

Перспективные рынки и технологии Интернета вещей

ПУБЛИЧНЫЙ АНАЛИТИЧЕСКИЙ ДОКЛАД

**ПЕРСПЕКТИВНЫЕ
РЫНКИ И ТЕХНОЛОГИИ
ИНТЕРНЕТА ВЕЩЕЙ**

Публичный аналитический доклад

Москва
ООО «Лайм»
2019

УДК 681.5:004.738.5-029:33

ББК 32.96 + 32.971.353

П27

Руководитель авторского коллектива:

Дежина Ирина Геннадиевна, д-р экон. наук, руководитель Аналитического Департамента научно-технологического развития, Сколковский институт науки и технологий (Сколтех)

Научные редакторы:

Дежина Ирина Геннадиевна, д-р экон. наук, руководитель Аналитического Департамента научно-технологического развития, Сколтех (Часть 1)

Список авторов:

Дежина Ирина Геннадиевна, руководитель авторского коллектива, д-р экон. наук, руководитель Аналитического департамента научно-технологического развития, Сколтех (введение, разделы 1.1, 1.2, 1.3, 1.5, заключение); *Пономарев Алексей Константинович*, канд. техн. наук, вице-президент по связям с промышленностью, Сколтех (введение); *Лаконцев Дмитрий Владимирович*, канд. техн. наук, директор Центра компетенций НТИ «Технологии беспроводной связи и «интернета вещей», Сколтех (введение); *Нафикова Тамам Низаятовна*, аналитик, Аналитический Департамент научно-технологического развития, Сколтех (разделы 1.1, 1.2, 1.3, 1.5); *Минов Александр Вадимович*, Генеральный директор, АО «Национальный исследовательский институт технологий и связи» (раздел 1.4); *Уткин Никита Александрович*; председатель Технического комитета 194 «Кибер-физические системы», руководитель программ АО «Российская венчурная компания» (раздел 2.1); *Гареев Тимур Рустамович*, канд. экон. наук, заместитель руководителя, Аналитический Департамент научно-технологического развития, Сколтех (раздел 2.1); *Павловский Евгений Николаевич*, канд. физ.-мат. наук, зав.лаб. аналитики потоковых данных и машинного обучения, ФГАОВ ВО «Новосибирский национальный исследовательский государственный университет» (раздел 2.2); *Федоров Максим Валериевич*, д.ф.-х. н., профессор, директор Центра по научным и инженерным вычислительным технологиям для задач с большими массивами данных (CDISE), Сколтех (раздел 3.1); *Пукальчик Мария Алексеевна*, канд. биол. наук, старший преподаватель, Центр по научным и инженерным вычислительным технологиям для задач с большими массивами данных, Сколтех (раздел 3.1); *Шадрин Дмитрий Германович*, аспирант, Центр по научным и инженерным вычислительным технологиям для задач с большими массивами данных, Сколтех (раздел 3.1); *Кабатянский Григорий Анатольевич*, д-р физ.-мат. наук, Советник Ректора по науке, Сколтех (раздел 3.2); *Крук Евгений Аврамович*, д-р техн. наук, профессор, и.о. директора, Московский институт электроники и математики им. А.Н. Тихонова, Национальный исследовательский университет «Высшая школа экономики» (раздел 3.2); *Бурнаев Евгений Владимирович*, канд. физ.-мат. наук, руководитель Advanced Data Analytics in Science and Engineering Group, Сколтех (раздел 3.3).

Технический редактор:

Пригарин Василий Евгеньевич

Перспективные рынки и технологии интернета вещей:

П27

публичный аналитический доклад - М.: ООО «Лайм», 2019.-272 с.:ил

ISBN 978-5-6042289-0-6

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	6
-----------------------	----------

1.Экономические аспекты развития «Интернета Вещей»	14
---	-----------

1.1 Современные определения понятия «Интернет Вещей»	14
---	-----------

1.1.1 Подход на основе перечисления компонентов.....	15
--	----

1.1.2 Функциональный подход	23
-----------------------------------	----

1.1.3 Определение методом перечисления желательных характеристик	24
---	----

1.1.4 Концептуальный подход	27
-----------------------------------	----

1.1.5 Определения «Интернета Вещей» в системе государственного регулирования в России	29
--	----

1.2 Эволюция интернета вещей	31
---	-----------

1.3 Динамика рынков интернета вещей	40
--	-----------

1.3.1 Глобальный рынок	40
------------------------------	----

1.3.2 Технологическая структура рынка «Интернета Вещей»	51
--	----

1.3.3 Отраслевой срез	54
-----------------------------	----

1.3.4 Географическая структура.....	63
-------------------------------------	----

1.3.5 Российский рынок интернета вещей.....	66
---	----

1.4 Перспективные бизнес–модели на рынке «Интернета Вещей».....	74
--	-----------

1.4.1 Варианты бизнес–моделей операторов услуг «Интернета Вещей»	74
---	----

1.4.2 Анализ бизнес–моделей операторов услуг «Интернета Вещей»	80
---	----

1.4.3 Рекомендации по выбору бизнес–модели оператора услуг «Интернета Вещей»	86
---	----

1.5 Государственная политика зарубежных стран и России в области интернета вещей	89
1.5.1 Китай.....	91
1.5.2 США.....	98
1.5.3 Франция.....	105
1.5.4 Германия.....	115
1.5.5 Россия	121

2 Международные и национальные стандарты и рекомендации в области интернета вещей 129

2.1 Практика разработки документов стандартизации на уровне ISO/IEC 134

2.1.1 Глобальная карта работы над стандартами технологии интернета вещей.....	135
2.1.2 Деятельность по международной стандартизации технологий интернета вещей	138
2.1.3 Участие России в деятельности по международной стандартизации в области интернета вещей и смежных технологий	142
2.1.4 Заключение	145
2.1.5 Приложение. Организации, работающие в области стандартизации интернета вещей (кроме ISO, IEC и ITU).....	149

2.2 Проблемы и перспективы стандартизации в области хранения и обработки данных 153

2.2.1 Введение	153
2.2.2 Решаемые проблемы в области беспроводных сетей и интернета вещей	153
2.2.3 Барьеры развития	158
2.2.4 Перспективные направления исследований и их применений.....	159
2.2.5 Выводы	161

3 Некоторые отраслевые приложения интернета вещей	162
3.1 Интернет вещей	
в агропромышленном комплексе	162
3.1.1 Введение	162
3.1.2 Тренды развития интернета вещей в сельском хозяйстве: глобальный рынок инноваций.....	163
3.1.3 Рынок интернета вещей в сельском хозяйстве.....	165
3.1.4 Области применения интернета вещей в сельском хозяйстве и технологические барьеры	166
3.1.5 Выводы	172
3.2 Обеспечение информационной безопасности в системах интернета вещей	173
3.2.1 Введение. Состояние вопроса	173
3.2.2 Тенденции в развитии технологий защиты информации	175
3.2.3 Направления прорывных научных исследований.....	179
3.3 Предсказательное техническое обслуживание	184
3.3.1 Введение	184
3.3.2 Предсказательное техническое обслуживание	186
3.3.3 Примеры приложений ПТО.....	191
3.3.4 Предсказательная аналитика для приложений ПТО. Обнаружение аномалий	200
3.3.5 Мониторинг дорожных условий. Одноклассовая классификация	214
3.3.6 Выводы	226
ЗАКЛЮЧЕНИЕ.....	228
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	237

Введение

Одним из важнейших направлений цифрового развития экономики является развитие совокупности технологий, которую принято называть «Интернетом Вещей». Взрывной рост количества подключенных к интернету устройств и комплексов, расширение спектра их применения в производстве и межотраслевом взаимодействии представляет собой ключевой вызов современности.

Несмотря на то, что представление об «Интернете Вещей» появилось около 20 лет назад, активное развитие технологий началось только в последние годы. Актуальность данного направления непрерывно растет. Так, на кривой Gartner, показывающей цикл зрелости технологий, платформы «Интернета Вещей», по данным на 2018 год, находятся на пике ожиданий.

Сложность описания феномена «Интернета Вещей» состоит в том, что это одновременно и концепция, и набор взаимосвязанных технологий, активно используемых, например, в таких областях, как средства измерения в режиме реального времени, робототехника, искусственный интеллект, машинное обучение, обработка и хранение больших данных. Именно поэтому некоторые эксперты называют «Интернет Вещей» «явлением», а не технологией.

В данной работе мы принимаем следующее определение: «Интернет Вещей» — это вычислительная сеть физических объектов, оснащенных встроенными (embedded) технологиями сбора и передачи информации в совокупности с устройствами и технологиями хранения и интеллектуальной обработки информации, а также устройствами и алгоритмами генерации управляющих воздействий как на части системы, так и глобальных.

С функциональной точки зрения «Интернет Вещей» можно разделить на несколько уровней: оконечные устройства (средства идентификации, датчики, исполнительные

устройства, носимая электроника), транспортный уровень (гетерогенная телекоммуникационная среда, включающая проводные и беспроводные сети) и уровень работы с данными (интеллектуальные платформы, осуществляющие сбор, хранение и обработку). Отдельной технологической проблемой, для всех уровней, является комплексная защита информации на всем пути ее обработки.

Интернет вещей позволяет оперативно получать фактическую информацию, быстро ее анализировать, и, соответственно, принимать обоснованные решения и меры. Использование интернета вещей дает возможность:

- перейти от косвенных показателей к непосредственным (от расчетов к прямому измерению);
- контролировать ситуацию в режиме реального времени;
- собирать сопутствующую информацию, которая обогащает основную;
- изучать свойства системы на более высоком качественном уровне;
- оперативно, в том числе упреждающе, реагировать на события.

Важно подчеркнуть, что собираемая информация – это актив, позволяющий делать более обоснованные выводы, нежели ранее. При этом информация может быть обогащена путем добавления любых иных доступных данных, связанных с областью применения интернета вещей (часовые пояса, погодные условия, информация о смежных системах и т.п.). В итоге, на основе собираемых данных можно построить рекомендательную систему, которая предлагает оптимальные параметры для конкретных условий технологического процесса.

С экономической точки зрения «Интернет Вещей» представляет собой сложное комплексное явление, вследствие чего прогноз его развития – нетривиальная задача. Именно поэтому разные консалтинговые и аналитические агентства постоянно корректируют свои оценки масштаба и направления развития данной предметной области. Между ключевыми

аналитиками, при этом, существуют значительные расхождения. Дополнительно усложняет дело постоянное формирование новых источников выручки и бизнес-кейсов не только за счет появления новых сервисов, но и благодаря совершенствованию уже используемых технологий, повышающему экономическую отдачу.

Соответственно, «Интернет Вещей» можно рассматривать как в разрезе технологий, так и приложений (направлений использования, типов создаваемой ценности). В данной работе «Интернет Вещей» изучается как экономико-технологический феномен, и потому он рассматривается с точки зрения экономики явления (масштабы применения, рынки, регулирование) и ряда его приложений.

Перспективы развития интернета вещей порождают целый комплекс ожиданий в смежных технологических областях.

Так, производители телекоммуникационного оборудования ждут роста спроса на устройства, способные перерабатывать больший объем информации с меньшими задержками в передаче сигнала, и с большими возможностями по числу подключений.

С учетом длительного периода эксплуатации такого оборудования (более 10 лет), расширение спроса на новое качество услуг беспроводной связи создает потенциал ускорения роста компаний-разработчиков и производителей оборудования, в определенной степени формирует условия для передела рынка между поставщиками комплексных решений, между производителями отдельных элементов, допускает, при некоторых условиях, и появление новых игроков.

Планируемое в скором времени принятие и распространение стандарта 5G вызывает особый интерес компаний, стремящихся существенно увеличить свою долю на рынке, «отодвинув» традиционных сверхкрупных поставщиков. Этот стандарт обеспечивает потребности в передаче информации для широкого класса технологически сложных и ответственных проектов интернета вещей в различных секторах экономики и социальной сферы (в частности,

таких, как беспилотные автомобили). Потребности в охвате средствами связи территорий, на которых прогнозируется развитие платежеспособных проектов интернета вещей, требует существенного увеличения плотности их покрытия элементами сотовой сети, либо создания или модернизации стационарных сетей. Сопровождаться это будет ростом спроса на оборудование нового поколения. В целом, разработчики и производители телекоммуникационного оборудования надеются, что запрос со стороны интернета вещей сформирует потребность в существенном увеличении плотности покрытия территорий сетями доступа нового стандарта. В свою очередь это ускорит приход новой инвестиционной волны на рынки сотовой связи, стационарных беспроводных сетей и соответствующего телекоммуникационного оборудования. Ожидания инвесторов особенно подогреваются новостями об успехах беспилотного транспорта, умных дорог и городов, обеспечиваемых кардинальным увеличением потоков информации между различными техническими устройствами, что, естественно, требует развития систем передачи информации и существенной модернизации оборудования.

В то же время, в ряде стран, где признается возможность и важность государственного регулирования телекоммуникационной отрасли, принимаются или готовятся предложения по существенному ужесточению требований к операторам и поставщикам оборудования в проектах 5G.

Требования безопасности, связанные с возможностью несанкционированного либо непреднамеренного вмешательства в функционирование все большего числа элементов современной технологической среды, являются, по сути, вполне обоснованными. В зависимости от принятых концепций и практик обеспечения безопасности, государства принимают соответствующие решения по корректировке правил, касающихся развития интернета вещей во всех его технологических проявлениях: от применяемой элементной базы до протоколов передачи данных в рамках конкретных проектов. В русле этого подхода, в ряде стран происходит и заметное перераспределение рынка услуг и оборудования,

как, например, отстранение ряда китайских компаний от участия в проектах внедрения указанного стандарта в Австралии и некоторых других странах.

Рост спроса на услуги беспроводной передачи информации дает основание государственным ведомствам пересматривать сложившуюся практику распределения частотного ресурса, что также является мощным рычагом регулирования рынка, способом как ограничения доступа, так и привлечения новых игроков на рынок телекоммуникаций. В зависимости от принимаемых государственных решений, национальные рынки могут трансформироваться как в сторону монополизации, так и в сторону развития конкуренции. При рациональном регулировании, развитие проектов интернета вещей создает предпосылки для снижения барьера входа на рынок телекоммуникационных услуг для относительно небольших компаний, например, берущихся за обустройство покрытия ограниченных территорий и площадей стационарными сетями нового поколения.

Ожидаемое повышение спроса на системы беспроводной передачи информации нового качества касается аппаратуры, используемой как операторами сотовой связи, так и эксплуатантами систем стационарного доступа. Передача данных может реализовываться в рамках приобретения услуг сотовых операторов, или путем создания автономных комплексов стационарного доступа (например, для организации работы беспилотной сельскохозяйственной техники). Выбор между сотовыми операторами и собственными системами стационарного доступа для многих проектов интернета вещей в городском хозяйстве и, тем более, на промышленных предприятиях, также не является очевидным.

Распространение проектов интернета вещей вызывает естественное оживление в среде производителей сенсоров, в частности, давая новый импульс развитию фотонных технологий. Ожидания резкого роста числа «долгоиграющих» автономных устройств рисуют благоприятные перспективы разработчикам и производителям нового поколения маломощных источников питания. Так, например, запрос на соответствующие технологии генерируют проекты

использования интернета вещей в задачах мониторинга и поддержания требуемых параметров состояния человеческого организма.

Интернет вещей начинает создавать спрос и на расширение номенклатуры компонентной базы, давая работу дизайн-центрам, ориентированным на создание систем очень разного класса сложности. Требование высокой кастомизации решений для ряда задач интернета вещей, от сложных транспортных систем до встроенных комплексов контроля состояния человеческого организма, ставит разработчиков сложных устройств перед серьезными вызовами.

Наряду с производителями сложных вычислительных комплексов, свое место ищут и компании, сохранившие производство элементной базы низкой степени интеграции, небезосновательно надеясь на массовость внедрения относительно простых и дешевых коммуникационных и вычислительных устройств в системы городских хозяйств, в ряд промышленных процессов, в среду домохозяйств.

Таким образом, распространение интернета вещей создает значительный мультипликативный эффект в ряде смежных секторов, таких как телекоммуникации, приборостроение, микроэлектроника. При этом неопределенность прогнозов оказывает неоднозначное влияние на активность различных категорий инвесторов. Это делает актуальным изучение и мониторинг развития как платформенной инфраструктуры самих проектов интернета вещей, так и производства широкой гаммы программно-аппаратных средств.

На сегодняшний день развитие интернета вещей замедляют различные факторы – чисто технологические, социально-экономические (различные аспекты спроса и предложения, координации между участниками рынка) и институциональные, связанные с несовершенством регуляторной базы и недостаточной стандартизацией (есть необходимость создания базы стандартов, регуляторных документов, а порой даже и единой терминологии). Подход к регулированию различается по странам. Есть страны с централизованным подходом и единой системой стратегического планирования, а есть страны, принявшие децентра-

лизированный подход: они рассматривают «Интернет Вещей» в контексте широкой повестки перехода на «цифровую экономику» либо в связи с формированием новых подходов в индустрии (Индустрия 4.0). Россия более тяготеет к централизованной модели. Анализировать это особенно интересно в международном контексте.

Описанные выше характеристики «Интернета Вещей» обусловили следующий подход к построению данной книги. Вначале будут рассмотрены экономические аспекты и проблемы стандартизации и регламентации, затем — избранные кейсы, показывающие возможные приложения.

В первой части книги анализируются экономические параметры и рынки «Интернета Вещей». В частности, показана многогранность самого понятия, его эволюция и связанное с ней расширение области приложений данной совокупности технологий. Значительное место уделено анализу рынков интернета вещей в разной типологии – по отраслям, в межотраслевом разрезе, по создаваемой ценности.

Затем рассматриваются страновые аспекты развития «Интернета Вещей». Особое внимание уделяется мерам государственной поддержки, реализуемым в США, Китае, Германии, Франции и России. Выбор зарубежных стран обусловлен их ролью. США и Китай являются лидерами в этом направлении, Германия и Франция представляют интерес как развитые европейские страны, практикующие разные подходы к стимулированию развития «Интернета Вещей» (у Франции есть отдельная программа, Германия не выделяет данную технологию из общих мер содействия цифровому развитию). Затем, в контексте сравнения рассматривается российский опыт.

Вторая часть обзора посвящена вопросам разработки международных и российских стандартов в области «Интернета Вещей».

Наконец, третью часть составляют избранные кейсы, демонстрирующие возможные отраслевые приложения интернета вещей и технологические аспекты, связанные с его использованием – предсказательное техническое обслуживание и обеспечение безопасности.

Безусловно, в одном обзоре нельзя полноценно представить весь спектр направлений для такого разнопланового явления. Вместе с тем, экономические и институциональные параметры можно отнести к критически важным для будущего развития. Данный обзор может представлять интерес для специалистов в области «Интернета Вещей», лиц, принимающих решения по научно–технологическому развитию, экономистов, маркетологов и студентов.

Алексей Пономарев,

к.т.н., вице-президент, Сколковский институт науки и технологий

Дмитрий Лаконцев,

к.т.н., директор Центра компетенций НТИ «Технологии беспроводной связи и «интернета вещей», Сколковский институт науки и технологий

Ирина Дежина,

д.э.н., руководитель Аналитического департамента научно–технологического развития, Сколковский институт науки и технологий

1. Экономические аспекты развития «Интернета Вещей»¹

1.1 Современные определения понятия «Интернет Вещей»

Термин «Интернет Вещей» (Internet of Things, далее – IoT) появился в 1999 году, когда сотрудник Procter & Gamble Кевин Эштон предложил оптимизировать логистику корпорации с помощью радиочастотных меток (radio-frequency identification, RFID) [1.1]. С тех пор появилось много определений IoT, которые можно разделить на несколько типов. Мы выделяем четыре подхода (Рис. 1.1): на основе перечисления компонентов, перечисления желательных характеристик, по функциональным признакам, а также принятие IoT как концептуальной конструкции.

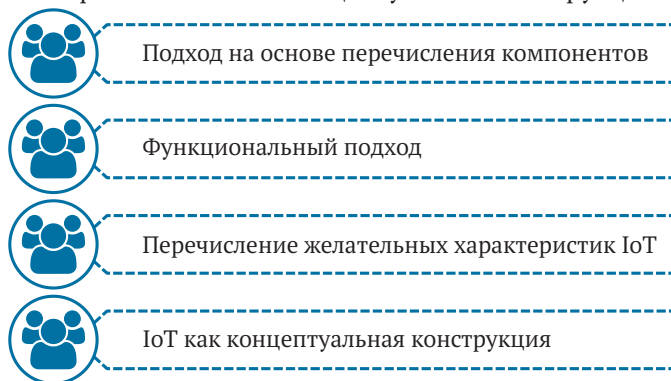


Рисунок 1.1 — Подходы к определению «Интернета Вещей»

Источник: составлено авторами

¹ Дежина И.Г. (Сколтех), Нафикова Т.Н. (Сколтех)

1.1.1 Подход на основе перечисления компонентов

В эту группу входят определения «Интернета Вещей», основанные на перечислении составных частей его структуры. Например, Ник Уэнрайт, глава Стратегической группы по будущему интернету Великобритании, предложил следующую формулу «Интернета Вещей» [1.2]:

IoT = Датчики + Данные + Сети + Услуги

Анализ показал, что в рамках данного подхода существуют две категории определений – 1) рассматривающие в качестве объекта простое сочетание нескольких элементов IoT, например, общую инфраструктуру приборов и соединяющих их сетей [Датчики + Сети]; 2) рассматривающие IoT как систему всей совокупности компонентов [Датчики + Данные + Сети + Услуги].

В Таблице 1.1 представлены некоторые примеры определений, соответствующие каждой категории.

Таблица 1.1— Определения «Интернета Вещей» по его компонентам

Определение	Категория
Интернет вещей – концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека [1.3]	1
Интернет вещей с узко технологической точки зрения – это сеть сетей, состоящих из уникально идентифицируемых объектов («вещей»), способных взаимодействовать друг с другом без вмешательства со стороны человека, через IP-подключение [1.4].	1
Интернет вещей — это глобальная сеть компьютеров, датчиков (сенсоров) и исполнительных устройств (актуаторов), связывающихся между собой с использованием интернет протокола IP (Internet Protocol) [1.5].	1

«Интернет вещей» — это концепция соединения физических предметов, оснащенных встроенными технологиями для взаимодействия друг с другом или внешней средой, общей автономной сетью [1.6].	1
Интернет вещей — это группы цифровых устройств, таких как промышленные датчики, собирающих и передающих данные через Интернет [1.7].	1
Интернет вещей — это сеть физических объектов: автомобилей, оборудования, бытовых устройств и т.д., которые используют датчики и API (Application Programming Interface) и обмениваются данными через интернет [1.8].	1
Интернет вещей по своей сути — это система машин или объектов, оснащенных технологиями сбора данных таким образом, чтобы эти объекты могли коммуницировать друг с другом [1.9]	1
Интернет вещей — это вселенная подключенных вещей, которые предоставляют ключевые физические характеристики для дальнейшей обработки этих данных в облачном сервисе для того, чтобы достичь глубинное понимание бизнеса [1.10].	2
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 совместимых информационно–коммуникационных технологий [1.11].	2
Инфраструктура взаимосвязанных объектов, людей, систем и информационных ресурсов в совокупности с интеллектуальными услугами, которые позволяют им обрабатывать информацию физического и виртуального миров и осуществлять в ответ действия [1.12].	2

Источник: составлено авторами

Определения первой категории более распространены, и при этом гораздо реже акцент делается на таких компонентах, как данные и услуги; чаще всего используется определение IoT как состоящего из двух компонентов – сенсоров (датчиков) и сетей:

$$\text{IoT} = \text{Датчики} + \text{Сети}.$$

Можно отметить некоторую субъективность в акцентировании того или иного элемента в определении IoT – видимо, это зависит от характера интересов и деятельности тех авторов, которые предлагают свою трактовку. Такие организации представляют, как правило, различные этапы цепочки создания стоимости в IoT. Предлагая определение, подчеркивающее значимость производимого ими компонента, они стремятся усилить свои позиции на рынке для того, чтобы способствовать перераспределению отраслевой маржи в свою пользу. С этой точки зрения можно выделить три позиции по отношению к понятию «Интернет Вещей» [1.13, 1.14]:

- ориентация на «Вещи», когда в центр внимания ставятся объединенные в совместную инфраструктуру объекты. Технологии отслеживания и адресации, такие как системы RFID-меток и сенсорные сети, занимают ключевое место в этой парадигме IoT;
- фокус внимания на «Интернете», то есть определение понятия с точки зрения сетевых взаимодействий;
- ориентация на данные или семантическая позиция (Semantic oriented), когда во главу угла ставится логическая организация информации. Она связана с развитием семантической паутины – надстройками над существующей Всемирной паутиной, предназначенными для того, чтобы размещенная информация стала более понятной для пользователей.

В случае со второй категорией – системными структурными определениями – понятие определяется через архитектуру «Интернета Вещей». Архитектура, или эталонная модель IoT, показывает, как связаны друг с другом лежащие в ее основе инфокоммуникационные технологии. Она

схематично иллюстрирует, каким образом устройства, сети и услуги участвуют в процессе сбора, обработки, анализа данных и доставки результатов потребителю, давая более полное и системное представление об «Интернете Вещей». Общепринятой эталонной модели архитектуры нет. Различные организации, такие как официальные международные органы стандартизации, отраслевые объединения, аналитические агентства предлагают свои определения архитектуры IoT. Кроме того, некоторые ученые полагают, что архитектура IoT обрastaет все новыми технологическими слоями, усложняясь по мере развития.

Среди организаций, предложивших свои версии архитектуры, можно выделить Международный союз электросвязи (МСЭ)², Всемирный форум IoT (Internet of Things World Forum, IoTWF)³, Европейскую комиссию, а также исследовательские агентства, подобные IoT Analytics. Различия в представленных ими архитектурах диктуются разными целями и задачами, стоящими перед организациями.

Исследовательские комиссии Сектора стандартизации электросвязи МСЭ–Т разработали целую серию рекомендаций по IoT – “Y: Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений”. Вопросы архитектуры интернета вещей рассматриваются в рекомендациях МСЭ–Т Y.2060 «Обзор интернета вещей» [1.11].

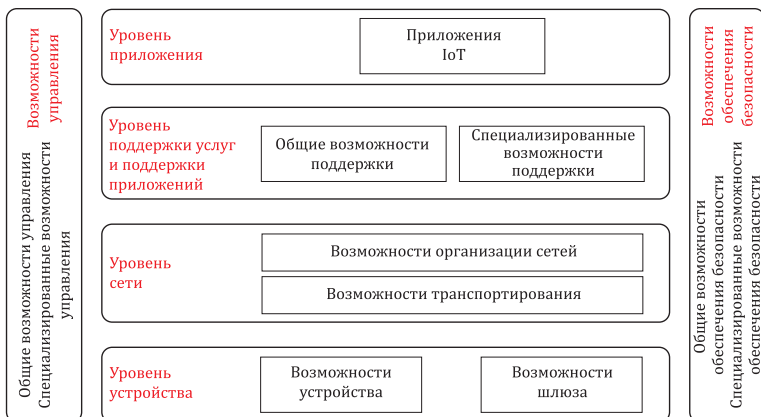
² МСЭ - специализированное подразделение ООН. В рамках МСЭ работают исследовательские комиссии Сектора стандартизации электросвязи - МСЭ-Т. Членами МСЭ-Т являются передовые компании мира в области ИКТ и администрации стран. Разрабатываемые исследовательскими комиссиями международные стандарты известны как Рекомендации МСЭ-Т.

³ Участниками IoTWF являются лидеры индустрии, такие как IBM, Intel и Cisco, а также ведущие ученые, исследователи и инноваторы, представители государственных структур

Согласно МСЭ–Т Y.2060 эталонная модель включает в себя четыре уровня (см. Рис. 1.2):

- уровень приложения;
- уровень поддержки услуг и поддержки приложений;
- уровень сети;
- уровень устройства.

В модель также включены возможности управления и обеспечения безопасности, которые связаны с этими четырьмя уровнями:



Y.2060(12)_F04

Рисунок 1.2 — Эталонная модель IoT, МСЭ–Т Y.2060

Источник: [1.11]

Организационный комитет Всемирного форума IoT предложил в 2014 г. свою эталонную модель [1.15]. Цель Всемирного форума IoT – ускорить развертывание «Интернета Вещей». Объединяя рыночных игроков, Всемирный форум решает вопросы разработки приложений, промежуточного ПО и функций поддержки для корпоративного сегмента. Предложенная им архитектура является инструментом решения указанных задач. Отличие этой модели от архитектуры МСЭ состоит в том, что в последней акцент сделан на уровнях устройства и шлюза, а верхние слои описываются только в общих чертах. Эталонная архитектура, предложенная Всемирным форумом [1.16], имеет семь уровней (Рис. 1.3).



Рисунок 1.3— Эталонная модель Всемирного форума IoT

Источник: [1.17]

Европейский союз разработал свою архитектуру интернета вещей [1.18] в рамках специального проекта IoT–Architecture (IoT–A), реализованного при поддержке Европейской Комиссии в 2010–2013 гг. (Рис. 1.4). Главной целью проекта было достижение совместимости систем IoT, поэтому в этой референтной архитектуре возможна полная интеграция RFID–меток и узлов беспроводных сенсорных сетей, однако большинство решений пока еще основано на системе EPCglobal⁴.

⁴ EPCglobal Network – ключевые элементы организации RFID-систем, соответствующих стандартам EPCglobal. В набор входят пять базовых компонентов: электронные коды продуктов (EPC) как таковые, система идентификации (EPC-совместимые метки и считыватели), межплатформенное программное обеспечение (EPC Middleware) и сервисы Object Name Service (ONS) и EPC Information Services (EPCIS). Эти пять компонентов образуют эталонную архитектуру, которой могут пользоваться компании по всему миру для внедрения собственных решений в сфере RFID.

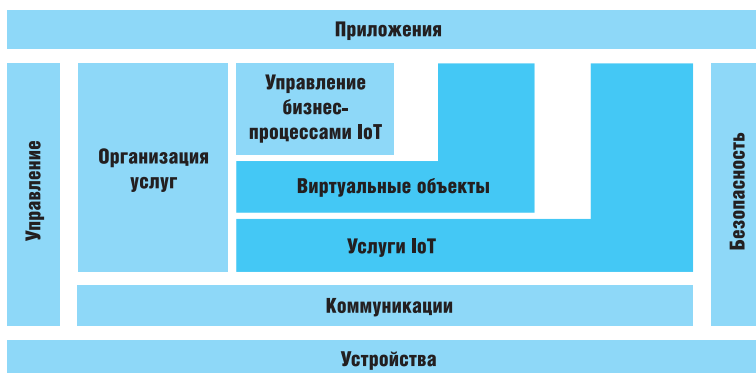


Рисунок 1.4— IoT-A архитектура.

Источник: [1.12]

Что касается компаний, занимающихся изучением рынков, то они преимущественно используют схему, предложенную МСЭ, но без выделения функции управления. Подобная архитектура, в частности, представлена исследовательской группой IoT Analytics (Рис. 1.5).

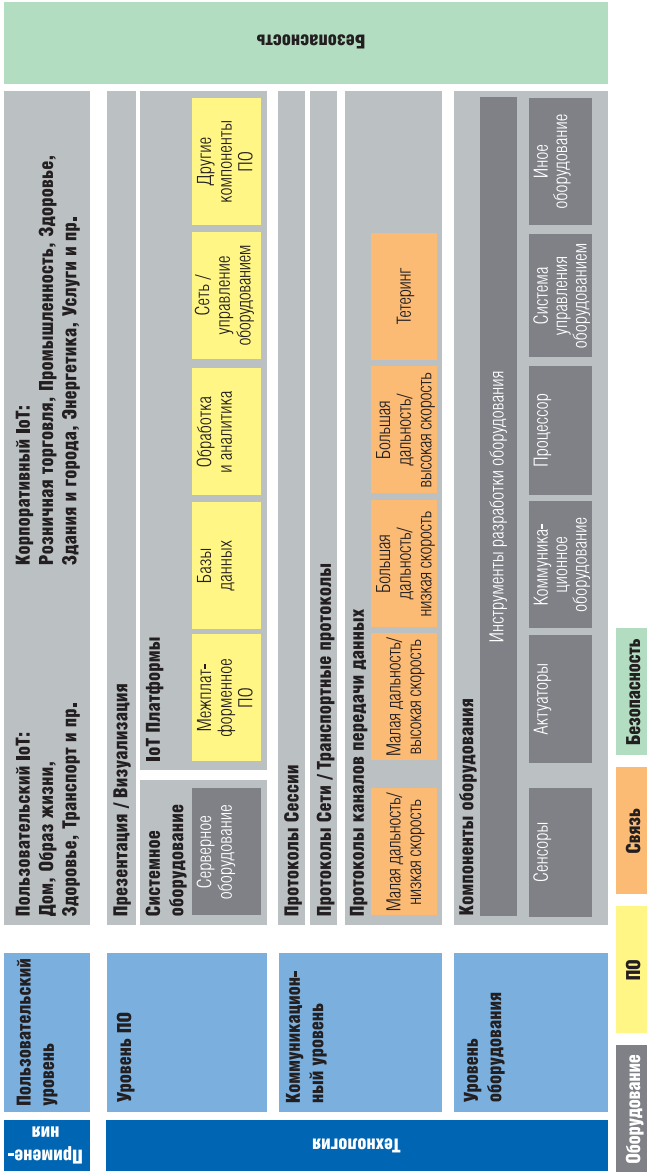


Рисунок 1.5— Эталонная модель IoT Analytics
 Источник: [1.19]

1.1.2 Функциональный подход

Функциональный подход подразумевает определение «Интернета Вещей» через его предназначение – то есть решаемые с его применением задачи. Перечень некоторых задач для каждой категории участников пространства «Интернета Вещей» представлены в Таблице 1.2.

Таблица 1.2— Задачи, решаемые «Интернетом Вещей»

Потребитель	Задача
Человек	Улучшение здоровья и увеличение продолжительности жизни Повышение уровня личной безопасности Улучшение качества досуга
Бизнес	Повышение удовлетворенности потребителей Оптимизация издержек Повышение качества продуктов и услуг Повышение производительности труда Управление рисками Оптимизация издержек Расширение клиентской базы Оптимизация НИОКР
Государство	Повышение уровня общественной безопасности Увеличение эффективности предоставления коммунальных и прочих государственных услуг Оптимизация структуры бюджета

Источник: составлено авторами

Приведем пример определения, которое базируется на функциональном подходе: «Интернет вещей – это обобщающее понятие, которое описывает многогранное основание для ряда приложений и целей, реализация которых становится возможной благодаря связи между уникально идентифицируемыми предметами (устройствами, сенсорами, маркированными вещами и живыми существами),

обладающими функциями сбора данных и коммуникации для передачи и/или приема данных в целях выполнения конкретных социальных и бизнес-задач, а также задач, стоящих перед отдельными людьми» [1.20].

1.1.3 Определение методом перечисления желательных характеристик

Еще одним способом определения понятия «Интернет Вещей» является перечисление его желаемых параметров. Среди таких параметров можно выделить, в том числе, следующие:

- комплексное восприятие (comprehensive sense): использование RFID-меток, сенсоров, двумерного кода для сбора информации об объектах в любом месте, в любое время;
- надежная передача данных: точная доставка информации об объектах в режиме реального времени посредством комбинирования разных телекоммуникационных сетей и интернета;
- интеллектуальная обработка данных: использование интеллектуальных вычислений (например, в облаке), для обработки и анализа больших объемов данных и информации в целях осуществления интеллектуального контроля над объектами [1.21].

Данные признаки соответствуют этапам процесса преобразования данных от их получения до результатов их обработки.

Несколько иной подход к определению признаков IoT представлен в работе Atzori et al. [1.13]. Согласно этому подходу «Интернет Вещей» должен удовлетворять следующим требованиям:

- присутствие глобальной сетевой инфраструктуры или сетевого подключения, которые обеспечивают совместимость элементов IoT, их беспрепятственную интеграцию и уникальный механизм адресации. В ее качестве может выступить любая глобальная инфраструктура (не обязательно на основе IP), которая позволяет выйти за рамки идеи обособленной внутренней сети вещей (Intranet of Things);

- повсеместность: главные объекты в IoT – предметы ежедневного использования, а не только устройства, относящиеся к сфере ИКТ. Данные объекты должны быть считываемыми, опознаваемыми, обнаруживаемыми и/или контролируемыми. Поэтому общепризнана потребность в решениях, которые позволяют связать физические и виртуальные объекты;
- автономность и самоуправление (autonomicity). Эти два признака, которые часто приписываются объектам, относящимся к интернету вещей, так как контроль над системой такого уровня сложности возможно достичь только посредством самоконтроля (self-governance) и самоуправления (self-management);
- эффективный (в идеале «умный») дизайн интерфейсов, как между людьми и вещами, так и между вещами;
- гетерогенность используемых технологий, которая подразумевает разработку подходящих решений, обеспечивающих сосуществование этих технологий на платформе, выбранной для внедрения IoT;
- связанность услуг с объектами. Эти услуги могут быть комплексными или простыми и строятся на основе информации, относящейся к каждому объекту.

Если предположить, что все эти признаки обязательно должны быть характерны для IoT, тогда, строго говоря, ни одно из доступных на данный момент решений не может быть отнесено к этому понятию. В Таблице 1.3 показаны как существующие, так и пока отсутствующие признаки IoT.

Таблица 1.3— Присущие и отсутствующие признаки IoT

Технология	Существующие признаки IoT	Недостающие признаки IoT
RFID платформы	Повсеместное распространение; часто интегрированы с сенсорами/актуаторами	Эффективная виртуализация объекта; автономность и самоуправление; взаимодействие между объектами
Всепроникающие вычислительные платформы	Повсеместное распространение, автономность и самоуправление; гетерогенность технологий; связь услуг с объектами	Глобальная сетевая инфраструктура; интерфейсы для коммуникации между вещами
Киберфизические системы	Повсеместное распространение, автономность и самоуправление; интерфейсы для коммуникации как между людьми и вещами, так и между вещами; гетерогенность технологий; связь услуг с объектами	Глобальная сетевая инфраструктура
Сенсорные сети	Автономность и самоуправление; взаимосвязь между услугами и физическими ресурсами	Глобальная сетевая инфраструктура; повсеместное распространение; гетерогенность технологий;
Системы межмашинной коммуникации	Доступ к каналам связи и глобальная сетевая инфраструктура; интерфейсы для коммуникации как между людьми и вещами, так и между вещами; гетерогенность технологий	Повсеместное распространение, автономность и самоуправление

Источник: [1.13]

Таким образом, согласно данному подходу, по своим признакам ни одна существующая система не является полноценным «Интернетом Вещей», – пока это только развивающееся явление.

1.1.4 Концептуальный подход

Именно концептуального подхода придерживаются многие исследователи. Так, Atzori et al [1.13] определяют «Интернет Вещей» следующим образом.

«IoT – концептуальная конструкция, которая максимально использует доступность гетерогенных приборов и решений в сфере каналов связи, а также дополненные физические объекты, предоставляющие общедоступную информационную базу на глобальном уровне, в целях поддержки разработки приложений, в которых на одном виртуальном уровне участвуют люди и образы объектов».

«IoT – это область пересечения людей (реальный мир), систем (киберпространство) и физического мира (атомическое пространство)».

«IoT – концептуальная конструкция с прорывным потенциалом, которая быстро набирает силу и привносит с собой новый энтузиазм и более широкое внимание к усовершенствованию уже существующих базовых технологий и систем».

В свою очередь группа разработки интернет–решений для бизнеса Cisco (IBSG) [1.22] считает, что IoT – почти философское понятие, «это новый этап развития Интернета, значительно расширяющий возможности сбора, анализа и распространения данных, которые человек может превратить в информацию, знания и, в конечном итоге, обрести мудрость».

Глобальная консультационная компания Zinnov Zones [1.23] делает акцент на рынках и компаниях: «IoT – это пространство объединения множества инфраструктурных и технологических слоев, где конкурируют между собой лидеры традиционных рынков и компании нового поколения».

Концепцию «Интернета Вещей» обычно рассматривают с трех позиций. Первая подчеркивает, что с точки зрения

технологий, IoT не является принципиально новой, недавно возникшей в сфере ИТ технологией, которая должна заметить уже существующие. Наоборот, IoT инклюзивен в том плане, что он охватывает существующие и будущие технологии с присущими им особенностями. При этом стоит отметить, что концепция «Интернета Вещей» выходит за рамки простого ребрендинга, так как включает совокупность прорывных технологий, создавая условия для того, чтобы новые компании конкурировали с лидерами отрасли. Вторая позиция заключается в том, что со стороны разработки услуг, IoT объединяет несколько технологий для передачи информации от источников. К ним относятся не только люди (использующие такие традиционные устройства, как ноутбуки, компьютеры, телефоны и прочее), но и другие реальные и виртуальные объекты. Все они являются частью окружающей среды, в которой пользователям предоставляются услуги. Такие потоки данных должны стать своего рода общей информационной базой, которая может быть организована в форме обычной сети. IoT становится потенциально ориентированной на сервис архитектурной моделью будущего интернета. Наконец, третья позиция основана на том, что с точки зрения предназначения (finalization) IoT – это новый путь решения вопросов, влияющих на социальные аспекты жизнедеятельности человека, новые способы строительства домов и городов, соразмерных человеку и отвечающих человеческим потребностям, новые методы решения проблем в сфере управления энергетикой и новые подходы к улучшению здоровья и благосостояния людей, включая образование [1.13].

1.1.5 Определения «Интернета Вещей» в системного-сударственного регулирования в России

В документах государственного уровня определение «Интернета Вещей» содержится в числе понятий, которыми оперирует Национальная Технологическая Инициатива (НТИ), а также в Дорожных картах развития «Интернета Вещей»⁵, разработанных по инициативе Правительства при участии Фонда развития интернет-инициатив (ФРИИ), и в Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы.

В НТИ определение IoT дано в двух рыночных дорожных картах – Энерджинет и Хелснет. В Энерджинете IoT определен как концепция вычислительной сети физических объектов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой. Организация таких сетей рассматривается как явление, способное перестроить экономические и общественные процессы и исключить человека из части действий и операций. Данное определение соответствует концептуальному подходу и рассматривает IoT с точки зрения его предназначения. В Хелснет предложено более простое определение, основанное на перечислении компонентов: это коммуникационная сеть, объединяющая обычные окружающие человека устройства (холодильник, куртка, ботинки и т.п.) и позволяющая расширить функционал этих предметов. Это определение из категории 1, где в качестве объекта рассматривают простое сочетание нескольких элементов IoT, в данном случае [Датчики+Сети], с акцентом на значимость сетей.

Есть также проект Дорожной карты Сейфнет, где IoT понимается в смысле определения, данного аналитической компанией Gartner: «Интернет Вещей» – сеть физических объектов, содержащих встроенную технологию, которая позволяет этим объектам измерять параметры собственного состояния или состояния окружающей среды, использовать

⁵ Плана мероприятий («дорожная карта») «Развитие технологий в области интернета вещей» и Плана мероприятий («дорожная карта») «Внедрение технологий интернета вещей в агропромышленном комплексе»

и передавать эту информацию. Данное определение также базируется на перечислении компонентов, только в совокупность включены еще и данные: IoT = [Датчики + Сети + Данные].

В Дорожных картах, разрабатывавшихся при участии ФРИИ, дано системное определение на основе перечисления компонентов: «интернет 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 совместимых информационно–коммуникационных технологий».

В Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы интернет вещей определен как «концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека.» Это концептуальное определение, учитывающее компоненты «сети» и «датчики» и подчеркивающее такую характеристику интернета вещей, как автономность.

Таким образом, единого определения «Интернета Вещей» в России на государственном уровне управления нет, и оно отсутствует даже на уровне дорожных карт НТИ. В каждой дорожной карте дана собственная интерпретация. Естественно, при попытках регулирования объекта, суть которого не до конца определена, возникают сложности.

В данном обзоре принимается определение, относящееся к подходу на основе перечисления технологических компонентов:

«Интернет Вещей» — это вычислительная сеть физических объектов, оснащенных встроенными (embedded) технологиями сбора и передачи информации в совокупности с устройствами и технологиями хранения и интеллектуальной обработки информации, а также устройствами и алгоритмами генерации управляющих воздействий как на части

системы, так и глобальных. Важной особенностью данного определения является его простота и функциональность.

С точки зрения архитектуры «Интернета Вещей», мы используем определение, данное компанией Intel (Рис. 1.6). Архитектура состоит из шести основных и двух сквозных уровней. К основным относятся коммуникации и средства связи, данные (в этом уровне отдельно выделяется аналитика), управление, контроль, приложения и бизнес-уровень; к сквозным – вспомогательный уровень для разработчиков и безопасность. Белые блоки в архитектуре обозначают пользовательские уровни. При этом, «бизнес-уровень» получает доступ к остальным уровням решения через приложения.

1.2 Эволюция интернета вещей⁶

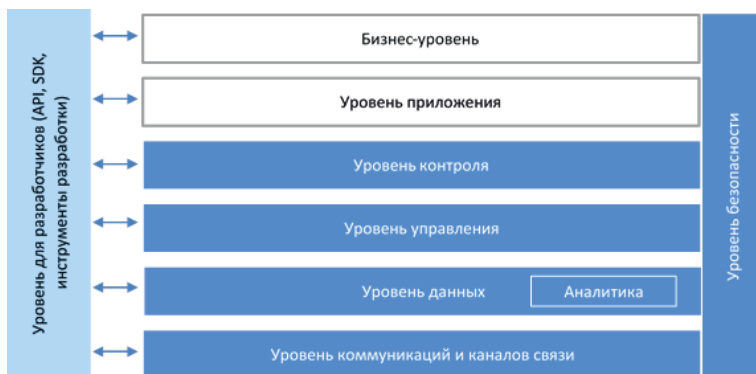


Рисунок 1.6— Архитектура интернета вещей компании Intel

Источник: [1.23]

Эволюция интернета вещей своеобразна тем, что есть своего рода асинхронность в развитии самого явления и его формального определения. С одной стороны, еще до 1999 года, когда К. Эштон впервые использовал понятие «Internet of Things», в научных и прикладных исследованиях уже произошли открытия, близкие по своей сути к IoT. Так, в 1982 г. сотрудники Университета Карнеги Меллон (Carnegie Mellon

⁶ Дежина И.Г. (Сколтех), Нафикова Т.Н. (Сколтех)

University) подключили к интернету вендинговую машину Coca-Cola, что позволяло им контролировать уровень запасов напитков и температуру хранения [1.25] Другие источники называют первым IoT устройством тостер, который выпускник Массачусетского технологического института (MIT) подсоединил к интернету и представил на конференции INTEROP в 1990 году. Среди других университетов, занимавшихся в тот же период исследованиями в этой области, можно назвать Колумбийский университет (Columbia University), Технологический университет штата Джорджия (Georgia Tech), университет Беркли (Berkeley University) и другие. В 1997 г. в Кембридже, штат Массачусетс прошел первый международный симпозиум IEEE⁷ по носимым компьютерам, организованный университетами Carnegie Mellon, MIT и Georgia Tech [1.26].

Корпорации также разрабатывали продукты, близкие по своей сути к IoT. В 1994 г. Xerox Euro PARC продемонстрировал носимое устройство Forget-Me-Not, которое собирало и хранило данные о взаимодействии с людьми и другими приборами [1.26, 1.27]. В 1995 г. компания Siemens внутри подразделения по мобильным телефонам учредила специальный департамент для разработки модуля беспроводной межмашинной коммуникации. В 1997 г. компания LG начала разработку первого в мире холодильника, подключенного к интернету. Европейская комиссия первым индустриальным применением IoT (в понимании RFID-меток, встроенных в объекты) называет сеть Presto, развёрнутую в 1998 г. Однако тогда все это еще не называлось интернетом вещей.

При этом, уже после появления термина «Интернет Вещей» внедрение соответствующих технологий происходило фрагментарно и медленно, на протяжении почти десяти лет. В период 1999–2005 гг. «Интернет Вещей» в большей степени был предметом академических исследований (главным образом в рамках работы лаборатория Auto-ID Массачусетского технологического института).

⁷ *Институт инженеров электротехники и электроники — IEEE — международная некоммерческая ассоциация специалистов в области техники, мировой лидер в области разработки стандартов по радиоэлектронике, электротехнике и аппаратному обеспечению вычислительных систем и сетей.*

чусетского технологического института), нежели областью интереса бизнеса и промышленности. В то же время сама концепция постепенно развивалась. Ей посвящали статьи как в специализированных научных (Journal of Information Systems, Computer, RFID Journal), так и научно-популярных изданиях (Wired, Scientific American), бизнес-журналах и СМИ (Forbes, Harvard Business Review, Guardian, Boston Globe, New York Times Magazine). Росло число университетов, занимающихся данной тематикой. Интернетом вещей стали интересоваться консалтинговые и аналитические агентства, например, Accenture.

Практические шаги по применению IoT начались с 2003 года. На этапе своего зарождения концепция «Интернета Вещей» была тесно взаимосвязана с RFID-метками. Считается, что именно эта технология легла в основу всего направления; именно на ней К. Эштон сделал основной акцент в своей презентации концепции «Интернета Вещей». Поэтому, по инициативе компаний, самые первые шаги в сфере IoT были связаны с созданием стандарта, поддерживающего более широкое применение электронного кода продукта – EPC (Electronic Product Code) и RFID-меток в глобальном масштабе⁸. Для этих целей была создана сеть EPCglobal Network, а в сентябре 2003 г. – первая версия спецификаций данной сети. В то время «Интернет Вещей» воспринимался как динамично развивающаяся глобальная информационная архитектура на базе интернета, облегчающая обмен товарами и услугами в сетях цепочек поставок. Тогда же, в 2003 г., крупнейший ритейлер Walmart объявил о планах к 2005 году обязать сто своих ключевых поставщиков использовать на паллетах и ящиках RFID-метки [1.28] с перспективой в будущем распространить это требование на всех поставщиков. В результате такого шага продажи сверхвысокочастотных меток, используемых компанией,

⁸ Сеть EPCglobal Network управляется организацией Auto ID Centre – глобальным консорциумом ритейлеров и ученых, базирующемся в Массачусетском Технологическом Институте в Бостоне. Консорциум, основанный в 1999 году компаниями Gillette, Proctor & Gamble и Unilever, включает в себя 100 глобальных компаний, пять лидирующих в мире исследовательский центра, включая Университет Кембриджа и MIT.

выросли с 2 млн. шт. в 2003 г. до 120 млн. шт. в 2005 г. В денежном выражении рынок вырос с 1 млн. долл. до 20 млн. долл. [1.29]. Кроме того, в 2005 г. аналогичные требования к своим поставщикам предъявило Министерство обороны США. Бурный рост рынка RFID в 2005 году ознаменовал начало развития рынка IoT.

На данную тему обратили внимание и международные организации: в 2005 г. специализированное учреждение ООН — Международный союз электросвязи (МСЭ, International Telecommunication Union, ITU) — издал седьмую публикацию в серии отчетов, посвященных интернету, под заголовком «The Internet of Things» [1.26]. В отчете были показаны рыночные возможности, которые открывает интернет вещей, однако оценка рынка была дана только для технологии RFID. Для нее уже были установлены стандартизированные протоколы, и росло коммерческое применение. По данным МСЭ, мировой рынок RFID продуктов и услуг рос высокими темпами, и в 2004 г. составил 1,5–1,8 млрд. долл.

К другим технологиям интернета вещей этого поколения относятся межмашинные коммуникации и предложенная ETSI⁹ их архитектура, а также технологии интеграции RFID и беспроводных сенсорных сетей (WSN) в единый комплекс. Беспроводные сенсорные сети, однако, стали темой доклада МСЭ только в 2008 году [1.30].

