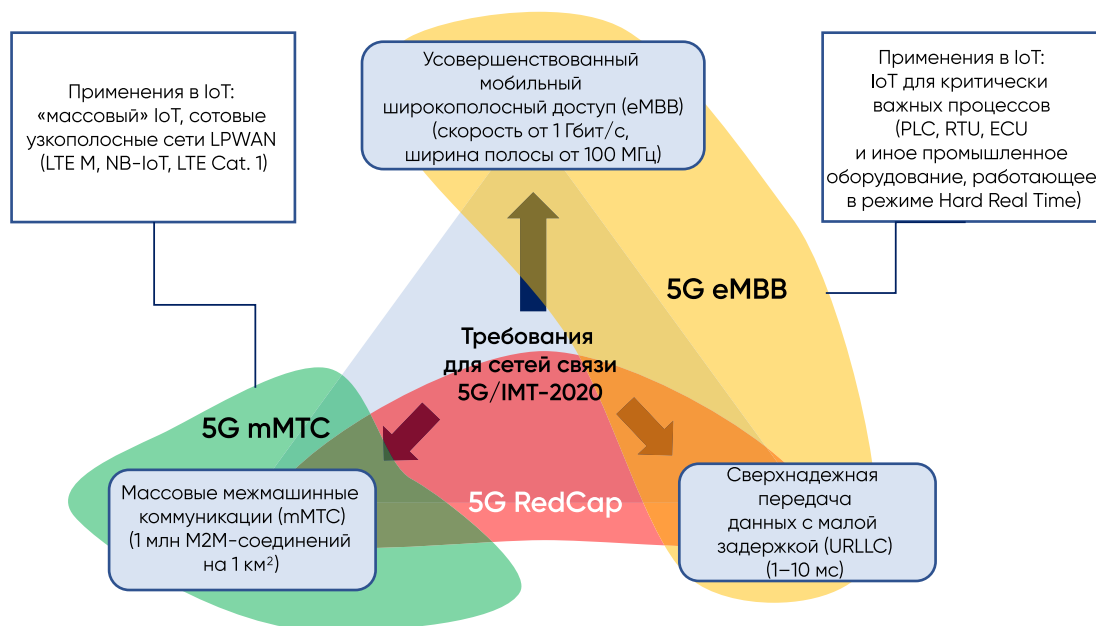
- Узкополосные сети LPWAN, адаптированные для поддержки массовых M2M-взаимодействий, энергоэффективные и экономичные.
- Высокоскоростная связь с низкими задержками 5G, способная гарантированно закрывать потребности IoT для критически важных процессов в промышленных применениях.

«Эпоха 4G» в широкополосном сотовом IoT продлится примерно до 2030–2033 гг., когда рост потребностей промышленного и автотранспортного IoT в сверхнадежной и сверхбыстрой связи выведет на первое место технологию 5G.

Технология 5G включает в себя различные сценарии применения, которые могут быть реализованы на одной сети, но качественно отличаются характеристиками. Такие сценарии объединяются как минимум в три крупные категории, которые развиваются в нише IoT с различной динамикой:

1. Сценарии применения 5G, соответствующие установленным МСЭ³⁸ критериям 5G в части расширенного широкополосного доступа (extended Mobile Broadband, eMBB) и сверхнадежной передачи данных с малой задержкой (Ultra-Reliable Low Latency Communications, URLLC). Такие сети связи 5G обеспечивают скорость передачи данных более 1 Гбит/с и задержку не более 2–10 мс. Иногда для этой категории используется обозначение **5G eMBB/URLLC**. Такие технологии наиболее востребованы для систем IoT жесткого реального времени (Hard Real Time), таких как управление подключенным автомобилем, робототехника для хирургических операций и отдельные виды подключенных систем непрерывного производства, передача мультимедийного контента высокого разрешения через сервисы VR/XR.
2. Сценарии применения 5G, соответствующие критериям МСЭ в части поддержки массового межмашинного взаимодействия (Massive Machine-Type Communication, mMTC), – **5G mMTC**. В этом направлении развиваются сотовые LPWAN, которые будут рассмотрены в следующем разделе.
3. Сценарии применения, в полной мере не соответствующие ни одному из критериев МСЭ, но соответствующие критериям 3GPP для связи 5G с ограниченными возможностями (5G Reduced Capability, **5G RedCap**)³⁹ для подключения промышленных беспроводных сенсоров, носимых устройств, систем видеонаблюдения и ряда других применений.

Соответствие различных сценариев применения связи 5G требованиям для сетей связи IMT-2020 и их применения в IoT



Широкополосное соединение используется в сценариях 5G eMBB и, с оговорками, 5G с ограниченными возможностями (5G RedCap). В свою очередь, сценарий поддержки массовых межмашинных взаимодействий (5G mMTC) применяется в узкополосных энергоэффективных сетях (LPWAN).

- На сегодняшний день число подключений IoT на базе 5G eMBB/RedCap в целом по миру незначительно и составляет порядка 15–25 млн⁴⁰. К 2027 г. нишу IoT на базе широкополосной связи 5G ожидает десятикратный рост (150–200 млн подключений)⁴¹.
- Основные сценарии применения широкополосной связи 5G в IOT – развертывание частных сетей индустриального IoT, развитие систем видеонаблюдения высокого разрешения и подключение высокоавтономных автомобилей. Прогнозы по рынку подключенных автомобилей предполагают 19,087 млн установленных модулей связи 5G в 2023 г., или 39 % от всех поставок модулей 5G для IoT⁴².
- По оценке McKinsey, продажи устройств индустриального IoT с модулями связи 5G вырастут с 1,2 млн в 2022 г. до 22,3 млн в 2030 г.⁴³
- Суммарная выручка поставщиков решений 5G eMBB для сервисов IoT к 2028 г. оценивается в 4,92 млрд долл. США⁴⁴.

При этом до сих пор внедрение 5G eMBB в IoT движется медленнее, чем это ожидалось изначально. Основные факторы, которые сдерживают перевод сервисов IoT на связь 5G, – высокая стоимость внедрения, сложность технической поддержки и неуверенность в ее надежной работе на этапах внедрения и эксплуатации. Однако мощным драйвером развития сервисов, связанных с eMBB, являются более эффективное использование радиочастотного спектра и, как следствие, возможность обеспечить лучшие характеристики услуг связи, включая QoS, количество обслуживаемых абонентов и емкость сетей.

Технологии 5G развиваются на базе предыдущего поколения сотовой связи и поэтапно внедряются в существующую инфраструктуру коммерческих сетей:

1. На сегодняшний день большинство подключений IoT на базе технологий связи пятого поколения обеспечивают так называемые неавтономные сети 5G (non-standalone 5G, 5G NSA). Такие сети развернуты на базе инфраструктуры сетей 4G/LTE и совмещают два ядра – ядро сети четвертого поколения (4G/LTE Evolved Packet Core, EPC) и ядро сети пятого поколения (5G Core, 5GC), а также технологии сети радиодоступа (RAN) двух поколений⁴⁵.
2. Параллельно развиваются технологии автономной сети 5G, которая должна в полной мере соответствовать всем трем сценариям применения (eMBB, URRLC и mMTC) и не использовать инфраструктуру 4G/LTE. Именно такие сети наилучшим образом отвечают потребностям «критического» IoT, включая M2M-системы жесткого реального времени (Hard Real Time IoT, HRT-IoT), такие как медицинские роботы, беспилотный транспорт, прецизионные операции в непрерывных производствах и прочее.

На октябрь 2021 г. из 176 коммерческих сетей 5G в мире 163 сети, или более 90 %, были развернуты в неавтономной архитектуре (NSA)⁴⁶. Соответственно, на сети 5G NSA приходится более 95 % подключений IoT на базе сотовой связи пятого поколения.

Однако в 2022 г. темпы развертывания автономных сетей 5G существенно ускорились. По оценке Ericsson, к ноябрю 2022 г. в мире были развернуты не менее 35 таких сетей⁴⁷. Ожидается, что к концу года число достигнет 40, при этом половину будут составлять сети общего доступа, а оставшуюся половину – частные сети (private 5G networks)⁴⁸.

На сегодняшний день и в горизонте ближайших трех лет технические возможности неавтономных сетей 5G закрывают потребности подавляющего большинства применений IoT. Более того, дальнейшая цифровая трансформация отраслей и расширение применения сервисов «реального времени» лишь увеличит спрос на IoT на базе связи пятого поколения. Один из ярких примеров – тенденции развития автоиндустрии и авторынка:

- Потребность рынка IoT в автономных сетях 5G будет плавно расти по мере развития беспилотного транспорта высокой степени автономности (L3–L5) и массового внедрения робототехники для медицинских, логистических и промышленных применений в жестком реальном времени.
- Кроме того, уже на текущем уровне развития массового рынка подключенных автомобилей (уровни автономности L1–L2) протоколы высокоскоростной беспроводной связи широко используются для обеспечения функций автопилота и вождения с поддержкой ИИ (AI-assisted driving).
- В ближайшие годы связь 5G окончательно закрепит за собой доминирующий статус в этой нише, вытеснив с рынка LTE и альтернативные протоколы.

В последние годы одним из драйверов роста промышленных применений IoT на базе LTE и 5G становятся частные промышленные сети (private LTE/5G networks, pLTE/5G). Такие сети чаще всего организуются для того, чтобы обеспечивать управление цифровой инфраструктурой крупных промышленных объектов. Частные сети могут обслуживаться операторами связи или собственниками объектов самостоятельно, с технической поддержкой поставщиков сетевого оборудования.

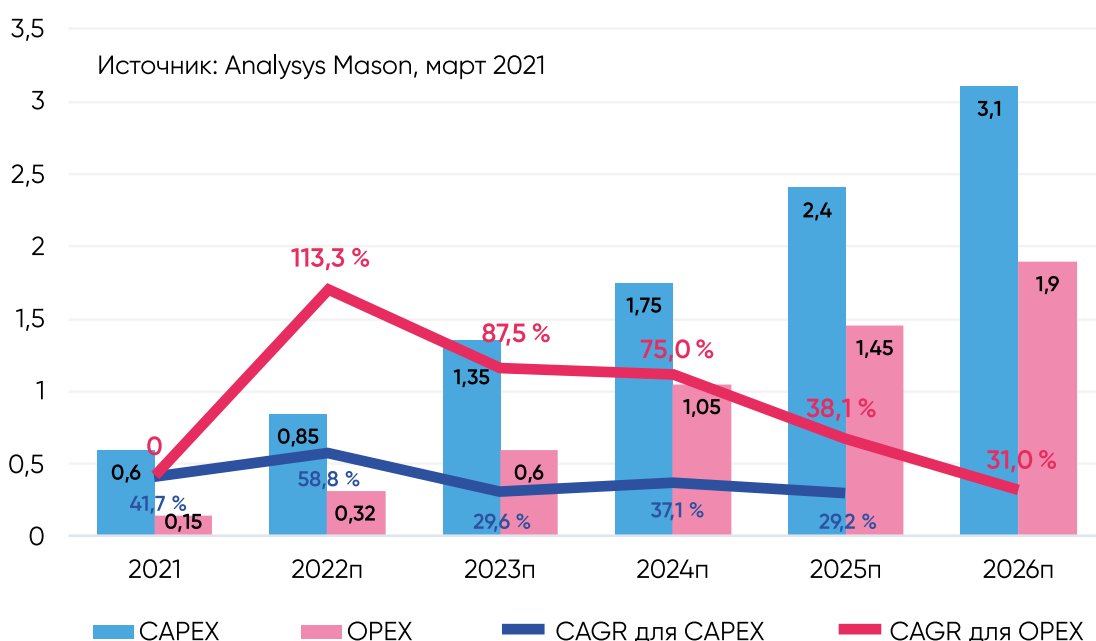
На конец 2022 г. в мире в различных стадиях реализации находились не менее 955 проектов частных сетей сотовой связи⁴⁹. На сегодня этот рынок характеризует быстрый рост и концентрация большей части проектов вокруг нескольких ключевых отраслей, а также опережающий прежние прогнозы рост доли технологии 5G⁵⁰:

- География проектов частных сетей LTE/5G существенно расширилась за последние 3 года и охватывает уже 72 страны.
- В третьем квартале 2022 г. рынок частных сетей продемонстрировал рекордный рост – число проектов выросло на 66, или примерно на 7 % к прошлому кварталу.
- Три ведущих сектора по числу и капитализации проектов внедрения частных сетей – горнодобывающее производство, оборонно-промышленный комплекс и обрабатывающая промышленность.
- В 57 % из всех проектов, включая как уже реализованные, так и недавно запущенные, используется только связь LTE, в 18 % – совместно LTE и 5G, в 23 % – только связь пятого поколения.⁵¹
- При этом из 214 проектов, анонсированных в 2022 г., связь 5G планируется использовать – совместно с LTE либо эксклюзивно – уже в 55 % случаев.

По прогнозам, до 2026 г. общее число частных сетей LTE/5G должно вырасти более чем в 10 раз и достичь 13,5 тыс.⁵² Таким образом, ежегодный рост этого сегмента по количеству сетей будет превышать 55 %.

- Сети pLTE/5G наиболее распространены на объектах обрабатывающих производств (28 %), транспортной и логистической инфраструктуры (15 %), энергогенерации и горнодобывающих производств (13 %)⁵³.
- Инвестиции промышленных предприятий и других бизнес-субъектов в частные сети многократно увеличатся в ближайшие годы. По консервативным оценкам, общие расходы на сети pLTE/5G с 2021 по 2026 г. вырастут в 6,5 раза и достигнут 5 млрд долл. США⁵⁴. Другие источники прогнозируют только сегменту pLTE рост до 16,7 млрд долл. США к 2025 г.⁵⁵

Расходы на внедрение и эксплуатацию частных сетей LTE и 5G (в \$ млрд)

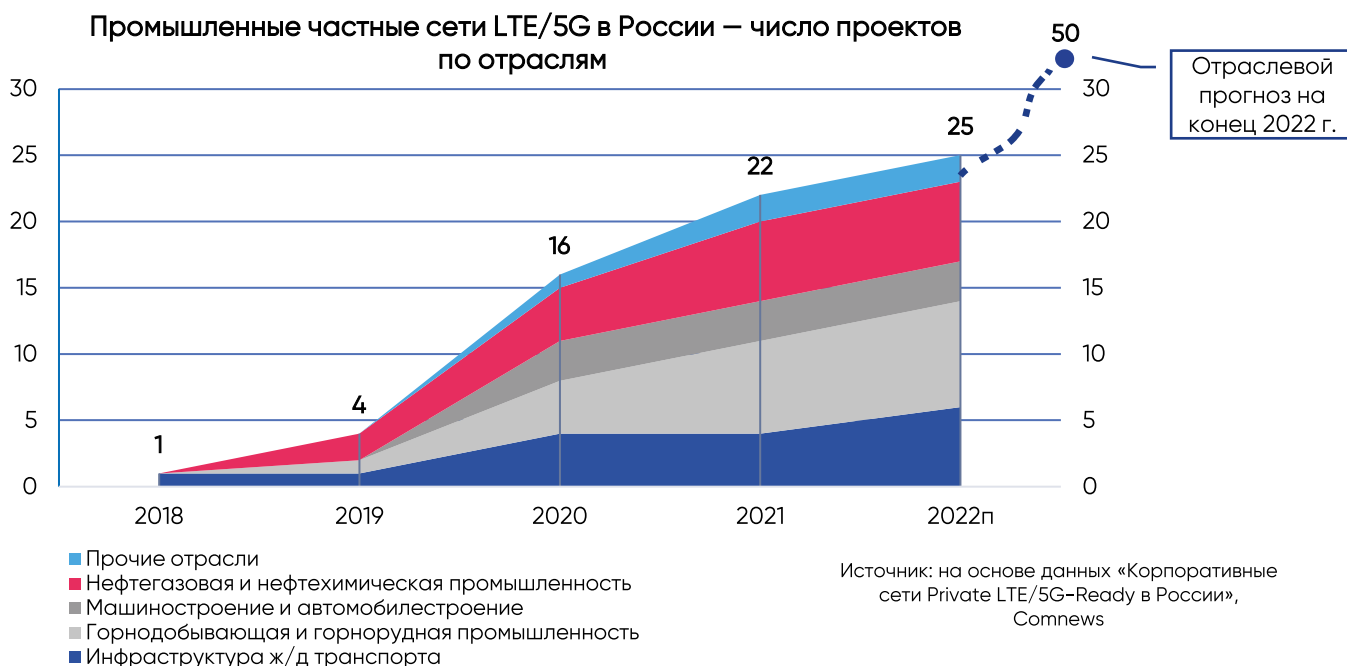


Индустриальные применения IoT служат главным драйвером внедрения частных сетей LTE и 5G. Традиционные способы организации беспроводных подключений на территории промышленных объектов, такие как Wi-Fi, сотовые сети общего доступа и прочее, все чаще оказываются недостаточны для растущего числа промышленных датчиков, сенсоров, систем видеонаблюдения и промышленной робототехники. Необходимость обеспечивать нужное качество сервиса (QoS) для большого числа устройств IoT с высокой плотностью размещения на таких объектах, как горнорудные шахты, карьеры, сборочные цеха, конвейерные линии, ж/д станции, толкает их операторов к развертыванию собственных частных сетей.

Общемировой тренд начал проявляться и в России – с 2018 г. количество проектов частных промышленных сетей LTE и 5G выросло почти с нуля до 22 в 2021 г.⁵⁶ По прогнозам участников рынка, по итогу 2022 г. общее число проектов в разных стадиях реализации может превысить 50, а к 2025 г. объем российского рынка сетей pLTE/5G достигнет 8,3 млрд руб.⁵⁷

- Ключевые ниши внедрения частных сетей в России в целом совпадают с мировой практикой – это горнодобывающая отрасль, ж/д транспорт и нефтегазовая промышленность, а также различные подотрасли машиностроения.

- Пока внедрение сетей рLTE/5G и количество подключений IoT, которые они обеспечивают, невелики в масштабах национального рынка. Но если темпы роста последних 4 лет сохранятся, к 2025–2027 гг. этот сегмент может стать одним из ведущих факторов развития индустриального IoT в стране.



Однако актуальные события могут затормозить тренд на ускоренное развитие частных сетей в российской промышленности и транспортной отрасли. В текущих условиях предприятия будут рассматривать следующий вариант: отказаться от дорогостоящих проектов частных сетей и пожертвовать качеством связи на своих объектах. В свою очередь, такой сценарий замедлит внедрение и модернизацию индустриальных сервисов IoT.

В этих условиях актуальна разработка точечных мер государственной поддержки для реализации проектов частных сетей на объектах промышленных производств. Во-первых, такие меры будут стимулировать развитие сразу двух технологических областей – индустриального IoT и перспективных технологий беспроводной связи. Во-вторых, развертывание частных сетей органично укладывается в повестку цифровой трансформации промышленных предприятий, которая предусмотрена действующими механизмами поддержки, в том числе по линии Минпромторга.

На нынешнем этапе развития российского рынка сетей рLTE/5G приоритетной задачей представляется поддержка не разработчиков решений, а предприятий-заказчиков, которые внедряют частные сети и сервисы индустриального IoT на их базе. По экспертным оценкам, включая собственные оценки АНО «Цифровая экономика», общее число объектов транспортно-логистической и производственной инфраструктуры в России, для которых могут быть востребованы решения на базе частных сотовых сетей в горизонте 5 лет, составляет от 450 до 700 в сумме по всем отраслям. Таким образом, сегодня подобными проектами охвачено от 7 до 11 % рынка.

При этом ряд поставщиков решений рLTE/5G и сервисов индустриального IoT, включая сотовых операторов «большой четверки», группу компаний «Цифра» и др., уже сформировали багаж компетенций для реализации таких проектов «под ключ». В результате относительная зрелость российского рынка выше со стороны поставщиков, чем со стороны потенциальных заказчиков, именно поэтому механизмы государственной поддержки имеет смысл фокусировать на последних.

От первого лица



Алексей Кузнецов,
руководитель
департамента
по работе
с федеральными
государственными
структурами,
ПАО «Вымпелком»

Цифровая трансформация отраслей промышленности и экономики сегодня плотно завязана на решения на стыке различных цифровых технологий. Одной из самых перспективных для российского рынка выглядит технологическая связка индустриального интернета вещей и современных сервисов мобильной связи. Сервисы IoT для предприятий, логистических хабов и площадок добычи полезных ископаемых все чаще развертываются на базе широкополосной связи LTE, в том числе в формате частных промышленных сетей, обеспечивающих бесшовную, высоконадежную и защищенную передачу данных во внутреннем контуре предприятия.

Возможности для быстрого роста российского рынка сохраняются и в нынешних условиях технологических санкций и ограничений. Российскими операторами связи, включая ПАО «Вымпелком», накоплен серьезный комплексный опыт внедрения частной промышленной связи LTE у заказчиков в самых разных отраслях – от нефтегазодобычи до автомобилестроения. Эти проекты зачастую реализуются в партнерстве с другими отечественными игроками, сформировавшими обширный портфель компетенций в развитии отраслевых платформенных сервисов промышленного IoT.

С завершением разработки и полноценным выводом на рынок отечественного оборудования LTE в ближайшие годы технологическая связка «мобильная связь + индустриальный IoT» окончательно окажется замкнута на отечественные решения и продукты, что позволит ей развиваться без оглядки на санкционные ограничения и международную турбулентность. На горизонте этого процесса в 2025 г. и позже – переход к решениям на базе 5G, определяющим долгосрочное будущее как мобильной связи, так и сервисов промышленного IoT. Исходя из этой долгосрочной перспективы, ПАО «Вымпелком» делает серьезную ставку на лидерство на российском рынке проектов «LTE + индустриальный IoT» и активно сотрудничает с другими компаниями и заинтересованными сторонами, включая АНО «Цифровая экономика».

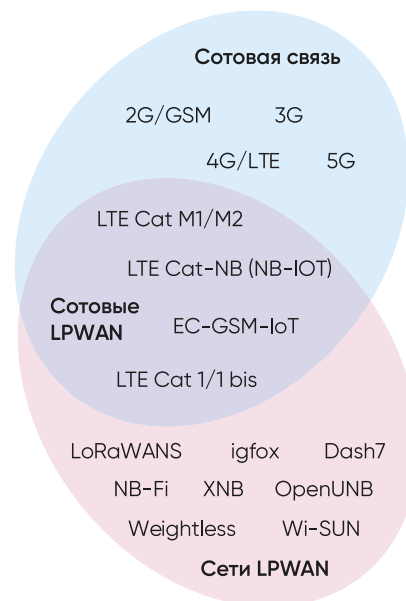
Конкретным механизмом такой поддержки может быть целевое субсидирование проектов российских промышленных предприятий по развертыванию частных сетей LTE и сервисов индустриального IoT на их базе. При этом одним из условий субсидирования должно стать построение частной сети на базе отечественного телекоммуникационного оборудования, соответствующего критериям ТОРП (включая базовую станцию LTE).

- На первом этапе (до конца 2023 г.) в зависимости от объема рыночного спроса на решения частных промышленных сетей LTE/5G-ready возможна поддержка их внедрения на базе имеющегося оборудования, в том числе базовых станций зарубежного производства.
- Ожидается, что российские производители оборудования для частных сетей LTE смогут перейти от тестирования и опытной эксплуатации базовых станций LTE к их мелко- и среднесерийному выводу на рынок во второй половине 2023 г. либо к началу 2024 г. С учетом этого целевого горизонта с 2024 г. предоставление поддержки может быть привязано к внедрению частных сетей на базе отечественного оборудования.
- По мере формирования российскими производителями ПО и оборудования технологического задела в технологиях сотовой связи пятого поколения, с 2025/2026 гг. в программу может быть включено субсидирование сервисов индустриального IoT поверх частной сети на базе отечественного оборудования 5G.

При этом ключевой вызов как для технологий LTE, так и для сотовой связи пятого поколения – вывод на коммерческий рынок именно оборудования (в том числе базовые станции), сопоставимого с зарубежными аналогами и совместимого с действующими сетями операторов. В сегменте программного обеспечения российские разработчики (прежде всего НТЦ «Протей») уже имеют работоспособные и готовые к промышленному внедрению продукты для ядра сети LTE; определенный задел также сформирован в нише ПО для сетей 5G, в том числе в рамках разработок НТЦ «Протей», Сколтеха и других разработчиков.

Узкополосные сети дальнего радиуса действия (LPWAN)

- Сети LPWAN продолжают активно развиваться в рамках двух ниш, различающихся по используемой базовой технологии беспроводной связи. Часть сетей LPWAN основаны на технологии сотовой связи либо развертываются поверх нее и, по сути, представляют собой разновидность «наложенной» сети. К этой категории относятся стандартизированные консорциумом 3GPP технологии NB-IoT (LTE Cat-NB), EC-GSM-IoT, eMTC (LTE Cat M1/M2) и LTE Cat 1 / Cat 1 bis. Узкополосные сети на базе сотовой связи представляют собой «побочную ветку» развития технологий 4G/LTE, запрос на которую возник в связи с ростом применений IoT и потребности в сетях связи с поддержкой массовых M2M-взаимодействий (mMTC). Таким образом, сегмент сотовых узкополосных сетей одновременно относится к технологиям сотовой связи и к LPWAN.
- Вторая группа LPWAN, напротив, не основана на сотовой сети и поэтому рассматривается как отдельный сегмент. Несотовые сети LPWAN используют полосы частот в нелицензируемых диапазонах, в отличие от сотовых узкополосных сетей, и включают такие технологии, как LoRa, SigFox, Weightless, RPMA, DASH7 и российские протоколы NB-Fi, GoodWan/OpenUNB, XNB.



Несмотря на различия в базовой технологии передачи данных, основные свойства сетей LPWAN остаются общими для обеих категорий:

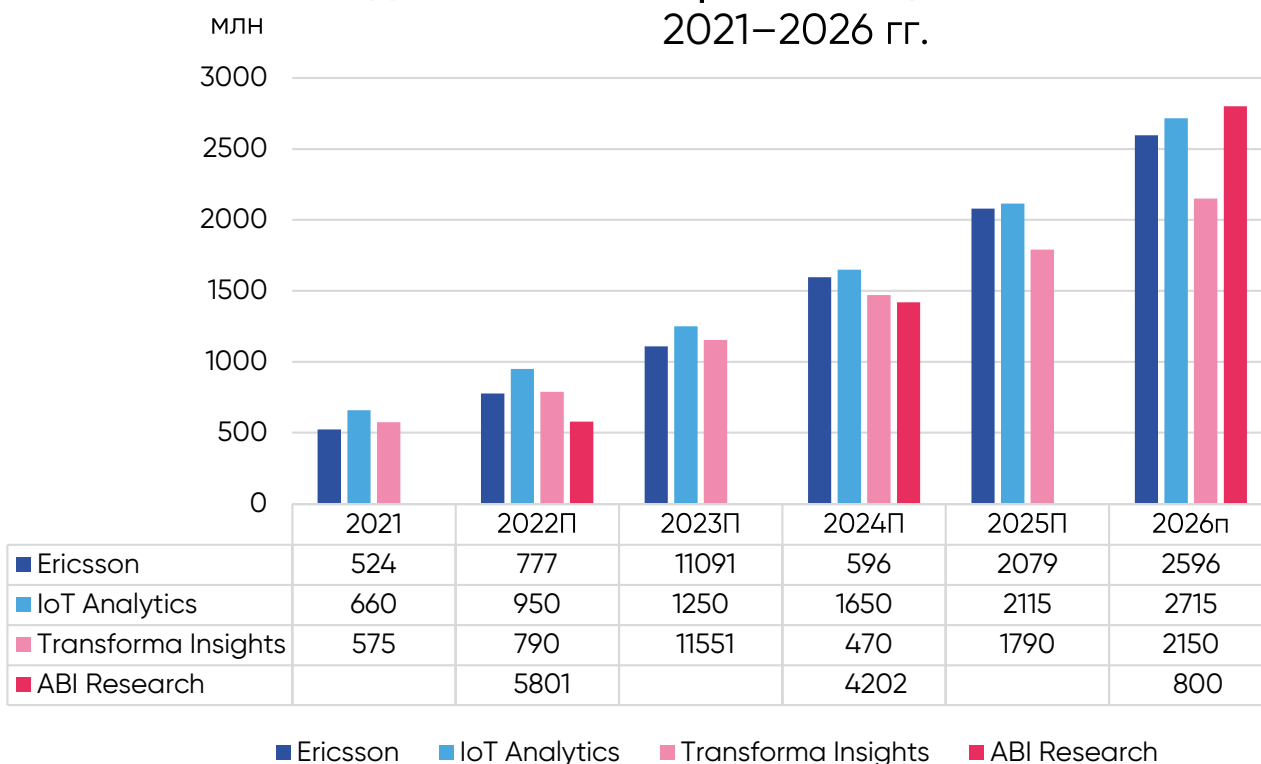
1. Большой радиус действия (до 2–5 км в городе, до 10 км и более на открытой местности).
2. Поддержка массовых M2M-взаимодействий (mMTC), то есть обмена данными большого числа устройств IoT с высокой плотностью их размещения в сети.
3. Низкая скорость передачи данных (от единиц бит до сотен килобит в секунду), которой достаточно для приема «легких» данных межмашинной телеметрии от простых устройств.
4. Экстремально низкое энергопотребление, способное продлевать срок жизни устройств IoT со встроенной батареей до 10 лет и более.

Основным драйвером развития узкополосных сетей выступает растущий запрос на «массовый» IoT (massive IoT) с поддержкой mMTC. В этот сценарий укладывается массовое использование датчиков и сенсоров на промышленных и складских

объектах, в носимых пользовательских устройствах, ритейле, контроле автотранспорта и т. п. Все больше сервисов, ранее использовавших для этих целей инфраструктуру сетей связи 2G и 3G, мигрируют на технологии 4G и LTE для IoT. На 2022 г. развитие сетей LPWAN окончательно закрепилось в качестве магистрального тренда среди технологий связи дальнего радиуса действия для IoT:

- В 2021 г. в мире к сетям LPWAN было подключено, по разным оценкам, от 524 до 660 млн устройств IoT, что составляло всего от 24,5 до 31 % всех подключений IoT дальнего радиуса действия с учетом сотовой связи.
- Прогнозы от различных источников сходятся в том, что в 2026 г. доля LPWAN в подключениях IoT по сетям дальнего радиуса действия превысит 50 %, достигнув от 2,596 до 2,800 млрд. Таким образом, сети LPWAN обойдут все вместе взятые поколения широкополосной сотовой связи, включая широкополосную 5G, по числу подключений IoT.
- Среднегодовой темп роста подключений LPWAN на временном промежутке с 2022 по 2026 г. не будет опускаться ниже 25 %. Эта цифра особенно впечатляет, потому что она скорректирована с учетом последствий пандемии COVID-19; «доковидные» прогнозы предполагали еще более высокие темпы роста.

Подключения интернета вещей в сетях LPWAN 2021–2026 гг.



Помимо роста числа подключений и «количественного» измерения рынка, быстрыми темпами растет «зрелость» технологий LPWAN:

- Наиболее широко используемые технологии (NB-IoT, LTE M, LoRaWAN, SigFox) эволюционируют в сторону вертикально интегрированных технологических экосистем для IoT. Такие экосистемы охватывают уровни от электронных компонентов и оборудования (чипы и модули, базовые станции, антенны) до пользовательских приложений, интерфейсов и сервисов M2M-аналитики. По

сути, на сегодняшний день имеет смысл говорить не столько о сетях связи LPWAN для IoT, сколько о технологических платформах на базе узкополосной связи LPWAN.

- Вокруг интегрированных экосистем LPWAN сложились технологические альянсы, куда вступает все больше крупнейших игроков отрасли связи (Ericsson, Orange, Vodafone, Tata Communications), ИТ (Intel, Microsoft), онлайн-коммерции (Alibaba, Amazon), производителей оборудования и полупроводников (Arduino, Huawei, NXP, Semtech) и так далее.
- Параллельно растет число проектов внедрения интегрированных решений на базе LPWAN в вертикальных секторах экономики. За 2020–2021 гг. наибольшая доля таких проектов была реализована прежде всего в нише бытовых и промышленных умных счетчиков, в точном земледелии, ТЭК и секторе энергораспределения.
- За 2020–2021 гг. резко выросло число крупных проектов по развертыванию инфраструктуры LPWAN, вплоть до обеспечения практически полного покрытия на национальном уровне в крупных странах, например внедрение NB-IoT в КНР.

Кроме того, в последние 2–3 года по мере роста ниши LPWAN на рынке обостряется конкуренция сразу по двум направлениям:

- между сотовыми и несотовыми узкополосными сетями;
- между различными протоколами и основанными на них продуктовыми и сервисными линейками внутри каждой из этих технологий.

Конкуренция узкополосных сетей с широкополосной сотовой связью развивается в пользу LPWAN и является главной движущей силой снижения доли 2G и 3G в подключениях IoT. Если в 2020–2021 гг. ежегодное снижение числа подключений IoT в сетях 2G/3G не превышало 3–4 %, то к 2024 г. оно может достичь 8 %, или 40–45 млн подключений в год⁵⁸. Большинство выпадающих подключений будут «поглощены» рынком LPWAN.

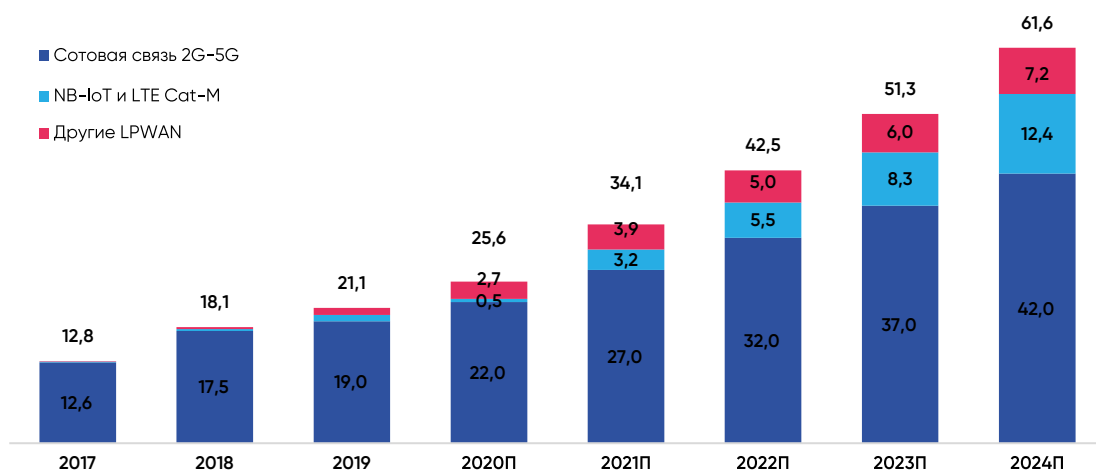
- Внутренняя конкуренция между сотовыми и несотовыми узкополосными сетями на национальных рынках все чаще ведет к доминированию одной из ниш LPWAN и одной-двух конкретных технологий. КНР с 2019 г. сделала тотальную ставку на сотовый протокол NB-IoT, на долю которого теперь приходится более 95 % внутреннего китайского рынка узкополосных сетей интернета вещей и порядка 75–80 % мирового. Напротив, во Франции в 2021 г. более чем в 60 % новых проектов IoT использовались несотовые узкополосные сети (LoRaWAN и Sigfox).
- На 2022 г. сотовые LPWAN занимают большую долю рынка по числу подключений IoT – от 475 до 544 млн против 250–285 млн у несотовых LPWAN⁵⁹. Прогнозы даже на среднесрочную перспективу отличаются большим разбросом значений, однако большинство участников рынка и аналитических компаний предсказывают, что при быстром росте всех видов узкополосных сетей IoT лидерство удержат за собой сотовые LPWAN:
 - Вендоры оборудования сотовой связи наиболее скептически к перспективам конкурирующей несотовой технологии: по прогнозам Ericsson, на 2026 г. в мире будет насчитываться 2214 млн подключений сотовых LPWAN против 382 млн несотовых⁶⁰.

- «Нейтральные» аналитические обзоры (Transforma Insights) к тому же году предсказывают 1365 млн подключений к сотовым LPWAN против 785 млн несотовых подключений⁶¹.
- Наконец, вендоры оборудования для LoRaWAN еще недавно исходили из обратной оценки: в исследовании Semtech и ABI Research прогнозировалось, что к 2026 г. несотовые LPWAN получат 1,3 млрд подключений (против 1,5 млрд. у сотовых узкополосных сетей). Однако на 2022 г. этот прогноз является устаревшим и радикально оптимистичным для несотовых сетей.

Российский рынок существенно выбивается из общемирового темпа. На 2021 г. все виды LPWAN обеспечивали не более 21 % подключений IoT из технологий с дальним радиусом действия, почти в 4 раза уступая сотовой связи 2G–4G. К 2024 г. этот разрыв должен был сократиться, позволив LPWAN занять до 32 % рынка.

Важно отметить, что телекоммуникационная составляющая несотовых LPWAN полностью погружена в стоимость проекта автоматизации либо в цену подключенного устройства на весь его жизненный цикл (например, приборы учета). В свою очередь, в проектах IoT сотовых операторов долгое время доминировала традиционная бизнес-модель на основе показателя ARPU⁶², применяемая при развитии сетей связи 2G–4G. Такой подход мог существенно замедлять развитие отечественного рынка Интернета вещей, поскольку сервисы на базе «умных» устройств чаще всего не могут обеспечить высокий показатель в его метрике. Переход российских сотовых операторов к сервисной модели в части IoT стартовал в последние несколько лет. Этот процесс набирает силу по мере того, как лидеры операторского рынка все чаще ориентируются на экосистемную модель развития и формируют собственные линейки цифровых сервисов, оборудования и инфраструктуры для них.

Структура подключений IoT по технологиям WAN в России



Источник: [Исследование ПАО «МТС»: IoT Барометр 2021](#)

Однако изменение ситуации после 24 февраля 2022 г. повлекло замораживание ряда проектов развития сетей IoT как в лицензируемом, так и в нелицензируемом спектре.

- Новые прогнозы для российского рынка находятся в процессе оценки. Важнейшим фактором будет влияние санкционных ограничений на инвестиционную политику операторов «большой четверки», которые выступают главной движущей силой развития сотовых LPWAN.

- Санкционная политика в части микроконтроллеров и радиочипов влияет на все российские решения LPWAN – как сотовые, так и несотовые. Перестройка логистических цепочек для поставки таких компонентов занимает время и увеличивает стоимость конечных продуктов. Разработка российских аналогов и насыщение ими домашнего рынка упираются в набор серьезных проблем производства микросхем в среднесрочной либо долгосрочной перспективе.
- В отсутствие новых крупных проектов развитие рынка будет преимущественно сконцентрировано на проектах малого и среднего масштаба (от нескольких сотен до нескольких десятков тысяч подключений). Здесь позитивным фактором будет наличие российских несотовых решений (NB-Fi, Open UNB), работающих в нелицензируемых частотах и возможность получения проектами развития таких сетей целевой господдержки. Еще одна предпосылка для малых и средних проектов связана с наличием уже построенных операторами сотовой связи крупных сетей NB-IoT. Даже в условиях сокращения числа проектов и объема рынка наличие сетевой инфраструктуры оставляет возможности для расширения ее «полезной нагрузки» по мере развития линейки российских оконечных устройств IoT, в том числе в сегментах «умного дома», «умного здания» и ЖКХ.
- В краткосрочной перспективе развитие LPWAN в России оказывается замкнуто на два источника роста:
 - Малые и средние проекты на базе как сотовых, так и несотовых технологий. Приоритетом станут краткосрочные низкобюджетные проекты, обеспечивающие быстрые изменения на рынке в условиях санкций и ограничения доступа к зарубежным технологиям.
 - Крупные проекты с госучастием, которые могут обеспечить базовую инфраструктуру для развертывания сетей LPWAN в федеральном масштабе. Такие проекты могут возникнуть в рамках программ цифровизации ЖКХ, транспортной инфраструктуры и энергосетей. Ускорить их реализацию может развитие нормативно-правовой базы, расширяющей принципы № 522-ФЗ от 27.12.2018 с интеллектуальных приборов учета электроэнергии на другие системы учета коммунальных ресурсов.
- Чтобы стимулировать спрос и не дать негативным трендам закрепиться, должны быть разработаны новые масштабные меры господдержки, учитывающие новые вводные и отражающие приоритеты отраслевого развития в новых условиях.

Узкополосные сети на базе сотовой связи: КНР определяет развитие рынка?

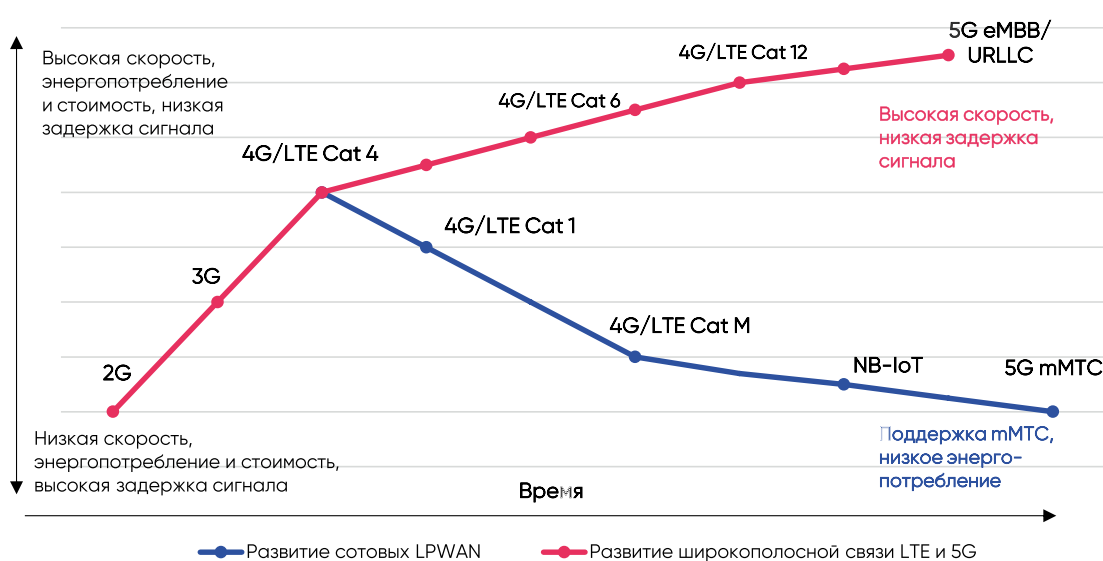
Как отмечалось выше, сотовые LPWAN – это выделившееся из магистрального развития широкополосной сотовой связи побочное направление, полностью адаптированное под потребности M2M-коммуникаций. Развитие сотовых LPWAN началось с 8-го релиза (выпуска) стандартов LTE от 3GPP, принятого в 2008 г. Описанная в релизе

спецификация LTE Cat 1 стала первым шагом «в сторону» от дальнейшего наращивания ширины полос, пропускной способности и скорости, а также уменьшения задержки сигнала в технологиях LTE⁶³.

Дальнейшее развитие спецификации LTE для M2M-взаимодействий получили в 2016–2017 гг. в релизах 13 и 14 3GPP. На сегодняшний день спектр технологий сотовых LPWAN включает в себя⁶⁴:

1. **LTE Cat 1 и Cat 1 bis:** первая версия стандарта LTE, адаптированная под M2M, и ее модернизированный вариант. Отличается от предыдущей версии широкополосной LTE Cat 4 меньшей скоростью и пропускной способностью, сниженной стоимостью и энергопотреблением. На сегодняшний день Cat 1 и Cat 1 bis менее популярны и реже используются для развертывания сетей IoT, чем их более поздние «родственники».

Развитие технологий LPWAN на базе сотовой связи



2. **EC-GSM-IoT (Extended Coverage GSM for IoT)** – M2M-адаптация одного из самых распространенных стандартов сотовой связи GSM, которую можно разворачивать поверх GSM-сети. Такая особенность должна была сделать EC-GSM-IoT оптимальным вариантом для перехода с сотовой связи 2G/3G в сетях IoT, но после первых тестовых запусков сетей в 2017–2018 гг. технология не получила широкого распространения.

3. Группа стандартов **LTE M** (LTE для машинных взаимодействий), из которой на сегодняшний день широко используются спецификации **LTE Cat M1** и **Cat M2**. Это необычная технология даже по меркам своей ниши – самая широкополосная и быстрая среди сотовых LPWAN (скорость до 7 Мбит/с, задержка сигнала не более 15 мс, ширина полос до 5 МГц у Cat M2)⁶⁵. В сочетании с поддержкой массовых M2M-взаимодействий такие характеристики позволяют использовать LTE M для применений в системах IoT в реальном времени (RT-IoT), включая управление:

- подключенным транспортом и сельхозтехникой;
- дронами и ИТС;
- системами видеонаблюдения;

- медицинской, логистической и иной робототехникой;
- системами автоматизации зданий в умном городе.

«Слабое место» связи LTE M – ее довольно высокая стоимость и энергопотребление, не рассчитанное на устройства IoT со встроенной батареей.

4. LTE Cat NB 1/NB 2 (Narrow Band IoT, NB-IoT) представляет собой противоположность LTE M: в этой технологии обычный функционал LTE урезан до предела в пользу поддержки M2M. Скорость соединения не превышает 127 кбит/с, задержка может достигать 10 секунд, а ширина рабочих полос составляет всего 180 кГц. При этом NB-IoT имеет низкое энергопотребление и радиус действия более 10 км на открытой местности и может обеспечивать срок жизни более 10 лет устройствам IoT со встроенной батареей. Эти параметры обеспечили широкое применение NB-IoT в нише умных датчиков и интеллектуальных систем учета ЖКХ, а также в сенсорах, применяемых на объектах ТЭК и электросетях. Также технология широко применяется в автопроме, логистике и ритейле, медицине, сельском хозяйстве и нишах умного дома и умного города.

- В сфере энергетики и ЖКХ NB-IoT применяется для удаленного сбора показаний, контроля и управления различными системами, включая мониторинг, реагирование и оповещение при нештатных ситуациях.
- В последние годы одной из наиболее динамично развивающихся ниш внедрения решений на базе NB-IoT становятся системы промышленной безопасности. Датчики, сенсоры и метки, подключенные к сотовой узкополосной сети, используются для контроля сближения объектов на производственных площадках, цифрового учета кадров, соблюдения норм охраны труда, контроля экологической обстановки и уровня вредных выбросов на опасных производствах.

Помимо своих характеристик, сотовые LPWAN имеют еще две особенности, которые во многом определяют их сегодняшнюю траекторию развития на рынке.

A. Совместимость с сотовой связью: NB-IoT, LTE M и другие технологии основаны на сотовой связи и организуются поверх нее как разновидность «наложенной» сети. В некоторых случаях развертывание режима узкополосной сети осуществляется на уровне изменений в программном обеспечении. Сотовые узкополосные сети используют те же типы оборудования, что и широкополосная сотовая связь. Логично, что продвижение технологий сотовых LPWAN во всем мире ведут операторы сотовой связи – от европейских Ericsson, Orange и Vodafone до американских AT&T и Verizon и китайской «большой тройки» (China Mobile, China Telecom и China Unicom).