⁹ Европейский институт по стандартизации в области телекоммуникаций (European Telecommunications Standards Institute, сокр. ETSI) – независимая, некоммерческая организация по стандартизации в телекоммуникационной промышленности (изготовители оборудования и операторы сетей) в Европе. Официально признан Европейским союзом (EU) и Европейской ассоциацией свободной торговли (EFTA) в качестве компетентного органа по стандартизации в указанных областях. Задачей Европейского института телекоммуникационных стандартов является поиск общих стандартов, на основе которых можно создать единую структуру электросвязи. ETSI успешно стандартизировал систему сотовой связи GSM и систему профессиональной мобильной радиосвязи TETRA. ETSI является одним из создателей 3GPP. В организацию входят более 800 членов из 66 стран.

Изначальную сфокусированность на RFID–метках можно объяснить недостаточным распространением в то время беспроводных сетей и отсутствием стандарта конфигурации мобильных протоколов. В свою очередь, технология RFID не требовала использования IP или прямого подключения к интернету для каждого устройства, поэтому это решение воспринималось как более дешевое и проще реализуемое, несмотря на появлявшиеся попытки выпустить продукты, подключенные к интернету через IP протокол¹⁰.

После отчета МСЭ в развитие интернета вещей постепенно стали включаться разные страны и отраслевые объединения. В 2006 г. первые шаги предпринял Европейский союз. Несмотря на то, что Европейская комиссия (ЕК) также сфокусировалась на технологии RFID, стал обсуждаться и вопрос перехода к более масштабному «Интернету Вещей». Первые конференции по RFID, проведенные Европейской комиссией, назывались «От RFID к интернету вещей» (март 2006 года) и «RFID: на пути к интернету вещей» (2007 год) [1.31]. Однако рынок все еще измерялся в количестве проданных RFID–меток. По данным ЕК, в 2006 г. объем рынка в физическом выражении составил 1,02 млрд. меток. Основными областями применения были транспорт и логистика, контроль доступа, локализация в режиме реального времени, управление цепями поставок, производство и переработка, сельское хозяйство, здравоохранение и фармацевтика [1.32].

В тот же период времени Китай активно включился в исследования в области «Интернета Вещей». Масштабные поддерживаемые государством проекты стали разрабатывать Шанхайский институт микросистем и информационных технологий (Shanghai Institute of Microsystem and Information Technology, SIMIT), Китайская Академия Наук (Chinese Academy of Sciences, CAS), Университет авиации и астронавтики г. Нанкин (Nanjing University of Aeronautics and Astronautics), Северо-западный политехнический университет Китая (North-western Polytechnical University of China).

¹⁰ Упомянутый выше подключенный холодильник LG был представлен в 2000 году и использовал LAN порт для связи по IP. По сути, в отсутствие облачных решений и распространённой сети беспроводной связи этот холодильник представлял из себя специфичный компьютер.

Исследования в этой области рассматривались правительством Китая как фактор экономического роста и возможность конкурировать с развитыми странами.

Тем не менее, по настоящему переломным моментом в развитии «Интернета Вещей» считается 2008 год [1.33], когда большинство разработчиков и визионеров приняли эту концепцию и увидели потенциал ее широкой реализации. В этом году произошло сразу несколько событий.

Во-первых, был сформирован Альянс IPSO (Internet Protocol for Smart Objects, интернет-протокол для «умных объектов») для усиления взаимодействия промышленных партнёров, заинтересованных в продвижении подключенных устройств. Среди основателей альянса были Cisco, SAP, Sun Microsystems, Swedish Institute of Computer Science, другие ведущие поставщики и пользователи технологии. Формирование альянса стало знаком того, что крупные корпорации стали проявлять растущий интерес к использованию IoT в своем производстве.

Во-вторых, через короткий промежуток времени после своего основания, альянс объявил о доступности uIPv6 – стека для IPv6 с открытым кодом, который позволял любому устройству получить IPv6 адрес.

В-третьих, Совет Европейского союза поддержал инициативы Европейской Комиссии в области «Интернета Вещей».

В-четвертых, в рамках разработки доклада для Национального совета США «Глобальные тренды 2025» агентство SRI Consulting Business Intelligence обозначило интернет вещей как одну из шести прорывных технологий, которые могут оказать значительное воздействие на экономическое развитие и военные позиции США [1.34].

В-пятых, тремя из семи академических исследовательских лабораторий, входящих в сеть Auto-ID Labs — Университетом Санкт-Галлена, Швейцарской высшей технической школой Цюриха (ETH Zurich) и MIT — в Цюрихе была организована и проведена первая научная конференция, посвященная IoT, в которой участвовали ведущие исследователи и практики из компаний и академии [1.35].

Европейская комиссия, расширяя свою деятельность в области IoT, в 2009 году разработала план, в котором интернет вещей рассматривался как новый этап в эволюционном развитии интернета [1.31, 1.36]. В 2010 г. Европейский союз учредил Европейский исследовательский кластер IoT. В тот же период времени правительство Китая начало проводить политику поддержки развития интернета вещей [1.37]: эта технология была включена в качестве стратегического приоритета в двенадцатый пятилетний план на 2011–2015 гг. [1.38]. Согласно плану, рынок интернета вещей в Китае к 2020 году должен вырасти до 163 млрд. долл. [1.39].

К 2010 г. по количеству публикаций по тематике IoT лидировал Китай (51,3% публикаций), и за ним следовала Европа (37,3%). Такие подсчеты, однако, не вполне корректны, поскольку в разных странах могли использоваться синонимы этого термина (всеобъемлющие вычисления, беспроводные сенсорные сети и т.д.) [1.40]. До сих пор наблюдается различие в использовании терминов: в Европе и Китае чаще упоминается «Интернет Вещей», а в США наибольшее применение нашли термины, содержащие слова «умный», «интеллектуальный». В развитии интернета вещей участвовала также Япония, для которой приоритетными были социально-значимые приложения: в здравоохранении, предсказании стихийных бедствий, в области сокращения выбросов парниковых газов, улучшения транспортной ситуации и др.

В 2011 году аналитическая компания Gartner включила технологию интернета вещей в свой Цикл зрелости технологии (Hype cycle); по их оценке, технология IoT должна была достигнуть пика завышенных ожиданий в 2014 году. Тогда же крупные компании (IBM, Cisco, Ericsson) запустили образовательные и маркетинговые инициативы по данной теме.

В 2012 г. стали возрастать государственные инвестиции. Правительство Китая учредило фонд поддержки интернета вещей в размере 775 млн. долл. Средства должны были направляться на строительство 10 промышленных парков по «Интернету Вещей» [1.41]. Что касается частных инвестиций, то по оценкам Deloitte University Press, на тот момент общий объем было сложно определить из-за неточности

определения IoT, но в своем отчете организация привела следующую оценку: в 2012 году венчурные фонды вложили более 750 млн. долл. в более чем 100 компаний в области IoT.

В 2013 году появились первые оценки мирового рынка IoT: исследовательская компания IDC выпустила доклад, в котором было заявлено, что к 2020 году рынок достигнет 8.9 трлн. долл. Чуть позже Business Insider Intelligence Research оценил физический объем рынка в 1.9 млрд. устройств [1.42].

Постепенно интернет вещей стал распространяться на массовый, потребительский рынок. Появились носимые устройства и фитнес-трекеры (например, компании Jawbone Up, Fitbit, Pebble), бытовая автоматизация (Nest, 4Control, Lixt), интеллектуальные счетчики энергии [1.43]. Промышленное применение развивалось не менее активно: например, выручка GE от промышленного интернета вещей составила в 2013 году 800 млн. долл. [1.44]. Кроме того, в 2014 г. такие технологические гиганты, как AT&T, Cisco, GE, IBM и Intel учредили Консорциум Промышленного Интернета (Industrial Internet Consortium, IIC) с целью создания инженерных стандартов для объектов IoT. В IIC также входят и правительственные агентства, которые совместно с частными компаниями разрабатывают решения в области государственных услуг.

Приведенные выше примеры указывают на то, что, в отличие от ЕС и Китая, в США интернет вещей развивался в большей мере благодаря активной деятельности частных компаний: инициативы бизнес-сектора позволяли США быстро продвигаться с практическими применениями IoT. В ЕС отраслевое объединение появилось только в 2015 году: Альянс по инновациям в области интернета вещей (The Alliance for Internet of Things Innovation, AIOTI) был основан по инициативе Европейской Комиссии для развития экосистемы IoT в Европе [1.45].

Распространению и росту разнообразия IoT-приложений способствовало несколько сопутствующих технико-технологических факторов:

- взрывной рост числа подключенных устройств и приложений и широкая доступность беспроводной связи. По отчету Cisco (2011 г.), если в 2003 году было около 500 млн. устройств, подключенных к интернету, то к 2010 году в результате появления планшетов и смартфонов количество подключенных устройств выросло до 12,5 млрд. Таким образом, всего за 7 лет количество подключённых устройств на одного человека выросло в 2,25 раза – с 0,8 до 1,8;
- снижение стоимости сенсоров. Сенсоры являются одним из важнейших элементов развития интернета вещей. На протяжении XX века высокая стоимость ограничивала их использование премиальными сегментами рынков. Однако в последние десятилетия стоимость сенсоров стремительно снижается. Например, в начале 1990–х стоимость твердотельных датчиков изображения (solid-state image sensors) составляла 20–25 долларов; к концу десятилетия она снизилась до 5 долларов. Стоимость других сенсоров, которые обычно используются в смартфонах, следовала аналогичному тренду: в 2007 году акселерометры (датчики ускорения) стоили около 7 долларов и измеряли движение только по одной оси, в 2015 году они стоили уже 0.5 доллара и при этом могли измерять движение по шести осям [1.46];
- широкомасштабное внедрение инструментов анализа «Больших Данных», которые позволяют обрабатывать информацию, снимаемую с огромного числа подключенных IoT устройств. Одновременно с этим – появление и широкое распространение облачных решений;
- создание стандартов: в 2012 году МСЭ утвердил первые, базовые рекомендации в области IoT – Y.2060 «Обзор интернета вещей» [1.11]; в 2015 году образована 20–я Исследовательская комиссия МСЭ–Т – «IoT и его приложения, включая “умные” города и сообщества (SC&C)». Среди других организаций, работающих над разработкой стандартов в области IoT – стартовавший в 2012 г. по инициативе шести региональных органов стандар-

тизации (ETSI, ARIB, TTA, CCSA, TTA и TTC) партнерский проект oneM2M с американской Ассоциацией ATIS. Есть также партнерский проект 3GPP (SA, RAN, GERAN), занимающийся развитием сетей мобильной связи.

Таким образом, концепция «Интернета Вещей» сильно эволюционировала, и началось развитие практических приложений. В немалой степени на эти процессы оказало влияние развитие технологий. Если на первоначальном этапе IoT ассоциировался в большей степени с технологиями RFID, то впоследствии акцент сместился в сторону решений, позволяющих наделить объекты функцией прямого выхода в интернет. Одновременно развивался новый подход к разработке web-приложений, что стало причиной скачка в развитии интернета вещей и началом эры «Веба Вещей», где данные с умных вещей или управление ими должно быть доступно через WWW-страницы [1.5].

Интернет вещей распространился от узких отраслевых решений до приложений практически во всех сферах. Многогранность «Интернета Вещей» проявляется во всех сегментах рынка. Для потребителя IoT обозначает носимые технологии и умные приборы, такие как термостаты и телевизоры. В промышленном секторе – автономность машин и оборудования. В бизнес-среде основной акцент сделан на анализ больших данных и маркетинговую аналитику в реальном времени. Наконец, расширяется применение интернета вещей и в секторе государственных услуг.

1.3 Динамика рынков интернета вещей¹¹

1.3.1 Глобальный рынок

1.3.1.1 Динамика объемов рынка

Методы оценки рынка «Интернета Вещей» менялись вместе с эволюцией трактовки этого явления. Если изначально рынок измерялся количеством проданных RFID-меток или подключенных к интернету устройств, то в дальнейшем стали появляться оценки интернета вещей как совокупности различных технологий, продуктов и услуг,

¹¹ Дежина И.Г. (Сколтех), Нафикова Т.Н. (Сколтех)

реализуемых за счет коммуникаций между виртуальными и физическими объектами без участия человека. Поскольку до сих пор нет единой методологии и консенсуса по поводу того, какие технологии, продукты и услуги входят в данную совокупность и что именно следует относить к рынку интернета вещей, то и оценки масштабов распространенности этого явления, как и его характеристик, сильно варьируются. То же касается текущего объема рынка и его прошлой динамики. Так, по данным, приводимым компанией Gartner, глобальный объем рынка IoT в 2017 году должен был составить почти 2 трлн. долл. [1.47], согласно IDC – 674 млрд. долл. [1.48], MarketsandMarkets – 639,7 млрд. долл. [1.49]. При этом есть компании, которые за последние годы кардинально изменили свою оценку рынка IoT. В частности, это аналитическая компания IDC, которая в 2013 г. оценивала рынок в 1,9 трлн. долл. с перспективой роста к 2020 г. до 7,1 трлн. долл. [1.50]. В 2014 г. объем рынка уже оценивался в 655,8 млрд. долл. с прогнозом роста до 1,7 трлн. долл. в 2020 г. [1.51], то есть в 4 раза ниже прогноза предыдущего года. В 2017 г. потенциальный объем рынка к 2020 году был оценен только в 1 трлн. долл. В 2014 г. среднегодовые темпы прироста в 2014–2020 гг. (CAGR) оценивались в 20%, в 2018 г. аналитики IDC ожидают CAGR на период 2017–2022 гг. только в 13,6% [1.52]. Это, вероятно, связано с прохождением пика завышенных ожиданий, который был в 2014 году. Динамика оценок рынка IoT по данным Gartner и IDC¹² представлена на Рис. 1.7.

¹² Для IDC использованы наиболее актуальные данные для каждого года, имеющиеся в открытом доступе.

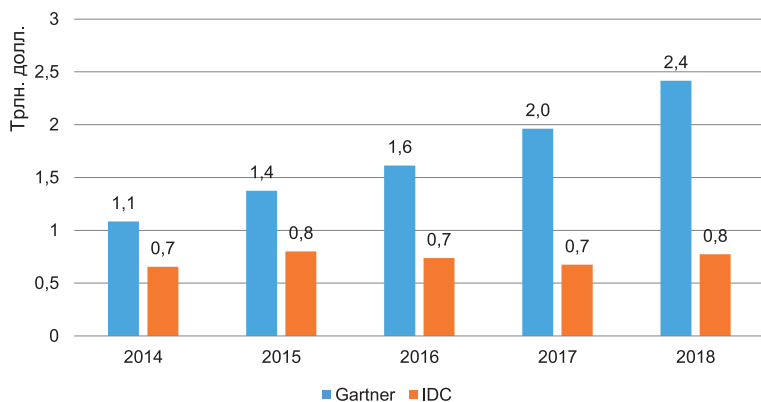


Рисунок 1.7 — Мировой рынок интернета вещей, 2014–2018 гг., трлн. долл.

Источник: рассчитано и составлено авторами по данным Gartner [1.47, 1.53] и IDC [1.48, 1.52, 1.54–1.56].

Существенная вариация в показателях характерна и для данных об объеме рынка IoT в физическом выражении. По данным компании Gartner объем рынка в 2014 г. составлял 3,8 млрд. подключенных устройств, а IDC оценила его в 10,3 млрд. устройств. Тем не менее, со временем, оценки прошлых лет, как правило, начинают колебаться в более узком диапазоне, но для текущих оценок рынка все еще характерна более значительная вариация показателей, как это видно из Рис. 1.8.

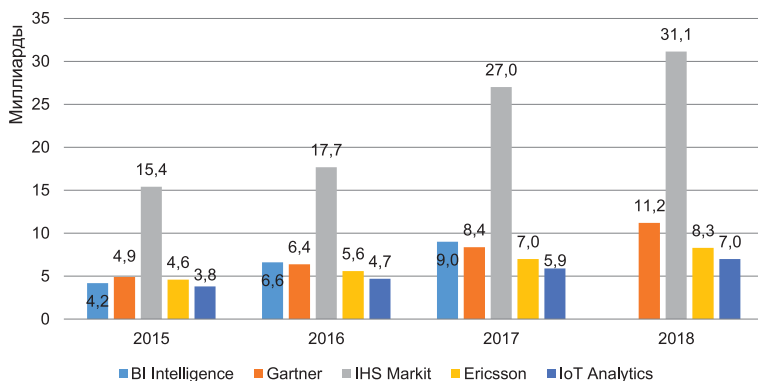


Рисунок 1.8 — Мировой рынок интернета вещей, 2014–2018 гг., млрд. устройств.

Источник: составлено авторами по данным BI Intelligence [1.57–1.59], Gartner [1.47, 1.53], IHS Markit [1.60–1.62], Ericsson Mobility Report [1.63–1.65], IoT Analytics [1.66].

Значительное превышение значений показателей, предоставляемых IHS Markit, может быть связано с методологией расчета IoT устройств, при которой учитываются подключенные устройства, такие как мобильные телефоны, ноутбуки, планшеты, компьютеры и фиксированные телефоны. В то же время Ericsson в своих расчетах выносит их в отдельную категорию и не учитывает в общем количестве. С учетом этих различий результаты Ericsson и IHS Markit практически совпадают: в 2017 году Ericsson насчитывал 17,5 млрд. подключенных устройств, IHS Markit – 17,7 млрд.

Однако прогнозы сильно различались не только в прошлом: и сегодня аналитические агентства и компании по-разному видят будущее развитие IoT (Рис. 1.9 и Рис. 1.10).

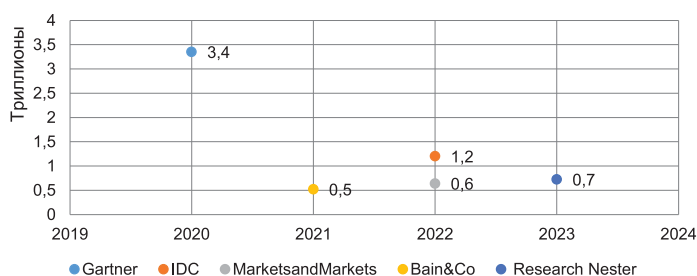


Рисунок 1.9 — Прогнозы роста мирового рынка интернета вещей в денежном выражении, трлн. долл.

Источник: составлено авторами по данным Gartner [1.47], IDC [1.52], MarketsandMarkets [1.49], Bain&Company [1.67], Research Nester [1.68].

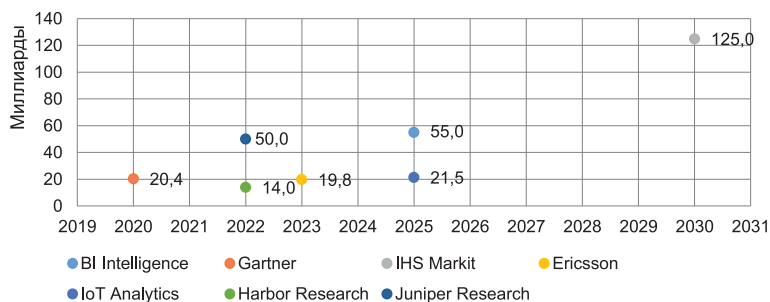


Рисунок 1.10 — Прогнозы роста физического объема мирового рынка интернета вещей, млрд. шт.

Источник: составлено авторами по данным BI Intelligence [1.59], Gartner [1.47], IHS Markit [1.61], Ericsson Mobility Report [1.65], IoT Analytics [1.66], Harbor Research [1.69], Juniper Research 1.70].

Среди причин большой вариации прогнозов изменения рынка IoT, а также сильного колебания оценок эксперты выделяют следующие:

- различия в методологии. Данная причина имеет два аспекта. Во-первых, это связано с использованием различных определений «Интернета Вещей», и значит

и его компонентов. Во-вторых, сказывается применение разных подходов к оценке. Это либо моделирование сверху вниз – то есть на уровне отраслей, либо снизу-вверх, когда определяются отдельные сценарии и направления использования IoT (характерно для компаний из сферы бизнеса и промышленности);

- изменение технологического ландшафта. Интернет вещей включает в себя значительное число различных технологий, поэтому тренды, касающиеся отдельных технологий, входящих в общий технологический стек IoT, могут оказывать сильное влияние на динамику рынка. Кроме того, различные организации по-разному видят перспективы развития той или иной технологии. Наконец, многие категории «вещей», которые появятся в будущем, сейчас не существуют и ожидания по возникновению новых типов продуктов тоже усиливают вариацию оценок рынка;
- не оправдывающиеся высокие ожидания по развитию потребительского сектора интернета вещей. На ранних этапах развития рынка IoT большие надежды возлагались на его расширение именно в потребительском секторе. Это было связано с двумя гипотезами: подключение «вещи» к интернету должно повысить ее привлекательность в глазах потребителей и, во-вторых, облегчение производства устройств IoT должно было привлечь большее число предпринимателей, которые могли бы воспользоваться стандартными компонентами, возможностями 3D печати, свободного программного обеспечения. Однако обе эти гипотезы не вполне оправдались. Кроме того, жесткая конкуренция со стороны крупных компаний затруднила развитие стартапов в этой области;
- заинтересованность организаций, выпускающих аналитические отчеты по оценке рынка, в достижении тех или иных показателей, их субъективность. Субъективность, в частности, связана с разностью в оценках бизнес- и регуляторных рисков, способных оказать существенное влияние на развитие рынка IoT.

Переоценка в сторону более низких темпов роста может быть связана с негативными трендами, которые проявляются в последние 1–1,5 года: по данным анализа Cisco, почти 75% проектов интернета вещей провалились [1.71]. Кроме того, ажиотаж вокруг интернета вещей немного спал после развития технологии блокчейна и искусственного интеллекта.

1.3.1.2 Инвестиции в IoT

Несмотря на ряд не оправдавшихся ожиданий, инвестиции в развитие технологий «Интернета Вещей» пока растут. По данным BI Intelligence, в период с 2017 г. по 2025 г. общий объем должен составить 15 трлн. долларов. При этом, по данным проведенного этой компанией опроса, в 2017 г. бизнес-сектор планировал увеличить инвестиции в ближайшие 5 лет (Рис. 1.11).

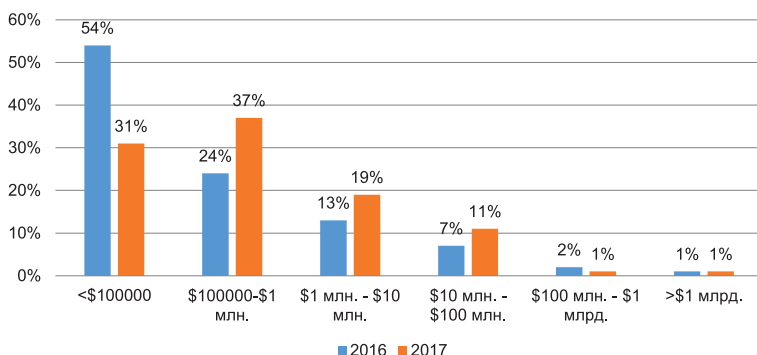


Рисунок 1.11 — Планы компаний по инвестированию в IoT на период 2017–2022 гг. (% от числа опрошенных)

Источник: [1.59]

Аналогичная тенденция характерна и для рынка венчурных инвестиций в IoT. Так, в США с 2014 г. венчурные фонды стали вкладывать значительные средства в IoT стартапы (Рис. 1.12).



Рисунок 1.12 — Венчурные инвестиции в IoT, млрд. долл., США, 2007–2016 гг.

Источник: [1.72]

Согласно данным на Рис. 1.12, до 2016 г. американские фонды последовательно наращивали инвестиции в IoT-стартапы. Примечательно произошедшее в 2016 г. сокращение числа сделок на фоне роста инвестиций. Это связано с переходом многих стартапов на более зрелые этапы развития. В результате фонды вкладывались в меньшее количество стартапов, но на большие суммы.

Однако глобальные венчурные инвестиции в IoT, по данным CB Insights, в 2017 г. несколько снизились (на 1,6% от уровня предыдущего года) и составили 3,77 млрд. долл. [1.73]. Аналитики связывают данное падение с процессами, проходящими на рынке технологий интернета вещей. По мере его развития более крупные, консолидированные инвестиции направляются в меньшее количество компаний, обычно находящихся на стадии роста. Как и в случае рынка США, это подтверждается резким сокращением (на 37,9%) числа сделок в 2017 г. по сравнению с предыдущим годом (295 сделок против 475). Сокращаются инвестиции в более ранние стадии развития: в 2016 г. посевные инвестиции и инвестиции раунда А составляли 73% от общего числа сделок, а в 2017 г. доля этих сделок в общем числе составила лишь 53%, и было мало выходов на IPO. Такие тенденции могут свидетельствовать о наступлении периода зрелости рынка. Данный вывод коррелирует со снижением прогнозных ожиданий роста рынка IoT в финансовом и физическом выражении.

1.3.1.3 Экономические эффекты

При оценке развития интернета вещей рассматривают не только объем рынка в физическом и денежном выражении, но также и экономическую ценность, создаваемую новыми технологиями. Измерение этого показателя еще более неоднозначно, так как нет общепринятого понятия «ценность». Так, Cisco формулировала это как «ценность, поставленную на карту», McKinsey как «потенциальную экономическую ценность», General Electric (GE) – «потенциальный глобальный ВВП для промышленного интернета», Gartner – «глобальную экономическую добавленную стоимость».

Большинство оценок измеряет ценность, которая будет создана в определенный год в будущем. В 2013 г. Gartner прогнозировал, что добавленная стоимость IoT¹³ в 2020 г. составит 1,9 трлн долл. [1.74]. Cisco представила агрегированную оценку на период 2013–2023 гг.: совокупная созданная ценность за этот период должна составить 19 трлн долл. Наиболее проработанную оценку диапазона влияния технологий IoT на экономическое развитие дает McKinsey Global Institute. Прогноз включает анализ различных сфер применения. По максимуму, потенциальный экономический эффект может составить \$11,1 трлн. в год; при этом IoT будет более значимым источником ценности по сравнению с другими прорывными технологиями (Рис. 1.13).

¹³ Совокупные выгоды, получаемые компаниями, за счет продажи и использования технологий IoT. Состоит из двух частей – зрелые IoT-решения, из которых уже можно извлекать выгоды, и быстрорастущие развивающиеся IoT-решения.

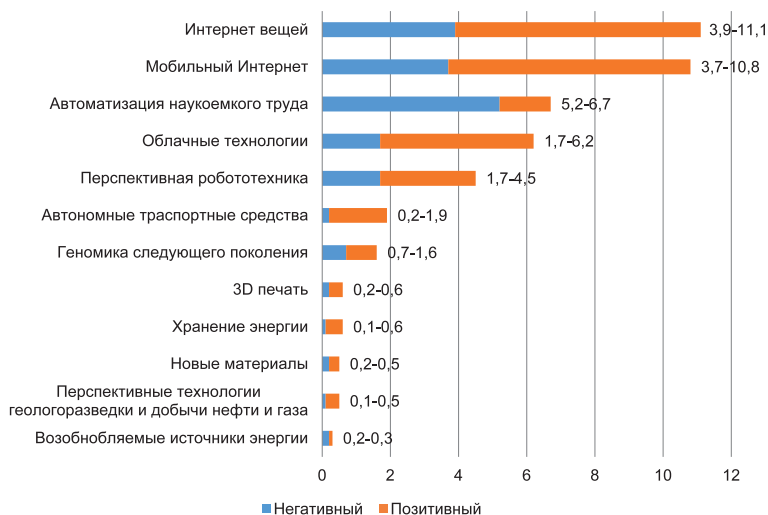


Рисунок 1.13 — Экономический эффект прорывных технологий к 2025 г., трлн. долл.

Источник: [1.75]

McKinsey вычисляет экономический эффект на основе трех компонентов: затраты на решения IoT, потребительская ценность IoT и профицит потребителя¹⁴. По их оценкам, потенциальная доля прямых затрат на интернет вещей в общем экономическом эффекте сократится с 15% в 2015 г. до 7% в 2025 г. (Рис. 1.14). Основной причиной такой динамики представляется высокая конкуренция поставщиков решений интернета вещей по всей цепочке создания стоимости.

¹⁴ McKinsey не раскрывает определение понятия «профицит потребителя», однако скорее всего имеется в виду разница между той суммой денег, которую потребитель был бы согласен уплатить, и той суммой, которую он реально уплатил.

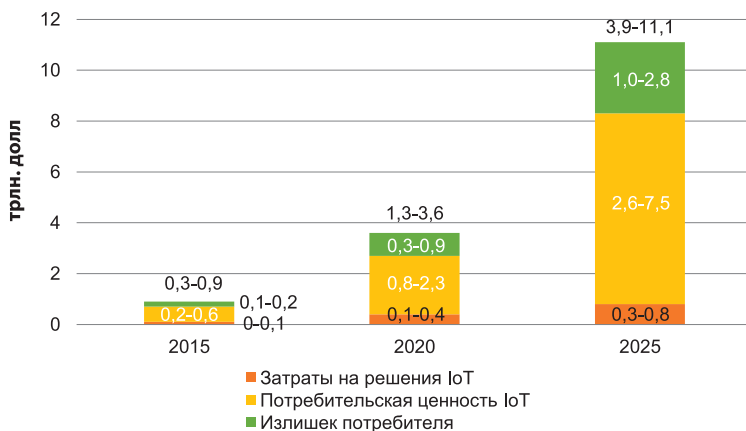


Рисунок 1.14 — Динамика компонентов экономического эффекта от IoT в 2015–2025 гг., трлн. долл.

Источник: [1.75]

По версии McKinsey, основными источниками создания ценности станут применения технологий IoT на производственных площадках (до 3,7 трлн. долл.) и в городской среде (до 1,7 трлн. долл.), Рис. 1.15. В городской среде основными драйверами станут: оптимизация перевозок (800 млрд. долл.), повышение уровня общественной безопасности и системы общественного здравоохранения (700 млрд. долл.), более эффективное управление ресурсами. При сравнении секторов ясно прослеживается, что большая ценность создается в B2B приложениях – на них приходится 2/3 создаваемой в результате инвестиций ценности в IoT. Потребительский сектор может усилить свои позиции в результате подключения потребительских устройств к B2B системам.

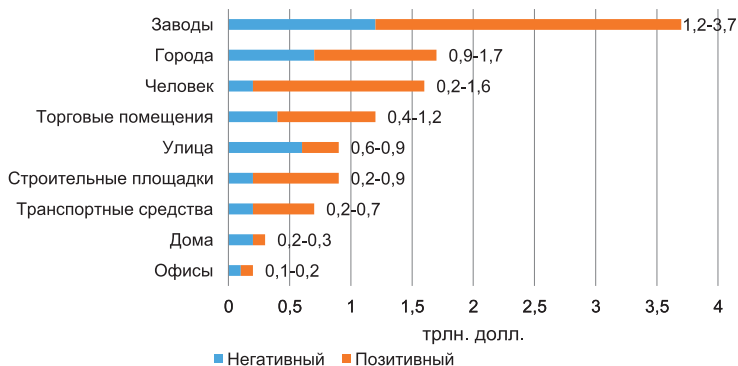


Рисунок 1.15 — Экономический эффект от внедрения IoT в различных физических средах, 2025 г., трлн. долл.

Источник: [1.75]

1.3.2 Технологическая структура рынка интернета вещей

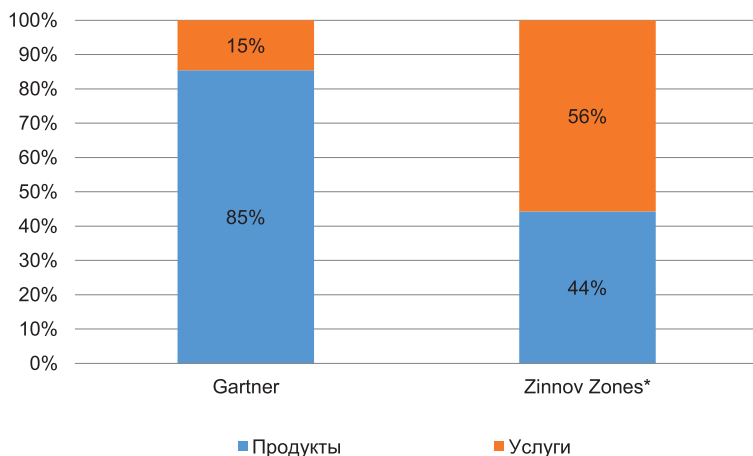
При анализе рынка с точки зрения технологий и продуктов, интернет вещей естественно рассматривать на основе входящих в него технологических и инфраструктурных слоев. При этом аналитические и консалтинговые компании используют разную сегментацию рынка по продукту.

Некоторые компании, такие как Gartner и Zinnov Zones, ограничиваются укрупненными группами – продукты и услуги. IDC, кроме устройств IoT и услуг, выделяет в отдельные сегменты программное обеспечение и каналы связи. BCG рассматривает еще более детальную сегментацию: услуги, приложения IoT, IoT аналитика, идентификация и безопасность, опорные элементы IoT (облако и платформа), связь, подключенные устройства. MarketsandMarkets делят рынок на узловые компоненты, сетевую инфраструктуру, программное обеспечение, платформы и услуги.

По данным Gartner, в 2017 г. на устройства IoT было потрачено 1,7 трлн. долл., тогда как сегмент услуг (профессиональные, потребительские и услуги связи) оценивался в 273 млрд. долл. Ключевыми на рынке в данный момент являются

именно профессиональные услуги по разработке, внедрению и поддержке IoT-систем, однако потребительские услуги и услуги связи растут более быстрыми темпами. Рост рынка услуг связи связан с падением издержек и появлением новых областей применения [1.47].

Zinnov Zones оценивает только затраты бизнес-сектора, поэтому оценки сильно отличаются от данных Gartner: в 2017 г. объем сегмента «Продукты» составил 62 млрд. долл., услуг – 78 млрд. долл. [1.76]. Кроме того, критическое отличие состоит в оценке объема рынка продуктов. Это связано с тем, что Zinnov Zones не учитывает потребительский сектор, и использует другой подход к определению структуры сегментов. Аналитики Zinnov Zones рассматривают только элементы, которые наделяют «вещи» необходимым функционалом. Это сенсоры, микроэлектромеханические системы, актуаторы и т.д. Gartner в своем исследовании отталкивается в большей степени от оценки стоимости подключенных устройств в целом. Поэтому структура рынка по версиям этих двух агентств выглядит по-разному (Рис. 1.16).



*Только бизнес-сектор

Рисунок 1.16 — Технологическая структура мирового рынка IoT в денежном выражении, 2017 г.

Источник: составлено авторами по данным [1.46], [1.75]

Таким образом, если в объемах сегментов рынка учитывается потребительский сектор, доля устройств и оборудования значительно вырастает из-за включения в оценку стоимости конечных устройств массового использования.

По данным IDC, в 2018 г. наиболее крупным сегментом рынка по продукту станут «устройства и оборудование» – 239 млрд. долл. (31% рынка), большая часть придется на модули и сенсоры. Вторым по размеру сегментом рынка являются услуги, затем следуют программное обеспечение и каналы связи. При этом ожидается, что к 2021 г. объем рынка услуг практически сравняется с таковым для устройств и оборудования. Сегменты рынка «программное обеспечение» и «услуги», на которые суммарно к 2021 г. придется более 55% рынка, будут расти более быстрыми темпами, чем рынок в целом – CAGR составит 16,1% и 15,1% соответственно. Программное обеспечение (куда входят такие решения, как программные приложения, аналитическое ПО, IoT платформы и ПО безопасности) будет самым быстрорастущим технологическим сегментом рынка [1.47].

Еще более детальное рассмотрение предлагает BCG, которая вводит более узкие сегменты рынка программного обеспечения. В дополнение к услугам, устройствам и каналам связи BCG рассматривает приложения IoT, IoT аналитику, идентификацию и безопасность, и опорные элементы IoT (облако и платформа). На них в 2015 г. в совокупности приходилось 32% рынка (Рис. 1.17). Таким образом, в 2015 г. самую большую долю рынка занимали подключенные устройства, затем следовало ПО, размеры рынков услуг и каналов связи был одинаковым. В программном обеспечении наиболее крупным подсегментом были программные приложения IoT (17%). По прогнозам на 2020 г. структура должна претерпеть значительные изменения: благодаря высоким темпам роста (CAGR более 40%) на первый план выйдет программное обеспечение (46% рынка), внутри которого наибольший объем также придется на приложения IoT (24%). Второе место по объему займут услуги (24% рынка). Подключенные устройства, которые в 2015 г. занимали большую часть рынка, станут к 2020 г. лишь третьим по объему сегментом с долей в 20%. Доля рынка каналов связи сократится на 7 процентных пунктов.

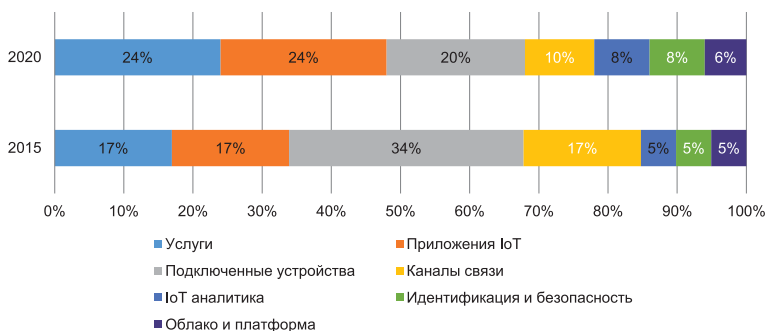


Рисунок 1.17— Технологическая структура мирового рынка IoT в 2015 г. и 2020 г., по оценкам BCG

Источник: составлено авторами по данным [1.77]

1.3.3 Отраслевой срез

Существует несколько подходов к оценке рынка интернета вещей по сфере применения. Они отличаются уровнем агрегирования и способами определения потребителя:

- сегментация рынка по пользовательскому сценарию представляет наименьший уровень агрегирования; сегменты определяются с точки зрения стоящих перед потребителями задач, на решение которых направлен тот или иной сценарий;
- сегментация по отраслевому принципу относится к среднему уровню агрегирования и определяет потребителя по его принадлежности к какой-либо отрасли экономики;
- сегментация по типу субъекта экономической деятельности определяет потребителя по секторам экономики (государство, компании, домохозяйства).

Большинство оценок рынков-потребителей попадают в одну из перечисленных выше категорий. Многие аналитики рассматривают одновременно и пользовательские сценарии, и отрасли, группируя сценарии по отдельным отраслям, или, наоборот, устанавливая, в каких отраслях используется определенный сценарий. Такой подход, например, харак-

терен для Machina Research¹⁵. Эта компания выделяет 200 сценариев, которые затем группируются в 58 категорий по 8 отраслям (секторам) – Автомобиль, Города, Здоровье, Промышленность, Дом, Бизнес, Энергетика, Потребительская электроника. Компания IoT Analytics на основе анализа 1600 приложений выделяет 10 отраслей: Умный город, Подключенная промышленность, Подключенное здание, Подключенный автомобиль, Умная энергетика, Мобильная медицина, Интеллектуальные цепочки поставок, Умное сельское хозяйство, Умная торговля и Другое. В свою очередь IDC выделяет 100 пользовательских сценариев и 20 вертикальных отраслей.

Различия связаны с характером внедрения и воздействия технологий интернета вещей на структуру рынков: в одних случаях эти решения остаются в рамках одной вертикальной отрасли, а в других IoT решения затрагивают сразу несколько отраслей, тем самым создавая предпосылки для появления новых, кросс-индустриальных рынков. Таким образом, отраслевая сегментация подразумевает либо отраслевые приложения интернета вещей в разбивке по традиционным отраслям, либо межотраслевые приложения.

Традиционные отрасли, как правило, соответствуют классификаторам видов деятельности по отраслям на национальном и международном уровнях. В России в Общероссийский классификатор видов экономической деятельности (ОКВЭД) входит 88 классов видов деятельности, распределенных по 21 разделам. На международном уровне известны, например, Международная стандартная отраслевая классификация всех видов экономической деятельности (МСОК; ISIC - International Standard Industrial Classification of All Economic Activities), разработанная ООН (является прототипом ОКВЭД); Глобальный стандарт классификации отраслей (ГСОК, Global Industry Classification Standard, GICS), разработанный MSCI и Standard & Poor's. Эти классификации предлагают наиболее полный и детальный перечень отраслей

¹⁵ В 2016 году Machina Research, компания —мировой лидер в области изучения межмашинных коммуникаций, интернета вещей и Больших данных, была приобретена аналитической компанией Gartner.

экономики. Однако, не все отрасли являются сферами применения интернета вещей и имеют соответствующий ему сегмент в своей структуре, поэтому применение данных классификаций огрубляет получаемые результаты. Кроме того, для удобства анализа некоторые отрасли объединяются в группы. Соответственно, в исследованиях рынка IoT используется более узкий перечень отраслей.

Второй вариант квази-отраслевой классификации появился как следствие возникновения новых, «умных», отраслей: Умный город, Умный дом, Умные сети, Умный транспорт, Умные здания, Умное освещение и т.д. И в данном случае нахождение оптимального уровня агрегирования является проблемой, так как умным может быть и город целиком, и, в то же время, отдельная муниципальная услуга – например, паркинг. В том, что касается «умных» объектов, в целом нет консенсуса касательно их содержания, границ и взаимосвязи. Так, в концепцию «Умного города» некоторые исследователи включают другие «умные» объекты – Умный дом, Умные сети, Умные транспортные системы и др. Как следствие, классификации, предлагаемые на данной основе не системны, и часто включают в себя не кросс-индустриальные сегменты, а «умные» сегменты традиционных отраслей. Например, IoT Analytics строит сегментацию, опираясь на понятия «умных» и «подключенных» решений различной степени агрегации, но в этой сегментации действительно кросс-индустриальными, на наш взгляд, являются только Умный город и Умный дом. Остальные «отрасли» – это новые сегменты традиционных отраслей – промышленного производства, строительства, энергетики, транспортировки и хранения, сельского хозяйства. При определении кросс-индустриальных отраслей, вероятно, стоит отталкиваться от тех систем, в рамках которых протекает личная, социальная и экономическая деятельность. С этой точки зрения можно выделить следующие среды:

- городское пространство – Умный город;
- общественные помещения – Умное здание (Smart Building);
- жилые помещения – Умный дом (Smart Home);

- промышленное производство – Умное производство;
- предприятия сельского хозяйства – Умная ферма.

Соотношение кросс-индустриальных сегментов с традиционными отраслями можно представить в виде матрицы (Таблица 1.4).

Таблица 1.4— Матрица сфер применения интернета вещей

	Сельское хозяйство	Нефтегазовая промышленность	Химическая промышленность	Фармацевтика и биотехнологии	Потребительские товары	Производство г/средств	Энергетика	Водоснабжение	Утилизация отходов	Строительство	Торговля	Транспортировка и хранение	Гостиничный бизнес	Общественное питание	Банковские, финансовые услуги и страхование	Коммерческие и профессиональные услуги	Госуправление и обеспечение безопасности	Образование	Здравоохранение	Социальные услуги	Культура, спорт, досуг и развлечения
Умный город																					
Умный дом																					
Умное здание																					
Умное производство																					
Умная ферма																					
Умное транспортное																					

Источник: составлено авторами

Разумеется, матрица может выглядеть и иначе – все зависит от того, какие границы определяются для той или иной среды. Поэтому при изучении отраслевой структуры рынка IoT сложно определить точный перечень входящих в нее отраслей.

Ниже рассматриваются некоторые оценки сегментов рынка по применению.

Консалтинговая компания BCG провела анализ сегментов рынка интернета вещей как в отраслевом разрезе (Рис. 1.18), так и с позиции пользовательских сценариев (Рис. 1.19).

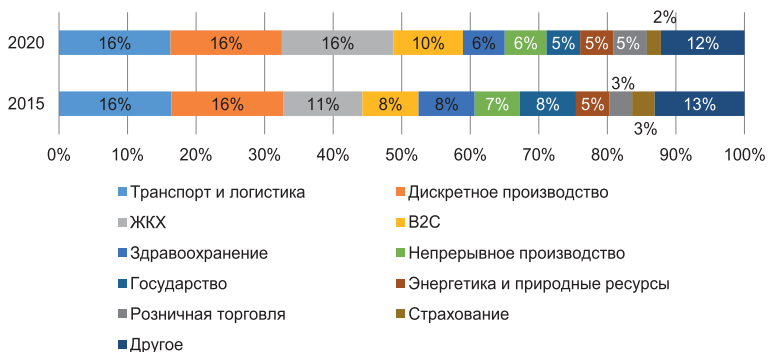


Рисунок 1.18— Отраслевая структура рынка интернета вещей в 2015 и 2020 гг. (в денежном выражении)

Источник: составлено авторами по данным [1.77]

Компания BCG сегментировала рынок в разрезе традиционных отраслей. Соответственно, наиболее крупными отраслями–потребителями решений интернета вещей, по ее оценкам, стали дискретное производство, транспорт и логистика, и коммунальные услуги; в 2020 г. на эти три сегмента придется около половины рынка.

Среди основных потребительских сценариев аналитики BCG выделяют следующие: предиктивное обслуживание, автоматическая оптимизация производства, автоматическое управление товарно–материальными запасами (ТМЗ), удаленный мониторинг состояния пациентов, умные счетчики, система учёта движения, распределенная генерация и хранение энергии, подключенный автомобиль, управление транспортным парком, управление спросом. Эти потребительские сценарии были выбраны из длинного перечня возможных по двум критериям: перспектива быстрого достижения зрелости и рыночный потенциал. На Рис. 1.19 представлено, как каждый из сценариев был оценен по этим двум параметрам, а также в каких отраслях эти сценарии находят свое применение. Так, наиболее зрелым решением является управление спросом – сегмент, который должен достичь зрелости в 2018–2019 гг., однако по потенциальному объему рынка он уступает всем остальным. Основная отрасль

для применения IoT– жилищно–коммунальные услуги. Наиболее крупным сегментом рынка по прогнозам станет предиктивное обслуживание, которое используют сразу в пяти отраслях —дискретное производство, транспорт и логистика, ЖКХ, здравоохранение и непрерывное производство. Этот сегмент рынка достигнет зрелости в среднесрочной перспективе. Вторым по объему рынка будет автоматическая оптимизация производства. Наименее зрелым является рынок удаленного мониторинга состояния здоровья пациентов.

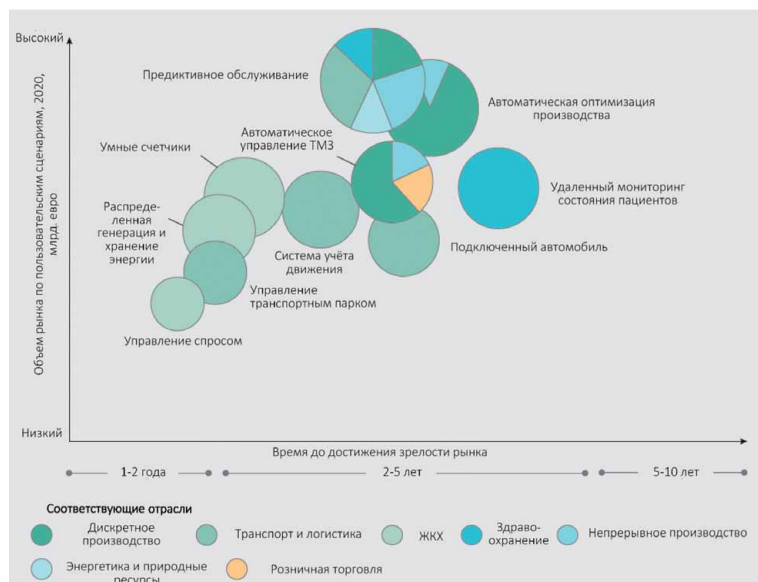


Рисунок 1.19— Тренды развития отраслевых сегментов рынка по 10 ключевым потребительским сценариям интернета вещей, 2015–2020 гг., млрд. евро.

Источник: [1.77]

Компания IDC также оценивает рынки в разрезе традиционных отраслей. По данным компании, в 2018 г. наиболее крупными отраслевыми сегментами станут производство (189 млрд. долл., прирост 3,2% по сравнению с 2017 г.), транспорт (85 млрд. долл., без прироста рынка), коммунальные услуги (73 млрд. долл., прирост 10,6% по сравнению с 2017 г.), потребительский интернет вещей (62 млрд. долл.) При этом

по темпам роста потребительский сектор обгонит другие сегменты рынка — среднегодовой темп прироста (CAGR) в 2017–2022 гг. составит 19%. В результате, по прогнозам IDC, потребительский сектор к 2021 г. станет третьим по объему для рынка IoT, после дискретного производства и транспортных услуг (объем каждого из этих двух сегментов рынка превысит 150 млрд. долл. к 2022 г.). Отдельно выделен кросс-индустриальный сегмент. Он включает общие для всех отраслей пользовательские сценарии, такие, как подключённые транспортные средства и умные здания. Объем этого сегмента в 2018 г. должен составить 92 млрд. долл. (прирост почти на 7% по сравнению с 2017 г.), уступая только производственному сектору.

Аналитики IDC также выделяют ключевые пользовательские сценарии для каждой из указанных отраслей. Наиболее распространенные сценарии для производства – поддержка производственных операций. Так, в сегменте транспорта 2/3 затрат направлены на мониторинг состояния грузов, вторым по частоте применения сценарием является управление транспортным парком. В сегменте коммунальных услуг доминирующим сценарием является использование умных сетей для передачи электричества, газа и воды. Для потребителей основные применения IoT связаны с умным домом – бытовая автоматизация, безопасность, умная бытовая техника. Наиболее перспективными пользовательскими сценариями аналитики IDC называют решения типа V2V (vehicle-to-vehicle, транспортное средство – транспортное средство) и V2I (vehicle-to-infrastructure, транспортное средство – инфраструктура) – их CAGR в 2017–2022 гг. составит 29% [1.52]. За ними следуют управление движением и безопасность подключенного автомобиля.

С иной отраслевой сегментацией работают аналитические компании IoT Analytics (Рис. 1.20) и GrowthEnabler (Рис. 1.21).

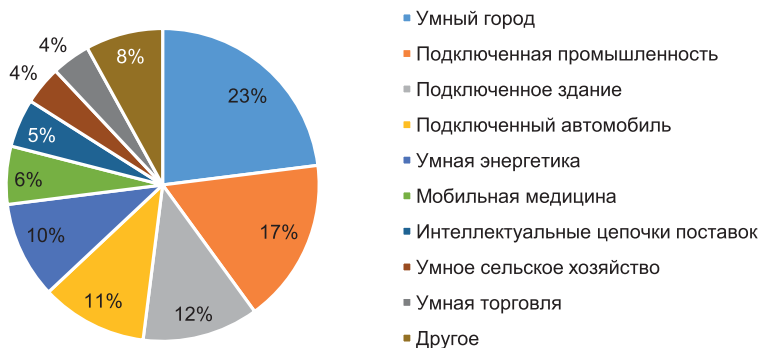


Рисунок 1.20—. Отраслевая структура рынка IoT, количество проектов, 2018 г.

Источник: [1.78]

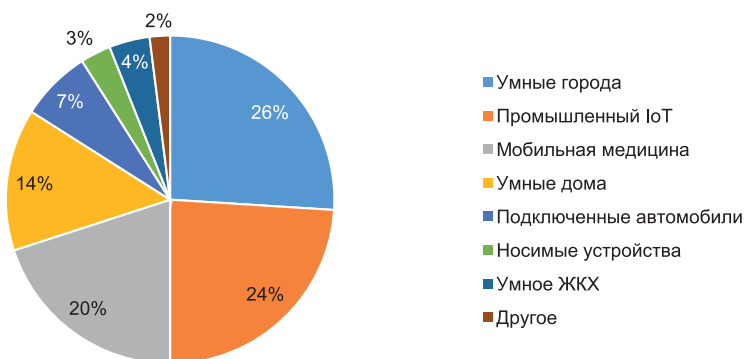


Рисунок 1.21— Отраслевая структура рынка IoT, денежная оценка, 2020 г.

Источник: [1.79]

Наконец, некоторые исследовательские организации рассматривают рынки применения IoT в еще более крупной сегментации – с точки зрения трех видов экономических субъектов (бизнес, домохозяйства/массовый рынок, государство). При этом зачастую игнорируется какой-либо один из трех секторов, или наоборот происходит дробление сектора на несколько подкатегорий. Например, бизнес-сектор может рассматриваться в двух проекциях – как сектор

вертикальных отраслей и межотраслевой. Такую сегментацию, в частности, приводит Gartner, как в денежном, так и в физическом выражении.

По данным Gartner, в 2016 г. в финансовом выражении доминирующим был бизнес-сектор, в структуре которого большую часть занимали вертикальные отрасли. Однако уже к 2021 г. ожидается, что потребительский сектор превысит по объему рынок B2B. При этом доля вертикальных отраслей значительно сократится (на 16,5 процентных пункта), а доля кросс-индустриальных применений в результате высоких темпов роста (самый высокий уровень CAGR среди трех секторов – 28%) вырастет на 4 п.п., до 19,4%, см. Рис. 1.22 и Рис. 1.23.

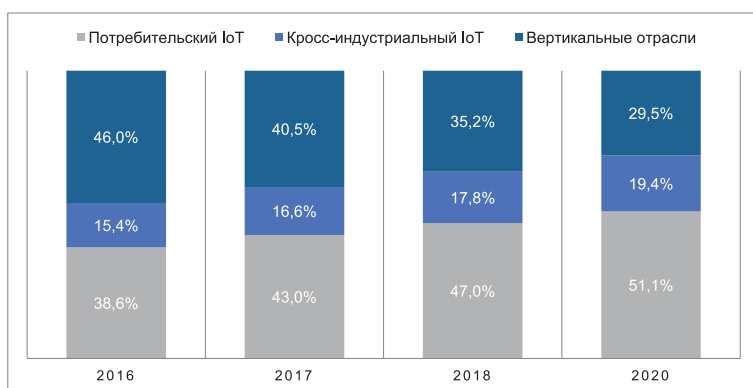


Рисунок 1.22— Отраслевая структура рынка IoT, денежная оценка, 2016–2020 гг.

Источник: составлено авторами по данным Gartner [1.47]

По параметру физического объема рынок интернета вещей на протяжении всех четырех лет прогноза имеет немного иную структуру: более 60% IoT устройств приходится на потребительский сектор. Различия наблюдаются и в динамике структуры. Несмотря на достаточно высокий CAGR в 34%, доля потребительского сектора будет возрастать медленно. Это связано с тем, что два других сектора будут расти быстрыми темпами, в особенности кросс-индустриальный, чей CAGR составит 41%. Доля вертикальных отраслей в физическом объеме также снизится.

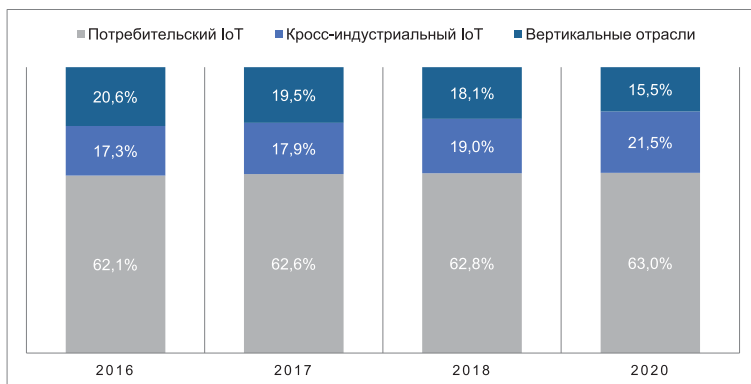


Рисунок 1.23— Отраслевая структура рынка IoT, физический объем, 2016–2020 гг.

Источник: составлено авторами по данным Gartner [1.47]

Избранные кейсы отраслевых применений IoT рассмотрены в третьем разделе данного отчета.

1.3.4 Географическая структура

Аналитическая компания MarketsAndMarkets назвала Северную Америку самым большим рынком IoT по состоянию на 2016 год. Причины успеха технологий IoT в этом регионе заключаются в развитой экосистеме информационных технологий и быстром внедрении IoT решений в различных областях. Однако уже по итогам 2016 г. стал прогнозироваться бурный рост рынков стран Азиатско-Тихоокеанского региона (АТР). Объясняется это действием четырех факторов. Первый—массивные инвестиции компаний, второй— растущий уровень проникновения интернета в различные среды, третий— большое число потенциальных потребителей IoT и четвертый – постоянный процесс совершенствования ИТ-инфраструктуры [1.49]. Соответственно, по оценкам IDC в 2018 г. самым большим рынком интернета вещей станет Азиатско-Тихоокеанский регион (без учета Японии). Его доля составит 40% от мирового рынка (Рис. 1.24). На страны Северной Америки и Европы придется 26% и 21% соответственно. Однако самые быстрые темпы роста будут наблюдаться в странах Латинской Америки: CAGR в 2016–2021 гг. составит 28,3%.

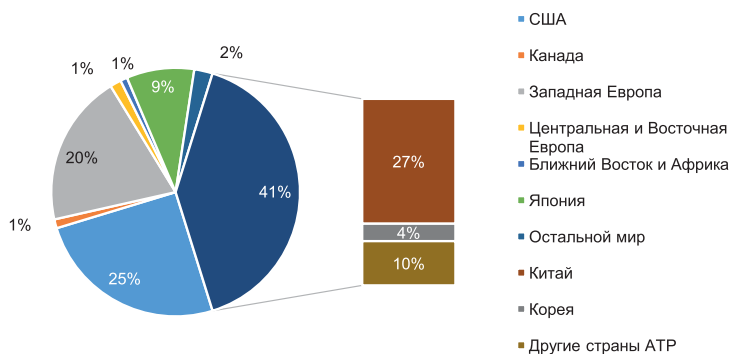


Рисунок 1.24— Географическая структура рынка IoT, 2018 г.

Источник: составлено авторами по данным IDC [1.48, 1.80, 1.81]

Если рассматривать географическую структуру по странам, а не регионам, то лидером является Китай с общим объемом затрат на IoT в размере 209 млрд. долл. (27% мирового рынка). Однако рынок США, основными драйверами которого являются производство, транспорт и потребительский сегмент, незначительно уступает по своим размерам Китаю, занимая четверть мирового рынка. Третье и четвертое места занимают Япония (68 млрд. долл.) и Корея (29 млрд. долл.) В обеих этих странах основным отраслевым сегментом является промышленность.

1.3.4.1 Азиатско-тихоокеанский регион (не включая Японию)

Объем рынка интернета вещей АТР в 2018 году вырос на 12,1% по сравнению с предыдущим годом и оставил 291,7 млрд. долл. Китай, мировой лидер, в этом регионе занимает 64,2% рынка. В прогнозируемом аналитиками IDC периоде (2017–2022 гг.) Китай, скорее всего, сохранит свои позиции при среднегодовом темпе прироста 12,8%. Решения IoT постепенно внедряются и в других странах региона. Так, на Корею и Индию приходится 9,8% и 8,8% рынка соответственно [1.82].

Основным пользовательским сценарием в этом регионе являются производственные операции (17,7% от общего объема рынка в 2018 г.). Распространение этого сценария, а также использование IoT в целях управления ресурсами

(5,8%) связано во многом с внедрением принципов Индустрии 4.0. Вторым по значимости стал мониторинг грузов (8%). Наибольшие темпы прироста ожидаются в сегменте подключенных автомобилей (33,8%).

В отраслевой структуре преобладают дискретное и непрерывное производство (31,9% рынка), перевозки (10,8%), пользовательский сегмент (10,2%) и коммунальные услуги; на них в общей сложности приходится 60% рынка. В пятерку самых перспективных сегментов по темпам роста входят потребительский сегмент (CAGR 22,4%), строительная отрасль (CAGR 20,3%), медицинские услуги (CAGR 17,1%), страхование (CAGR 16,1%) и торговля (CAGR 14,8%).

В технологическом разрезе в 2018 году наиболее крупным рынком стало предоставление услуг IoT – 84,1 млрд. долл. (28,9% от общего объема). Затем следует сегмент программного обеспечения, на третьем месте – устройства и оборудование, на последнем – каналы связи. По прогнозам, к 2022 г. сегменты услуг и ПО вместе займут 56,1% рынка, а устройства и связь – 23,9% и 20% соответственно.

1.3.4.2 Центральная и Восточная Европа

По прогнозам IDC, затраты на интернет вещей в Центральной и Восточной Европе (ЦВЕ) в 2018 г. вырастут по сравнению с 2017 г. на 15% и составят 11,3 млрд. долл. Технологии интернета вещей быстро распространяются в регионе, растущее число компаний тестирует или полноценно применяет соответствующие решения. В 2017–2022 гг. прогнозируется среднегодовой темп прироста 18,1%, общий объем инвестиций в 2022 г. – 22 млрд. долл. [1.83].

В отраслевой структуре преобладают потребительский сегмент, коммунальные услуги и производство, которые в 2018 г. в совокупности займут 62% рынка, при этом самый крупный сегмент – потребительский (16,2%). Самые быстрые темпы роста наблюдаются в сфере образования, в страховой отрасли, потребительском секторе и в оптовой торговле.

Среди потребительских сценариев преобладают мониторинг грузов (9,1%), производственные операции (7,8%) и управление ресурсами (7,6%). Наибольшие темпы прироста ожидаются на рынке технологий умного строительства (CAGR 31,3%).

Что касается сегментации рынка по продукту, то на ПО и услуги придется 59% рынка в 2018 году, на каналы связи – 7% рынка.

Российский рынок является самым большим в регионе. На него приходится 36% (Рис. 1.25).

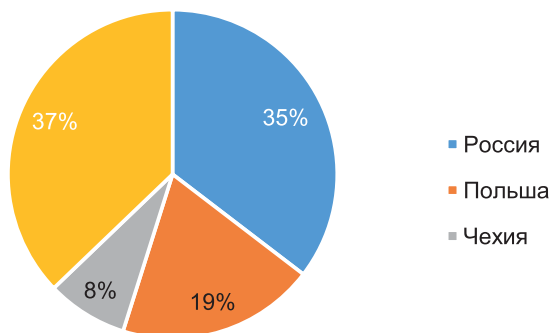


Рисунок 1.25— Географическая структура рынка IoT Центральной и Восточной Европы (в денежном выражении)

Источник: составлено авторами по данным IDC [1.83]

1.3.5 Российский рынок интернета вещей

Оценки российского рынка интернета вещей неоднозначны. По данным опроса отечественных экспертов, проведенного аналитическим агентством TAdviser [1.84], по итогам 2017 г. рынок IoT в России оценивается в широких границах от 40 до 600 млрд. рублей. Нет среди экспертов и консенсуса по поводу структуры. Например, оценки доли промышленного интернета вещей варьируются от 20% до 95% [1.84]. На Рис. 1.26 представлены оценки некоторых аналитических агентств¹⁶.

¹⁶ Данные в российских рублях переведены в доллары США по среднегодовому курсу ЦБ РФ за 2015 г. (61,3194 рубля за 1 доллар США), 2016 г. (66,8335 рубля за 1 доллар США) и 2017 г. (58,2982 рубля за 1 доллар США) по данным RateStats.com

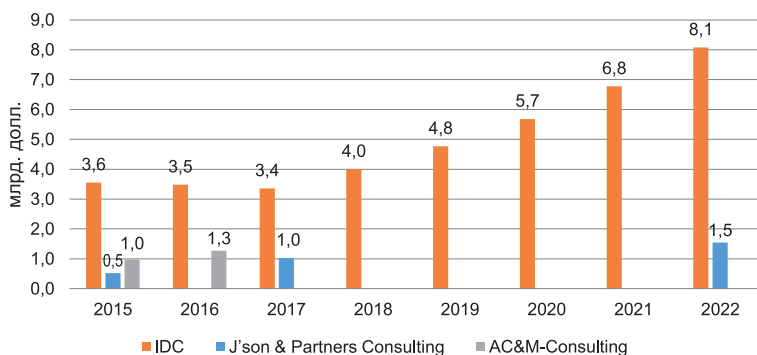


Рисунок 1.26— Оценки российского рынка интернета вещей, 2015–2022 гг., млрд. долл.

Источник: составлено авторами по данным IDC [1.83, 1.85, 1.86], J'son & Partners Consulting [1.86, 1.87] и AC&M Consulting [1.89]

Международная компания IDC оценивает российский рынок и перспективы его роста в разы выше, чем российские компании J'son & Partners Consulting и AC&M Consulting. Возможно, это связано с тем, что российские агентства оценивают рынок межмашинных коммуникаций (M2M), а не рынок интернета вещей. В своем отчете, выпущенном в начале 2018 г., J'son & Partners Consulting объясняет, что рынок интернета вещей на самом деле еще не сформировался и является в большей степени рынком распределенных систем телеметрии.

По данным IDC, объем российского рынка в 2018 г. составит 4 млрд. долл., а CAGR за 2017–2022 гг. – 19,2% [1.83]. Следовательно, аналитики IDC прогнозируют, что в 2022 г. объем рынка интернета вещей в России составит 8,1 млрд. долл. Основными драйверами рынка являются цифровая трансформация компаний, создание экосистемы и рост взаимодействия поставщиков решений, а также государственная поддержка. Также положительное влияние оказали первые успешные проекты, посвященные сбору данных и интеграции решений интернета вещей с существующими ИТ-системами. Тем не менее, по сравнению с более ранними отчетами IDC, оценки темпов роста снижены. Ранее для периода 2017–

2021 г. прогнозировался CAGR 22% и объем рынка более 9 млрд. долл. к 2022 г. [1.86]. Кроме общей тенденции к корректровке оценок рынка в сторону понижения, характерной не только для России, можно отметить и влияние специфического российского фактора – укрепление рубля.

Российская аналитическая компания J'son & Partners Consulting в 2017 г. оценила объем рынка IoT/M2M в 60 млрд. руб. [1.88], или чуть более 1 млрд. долл. по среднегодовому курсу доллара за 2017 г. По данным этой компании, к 2022 г. объем рынка составит 90 млрд. руб. (1,5 млрд. долл.¹⁷, CAGR 8,4%) [1.88]. Несмотря на то, что оценки J'son & Partners значительно ниже прогнозов IDC, эта компания также придерживается мнения, что рынок интернета вещей будет устойчиво расти как в денежном, так и в физическом выражении. По прогнозам J'son & Partners количество подключенных устройств должно вырасти с 15,9 млн. в 2016 г. до 43 млн. в 2022 г. [1.88], что составляет CAGR в 18%. При этом основным фактором роста считается вытеснение облачными сервисами текущих проприетарных телеметрических решений.

По оценкам AC&M Consulting, на конец 2016 г. объем российского рынка составил 85 млрд. руб. [1.89]. В свою очередь, исследование Orange Business Services и iKS–Consulting посвящено российскому бизнес–сектору (enterprise) «Интернета Вещей». Предполагается, что в 2018 г. рынок IoT составит 20,8 млрд. рублей с перспективой роста к 2020 г. до 30 млрд. руб. (CAGR 12% в год) [1.90].

Пока доля российского рынка IoT в четыре раза ниже доли России в мировом ВВП (Рис. 1.27), что свидетельствует об отставании развития интернета вещей. Тем не менее, по прогнозам IDC к 2022 г. это отставание должно сократиться.

¹⁷ По среднегодовому курсу ЦБ РФ за 2017 г.

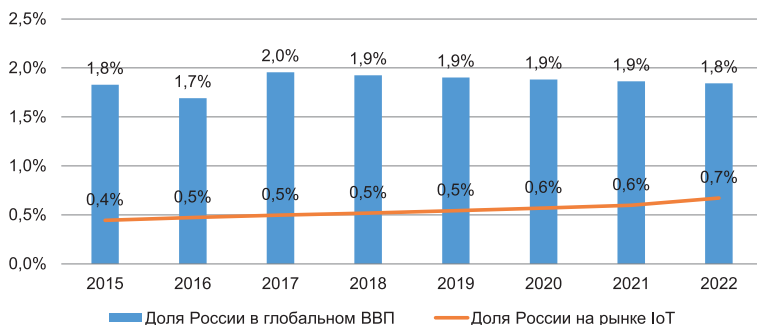


Рисунок 1.27— Доля России в мировом ВВП по текущим ценам и сравнение с оценками доли рынка IoT, 2015–2022 г.

Источник: рассчитано и составлено авторами по данным IDC [1.48, 1.52, 1.54-1.56, 1.83-1.85] и World Bank Group [1.91-1.93]

Однако есть и сдерживающие рост факторы, к которым можно отнести неуверенность участников рынка в достаточном уровне возврата инвестиций и почти полное отсутствие стандартов. В этом смысле большую роль может сыграть государственная программа «Цифровая экономика Российской Федерации», в рамках которой предполагается разработка стандартов и развитие нормативно-правового регулирования, а также необходимой инфраструктуры.

С точки зрения секторальной структуры экономики, более 60% рынка IoT, по версии IDC основанной на данных за 2015 г., приходится на промышленный интернет вещей, а самый маленький сегмент – это потребительский рынок (Рис. 1.28). По данным 2016 г. эти два сегмента показали стабильную динамику развития благодаря инвестициям в умные города и распространению среди населения решений категории «безопасность жилья» [1.86]. Аналитики J’son & Partners подчеркивают, что спрос на этом рынке в основном формируется крупными проектами государственных организаций и корпораций.



Рисунок 1.28—. Структура российского рынка IoT по секторам, 2015 г.

Источник: [1.85]

В отраслевом разрезе, по данным IDC за 2016 г., половина рынка IoT приходилась на производство, транспорт, а также объединенный сегмент «телекоммуникации и энергетика». Для производства основным сценарием было управление ресурсами, для транспорта — управлению транспортными средствами, мониторинг транспорта. Также стоит выделить такие отрасли, как розничная торговля и сельское хозяйство, которые в 2016 г. активно использовали решения IoT, но в денежном выражении объем этих сегментов рынка был незначительным [1.86]. Важное место на рынке занимает государственный сектор, что в первую очередь связано с инвестициями в умные города.

AC&M-Consulting также оценивал отраслевую структуру российского рынка, но по его физическому объему – количеству модулей для соединения автоматических устройств (M2M-модулей). Наибольшую долю рынка в 2017 г. занимал транспорт (Рис. 1.29).

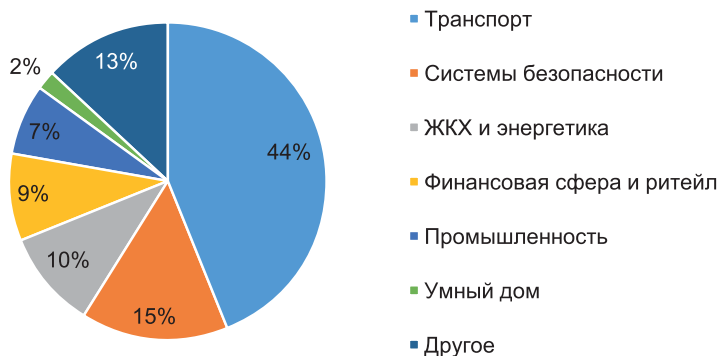


Рисунок 1.29 — Структура российского рынка IoT по отраслям, 2017 г.

Источник: [1.94]

Компании Orange Business Services и iKS–Consulting, которые оценивали размеры бизнес–сектора IoT, считают [1.90] крупнейшим рынком транспортную отрасль (16%), умные здания (4%), промышленность (2,5%), сельское хозяйство (2%), розничную торговлю (1,6%). Наименьшие расходы приходятся на финансовую сферу (1%). Самые высокие темпы роста ожидаются в сегменте розничной торговли. Драйверами этого рынка станут обширное внедрение CRM и SCM–систем, а также высокая конкуренция.

В технологической структуре преобладают инвестиции в услуги и оборудование: по данным IDC в 2016 г. их доля составила более 60%. Одним из возможных объяснений столь значительной роли этих сегментов является проведение собственных разработок при создании решений в области интернета вещей. Однако наиболее перспективным, по мнению аналитиков IDC, будет сегмент программного обеспечения, чьи среднегодовые темпы прироста в 2017–2021 гг. превысят средние по рынку и составят 24%. Такой рост должен быть поддержан более активным использованием коммерческих платформ IoT [1.86].

В J’son & Partners несколько иначе оценивают структуру рынка: по их данным наибольший объем приходится на сегмент «связь» (более 50% в 2016 г.). При этом в период до 2022 г. рост этого сегмента рынка в денежном выражении будет

практически нулевым. Причина столь важной роли «связи» на текущем рынке обусловлена невысокими темпами прироста количества подключенных «вещей» и низким уровнем добавленной стоимости IoT/M2M-решений на базе сервисов и облачных платформ из-за их неразвитости. Иными словами, российский рынок, в отличие от мирового, характеризуется низким уровнем ценности, получаемой от обработки данных.

Таким образом, несмотря на то, что глобальные оценки рынка и прогнозы его развития различаются, очевидно, что, по всем прогнозам, рынок будет расти. Среди основных драйверов глобального рынка интернета вещей можно выделить:

- снижение стоимости хранения и обработки данных, в том числе благодаря развитию облачных вычислений и распространению методов работы с большими данными;
- улучшение инфраструктуры: рост применения сенсоров, актуаторов и прочих устройств, необходимых для распространения решений IoT, соединение интернет-сетей с индустриальными сетями [1.95], увеличение покрытия сетью Интернет и развитие технологий связи (5G, LPWAN и др.);
- развитие международных стандартов;
- повышение уровня безопасности и конфиденциальности [1.96];
- развитие новых бизнес-моделей [1.62].

Начиная с 2014 г. прогнозы аналитиков по темпам роста рынка IoT несколько снизились из-за не оправдавшихся по ряду направлений ожиданий, таких как быстрое введение новых стандартов, обеспечением требуемого уровня безопасности и конфиденциальности. Соответственно, новые прогнозы роста оказались более консервативными: технологии, обеспечивающие работу интернета вещей, развиваются не так быстро.

В технологической структуре драйверами роста станут сегменты программного обеспечения и услуг, при этом к 2020 г.

программное обеспечение должно стать самым крупным сегментом. В отраслевом разрезе рост рынка будет обеспечен такими сегментами, как дискретное производство, транспорт¹⁸, ЖКХ¹⁹, потребительский сегмент и страхование. Также будут развиваться такие межотраслевые направления, как «Умный город» и «Подключенная Промышленность»²⁰.

Интернет вещей будет наиболее активно использоваться для предиктивного обслуживания, автоматической оптимизации производства²¹, V2V (vehicle-to-vehicle/ транспортное средство – транспортное средство) и V2I (vehicle-to-infrastructure/ транспортное средство – инфраструктура)²².

В географическом разрезе главным трендом является укрепление позиций Азиатско-Тихоокеанского региона во главе с Китаем. Российский рынок интернета вещей по сравнению с мировым еще находится на ранней стадии развития. Отставание заметно как по размеру доли российского рынка в глобальном, так и в сравнительной перспективе: доля российского рынка IoT в мировом будет расти медленнее, чем доля России в глобальном ВВП. К 2022 г. предполагается, что разрыв (отставание) сократится.

Российский рынок отличается от мирового и по своей структуре. В частности, по некоторым оценкам, ведущим сегментом в бизнес-секторе является транспорт, тогда как в мире главенствует промышленный интернет вещей. Менее заметное место в России занимает и программное обеспечение. Однако, в соответствии с общемировым трендом, ожидается значительный рост этого сегмента в ближайшие годы. Вероятно, в среднесрочной перспективе по своей технологической структуре рынок России хоть и приблизится к мировому, но все еще будет соответствовать более ранним

¹⁸ Самые большие сегменты рынка в 2022 г. по версии IDC [1.51], самые крупные сегменты по версии в 2020 г. BCG [1.76]

¹⁹ Третий по объему сегмент по оценкам BCG на 2020 г., темпы прироста (CAGR) в 2015-2020 гг. более 40%.

²⁰ Сегменты с наиболее высокими темпами роста по версии IDC

²¹ Наиболее крупные сегменты в перспективе к 2020 г. по версии BCG

²² Сегменты с наиболее высокими CAGR в 2017-2022 гг. по версии IDC

этапам развития IoT, где значительное место занимает сегмент оборудования и комплектующих.

1.4 Перспективные бизнес–модели на рынке «Интернета Вещей»²³

Развитие информационных и коммуникационных технологий способствует формированию нового феномена – цифровой экономики. Базовым элементом цифровой экономики является «Интернет Вещей». В России и в мире развивается рынок услуг «Интернета Вещей», понимаемый как совокупность экономических отношений между поставщиками услуг «Интернета Вещей» и их потребителями.

1.4.1 Варианты бизнес–моделей операторов услуг «Интернета Вещей»

Для оказания услуг «Интернета Вещей» необходимой является совокупность деятельности, выполняемых участниками рынка таких услуг. Такая совокупность формирует последовательность деятельности по созданию добавленной стоимости рынка услуг «Интернета Вещей» – организованный и взаимосвязанный набор деятельности, необходимый для создания и поставки потребителям определенной группы продуктов или услуг, представляющих для них ценность.

Анализ исследований рынка услуг «Интернета Вещей» показал, что в последовательности деятельности по созданию добавленной стоимости на этом рынке можно выделить пять видов деятельности [1.12, 1.97–1.111] (Рис. 1.30).

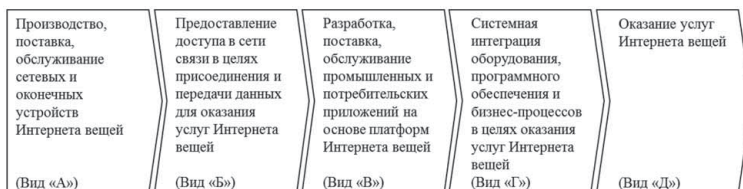


Рисунок 1.30 — Основные виды деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» и примеры организаций

Источник: составлено автором на основе данных [1.12, 1.97–1.111]

²³ Минов А. В. (АО «НИИТС»)

Структура доходов в последовательности деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» в мире в 2012 г. и 2016 г. приведена на Рис. 1.31 [1.111, 1.112].

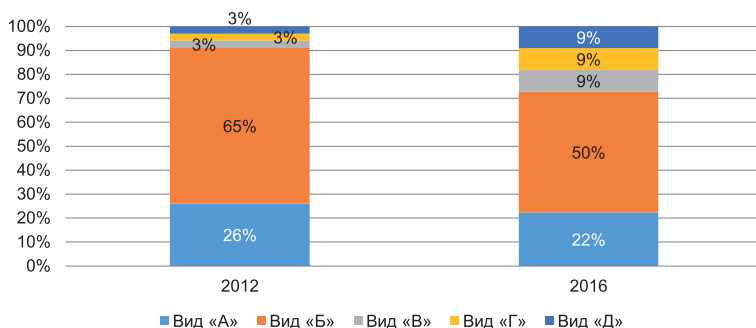


Рисунок 1.31 — Структура доходов в последовательности деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» в мире

Источник: составлено автором на основе данных [1.111, 1.112]

Доминирующую долю в структуре доходов занимает деятельность вида «Б» (65% в 2012 г. и 50% в 2016 г.). Структура доходов значительно трансформируется с развитием рынка «Интернета Вещей». За период с 2012 г. по 2016 г. доля деятельности вида «Б» уменьшилась в 1,3 раза, а деятельность вида «В» выросла в 3 раза (с 3% в 2012 г. до 9% в 2016 г.), что свидетельствует о расширении предоставления комплексных услуг «Интернета Вещей», а также изменении стратегии операторов связи и переходе от предоставления низкомаржинальных услуг передачи данных к оказанию комплексных услуг «Интернета Вещей» с высокой маржинальностью.

Статистическая информация о структуре доходов в последовательности деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» в России доступна только с объединенными данными по доходам от деятельности вида «В», «Г», «Д» (Рис. 1.32) [1.111, 1.113, 1.114].

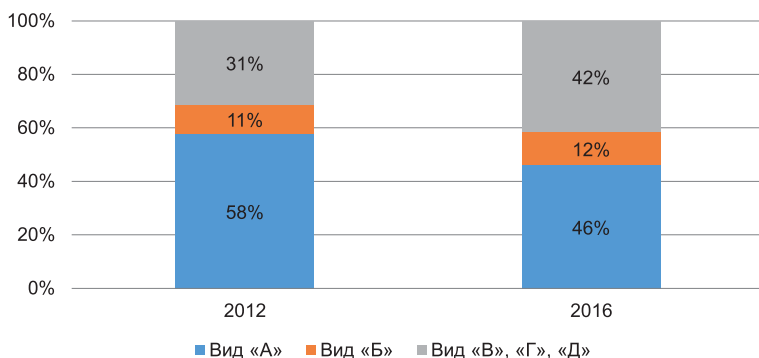


Рисунок 1.32 — Структура доходов в последовательности деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» в России

Источник: составлено автором на основе данных [1.111, 1.113, 1.114]

В 2012 г. и 2016 г. наибольшую долю (58% и 46% соответственно) в структуре доходов имела деятельность вида «А». Доля этого вида деятельности более чем в два раза превышает мировые показатели.

Особенность структуры доходов в последовательности деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» в России, по сравнению с мировым рынком, состоит в низкой доле доходов от услуг (виды «Б», «В», «Г», «Д») и высокой доли доходов от деятельности вида «А». Структура доходов меняется с развитием рынка услуг «Интернета Вещей» – уменьшается доля от деятельности вида «А» (снижение в 1,6 раза с 2012 г. по 2016 г.), и увеличивается доля от деятельности вида «Б» (рост в 1,6 раза с 2012 г. по 2016 г.), деятельности видов «В», «Г», «Д» (рост доли указанных трех видов деятельности в 1,9 раза с 2012 г. по 2016 г.). Тенденции развития российского рынка коррелируют с таковыми для мирового рынка.

Участники, выполняющие деятельность вида «А», в настоящее время занимают значительную долю в структуре доходов в последовательности деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей». В мире и в России существует большое количество органи-

заций, выполняющих этот вид деятельности и производящих различные виды устройств «Интернета Вещей». Такие производители поставляют свою продукцию всем участникам рынка услуг «Интернета Вещей». Также они предлагают решения, включающие, в том числе, деятельность вида «В». Доля участников, выполняющих только вид деятельности «А», в структуре доходов в последовательности деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» в мире будет уменьшаться. Это обусловлено снижением удельной цены устройств, несмотря на увеличение их количества.

В структуре доходов в последовательности деятельности по созданию добавленной стоимости на российском и мировом рынке услуг «Интернета Вещей» в настоящее время доминирующую роль играют операторы связи, выполняющие, в том числе, деятельность вида «Б» [1.115]. В России все крупнейшие операторы связи («МТС», «Мегафон», «ВымпелКом», «Ростелеком», «Т2 Мобайл» и др.) выполняют деятельность вида «Б», а также, в некоторых случаях, все остальные виды («А», «В», «Г», «Д»). Анализ стратегий развития, а также официальных отчетов операторов связи и статистической информации отрасли «связь» показал, что с развитием рынка услуг «Интернета Вещей» такие операторы расширяют долю доходов от деятельности вида «В» и «Д» [1.116–1.123].

Для управления большим количеством устройств «Интернета Вещей», необходимым является использование платформ «Интернета Вещей». В структуре доходов в последовательности деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» растет доля организаций, выполняющих деятельность вида «В». Крупнейшими в мире (по доле рынка) компаниями, специализирующимися на платформах «Интернета Вещей», являются Aeris, Amdocs, Axeda, Ericsson, ILS Technology, Jasper Wireless, Oracle, Qivicon; в России – «Петер-Сервис», «Связьком» и другие [1.111]. Другие участники рынка также внедряют собственные платформы «Интернета Вещей», в том числе российские «Мегафон», «МТС», «ВымпелКом», «Ростелеком» и другие. Растет количество организаций, выполняющих деятельности

вида «В» с предоставлением универсальных платформ, работающих в различных, как по технологии передачи данных, так и по принадлежности к оператору связи, сетях связи с различными видами устройств.

Внедрение услуг «Интернета Вещей» в организациях из различных секторов экономики требует изменений их бизнес-процессов, интеграции с существующими и планируемыми к внедрению системами автоматизации и управления технологическими процессами, а также экономического обоснования таких изменений. Решением таких комплексных задач занимаются организации, имеющие соответствующие компетенции для различных отраслей экономики. Мировыми лидерами в этой области являются: Amdocs, Accenture, IBM, HP, Numerex, Qualcomm и другие. Доля деятельности вида «Г» в структуре доходов в последовательности деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» в настоящее время растет (Рис. 1.31, 1.32). С развитием рынка, стандартизации и внедрения универсальных решений темп роста этой доли будет снижаться.

Таким образом, деятельности по созданию добавленной стоимости на рынке услуг интернета вещей в их последовательности выполняются участниками этого рынка. Каждый из них может выполнять минимум один из видов деятельности. Однако, существуют участники, которые выполняют несколько видов деятельности одновременно (Рис. 1.33). На этом рисунке жирным шрифтом выделены примеры организаций, выполняющих одновременно несколько видов деятельности по созданию добавленной стоимости.

Производство, поставка, обслуживание сетевых и оконечных устройств Интернета вещей (Вид «А»)	Предоставление доступа в сети связи в целях присоединения и передачи данных для оказания услуг Интернета вещей (Вид «Б»)	Разработка, поставка, обслуживание промышленных и потребительских приложений на основе платформ Интернета вещей (Вид «В»)	Системная интеграция оборудования, программного обеспечения и бизнес-процессов в целях оказания услуг Интернета вещей (Вид «Г»)	Оказание услуг Интернета вещей (Вид «Д»)
Intel, Qualcomm, AMD, GE, China Mobile, Telefonica и др.; «Ангстрем», «Микрон», «Ростех», «Стриж» и др.	China Mobile, Vodafone, Bharti Airtel, America Movil, Telefonica и др.; «Ростелеком», «Мегафон», Tele2, «МТС», «Билайн», «Глобасс» и др.	Microsoft, IBM, Oracle, SAP, Google, China Mobile, Telefonica и др.; Mail.Ru Group, «Петер-Сервис», «Делимобиль», «Глобасс» и др.	Accenture, Numerex, HP, China Mobile, Telefonica и др.; «Ланит», «Энвижан Групп», «Крок», «Техносерв», и др.	China Mobile, Google, Telefonica и др.; «АгроНетворк», «Делимобиль», «Ростелеком», «Глобасс» и др.

Рисунок 1.33 — Основные виды деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» и примеры организаций

Источник: составлено автором

Оператор услуг «Интернета Вещей» по определению должен выполнять вид деятельности «Д». При этом также он может выполнять и другие виды деятельности («А», «Б», «В», «Г») в различных комбинациях. Таким образом теоретически возможны 16 бизнес-моделей оператора услуг «Интернета Вещей». Концептуальное описание совокупности взаимосвязанных видов деятельности, выполняемых оператором «Интернета Вещей», направленных на оказание услуги «Интернета Вещей», понимается как бизнес-модель оператора услуг «Интернета Вещей».

Как показано выше, наблюдаются тенденции изменения структуры доходов в последовательности деятельности по созданию добавленной стоимости на рынке услуг интернета вещей в России и в мире. Развитие рынка услуг «Интернета Вещей» показывает также, что деятельность по оказанию услуг «Интернета Вещей» в России и в мире носит продолжительный характер. Поэтому перспективными являются бизнес-модели, представленные в Таблице 1.5[1.124].

Таблица 1.5 — Совокупность перспективных бизнес–моделей операторов услуг «Интернета Вещей»

Номер модели	Виды деятельности, выполняемые одной организацией	Название бизнес–модели
1	«Д»	«Чистая»
3	«В», «Д»	«Платформоцентричная»
4	«Б», «Д»	«Сетецентричная»
7	«Б», «В», «Д»	«Комплексная»

Источник: составлено автором

1.4.2 Анализ бизнес–моделей операторов услуг «Интернета Вещей»

Эффективным инструментом для анализа бизнес–моделей является «Канва бизнес–модели» Остервальдера [1.125–1.138]. Анализ модели производственной деятельности организации осуществляется по девяти видам факторов, включающим характеристики:

- продукта (ценностные предложения);
- клиента (потребительские сегменты; каналы сбыта; взаимоотношения с клиентами);
- производства (ключевые виды деятельности; ключевые партнеры; ключевые ресурсы);
- финансов (структура издержек; потоки поступления доходов).

Потребительский сегмент – группа покупателей, обладающая похожими потребностями, желаниями и возможностями [1.139, 1.140]. Услуги «Интернета Вещей» востребованы во всех отраслях экономики, среди предприятий (B2B, англ. Business–to–Business) и органов власти (B2G. Business–to–Government). Услуги «Интернета Вещей» также востребованы в массовом сегменте (B2C. Business–to–Consumer). Соответствие примеров оказываемых услуг «Интернета Вещей», потребительских сегментов и бизнес–моделей оператора услуг «Интернета Вещей», приедено в Таблице 1.6.

Таблица 1.6— Соответствие примеров оказываемых услуг интернета вещей, потребительских сегментов и бизнес-моделей оператора услуг «Интернета Вещей»

Пример услуги интернета вещей	Бизнес-модель: 1 — 4
Страхование транспорта с персональными условиями с учетом информации от устройства интернета вещей, установленного в нем	B2C, B2B, B2G и др.
Обеспечение безопасности на основании видеонаблюдения с устройств интернета вещей	B2C, B2B, B2G и др.
Логистические услуги с предоставлением информации о местоположении на основании информации от устройств интернета вещей	B2C, B2B, B2G и др.

Примечания:

Бизнес-модель оператора услуг «Интернета Вещей»: 1 – «Чистая», 2 – «Платформоцентричная», 3 – «Сетецентричная», 4 – «Комплексная»

Источник: составлено автором

Таким образом, потребительские сегменты для различных моделей аналогичны.

Ценностные предложения – это совокупность товаров и услуг, которые отвечают запросам определенного потребительского сегмента. Основные ценностные предложения, которые предоставляются оператором услуг «Интернета Вещей», определяются видом деятельности, которые выполняются им в соответствии с моделью.

Так, при выполнении оператором услуг «Интернета Вещей» деятельности вида «Д», основные ценностные предложения основываются на услугах «Интернета Вещей». Такими ценностными предложениями могут быть, например, повышение эффективности растениеводства за счет автоматизированного управления бизнес-процессами на основании информации с устройств «Интернета Вещей». При этом оператор таких услуг поставляет только услуги управления

на базе «Интернета Вещей», а потребитель сам обеспечивает связь между устройствами «Интернета Вещей».

При модели «Сетецентричная» (выполнении деятельности вида «Б» и «Д»), на базе услуг доступа в сети связи в целях присоединения и передачи данных для оказания услуг «Интернета Вещей», операторы услуг «Интернета Вещей» предоставляют дополнительные ценности для потребителя. Например, основные операторы мобильной связи предоставляют возможность контроля местоположения и других характеристик грузов в любой точке мира на базе собственных и партнерских сетей связи.

При модели «Платформоцентричная» (выполнении деятельности вида «В» и «Д») оператор услуг «Интернета Вещей» оперирует возможностями платформы «Интернета Вещей», которая, например, имеет возможность взаимодействия с несколькими операторами связи. Такая особенность может быть предложена в виде ценностного предложения при услугах, для которых критичным является надежность связи. Например, для обеспечения управления сетью банкоматов, в каждом из них устанавливаются модули связи с подключением одновременно к сетям нескольких операторов связи.

Таким образом, существует зависимость основных ценностных предложений, предоставляемых операторами услуг «Интернета Вещей», от вида бизнес-модели. Для различных таких моделей ценностные предложения различаются.

Ключевые виды деятельности, выполняемые оператором каждого из четырех видов бизнес-моделей, определяются самой моделью. Как показано в пункте 1.4.1, оператор с моделью «Чистая» выполняет один вид деятельности – вид «Д». «Платформоцентричная» организация, кроме вида «Д», также выполняет деятельность вида «В». Модель оператора услуг «Интернета Вещей» «Сетецентричная» предполагает выполнение деятельности видов «Б» и «Д». При «Комплексной» модели – «Б», «В», «Д». Таким образом, ключевые виды деятельности бизнес-моделей операторов услуг «Интернета Вещей» различаются.

Каналы сбыта описывают, как организации взаимодействуют с потребительскими сегментами и доносят до них свои ценностные предложения. Классификация применения различных каналов сбыта различными бизнес-моделями операторов услуг «Интернета Вещей» приведена в Таблице 1.7.

Таблица 1.7— Классификация применения различных каналов сбыта различными бизнес-моделями операторов услуг «Интернета Вещей»

Каналы сбыта		Бизнес-модель			
		1	2	3	4
Собственные	Торговые агенты	Да	Да	Да	Да
	Продажи через интернет	Да	Да	Да	Да
	Фирменные магазины	Да	Да	Да	Да
	Другие	Да	Да	Да	Да
Партнерские	Партнерские магазины	Да	Да	Да	Да
	Другие	Да	Да	Да	Да

Примечания:

Бизнес-модель оператора услуг «Интернета Вещей»: 1 – «Чистая», 2 – «Платформоцентричная», 3 – «Сетецентричная», 4 – «Комплексная»

Источник: составлено автором

Блок взаимоотношения с клиентами описывает типы отношений, которые устанавливаются у организации с отдельными потребительскими сегментами. Для различных операторов услуг «Интернета Вещей» характерным является использование различных взаимоотношений с клиентами. Примеры видов взаимодействия с клиентами и применения их операторами услуг «Интернета Вещей» с различными бизнес-моделями приведены в Таблице 1.8.

Таблица 1.8— Примеры видов взаимодействия с клиентами и применения их операторами услуг «Интернета Вещей»

Вид взаимоотношения с клиентами	Бизнес–модель			
	1	2	3	4
Персональная поддержка	Да	Да	Да	Да
Автоматизированное обслуживание	Да	Да	Да	Да
Сообщества	Да	Да	Да	Да
Другие	Да	Да	Да	Да

Примечания:

Бизнес–модель оператора услуг «Интернета Вещей»: 1 – «Чистая», 2 – «Платформоцентричная», 3 – «Сетецентричная», 4 – «Комплексная»

Источник: составлено автором

Ключевые партнеры – сеть поставщиков и партнеров, благодаря которым функционирует бизнес–модель. В последовательности деятельности по созданию добавленной стоимости на рынке услуг «Интернета Вещей» можно выделить пять видов деятельности, которые выполняются различными организациями. При этом, оператор таких услуг, в соответствии с собственной бизнес–моделью, может выполнять несколько из них. Поэтому ключевыми партнерами являются организации, выполняющие все остальные виды деятельности, кроме тех, которые выполняет сам оператор. Ключевые партнеры для каждого из видов бизнес–моделей, приведены в Таблице 1.9.

Таблица 1.9— Ключевые партнеры для операторов услуг «Интернета Вещей»

Ключевые партнеры (организации выполняющие указанный вид деятельности)	Бизнес–модель			
	1	2	3	4
«А»	Да	Да	Да	Да
«Б»	Да	Да	Нет	Нет
«В»	Да	Нет	Да	Нет
«Г»	Да	Да	Да	Да

Примечания:

Бизнес–модель оператора услуг «Интернета Вещей»: 1 – «Чистая», 2 – «Платформоцентричная», 3 – «Сетецентричная», 4 – «Комплексная»

«А», «Б», «В», «Г» – буквенное обозначение вида деятельности по созданию добавленной стоимости.

Источник: составлено автором

Ключевые ресурсы – наиболее важные активы, необходимые организации для функционирования ее бизнес–модели. Модель определяется видами деятельности, которые выполняет оператор услуг «Интернета Вещей». Для различных деятельности нужны различные активы. Для выполнения деятельности вида «Б» необходимыми являются активы, с использованием которых таким оператором обеспечивается доступ в сети связи в целях присоединения и передачи данных для оказания услуг «Интернета Вещей». Для выполнения деятельности вида «В» – разработка, поставка, обслуживание промышленных и потребительских приложений на основе «Интернета Вещей». Ключевые ресурсы, необходимые для функционирования такой модели, приведены в Таблице 1.10.

Таблица 1.10— Ключевые ресурсы, необходимые для функционирования бизнес–модели оператора услуг «Интернета Вещей»

Ключевой ресурс	Бизнес–модель			
	1	2	3	4
Активы, с использованием которых обеспечивается доступ в сети связи в целях присоединения и передачи данных для оказания услуг интернета вещей	Нет	Нет	Да	Да
Активы, с использованием которых обеспечивается разработка, поставка, обслуживание промышленных и потребительских приложений на основе платформ интернета вещей	Нет	Да	Нет	Да

Примечания:

Бизнес–модель оператора услуг «Интернета Вещей»: 1 – «Чистая», 2 – «Платформоцентричная», 3 – «Сетецентричная», 4 – «Комплексная»

Источник: составлено автором

Блок структуры затрат описывает наиболее существенные затраты, необходимые для работы в рамках конкретной бизнес-модели. У различных бизнес-моделей операторов услуг «Интернета Вещей», как показано выше, различаются ценностные предложения, ключевые виды деятельности, ключевые партнеры, ключевые ресурсы. Поэтому структура затрат, характерная для различных бизнес-моделей таких операторов, также различается.

Потоки поступления доходов учитывают прибыль, которую организация получает от каждого потребительского сегмента. Как показано в пункте 1.4.1, для услуг «Интернета Вещей» характерным является продолжительный характер их оказания. Поэтому для операторов таких услуг потоки поступления доходов характеризуются регулярным доходом от периодических платежей, получаемых от потребителей за ценностные предложения или постпродажное обслуживание. Таким образом, потоки поступления доходов определяются для каждого из видов бизнес-моделей регулярными платежами за ценностные предложения или постпродажным обслуживанием. Так как ценностные предложения различны для различных бизнес-моделей, то различаются и потоки поступления доходов.

1.4.3 Рекомендации по выбору бизнес-модели оператора услуг «Интернета Вещей»

На рынке услуг «Интернета Вещей» обоснованными являются четыре вида бизнес-моделей операторов услуг «Интернета Вещей». Организации, которые их используют, уже оказывают такие услуги. Поэтому такие организации определены как «зрелые».

На участие в рынке услуг «Интернета Вещей» могут претендовать также организации, которые в настоящее время не оказывают услуги «Интернета Вещей» – «новые» организации. Основные виды «Новых» организаций следующие:

- «IT организация» – организация, которая планирует выйти на рынок услуг «Интернета Вещей» и имеет платформу «Интернета Вещей», как это определено в пункте 1.4.1;

- «Организация связи» – организация, которая планирует выйти на рынок услуг «Интернета Вещей» и имеет инфраструктуру сети связи, использующуюся в целях присоединения и передачи данных для оказания услуг «Интернета Вещей»;
- «Новая организация» – организация, которая планирует выйти на рынок услуг «Интернета Вещей», но не имеет ни платформы «Интернета Вещей», ни инфраструктуры сети связи. Такой организацией может быть, в том числе, вновь создаваемая организация.

Проведено исследование, включающее анализ различных аспектов рынка услуг «Интернета Вещей» и бизнес-моделей операторов услуг «Интернета Вещей», в том числе:

- анализ модели рынка услуг «Интернета Вещей»;
- анализ бизнес-модели, классификацию факторов эффективности;
- анализ факторов эффективности бизнес-моделей экспертным оцениванием;
- многокритериальный анализ значений и весов факторов эффективности бизнес-моделей;
- анализ семантической сети (ориентированного графа) и необходимого уровня инвестиций бизнес-модели оператора услуг «Интернета Вещей».

В результате этого исследования получены рекомендации для всех видов бизнес-моделей («Новая организация», «Организация связи», «IT организация», «Чистая», «Платформоцентричная», «Сетецентричная», «Комплексная»).

Рекомендации по выбору модели производственной деятельности оператора услуг «Интернета Вещей» в России в виде семантической сети (ориентированного графа), которая расположена относительно прямоугольной системы координат, приведены на Рис. 1.34. По оси абсцисс (Q) на нем учитывается значение обобщенного показателя эффективности моделей производственной деятельности операторов услуг «Интернета Вещей». По оси ординат (I) – уровень инвестиций для модели производственной деятельности.

Вершинами ориентированного графа являются модели производственной деятельности, а ребрами – отношения между ними. Зеленый и коричневый цвет вершины графа – характеристика организации как «нового» и «зрелого» участника рынка услуг «Интернета Вещей» соответственно. Высокая и средняя практическая вероятность смены бизнес-модели обозначены подписями «В» и «С» соответственно.

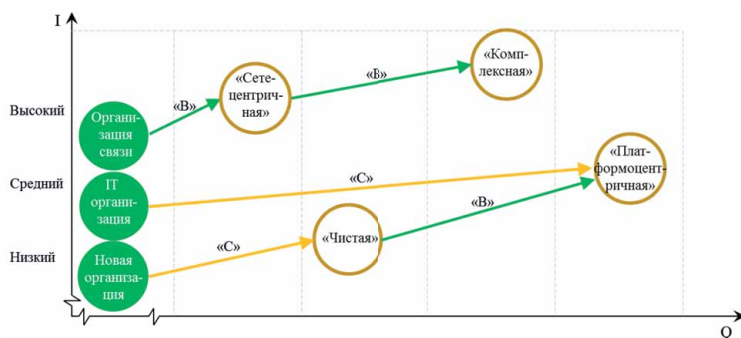


Рисунок 1.34— Семантическая сеть выбора модели производственной деятельности оператора услуг «Интернета Вещей» с учетом практической вероятности такой смены

Источник: составлено автором

Таким образом, для всех бизнес-моделей существуют возможные варианты развития организации с учетом текущего состояния организации («новые» и «зрелые»). При выборе модели, которая обладает более высоким значением обобщенного показателя эффективности, организации требуется повышение уровня инвестиций. Высокую вероятность смены бизнес-модели имеют варианты развития «Чистая» – «Платформоцентричная», «Сетецентричная» – «Комплексная», «Организация связи» – «Сетецентричная». Среднюю вероятность имеют варианты «Новая организация» – «Чистая», «ИТ организация» – «Платформоцентричная».

1.5 Государственная политика зарубежных стран и России в области интернета вещей²⁴

Для успеха распространения технологий интернета вещей имеет значение государственное регулирование, особенно в части разработки национальных стратегий развития и снятия барьеров к внедрению этих технологий. Политика регулирования в области интернета вещей проводится как на национальном, так и на наднациональном уровне. На наднациональном уровне формируются некоторые стандарты, готовятся аналитические обзоры и рекомендации по мерам развития интернета вещей. К организациям наднационального уровня относятся следующие специализированные структуры:

- Международная электротехническая комиссия (МЭК; англ. International Electrotechnical Commission, IEC); это международная некоммерческая организация по стандартизации электрических, электронных и смежных технологий. Некоторые из стандартов МЭК разрабатываются совместно с Международной организацией по стандартизации (ISO);
- Международный союз электросвязи (МСЭ, англ. International Telecommunication Union, ITU) — международная организация, определяющая рекомендации в области телекоммуникаций и радио, а также регулирующая вопросы международного использования радиочастот (распределение радиочастот по назначению и по странам), является специализированным учреждением ООН;
- Институт инженеров электротехники и электроники — IEEE (англ. Institute of Electrical and Electronics Engineers, I triple E — «Ай трипл и») — международная некоммерческая ассоциация специалистов в области техники, мировой лидер в области разработки стандартов по радиоэлектронике, электротехнике и аппаратному обеспечению вычислительных систем и сетей.