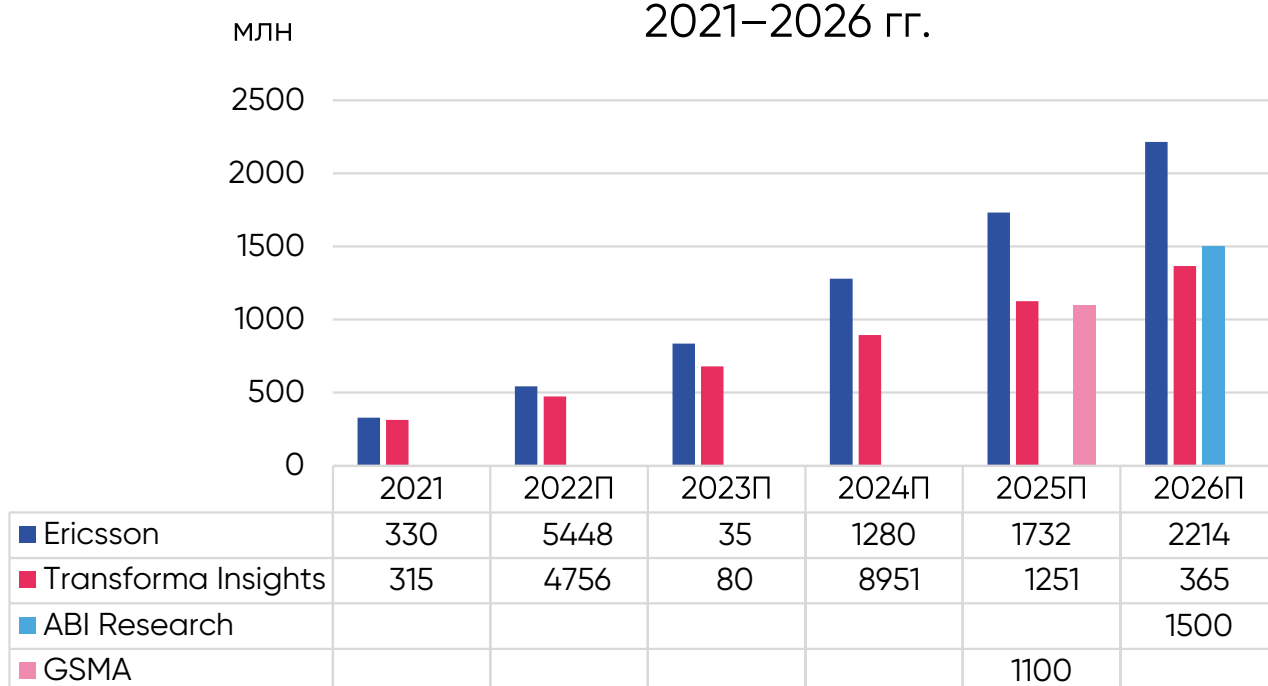
B. Сотовые сети LPWAN активно развиваются в направлении «межмашинной» связи пятого поколения; на 2022 г. обновленные версии NB-IoT и LTE Cat M2 могут рассматриваться в качестве технологий связи 5G.

- Несмотря на несоответствие установленным МСЭ критериям связи 5G в части ширины рабочих полос, скорости и задержки сигнала (критерии eMBB и URLLC), сотовые LPWAN приближаются к 5G⁶⁶ в части поддержки массовых M2M-взаимодействий (mMTC). В этот сценарий применения входит увеличенный радиус покрытия сети, сниженное энергопотребление и поддержка большого количества взаимодействий с высокой плотностью сетевого трафика.

- В итоге сотовые LPWAN могут рассматриваться и сегодня уже рассматриваются рынком в качестве связи 5G с ограниченной функциональностью (**5G RedCap** или **5G mMTC**).
- Ассоциация GSMA еще в 2018 г. заявила⁶⁷, что технологии LTE M и NB-IoT входят в семейство 5G; Huawei⁶⁸ и Ericsson⁶⁹ в своих материалах также рассматривают такие подключения, как 5G mMTC.

Таким образом, на сегодняшний день сотовые LPWAN обеспечивают сотни миллионов подключений IoT, которые рассматриваются многими участниками рынка как подключения 5G. При этом если в 2021 г. на долю узкополосных сотовых сетей приходилось от 315 до 330 млн подключений IoT, то на 2026 г. прогнозы находятся в диапазоне 1,5–2 млрд подключений.

Подключения интернета вещей в сотовых сетях LPWAN 2021–2026 гг.

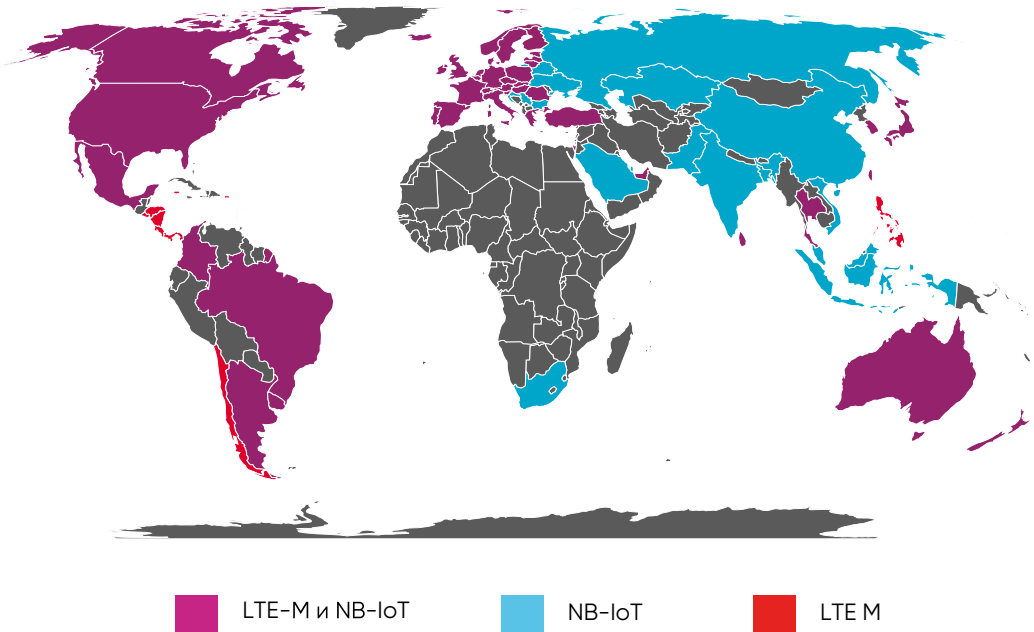


■ Ericsson ■ Transforma Insights ■ ABI Research ■ GSMA

В части коммерческих сетей рынок сотовых LPWAN представлен тремя технологиями: NB-IoT, LTE M и LTE Cat 1/Cat 1 bis.

- На февраль 2022 г. из 170 сетей сотового узкополосного IoT 110 сетей были развернуты на NB-IoT, 60 сетей – на LTE M⁷⁰.
- В большинстве стран Европы, Северной и Южной Америки обе технологии внедряются параллельно, в то время как в Восточной Европе и большинстве стран Азии внедряется NB-IoT.

Преобладающие виды сотовых сетей LPWAN по странам на февраль 2022 г.
(по числу развернутых сетей)

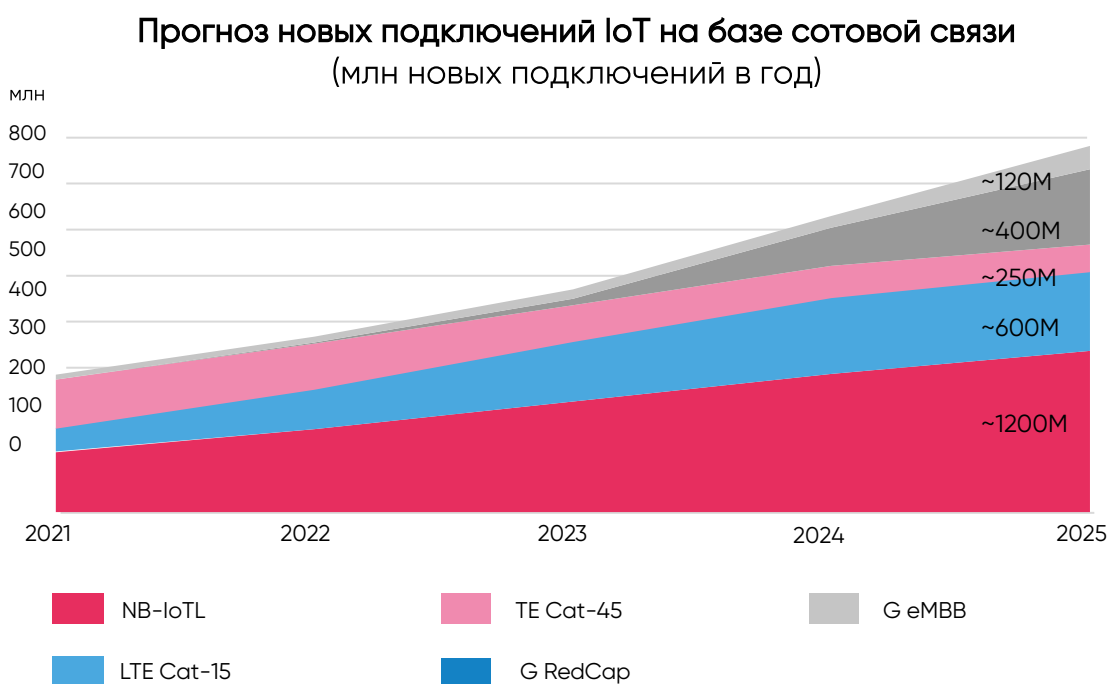


Источник: [IoT Deployment Map, GSMA](#)

Однако количество и география сетей не отражают реальной концентрации рыночной ниши в одной технологии и, более того, на одном национальном рынке – NB-IoT в КНР.

- С 2019 г. «большая тройка» китайских сотовых операторов начала масштабное и почти синхронное развертывание сетей NB-IoT на своей инфраструктуре. В результате уже к 2020 г. КНР обеспечивала порядка 80 % всех подключений NB-IoT в мире⁷¹, а на конец 2021 г. оценки колебались от 76⁷² до 95 %⁷³.
- В середине 2021 г. оператор China Telecom объявил, что число подключений NB-IoT на его инфраструктуре превысило 100 млн, из них 30 млн составили умные газовые счетчики⁷⁴.
- По данным на июль 2021 г., работу в режиме NB-IoT поддерживали более 700 тыс. базовых станций сотовой связи операторов китайской «большой тройки»⁷⁵.
- С учетом других данных и оценок рынка, общее количество подключений NB-IoT в КНР на начало 2022 г. можно оценить в 220–250 млн, при общем количестве подключений по миру – 260–300 млн. Таким образом, доля КНР может оцениваться в 75–80 % от всего мирового рынка NB-IoT по числу подключений.
- Мощным преимуществом для китайских участников рынка является крайне низкая цена на чипы и модули для сетей NB-IoT: текущая стоимость модуля в КНР не превышает 2,5 долл. США и, по прогнозам, снизится еще на 40 % к 2025 г., что многократно дешевле модулей для других сетей IoT⁷⁶.

Будущие планы китайских участников рынка не менее амбициозны: по прогнозам Huawei, озвученным в середине 2021 г., к 2025 г. ожидается 1,2 млрд новых подключений NB-IoT, значительную часть которых обеспечит КНР.



Источник: [Huawei Insights, 2021](#)

С китайской экспансией в нише NB-IoT связаны два момента:

- Во-первых, она косвенно определяет развитие технологий LPWAN в целом — учитывая огромную роль Huawei в разработке оборудования для NB-IoT и ставку китайского государства на эту технологию, западные страны и операторы связи предпочитают развивать LTE-M и другие LPWAN, руководствуясь рисками технологической зависимости и кибербезопасности.
- Во-вторых, несмотря на впечатляющие цифры подключений, экономическая состоятельность китайской модели развития сотовых LPWAN пока не доказана — по некоторым оценкам, проекты операторов «большой тройки» в части NB-IoT реализуются прежде всего в рамках государственных планов развития интернета вещей и не приносят прибыли⁷⁷.

В любом случае развитие NB-IoT в КНР продолжит оказывать огромное влияние на мировой рынок сотовых LPWAN в обозримой перспективе. Более того, с долей рынка порядка 75–80 % от мирового КНР во многом замыкает на себе мировые тренды развития NB-IoT. В данный момент общие перспективы развития этого протокола невозможно оценить в отрыве от анализа китайского странового рынка. В этом кроется потенциальная «хрупкость» успеха NB-IoT с рыночной точки зрения: ситуация может в одночасье измениться под влиянием нескольких крупных компаний (Huawei) и китайских регуляторов, курирующих национальную политику в сфере цифровой инфраструктуры. Дополнительным фактором риска могут выступать технологические санкции США, ограничивающие доступ китайских компаний к разработкам в области микроэлектроники и производства микропроцессоров с передовыми размерами технологического процесса.

Таким образом, из перечисленных технологий сотовых LPWAN именно вокруг NB-IoT на сегодняшний момент сформировалась наиболее мощная коалиция крупнейших сотовых операторов и других игроков глобального рынка, продвигающих технологию. Не менее важна широкая экосистема участников рынка, включая не только производителей компонентной базы и сетевого оборудования, но и поставщиков конечных устройств и разработчиков ПО. В результате NB-IoT на мировом рынке занимает лидирующую позицию среди всех технологий LPWAN и продолжит удерживать ее как минимум в среднесрочной перспективе, несмотря на параллельный рост конкурирующих решений.

От первого лица

Телеком-операторы, начавшие с M2M-направления более десяти лет назад, сейчас активно развивают сферу интернета вещей. IoT уже входит в нашу жизнь – это и сбор показаний с интеллектуальных счетчиков, и контроль потерь электроэнергии, и умный дом с всевозможными цифровыми сервисами. В промышленности это безопасность сотрудников, диагностика, предиктивный ремонт и многое другое. Уверен, что в ближайшем будущем умные устройства будут для каждого из нас естественным критерием комфорта и удобства нашей повседневной жизни.

Чтобы все перечисленное стало реальностью, мобильные операторы запустили NB-IoT сети в большинстве регионов России. Так, сеть «МТС» работает более чем в 80 субъектах страны. Также мы сформировали инфраструктуру и сами разработали около 100 устройств IoT. Вся инфраструктура продуктов NB-IoT переводится на платформу собственной разработки, что позволит сделать работу устройств интернета вещей независимой от зарубежных компаний и внешних событий, а также гарантировать их стабильную работу.

Ранее развитие NB-IoT сдерживало отсутствие устройств интернета вещей, но сейчас этот пробел восполняется. «МТС» выпустил первый в России набор для создания прототипов устройств, работающих в сети NB-IoT Development Kit. Он ориентирован на разработчиков решений интернета вещей и позволяет упростить создание образцов устройств и ускорить вывод продуктов IoT на рынок. Наши разработчики создали умную кнопку, метеостанцию, умный замок и ряд других устройств.

На сети NB-IoT «МТС» запустила технологию SCEF, которая обеспечивает взаимодействие любых устройств с сетью интернета вещей через единый интерфейс. В результате IoT-продукты быстрее выходят на рынок, снижаются издержки разработчиков решений, повышается автономность и энергоэффективность устройств.

Мы видим, что решения NB-IoT широко применяются в различных отраслях экономики, охватывают огромный рынок разработчиков и поставщиков устройств, а уже развернутые в России сети NB-IoT позволяют быстро интегрировать в существующую инфраструктуру устройства и существенно экономить затраты. Созданный и активно развивающийся технологический задел говорит о том, что NB-IoT станет одной из глобальных доминирующих технологий LPWAN и обеспечит кратный рост рынка интернета вещей. Нам нужно загружать сети, активно продвигать и развивать собственные решения для IoT. Мы со своей стороны сделаем все возможное, чтобы технологии IoT развивались в нашей стране и в ближайшее время стали простыми, но важными и удобными дополнениями нашей жизни.



Антон Салов,
руководитель
IoT, ПАО «МТС»

В России рынок развивается в направлении NB-IoT в русле общемировых трендов – за последние годы операторы связи приступили к развертыванию крупных сетей на базе технологии.

- Лидером по масштабу проектов среди российских сотовых операторов является ПАО «МТС», в 2018 г. запустившее первую в России сеть NB-IoT федерального охвата. На март 2022 г. сеть компании действовала более чем в 80 российских регионах. Помимо инвестиций в сетевую инфраструктуру, «МТС» формирует продуктовую линейку для применений на сетях NB-IoT. На середину 2022 г. портфель продуктов компании насчитывал более 73 датчиков и иных приборов собственной разработки, включая IoT Development Kit и 5G Development Kit, которые позволяют разработчикам создавать прототипы устройств IoT и сервисы на их основе.
- С 2019 г. крупные проекты запустило ПАО «Мегафон» – компания развернула сеть NB-IoT в 59 регионах России и планировала расширить ее покрытие до 83 регионов⁷⁸.
- В 2018 г. тестирование коммерческой гибридной сети в Москве с поддержкой двух технологий (NB-IoT и LTE Cat-M) начал «Билайн»⁷⁹.

Развитию технологии NB-IoT на российском рынке способствует расширение спектра ее применений, включая промышленные производства. Утвержденная в 2019 г. Концепция построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации отводит NB-IoT приоритетную роль, в том числе для применений в критически важных секторах экономики⁸⁰. Кроме того, в нынешних условиях на первый план выходят возможности технологии в части обеспечения информационной безопасности, включая поддержку встроенных протоколов и алгоритмов шифрования. Стоит отметить, что с 13-го релиза стандартов 3GPP в архитектуре сети NB-IoT реализован элемент SCEF (Service Capability Exposure Function), который позволяет передавать данные от подключенных устройств на платформу без использования IP-адресации. Такая функция позволяет сузить контур рисков ИБ для использующих протокол сервисов и самой сети⁸¹.

За счет того, что операторы связи создали развитую инфраструктуру сетей NB-IoT в России, данная технология претендует на ведущую роль на рынке. Несмотря на то, что узкополосный протокол был изначально разработан и специфицирован за рубежом, с 2020 г. он полноценно стандартизирован в рамках ГОСТ Р 59026–2020⁸². Стандартизация способствует более широкому проникновению NB-IoT на российском рынке, прежде всего облегчая доступ к проектам с государственными заказчиками. По прогнозу «МТС» общее число подключений NB-IoT в России по итогам 2023 г. превысит 10 млн⁸³ (по другим данным, 8,3 млн)⁸⁴.

Как отмечалось выше, изменение обстановки и санкционная нагрузка на операторов в 2022 г. могут повлечь либо заморозку, либо свертывание проектов как сотовых, так и несотовых проектов сетей LPWAN, не вышедших из стадии тестирования и не показавших окупаемость. Наиболее значимым фактором для всех участников рынка является сокращение доступа к зарубежному сетевому оборудованию, от компонентной базы до базовых станций и других готовых решений для сотовых узкополосных сетей. Развитию рынка IoT в этих условиях будет способствовать поддержка со стороны государства проектов по разработке и внедрению интегрированных решений LPWAN в лицензируемом спектре, в том числе за счет принятия НПА, расширяющих применение интеллектуальных систем учета ресурсоснабжения.

С учетом крупных инвестиций участников российского рынка в развертывание сотовых LPWAN, развитие компонентной базы и оборудования для таких сетей, в нынешней ситуации для этой технологической ниши также актуальны механизмы целевой поддержки, в том числе производителям отечественных IoT-решений. Конкретными направлениями такой поддержки могут быть:

- Расширенное субсидирование проектов по разработке отечественной линейки сетевого оборудования (чипсеты, радиомодули) и оконечных устройств IoT для сотовых LPWAN.
- Включение проектов комплексного внедрения сотовых LPWAN в список приоритетных направлений поддержки цифровой трансформации российских предприятий – в том числе для проектов частных беспроводных сетей.
- Грантовое финансирование разработки отечественных платформенных решений для сотовых LPWAN, в том числе с поддержкой российских средств обеспечения информационной безопасности.
- Поддержка в части нормативного регулирования внедрения интеллектуальных приборов учета с использованием беспроводных технологий в ЖКХ (приборы учета газа, воды, тепла).

Несотовые LPWAN: раздел рынка между LoRa и Sigfox

Развитие сетей LPWAN, не использующих инфраструктуру сотовой связи, также следует растущему запросу на «массовый» IoT в тех применениях, где не нужна высокая скорость передачи данных и широкополосный доступ. Подавляющее большинство устройств IoT, подключенных через несотовые сети, – это относительно простые датчики и сенсоры, передающие данные не в реальном времени, малыми объемами и со значительными интервалами. По своим характеристикам несотовые LPWAN находятся ближе к NB-IoT, чем к LTE M и другим сотовым узкополосным сетям:

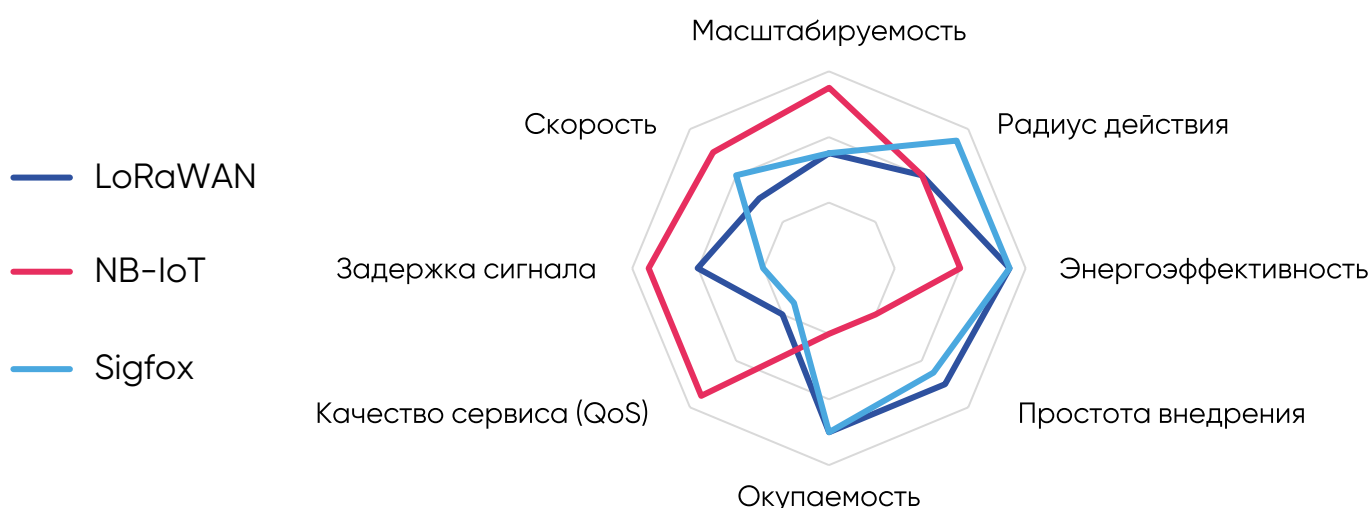
- очень низкая скорость передачи данных (до 100 Кб/с) и высокая задержка передачи сигнала (от 1 до 10 с и более);
- использование для работы узких и сверхузких полос радиочастот (до 250 кГц);
- расширенный радиус действия (до 3–5 км в городе, до 15 км и более на открытой местности);
- максимально сниженное энергопотребление, продлевающее «жизненный цикл» устройств IoT со встроенной батареей до 10 лет и более.

В то же время ряд отличий делает сотовые и несотовые узкополосные сети разными продуктами для участников рынка:

- В отличие от LPWAN на базе сотовой связи их несотовые аналоги используют нелицензируемые полосы частоты в субгигагерцевом диапазоне. Это существенно снижает капитальные издержки и порог входа на рынок для операторов таких сетей.

- Независимость от сетей сотовой связи, простота устройства и низкая стоимость модулей и базовых станций, наряду с другими характеристиками несотовых LPWAN, снижают расходы на их внедрение и эксплуатацию.
- По результатам исследований за 2021 г., в 7 из 8 различных сценариев внедрения узкополосных сетей совокупные расходы на внедрение и эксплуатацию самой распространенной несотовой LPWAN (LoRaWAN) составили от 22 % до 67 % расходов на внедрение NB-IoT для разных сценариев. Другие сотовые LPWAN оказались еще дороже⁸⁵. Единственный сценарий, при котором внедрение LoRaWAN оказалось на 20 % дороже внедрения NB-IoT и практически равно стоимости внедрения LTE M – внедрение в сельской местности с высокой плотностью размещения устройств IoT.
- В то же время, по мере развития производства отечественных NB-IoT устройств, себестоимость внедрения решений на базе сотового протокола в России будет снижаться и все более жестко конкурировать с решениями на базе LoRaWAN. На российском рынке в пользу сотовых технологий играет наличие уже построенной операторами связи развитой инфраструктуры сетей NB-IoT, за счет чего обеспечивается снижение расходов по сравнению с реализацией проектов «с нуля», включая проекты LoRaWAN.
- Несотовые LPWAN серьезно уступают технологиям на базе сотовой связи в гарантированном качестве обслуживания (QoS) и возможностях масштабирования.
- Кроме того, почти все несотовые узкополосные сети не способны поддерживать сервисы IoT в реальном времени, когда необходима двусторонняя передача данных с малой задержкой и поддержкой гарантированного качества сервиса.

Сравнение основных характеристик несотовых LPWAN (LoRaWAN, Sigfox) и NB-IoT



Различия между двумя типами технологий определяют развитие их рыночных ниш. Если сотовые LPWAN развивают прежде всего операторы связи с упором на крупные проекты индустриального уровня, то технологии несотовых LPWAN доступны для самостоятельного развития и внедрения гораздо более широкому кругу игроков.

Заметная на рынке ниша несотовых LPWAN сформировалась к 2014–2015 гг. и с тех пор растет темпами от 50 до 100 % ежегодно, опережая любые другие технологии беспроводной связи для IoT.

- Если в 2020 г. на несотовые узкополосные сети приходилось не более 150 млн подключений IoT⁸⁶, то в 2021 г. – уже 260–265 млн, а оценки на 2022 г. находятся в диапазоне 315–330 млн подключений.
- Несмотря на торможение роста глобального рынка IoT в связи с COVID-19 и нарушением производственного цикла и цепочек поставок полупроводников и оборудования, темпы роста несотовых LPWAN должны сохраниться на уровне порядка 50 % в год.
- При этом может сохраниться сегодняшняя ситуация, когда мировой рынок на 90 % поделен между двумя технологиями – LoRa и Sigfox.

Доминирующей технологией на рынке несотовых узкополосных сетей останется **LoRa/LoRaWAN**⁸⁷ – проприетарная технология модуляции радиосигнала, описанная в 2015 г. и сформировавшая вокруг себя продуктовую линейку от оборудования до ПО.

- На апрель 2022 г. сети LoRaWAN были развернуты 170 операторами связи, по сравнению со 103 операторами в 2019 г.⁸⁸ Общее число подключений в сетях LoRaWAN составляет 225 млн на 2022 г. и может превысить 650 млн к 2025 г.⁸⁹
- Технология продолжит занимать более 50 % рынка в своем сегменте по числу подключений и активно расширять географию и отраслевой спектр внедрений. Суммарные инвестиции в оборудование и развертывание сетей на базе LoRa к 2026 г. вырастут на 250–300 % и составят от 5,55 до 6,2 млрд долл. США⁹⁰.
- Среди национальных рынков, где наиболее активно развивается LoRaWAN, выделяется Франция, где по итогам 2022 г. ожидается более 5 млн подключений⁹¹.
- Инфраструктурный оператор American Tower в 2021 г. начал реализацию контракта на подключение на базе LoRaWAN 5 млн умных счетчиков и других устройств в Бразилии⁹².
- KHP входит в число мировых лидеров и в развитии сетей на базе LoRaWAN. По состоянию на март 2022 г. половина выручки Semtech от поставки чипсетов LoRaWAN приходилась на китайский рынок⁹³. Позиции технологии на рынке с 2018 г. укрепляют ее внедрение в инфраструктуру крупнейших цифровых платформ – Tencent и Alibaba⁹⁴. Таким образом, Китай представляет собой единственный национальный рынок, который лидирует в мире по числу подключений IoT на базе несотовой LoRaWAN – и одновременно обеспечивает ¾ мировых подключений к сотовой сети NB-IoT.

От первого лица



Андрей Колесников,
директор,
Ассоциация
участников рынка
интернета вещей

У российского рынка технологий связи для IoT есть возможности, которые важно использовать в нынешней ситуации. Для реализации быстрых и низкобюджетных проектов в турбулентных экономических условиях технологии LPWAN – отличное решение. При этом необходимо дальнейшее движение российских протоколов LPWAN в сторону открытых экосистем. Это поможет им вырасти в конкурентоспособные зрелые решения, которые позволят сохранить базу для роста рынка и внедрения IoT в условиях сокращения доступа к зарубежному оборудованию и технологиям.

Такой путь потребует от разработчиков ПО, оборудования, сетевых решений и платформ готовности действовать в логике кооперации, развивать общие стеки решений на основе имеющихся протоколов, преследовать совместные цели на площадках отраслевых альянсов и консорциумов. Государство может ускорить этот процесс, точно поддерживая разработку интегрированных совместимых решений на базе российских открытых стандартов LPWAN.

Еще одно перспективное направление – поддержка проектов, продвигающих гибридную мультитехнологичную связь для применений IoT, таких как интеграция LPWAN со спутниковыми сервисами. В долгосрочной перспективе спутниковые коммуникации могут перевернуть рынок IoT, поэтому важно смотреть в эту нишу и способствовать ее развитию сегодня.

Позиция LoRaWAN на рынке укрепляется за счет следующих преимуществ:

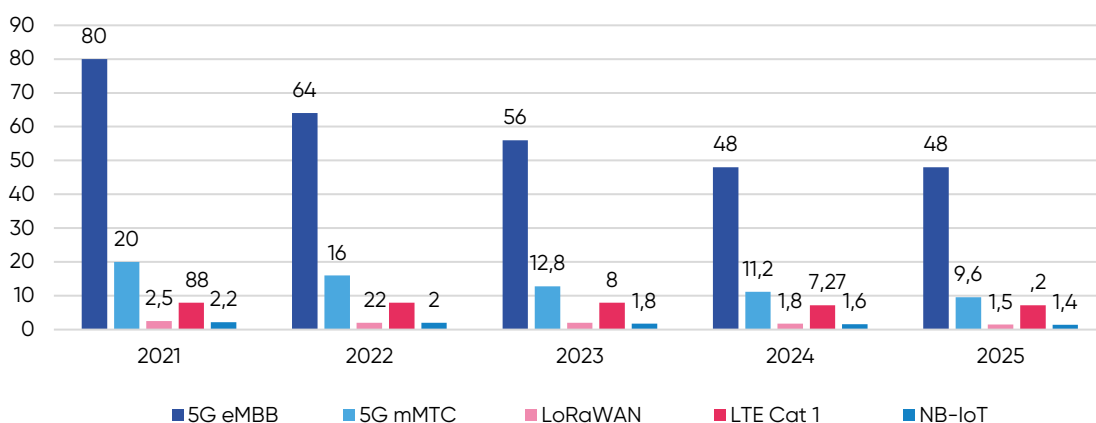
- 1. Открытость:** базовая технология модуляции LoRa является проприетарной и запатентована; монопольным вендором чипов радиочастотных трансиверов для оборудования сетей LoRaWAN выступает владелец патента^{95 96}, компания Semtech⁹⁷. Однако сетевой протокол LoRaWAN целенаправленно развивается на базе открытого стандарта. Такой подход открывает стек технологий LoRaWAN для заинтересованных компаний и способствует расширению отраслевого сообщества, производящего и продвигающего продукты на базе LoRa. Например, рынок модулей и базовых станций LoRaWAN на сегодняшний день включает более 30 производителей, в том числе Advantech, Cisco Systems, Gemtek, Kerlink, Lansitec, MultiTech, Netvox, Sseed и т. д.⁹⁸ Открытость LoRaWAN обеспечивается в том числе ее продвижением на уровень международного стандарта – в ноябре 2021 г. МСЭ включил LoRaWAN в число стандартов энергоэффективной узкополосной сети⁹⁹.
- 2. Экосистемный подход:** с 2015 г. вокруг технологии LoRa и протокола LoRaWAN сформировалась развитая рыночная экосистема альянсов и партнерств, включая:
 - головной альянс (LoRa Alliance) с более чем 500 участниками¹⁰⁰;
 - китайский альянс (China LoRa Application Alliance (CLAA)), продвигающий мультисервисную платформу IoT на базе LoRa¹⁰¹;
 - иные альянсы и консорциумы в сфере IoT, вовлеченные в разработку и продвижение продуктов и технологий, совместимых с LoRa (Continental Automated Buildings Association (CABA); Euridis Association, IoT Connectivity Alliance (ICA); Wireless Broadband Alliance (WBA) и другие)¹⁰².

3. Интегрированный стек и сертификация: построение вертикально интегрированных технологических стеков типично для всех технологий связи IoT, но сообществу LoRa удалось добиться в этом особенных успехов. Продуктовая линейка LoRa на сегодняшний день охватывает уровни оборудования и устройств (датчики, сенсоры, модули связи и чипсеты, базовые станции и др.), ПО, сервисов и сетевых решений. На апрель 2022 г. по этим категориям был сертифицирован 301 продукт, большую часть (185 шт.) составили устройства и оборудование¹⁰³. Это существенно выше числа сертификаций для NB-IoT и LTE M (менее 100 для каждой технологии).

Одна из главных причин такого разрыва – более сложный процесс сертификации для продуктов на базе сотовой связи, требующей радиочастотного лицензирования, в ряде стран и регионов, включая США и ЕС¹⁰⁴. Процессы сертификации определяют доступ к технологиям со стороны широкого круга участников рынка, таким образом косвенно влияя на конкурентоспособность продуктовых линеек на базе тех или иных протоколов LPWAN. В конечном счете это сказывается на рыночной доле продуктовых линеек на базе сотовых и несотовых узкополосных сетей. Как показывает приведенная выше в этом разделе статистика, более открытые экосистемы, сформированные вокруг несотовых технологий, растут быстрее, чем их конкуренты, если исключить из выборки особый страновой кейс KНР.

Наконец, в пользу LoRa развивается ситуация с рыночными ценами на оборудование для сетей LPWAN. На сегодняшний день модули для LoRaWAN и NB-IoT стояткратно дешевле модулей других технологий LPWAN – в значительной степени из-за влияния китайских производителей на формирование стоимости оборудования NB-IoT. В дальнейшем снижение цен продолжится, при этом модули LoRa будут стоить дешевле относительно модулей других стандартов сотового IoT, за исключением NB-IoT.

Динамика стоимости модулей оконечных устройств для сетей IoT дальнего радиуса действия (долл. США за 1 шт.) 2021–2026 гг.



Источник: Huawei Insights, LoRa Alliance

Вторым крупнейшим игроком на рынке несотовых LPWAN остается Sigfox, «легкий» сверхузкополосный протокол французского происхождения, разработанный в 2009 г.

- На апрель 2022 г. к сети Sigfox было подключено 20 млн устройств IoT¹⁰⁵, общее покрытие сети в 75 странах достигло 6 млн км².

- По прогнозам, в ближайшие годы Sigfox может развиваться еще быстрее, чем LoRaWAN, в результате чего рыночная доля французского протокола в нише несотовых LPWAN к 2026 г. достигнет 30 %¹⁰⁶.
- Вместе с тем пока что развитие Sigfox неустойчиво в части финансового результата. В декабре 2021 г. компания – разработчик протокола подала заявление на процедуру защиты от банкротства¹⁰⁷. Среди причин, которые привели оператора к такому шагу, отмечалась неудовлетворенность крупных корпоративных клиентов показателями работы сетей IoT на базе Sigfox.
- В апреле 2022 г. французскую компанию – разработчика технологии за 25 млн евро приобрел сингапурский провайдер решений для «массового» IoT UnaBiz¹⁰⁸.

Таким образом, развитие несотовых LPWAN в ближайшие несколько лет, несмотря на прогнозируемые высокие темпы, может сдерживаться недостаточной зрелостью технологий и их медленной окупаемостью.

В этом смысле независимость LoRaWAN, Sigfox и прочих подобных решений от крупнейших операторов связи и производителей оборудования играет против них. Телекоммуникационные гиганты уровня Vodafone, Ericsson, AT&T могут поддерживать свои технологии «на плаву», даже если они продолжительное время не выходят на окупаемость. У участников экосистемы несотовых LPWAN на это меньше ресурсов.

Одна из перспективных стратегий для несотовых LPWAN, которую уже реализует альянс LoRa¹⁰⁹, – развивать совместимость несотовых узкополосных сетей с сотовыми, повышая интерес крупных операторов связи к гибридным решениям. Еще один сходный вектор – развитие совместимости несотовых LPWAN с технологиями спутникового IoT¹¹⁰.

Главная особенность рынка несотовых узкополосных сетей в России – параллельное развитие сразу нескольких технологий, в том числе отечественной разработки:

- В 2021 г. была предварительно утверждена российская спецификация стандарта (ПНСТ) для сетей LoRaWAN¹¹¹. Утверждение итогового стандарта ГОСТ Р ожидается в середине 2024 г. По состоянию на октябрь 2020 г. число подключенных модулей LoRaWAN в России превысило 1 млн¹¹², что составляет порядка 35–40 % всех подключений к несотовым узкополосным сетям (2,5–2,7 млн). Основную долю подключений обеспечили сети компаний «ЭР-Телеком», «Ростелеком». Из крупных международных игроков сеть LPWAN в России в 2021 г. запустил телекоммуникационный оператор Orange¹¹³.
- В мае 2020 г. в России была запущена первая сеть промышленного IoT на базе Sigfox (сеть Zero G); в развитие сетей Sigfox планировалось вложить 2 млрд руб.¹¹⁴ В 2021 г. началась работа над национальной адаптацией стандарта Sigfox. В 2022 году компания ушла с российского рынка.

Российские решения в нише несотовых LPWAN включают 3 технологии, созданные с учетом наработок Sigfox и занимающие значимую долю домашнего рынка:

1. **XNB** (Extended Narrowband) – разработка компании ООО «СРТ» (торговая марка «Стриж Телематика»), которая занимает довольно уникальную нишу – это единственная в России несотовая технология LPWAN, которая помимо работы в нелицензируемых частотах (868,8 МГц) имеет возможность работать в лицензируемых частотах. При этом параметры работы оборудования для

стандартной сети XNB технически не превышают порог мощности, установленный для использования нелицензируемых частот. Особый статус технологии в этом плане связан с тем, что в 2018 г. частоты, которые использует XNB, были выделены оператору спутниковой системы ГЛОНАСС (ООО «ГЛОНАСС ТМ»). Предполагалось, что технология будет использована для ряда инфраструктурных проектов федерального масштаба в нише транспортной телематики.

Протокол поддерживает двустороннюю связь дальностью более 15 км¹¹⁵ на открытой местности и разработан для обмена данными подключенных устройств на больших территориях с малыми затратами энергии. ООО «СРТ» развивает протокол с 2014 г., разработало IoT-платформу и предлагает достаточно широкую линейку отраслевых решений – от умного ЖКХ до сельского хозяйства и промышленности. В то же время развитие XNB сдерживает закрытость его экосистемы. До сих пор технология развивалась как проприетарное запатентованное решение, а ООО «СРТ» оставалось монопольным владельцем интеллектуальной собственности и разработчиком самой технологии, сетевого оборудования, инфраструктуры и большей части ПО. В отсутствие государственных инфраструктурных проектов такая стратегия тормозит развитие протокола и его проникновение на рынок. В последние 1–2 года компания-разработчик стала ориентироваться на большую открытость и построение рыночной экосистемы¹¹⁶, но пока такую экосистему лишь предстоит создать.

2. **NB-Fi** – открытый узкополосный протокол, в России работает в нелицензируемом диапазоне 868,7–869,2 МГц со скоростью до 25 кбит/с и дальностью до 30 км на открытой местности. Стандарт NB-Fi может поддерживать до 4,3 млрд устройств в одной сети и в целях сокращения размера сообщений не использует IP-адресацию; для обмена данными используется API IoT-платформы компании – разработчика WAVIoT (ООО «Телематические Решения»)¹¹⁷. Такое специфическое решение повышает эффективность технологии, но на практике может ограничивать открытость, привязывая использование NB-Fi к платформе WAVIoT. На август 2023 г. решения на основе NB-Fi заняли значимую нишу на рынке – поставки устройств с поддержкой протокола превысили 2,1 млн¹¹⁸. Позиции NB-Fi на российском рынке дополнительно укрепляет его утверждение в качестве национального стандарта в апреле 2022 г.
3. **Open UNB** – протокол, работающий на частоте и использующий сверхузкие полосы в нелицензируемом диапазоне 868,8 МГц. Протокол, разработанный консорциумом Сколтеха в 2019 г., является открытым и реализован на оборудовании компании GoodWAN (ООО «РадиоТех»)¹¹⁹. В основе разработки лежит идея радикально «облегченного» протокола, позволяющего передавать минимально необходимый объем данных преимущественно в одностороннем режиме (от устройств к шлюзу) на малой скорости (до 300 б/с). Преимуществами должны выступать высокая энергоэффективность и дальность связи (до 40 км, по данным разработчиков). Такие характеристики делают Open UNB потенциально перспективным для той же ниши рынка, к которой относятся и другие «облегченные» протоколы LPWAN, такие как Sigfox и NB-Fi, а также сотовый NB-IoT. Это прежде всего сегмент счетчиков в умном ЖКХ, сенсоров и датчиков без внешних источников питания на инфраструктуре ТЭК и энергосетях. На 2022 г. коммерческое применение Open UNB остается достаточно узким, но отдельные независимые от GoodWAN дистрибьюторы на рынке начали его продвижение¹²⁰.

Таким образом, российские технологии несотовых узкополосных сетей развиваются достаточно активно, но пока не достигают уровня лидеров рынка, которые обеспечивают свое преимущество за счет двух характеристик: зрелости технологии

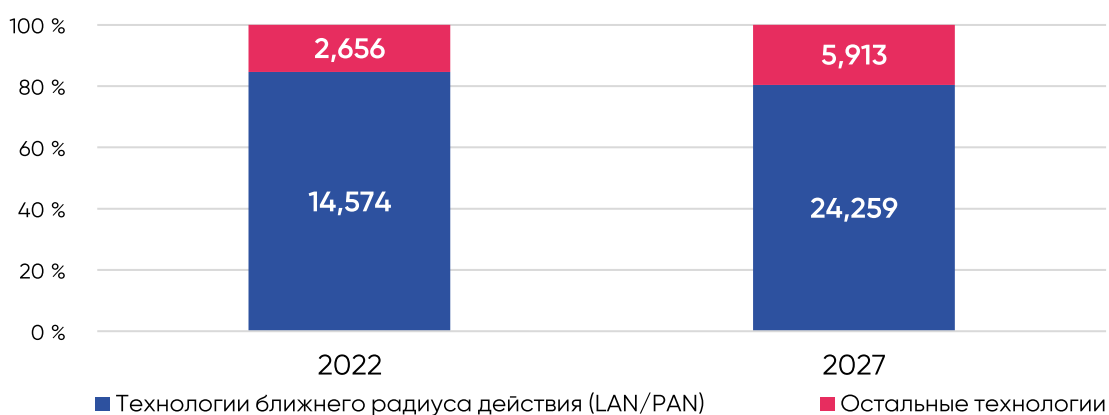
и ее открытости. Каждое российское решение по отдельности может обладать одним из этих качеств, но ни одно из этих решений пока не совмещает в себе оба качества, в отличие от той же LoRaWAN.

- Недостаточная зрелость технологий – применимо прежде всего к Open UNB и в меньшей степени к NB-Fi. В определенной доработке нуждаются сами стандарты. Для серьезного масштабирования сетей на базе российских технологий и их более универсального применения в различных отраслях и сценариях необходимы финансовая поддержка и продвижение на рынке. Наконец, механизмы обеспечения ИБ и защиты сетевой инфраструктуры российских несотовых LPWAN адаптированы для ЖКХ и других ниш с низким энергопотреблением, не всегда соответствуют требованиям к безопасности для промышленных систем и критической инфраструктуры.
- Отсутствие полноценных экосистем и недостаточная открытость в наибольшей степени тормозят развитие протокола XNB, который мог бы дорасти до зрелой российской технологии узкополосных сетей. Базовые возможности сформировать вокруг протокола полноценную экосистему есть – как показывает опыт LoRaWAN, даже проприетарный характер базовой технологии модуляции сигнала не становится препятствием. Но для этого необходимо делать открытым ПО технологии и развивать открытый рынок оборудования, поддерживающего различные настройки и спецификации сетей. Не менее важно сформировать вокруг технологии широкие консорциумы и альянсы разработчиков ПО и производителей устройств, сетевого оборудования и доводить протокол до статуса открытого стандарта.

Беспроводные сети малого радиуса: дополняя LPWAN или конкурируя с ними?

В совокупности сети локального и персонального доступа (Local Area Network, LAN, и Personal Area Network, PAN) продолжают обеспечивать львиную долю подключений для сегодняшнего интернета вещей – 84,5 % (14,574 млрд на 2022 г.)¹²¹. По прогнозам на 2027 г., доля LAN/PAN в общем числе подключений IoT снизится до 80,4 %, но в количественном выражении вырастет до 24,26 млрд. При этом статистика использования конкретных технологий LAN и PAN не всегда измеряется по количеству подключений – ряд компаний и технических организаций предпочитают указывать данные о продажах чипов и модулей для подключения устройств к сети.

Доля подключений IoT на базе сетей ближнего радиуса действия (млрд)



Сети ближнего радиуса, как правило, в том числе в применениях IoT, используются как вспомогательная технология подключения – в дополнение к сетям сотовой связи, несотовым LPWAN, магистральной проводной связи и так далее. Помимо малого радиуса действия LAN/PAN (как правило, до 100 метров), роль играет то, что основные технологии связи таких сетей начали развиваться задолго до «расцвета» IoT и не были ориентированы на максимально низкое энергопотребление и подключение тысяч устройств с небольшим объемом трафика с одной точки доступа. Эти особенности не критичны в сегменте потребительского IoT (B2C), но выходят на первый план в индустриальных применениях.

Вместе с тем технологии LAN и PAN имеют ряд преимуществ перед «дальними» беспроводными сетями:

- лучшее проникновение сигнала в помещениях в ряде диапазонов;
- более высокая скорость передачи данных, особенно по сравнению с LPWAN;
- практически универсальная поддержка производителями коммуникационного оборудования, максимальная гибкость настроек и конфигураций сети;
- широкая поддержка технологий удаленной сетевой аутентификации оборудования (например, протокол RADIUS на базе стандарта IEEE 802.1X).