²⁴ Дежина И.Г. (Сколтех), Нафикова Т.Н. (Сколтех)

К наднациональным финансовым структурам относятся:

- Всемирный экономический форум - (ВЭФ, World Economic Forum) — международная организация государственно–частного сотрудничества. В январе 2018 года ВЭФ выпустил доклад «Интернет Вещей. Рекомендации для устойчивого развития», в котором предложены меры по развитию интернета вещей для трех видов субъектов – частного сектора, правительства и некоммерческих организаций, в контексте достижения Целей устойчивого развития ООН;
- Всемирный банк – международная финансовая организация, созданная с целью организации финансовой и технической помощи развивающимся странам. В 2017 году Исследовательская Группа Всемирного банка выпустила доклад по интернету вещей, в рамках которого была проанализирована государственная политика в разных странах на национальном уровне и уровне муниципалитетов.

На национальном уровне вовлеченность государств в развитие интернета вещей сильно варьируется. Во многих странах интернет вещей сложно выделить из общей системы поддержки цифровой экономики. Страны, которые представляют наибольший интерес с точки зрения типологии государственных подходов к поддержке интернета вещей – самостоятельно или в общем контексте цифрового развития – это США, Китай, Франция и Германия. США являются лидером рейтинга стран G20, который составляет компания IDC для сравнительной оценки развития интернета вещей. Китай интересен тем, что это крупнейший рынок IoT, и там, наряду с развитием цифровой экономики, реализуется государственная политика поддержки интернета вещей. В свою очередь Германия и Франция входят в группу стран – лидеров по развитию цифровой экономики [1.141]. При этом, если в Германии политику по отношению к интернету вещей сложно отделить от общей стратегии развития в области цифровой экономики, во Франции интернету вещей уделяется специальное внимание и есть несколько специфических инструментов развития этого направления. Стоит

также отметить, что Германия и Франция являются членами Европейского союза и на них распространяются общие для ЕС правила. Поэтому, если даже в политике отдельной страны интернет вещей не занимает значимого места, это еще не значит, что страна не является активным участником этого рынка и не осуществляет политику в рамках общеевропейских программ (таких, как проект CREATE–IoT, который был создан по программе Горизонт 2020).

Для развития интернета вещей правительства стран используют два вида инструментов: нормативно–регулятивный и аналитико–рекомендательный. От страны к стране соотношение этих инструментов может сильно различаться. Так, большинство стран заинтересовано в том, чтобы четко регламентировать вопросы безопасности, связанные с интернетом вещей. Технологические стандарты, как правило, не имеют обязательного характера. То же касается финансовых инструментов – они могут быть таргетированными, либо общего характера, либо вообще не применяться как мера стимулирования развития интернета вещей.

Далее на примере выбранных стран – Китая, США, Франции и Германии — анализируется государственная политика стимулирования развития интернета вещей.

Затем проводится сопоставление с ситуацией в России.

1.5.1 Китай

Китай стал одной из первых стран, где государство инициировало масштабную поддержку развития интернета вещей. В августе 2009 г. премьер–министр Китая Вэнь Цзябао, выступая в одном из учреждений Китайской Академии Наук (КАН), объявил о принятии концепции «Sensing China» (развитие сенсорной сети) и учреждении одноименного исследовательского центра [1.142]. За этим последовало развертывание общенациональных и локальных мер поддержки развития IoT.

В Китае государственная политика в области интернета вещей имеет несколько важных особенностей. Во–первых, у экономических субъектов есть реальная заинтересованность

в развитии технологий IoT как с точки зрения потенциала решения общественных проблем, так и будущего экономического роста, и повышения уровня занятости. Интерес Китая к интернету вещей связан с необходимостью разрешения общеэкономических и социальных последствий быстрого роста экономики в предыдущие годы, который сопровождался ростом уровня урбанизации, ухудшением транспортной ситуации, критическим загрязнением воздуха и другими проблемами. Правительство решило, что технологии интернета вещей помогут в решении этих проблем, а также будут способствовать балансировке спроса и предложения в ключевых секторах экономики (транспорт, энергетика) и реструктуризации отстающих отраслей.

Во-вторых, это сочетание мощной поддержки центральной власти и активной комплементарной деятельности провинций в создании благоприятных условий для развития интернета вещей. Китай отличает жесткая конкуренция между городами, которые откликнулись на данную центральную властью установку. В ответ на инициативу, объявленную премьер-министром, провинции и города Китая стали создавать собственные стратегии развития IoT, учреждать исследовательские центры и реализовывать свои пилотные проекты. Развитие IoT приобрело общенациональный размах. При этом ключевым направлением деятельности региональных властей фактически стали пилотные проекты умных городов, в рамках которых идет системное развитие и внедрение технологий интернета вещей.

В-третьих, в Китае слабее, чем в развитых странах, проявлены препятствия развитию интернета вещей – в частности, в сфере защиты частной жизни, конфиденциальности и безопасности [1.143]. В силу специфики общества люди меньше обеспокоены конфиденциальностью своей информации и концентрацией ее в руках государства. Поэтому пока в других странах внедрение технологий IoT тормозится дискуссиями о том, как обеспечить безопасность данных, и кому эти данные должны принадлежать, китайские власти и компании могут быстрее осуществлять проекты в этой области.

Организационно политика по поддержке развития интернета вещей проводится в рамках пятилетних планов. Интернет вещей занял важное место в последних двух пятилетних планах – двенадцатом (2011–2015 гг.) и тринадцатом (2016–2020 гг.). В марте 2010 года на Всекитайском собрании народных представителей (ВСНП) интернет вещей был выделен как стратегическая область, требующая усиленных мер государственной поддержки и больших инвестиций. Он был определен как один из стратегических перспективных рынков в рамках двенадцатого пятилетнего плана [1.142]. В том же году в Шанхае был создан Национальный центр интернета вещей. Вслед за утверждением 12-го пятилетнего плана Государственный совет Китая выпустил Руководство по развитию интернета вещей, в котором указаны цели, идеи и фокусные тематики для развития китайского IoT [1.144].

В плане развития на 12-ю пятилетку была поставлена цель увеличения объема рынка IoT до 500 млрд. юаней (80,5 млрд. долл.) к 2015 г. и 1 трлн. юаней (163 млрд. долл.) к 2020 г. По данным на 2010 г. он составлял 200 млрд. юаней [1.39]. В промежуточном отчете Центрального комитета КПК XVIII съезду коммунистической партии Китая, посвященном развитию информационно-коммуникационных технологий, был подчеркнут приоритет интернета вещей и предоставлены значительные налоговые послабления для производителей IoT решений.

В 2013 г. правительство Китая учредило межведомственный совет для координации государственной политики и деятельности в сфере IoT. В совет входят представители Национальной комиссии по развитию и реформам (НКРР), Министерства промышленности и информатизации, Министерства образования и Администрации стандартизации КНР. При поддержке этого совета в том же году были выпущены Директива по развитию индустрии IoT и Дорожная карта IoT, в которых были обозначены цели на 2015 год по формированию стандартов, исследованиям и разработкам, внедрению и продвижению технологий, отраслевой поддержке, бизнес-моделям, безопасности, регулятивным мерам, подготовке кадров и т.д.

В рамках 13-го пятилетнего плана интернет вещей появился в двух ключевых государственных программах развития – «Интернет+» и «Сделано в Китае 2025». Реализация стратегического плана экономического роста «Интернет+» послужит продвижению интернет-технологий (мобильного интернета, облачных вычислений, больших данных и интернета вещей) в производство и бизнес для дальнейшего развития новых отраслей, включая электронную торговлю, промышленный интернет и интернет-технологии в финансовой сфере. В свою очередь, в рамках принятой в 2015 году программы «Сделано в Китае 2025» приоритет получили направления, такие как IoT, умные приборы и высокотехнологичная бытовая электроника, которые способствуют быстрому внедрению инноваций в производство. Согласно плану, государство вложит в эти направления 10 млрд. юаней (1,5 млрд. долл.) [1.145].

Следует отметить, что Китай, благодаря возможности мобилизовать масштабные государственные инвестиции, имеет выигрышную позицию по сравнению с другими странами. Именно это и было сделано – для продвижения исследований, разработок, приложений и услуг в области IoT был создан Специальный фонд интернета вещей. В 2014 г. бюджет Фонда составил 10 млрд. юаней (1,6 млрд. долл.) [1.39]. Проекты, имеющие софинансирование, могут получить из Фонда гранты, а использующие банковские займы — претендовать на субсидии.

Правительство Китая также играет ключевую роль в развитии стандартов в области интернета вещей. Оно поддержало инициативы Ассоциации по стандартизации в области коммуникаций, рассчитывая, что разработанные ей стандарты в области интернета вещей получат международный статус. Для китайских властей важным достижением стало то, что в 2012 г. МСЭ принял первый общий IoT-стандарт, разработанный в Китае [1.39]. В рамках 13-й пятилетки планируется разработать более 200 национальных и отраслевых стандартов и постепенно улучшить систему стандартизации для того, чтобы успешно ответить на вызовы масштабирования рынка IoT [1.146].

Среди других направлений развития IoT, указанных в 13-м пятилетнем плане можно отметить следующие:

- технологические инновации: реализация НИОКР силами компаний для обеспечения значимых прорывов в развитии инфраструктуры IoT, сенсорных технологий, экосистемы и технологий безопасности, и сопутствующего значительного роста числа одобренных патентов;
- стимулирование внедрения IoT технологий: продвижение ряда интегрированных решений в области промышленного производства, современного сельского хозяйства и потребительских сегментов, таких как «умные дома» и медицинские услуги; формирование междисциплинарного механизма поддержки в области строительства и управления «умными городами», который характеризуется открытым доступом к данным и обменом данными;
- модернизированные отрасли: создание 10 отраслевых агломераций, развитие 200 опорных компаний, общий выпуск которых превысит 1 млрд. юаней (130,1 млн. евро), создание системы платформ по предоставлению широкого спектра государственных услуг и государственной поддержки. Одной из агломераций является г. Уси, где в том числе создана демонстрационная зона интернета вещей совместно муниципальными властями и технологическим гигантом Alibaba Group [1.147];
- гарантирование безопасности: достижение прорыва в исследованиях и разработке ключевых технологий безопасности и специализированных продуктов в этой области, разработка национальных и отраслевых стандартов безопасности в соответствии с текущими потребностями.

Также развитию интернета вещей способствует общая научно-технологическая политика Китая. В 2009 г. правительство учредило фонд поддержки международных патентных заявок, который выделяет 100 тыс. юаней (16 тыс. долл.)

на каждую зарубежную патентную заявку китайских авторов. В частности, по данным Немецкого Института промышленной инженерии им. Фраунгофера в период с 2013 г. по третий квартал 2015 г. китайские исследователи подали 2541 патентную заявку в области интернета вещей (для сравнения от США было подано 1065 заявок, от Германии – 441). Однако исследователи ставят под вопрос качество китайских заявок, утверждая, что их количество стимулировано именно политикой властей. Действительно, из 2451 патентных заявок были одобрены только 515 [1.143].

Стимулирующее воздействие на развитие интернета вещей в Китае оказывает и отраслевая политика. Государство поддерживает развитие технологий интернета вещей в промышленном контроле, финансовых услугах, здравоохранении и других ключевых отраслях, в том числе посредством мер регулирования. Так, например, в транспортной отрасли повышение регулятором розничных цен на топливо стимулирует рост применения систем управления транспортным парком в целях сокращения издержек. Кроме того, государство в некоторых случаях обязывает внедрять системы отслеживания грузов. В энергетике правительство установило целевой показатель по уровню распространения умных счетчиков – к 2017 г. такие счетчики планировалось установить в 95% домашних хозяйств [1.39]. В соответствии с этим указанием, две государственные компании – Государственная электросетевая корпорация Китая и Китайские южные электросети – начали масштабное установление подключенных счетчиков электроэнергии. Наконец, Национальный план по развитию здравоохранения и медицинских услуг на 2015–2020 гг. предусматривает использование технологий интернета вещей наряду с другими развивающимися информационными технологиями [1.144].

Правительство также осуществляет финансирование муниципалитетов и специальных экономических зон в рамках официальных пилотных проектов «умных городов». Эти проекты нацелены на применение IoT для решения ключевых городских проблем, таких как транспортная загруженность и загрязнение окружающей среды. Министер-

ство промышленности и информатизации определило 202 города, в которых должны быть развернуты пилотные проекты «умных городов» за счет проведения там интенсивных НИОКР в области интернета вещей и продвижения этой технологии [1.39]. Кроме того, в 2015 г. правительство учредило зоны свободного предпринимательства, например, в Институте технологий интернета вещей г. Чэнду провинции Сычуань [1.148]. В результате Пекин, Шанхай, Гуанчжоу, Ханчжоу и некоторые другие крупные города установили обширные сенсорные сети и центры данных для сбора, хранения и анализа информации о транспорте, потреблении электричества, общественной безопасности и состоянии окружающей среды. Стоит отметить, что по заявлению НКРП центральная власть в рамках 13-го пятилетнего плана будет финансировать только 25% от общей суммы инвестиций, остальную сумму должны вложить местные власти [1.149].

В целом в 2014 году более 90% китайских провинций и муниципалитетов обозначили интернет вещей как основу для реализации своих планов развития [1.143]. Однако темпы развития IoT неравномерны. Так, власти провинции Цзянсу уже в 2009 г. подписали соглашение с КАН и муниципалитетом города Уси о совместном создании китайского Центра научных исследований и разработок в области интернета вещей [1.150]. В том же году власти города Уси первыми подали заявку в Государственный совет о присуждении статуса «Пилотного города IoT». Примеру этого города последовали города соседней провинции Чжэцзян – Ханчжоу и Цзясин. В партнерстве с КАН власти города Ханчжоу учредили Инновационный центр технологий RFID. Также в городе был построен индустриальный парк IoT для продвижения промышленного развития в областях умных транспортных систем, городского управления и информационной безопасности. В Пекине в районе Чжунгуаньцунь, известном как «Китайская силиконовая долина», в ноябре 2009 г. была учреждена отраслевая Ассоциация интернета вещей. Кроме того, в ответ на общегосударственный план «Sensing China» муниципальные власти запустили свою собственную инициативу с идентичным названием. Власти Пекина стремятся

привлечь в город команды разработчиков, реализующих проекты в области интернета вещей и поддержать лучших из них. В 2010 году в 43 таких проекта было инвестировано 60 млн. юаней. Впоследствии 17 из этих проектов были выбраны для следующего раунда поддержки. Другие города также активно развивают проекты в области IoT [1.142]. Например, правительство города Уси ежегодно проводит конкурс инноваций, призовой фонд которого составляет 10 млн. юаней (1,5 млн. долл.) [1.145]. При строительстве «умных городов» многие местные власти занимаются внедрением новых строительных норм.

Таким образом, в Китае реализуется как централизованная, так и региональная политика поддержки IoT. Данная технология была признана ключевой для развития ряда отраслей, преодоления негативных последствий бурного роста экономики, и для создания «умных городов». При этом стимулируется масштабное использование IoT, в том числе за счет диверсификации мер поддержки, от финансовых инструментов до нормативно-правового регулирования, включая работу центральных властей и провинций по разработке стандартов в области IoT.

1.5.2 США

Принципы поддержки технологий интернета вещей в США находятся в русле общей государственной парадигмы развития научно-технологической и инновационной сферы. Роль государства заключается в создании экосистемы, способствующей появлению новых технологий. Основными элементами этой парадигмы являются стимулирование лидерства частного сектора в развитии технологий и стандартов, и разработка государственной политики при участии всех заинтересованных сторон (стейкхолдеров).

Для технологий интернета вещей государственная стратегия не разрабатывалась, однако отдельные ведомства обозначили важность данного направления. В 2008 г. Национальный разведывательный совет США назвал технологии интернета вещей прорывными [1.151]. Сенат в 2015 г. принял

резолюцию о важности разработки стратегии развития интернета вещей [1.152].

Среди основных государственных органов и агентств, которые занимаются теми или иными вопросами в области интернета вещей, можно выделить:

- Министерство торговли США, а также входящие в его состав Рабочая группа по интернет-политике (ITPF), Руководящая группа по цифровой экономике (DELT), Национальный институт стандартов и технологий США (NIST) и Национальная телекоммуникационная и информационная администрация (NTIA);
- Конгресс США, включая обе палаты – Сенат и Палату представителей – а также аудиторский, оценочный и аналитически-следственный орган Конгресса – Счетную палату США (GOA);
- Министерство внутренней безопасности США, Министерство обороны, Федеральная торговая комиссия.

Активную деятельность ведет Торговая палата США, которая не является государственным органом, но лоббирует развитие интернета вещей в государственных структурах²⁵.

Основной вопрос, который решают государственные ведомства США, состоит в определении таких стимулов к развитию интернета вещей, которые бы не стали преждевременными и чрезмерно ограничительными, но при этом обеспечивали бы безопасность для потребителей, в том числе и самих госструктур. Прямые меры поддержки, которые реализует американское правительство, сосредоточены преимущественно на создании «умных городов». В рамках инициативы Белого дома по Умным городам, в 2015 г.

²⁵ В настоящее время ТП США является крупнейшей в мире организацией такого рода, в состав которой входят свыше 3 миллионов компаний, почти 3 тыс. торговых палат отдельных штатов и муниципальных образований, 830 ассоциаций и 111 американских торговых палат в зарубежных странах. Следует отметить, что 96% членов – это компании с числом занятых менее 100. Основная задача, которую выполняет ТП США – лоббирование интересов американского делового сообщества в Конгрессе США, Администрации, регулирующих органах, судах, работа с общественностью и правительствами зарубежных стран.

правительство выделило 160 млн. долл. на исследования и технологические партнерства в этой области [1.153], а в 2016 г. - еще 80 млн. долл. При этом количество участвующих городов и сообществ достигло 70 [1.154].

1.5.2.1 Деятельность Министерства торговли США и его подразделений

Министерство торговли США играет важную роль в государственной политике по развитию интернета вещей. Среди основных тем, которые находятся в зоне внимания министерства с IoT связаны кибербезопасность, обеспечение конфиденциальности, трансграничные потоки данных, частотный ресурс, международная торговля, новые производственные технологии, защита интеллектуальной собственности, политика стандартизации, управление интернетом, большие данные, предпринимательство и компетенции кадров.

Министерство торговли США в лице агентства NTIA в апреле 2016 г. в рамках своей повестки по цифровой экономике начало сбор мнений по теме «Преимущества, вызовы и потенциальная роль государства в содействии продвижению интернета вещей» [1.155]. Запрос на комментарии был открытым, и отреагировать на него могли все заинтересованные стороны. При этом министерство подчеркнуло, что пока ни один из государственных органов США не имеет целостного взгляда на развитие данной области, и потому важна инициатива бизнеса и его участие в поиске решений, которые определяли бы возможности и риски развития IoT.

По результатам сбора комментариев в январе 2017 г. была издана «Зеленая книга» под названием «Ускоряя продвижение интернета вещей» [1.156]. Ее цель состояла в определении элементов политики, которую должно реализовывать министерство в области развития интернета вещей. Были сформированы следующие основные принципы такой политики, согласно которым министерство:

- станет инициатором мер по созданию инклюзивной и широкодоступной для потребителей, работников и бизнеса экосистемы интернета вещей;

- будет давать рекомендации по политике и предпринимать меры по поддержке стабильного, безопасного и заслуживающего доверия IoT;
- будет продвигать и защищать глобальную, открытую и совместимую экосистему IoT, построенную на стандартах, инициированных компаниями и принятых на основе консенсуса;
- будет стимулировать рост и инновации в области интернета вещей, поддерживать расширяющиеся рынки и снижать входные барьеры, привлекать заинтересованные стороны к поиску ответов на политические вызовы.

На основе этих принципов министерство выделило четыре основные области своей деятельности, объединив как применявшиеся ранее меры, так и те, которые только запланированы. Во-первых, это обеспечение доступности на условиях равенства и социальной справедливости в условиях повышенного спроса со стороны пользователей решений интернета вещей на инфраструктуру, частоты и распространение интернет-протокола IPv6. Во-вторых, проведение сбалансированной политики и формирование коалиций по таким вопросам, как кибербезопасность, защита частной информации, интеллектуальная собственность, свободный трансграничный поток информации. В-третьих, продвижение стандартов и развитие технологий. Четвертое направление деятельности связано со стимулированием развития рынков (государственно-частное партнерство и государственные закупки, вопросы трудовых ресурсов в области образования, подготовки и гражданских прав, статистические измерения рынка интернета вещей). Наиболее широкой является область безопасности применений IoT. В целом большинство мер носит просветительский или инфраструктурный характер с целью создания благоприятных условий без осуществления прямого вмешательства государства в развитие технологий и рынка. Единственным регулятивным пунктом является управление частотным ресурсом, который находится в ведении NTIA.

1.5.2.2 Законотворческая деятельность обеих палат Конгресса

Обе палаты Конгресса в последние годы запустили процессы по принятию законов, регулирующих интернет вещей. В частности Сенат инициировал законопроекты S.88 «Развитие инноваций и рост интернета вещей» (DIGIT Act, январь 2017 г.) [1.157], S.1691 «Акт по улучшению кибербезопасности интернета вещей 2017» [1.158], Палата представителей – H.R. 6032 «Состояние современных приложений, исследований и трендов интернета вещей» (SMART IoT Act, июнь 2018 г.) [1.159], H.R. 3388 «Обеспечение безопасного развития и исследований в области транспортных средств» (SELF DRIVE Act, июль 2017 г.) [1.160]. Ни один из этих законопроектов пока не принят – DIGIT Act с августа 2017 года находится на рассмотрении в Подкомитете по связи и технологиям Комитета энергетики и торговли Палаты представителей. SELF DRIVE Act с сентября 2017 г. находится на рассмотрении Комитета по торговле, науке и транспорту Сената. Акт по кибербезопасности был представлен в январе 2017 г. и отправлен на рассмотрение в Комитет по Национальной безопасности и Государственным делам. Наконец, самый «свежий» из законопроектов SMART IoT Act в июле 2018 г. был направлен на голосование в Палату представителей, но оно пока не состоялось. Согласно SMART IoT Act, глава Министерства торговли ответственен за проведение исследований рынка интернета вещей, как в отраслевых сегментах, так и в государственно–частных партнерствах и государственном секторе. Должны быть рассмотрены сферы ответственности и влияние на развитие интернета вещей отдельных государственных органов, применяемые ими регулятивные и иные меры. Кроме того, должна представляться информация по отраслевым инициативам, в том числе по стандартизации. В течение года после принятия данного акта Министр торговли должен представить обеим палатам Конгресса доклад, содержащий результаты проведенного исследования и рекомендации по стимулированию роста экономики на основе развития IoT.

Возможно, и этот акт ожидает такой же длительный,

как и у его предшественников, процесс принятия. С другой стороны, он является наиболее общим и его принятие может ускорить процесс прохождения остальных проектов. Кроме того, ускорить процессы принятия законопроектов на федеральном уровне может прецедентный кейс в Калифорнии, законодательное собрание которого в сентябре 2018 г. одобрило акт по информационной безопасности подключенных устройств. Он вступит в силу 1 января 2020 г. Еще одним важным событием на уровне штатов в этой области стала публикация аудиторского отчета штата Массачусетс по применению интернета вещей в органах управления штата. В отчете систематизированы потенциальные угрозы безопасности, связанные с использованием интернета вещей.

Близким по своей сути к этому проекту является запущенный ранее законопроект Сената DIGIT Act. Его основная задача — обеспечение рационального планирования при распределении частот и межведомственная координация поддержки интернета вещей. Согласно данному законопроекту министерство торговли должно создать из представителей федеральной власти рабочую группу для предоставления рекомендаций и доклада Конгрессу по развитию IoT. Рабочая группа определит, какие регулятивные меры, практики выделения грантов, бюджетные и нормативные ограничения мешают или могут помешать развитию интернета вещей. Также эта группа изучит вопросы, связанные с использованием технологий интернета вещей в государственных ведомствах. Кроме того, в министерстве должен быть создан Координационный комитет для консультирования Рабочей группы.

Стоит отметить и роль Счетной Палаты США, которая проводила исследования IoT по запросам представителей Конгресса. С мая по ноябрь 2017 г. были выпущены следующие доклады: «Интернет вещей. Текущее состояние и возможные последствия все более подключенного мира» [1.161], «Интернет вещей. Уточненные оценки и необходимые инструкции для решения вопросов оценки рисков безопасности в Министерстве обороны» [1.162], «Интернет вещей. Сообщества реализуют проекты при помощи сочетания федеральной

поддержки и других фондов и источников» [1.163], «Интернет вещей. Федеральная комиссия по связи должна отслеживать рост для обеспечения достаточного частотного ресурса» [1.164].

1.5.2.3 Деятельность других органов власти

Другие органы власти, в рамках своей компетенции, также рассматривали тематику интернета вещей. Так, в ноябре 2014 г. Консультативный комитет по связи в системе национальной безопасности США (National Security Telecommunications Advisory Committee, NSTAC) подготовил доклад президенту, в котором подчеркнул необходимость обеспечения развития максимально надежного IoT при минимизации рисков. Было указано, что окно возможностей для этого весьма узкое – от трех до пяти лет [1.165]. В свою очередь, Управление по контролю за качеством пищевых продуктов и лекарственных препаратов (Food and Drug Administration, FDA) озабочено подключением к сети медицинских устройств [1.166]²⁶. Главное управление по обеспечению безопасности дорожного движения (National Highway Traffic Safety Administration, NHTSA) – подключением автомобилей [1.167]. Федеральная Торговая комиссия (FTC) уделила внимание таким аспектам интернета вещей, как конфиденциальность и кибербезопасность. В частности, в 2015 г. FTC выпустила отчет о лучших практиках в этих областях [1.168, 1.169], а в 2017 г. объявила конкурс с общим фондом 34 тысячи долл. по созданию технического решения для потребителей, которое позволило бы им защититься от уязвимостей в используемых дома устройствах IoT [1.170, 1.171].

Федеральная комиссия по связи США (Federal Communications Commission, FCC) определяет диапазоны частот для устройств IoT. Действия FCC предполагают контроль над обширным спектром частот, разрешенных для использования в IoT-устройствах, а также при необходимости выделение дополнительных частот. С 2015 г. были введены 4 полосы частот до 11 ГГц. По-прежнему остается открытым вопрос мониторинга IoT-устройств, действующих на незарегистрированных частотах [1.172].

²⁶ Первичный вариант документа был опубликован в январе 2007 года

Министерство обороны, на которое по некоторым оценкам приходится 88% государственных расходов на интернет вещей, в 2016 г. выпустило «Рекомендации по политике в области интернета вещей», которые были посвящены общему обзору интернета вещей, а также возникающим рискам и возможностям [1.173].

Министерство национальной безопасности США также выпустило «Стратегические принципы обеспечения безопасности интернета вещей» (ноябрь 2016 г.), среди которых - учет требований безопасности на этапе разработки решений, продвижение обновлений и управление уязвимостями, развитие известных практик в области безопасности, приоритизация мер в зависимости от их потенциального эффекта, стимулирование прозрачности, обеспечение безопасного подключения [1.174].

Это далеко не полный перечень предпринятых различными органами США действий, касающихся развития «Интернета Вещей», однако он дает представление об общих подходах, практикуемых ведомствами США. Главный принцип деятельности – это обеспечение общего видения и нормативно-правового регулирования. Прямые меры поддержки используются редко, и касаются только отдельных направлений развития интернета вещей (умных городов). Важно также отметить, что основные прямые государственные расходы на развитие интернета вещей несет Министерство обороны США.

1.5.3 Франция

1.5.3.1 Инициирование поддержки

Компании, работающие в области интернета вещей, изначально развивались во Франции без специализированной поддержки со стороны государства. По данным EuroRFID, на конец 2013 г. во Франции уже был целый ряд растущих компаний, предоставляющих решения в сфере интернета вещей. Среди них - Sen.Se, Withings, JoshFire, Natatmo, Connectthings и другие.

Государственная поддержка началась в 2015 г. Правительство Франции оценило интернет вещей как перспективный

рынок и социальный тренд, который также, как в свое время интернет, откроет новые возможности для французских предприятий и граждан. Роль правительства была определена как содействие в преодолении технологических и социальных барьеров развития интернета вещей, а также решение проблем безопасности и хранения данных [1.175]. Среди государственных институтов, вовлеченных в поддержку интернета вещей, можно выделить экономическое агентство при правительстве Франции France Strategie, которое занимается программой «Индустрия будущего», Генеральную дирекцию предприятий Франции (DGE), Национальную комиссию по информатике и гражданским правам (CNIL), регулирующий орган в области телекоммуникаций ARCEP, Национальное агентство безопасности информационных систем (ANSSI), Национальное агентство по частотам (ANFR) [1.176]. Реализация поддержки осуществляется по трем основным направлениям:

- программа «Новая промышленная Франция»;
- программа «French Tech»;
- мягкая регуляторная политика ARCEP.

1.5.3.2 Целеполагание в области интернета вещей

Программа «Новая промышленная Франция». Программа была запущена в мае 2015 г. с целью реиндустриализации Франции путем стимулирования компаний к модернизации своих промышленных активов и трансформации экономической модели на основе цифровых технологий. В данной программе выделено девять основных индустриальных решений, три из них названы цифровыми, они сгруппированы и отнесены к интернету вещей:

- экономика данных (цифровая экономика) – для создания ценности посредством использования имеющихся данных, объемы которых растут экспоненциально. Возможности эффективного использования этих данных основаны на технологиях Больших Данных, Облачных вычислений и суперкомпьютеров;
- цифровое доверие (confiance numérique) — для сохранения технологического суверенитета стратегических

отраслей, усиления безопасности и повышения уровня доверия в цифровом мире, обеспечение развития во Франции компаний этих отраслей;

- умные устройства – для улучшения повседневной жизни жителей Франции посредством развития новых практик.

В декабре 2016 г. была опубликована дорожная карта по интернету вещей, учитывающая три перечисленные выше направления. Она стала дополнением к карте, применяемой в рамках тематической сети French Tech #IoT для поддержки стартапов в сфере интернета вещей, и к мерам, реализуемым ARCEP. В ней выделено четыре направления работы и одиннадцать задач (Таблица 1.11).

Таблица 1.11— Направления и задачи Дорожной карты «Интернет Вещей» программы «Новая промышленная Франция»

Направление	Задачи
Стимулирование дальнейшего роста предложения отечественных товаров и услуг в области интернета вещей	<ol style="list-style-type: none"> 1. Реализовать пилотные проекты в рамках инициативы France Expérimentation для подтверждения концепции и роста осведомленности общества; 2. Удостовериться в развитии защищенных и гибких элементов инфраструктуры;
Обеспечение распространения технологий среди компаний и населения	<ol style="list-style-type: none"> 3. Запустить конкурсы по цифровым технологиям, касающимся интернета вещей; 4. Повысить заинтересованность компаний в использовании возможностей интернета вещей;
Создание доверительной среды	<ol style="list-style-type: none"> 5. Снять опасения частных и профессиональных пользователей по поводу защиты и хранения данных; 6. Оказать поддержку компаниям в вопросах использования и обеспечения безопасности данных; 7. Стимулировать развитие элементов, архитектур, протоколов, облачных технологий и др. для интернета вещей;

Развитие национальной экосистемы интернета вещей	<ol style="list-style-type: none"> 8. Способствовать развитию производства подсоединенных вещей во Франции в средних и крупных масштабах; 9. Создать платформу, посвященную интернету вещей, которая позволит информировать и быстро устанавливать связь между поставщиками технологий интернета вещей и потребителями; 10. Поддерживать развитие стартапов в сфере интернета вещей; 11. Развить образовательные программы по специальностям интернета вещей, в частности в рамках сети La Grande Ecole du Numérique
--	--

Источник: составлено авторами по данным [1.177]

В рамках программы «Новая промышленная Франция» существует еще один значимый документ, который затрагивает интернет вещей: это перечень ключевых технологий для Индустрии Будущего, составленный Генеральной дирекцией предприятий Франции в 2016 г. по итогам исследования, начатого в 2014 году. Интернет вещей вошел в данный перечень в качестве сквозной технологии с применением в 9 областях (пищевая промышленность, энергетика, мобильность, цифровая экономика, досуг и культура, защита окружающей среды, безопасность, здоровье и благосостояние, частные и общественные помещения).

Программа French Tech была учреждена Министерством экономики и финансов Франции в конце 2013 г. [1.178] с целью содействия созданию французских стартапов, поддержке их роста и развития на международной арене, а также продвижения французской стартап-экосистемы за рубежом. Программа направлена на выравнивание законодательства и увеличение прозрачности деятельности органов государственной власти по отношению к стартапам и представляет собой совместный проект государства и других субъектов экономики. Задача правительства состоит в том, чтобы сделать известные инструменты поддержки более эффективными в отношении инициатив, исходящих от предпринимателей и региональных властей. Приоритет отдается предложениям

со стороны стартап-сообществ. Именно поэтому под French Tech понимают экосистему французских стартапов – предпринимателей, инвесторов, инженеров, дизайнеров, разработчиков, большие группы компаний, ассоциации, СМИ, исследовательские центры и других, имеющих отношение к функционированию стартапов. Ее участники представлены под коллективным брендом La French Tech, что создает для них дополнительные преимущества.

За реализацию инициативы French Tech отвечает небольшая рабочая группа, сотрудники которой тесно взаимодействуют с соответствующими управлениями Министерства экономики и финансов (Главное управление предприятий, Главное управление казначейства), управлениями Министерства Европы и иностранных дел и Генеральным комиссариатом по инвестициям [1.178, 1.179]. С февраля 2015 г. обеспечением проведения инициатив в рамках программы French Tech стало заниматься Цифровое агентство, которое было учреждено при Государственном секретариате цифровой экономики и инноваций в составе Генерального управления предприятий Министерства экономики и Финансов Франции. Среди партнеров проекта French Tech есть несколько французских банков – французский государственный банк развития Caisse des dépôts et consignations (CDC), Государственный инвестиционный банк Bpifrance и Агентство по развитию экономической деятельности французских предприятий на международной арене Business France [1.180].

В программе French Tech применяются два нефинансовых инструмента поддержки: знак соответствия «Метрополия французских технологий» (Métropoles French Tech) и тематические сети French Tech. Знаки соответствия были присуждены городам с благоприятной для высокотехнологичных стартапов экосистемой [1.181]. Тематические сети представляют собой объединения территорий, которые функционируют как деловые сообщества, стимулирующие развитие стартапов определенной тематики во Франции и за рубежом. Девять тематических сетей были впервые представлены Миссией French Tech в июле 2016 г., и одна из них сфокусирована

на интернете вещей и промышленности: «Réseau Thématique #IOT #Manufacturing». В сеть входят 16 членов, 9 из них имеют статус метрополий. У сети есть достаточно лаконичная дорожная карта, включающая четыре направления деятельности [1.182, 1.183]:

- организация встреч «Meetup IoT & Manufacturing» – серия мероприятий, проводимых во Франции при участии членов сети интернета вещей и промышленности;
- продвижение программы Pass French Tech. Это запущенная в 2014 г. национальная программа по поддержке компаний с очень высокими темпами развития, входящих в сети French Tech [1.184]. Компании Pass French Tech получают разные виды финансовой и нефинансовой поддержки (консультации, продвижение на зарубежные рынки, пиар). Программу можно рассматривать как аналог российской инициативы «Национальные Чемпионы»;
- доклад по привлекательности IoT-экосистемы Франции – документ, направленный на продвижение французской экосистемы «Интернет вещей и Промышленность» на международном уровне с целью привлечения иностранных инвестиционных фондов и предпринимателей;
- международные мероприятия, в том числе участие французских компаний под единым знаком French Tech в международных салонах, таких как Международная выставка потребительской электроники (CES, Лас-Вегас), Mobile World Congress (Барселона), Ганноверская промышленная выставка-ярмарка, IFA Berlin, а также взаимодействие с лидерами государств и международных компаний во время мероприятий мирового уровня, проводимых во Франции. К таким мероприятиям относятся Шоурум интеллекта вещей (Le Showroom de l'Intelligence des Objets (SIDO), Леон), Viva Technology (Париж), World Electronic Forum (Анже).

Деятельность ARCEP в области интернета вещей. Цель деятельности регуляторного органа электронных средств

связи и почты ARCEP в области интернета вещей заключается в содействии самоорганизации экосистемы. Основным инструментом является картирование целей внедрения решений интернета вещей. В свою деятельность ARCEP активно вовлекает как другие органы власти, так и представителей бизнес–сообщества (Intel, Huawei, Bouygues Telecom, Sigfox, Legrand, IBM и др.).

ARCEP стал активно заниматься продвижением интернета вещей с 2015 г., а с 2016 г. эта тематика была выделена в отдельное направление. Задача ARCEP — гарантировать доступность дефицитных ресурсов (IP адреса, коды сети, доступ к частотному спектру и т.д.) для поддержания развития сетей интернета вещей, умных городов и регионов [1.185].

ARCEP выделяет четыре крупных направления – Связь, Безопасность, Данные, Совместимость – и узкие задачи, которые необходимо решить [1.186]:

- гарантировать множество каналов мобильной, надежной, недорогой связи;
- обеспечить доступность дефицитных ресурсов – частот и идентификаторов;
- обеспечить открытость рынка для всех участников;
- оказывать поддержку участникам рынка, стимулировать развития экосистемы.

В рамках этой деятельности ARCEP опубликовал в 2016 г. Белую книгу по интернету вещей, которая состоит из двух частей: дорожной карты целей и описание стимулирующей инновации регуляторной политики. Первая часть посвящена широкому перечню общих вопросов интернета вещей: определением, обсуждению ценности технологий, экосистеме, инфраструктуре каналов связи и требованиям к ней, дефицитным ресурсам, необходимым для развития сферы IoT (в том числе частотам), открытости технологий и совместимости решений, вопросам доверия, а также взаимодействию государства и бизнеса в вопросах развития данной области, международной политике. Второй раздел описывает пять направлений деятельности для улучшения регулирования интернета вещей. Один из примеров в этом направлении

– это так называемая регулятивная «песочница», направленная на создание благоприятных условий для компаний, реализующих проекты в области цифровой экономики. Компании, чьи инновационные проекты используют частоты, распределяемые ARCEP, в течение двух лет могут тестировать свои проекты без соблюдения регулятивных мер, которые в ином случае были бы к ним применены.

1.5.3.3 Финансирование

В рамках программы «Новая промышленная Франция» существуют межотраслевые и специфические инструменты финансирования. Для интернета вещей [1.187] применимы следующие инструменты:

- «Фонд цифровых перспектив» (Fonds ambition numérique). Фонд создан для поддержки стартапов в области цифровых технологий в рамках программы «Инвестиции в будущее» и управляется Bpifrance. Фонд может выступать соинвестором частных инвестиций в форме покупки миноритарной доли в компании на сумму от 1 до 10 млн. евро; не участвует в стадии запуска проекта [1.188];
- Fonds 3A (Fonds Ambition Amorçage Angels), задача которого состоит в софинансировании инвестиций, осуществляемых бизнес-ангелами на стадии запуска бизнеса [1.189];
- программа «Большие цифровые вызовы», предусматривающая предоставление субсидии или беспроцентного возвратного займа в размере от 30 до 50% от общей стоимости проекта. На данный момент 2 из 17 поддержанных проектов относятся к интернету вещей.

Помимо этого, в июле 2018 г. был запущен конкурс «Voucher IoT». Цель конкурса – помочь молодым компаниям–производителям подключенных устройств, которые впервые внедряют свои разработки. Производители IoT устройств могут получить субсидию на оплату услуг компаний по заключенным договорам в размере до 15% от общей суммы контракта.

Все инструменты финансирования Программы French Tech являются общими для всех приоритетных тематик. Соответственно, интернет вещей не выделяется с точки зрения мер регулирования. French Tech предоставляет два вида поддержки:

- софинансирование частных акселераторов для стартапов (200 млн. евро);
- финансирование повышения международной привлекательности (15 млн. евро).

Кроме того, в рамках данной инициативы была запущена специальная программа для привлечения иностранных предпринимателей – French Tech Ticket. По ней можно получить финансирование в размере 45 тыс. евро на команду, есть упрощенная процедура получения вида на жительство, акселерационная программа, бесплатное место на год в одном из 41 партнерских бизнес-инкубаторов, помощь в оформлении документов и консультирование по всем вопросам жизни во Франции.

Общее финансирование French Tech включает кроме государственных средств также и частные французские и иностранные инвестиции в компании, входящие в экосистему French Tech. Компании-участники French Tech в 2017 г. смогли привлечь более 2,161 млрд. евро в результате проведения 517 сделок – это максимальный объем инвестиций за все время действия Программы [1.190].

1.5.3.4 Результаты государственной политики Франции в области интернета Вещей

Франция изначально имела неплохие позиции для развития интернета вещей: в стране самостоятельно развивались компании, были созданы две передовые сети для IoT – LoRA и Sigfox. В стране есть хорошие наработки в области безопасности и защиты персональных данных. Внимание государства к этой сфере, вероятно, стало следствием успехов французских компаний и одновременно результатом влияния мирового тренда развития интернета вещей. После 3 лет государственной поддержки можно говорить о появлении некоторых результатов [1.175].

По данным исследования компании Wavestone 61% инвесторов отнесли Францию к пяти наиболее привлекательным странам для инвестирования в технологии Deep Tech. При этом 88% инвесторов считают, что данный сегмент будет развиваться во Франции быстрее, чем в других странах Европы, в том числе благодаря выдающимся результатам в области IoT [1.191]. На одной из самых значимых конференций в мире в сфере IoT CES 2017 на выставке Eureka Park 36% компаний были французскими [1.192]. Во Франции за это время выросли такие значимые игроки, как Sigfox, LoRa Alliance, Actility, а также Parrot, Netatmo, Devialet, Legrand, Somfy и другие.

Ярким примером развития французской компании в области «Интернета Вещей» является компания Sigfox. Компания, обеспечивающая беспроводную низкоскоростную связь устройств в сетях с низким потреблением энергии, запатентовала свою технологию в 2009 г. В 2012 г. она привлекала частные инвестиции (в том числе компании Intel) в размере 10 млн. евро и развернула первую сеть во Франции [1.193]. В 2013 г. Sigfox впервые привлекла государственные инвестиции в рамках программ «Цифровая цель» (Ambition Numérique) фонда «Инвестиции в будущее» и государственного фонда Large Venture [1.194]. Стоит отметить, что фонд Large Venture предоставляет средства только компаниям, уже привлечшим венчурные средства и софинансирует новые раунды инвестиций [1.195]. С каждым годом стартап привлекал все больше частных инвестиций, при этом фонд Large Venture участвовал в новых этапах финансирования. На данный момент компания привлекла более 270 млн. евро [1.196] и имеет представительства на территории 45 стран; до конца 2018 г. сеть Sigfox планирует развернуть свою деятельность уже в 60 странах [1.197].

По мнению аналитиков IDG Connect [1.198], благодаря успеху французских стартапов в сфере IoT Франция может стать лидером в интернете вещей. Успех компаний причисляют к удачной комбинации технологических компетенций и амбиций. Среди положительных факторов обозначены рост значимости стартапов в корпоративной среде, усиление

взаимодействия между крупными компаниями и стартапами, смещение фокуса с B2C решений на B2B, установление контакта между промышленными компаниями и стартапами, глубина инженерных компетенций. Как мы видим, достигнутые результаты перекликаются с задачами, которые были поставлены в рамках целеполагания в области IoT.

О переходе рынка интернета вещей Франции в качественно новое состояние говорит доклад института рыночных исследований GfK. По данным института, объем рынка интернета вещей во Франции в 2017 г. преодолел отметку в 1 млрд. евро (физический объем – 5,2 млн. устройств в год). По всем показателям наблюдаются двухзначные темпы роста [1.199]. Например, сегмент «Умный дом», на который приходится 2/3 рынка, в физическом объеме вырос на 42%.

Есть и первые результаты целевых мер государственной поддержки. На данный момент в тематическую сеть French Tech #IoT #Manufacturing входят 907 стартапов [1.200]. Из 535 французских стартапов, успешно осуществляющих свою деятельность за границей, IoT- компании составляют 4,2% [1.201]. 9 стартапов из сферы IoT входят в число быстроразвивающихся высокотехнологичных компаний программы Pass French Tech [1.184].

Однако, в области государственного регулирования этой сферы остается целый ряд проблемных областей. Одна из них – низкий уровень коммерциализации данных. По информации агентства Forrester, только 35% компаний во Франции пользуются данными с IoT устройств в коммерческих целях [1.202]. Все еще медленно развивается потребительский сектор интернета вещей, несмотря на то, что среди французских компаний есть мировые лидеры (Netatmo, Withings, Parrot, Awox и др.) [1.176]. Кроме того, не до конца решены общие для всех проблемы – безопасность и конфиденциальность.

1.5.4 Германия

Интернет вещей в Германии не относится к числу специально поддерживаемых технологических направлений. Упоминания о нем можно найти в программах и стратегиях,

направленных на индустриальное развитие и цифровизацию экономики. Кроме того, сама интерпретация IoT характеризуется переплетением и взаимосвязью таких понятий, как «Интернет Вещей», «Киберфизические системы» и «встроенные системы». Поэтому нет мер и инструментов, которые однозначно можно было бы отнести к поддержке IoT.

В ноябре 2010 г. Федеральное министерство экономики и энергетики Германии (BMWi) представило первую стратегию цифрового развития Германии «Цифровая Германия 2015». Одним из направлений программы были заявлены исследования и разработки в области IoT [1.203]. И уже в этой программе появилось несколько терминов, которые в целом можно считать IoT: киберфизические системы (CPS), встроенные системы, а также Интернет Услуг [1.204]²⁷. В последующих государственных программах появилось понятие «Интернет Вещей и Услуг» (Internet of Things and Services, далее IoTS), которое, однако, не было четко определено. При этом, Агентство экономического развития Германии Germany Trade & Invest предложило схему, которая частично объясняет предполагаемую взаимосвязь всех упомянутых выше понятий (Рис. 1.35).

Согласно Germany Trade & Invest²⁸, федеральное правительство поддерживало IoTS в рамках стратегии «Высокие технологии» с 2006 г. [1.206]. Данная стратегия предполагала многомиллиардные ежегодные инвестиции в развитие наиболее перспективных технологий. В 2010 г. была опубликована обновленная «Стратегия в области высоких технологий 2020». В ней была обозначена необходимость разработки

²⁷ Ключевая идея «Интернета Услуг» заключается в создании новой ценности в секторе услуг при помощи подключения к интернету.

²⁸ Germany Trade & Invest является Агентством экономического развития Федеративной Республики Германии. Агентство создает и сохраняет рабочие места, укрепляя таким образом экономику Германии. Имея более 50 представительств и разветвленную партнерскую сеть по всему миру, Germany Trade & Invest поддерживает немецкие компании при их выходе на зарубежные рынки, продвигает Германию как площадку для ведения бизнеса и сопровождает зарубежные компании при размещении их бизнеса в Германии. Деятельность агентства поддерживается BMWi.

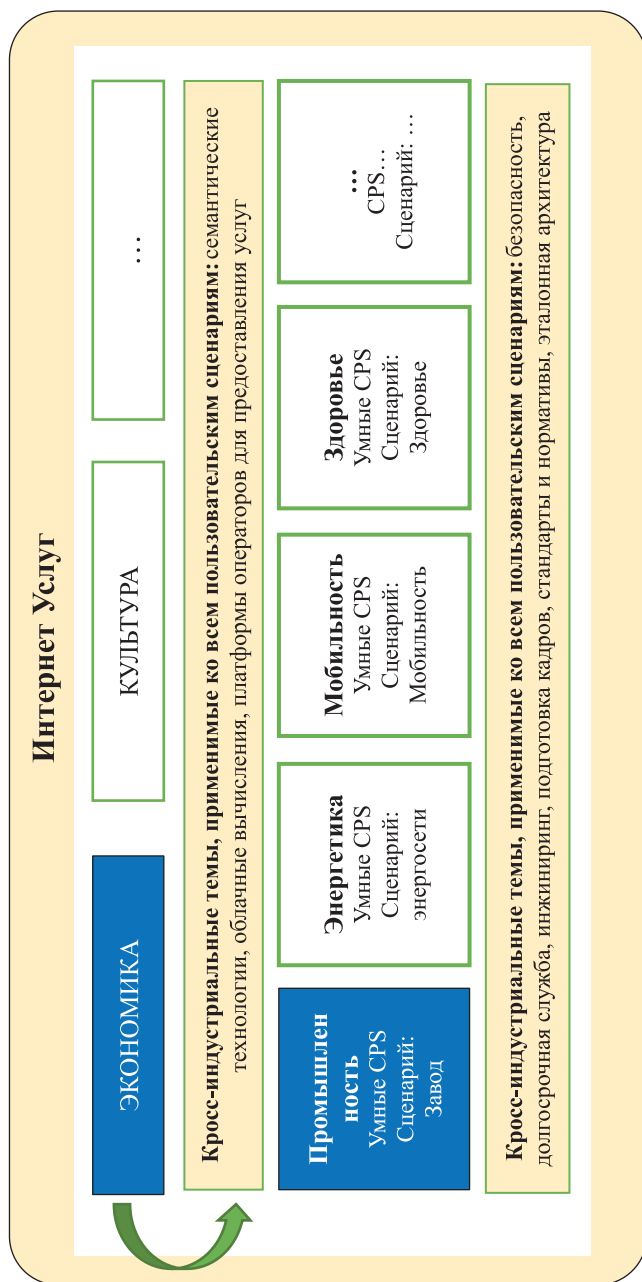


Рисунок 1.35— Интернет Вещей и Услуг
Источник: [1.205]

национальной дорожной карты для встроенных систем и интернета вещей при участии различных заинтересованных сторон и отраслей, а также активизация исследований и продвижения «умных вещей» с особым акцентом на промышленную робототехнику [1.203]. Кроме того, в 2012 г. правительство выпустило «План действий Стратегии в области высоких технологий 2020», где были определены 10 «Проектов будущего», среди которых выделяется стратегическая инициатива «Индустрия 4.0» [1.206].

Программа «Индустрия 4.0» – национальная стратегическая инициатива, реализуемая Федеральным министерством образования и научных исследований (BMBF) и BMWi. Инициатива поддерживает интеграцию киберфизических систем и IoTS для повышения продуктивности, эффективности и гибкости производственных процессов с целью ускорения экономического роста. Ключевой задачей инициативы являются структурные изменения в промышленности посредством внедрения технологий IoTS и CPS [1.207]. Киберфизические системы и интернет вещей и услуг считаются движущей силой новой промышленной революции. Федеральное министерство образования и научных исследований Германии суммарно выделило 120 млн. евро на исследования в области CPS, IoTS и Индустрии 4.0. Министерство экономики и энергетики, которое отвечает за стандартизацию в области Индустрии 4.0, выделило 80 млн. евро на исследования в рамках этой программы [1.207]. Кроме того, в 2015 г. правительство придало государственный статус частной инициативе «Платформа Индустрии 4.0», которая была создана тремя предпринимательскими ассоциациями – Bitkom (Федеральная ассоциация информационных технологий, телекоммуникаций и новых средств связи), VDMA (Ассоциация немецких машиностроителей), и ZVEI (Немецкая ассоциация производителей электрических компонентов и электроники) в 2013 г. [1.208]. Платформа представляет информационный ресурс для различных участников инициативы. В частности, на сайте платформы есть своя онлайн-библиотека, где публикуются доклады и отчеты по различным тематикам Индустрии 4.0, карта «Кейсы использования Индустрии 4.0», представляющая

примеры практического применения в этой области (186 кейсов) [1.209], даны ссылки на аналогичные карты Франции и Японии [1.210]. Там же можно найти карту более 500 испытательных центров и центров компетенций [1.211], которая показывает расположение институтов, ведущих НИОКР в области Индустрии 4.0. Особое внимание уделяется международному сотрудничеству: заключены соглашения с Францией, Италией, Китаем, Японией, США, Чехией и Австралией, ведется активное продвижение в рамках G20 [1.212].

Платформа «Индустрии 4.0» участвуют в разработке стандартов. Рабочей группой «Эталонная архитектура, стандартизация и нормы» была разработана эталонная архитектура RAMI 4.0 для промышленного производства. В 2017 г. она стала официальным немецким стандартом (DIN SPEC 91345) и получила статус предварительного международного стандарта МЭК (IEC PAS 63088) [1.213].

Инициатива «Индустрия 4.0» интегрирована в другие действующие программы правительства, такие, как «Цифровая стратегия», «Национальная Дорожная карта по встроенным системам» (2009 г.), «ИКТ 2020: Исследования для инноваций», «Автономные системы для Индустрии 4.0», «Киберфизические производственные системы», «Умные данные». Все они в той или иной форме упоминают интернет вещей.

Так, в рамках программы «ИКТ 2020: Исследования для инноваций» предусматривается финансирование исследовательской деятельности в области CPS, встроенных систем и IoTS. Другая программа, которая также подразумевает финансирования технологий интернета вещей – «Автономные системы для Индустрии 4.0» – является технологической программой, инициированной Министерством экономики и энергетики в рамках достижения целей «Стратегии в области высоких технология 2020». Программа «Автономные системы для Индустрии 4.0» должна обеспечить автоматизацию при помощи технологий IoTS. Реализация этой программы, в частности, продвинула разработку сенсорных технологий [1.214].

Развитие интернета вещей также было затронуто в программах, предшествовавших «Автономным системам

для Индустрии 4.0»: «Средства информации следующего поколения» (новые технологии и повсеместные вычисления, 2004 г.) [1.215] и «Автономные системы» [1.206]. Программа «Автономные системы» входила в число ключевых при реализации стратегии «Цифровая Германия 2015» (2010 г.). В этой стратегии интернет вещей был назван одной из ключевых областей исследования. Стратегия предусматривала развитие продуктовых инноваций и инновационных бизнес-моделей для таких рынков, как, например, домашние роботы. Кроме технологической программы «Автономные системы» в число мер по развитию интернета вещей в этом документе также входили государственная инициатива «Подключенное жилье», «Национальная Дорожная карта по встроенным системам», «Лучшие кластеры по программному обеспечению» [1.216].

В рамках «Цифровой Стратегии 2025» отмечен большой потенциал развития, связанный с IoT: по оценкам правительства, IoT может стать источником экономического роста в размере 11 млрд. долл., при этом большая часть этой суммы придется на промышленное производство. Кроме того, в документе подчеркнуто, что технологические программы будут постоянно улучшаться и расширяться для того, чтобы включить новые тематики в области интернета вещей [1.217].

Это неполный перечень документов (в том числе Белых и Зеленых книг), стратегий, программ и платформ, которые затрагивают интернет вещей или его компоненты. Однако из перечисленных примеров следует, что деятельность правительства Германии в области поддержки интернета вещей не сфокусирована. Она расплывлена по множеству государственных планов и инициатив и носит скорее декларативный характер. Об этом свидетельствуют и исследования экономистов, посвященных «Индустрии 4.0». В частности, утверждается, что, несмотря на внимание ключевых германских политиков к теме «Индустрия 4.0», а также на выпуск разнообразных стратегических документов, в сфере инновационного развития не произошло резкого роста числа государственных проектов [1.218].

Таким образом, несмотря на то, что интернет вещей в Германии декларируется как один из инструментов достижения

стратегических целей, стоящих перед страной, он не получает специальной государственной поддержки. Государственная политика в отношении IoT фрагментарна и направлена на отдельные элементы IoT в множестве различных программ и проектов, а не на систему в целом. Она размыта в промышленной политике страны, которая, впрочем, дает определенную отдачу, важную для развития IoT, например, принятие стандарта эталонной архитектуры RAMI 4.0.

1.5.5 Россия

1.5.5.1 Приоритетность тематики

В России государственная политика по продвижению интернета вещей имеет относительно недолгую историю. Внимание к технологиям, важным для развития интернета вещей, усилилось в 2015 г. в связи с началом развертывания Национальной технологической инициативы (НТИ). В рамках НТИ были определены «сквозные технологии» — ключевые научно-технологические направления, которые оказывают определяющее влияние на то, чтобы Россия расширила свое присутствие на перспективных рынках. К числу таких «сквозных технологий», имеющих значение для развития интернета вещей, можно отнести «технологии беспроводной связи», «большие данные», «сенсорику», «новые производственные технологии». Примерно в тот же период времени по запросу Министерства промышленности и торговли РФ начал разрабатываться ряд «дорожных карт» по развитию интернета вещей.

В 2017 г. была утверждена «Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы», в которой дано свое определение интернета вещей (интернет вещей - концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека), а направление «интернет вещей и индустриальный интернет» названо одним из ключевых для развития российских информационных и коммуникационных технологий [1.3]. В том же году в целях реализации данной стратегии была принята

государственная программа «Цифровая экономика Российской Федерации» (далее – ЦЭ), в которой также перечислены «сквозные технологии», одна из которых – «промышленный интернет вещей». Таким образом, государственное содействие развитию технологий интернета вещей имеет менее, чем пятилетнюю историю. Значительно раньше технологиями интернета вещей стали заниматься российские компании, однако их деятельность не поддерживалась в рамках какой-либо официальной государственной политики.

1.5.5.2 Дорожные карты «Интернета Вещей»

Первая дорожная карта (ДК) «Интернета Вещей» (ИВ) – «Развитие технологий в области интернета вещей» – была составлена в 2016 г. при участии Фонда развития интернет-инициатив (ФРИИ) и по поручению Минпромторга [1.219]. ФРИИ организовал экспертную группу из представителей науки и бизнеса. Главной целью, сформулированной в ДК, было повышение качества жизни населения и рост конкурентоспособности. ДК включала блоки по развитию инфраструктуры, широкополосного доступа, стандартам протокола в области индустриального интернета. Отдельный большой блок был по микроэлектронике, с идеей организации производства на территории России. Побочным эффектом данной работы стало учреждение осенью 2016 г. Ассоциации интернета вещей. Ассоциация нацелена на то, чтобы ее члены – компании разных размеров, университеты и НКО – развивались и продвигали данную технологическую область. Для компаний важен рост продаж, а также совместная разработка стандартов, для вузов – современные учебные программы по IoT. Среди членов ассоциации есть такие операторы связи, как МТС и Мегафон, среди вузов – Сколтех, МГТУ им. Баумана, МИЭТ, ВШЭ, Донской государственный технический университет, Южно-российский государственный политехнический университет. Для вузов важно обновление содержания образовательных программ, и Ассоциация может помочь это сделать с помощью компаний-участников, а также благодаря наработкам по ДК. Такая сетевая структура помогает развиваться всем ее участникам.

После первой ДК последовали еще две, также по заказу Минпромторга. Вторая карта называлась «Интернет + город», и она затрагивала более широкие области. Третья ДК была связана с IoT в сельском хозяйстве – «Внедрение технологий интернета вещей в агропромышленном комплексе». Эту карту согласовали со всеми заинтересованными ведомствами, однако ни одна из карт не стала руководством к действию.

Таким образом, первые дорожные карты касались трех отраслей: промышленности, ЖКХ и сельского хозяйства. При этом в общей дорожной карте по развитию технологий в области IoT акцент сделан именно на промышленности. Интернет вещей рассматривается как усовершенствование автоматизированных информационных систем управления и общих подходов к управлению предприятиями и организациями.

В июле 2017 г. была утверждена программа «Цифровая экономика Российской Федерации», где промышленный интернет вещей определен в качестве одной из сквозных технологий. Часть разработчиков первых дорожных карт ФРИИ стали участниками формирования программы ЦЭ. Программа ЦЭ постоянно развивается и дополняется новыми блоками. Интернет вещей упоминается в ней в нескольких направлениях, в первую очередь связанных с безопасностью, обеспечением конфиденциальности, и со стандартами (создание и обеспечение правового режима в области сбора, хранения, обработки и использования данных, функционирование машинных и когнитивных интерфейсов, защита прав и свобод личности). Информационная инфраструктура ЦЭ также отчасти будет базироваться на технологиях IoT: для них планируется построить узкополосные беспроводные сети связи. В проекте перспективного нового направления по сельскому хозяйству среди предметных задач цифровой трансформации сельского хозяйства выделено внедрение платформ интернета вещей.

Наряду с разработкой ДК ФРИИ провел ряд мероприятий по поддержке IoT. В 2016 г. Фонд заявил, что готов вкладывать в российские команды, занимающиеся разработкой продуктов и услуг в сфере IoT, от 2 до 320 млн. рублей (в каждую компанию) [1.220]. В 2017 г. ФРИИ проводил специальную

отраслевую акселерационную программу для проектов в области интернета вещей [1.221], с перспективной дальнейшей их финансирования. Проекты отбирались по четырем направлениям: Умный дом/Умная квартира, Smart City, Агро, Индустриальный интернет. По итогам нескольких раундов акселерационных программ, инвестиции на развитие IoT получило только около 5 компаний [1.222–1.224]. Столь скромное число поддержанных проектов говорит либо о низком интересе компаний к участию в такого рода программах, либо о недостаточно высоком качестве проектов.

1.5.5.3 Национальная технологическая инициатива

Рынки НТИ. Для развития подавляющего большинства рынков НТИ требуются технологии IoT. В разных документах упоминается важность IoT для таких рынков НТИ, как Сейфнет, Энерджинет, Нейронет, Фуднет, Маринет, Автонет и Хелснет. Изначально наиболее проработанным с точки зрения использования технологии IoT было направление Нейронет. Там был выделен такой сегмент, как «Управление интернетом вещей», а также была дана оценка сегмента «Нейробыт и IoT», доля которого в общем потенциальном объеме рынка составляла более 70%. Кроме того, IoT был определен в качестве важного компонента инфраструктуры Нейронет. Тем не менее, в дорожной карте, одобренной Президиумом Совета при Президенте Российской Федерации по модернизации экономики и инновационному развитию России, интернет вещей не упомянут.

«Интернет Вещей» может получить новый импульс к развитию после принятия дорожной карты Сейфнет (пока есть только ее концепция²⁹). Анализ ключевых идей концепции показывает, что эта дорожная карта будет в значительной мере акцентировать внимание на технологиях IoT, что соответствует мировому тренду разработки мер безопасности в связи с рисками полномасштабного внедрения интернета вещей в различные сферы деятельности общества. Развитие концепции и инфраструктуры интернета вещей названо в качестве основного ключевого тренда, влияющего

²⁹ По данным на сентябрь 2018 г.

на информационные технологии, безопасности и защищенности которых посвящена данная дорожная карта. В рабочей версии концепции обозначено, что традиционный рынок кибербезопасности уступает место формирующемуся рынку киберфизической безопасности интернета вещей [1.225].

Среди одобренных дорожных карт наибольшее внимание интернету вещей уделено в Энерджиинет. Однако с точки зрения практической реализации результаты пока скромные. Не был реализован пилотный проект умного здания, который намечался на 2017 год, не созданы венчурный фонд и акселератор новых технологий Internet of Things (в т.ч. в энергетике), хотя концепцию фонда предполагалось одобрить еще в 2016 г., а в 2018 г. – пройти уже второй раунд инвестиций. Тем не менее, финансирование проектов НТИ стартовало, но через другой инструмент – программы Фонда содействия инновациям. Там начиная с 2016 г. проводятся ежегодные конкурсы грантов на общую сумму 2 млрд. руб., тематически привязанные к целевым рынкам НТИ. Всего грантами Фонда было поддержано 507 проектов по 7 дорожным картам НТИ³⁰, но сколько среди них было тех, которые направлены на развитие IoT – неизвестно. Такой классификации в Фонде не ведется³¹.

Сквозные технологии НТИ. Интернет вещей не выделен в качестве «сквозной технологии» Национальной Технологической Инициативы, но ряд технологий, определенных в качестве сквозных, непосредственно связаны с развитием интернета вещей (Таблица 1.12).

³⁰ Данные на сентябрь 2018 г.

³¹ Личное сообщение представителей Фонда содействия.

Таблица 1.12— Группы технологий НТИ, связанные с развитием интернета вещей

Наименование группы технологий	Примеры технологий, входящих в группу
Технологии хранения и анализа больших данных	Прогнозирование сигналов устройств интернета вещей и обнаружение и прогнозирование неполадок и аномалий в их работе
Новые производственные технологии	Сенсоры для индустрии «Интернета вещей»
Технологии беспроводной связи	Мобильные сети поколения 5G Light Fidelity RFID NFC low-energy radio protocols LTE-A WiFi-Direct Технологии обеспечения надежности и безопасности беспроводной связи

Источник: составлено авторами по материалам дорожных карт НТИ.

Вместе с тем, в рамках поддержки «сквозных технологий» НТИ были образованы 14 Центров компетенций НТИ. «Интернет Вещей», объединенный с технологиями беспроводной связи, стал темой деятельности одного из Центров (создан на базе Сколтеха) [1.226].

Кроме того, в мае 2018 г. на Петербургском международном экономическом форуме был подписан Меморандум о создании Фонда Национальной технологической инициативы, который будет осуществлять венчурные инвестиции в инновационные проекты по «сквозным технологиям» НТИ [1.227, 1.228]. Первыми частными соинвесторами фонда стали АО «УК ГазСервисКомпозит» и «УК Ломоносов Капитал». Совокупный объем их инвестиционных обязательств составил 600 млн. руб. Суммарный размер Фонда и привлекаемых средств в виде соинвестиций в портфельные компании составит не менее 3,5 млрд руб., причем 1,5 млрд.

руб. вносит Инфрафонд РВК за счет средств субсидии НТИ. Масштабы деятельности нового Фонда не очень большие: планируется, что объем инвестиций в одну портфельную компанию, находящуюся на посевной или ранней стадии, составит не более 10% от общего объема инвестиционных обязательств, и в совокупности Фонд поддержит около 8 портфельных компаний.

Таким образом, на текущий момент государственная поддержка технологий IoT только начинает разворачиваться. При этом на российском рынке есть ряд компаний, самостоятельно разрабатывающие уникальные решения в области IoT.

1.5.5.4 Компании на российском рынке

Представленность разных технологий интернета вещей на российском рынке небольшая, конкурентоспособных на мировом рынке компаний–производителей уникальных решений немного. В качестве примеров можно привести следующие:

- компания Вавиот – производитель беспроводных систем для учета в сферах ЖКХ, сельском хозяйстве, городской инфраструктуре. Первыми вышла на рынок с решением на базе LPWAN (Low Power Wide Area Network), разработав протокол с низким энергопотреблением. Может работать на приборах, не подключенных к внешним источникам;
- концерн Goodwin – беспроводные телекоммуникации для корпоративных и индивидуальных пользователей. Компания создана на базе НПО «Физика», где радиоинженерам удалось создать собственный протокол, благодаря которому IoT работает на подвижных объектах. Это уникальные для мирового рынка разработки;
- компания Thingenix – занимается разработкой решений, позволяющих использовать технологии интернета вещей в производстве, ЖКХ, сельском хозяйстве и многих других отраслях. Есть опыт как в разработке устройств и программного обеспечения, так и в области построения и эксплуатации сетей, в том числе национального масштаба. Компания сделала прибор — аналог

устройства, разработанного НПО «Тайфун», но его стоимость в 10 раз ниже;

- компания «Вега Абсолют» предлагает готовые решения на базе технологии LoRaWAN™, включающее в себя оконечные устройства, базовые станции, а также серверное и клиентское программное обеспечение. В основе принципа передачи данных по технологии LoRaWAN™ на физическом уровне лежит известное свойство радиосистем – увеличение дальности связи при уменьшении скорости передачи, при этом каждое устройство взаимодействует с базовой станцией напрямую, а энергопотребление низкое. Устойчивая связь обеспечивается на расстоянии до 5 км в городских условиях и до 15 км в зоне прямой видимости.

Не во всех областях применение IoT целесообразно и оправдано. Пока слабо развиваются технологии IoT в промышленности и энергетике. В то же время есть большой потенциал развития IoT на транспорте, в логистике, сельском хозяйстве, для умного города, а также при утилизации отходов.

Таким образом, Россия относится к типу стран, которые вводят специальные меры поддержки технологий интернета вещей. В российском варианте на первый план выходит государственная Программа «Цифровая экономика Российской Федерации», где промышленный интернет вещей выделен в качестве одной из ключевых, сквозных технологий. При этом создаются Центры компетенций НТИ, и один из них специализируется именно на интернете вещей. Таким образом можно говорить о том, что выбран комплексный подход к развитию этой технологии, включающий меры по поддержке науки, образования и коммерциализации результатов НИОКР.

2 Международные и национальные стандарты и рекомендации в области интернета вещей³²

Нормативно-техническое регулирование интернета вещей и смежных областей осуществляется на нескольких уровнях. В нем принимают участие международные, региональные и национальные организации по стандартизации, различные неправительственные ассоциации, союзы и консорциумы, альянсы производителей и операторов, партнерские проекты, а также отдельные исследовательские группы.

Различными аспектами тематики интернета вещей, по приблизительным оценкам из открытых источников, занимаются более 100 таких организаций. В разделе 2.1.5 приведен перечень некоторых из них и дана краткая характеристика их деятельности в области стандартизации интернета вещей.

По сложившейся практике ведущую роль в создании и разработке международных стандартов играют Международная организация по стандартизации (International Organization for Standardization, ISO, ИСО [2.1]), Международная электротехническая комиссия (International Electrotechnical Commission, IEC, МЭК [2.2]) и Международный союз электросвязи (International Telecommunication Union, ITU, МСЭ [2.3]).

В ИСО и МЭК работают уполномоченные национальными органами по стандартизации представители стран, – по одному от каждой страны-участника. Полноправными членами ИСО являются 120 стран, членом-корреспондентов и наблюдателей – 42 [2.1]. МЭК объединяет Национальные Комитеты стран-участников, представляя им полноправное или ассоциированное членство [2.2]. В основу МСЭ положена концепция частно-государственного партнерства. В его работе участвуют 193 государства и почти 800 фирм,

³² Вводная часть составлена по данным Википедии соответствующих сайтов (ред.).

академических институтов и неправительственных организаций. Формально, статус стандартов имеют только документы, выпускаемые ИСО/МЭК. МСЭ же разрабатывает рекомендации, зачастую составляющие основу международных технических стандартов [2.3].

ISO (ИСО) была создана ООН в 1946 г. на основе ISA³³ и UNSCC³⁴. Первоначально в нее вошли двадцать пять национальных организаций по стандартизации и UNSCC. Задачами ИСО являются содействие развитию стандартизации и смежных видов деятельности в мире с целью обеспечения международного обмена товарами и услугами, а также развития сотрудничества в интеллектуальной, научно-технической и экономической областях.

Фактически работа ИСО началась с 1947 года. СССР был одним из основателей организации, являлся постоянным членом руководящих органов. Авторитет СССР в ИСО отражает тот факт, что представитель Госстандарта дважды избирался председателем организации. Россия стала членом ИСО как правопреемник СССР. 23 сентября 2005 года Россия вошла в Совет ИСО.

Официальными языками ИСО являются: английский, французский и, что важно, русский язык. На практике это означает, что проекты нормативных технических документов, изначально разработанных на русском языке, могут вноситься в ИСО наравне с другими официальными языками. Однако непосредственно разработка международных документов все равно осуществляется на основном языке – английском.

Стандарты ИСО распространяются почти на все аспекты технологий и бизнеса, от стандартов качества и безопасности до сельского хозяйства и здравоохранения. Электротехника и электроника относятся к компетенции МЭК.

Некоторые виды работ выполняются совместными усилиями этих организаций.

³³ *International Federation of the National Standardizing Associations*), учреждена в Нью-Йорке в 1926 г. расформирована в 1942 г.

³⁴ *United Nations Standards Coordinating Committee*, учреждена в 1944 г.

IEC (МЭК) — международная некоммерческая организация по стандартизации в области электрических, электронных и смежных технологий. Кроме стандартизации, МЭК занимается проблемами сертификации (подтверждения соответствия). МЭК основана в 1906 году. Она имеет 62 полноправных и 24 ассоциированных члена. Первоначально комиссия располагалась в Лондоне, с 1948 года по настоящее время штаб-квартира находится в Женеве. Организация имеет региональные центры в Юго-восточной Азии (Сингапур), Латинской (Сан-Пауло, Бразилия) и Северной Америке (Бостон, США).

МЭК является ведущей организацией в мире по разработке международных стандартов для всех электрических, электронных и смежных технологий. В работе Международной электротехнической комиссии участвуют более 20 тысяч экспертов из промышленности, торговли, правительства, испытательных и исследовательских лабораторий, научных кругов и групп потребителей.

МЭК способствовала развитию и распространению стандартов для единиц измерения, особенно гаусса, герца, и вебера. Также МЭК предложила систему стандартов, которая в конечном счёте стала единицами СИ.

МЭК включает в себя национальные электротехнические комитеты (национальные комитеты МЭК), и ее деятельность направлена на публикацию международных стандартов, технических спецификаций, технических отчетов, общедоступных спецификаций (PAS) и руководств. Подготовкой этих документов занимаются технические комитеты. В подготовительной работе может участвовать любой заинтересованный национальный комитет. В этом процессе также участвуют международные, правительственные и неправительственные организации, поддерживающие связь с МЭК.

Документы, выходящие в результате деятельности ИСО и МЭК, имеют статус международных стандартов. Но, вообще говоря, все стандарты и рекомендации, разработанные ИСО, МЭК и МСЭ, не являются обязательными, если не признаны таковыми на национальных уровнях или промышленностью.

МСЭ является специализированным учреждением Организации Объединенных Наций в области информационно-коммуникационных технологий – ИКТ.

МСЭ в глобальном масштабе распределяет радиочастотный спектр и спутниковые орбиты, разрабатывает технические стандарты, обеспечивающие возможность эффективного присоединения сетей и технологий, и стремится улучшить доступ к ИКТ для недостаточно обслуживаемых сообществ всего мира [2.3]. Кроме того, в МСЭ ведется работа по международным договорам, обязательным для исполнения всеми государствами – членами: Регламенту радиосвязи и Регламенту международной электросвязи (телекоммуникациям).

Существуют также отраслевые/региональные организации по стандартизации в области телекоммуникаций, в частности: 3GPP, ETSI и пр., которые входят или тесно сотрудничают с МСЭ, разрабатывая стандарты (рекомендации) в этой области. МСЭ продолжает дело Международного телеграфного союза, основанного в 1865 году для решения вопросов развития наиболее прогрессивного на тот момента способа коммуникаций – электрического телеграфа: телеграфная сеть развивалась, соединяя различные страны мира, что потребовало совместных усилий для обеспечения совместимости телеграфного оборудования, и решения многих других проблем, которые не могли быть эффективно преодолены вне совместной работы.

Технологический прогресс в области систем связи потребовал переименования Международного телеграфного союза в Международный союз электросвязи в 1932 году.

В 1947 году МСЭ стал специализированным учреждением ООН. В МСЭ входит 193 страны и более 700 членов по секторам и ассоциациям (научно-промышленных предприятий, государственных и частных операторов связи, радиовещательных компаний, региональных и международных организаций). Во многом такая структура связана с тем, что Международный союз электросвязи создает не стандарты, а так называемые рекомендации.

Рекомендации МСЭ не являются обязательными, однако широко признаются в мире, позволяя производителям и операторам рынка эффективно решать вопросы взаимодействия между сетями связи. Для нашего обзора особенно важна деятельность МСЭ-Т – сектора стандартизации электросвязи (Telecommunication Standardization Sector, ITU-T).

МСЭ, ИСО и МЭК выступают и с совместными глобальными инициативами, такими, как «World Standards Cooperation (WSC)» для укрепления и продвижения основанных на консенсусе систем международных стандартов и решения любых вопросов, касающихся сотрудничества в технической работе трех организаций, и «Global Standards Collaboration (GSC)» в целях расширения глобального сотрудничества и сотрудничества в области развития стандартов связи и соответствующей среды разработки стандартов. GSC не является организацией по разработке стандартов и поэтому не будет разрабатывать стандарты.

Кроме того, в последние годы растет кооперация ИСО и МЭК, что повышает эффективность работы над актуальными тематиками и способствует концентрации экспертных ресурсов. Инструментом такой кооперации становятся так называемые Объединенные комитеты (Joint Committees).

Одним из центральных элементов совместной деятельности ИСО и МЭК является Совместный технический комитет № 1 «Информационные технологии» – Joint Technical Committee (СТК 1 ИСО/МЭК, JTC1 ISO/IEC).

СТК №1 был создан в 1987 году путём слияния Технического Комитета 97 (Информационные технологии) Международной организации по стандартизации (англ. ISO/TC 97 Information Technology) и Технического Комитета 83 Международной электротехнической комиссии (IEC/TC 83). Подкомитет 47 Международной электротехнической комиссии (IEC/SC 47B) присоединился позже.

С 1 января 2017 года в рамках ИСО/МЭК функционирует новый подкомитет ИСО/МЭК СТК 1/ПК 41 «Интернет вещей и смежные технологии» (ISO/IEC JTC 1/ SC 41 «Internet of Things and related technologies»).

В подразделах 2.1 и 2.2 данного раздела освещаются вопросы взаимодействия российских учреждений с ИСО/МЭК и МСЭ, соответственно. В подразделе 2.3 пойдет речь о стандартах в области безопасности интернета вещей.

2. 1 Практика разработки документов стандартизации на уровне ISO/IEC³⁵

С позиций стандартизации, под интернетом вещей в широком смысле понимается система объединенных компьютерных сетей и подключенных физических объектов (вещей) со встроенными датчиками и программным обеспечением для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме без участия человека. Кроме того, в рамках данной концепции находится место и промышленному (индустриальному) интернету вещей (далее также – IIoT, Industrial Internet of Things), как более специализированному решению, основанному на распределённой сетевой инфраструктуре в автоматизированных системах управления технологическими процессами [2.4].

За участие российских экспертов в работе подкомитета ИСО/МЭК СТК 1/ПК 41 «Интернет вещей и смежные технологии» отвечает Технический комитет 194 «Кибер-физические системы» (далее – ТК 194), созданный в 2017 году на базе института развития Российской Федерации АО «Российская венчурная компания» (далее – АО «РВК») при участии целого ряда профильных организаций. ТК 194 агрегирует позицию российского рынка для представления ее на национальном и международном уровне, формирует состав экспертов для работы над стандартами, согласовывает и верифицирует позиции бизнеса и государства, утверждает состав российских специалистов, участвующих в заседаниях международного уровня ИСО/МЭК и т.д. Техническому комитету также принадлежит инициатива разработки стандартов и обеспечения работы над ними на национальном и межгосударственном уровне.

³⁵ Уткин Н.А. (РВК, ТК 194 «Кибер-физические системы»), Гареев Т.Р. (Сколтех)

2.1.1 Глобальная карта работы над стандартами-технологии интернета вещей

Технологии интернета вещей привлекают внимание технического и бизнес-сообщества примерно с 2009 года, когда данный термин был введен в широкий оборот. По нашему мнению, изначально термин использовался скорее в маркетинговых целях, однако достаточно быстро стало понятно, что он отражает важный этап в развитии технологии – начавшийся переход к глобальному межмашинному взаимодействию. Уже в 2012 году ИСО и МЭК приступили к предварительному изучению тематики интернета вещей. Эксперты пришли к выводу, что отсутствие качественной системы стандартов в этой технологической области сдерживает полномасштабное практическое использование продуктов и сервисов, не ее основе.

Значительный интерес к стандартизации интернета вещей вызван рядом причин.

Во-первых, со времени основания интернета ключевую роль в стандартизации всех аспектов этого технологического феномена современности играют США. Включение тематики интернета вещей в повестку стандартизации дает возможность стратегическим конкурентам и союзникам США пересмотреть сложившийся статус-кво в сфере контроля за технологиями на стыке цифрового и физического миров, в том числе через формирование новых комитетов и рабочих групп (и связанных с ними секретариатов) в области стандартизации.

Во-вторых, возможность выделения промышленного интернета вещей в отдельное направление является стратегически важной задачей для таких стран как Япония и Германия, конкурентоспособность которых в значительной степени зависит от контроля над технологиями перехода к цифровой экономике и промышленной автоматизации. С этой точки зрения, одной из важнейших недекларируемых целей разработки концепции Industry 4.0 являлось именно позиционирование Германии в качестве глобального лидера стандартизации Промышленного интернета вещей.

Наконец, современный этап характеризуется активным участием растущих китайских компаний, которые стремятся зафиксировать свой заметно изменившийся статус в мире технологий и стандартизации.

Укрупненная схема участников работы над стандартами изображена на Рис. 2.1.

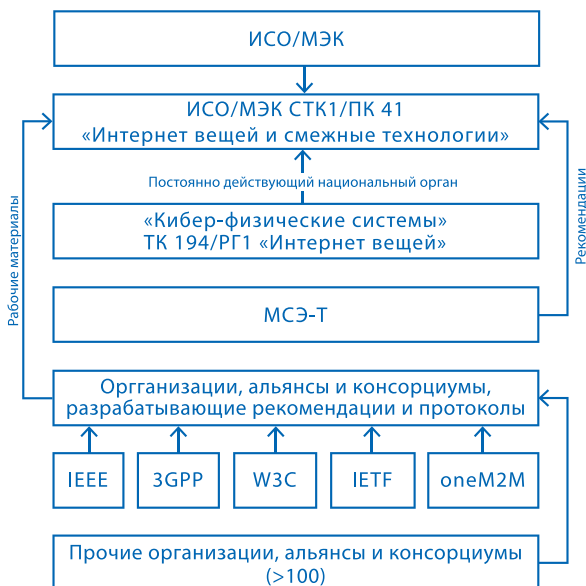


Рисунок 2.1–. Участники разработки стандартов, рекомендаций и протоколов в сфере Интернета вещей

Источник: составлено авторами

Как видно на схеме, наиболее статусными и значимыми в международном масштабе являются Международные организации в области стандартизации, к которым в полной мере относятся ИСО и МЭК (с соответствующим совместным подкомитетом ИСО/МЭК СТК 1/ПК 41 «Интернет вещей и смежные технологии» (ISO/IEC JTC 1/ SC 41 «Internet of Things and related technologies»).

Важным и интересным игроком в международной стандартизации интернета вещей является также МСЭ-Т, разрабатывающий рекомендации, которые могут рассматриваться и учитываться при независимой работе на уровне ИСО/МЭК.

Отдельно можно отметить такие национальные организации как:

- Американский национальный институт стандартов (American National Standards Institute, ANSI);
- Немецкий институт по стандартизации (Deutsches Institut für Normung e.V., DIN);
- Немецкая Комиссия по Электротехнике, Электронике и Информационным Технологиям (DKE) при Немецком институте по стандартизации и Немецком Союзе электротехники (German Commission for Electrical, Electronic & Information Technologies of DIN and VDE);
- Британский институт стандартов (British Standards Institution, BSI).

Заметным авторитетом в отраслевых сообществах также пользуются некоммерческие международные организации, которые профессионально занимаются узкоспециализированными вопросами, например, разработкой конкретных протоколов в системах связи.

В целом, данные организации занимаются подготовкой различных материалов в области технологии интернета вещей. Эти материалы, однако, часто ошибочно или намеренно, но некорректно называемые «стандартами», могут содержать выраженные признаки заинтересованности узкого круга разработчиков. Поэтому на уровне международных организаций они рассматриваются с повышенной аккуратностью и осмотрительностью.

Все эти организации регулярно докладывают результаты своей работы по особо значимым проблемам, вне зависимости от узости их применения и степени смежности областей, в соответствующих международных комитетах, подкомитетах и рабочих группах ИСО/МЭК. Заметим, что данные материалы также проходят через Технический комитет 194 «Кибер-физические системы».

2.1.2 Деятельность по международной стандартизации технологий интернета вещей

Кратко опишем особенности работы над нормативно-техническими документами в рамках ИСО и МЭК.

Одним из центральных в совместной деятельности ИСО и МЭК является Совместный технический комитет № 1 «Информационные технологии» – Joint Technical Committee (СТК 1 ИСО/МЭК, JTC1 ISO/IEC).

Комитет по информационным технологиям был создан для объединения деятельности двух родственных организаций. Основная цель СТК1 состоит в разработке, поддержке, продвижении и содействии развитию ИТ-стандартов, необходимых глобальному рынку для согласования требований производителей и потребителей по следующим направлениям:

- разработка и развитие ИТ-систем и средств их разработки;
- производительность и качество ИТ-продуктов и систем;
- безопасность ИТ-систем и информации;
- мобильность, т.е. способность программного обеспечения работать на различных аппаратных платформах или под управлением различных операционных систем;
- интероперабельность ИТ-продуктов и систем (способность программного продукта или системы функционировать во взаимодействии с другими продуктами или системами при наличии информации только об интерфейсах этих программ или систем);
- унификация инструментов и средств разработки;
- гармонизация ИТ-словаря;
- дружелюбность и эргономичность дизайна пользовательских интерфейсов.

Большая часть работы по конкретным направлениям проходит в подкомитетах (ПК). Большинство подкомитетов имеет несколько рабочих групп (РГ).

В настоящее время в работе СТК1 полноправно участвуют 33 страны, в частности, Казахстан и Россия; 62 страны – являются наблюдателями (в т.ч. Азербайджан, Армения, Беларусь,

Молдова, Узбекистан, Украина). Важно отметить, что функции секретариата СТК1 выполняет ANSI – Американский национальный институт стандартов, который достаточно внимательно отслеживает те инициативы, которые потенциально ведут к перераспределению контроля над ключевыми стандартами и протоколами интернета.

Как отмечалось, вопросами интернета вещей в рамках СТК 1 занимается специально созданный в 2017 году Подкомитет (ПК) №41. Исполнение функций секретариата ПК41 поручено Южной Корее в лице Корейского агентства по технологиям и стандартам (Korean Agency for Technology and Standards, KATS).

С 2017 года на базе подкомитета ИСО/МЭК СТК 1/ПК 41 «Интернет вещей и смежные технологии» реализуется план по разработке стандартов интернета вещей. В деятельности подкомитета принимает 25 стран – полноценных участников и 9 наблюдателей.

Структура подкомитета по состоянию на ноябрь 2018 года представлена на Рис. 2.2. (стр. 140)

В настоящий момент ПК 41 «Интернет вещей и смежные технологии» состоит из трех полноценных рабочих групп:

- рабочая группа 3: Архитектура интернета вещей;
- рабочая группа 4: Интероперабельность (совместимость) решений интернета вещей;
- рабочая группа 5: Приложения интернета вещей.

Рабочие группы организованы по особо востребованным направлениям рынка международных стандартов. К моменту написания настоящего отчета эксперты соответствующих рабочих групп завершают разработку семейства базовых стандартов, в состав которого входят следующие документы:

- ISO/IEC 20924 «Интернет вещей. Термины и определения»;
- ISO/IEC 21823-1 «Интернет вещей. Интероперабельность систем Интернета вещей». Часть 1. Структура»;
- ISO/IEC 30141 «Интернет вещей. Эталонная архитектура».

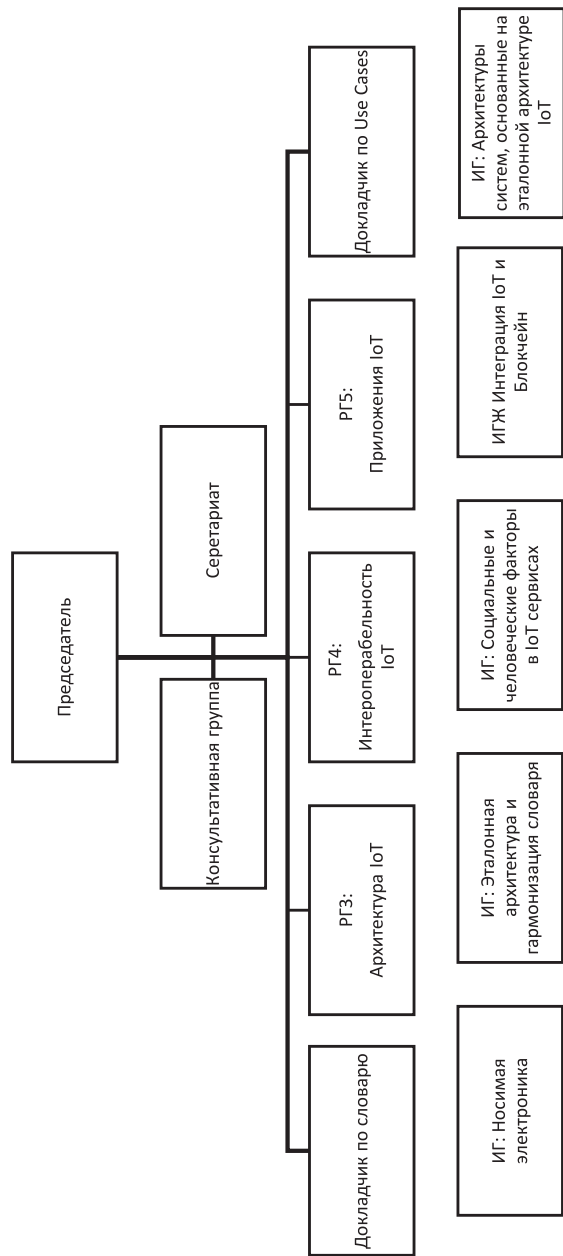


Рисунок 2.2 – Структура ИСО/МЭК СТК 1/ПК 41 «Интернет вещей и смежные технологии»

Источник: составлено авторами

Как видно, фундаментом данного семейства выступает классический терминологический стандарт [2.5], в котором закладывается единое понимание всего инженерного языка, рекомендуемого к применению в рамках тематики интернета вещей. Сложность в разработке терминологического стандарта связана с необходимостью учета и отражения разнообразных рыночных потребностей. На его основе будут развиваться все последующие стандарты.

Второй из упомянутых выше стандартов посвящен проблеме интероперабельности [2.6], или совместимости систем и устройств интернета вещей. Проблема совместимости обусловлена значительным разнообразием продвигаемых на рынке систем и устройств IoT и, следовательно, разнообразием протоколов для обеспечения функционирования этих систем и устройств. В экспертном сообществе сложившаяся ситуация часто неформально характеризуется как «хаос» или «зоопарк» протоколов.

Проблема совместимости проявляется на всех уровнях использования систем и устройств, повышая затраты на создание и обслуживание систем, доставляя неудобства и усложняя жизнь конечным пользователям и бизнесу. Непосредственно затрагиваются также государственные интересы, из-за усложнения и удорожания любых проектов с использованием технологии или элементов технологии интернета вещей. Каждый реализуемый проект, вкуче с аналогичными инициативами, предъявляет требования к совместимости (начиная с уровня передачи данных), что особенно ярко проявляется при осуществлении государственных и муниципальных закупок.

Одним из ключевых моментов в общей системе стандартизации интернета вещей является регламентация типовой (эталонной) архитектуры [2.7]. Архитектура в данном случае представляет собой онтологию предметной области «Интернет Вещей» и включает взаимосвязанный набор определений (понятий), связей и правил. Она описывает некоторую унифицированную IoT-систему (процессы, принципы построения), очерчивает проблемные области интернета вещей. Архитектура является отправной точкой для разработки остальных стандартов интернета вещей.

Как отмечалось выше, весьма важна и задача нормативного технического регулирования (стандартизации) технологии промышленного интернета вещей. С точки зрения технологической составляющей, работа над вопросами стандартизации IoT фокусируется на стыке интернета вещей и «Умного производства». На нынешнем этапе, к задачам ПК 41 «Интернет вещей и смежные технологии» относится проведение анализа требований рынка и состояния текущих мероприятий по стандартизации в области промышленного интернета вещей. Типовая (эталонная) архитектура IoT является частью типовой (эталонной) архитектуры интернета вещей, что отмечено в соответствующем стандарте.

2.1.3 Участие России в деятельности по международной стандартизации в области интернета вещей и смежных технологий

Статьи 8 и 9 Федерального закона «О стандартизации в Российской Федерации» от 29.06.2015 г. N 162-ФЗ разделяют зоны ответственности Федеральных Органов Исполнительной Власти (ФОИВ), осуществляющих функции по выработке государственной политики и нормативно-правовому регулированию в сфере стандартизации, и ФОИВ в сфере стандартизации [2.8].

Министерство промышленности и торговли Российской Федерации (Минпромторг России) является ФОИВ, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в области технического регулирования, стандартизации и обеспечения единства измерений (Положение о Министерстве промышленности и торговли Российской Федерации, утв. постановлением Правительства РФ от 5 июня 2008 г. N 438).

При этом Минпромторг России осуществляет координацию и контроль деятельности подведомственного Федерального агентства по техническому регулированию и метрологии (Росстандарта), которое организует работы по стандартизации в национальной, международной, и региональной системах стандартизации, а также по межгосударственной стандартизации (постановление Правительства Российской

Федерации от 17 июня 2004 года № 294 «О Федеральном агентстве по техническому регулированию и метрологии»).

ФОИВ в сфере стандартизации, помимо прочего, представляет Россию в международных и региональных организациях по стандартизации.

Задачи по инициированию и разработке нормативных технических документов (например, национальных стандартов) Росстандарт делегирует специализированным техническим комитетам. Технические комитеты, в свою очередь, объединяют рыночных игроков для разработки стандартов по соответствующим тематикам.

В 2017 году введен в действие ГОСТ Р 57564-2017 «Организация и проведение работ по международной стандартизации в Российской Федерации». Данный стандарт рассматривает организационно-технические функции представительства Российской Федерации в ИСО и МЭК, порядок деятельности исполнительных органов Российского комитета – члена ИСО и Российского национального комитета по участию в МЭК, а также функции российских технических комитетов (ТК) в части работы по международной стандартизации с учетом специфики этой деятельности в ИСО и МЭК [2.9].

Техническим комитетом, ответственным как за разработку национальных стандартов интернета вещей, так и за участие Российской Федерации в разработке стандартов на международном уровне, является Технический комитет 194 «Кибер-физические системы», созданный на базе АО «РВК» в 2017 году [2.10].

Комитет выступает платформой для развития цифровой экономики и Национальной технологической инициативы (НТИ) за счет разработки стандартов для новых перспективных рынков. Комитет объединяет ведущие научные и общественные организации, технологические компании, некоммерческие организации разработчиков оборудования и программного обеспечения. Среди его участников – «Газпром нефть», «Ростелеком», «Ангстрем-Т», «РУССОФТ», МГТУ им. Н.Э. Баумана, НИУ ВШЭ, МГУ и другие организации.

В рамках ТК «Кибер-физические системы» выделена Рабочая группа «Интернет вещей» (ТК 194/РГ 1 «Интернет вещей»), которая непосредственно занимается разработкой национальных и международных стандартов Интернета вещей.

Рабочая группа ТК 194/РГ 1 «Интернет вещей» собирает предложения по стандартизации от представителей российского технологического рынка, обеспечивает отстаивание требований и интересов Российской Федерации при разработке международных стандартов, а также содействует продвижению российских инновационных продуктов и сервисов на международных рынках через закрепление конкурентных преимуществ российских компаний механизмами международной стандартизации.

Деятельность данной Рабочей группы координируется с другими рабочими группами ТК «Кибер-физические системы», которые связаны со стандартизацией смежных направлений, таких как «Искусственный интеллект», «Умный город», «Умный дом», «Большие данные», «Носимые устройства», «Умное производство», «Умная энергетика», «Квантовые коммуникации», «Доверенная среда» и др.

Так, на третьем заседании ПК 41 «Интернет вещей и смежные технологии», проходившим в Берлине в Немецком институте по стандартизации (DIN) с участием более 90 ведущих международных экспертов (включая и экспертов ТК «Кибер-физические системы»), были приняты ключевые для развития интернета вещей в России решения:

- о разработке терминологического стандарта в области интернета вещей ISO/IEC FDIS 20794 Information technology - Internet of Things - Definition and Vocabulary в мультязычном формате, включающем кроме базовой английской – русскоязычную версию;
- о проведении заседания ИСО/МЭК СТК 1 ПК 41 во второй половине 2019 года в Российской Федерации (по представлению совместной заявки ТК «Кибер-физические системы», АО «РВК» и ПАО «Ростелеком»);
- о разработке международного стандарта, устанавливающего требования к совместимости для устройств

и систем индустриального (промышленного) интернета вещей, предложенного российской стороной, что открывает возможность для участия российских компаний в тематике «Умного производства»;

- о включении экспертов ТК «Кибер-физические системы» в качестве соредакторов разрабатываемого международного стандарта, устанавливающего требования к архитектуре сенсорной сети для электрических подстанций, что открывает новые возможности для развития направления «Умной энергетики» и динамично развивающемуся в его рамках подразделу «Internet of Energy»;
- о создании исследовательской группы по внедрению технологии интернета вещей в блокчейн, в состав которой включены также специалисты ТК «Кибер-физические системы».

Еще раз подчеркнем, что ТК «Кибер-физические системы» (ТК 194) в целом отвечает за участие Российской Федерации в работе ИСО/МЭК СТК 1/ПК 41 «Интернет вещей и смежные технологии».

2.1.4 Заключение

Продолжение сложившейся за последние десятилетия практики игнорирования активной работы над нормативно-техническими документами (в первую очередь, стандартами) в сфере высоких технологий и формирующихся рынков гарантированно приведет к значительным потерям не только в национальном технологическом секторе, но и в национальной экономике в целом.

Разработка и выпуск соответствующих стандартов критически важна, и на порядок облегчает внедрение технологий в любом сегменте рынка, особенно в таких консервативных областях, как промышленность, медицина, строительство, энергетика. Кроме того, работа над стандартами позволяет повысить эффективность экономики, ее технологического сектора. Это касается всех участников рыночных процессов: производителей, пользователей, регуляторов и т.д. Кроме того, участие российских экспертов в разработке

международных стандартов способствует распространению российских технологий и требований российских производителей и разработчиков на внешние рынки, что может увеличить экспортный потенциал их продуктов и сервисов, и повысить вероятность успешного встраивания в глобальные технологические цепочки.

Разработка стандартов в новых областях, таких, как интернет вещей, проходит несколько стадий – от появления новых концепций до планомерной деятельности по утверждению стандартов в рамках признанных международных организаций. Особенно актуальными для современной экономики становятся вопросы стандартизации технологий на стыке цифрового и физического миров – так называемых кибер-физических систем (cyber-physical systems). Среди таких технологий интернет вещей, безусловно, занимает одно из наиболее заметных мест.

Период 2009-2014 годов характеризовался «хайповым» интересом к тематике интернета вещей. По разным оценкам, в этот период появилось более 100 заметных инициатив по разработке так называемых «стандартов» и протоколов, связанных с интернетом вещей; в открытых справочниках можно насчитать сотни аббревиатур протоколов и технологий, имеющих отношение к архитектуре IoT.

Как правило, о зрелости той или иной группы технологий можно судить по уровню и статусу их рассмотрения в международных организациях.

ИСО/МЭК официально приступила к предварительному изучению тематики интернета вещей в 2012 году, выделив специальную рабочую группу в рамках СТК 1. Уже через два года, работа перешла в более активную фазу, и в 2014 году она переросла в одноименную рабочую группу JG 10 «Интернет вещей» (WG 10 “Internet of Things”), а еще через два года было принято ключевое решение о создании профильного подкомитета ПК 41 «Интернет вещей и смежные технологии», который действует с начала 2017 года.

Соответственно, ведущие международные организации начиная с 2014 года публикуют аналитические и программные

материалы по проблематике интернета вещей. Среди наиболее значимых можно отметить одноименный доклад ИСО/МЭК СТК 1 [2.11], а также «Белую книгу» МЭК по интернету вещей [2.12], в которой организация обозначила основные подходы к стандартизации.

В области интернета вещей МЭК рекомендует опираться на следующую группу источников при разработке нормативных технических документов:

- «горизонтальные» стандарты ISO, IEC;
- рекомендации ITU, IEEE;
- протоколы интернета IETF;
- «горизонтальные» рекомендации oneM2M;
- рекомендации по моделированию от Object Management Group;
- рекомендации по сетям от W3C.

Параллельно с деятельностью ИСО/МЭК ведущие мировые вендоры и консорциумы выпустили значительное количество аналитических материалов. Как свидетельствует анализ [2.12], МЭК хорошо осведомлена о многообразии существующих инициатив и рекомендаций (выпускаемых под видом стандартов), о влиянии на рынок со стороны крупных вендоров и о роли геополитических интересов в процессе стандартизации.

На момент подготовки настоящего отчета на уровне ИСО/МЭК ведутся дискуссии по одному из наиболее острых, стратегически важных вопросов, которым является признание Промышленного интернета вещей в качестве самостоятельной темы для разработки (с соответствующей институционализацией путем создания рабочих органов в рамках этих организаций).

Для ключевых игроков принципиально выделение данной тематики как с технической, так и с экономической точки зрения. Важным драйвером этого процесса являются немецкая инициатива Industrie 4.0 и японская Japanese Robot Revolution Initiative, которые поддержаны соглашением между профильными министерствами Японии (METI) и Германии

(BMWi). Россия в целом поддерживает инициативу по выделению Промышленного интернета вещей в отдельную тематику в рамках международной стандартизации и даже ведет разработки по этому вопросу как на национальном, так и на международном уровне. Такая инициатива, безусловно, создает новые вызовы для активизации нормативно-технического регулирования с российской стороны.

В настоящее время основным механизмом развития экосистемы интернета вещей на национальном уровне является актуализация и постоянное информирования заинтересованных российских организаций о разработке опережающих технологий, стандартов и протоколов, а также продвижение предложений российских разработчиков на международном уровне.

2.1.5 Приложение. Организации, работающие в области стандартизации интернета вещей (кроме ISO, IEC и ITU)³⁶

Название организации, источник	Вид деятельности по в области стандартизации
Allseen Alliance, https://allseenalliance.org/	AllJoyn — это программная платформа с открытым исходным кодом, позволяющая устройствам и приложениям легко обнаруживать и общаться друг с другом.
AIM (Association for Automatic Identification and Mobility), http://www.aimglobal.org/	Комитет по интернету вещей данной ассоциации предоставляет площадку для участников организации, в рамках которой они могут исследовать и изменять быстро меняющийся ландшафт взаимосвязанного мира продуктов, услуг и информации. Комитет позволяет участникам заложить основу для более умного и эффективного мира, используя технологии автоматической идентификации и мобильности. В состав комитета входят компании-члены AIM, заинтересованные в оказании влияния на определение и направление развития Интернета вещей, особенно в том, что касается технологий штрих-кодов, RFID и мобильных вычислительных решений.
Bluetooth Special Interest Group (SIG), https://www.bluetooth.com/	Специальная группа по интересам Bluetooth анонсировала версию 4.1. С продвижением версии 4.1, Bluetooth SIG стремится стать основным игроком на быстроразвивающемся рынке интернета вещей.
CCSA (China Communications Standards Association), http://www.ccsa.org.cn/english/	Общие рамки и технические требования IoT (Интернет вещей) Документ № YD / T2437-2012
Eclipse Foundation, http://iot.eclipse.org/	Рабочая группа по IoT поддерживает открытые стандарты интернета вещей. Предоставляет реализации протоколов IoT, таких как CoAP, ETSI SmartM2M, MQTT или LwM2M с открытым исходным кодом.
ETSI (European Telecommunications Standards Institute), http://www.etsi.org/	European Telecommunications Standards Institute (ETSI) позиционирует себя как независимую некоммерческую организацию по стандартизации в области телекоммуникаций в Европе.

³⁶ Адаптировано авторами по материалам Kess P., Kropsu-Vehkaperä H. Standardization with IoT, Managing Knowledge and Learning, Joint International Conference 2016. 25-27 May, Romania.