В результате близкой к стандарту организации сетей корпоративного и индустриального IoT является следующая схема:

- Технология дальнего радиуса действия (или проводная связь) обеспечивает базовое покрытие территории и используется для организации транспортной или опорной сети (backhaul service).
- Технологии малого радиуса действия обеспечивают «нижний этаж» связности на уровне интегрированных в основную сеть локальных подключений, в том числе внутри помещений.

Однако последние тренды в развитии LAN и PAN могут частично поменять эту картину. Растущее значение IoT разворачивает развитие технологий LAN и PAN под нужды и параметры промышленных применений M2M-коммуникаций:

- За последние несколько лет были разработаны новые версии наиболее широко используемых протоколов с эффективным радиусом сигнала до 1 км и более (например, Wi-Fi HaLow и Bluetooth LE).
- Параллельно в этих же версиях протоколов реализованы решения, многократно снижающие их энергопотребление.
- В последних версиях используемых протоколов LAN и PAN широко внедряется поддержка массовых подключений к одной точке доступа (до 8 тыс. и более), наряду с поддержкой архитектур, оптимальных для M2M-взаимодействий (ячеистые одноранговые сети, mesh networks).

Такие разработки приближают сети LAN по своим характеристикам к сетям дальнего радиуса действия, а в случае дальнейшего развития в среднесрочной и долгосрочной перспективе (2030–2035 гг.) могут существенно размывать границу между ними.

Яркий пример этих тенденций показывает развитие **Wi-Fi**. Семейство протоколов Wi-Fi на сегодняшний день включает более 20 версий протокола, разбитых на 6 поколений. За время с запуска первой версии протокола в 1997 г. Wi-Fi превратился в разветвленную технологическую экосистему, совокупный накопленный вклад которой в глобальную экономику оценивался в 3,1 трлн долл. США на 2021 г.¹²² В 2022 г. общее число подключений по Wi-Fi в мире достигло 18 млрд, еще 4,4 млрд подключений могут добавиться к этой цифре до конца года¹²³. По консервативной оценке, не менее 50 % всех подключений по Wi-Fi, то есть порядка 9 млрд, используются для M2M-коммуникаций.

До 2020 г. Wi-Fi в основном использовался для подключения устройств IoT в рамках двух сценариев:

- Подключения для применений IoT с небольшим числом устройств и компактной территорией, на которой разворачивается сервис, например умный дом.
- Упомянутая выше модель для промышленных и корпоративных применений: точечное покрытие, дополняющее основную технологию связи (беспроводную сотовую связь либо магистральную проводную связь) на территории объекта.

С 2020 г. идет процесс вывода на рынок двух наиболее значимых технических обновлений Wi-Fi с момента его создания, которые нацелены прежде всего на применения IoT:

1. В модификации шестого поколения протокола (Wi-Fi 6E) найдены инженерные решения, которые обеспечивают передачу данных на скоростях, сравнимых с 5G (до 1 Гбит/с и более), и существенно меньшую задержку сигнала. Wi-Fi 6E позволяет обслуживать большое количество клиентов в высоконагруженных сетях за счет поддержки новой версии модуляции (OFDMA). Также в протоколе реализована функция экономии расхода энергии подключенных устройств (Target Wake Time, TWT). В версии 6E все эти преимущества усиливаются за счет того, что для работы используются полосы частот суммарной шириной в 1200 МГц в новом для Wi-Fi диапазоне 6 ГГц, гораздо менее загруженном, чем «классические» диапазоны 2,4 ГГц и 5 ГГц¹²⁴.

Продвижение Wi-Fi 6E на рынок, включая появление поддерживающих протокол роутеров, смартфонов и иных устройств, стало ускоряться после того, как 2 апреля 2020 г. Федеральная комиссия по коммуникациям США (FCC) освободила для нелицензируемого использования диапазон 6 ГГц. Доступ к этим полосам частот ранее был закреплен за вооруженными силами. За США последовали и другие страны, и с 2021 г. география применения Wi-Fi 6E быстро расширяется.

Выделение частотных диапазонов для Wi-Fi 6E в мире по состоянию на апрель 2022 г.

- Adopted 5925-6425 MHz
- Adopted 5925-7125 MHz
- ▨ Adopted 5925-6425 MHz, Considering 6425-7125 MHz
- Considering 5925-6425 MHz

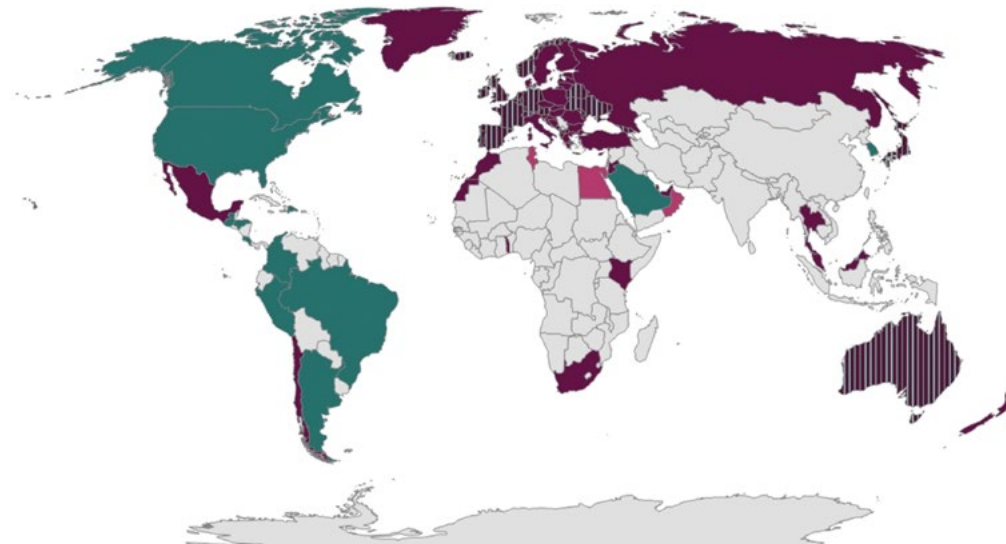


Схема: выделение частотных диапазонов для Wi-Fi 6E в мире по состоянию на апрель 2022 г.

Источник: [Countries Enabling Wi-Fi 6E](#)

Некоторые крупнейшие участники рынка коммуникационного оборудования уже оценили перспективы новой спецификации для промышленного IoT.

- Siemens внедряет поддержку Wi-Fi 6E в собственной линейке оборудования для промышленных M2M-сетей ближнего радиуса действия (IWLAN)¹²⁵.
- Cisco активно развивает линейку сетевого оборудования с поддержкой Wi-Fi 6/6E и продвигает новый протокол на рынок, позиционируя его в том числе для применений в промышленном IoT¹²⁶.

В результате сегодня Wi-Fi 6E – самая быстрорастущая технология локальных беспроводных подключений в мире. По оценкам участников рынка, в 2021 г. глобальные продажи устройств с поддержкой новой версии протокола могли достичь 310 млн, с перспективой роста до 1 млрд в 2025–2026 гг.¹²⁷

2. Помимо 6E, в семействе Wi-Fi к началу 2020-х гг. появилась первая спецификация, спроектированная специально для подключения устройств и поддержки инфраструктуры IoT, – Wi-Fi HaLow (IEEE 802.11ah). Особенности протокола – расширенный до 1 км и более радиус действия вне помещений (outdoor), поддержка 8 тыс. подключений с одной точки доступа, узкополосная связь и сниженное энергопотребление, сравнимое по уровню с Bluetooth. Кроме того, HaLow имеет встроенный механизм безопасности (WPA 3) и является первой из всех версий Wi-Fi, которая работает в субгигагерцевом диапазоне (750–928 МГц).

Эти и другие особенности позволяют позиционировать Wi-Fi HaLow на рынке как решение для сервисов промышленного IoT, частично конкурирующее с сетями LPWAN. В конце 2021 г. Wi-Fi HaLow был сертифицирован для применений

в промышленном IoT¹²⁸. Ближайшие два года должны показать, насколько новое решение будет востребовано в своих целевых нишах: управлении промышленными платформами IoT в автоиндустрии, ТЭК и обрабатывающих производствах.

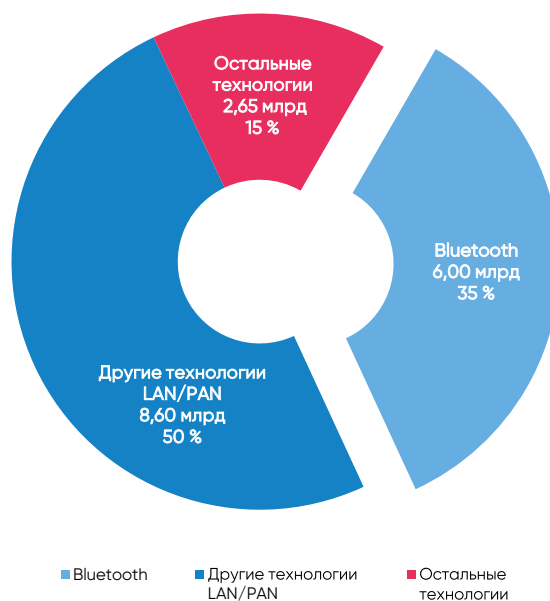
Еще один широко используемый LAN-протокол, развитие которого стало определяться потребностями IoT, – **Bluetooth**. По оценке ABI Research, на 2022 г. Bluetooth обеспечивает 35 % всех подключений IoT в мире¹²⁹, что соответствует не менее чем 6,0 млрд подключенных «умных» устройств. Ежегодные поставки чипов Bluetooth достигли 5,1 млрд в 2022 г. и, по прогнозам, вырастут до 7,0 млрд к 2026 г.¹³⁰; порядка 40 % из них составляют поставки для применений в IoT.

Bluetooth (IEEE 802.15.1) – энергоэффективный протокол с невысокой скоростью передачи данных (1–3 Мбит/с), работающий в частотном диапазоне 2,4 ГГц. Изначально технология была разработана в 2002 г. для обмена данными между персональными устройствами пользователей (ПК, смартфоны, периферийные устройства). Однако сегодня Bluetooth используется для все более широкого спектра применений в IoT:

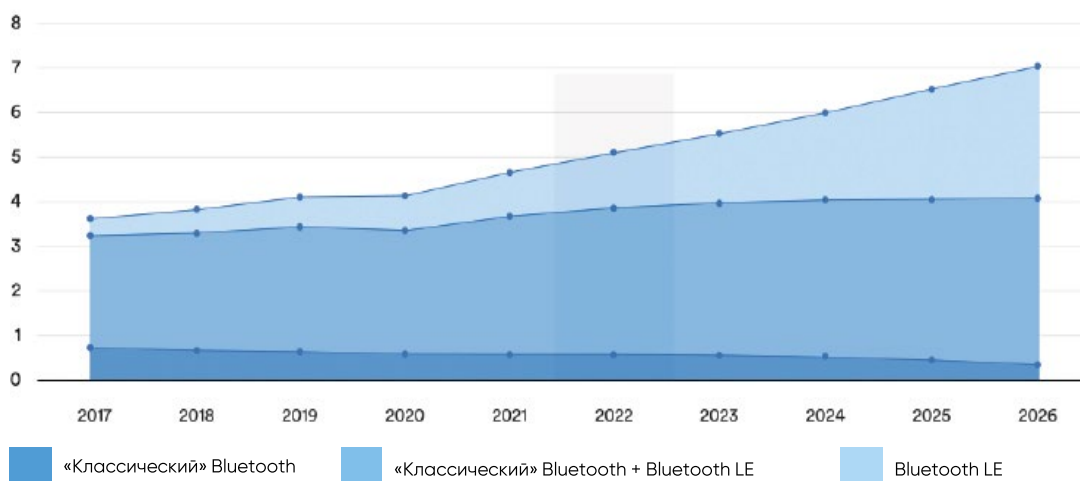
- Пользовательские носимые устройства: умные часы и фитнес-трекеры, умные ошейники для домашних животных, AR/VR-гарнитуры, умные очки и прочее.
- Умные медицинские приборы: подключенные тонометры, портативные устройства ультразвуковой и рентгеновской диагностики и прочее.
- Системы локального позиционирования в реальном времени (RTLS) и навигации в помещениях (IPS): маячки (beacons) с Bluetooth широко используются для сервисов локальной навигации внутри зданий и сооружений в промышленности, культурных объектах и музеях, административных учреждениях и так далее.
- Умные цифровые замки, турникеты и иные системы контроля физического доступа и перемещения.
- Оснащение радиометками Bluetooth личных вещей и предметов (кошельки, ключи, сумки и прочее) на случай их потери или для более быстрого поиска в помещении.
- Управление беспроводными сенсорными сетями (WSN), к которым подключаются датчики температуры, освещенности, влажности и прочее.
- Управление системами домашней, офисной и промышленной автоматизации (контроль освещения, вентиляции и кондиционирования, отопления).

В 2009 г. в развитии протокола был сделан серьезный шаг навстречу растущим потребностям рынка IoT: была создана спецификация протокола Bluetooth для устройств IoT с низким энергопотреблением (Bluetooth Low Energy (BLE)). За счет

Оценочная доля Bluetooth в подключениях IoT на 2022 г., %



сниженного потребления энергии и увеличенного радиуса действия (до 1 км и более)¹³¹ новая версия протокола подходит для тех ниш IoT, которые обычно занимают сети LPWAN, в том числе для подключения устройств со встроенной батареей и ограниченным запасом энергии. Протокол BLE оказался востребован на рынке: по прогнозам, ежегодные поставки модулей Bluetooth LE вырастут с 1,1 млрд в 2022 г. до 3,1 млрд в 2026 г., составив более 35 % от всех поставляемых модулей Bluetooth.



Поставки модулей Bluetooth в 2017–2026 гг., млрд.

Источник: [2022 Market Update, Bluetooth](#)

Развитию межмашинных коммуникаций отвечают и другие нововведения в Bluetooth. В 2017 г. в протоколе была реализована поддержка ячеистой сетевой архитектуры¹³². Такое решение позволяет расширить применение Bluetooth в сетях промышленного IoT с большим количеством и высокой плотностью размещения сенсоров, датчиков и иных устройств, генерирующих M2M-данные¹³³.

Поворот в развитии широко используемой сетевой технологии в сторону применений в IoT – все более частое явление в последние годы. Более того, как и в случае с сетями LPWAN, в нише LAN/PAN продолжают развиваться целые семейства протоколов, изначально спроектированных для M2M-коммуникаций. Яркий пример – группа протоколов на базе стандарта **IEEE 802.15.4**, который определяет параметры нижних уровней для беспроводных персональных сетей с низким уровнем мощности сигнала. IEEE 802.15.4 послужил основой для выработки нескольких протоколов, каждый из которых предлагает свои решения для верхних слоев. К их числу относятся **ZigBee**, **WirelessHART**, **ISA100.11**, **Thread**.

Сети на основе IEEE 802.15.4 отличаются низкой скоростью передачи данных (около 100–250 кбит/с), очень низким энергопотреблением, относительно небольшой задержкой сигнала и дальностью до 100 метров. Почти во все протоколы на базе IEEE 802.15.4 к настоящему моменту встроена поддержка ячеистой сетевой архитектуры, что в том числе важно для M2M-взаимодействий с использованием граничных вычислений.

Наибольший эффект от внедрения решений на базе IEEE 802.15.4 ощущается в тех отраслях, где массово используются сенсоры с долгим «жизненным циклом» и низким энергопотреблением:

- Строительство: мониторинг энергии, света, контроль доступа.
- Промышленное оборудование и энергетика: контроль технологических процессов, промышленных устройств, управление энергией и имуществом.
- Управление ЖКХ и безопасностью в умном доме: датчики воды и энергии, мониторинг энергопотребления, датчики задымления и пожара.



Схема ячеистой сети на базе Bluetooth с высокой плотностью размещения сетевых узлов (пример: сеть сенсоров и датчиков в умном здании или производственном помещении)

Источник: [Bluetooth Blog](#)

На 2022 г. наиболее распространенным на рынке решением на базе IEEE 802.15.4 является спецификация **ZigBee** китайско-американского альянса CSA. Сам альянс, изначально созданный в 2002 г. под названием ZigBee Alliance, на сегодня насчитывает порядка 500 участников, включая таких технологических гигантов, как Amazon, Apple, Comcast, Ikea, Intel, Google, Legrand, MasterCard, Qualcomm, Samsung SmartThings. В последние годы, помимо протокола ZigBee, альянс также развивает и продвигает открытый стандарт беспроводного подключения для устройств IoT Matter. Стратегия участников объединения – на базе простых и нетребовательных протоколов создать экосистему продуктов для умного дома, захватив глобальное лидерство в этой нише рынка.

С учетом высокой роли крупных западных компаний в продвижении в CSA Alliance, Россия на ближайшие годы выпадает из списка целевых рынков для технологий умного дома на базе ZigBee. При этом отечественная ниша сервисов для умного дома пока по большей части не насыщена, несмотря на попытки отдельных игроков создавать собственные продуктовые линейки (например, МТС Smart Home) и даже участвовать в глобальных экосистемах. В качестве примера можно привести компанию Sber Devices, которая в феврале 2022 г. присоединилась к CSA Alliance¹³⁴ для работы над единым стандартом умного дома и по состоянию на конец 2022 г. сохраняла статус участника проекта.

По оценкам, к 2018 г. совокупный объем продаж чипов ZigBee для устройств интернета вещей достиг 0,5 млрд¹³⁵. К 2023 г. общие ежегодные продажи чипов для сетей на базе стандарта IEEE 802.15.4 могут достичь отметки в 1 млрд, при этом доля ZigBee среди них может составить от 50¹³⁶ до 85 %¹³⁷.

В последние 3 года развитие решений для IoT на базе IEEE 802.15.4 укладывается в еще одну значимую тенденцию на рынке – консолидацию нишевых решений для IoT и их курс на взаимную совместимость.

- В декабре 2019 г. Zigbee (компания – разработчик протокола), Google (разработчик Thread), Amazon и Apple объявили о запуске совместного проекта Connected Home over IP (CHIP)¹³⁸, позднее переименованного в Matter¹³⁹.
- Цель проекта – разработка открытого стандарта для умного дома, использующего протоколы Thread, Wi-Fi и Bluetooth LE.
- По сути, речь идет о создании стека решений верхнего уровня, что должно повысить совместимость и унификацию продуктов IoT для умного дома на глобальном рынке. Релиз первой версии стандарта ожидается в первой половине 2022 г.¹⁴⁰
- На сегодняшний день в проекте участвуют несколько десятков компаний, а базовая площадка альянса CSA насчитывает более 500 участников¹⁴¹.

Именно такие процессы формирования альянсов с участием технологических гигантов, сфокусированных на продвижении одной конкретной технологии, могут менять рынок. Примерами служат развитие экосистемы LoRaWAN и формирующаяся история V2X на базе сотовой связи. Из нескольких решений, условно сопоставимых по своим техническим характеристикам, де-факто стандартом для рынка становится то, которое организовано продвигают международные технологические гиганты через механизм промышленных альянсов. Для стандартов семейства IEEE 802.15.4 это означает вероятную победу Thread и существенное расширение его доли рынка в ближайшие 3–4 года.

Еще одним активным участником рынка решений для ниши умного дома в последние годы стал протокол **Z-Wave**.

- Несмотря на небольшую скорость передачи данных (до 100 кбит/с), Z-Wave очень энергоэффективен.
- Протокол использует частотный диапазон 908 МГц, который во многих странах менее загружен, чем более широко используемый диапазон 2,4 ГГц.
- Росту применения Z-Wave в сервисах IoT способствует нишевой экосистемный подход. Разработчики протокола сконцентрировались на развитии на его базе комплексного пакетного решения для умного дома – от систем безопасности до контроля освещения, управления микроклиматом и т. д.¹⁴²
- На 2022 г. на рынке были представлены более 1 300 устройств, совместимых с Z-Wave, а общее число проданных чипов достигло 50 млн.¹⁴³

Еще одним примером нишевого развития технологии LAN для интернета вещей является **DSRC** (Dedicated Short-Range Communications) – беспроводной протокол с радиусом действия до 300–500 метров, основанный на стандарте IEEE 802.11.p, по сути, представляющий собой глубокую модификацию Wi-Fi.

- С 2015 г. DSRC удерживал долю рынка в нише технологий интеллектуальных транспортных систем (ИТС), включая технологии взаимодействия транспортных средств с подключенными объектами внешнего окружения (Vehicle to Everything, V2X).

- На 2022 г. развитие протокола все больше определяет растущая конкуренция со стороны сотовых технологий V2X (Cellular V2X, C-V2X). Использование DSRC до сих пор поддерживают такие крупные OEM-производители, как Volkswagen и Toyota. Однако рыночные прогнозы и формирование мощной коалиции поддержки C-V2X из числа автоконцернов и операторов сотовой связи говорят о том, что в перспективе 3–5 лет LAN-технология DSRC может проиграть сотовой связи.
- Дополнительный фактор, который указывает на скорую утрату DSRC конкурентных перспектив, – стартовавший процесс выделения частот под C-V2X и модернизации стандартов связи на ключевом мировом авторынке в США. В ноябре 2020 г. Федеральная комиссия по коммуникациям (FCC) выделила под C-V2X полосу в 30 Мб в диапазоне 5,895–5,925 ГГц, а также признала сотовый протокол технологическим стандартом обеспечения связи для безопасного транспорта и ИТС¹⁴⁴. Предыдущим стандартом, утвержденным более 20 лет назад, как раз был DSRC, таким образом, решение американских регуляторов во многом ставит точку в конкуренции двух технологий.

RFID: развитие технологий «на границе» IoT

Сегодня RFID является самой массово применяемой технологией беспроводного взаимодействия: по итогам 2021 г. количество проданных за все время RFID-меток превысило отметку в 100 млрд¹⁴⁵. Рынок радиочастотной идентификации продолжает активно расти. По оценкам, расходы на весь спектр оборудования от меток до сканеров и чипов RFID увеличатся с 12,2 млрд долл. США в 2019 г. до 22,2 млрд долл. США к 2032 г.¹⁴⁶ Пассивные сверхвысокочастотные метки RAIN RFID остаются наиболее крупной рыночной нишей объемом в 2,2 млрд долл. США на 2019 г.¹⁴⁷

Радиочастотные метки повсеместно применяются для идентификации и прослеживаемости фармацевтических средств, медицинских приборов и имплантов, грузовых контейнеров и отдельных грузов, розничных товаров, животных, книг и документов, багажа, сельскохозяйственной техники, промышленных инструментов и оборудования и так далее.

С технологической точки зрения RFID выросла в разветвленную экосистему технологий, различных по типам и видам меток (электронные и электромагнитные, активные и пассивные, имеющие и не имеющие встроенный источник питания), используемым диапазонам частот (от 30 кГц до 5,8 ГГц) и радиусу действия (от 10 см до 300 м).

Парадокс RFID в том, что, несмотря на ключевой вклад этой технологии в формирование и распространение самого понятия «интернет вещей», в современных условиях устройства, а значит и технологии связи, RFID не вполне соответствуют критериям IoT. Однако в последние годы технологии RFID активно развиваются в направлении умных устройств IoT:

1. Быстро растет сегмент активных меток RFID со встроенными чипом и источником энергии, а также поддержкой функции перезаписи данных. Такие метки обладают повышенной дальностью передачи сигнала (до 150–300 метров) и используются в качестве маячков для отслеживания объектов в реальном времени, передавая сигнал каждые 3–5 секунд. За последние годы расширяется применение активных RFID-маячков в секторах нефте- и газодобычи, горнодобывающей промышленности и товарных грузоперевозках.

2. Еще в большей степени критериям устройств IoT соответствуют RFID-сенсоры: устройства сбора данных, в которых интегрирована активная или полупассивная метка, оснащенная батареей, микроконтроллером и вычислительным модулем.

RFID-сенсоры применяются в том числе в платформенных сервисах, где имеется уровень передачи собранных данных в сервисы облачной аналитики, и полностью соответствуют критериям умного устройства IoT.

На 2022 г. активные метки и сенсоры составляют порядка 3 % от общего объема рынка RFID (350 млн долл. США)¹⁴⁸. Наиболее часто RFID-сенсоры применяются в следующих типах устройств:

- Датчики температуры: Axzon (RFmicron), Melexis, NXP, ON Semiconductor, PST Sensors, Smartrac, Texas Instrument.
- Датчики влажности: Farsens, ON Semiconductor, Phase IV, PowerCast, Radio Force.
- Датчики давления: Farsens, PowerCast, Radio Force.
- Сенсоры освещенности, движения, ориентации в пространстве и магнитного поля: Farsens, PowerCast.
- Иные ниши: датчики износа шин (Silent Sensors), состояния пищевых продуктов (Infratab) и прочее.

Отдельно стоит упомянуть развитие ниши RFID-сенсоров с интегрированным модулем сотовой связи для передачи M2M-данных. Производители (например, компания Savi) позиционируют такие сенсоры как устройства IoT для применений в товарной и военной логистике¹⁴⁹.

Таким образом, как и в других рассмотренных нишах, развитие технологий RFID размывает их границы с другими решениями в области беспроводной передачи данных (в частности, сетями LAN). Кроме того, архитектура и функционал устройств RFID усложняются по мере роста потребности в интеллектуальных сервисах IoT. Вполне вероятно, что, по мере расширения возможностей радиочастотной идентификации и ее конвергенции с сотовой связью и другими технологиями, метки и сенсоры RFID окончательно перейдут в статус умных устройств и пополнят статистику IoT сразу на десятки и сотни миллиардов подключений.

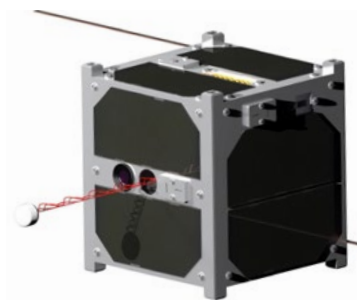
Спутниковый IoT: приход новых игроков

До сих пор рынок спутникового IoT остается относительно узкой нишей, несопоставимой по своему объему с сотовой связью или сетями LPWAN. По итогам 2020 г. спутниковая связь обеспечивала подключениями от 2,5 до 3,4 млн устройств IoT¹⁵⁰, или порядка 0,01–0,015 % от их общего числа. Крупнейшими операторами спутниковых сетей IoT пока остаются спутниковые компании «старого поколения» – Orbcomm и Inmarsat (1,2 млн подключений IoT на совместной сети на конец 2020 г.)¹⁵¹, Iridium (1,1 млн подключений) и Globalstar (0,4 млн подключений)¹⁵².

При этом экономическое значение и объем рынка спутниковых технологий для M2M-коммуникаций растут опережающими темпами: спутниковая связь может обеспечить подключения до 15,7 млн устройств IoT к 2025 г. и до 30,3 млн к 2030 г.¹⁵³ В денежном выражении для этой ниши прогнозируется рост до 5,8 млрд долл. США к 2025 г.¹⁵⁴ и до 8,4 млрд долл. США к 2030 г.¹⁵⁵ Таким образом, и по числу подключений, и по расходам на внедрение решений для IoT спутниковая связь представляет собой крайне динамичную нишу с ежегодным темпом роста более 35 %.

Такие высокие темпы роста основаны сразу на нескольких факторах, которые должны в полной мере проявиться в 2022–2024 гг.:

- Массовый приход в нишу спутниковой связи для IoT новых игроков. На 2021 г. в нише спутникового IoT действовали не менее 38 операторов, более половины из них вышли на рынок в течение последних 8 лет¹⁵⁶. Этот тренд – «эхо» общего процесса близкого к взрывному роста количества частных компаний и проектов в сфере спутниковых коммуникаций с 2013–2014 гг.¹⁵⁷



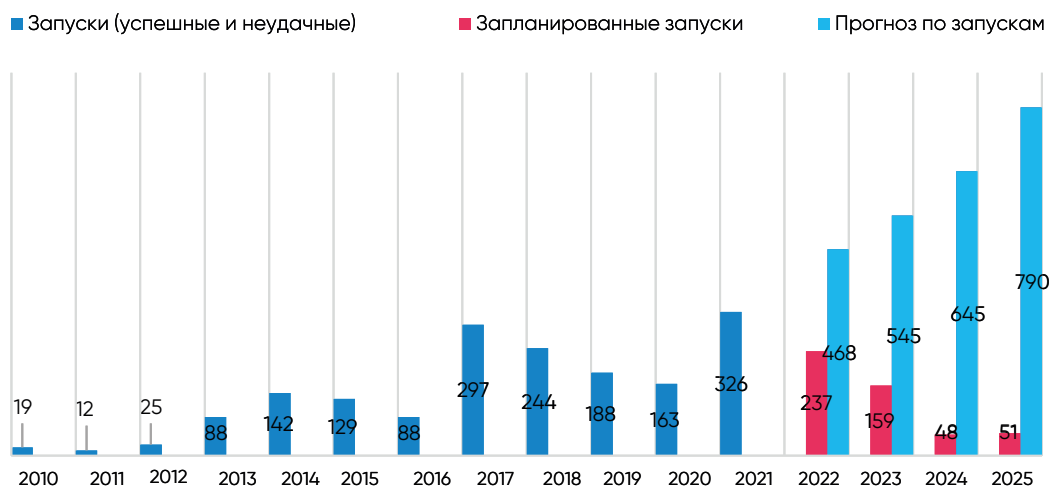
Микроспутник ESTCube-1, размер 10 × 10 × 11,35 см, масса 1,048 кг

- Расширение потребности в связи для устройств IoT в тех нишах и секторах, где покрытие другими сетями труднодоступно: на морских судах, пастбищах и иных протяженных сельхозугодьях, на магистральной инфраструктуре ТЭК и энергосетей в удаленных районах и т. д.

Источник: [ESTCube-1](#), [eoPortal Directory](#)

- Резкое снижение стоимости услуг спутниковой связи для IoT в связи с ростом конкуренции и, главное, развитием спутниковых технологий. Прежде всего речь идет о сверхкомпактных микро- и наноспутниках массой от 1 кг до 10 кг и менее, наиболее широко представленных в форм-факторе CubeSat. На начало 2022 г. на орбиты, как правило низкие, были выведены в общей сложности 1802 наноспутника (включая 1663 CubeSat)¹⁵⁸. При этом более половины всех запусков наноспутников были выполнены за последние 4 года. Низкая стоимость производства и вывода на орбиту наноспутников позволяет их операторам радикально снижать стоимость услуг связи для подключения устройств IoT – вплоть до прямой конкуренции с сетями LPWAN.

Запуски наноспутников (от 1 кг до 10 кг и менее) в 2010–2025 гг.



Источник: [NanoSats.EU](#)

1. Крупные «старые» спутниковые операторы, такие как Eutelsat, Intelsat и Asiasat, активно продвигают свои услуги фиксированной спутниковой связи (FSS) в Ka- и Ku-диапазонах (26,5–40 ГГц и 10,7–18,0 ГГц) для наземных транспортных сетей IoT (Backhaul service). В этой бизнес-модели реализуется формат гибридной сети: за счет спутниковой связи обеспечивается подключение для наземных сетей IoT, таких как LPWAN. Такое решение позволяет существенно масштабировать наземную сетевую инфраструктуру, прежде всего в малонаселенных и труднодоступных районах, где специализированные сети для IoT экономически нецелесообразно развивать на базе сотовой связи или иной технологии дальнего радиуса действия.

Один из недавних примеров внедрения таких решений – запущенные оператором EutelSat в 2021 г. сервисы IoTFIRST и IoTADVANCE, предназначенные для масштабирования наземных сетей Sigfox. Однако в этой нише «старые» спутниковые компании сталкиваются со все более острой конкуренцией со стороны новых участников рынка. Спутниковое масштабирование сетей IoT на базе 4G/5G предлагают OQ Technology, AST SpaceMobile, Omnispace, Sateliot и Galaxy Space; компании EchoStar Mobile и Lacuna Space масштабируют сети LoRaWAN.

Бизнес-модель сервиса спутниковой связи для IoT от EutelSat



Источник: [EutelSat IoT Services](#)

2. Вторая бизнес-модель на рынке – прямая спутниковая связь для устройств IoT (Direct-to-Satellite IoT, DSTIoT). Эту нишу в большей степени формирует новое поколение компаний, создающих многоспутниковые низкоорбитальные группировки: Astrocast, Myrioata, Lacuna, Kineis, Kepler Communications, Swarm Technologies (Space X), Hiber и другие. Преимуществами низкоорбитальных наноспутников в такой бизнес-модели выступают использование широкого спектра частотных диапазонов (Ku-диапазон, S-диапазон и др.), низкая задержка сигнала и возможность передачи данных через маломощные энергоэффективные модемы, что особенно важно для сенсоров и датчиков с ограниченным запасом энергии.

В результате развития этих тенденций рынок спутникового IoT может сильно измениться по составу лидеров и доле основных сегментов уже в ближайшие 3–5 лет:

- Новые игроки, включая наноспутниковые стартапы, могут потеснить традиционных спутниковых операторов.
- Прямая спутниковая связь для устройств IoT имеет потенциал для того, чтобы конкурировать с бизнес-моделью спутниковой транспортной сети для наземного IoT и напрямую с наземными сетями, включая LPWAN.
- В долгосрочной перспективе (примерно к 2030 г.) спутниковые коммуникации могут стать одним из главных конкурентов сотовых технологий в организации сервисов связи для IoT.

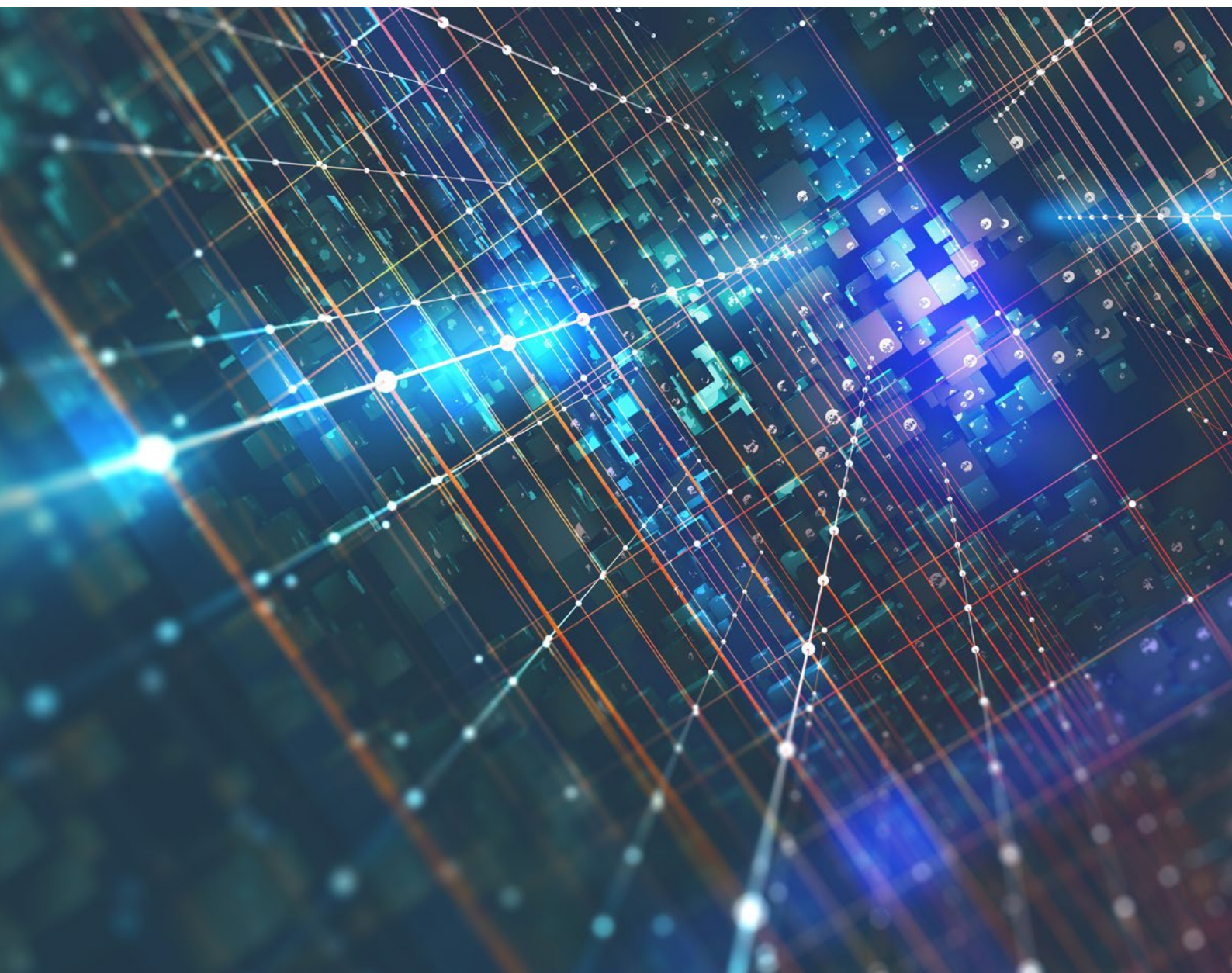
На фоне глобальных тенденций особенно интересно развитие технологий спутниковой связи для IoT в России. За последние два года российский рынок начал разворачиваться в сторону целенаправленного развития спутникового IoT, что видно как минимум по двум крупным проектам:

1. В 2021 г. аффилированная с АО «ГЛОНАСС» компания «ГЛОНАСС Мобайл» получила лицензию виртуального сотового оператора (MVNO) и создала платформу для подключения устройств, включая устройства IoT, к сотовым сетям через eSIM¹⁵⁹.
2. В 2019 г. российское ООО «Спутникс» совместно с туниской компанией TELNET Holding и дочерней организацией «Роскосмоса» АО «Главкосмос Пусковые Услуги» запустило проект создания группировки из 30 малых спутников формата CubeSat для сервисов спутникового IoT¹⁶⁰. В марте 2021 г. на низкую орбиту был выведен тестовый спутник дистанционного зондирования Земли – «Орбикрафт-Зоркий»¹⁶¹. Аппарат создан на базе спутниковой платформы «Орбикрафт-Про SXC6» – собственной разработки компании, которая должна лечь в основу аппаратов для будущей спутниковой группировки¹⁶². В феврале 2022 г. руководство компании подтвердило планы развивать спутниковый сервис IoT для широкого круга заказчиков на базе собственной группировки наноспутников формата CubeSat. Среди возможных применений сервиса называлось судоходство, разработка шельфовых и удаленных месторождений¹⁶³. Планы ООО «Спутникс» укладываются в общую стратегию развития компании, в рамках которой спутниковые данные уже применяются для автоматических идентификационных систем в судоходстве (AIS) и гражданской авиации (ADS-B).
3. В 2020 г. стало известно о старте проекта первой российской многоспутниковой системы «Марафон IoT». Концепция АО «ИСС» имени академика М. Ф. Решетнёва» предусматривает создание 264 микроспутников массой до 50 кг для размещения на полярных средневысотных орбитах (около 750 км). В январе 2022 г. проект получил государственное финансирование¹⁶⁴, а начало формирования спутниковой группировки планируется на 2024 г.¹⁶⁵ В случае реализации «Марафон IoT» станет первым российским и одним из первых в мире государственных проектов по созданию спутниковой группировки для оказания сервисов прямого подключения устройств IoT. Цель разработчиков проекта – выйти на предоставление сервиса прямого сбора информации с типовых устройств IoT с ценовыми и техническими параметрами, сопоставимыми с сетями LPWAN¹⁶⁶. Систему планируется применять в широком спектре ниш и бизнес-кейсов, включая технический контроль электросетей, сооружений и трубопроводов, контроль ЖКХ в удаленных населенных пунктах, контроль оборудования геофизических методов разведки, контроль паводков и гидротехнических сооружений, предупреждение

чрезвычайных ситуаций, экологический мониторинг, умное сельское хозяйство и социальные сервисы¹⁶⁷.

Создание такой системы стало бы мощным импульсом для развития российского рынка IoT. Однако преградами к завершению проекта в текущих условиях могут стать дефицит компонентной базы для спутникового оборудования вследствие санкций и возможная переориентация приоритетных направлений развития инфраструктуры спутниковой связи в России на двойные и военные применения.

2 Национальные стратегии развития интернета вещей



С каждым годом все больше государств разрабатывают программы и стратегии развития, развивают модели регулирования интернета вещей и связанных с ним смежных технологических ниш. Необходимость участия государства в развитии интернета вещей диктуется растущим вкладом его решений в экономику и рост ВВП, потребностью игроков национальных рынков в поддержке проектов по развитию базовой инфраструктуры для передачи и обработки межмашинных данных и, наконец, вызовами с точки зрения кибербезопасности, защиты M2M-данных и соблюдения прав граждан и других участников бизнес-процессов, основанных на решениях IoT. В этом разделе фокус сделан на подходах трех крупнейших рынков IoT в страновом разрезе – ЕС, США и КНР. Кроме того, рассматривается выборка представляющих различные регионы мира государств, которые активно формируют и развивают стратегии в области IoT.

Мировые лидеры

Европейский союз



Стратегия для IoT

Общая стратегия ЕС в отношении развития технологий и формирования спроса на рынке интернета вещей строится не на прямых инвестициях и финансовой поддержке участников рынка, а на развитии экосистемы технологических альянсов и сообществ, стимулировании совместных проектов и точечной поддержке малых и средних предприятий (МСП). Вторым ключевым инструментом является разработка регуляторных моделей, способствующих расширению рынка M2M-данных в рамках развития комплексной концепции экономики данных в ЕС.

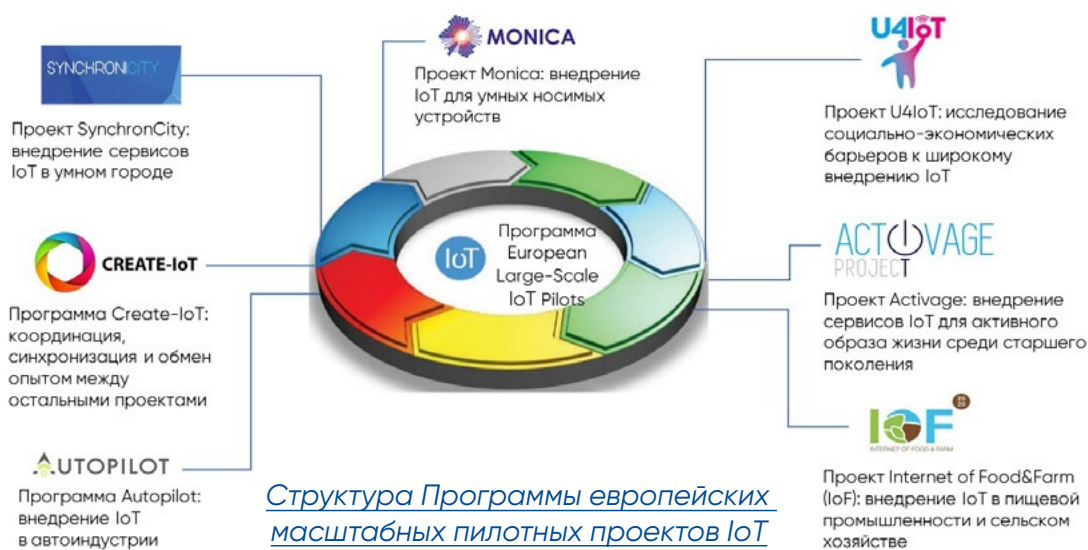
В принятой в 2015 г. основополагающей Стратегии для единого цифрового рынка ЕС (Digital Single Market Strategy) IoT был определен в качестве одной из технологий, имеющих решающее значение для глобальной рыночной конкурентоспособности Евросоюза, наряду с технологиями облачных сервисов и обработки больших данных¹⁶⁸. В качестве одной из приоритетных задач указывалось выстраивание четкой системы норм, регулирующих доступ к M2M-данным, ответственность за их хранение, обработку и использование.

Комплексный подход к повестке IoT оформился в рабочем документе Еврокомиссии «Продвигая развитие интернета вещей в Европе»¹⁶⁹, принятом в 2016 г. в рамках развития Стратегии единого цифрового рынка. Документ вобрал в себя широкий спектр вопросов, связанных с развитием технологий, стандартов, рынка и отраслевого сообщества IoT. В части механизмов поддержки и формирования спроса на рынке акцент сделан на внедрение прикладных решений IoT в конкретные отрасли и ниши, такие как умный дом и умный город, цифровая агропромышленность, ИТС и прочее.

Финансирование проектов IoT

Реализация разработанных стратегических подходов обеспечивается за счет развития системы параллельных потоков и инструментов грантового финансирования. Такие механизмы в основном были сконцентрированы в нише R&D и направлены на сектор МСП:

- В 2015 г. Еврокомиссия выделила первый раунд финансирования в 53 млн евро для МСП на реализацию проекта «Платформы подключенных умных объектов».¹⁷⁰ Цель проекта состояла в разработке платформенных решений IoT, которые помогли бы обеспечить совместимость решений различных участников рынка.
- В декабре 2018 г. Еврокомиссия согласовала совместный проект Франции, Германии, Великобритании и Италии.¹⁷¹ Государства – участники проекта выделили в общей сложности 1,75 млрд евро на реализацию совместного проекта в области микроэлектроники для IoT и отрасли беспилотного автотранспорта. Проект предполагал совместные разработки и тестирование инноваций 29 участниками в рамках 40 связанных субпроектов, из которых 10 направлены на создание умных сенсоров нового поколения для различных применений IoT. По расчетам авторов проекта, до момента завершения в 2024 г. в проект удастся привлечь 6 млрд евро частных инвестиций.
- В общей сложности к концу 2020 г. ЕС выделил почти 500 млн евро на реализацию проектов по НИОКР, тестированию и внедрению инноваций в нише IoT в рамках основополагающей программы финансирования исследований и разработок в перспективных технологических нишах Horizon 2020¹⁷². Основным проектным направлением стала разработка совместимых сервисных платформ, в том числе для индустриальных применений IoT.
- Одной из крупнейших профинансированных в рамках Horizon 2020 инициатив развития IoT стала Программа европейских масштабных пилотных проектов IoT (European Large-Scale IoT Pilots) с общим бюджетом более 100 млн евро на 2016–2020 гг.¹⁷³ В структуру программы вошли 7 проектов, нацеленных на создание и масштабирование пилотных моделей применений IoT в отдельных отраслях и нишах (см. схему ниже)¹⁷⁴.



- В 2020 г. на смену Horizon 2020 пришла новая основополагающая программа – Horizon Europe с бюджетом 95,5 млрд евро до 2027 г. В рамках программы в том же году было объявлено о направлении 150 млн евро на НИОКР и тестирование инноваций в нише решений для IoT на базе периферийных вычислений и облачных сервисов¹⁷⁵.
- В структуру Horizon Europe входит кластер № 4 «Цифровые технологии, промышленность и космос»¹⁷⁶, через который до 2027 г. будут проходить и другие тендеры на распределение финансирования по проектам IoT.