GISFI (Global ICT Standardization Forum for India), http://www.gisfi.org/	Рабочая группа по Интернету Вещей http://www.gisfi.org/workinggroups.php?wg=IoT
GS1 / EPCGlobal, http://gs1oliot.github.io/oliot/	Oliot (Открытый язык для Интернета вещей) должен стать платформой инфраструктуры интернета вещей (IoT) на основе международного стандарта путем расширения системы кодирования GS1 и ее стандартной архитектуры для поддержки различных каналов связи IoT и протоколов, таких как штрих-код, RFID, ZigBee, 6LoWPAN и т. д. Oliot также стремится к полной реализации стандарта GS1 / EPCglobal.
HART Communication Foundation, http://en.hartcomm.org/	WirelessHART
IEEE (Institute of Electrical and Electronics Engineers), http://standards.ieee.org/innovate/iot/	Ассоциация стандартов IEEE (IEEE-SA) имеет ряд стандартов, проектов и мероприятий, которые непосредственно связаны с созданием среды, необходимой для активного рынка IoT.
IETF (Internet Engineering Task Force), https://www.ietf.org/	Управление IoT улучшит координацию между рабочими группами, ориентированными на технологии, связанные с IoT, предоставит по запросу обзор спецификаций, связанных с IoT, для директора или председателя рабочей группы в любой области, и предоставит информацию рабочим группам по IoT и IESG о том, как работа по IoT продвигается вне IETF.
IIC (Industrial Internet Consortium), http://www.iiconsortium.org/	Эталонная архитектура Промышленного интернета определяет промышленные интернет-системы и структуру, помогающую в разработке, документировании и коммуникации промышленного Интернета. Дальнейшее развитие и осмысление происходит в ПК 41 «Интернет вещей и смежные технологии».
INCITS (InterNational Committee for Information Technology Standards), http://www.incits.org/	Технический комитет по Интернету вещей (IoT), INCITS участвует в работе над вопросами стандартизации в областях, отнесенных к JTC 1 по Интернету вещей (IoT) (ПК 41 «Интернет вещей и смежные технологии», ранее - РГ 10 «Интернет вещей»).

<p>IPSO Alliance (The Internet Protocol for Smart Objects Alliance), http://www.ipso-alliance.org/</p>	<p>IP (интернет-протокол) для сетей интеллектуальных объектов. Сообщество IPSO предоставляет информацию людям, заинтересованным в спецификации, создании, тестировании или ознакомлении с системами Smart Object.</p>
<p>ISA (International Society of Automation) https://www.isa.org/</p>	<p>ISA100 Committee</p>
<p>NIST (National Institute of Standards and Technology), http://www.nist.gov</p>	<p>Проект NIST в Интернете вещей: фреймворк для кибер-физических систем. Призван служить общим планом для разработки безопасных, защищенных и совместимых систем, таких как интеллектуальные энергосистемы, носимые устройства и подключенные автомобили.</p>
<p>OASIS (Organization for the Advancement of Structured Information Standards), https://www.oasis-open.org/</p>	<p>http://interoperate-iot.oasis-open.org/</p>
<p>OGC (Open Geospatial Consortium), www.opengeospatial.org/</p>	<p>The OGC Sensor Web for IoT Standards Working Group http://www.ogcnetwork.net/IoT</p>
<p>OIC (Open Interconnect Consortium), http://openconnectivity.org/</p>	<p>Архитектура IoTivity предоставит план действий для производителей и поставщиков услуг, включая:</p> <ul style="list-style-type: none"> — общее решение; — установленные протоколы; — общие подходы; — определенные общие черты; — совместимость; — инновационные возможности; — • необходимые каналы связи.
<p>OMA (Open Mobile Alliance), http://openmobilealliance.org</p>	<p>Спецификации рабочей группы по требованиям OMA:</p> <p>The Always Online Infrastructure (AOI);</p> <ul style="list-style-type: none"> — The Converged Address Book (CAB); — The Converged IP Messaging (CPM); — The Converged Personal Network Service (CPNS); — The Mobile Advertising (MobAd); — The Mobile Augmented Reality (MobAR); — The Open Connection Manager API (OpenCMAPI); — The Mobile Spam Reporting (SpamRep); — The Unified Virtual Experience (UVE); — The Social Network Web (SNeW).

OMG (Object Management Group), http://www.omg.org/	Стандарты и деятельность OMG IoT включают в себя: <ul style="list-style-type: none"> — Data Distribution Service (DDS); — Dependability Assurance Framework; — Threat Modeling; — Structured Assurance Case Metamodel; — Unified Component Model; — Automated Quality Characteristic Measures; — Interaction Flow Modeling Language™ (IFML™) http://www.omg.org/hot-topics/iot-standards.htm
OneM2M, http://www.onem2m.org/	OneM2M - это глобальная инициатива в области стандартов для межмашинных коммуникаций и интернета вещей.
OPC Foundation, https://opcfoundation.org/	OPC UA, Инфраструктура для интернета вещей, Промышленного интернета вещей, Индустрий 4.0
Open Group, http://www.opengroup.org/	Рабочая группа «Интернет вещей» (IoT) разрабатывает открытые стандарты для интернета вещей. Она разработала две группы открытых стандартов IoT для Open Group: открытый формат данных (ODF) и открытый интерфейс обмена сообщениями (O-MI).
Thread Group, http://www.threadgroup.org/	Thread собирается создать лучший способ подключения и управления продуктами в домашних условиях. Концепция основана на открытых стандартах и протоколах IPv6 / 6LoWPAN
TTA (Telecommunications Technology Association), http://www.tta.or.kr/English/	Специальный технический комитет IoT (STC1): IoT/M2M Convergence (SPG11) и IoT/M2M Networking (SPG12)
W3C, https://www.w3.org	Группа сообщества Web of Things предоставляет площадку для неофициальных дискуссий, предшествующих созданию стандартов, в целях исследования, создания прототипов и рабочих систем для Web of Things.
XMPP Standards Foundation, http://xmpp.org	http://xmpp.org/uses/internet-of-things.html

2.2 Проблемы и перспективы стандартизации в области хранения и обработки данных³⁷

2.2.1 Введение

В стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы [1.3] определяются понятия интернета вещей и обработки больших объёмов данных: «интернет вещей – концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой», «обработка больших объемов данных – совокупность подходов, инструментов и методов автоматической обработки структурированной и неструктурированной информации, поступающей из большого количества различных, в том числе разрозненных или слабосвязанных, источников информации, в объемах, которые невозможно обработать вручную за разумное время». Такая формулировка отражает далеко не все взгляды экспертного сообщества на данную тему [2.13]. Тем не менее, такое определение позволяет поставить проблемы и обозначить границы в области стандартизации хранения и обработки больших данных для интернета вещей.

В настоящем разделе мы обсудим проблемы стандартизации, сформулируем научные, технологические и экономические барьеры развития сферы больших данных, а также рассмотрим некоторые перспективные направления исследований и приложений.

2.2.2 Решаемые проблемы в области беспроводных сетей и интернета вещей

В области беспроводных сетей и интернета вещей в настоящий момент существует множество стандартов. Развиваются сети пятого поколения. Во многом проблема больших данных обусловлена отставанием пропускной способности в сравнении с развитием генераторов данных – удешевлением устройств и средств первоначального сбора

³⁷ Павловский Е.Н. (НГУ)

и удешевлением хранения данных. Каналы передачи данных ещё в начале 2000-х стали «бутылочным горлышком» в общей экосистеме анализа данных. Развитие интернета вещей необходимо приводит не только к проблеме сетевой адресации устройств и ускорению перехода к IPv6, но и к проблеме недостаточной пропускной способности каналов. Это в свою очередь ставит, с одной стороны, задачу минимизации передаваемых данных с максимизацией передаваемой информации, с другой – задачу распределения коммуникаций. В идеале, каждое устройство, генерирующее данные, должно также обладать способностью принимать и передавать данные других устройств, чтобы организовать одноранговую сеть и снизить нагрузку на центральные узлы.

В этих условиях критически важно понимать разницу между данными и информацией. В классической информатике между данными и информацией ставится знак равенства. Минимальной единицей данных является бит, как и для информации. В то же время для человека, как для основного приёмника информации, наборы данных становятся слишком массивными и неоднородными, чтобы устранять неопределённость непосредственно в приёмнике. Информация с точки зрения хранения данных означает устранение неопределённости в носителе информации – какой бит записать: 0 или 1. Т.е. с точки зрения хранения – это информация, а с точки зрения стороннего наблюдателя – это просто данные с неизвестной структурой. Именно такая путаница с понятиями «данные» и «информация» определяет ту неразбериху, которая возникла с понятием «большие данные».

Естественно, с ростом объема данных растёт и их шумовая составляющая. При этом росте количества данных, видоизменения их структуры, человеческая способность обработать входящий поток информации не растёт. Это рождает проблему – как большой поток данных представить для решения человеку в таком виде, чтобы он извлекал максимум ценности? В этой связи мы вынуждены отделить понятие «данные», как зафиксированного набора фактов, от понятия «информация», как ответа, устраняющего неопределённость

в источнике. С точки зрения системы хранения, данные и есть информация. Но с точки зрения пользователя, файл объёмом 1 Гб не будет означать 1 Гб информации. Если человека интересует лишь вопрос, есть в этом файле номер его кредитной карты или нет, то этот объём будет соответствовать одному биту информации. При этом, конечно, вопросов к такому объёму данных может быть гораздо более одного миллиарда, что показывает потенциально бесконечную информационную ёмкость даже у ограниченного набора данных, в зависимости контекста, в котором мы размещаем вопрос. Таким образом, мы приходим к относительности структуры данных и пониманию того, что структура не является неотъемлемым свойством данных. Структура данных – есть эмерджентное свойство данных в определённом контексте становится информацией. В этом смысле, из-за контекстуальности, это свойство, как и в квантово-механических системах возникает лишь при изменении (вопрошании) [2.14]. Исходя из этого, атрибутирование свойства к большим данным, проводимое в предложениях рабочей группы NIST по большим данным [2.15], лишь смешивает исходные понятия. Заметим также, что относительно мощный импульс к развитию системы хранения данных получили после отказа от реляционной структуры. Так, нашли свои ниши системы key-value, документные и другие NoSQL системы управления базами данных (СУБД).

Возможность задавать различные вопросы к один и тем же данным открывает и другую возможность – использовать данные для иной цели, нежели для которой они были собраны. В основном именно в этом и заключается потенциальная ценность больших данных. Социальные сети используются для кредитного скоринга, поисковые запросы – для показа рекламы, – в целом, собранные один раз данные можно применять в разных контекстах. Однако, это порождает и проблему несоответствия цели сбора целям обработки.

Вместе с тем, проблема разнородной структуры собранных и уже хранящихся данных обнажает различие в понимании «информации» с точки зрения инструментов хранения и обработки данных. Как мы отметили, данные с этой точки

зрения являются информацией, так как отвечают на вопрос системы хранения «какое значение 0 или 1 записать в i -ю ячейку?». Система считывания также получает однозначный ответ на вопрос «какое значение 0 или 1 сейчас хранится в i -й ячейке?». Однако при обработке данной информации она проходит через различные уровни абстракции, где человеку уже не важны пиксельные детали, ему необходимы логические выводы над этой структурой. Таким образом можно сформулировать задачи, связанные с проблемой структурированности. Необходимо создавать такие обработчики данных, которые автоматически отвечают на частные вопросы, например, «есть ли в этой видеозаписи террорист?» или «сообщается ли в настоящей статье важная информация?». Наборы таких автоматических распознавателей и призван реализовать искусственный интеллект в его узком понимании. Это можно назвать первичным уровнем интеллектуализации больших данных – фаза развития, на которой строятся алгоритмы для автоматического определения структуры данных и извлечения из них полезной информации. Именно на этом этапе свои успехи продемонстрировали искусственные нейронные сети, в частности – свёрточные, решающие задачи распознавания на уровне, превосходящим человеческий [2.16].

Вторичным уровнем интеллектуализации больших данных следует назвать автоматизацию извлечения знаний. При этом мы понимаем знания как способность прогнозировать информацию о будущем состоянии системы по известным её состояниям. Эта способность может быть приобретена как человеком, так и машиной. Поэтому, можно предположить, что системы обработки данных будут развиваться в сторону извлечения, применения и представления знаний.

Стоит отметить изменившуюся роль данных в человеческой деятельности. Если раньше человек принимал решения на основе исходных данных, то сейчас он использует уже обработанные, и часто не имеет даже доступа к исходным. В эпоху больших данных для человека появляется возможность иметь наиболее полное описание явления, в том

смысле, что стало дешевле и проще иметь полный набор данных [2.17]. Это же обуславливает проблему достоверности набора данных, на который можно опереться для принятия решений. Подобное же развитие ожидается в сфере интернета вещей, где данные сначала используются в исходном виде для хранения и передачи, а затем преобразуются в информацию, позволяющую другим устройствам принимать решения и действовать. Впоследствии это порождает проблемы интеллектуализации при использовании данных между устройствами. Например, камера с интеллектуальной подстройкой баланса белого не годится для решения задач детектирования. В этом случае данные сначала стали информацией, а затем были использованы как данные безотносительно исходного набора. Таким образом можно обозначить общую проблему перемещения между уровнями представления в системе данные-информация-знания [2.18, 2.19].

Стандартизация обработки и хранения данных должна определять понятия не только для данных, но и фиксировать понятия «информация», «знания», их отличия и способы обработки. Известные попытки стандартизировать представление знаний с помощью формальных языков, таких как RDF, OWL, пока так и не привели к общепринятым стандартам главным образом из-за массивности представлений исходных фактов, невозможностью работать с противоречивыми фактами и недостаточным быстродействием систем вывода.

Мыслится, что определение «данных» должно быть дополнено представлениями о квантификации познаваемых явлений. В любом случае, устройство, генерирующее исходные данные, получает их как информацию от взаимодействия с другими объектами (датчик температуры, счётчик Гейгера) и регистрирует только лишь квант взаимодействия в допустимых пределах собственной точности. В этом смысле, любые данные должны сопровождаться метайнформацией об источнике получения, способе сбора и уровне точности. Это поможет решить проблему достоверности данных организационными методами и избежать необходимости дорогостоящего использования автоматизированных методов оценки достоверности.

2.2.3 Барьеры развития

Отсутствие стандартов в области форматов передаваемых данных сложно назвать проблемой. Напротив, наличие жёсткой структуры передаваемых данных может сдерживать развитие интернета вещей.

Главным научным барьером в стандартизации больших данных можно назвать отсутствие рабочей методологии, отделяющей понятия «данные», «информация» и «знания» на уровне представления, хранения и оперирования. В настоящий момент алгоритмы равно оперируют знаниями и информацией как данными, в то время как для каждого класса должны быть свои методы и чёткие границы их применения.

Вторым научным барьером можно назвать отсутствие методик оценки потенциальной ценности больших данных. Это происходит из-за самой природы процесса: если мы не знаем, в каком контексте мы будем использовать данные, то как можно оценить их ценность? Возможно, существуют какие-то научные подходы, позволяющие очертить класс возможных ситуаций, в которых конкретные наборы данных будут особенно полезны.

К третьему научному барьеру можно отнести проблему соединения логического подхода принятия решений с коннекционистским походом в области распознавания. Проблема заключается в том, что исследователи из этих групп часто непримиримы и мало пересекаются в исследовательской деятельности. Для логического подхода недопустимым считается наличие противоречий, в то время как для коннекционистов – это данность, с которой надо уметь работать. Возможность соединить эти подходы открывает путь к преодолению барьера, при тесном сотрудничестве между научными группами на основе единства культур, базового образования и стремления к получению прорывных результатов.

Основным технологическим барьером развития интернета вещей является недостаточное развитие сетей передачи данных. Сети пятого поколения могут решить эту проблему. Однако, важно не только существенное ускорение передачи, но и диверсификация каналов, переход на распределённые

коммуникации без необходимости обращения к облакам. В этом смысле производителям устройств интернета вещей необходимо находить компромисс между, с одной стороны, возможностью быстро обновить прошивку устройства и его привязкой к облачному сервису, и с другой стороны – работоспособностью устройства и его способностью к коммуникации без доступа к облачному сервису. Известным препятствием для развития интернета вещей в потребительском сегменте можно назвать малое количество разрешённых в Российской Федерации стандартов частоты вещания датчиков для умного дома.

Вторым технологическим барьером можно назвать недостаточное развитие систем распознавания, преобразующих данные в информацию в зависимости от задачи. Ранее такой барьер преодолели глубокие нейронные сети, продемонстрировав, что способны решать задачи распознавания изображений, транскрибирования и синтеза речи на уровне человека и даже лучше него. Однако, количество таких применений всё ещё сдерживается недостаточной адаптированностью нейронных сетей к мобильным архитектурам, высокими требованиями к выборкам данных для обучения глубоких нейронных сетей. Остаются сильно недооценёнными технологии распознавания акустических событий в применении к задачам умного города.

Законодательным барьером до сих пор является неопределённый статус брокеров данных — компаний, занимающихся коммерческим сбором данных и продажей доступа к ним. В то время как на западе наличие таких компаний существенно ускоряет развитие методов оценки ценности данных, в России данная сфера всё ещё остаётся условно законной.

2.2.4 Перспективные направления исследований и их применений

В направлении преодоления научных барьеров в области конкретизации понятий «данные» – «информация» – «знания» мыслится перспективным разработать новые форматы представления, более адекватные текущим задачам. Например,

для семантической обработки текстов, возможно не требуется сначала сохранять текст в двоичной кодировке букв и символов, чтобы затем из такой кодировки вновь восстанавливать структуру текста и смыслы. Возможно, есть и другие формы исходного представления текстов, например, в виде графов или нечётких булевозначных моделей [2.20]. Для сохранения аудиовизуальных данных, возможно, правильным будет их семантическое представление, натренированное в глубоком обучении на простых примитивах, где доступ к повторному использования данных будет осуществляться посредством проекции натренированного представления на конкретный контекст использования — по аналогии с восприятием человека. Дополняющим к этому подходу, в машинном обучении развивается подход мультимодального обучения, где данные об одном моделируемом объекте представляются в разных формах: звуки, изображения и текстовые данные. Также возможно развитие семантического подхода, имеющего в своей основе исходное представление задач безотносительно способа их решения [2.21].

Представляют интерес исследования по определению потенциальных контекстов использования накопленных данных. Класс контекстов может быть очерчен по общесистемным представлениям всех подсистем, могущих вступить во взаимодействие с данными, таким образом определяя собой контекст использования. Перспективными в этой области могут стать исследования в области применения квантового подхода. Так, например, в настоящий момент развиваются подходы квантовой семантики естественного языка [2.22, 2.23], вобравшей в себя лучшее от квантовой механики и дистрибутивных семантик.

В области сопряжения логических и коннекционистских подходов перспективными выглядят методы, основанные на теории вероятностей, в то же время использующие логический или байесовский вывод [2.24].

В области преодоления технологических барьеров следует отметить движение в сторону миниатюризации элементной базы беспроводных приёмников, расширение стандартов IEEE 802.11. Также наметился тренд на улучшение быстродействия методов машинного обучения на мобильных платформах [2.25], что открывает новые перспективы в массовом

решении задач искусственного интеллекта в условиях отсутствия доступа к облакам и другим большим вычислительным ресурсам.

Отдельного внимания заслуживает тема с нахождением минимальных наборов данных, достаточных для машинного обучения. Эта тема актуальна как в сфере глубокого обучения – для эффективного построения нейросетевых классификаторов, так и в сфере моделирования цифровых двойников – какой минимальный набор данных о поведении системы достаточен для моделирования этой системы? Представляется, что могут быть даны теоретические оценки по нижней границе необходимого объёма данных для отдельных классов моделей и явлений

В сфере законотворчества большие надежды возлагаются на Национальную технологическую инициативу, опирающуюся как на большую экспертную поддержку, так и на существенный административный ресурс в целях выполнения Стратегии научно-технического развития России и преодоления других барьеров, не позволяющих в настоящий момент занять лидерские позиции.

2.2.5 Выводы

В ближайшие годы будет нарастать количество применений интернета вещей в промышленности и в меньшей степени – в потребительском сегменте. Это в свою очередь подстегнёт развитие сетевого оборудования, позволяющего объединять в сети множество конечных устройств. Увеличивающиеся потоки данных между устройствами способствуют развитию мобильных систем интеллектуальной обработки данных интернета вещей, что в свою очередь потянет за собой миниатюризацию глубоких нейронных сетей под мобильные архитектуры и поиску других эффективных методов машинного обучения.

В перспективе 5-10 лет могут быть изобретены новые подходы к представлению данных, что изменит назначение и способы применения уже существующих устройств интернета вещей, а также позволит заранее знать набор контекстов, в которых может быть использована та или иная автоматическая система, в том числе для решения вопросов информационной безопасности.

3 Некоторые отраслевые приложения интернета вещей

3.1 Интернет вещей в агропромышленном комплексе³⁸

3.1.1 Введение

Глобальные потепление, экспоненциальный рост численности населения и изменение потребительской стратегии в растущих экономиках мира влечет за собой существенное снижение потенциала производства продуктов питания во многих традиционных регионах земледелия. По прогнозам ООН, чтобы прокормить растущее население Земли, к 2050 году будет необходимо производить на 70% больше продовольствия, чем в настоящее время. Для сельского хозяйства это означает повышение экономических рисков в среднесрочной перспективе, а также обуславливает трансформацию издержек на адаптацию к природным факторам из «предсказуемых условно постоянных» в «плохо предсказуемые переменные» [3.1].

Исторически, сельское хозяйство – это отрасль, расположенная на противоположном полюсе от информационных и цифровых технологий. Однако, тенденция превращения сельского хозяйства в высокотехнологичную отрасль оказывает влияние на кадровую структуру предприятий АПК во всем мире: стремительно растет спрос на специалистов в области Big Data, Data Science, математиков, аналитиков, робототехников для АПК [3.2]. Переход к цифровым технологиям и автоматизация максимального количества сельскохозяйственных процессов становится осознанной необходимостью и основной стратегией развития крупнейших компаний в мире. Основной вклад в рост продуктивности и снижение издержек теперь связан не с внедрением узкоспециализированных технологий, специальной сельскохозяйственной техники, удобрений, пестицидов направ-

³⁸ Пукальчик М.А. (Сколтех), Шадрин Д.Г.(Сколтех), Федоров М.В. (Сколтех)

ленного действия и т.п., а с реализацией комплексных платформенных технологических пакетов и, в особенности, во внедрении интернета вещей.

3.1.2 Тренды развития интернета вещей в сельском хозяйстве: глобальный рынок инноваций.

Пристальное внимание научного мира в последнее время привлечено к трендам разработок в области интернета вещей для сельского хозяйства. Согласно данным Scopus и Web of Knowledge (WoS) общее количество публикаций на эту тему выросло за 5 лет в 2 раза (поиск «IoT for Agriculture»). По данным Dimensions [3.3], за то же время суммарный объем выделенных средств на НИР по линиям различных фондов увеличился более чем в 20 раз (с 217 тыс. долл. в 2014 г. до 4,7 млн. долл. к 2018 г., Рис. 3.1). Данная тенденция, по-видимому, отражает появление технологических прорывов в данной области и рост интереса крупнейших научных организаций, занимающих лидирующее место на открытом рынке грантов, к данным технологиям.

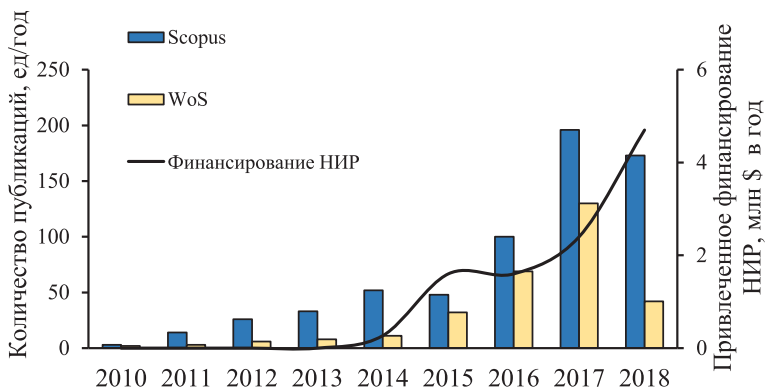


Рисунок 3.1– Публикационная активность и тенденции финансирования НИР в области интернета вещей в АПК за 2010-2018 гг. (Ось абсцисс отражает год публикации статьи или начала финансирования проектов; левая ось ординат – количество публикаций в год, правая ось ординат – объем выделенных средств согласно Dimensions, млн. долл. в год).

Источник: составлено авторами

Анализ распределения статей по направлениям исследований позволяет выделить области, на которых в большей степени фокусируются компании, продвигающие интернет вещей в АПК. Структурный срез направлений исследований в рамках опубликованных статей 2010-2018 гг. согласно Scopus и WoS представлен на Рис. 3.2. Этот перечень дает реальную картину ключевых точек роста в области интернета вещей для сельского хозяйства. Постоянно усиливается взаимопроникновение смежных, ранее развивавшихся отдельно, научных областей: компьютерные технологии и инженерные науки находят все большее применение в сельском хозяйстве.

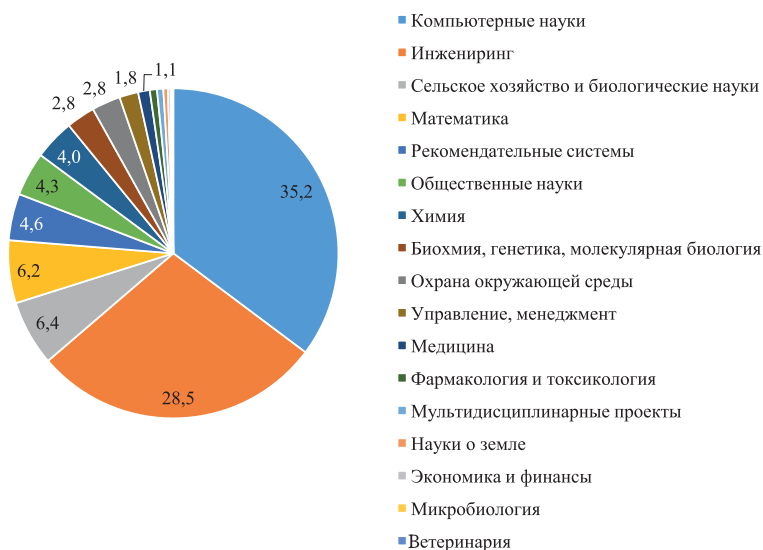


Рисунок 3.2—Структурный срез направлений исследований публикаций по тематике Интернет Вещей в сельском хозяйстве за 2010-2018 гг. согласно WoS, Scopus (на круговой диаграмме отражен % публикаций по каждой тематике относительно общего количества публикаций).

Источник: составлено авторами

3.1.3 Рынок интернета вещей в сельском хозяйстве

Если в 2010 году в мире насчитывалось не более 20 высокотехнологичных компаний, работающих в сфере сельского хозяйства, и рынок венчурных инвестиций составлял не более \$400 тыс., то уже с 2013 начался экспоненциальный рост венчурного капитала. К примеру, в 2013 г. Monsanto купила за 930 млн долларов компанию Climate Corporation, занимавшуюся разработкой системы прогнозирования урожая для страховых компаний. и стала продавать программное обеспечение для фермеров, покупающих у нее семена и гербициды. К 2018 году интерес мировых венчурных фондов к инновационным разработкам в области сельского хозяйства многократно вырос, инновационные компании привлекли более 10,1 млрд. долларов финансирования только за 2017 год [3.4]. Аналогичный тренд поддержали и мировые гиганты индустрии АПК: DowDuPont потратил 300 миллионов долларов на покупку компании Granular, разрабатывающей и реализующей программное обеспечение по управлению фермами, а Deere & Co потратила почти 305 миллионов долларов на покупку Blue River Technology – компании по производству роботов для АПК.

Сельское хозяйство становится сектором с очень интенсивными потоками данных. Информация поступает от различных устройств, расположенных в поле, на ферме, от датчиков, агротехники, метеорологических станций, дронов, спутников, внешних систем, партнерских платформ, поставщиков. Собранные от различных участников производственной цепочки общие данные позволяют получать информацию нового качества, находить закономерности, создавать добавочную стоимость для всех вовлеченных сторон, применять современные научные методы обработки и на их основе принимать правильные решения, снижающие риски, улучшающие бизнес производителей и клиентский опыт.

Рост объем рынка цифровых технологий в АПК зачастую связывают с расширяющимся доступом к сети Интернет. К примеру, в США – мировом лидере по внедрению технологий интернета вещей в сельское хозяйство – доля

сельхозпроизводителей с выходом в интернет в 2017 год достигла 70% [3.5]. В России ситуация несколько иная, однако также прослеживается тенденция расширения охвата интернетом сельскохозяйственных предприятий. По данным Всероссийской сельскохозяйственной переписи 2006 года (далее ВСХП 2016) за 10 лет охват увеличился более чем в 4 раза: если в 2006 году выход в сеть Интернет имели 12,9 % сельскохозяйственных организаций, то в 2016 году уже 46,9 % [3.6]. Объем производства продукции в сельскохозяйственных организациях за этот срок увеличился в 1,75 раза. Согласно выборочной оценке Департамента развития и управления государственными информационными ресурсами АПК Минсельхоза России объем рынка IT и интернета вещей в АПК должен увеличиться в ближайшие 7 лет в 5 раз, с 400 млрд руб. в 2017 год до 2 трлн. руб. к 2024 г. за счет перехода сельского хозяйства на цифровые технологии.

3.1.4 Области применения интернета вещей в сельском хозяйстве и технологические барьеры

Мировые тренды развития платформенных решений и сервисов по применению интернета вещей в АПК формируются на основании запросов рынка. В целом, инновационные решения нужны для оптимизации полива и внесения средств обработки растений, оптимизации использования рабочей силы, прослеживаемости цепочек поставок, а также для повышения эффективности и рентабельности фермерских хозяйств. Фермерам, агрономам, консультантам становятся доступны мобильные или онлайн-приложения, которые при загрузке данных о поле (координаты, площадь, тип культур, прошлая урожайность) и предустановке датчиков контроля с беспроводным обменом данных (WiFi, LoRa, 3G|4G|5G и др.) способны предоставлять точные рекомендации и рекомендовать последовательность действий с учетом анализа многих исторических и текущих факторов, как на своем участке, так и во внешнем окружении, комбинируя данные с техники, датчиков, дронов, спутника, других внешних приложений. Таким образом производителя получают оперативную информацию о состоянии их полей,

садов, ферм, теплиц и возможность превратить их в «умные» объекты АПК (Рис. 3.3).

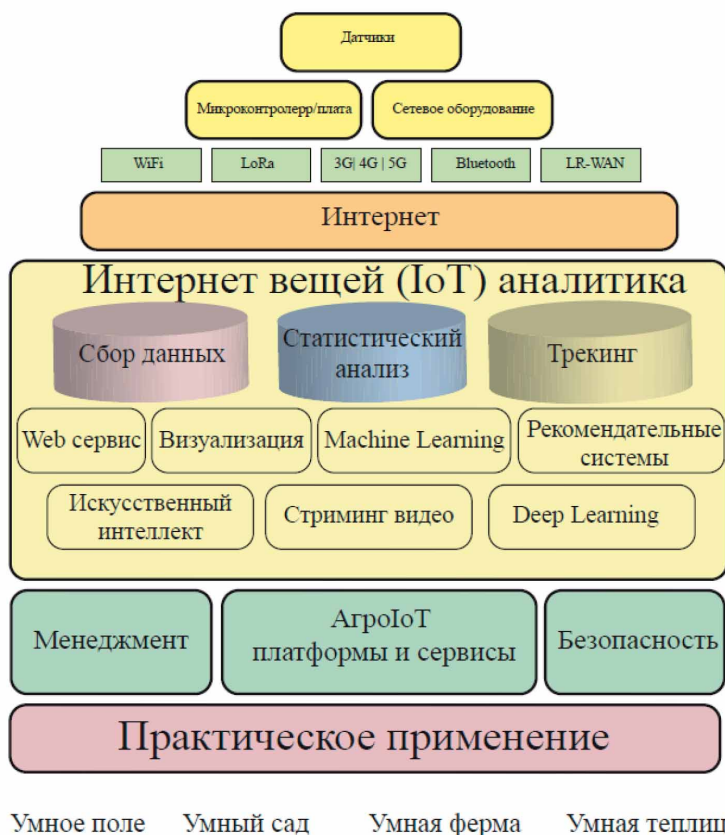


Рисунок 3.3– Концепция технологической архитектуры Интернета Вещей для решения проблем в сельском хозяйстве
Источник: составлено авторами

Несовершенство оборудования, ограниченность каналов передачи информации и иные причины могут существенно ограничивать внедрение интернета вещей в АПК. Некоторые из этих причин представлены в Таблице 3.1 на примере популярных в мире продуктов.

Таблица 3.1– Примеры актуальных вопросов в сельском хозяйстве, для которых коммерчески доступны решения, базирующиеся на интернете вещей

Решаемая проблема	Технология Интернета Вещей, способная решить проблему	Пример доступного оборудования	Технологические барьеры к внедрению
Контроль влажности почвы в теплицах и на полях, автоматические оросительные системы	Установка программируемых датчиков полива и их синхронизация с микроконтроллерами и сервисами прогноза погоды в сети Интернет в режиме реального времени	RainMachine Mini-8® от Amazon, датчики влажности почв от CropX, система контроля влажности почв с базовой радиостанцией LPWAN «Вавиот»	Несовершенство прогнозов погоды. Прогнозы составляются на основании данных с метеостанций и экстраполируются на довольно большую территорию. Фактически система умного полива может включиться во время осадков. Дефицит квалифицированных кадров. Менее 10% пользователей, которые приобрели оборудование для ирригации, продолжают его долгосрочную эксплуатацию. У многих не хватает опыта для самостоятельного внедрения.
Селективное внесение удобрений	Датчики контроля показателей почв, интегрированные по каналу беспроводной связи с облачными сервисами интернета вещей способны в режиме реального времени передавать информацию фермеру о рекомендуемых дозах внесения и эффективности действия удобрений.	Зонды Teralytic, включающие в себя датчики на 26 показателей почв, производят снимки почвенных условий, и передают информацию на облачный сервер с помощью беспроводной технологии LoRa	Главным недостатком является точечный характер получаемых показателей. Чтобы дать правильную оценку состоянию почвы будет недостаточно одного датчика. Чем больше точек измерения, тем достовернее будет информация о содержании и эффективности

			<p>действия удобрений на выбранном участке.</p> <p>Аккумуляторные батареи беспроводных датчиков не приспособлены к условиям зимы и резким перепадам температур в осенне-весенний период.</p>
<p>Учёт и увеличение поголовья животных, контроль пастбищ и полей, расширение площадей выпаса без увеличения расходов на персонал</p>	<p>Дистанционное отслеживание количества, перемещений животных и их здоровья</p>	<p>Pet®, KingNeed 3G Cow Collar Solar® беспроводные датчики местоположения (GPS), движения (акселерометр) и температуры, а также платформенные продукты (например, SAP Cloud Platform) для удаленного контроля за поголовьем скота</p>	<p>Большинство датчиков местоположения животных основано на технологии GPS, что дает дополнительное преимущество в виде автономности. Однако, есть проблема большого энергопотребления на подвижном объекте. Кроме того, большим недостатком является ограниченный радиус действия такой системы, как правило, не превышающий 15-20 км.</p>
<p>Дозированное применение пестицидов и инсектицидов на полях и в теплицах</p>	<p>Системы контроля количества вредителей, основанные на видео-фиксации и распознавании количества вредителей определенных видов в специальных ловушках, экстраполяции полученных данных; онлайн рекомендации для фермеров по дозам обработки</p>	<p>Semios ловушки насекомых, камеры и алгоритмы распознавания видов, удаленная рекомендательная система [3.7]</p>	<p>Возможности распознавания насекомых ограничены и лимитированы предустановленным разработчиком датасетом («популярными» вредителями насекомыми для страны в которой разрабатывали ПО)</p>
<p>Удаленный мониторинг объектов АПК</p>	<p>Системы контроля, мониторинга и оперативного управления,</p>	<p>OpIRIS [3.8], Plantik [3.9], GetSenso [3.10], Monnit [3.11], Sensaphone [3.12]</p>	<p>Эффективность систем существующим образом зависит от скорости «отклика»</p>

	организованные в форме веб-приложения, сервера сбора данных и аналитики, общающихся с удаленными сенсорами/датчиками		используемых каналов передачи данных. Вопрос квалификации исполнителей по установке и поддержке данных систем выходит на первый план.
--	--	--	--

Источник: составлено авторами

В России АПК всегда считался одним из крупнейших и важнейших секторов экономики. К примеру, в Указе Президента России №204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [3.13] была поставлена задача преобразования АПК в высокопроизводительный экспортно-ориентированный сектор, развивающийся на основе современных технологий и обеспеченный высококвалифицированными кадрами. Однако для развития Интернета Вещей в АПК России необходимо преодолеть ряд барьеров:

— Инфраструктурный:

- недостаточное развитие в сельской местности цифровой инфраструктуры, качественных каналов связи, особенно в «глубинке». Несмотря на то, что в этой области происходят радикальные изменения, цифровое неравенство между городом и селом сохраняется. Согласно выборочному федеральному статистическому наблюдению Росстата в 2016 г. доступ к сети Интернет в личных подсобных хозяйствах имело всего 19,2% населения;
- недостаточное покрытие сетями связи, что затрудняет оперативную передачу данных с электронных устройств. Во многих регионах отсутствует устойчивый GSM сигнал, вследствие чего аграрии вынуждены оплачивать услуги спутниковой связи [3.14];

— дефицит квалифицированных кадров. По данным Минсельхоза России, сегодня в России вдвое меньше IT-специалистов, работающих в сельском хозяйстве, чем в странах с традиционно развитой сферой АПК. Нехватка IT специалистов может достигать 90 тыс.

человек. При этом деятельность научных организаций и вузов сельскохозяйственного профиля в значительной степени оторвана от отраслевого заказа. По состоянию на 2018 года в России отсутствуют образовательные стандарты подготовки бакалавров и магистров не только в сфере инновационного сельского хозяйства, но и в таких направлениях как «ИТ в сельском хозяйстве», «математика, анализ больших данных, ИИ в сельском хозяйстве», «робототехника в сельском хозяйстве», «автоматизация и управление бизнес-процессами» [3.15]. Ряд образовательных центров (Сколковский институт наук и технологий, РГАУ-МСХА и др.) в пилотном режиме запускают собственные образовательные программы, курсы повышения образования и квалификации, однако количество выпускаемых специалистов в среднесрочной перспективе будет исчисляться десятками человек в год, а не требуемыми сотнями;

- серьезной угрозой долгосрочной конкурентоспособности АПК является недостаточная инновационная и инвестиционная активность на фоне слабого взаимодействия между бизнесом, образованием и наукой. В настоящее время инновационное развитие сельского хозяйства носит инерционный характер. В частности,
 - внедрение продуктов и цифровых платформ происходит с существенным опозданием;
 - отсутствуют комплексные «коробочные» решения в области интернета вещей для АПК. На рынке представлены отдельные сервисы и приложения, однако предприятия повсеместно сталкиваются с трудностями при адаптации этих решений под свои потребности и интеграции решений между собой;
 - наблюдается диспропорция в технологической модернизации АПК: прогрессивные технологии внедряются, главным образом, на крупных предприятиях, имеющих финансовые возможности для их приобретения;
- общий консерватизм аграриев – согласно данным всероссийской переписи населения по состоянию

на 2016 год всего 6% сельскохозяйственных организаций и 0,98% фермерских хозяйств и индивидуальных предпринимателей пользовались такими элементами цифрового сельского хозяйства и интернета вещей как системы точного вождения и дистанционного контроля качества выполнения технологических процессов, вмонтированные в отдельные виды техники;

- правовой – несовершенство нормативно-правового регулирования освоения технологий интернета вещей в сельском хозяйстве и необходимость упрощения бюрократических процедур на всех этапах сбора, хранения, передачи и обработки информации в сельском хозяйстве.

3.1.5 Выводы

Внедрение технологий интернета вещей в российском АПК связана с решением целого комплекса задач — начиная от формирования единой национальной системы стандартов цифровой экономики и разработки модельных архитектур высокоавтоматизированных и роботизированных интеллектуальных цифровых производств и заканчивая созданием специализированной цифровой инфраструктуры и внедрением профильных образовательных программ, ориентированных на подготовку специалистов «цифрового сельского хозяйства» в системе высшего и среднего специального образования.

В среднесрочной перспективе качественный рывок в производительности, обеспечение конкурентоспособности основных групп российских продуктов и экономическое вытеснение ими импортных товаров способны обеспечить: рост механизации сельского хозяйства (комбайны, тракторы, дроны, робототехника, малая самоходная и другая сельхозтехника) и увеличение сетевого покрытия сельскохозяйственных земель России. В долгосрочной перспективе в основе трансформации АПК, по-видимому, будет принятие и распространение интернета вещей и технологий обработки больших массивов данных в сельском хозяйстве, а также повышение образования и квалификации специалистов.

3.2 Обеспечение информационной безопасности в системах интернета вещей³⁹

3.2.1 Введение. Состояние вопроса

Современные сети передачи данных и, в частности, системы интернета вещей (мобильные сети, сенсорные сети, автоматизирование системы контроля и учета коммунальных услуг и т.п.), с одной стороны, находят широкое применение в промышленности и становятся важным элементом информационной инфраструктуры общества, а с другой, предполагают использование не только надежных, но и совершенно новых специальных безопасных телекоммуникационных технологий и технологий защиты информации. На сегодняшний день не только не решены вопросы создания аппаратуры, реализующей безопасные технологии, но и сами эти технологии нуждаются в дальнейшем развитии. Разрабатываемые в настоящее время международные стандарты, поддерживающие технологии защиты информации, далеки от совершенства и требуют адаптации к отечественным условиям. В силу ряда объективных и субъективных причин российские компании и научные центры практически не принимают участия в разработке и принятии международных рекомендаций в области защиты информации, что естественно приводит к влиянию маркетинговых интересов иностранных корпораций на российских производителей аппаратуры.

Другой серьезной проблемой в области развития безопасных инфокоммуникационных технологий является отсутствие независимого сообщества производителей средств защиты. Многолетнее использование государством регуляторных механизмов во всех областях, связанных с защитой информации (в том числе и тех, где такая регуляция не соответствует мировой практике) привело к тому, что в стране фактически отсутствует свободная конкуренция в сфере разработки алгоритмов, протоколов, технических средств и систем информационной безопасности. Как следствие, отсутствует и независимая экспертиза существующих и перспективных разработок в области безопасных ИКТ

³⁹ Кабатянский Г.А. (Сколтех), Крук Е.А. (МИЭМ НИУ ВШЭ)

технологий, нет структур, которые могли бы успешно представлять Россию в международных институтах соответствующего профиля.

В настоящее время за рубежом действуют сразу несколько крупных структур, осуществляющих и координирующих образовательные, исследовательские, аналитические и технологические программы в области информационной безопасности.

В первую очередь, это Международный совет консультантов по электронной коммерции (International Council of Electronic Commerce Consultants, EC-Council), Институт SANS и Международный консорциум по сертификации в области информационной безопасности (International Information Systems Security Certification Consortium, (ISC)²), Европейский исследовательский проект для определения безопасных шифровальных алгоритмов (NESSIE), Европейская сеть передовых технологий в области криптологии (ECRYPT II). Область их компетенции включает мониторинг вредоносной и подозрительной активности в сети, проведение аудита безопасности организаций и технических средств, поддержку исследований и научных программ, организацию конференций, образовательную деятельность и т.д. Всё это позволяет им оперативно реагировать на любые вызовы в области компьютерной и сетевой безопасности и в кратчайшие сроки предоставлять специалистов по запросу бизнеса и государства.

Ключевая компетенция подобных центров – это программы, направленные на обучение, тестирование и выдачу сертификатов, подтверждающих квалификацию специалистов в области информационной безопасности: CISSP (Certified Information Systems Security Professional) от (ISC)², SANS GIAC (Global Information Assurance Certification) и Certified Ethical Hacker от EC-Council.

Наряду с сертификационными программами крупных западных вендоров (Microsoft, Oracle, Cisco) данные программы полностью занимают нишу подтверждения профессиональной квалификации в области информационной безопасности в нашей стране. Со временем это грозит «ползучей» потерей суверенитета в области безопасных информационных технологий, как с позиции программ-

но-технического обеспечения (подавляющая часть специализированного оборудования и ПО разработана за рубежом), так и с позиций организационно-юридических (отечественное законодательство игнорируется). Как итог – в области безопасных информационных технологий РФ, во многом, исключена из профессионального сообщества и выступает только в роли конечного потребителя решений.

Характерным примером является полное отсутствие российских специалистов в международных комитетах по стандартизации (на уровне ООН, МЭК и ИСО) в области информационной безопасности.

Наконец, еще одной проблемой в отечественной практике является, прямо вытекающее из сказанного выше, отсутствие у разработчиков и пользователей культуры информационной безопасности. Имеющаяся у России репутация страны – источника спама и хакерских атак, хотя, быть может, и преувеличена, но базируется на безусловно имеющих место явлениях. Так, по данным «Лаборатории Касперского» во втором полугодии 2011 г. Россия лидировала по количеству атак, исшедших с территории страны, являясь источником не менее 16% всего мирового DDoS-трафика. Считается, что на долю «русских хакеров» приходится не менее трети мирового рынка киберпреступлений, что в 2011 г. составило почти \$4,5 млрд. При этом, объем рынка киберпреступлений ежегодно удваивается, происходит централизация и укрупнение хакерских группировок и сообществ.

Преодоление описанных выше проблем требует сочетания организационных, технологических мер и популяризации культуры информационной безопасности в среде разработчиков и пользователей систем беспроводной связи.

3.2.2 Тенденции в развитии технологий защиты информации

В ближайшие десятилетия развитие автоматизированных систем и сетей связи, беспроводных средств передачи и обработки информации в значительной степени пройдет под знаком внедрения безопасных технологий. Наиболее значимые тенденции в области инфокоммуникационных технологий связаны с развитием систем IoT и индустриального

интернета, которые неразрывно связаны с использованием мобильной связи, облачных и RFID-технологий.

При использовании облачных систем пользователь должен передать собственные данные для обработки с привлечением сторонних ресурсов. При этом он даже не знает, кому принадлежат вычислительные средства, которые обрабатывают его запросы. Поэтому ключевым ограничением для распространения облачных систем могут стать вопросы защиты информации. Вопросы создания безопасных облачных технологий не только не решены, но находятся в начале своей разработки.

Развитие мобильной связи было обусловлено грандиозными успехами в области микроминиатюризации средств вычислительной техники, но и само это развитие стимулировало дальнейшие успехи в этой области. В результате сегодняшние мобильные устройства обладают настолько серьезными вычислительными возможностями, что с их помощью могут осуществляться уже многие коммерческие процессы. В частности, огромные перспективы мобильных устройств связаны с их использованием в банковской сфере. В перспективе большинство платежных операций будет выполняться с помощью мобильных телефонов. И здесь одними из ключевых становятся вопросы, связанные с защитой информации. Вопросы защиты являются первостепенными и при использовании RFID-устройств, вычислительные возможности которых, как правило, очень ограничены. Возникает новое направление прикладной защиты информации – разработка систем информационной безопасности, ориентированных на устройства с ограниченными вычислительными и энергетическими ресурсами. В частности, при обеспечении информационной безопасности «интеллектуального дома», различных коммерческих приложений, при разработке систем информационной безопасности сенсорных сетей и в ряде других сетевых приложений, стоимостные, энергетические или габаритные требования накладывают ограничения на память и/или быстродействие используемых процессоров. Между тем стандартизированные алгоритмы аутентификации и распределения ключей

вычислительно трудоемки, что делает проблематичным их использование. Встает вопрос о развитии так называемых «легких» алгоритмов защиты, ориентированных на реализацию с помощью устройств, обладающих ограниченными вычислительными ресурсами.

Появление этих и некоторых других новых направлений в области построения безопасных информационных технологий дает уникальный шанс преодолеть наметившееся отставание в области защиты информации – принять участие на самых начальных этапах разработки. Следует отметить, что безопасные технологии фактически представляют ветвь не отрасли информационной безопасности, а отрасли ИКТ. Поэтому реальность использования указанного шанса базируется на долгой и успешной истории построения инфокоммуникационных технологий в нашей стране.

Без развития безопасных инфокоммуникационных технологий и вовлеченности в мировые сообщества в области информационной безопасности трудно рассчитывать на серьезные позиции в мировом инновационном процессе создания ИТ-отрасли. Представляется, что мировому сообществу специалистов информационной безопасности потребуются и соответствующий партнер в России. Поэтому кажется целесообразным развивать в России не только сами исследования безопасных технологий, но и инициировать шаги по формированию независимого профессионального сообщества в области информационной безопасности. Таким образом, основными целями в области обеспечения безопасности для систем беспроводной связи и IoT являются:

- проведение и координация исследований в области создания безопасных информационных технологий для быстро развивающихся направлений ИКТ;
- создание независимого профессионального сообщества специалистов в области безопасных информационных технологий;
- просветительская работа, направленная на обучение безопасным информационным технологиям широкого круга разработчиков и пользователей информационных технологий.

Для реализации указанных целей необходимы:

- координация и инициирование коммерческих проектов в области создания безопасных информационных систем на базе исследований, проводимых на стыке инфокоммуникационных технологий и технологий информационной безопасности;
- проведение исследований, разработка новых методов и алгоритмов в области создания безопасных информационных технологий для прорывных направлений (в том числе для облачных технологий, технологий «больших данных», легкой криптографии и др.);
- развитие системы независимой сертификации специалистов и технологий в области безопасных информационных технологий;
- создание открытой технологической площадки для апробации новых технологий и методов защиты информации;
- проведение независимой экспертизы АИС и ПО с точки зрения информационной безопасности;
- заключение соглашений о сотрудничестве с рядом университетов и академических институтов с целью координации усилий в области создания безопасных информационных технологий;
- заключение соглашений о сотрудничестве с рядом международных организаций, осуществляющих координацию исследований в области информационной безопасности;
- привлечение к работе ведущих зарубежных ученых и инженеров;
- заключение договоров о сотрудничестве с сообществами производителей инфокоммуникационной техники;
- создание условий для развития экосистемы безопасного интернета;
- разработка рекомендаций по созданию безопасного ПО и проектированию защищенных АИС;

- организация конкурсов по прорывным направлениям с целью выявления перспективных идей и коллективов, ориентированных на создание интеллектуальной собственности стартапов.

3.2.3 Направления прорывных научных исследований

В соответствии с выделенными нами тенденциями в развитии систем безопасности для IoT прорывными направлениями исследований центра в области ИБ предполагаются:

1. Защита информации в «облачных» системах.
2. Безопасные ИКТ-технологии для систем с ограниченными вычислительными ресурсами.

Еще одним направлением прорывных исследований должно стать направление постквантовой криптографии, которое связано с предотвращением атак с использованием квантового компьютера. Это направление является важным не только для систем беспроводной связи и ИВ, но и для всей отрасли безопасности в целом.

3.2.3.1 Защита информации в «облачных» системах

Для организации защищенной работы в облачных системах требуется, как минимум, решить три основные задачи.

- создание общего защищенного хранилища данных;
- организация защищенных вычислений;
- разработка «облачной» политики безопасности.

Создание общего хранилища, по-видимому, наиболее простая из сформулированных задач, но даже она не может в настоящее время считаться решенной. Для того, чтобы организовать защищенное хранилище необходимо не только разграничить доступ к данным этого хранилища, но и обеспечить работу с данными, при которой владелец предоставляемых пользователю вычислительных ресурсов не может, по крайней мере, полностью, ознакомиться с данными, которые он хранит. Более того, организация защищенных вычислений требует проводить их, не расшифровывая данные. Эта задача решается с помощью так называемых гомоморфных алгоритмов, теория которых находится в зачаточном

состоянии. Наряду с криптографическими примитивами требуется определить и порядок пользования облачными системами. Известно, что все случаи удачных компьютерных преступлений связаны не с вскрытием алгоритмов шифрования, а с использованием неудачных настроек и нарушением политик безопасности в сети. В облачных системах также возможен несанкционированный доступ к данным без вскрытия защищенного хранилища или защищенных вычислений. Нужны правила работы в облачных системах – политики безопасности таких систем.

Первоочередными задачами можно назвать следующие:

- дать классификацию задач защиты информации в облачных системах;
- разработать и реализовать защищенную программно-аппаратную систему хранения данных в облаке;
- разработать и реализовать защищенные алгоритмы для проведения вычислений в облаке;
- разработать принципы создания политик безопасности для облачных систем.

3.2.3.2 Безопасные ИКТ-технологии для систем с ограниченными вычислительными ресурсами.

В настоящее время эта область пользуется наиболее пристальным вниманием со стороны производителей, потребителей и разработчиков. Именно легкие (не требующие больших вычислительных ресурсов) алгоритмы должны обеспечить безопасность многочисленных устройств с NFC (Near Field Communication), систем с RFID и сенсорных сетей. Коммерческое использование таких систем в настоящее время имеет очень широкий спектр применения – начиная от систем дистанционной медицины (Distance Healthcare), где безопасность особенно актуальна при использовании энергонезависимых пассивных и активных датчиков, до систем контроля и учета в крупных торговых сетях и логистике.

Возможность построения достаточно стойких алгоритмов защиты информации на устройствах с ограниченными

ресурсами основана на том, что многие принятые в современной практике требования к системам безопасности оказываются слишком жесткими для определенных коммерческих приложений. Некоторые особенности самих устройств также могут быть использованы для обеспечения безопасности. Вычислительно легкие алгоритмы обеспечения безопасности могут строиться с учетом того, что:

- они (алгоритмы) предназначены для передачи ограниченного, сравнительно небольшого, числа сообщений за сеанс;
- защищаемая информация, как правило, имеет ограниченное время актуальности;
- для вычислений можно использовать несколько слабых устройств;
- защищаемая информация может храниться распределенным образом.

При использовании слабых устройств вряд ли могут быть применены стандартные криптографические алгоритмы. Естественный подход, состоящий в том, чтобы на слабых устройствах использовать стандартные алгоритмы с уменьшенным ключом, не дает удовлетворительных результатов, т.к. стойкость этих алгоритмов быстро падает с уменьшением длины ключа. Для построения безопасных информационных технологий, ориентированных на применение в устройствах с ограниченными вычислительными ресурсами, требуются алгоритмы, стойкость которых растет экспоненциально относительно сложности самих этих устройств. Поэтому перспективными представляются алгоритмы, построенные на базе корректирующих кодов и алгебро-геометрических конструкций.

В рамках рассматриваемого направления построения безопасных ИКТ-технологий важно:

- дать классификацию задач и алгоритмов для систем с ограниченными вычислительными ресурсами;
- провести сравнительный анализ подходов и конструкций для решения этих задач;

- разработать полную систему алгоритмов защиты информации для устройств с ограниченными ресурсами;
- разработать и реализовать технологическую платформу для решения задач построения безопасных ИКТ-технологий для систем с ограниченными ресурсами.

Отдельным и особенно востребованным в настоящее время направлением систем с ограниченными вычислительными ресурсами являются RFID-системы.

3.2.3.3 Обеспечение информационной безопасности RFID-технологий

Энергоэффективные RFID-технологии активно используются в различных бизнес-приложениях. При этом остро встает вопрос обеспечения требуемого уровня информационной безопасности RFID-систем, что приводит к необходимости разработки алгоритмов и протоколов безопасной обработки и передачи данных. Разработка таких алгоритмов и протоколов позволит существенно ускорить внедрение инновационных RFID-систем в различных областях хозяйственной деятельности, и повысить эффективность их работы за счет мобильности и оперативности предоставления защищенных данных.

Ограниченные возможности RFID-систем по объему памяти и вычислительным ресурсам требуют использования специальных методов обеспечения информационной безопасности. Такие методы должны быть адаптированы к существующим ограничениям и учитывать особенности обрабатываемой и передаваемой информации. Необходимо разработка легких алгоритмов и протоколов безопасного хранения, обработки и обмена данными, а также их программно-аппаратная реализация, как для RFID-меток (активные, полуактивные и пассивные RFID), так и для элементов, взаимодействующих с RFID-метками (RFID-считыватели, автономные или объединенные в сеть).

В рамках разработки легких алгоритмов защиты информации для RFID-систем важно провести следующие работы:

- разработать систему алгоритмов для решения задач конфиденциальности, целостности и аутентификации в RFID-системах;
- разработать безопасные протоколы взаимной аутентификации, выработки, распределения ключей и т.д., ориентированные на использование в RFID-системах.

3.2.3.4 Постквантовая криптография

Одним из главных достижений теории квантовых алгоритмов стала разработка Шором полиномиального алгоритма решения задачи факторизации. Появление этого алгоритма означает, что после создания достаточно мощного квантового компьютера алгебраические криптосистемы, основанные на задаче факторизации (а это большинство известных систем), окажутся скомпрометированными. В связи с этим появилось понятие постквантовой криптографии, т.е. криптографии, стойкость которой не подвергнется сомнению в связи с появлением квантовых компьютеров. Одним из основных направлений, разрабатываемых в рамках постквантовой криптографии, является построение криптосистем, основанных на использовании корректирующих кодов (кодовые криптосистемы). Возникшие одновременно с алгебраическими, кодовые криптосистемы долгое время рассматривались, как чисто теоретические. Однако, значительные успехи в области реализации средств кодирования-декодирования в сочетании с прогрессом в разработке квантовых алгоритмов и появлением новых постановок задач защиты информации привели к возрождению интереса к кодовой криптографии.

Прежде всего, следует отметить, что задача декодирования линейных кодов, которая лежит в основе кодовых криптосистем, является NP-полной и, по-видимому, не будет решена за полиномиальное время даже с помощью квантовых компьютеров.

Практическое значение кодовых криптосистем не исчерпывается вопросами защиты информации от атак с использованием квантового компьютера. Кодовые криптосистемы имеют большие перспективы и при реализации на малоресурсных устройствах (легкая криптография)

3.3 Предсказательное техническое обслуживание⁴⁰

3.3.1 Введение

В настоящее время технологии интернета вещей являются одними из самых быстрорастущих, привлекают колоссальные объемы частных и государственных венчурных инвестиций и входят в список стратегических направлений, поддерживаемых правительством РФ. Как показано в первом разделе данной книги, рынок интернета вещей растет как в физическом, так и в денежном выражении.

«Индустриальный интернет вещей» (Промышленный интернет, ПоТ) – разновидность «Интернета Вещей», концепция вычислительной сети, промышленных производств и сложных физических машин, интегрированных с интеллектуальными системами, см. [3.25].

Организация таких сетей способна перестроить экономические и производственные процессы, исключая человека из части действий и операций и способствуя росту экономики.

Например, с помощью ПоТ огромное количество устройств энергосистемы могут обмениваться данными в режиме реального времени, которые затем оперативно доставляются потребителям и поставщикам коммунальных услуг.

Обработка и анализа данных, собираемых в рамках ПоТ с помощью современных методов предсказательной аналитики позволит

- обслуживать оборудование на основе автоматического контроля его состояния (т.н. предсказательное техническое обслуживание, ПТО);
- обеспечивать надежность и эффективность работы сложных технических и информационных систем (самолетов, судов, ракет, ядерных электростанций, различных интернет-сервисов, и т.д.);
- проводить автоматический контроль качества выпускаемой продукции и т.д.

⁴⁰ Бурнаев Е.В. (Сколтех)

Отметим, что в 2015 г. оборот рынка только операционного предсказательного обслуживания составил 582 миллиона долларов. Как прогнозируется, он вырастет к 2020 г. до 1.8 миллиарда долларов [3.26, 3.27]. Многие высокотехнологичные компании достигли значительного снижения затрат и сумели повысить свою прибыль за счет использования даже относительно простых методов интеллектуального анализа данных индустриального интернета вещей (см. раздел 3.3.3).

Значит, крайне важна разработка технологий и методов предсказательной аналитики, которые позволят эффективно проводить интеллектуальный анализ данных индустриального интернета вещей и решать соответствующие практически важные задачи.

- Таким образом, цель данной работы состоит в том, чтобы
- описать структуру и особенности приложений ПТО (раздел 3.3.2);
 - привести примеры приложений ПТО и на их основе охарактеризовать требования индустриальных приложений к реализации соответствующих алгоритмов предсказательной аналитики (раздел 3.3.3);
 - привести краткий обзор моделей и методов решения задачи обнаружения аномалий, которая часто возникает при реализации приложений ПТО, в частности, описать подход к её решению с помощью описания нормального состояния инженерной системы, которое может быть сделано, например, с помощью однокласовой классификации (раздел 3.3.4);
 - описать пример применения специализированного метода обнаружения аномалий с использованием привилегированной информации для обнаружения поломок датчиков автоматических дорожных метеостанций в контексте системы прогнозирования параметров дорожного полотна (раздел 3.3.5);
 - сделать выводы из проделанной работы и обозначить пути решения поставленных задач (раздел 3.3.6).

3.3.2 Предсказательное техническое обслуживание

До недавнего времени возможности доступа к информации были ограничены, а ее получение и хранение дорогостоящи (см. Рис. 3.4).



Теплоэлектростанция - 10^3 наблюдений/мс



Завод металлопроката - 10^4 наблюдений/мс



Современный самолет - до **0.5 Тб за полет**

- Сейчас используется менее 1%, большая часть информация не хранится и не анализируется
- Следующее поколение двигателей Pratt & Whitney до **10 Гб/сек**



Автопилотируемые машины Google - до **1 Гб/сек**

- Болид Формулы-1 - **1.2 Гб/сек**

Данные внутренних исследований, публикаций компаний Airbus, Boeing, Google, Pratt & Whitney

Рисунок 3.4– Какие данные уже собираются и могут быть использованы для построения сервисов на основе ИИТ

Источник: составлено автором на основе материалов совместной с П. Ерофеевым презентации

В последние годы появились новые возможности, в том числе:

- возможность быстрого преобразования различных видов информации (текстов, сигналов, изображений, видео и т.п.) в цифровую форму;
- возможность хранения большого объема цифровых данных и быстрого поиска необходимых данных в соответствующих хранилищах;
- возможность быстрой передачи по каналам связи больших объемов данных (а также возможность удаленного доступа к данным, в том числе одновременного доступа для большого числа пользователей);
- возможность быстрой обработки больших массивов данных (с использованием средств сверхвысокой производительности, распределенных вычислений и т.д.);

- недорогие способы сбора данных о показателях функционирования различных сложных технических и информационных систем.

Примерами сложных многокомпонентных и распределенных технических и информационных систем являются распределенные многосенсорные системы, аэрокосмические системы, роботизированные сети, электрические сети, производственные системы.

Такие системы генерируют большие объемы гетерогенной информации, например, мультимодальные временные последовательности, изображения и видео. Предполагается, что следующее поколение этих систем будет обладать способностью к обучению и автономному обнаружению квазистационарных паттернов в больших объемах информации, генерируемой нестационарными и нелокальными процессами. Целью является всесторонняя оценка ситуации в реальном времени через выявление причинной динамики системы, а также адекватное стохастическое моделирование и количественная оценка неопределенности. Это необходимо для того, чтобы:

- вести более точный и своевременный контроль работоспособности отдельных узлов и всей системы в целом;
- проводить постоянный мониторинг и анализ внутреннего и внешнего состояния оборудования;
- повысить безопасность работы и более оперативно и в некоторых случаях превентивно реагировать на возможные аварии и выходы из строя оборудования (в том числе трудно контролируемого, например, спутников), тем самым повышая время жизни оборудования.

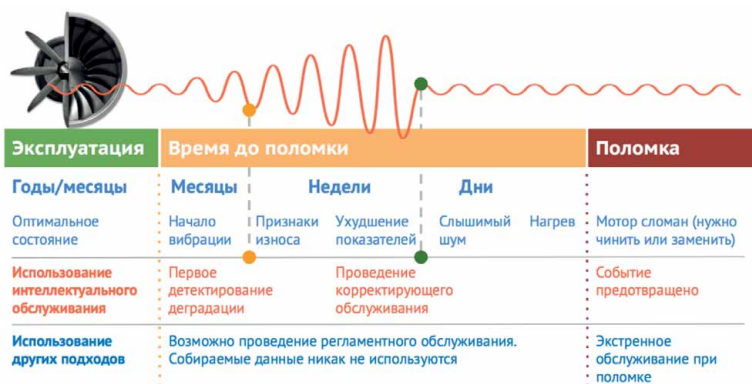


Рисунок 3.5– Концепция предсказательного технического обслуживания (ПТО)

Источник: составлено автором на основе материалов совместной с П. Ерофеевым презентации

Общим подходом к решению этих прикладных задач является разработка методов заблаговременного обнаружения поломок. На практике это возможно потому, что перед наступлением поломки характер поведения инженерной системы меняется, и в данных, снимаемых с датчиков инженерной системы, зачастую содержатся паттерны, косвенно свидетельствующие о приближении поломки. Анализируя обнаруженные паттерны⁴¹, можно выявить условия, которые с большой вероятностью приводят к той или иной поломке, и, в конечном итоге, её предсказать. Задача ПТО (см. Рис. 3.5) и состоит в том, чтобы выявлять эти паттерны как можно раньше и предотвращать критические поломки.

Неудивительно, что точные и надежные математические методы и модели играют ключевую роль при решении задач ПТО. Действительно, в таких областях, как авиация, принципиально важно иметь модели и алгоритмы принятия решений, обеспечивающие максимальную точность предсказаний и строго ограниченный уровень ложных тревог.

⁴¹ Другими словами, аномалии в поведении системы, когда наблюдаемые процессы претерпевают изменения распределения в ответ на изменение окружающих условий или, в более общем виде, в ответ на изменение тех или иных характеристик.

Очевидно, что стандартная практика обслуживания по регламенту не позволяет решить задачи ПТО, хотя и обеспечивает выполнение авиационной отраслью требований государственных регулирующих органов по безопасности.

Часто при выборе стратегии технического обслуживания необходимо оптимизировать сразу несколько целевых показателей. Например, в авиации необходимо, с одной стороны, обеспечить безопасность и надежность перевозок (safety and reliability), с другой – увеличить доступность воздушного судна (availability), снизить затраты на обслуживание (maintenance costs) и минимизировать число перерывов в эксплуатации (operational interruptions). Именно использование современных методов интеллектуального анализа данных и позволяет сбалансировать эти противоречивые целевые показатели, а также

- значительно сократить затраты на техническое обслуживание, благодаря исключению плановых замен технически исправных и надежных компонент и узлов системы;
- улучшить логистику для обеспечения необходимыми комплектующими;
- более эффективно распределять энергию, совершенствовать управление энергопотребляющими продуктами и снижать энергозатраты и т.п.

Использование ПТО потенциально может привести к построению новых сервисных моделей, см. пример на Рис. 3.6. В частности, в перспективе возможно, например, продавать не конкретный тип оборудования, а время его бесперебойной работы.



Рисунок 3.6– Пример (из авиации) построения принципиально новых сервисов на основе предсказательной аналитики уже собираемых данных

Источник: составлено автором на основе материалов совместной с П. Ерофеевым презентации.

Высокоуровневая схема системы ПТО приведена на Рис. 3.7

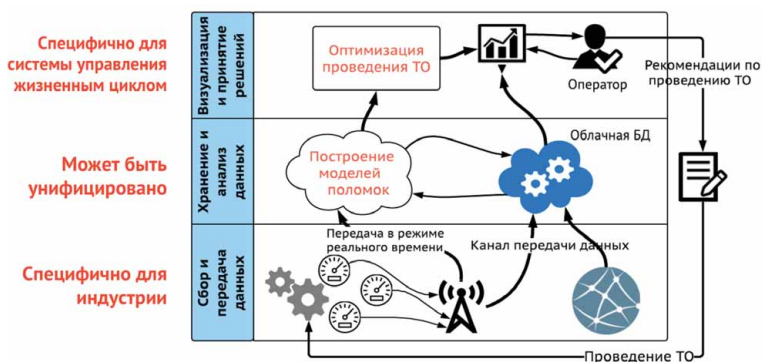


Рисунок 3.7– Схема системы ПТО

Источник: составлено автором на основе материалов совместной с П. Ерофеевым презентации

На нижнем уровне происходит сбор и передача данных с инженерных систем. Соответствующее аппаратное и программное обеспечение специфичны для рассматриваемой индустрии, поскольку требуют сопряжения с инженерным оборудованием (станками, турбинами, и т.п.). На следующем уровне происходит хранение данных, их предобработка

и приведение к единому формату, построение предсказательных моделей. В этом случае соответствующее программное обеспечение и необходимый для решения задач набор методов интеллектуального анализа данных будут мало зависеть от специфики индустриального приложения, поскольку требования к реализации соответствующих алгоритмов предсказательной аналитики в данном случае могут быть в значительной степени унифицированы. Третий уровень системы ПТО обеспечивает визуализацию результатов предсказательной аналитики и повышает эффективность принятия решений оператором системы. В данном случае реализация программного обеспечения может сильно зависеть от специфики системы управления жизненным циклом изделия.

3.3.3 Примеры приложений ПТО

Приведем примеры приложений ПТО для задач аэрокосмической отрасли и на их основе охарактеризуем требования индустриальных приложений к разработке и реализации соответствующих алгоритмов предсказательной аналитики.

Аэрокосмическая индустрия является одной из наиболее регулируемых отраслей, поскольку качество, безопасность и эффективность работы сложных инженерных систем имеет прямые экономические последствия и оказывает непосредственное влияние на жизнь и здоровье людей. Неудивительно, что именно предсказательное обслуживание играет ключевую роль в обеспечении надежности и эффективности работы: важно предсказывать и предотвращать возможные отказы, уменьшать стоимость обслуживания и увеличивать коэффициент использования самолетного парка, соблюдая в то же время правила и процедуры, введенные регулирующими органами.

На практике, сервисная служба, для увеличения уверенности в надежности оборудования, зачастую делает больше профилактической работы, чем необходимо, даже если эти дополнительные предосторожности не всегда приводят к дополнительным выгодам. Более того, в процессе

сертификации аэрокосмического оборудования разрабатываются специальные политики технического обслуживания. Обычно авиакомпании придерживаются этих политик и не предпринимают никаких действий для повышения эффективности процесса обслуживания.

В последние годы крупнейшие производители самолетов и авиакомпании пришли к выводу, что за счет использования методов предсказательной аналитики и инженерного знания можно преобразовать изначально лежащие мертвым грузом данные в полезную информацию и получить дополнительную прибыль. Сервисы ПТО могут оценивать текущее состояние оборудования, определять его операционный статус, своевременно обнаруживать аномальные условия, предотвращать возможный вынужденный простой [3.28 –3.33].

Важными особенностями применения ПТО являются:

- данные для самолетов имеют очень сложную структуру:
 - временные ряды большой размерности (размерность обычно больше нескольких сотен);
 - частота измерений также может быть очень большой (до нескольких десятков тысяч измерений в каждом полете). В то же время частота измерений может быть разной для разных параметров;
 - большие объемы данных (типичный размер выборки данных для обучения измеряется в терабайтах);
 - пропущенные значения, нестационарный шум;
 - сложная иерархическая структура классификатора типов поломок;
 - сложная структура и распределенная природа соответствующего хранилища данных;
- поломки – редкие события. Классические статистические подходы неэффективны для моделирования событий с редкой частотой появления;
- при предсказании поломок мы должны обеспечить обнаружение достаточного (с экономической точки зрения) количества поломок и в то же время поддерживать достаточно низкую частоту ложных тревог.

В результате, разработка автоматизированной системы для предсказания поломок и раннего оповещения о возможных дорогостоящих неисправностях – очень сложная задача.

Многие приложения в области предсказательного обслуживания самолетов основаны на элементарных пороговых правилах мониторинга, способных обнаруживать только очень простые поломки и имеющих высокую частоту ложных тревог. Однако, этого недостаточно для эффективного прогноза поломок.

Например, в каждом из 8 самолетов (A330 и A340) Finnair в течение 2012 г. из-за проблем с системой отбора воздуха произошли задержки вылета длительностью около 20 часов, стоившие авиакомпании около 100 евро в минуту. При этом система мониторинга Airman от производителя самолета компании Airbus или предоставляла предупреждения о таких событиях слишком поздно, или не предоставляла предупреждений совсем [3.34]. Одной из причин было отсутствие эффективных методов предсказания поломок. Компания Finnair смогла решить эту проблему и улучшить доступность своего парка самолетов только после того, как одна из инженеринговых компаний, специализирующаяся на создании систем контроля качества промышленной продукции, разработала для неё необходимые модели и методы на основе интеллектуального анализа данных.

В 2018 г. авиакомпания S7 Airlines первой среди российских авиакомпаний завершила разработку пилотной системы ПТО для воздушных судов Airbus A319 [3.33]. В течение года планируется подключить к системе большую часть парка S7 Airlines. Анализируя массив исторических данных по техническому обслуживанию воздушных судов и работе отдельных компонентов, система позволяет в долгосрочной перспективе прогнозировать возможные дефекты по каждому самолету S7 Airlines. Планируется, что в результате работы системы удастся снизить количество задержек вылетов по техническим причинам. Система определяет вероятность возникновения разных типов дефектов в определенный период в будущем. В случае, если вероятность оказывается выше установленного порога, рекомендуется провести

дополнительную диагностику воздушного судна. Для анализа данных и построения математической модели используется программное обеспечение, разработанное специалистами S7 Airlines совместно с компанией DATADVANCE [3.35], одной из ведущих российских компаний по прогнозной аналитике. Консультантами по инженерно-техническому обслуживанию воздушных судов выступили специалисты S7 Technics. На сегодняшний день массив данных включает значения, зафиксированные в системах телеметрии самолетов, базы данных холдинга технического обслуживания и ремонта авиатехники S7 Technics и метеорологические данные за период с 2012 по 2017 год.

Приведем несколько конкретных приложений ПТО в аэрокосмической отрасли.

Пример 1: ПТО системы охлаждения самолета (проект с компанией DATADVANCE).

Задача состояла в быстром детектировании утечки в системе охлаждения самолета, определении критического уровня хладагента и оценке времени до достижения заданного уровня. Данные для построения модели содержали информацию о временных рядах уровней хладагента по 17 самолетам (~400 полетов каждый год, одно измерение за полет).

Для решения задачи мы построили модель скорейшего обнаружения разладки (появления нисходящего тренда в зашумленном сигнале). На вход модель принимала исторические значения уровня хладагента в скользящем окне и некоторые характеристики от них (среднее, дисперсия, и т.п.), и на выходе оценивалась вероятность наличия нисходящего тренда в сигнале, см. Рис. 3.8.

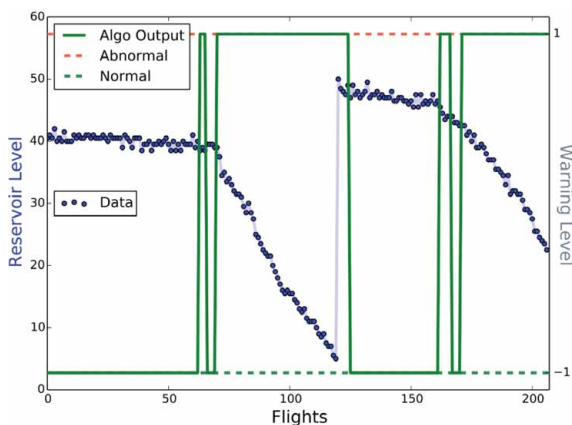


Рисунок 3.8–Зависимость уровня хладагента от времени (в полетах) в системе охлаждения самолета (изображено синим) и зависимость оценки вероятности наличия нисходящего тренда от времени (изображено зеленым)

Источник: совместный проект с компанией DATADVANC

В случае, если происходило обнаружение нисходящего тренда, делался прогноз момента времени достижения уровнем хладагента критического значения (Рис. 3.9).

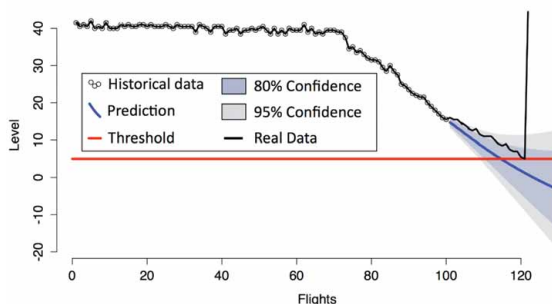


Рисунок 3.9–Зависимость уровня хладагента от времени (в полетах) в системе охлаждения самолета (изображено черным) и прогноз (изображено синим) момента времени достижения уровнем хладагента критического значения (изображено красным).

Источник: совместный проект с компанией DATADVANC

Таким образом, математически данную задачу можно описать как задачу обнаружения разладки (см. раздел 3.3.4.2) в значениях временного ряда в режиме реального времени, с целью обеспечить наискорейшее обнаружение при заданном уровне ложных тревог. В рассматриваемой ситуации удалось добиться, чтобы процент ложных срабатываний был меньше 1%, процент правильно детектированных утечек был больше 99%, а средняя ошибка предсказания достижения критического уровня на 10 полетов вперед – не более 1 полета.

Пример 2: ПТО масляного фильтра двигателя самолета (проект с компанией DATADVANCE).

Задача состояла в предсказании засорения масляного фильтра для оптимизации его обслуживания (минимизации количества проверок и стоимости материалов). Данные для построения модели содержали информацию о значениях более чем 200 параметров, которые автоматически измерялись для 30 самолетов в течение 3 лет (~400 полетов каждый год, несколько измерений в течение полета).

Для решения задачи мы автоматически выявили параметры, связанные с событием (засорение масляного фильтра), и построили модель предсказания засорения фильтра с использованием наблюдаемых данных. Задача предсказания несбалансированная, так как число поломок мало по сравнению с количеством примеров нормального режима работы. По этой причине при отборе параметров использовались методы построения моделей несбалансированной классификации [3.36, 3.37]. Последовательное исключение параметров в конце концов позволило оставить лишь несколько самых важных, включая значение давления масла.

На следующем шаге мы разбили данные на обучающую и тестовую выборки и построили модель для обнаружения поломок, зависящую от глубины памяти значений параметров при прогнозировании; мы настроили значение этого параметра, минимизируя ошибку прогноза. Оказалось, что история, включающая информацию о трех недавних полетах, позволяет получить наиболее точные прогнозы.

Чтобы оценить преимущества предложенного подхода, мы сравнили его с простым пороговым алгоритмом, который прогнозирует поломки, основываясь на том, что в текущий момент времени уровень давления масла ниже чем некоторый фиксированный порог. Результаты для разных горизонтов предсказания вместе с простым пороговым алгоритмом, использующим только величину уровня давления масла, представлены на Рис. 3.10 и Рис. 3.11. Метрики качества для предложенного подхода превосходят метрики качества для простого порогового алгоритма, позволяя предсказать события поломки раньше с той же частотой ложных тревог.

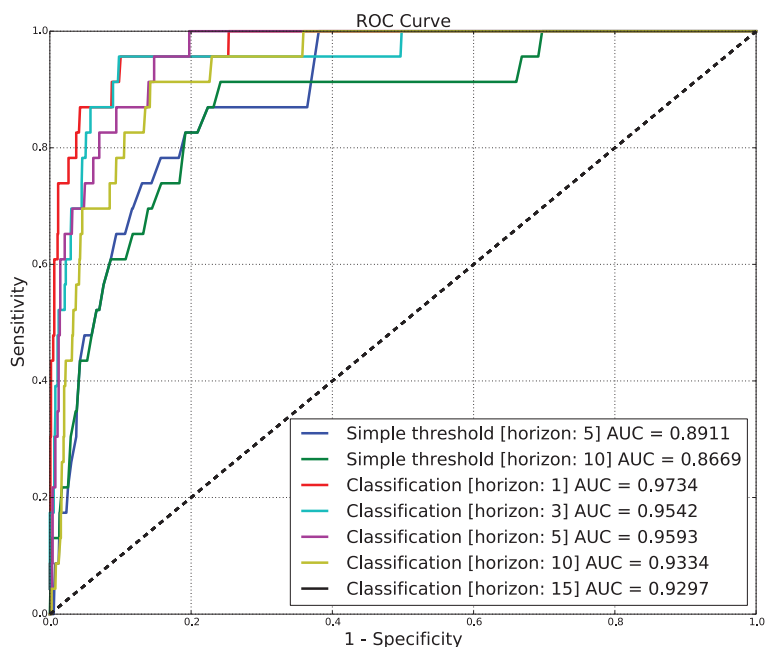


Рисунок 3.10– Низкое давление масла: ROC кривые

Источник: проект с компанией DATADVANCE

На практике прогнозирование в окрестности реальной поломки также допустимо и не будет считаться ложной тревогой. Результаты для поломок, предсказанных в окрестности из ± 2 полетов для реальной поломки, представлены на Рис. 3.11.

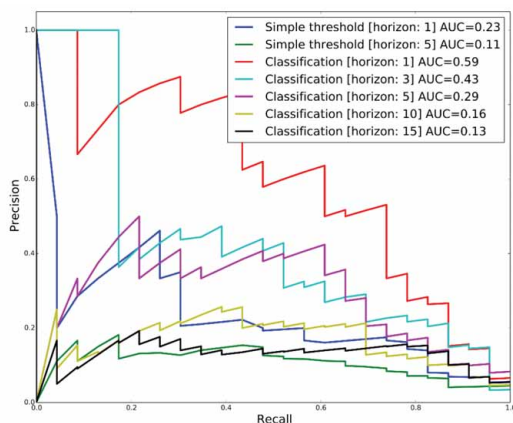


Рисунок 3.11– Низкое давление масла: кривые чувствительности-специфичности

Источник: Проект с компанией DATADVANCE

В результате использования модели появилась возможность обеспечить раннее предупреждение о возможности засорения масляного фильтра. По предварительным оценкам, это дает возможность сократить затраты на обслуживание на 50%.

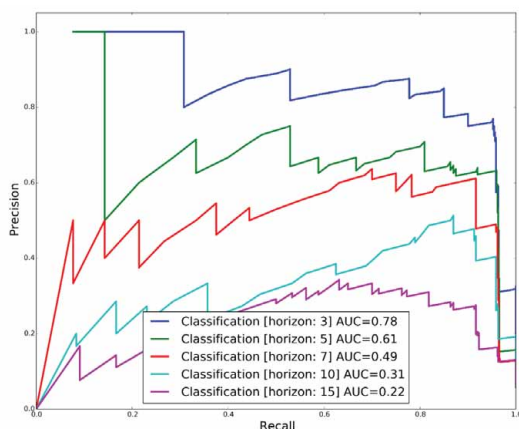


Рисунок 3.12– Низкое давление масла: кривые чувствительности-специфичности для допуска ± 2 полета

Источник: Проект с компанией DATADVANCE

Таким образом, в данной задаче необходимо выделить наиболее значимые параметры, которые позволяют спрогнозировать интересующее событие в будущем, то есть решить задачу несбалансированной классификации будущего события.

Пример 3. Выход из строя вспомогательной силовой установки (совместно с компанией DATADVANCE).

Задача состояла в предсказании поломок заданных типов вспомогательной силовой установки по данным телеметрии, а также логам событий некритических ошибок, зарегистрированных в системе. В каждом полете фиксировались основные физические характеристики ВСУ в трех режимах: запуск ВСУ, запуск двигателей самолета и остановка ВСУ. В качестве параметров (данных телеметрии) выступают температура исходящих газов в различных частях ВСУ, давление, нагрузки, частота оборотов компрессора и т.п.

Такого рода прогнозы необходимы для сокращения затрат из-за задержек вылета самолета по причине поломок вспомогательной силовой установки.

Данные для построения модели содержали информацию о значениях более чем 200 параметров, показания которых автоматически измерялись для 30 самолетов в течение 3 лет (~400 полетов каждый год, несколько измерений в течение полета). Эта задача существенно сложнее предыдущей, так как, во-первых, число примеров реальных поломок в исторических данных небольшое (несколько десятков), во-вторых, на модель налагаются очень жесткие требования в смысле уровня ложных тревог и количества правильно предсказанных поломок, и, наконец, данные, на основе которых строится модель, разнородные (потoki событий и многомерные временные ряды), зашумленные, содержат пропущенные значения и т.п. В данной задаче, таким образом, необходимо построить модели, которые принимают на вход временные ряды телеметрии (за полет может фиксироваться от нескольких десятков до десятков тысяч измерений по сотням параметров) и потоки регистрируемых в системе событий, а на выходе прогнозируют поломку заданного типа с заданным упреждением. Более того, в каждом конкретном случае требуется объяснить, почему модель выдала тот или иной прогноз, в частности, выделить входные параметры, наиболее на него повлиявшие.

В разделе 3.3.4 будет представлена методология, на основе которой возможно эффективное построение моделей, удовлетворяющих указанным условиям.

В результате использования модели появилась возможность обеспечить раннее предупреждение о выходе из строя вспомогательной силовой установки. По предварительным оценкам, это дает возможность сократить затраты от простоя самолета из-за непредвиденной поломки на ~34%. Построенная модель выявляет поломки с точностью ~90% (на 9 правильно предсказанных поломок приходится 1 ложная тревога).

3.3.4 Предсказательная аналитика для приложений ПТО. Обнаружение аномалий

Новые типы источников данных, новые требования прикладных областей, новые технические возможности сбора и обработки данных требуют новых математических моделей, новых постановок задач математической статистики и методов их решения, разработки новых методов машинного обучения для создания приложений ПТО. Так, традиционные математические модели предполагают, что данные математически описываются с помощью независимых и одинаково распределенных (н.о.р.) многомерных наблюдений или с помощью многомерных стохастических процессов в непрерывном времени. Однако, в настоящее время имеется острая потребность в анализе данных, порождаемых различными сенсорными сетями, распределенными структурами (данные на графе). Типичным примером такой многокомпонентной стохастической системы может служить социальная сеть. Таким образом, возникли новые реальные объекты, анализ которых требует новых методов моделирования, обработки данных и машинного обучения. Существующие методы основаны зачастую на инженерных подходах, эвристиках и т.п. Иными словами, эти решения создаются *ad hoc* и, как следствие, не являются оптимальными и не дают возможности точно оценить, насколько далеки они от оптимальности; они не гарантируют надежность; они не дают четкого понимания границ, в которой данные методы могут эффективно работать.

Соответственно, к числу математических задач, которые

надо решать при разработке моделей для современных приложений ПТО, относится анализ больших массивов информации, снижение размерности данных и моделирование многообразий, кластеризация, классификация, обнаружение аномалий и разладок, консолидация разноточных мультимодальных данных и распознавание образов, обработка нестандартных типов данных, таких как последовательности графов и потоки событий. Это в свою очередь требует новых вероятностных методов для выработки эффективных стратегий принятия решений и анализа характеристик этих стратегий. Для разработки этих методов требуется использовать различные методы машинного обучения и их модификации (Рис. 3.13)

- методы восстановления многообразий, аппроксимирующих носитель данных;
- подходы к обучению с привилегированной информацией, включая одноклассовую классификацию;
- методы несбалансированной классификации;
- методы непараметрического оценивания доверительных интервалов для предиктивных моделей, и т.д.

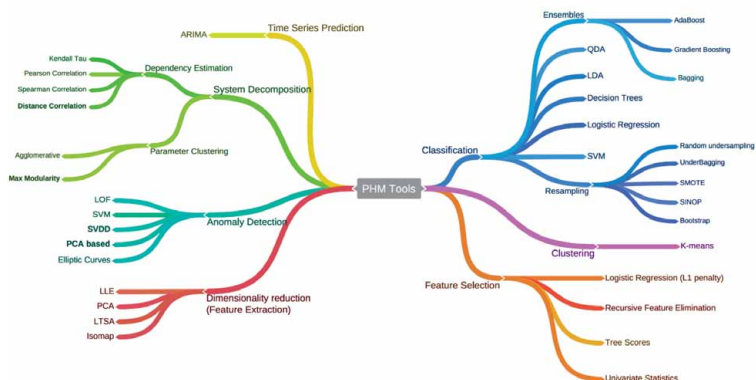


Рисунок 3.13–Схема деления методов машинного обучения для создания моделей предиктивной аналитики в современных приложениях ПТО

Источник: Составлено автором на основе материалов совместной с П. Ерофеевым презентации

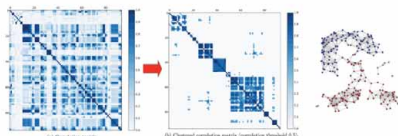
Соответствующие технологии и алгоритмы и их оптимальные комбинации позволяют осуществлять принятие решений в реальном времени, обеспечивая динамическую адаптацию к неопределенностям во вновь поступающих данных.

3.3.4.1 Методология построения предиктивных моделей для приложений ПТО

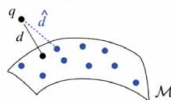
Опишем на примере решения задачи прогнозирования выхода из строя вспомогательной силовой установки (ВСУ, см. раздел 3.3.3) общую методологию построения предиктивных моделей для приложений ПТО. Основная идея, которая стоит за данной методологией, состоит в следующем очевидном наблюдении: неожиданно происходящие события могут повлиять на поток информации с датчиков и привести к изменению определенных паттернов в данных. Например, оборудование (скажем, турбина) обычно входит в предаварийное состояние из-за появления каких-то мелких дефектов, таких как трещины или протечки. Эти дефекты со временем усугубляются и приводят к критическим сбоям, вплоть до полного отказа оборудования.

В рамках решения задачи предсказания поломок ВСУ, и других подобных задач, может быть применена следующая методология (Рис. 3.14):

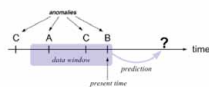
Шаги 1-2. Выделение подсистем: Выявление групп зависимых параметров, соответствующих разным подсистемам



Шаг 3. Обнаружение аномалий: Детектирование аномалий на основе моделирования многообразия для выделенных подсистем параметров



Шаги 4-5. Соотнесение событий: Стат. методы для выделения подпоследовательностей аномалий, предшествующих поломкам (и нигде больше не появляющихся)



Шаг 6. Валидация: Применение правила, «обученного» на одних объектах, к данным об аналогичных объектах



Рисунок 3.14– Прогнозирование поломок: основные этапы
Источник: Составлено автором

Шаг 1. Фильтрация и нормализация данных.

Шаг 2. Декомпозиция системы: разбиение всех наблюдаемых параметров на группы, где параметры внутри группы сильнее всего зависимы (например, коррелированы), но между собой группы параметров зависимы незначительно. Обычно, такая декомпозиция соответствует физическому разбиению инженерной системы на слабо зависимые части, соответствующие конкретным узлам инженерной системы.

Шаг 3. Детектирование и классификация различных типов аномалий в комбинациях наблюдаемых физических параметров внутри каждой из выделенных групп зависимых параметров. Появление аномалии внутри группы зависимых параметров свидетельствует об изменении зависимостей между этими параметрами, что в свою очередь означает изменение режима работы соответствующей части инженерной системы, описываемой этой группой параметров, и может быть предвестником будущей поломки всей системы.

Шаг 4. Ассоциирование наблюдаемых аномалий с событиями последующих (в будущих полетах) поломок ВСУ. На этом этапе поток телеметрии представляется потоком событий (аномалий), выявленных в каждой из групп изначально зависимых параметров. Гипотеза состоит в том, что появление некоторых комбинаций аномалий в части из выделенных групп зависимых параметров (изменение режимов работы некоторых конкретных узлов инженерной системы) приводит к поломке. Эта гипотеза и проверяется на исторических данных, в которых должны присутствовать примеры поломок, которые необходимо прогнозировать. Для проверки гипотезы можно применять как методы несбалансированной классификации, так и переборные алгоритмы, цель которых – выделить приводящие к поломкам в будущем подмножества событий (аномалий в рассматриваемом случае).

Шаг 5. Строится финальная модель для прогнозирования поломок – композитная, состоящая из нескольких решающих правил:

- a. для каждой группы параметров, выделенных на шаге 2, применяется выбранный набор методов обнаружения аномалий;
- b. для полученного множества аномалий проверяется, есть ли среди обнаруженных аномалий такая последовательность аномалий, которая (согласно оценке по историческим данным) с большой вероятностью предшествует поломкам;
- c. отметим, что полученная модель позволяет в каждом конкретном случае объяснить «причину» того или иного прогноза, в частности, выделить входные параметры, наиболее на него повлиявшие. Действительно, при прогнозе поломки срабатывает определенная комбинация аномалий, соответствующих конкретным группам параметров. Их, в свою очередь, можно связать с конкретными узлами инженерной системы. Следовательно, возможна интерпретация прогноза модели.

Шаг 6. Проверка найденных решающих правил на основе методики перекрестной проверки:

- a. имеющаяся историческая выборка наблюдений делится в разрезе различных самолетов, то есть различные части выборки соответствуют данным, полученным с разных самолетов;
- b. предиктивная модель обучается по всем данным кроме данных, соответствующих одному из самолетов;
- c. оценивается точность прогноза обученной модели на данных, которые не использовались для обучения модели;
- d. пункты b и c повторяются количество раз, равное количеству разных самолетов, данные с которых были собраны;
- e. значения метрик точности прогноза моделей агрегируются (например, усредняются).

Данная методология является довольно универсальной, и может быть применена к различным инженерным техническим системам.

3.3.4.2 Обнаружение аномалий

Как следует из описанной в подразделе 3.3.4.1 методологии построения предиктивных моделей для приложений ПТО, обнаружение аномалий является одним из важнейших инструментов для решения такого рода задач.

Задача обнаружения аномалий состоит в обнаружении определенных отличий тестовых данных от тех, которые были доступны на этапе обучения. На Рис. 3.15 приведен “жизненный” пример аномалии: Mrs. Hadlum родила через 349 дней после того, как Mr. Hadlum ушел служить в армию; как известно, средний срок беременности составляет 280 дней (40 недель), соответственно, статистически 349 дней – выброс в наблюдениях. Согласно определению известного статистика Howkins (1980 г.): выброс (аномалия) – это наблюдение, которое настолько сильно отличается от остальных наблюдений, что возникает подозрение, что это наблюдение было порождено другими механизмами.

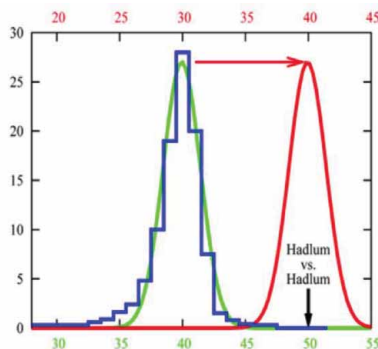


Рисунок 3.15– *Hadlum против Hadlum*

Источник: [3.38]

В реальных задачах определение аномалии/аномальности сильно зависит от контекста. Например, на Рис. 3.16 приведен пример аномалий типа “выбросы”: основная масса двумерных наблюдений группируется в виде двух двумерных облаков точек, при этом имеется одно наблюдение (изображено красным цветом) – аномалия относительно основной совокупности данных.

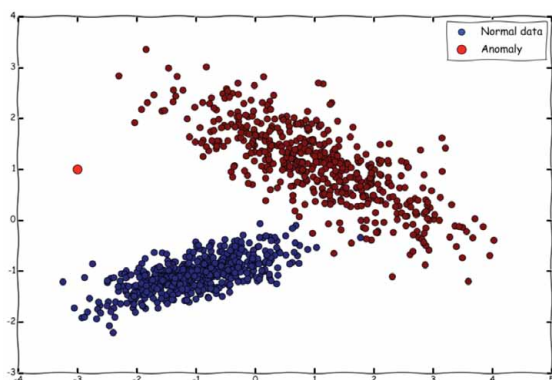


Рисунок 3.16– Типы аномалий: выбросы

Источник: Составлено автором на основе материалов совместной с П. Ерофеевым презентации

На Рис. 3.17 приведен пример аномалий типа «разладка в сигнале»: основная часть сигнала имеет регулярную структуру, но имеется промежуток времени, в течении которого поведение сигнала сильно отличается от типичного; внутри этого промежутка времени наблюдения не являются аномальными относительно друг друга; при обнаружении такого типа аномалий требуется учитывать зависимость наблюдений от времени.

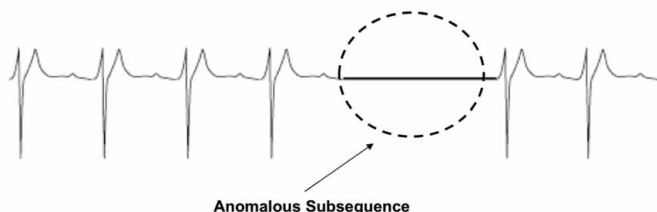


Рисунок 3.17– Типы аномалий: разладка в сигнале

Источник: составлено автором на основе материалов [3.39]

Для того, чтобы оценить точность метода обнаружения аномалий необходимо либо использовать ручную размеченную выборку с метками аномалия/нормальное наблюдение, либо же оценивать точность метода за счет оценки качества решения последующей задачи. Действительно, методы обнаружения аномалий редко когда используются

просто так, обычно они требуются для того, чтобы, например, предобработать выборку данных для построения предиктивной модели. Соответственно, предполагается, что после очистки выборки предиктивная модель сможет обеспечить более высокую точность прогноза, которую можно измерить, применяя методы кросс-проверки.

Практическая значимость и трудность задачи обнаружения аномалий привели к тому, что было разработано большое количество различных методов решения. Эти методы обычно применяются для анализа таких данных, в которых имеется большое число “нормальных” ситуаций/условий (положительных примеров), а данных для описания аномалий (отрицательных примеров) – недостаточно или такие данные вовсе отсутствуют.

Обнаружение аномалий получило распространение в тех прикладных областях, в которых имеются сложные многокомпонентные системы, порождающие большие массивы данных. Например, в задачах обнаружения опухолей в маммограммах [3.40] и других задачах медицинской диагностики [3.41, 3.42], при обнаружении ошибок и поломок в сложных промышленных системах [3.43], мониторинге состояния конструкций [3.44], обнаружении внедрений в электронные системы безопасности для мошенничества с кредитными карточками или мобильными телефонами [3.45, 3.46]. Другой пример – современные программно-интенсивные системы, которые достигли больших размеров и поэтому принципиально важны процедуры обнаружения отказов для предотвращения дорогостоящих простоев. Многообещающим направлением в создании таких схем является использование легкодоступных измерений характеристик системы, таких как среднее число обработанных требований и размер очереди в единицу времени, которые, вместе с тем, обладают рядом свойств, усложняющих решение задачи построения эффективных моделей обнаружений аномалий: имеются в виду сильная корреляция (т.н. длинная память) и квазипериодические сезонные тренды.

Итак, сложность современных многокомпонентных систем в том, что представление о соотношениях между

различными компонентами системы получить зачастую крайне затруднительно. Как следствие, существует огромное число различных аномальных режимов, причем некоторые могут быть неизвестны заранее, что делает стандартные многоклассовые классификационные схемы неподходящими для этих приложений. Решение проблемы возможно за счет использования методов обнаружения аномалий, в которых модель обучается тому, что такое нормальное состояние, на большой выборке положительных примеров (то есть данных, соответствующих нормальному поведению системы). Тестовые паттерны проверяются на аномальность путем сравнения с моделью нормальности, степень их аномальности характеризуется соответствующим показателем. Этот показатель, который может как иметь, так и не иметь вероятностный смысл, сравнивается с порогом принятия решений, и тестовые данные считаются аномальными, если значение показателя оказывается больше значения порога, выбираемого исходя из допустимого уровня ложных тревог.

В данном разделе мы приведем краткий обзор некоторых основных подходов к обнаружению аномалий в многомерных данных, в первую очередь в выборках независимых и одинаково распределенных наблюдений. Большое разнообразие методов обнаружения аномалий обусловлено разнообразием практических ситуаций, в которых понятие аномальности будет зависеть от типа приложения, свойств и структуры данных, и т.п.

Обнаружение аномалий на основе вероятностных моделей. Вероятностные подходы к обнаружению аномалий основаны на оценке генеративной плотности вероятностного распределения данных. Результирующее распределение далее может быть «урезано» для определения границ нормальности в пространстве данных и тестирования, была ли порождена тестовая выборка рассматриваемым распределением. Предполагается, что обучающая выборка порождена некоторым вероятностным распределением, которое можно оценить по данным. Соответствующая оценка обычно и представляет собой некоторую модель нормальности. В свою очередь, если есть соответствующие требования, то порог

для принятия решения о том, является ли наблюдение аномальным, можно придать и вероятностную интерпретацию.

В рамках этого направления предлагаемые методы обычно различаются степенью их сложности. Простейшие статистики для обнаружения аномалий основаны на проверке статистических гипотез, которые зачастую эквивалентны известным из литературы по статистике [3.47] тестам для обнаружения выбросов. Эти подходы позволяют определить, порождено ли наблюдение тем же распределением, что и нормальные данные. Большинство из этих тестов основаны на гипотезе нормальности данных, см. [3.48] для примера, и работают только для одномерных непрерывных данных, хотя варианты этих тестов были адаптированы и на случай многомерных данных, см., например, [3.49, 3.50]. Далее, мы не будем рассматривать классические одномерные статистики обнаружения выбросов в данных, а сосредоточимся на современных методах, которые позволяют работать и со сложными, многомерными распределениями данных.

Задача оценки распределения, породившего многомерные данные, хорошо изучена, см. [3.50, 3.51]. Соответствующие методы бывают как параметрические, так и непараметрические. В случае параметрических методов используются ограниченные параметрические модели данных, применение которых на практике зачастую приводит к появлению значительного смещения в случае, если реальная модель рассматриваемому параметрическому классу не принадлежит. Непараметрические модели обычно гораздо более гибкие, но при этом требуют для своего оценивания выборки значительных размеров. Одной из наиболее часто встречающихся на практике параметрических моделей является модель смеси гауссовских распределений [3.52–3.54], в непараметрическом случае обычно используется ядерная оценка плотности распределения [3.52–3.55].

Методы обнаружения аномалий на основе мер близости. Методы обнаружения аномалий на основе метрики, включая кластеризацию или методы на основе ближайших соседей, представляют собой другой вариант подхода, с помощью которого можно решить задачу, эквивалентную оценке плотности

распределения данных. Соответствующие методы основаны на специальных метриках, которые позволяют оценивать близость между наблюдениями. Подход на основе k -ближайших соседей основан на предположении, что у нормальных наблюдений соседи принадлежат “нормальной” выборке данных, в то время как аномальные точки расположены далеко от них [3.56]. Наблюдение считается выбросом/аномалией, если оно расположено далеко от его соседей. Обычно используется евклидова метрика, реже – расстояние Махаланобиса.

Чтобы подсчитать, насколько близки два наблюдения, на практике используются обычно следующие подходы [3.57]: методы на основе расстояния, такие, как расстояние до k -го ближайшего соседа [3.56], локальные методы на основе плотности, в которых используется расстояние до среднего из k -ближайших соседей [3.56]. Многие из подобных методов плохо работают в случае многомерных данных.

Подход на основе плотности распределения для обнаружения аномалий был предложен в [3.58]. В этом подходе считается показатель Local Outlier Factor (LOF) для каждого нового наблюдения, который основан на отношении локальной плотности области вокруг точки и локальной плотности ее соседей. Размер окрестности точки определяется областью, содержащей заданное пользователем минимальное число точек. Отметим, что LOF ранжирует точки по степени их аномальности, но при этом может пропустить потенциальные выбросы, чья плотность достаточно велика и близка к плотности соседей.