Магистральный тренд последних 2–3 лет – все большее включение в фокус тематики для грантовой поддержки проектов умных периферийных вычислений и «распределенного IoT». За 2021–2022 гг. в рамках Horizon Europe было предусмотрено распределение грантов на исследования сред и инструментов для распределенного интеллекта в периферийных системах (4–8 млн евро), метаоперационных систем для граничных вычислений (8–12 млн евро) и фреймворков когнитивных облаков с поддержкой ИИ на периферии (4–6 млн евро)¹⁷⁷. На 2023 г. планируется финансирование «вертикальных» исследований с масштабированием и апробацией проектов по теме умного промышленного IoT с поддержкой распределенного на периферию вычислительного ядра¹⁷⁸.

Радиочастотное регулирование для развития IoT

Параллельно с финансовым стимулированием сектора IoT власти ЕС приняли ряд мер для расширения доступа участникам рынка к радиочастотам. Базовым инструментом в этой сфере является рамочное решение Еврокомиссии № 676/2002/ЕС, которое позволяет регулятору гармонизировать необходимые полосы частот для своевременной поддержки инноваций и перспективных технологий на европейском рынке¹⁷⁹.

В октябре 2018 г. решением Еврокомиссии были гармонизированы полосы частот в диапазоне 874–876 МГц и 915–921 МГц¹⁸⁰. Указанные полосы частот востребованы для сервисов IoT, использующих беспроводные подключения малого радиуса действия, такие как новые версии RFID. Следующим шагом в октябре 2020 г. стала гармонизация полос частот в диапазоне 5875–5935 МГц¹⁸¹. Это решение вдвое расширило полосу частот, доступную для организации беспроводных широкополосных подключений к инфраструктуре ИТС. Гармонизация дополнительных частот в диапазоне 5,9 ГГц существенно расширила возможности для решений по управлению подключенными автомобилями и беспилотными поездами в ЕС. Наконец, в июне 2021 г. были освобождены еще 480 МГц в диапазоне 6 ГГц (5945–6425 МГц)¹⁸², что открыло широкие возможности для развития беспроводных подключений IoT прежде всего на базе Wi-Fi 6E.

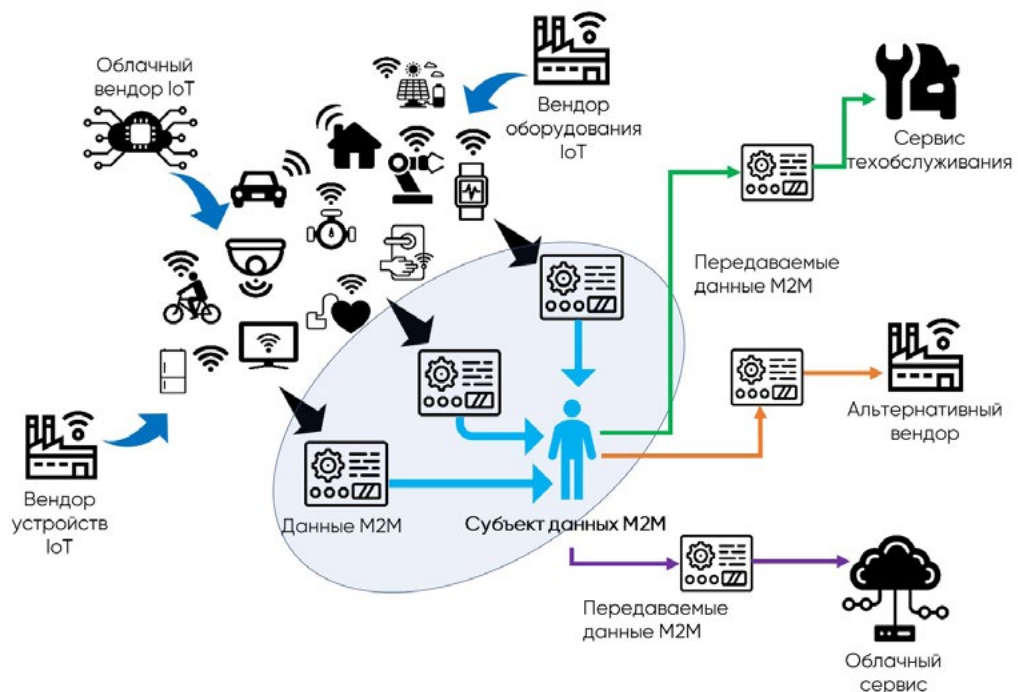
Регулирование M2M-данных

В 2022 г. ЕС приступил к выстраиванию кардинально нового подхода к регулированию M2M-данных в рамках реализации Стратегии в отношении данных (European Data Strategy), утвержденной в 2020 г.¹⁸³ 23 февраля 2022 г. Еврокомиссия одобрила проект европейского Закона о данных (EU Data Act)¹⁸⁴, который в случае принятия будет иметь прямое действие на территории всех государств – членов Евросоюза. Законопроект первым из всех национальных НПА в мире создает комплексную систему регулирования

прав на данные, генерируемые в результате межмашинных взаимодействий, включая права на доступ к таким данным и распоряжение ими для различных субъектов. В частности, согласно Data Act:

- Производители оборудования и устройств IoT обязаны предоставить пользователям доступ к данным, генерируемым в процессе работы этих устройств и оборудования.
- Разработчики и вендоры оборудования и устройств IoT должны будут проектировать свои решения таким образом, чтобы изначально закладывать в них возможность доступа пользователей (граждан и бизнеса) к генерируемым M2M-данным.
- Кроме того, как физические лица, так и бизнесы, использующие сервисы на базе устройств и оборудования IoT, уполномочены предоставлять право на доступ к «своим» M2M-данным третьим сторонам, в том числе сервисам постпродажного технического обслуживания. От этого требования освобождены вендоры в сегменте СМП.
- Раскрытие доступа к M2M-данным коммерческих сервисов государственным органам предусмотрено в случае чрезвычайной ситуации или иной государственной необходимости в исключительных обстоятельствах.
- Закрепляется система минимальных требований к провайдерам сервисов облачных и граничных вычислений (куда попадает большая доля сервисов IoT) по обеспечению технической возможности для миграции их пользователей на другие аналогичные сервисы без потери данных. Таким образом, законопроект впервые вводит в действие концепцию переносимости M2M-данных.
- Наконец, закон вводит требования о применении открытых стандартов совместимости для сервисов облачной и граничной обработки данных, включая прежде всего M2M-данные.

Реализация права пользователей устройств и сервисов IoT на доступ к данным M2M и их передачи третьим сторонам в рамках EU Data Act



Data Act оценивается как огромный шаг вперед в регулировании данных IoT и преследует глобальные амбиции. Конечная цель законопроекта – обеспечить ЕС лидерство на мировом рынке данных IoT, а также трансформировать нишу облачных и граничных сервисов в единый мультивендорный рынок, где для всех участников открыты возможности бесшовного переключения между сервисами обработки M2M-данных.

Разработчики Data Act ожидают, что новая модель регулирования принесет в ВВП ЕС дополнительные 280 млрд евро до 2028 г. и расширит объем экономики данных ЕС до 829 млрд евро (по сравнению с 301 млрд евро в 2018 г.)¹⁸⁵. Только в сегменте управления дорожным трафиком оценочный экономический эффект в шестилетнем временном горизонте составит до 20 млрд евро¹⁸⁶. Потенциал рынка межмашинных данных для ЕС подтверждают и другие источники: проведенное в 2018 г. углубленное эконометрическое моделирование Deloitte показало, что создание оптимального комплексного режима регулирования M2M-данных может добавить 1,4 трлн евро к ВВП ЕС в горизонте 10 лет (с 2018 по 2027 гг.)¹⁸⁷.

Таким образом, если в ближайшие годы новые модели регулирования, включая EU Data Act, будут утверждены и окажутся в полной мере востребованы рынком, ЕС может упрочить глобальное лидерство в нише экономики M2M-данных и на равных конкурировать с США и КНР как минимум в среднесрочной перспективе.

При этом избыточное регулирование одновременно является главным барьером на пути развития сервисов IoT нового поколения и расширения их рынка в ЕС. Комплексное исследование Vodafone от 2019 г. выявило, что на проекты IoT в 12 отраслях экономики ЕС распространяются требования как минимум 24 нормативно-правовых актов (НПА) общеевропейского уровня¹⁸⁸. По отзывам участников рынка IoT, для беспрепятственного развития технологий и бизнес-моделей в пользовательском сегменте (B2C) 61 % этих НПА требовали отмены, обновления либо иного изменения. В сегменте B2B такими оказались все действующие на тот момент НПА, затрагивающие рынок IoT¹⁸⁹.

КНР



Стратегия для IoT

В отличие от западных стран, государственное целеполагание в ключевых технологических нишах в КНР намного более директивно. Правительство и Коммунистическая партия, действуя в горизонте общих пятилетних планов развития, формируют жесткие целевые показатели по проникновению/доступу граждан и бизнеса к технологической инфраструктуре, числу платформ и установленных узлов оборудования, переходу предприятий на новые спецификации и технические решения и даже росту рынков и бизнесов.

Комплексный подход государства к развитию интернета вещей сформировался к 2015 г., когда была разработана и утверждена серия национальных планов «Интернет +». Вопросы развития IoT по большей части сконцентрировались в плане «Интернет + производство». Планы развития «Интернет +» продвигались и реализовывались совместно с инициативой «Сделано в Китае 2025», принятой в 2015 г.¹⁹⁰ Инициатива, спроектированная под сильным влиянием германской стратегии «Индустрия 4.0», рассматривала IoT, прежде всего в промышленных применениях,

как один из главных технологических факторов повышения производительности и конкурентоспособности китайских производств. В число наиболее перспективных применений IIoT включались умный мониторинг технологических процессов, удаленная диагностика оборудования и управление производственными процессами и оцифрованными цепочками поставок.

Среди конкретных целей в части IoT документ «Сделано в Китае 2025» указывал создание системы технических стандартов и производственно-технологической базы, достаточной для того, чтобы к 2020 г. китайские производители занимали 40 % домашнего рынка в сегментах оборудования для индустриального IoT, промышленных сенсоров и цифровых АСУ ТП¹⁹¹.

За общей стратегией последовала выработка и других документов, уточнявших и конкретизировавших ее положения в части развития IoT. По данным исследований, только за период 2010–2017 гг. на уровне центрального правительства и КПК было принято не менее 15 документов стратегического планирования, посвященных вопросам развития отрасли IoT или включавших эту тему как одну из основных¹⁹².

Новый уровень проработки государственной стратегии в отношении развития IoT был обеспечен в 2021 г. с параллельным утверждением двух трехлетних планов действий:

1. План действий по развитию и внедрению инноваций для индустриального интернета вещей на 2021–2023 гг.¹⁹³
2. План действий по созданию новой инфраструктуры интернета вещей на 2021–2023 гг.¹⁹⁴

В обоих планах устанавливаются сходные и взаимосвязанные целевые ориентиры, в том числе (подробнее см. Приложение № 1):

- Максимально глубокая интеграция IoT и индустриального IoT с другими прорывными технологиями, включая прежде всего 5G (связка IoT+5G) и граничные вычисления, ИИ, блокчейн, большие данные и облачные сервисы.
- «Выращивание» пула компаний – рыночных лидеров первого и второго эшелонов, которые смогут осуществлять экспансию на международные рынки и насыщать лучшими практиками и инновациями малых игроков домашнего рынка.
- Опережающее и массовое внедрение интегрированных платформ IoT на национальном, региональном и отраслевом уровнях.
- Качественный рывок в уровне развития и конкурентоспособности ключевых технологий, таких как высокоточные сенсоры, чипы и операционные системы IoT.
- Создание национальной кросс-отраслевой системы демонстрационных полигонов технологий индустриального IoT для тиражирования лучшего опыта и продвижения инноваций.
- Укрепление регуляторной, инновационной и нормативно-технической поддержки развития рынка, включая формирование комплексной системы национальных стандартов IoT.

Масштабная финансовая поддержка отрасли IoT предусмотрена в принятых стратегических документах на системном уровне. В частности, План развития отрасли ИКТ на 2016–2020 гг. призывал центральное правительство расширить налоговые стимулы для производителей устройств и разработчиков сервисов интернета вещей, поддержать R&D и коммерциализацию ключевых технологических решений IoT, расширить кредитную поддержку крупных нишевых проектов¹⁹⁵. Кроме того, в документе предлагалось создать стимулы для привлечения частных и венчурных инвестиций в интернет вещей и подталкивать региональные и местные администрации к расширению сети фондов поддержки проектов IoT¹⁹⁶.

На основе анализа положений стратегических документов и открытых данных по поддержке проектов IoT просматриваются 3 основных канала поддержки проектов IoT в стране:

1. Инвестиции из бюджета центрального правительства, распределяемые, как правило, через сеть целевых отраслевых фондов.
 - Созданный в 2011 г. Специальный фонд проектов IoT за 2011–2015 гг. вложил не менее 320 млн долл. США из бюджета Министерства финансов в более 500 проектов R&D в нише IoT¹⁹⁷. Деньги распределялись в форме грантов и льготных кредитов¹⁹⁸ в пределах общего бюджета фонда в 500 млн долл. США.
 - С 2017 г. на поддержку проектов индустриального IoT начало выделяться целевое финансирование из средств Китайского фонда инвестиций в интернет вещей (общий бюджет фонда – порядка 14,5 млрд долл. США)¹⁹⁹.
2. Инвестиции из бюджетов региональных властей и местных администраций, которые составляют существенную долю государственной поддержки IoT в целом.
 - В 2010 г. администрация г. Цзянсу выделила порядка 28 млн долл. США на местные R&D-проекты в нише IoT. Специальные проектные фонды инвестиций в IoT были созданы в начале 2010-х гг. правительствами провинций Аньхой и Фуцзянь²⁰⁰.
 - Еще одним из «пионеров» в поддержке интернета вещей на местном уровне стал Шанхай, в 2010 г. открывший линию финансирования в объеме порядка 62 млн долл. США в рамках Фонда инвестиций в предпринимательство в области IoT²⁰¹.
 - Похожие по структуре, задачам и механизмам финансирования (субсидии, гранты, льготные займы и прочее) фонды в 2012–2017 гг. были созданы и в ряде других городов и провинций, включая города Сиань и Уси. В 2012 г. в Уси был сформирован Фонд капитальных инвестиций в IoT для национальной аэрокосмической элиты, через который финансировались проекты IoT двойного назначения на общую сумму порядка 50 млн долл. США²⁰². В 2017 г. городскими властями Уси был учрежден Целевой фонд инвестиций в отрасль IoT с бюджетом порядка 760 млн долл. США²⁰³.

3. Третий «столп» финансовой поддержки развития IoT в КНР – венчурные инвестиции. Формально большинство венчурных фондов в стране не считаются государственными и по составу учредителей могут быть названы частными. Однако в расширенном смысле ниша венчурных инвестиций в IoT в стране является прямым продолжением государственной стратегии в сфере развития IoT.
- Многие фонды венчурных инвестиций имеют смешанный состав учредителей и «гибридный» бюджет, в который в том числе распределяются средства крупных государственных фондов.
 - Во-вторых, сам факт бурного разрастания венчурных фондов для проектов IoT во многом обусловлен вектором государственной политики в этой сфере.
 - По последним данным, за 2021 г. частное и венчурное финансирование на общую сумму порядка 460 млн долл. США получили 16 проектов IoT²⁰⁴. При этом, по сравнению с предыдущими годами (2018–2020), финансирование венчурных проектов IoT в стране укрупнилось по суммам на проект и уменьшилось по числу проектов²⁰⁵.
 - Общая оценка объема частных и венчурных инвестиций в проекты IoT за 2014–2021 гг. составляет 48 млрд юаней, или порядка 7 млрд долл. США²⁰⁶.

Радиочастотное регулирование для развития IoT

В части высвобождения радиоспектра для развития IoT китайский подход в последние годы отличается от подходов западных государств. Все больший приоритет уделяется нуждам «расчистки» диапазона для развития 5G.

- Один из примеров – решение использовать под 5G весь диапазон 6 ГГц (5925–7125 МГц)²⁰⁷, который в ЕС, США и ряде других стран в основном гармонизирован под беспроводную связь малого радиуса действия (прежде всего Wi-Fi 6, обеспечивающий значительную долю всех подключений IoT).
- Такое решение служит подтверждением того, что в качестве перспективной технологической связки на ближайшее будущее рассматривается именно IoT на базе 5G.

Регулирование M2M-данных и обеспечение кибербезопасности IoT

В части регулирования M2M-данных значимым фактором для развития рынка стало принятие закона о безопасности данных²⁰⁸ в июне 2021 г. и закона о защите персональной информации²⁰⁹ в августе того же года. Оба НПА совместно формируют комплексную систему регулирования электронных данных в КНР, включая требования по их обработке, хранению, обеспечению безопасности и ограничения на их трансграничную передачу. Хотя M2M-данные не выделены в законах в отдельную категорию, они не исключены из их действия. Поэтому к вендорам сервисов IoT, собирающих и обрабатывающих данные пользователей и их устройств, применяется вся линейка новых требований (за исключением ряда положений, касающихся персональной информации). Окончательный эффект нового законодательства для китайского рынка IoT пока не оценен, однако субъекты рынка могут столкнуться

с серьезными трудностями при развитии трансграничных сервисов, таких как облачные платформы IoT и распределенные системы на базе граничных вычислений.

Несмотря на это, системная стратегическая работа, техническое регулирование и масштабные инвестиции государства в технологическое развитие и рыночную экспансию пока что ведут к успешному развитию IoT в КНР, если судить по цифрам.

- По официальным данным на март 2022 г., только в сегменте подключений на базе сотовой связи число активных IoT-устройств в КНР составило 1,464 млрд²¹⁰, то есть от 60 до 80 % таких подключений в целом по миру. Даже если эта статистика завышена, КНР остается крупнейшим в мире рынком сотового IoT, кратно превосходя США, ЕС и другие государства.
- По данным GSMA, сотовые подключения IoT в КНР вырастут до 2,29 млрд к 2025 г.²¹¹
- В денежном выражении, по последним оценкам IDC за декабрь 2021 г., объем китайского рынка IoT достигнет 300 млрд долл. США к 2025 г. и займет 26,1 % всего мирового рынка²¹².

США



Стратегия для IoT

Отдельные государственные инициативы по внедрению технологий IoT в США стартовали начиная с конца 2000-х гг. В 2012 г. в целях исполнения указа Президента США от 2009 г. о сокращении энергопотребления зданиями федеральных ведомств на 30 % к 2015 г.²¹³, Управление общих служб США (GSA) запустило программу Smart Buildings. Всего федеральные органы США с 2011 по 2015 г. потратили на закупки, связанные с IoT, порядка 35 млрд долл. США²¹⁴. Крупнейшие статьи расходов составили ПО для сервисов IoT (30,5 %), решения по обеспечению кибербезопасности IoT (24,5 %), а также устройства и оборудование, включая серверы для обработки M2M-данных (11 %) ²¹⁵.

Переход от ведомственных инициатив к системному рассмотрению повестки развития IoT начался с середины прошлого десятилетия. В марте 2015 г. Сенат принял резолюцию, призывавшую к разработке комплексной национальной стратегии для содействия опережающему внедрению интернета вещей в государственном и частном секторах²¹⁶. За резолюцией в марте 2016 г. последовало внесение в Сенат законопроекта о развитии инноваций и стимулировании роста IoT (DIGIT ACT)²¹⁷.

Законопроект выстраивал систему координации работы федеральных органов США по развитию IoT, описывал механизмы и площадки взаимодействия государства с отраслью и техническим сообществом и задавал общий фронт работ по стандартизации технологий IoT на национальном уровне. На площадке рабочих групп смешанного состава предлагалось выработать углубленные рекомендации по созданию условий для ускоренного внедрения технологий IoT в стране. На Федеральную комиссию по коммуникациям (FCC) возлагалась задача провести оценку потребностей участников рынка в доступе к радиочастотам, необходимым для развития IoT, и сформировать комплексную программу работы по высвобождению таких частот. Кроме того, DIGIT ACT призывал выработать комплексную национальную стратегию развития IoT.

Несмотря на то, что DIGIT Act неоднократно направлялся на доработку и был окончательно одобрен Сенатом только в 2020 г.²¹⁸, предложенные в нем меры уже реализованы как минимум в части радиочастотного регулирования.

2 апреля 2020 г. FCC опубликовала решение и отчет о высвобождении для нелицензируемого использования полос радиочастот суммарной шириной в 1200 МГц в диапазоне 6 ГГц²¹⁹. Доступ к этим полосам частот ранее был закреплен за вооруженными силами. В частности, указанный диапазон стал полностью открыт для беспроводных подключений низкой мощности внутри помещений. Как подчеркивается в документе FCC, решение открывает возможность проектирования целой ниши устройств, прежде всего датчиков, сенсоров и гаджетов умного дома, для работы в диапазоне 6 ГГц.

Решение Комиссии было принято с учетом продвижения на рынок протокола Wi-Fi 6E, наиболее эффективно работающего именно в этом диапазоне частот и адаптированного для сервисов IoT. Таким образом, FCC своим решением открыла для американского рынка огромную нишу для развития интернета вещей на базе локальных подключений по Wi-Fi 6E как в пользовательском сегменте, так и в промышленных применениях.

Отраслевое регулирование

Помимо радиочастотного регулирования, стимулирование внедрения интернета вещей в экономику США осуществляется и на отраслевом уровне. В апреле 2021 г. в Сенат был внесен проект закона о продвижении внедрения IoT для точного земледелия (Advancing IoT for Precision Agriculture Act of 2021)²²⁰. В законопроекте предлагается расширить грантовую поддержку R&D в области IoT для точного земледелия за счет бюджета Национального фонда науки (NSF), включить аграрные применения IoT в программы образования NSF по передовым технологиям, подготовить правительственный отчет о внедрении IoT в агросектор и провести оценку государственных программ поддержки точного земледелия.

Финансирование R&D в нише IoT

Модель финансовой поддержки развития IoT в США не предполагает массивных прямых государственных инвестиций. Основными задачами являются создание благоприятной регуляторной среды для развития рынка и поддержка R&D. В рамках последнего направления наибольшая часть финансирования выделяется через механизм Программы исследований и разработок в области информационных и сетевых технологий (Networking and Information Technology Research and Development, NITRD) – комплексного механизма координации и управления R&D под нужды федеральных властей, как гражданских, так и оборонных²²¹. IoT включен в качестве одной из ведущих тематик работы как минимум в 3 направления программы: сетевые киберфизические системы (CNPS), кибербезопасность и приватность (CSP), промышленная робототехника и автономные системы (IRAS)²²². Общий бюджет этих 3 направлений за 2022 г. составляет 1,188 млрд долл. США, а с 2015 г. по настоящее время – более 9 млрд долл. США²²³.

Еще одним важным направлением государственной активности в последние годы стало обеспечение кибербезопасности решений на базе IoT. В декабре 2020 г. был принят закон о повышении кибербезопасности IoT (IoT Cybersecurity Improvement Act)²²⁴, который обязал Национальный институт стандартизации и технологии (NIST) разработать минимальные требования по обеспечению кибербезопасности подключаемых устройств IoT. Такие требования будут применяться лишь в отношении закупок устройств и оборудования IoT государственными органами США, однако ожидается, что значительная часть частных компаний будет осуществлять комплаенс добровольно²²⁵. Первая версия руководства по внедрению и выполнению требований к кибербезопасности устройств IoT для федеральных государственных органов была опубликована NIST в ноябре 2021 г.²²⁶

Таким образом, основной вектор американского подхода к развитию IoT направлен не на прямую поддержку компаний или отраслей, а на регуляторную работу по устранению рисков (кибербезопасность) и расчистку барьеров, тормозящих развитие рынка (доступ к нужным диапазонам радиоспектра). Пока что принятые меры делают США одним из мировых «пионеров» как по созданию общих правил рынка в нише кибербезопасности IoT, так и в «расчистке» имеющего огромное значение для рынка диапазона 6 ГГц.

Региональные примеры

Австралия



Стратегия для IoT и отраслевое регулирование

Австралия относится к числу стран, в которых развитие государственной политики в отношении IoT не включает в себя разработку единой стратегии на национальном уровне. Однако австралийская Стратегия цифровой экономики до 2030 г. включает IoT в список перспективных технологий, развитие которых обеспечит наибольший эффект для национальной экономики в 10-летней перспективе²²⁷.

Из отраслевых применений IoT в Стратегии указана электроэнергетика и внедрение умных сенсоров следующего поколения на объектах генерации и энергораспределения. Условием цифровой трансформации для отдельных рынков и экономики в целом выступает развитие IoT в связке с технологиями, усиливающими его преимущества, прежде всего мобильной связью пятого поколения. IoT не был выделен в качестве отдельной статьи расходов в бюджете Стратегии, однако ряд направлений в той или иной степени включают в себя связанные с ним проекты²²⁸:

- Развитие передовых технологий для авиационной отрасли и БПЛА (35,7 млн долл.).
- Поддержка внедрения перспективных цифровых технологий (включая сервисы на базе IoT и граничных вычислений) малым и средним бизнесом (12,7 млн долл.).

- Трансформация и повышение качества госуслуг, включая внедрение технологий IoT для государственных центров оказания услуг (200,1 млн долл.).

В 2021 г. развитие инфраструктуры для IoT вошло в число стратегических рекомендаций в обновленный долгосрочный План инфраструктурного развития Австралии (2021 Australian Infrastructure Plan)²²⁹. В документе ставится задача в течение 10–15 лет обеспечить покрытие национальной территории (в первую очередь, городских районов) высокоскоростной инфраструктурой связи для развития экосистемы умных городов на базе IoT и 5G.

Финансирование проектов IoT

Государственные механизмы поддержки развития IoT в большинстве случаев включают в себя инвестиции в инфраструктурные проекты, приоритетными нишами для которых являются умные города, сельское хозяйство, развитие инфраструктуры для местных сообществ и развертывание базовой инфраструктуры сетей связи для сервисов IoT. За последние 5 лет были запущены и реализованы следующие проекты:

- В 2017 г. правительством была запущена программа «Умные города и пригороды» (Smart Cities and Suburbs) общим бюджетом в 50 млн долл. На данный момент были закрыты два раунда финансирования проектов, более 50 % которых включали в себя применение технологий IoT для улучшения городской среды и инфраструктуры²³⁰.
- В том же году государственный Фонд инноваций для чистой энергетики выделил 10 млн долл. на поддержку проекта компании Thinxtra по строительству сети LPWAN для развертывания сервисов IoT в энергетическом секторе²³¹.
- Тогда же федеральное правительство профинансировало пятилетнюю программу «Умные фермы» (Smart Farms), в рамках которой 136 млн долл. распределяются в двух форматах: крупные гранты на партнерские проекты (до 4 млн долл.) и малые гранты для малых ферм (Small Grants for Small Farms)²³². Основная доля проектов связана с внедрением технологий IoT (умные сенсоры и датчики, видеонаблюдение, дроны, интеллектуальное управление сельхозоборудованием) в нишах точного земледелия, защиты биоразнообразия и экомониторинга.
- В 2017–2019 гг. была реализована грантовая программа Testlabs for Australia бюджетом в 6 млн долл.²³³ В рамках программы были поддержаны грантовые проекты по созданию 6 площадок для тестирования технологий производства 4.0, включая прежде всего промышленный IoT.

Помимо федеральных проектов, в развитие инфраструктуры и сервисов IoT инвестируют власти отдельных штатов. Так, в конце 2020 г. штат Новый Южный Уэльс запустил трехлетнюю программу Smart Places, в рамках которой государственные средства совместно с партнерским софинансированием на общую сумму 45 млн долл. будут направлены на грантовую поддержку проектов по улучшению городской среды за счет технологий умного видеонаблюдения, анализа и мониторинга трафика, умного менеджмента отходов и т. д.²³⁴ Весной 2021 г. правительство штата Виктория объявило, что совместно с компанией Xerox инвестирует 50 млн долл. в оснащение сенсорами IoT мостов и другой значимой дорожной инфраструктуры для мониторинга ее состояния²³⁵.

Обеспечение кибербезопасности IoT

Еще одним направлением работы регуляторов является повышение осведомленности участников рынка IoT о рисках кибербезопасности и снижение таких рисков. Осенью 2020 г. правительство опубликовало добровольный Кодекс практик по обеспечению кибербезопасности IoT для конечных пользователей²³⁶. В этом направлении Австралия движется синхронно с рядом других государств, включая Великобританию, США и ЕС. Вероятным следующим шагом станет разработка в 2023–2024 гг. законодательных требований по обеспечению безопасности устройств IoT для сегмента B2C.

Радиочастотное регулирование для развития IoT

Наконец, с середины 2010-х гг. австралийские регуляторы начали достаточно системно работать над расширением доступа операторов сервисов IoT к радиоспектру. В 2015 г. австралийское Управление по коммуникациям и медиа (ACMA) предложило освободить для нелицензируемого использования полосы частот в диапазонах 900 МГц, 2,4 ГГц и 5,8 ГГц, подходящие для энергоэффективных узкополосных сетей IoT²³⁷. В 2019 г. регулятор предложил упростить лицензирование для отдельных видов радиооборудования, используемых для построения сетей IoT²³⁸.

Общая оценка развития отрасли IoT в Австралии и усилий государства в этой области в конце 2020 г. приводилась в отчете Национального совета ученых-академиков (ACOLA)²³⁹. Согласно отчету, несмотря на успехи в ряде нишевых применений IoT, отрасль страдает от отсутствия комплексного подхода к ее развитию на государственном уровне. Для укрепления своих позиций на глобальном рынке решений IoT государству и частному сектору необходимо сконцентрироваться на опережающем развитии и поддержке тех ниш, где уже наработаны успешные кейсы и развиты компетенции, и ускорить внедрение перспективной инфраструктуры связи в общенациональном масштабе.

Бразилия



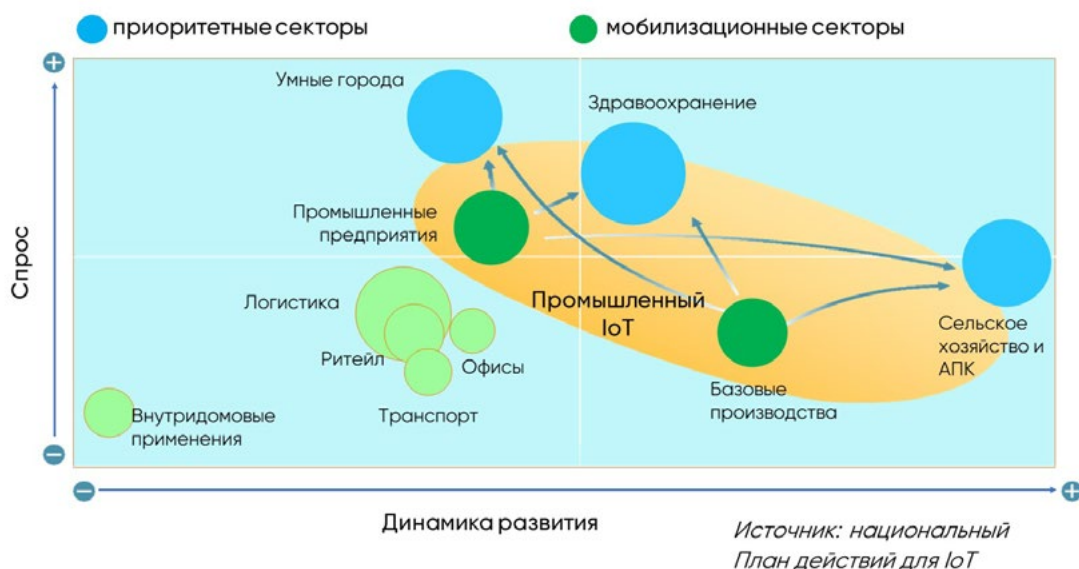
Стратегия для IoT

Развитие государственной политики в отношении IoT в Бразилии представляет собой пример «догоняющей стратегии». Систематизированная проработка развития отрасли и стимулирования рынка интернета вещей в Бразилии стартовала сравнительно поздно. Первый орган, координирующий вопросы развития IoT, – Управляющий офис по развитию систем M2M-коммуникаций – был создан при Министерстве по коммуникациям в 2014 г. и включил в свой состав представителей госструктур, отраслевых ассоциаций и научного сообщества²⁴⁰. До 2016 г. представители офиса в основном работали над расширением компетенций и обменом опытом в рамках программы сотрудничества с ЕС²⁴¹.

В 2016 г. бразильский Национальный банк развития (BNDES) совместно с Министерством коммуникаций заказал исследование с целью определить перспективные ниши экономико-технологического развития для страны на среднесрочную перспективу²⁴².

По результатам проведенной работы в ноябре 2017 г. был сформирован План действий для IoT – первый стратегический документ национального уровня в этой области²⁴³. В Плане были определены 4 приоритетных сектора для развития экосистемы IoT в Бразилии: сельское хозяйство и АПК, здравоохранение, промышленное производство и умные города.

Матрица приоритетных секторов развития IoT в Бразилии



Документ предлагал сконцентрировать работу правительства в части содействия развитию IoT на трех ключевых направлениях²⁴⁴:

1. Формирование национальной экосистемы инноваций для IoT, которая включала бы в себя координацию работы между ключевыми госорганами, концентрацию средств и проектов по поддержке IoT в нескольких крупных фондах, создание отраслевых «сетей инноваций» и системы «центров навыков» IoT для стимулирования спроса и выращивания компетентных кадров.
2. Создание онлайн-платформы «Обсерватория IoT», которая смогла бы играть роль базы знаний и лучших практик для бизнеса, а также служить площадкой для тренинговых программ и распределения финансирования рыночных проектов.
3. Разработка обновляемого руководства по внедрению технологий IoT в городах, которое бы охватывало кейсы и бенчмарки внедрения сервисов IoT в городское хозяйство, освещало вопросы технического регулирования и прочее.

В июне 2019 г. доработанный План был утвержден указом президента Бразилии²⁴⁵. Этим же указом был закреплён важный налоговый стимул: документ зафиксировал определение IoT как инфраструктуры, создающей добавленную стоимость. Таким образом, сервисы IoT оказались выведены из категории услуг электронных коммуникаций, а их вендоры и операторы освобождены от уплаты специального налога в государственный фонд фискального аудита телекоммуникаций (Fistel).²⁴⁶ С принятием указа План действий оказался вписан в общий контур национальной стратегии цифровой трансформации, утвержденной в 2018 г.²⁴⁷

Дальнейшая реализация плана в части финансового стимулирования рынка и спроса на сервисы IoT поддерживалась прежде всего через механизм налоговых льгот. Так, в декабре 2020 г. в ряд законов были внесены поправки, которые обнуляли ставку по 4 различным видам налогов для телекоммуникационного оборудования, предназначенного для поддержки систем M2M-взаимодействий²⁴⁸. Действие налоговых льгот распространяется на 2021–2025 гг. В результате на сегодняшний день сервисы IoT в Бразилии освобождены от большей части налогов, действующих в отношении телекоммуникационных сервисов, включая, например, налог на услуги по межрегиональным и межмуниципальным перевозкам и коммуникациям, ставка которого может составлять до 18 % от оборота²⁴⁹.

В дополнение к налоговым стимулам правительство начало развивать механизм венчурных инвестиций в отрасль IoT. В 2021 г. Банк развития Бразилии совместно с компанией Qualcomm Ventures создал первый в стране венчурный фонд для поддержки стартапов IoT. Фонд действует под управлением венчурной компании Indicator Capital и распоряжается бюджетом порядка 45 млн долл. США. Ожидается, что за 10 лет новый механизм позволит поддержать посевными инвестициями не менее 30 стартапов в нише IoT²⁵⁰.

Мероприятия Плана действий IoT включают в себя и проведение исследований. В июле 2021 г. правительством был создан первый центр технологических разработок, в основные направления работ которого вошел IoT, робототехника и 5G²⁵¹.

Таким образом, за последние 3–5 лет в Бразилии сформировался и начал наполняться контур государственной стратегии по развитию технологической ниши и рынка IoT. Среди других стран Бразилию выделяет выраженный акцент на налоговые стимулы на фоне незначительных объемов прямого государственного финансирования сектора. Согласно исследованию McKinsey, проведенному в 2017 г. в рамках разработки Плана действия для IoT, в позитивном сценарии развитие IoT может добавить порядка 200 млрд долл. США в ВВП Бразилии до 2025 г.²⁵² Однако для реализации такого сценария необходимо преодолеть ряд сохраняющихся проблем, включая дефицит покрытия территории страны сетями связи для подключений устройств IoT и нехватку компетентных кадров.

Великобритания



Стратегия для IoT

Общие контуры государственного подхода к стимулированию инноваций и развития рынка IoT в Великобритании оформились в рамках работы над стратегией развития «Индустрии 4.0» в 2014–2015 гг. В основу британского подхода легли два механизма, применявшихся и для стимулирования развития национального рынка IoT:

1. Упор на поддержку МСП и стартапов через большое количество небольших проектных грантов, дающих возможности для их акселерации и ускоренного вывода решений на коммерческий рынок.

2. Проект High Value Manufacturing Catapult (HVMC)²⁵³ — эффективный механизм для кооперации между технологическими центрами «Индустрии 4.0». В рамках проекта была создана сеть центров, через которые шло распределение грантовых средств, а также площадок для их взаимодействия между собой, отраслевыми компаниями и стартапами в инновационных нишах, включая IoT. Все центры обменивались между собой полученной информацией и, кроме того, получили отдельный бюджет для поддержки совместных, межцентровых проектов.

При этом отдельная государственная стратегия для IoT в Великобритании так и не была выработана с середины 2010-х гг. по сей день, в отличие, например, от стратегий развития ИИ²⁵⁴ и 5G²⁵⁵. В результате работа по развитию отрасли и стимулированию рынка IoT ведется рядом государственных органов и с акцентом на различные темы и ниши.

Финансирование проектов IoT

Из финансовых инструментов основным являются малые по сумме, но многочисленные гранты, как правило направленные на R&D и акселерацию с выводом на рынок небольших пилотных проектов IoT. Основной объем прямых государственных инвестиций в таких форматах пришелся на середину 2010-х гг.:

- В рамках исследовательской программы EC Horizon 2020 в 2014 г. правительство Великобритании выделило 73 млн фунтов на R&D в нише IoT, включая проекты по развитию умных городов (18,5 млн фунтов) и умной энергетики (4,6 млн фунтов)²⁵⁶.
- В 2015 г. для управления распределением этих средств и созданием системы IoT-проектов была запущена трехлетняя программа IoTUK²⁵⁷. Ключевой амбицией программы было создать условия для массовой, поточной акселерации стартапов и малых проектов в сфере IoT до полноценных рыночных решений²⁵⁸.

Радиочастотное регулирование для развития IoT

За последние годы правительственные органы предприняли ряд мер для увеличения объема радиочастотного ресурса, доступного для использования сервисами IoT. Еще после утверждения в 2015 г. предыдущей версии Стратегии управления радиочастотным спектром британское Управление по коммуникациям (Ofcom) освободило частоты в диапазонах 2,4 ГГц и 5 ГГц, широко используемых в различных отраслях IoT для подключений малого радиуса действия на базе Wi-Fi²⁵⁹.

В 2020 г. Ofcom предложил высвободить для нелицензируемого использования нижнюю часть 6-гигагерцевого диапазона (5925–6425 МГц)²⁶⁰. В частности, такие частоты смогут использоваться для подключений малого радиуса действия внутри помещений и (на малой мощности) вне помещений. Предложение регулятора актуально прежде всего для сервисов IoT, в которых подключение обеспечивается за счет последних поколений Wi-Fi (Wi-Fi 6E и в перспективе Wi-Fi 7). В обновленной в 2021 г. Стратегии управления радиочастотным спектром Ofcom отмечает развитие IoT в качестве одного из приоритетов, исходя из которых будет осуществляться распределение радиоресурса²⁶¹.

Обеспечение кибербезопасности IoT

За последние годы в фокус внимания правительства вошло обеспечение кибербезопасности устройств интернета вещей в пользовательском сегменте. Работа в этом направлении ведется как через механизмы государственной поддержки, так и за счет развития регулирования:

- В 2019 г. государственное Агентство исследований и инноваций (UKRI) запустило программу грантов на разработку решений по повышению кибербезопасности пользовательских устройств IoT бюджетом в 6 млн фунтов²⁶².
- Аналогичный грантовый фонд на 400 тыс. фунтов запустило в 2020 г. Министерство по цифровым технологиям, культуре, медиа и спорту (DCMS)²⁶³.
- В 2021 г. исследовательский консорциум PETRAS IoT Hub, созданный UKRI совместно с ведущими британскими вузами в 2016 г., распределил 3,6 млн фунтов на исследовательские проекты в нише кибербезопасности сервисов граничных вычислений²⁶⁴.

Проработка вопросов кибербезопасности устройств и сервисов IoT, а также защиты M2M-данных началась на законодательном уровне. В 2018 г. правительство разработало Свод правил по обеспечению безопасности в пользовательском сегменте IoT (Code of Practice for Consumer IoT Security)²⁶⁵. Документ был адресован вендорам пользовательских умных устройств и содержал рекомендации по повышению уровня их кибербезопасности.

Однако рекомендательных норм оказалось недостаточно. В ноябре 2021 г. в парламент был внесен проект Закона о безопасности продуктов и телекоммуникационной инфраструктуры (PSTI Bill)²⁶⁶. Законопроект²⁶⁷ устанавливает набор минимальных требований к кибербезопасности подключенных устройств, включая как смартфоны, так и устройства IoT в сегменте для конечных пользователей. В том числе вводятся запрет стандартных заводских паролей для устройств IoT, обязательная разработка их вендорами политики раскрытия уязвимостей и обязательное информирование пользователей о сроках поддержки обновлений безопасности для продуктов. Перечисленные требования вводятся в силу в течение 12 месяцев с момента принятия закона и распространяются на производителей, вендоров и дистрибьюторов устройств IoT. Соблюдение требований обеспечивается в том числе за счет достаточно жестких штрафов (до 4 % от общего оборота компании).

В итоге на сегодняшний день Великобритания представляет собой интересный и противоречивый пример с точки зрения эффективности государственной политики развития IoT. Объем британского рынка интернета вещей, по оценкам, составит порядка 21,8 млрд долл. США к 2026 г., что существенно меньше прогнозируемого объема рынка Германии и ближе к оценке рынка Италии, в целом чуть менее развитой экономически. Кроме того, британские компании не доминируют в сегменте крупных платформ IoT, где гораздо сильнее представлены немецкие, китайские и американские компании. В то же время в нише регулирования кибербезопасности IoT Великобритания опережает большинство государств; кроме того, эффективной можно назвать и работу по регулированию радиочастотного спектра. Слабые места британского подхода – отсутствие единой национальной стратегии развития IoT, невысокие объемы государственной поддержки в сфере R&D и недостаточная координация между регуляторами.



Южная Корея

Стратегия для IoT

Южная Корея одной из первых в мире разработала и приняла комплексную национальную стратегию развития IoT. Утвержденный в мае 2014 г. Мастер-план по развитию IoT²⁶⁸ ставил долгосрочные цели по созданию открытых IoT-платформ за счет совместных проектов крупных компаний, активизации участия корейских игроков на международном рынке и глобальных индустриальных альянсов, формирующих стандарты де-факто для применений интернета вещей.

Ключевым приоритетом в Мастер-плане было названо создание среды открытых инноваций для разработки совместимых IoT-решений и формирования национальной технологической экосистемы интернета вещей²⁶⁹. Как и в стратегиях других государств, прорывное развитие рынка IoT в Южной Корее в Мастер-плане 2014 г. было тесно связано с развитием сетей 5G и массовым переходом на IPv6²⁷⁰.

Правительство предоставило масштабные финансовые ресурсы для достижения заявленных целей:

- В соответствии с дорожной картой по реализации Мастер-плана до 2020 г. предполагалось инвестировать 5 млрд долл. США в различные ниши IoT-рынка – от подключенных автомобилей и промышленных платформ до носимых устройств²⁷¹.
- В 2015 г. в рамках исполнения дорожной карты правительство выделило 350 млн долл. США более чем 300 корейским производителям подключаемых устройств IoT²⁷².

Финансирование проектов IoT

Параллельно с реализацией Мастер-плана была сформирована государственная программа поддержки внедрения IoT на малых и средних предприятиях, связанных с промышленным сектором. Это направление было запущено еще в 2014 г. с принятием Стратегии инноваций в промышленном производстве 3.0 и разработкой в ее рамках стратегической инициативы «Умная фабрика» (Smart Factory)²⁷³. Внедрение технологий промышленной автоматизации, сенсорных сетей и киберфизических систем было определено одним из ключевых направлений инициативы. Долгосрочная цель была определена как создание в стране 10 тыс. умных фабрик к 2020 г., позднее показатель был скорректирован на 30 тыс. умных фабрик к 2025 г.²⁷⁴

Основными механизмами государственной поддержки предприятий в рамках инициативы стали:

- Прямые государственные инвестиции. В 2014–2017 гг. государство вложило порядка 190 млн долл. США в малые и средние промпредприятия по схеме «50:50»²⁷⁵.
- С 2018 г. государство стало включаться в качестве соинвестора в добровольные совместные проекты крупных промышленных компаний с малыми и средними промпредприятиями по трансформации последних в умные фабрики. Финансовое участие государства строилось по схеме «3:3:4» (государство – крупные предприятия – малые и средние производства)²⁷⁶.

- Передача малым и средним промпроизводствам промышленно-технологических ноу-хау других предприятий через специально созданный механизм ГЧП Korea Smart Factory Foundation (KSFF)²⁷⁷.
- Через KSFF, выступающий управляющим центром инициативы, государство координировало планирование и управление технологическим развитием умных фабрик.

Реализация инициативы «Умная фабрика» за 2014–2020 гг. обернулась серьезным успехом: по консолидированным отчетным данным, предприятия, принявшие участие в программе, повысили производительность на 25 %, сократив объем брака на 27 %²⁷⁸. При этом одним из наиболее успешных решений было признано внедрение индустриального IoT и систем автоматизации на его базе.

Полученные результаты обусловили продолжение и расширение инициативы «Умная фабрика» в план по развитию «умных» индустриальных комплексов. В рамках плана в 2020 г. правительство инвестировало 414 млн долл. США в создание умных фабрик по 11 направлениям, включая создание платформ обработки промышленных данных и кастомизированную автоматизацию производственных процессов на базе IoT²⁷⁹. Общий трехлетний бюджет плана на 2020–2022 гг. составляет порядка 650 млн долл. США и включает инвестиции в создание 10 «умных» производственных комплексов на базе технологий индустриального IoT и интеллектуальной автоматизации, платформ индустриальных облаков, ИИ и больших данных²⁸⁰.

В 2021 г. повестка развития IoT в стране была вписана в новую всеобъемлющую национальную программу цифровой трансформации – «Цифровую новую сделку» (Digital New Deal)²⁸¹. Интернет вещей включен как минимум в 2 из 9 ведущих направлений программы: создание кросс-отраслевых IoT-платформ с интегрированным блокчейном и развитие цифровых двойников в ключевых промышленных центрах.

В рамках реализации программы «Цифровая новая сделка» Министерство науки и ИКТ объявило о планах до 2025 г. вложить 2,2 млрд долл. США в развитие технологий гиперсвязности (Hyperconnectivity Plan)²⁸². Мегапроект фокусируется на внедрении прорывных технологий, включая блокчейн, технологии дополненной реальности и IoT, в ключевые отрасли национальной экономики.

Радиочастотное регулирование для развития IoT

Планы развития технологий всеобщей связности, включающей сети связи для IoT, поддерживаются достаточно активной работой корейских регуляторов по обеспечению необходимого радиочастотного ресурса. Гармонизация необходимых полос частот для сетей LPWAN (в диапазонах, близких к европейским) была реализована к 2016 г. В 2020 г. Южная Корея, вторая после США в мире, полностью освободила 6-гигагерцевый диапазон (5925–7125 МГц) для беспроводных подключений малого радиуса действия (Wi-Fi 6 и его модификации)²⁸³.

Таким образом, к 2022 г. Южная Корея, одной из первых в мире разработавшая отдельный комплексный план развития IoT, пришла к подходу, когда стратегическое видение развития интернета вещей интегрировано в комплексные программы цифровой трансформации и тесно взаимосвязано с развитием ряда других перспективных и прорывных технологий. Основной «рабочий инструмент»

государства – масштабные прямые инвестиции и соинвестиции в проекты цифровой трансформации МСП, включая прежде всего малые промпредприятия, – оказался эффективен как в целом для экономики, так и конкретно в части массового внедрения технологий IoT в промышленность.

Развитие IoT в России: возможности и барьеры для перехода на отечественные решения

Повестка управления развитием IoT в России в текущих условиях складывается из нескольких тематических блоков: государственные проекты, включая национальную программу «Цифровая экономика» и входящие в нее федеральные проекты; соглашения государственных корпораций и иных субъектов о развитии высокотехнологичных направлений (ВТН); ведомственные проекты отдельных ФОИВ; а также программы венчурного и грантового финансирования проектов по развитию IoT. Эти инициативы подробно рассматриваются в Приложении № 2 к настоящему отчету.

Общей ключевой проблемой в их реализации остается отсутствие у повестки развития IoT единой «точки прикрепления» и единого центра координации на уровне как правительства в целом, так и отдельных инициатив и программ финансирования и государственно-частного партнерства. В результате управление развитием IoT и созданием полноценной базы отечественного оборудования, программного обеспечения и сервисов интернета вещей происходит разнонаправленно на уровне различных ведомств, госкорпораций и институтов развития, а также источников финансирования.

Имеет смысл более подробно рассмотреть четыре аспекта, которые в наибольшей степени определяют перспективы формирования комплексного ландшафта отечественных технологий и продуктов IoT:

1. Мероприятия, направленные на импортозамещение оборудования IoT.
2. Разработка комплекса отечественных технических стандартов IoT.
3. Формирование в России отраслевого сообщества, способного координировать и объединять усилия для создания и продвижения на рынок отечественных решений IoT.
4. Развитие технологической и нормативно-правовой базы для обеспечения информационной безопасности инфраструктуры, ПО и сервисов IoT.

С 2019–2020 гг. активизируется курс на импортозамещение в нише оборудования для IoT, в том числе в рамках работы над задачами дорожных карт СЦТ, ВТО и других мероприятий, предусмотренных национальной программой. На сегодняшний день основные требования затрагивают сегмент оборудования для сетей LPWAN:

- В декабре 2018 г. ГКРЧ своим решением²⁸⁴ обязала операторов сетей LPWAN в нелицензируемых диапазонах 864–870 МГц с 1 декабря 2020 г. использовать только базовые станции, включенные в Реестр телекоммуникационного оборудования российского происхождения (ТОРП). Кроме того, вводилось требование об обязательной регистрации базовых станций.

От первого лица

Государственные регуляторные инициативы и требования уже выступают одним из ведущих драйверов развития российского рынка IoT, однако их эффект может быть усилен. Одним из полезных направлений работы может стать расширение сферы применения регулирования, аналогичного по своим принципам № 522-ФЗ от 27.12.2018, то есть предписывающего ресурсоснабжающим организациям внедрять «умные системы учета ресурсов». Распространение подобных норм на ниши водо-, газо- и теплоснабжения позволит формировать потребности рынка поставок этих ресурсов для производителей умных счетчиков, платформ автоматизированного учета и иных сервисов IoT.

Вторая перспективная область для регуляторных новаций как стимулов к развитию рынка – закрепление требований к сценариям работы устройств промышленного IoT, подразумевающих не только одностороннюю связь (сбор показаний/данных), но и управляющие воздействия (управление работой приборов/оборудования/объектов инфраструктуры). Для таких сценариев видятся логичными государственное регулирование радиочастотного ресурса и обязательная сертификация используемого оборудования IIoT.

Наконец, полезным может оказаться введение в поле публичного обсуждения и анализа вопроса государственного надзора за M2M-данными. Основная задача здесь – выбрать модель регулирования, которая позволит избежать чрезмерного обременения и расходов участников рынка на установку оборудования СОПМ и хранения данных (по аналогии с оборудованием, устанавливаемым на сетях операторов связи в рамках «пакета Яровой») на сетях и оборудовании IoT. Регуляторные принципы и нормы государственного надзора за данными должны применяться к сектору интернета вещей с учетом его специфики, в том числе колоссального числа подключений и объемов передаваемых M2M-данных.

- В январе 2020 г. ГКРЧ перенесла вступление в силу требования об использовании базовых станций, включенных в ТОРП²⁸⁵; соответствующее положение в итоге вступило в силу с 1 декабря 2021 г.
- Основными причинами отсрочки стали минимальное число российских решений для сетевого оборудования LPWAN в ТОРП и непрозрачность самой процедуры включения продукции в реестр²⁸⁶.



Елена Дубинская,
директор по
индустриальному
интернету,
ПАО «Ростелеком»

На сегодняшний день, уже после вступления требования ГКРЧ в силу, ситуация в части наполнения ТОРП российскими решениями принципиально не изменилась:

- На апрель 2022 г. в реестре ТОРП было представлено 5 базовых станций для несотовых сетей LPWAN от 4 производителей, из них 1 базовая станция NB-Fi, 3 базовые станции LoRaWAN^{287 288} и базовая станция для узкополосной сети на базе технологии «Стриж»²⁸⁹.
- В случае с оборудованием для сетей LoRaWAN речь не может идти о полном переходе на отечественные решения на уровне компонентной базы. Как отмечалось выше, монопольным производителем трансиверов для оборудования LoRaWAN является Semtech, держатель патента на базовую технологию модуляции сигнала LoRa.
- Представителями отрасли отмечалось, что текущая ситуация создает «бутылочное горлышко» в поставках базовых станций для рынка: два производителя в реестре ТОРП не способны удовлетворить рыночный спрос на оборудование LoRaWAN²⁹⁰.

Таким образом, требования по импортозамещению как инструмент в этом случае работают не вполне удачно, так как не учитывают низкую зрелость российских решений для оборудования сетей LPWAN. Более гибким вариантом могло быть введение требований по постепенной прогрессирующей локализации российского оборудования, уложенной в цикл от 3 до 5 лет.

Вопросы импортозамещения в нише IoT также были затронуты вторым пакетом мер поддержки отрасли ИТ как минимум по двум направлениям:

- С декабря 2021 г. предусматривалось введение требований об обязательном использовании российских операционных систем (ОС) в устройствах IoT в регулируемых государством сферах с целью повышения информационной безопасности.
- К тому же сроку предлагалось законодательно закрепить использование российских решений для IoT в жилищно-коммунальном комплексе, сфере обеспечения пожарной и другой безопасности.

Первое из этих предложений сопряжено с тем же риском, что и требования ГКРЧ к базовым станциям LPWAN, – на российском рынке пока недостаточно зрелых решений в нише ОС для IoT, чтобы заменить выпадающих зарубежных вендоров.

Альтернативный пример проработки вопросов импортозамещения оборудования для IoT представлен на площадке Общественного экспертного совета по использованию электроники в отраслях экономики при Президиуме Правительственной комиссии по цифровому развитию Российской Федерации²⁹¹. В функции Совета входит рассмотрение и отбор сквозных цифровых проектов отраслевого внедрения российских решений в области электронной продукции. Ключевое требование для рассматриваемых на площадке проектов – вклад в укрепление технологической независимости России.

- Механизм поддержки Совета предполагает субсидирование закупок компаниями российского оборудования, как для собственных нужд, так и для производства конечной продукции, на сумму от 300 млн руб. в течение 3 лет. Субсидия покрывает до половины стоимости закупок и затрат на внедрение

и разработку отечественной радиоэлектронной продукции²⁹². Виды оборудования, на которое распространяется поддержка, в том числе включают радиомодули и оконечные устройства IoT.

- В 2021 г. во внутренней структуре Совета создан Центр компетенций «Интернет вещей», работу которого в качестве базовой организации координирует ПАО «МТС». Цель структуры – способствовать формированию спроса на отечественную электронику в нише IoT по широкому спектру направлений, от недвижимости и ЖКХ до промышленности, ритейла и финтеха. Центр компетенций выполняет функцию экспертного фильтра для отбора проектов – получателей государственных субсидий, оценивая конкурентоспособность разработок, экономический эффект от внедрения, влияние на развитие российского рынка радиоэлектроники, экспортный потенциал и другие показатели. Один из примеров – согласованная в октябре 2022 г. господдержка проекта «Модернизация систем управления доступом», в рамках которой государство компенсирует инвестиции на внедрение умных домофонов на базе российской радиоэлектронной аппаратуры. В настоящее время Центром компетенций формируются новые проекты по направлению IoT.

В этой схеме продвижение отечественной продукции отталкивается от решений, предлагаемых участниками рынка. Такой подход снижает риск ситуации, когда требования по импортозамещению опережают возможности отечественных производителей. При этом объем средств на поддержку проектов IoT, распределенных через механизм площадки Общественного экспертного совета, затруднительно оценить.

Импортозамещение программного обеспечения для IoT

На уровне импортозамещения ПО и сервисов IoT основной импульс задает работа в рамках центров компетенций импортозамещения цифровых решений в ключевых отраслях экономики (ИЦК) и центров компетенций по развитию российского общесистемного и прикладного программного обеспечения (ЦКР). В совокупности созданные при участии государства и рыночных игроков координационные структуры 36 ИЦК и 9 направлений работы ЦКР охватывают практически все отрасли и секторы российской экономики.

Однако IoT в сформированной рамке ЦКР не выделен в отдельную технологическую нишу и направление работы по импортозамещению ПО. При этом в той или иной степени вопросы развития инфраструктуры и сервисов интернета вещей затрагивают как минимум 5 из 9 ЦКР: ОС, системы управления базами данных, облачные платформы, управление разработкой программного обеспечения и управление ИТ-инфраструктурой.

Аналогичным образом абсолютное большинство из 36 созданных ИЦК включили в свои шорт-листы проектов, выносимых на согласование Минцифры России, инициативы в области разработки и внедрения ПО систем сбора и передачи данных, облачных сервисов и промышленных интегрированных платформ IoT. В настоящий момент отобранные в рамках ИЦК проекты проходят стадию согласования ответственным ФОИВ, после чего можно будет более предметно оценить объем и структуру одобренных расходов, приходящихся на развитие IoT.

От первого лица



Павел Федосов,
директор по
стратегическим
проектам,
Группа компаний
«Цифра»

Один из ведущих трендов отечественного рынка сервисов промышленного IoT за последний год – ускоренное развитие и вывод на рынок платформенных решений, специализированных под нужды конкретных отраслей и технологических процессов предприятий. Прежде всего речь идет о платформенных сервисах промышленного IoT для горнодобывающих производств, нефте- и газодобывающего комплекса, а также нефтехимической отрасли и других сегментов ТЭК.

События 2022 г. поставили российских разработчиков продуктов IoT перед рядом вызовов, прежде всего в части доступа к аппаратным составляющим и микроэлектронным компонентам. Вместе с тем санкционные ограничения высветили необходимость поддержки интегрированных платформенных решений промышленного IoT отечественной разработки для текущих нужд предприятий. На текущий год портфель группы компаний «Цифра» насчитывает более 30 таких проектов. Также значительное количество таких проектов с нашим участием было поддержано в рамках отбора заявок по отраслевым ИЦК.

Если говорить о технологических трендах и бизнес-потребностях, мы также видим несколько ключевых моментов. Во-первых, все более перспективным и востребованным рынком становится развертывание платформенных сервисов IoT на базе частных промышленных сетей LTE. Согласно нашей аналитике, число проектов промышленных сетей 4G/LTE в России может достичь 50 по итогам текущего года и 380 – по итогам 2025 г. Накопленный объем рынка к концу 2025 г. может составить порядка 23 млрд руб.; при этом с каждым годом его рост будет все больше конвертироваться в увеличение объема рыночного сегмента сервисов промышленного IoT на базе бесшовной связи LTE в контуре предприятий.

Будет расширяться и функциональный спектр применений IoT для промышленных предприятий. В ближайшие годы возможности таких сервисов будут существенно усилены за счет интеграции промышленного IoT с все более зрелыми российскими решениями на базе ИИ. Мы рассматриваем технологии ИИ, промышленного IoT и частных сетей LTE (и в перспективе 5G) как ключевую технологическую связку, которая будет определять вектор и возможности цифровой трансформации российской промышленности в ближайшие годы. Наша задача – выступать флагманом развития этого «технологического треугольника» на базе импортонезависимых отечественных решений.

Развитие системы отечественных технических стандартов IoT

Активная работа по стандартизации технологий IoT стартовала с создания в структуре Росстандарта Технического комитета № 194 «Кибер-физические системы» (ТК 194).

- ТК 194 был учрежден 27 марта 2017 г., роль его базовой организации и секретариата была закреплена за «Российской венчурной компанией» (АО «РВК»).
- В составе ТК более 100 организаций, включая крупнейшие технологические и инфраструктурные компании, государственные органы, ведущие российские вузы, участников российского рынка IoT и отраслевые ассоциации²⁹³.

Стратегическую основу для деятельности ТК 194 заложил «Перспективный план по вопросам стандартизации в области передовых производственных технологий на период 2018–2025 гг.», разработанный в рамках НТИ²⁹⁴. Документ предусматривал разработку 32 стандартов для IoT, 19 стандартов для умного производства и 4 стандартов киберфизических систем. Дополнительными ориентирами для развития стандартизации IoT стали дорожные карты по направлениям НТИ «Технет» и «Энерджинет».

- Дорожная карта «Технет», принятая в 2017 г., предусматривала разработку и принятие до конца 2019 г. стандартов и технических регламентов, охватывающих полный цикл продукции и технических решений для M2M-взаимодействий и обмена данными на основе когнитивных интерфейсов²⁹⁵.
- В пакет предложений дорожной карты «Энерджинет» входила разработка набора стандартов для интеллектуальной энергетики на базе технологий IoT («Интернет энергии»)²⁹⁶.
- Отдельные упоминания стандартов для ниш IoT и M2M содержали паспорта федеральных проектов национальной программы «Цифровая экономика».

На 2022 г. в составе ТК 194 действуют 6 рабочих групп по технологическим направлениям: «Умные города», «Большие данные», «Умное производство», «ИИ» и «Умная энергетика»; еще одна РГ занимается разработкой рамочных стандартов для IoT. К 2020 г. по ряду этих направлений Техническим комитетом были разработаны первые серии проектов национальных стандартов:

- Январь 2020 г.: первая серия из 9 предварительных национальных стандартов (ПНСТ) для IoT, охватывавших общие термины и рамочную архитектуру IoT и промышленного IoT, требования к совместимости и платформам обмена данными IoT и сенсорным сетям.
- Январь 2020 г.: 10 ПНСТ по направлению «Умное производство», описывающих рамочную архитектуру производства 4.0 и цифровых двойников, требования к совместимости, взаимодействию и обмену данными.
- Март 2020 г.: 7 ПНСТ по направлению «Умный город». Проекты стандартов включали в себя общую онтологию и архитектуру показателей умного города, требования к интеграции и взаимодействию систем и данных, а также обзор передовых практик в отдельных нишах экосистемы умных городов.

Кроме того, работа ТК 194 позволила приступить к задаче адаптации международных стандартов для беспроводных сетей связи IoT и разработать первые собственные стандарты для российских технологий.

- С января 2021 г. введен в действие ГОСТ Р 59026-2020, вводящий российскую спецификацию **NB-IoT** и описывающий применения технологии.
- В июле 2021 г. вступил в силу проект стандарта ПНСТ 516-2021, описывающий российскую спецификацию сетевого протокола **LoRaWAN**.
- 5 марта 2022 г. был утвержден национальный стандарт ГОСТ Р 70036-2022, описывающий спецификацию NB-Fi. Технология **NB-Fi** стала первой российской разработкой в нише LPWAN, получившей статус национального стандарта.

Помимо ТК 194, развитием стандартов для IoT занимается проектно-технический комитет (ПТК) № 706 «Цифровые электрические сети». На площадке ПТК разработан вступивший в силу с 1 января 2021 г. ГОСТ Р 58940–2020. Стандарт определяет требования к протоколам обмена информацией между компонентами интеллектуальной системы учета и приборами учета электроэнергии, которые в том числе были учтены в № 522-ФЗ и других НПА, регулирующих установку интеллектуальных электросчетчиков с 2022 г.

За последние 3–4 года Росстандарт и российские компании серьезно нарастили свое участие в международной стандартизации. Основным механизмом для этого стало участие ТК 194 как организации, представляющей Россию в работе Подкомитета 41 «Интернет вещей и смежные технологии» в составе Совместного технического комитета СТК 1 ИСО/МЭК.

- В 2019 г. был принят первый из международных стандартов ISO/IEC в области цифровых технологий (ИСО/МЭК 30146:2019), соредакторами которого выступили эксперты ТК 194.
- В феврале 2022 г. Подкомитетом 41 ИСО/МЭК был принят разработанный по российской инициативе стандарт ИСО/МЭК 30162:2022, описывающий требования к совместимости и образцы устройств промышленного IoT²⁹⁷. Проект стандарта был доработан на площадке ПК 41 ИСО/МЭК в сотрудничестве с представителями Республики Корея, КНР, США и Японии²⁹⁸. В итоге был получен первый успешный опыт продвижения российских предложений на одну из ключевых международных площадок стандартизации IoT.

На сегодняшний день есть заметный прогресс в развитии стандартизации IoT в России. Работа, начатая в 2017–2018 гг. прежде всего на площадке ТК 194, позволила к 2022 г. сформировать основу национальной системы стандартов для различных ниш и применений IoT. Еще один важный критерий успеха – продвижение российских предложений по стандартизации IoT на международные площадки. В мировой практике именно такой путь оптимален, так как одновременно позволяет обеспечить применимость зарубежных решений на домашнем рынке и создать потенциал для экспорта российских решений за рубеж.

При этом работа по стандартизации IoT в России на сегодняшний день остается далека от завершения и сталкивается с несколькими вызовами:

- Отставание от международной стандартизации в области IoT по ряду приоритетных ниш и направлений, включая стандарты форматов данных M2M-взаимодействий, протоколов обмена и интегрированных фреймворков для управления данными, стандарты в области граничных вычислений и распределенных облачных систем для применений в IoT. Направлением, требующим скорейшей проработки, является стандартизация в области совместного и гибридного использования технологий, включая ИИ на базе IoT (AIoT), обработку M2M-данных при помощи платформ и сервисов Big Data, организацию сервисов IoT на базе связи 5G и прочее. Еще один приоритет, который диктуется вызовами кибербезопасности IoT и международной динамикой кибератак, – выработка стандартов для защиты данных M2M, реализации использования криптографических средств в инфраструктуре IoT, в том числе для сервисов на базе граничных вычислений.
- Риск выпадения из международного трека стандартизации IoT. Изменение ситуации после 24 февраля 2022 г. ставит под вопрос участие российских представителей в работе международных площадок по стандартизации и может частично обнулить те результаты, которые были достигнуты в 2019–2021 гг. Кроме

того, неясно, насколько следование международным стандартам в сфере IoT и M2M-взаимодействий вообще останется актуально для российских технических площадок, регуляторов и рынка. Наиболее вероятной выглядит долгосрочная «расстыковка» с международными стандартами в части кибербезопасности IoT.

- Успехи технического сообщества на площадке Росстандарта сочетаются с низкой осведомленностью о работе по стандартизации IoT и ее востребованностью участниками рынка. Представители отрасли зачастую не видят прямого влияния технической стандартизации на их бизнес и создаваемые ими решения. Более того, некоторые представители бизнеса рассматривают стандартизацию как фактор, ограничивающий их возможности и «свободу маневра» в развитии собственных технологических решений и продуктов для IoT.

Позитивным моментом является рост совместной активности государственных органов и участников рынка по выработке наборов стандартизированных требований для внедрения решений IoT в отдельных отраслях. Помимо стандарта «Умного города» Минстроя РФ, к этой категории относится набор требований к сервисам умного многоквартирного дома, над которым работают Минцифры РФ, Минстрой РФ, Минпромторг России совместно с ИТ-компаниями и застройщиками. В январе 2022 г. проект такого стандарта был разослан участникам рынка²⁹⁹. Набор упомянутых в документе сервисов указывает на то, что центральную роль в создании умного дома будут играть технологии IoT, прежде всего в части систем видеонаблюдения и управления интеллектуальной инфраструктурой ЖКХ.

Позитивная роль таких инициатив для развития рынка IoT в том, что они предполагают прямое вовлечение коммерческих поставщиков решений в процесс разработки и согласования единого набора требований к ним. Это дает возможность создать типовые и взаимно совместимые продукты IoT, за счет чего расширяется рыночное предложение.

Развитие отечественных решений силами отраслевого сообщества IoT

Причины описанной выше проблемы могут корениться не в самой стандартизации, а в плохо налаженной коммуникации между государством, техническим сообществом и участниками рынка. Несмотря на то, что отрасль IoT достаточно широко представлена на площадке ТК 194, российское сообщество страдает от дефицита площадок и механизмов для диалога, обмена лучшим опытом и практиками, а также совместной работы с регуляторами. Наиболее яркий показатель – отсутствие в России полноценных рыночных консорциумов IoT, которые в других странах служат ключевым механизмом для сотрудничества участников рынка, выработки и продвижения ими совместных решений. Попытки сформировать такие площадки предпринимались с середины 2010-х гг.:

- В октябре 2015 г. был создан «Национальный консорциум промышленного Интернета», учредителями которого стали ПАО «Ростелеком» и АО «Российские космические системы»³⁰⁰. В 2016 г. площадка была перезапущена уже под названием «Национальная ассоциация участников рынка промышленного интернета» (НАПИ)³⁰¹.
- В 2017 г. была создана ассоциация «Национальная платформа промышленной автоматизации» (НППА), учредителями которой выступили ГК InfoWatch, «Предприятие «Элтекс» и «Модульные системы Торнадо»³⁰².

- Собственный консорциум начал формировать Центр компетенций НТИ на базе Сколтеха по направлению «Технологии беспроводной связи и интернета вещей»³⁰³.

Однако до сих пор эти площадки не смогли собрать вокруг себя критическую массу участников рынка, запустить постоянный рабочий процесс и стать «центрами притяжения» отрасли IoT в части публичных мероприятий, продвижения бизнесом своих продуктов и технологий. Часть из перечисленных консорциумов упразднена, часть – законсервирована или переведена в закрытый режим работы. Некоторые площадки, такие как консорциум Сколтеха, только начинают формироваться и собирать вокруг себя пул отраслевых игроков.

Одной из активных площадок российского рынка IoT, организующей отраслевой диалог и деятельность рабочих групп, обмен рыночными практиками и публичными мнениями, является Ассоциация участников рынка интернета вещей (АИВ)³⁰⁴.

- Ассоциация была учреждена по инициативе Фонда развития интернет-инициатив (ФРИИ) и МГТУ им. Н. Э. Баумана в декабре 2016 г. и насчитывает 50 участников.
- В их число входят участники российского рынка IoT («Вега Абсолют», «Sigfox Россия», ООО «Телематика», «УРУС – Умные цифровые сервисы», ГК «Цифра» и др.), операторы мобильной связи, компании отрасли информационной безопасности и других ниш ИТ, крупные российские вузы и фонды³⁰⁵.
- Относительный успех АИВ может объясняться тем, что ее работа находится ближе к модели «горизонтального», низового объединения рынка, когда за самой площадкой не стоит крупный рыночный игрок со своими интересами, а среди участников преобладают компании среднего и малого размера.
- Вместе с тем пока что охват Ассоциации далек от полного покрытия российского рынка IoT, общее число участников которого измеряется несколькими тысячами, а доступные на площадке механизмы взаимодействия не достигают уровня рыночного консорциума.

Стоит также выделить начавший формироваться круг площадок взаимодействия отрасли и государства по вопросам IoT, в том числе в формате, когда организации отраслевого сообщества приглашаются регуляторами для экспертизы проектов, претендующих на государственную поддержку. Одним из примеров такого механизма является упомянутый выше Центр компетенций IoT в составе Общественного экспертного совета при президиуме Правительственной комиссии по цифровому развитию. На созданной в 2021 г. площадке представлены крупные производственные компании, производители электроники, дизайн-центры, ТК 194, АИВ и другие участники. Такой формат отвечает мировым практикам и позволяет сблизить приоритеты государства и самих участников отрасли, обеспечивая экспертизу изнутри рынка для проектов – кандидатов на государственную поддержку.

Учитывая, что в текущей ситуации поддержка отечественных компаний более актуальна, чем ранее, опыт АИВ, консорциума Сколтеха, Центра компетенций IoT при президиуме Правительственной комиссии и других существующих площадок может быть масштабирован для развития полноценных отраслевых консорциумов на российском рынке IoT.

Обеспечение кибербезопасности IoT на сегодняшний день остро требует проработки не только на уровне стандартизации, но и в нормативно-правовом и информационном ключе.

Дополнительный приоритет и импульс этой работе сегодня придает принятие Указов Президента Российской Федерации № 166 и № 250, ставящих целью импортозамещение программно-аппаратных решений и средств обеспечения информационной безопасности (СОИБ) на объектах критической информационной инфраструктуры (ОКИИ) России. По состоянию на 2019 г. ФСТЭК России было проведено категорирование более 50 тыс. таких объектов, из которых порядка 71 % составляли объекты топливно-энергетического комплекса (ТЭК). Стоит подчеркнуть, что на объектах ТЭК, наряду с предприятиями обрабатывающей и горнорудной промышленности, наиболее широко распространены сервисы, основанные на телеметрическом сборе и передаче данных, а также иные сервисы интернета вещей.

По предварительным оценкам, на сегодняшний день действие Указов № 166 и № 250 затрагивает инфраструктуры и сервисы IoT не менее чем на 50–60 % от общего числа объектов КИИ России, то есть более 20 тыс. таких объектов.

При этом как в контуре КИИ, так и на других объектах импортозамещение инфраструктуры и сервисов IoT сопряжено с рядом вызовов и барьеров, наиболее актуальных в части перехода на отечественные средства обеспечения информационной безопасности. Прежде всего это касается потребительского сегмента (B2C):

- В России до сих пор не выработаны своды лучших практик, рекомендации и отраслевые стандарты по обеспечению кибербезопасности пользовательских устройств IoT, в частности носимых устройств и устройств умного дома. Отчасти это объясняется тем, что такой формат, в принципе, не очень характерен для российских регуляторов в сфере ИБ. В свою очередь, отсутствие собственных наработок со стороны индустрии упирается в проблему, описанную ранее, – слабую самоорганизацию сообщества и дефицит площадок для совместной работы над такими инициативами.
- Не выработаны законодательные меры, нацеленные на защиту конечных пользователей сервисов IoT в сегменте B2C, в том числе требования к вендорам по обеспечению защищенности пользовательских устройств, политике паролей и раскрытию уязвимостей.

В корпоративном и промышленном сегменте ситуация немного отличается.

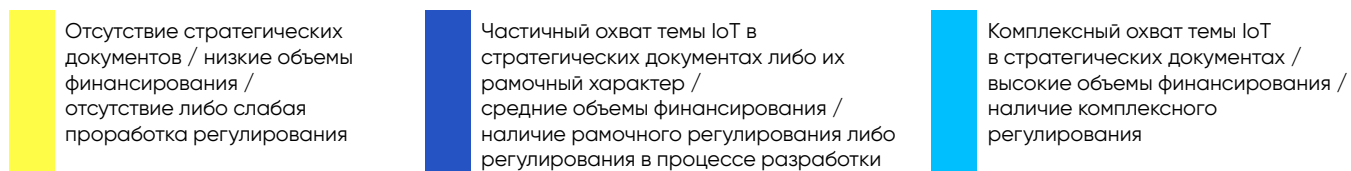
- IoT не является отдельным предметом регулирования в сфере информационной безопасности промышленных систем. При этом на его технологии и применения распространяются нормы и требования по обеспечению безопасности для систем промышленной автоматизации и управления³⁰⁶, объектов критической информационной инфраструктуры (КИИ)³⁰⁷ и топливно-энергетического комплекса³⁰⁸.
- Вопросы безопасности программных компонентов в сервисах IoT частично охватываются общими руководящими и методическими документами ФСТЭК, такими как новая Методика оценки угроз безопасности информации³⁰⁹, Методика выявления уязвимостей и недеklarированных возможностей в ПО³¹⁰ и прочее.

Однако почти все перечисленные НПА и заложенные в них инструменты служат общей задаче обеспечения информационной безопасности в промышленном сегменте и КИИ. В дополнение к ним необходимы средства и механизмы, которые бы адресно учитывали технологические особенности IoT и связанных с ним рисков безопасности, в том числе обозначенных в Концепции развития LPWAN в России:

1. Стандартизированные, в том числе наложенные, решения по шифрованию трафика в промышленных сетях IoT, которые бы позволяли обеспечить доступность, целостность и конфиденциальность M2M-данных, при этом существенно не снижая энергоэффективность сетей.
2. Требования и фреймворки к доверенному ПО и программно-аппаратным компонентам оконечных устройств и сетевого оборудования индустриального IoT. Нужно подчеркнуть, что локализация производства сетевого оборудования IoT в рамках импортозамещения важна сама по себе, но не отменяет и не заменяет задачу по созданию доверенной среды для инфраструктуры и сервисов IoT на объектах промышленности и КИИ.
3. Еще один момент, особенно заметный на контрасте между Россией и другими странами, – отсутствие НПА и других инструментов, обеспечивающих безопасность, целостность и прослеживаемость цепочек поставок ПО и оборудования для сервисов IoT. Переориентация рынка на российских поставщиков может сужать масштаб этой проблемы, но не отменяет ее. В этой связи актуальная задача – разработать отдельную модель угроз для цепочек поставок оборудования и ПО для сервисов IoT, охватывающую как программную, так и аппаратную ниши. При этом модель угроз для цепочек поставок IoT должна дополнять аналогичную модель, описывающую угрозы информационной безопасности при использовании сервисов IoT.

Основные международные тренды и особенности российского подхода

Приведенная ниже «тепловая карта» позволяет условно отобразить сравнительный прогресс рассмотренных выше государств в формировании и реализации своих стратегий развития технологической ниши и рынка IoT.



	Австралия	Бразилия	Великобритания	Евросоюз	КНР	Республика Корея	США	Россия
Комплексная государственная стратегия / план развития IoT	Yellow	Lightblue	Yellow	Lightblue	Lightblue	Lightblue	Blue	Yellow
Стратегии и программы для отдельных ниш рынка IoT	Lightblue	Blue	Blue	Lightblue	Lightblue	Lightblue	Blue	Yellow
Стратегическая увязка развития IoT с другими перспективными технологиями (5G, ИИ, Big Data и прочие)	Lightblue	Blue	Blue	Lightblue	Lightblue	Lightblue	Lightblue	Blue
Прямое финансирование инфраструктурных проектов IoT государством	Blue	Yellow	Yellow	Blue	Lightblue	Lightblue	Blue	Blue
Государственная поддержка венчурного финансирования проектов IoT	Blue	Blue	Blue	Lightblue	Lightblue	Lightblue	Lightblue	Blue
Государственная поддержка R&D в нише IoT	Blue	Blue	Lightblue	Lightblue	Lightblue	Lightblue	Lightblue	Blue
Приоритетное выделение радиочастотного ресурса для IoT	Blue	Blue	Lightblue	Lightblue	Blue	Lightblue	Lightblue	Blue
Развитие регулирования рынка M2M-данных	Blue	Yellow	Blue	Lightblue	Yellow	Blue	Yellow	Yellow
Развитие регулирования в сфере кибербезопасности / ИБ IoT	Blue	Yellow	Lightblue	Lightblue	Lightblue	Yellow	Blue	Yellow

Таблица выше помогает наглядно отобразить некоторые ключевые различия между Россией и другими государствами в выборке анализа:

1. Россия существенно отстает от мировых лидеров в части комплексной стратегии развития технологий интернета вещей и управления их масштабным внедрением. В первую очередь это обусловлено тем, что технологическая область IoT «выпала» из конструкции дорожных карт сквозных цифровых технологий (СЦТ) и до сих пор полноценно не заработала в контуре дорожных карт высокотехнологичных областей (ВТО). Такая ситуация имеет несколько последствий:

- Во-первых, размывается и устаревает видение стратегических целей развития IoT на государственном уровне. Пример: отсутствие в текущих программных документах фокуса на развитие и продвижение технологий граничных вычислений, которые в последние годы становятся одним из ключевых приоритетов в развитии IoT среди стран – технологических лидеров.
- Во-вторых, по мере того как продвигается реализация других федеральных и ведомственных проектов, дорожных карт и прочих инициатив, повестка развития IoT начинает расстыковываться с остальными технологическими направлениями и отставать от них, теряя свою актуальность. Это особенно важно с учетом общемирового тренда на глубокую конвергенцию IoT с другими сквозными технологиями: 5G, обработкой больших данных, ИИ, граничными вычислениями, программно-определяемыми сетями (SDN) и т. д. В России уже как минимум два года развитие IoT лишь точечно, фрагментарно учитывается в обновлениях программных инициатив по смежным технологическим направлениям.
- В-третьих, формальное отсутствие дорожной карты как минимум до 2021 г. тормозило распределение ресурсов государственной поддержки на разработку и внедрение решений IoT российскими компаниями и стартапами.

2. Схожим образом ситуация обстоит с управлением развитием IoT по отдельным нишам и вертикальным секторам.

- Из ведомственных проектов на данный момент относительно масштабное и систематическое внедрение технологий IoT обеспечивает лишь «Цифровая промышленность». Но и этот результат прежде всего обусловлен тем, что в обрабатывающих производствах ряд технологий (интеллектуальная автоматизация, MES, промышленная робототехника) «тянут за собой» внедрение IoT, даже если это направление не относится к целевым.
- По ряду приоритетных ниш, где IoT обладает высоким трансформирующим потенциалом, программные инициативы либо не были согласованы и запущены (сельское хозяйство, транспортный сектор), либо дублируют и конкурируют друг с другом (умный город).
- Ряд государственных инфраструктурных проектов, потенциально способных придать импульс развитию национального рынка IoT, пока не вошли в активную фазу реализации (Федеральная сеть транспортной телематики).
- В нише умного города особенно востребован отдельный мастер-план, фиксирующий межведомственное распределение ролей и бюджетов в комплексе задач развития и внедрения IoT. Также востребована сквозная система целевых показателей, которая обеспечивала бы взаимосвязь задач и направлений работы между ФОИВ. Единая система показателей должна обеспечить синхронизацию мероприятий разных ведомств и перевести их взаимодействие по направлению умного города в режим кооперации.

Упор может быть сделан на внедрение решений IoT для умного города в населенных пунктах среднего размера (от 100 до 500 тыс. чел.). Такие города обладают хозяйственным и инфраструктурным комплексом, который обеспечивает достаточный потенциал для масштабного внедрения IoT, в отличие от малых поселений. При этом дефицит собственных ресурсов

на эти задачи у них существенно острее, чем у 3–4 крупнейших агломераций, составляющих более 95 % российского рынка решений умного города на сегодняшний день.

3. Система государственной поддержки проектов по разработке и внедрению решений IoT существенно усилилась с 2019 г. Но в нынешних условиях требуется переосмысление и актуализация всей системы критериев, на основе которой осуществляется поддержка проектов IoT.

- Объемы бюджетных ресурсов, направляемых на венчурное финансирование проектов СЦТ, включая смежные с IoT ниши, находятся на уровне таких стран, как Великобритания и Австралия, хотя серьезно отстают от мировых лидеров, таких как Германия, КНР и США.
- Из-за отсутствия стратегии развития IoT не имеется и единого целевого плана инвестирования бюджетных средств в этой технологической области. В итоге венчурные фонды и другие операторы мер господдержки сами не имеют полной картины инвестиций и их результатов в разрезе IoT. Такая прослеживаемость не должна быть самоцелью – технологии цифровой трансформации работают в комплексе и в глубокой взаимосвязи, особенно в крупных проектах. Но ее отсутствие мешает понять и измерить вклад IoT в достижение целевых показателей трансформации, оценить эффективность вложений средств государственного бюджета и предприятий и своевременно корректировать механизмы поддержки.
- Еще одно отличие России от мировых лидеров внедрения IoT – стратегический фокус последних на поддержку проектов, формирующих кластеры различного масштаба: от площадок кооперации стартапов в Великобритании и ЕС до районных промышленных кластеров в Южной Корее и кластеров индустриального IoT городского и регионального масштаба в КНР. Российские проекты промышленных внедрений IoT и механизмы их господдержки могут обеспечивать серьезный масштаб и глубину цифровой трансформации. Но при этом они слабо ориентированы на горизонтальный переток инноваций к смежным предприятиям, контрагентам и участникам цепочки поставок. За рубежом именно такая горизонтальная дисперсия технологий IoT зачастую ставится во главу угла государственных стратегий, поскольку за счет нее ускоряется развитие рынка в целом и его насыщение M2M-сервисами.

4. Слабое горизонтальное взаимодействие между участниками рынка IoT отличает Россию от других государств в выборке анализа.

- Россия представляет практически единственный в мире пример крупного рынка, на котором отсутствуют полноценные национальные консорциумы в нише IoT. На данный момент деятельность ведут Ассоциация интернета вещей (АИВ) и Центр компетенций НТИ на базе Сколтеха, Центр компетенций «Интернет вещей» на базе ПАО «МТС». Но ресурсная база и набор инструментов этих площадок не достигают уровня индустриальных консорциумов, действующих на международном рынке и на национальных рынках ЕС, США, КНР. В частности, нет массового охвата участников рынка (100 организаций и более), собственных инструментов тестирования, обкатки и продвижения наработок (полигоны, тестбеды и промышленные испытательные стенды, софинансирование проектов участников со стороны консорциума).

- В 2015–2017 гг. предпринимались попытки сформировать консорциум под доминирующего участника рынка. Альтернативой может стать модель нейтральной площадки, ориентированной на массовое участие средних и малых игроков, вплоть до микробизнеса и проектов IoT уровня «гаражной экономики». Такая площадка вряд ли сможет обеспечивать собственную ресурсную базу для продвижения проектов участников на уровне крупнейших мировых консорциумов. Однако она сможет ускорить обмен наработками и лучшими практиками между участниками рынка, стать платформой для формирования позиции широкого отраслевого сообщества.
5. Для развития рынка критически важно объединение его ведущих участников вокруг технологии и развития основанной на ней продуктовой и сервисной экосистемы. История успеха LoRaWAN, как отмечалось в разделе 1, – это прежде всего история консолидации критической массы рыночных игроков вокруг открытой экосистемы, где каждый может претендовать на свою нишу и долю рынка в интегрированном технологическом стеке (за исключением проприетарной базовой технологии физического уровня).
- У российских компаний есть основа в виде собственных технологических решений (XNB, NB-Fi и др.) для создания схожих экосистем в нише несотовых LPWAN. До сих пор этого не происходит потому, что российские технологии либо недостаточно зрелые, либо в принципе не ориентированы на открытую модель развития.
 - Выбор рыночной модели и траектории развития в конечном счете всегда остается за разработчиком технологии. Но государство может действовать по обоим направлениям, а именно: а) ускорять «дозревание» российских разработок путем их адресной поддержки и б) стимулировать разработчиков к «открытию» своих технологий и созданию вокруг них рыночных экосистем. Инструментами по второму направлению могут служить налоговые преференции и адресное субсидирование расходов на открытое ПО и сетевое оборудование в нише IoT, а также гранты и целевое финансирование на создание открытых интегрированных стеков в нише LPWAN.
 - В качестве стимула может выступать и государственная поддержка в виде льготных режимов налогообложения и/или субсидирования отдельных категорий расходов для площадки рыночного консорциума, собранного вокруг открытой российской технологии в нише IoT.
 - Инструмент импортозамещения, который начал активно применяться для регулирования российской отрасли IoT, требует тонкой настройки. Опыт его применения в нише сетевого оборудования LPWAN показывает, что требования к переходу на отечественные решения должны учитывать ограничения возможностей российских производителей, в том числе в части масштабирования поставок и закрытия потребности рынка.
 - Развитию и расширению рынка IoT также будет способствовать нормативное регулирование в сфере ЖКХ (внедрение интеллектуальных приборов учета газа, воды, тепла) и в других отраслях экономики.

6. С 2017 г. удалось обеспечить серьезный прогресс в создании национальной системы технических стандартов для IoT.
 - Работа ТК 194 и ряда других площадок Росстандарта с 2017 г. позволила закрыть основные пробелы в стандартизации ключевых технологий IoT и в этом плане приблизить Россию к уровню среднестатистического развитого рынка. При этом по отдельным направлениям имеются незакрытые пробелы и сохраняется отставание от других развитых стран.
 - Скорейшей проработки требует стандартизация в области совместного и гибридного использования IoT и других сквозных технологий, включая ИИ на базе IoT (AIoT), применение к M2M-данным технологий обработки Big Data, организацию сервисов IoT на базе связи 5G и граничные вычисления.
7. Отдельной проблемой является отсутствие национальных и отраслевых стандартов, НПА и нормативно-технических документов по информационной безопасности, учитывающих специфику IoT.
 - В ближайшее время актуальна разработка отдельной модели и методики оценки угроз для устройств, сетевой инфраструктуры и платформ IoT. Без методологических инструментов нецелесообразно решение следующей приоритетной задачи, а именно разработки программно-технических средств для обеспечения информационной безопасности инфраструктуры и сервисов IoT.
 - Также нужны стандартизированные решения по шифрованию сетевого трафика IoT на объектах промышленности и КИИ, способные обеспечить доступность, целостность и конфиденциальность M2M-данных, существенно не снижая энергоэффективность сетей.
 - Политика импортозамещения в нише IoT должна дополняться разработкой фреймворков и требований к доверенному программному обеспечению и программно-аппаратным компонентам конечных устройств и сетевого оборудования IoT. Основное направление работы – продвижение доверенной бизнес-модели (Security Assurance) для IoT в критически важных системах промышленного уровня.
 - Международный опыт подтверждает востребованность рекомендательных инструментов и обязательных требований для обеспечения безопасности сервисов и устройств IoT для конечных пользователей. Сюда входит введение требований к вендорам устройств и сервисов для сегмента B2C в части политики паролей конечных устройств IoT, информирования об уязвимостях и иных стандартов безопасности.

Выводы: ключевые тренды и рекомендации



1. Макроэкономические тренды

- Интернет вещей стал значимым фактором глобального макроэкономического развития, обеспечивая прирост национальных ВВП от 0,3 до 0,8 % и генерируя триллионы долларов накопленного вклада в мировую экономику.
- Дивиденды от развития IoT распределяются по миру все более неравномерно: ЕС, КНР и США в сумме занимают более 75 % по доходам, расходам, числу подключений и в первую очередь выигрывают от масштабных проектов развития и внедрения технологий IoT, прежде всего в промышленном сегменте.
- Для развивающихся стран опережающее внедрение технологий IoT может обеспечить рост ВВП на 2 % и более; с другой стороны, ценой инерционного сценария становится общее отставание в технологическом и экономическом развитии.
- Дальнейший рост вклада IoT в экономическое развитие принципиально зависит от масштабов и скорости внедрения инфраструктуры и сервисов связи 5G, которая в перспективе 2028–2030 гг. будет обеспечивать порядка 50 % инфраструктуры и функциональных возможностей интернета вещей.

2. Технологические тренды

- Развитие IoT все более тесно взаимосвязано с технологиями связи 5G, граничных вычислений, обработки больших данных, искусственного интеллекта, промышленной автоматизации и робототехники.
- Ключевой сквозной тренд – потребности индустриального IoT начинают определять магистральный вектор развития большинства технологий беспроводной связи:
 - «Глобальный закат» сотовых сетей 2G и 3G завершится в ближайшие годы, сотни миллионов подключений IoT переходят в сети 4G, 5G и сети LPWAN.
 - Мы находимся в самом начале массового развития критически важных сервисов IoT в промышленности и автоиндустрии на базе широкополосной связи 5G. Одновременно массово реализуются и другие сценарии применения 5G для IoT, а именно сети 5G с поддержкой массовых межмашинных коммуникаций (mMTC), представляющие собой развитие сотовых LPWAN на базе 4G/LTE.
 - Одним из «локомотивов» развития индустриального IoT становится внедрение частных сетей 5G и LTE 5G-Ready на производственных объектах.
 - Одну из наиболее быстрорастущих рыночных ниш образуют узкополосные сети, не основанные на сотовой связи и сформировавшие вокруг себя независимые рыночные экосистемы, такие как LoRaWAN.

- «Под запрос» промышленного IoT меняются и технологии малого радиуса действия, такие как Wi-Fi и Bluetooth, что в дальней перспективе может размыть границы между ними и сетями LPWAN.
- Огромный потенциал для трансформации рынка в перспективе на 2030 г. накапливает сегмент спутниковой связи IoT прежде всего за счет массового развертывания группировок малых спутников коммерческими операторами, стремящимися сравняться по цене сервисов для IoT с широкополосными сотовыми сетями и LPWAN.

3. Стратегические тренды

1. По мере повышения значения IoT для экономики и цифровой трансформации растет роль государства в управлении и стимулировании развития технологий интернета вещей:
 - Все больше стран – лидеров цифровой трансформации переходят от не прямых инструментов поддержки IoT (облегченное нормативно-правовое регулирование, консультации с частным бизнесом, создание институциональной среды для развития экосистемы стартапов и инноваций) к более масштабным и директивным форматам:
 - Разрабатываются комплексные государственные стратегии и планы развития IoT с межотраслевым охватом и четким горизонтом планирования.
 - Реализуются крупномасштабные программы прямых государственных и государственно-частных инвестиций, ориентированные прежде всего на отраслевое внедрение инфраструктуры и сервисов промышленного IoT.
 - Государственная поддержка интернета вещей расширяется на все этапы жизненного цикла технологий и продуктов: от грантов на разработку протоколов и R&D для создания оборудования до прямого внедрения готовых продуктов в промышленном масштабе на открытом рынке.
 - В отдельных случаях технологическая политика государственных регуляторов через механизмы господдержки и НПА напрямую определяет, какая из технологий IoT выбирается в качестве опорной для национального рынка, присутствующих на нем коммерческих игроков, экспортеров и конечных потребителей (NB-IoT и широкополосная связь 5G в Китае).
 - В интересах развития интернета вещей страны-лидеры также осуществляют комплексные регуляторные меры в смежных областях технологической политики:
 - расчистка радиочастотного спектра под широкое применение перспективных протоколов связи для IoT;
 - стимулирование внедрения IPv6 операторами связи и цифровыми сервисами;

- доработка и адаптация требований по обеспечению информационной безопасности, защите персональных данных и критической информационной инфраструктуры к специфике IoT и M2M-данных.

2. При сохранении нынешней тенденции к росту экономической турбулентности, шоков на энергетических рынках, дефициту полупроводников и расширению технологической санкционной политики перечисленные выше тренды могут быть еще более выраженными в перспективе до 2030 г.:

- В отдельных регионах (Юго-Восточная Азия) может утвердиться квазиплановая модель прямого государственного управления технологическими инновациями и развитием инфраструктуры для IoT.
- Усиление санкционной политики в отношении РФ, Китая, Ирана и ряда других стран делает сервисы индустриального IoT в сочетании с интеллектуальной аналитикой остро востребованными для удлинения жизненного цикла оборудования и иных основных фондов в ключевых отраслях промышленности.
- До 2030 г. индустриальный IoT будет все более значимым драйвером развития отраслей экономики, а государства продолжают все более директивно определять и формировать национальный ландшафт технологий интернета вещей. В этих условиях государственная инновационная политика в отношении IoT имеет шансы превратиться в один из ключевых и наиболее действенных рычагов государственного управления развитием реального сектора экономики, включая прежде всего обрабатывающую и добывающую промышленность, логистику и транспортную отрасль.

4. Специфические для России тренды

- В России до сих пор отсутствует комплексная стратегия развития IoT, что мешает государству выстроить единый подход к развитию этой технологической области. Дополнительную необходимость в таком подходе обуславливает программа импортозамещения в ИТ, в том числе в части обеспечения безопасности объектов критической информационной инфраструктуры РФ.
- В национальной программе «Цифровая экономика» повестка IoT также «распылена» между различными федеральными проектами и их отдельными мероприятиями, не имея сквозного комплексного видения, целеполагания и инструментария мер поддержки.
- Отдельную проблему представляет дублирование и конкуренция ведомственных проектов в кросс-нишевых направлениях внедрения IoT, таких как «Умный город».
- Отсутствие комплексной государственной политики развития IoT «отзеркаливается» российским рынком, на котором имеет место параллельное движение различных игроков в сторону конкурирующих технологий, бизнес-моделей и международных альянсов.

- При этом Россию на фоне многих других стран выделяет существенный технологический задел для развития IoT: разработаны несколько протоколов LPWAN; эксплуатируются и внедряются собственные платформы промышленного IoT для отраслевых предприятий; имеются кейсы масштабных городских проектов видеоаналитики; крупные частные игроки развивают собственные сети связи IoT федерального охвата и формируют линейки продуктов для конечных пользователей. Таким образом, наблюдается и растет разрыв между потенциалом российского рынка IoT и фактической реализацией этого потенциала при содействии государства.

5. Рекомендации

1. Рассмотреть возможность формирования единого сквозного плана развития технологий IoT до 2030 г. с упором на промышленные применения и связкой с ключевыми смежными технологиями (технологии связи 5G) в рамках нескольких рабочих треков:
 - 1.1 В рамках обновленных Дорожных карт высокотехнологичных направлений (ДК ВТН), разрабатываемых и реализуемых технологическими компаниями по соглашению с Правительством Российской Федерации. Проработка технологической повестки IoT в таком формате также должна включать увязку технологий промышленного IoT и связи 5G, формирования рамки целевых показателей развития и внедрения сервисов промышленного IoT в ключевых отраслях экономики и формирования линейки целевых мер государственной поддержки (субсидирование промышленных внедрений, расширенные гранты на R&D и тестовое внедрение, налоговые льготы и гранты для разработчиков отечественных ПАК оборудования связи для IoT).
 - 1.2 Сформировать целевой долгосрочный трек поддержки проектов по разработке ПО для промышленного IoT в рамках центров компетенций по развитию российского общесистемного и прикладного программного обеспечения (ЦКР). В рамках такого трека целесообразно:
 - свести воедино информацию о проектах по разработке и внедрению сервисов промышленного IoT из 36 промышленных центров компетенций по замещению зарубежных отраслевых цифровых продуктов и решений, включая программно-аппаратные комплексы, в ключевых отраслях экономики (ИЦК); обеспечить их синхронизацию и межотраслевой трансфер текущих наработок;
 - на основе обработки сводных данных по отраслевым ИЦК сформировать детализированную «карту потребностей» в сервисах и продуктах промышленного IoT по отдельным отраслям до 2028–2030 гг.;
 - на базе отраслевой «карты потребностей» сформировать целевой образ и целевой ландшафт развития ниши ПО для промышленного IoT для отдельных отраслей и в межотраслевой рамке до 2030 г.; использовать полученные наработки для текущего обновления и корректировки карты ВТН.

1.3 В рамках отдельных отраслевых ИЦК или отраслевых промышленных альянсов на базе ведущих технологических компаний выстроить целевую модель развития инфраструктуры и сервисов промышленного IoT в рамках вертикально интегрированных доверенных программно-аппаратных стеков:

- использовать для формирования стеков модель: ПАК, входящие в ТОПП Минпромторга России, + ПО, входящее в реестр Минцифры России, + средства обеспечения ИБ, сертифицированные ФСБ и ФСТЭК России;
- провести пилотное формирование целевой модели стеков на базе отечественного ПО и оборудования для промышленного IoT в рамках одной отрасли до 2024 г.;
- распространить интегрированную модель стеков для отраслевых применений промышленного IoT на остальные отрасли после 2024 г., в том числе используя инструменты целевого субсидирования внедрения для якорных заказчиков в рамках такой модели.

1.4 Поддерживать и развивать инициативы по созданию сквозных проектов для формирования спроса на отечественную радиоэлектронную продукцию в сфере IoT+5G в рамках работы центра компетенций «Интернет вещей» на базе ПАО «МТС» для формирования рынка отечественных IoT-решений, устройств.

2. Сформировать и запустить целевые механизмы государственной и государственно-частной поддержки развития инфраструктуры и сервисов IoT для приоритетных технологических ниш:

- Выделить (в рамках нацпрограммы «Цифровая экономика», переработанных дорожных карт ВТО/ВТН либо поддержки проектов ИЦК и ЦКР) целевое грантовое финансирование на доработку и повышение уровня готовности к коммерческому внедрению на рынке российских протоколов связи для несотовых узкополосных сетей (NB-Fi, OpenUNB), а также для сотовых LPWAN для масштабируемости внедрения IoT.
- Проработать возможность целевого субсидирования внедрения сетевого оборудования и конечных устройств IoT, функционирующих на базе российских протоколов LPWAN, государственными и частными промышленными заказчиками.
- Оказать целевую поддержку операторам связи и иным участникам рынка в повышении эффективности использования существующей инфраструктуры сетей связи NB-IoT федерального и межрегионального охвата. В том числе проработать выделение грантов на R&D пользовательских устройств на базе NB-IoT. Оценить целесообразность использования сетей NB-IoT для выполнения задач федеральных и ведомственных проектов в нишах энергетики, сельского хозяйства, ЖКХ и транспортных систем.
- В рамках подхода, основанного на продвижении интегрированных программно-аппаратных стеков: субсидировать разработку и внедрение интегрированных продуктов на базе протоколов NB-IoT, LoRaWAN, NB-Fi и OpenUNB, включающих соответствующее критериям ТОПП сетевое оборудование, отечественное встроенное системное ПО и прикладное ПО для сервисов IoT.

3. Сформировать и запустить целевые механизмы государственной и государственно-частной поддержки приоритетных ниш рынка IoT:
 - Сформировать и запустить программу субсидирования промышленным предприятиям проектов по внедрению цифровых сервисов индустриального IoT на базе частных сетей связи LTE/5G (private LTE/5G). Предлагаемые основные параметры программы:
 - пилотная реализация программы может стартовать на промышленных предприятиях, входящих в структуру технологической компании – партнера Правительства России по реализации дорожных карт ВТО/ВТН;
 - субсидию предлагается выделять промышленным предприятиям, внедряющим сервисы индустриального IoT поверх частной сети LTE, функционирующей на базе отечественного телекоммуникационного оборудования, соответствующего критериям ТОРП (включая базовую станцию LTE);
 - с 2025/2026 гг. в программу может быть включено субсидирование сервисов индустриального IoT поверх частной сети на базе отечественного оборудования 5G.
 - На площадке рабочей группы с участием Росстандарта, Минцифры России, Минпромторга России и частных компаний:
 - разработать среднесрочный план продвижения отечественных технических стандартов для протоколов связи IoT (OpenUNB, NB-Fi) и продукции на их основе на внешние рынки (рынки государств БРИКС и иных дружественных стран Юго-Восточной Азии, Ближнего Востока, Африки и Латинской Америки);
 - проработать упрощенный порядок экспорта и декларирования промышленной продукции на базе отечественных протоколов LPWAN.
4. Целесообразно выделить отдельные категории информационной инфраструктуры и сегментов рынка, в которых применение решений IoT имеет критическое значение для обеспечения ИБ. Предлагается ввести ранжирование требований для таких решений в зависимости от различных уровней и критичности сферы их применения, включая объекты КИИ Российской Федерации.
 - В сегменте B2C, в зависимости от критичности применения:
 - ФСТЭК России совместно с компаниями-вендорами и компаниями – лидерами в области ИБ: опубликовать свод лучших практик и рекомендаций для пользователей по безопасному использованию устройств и сервисов IoT;
 - ФСТЭК России: принять требования к вендорам по обязательным политикам паролей и раскрытию уязвимостей в ПО конечных устройств и сервисов IoT.

- Для применений в промышленности и объектах КИИ:
 - разработать специализированную модель и методику оценки угроз для цепочки поставок оборудования и сервисов IoT;
 - сформировать периодически обновляемый перечень угроз ИБ для промышленных сервисов IoT, в том числе внедренных на объектах КИИ Российской Федерации;
 - разработать рамочные требования к доверенному ПО и программно-аппаратным компонентам сетевого оборудования и конечных устройств IoT;
 - выделить целевое грантовое финансирование на доработку программно-технических средств защиты информации и решений по шифрованию сетевого трафика в M2M-сетях.

Авторы



Олег Демидов
Аналитик
АНО «Цифровая экономика»



Андрей Колесников
Директор
Ассоциация участников рынка
интернета вещей

Редакционная коллегия

Сергей Плуготаренко

Генеральный директор АНО «Цифровая экономика»

Карен Казарьян

Директор по аналитике АНО «Цифровая экономика»

Владислава Васильева

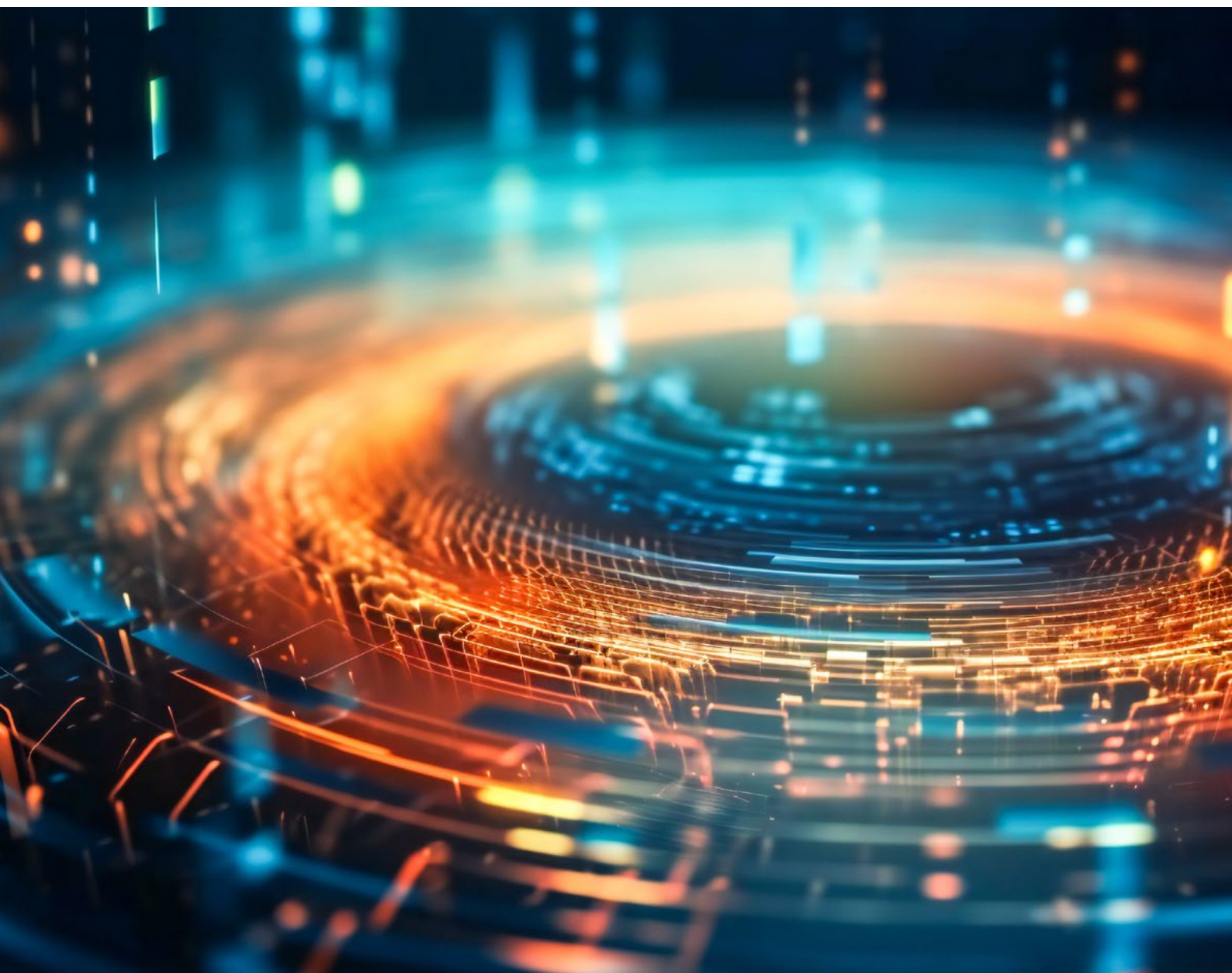
Заместитель директора по развитию направления
«Безопасная и открытая инфраструктура» АНО «Цифровая экономика»

Максим Чернов

Руководитель направления развития цифровых продуктов
АНО «РТ-Национальные инициативы»

Указанные должности актуальны на момент работы над аналитическим отчетом

Приложения



Приложение № 1: Примеры и характеристики основных технологий беспроводной связи для IoT

№	Тип технологии	Протокол	Стандарт / спецификация	Используемые частотные диапазоны	
1.	Сети на базе сотовой связи	Поколения сотовой связи 3GPP	2G (GSM/GPRS/EDGE)	3GPP TS 41.101.	полосы в лицензируемых диапазонах 880–960 МГц (GSM)
2.			3G (UMTS/HSPA)	3GPP TS 25.101, 25.102 и другие	полосы в лицензируемых диапазонах от 700 МГц до 4 ГГц
3.			4G/LTE	3GPP 36 series и другие	полосы в лицензируемых диапазонах от 453 МГц до 2,6 ГГц
4.			5G (eMBB/URLLC)	3GPP Release 15–17	полосы в лицензируемых диапазонах 1–6 ГГц / 25–39 ГГц и выше
5.		Узкополосные сети (LPWAN) на базе сотовой связи	LTE Cat 1/Cat 1 bis	3GPP Release 8, 13	полосы в лицензируемых диапазонах от 453 МГц до 2,6 ГГц
6.			Narrow Band IoT (NB-IoT)	LTE Cat-NB1/NB2 (3GPP Release 13–17)	частоты LTE (полосы в лицензируемых диапазонах от 453 МГц до 2,6 ГГц)
7.			EC-GSM-IoT	EC-GSM-IoT (3GPP Release 13–17)	частоты LTE (полосы в лицензируемых диапазонах от 453 МГц до 1,95 ГГц)
8.			eMTC	LTE Cat M-1/M-2 (3GPP Release 13–17)	частоты LTE (полосы в лицензируемых диапазонах от 453 МГц до 2,6 ГГц)
9.	Узкополосные сети дальнего радиуса действия (LPWAN), не основанные на сотовой связи	DASH7	DASH7 Alliance Protocol Specification (проприетарный)	433 МГц / 868 МГц / 915 МГц	
10.		LoRaWAN	LoRaWAN® (проприетарный)	433 МГц / 863–876 МГц / 915 МГц	
11.		NB-Fi	ГОСТ Р 70036-2022	863–876 МГц / 433 МГц	
12.		Sigfox	AN5480 (проприетарный)	863–876 МГц	
13.		XNB (Extended Narrowband)	N/A (проприетарный)	868,8 МГц	
14.		Weightless	Weightless-N/-P/-W (проприетарный)	863–876 МГц	
15.		Wi-SUN	IEEE 802.15.4g	868 МГц / 915 МГц / 2,4 ГГц	
16.	Беспроводные сети масштаба города (WMAN)	Мобильный WiMAX	IEEE 802.16e/m	2–11 ГГц	
17.	Беспроводные сети локального и персонального доступа (LAN / PAN)	Wi-Fi	Wi-Fi HaLow	IEEE 802.11ah	750–928 МГц
18.			Wi-Fi 6E (HEW)	IEEE 802.11ax	2,4 ГГц / 5 ГГц / 6 ГГц
19.			Wi-Fi 6 (HEW)	IEEE 802.11ax	2,4 ГГц / 5 ГГц
20.			Wi-Fi 5	IEEE 802.11ac	2,4 ГГц / 5 ГГц
21.		Bluetooth	IEEE 802.15.1	2,402–2,48 ГГц	
		Bluetooth Low Power (BLE)	IEEE 802.15.1	2,402–2,48 ГГц	
22.		IEEE 802.15.4	ISA100 Wireless (ISA.100.11)	IEC 62734	2400–2483,5 МГц
23.			Thread	N/A	2400–2483,5 МГц
24.			WirelessHART	IEC 62591	2400–2483,5 МГц
25.			ZigBee	N/A	868 МГц / 915 МГц / 2,4 ГГц
26.			DSRC (WAVE)	IEEE 802.11p	5,850–5,925 ГГц
27.		Z-Wave	N/A (проприетарный)	868 МГц / 908 МГц / 2,4 ГГц	
28.		RFID	RFID и NFC	ISO/IEC/IEEE 21451-7:2011, ISO 11784-85, ISO 18000-01 и другие	30–300 кГц (НЧ) / 3–30 МГц (ВЧ) / от 300 МГц до 5,8 ГГц (СВЧ)

Дальность	Скорость передачи данных (downlink)	Энергопотребление	Задержка сигнала
до 35 км	35–385 кбит/с	Среднее	от 500 мс до 1 с
до 25 км	от 400 кбит/с до 10 Мбит/с	Высокое	100–200 мс
2–4 км в городе, до 15 км на открытой местности	50–500 Мбит/с	Высокое	50 мс
от 300 м до 1–2 км	от 500 Мбит/с до 5 Гбит/с и более	Очень высокое	1–10 мс
до 5 км в городе, до 15 км на открытой местности	до 10 Мбит/с	Среднее	50–100 мс
до 5 км в городе, до 20 км на открытой местности	до 127 кбит/с	Очень низкое	1–10 с
до 10 км в городе, до 20 км на открытой местности	от 474 кбит/с до 2 Мбит/с	Низкое	от 700 мс до 2 с
до 10 км в городе, до 20 км на открытой местности	1–4 Мбит/с	Низкое	10–50 мс
до 1–2 км (городе)	до 167 кбит/с	Очень низкое	1–2 с
до 5 км (в городе)	до 50 кбит/с	Очень низкое	1–10 с
до 10 км (в городе)	от 50 бит/с до 25,6 кбит/с	Очень низкое	1–10 с
до 10 км (в городе)	до 100 бит/с	Очень низкое	1–15 с
до 10 км (в городе)	до 100 кбит/с	Очень низкое	1–10 с
до 3 км (в городе)	до 100 кбит/с	Очень низкое	1–30 с
до 3 км (в городе)	до 300 кбит/с	Очень низкое	1–10 с
до 15 км (в городе)	до 50 Мбит/с	Среднее	25–40 мс
до 1–3 км	от 100 кбит/с до 40 Мбит/с	Среднее	100–200 мс
до 100 м	от 100 Мбит/с до 9,6 Гбит/с	Среднее	2–10 мс
		Среднее	2–10 мс
до 70 м	до 1 Гбит/с	Среднее	10–50 мс
до 50 м	до 2 Мбит/с	Среднее	до 800 мс
до 1,0 км	до 1 Мбит/с	Низкое	до 260 мс
до 250 м	250 кбит/с	Очень низкое	до 1 с
до 50 м	250 кбит/с	Очень низкое	до 100 мс
50–250 м	250 кбит/с	Очень низкое	до 100 мс
до 100 м	до 250 кбит/с	Очень низкое	80–200 мс
до 300–500 м	до 27 Мбит/с	Среднее	до 150 мс
до 100 м	до 100 кбит/с	Очень низкое	до 500 мс
от 1 см до 300 м	40–640 кбит/с	Нулевое / очень низкое	1–200 мс

Приложение № 2: Справочная информация о государственных и государственно-частных инициативах развития технологической области IoT в России в 2018–2021 гг.

1. Развитие IoT в национальной программе «Цифровая экономика» и ее федеральных проектах

В настоящее время технологическая область интернета вещей в России не охвачена единым программным или стратегическим документом, который бы рассматривал задачи ее развития в комплексе. Развитие технологий, инфраструктуры, включая сети беспроводной связи, оборудования и ПО, сервисов и бизнес-моделей применения IoT на уровне государственной повестки фрагментировано и распределено по сложной многоуровневой системе инициатив и проектов.

- Общий контур стратегического целеполагания обеспечивают национальная программа «Цифровая экономика» и отдельные федеральные проекты в ее составе.
- Отдельный уровень планирования, частично вытекающий из федеральных проектов, формируют дорожные карты сквозных цифровых технологий (СЦТ) и развития высокотехнологичных областей (ВТО).
- В задачи и мероприятия ведомственных проектов входит развитие IoT в разрезе отдельного вертикального сектора или инфраструктурной ниши («Умный город», «Безопасный город», «Цифровое сельское хозяйство», Федеральная сеть транспортной телематики (ФСТТ) и прочее).

Сама национальная программа «Цифровая экономика»³¹¹ содержит упоминания IoT, но не рассматривает его технологии как отдельную целевую область развития. Различные задачи, связанные с развитием и внедрением технологий и сервисов интернета вещей и M2M-коммуникаций, распределены по федеральным проектам программы.

1. Федеральный проект «Информационная инфраструктура» в редакции 2019 г. в части IoT включал³¹²:
 - Разработку Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации и реализацию предлагаемых в ней решений в части высвобождения необходимых для развития сетей LPWAN полос частот и правил их выделения. Сама концепция была разработана и утверждена в том же году и охватила широкий круг вопросов, включая³¹³:
 - создание отдельной сети связи для транспортной инфраструктуры – Федеральной сети транспортной телематики (ФСТТ), в том числе на базе LPWAN и других технологий беспроводной связи для IoT;
 - выделение дополнительных диапазонов частот для развития сетей LPWAN в России;

- развитие системы национальных стандартов беспроводной связи для LPWAN;
- реализацию комплекса мер для обеспечения информационной безопасности и защиты M2M-данных, передаваемых через беспроводные сети связи.
- Разработку и применение мер господдержки к отечественным производителям инженерного оборудования для инфраструктуры связи и обработки данных, включая оборудование для узкополосных сетей связи IoT.
- Запуск 5 пилотных проектов по развитию российских LPWAN-сетей.
- Создание единой цифровой платформы ЖКХ с мониторингом и учетом состояния имущества и инфраструктуры через сервисы IoT. Такая платформа должна была обеспечить обновление ГИС ЖКХ, введенной в эксплуатацию с 2016 г.

Также в привязке к мероприятиям федерального проекта и концепции развития сетей LPWAN Министерство транспорта Российской Федерации в 2019 г. утвердило отдельную концепцию покрытия транспортной инфраструктуры сетями связи для систем передачи данных³¹⁴. Документ предлагал развивать Федеральную систему транспортной телематики за счет широкого покрытия железнодорожной, автомобильной и иной транспортной инфраструктуры сетями узкополосной связи (LPWAN) и беспроводной широкополосной связи дальнего (LTE) и малого радиуса действия (технология DSRC/ITS-G). Под создание ФСТТ предусматривалось выделение ряда радиочастотных диапазонов, включая:

- 660–870 МГц для сетей LPWAN;
- 350–370 МГц для широкополосных сетей LTE;
- 1785–1805 МГц для технологической сети на железнодорожном транспорте по технологии FRMCS.

Необходимые для ФСТТ частоты были выделены решениями Государственной комиссии по радиочастотам (ГКРЧ) с 2018 по 2020 гг. В этот же период началось создание системы: были развернуты отдельные сегменты на инфраструктуре автодорог и метрополитена³¹⁵, общая сумма заключенных госконтрактов достигла 1,4 млрд руб.³¹⁶ Однако с середины 2021 г. расходы на завершение реализации концепции и создания ФСТТ были исключены из обновленного паспорта федерального проекта³¹⁷. В результате на апрель 2022 г. развертывание сетевой инфраструктуры ФСТТ приостановлено, а выделенные под нее частоты для сетей LPWAN не используются по целевому назначению. С 2021 г. из бюджета федерального проекта исключено дальнейшее финансирование проектов развертывания сетей LPWAN.

Также в апреле 2022 г. распоряжением Правительства срок перехода к целевой модели эксплуатации единой цифровой платформы ЖКХ был перенесен на сентябрь того же года³¹⁸.

Таким образом, более 50 % изначально включенных в федеральный проект мероприятий, затрагивающих развитие IoT, на сегодняшний день реализованы частично или заморожены.

2. Федеральный проект «Информационная безопасность»³¹⁹ на момент своего утверждения в 2019 г. предусматривал:

- разработку требований к операторам промышленного IoT и стандартов безопасности для устройств IoT;
- создание системы отраслевого регулирования использования устройств IoT, включая требования по идентификации устройств и регистрации сетевого оборудования;
- меры по развитию российской телекоммуникационной инфраструктуры и пользовательского оборудования IoT с учетом требований ИБ.

Отдельное финансирование для этих мероприятий не было заложено в бюджет федерального проекта. В редакции на апрель 2022 г. эти мероприятия были исключены из федерального проекта.

На данный момент предлагаемые требования к устройствам и оборудованию IoT не были утверждены отдельными НПА. Проекты национальных стандартов ИБ для IoT до сих пор не были утверждены на площадке Росстандарта.

При этом в обновленный, по состоянию на апрель 2022 г., паспорт федерального проекта вошло создание российского ресурса с уязвимостями уровня АСУ ТП и промышленного IoT для объектов критической инфраструктуры. Расходы бюджета на реализацию этой задачи должны составить 399,9 млн руб. до 2024 г.³²⁰

3. Федеральный проект «Цифровое государственное управление» предусматривал создание и запуск Единой государственной платформы сбора и анализа данных промышленного IoT в составе Платформы исполнения государственных функций.

- Государственная платформа сбора данных (ГПСД) была запущена в ноябре 2020 г. на основе разработок Mail.Ru Group³²¹. Пока функционал платформы в большей степени ориентирован на мониторинг культурных объектов и экологический мониторинг: контроль качества воздуха и промышленных выбросов, контроль вырубки лесов и прочее. Платформа выполняет роль инструмента для автоматизации контрольно-надзорной деятельности и наполнения данными соответствующих ГИС³²². Таким образом, по итогам этого мероприятия федерального проекта есть результат в виде работающей государственной платформы IoT на стадии поэтапного внедрения в регионах.

4. Наиболее системно развитие технологической области интернета вещей должен был охватить федеральный проект «Цифровые технологии».

- Утвержденный в 2019 г. паспорт проекта³²³ предусматривал разработку дорожных карт для 9 сквозных технологий. Интернет вещей изначально не был представлен в этом списке, но позднее разработка такой дорожной карты была включена в список мероприятий федерального проекта.
- Наряду с дорожными картами и соглашениями по развитию высокотехнологичных областей, эти документы уточняют систему государственного планирования в части развития IoT, определяя механизмы поддержки, ответственные организации и результаты работы.

Интернет вещей в дорожных картах развития сквозных цифровых технологий (СЦТ) и высокотехнологичных областей (ВТО)

Дорожные карты СЦТ

К настоящему моменту приняты 7 из предусмотренных федеральным проектом «Цифровые технологии» дорожных карт СЦТ³²⁴. Технологическая область IoT не представлена отдельным документом – разработка соответствующей дорожной карты СЦТ была прекращена в 2019 г. Из принятых документов отдельные вопросы развития IoT затрагивают 3 документа:

1. Дорожная карта «Робототехника и сенсорика» предполагает развитие субтехнологии «Сенсоры и обработка сенсорной информации» за счет поддержки в размере 8,7 млрд руб. бюджетных средств³²⁵.
2. Дорожная карта «Новые производственные технологии» включает в себя развитие компонентов MES-систем, обеспечивающих использование ряда технологий, включая промышленный IoT³²⁶. Этот пункт входит в субнаправление развития технологий умного производства (Smart Manufacturing), общее финансирование которого до 2024 г. должно было составить 18,91 млрд руб., включая 7,6 млрд руб. бюджетных средств.
3. Дорожная карта «Беспроводные технологии связи»³²⁷ предусматривала широкий комплекс мер по развитию сетей LPWAN и во многом дублирует концепцию по их развитию, подготовленную в рамках федерального проекта «Информационная инфраструктура». В частности, согласно дорожной карте:
 - российское оборудование для основных технологий LPWAN, включая NB-IoT, LoRaWAN, NB-Fi и XNB, должно к 2024 г. составить не менее 50 % от используемого на домашнем рынке, а число российских производителей должно вырасти до 4 для каждой технологии;
 - в частности, к 2024 г. должны быть разработаны российские RF-модули для NB-IoT и LTE-M; чипы, трансиверы базовых станций и оконечное оборудование доступа для российских технологий XNB и NB-Fi;
 - предполагается обеспечить создание не менее 30 российских платформ сбора M2M-данных на базе LoRaWAN и не менее 15 платформ на базе XNB.

В дорожной карте также предусмотрено развитие спутниковой связи IoT, включая следующее:

- К 2024 г. развернуть полноценный сервис спутниковой связи для IoT на территории России с ценовыми параметрами услуг и абонентских устройств, конкурирующими с сотовыми и иными наземными сетями.
- К тому же сроку обеспечить подключение к сервисам спутникового IoT не менее 100 тыс. устройств.
- Достижение этих показателей должна обеспечить созданная с нуля система спутниковой связи «Марафон IoT».

Общее финансирование субнаправления LPWAN до 2024 г. должно было составить 30,41 млрд руб., включая 8,7 млрд руб. бюджетных средств; для спутниковой связи предполагается обеспечить 9,95 млрд руб. финансирования, в том числе 2,2 млрд из бюджета.

Дорожные карты развития высокотехнологичных областей (ВТО)

Несмотря на проработку отдельных технологических ниш IoT в перечисленных дорожных картах СЦТ, с отказом от отдельной дорожной карты в стратегическом планировании развития интернета вещей возник очевидный пробел. Попытка заполнить его была предпринята в контуре дорожных карт развития высокотехнологичных областей (ВТО) / высокотехнологичных направлений (ВТН).

- Создание таких дорожных карт по 8 направлениям, включая отдельную дорожную карту для IoT, предусмотрено распоряжением Правительства Российской Федерации от 8 июля 2019 г. № 1484-р³²⁸.
- По сути, дорожные карты развития ВТО были вписаны в логику и контур задач национальной программы «Цифровая экономика» постфактум и заменили дорожные карты СЦТ в актуализированной версии национальной программы с 2021 г.

Соглашение о развитии высокотехнологичного направления «Интернет вещей» было заключено между Правительством Российской Федерации и Госкорпорацией «Ростех» в декабре 2020 г., к соглашению прилагалась разработанная Госкорпорацией дорожная карта до 2024 г.

- Предложение Ростеха охватило широкий спектр задач: от комплексной подготовки кадров для IoT до разработки российских платформ и протоколов, облегчения доступа операторов IoT-сетей к необходимым полосам частот, венчурного финансирования российских разработок, развития индустриального IoT, инвестиций в R&D и развития российских патентных наработок и технических стандартов в области IoT.
- Магистральным направлением работы должно было стать создание российской платформенной экосистемы для IoT: от нишевых платформ и маркетплейсов до развития архитектурных фреймворков совместимости и открытой инфраструктуры разработки ПО для сервисов IoT.
- Ростехом ставились цели к 2024 г. довести объем продаж российских производителей на внутреннем рынке до 207,3 млрд руб., долю российских компаний на мировом рынке – до 0,36 %, а число подключенных устройств IoT – до 458,8 млн.
- Документ предполагал инвестирование в развитие IoT в общей сложности 41,6 млрд руб., включая 22,4 млрд руб. бюджетного финансирования. При этом Ростех не планировал вкладывать в реализацию дорожной карты собственные средства, что стало одной из причин критики документа в отраслевом и экспертном сообществе.

В 2021 г. в течение нескольких месяцев после утверждения дорожная карта решением Правительства Российской Федерации была разбита на отдельные мероприятия с усечением бюджета.

- В результате по состоянию на апрель 2022 г. реализация мероприятий дорожной карты полноценно не началась.
- Сам документ находится в процессе переработки Ростехом с целью последующего переутверждения в правительстве.
- Изменение ситуации после 24 февраля 2022 г. создает дополнительные задачи по обновлению и актуализации дорожной карты в части корректировки целевых показателей развития, ориентации на международный рынок и доступа к зарубежным технологиям для IoT.

2. Интернет вещей в ведомственных проектах российских ФОИВ

На следующем уровне мероприятия и задачи дорожных карт и федеральных проектов «приземляются» в отдельные ведомственные проекты федеральных органов власти. С момента утверждения национальной программы «Цифровая экономика» по апрель 2022 г. было публично анонсировано не менее 15 ведомственных проектов ФОИВ, в которых так или иначе фигурирует IoT³²⁹. Однако далеко не все из этих проектов получили финансовое наполнение, были утверждены и фактически запущены; еще меньше из них реализуются в соответствии с изначальными планами. Наиболее крупные и проработанные ведомственные проекты сконцентрированы в нишах промышленности, АПК и умного города.

Промышленность: Минпромторг России с 2019 г. реализует ведомственный проект «Цифровая промышленность», основанный на мероприятиях дорожной карты НПТ³³⁰. Одно из ключевых направлений проекта – создание системного механизма поддержки для цифровой трансформации промпредприятий по ряду технологических направлений, включая промышленный IoT.

- Министерство на основании Постановления Правительства Российской Федерации от 30.04.2019 № 529³³¹ предоставляет предприятиям обрабатывающих отраслей ежегодные субсидии на разработку цифровых платформ и ПО, включая платформы индустриального IoT. Общий распределяемый объем субсидий составляет 2 млрд руб. ежегодно, одним из условий является 50-процентное софинансирование проектов.
- Внедрение платформ индустриального IoT в 3 обрабатывающих отраслях поддерживается программой Фонда развития промышленности (ФРП) «Цифровизация промышленности». В рамках программы предприятиям предоставляются льготные займы на проекты по внедрению и масштабированию цифровых и технологических решений (1 %, сумма от 20 до 500 млн руб., срок до 5 лет).

На 2022 г. «Цифровая промышленность» – один из наиболее наполненных и активно реализуемых ведомственных проектов, затрагивающих область IoT. В то же время Минпромторг еще в 2019 г. отмечал ряд рисков, угрожающих достижению проектных целей³³²:

1. Низкая готовность промпредприятий к масштабной цифровой трансформации, включая внедрение интегрированных платформ IoT (готовы 14 % предприятий).

2. Низкая доля расходов на внедрение ИТ в бюджетах предприятий, невысокая рентабельность производств и потребность в дополнительных мерах господдержки, помимо уже действующих, для масштабных проектов внедрения цифровых решений.
3. Рост рисков информационной безопасности в промышленном секторе и потребность в крупных инвестициях в комплексные решения для ИБ как следствие цифровой трансформации.

Стоит отметить, что по промежуточным результатам проекта в части разработки и внедрения платформ промышленного IoT пока нет полных открытых данных, что мешает оценить его эффективность.

Сельское хозяйство: Министерство сельского хозяйства Российской Федерации в 2018 г. разработало ведомственный проект «Цифровое сельское хозяйство» (ЦСХ), рассчитанный на реализацию в 2019–2024 гг.

- Проект предусматривал создание и внедрение в составе национальной платформы «Цифровое сельское хозяйство» модуля «Агрорешения», включающего подсистему «Комплексные цифровые системы для АПК».
- В состав подсистемы должен был войти ряд нишевых функциональных модулей («Умная ферма», «Умное поле», «Умное стадо» и прочие), основанных в том числе на сборе и обработке M2M-данных с использованием технологий RFID и LPWAN, с упором на LoRaWAN.
- Собираемые M2M-данные планировалось использовать в том числе для наполнения и предоставления сервисов национальной платформы «Цифровое сельское хозяйство». Приказ Минсельхоза о создании платформы был утвержден в феврале 2020 г.³³³
- Паспорт проекта предусматривал в общей сложности 4,05 млрд руб. бюджетного финансирования на проектирование и реализацию модуля «Агрорешения».

По состоянию на апрель 2022 г. ведомственный проект не был запущен из-за отсутствия финансирования. Министерство продолжает продвигать инициативу создания платформы ЦСХ, однако до сих пор она не была реализована.

Умный город: с ведомственными проектами развития IoT в нише «Умный город» в России сложилась достаточно интересная и запутанная ситуация. На данный момент действуют, разрабатываются или обсуждаются не менее 4 проектов, нацеленных примерно на одни и те же отраслевые ниши и технологические решения для них.

1. С 2014 г. Министерством чрезвычайных ситуаций России (МЧС) реализуется проект «Безопасный город», в основе которого лежит концепция построения и развития одноименного аппаратно-программного комплекса (АПК)³³⁴.
 - Функционал АПК предполагает интеграцию с городскими системами видеонаблюдения, мониторинга общественной безопасности и экологической обстановки, ИТС и другими системами, основанными на технологиях IoT и M2M-коммуникаций.
 - К 2020 г., по данным МЧС, «Безопасный город» был запущен в 12 регионах РФ, суммарные расходы бюджета на его внедрение превысили 16 млрд руб.³³⁵
 - В 2021 г. координация проекта в целях снижения бюджетных расходов на него была передана от МЧС к Минцифры. На тот момент МЧС оценивало расходы на полноценный запуск комплекса «Безопасный город» во всех субъектах Российской Федерации в 97 млрд руб. до 2030 г.³³⁶

Исходя из доли российских субъектов, подключенных к АПК «Безопасный город», ведомственный проект с 2014 г. реализован на 14 %.

2. В 2018 г. Минстрой России разработал и утвердил паспорт³³⁷ ведомственного проекта цифровизации городского хозяйства «Умный город»³³⁸.
 - Проект предполагал внедрение и тиражирование решений по цифровизации городского хозяйства в 2019–2024 гг.
 - Концепция проекта была доработана в декабре 2020 г.³³⁹ и включала в себя ряд направлений, связанных с внедрением сервисов IoT, включая умное ЖКХ, ИТС, системы дистанционного контроля и мониторинга качества воды, воздуха и т. д.
 - С 2021 г. реализация проекта была преимущественно заморожена, а значительная часть его наполнения, включая цифровизацию городского хозяйства, была перенесена в проект «Цифровой регион».
 - Несмотря на приостановку проекта, в мае 2022 г. Минстрой России утвердил базовый стандарт «Умного города»³⁴⁰. Речь в данном случае идет не о национальном стандарте ГОСТ Р, а о едином наборе базовых и дополнительных требований к цифровой инфраструктуре городского хозяйства и управлению ей. Утвержденный документ охватывает 18 тематических блоков, описывающих требования по конкретным нишам «Умного города»: образованию, здравоохранению, городским услугам, транспортным системам и т. д.³⁴¹

3. В октябре 2019 г. Совет по развитию цифровой экономики при Совете Федерации предложил дополнить «Умный город» новым проектом «Цифровой регион»³⁴². Проект должен обеспечить внедрение цифровых технологий в населенных пунктах, помимо крупных городов, и связать воедино информационные системы «Умного города» в масштабе каждого региона. Координацию проекта обеспечивают Минцифры, Минэкономразвития и Минвостокразвития РФ.
 - Подготовка концепции «Цифрового региона» стартовала в апреле 2020 г. на площадке АНО «Цифровая экономика».
 - В приоритетные направления проекта вошли цифровая трансформация ЖКХ и сектора энергораспределения за счет внедрения систем интеллектуального контроля, мониторинга и прослеживаемости на базе технологий IoT.
 - С июня 2020 г. Минцифры неоднократно переносило³⁴³ утверждение проекта, в том числе с учетом того, что его мероприятия дублируют проект «Безопасный город» и другие ведомственные проекты, а также проекты субъектов Российской Федерации по цифровизации городского хозяйства. В итоге на апрель 2022 г. «Цифровой регион» не был запущен.
4. В 2021 г. Минцифры объявило о планах внедрить в субъектах Российской Федерации систему «Безопасный регион»³⁴⁴.
 - Платформа должна объединить управление процессами обеспечения городской безопасности, включая видеонаблюдение, мониторинг дорожного движения и экологической обстановки, работу и состояние особо опасных объектов и объектов критической инфраструктуры³⁴⁵.
 - При этом Минцифры публично не разъясняло связь этого проекта с проектом «Безопасный город», их различия и необходимость запуска новой инициативы.

Таким образом, ниша управления умным городом, основанная прежде всего на применениях IoT, остается полем конкуренции дублирующих друг друга проектов различных ведомств и групп интересов, что снижает темпы и качество ее развития.

- Основной вклад в развитие инфраструктуры умного города, в том числе за счет IoT, в этих условиях вносят проекты субъектов Российской Федерации и городов федерального значения, а также корпоративные инициативы.
- Без федеральной поддержки масштабные инвестиции в развитие умного города оказываются сконцентрированы в нескольких крупнейших городах, таких как Москва, Санкт-Петербург, Казань, Сочи. Так, по одной из оценок на 2019 г., Москва занимала 93 % российского рынка умных городов³⁴⁶. Остальные населенные пункты оказываются выключены из повестки «Умного города» в силу нехватки ресурсов.
- Для изменения ситуации необходим отдельный мастер-план, фиксирующий межведомственное распределение ролей и бюджетов в комплексе задач по развитию умных городов. Не менее востребована единая сквозная система целевых показателей для различных ФОИВ, которая обеспечивала бы взаимоувязку их задач и способствовала слому ведомственных функциональных колодцев.

- Как альтернативный вариант, развитие инфраструктуры умного города, в том числе за счет применений IoT, может быть полностью делегировано на региональный и муниципальный уровни с поддержкой из федерального бюджета и расширением возможностей формирования государственно-частных партнерств (ГЧП).

3. Венчурное и грантовое финансирование развития IoT

Система грантового финансирования проектов IoT в России начала формироваться с 2015–2016 гг. с развитием НТИ. В 2018 г. с принятием национальной программы «Цифровая экономика» была сформирована более комплексная система инструментов грантовой и иной поддержки, в основном описанная в дорожных картах СЦТ федерального проекта «Цифровые технологии».

- В число таких инструментов вошли субсидии на грантовые конкурсы, субсидирование процентной ставки по кредиту, выделение финансирования по модели господдержки программ деятельности лидирующих исследовательских центров (ЛИЦ) и несколько иных вариантов поддержки разработки и внедрения цифровых решений российскими компаниями и промпредприятиями.
- Операторы мер поддержки были определены рядом постановлений Правительства Российской Федерации в мае 2019 г.³⁴⁷ в привязке к конкретным технологическим направлениям СЦТ и механизмам поддержки. Из участников системы венчурного финансирования в число операторов мер господдержки вошли Российская венчурная компания (РВК) и Российский фонд прямых инвестиций, Фонд «Сколково», Российский фонд развития информационных технологий (РФРИТ), Фонд содействия инновациям (ФСИ) и Фонд развития интернет-инициатив (ФРИИ).
- При этом выделение средств на проекты по направлению IoT как минимум до 2021 г. оказалось заморожено в программах некоторых из перечисленных фондов из-за отсутствия утвержденной дорожной карты СЦТ по нему.

Российский фонд развития информационных технологий (РФРИТ)

С 2019 г. РФРИТ является одним из наиболее значимых операторов грантового финансирования для проектов в области сквозных технологий, включая IoT.

- Фонд на основании Постановления Правительства Российской Федерации от 3 мая 2019 г. № 550³⁴⁸ распределяет крупные гранты и мегагранты для особо значимых проектов по разработке отечественных ИТ-решений³⁴⁹. С 2022 г. максимальный объем крупных грантов был увеличен до 500 млн руб., а мегагрантов – до 6 млрд руб.
- С 2019 г. РФРИТ, наряду с Фондом «Сколково», стал оператором грантовых средств на разработку и внедрение отечественного ПО на основе «сквозных технологий» на 2019–2024 гг., выделенных в рамках федерального проекта «Цифровые технологии»³⁵⁰.

- В связи с отсутствием IoT в списке дорожных карт СЦТ проекты по этому направлению не принимались фондом как минимум до 2021 г. С 2021 г. в список действующих грантовых направлений входят³⁵¹ ПО для интернета вещей, робототехники и сенсорики и несколько смежных с IoT ниш:
 - решения для оборудования с числовым программным управлением (CAM);
 - средства управления производственными процессами (MES);
 - АСУ ТП и SCADA;
 - средства автоматизированного управления техникой;
 - средства централизованного управления конечными устройствами³⁵².

В общей сложности до 2024 г. РФРИТ должен был распределить по всем направлениям грантового финансирования 38,36 млрд руб.³⁵³ Объемы грантовой поддержки проектов, связанных с IoT, можно оценить лишь косвенно на основе анализа уже распределенных средств.

- За 2021 г. Фонд распределил в общей сложности 4,557 млрд руб. на 62 проекта, включая как разработку, так и внедрение ИТ-решений³⁵⁴.
- Анализ списка грантополучателей показывает, что общая сумма финансирования проектов, в которых в той или иной степени задействованы технологии IoT, составляет 985 млн руб., включая как разработку, так и внедрение ИТ-решений (21,6 % от общей суммы).
- Однако объем финансирования, который приходится непосредственно на ПО и оборудование IoT в этих проектах, оценить сложно, так как проекты предполагают создание мультитехнологичных платформенных решений или комплексную цифровую трансформацию предприятий. Применение подключенных датчиков, сенсоров, цифровых двойников, облачных и платформенных сервисов IoT может входить в работы, но их доля в структуре бюджета непрозрачна.

Фонд «Сколково»

- Постановление Правительства Российской Федерации от 03.05.2019 № 555³⁵⁵ определило Фонд «Сколково» в качестве оператора грантового финансирования проектов масштабного внедрения ИТ-решений российскими компаниями. Одновременно Фонд выступает оператором мер поддержки в рамках механизмов, закрепленных Постановлениями Правительства № 550 и № 554.
- Общая сумма финансирования, выделяемая Фонду из государственного бюджета на эти цели, должна составить 11,37 млрд руб. до 2024 г.³⁵⁶
- В число направлений, по которым осуществляется поддержка проектов, с 2021 г. входит ПО интернета вещей, робототехники и сенсорики³⁵⁷. Общая сумма грантового финансирования по данному направлению, распределенная на 2022 г., неизвестна, так как статистика проектов – получателей грантовой поддержки не ведется Фондом в разрезе направлений.

Фонд развития интернет-инициатив (ФРИИ)

ФРИИ одним из первых российских фондов начал инвестировать в проекты развития IoT. В 2016 г., еще до начала разработки национальной программы «Цифровая экономика», Фонд запустил серию проектов, нацеленных на акселерацию, пилотирование и масштабирование проектов IoT.

- В 2016 г. ФРИИ объявил о создании первого кросс-отраслевого полигона для тестирования пилотных проектов IoT в нише умного города в г. Иннополис. Для этих целей Фондом выделялись дополнительные инвестиции на сумму 500 млн руб.³⁵⁸
- В том же году Фонд объявил, что готов вкладывать средства в российские команды, занимающиеся разработкой продуктов и услуг в сфере IoT, от 2 до 320 млн руб. на компанию³⁵⁹. Программу акселерации IoT-стартапов предполагалось реализовать в партнерстве с бизнесом, в том числе используя для масштабирования проектов производственные площадки частных компаний (в т. ч. холдинг GS Group)³⁶⁰. Проекты отбирались по четырем направлениям: умный дом, умный город, агротех и промышленный IoT³⁶¹.
- Итоговый охват программы акселератора оказался точечным; по итогам нескольких раундов акселерационных программ инвестиции на развитие получили порядка 8 стартапов в области IoT, на 2022 г. большая часть из этих проектов не активна³⁶².
- За 2019–2024 гг. ФРИИ должен получить 1 млрд руб. из федерального бюджета на акселерацию разработки российских ИТ-решений по направлениям дорожных карт СЦТ³⁶³. Текущая статистика по акселерации проектов, связанных с разработкой решений для IoT, недоступна.

Фонд содействия развитию малых форм предприятий в научно-технической сфере (Фонд содействия инновациям, ФСИ)

- ФСИ выступает оператором мер господдержки в рамках направлений дорожных карт СЦТ. С 2019 по 2024 гг. Фонду должно быть выделено из бюджета в общей сложности 11,70 млрд руб. на поддержку проектов малых предприятий по разработке, применению и коммерциализации российских цифровых решений³⁶⁴.
- С 2020 г. Фонд запустил конкурсную программу «Старт – Цифровые технологии», нацеленную на поддержку стартапов. Программа доступна для физических лиц и микробизнеса и обеспечивает победителям отбора до 4/8/12 млн руб. финансирования по разным трекам программы. Интернет вещей, робототехника и сенсорика входят в список приоритетных направлений поддержки³⁶⁵.
- В 2020 г. по линии «Старта» было распределено 234,2 млн руб.³⁶⁶, в 2021 г. по итогам конкурсного отбора «Старт-1» и «Старт-2» были одобрены 113 заявок на сумму 372 млн руб.³⁶⁷ Доля проектов, связанных с IoT, среди них составляет порядка 15–20 %.
- Кроме того, Фонд реализует программу поддержки вывода на рынок ИТ-разработок российских малых инновационных предприятий – «Коммерциализация». За 2021 г. в рамках программы были поддержаны 285 проектов. Общая сумма грантов составила 4,7 млрд руб.³⁶⁸ Доля проектов, связанных с IoT, может быть оценена в 12–15 %.

Российский фонд прямых инвестиций (РФПИ) и Российская венчурная компания (РВК)

Российская венчурная компания, включенная в состав РФПИ в 2020 г., была назначена оператором двух мер поддержки, предусмотренных дорожными картами СЦТ.

- В 2019 г. РВК начала конкурсный отбор программ лидирующих исследовательских центров (ЛИЦ) и проектов компаний-лидеров с предоставлением трехлетних грантов на НИОКР и внедрение сквозных технологий. Суммы грантов составили до 300 млн для проектов ЛИЦ и до 250 млн для компаний-лидеров.
- Однако с 2020 г. программа ЛИЦ была свернута в связи с переработкой механизмов поддержки под новые приоритеты дорожных карт высокотехнологичных областей (ВТО).

Наконец, отдельные российские венчурные фонды, связанные с государственным капиталом, инвестируют в проекты в нише IoT и вне рамок механизмов поддержки, предусмотренных дорожными картами национальной программы. Наиболее масштабную деятельность такого рода в последние годы ведет венчурный фонд Внешэкономбанка (ВЭБ).

Венчурный фонд ВЭБ (VEB Ventures)

Фонд VEB Ventures существенно нарастил инвестиционную активность в нише IoT за последние два года. Предпочтение отдается крупным проектам, нацеленным на создание платформенных либо иных интегрированных инфраструктурных сервисов.

- В 2020 г. VEB Ventures и венчурный фонд ГК «Росатом» инвестировали 260 млн руб. в компанию Alphaopen, которая разрабатывает программные решения для инфраструктурных проектов в области умных городов и умного строительства. На первом этапе предполагалось вложить в проект 260 млн руб. с возможностью дополнительного финансирования в будущем. Alphaopen планировала направить средства на развитие программной платформы Alphalogic, обеспечивающей единую среду управления для различных сервисов IoT (умные датчики, видеонаблюдение, освещение, сигнализация)³⁶⁹.
- В декабре 2021 г. VEB Ventures за 400 млн руб. приобрел долю у компании Mircod, производителя устройств IoT, специализирующегося в нише медицинского интернета вещей (IoMT)³⁷⁰.

4. Государственные регуляторные инициативы: обязательные требования как драйверы рынка

Одной из особенностей России является сильное влияние на рынок регуляторных инициатив, которые генерируют спрос на IoT за счет обязательных требований по применению умных подключенных устройств. Такие требования особенно активно вводятся в последние 2–3 года и в значительной степени формируют спектр применений технологий интернета вещей.

- В автотранспортном секторе все более значимым драйвером рынка IoT является ЭРА-ГЛОНАСС для автоматического оповещения экстренных служб в случае ДТП. В России с 2017 г. система в обязательном порядке устанавливается на покупаемые и ввозимые автомобили³⁷¹. По данным на 2022 г., число зарегистрированных в ЭРА-ГЛОНАСС автомобилей составило 8,6 млн³⁷². С 1 сентября 2021 г. вступило в силу Постановление Правительства Российской Федерации от 22.12.2020 № 2216, которое обязывает устанавливать средства спутниковой навигации ЭРА-ГЛОНАСС на транспортные средства, используемые для пассажирских перевозок и перевозок опасных грузов³⁷³. Это требование дополнительно расширяет рынок модулей ЭРА-ГЛОНАСС как минимум на 30 % и позволит сохранить объемы их производства на ближайшие 5–7 лет, несмотря на «насыщение» ниши легкового автотранспорта. Еще один источник роста рынка ЭРА-ГЛОНАСС – возможность использования модулей системы в коммерческих сервисах перевозчиков, в том числе для управления автопарком.
- Государственная система взимания платы с грузового автотранспорта «Платон» продолжает расширять спрос на телематические устройства. По данным на апрель 2022 г., в системе было зарегистрировано 1,624 млн транспортных средств, а общее число выданных бортовых устройств (БУ) превысило 2,35 млн с учетом ранее замененных³⁷⁴. С учетом закупочной стоимости БУ порядка 4–5 тыс. руб. и гарантийного срока эксплуатации 3 года, «Платон» с момента своего запуска в 2015 г. обеспечил прямой спрос на устройства IoT в объеме не менее 5 млрд руб., не считая ПО для обработки данных с бортовых устройств и иного оборудования системы.
- Новым фактором роста для рынка телематики в транспортной отрасли в ближайшие годы может стать масштабирование системы автоматического весогабаритного контроля (АС ВГК) для грузового транспорта весом свыше 12 тонн. Согласно паспорту национального проекта «Безопасные и качественные автомобильные дороги», его общий бюджет с 2020 по 2030 гг. должен составить 134,26 млрд руб., в том числе 121,54 млрд руб. средств федерального бюджета³⁷⁵. В рамках национального проекта к 2024 г. планируется разместить 387 пунктов весогабаритного контроля на федеральных трассах и 366 – на региональных, в 5,5 раза увеличив число пунктов ВГК по сравнению с 2020 г. (140)³⁷⁶. Реализацию проекта пока тормозит отсутствие полноценной законодательной базы и затянувшийся выбор поставщика технических решений. На середину 2021 г. Министерство транспорта рассматривало в качестве основного варианта концессионный договор с ООО «Ростелематика»³⁷⁷.
- Яркий пример формирования спроса на устройства IoT за счет введения обязательных требований появился в нише энергоучета. С января 2022 г. вступило в силу положение № 522-ФЗ от 27.12.2018, согласно которому в многоквартирных домах должны устанавливаться только интеллектуальные счетчики электроэнергии³⁷⁸. В требованиях к таким приборам учета, установленных в 2020 г. Правительством РФ, описываются полноценные энергоэффективные устройства IoT с поддержкой беспроводной связи и автоматизированной записи и передачи данных³⁷⁹. Эффект нового регулирования для рынка особенно значим в силу того, что уровень внедрения интеллектуальных электросчетчиков пока достаточно низок – 14–15 % на начало 2022 г.³⁸⁰ Минэнерго в 2020 г. оценило потребность в таких приборах учета в 76 млн шт. до 2035 г.³⁸¹ Стоимость таких приборов учета составляет от 3 до 5 тыс. руб.³⁸², а совокупная потребность рынка в них оценивается в 1,5 млн счетчиков ежегодно. Исходя из этих вводных, нормы № 522-ФЗ могут

обеспечить спрос на устройства IoT объемом 4,5–7,5 млрд руб. ежегодно на ближайшие 8–12 лет. Однако в нынешнем варианте принятые НПА не делают такой спрос твердо гарантированным и позволяют управляющим компаниям откладывать переход на энергосберегающее умное оборудование учета. Поэтому приведенные оценки описывают потенциальный, а не фактический объем генерируемого спроса.

- С июля 2019 г. вступили в силу положения Приказа № 227 Министерства транспорта Российской Федерации от 26.07.2017³⁸³, которые обязывают оснащать цифровыми тахографами с блоком средств криптографической защиты информации грузовой и пассажирский автотранспорт. По оценке ПАО «МТС» от 2021 г., это требование может обеспечить суммарный рост числа новых подключений IoT на российском рынке на 40 %³⁸⁴.
- Как отмечается в исследованиях российского рынка³⁸⁵, в перспективе 2022–2024 гг. генерировать спрос на устройства IoT могут и другие государственные требования. К наиболее вероятным и значимым для рынка инициативам относятся обновление требований к:
 - контрольно-кассовой технике с поддержкой онлайн-передачи данных;
 - оснащению автомобилей цифровыми тахографами;
 - телематическому контролю транспортировки скоропортящихся грузов и транзитных перевозок санкционных товаров и т. п.
- Кроме того, схожие инициативы содержатся во «втором пакете» мер поддержки ИТ-отрасли, принятом в сентябре 2021 г.³⁸⁶ Документ предусматривает принятие НПА с целью создания государственных систем мониторинга погоды и экологической ситуации, опасных производств и потребления коммунальных услуг бюджетными организациями на базе российских решений для IoT.

В условиях санкционных ограничений, ухода с российского рынка IoT ряда крупных игроков и общего сжатия платежеспособного спроса роль ниш, в которых спрос обеспечен обязательными требованиями, становится особенно значима. Причем речь идет не только о финансовом объеме рынка, но и о росте числа устройств IoT.

- Только три из рассмотренных выше наборов требований (НПА по ЭРА-ГЛОНАСС и системе «Платон», № 522-ФЗ) за ближайшие 10 лет могут обеспечить рост числа устройств в российском сегменте IoT более чем в 1,5 раза (с 29,6 млн до более чем 50 млн).
- Как минимум с 2017 г. обсуждается функциональная интеграция ЭРА-ГЛОНАСС, «Платона» и систем ВГК³⁸⁷. Подобные проекты потенциально способны создавать объединенные телематические «мегасервисы», в которых комплект встроенного телематического оборудования сможет передавать широкий и многосоставный набор данных о состоянии транспортного средства. Парадокс в том, что такой подход снизит темпы роста числа подключенных устройств IoT за счет интеграции различных функций в одном телематическом модуле, но одновременно он может сократить издержки и для операторов «мегасервиса», и для его пользователей.

При этом государственные инициативы и требования по цифровизации не застрахованы от сценариев выполнения в ущерб экономической и управленческой эффективности и должны балансироваться спросом, основанным на конкурентных рыночных механизмах.

5. Радиочастотное регулирование IoT в России

Выделение частот для сотовых LPWAN

Выделение радиочастотного спектра для LPWAN на базе сотовой связи происходило параллельно с проникновением этих технологий на российский рынок и, в отличие от ситуации со связью 5G, не носило запаздывающий характер. С 2017 г. Государственная комиссия по радиочастотам (ГКРЧ) приняла ряд решений, расширяющих доступные частоты в лицензируемых диапазонах для сотовых LPWAN:

- Решением ГКРЧ от 28 декабря 2017 г. № 17-44-06³⁸⁸ были выделены 14 полос частот в субгигагерцевом диапазоне и диапазонах 1,7 ГГц, 1,8 ГГц, 1,9 ГГц, 2,1 ГГц, 2,5 ГГц для развития операторами связи сетей NB-IoT.
- Для развертывания сетей IoT на базе технологии eMTC (LTE M) и EC-GSM-IoT могут использоваться ранее выделенные операторам сотовой связи частоты. В частности, для сетей LTE M доступен частотный диапазон 1,8 ГГц. Для более масштабного внедрения LTE M может потребоваться выделение полос частот в диапазоне 694–790 МГц, оптимальном для этой технологии. В данный момент эти полосы частот недоступны, так как на них работают сети эфирного телевидения.
- Также могут быть востребованы диапазоны 800 МГц и 900 МГц для развертывания сетей за пределами городской черты. Использование этих диапазонов ограничено из-за работы систем воздушной радионавигационной службы (ВРНС). Однако на данный момент дефицит частот для LTE M не является острой проблемой, так как технология менее востребована, чем NB-IoT, и число крупных сетей на ее базе невелико.

Выделение частот для несотовых LPWAN

Полосы радиочастот в нелицензируемых диапазонах для несотовых LPWAN выделены решением ГКРЧ от 07.05.2007 № 07-20-03-001³⁸⁹, в которое впоследствии неоднократно вносились изменения. В настоящее время используются технологии LoRaWAN (полосы 864–865 МГц, 868,7–869,2 МГц) и узкополосные протоколы российской разработки:

1. NB-Fi – 863–876 МГц / 433 МГц.
2. Open UNB – 868,8 МГц.
3. XNB – 868,8 МГц.

Основная проблема состоит в том, что в России не выделены полосы частот достаточной мощности в диапазоне 868,7–869,2 МГц. Именно этот диапазон является наиболее востребованным для развития LPWAN-сетей в мире, в том числе в ЕС и других странах, которые до февраля 2022 г. выступали основными поставщиками оборудования и технологических решений для развития сервисов IoT на базе сетей LPWAN в России.

Текущая ситуация с выделением полос частот в диапазоне 868,7–869,2 МГц и «вокруг» него (863–876 МГц) ведет к тому, что:

- во-первых, использование зарубежных протоколов и технологий для развития несотовых LPWAN, включая LoRaWAN, требует перенастройки оборудования под российские полосы частот. При этом в международном реестре сертифицированных продуктов для LoRaWAN, который ведет LoRa Alliance, пока нет ни одного решения, поддерживающего региональные параметры российской сети³⁹⁰;
- во-вторых, нехватка ширины и мощности выделенных полос частот становится барьером для массированного развертывания узкополосных сетей участниками рынка.

Выделение частот для ИТС

Решениями ГКПЧ от 19.02.2010 № 10-06-03-2 и от 10.03.2011 № 11-11-01-2 предусмотрено нелицензируемое использование полос радиочастот 5855–5925 МГц и 63–64 ГГц соответственно. В этих полосах частот, в частности, работает протокол DSRC, широко применяемый в подключенных автомобилях и управлении ИТС.

Выделение частот для технологий ближнего радиуса действия для IoT

Одним из актуальных вопросов на 2022 г. остается выделение радиочастотного ресурса для спецификации Wi-Fi 6E, которая имеет большой потенциал применений в IoT.

- Частоты в диапазоне 6 ГГц остаются недоступны для коммерческих применений, в том числе в сетях беспроводной связи на базе Wi-Fi, так как диапазон 5925–7125 МГц преимущественно используется средствами фиксированной радиосвязи и радиорелейными линиями связи (РРЛ).
- Частотный диапазон для Wi-Fi 6E в России предполагается использовать для развития технологии 5G. На начало 2021 г. полосы в диапазонах 6,4–6,8 ГГц для развития 5G были выделены ФГУП «НИИ Радио» для тестирования оборудования сетей связи 5G³⁹¹.

Выделение частот для спутниковой связи IoT

Отдельные полосы частот для развития IoT-сетей были выделены ООО «ГЛОНАСС-ТМ» в 2018 г. для расширения применения спутниковой системы ГЛОНАСС и создания Федеральной сети транспортной телематики.

- Полосы в диапазоне 863–865 МГц и 874–876 МГц были выделены решением ГКРЧ от 30 ноября 2018 г. № 18-47-05³⁹².
- На сегодняшний день оператор ГЛОНАСС использует российский LPWAN-протокол XNB, передающий сигнал в частоте 868,8 МГц.

Однако с учетом того, что проект ФСТТ на сегодняшний день не завершен, вопрос полезного использования этих частот остается открытым.

Источники

- 1 IoT connections outlook. Ericsson Mobility Report. Ericsson. <https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook>
- 2 Measuring digital development Facts and figures 2021. International Telecommunication Union, 2021. <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf>
- 3 МСЭ-Т Y.2060. Серия Y: глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений – структура и функциональные модели архитектуры. Обзор интернета вещей. Сектор стандартизации электросвязи МСЭ (06/2012). https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-1!!!PDF-R&type=items
- 4 Перспективные рынки и технологии интернета вещей: публичный аналитический доклад. Пригарин Василий Евгеньевич. М.: ООО «Лайм», 2019, 272 с.: ил. <https://publications.hse.ru/books/323662569>
- 5 M2M standardization in ITU-T and its perspective. ITU Workshop on “Standardization on IMT, M2M, IoT, Cloud Computing and SDN”. Hyoung Jun Kim, ETRI. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/standardization/201309/Documents/S2P4_Hyoungh-Jun-Kim.ppt
- 6 Источники данных:
 - a) Ericsson Mobility Report 2021. Ericsson. <https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/november-2021>
 - b) GSMA Intelligence. Internet of Things. GSMA. <https://data.gsmaintelligence.com/data>
 - c) The Mobile Economy 2022. GSMA. <https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf>
 - d) State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. IoT Analytics. <https://iot-analytics.com/number-connected-iot-devices/>
 - e) The Internet of Things 2020: Here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue. Business Insider Intelligence. <https://www.businessinsider.com/internet-of-things-report>
 - f) IoT Connections Forecast 2019–2030. Transforma Insights. <https://transformainsights.com/research/forecast/highlights>
- 7 Digital Economy Report 2021. Cross-border data flows and development: For whom the data flow. UNCTAD. https://unctad.org/system/files/official-document/der2021_en.pdf
- 8 State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. IoT Analytics. <https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/>
- 9 Данные Ericsson Mobility Report 2021, GSMA Mobile Economy 2022.

- 10 Данные BusinessInsider Intelligence, IoT Analytics, Transforma Insights.
- 11 Connected world. An evolution in connectivity beyond the 5G revolution. McKinsey Global Institute. February 2020. https://www.mckinsey.com/~media/mckinsey/industries/technology%20media%20and%20telecommunications/telecommunications/our%20insights/connected%20world%20an%20evolution%20in%20connectivity%20beyond%20the%205g%20revolution/mgi_connected-world_discussion-paper_february-2020.pdf
- 12 IoT & Industry 4.0 in the 5G era Huawei's perspective. Huawei. June 2021. https://www.gsma.com/iot/wp-content/uploads/2021/07/Mobile-IoT-Summit-2-Huawei_IoT-and-Industry-4.0-in-the-5G-Era.pdf
- 13 The contribution of IoT to economic growth Modelling the impact on business productivity. GSM Association. April 2019. <https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=41091146&file=2749-240419-IoT-Productivity.pdf>
- 14 Connected world. An evolution in connectivity beyond the 5G revolution. McKinsey Global Institute. February 2020. https://www.mckinsey.com/~media/mckinsey/industries/technology%20media%20and%20telecommunications/telecommunications/our%20insights/connected%20world%20an%20evolution%20in%20connectivity%20beyond%20the%205g%20revolution/mgi_connected-world_discussion-paper_february-2020.pdf
- 15 13Б – 1024 ЭБ или 1,024*1012 ГБ.
- 16 Future of Industry Ecosystems: Shared Data and Insights. Shared Data and Insights are Making Organizations More Resilient, Flexible and Profitable. IDC. January 6, 2021. <https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/>
- 17 a) Internet of Things (IoT) Market to Witness 26.4% CAGR from 2022 to 2029; Oracle Corporation Launched Portable Server for Edge Computing to Expand Footfall. March 2022. <https://www.fortunebusinessinsights.com/press-release/internet-of-things-iot-market-9155>;
- b) Digital economy report 2021. Cross-border data flows and development: For whom the data flow. UNCTAD. 2021. https://unctad.org/system/files/official-document/der2021_en.pdf
- 18 Данные Fortune Business Insights, McKinsey.
- 19 Worldwide Spending on the Internet of Things Will Slow in 2020 Then Return to Double-Digit Growth, According to a New IDC Spending Guide. BusinessWire. June 18, 2020. <https://www.businesswire.com/news/home/20200618005125/en/Worldwide-Spending-on-the-Internet-of-Things-Will-Slow-in-2020-Then-Return-to-Double-Digit-Growth-According-to-a-New-IDC-Spending-Guide>
- 20 См. Digital economy report 2021, UNCTAD.
- 21 China to become world's largest IoT market in 2024, says report. Business Insider India. 17.01.2022. <https://www.businessinsider.in/tech/news/china-to-become-worlds-largest-iot-market-in-2024-says-report/articleshow/80312630.cms>
- 22 См. Digital economy report 2021, UNCTAD.

- 23 The mobile Economy 2021. GSM Association. https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/07/GSMA_MobileEconomy2021_3.pdf
- 24 См. Digital economy report 2021, UNCTAD.
- 25 Российский и мировой рынок межмашинных коммуникаций и интернета вещей по итогам 2020 года, предварительные оценки на 2021 год и прогноз до 2025 г. Json. TV. 15 января 2022 г. https://json.tv/ict_telecom_analytics_view/rossiyskiy-i-mirovoy-ry-nok-mejmashinnyh-kommunikatsiy-i-interneta-veschey-po-itogam-2020-goda-pred-varitelnye-otsenki-na-2021-god-i-prognoz-do-2025-goda-20220115025817
- 26 Global gross domestic product (GDP) at current prices from 1985 to 2026. Statista. January 2022. <https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/>
- 27 The Internet of Things: Catching up to an accelerating opportunity. McKinsey & Company. November 2021. <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf>
- 28 The contribution of IoT to economic growth. Modelling the impact on business productivity. GSM Association. April 2019. <https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=41091146&file=2749-240419-IoT-Productivity.pdf>
- 29 The Internet of Things and economic growth in a panel of countries. December 2019. Economics of Innovation and New Technology. <https://www.tandfonline.com/doi/full/10.1080/10438599.2019.1695941>
- 30 The contribution of IoT to economic growth. Modelling the impact on business productivity. GSM Association. April 2019. <https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=41091146&file=2749-240419-IoT-Productivity.pdf>
- 31 См. The Internet of Things: Catching up to an accelerating opportunity. McKinsey & Company.
- 32 Здесь и далее по тексту абзаца: данные GSMA Mobile Economy 2021/2022 и GSMA Intelligence, Ericsson Mobility Report, IoT Analytics, Transforma Insights и Digital Economy Report 2021.
- 33 a) Ericsson Mobility Visualizer. Ericsson. <https://www.ericsson.com/en/reports-and-papers/mobility-report/mobility-visualizer?f=16&ft=2&r=1&t=21,23&s=14&u=1&y=2016,2027&c=1>
- b) Current Forecast Highlights. Transforma Insights. May 2022. <https://transformainsights.com/research/forecast/highlights>
- c) State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. IoT Analytics. May 2022. <https://iot-analytics.com/number-connected-iot-devices>
- d) Hyperscale Cellular IoT. Add a programmable layer of policy and security. January 2022. <https://www.aptilo.com/wp-content/uploads/2022/01/Hyperscale-Cellular-IoT-Connectivity-v2-01-22.pdf>

- 34 Данные GSMA, Ericsson, Transforma Insights.
- 35 2G and 3G Sunsets: When They'll Happen and How to Prepare. EMnify. April 2022. <https://www.emnify.com/blog/global-2g-3g-phase-out>
- 36 Там же.
- 37 Данные Ericsson, GSMA, Transforma Insights.
- 38 а) M.2083: IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond. International Telecommunication Union. September 2015. <https://www.itu.int/rec/R-REC-M.2083-0-201509-1/en>
- b) Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2020. Radiocommunication center of ITU. February 2022. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2150-1-202202-1!!PDF-E.pdf
- 39 New WID on support of reduced capability NR devices. Ericsson. December 2020. https://www.3gpp.org/ftp/TSG_RAN/TSG_RAN/TSGR_90e/Docs/RP-202933.zip
- 40 Данные Transforma Insights; IoT Analytics.
- 41 Данные IoT Analytics, Transforma Insights. В оценку входят только подключения в сценариях 5G eMBB/URLLC. Таким образом, из оценки исключен сценарий 5G mMTC для подключения устройств IoT.
- 42 Gartner Predicts Outdoor Surveillance Cameras Will Be Largest Market for 5G Internet of Things Solutions Over Next Three Years. Gartner. October 2019. <https://www.gartner.com/en/newsroom/press-releases/2019-10-17-gartner-predicts-outdoor-surveillance-cameras-will-be>
- 43 Connected world. An evolution in connectivity beyond the 5G revolution. McKinsey Global Institute. February 2020. https://www.mckinsey.com/~media/mckinsey/industries/technology%20media%20and%20telecommunications/telecommunications/our%20insights/connected%20world%20an%20evolution%20in%20connectivity%20beyond%20the%205g%20revolution/mgi_connected-world_discussion-paper_february-2020.pdf
- 44 The Future of Global 5G IOT Market Expected to Generate a Revenue of \$12,556.5 Million by 2028, Growing at a CAGR of 28.1% from 2021 to 2028. Research Dive. November 2021. <https://www.globenewswire.com/news-release/2021/11/23/2339918/0/en/The-Future-of-Global-5G-IOT-Market-Expected-to-Generate-a-Revenue-of-12-556-5-Million-by-2028-Growing-at-a-CAGR-of-28-1-from-2021-to-2028-Exclusive-220-pages-Report-by-Research-Div.html>
- 45 а) Cellular IoT in the 5G era. Ericsson. <https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-in-the-5g-era>
- b) Целевая сеть NetX2025: технический документ. Huawei. <https://huawei.ru/upload/medialibrary/909/909d5ebb82ff8c1237b9abce6c9f2959.pdf>
- 46 The Sorry State of 5G SA Core Networks – Smart Communications in Phillipines. IEEE ComSoc. October 4, 2021. <https://techblog.comsoc.org/2021/10/04/the-sorry-state-of-5g-sa-core-networks-smart-communications-in-phillipines/>

- 47 Ericsson Mobility Report. November 2022. Ericsson. <https://www.ericsson.com/4ae28d/assets/local/reports-papers/mobility-report/documents/2022/ericsson-mobility-report-november-2022.pdf>
- 48 Там же.
- 49 Private-Mobile-Networks December-2022 Summary Report. GSA. <https://gsacom.com/paper/private-mobile-networks-december-2022-summary-report/>
- 50 Там же.
- 51 В оставшихся 2 % проектов частных сотовых сетей используется стандарт GSM-R.
- 52 Private LTE/5G nets to hit 13,500 in '26, 5G to lead from '24, 5G IoT devices to flow from '23. Enterprise IoT Insights. <https://enterpriseiotinsights.com/20220318/smart-factory/private-lte-5g-nets-to-hit-13500-in-26-5g-to-lead-from-24-5g-iot-devices-to-flow-from-23>
- 53 The state of the private wireless market 2022 for Industry 4.0. Nokia. May 2022. <https://pf.content.nokia.com/t007hb-what-is-private-wireless/blog-post-the-state-of-the-private-wireless-market-2022-for-industry-4-0?lb-mode=overlay>
- 54 Spend on private LTE/5G networks will be small but an important opportunity for future IoT growth. Analysys Mason. March 2021. https://www.analysismason.com/contentassets/468f088ce54b4e8fa4f766ce56b66bc3/analysys_mason_private_networks_5g_march2021_rdme0.pdf
- 55 Private LTE Will be a US\$16.3 Billion Opportunity by 2025 and the Foundation for 5G Services in End-Vertical Markets. ABI research. February 2019. <https://www.abiresearch.com/press/private-lte-will-be-us163-billion-opportunity-2025-and-foundation-5g-services-end-vertical-markets/>
- 56 Корпоративные сети Private LTE/5G-Ready в России: география и отраслевая принадлежность предприятий. ComNews. Май 2021 г. <https://www.comnews.ru/content/214409/2021-05-26/2021-w21/korporativnyye-seti-private-lte5g-ready-rossii-geografiya-i-otraslevaya-prinadlezhnost-predpriyatiy>
- 57 Аналитика компаний – участников российского рынка в распоряжении АНО «Цифровая экономика», данные актуальны на октябрь 2022 г.
- 58 Данные Ericsson Mobility Report 2021.
- 59 На основе данных Transorm Insight, IoTAnalytics, Ericsson Mobility Report 2021.
- 60 См. Ericsson Mobility Report 2022.
- 61 См. IoT Connections Forecast 2019-2030. Transforma Insights.
- 62 ARPU – Average Revenue per User, среднемесячная выручка на одного абонента услуг связи.

- 63 LTE ue-Category. 3Gpp. August 2016. <https://www.3gpp.org/keywords-acronyms/1612-ue-category>
- 64 См. подробные характеристики в Приложении № 1: Примеры и характеристики основных технологий беспроводной связи для IoT.
- 65 Здесь и далее: Evolution of LTE in Release 13. 3Gpp. February 2015. <https://www.3gpp.org/news-events/1628-rel13>
- 66 a) M.2083: IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond. International Telecommunication Union. September 2015. <https://www.itu.int/rec/R-REC-M.2083>
- b) Guidelines for evaluation of radio interface technologies for IMT-2020. ITU. November 2017. <https://www.itu.int/pub/R-REP-M.2412-2017>
- c) Minimum requirements related to technical performance for IMT-2020 radio interface(s). ITU. November 2017. <https://www.itu.int/pub/R-REP-M.2410-2017>
- 67 Mobile IoT. In the 5G future. NB-IoT and LTE-M in the context of 5G. GSMA. April 2018. <https://www.gsma.com/iot/wp-content/uploads/2018/05/GSMA-5G-Mobile-IoT.pdf>
- 68 IoT & Industry 4.0 in the 5G era Huawei's perspective. GSMA. June 2021. https://www.gsma.com/iot/wp-content/uploads/2021/07/Mobile-IoT-Summit-2-Huawei_IoT-and-Industry-4.0-in-the-5G-Era.pdf
- 69 Ericsson Mobility Report. Ericsson. November 2021. <https://www.ericsson.com/en/reports-and-papers/mobility-report>
- 70 Mobile IoT Network Launches. GSMA. <https://www.gsma.com/iot/mobile-iot-commercial-launches/>
- 71 5 things to know about the LPWAN market in 2021. IoT Analytics. October 2021. <https://iot-analytics.com/5-things-to-know-lpwan-market/>
- 72 Там же.
- 73 'No one is making money' – the China NB-IoT story is a cautionary tale, says Nordic. Enterprise IoT insights. October 2021. <https://enterpriseiotinsights.com/20211012/channels/news/no-one-is-making-money-the-china-nb-iot-story-is-a-cautionary-tale-says-nordic>
- 74 China Telecom claims over 100 million NB-IoT connections. Enterprise IoT insights. June 2021. <https://enterpriseiotinsights.com/20210601/nb-iot/china-telecom-claims-over-100-million-nb-iot-connections>
- 75 Chinese telcos deploy 961,000 5G sites, 700,000 NB-IoT base stations. RCR Wireless News. August 2021. <https://www.rcrwireless.com/20210805/5g/chinese-telcos-deploy-961000-5g-sites-700000-nb-iot-base-stations>
- 76 IoT & Industry 4.0 in the 5G era Huawei's perspective. GSMA. June 2021. https://www.gsma.com/iot/wp-content/uploads/2021/07/Mobile-IoT-Summit-2-Huawei_IoT-and-Industry-4.0-in-the-5G-Era.pdf

- 77 См.: 'No one is making money'. Enterprise IoT Insights.
- 78 «Большая четверка» улучшает сеть интернета вещей. ComNews. Ноябрь 2019 г. <https://www.comnews.ru/content/202905/2019-11-14/2019-w46/bolshaya-chetverka-uluchshaet-set-interneta-veschey>
- 79 «ВымпелКом» тестирует гибридную IoT-сеть. ComNews. 29 ноября 2018 г. <http://www.comnews.ru/content/116100/2018-11-29/vympelkom-testiruet-gibridnuyu-iot-set>
- 80 Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Приказ от 29 марта 2019 года № 113 «Об утверждении Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации», 2019. <https://digital.gov.ru/uploaded/files/113-tekstoviyj-variant.pdf>
- 81 3GPP SCEF Primer. Definition Networks. <http://www.definitionnetworks.com/3gpp-scef-primer/>
- 82 ГОСТ Р 59026-2020. Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе стандарта LTE в режиме NB-IoT. Основные параметры. Росстандарт. <https://protect.gost.ru/document.aspx?control=7&id=238809>
- 83 МТС и Microsoft подключили NB-IoT к глобальной платформе интернета вещей. МТС. Декабрь 2020. <https://moskva.mts.ru/about/media-centr/soobshheniya-kompanii/novosti-mts-v-rossii-i-mire/2020-12-17/mts-i-microsoft-podklyuchili-nb-iot-k-globalnoj-platforme-interneta-veshhej>
- 84 Исследование ПАО «МТС»: IoT Барометр 2021. ПАО «МТС». http://s22.q4cdn.com/722839827/files/doc_downloads/2021/07/MTS-2021-IoT-Barometer.pdf
- 85 Comparison of LPWAN Technologies: Cost Structure and Scalability. Wireless Personal Communications. November 2021. https://www.researchgate.net/publication/353069558_Comparison_of_LPWAN_Technologies_Cost_Structure_and_Scalability
- 86 Здесь и далее данные IoT Analytics, Transforma Insights, ABI Research.
- 87 LoRa – проприетарная технология модуляции сети передачи данных; LoRaWAN – сетевой протокол для беспроводной сети.
- 88 LoRa Alliance. <https://lora-alliance.org/>
- 89 Данные ABI Research.
- 90 a) Global LoRaWAN Market Ecosystem – Forecast to 2026. All the Research. October 2020. <https://www.alltheresearch.com/report/411/global-lorawan-market-ecosystem>
- b) LoRa and LoRaWAN Devices Market – Forecast (2022–2027). Industry ARC. <https://www.industryarc.com/Report/19424/lora-and-lorawan-devices-market.html>
- 91 LoRaWAN® Deployments Achieve Market Leadership; Deliver Strong ROI for IoT Across Wide Spectrum of Industries Across France and Spain. LoRa Alliance. <https://lora-alliance.org/lora-alliance-press-release/lorawan-deployments-achieve-market-leadership-deliver-strong-roi-for-iot-across-wide-spectrum-of-industries-across-france-and-spain-2/>

- 109 The Future of 5G and LoRaWAN®: Friends or Foes? Inside Out. Semtech's Corporate Blog. February 2021. <https://blog.semtech.com/the-future-of-5g-and-lorawan-friends-or-foes>
- 110 LoRa®: Delivering Internet of Things Capabilities Worldwide. Inside Out. Semtech's Corporate Blog. February 2022. <https://blog.semtech.com/lora-delivering-internet-of-things-capabilities-worldwide>
- 111 Информационные технологии. Интернет вещей. Спецификация LoRaWAN RU. Предварительный национальный стандарт Российской Федерации. Июль 2021 г. <https://docs.cntd.ru/document/1200177821>
- 112 В России используется 1 миллион устройств с радиомодулями LoRa. Ассоциация интернета вещей. 15.10.2020. https://iotas.ru/media/news_aiv/1167/
- 113 Orange работает с упором на инновационные услуги. ComNews. Апрель 2021 г. <https://www.comnews.ru/content/214360/2021-04-29/2021-w17/orange-rabotaet-uporom-innovacionnye-uslugi>
- 114 Sigfox покорит Россию. ComNews. Май 2020 г. <https://www.comnews.ru/content/207190/2020-05-20/2020-w21/sigfox-pokorit-rossiyu>
- 115 XNB – энергоэффективный LPWAN-протокол дальнего радиуса действия. Стриж. <https://strij.tech/protokol-xnb>
- 116 Круглый стол от iot.ru «IoT-рынок: текущая обстановка, новые вызовы, поиск перспектив». IoT.ru. Апрель 2022 г. <https://www.youtube.com/watch?v=domzU9t2aLk>
- 117 IoT-платформа WAVIoT. WAVIoT. <https://waviot.ru/technology/waviot-iot-platform/>
- 118 Беспроводной сбор показаний энергоресурсов на технологии NB-Fi. M-Сервис. <https://waviot.ru/news/opening-a-new-production-facility--detail/>
- 119 Разработанный в Сколтехе протокол OpenUNB будет реализован на оборудовании GoodWAN. SkolTech NTI CoE. 24.08.2020. <https://iot.skoltech.ru/2020/08/24/razrobotannyj-v-skoltehe-protokol-openunb-budet-realizovan-na-obrudovanii-goodwan/>
- 120 OCS предлагает ИТ-каналу решения GoodWAN. OCS Distribution. 22 декабря 2021 г. <https://ocs.ru/presscenter/pressreleases/ocs-predlagaet-it-kanalu-resheniya-goodwan/>
- 121 Данные Ericsson Mobility Report November 2021 и Transforma Insights. Также см.: Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by communications technology (in millions). Statista. <https://www.statista.com/statistics/1194688/iot-connected-devices-communications-technology/>
- 122 Global Economic Value of Wi-Fi. Wi-Fi Alliance. September 2021. https://www.wi-fi.org/download.php?file=/sites/default/files/private/Global_Economic_Value_of_Wi-Fi_2021-2025_202109.pdf
- 123 2022 Wi-Fi® trends. Wi-Fi Alliance. <https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-2022-wi-fi-trends>

- 124 What is Wi-Fi 6E? Juniper Networks. <https://www.juniper.net/us/en/research-topics/what-is-wi-fi-6e.html#:~:text=Wi%2DFi%206E%20networks%20will,capacity%20to%20handle%20more%20devices>.
- 125 Wi-Fi 6 in the Industry. Siemens. 2020. <https://assets.new.siemens.com/siemens/assets/api/uuid:7066e6d0-6ba8-487a-b78d-f8c6e6bec8a0/whitepaper-wlan-11ax-2020-en.pdf>
- 126 Wi-Fi 6/6E Solutions. Cisco. <https://www.cisco.com/c/en/us/solutions/enterprise-networks/802-11ax-solution/index.html>
- 127 Wi-Fi is getting its biggest upgrade in 20 years. 6GHz Wi-Fi is coming soon. The Verge. 2021. <https://www.theverge.com/2020/4/23/21231623/6ghz-wifi-6e-explained-speed-availability-fcc-approval>
- 128 Wi-Fi HaLow: Designed for the Internet of Things. IoT Times. March 2022. <https://iot.eetimes.com/wi-fi-halow-designed-for-the-internet-of-things/>
- 129 2022 Market Update. Bluetooth. https://www.bluetooth.com/2022-market-update/?utm_source=internal&utm_medium=blog&utm_campaign=bmu&utm_content=new-trends-and-forecasts-for-the-next-5-years
- 130 Там же.
- 131 Bluetooth Low Energy (BLE) based wireless sensors. IEEE Xplore. <https://ieeexplore.ieee.org/document/6411303>
- 132 Bluetooth IoT Applications: From BLE to Mesh. IoT for all. June 2020. <https://www.iotforall.com/bluetooth-iot-applications>
- 133 How Bluetooth Mesh Puts the 'Large' in Large-Scale Wireless Device Networks. Bluetooth. June 2018. https://www.bluetooth.com/blog/mesh-in-large-scale-networks/?utm_campaign=mesh&utm_source=internal&utm_medium=blog&utm_content=introducing-bluetooth-mesh-networking
- 134 SberDevices – теперь в альянсе CSA для разработки единого стандарта систем умного дома. 7 февраля 2022 г. Habr. <https://habr.com/ru/company/sberbank/news/t/650201/>
- 135 Analysts Confirm Half a Billion Zigbee Chipsets Sold, Igniting IoT Innovation; Figures to Reach 3.8 Billion by 2023. CSA Alliance. August 7, 2018. <https://csa-iot.org/newsroom/analysts-confirm-half-a-billion-zigbee-chipsets-sold-igniting-iot-innovation-figures-to-reach-3-8-billion-by-2023/>
- 136 1 Billion 802.15.4 Chipset Shipments by 2024. ON World. <https://onworld.com/news/1-Billion-802.15.4-Chipset-Shipments-by-2024.html>
- 137 Данные CSA Alliance.
- 138 Project Connected Home over IP. Google Developers. December 2019. <https://developers.googleblog.com/2019/12/project-connected-home-over-ip.html>
- 139 Matter. The Foundation for Connected Things. Connectivity Standards Alliance. <https://csa-iot.org/all-solutions/matter/>

- 140 Matter's interoperable smart home standard has been delayed to 2022. The Verge. August 2021. <https://www.theverge.com/2021/8/13/22623275/matter-interoperable-smart-home-standard-delay-2022-project-chip-csa>
- 141 Building the Foundation and Future of the IoT. Connectivity Standards Alliance. <https://csa-iot.org/>
- 142 2022 state of the ecosystem report. Z Wave Alliance. <https://z-wavealliance.org/wp-content/uploads/2022/01/FINAL-2022-Z-Wave-State-of-the-Ecosystem-Report.pdf>
- 143 Z-Wave Products Market – Forecast (2022–2027). ARC Industry. <https://www.industryarc.com/Report/15830/z-wave-products-market.html>
- 144 FCC modernizes the 5.9GHz band; Wi-Fi and C-V2X. 19 November 2020. Green Car Congress. <https://www.greencarcongress.com/2020/11/20201119-fcc.html>
- 145 Of Hamburgers . . . and RAIN RFID IC Tags. RAIN Alliance. April 2022. <https://rainfid.org/blog/of-hamburgers-and-rain-rfid-ic-tags/>
- 146 RFID Forecasts, Players and Opportunities 2022-2032. The complete analysis of the global RFID industry. IDTechEx. <https://www.idtechex.com/en/research-report/rfid-forecasts-players-and-opportunities-2022-2032/849>
- 147 RAIN RFID. Market research report. RAIN Alliance. <https://rainfid.org/rain-rfid-market-research-report/>
- 148 См. RFID Forecasts, Players and Opportunities 2022-2032. IDTechEx.
- 149 IoT Sensors & aRFID Infrastructure. SAVI. <https://www.savi.com/products/iot-sensors-rfid-tags/>
- 150 a) The Satellite IoT Communications Market. 1st edition. Berg Insight. October 2021. <https://www.berginsight.com/the-satellite-iot-communications-market>
- b) Satellite IoT market to reach \$5.9bn by 2025. Specifier. July 2019. <https://www.electronicsspecifier.com/products/communications/satellite-iot-market-to-reach-5-9bn-by-2025>
- 151 ORBCOMM and Inmarsat to provide Next-generation, global IOT service. Inmarsat. October 2020. <https://www.inmarsat.com/en/news/latest-news/enterprise/2020/orbcomm-and-inmarsat-to-provide--next-generation--global-iot-ser.html>
- 152 Данные BergInsight.
- 153 Там же.
- 154 Там же.
- 155 Рынок спутникового интернета вещей в перспективе до 2024–2030 гг. Json.TV. https://json.tv/en/ict_telecom_analytics_view/satellite-iotm2m-market-until-2024-2030
- 156 The Satellite IoT Communications Market. 1st edition. Berg Insight. October 2021. <https://www.berginsight.com/the-satellite-iot-communications-market>

- 157 Founding years of companies active in nanosats since 1990. Nanosats. https://www.nanosats.eu/img/fig/Nanosats_companies_founded_black_2022-01-01_large.png
- 158 Nanosats Database. Facts as of 2022 January 1. <https://www.nanosats.eu/>
- 159 АО «ГЛОНАСС» займется интернетом вещей. Ведомости. Февраль 2021 г. <https://www.vedomosti.ru/technology/articles/2021/02/16/858209-ao-glonass>
- 160 Космический подход к интернету вещей. ComNews. 25.06.2019. https://www.com-news.ru/content/120404/2019-06-25/kosmicheskij-podhod-k-internetu-veshchey?utm_source=yxnews&utm_medium=desktop
- 161 С космодрома Байконур стартовала ракета «Союз-2.1а» с 38 спутниками. Российская Газета. 22.03.2021. <https://rg.ru/2021/03/22/s-kosmodroma-bajkonur-startovala-raketa-soiuz-21a-s-38-sputnikami.html>
- 162 ОРБИКРАФТ-ЗОРКИЙ. Запущенные миссии. ООО «Спутникс». <https://sputnix.ru/ru/sputniki/na-orbite/cubesat-6u>
- 163 «Спутникс» рассказал о возможностях спутникового интернета вещей и трендах применения наноспутников. ООО «Спутникс». 16.02.2022. <https://sputnix.ru/ru/o-nas/novosti/sputniks-rasskazal-o-vozmozhnostyax-sputnikovogo-interneta-veshej-i-trendax-primeneniya-nanosputnikov>
- 164 Реализация проектов «Марафон IoT» и «Скиф». Роскосмос. 14.01.2022. <https://www.roscosmos.ru/33835/>
- 165 Проекты спутниковых группировок «Марафон IoT» и «Скиф» получили госфинансирование. RSpectr.com. 17.01.2022. <https://rspectr.com/novosti/proekty-sputnikovyh-gruppirovok-marafon-iot-i-skif-poluchili-gosfinansirovanie>
- 166 Многоспутниковая система передачи данных «Марафон IoT»: сервисы спутникового интернета вещей и их конкурентоспособность. Круглый стол «Место спутниковых технологий на рынке интернета вещей». 02.11.2020. <https://ka-band.info/resources/RTable-IoT-2-nov-2020/Anpilogov-2020.pdf>
- 167 Там же.
- 168 SWD (2015) 100 final. Communication from The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. A Digital Single Market Strategy for Europe. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192&from=EN>
- 169 SWD (2016) 110 final. Commission staff working document. Advancing the Internet of Things in Europe. European Commission. Brussels, 19.04.2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0110&from=EN#footnote75>
- 170 Там же.
- 171 State aid: Commission approves plan by France, Germany, Italy and the UK to give €1.75 billion public support to joint research and innovation project in microelectronics. Press release. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6862

- 172 Horizon 2020. European Commission. https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en
- 173 The European Large-Scale Pilots Programme Driving IoT Innovation at Scale in Europe. Create-IoT. https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf
- 174 IoT European Large-Scale Pilots – Integration, Experimentation and Testing. River Publishers. https://www.riverpublishers.com/pdf/ebook/chapter/RP_9788793609105C8.pdf
- 175 The next generation Internet of Things. European Commission. <https://digital-strategy.ec.europa.eu/en/policies/next-generation-internet-things>
- 176 Cluster 4: Digital, Industry and Space. Policy, strategy, how to apply and work programmes. Horizon Europe. https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-4-digital-industry-and-space_en
- 177 EU perspective IoT and EDGE computing for the green digital transition. European Commission. https://oascities.org/wp-content/uploads/2022/02/Svet-Mihaylov_CxC22_IoT-and-Edge-Computing-in-the-green-digital-transformation.pdf
- 178 Там же.
- 179 Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision). EUR-Lex. April 2002. <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1410442813386&uri=CELEX:32002D0676>
- 180 The Commission harmonises radio spectrum in support of the Internet of Things. European Commission. October 2018. <https://digital-strategy.ec.europa.eu/en/news/commission-harmonises-radio-spectrum-support-internet-things>
- 181 Commission Implementing Decision (EU) 2020/1426 of 7 October 2020 on the harmonised use of radio spectrum in the 5875–5935 MHz frequency band for safety-related applications of intelligent transport systems (ITS) and repealing Decision 2008/671/EC (notified under document C(2020) 6773) (Text with EEA relevance). EUR-Lex. October 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020D1426>
- 182 6GHz harmonisation decision: more spectrum available for better and faster Wi-Fi. European Commission. June 2021. <https://digital-strategy.ec.europa.eu/en/library/6ghz-harmonisation-decision-more-spectrum-available-better-and-faster-wi-fi>
- 183 Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. A European strategy for data. European Commission. February 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066>
- 184 a) Data Act. European Commission. <https://digital-strategy.ec.europa.eu/en/policies/data-act>
- b) Data Act. European Commission. February 2022. <https://ec.europa.eu/newsroom/dae/redirection/document/83517>

- 185 European data strategy. European Commission. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en#documents
- 186 Там же.
- 187 Realising the economic potential of machine-generated, non-personal data in the EU. Deloitte. July 2018. https://www.vodafone.com/content/dam/vodacom/files/public-policy/Realising_the_potential_of_loT_data_report_for_Vodafone.pdf
- 188 A new IoT regulatory framework for Europe. Vodafone. June 2019. <https://investors.vodafone.com/sites/vodafone-ir/files/vodafone/our-purpose/social-contract/policy-papers/a-new-iot-regulatory-framework-for-europe.pdf>
- 189 Там же.
- 190 Made in China 2025 《中国制造 2025》 State Council, July 7, 2015. <http://www.citta-dellascienza.it/cina/wp-content/uploads/2017/02/loT-ONE-Made-in-China-2025.pdf>
- 191 Made in China 2025: Global Ambitions built on local protections. US Chamber of Commerce. https://www.uschamber.com/assets/archived/images/final_made_in_china_2025_report_full.pdf
- 192 China's Internet of Things. SOSi. October 2018. https://www.uscc.gov/sites/default/files/Research/SOSi_China%27s%20Internet%20of%20Things.pdf
- 193 关于印发《工业互联网创新发展行动计划（2021-2023年）》的通知 工信部信管〔2020〕197号. 2020年12月22日. http://www.gov.cn/zhengce/zhengceku/2021-01/13/content_5579519.htm
- 194 工信部等八部门印发《物联网新型基础设施建设三年行动计划（2021-2023年）》. 2021年09月29日. http://www.cac.gov.cn/2021-09/29/c_1634507925423247.htm
- 195 См. China's Internet of Things. SOSi. October 2018.
- 196 Там же.
- 197 国家工信部:中国物联网产业规模达7500亿 互联网巨头成重要力量. Sohu. October 2016. https://www.sohu.com/a/117605461_119778
- 198 财政部 工业和信息化部关于印发《物联网发展专项资金管理暂行办法》的通知. April 2011. http://www.gov.cn/gongbao/content/2011/content_2004726.htm
- 199 重磅|中国互联网投资基金成立·总规模1000亿元人民币·首期300亿已到位. PEdaily. <https://pe.pedaily.cn/201701/20170122408334.shtml>
- 200 安徽省物联网发展专项资金. http://wotaochina.com/info.asp?second_id=3014
- 201 上海物联网创业投资基金. <http://www.simicholdings.com/venture/ventureInvestment/6cb50e88fd9b44aeab7a82905a74048d>
- 202 См. China's Internet of Things. SOSi. October 2018.
- 203 中共无锡市委 无锡市人民政府关于无锡国家传感网创新示范区建设（2017-2020年）实施意见. March 2017.

<https://www.wuxi.gov.cn/uploadfiles/201704/01/2017040113263886795157.doc>

204 私募机构布局物联网赛道渐趋理性早期投资比重下降中后期投资占比提升. Financial News. February 2022. https://www.financialnews.com.cn/zq/pevc/202202/t20220217_239547.html

205 Там же.

206 2022 China's IoT Industry Report. iResearch. February 2022. https://www.iresearch-china.com/content/details8_69333.html

207 GSMA Calls on Governments to License 6 GHz to Power 5G. GSMA. 17 May, 2021. <https://www.gsma.com/newsroom/press-release/gsma-calls-on-governments-to-license-6-ghz-to-power-5g/>

208 中华人民共和国数据安全法. June 2016. <http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml>

209 中华人民共和国个人信息保护法. August 2021. <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>

210 2022年1-2月份通信业经济运行情况. March 2022. https://wap.miit.gov.cn/gxsj/tjfx/txy/art/2022/art_4f29bc2367764f2788737ee2e7d864c7.html

211 The Mobile Economy. China 2021. GSMA. 2021. https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/02/GSMA_MobileEconomy2021_China_Eng-1.pdf

212 2021下半年全球物联网支出指南发布·中国物联网市场规模有望在2025年超3,000亿美元. IDC. December 2021. <https://www.idc.com/getdoc.jsp?containerId=prCHC48454321>

213 Administration of Barack H. Obama. Executive Order 13514—Federal Leadership in Environmental, Energy, and Economic Performance. October 2009. <https://www.govinfo.gov/content/pkg/DCPD-200900783/pdf/DCPD-200900783.pdf>

214 The US government is pouring money into the Internet of Things. Insider. May 2016. <https://www.businessinsider.com/the-us-government-is-pouring-money-into-the-internet-of-things-2016-5>

215 Там же.

216 ERN15061 Resolution. 114th Congress 1st Session. United States Senate. https://www.fischer.senate.gov/public/_cache/files/2b3ad47d-f4df-4cb8-b6e3-877de18be0a8/ern15061.pdf

217 An Act to ensure appropriate spectrum planning and interagency coordination to support the Internet of Things. GPO. August 2017. <https://www.congress.gov/115/bills/s88/BILLS-115s88rfh.pdf>

218 IoT gets a big boost as DIGIT Act passed US Senate. Gigi Onag, Future IoT Tech. January 16, 2020. <https://futureiot.tech/iot-gets-a-big-boost-as-digit-act-passed-us-senate/>

219 Unlicensed Use of the 6 GHz Band Report and Order and Further Notice of Proposed Rulemaking ET Docket No. 18-295; GN Docket No. 17-183. Federal Register. The

Daily Journal of the United States Government. <https://www.federalregister.gov/documents/2020/05/28/2020-11320/unlicensed-use-of-the-6-ghz-band>

220 S.1395 – Advancing IoT for Precision Agriculture Act of 2021. 117th Congress. April 2021. <https://www.congress.gov/bill/117th-congress/senate-bill/1395>

221 NITRD Program Budget Reporting. NITRD. <https://www.nitrd.gov/apps/itdashboard>

222 The Networking & Information Technology R&D Program and the National Artificial Intelligence Initiative Office Supplement to The President's FY2022 Budget. NITRD. 2021. <https://www.nitrd.gov/pubs/FY2022-NITRD-NAIIO-Supplement.pdf>

223 NITRD R&D Budgets: Fiscal Years 1992–2022. NITRD. <https://www.nitrd.gov/apps/itdashboard/dashboard/#NITRD-RD-Budgets-Fiscal-Years-19922022>

224 IoT Cybersecurity Improvement Act of 2020. US Congress HR1668. <https://trackbill.com/bill/us-congress-house-bill-1668-iot-cybersecurity-improvement-act-of-2020/1723165/>

225 New IoT Cybersecurity Improvement Act: Creating a Floor For IoT Security? Evan Schuman, IoT world Today. <https://www.iotworldtoday.com/2021/02/02/new-iot-cybersecurity-improvement-act-creating-a-floor-for-iot-security/>

226 SP 800-213. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. NIST. November 2021. <https://csrc.nist.gov/publications/detail/sp/800-213/final>

227 Australia's Digital Economy. <https://digitaleconomy.pmc.gov.au/>

228 Там же.

229 Reforms to meet Australia's future infrastructure needs. Australian Government. August 2021. https://www.infrastructureaustralia.gov.au/sites/default/files/2021-09/2021%20Master%20Plan_1.pdf

230 a) Smart Cities and Suburbs. Australian Government. <https://www.infrastructure.gov.au/territories-regions-cities/cities/smart-cities-and-suburbs>

b) Industry 4.0 Testlabs in Australia. Australian Government. August 2017. <https://www.industry.gov.au/data-and-publications/industry-40-testlabs-in-australia>

231 Australian government to invest A\$10m in IoT. Computer Weekly. August 2017. <https://www.computerweekly.com/news/450424747/Australian-government-to-invest-A10m-in-IoT>

232 Australian Government investment in Landcare. Australian Government. <https://www.awe.gov.au/agriculture-land/farm-food-drought/natural-resources/landcare/national-landcare-program/australian-government-investment-in-landcare>

233 4.0 Testlabs in Australia. Australian Government. August 2017. <https://www.industry.gov.au/data-and-publications/industry-40-testlabs-in-australia>

- 234 a) NSW Government: \$45M Smart Places Boost. Outcomex. <https://www.outcomex.com.au/news/nsw-government-45m-smart-places-boost/>;
- b) Smart Places Strategy. NSW Government. <https://www.dpie.nsw.gov.au/our-work/strategy-and-innovation/smart-places/smart-places-strategy>
- 235 Victorian government to monitor bridges using IoT sensors. IoT HUB. May 2021. <https://www.iothub.com.au/news/victorian-government-to-monitor-bridges-using-iot-sensors-565213>
- 236 Voluntary Code of Practice. Securing the Internet of Things for Consumers. Australian Government. <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice>
- 237 ACMA proposes IoT spectrum access changes. ZD Net. December 2015. <https://www.zdnet.com/home-and-office/networking/acma-proposes-iot-spectrum-access-changes/>
- 238 ACMA proposes new radio licence, suggests IoT use. IoT HUB. June 2019. <https://www.iothub.com.au/news/acma-proposes-new-radio-licence-suggests-iot-use-527377>
- 239 The Internet of Things. Horizon Scanning Series. ACOLA. November 2020. <https://acola.org/hs5-internet-of-things-australia/>
- 240 Dialogues. European Union. Brazil. <https://eubrdialogues.com/project.php/development-of-the-m2miot-ecosystem-and-eu-brazil-mapping-and-comparative-study?url=development-of-the-m2miot-ecosystem-and-eu-razil-mapping-and-comparative-study>
- 241 MCTIC representatives learn about IoT application systems during a mission to Europe. Dialogues. European Union. Brazil. July 2016. <https://www.eubrdialogues.com/news/mctic-representatives-learn-about-iot-application-systems-during-a-mission-to-europe>
- 242 Brazil's Internet of Things. Pesquisa. September 2017. <https://revistapesquisa.fapesp.br/en/brazils-internet-of-things/>
- 243 Internet of Things An Action Plan for Brazil.
- Fundação Alexandre de Gusmão – FUNAG. November 2017. http://www.funag.gov.br/images/2017/Novembro/Dialogos/Claudio_Leal-Internet-of-Things.pdf
- 244 Там же.
- 245 Presidência da República Secretaria-Geral Subchefia para Assuntos Jurídicos. June 2019. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9854.htm
- 246 Introducing Brazil's National IoT Plan: IoT As Value-Added Infrastructure. Access Partnership. 1 July 2019. <https://www.accesspartnership.com/introducing-the-brazilian-national-iot-plan-iot-as-added-value-infrastructure/>
- 247 См. Presidência da República Secretaria-Geral Subchefia para Assuntos Jurídicos. June 2019.

- 248 a) Introducing Brazil's National IoT Plan: IoT As Value-Added Infrastructure. Access Partnership. June 2019. <https://www.in.gov.br/en/web/dou/-/lei-n-14.108-de-16-de-dezembro-de-2020-294616158>
- b) New Brazilian Law to promote the Internet of Things. Inlea. January 2021. <https://inlea.com/new-brazilian-iot-law/>
- 249 Telecoms Series. IoT – Recent Developments. Azevedo Sette. 04 January 2021. <https://www.azevedosette.com.br/news/en/telecoms-series-iot-recent-developments/6066#:~:text=In%20Brazil%2C%20Decree%20No.,security%20and%20personal%20data%20protection>
- 250 a) Indicator Capital, BNDES and Qualcomm Ventures launch the first fund in Latin America with a focus on Internet of Things (IoT). Indicator Capital. May 2021. <https://indicatorcapital.com/news/2021/5/21/baybrazil-indicator-capital-bndes-and-qualcomm-ventures-launch-the-first-fund-in-latin-america-with-a-focus-on-internet-of-things-iot> ;
- b) The plans of LatAm's largest venture capital fund for IoT investments. BNAmericas. February 2022. <https://www.bnamericas.com/en/interviews/the-plans-of-latams-largest-venture-capital-fund-for-iot-investments>
- 251 Brazilian government launches first IoT research center. ZD Net. July 2021. <https://www.zdnet.com/article/brazilian-government-launches-first-iot-research-center/#:~:text=Brazil's%20National%20IoT%20Plan%20was,national%20innovation%20ecosystem%20and%20development>
- 252 McKinsey's IoT strategy plan could boost Brazilian economy by \$200 billion. Consultancy.lat. June 2018. <https://www.consultancy.lat/news/400/mckinseys-iot-strategy-plan-could-boost-brazilian-economy-by-200-billion>
- 253 Manufacturing a clean green recovery. High Value Manufacturing Catapult. <https://hvm.catapult.org.uk/>
- 254 National AI Strategy. UK Government. September 2021. <https://www.gov.uk/government/publications/national-ai-strategy>
- 255 Next Generation Mobile Technologies: A 5G strategy for the UK. UK Government. March 2017. <https://www.gov.uk/government/publications/next-generation-mobile-technologies-a-5g-strategy-for-the-uk>
- 256 PM at CeBIT: UK and Germany can lead technological revolution. Gov.UK. <https://www.gov.uk/government/news/pm-at-cebit-uk-and-germany-can-lead-technological-revolution>
- 257 IoTUK. The world's leading national IoT programme. Idris Jahn, Lead for Health, Funding and International Digital Catapult. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/666943/DC-IoTUK_for_distribution.pdf
- 258 Evaluation Scoping Study for the IoT UK Research and Innovation Programme (2015-2018). Gov.UK. <https://www.gov.uk/government/publications/evaluation-scoping-study-for-the-iot-uk-research-and-innovation-programme2015-2018>

- 259 Ofcom publishes plan to support UK internet of things. Computer Weekly. January 2015. <https://www.computerweekly.com/news/2240239030/Ofcom-publishes-plan-to-support-UK-internet-of-things>
- 260 UK to release 6 GHz and 100 GHz spectrum for Wi-Fi in smart homes, offices, factories. Enterprise IoT Insights. January 2020. <https://enterpriseiotinsights.com/20200127/channels/news/uk-release-of-6-ghz-and-1000ghz-spectrum-for-wi-fi-in-homes-offices-factories>
- 261 Supporting the UK's wireless future. Our spectrum management strategy for the 2020s. Ofcom. July 2021. https://www.ofcom.org.uk/___data/assets/pdf_file/0017/222173/spectrum-strategy-statement.pdf
- 262 Improve cyber security in the Internet of Things: apply for funds. Gov.UK. 4 February 2019. <https://www.gov.uk/government/news/improve-cyber-security-in-the-internet-of-things-apply-for-funds>
- 263 UK Gov launches IoT cybersecurity fund. Telecoms.com. 29 May 2020. <https://telecoms.com/504652/uk-gov-launches-iot-cybersecurity-fund/>
- 264 PETRAS awards £3.6 M to tackle issues of cybersecurity, privacy and trust at the edge. PETRAS. <https://petras-iot.org/update/petras-awards-3-6-m-to-tackle-issues-of-cybersecurity-privacy-and-trust/>
- 265 Code of Practice for Consumer IoT Security. UK Government. October 2018. <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security>
- 266 Product Security and Telecommunications Infrastructure (PSTI) Bill: Factsheets. UK Government. November 2021. <https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets>
- 267 Там же.
- 268 Master Plan for Building the Internet of Things (IoT) that leads the hyper-connected, digital revolution. Government of South Korea. <https://www.rfid-alliance.com/KOREA-IoT%20Master%20Plan.pdf>
- 269 Там же.
- 270 Там же.
- 271 IoT Innovation and Deployment: A Blueprint for U.S. and Korean Leadership Written by Dr. Gwanhoo Lee, American University Kogod School of Business. https://www.uschamber.com/assets/archived/images/final_accelerating_iiot_growth_and_deployment_uskbc.pdf
- 272 South Korea to invest \$350 million in IoT smart device makers. ZDNet. Philip Iglauder, ZDNet. <https://www.zdnet.com/article/south-korea-to-invest-350-million-in-iiot-smart-device-makers/>
- 273 South Korea – Country Commercial Guide. International Trade Administration. August 2021. <https://www.trade.gov/country-commercial-guides/south-korea-manufacturing-technology-smart-factory>

- 274 Korea – Mfg Tech – Smart Factory. Privacy Shield Framework. <https://www.privacyshield.gov/article?id=Korea-Manufacturing-Technology-Smart-Factory>
- 275 Korea Smart Factory Initiative Colloquium on Digital Industrial Policy Programme. Korea Institute for Industrial Economics & Trade. November 2018. https://static1.squarespace.com/static/52246331e4b0a46e5f1b8ce5/t/5bf25bdc758d46dbf17f821b/1542609889778/Dr+Yu_Korea+Smart+Factory+Initiative.pdf
- 276 Там же.
- 277 Там же.
- 278 South Korea – Country Commercial Guide. Manufacturing Technology – Smart Factory. International Trade Administration. August 2021. <https://www.trade.gov/country-commercial-guides/south-korea-manufacturing-technology-smart-factory>
- 279 Korean govt to spend \$414.4 mn to back smart factory expansion in 2020. Pulse. January 2020. <https://pulsenews.co.kr/view.php?year=2020&no=101075>
- 280 Там же.
- 281 Digital New Deal Harness the Winds of Change, Bringing Innovation! Ministry of Science and ICT. <https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mld=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=527&searchOpt=ALL&searchTxt=>
- 282 South Korea Invests \$2.2bn In Hyperconnectivity Plan. XRToday. <https://www.xrtoday.com/mixed-reality/south-korea-invests-2-2bn-in-hyperconnectivity-plan/>
- 283 South Korea Ushers in New Era of Wi-Fi. Business Korea. October 2020. <http://www.businesskorea.co.kr/news/articleView.html?idxno=53292>
- 284 Решения. Государственная комиссия по радиочастотам (ГКРЧ). https://grfc.ru/upload/medialibrary/f2f/protokol_18_48_ver._1_1016408481115.pdf
- 285 Перевод интернета вещей на российское «железо» перенесли на год. На страну есть всего 2 производителя. Snews. Январь 2021 г. https://www.cnews.ru/news/top/2021-01-12_perevod_interneta_veshchej
- 286 IoT нужно больше ТОРП. Comnews. Март 2022 г. <https://www.comnews.ru/content/219368/2022-03-22/2022-w12/iot-nuzhno-bolshe-torp>
- 287 Базовая станция NB-Fi. Реестр РЭП. <https://gisp.gov.ru/pprf/marketplace/#/product/619d22cb-2318-4ef8-983b-a6894e33953c>
- 288 Оборудование для разворачивания сетей LoRaWAN: базовая станция Вега БС-2.2. Реестр РЭП. <https://gisp.gov.ru/pprf/marketplace/#/product/49d0ca0a-222d-4b82-93dc-d02b4adf4fd8>
- 289 Базовая станция «Звезда» версии 4-LP. Реестр РЭП. <https://gisp.gov.ru/pprf/marketplace/#/product/3bc8b044-e3c7-4866-b793-50f8daea034f>
- 290 IoT нужно больше ТОРП. Comnews. Март 2022 г. <https://www.comnews.ru/content/219368/2022-03-22/2022-w12/iot-nuzhno-bolshe-torp>

- 291 Дмитрий Чернышенко провел заседание Общественного экспертного совета по использованию электроники в отраслях экономики. Правительство РФ. 30 июня 2021 г. <http://government.ru/news/42644/>
- 292 Постановление Правительства Российской Федерации от 30 октября 2021 г. № 1867 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам предоставления субсидий российским организациям радиоэлектронной промышленности». Гарант. <https://base.garant.ru/403004888/>
- 293 ТК 194. Кибер-физические системы. Цели технического комитета. <http://tc194.ru/>
- 294 Перспективный план стандартизации в области передовых производственных технологий на 2018–2025 годы. <https://nti2035.ru/upload/iblock/41c/41cb2bc-4c3bad4a7b6a2d99486abfdad.pdf>
- 295 Распоряжение от 28 июля 2017 г. № 1632-р. Правительство РФ. Июль 2017 г. <http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf>
- 296 План мероприятий («дорожная карта») «Энерджинет» Национальной технологической инициативы. https://nti2035.ru/markets/docs/DK_energynet.pdf
- 297 ISO/IEC 30162:2022. Internet of Things (IoT) – Compatibility requirements and model for devices within industrial IoT systems. International Standardization Organisation. <https://www.iso.org/standard/53282.html?browse=tc>
- 298 О стандартизации цифровых технологий Никита Уткин, Председатель ТК 194 «Кибер-физические системы». РусКрипто 2020. https://www.ruscrypto.ru/resource/archive/rc2020/files/06_utkin.pdf
- 299 Домам прививают единомыслие. Коммерсантъ. 20.01.2022. <https://www.kommer-sant.ru/doc/5172933>
- 300 В России появится «Национальный консорциум промышленного интернета». DRussia.ru. Август 2015 г. <https://d-russia.ru/v-rossii-poyavitsya-nacionalnyj-konsorci-um-promyshlennogo-interneta.html>
- 301 В России создана Национальная ассоциация участников рынка промышленного интернета (НАПИ). Ростелеком. Июль 2016 г. https://www.company.rt.ru/projects/digital_economy_rf/IIoT/news/d436327/
- 302 Российские разработчики в области промышленной автоматизации создали Ассоциацию развития систем индустриального интернета. InfoWatch. Май 2017 г. <https://www.infowatch.ru/company/presscenter/news/17911>
- 303 Промышленность, обработка промышленных данных и IIoT. Skoltech NTI CoE. <https://iiot.skoltech.ru/consortium-industry-partners-iiot/>
- 304 Об Ассоциации интернета вещей. IoTas. <https://iotas.ru/about/>
- 305 Члены Ассоциации интернета вещей. IoTas. <https://iotas.ru/members/>

306 Приказ ФСТЭК России № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах (2014 г.); Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов критической инфраструктуры Российской Федерации (в редакции Приказа ФСТЭК России от 26 марта 2019 г. № 60)»; Руководящий документ «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007); Руководящий документ «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007); Руководящий документ «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007); Руководящий документ «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007); Методические рекомендации по организации контроля состояния обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации (утв. ФСТЭК России 18.11.2008 246-дсп) и др.

307 ФЗ № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». <https://rg.ru/2017/07/31/bezopasnost-dok.html>

308 Федеральный закон от 21.07.11 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса». <https://rg.ru/2011/07/26/tek-dok.html>

309 Методика оценки угроз безопасности информации. Федеральная служба по техническому и экспортному контролю. Февраль 2021 г. <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhdn-fstek-rossii-5-fevralya-2021-g>

310 Информационное сообщение «Об утверждении методики выявления уязвимостей и недеklarированных возможностей в программном обеспечении» от 10 февраля 2021 г. № 240/24/647. Федеральная служба по техническому и экспортному контролю. Февраль 2021 г. <https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/2171-informatsionnoe-soobshchenie-fstek-rossii-ot-10-fevralya-2021-g-n-240-24-647>

311 Паспорт национальной программы «Цифровая экономика Российской Федерации» от 04.06.2019. Аналитический центр при Правительстве Российской Федерации. https://digital.ac.gov.ru/upload/iblock/219/NP_Cifrovaya_ekonomika.docx

312 Паспорт федерального проекта «Информационная инфраструктура» национальной программы «Цифровая экономика Российской Федерации» от 26.12.2019. Аналитический центр при Правительстве Российской Федерации. https://digital.ac.gov.ru/upload/iblock/89d/FP_Informacionnaya_infrastruktura_26_12_2019.docx

313 Приказ от 29 марта 2019 года № 113 «Об утверждении Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации». Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Март 2019 г. <https://docs.cntd.ru/document/554066760>

- 314 Распоряжение об утверждении Концепции и технических требований покрытия транспортной инфраструктуры сетями связи для систем передачи данных, включая координатно-временную информацию ГЛОНАСС, дифференциальных поправок, автоматического зависимого наблюдения и многопозиционных систем наблюдения, в том числе предложения по источникам финансирования. Министерство транспорта РФ. Октябрь 2019 г. <https://digital.ac.gov.ru/upload/iblock/e5d/%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D1%8F%20%D0%9C%D0%B8%D0%BD%D1%82%D1%80%D0%B0%D0%BD%D1%81%D0%B0%2031%2010%202019%20%D0%90%D0%A1-152-%D0%A0.pdf>
- 315 Работы по обеспечению покрытия первоочередных объектов транспортной инфраструктуры. Защита Инфо Транс. <https://www.z-it.ru/projects/kontseptsiya-pokrytiya-transportnoy-infrastruktury-tehnologicheskimi-setyami-mobilnogo-shirokopolos/>
- 316 Власти передумали тратить миллиарды на покрытие дорог интернетом по проекту Ротенбергов. СNews. Август 2021 г. https://www.cnews.ru/news/top/2021-08-06_vlasti_peredumali_tratit
- 317 См. утвержденные версии паспорта федерального проекта «Информационная инфраструктура» начиная с августа 2021 г.
- 318 Распоряжение № 663-р. Правительство РФ. Март 2022 г. <http://publication.pravo.gov.ru/Document/View/0001202203310030>
- 319 Паспорт федерального проекта «Информационная безопасность». Цифровая экономика 2024. <https://digital.ac.gov.ru/poleznaya-informaciya/4103/>
- 320 Там же.
- 321 В России начали дистанционно контролировать охраняемые законом объекты. Министерство цифрового развития, связи и массовых коммуникаций. Ноябрь 2020 г. <https://digital.gov.ru/ru/events/40206/>
- 322 Там же.
- 323 Паспорт федерального проекта «Информационная безопасность». Цифровая экономика 2024. <https://digital.ac.gov.ru/poleznaya-informaciya/4106/>
- 324 Дорожные карты 2020 по сквозным цифровым технологиям ФП «Цифровая экономика РФ» (road map digital technology economy). Нейротехнологии, искусственный интеллект AI. Технологии VR AR. <https://xn----dtbhaacat8bfloi8h.xn--p1ai/road-map-digital-technology-economy>
- 325 Дорожная карта развития «сквозной» цифровой технологии «Компоненты робототехники и сенсорики». 2019. https://d-russia.ru/wp-content/uploads/2019/10/plan_robototekhnika-sensorika.pdf
- 326 Дорожная карта развития «сквозной» цифровой технологии «Новые производственные технологии». 2019. https://d-russia.ru/wp-content/uploads/2019/10/plan_NPT.pdf
- 327 Дорожная карта развития «сквозной» цифровой технологии «Технологии беспроводной связи». 2019. https://d-russia.ru/wp-content/uploads/2019/10/plan_TBS.pdf

- 328 Распоряжение № 1484. Правительство РФ. Июль 2019 г. <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=558623#Gwvrn5TP3QrwzNP9>
- 329 Анализ по открытым источникам и документам ФОИВ в распоряжении АНО «Цифровая экономика».
- 330 Ведомственный проект «Цифровая промышленность». МинПромТорг России. <https://www.digital-energy.ru/trends/analytics/projects/digital-industry/>
- 331 Постановление от 30 апреля 2019 г. № 529 «Об утверждении Правил предоставления субсидий российским организациям на возмещение части затрат на разработку цифровых платформ и программных продуктов в целях создания и (или) развития производства высокотехнологичной промышленной продукции. Правительство РФ. Апрель 2019 г. <http://publication.pravo.gov.ru/Document/View/0001201905060036>
- 332 Материалы заседания отраслевой рабочей группы «Цифровая промышленность» при АНО «Цифровая экономика», 2019 г.
- 333 Приказ от 25 февраля 2020 года № 84 «О создании национальной платформы «Цифровое сельское хозяйство». Министерство сельского хозяйства РФ. Февраль 2020 г. <https://docs.cntd.ru/document/564437710>
- 334 Распоряжение № 2446-р. Декабрь 2014 г. <https://rulaws.ru/goverment/Rasporyazhenie-Pravitelstva-RF-ot-03.12.2014-N-2446-r/>
- 335 В «Безопасный город» заселяется Минцифры. ИКС Медиа. Февраль 2021 г. <https://www.comnews.ru/content/212917/2021-02-03/2021-w05/bezopasnyy-gorod-zaselyaetsya-mincifry>
- 336 МЧС съезжает из «Безопасного города». Коммерсантъ. Декабрь 2020 г. <https://www.kommersant.ru/doc/4636274>
- 337 Приказ Минстроя России от 31 октября 2018 г. № 695/пр «Об утверждении паспорта ведомственного проекта Цифровизации городского хозяйства «Умный город». Минстрой России. Октябрь 2018 г. <https://minstroyrf.gov.ru/docs/17594/>
- 338 Проект Цифровизации городского хозяйства «Умный город». Минстрой России. <https://minstroyrf.gov.ru/trades/gorodskaya-sreda/proekt-tsifrovizatsii-gorodskogo-khozyaystva-umnyy-gorod/>
- 339 Приказ «Об утверждении Концепции проекта цифровизации городского хозяйства «Умный город»». Министерство строительства и жилищно-коммунального хозяйства РФ. Декабрь 2020 г. https://d-russia.ru/wp-content/uploads/2020/12/minstroj_ug_kontseptciia.pdf
- 340 Минстрой утвердил новый Стандарт «Умного города». Минстрой России. Май 2022 г. <https://minstroyrf.gov.ru/press/minstroy-utverdil-novyj-standart-umnogo-goroda/>
- 341 Там же.

- 342 В «Цифровом регионе» не сошлись цифры. Коммерсантъ. Сентябрь 2021 г. <https://www.kommersant.ru/doc/4996290>
- 343 Там же.
- 344 Запуск федерального проекта «Цифровой регион» перенесен на осень с туманными перспективами. Cnews. Апрель 2021 г. https://www.cnews.ru/news/top/2021-04-27_zapusk_federalnogo_proekta
- 345 Там же.
- 346 Рынок технологий для умного города. 2019. iKS Consulting. <http://survey.iksconsulting.ru/page5160775.html>
- 347 Постановления Правительства Российской Федерации от 03.05.2019 № 548–555. <http://publication.pravo.gov.ru/Document/View/0001201905060050>
- 348 Постановление Правительства Российской Федерации от 3 мая 2019 г. № 550 «Об утверждении Правил предоставления субсидии из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений в сфере информационных технологий». https://xn--h1apajh.xn--p1ai/media/documents/%D0%9F%D0%BE%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_550_1.pdf
- 349 Грант на разработку отечественных ИТ-решений. Российский фонд развития информационных технологий. <https://xn--h1apajh.xn--p1ai/support-measure/grants/grant-na-razrabotku-otechestvennykh-it-reshenii/>
- 350 Постановление Правительства Российской Федерации от 03.05.2019 № 550. https://рфрит.рф/media/documents/%D0%9F%D0%BE%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_550_1.pdf
- 351 Распределение по направлениям развития технологических областей. Российский фонд развития информационных технологий. Сентябрь 2021 г. https://xn--h1apajh.xn--p1ai/media/documents/2021.09_%D1%81%D0%B2%D0%BE%D0%B4_%D0%BD%D0%B0_%D1%81%D0%B0%D0%B9%D1%82.pdf
- 352 Список утвержден Приложением № 3 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 30 июня 2021 г. № 21.
- 353 См. федеральный проект «Цифровые технологии» на сайте <http://budget.gov.ru/>, строка D5.08.20
- 354 Грантополучатели 2021. Российский фонд развития информационных технологий. https://рфрит.ру/media/documents/%D0%B3%D1%80%D0%B0%D0%BD%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D1%83%D1%87%D0%B0%D1%82%D0%B5%D0%B%D0%B8_2021_4KWeIRG.pdf
- 355 Постановление от 3 мая 2019 г. № 555 «Об утверждении Правил предоставления субсидии из федерального бюджета некоммерческой организации Фонд развития Центра разработки и коммерциализации новых технологий на обеспечение первого

- масштабного внедрения российских решений в сфере информационных технологий». Правительство РФ. Май 2019 г. <http://pravo.gov.ru/proxy/ips/?docbody=&prev-Doc=102628738&backlink=1&&nd=102547447>
- 356 См. федеральный проект «Цифровые технологии» на сайте <http://budget.gov.ru/>, строка D5.14.21.
- 357 Приложение № 3 к протоколу президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 30 июня 2021 г. № 21. <https://dtech.sk.ru/files/309/prioritetnye-napravleniya.pdf>
- 358 ФРИИ и Иннополис запускают первый IoT-полигон. ФРИИ. Июнь 2016 г. https://www.iidf.ru/media/articles/fond/frii-i-innopolis-zapuskayut-pervyy-iot-poligon/?sphrase_id=297229
- 359 ФРИИ начинает отбор стартапов для пилотных проектов в IoT. ФРИИ. Апрель 2016 г. <https://www.iidf.ru/media/articles/fond/frii-nachinaet-otbor-startapov-dlya-pilotnykh-proektov-v-iot/>
- 360 GS Group и ФРИИ запустят акселератор IoT-проектов. ФРИИ. Февраль 2016 г. https://www.iidf.ru/media/articles/fond/gs-group-i-frii-zapustyat-akselerator-iot-proektov/?sphrase_id=297230
- 361 ФРИИ инвестирует в проекты в области «интернет вещей». ФРИИ. Май 2016 г. https://www.iidf.ru/media/articles/fond/frii-investiruet-v-proekty-v-oblasti-internet-ve-shchey/?sphrase_id=297229
- 362 На основе анализа данных портфолио Фонда развития интернет-инициатив (ФРИИ): <https://www.iidf.ru/fond/projects/>
- 363 См. федеральный проект «Цифровые технологии» на сайте <http://budget.gov.ru/>
- 364 Там же, строка D5.14.25.
- 365 Программа «СТАРТ». Фонд содействия инновациям. <https://fasie.ru/programs/programma-start/>
- 366 Мониторинг СМИ. Цифровая экономика (АНО). Октябрь 2021 г. <https://files.data-economy.ru/Digest/2021-10-20-digest.pdf>
- 367 Утверждены результаты конкурсных отборов проектов по программе «СТАРТ». Фонд содействия инновациям. Март 2022 г. <https://fasie.ru/press/fund/start-2022-results/>
- 368 Более 280 проектов инновационного бизнеса получили гранты «Коммерциализация» в 2021 году. Фонд содействия инновациям. Декабрь 2021 г. <https://fasie.ru/press/fund/bolee-280-proektov-innovatsionnogo-biznesa-poluchili-granty-kommercializatsiya-v-2021-godu/>
- 369 ВЭБ.РФ прописался в «умном городе». Коммерсантъ. Октябрь 2020 г. <https://www.kommersant.ru/doc/4528937>

- 370 ВЭБ.РФ инвестирует 400 млн руб. в разработчика интернета вещей. Коммерсантъ. Декабрь 2021 г. <https://www.kommersant.ru/doc/5154616>
- 371 Там же.
- 372 Машины опять будут делать без ЭРА-ГЛОНАСС: что это значит для водителей. ЭРА-ГЛОНАСС. Апрель 2022 г. <https://www.autonews.ru/news/6264fd429a7947175664fdbbc>
- 373 Постановление Правительства Российской Федерации от 22.12.2020 № 2216 «Об утверждении Правил оснащения транспортных средств категорий М2, М3 и транспортных средств категории N, используемых для перевозки опасных грузов, аппаратурой спутниковой навигации». Декабрь 2020 г. <http://publication.pravo.gov.ru/Document/View/0001202012250015>
- 374 Более 712 тысяч грузоперевозчиков и логистических компаний зарегистрировались в госсистеме «Платон». Платон. Апрель 2022 г. <https://platon.ru/ru/front-page/20-04-2022/13670/>
- 375 Паспорт проекта «Создание федеральной автоматизированной системы весогабаритного контроля транспортных средств на автомобильных дорогах общего пользования федерального значения». <https://mintrans.gov.ru/file/426270>
- 376 Там же.
- 377 Операторы встали на весы. Коммерсантъ. Июль 2021 г. <https://www.kommersant.ru/doc/4901086>
- 378 Федеральный закон от 27.12.2018 № 522-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с развитием систем учета электрической энергии (мощности) в Российской Федерации». Государственная Дума РФ. Декабрь 2018 г. <http://publication.pravo.gov.ru/Document/View/0001201812280018>
- 379 Постановление Правительства Российской Федерации от 19.06.2020 № 890. Июнь 2016 г. <http://government.ru/docs/all/128585/?page=4>
- 380 Исследование: доля умных счетчиков в Российской Федерации достигнет 40 % уже в ближайшие два года. Фонтанка.ру. Январь 2022 г. <https://www.fontanka.ru/2022/01/31/70405571/>
- 381 Минэнерго оценило потребность рынка в «умных» счетчиках электроэнергии. ТАСС. Июль 2020 г. <https://tass.ru/ekonomika/9028631>
- 382 Электросчетчики однофазные многотарифные с радиоканалом LoRaWAN™ и реле. Бетар. <http://www.betar.ru/catalog/elektroschetchiki/mnogotarifnye-s-radiokanalom-lorawan-i-rele/>
- 383 Приказ Министерства транспорта Российской Федерации от 26.07.2017 № 277. Официальный интернет-портал правовой информации. <http://publication.pravo.gov.ru/Document/View/0001201711090028>
- 384 IoT Барометр 2021. ПАО «МТС». Июль 2021 г. http://s22.q4cdn.com/722839827/files/doc_downloads/2021/07/MTS-2021-IoT-Barometer.pdf

385 а) Российский и мировой рынок межмашинных коммуникаций и интернета вещей по итогам 2020 года, предварительные оценки на 2021 год и прогноз до 2025 г. Json. TV. 15 января 2022 г. https://json.tv/ict_telecom_analytics_view/rossiyskiy-i-mirovoy-rynok-mejmashinnyh-kommunikatsiy-i-interneta-veschey-po-itogam-2020-goda-predvaritelnye-otsenki-na-2021-god-i-prognoz-do-2025-goda-20220115025817 ;

б) Исследование МТС: к концу 2021 года российский рынок интернета вещей достигнет 117 миллиардов рублей. МТС. Июль 2021 г. <https://moskva.mts.ru/about/media-centr/soobshheniya-kompanii/novosti-mts-v-rossii-i-mire/2021-07-15/issledovanie-mts-k-koncu-2021-goda-rossijskij-rynok-interneta-veshhej-dostignet-117-milliardov-rublej>

386 План мероприятий («дорожная карта») «Создание дополнительных условий для развития отрасли информационных технологий». Правительство РФ. Сентябрь 2021 г. <http://static.government.ru/media/files/gwQRcF4e3G6IA8vTMTNfNAcTWGeQxrt2.pdf><http://static.government.ru/media/files/gwQRcF4e3G6IA8vTMTNfNAcTWGeQxrt2.pdf>

387 а) Системы ГЛОНАСС и «Платон» объединят чипированием. IoT. Март 2017 г. <https://iot.ru/transportnaya-telematika/sistemy-glonass-i-platon-obedinyat-chipirovaniem> ;

б) Универсальное устройство контроля для грузового транспорта. Сиб НПО. http://sibnpo.ru/novosti/universalnoe_ustrojstvo_kontrolya_dlya_gruzovogo_transporta/

388 Министерство связи и массовых коммуникаций Российской Федерации. Государственная комиссия по радиочастотам. Решение от 28 декабря 2017 года № 17-44-06 «Об использовании полос радиочастот радиоэлектронными средствами стандарта LTE и последующих его модификаций в режиме NB-IoT (решение ГКРЧ № 17-44-06)» (с изменениями на 8 декабря 2020 года). <https://docs.cntd.ru/document/556329581#6580IP>

389 Государственная Комиссия по радиочастотам при Министерстве Российской Федерации по связи и информации. Решение от 7 мая 2007 года № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия» (с изменениями на № 21-60-04). <https://docs.cntd.ru/document/902048009?section=operative>

390 Filter Products. LoRa Alliance. <https://lora-alliance.org/showcase/search>

391 В России выделяют дополнительные частоты под сети 5G, но не те, что хотели бы операторы. 3D news. Декабрь 2021 г. <https://3dnews.ru/1054928/v-rossii-budut-videleni-dopolnitelnie-chastoti-pod-seti-5g>

392 Решение от 30 ноября 2018 года № 18-47-03 «О выделении полос радиочастот, внесении изменений в решения ГКРЧ и продлении срока действия решений ГКРЧ» (решение ГКРЧ № 18-47-03). Государственная комиссия по радиочастотам при Министерстве связи и массовых коммуникаций РФ. Ноябрь 2018 г. <https://docs.cntd.ru/document/560857769>



Сайт АНО «Цифровая экономика»

data-economy.ru



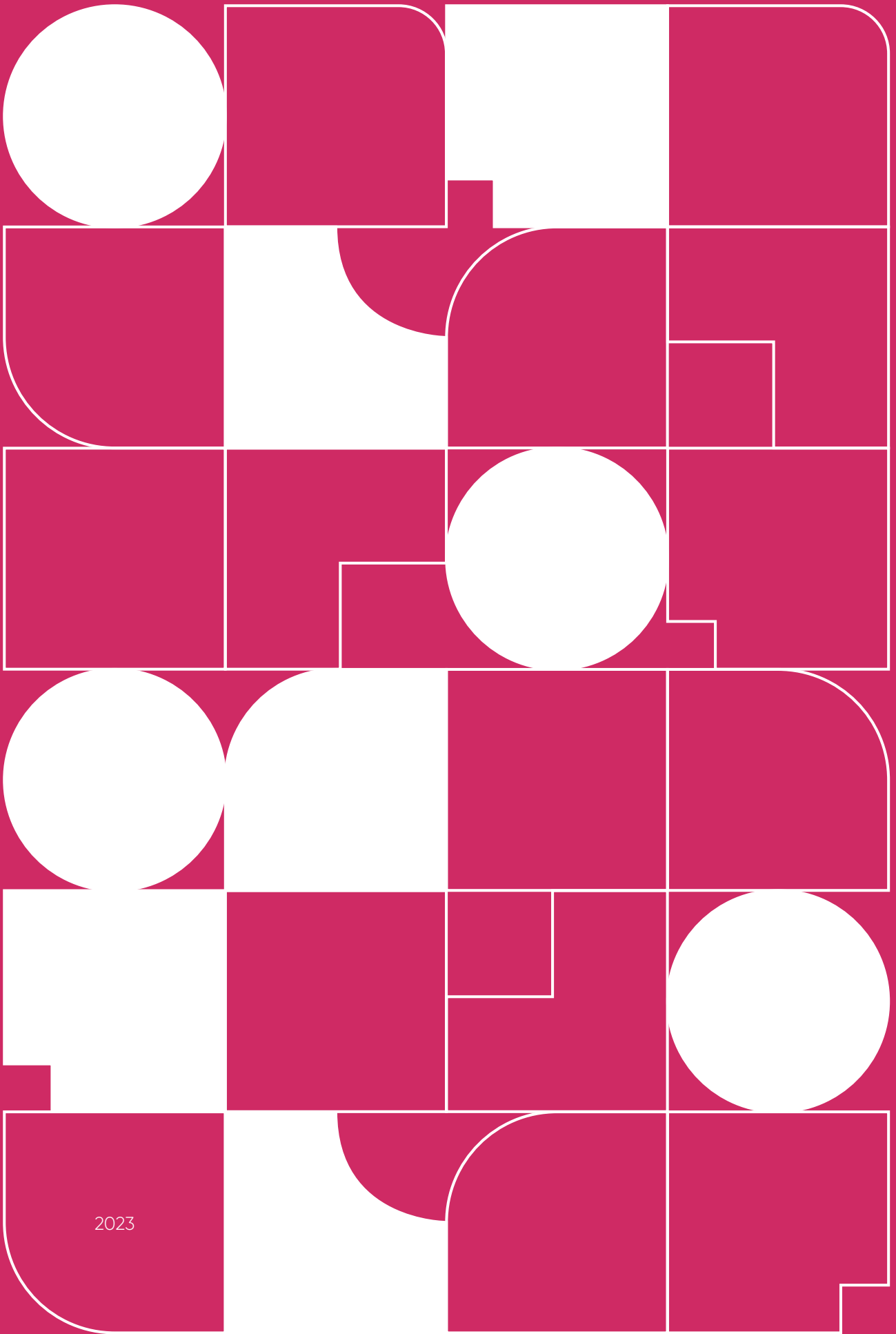
Технологическое лидерство 2030

техлид.рф



Сайт CDO2DAY

cdo2day.ru



2023