Подходы к обнаружению аномалий на основе кластеризации основаны на идее того, что «нормальный» класс можно описать небольшим числом прототипов. Соответственно, для оценивания степени аномальности используется минимальное расстояние от тестового наблюдения до ближайшего прототипа. Одним из наиболее популярных алгоритмов является алгоритм кластеризации k -means, см. [3.59, 3.60].

Обнаружение аномалий на основе прогнозирования. В рамках подхода к обнаружению аномалий на основе прогнозирования используются методы регрессионного анализа и классификации, с помощью которых моделируется выборка

данных. Для тестового наблюдения считается ошибка прогноза, определяемая как расстояние между тестовым вектором и выходом системы, и по этой ошибке подсчитывается показатель аномальности наблюдения. Например, в [3.61] для этого используются нейронные сети (многослойный перцептрон). В [3.62, 3.63] рассмотрен поход к обнаружению аномалий для больших многомерных данных на основе репликативных нейронных сетей. Репликативные нейронные сети представляют собой многослойный перцептрон специального вида, который обучается для того, чтобы наилучшим образом воспроизводить на выходе поданные на вход вектора наблюдений. При этом, так как размерность центрального слоя нейронов сети значительно меньше размерности векторов наблюдений, происходит сжатие информации и снижение размерности данных. Наблюдение считается аномальным, если ошибка его восстановления в рамках такой модели велика.

Другой тип алгоритмов для обнаружения аномалий (иногда еще называемых спектральными методами, см. [3.52]) состоит в построении таких комбинаций исходных признаков, которые наилучшим образом описывают степень изменчивости (вариабельность) исходных данных. Предполагается, что проекция данных или их вложение в подпространство низкой размерности позволят отличить «нормальные» данные от аномальных. Метод Главных Компонент является стандартной техникой для проекции данных в пространство низкой размерности и позволяет выделять такой ортогональный набор направлений, вдоль которых изменчивость данных максимальна. Эту технику можно использовать для построения модели распределения обучающих данных в преобразованном пространстве [3.64]. Методы обнаружения аномалий на основе анализа главных компонент рассмотрены в [3.65, 3.66]. В [3.67, 3.68] рассмотрено обобщение метода главных компонент на нелинейный случай за счет использования нелинейного преобразования данных с помощью специального ядерного отображения (ядерные главные компоненты).

Обнаружение аномалий на основе описания границы носителя данных. Еще один класс методов обнаружения аномалий использует описание границы носителя нормальных данных. Такого рода методы обычно нечувствительны к плотности нормального класса, так как они описывают только границу соответствующей области, а не плотность расположения наблюдений в ней. Принадлежность неизвестному классу затем определяется расположением наблюдения по отношению к границе. Как и в случае двухклассового SVM, SVM для обнаружения аномалий (одноклассовый SVM) определяет положение границы аномальной области используя только наблюдения, близкие к границе (опорные вектора). Остальные наблюдения из выборки в определении решающего правила не участвуют, см. [3.69 – 3.71]. Построение решающего правила основано на решении задачи оптимизации, в которой в пространстве признаков, соответствующем некоторому ядру, строится гиперплоскость, максимально отделяющая начало координат от выборки данных.

Отметим, что в случае ядерных методов крайне важно уметь учитывать локальные особенности геометрической структуры данных (характерные размеры областей сгущения точек в подпространстве нормальных значений характеристик поведения системы) при настройке ширины ядер, что существующие алгоритмы детектирования аномалий делать не позволяют. Поэтому в [3.72] предложен метод учета локальных особенностей геометрической структуры данных при настройке ширины ядер в задаче детектирования аномалий с помощью одноклассовой классификации на основе машины опорных векторов.

Обнаружение аномалий (разладок) во временных рядах. Стандартным подходом к обнаружению разладок и аномалий во временных рядах являются оптимальные статистики типа статистики кумулятивных сумм, Ширяева-Робертса и т.п., которые предполагают известным распределение данных, порождаемых источником, как в случае нормального, так и в случае аномального режимов работы [3.73]. Однако, на практике данные предположения обычно неприемлемы.

Разработка эффективной системы ПТО требует разработки эффективных методов обнаружения аномалий во временных рядах. При этом методы обнаружения аномалий должны быть:

- непараметрическими, то есть основываться на минимальных предположениях о механизме генерации данных, порождаемых системой как в нормальном состоянии, так и тем более – в аномальном состоянии;
- вычислительно эффективными, позволять обрабатывать потоки многомерных данных в режиме реального времени;
- обеспечивать малое число ложных тревог и высокий уровень покрытия событий, выявление которых представляет интерес;
- эффективно учитывать нестационарность данных, наличие квазипериодических циклов (особенно это характерно для масштабных информационных систем, предназначенных для обслуживания большого числа пользователей), компонент с длинной памятью;
- эффективно учитывать наличие признаков/дополнительной информации об анализируемом объекте, получение которых затратно в смысле ресурсов и по этой причине возможно только на этапе обучения интеллектуальной системы ПТО.

В [3.74, 3.75] были разработаны методы, которые, за счет использования конформных мартингалов, позволяют непараметрическим образом оценивать вероятностный показатель, характеризующий достоверность решения об аномальности рассматриваемого наблюдения и не используют существенных предположений о распределении данных до и после разладки.

В серии работ [3.76–3.78] были разработаны непараметрические методы обнаружения аномалий, разработана методология обнаружения резких изменений во временных рядах в присутствии квазипериодических трендов и сильной зависимости, с акцентом на обнаружении сбоев и отказов в компьютерных системах.

3.3.5 Мониторинг дорожных условий. Одноклассовая классификация

В данном разделе будет описана задача обработки данных, поступающих с системы датчиков автоматических дорожных метеорологических станций (АДМС), считывающих информацию о погодных условиях [3.79], приведена постановка задачи одноклассовой классификации и показано, как её решение – модель для обнаружения аномалий – может быть адаптировано и использовано для обработки данных с АДМС.

3.3.5.1 Мониторинг дорожных условий (совместно с компанией Минимакс-94)⁴²

Развитие автотранспортной инфраструктуры и обеспечение безопасности дорожного движения требует решения широкого круга проблем. Часть из них находится в области поведения участников дорожного движения, другая часть имеет технический характер и связана с обеспечением развития и функционирования современной автомобильной транспортной системы. В условиях России требования по нормальному функционированию дорожной системы в зимний период приводят к необходимости удаления снега и борьбы с обледенением дорог.

По данным гидрометеослужбы, длительность зимнего периода в Московском регионе составляет 166 дней, при этом, в среднем за этот период бывает около 10 дней с обледенением покрытия, около 50 снегопадов и 50–60 циклов перехода температуры через 0 °С. Сильный снегопад и гололедные явления способны привести к значительному снижению пропускной способности автомагистралей. При гололеде и снежном накате существенно увеличивается вероятность возникновения дорожно-транспортных происшествий. Одновременно это приводит к снижению скорости движе-

⁴² В данном разделе приводятся результаты, полученные в рамках проекта “Интеллектуальная информационная система прогнозирования параметров и оценки состояния дорожного покрытия автомагистралей на основе искусственных нейронных сетей для обеспечения безопасности дорожного движения”, поддержанного МОН РФ, №. 14.606.21.0004, уникальный идентификатор – RFMEFI60617X0004.

ния транспортных средств и пропускной способности дорог с соответствующим увеличением себестоимости перевозок. В общей сложности, доля затрат на борьбу с зимней скользкостью составляет в настоящее время около 40% от общих затрат на зимнее содержание дорог (общедоступные данные по г. Москва).

Обледенение в зимний период может служить причиной дорожно-транспортных происшествий [3.80], и возможность заранее предсказать появление льда и другие неблагоприятные явления позволяет существенно сэкономить на обслуживании дорог.

Действительно, зарубежный опыт по содержанию автомобильных дорог в зимнее время показывает, что наиболее эффективна предварительная обработка дороги перед образованием гололеда или обработка во время появления льда и выпадения снега для предотвращения возникновения скользкости. Такая технология отличается от традиционной технологии «по факту» (после образования льда) тем, что предотвращает образование корки льда или снежного наката. Результаты отечественных исследований [3.81, 3.82] показали, что применение технологии, упреждающей образование скользкости, уменьшает количество используемых химических реагентов и снижает общие затраты на содержание дорог. Отметим, что в настоящее время в США, Канаде и ряде стран Западной Европы разрабатываются и функционируют системы прогнозирования состояния поверхности дороги, основанные на данных автоматических метеорологических станций [3.83–3.85].

Таким образом, создание условий безопасного движения транспортных средств требует заблаговременных и точных прогнозов ухудшения состояния дорожного покрытия. Для предсказания подобных ситуаций можно использовать специальные алгоритмы прогноза погоды, ориентированные на автомагистрали [3.86], однако такие методы сильно зависят от расположения метеорологических станций.

Другой подход к построению моделей, методов и алгоритмов прогнозирования возможен при наличии соответствующих данных о состоянии дорожного покрытия

за продолжительный временной период, которые получены от датчиков, находящихся в непосредственной близости от дороги, и установленных на т.н. автоматические дорожные метеорологические станции, считывающие информацию о погодных условиях [3.79]. Такие объединенные системы датчиков можно рассматривать как одно из практических приложений интернета вещей (IoT).

Во многом эффективность предсказания параметров дорожного покрытия зависит от источника данных. При этом могут использоваться показания с метеорологических станций, как это делается в работе [3.86]. Однако приемлемое качество определения погодных условий может быть в ряде случаев получено и при использовании более дешевых датчиков (это могут быть, например, простейшие датчики, измеряющие единственный параметр, они рассмотрены в работе [3.87]), при условии их установки непосредственно на дорогах. Так же для обнаружения обледенения можно использовать наблюдение при помощи видеокамер [3.88] и лазерных радаров [3.89].

Для обеспечения эффективного мониторинга дорожных условий компанией Минимакс-94 была разработана и внедрена сеть из более чем 1000 АДМС, покрывающая основные федеральные трассы Российской Федерации. Общий вид блока датчиков станции АДМС, и ее установка на автодороге показаны на Рис. 3.18. Каждая АДМС агрегирует и отправляет в систему через интервалы приблизительно в 30 минут значения температуры и влажности воздуха, направление, скорость и величину порывов ветра, и т.д.

Однако классические методы и модели прогнозирования не позволяют создать интеллектуальные системы, устойчивые к шумовым сигналам и работающие в режиме онлайн. Это обуславливает актуальность задачи разработки интеллектуальной информационной системы прогнозирования параметров и оценки состояния дорожного покрытия для обеспечения безопасности движения на основе современных методов машинного обучения.



Рисунок 3.18–Автоматическая дорожная метеостанция (АДМС)

Источник: Проект с компанией Минимакс-94

При решении указанной задачи важно разработать алгоритмы машинного обучения для детектирования и очистки данных от аномалий. Данные, получаемые от АДМС, содержат в себе значительное число аномалий, вызванных возможной неисправностью датчиков, ошибками при передаче данных на сервер, нарушением правил установки и эксплуатации, внешними физическими воздействиями и прочими факторами. Полученные некорректные данные крайне негативно влияют на качество прогноза и, как следствие, на качество работы дорожных служб.

В дальнейшем под термином аномалия мы будем иметь в виду событие или наблюдение, которое не соответствует ожидаемому шаблону или сильно отличается от остальных элементов в наборе данных. Очистка данных от аномалий может привести к улучшению качества содержания дорог за счет предоставления дорожным службам более точной информации о погодно-климатических условиях и более точных прогнозов, а также позволит автоматически обнаруживать неисправности датчиков и высылать предупреждения об их поломках операторам АДМС.

3.3.5.2 Постановка задачи одноклассовой классификации

Перспективным подходом для построения моделей обнаружения аномалий во временных рядах для выявления неисправных датчиков являются методы на основе одноклассовой классификации [3.90], например, одноклассовая машина опорных векторов (One Class SVM) [3.70], или описание носителя данных на основе опорных векторов (Support Vector Data Description, SVDD) [3.71]. Эти методы позволяют выделить из исторических данных паттерны, соответствующие нормальному режиму функционирования системы, и затем обнаруживать вышедшие из строя сенсоры (порождающие аномальные данные) путем оценки схожести наблюдаемых данных на выделенные паттерны.

Обнаружение аномалий на основе одноклассовой классификации состоит в том, чтобы по неразмеченной выборке данных (м.б. содержащей небольшую долю аномальных наблюдений)

$$S_m = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m\}, \mathbf{x}_i \in \mathbb{R}^p$$

построить решающее правило

$$f: \mathbf{x} \rightarrow \{-1, +1\},$$

такое, что для любого нового наблюдения

$$\mathbf{x} = \begin{cases} \text{normal, если } f(\mathbf{x}) = +1, \\ \text{anomaly, если } f(\mathbf{x}) = -1. \end{cases}$$

Данную задачу можно описать геометрически: будем считать, что «нормальные» элементы выборки группируются в некоторой компактной области, границу которой легко описать; наблюдения, которые находятся за пределами этой области, считаются аномальными. На Рис. 3.19 изображен пример, иллюстрирующий данную идею.

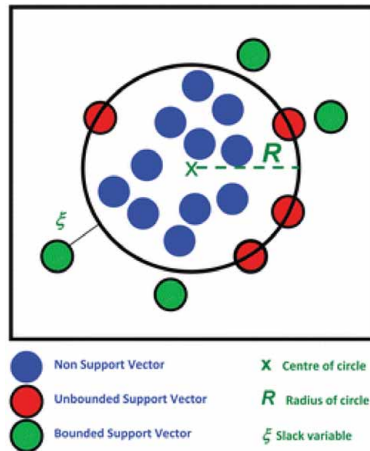


Рисунок 3.19– Иллюстрация идеи описания носителя распределения, породившего данные, на основе машины опорных векторов: синим изображены «нормальные» элементы выборки, зеленым – «аномальные», а красным – опорные векторы, определяющие положение разделяющей поверхности.

Источник: [3.91]

Математически это можно описать следующим образом:

$$\begin{aligned}
 R + \frac{1}{mv} \sum_{i=1}^m \xi_i &\rightarrow \min_{R, a, \xi}, \\
 \text{s. t. } \|\phi(x_i) - a\|_2^2 &\leq R + \xi_i, \\
 \xi_i &\geq 0, \\
 R &\geq 0.
 \end{aligned}$$

Таким образом, мы хотим найти сферу (положение её центра и радиус), внутри которой находится «большая» часть выборки, так, чтобы, с одной стороны, радиус сферы был как можно меньше, а с другой – среднее расстояние (задаваемое величинами ξ_i) от точек, находящихся вне сферы, до её поверхности, было как можно меньше. Здесь величина параметра v играет роль коэффициента регуляризации (легко показать, что значение этого параметра ограничивает сверху долю аномальных наблюдений, которые могут содержаться в выборке), $\phi(x_i)$ – признаки i -го объекта.

Можно доказать, что итоговое уравнение границы определяется через решение задачи квадратичного программирования [3.71], при этом уравнение границы будет задаваться через величину ядерной функции, задающей похожесть элементов выборки друг на друга через скалярное произведение в соответствующем признаковом пространстве (задаваемом отображением $\phi(\cdot)$):

$$K(x, x') = \phi(x) \cdot \phi(x').$$

В простейшем случае признаки i -го объекта $\phi(x_i) = x_i$; также их можно задать, как исходя из структуры задачи, какой-то физической интерпретации данных, так и автоматически, через ядерную функцию: в [3.92] показано, что ядерным функциям (например, гауссовской ядерной функции) соответствуют пространства (которые могут быть и бесконечномерными) с определенным образом заданными векторами признаков. При этом в исходном пространстве признаков разделяющая граница, разделяющая пространство признаков на аномальную и нормальную части, будет неквадратичной (несферической), в отличие от примера, изображенного на Рис. 3.19, который соответствует использованию исходного признакового описания и соответствующего ему линейного ядра), см. пример на Рис. 3.20.

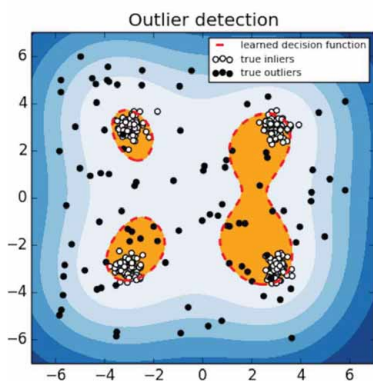


Рисунок 3.20– Пример построения границы, описывающей носитель выборки, на основе одноклассовой классификации с гауссовской ядерной функцией.

Источник: [3.93]

В контексте рассматриваемого приложения в качестве наблюдений x используются текущее и прошлые известные значения временного ряда (за последние три часа). Вектор признаков $\phi(x)$, в свою очередь, может содержать какие-то нелинейные функционалы от значений x и дополнительные признаки. Например, мы использовали календарные признаки включая день d года и время t дня. Для того, чтобы учесть сезонность, мы использовали «тригонометрические» признаки $\sin\left(\frac{2\pi d}{365}\right)$, $\cos\left(\frac{2\pi d}{365}\right)$, $\sin\left(\frac{2\pi t}{24}\right)$, $\cos\left(\frac{2\pi t}{24}\right)$.

3.3.5.3 Описание сенсорных данных, собираемых с АДМС

С АДМС, установленных в различных регионах РФ, собираются данные следующих видов: температура и влажность воздуха, направление, скорость и порывы ветра, атмосферное давление, температура точки росы, тип и интенсивность осадков, температура поверхности дороги, температура в глубине дорожной одежды (4-7 см), количество отложений на поверхности дороги, наличие реагентов на поверхности дороги, и т.д.

На Рис. 3.21 приведен пример данных о температуре поверхности дороги. Запись сенсорных данных производится в нерегулярные моменты времени. По этой причине была произведена предобработка данных: произведена линейная интерполяция имеющихся наблюдений и получены регулярные наблюдения, разделенные 30-минутными интервалами.

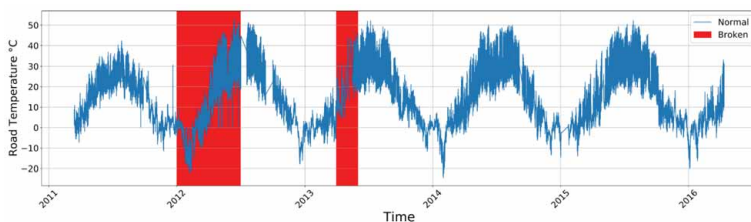


Рисунок 3.21– Зависимость температуры поверхности дороги от времени

Источник: Проект с компанией Минимакс-94

3.3.5.4 Одноклассовая классификация с привилегированной информацией

Итак, как описано в разделе 3.3.5.2, задача обнаружения аномалий во временном ряду может быть решена с помощью одноклассовой классификации: по известным значениям временного ряда $x(s), s \leq t$ до текущего момента времени t включительно, строятся различные признаки, которые потом используются в качестве входного вектора в алгоритме описания носителя данных на основе опорных векторов для того, чтобы детектировать аномалии в данных в некоторой окрестности $[t - \Delta_1, t]$ текущего момента времени t .

Очевидно, что знание о поведении временного ряда после момента времени t позволило бы более точно детектировать наличие аномалии на отрезке $[t - \Delta_1, t]$. Грубо говоря, наиболее значимые “симптомы” выхода из строя сенсора можно выявить в данных, снятых с датчиков непосредственно после поломки. Однако, такого рода информация (привилегированная информация) известна только на этапе обучения модели для обнаружения аномалий и не может быть получена на этапе применения модели в режиме реального времени («будущее» не известно), см. Рис. 3.22.

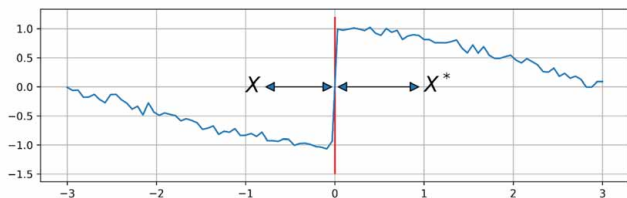


Рисунок 3.22– Признаки x , подсчитанные по значениям временного ряда, соответствующим периоду времени $[t - \Delta_1, t]$, и привилегированные признаки x^* , подсчитанные по значениям временного ряда, соответствующим периоду времени $[t, t + \Delta_2]$, и доступные только на этапе обучения модели

Источник: [3.94]

Другой пример привилегированной информации – признаки, получение которых затратно по времени/стоимости измерений. Например, в случае данных о вредоносном ПО

стандартные признаки \mathbf{x} будут представлять собой различные простые статистики, подсчитанные по шестнадцатеричному представлению содержимого файла вредоносного ПО, а привилегированные признаки \mathbf{x}^* будут содержать такую информацию, как число вызовов функций, число строк, и т.п., которую можно получить только вычислительно трудоемким способом за счет дизассемблирования.

В рассматриваемом случае в качестве таких привилегированных признаков могут выступать прогнозы температуры на поверхности дороги, полученные с помощью затратной для вычисления физической модели, основанной на расчете потока тепла через поверхность дороги, см. описание модели METRo в разделе 3.3.5.5. Вычислительная трудоемкость физической модели не позволяет рассчитывать в режиме реального времени прогноз, который мог бы использоваться на этапе применения модели для обнаружения аномалий в качестве входного признака.

Таким образом, возникает постановка задачи одноклассовой классификации с привилегированной информацией.

На этапе обучения вместо векторов признаков \mathbf{x}_i известны пары векторов $(\mathbf{x}_i, \mathbf{x}_i^*)$, где вектор признаков \mathbf{x}_i^* содержит привилегированную информацию. Необходимо построить модель для обнаружения аномалий по расширенной обучающей выборке

$$S_m^* = \{(\mathbf{x}_1, \mathbf{x}_1^*), \dots, (\mathbf{x}_m, \mathbf{x}_m^*)\}, \mathbf{x}_i \in \mathbb{R}^p, \mathbf{x}_i^* \in \mathbb{R}^{p^*}.$$

При этом на этапе применения модели в качестве входных признаков возможно использовать только признаки \mathbf{x} .

В работах автора [3.94, 3.95] предложена модификация классического алгоритма обнаружения аномалий на основе одноклассовой классификации (описание носителя данных на основе опорных векторов, см. раздел 3.3.5.3), которая позволяет решить поставленную задачу. Основная идея состоит в том, чтобы за счет учета привилегированных признаков уточнить значения переменных отступа ξ_i , которые определяют положение разделяющей поверхности. Для этого делается предположение, что

$$\xi_i \approx w^* \cdot \phi^*(\mathbf{x}_i^*) + b^*$$

Далее, модель для обнаружения аномалий (задающая положение разделяющей поверхности) строится как решение оптимизационной задачи, аналогичной оптимизационной задаче из раздела 3.3.5.3.

3.3.5.5 Модель METRo

Данные, полученные с датчиков АДМС, можно использовать для построения моделей и систем прогнозирования состояния дороги. Одной из наиболее распространенных моделей является модель METRo [3.84]. Данная модель рассчитывает поток тепла через поверхность дороги, представляя его в виде суммы:

$$R = (1 - \alpha)S + \varepsilon I - \varepsilon \sigma T^4 - H - L_a E \pm L_f P + A,$$

где $(1 - \alpha)S$ – солнечное излучение, εI – поглощенное инфракрасное излучение, $\varepsilon \sigma T^4$ – излучаемая энергия, H – турбулентный тепловой поток, $L_a E$ – латентный тепловой поток, $\pm L_f P$ – изменение теплоты за счет фазового перехода, A – антропогенные источники.

Модель METRo позволяет предсказывать состояние дорожного покрытия, включая вероятность обледенения. На данный момент ее эффективно протестировали в Чехии [3.96], Канаде [3.84], США [3.80]. Во всех случаях использование этой модели позволяло получить приемлемое качество прогноза.

Важно отметить, что модель METRo на практике требует знания величины потока тепла, связанное не только с погодными условиями, но и с деятельностью человека. К сожалению, его довольно сложно моделировать [3.97]. Другой проблемой можно назвать детерминированность прогнозов – нет возможности оценить доверительный интервал при прогнозировании. Эту проблема можно пытаться решить при помощи методов Монте-Карло, что, однако требует многократного решения уравнения с различными начальными условиями [3.98, 3.99] и значительных вычислительных ресурсов.

Описанные проблемы частично можно решить, используя методы машинного обучения. Даже простейшие методы

прогнозирования, такие как линейная регрессия, позволяют получить приемлемый прогноз точности состояния дорожного покрытия [3.100]. Методы машинного обучения позволяют как непосредственно строить прогноз на основе текущих показателей [3.101, 3.102], так и могут применяться для агрегации прогнозов полученных с использованием физических моделей [3.103, 3.104]. Пример применения этих методов совместно с АДМС можно найти в статье [3.105], где на основе дорожных датчиков оценивалось состояние дорожного покрытия на парковке. При этом методы были применимы для различных типов покрытия в зимний период.

Однако на сегодняшний день остается ряд нерешенных проблем. В частности, определение оптимального расположения датчиков для обслуживания нужного участка дороги представляет значительную сложность. Ряд исследований показывает (см., например, [3.90]), что реальное состояние дороги может существенно отличаться от состояния, зафиксированного на тех участках, где установлены датчики.

3.3.5.6 Результаты экспериментов

Приведем полученные результаты анализа различных методов обнаружения аномалий в архивных данных, собранных с АДМС. Для обучения конкурирующих методов обнаружения аномалий и оценки их точности (с помощью F1-меры [3.92]) была проведена экспертная разметка части архивных данных с АДМС. Сравнение проводилось с рядом типичных методов классификации и обнаружения аномалий, реализованных в программной библиотеке машинного обучения scikit-learn [3.106]. Пример результатов сравнения приведен в Таблице 3.2. В качестве привилегированной информации использовались данные прогнозов модели METRo.

Таблица 3.2–Результаты сравнения

Алгоритм	F1 мера
Elliptic Envelope	0.577
Logistic Regression	0.684
Gradient Boosting Decision Trees	0.705
Предложенный подход	0.797

Источник: результаты получены в рамках исследовательской работы, проводимой Свириденко Н.Ю. и Смоляковым Д.С. под руководством Бурнаева Е.В.

Таким образом, предложенный подход позволяет увеличить точность обнаружения аномалий более чем на 10% по сравнению со стандартными подходами, то есть является перспективным методом решения задачи очистки архивных данных от аномалий и автоматизированного выявления вышедших из строя датчиков.

3.3.6 Выводы

Из проведенного обзора методов и приложений предсказательного технического обслуживания можно сделать ряд выводов.

Вывод 1. Значимая часть оборудования, которое используется на производстве, не оборудована датчиками для передачи необходимой информации о параметрах работы оборудования. Более того, беспроводная передача данных на производстве может быть затруднена. Таким образом, требуется разработка специализированных датчиков для оснащения оборудования и новых технологий беспроводной передачи данных на производственных площадках.

Вывод 2. Для построения моделей обнаружения аномалий и прогнозирования поломок требуется применение целого «зоопарка» инструментов машинного обучения, а также разработка новых методов машинного обучения, способных работать с нестандартными постановками задач анализа данных.

Вывод 3. В значительной доле случаев задачи предсказательного технического обслуживания требуют использования стандартных методов машинного обучения.

При этом процесс построения предиктивных моделей однотипен (генерация признаков, построение модели, чаще всего с помощью градиентного бустинга на основе деревьев решений, выбор гиперпараметров метода машинного обучения, верификация модели, и т.п.). Этот однотипный процесс должен быть полностью автоматизирован. В настоящее же время значительная часть работы выполняется вручную.

Вывод 4. В данной работе мы рассматривали модели на основе данных, однако, не стоит и забывать о моделях на основе «физики процессов». Во-первых, такого рода модели могут быть использованы для порождения новых признаков (см. также раздел 3.3.5.5). Во-вторых, учёт физических моделей может помочь сохранить «физические» тренды и/или зависимости между переменными, которые не всегда просто выявить, особенно если модель машинного обучения при некоторых значениях входных параметров делает прогноз в режиме экстраполяции. И, наконец, в тех случаях, когда в обучающей выборке не присутствуют целевые события (например, не было примеров поломки турбины в течение периода времени, когда собиралась обучающая выборка данных), физические модели можно использовать для симуляции «искусственных» примеров поломок и предварительного обучения на них предсказательных моделей.

Вывод 5. В настоящее время в приложениях ПТО имеется две крайности. Одна связана с тем, что многие компании, которые осуществляют внедрение приложений предсказательного технического обслуживания, делают большое количество прикладных проектов и по сути занимаются консалтингом. Конечно, такого рода прикладной опыт полезен, но он не всегда может быть обобщен надлежащим образом, чтобы в итоге разработать продукт, направленный на решение некоторого класса задач в иной отрасли. Другая крайность состоит в том, что есть ряд компаний, разрабатывающих достаточно общие платформы индустриального интернета вещей, использование которых для решения конкретных прикладных задач и последующее внедрение в производственные процессы затруднено именно по причине излишней общности. «Золотая середина» в этих процессах по мнению автора пока не достигнута.

Заключение⁴³

Понятие «Интернет вещей» является комплексным и до сих пор развивается. Интернет вещей может рассматриваться и как совокупность составляющих его технологий (в различных комбинациях и с разной степенью агрегирования, устоявшегося «набора» компонентов нет), и как желаемое сочетание компонентов (часть из которых только предстоит разработать), и функционально – через задачи, которые решаются с его помощью, и как концептуальная модель (то есть область пересечения людей, киберпространства и технического мира). Это говорит о том, что сегодня нет общепризнанного определения такого технологического феномена, как «Интернет Вещей».

В данной работе принимается определение, которое обеспечивает простоту понимания и при этом является функциональным. «Интернет Вещей» трактуется как вычислительная сеть физических объектов, оснащенных встроенными (embedded) технологиями сбора и передачи информации в совокупности с устройствами и технологиями хранения и интеллектуальной обработки информации, а также устройствами и алгоритмами генерации управляющих воздействий как на части системы, так и глобальных.

Первое время «Интернет Вещей» был в основном предметом академических исследований, а не практических приложений. Только с середины 2000-х гг. к нему стали проявлять интерес бизнес и промышленность. Применение IoT началось с использования RFID-меток, и поэтому рынки изначально оценивались не в денежном выражении, а в количестве проданных RFID-меток. Основными областями применения стали транспорт, логистика, производство и переработка, сельское хозяйство, здравоохранение и фармацевтика.

В 2009 г. Европейская комиссия приняла план, согласно которому интернет вещей рассматривался как новый этап в эволюционном развитии сети Интернет в целом, а в 2011 г. аналитическая компания Gartner включила интернет вещей

⁴³ Дежина И.Г. (Сколтех)

в свой Цикл зрелости технологий (Hype cycle). В 2013 г. появились первые оценки мирового рынка IoT.

Распространению IoT способствовало несколько сопутствующих технико-технологических факторов: взрывной рост числа подключенных устройств и приложений и широкая доступность беспроводной связи, снижение стоимости сенсоров, внедрение инструментов анализа больших данных, появление и широкое распространение облачных решений. Наконец, важным этапом стала разработка стандартов и рекомендаций в области IoT и его приложений.

Проблемы с оценками рынка интернета вещей и, тем более, прогнозом его развития обусловлены сложностью самого явления. При наличии консенсуса о том, что, в целом, рынок интернета вещей растет, прогнозы, разрабатываемые несколькими мировыми аналитическими и консалтинговыми компаниями, корректируются практически каждый год. Сказанное справедливо и относительно инвестиций. Первоначальные ожидания были очень высокими, однако впоследствии прогнозы темпов роста неоднократно пересматривались в сторону более низких. Среди причин большой вариабельности прогнозов, а также сильного колебания оценок, можно выделить не только различие методологий расчетов, но и иное, чем ожидалось, развитие собственно технологического ландшафта. Поскольку интернет вещей включает в себя значительное число различных технологий, то тренды развития отдельных компонентов общего технологического стека IoT оказывают неоднозначное влияние на динамику рынка. Кроме того, разные эксперты по-разному видят категории «вещей», которые ожидаются в будущем в качестве новых компонентов. Это также усиливает вариацию оценок развития рынка.

В целом, инвестиции в развитие интернета вещей растут, и, согласно опросам, в среднесрочной перспективе планируется продолжение роста. По данным BI Intelligence, в период с 2017 г. по 2025 г. общий объем инвестиций в IoT должен составить 15 трлн. долларов. При этом ожидается, что уже к 2021 г. потребительский сектор превысит по объему отраслевые рынки.

В технологической структуре драйверами роста станут сегменты программного обеспечения и услуг. Предполагается, что к 2020 г. программное обеспечение должно стать самым крупным сегментом. В отраслевом разрезе рост рынка будет обеспечен такими сегментами, как дискретное производство, транспорт, жилищно-коммунальное хозяйство, потребительский сегмент и страхование. Также будут развиваться такие кросс-индустриальные направления, как «Умный город» и «Подключенная промышленность».

В географическом разрезе главным трендом является укрепление позиций Азиатско-Тихоокеанского региона во главе с Китаем. Российский рынок интернета вещей по сравнению с мировым еще находится на ранней стадии развития, однако к 2022 г. следует ожидать сокращения разрыва. При этом рынок оценивается в очень широких границах – от 40 до 600 млрд. рублей (по итогам 2017 г.). Среди экспертов нет консенсуса и в том, какие приложения IoT доминируют в России. Так, оценки доли рынка промышленного интернета вещей варьируются от 20% до 95%.

Основными драйверами развития российского рынка IoT являются цифровая трансформация компаний, создание экосистемы и рост взаимодействия поставщиков решений, а также государственная поддержка. Положительное влияние оказали и первые успешные проекты, посвященные сбору данных и интеграции решений интернета вещей с существующими ИТ-системами. Есть и сдерживающие рост факторы, такие как неуверенность участников рынка в достаточном уровне возврата инвестиций, проблемы защиты информации и стандартизации. Для улучшения ситуации большую роль может сыграть государственная программа «Цифровая экономика Российской Федерации», в рамках которой предполагается развитие необходимой инфраструктуры и нормативно-правового регулирования, разработка стандартов.

В целом, государственное стимулирование развития интернета вещей имеет большое значение. Поддержка, однако, далеко не всегда оказывается в прямой форме – в виде финансирования проектов, субсидирования, льготного налогообложения. Важным элементом государственного стимулирования

является нормативно-правовое регулирование, включая разработку технических рекомендаций и стандартов.

Следует отметить, что во многих странах интернет вещей сложно выделить из общей системы поддержки цифровой экономики. На сегодняшний день наиболее последовательную и самостоятельную политику в области развития интернета вещей проводит Китай. Поддержка, включая как проектное финансирование, так и разработку стандартов, встроена в пятилетние планы развития этой страны. Государство поддерживает, в том числе посредством мер регулирования, технологии интернета вещей в самых разных областях, включая промышленный контроль, финансовые услуги и здравоохранение. Важно и то, что реализуется как централизованная, так и региональная политика поддержки.

Релевантным для России опытом можно также считать политику правительства Франции. Там государственные органы содействуют преодолению технологических и социальных барьеров развития интернета вещей, а также решению проблем безопасности и хранения данных. Финансовая и нефинансовая поддержка реализуется через несколько программ («Новая промышленная Франция», «French Tech»), и дополняется мягкой регуляторной политикой в области телекоммуникаций. Важным элементом политики является поддержка стартапов в этой сфере. В результате, по оценке аналитиков IDG Connect, успех французских стартапов может вывести Францию в число мировых лидеров развития интернета вещей. Успехи можно оценить и в финансовом выражении – объем рынка интернета вещей во Франции в 2017 г. преодолел отметку в 1 млрд. евро (физический объем – 5,2 млн. устройств в год), и по всем показателям наблюдаются двухзначные темпы роста.

В России государственная политика по продвижению интернета вещей в первую очередь связана с развертыванием Национальной технологической инициативы. Ее перспективы связывают с дополнительными мерами в государственной программе «Цифровая экономика Российской Федерации», где промышленный интернет вещей выделен в качестве одной из сквозных технологий. Помимо

промышленности, большой потенциал использования технологий интернета вещей есть на транспорте, в логистике, сельском хозяйстве, для формирования умных городов, а также в утилизации отходов.

Один из ключевых аспектов развития интернета вещей, который отмечают эксперты, представляющие как научное сообщество, так и бизнес-сектор, – это стандартизация IoT и гармонизация стандартов на международном уровне. Разработка и выпуск соответствующих стандартов критически важны, это на порядок облегчает внедрение технологий в любом сегменте рынка, и особенно в таких консервативных областях, как промышленность, медицина, строительство, энергетика.

Главная роль в стандартизации IoT на международном уровне принадлежит ИСО, МЭК и МСЭ, в работе которых участвует и Россия. На международном уровне наиболее острым и стратегически важным вопросом является признание «Промышленного интернета вещей» в качестве самостоятельного объекта стандартизации. Одна из трудно решаемых проблем – это обеспечение совместимости систем и устройств, образующих сети связи. Развитию стандартизации в области хранения и обработки данных препятствует ряд научных (вплоть до отсутствия рабочей методологии определения понятий), технологических (связанных с недостаточным развитием сетей передачи данных, систем распознавания) и законодательных барьеров.

Для преодоления технологических барьеров, в качестве перспективных направлений работ можно выделить следующие: разработку новых форматов представления понятий «данные» – «информация» – «знания», исследования по определению потенциальных контекстов использования накопленных данных, миниатюризацию элементной базы беспроводных приёмников, расширение стандартов IEEE 802.11, поиск минимальных наборов данных, достаточных для машинного обучения.

Рынок приложений интернета вещей постоянно растет. Как один из примеров, в книге рассмотрена сельскохозяйственная отрасль, где использование интернета вещей критично для повышения производительности.

В последние годы в сельском хозяйстве значительно возросла активность внедрения информационных и цифровых технологий. Развиваются исследования и разработки в области IoT, многократно вырос интерес мировых венчурных фондов к инновационным проектам в этой области (объем инвестиций за 2017 г. составил 10,1 млрд. долл.), увеличивается сетевое покрытие сельскохозяйственных земель. Ключевой точкой роста в этой области является усиливающееся взаимопроникновение компьютерных и инженерных технологий. Благодаря комбинированию данных (в том числе, с датчиков и дронов), различным каналам связи и специальным мобильным и онлайн-приложениям, участникам рынка становится доступна оперативная информация о состоянии их сельхозугодий, что создает необходимые условия для развертывания IoT.

Правительство России уделяет значительное внимание внедрению цифровых технологий в сельское хозяйство. За счет этого в ближайшие 7 лет ожидается пятикратный рост рынка IT и интернета вещей в данной отрасли, с 400 млрд. руб. в 2017 г. до 2 трлн. руб. к 2024 г. Однако пока Россия отстает от мировых лидеров. Для развития IoT в сельском хозяйстве необходимо преодолеть ряд барьеров: инфраструктурных (покрытие сетями связи), кадровых, экономических (недостаточная инновационная и инвестиционная активность), культурных (консерватизм аграриев) и правовых (несовершенство нормативно-правового регулирования, необходимость упрощения бюрократических процедур на всех этапах работы с информацией). Среди необходимых мер для внедрения технологий интернета вещей в российское сельское хозяйство – создание специализированной цифровой инфраструктуры и внедрение профильных образовательных программ, ориентированных на подготовку специалистов «цифрового сельского хозяйства».

Интернет вещей как комплексное явление зависит от технологических компонентов, которые задействованы в его работе. Практически для всех отраслевых и межотраслевых приложений одними из наиболее важных становятся проблемы обеспечения безопасности и предсказательное техническое обслуживание.

В сфере обеспечения безопасности остро стоят вопросы создания аппаратуры, реализующей безопасные технологии, дальнейшего развития этих технологий и незавершённости международных стандартов, поддерживающих технологии защиты информации. Точками роста являются защита информации в «облачных» системах, безопасные технологии для систем с ограниченными вычислительными ресурсами (легкая криптография) и постквантовая криптография.

На национальном уровне к перечисленным проблемам добавляется отсутствие независимого сообщества производителей средств защиты, свободной конкуренции, независимой экспертизы существующих и перспективных разработок и культуры информационной безопасности. Есть и зависимость от сертификационных программ международных организаций (EC-Council, Институт SANS, (ISC)², NESSIE, ECRYPT II) и крупных западных вендоров (Microsoft, Oracle, Cisco). В результате, в программно-техническом обеспечении и организационно-юридическом оформлении решений IoT, Россия практически исключена из мирового профессионального сообщества и выступает только в роли конечного потребителя, что грозит «ползучей» потерей суверенитета в данной области. Преодоление этих препятствий требует реализации комплекса организационных, технологических и популяризационных мер в среде разработчиков и пользователей. В то же время, развитие на глобальном уровне новых направлений в информационной безопасности создает уникальные возможности для преодоления наметившегося отставания путем участия в разработке указанных технологий с начальных этапов.

Предиктивное обслуживание считается одним из самых перспективных рынков применения интернета вещей. Для его реализации одной из ключевых технологических проблем является обработка и анализ данных, собираемых в рамках промышленного интернета вещей. Использование современных методов предсказательной аналитики позволит:

- обслуживать оборудование на основе автоматического контроля его состояния (предсказательное техническое обслуживание);

- обеспечивать надежность и эффективность работы сложных технических и информационных систем (самолетов, судов, ракет, ядерных электростанций, различных интернет-сервисов, и т.д.);
- проводить автоматический контроль качества выпускаемой продукции, и т.д.

При выборе стратегии технического обслуживания необходимо, как правило, решать задачу многокритериальной оптимизации. Использование современных методов интеллектуального анализа данных позволяет сбалансировать противоречивые целевые показатели, и, благодаря исключению плановых замен технически исправных и надежных компонент и узлов системы, значительно сократить затраты на техническое обслуживание. Это также позволяет улучшить логистику обеспечения необходимыми комплектующими, более эффективно распределять энергию, совершенствовать управление энергопотребляющими продуктами и снижать энергозатраты. Более того, использование предсказательного технического обслуживания может привести к построению новых сервисных моделей, когда, например, продается не конкретный тип оборудования, а время его бесперебойной работы.

Рассмотренные в книге конкретные отраслевые кейсы использования предсказательной аналитики позволяют очертить барьеры, стоящие на пути широкого внедрения этой перспективной технологии. В частности, сегодня значительная часть производственного оборудования не оснащена датчиками и средствами передачи необходимой информации о параметрах. В целом, предсказательное техническое обслуживание на современном этапе тяготеет к одной из двух крайностей. Первая связана с тем, что многие компании, которые осуществляют внедрение приложений ПТО, делают большое количество прикладных проектов и, по сути, занимаются консалтингом. Конечно, такого рода прикладной опыт полезен, но он не всегда может быть надлежащим образом обобщен, чтобы в итоге разработать продукт, направленный на решение некоторого класса задач в одной из индустрий. Другая крайность состоит в том, что ряд

компаний разрабатывает достаточно общие платформы индустриального интернета вещей, использование которых для решения конкретных прикладных задач и последующее внедрение в производственные процессы затруднено именно по причине излишней общности.

Во многих случаях задачи предсказательного технического обслуживания требуют использования стандартных методов машинного обучения. При этом процесс построения предиктивных моделей однотипен (генерация признаков, построение модели, чаще всего с помощью градиентного бустинга на основе деревьев решений, выбор гиперпараметров метода машинного обучения, верификация модели, и т.п.). Этот процесс может быть полностью автоматизирован.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Раздел 1

- 1.1 Интернет вещей — что это такое и как применять IoT в реальном бизнесе // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://rb.ru/longread/iot-cards/>
- 1.2 Nick Wainwright, HP Labs and Chair of the UK future Internet Strategy Group.
- 1.3 Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://static.kremlin.ru/media/acts/files/0001201705100002.pdf>
- 1.4 Интернет вещей (IoT) // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.ibs.ru/datalab/works/internet-veshchey-iot/>
- 1.5 Росляков А. В. и др. Интернет вещей // Самара: ПГУТИ, ООО «Издательство Ас Гард». – 2014. – Т. 340.
- 1.6 В России создадут национальную операционную систему для «интернета вещей» // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.rbc.ru/technology_and_media/10/10/2017/59dc390b9a794788fee33842
- 1.7 Что такое Интернет вещей? // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.hpe.com/ru/ru/what-is/internet-of-things.html>
- 1.8 Что такое Интернет вещей (IoT)? // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.sap.com/cis/trends/internet-of-things.html>
- 1.9 Internet of Things (IoT) 2018 – Market Statistics, Use Cases and Trends // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://asiandatascience.com/wp-content/uploads/2017/12/eBook-Internet-of-Things-IoT-2018-Market-Statistics-Use-Cases-and-Trends.pdf>
- 1.10 Three major Challenges Facing IoT // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html>

- 1.11 Рекомендации МСЭ -Т Y.2060 «Обзор интернета вещей» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=11559&lang=ru>,
- 1.12 Internet of Things (IoT). Preliminary Report 2014 // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf
- 1.13 Atzori L., Iera A., Morabito G. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm //Ad Hoc Networks. – 2017. – Т. 56. – С. 122-140
- 1.14 Paul P. V., Saraswathi R. The Internet of Things—A comprehensive survey //Computation of Power, Energy Information and Commuication (ICCPEIC), 2017 International Conference on. – IEEE, 2017. – С. 421-426.
- 1.15 Лидеры Всемирного форума по Интернету вещей анонсировали эталонную модель IoT и Кадровый консорциум IoTWF //Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.cisco.com/c/ru_ru/about/press/press-releases/2014/10-102014e.html
- 1.16 Интернет вещей: сетевая архитектура и архитектура безопасности // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://internetinside.ru/internet-veshhey-setevaya-arkhitektura-i/>
- 1.17 Stallings W. The Internet of Things: Network and Security Architecture //Internet Protocol J. – 2015. – Т. 18. – №. 4. – С. 2-24.
- 1.18 Internet of Things Architecture // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://cordis.europa.eu/project/rcn/95713_en.html
- 1.19 Knud Lasse Lueth, IoT basics: Getting started with the Internet of Things // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://iot-analytics.com/wp/wp-content/uploads/2015/03/2015-March-Whitepaper-IoT-basics-Getting-started-with-the-Internet-of-Things.pdf>
- 1.20 What is the Internet of Things? Internet of Things definitions // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.i-scoop.eu/internet-of-things/#Internet_of_Things_definitions_what_the_Internet_of_Things_is_not

- 1.21 Yun M., Yuxin B. Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid //Advances in Energy Engineering (ICAEE), 2010 International Conference on. – IEEE, 2010. – С. 69-72.
- 1.22 Интернет вещей. Как изменится вся наша жизнь на очередном витке развития Всемирной сети. / Группа разработки интернет-решений Cisco для бизнеса (IBSG) // Электрон. дан. – Заглавие с экрана. – Режим доступа:
- 1.23 Zinnov Zones 2017 IoT Technology Services // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.slideshare.net/zinnov/zinnov-zones-for-iot-services>
- 1.24 Intel® IoT Platform Reference Architecture // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.intel.ru/content/www/ru/ru/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html>
- 1.25 The First IOT Device... A Coke machine? // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://thefutureofsmart.wordpress.com/2014/10/04/the-first-iot-device-a-coke-machine/>
- 1.26 A Very Short History of the Internet of Things // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/#5f7713a510de>
- 1.27 Lamming M., Flynn M. Forget-me-not: Intimate computing in support of human memory // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://marengo.info-science.uiowa.edu/eichmann/fmn.pdf>,
- 1.28 The internet of things // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.theguardian.com/technology/2003/oct/09/shopping.newmedia>
- 1.29 Did Wal-Mart love RFID to death? // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.zdnet.com/article/did-wal-mart-love-rfid-to-death/>
- 1.30 Ubiquitous Sensor Networks (USN) ITU -T Technology Watch Report #4, February 2008// Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000040002PDFE.pdf
- 1.31 Mattern F., Floerkemeier C. From the Internet of Computers to the Internet of Things // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf>

- 1.32 Radio Frequency IDentification RFID: The Internet of things // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://ec.europa.eu/information_society/doc/factsheets/054-rfid-en.pdf
- 1.33 The History of IoT (Internet of Things) and How It's Changed Today// Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://avancer.in/history-iot-internet-things-changed-today/>
- 1.34 Santucci G. From internet of data to internet of things. International Conference on Future Trends of the Internet. // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://www.ipv6council.lu/docs/G_Santucci_paper.pdf
- 1.35 Vision and Challenges for Realizing the Internet of Things // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.etsi.org/website/document/newsandevents/vision_and_challenges_for_realising_the_internet_of_things.pdf
- 1.36 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Internet of Things — an action plan for Europe//Электрон.дан.– Заглавие с экрана. – Режим доступа: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF>
- 1.37 China's initiative for the internet of things and opportunities for Japanese businesses // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.nri.com/global/opinion/papers/2011/pdf/np2011165.pdf>
- 1.38 Why the Internet of Things is called Internet of Things: Definition, history, disambiguation // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://iot-analytics.com/internet-of-things-definition/>
- 1.39 How China is scaling the Internet of Things. An insight report from the GSMA Connected Living Programme, July 2015. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gsma.com/newsroom/wp-content/uploads/16531-China-IoT-Report-LR.pdf>
- 1.40 Van Kranenburg R. et al. The internet of things. Proc. of the First Berlin Symposium on Internet and Society. // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://www.pyfn.com/PDF/iot_pdfs/the_iot_paper_2011.pdf

- 1.41 Europe's policy options for a dynamic and trustworthy development of the Internet of Things // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR356/RAND_RR356.pdf
- 1.42 Here is Why 'The Internet of Things' Will Be Huge, And Drive Tremendous Value for People and Businesses // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.businessinsider.com/growth-in-the-internet-of-things-2013-10>
- 1.43 IoT Past and Present: The History of IoT, and Where It's Headed Today// Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.channelfutures.com/msp-501/iot-past-and-present-history-iot-and-where-its-headed-today>
- 1.44 GE says data business on track for over \$1 billion in sales // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://finance.yahoo.com/news/ges-data-analysis-business-track-deliver-1-billion-143132586--sector.html>
- 1.45 Digital Single Market Policy. The Internet of Things// Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://ec.europa.eu/digital-single-market/en/internet-of-things>
- 1.46 The Internet of Things: Evolution or Revolution?// Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.aig.com/content/dam/aig/america-canada/us/documents/insights/aig-iot-evolution-or-revolution.pdf>
- 1.47 Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016// Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>
- 1.48 IDC Forecasts Worldwide Spending on the Internet of Things to Reach \$772 Billion in 2018 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.idc.com/getdoc.jsp?containerId=prUS43295217>
- 1.49 Internet of Things Technology Market by Node Component (Processor, Sensor, Connectivity IC, Memory Device, and Logic Device), Network Infrastructure, Software

- Solution, Platform, Service, End-use Application, and Geography - Global Forecast to 2022 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.marketsandmarkets.com/Market-Reports/iot-application-technology-market-258239167.html>
- 1.50 MARKET ANALYSIS Worldwide and Regional Internet of Things (IoT) 2014–2020 Forecast: A Virtuous Circle of Proven Value and Demand // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.business.att.com/content/article/IoT-worldwide_regional_2014-2020-forecast.pdf
- 1.51 Internet of Things Market to Reach \$1.7 Trillion by 2020: IDC// Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://blogs.wsj.com/cio/2015/06/02/internet-of-things-market-to-reach-1-7-trillion-by-2020-idc/>
- 1.52 IDC Forecasts Worldwide Technology Spending on the Internet of Things to Reach \$1.2 Trillion in 2022// Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.idc.com/getdoc.jsp?containerId=prUS43994118>
- 1.53 Gartner Says 6.4 Billion Connected “Things” Will Be in Use in 2016, Up 30 Percent From 2015 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gartner.com/newsroom/id/3165317>
- 1.54 IoT-Enabled Analytic Applications Revolutionize Supply Chain Planning and Execution, White Paper, IDC // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.savi.com/wp-content/uploads/IDC-IoT-enabled-analytics-applications_final.pdf
- 1.55 Reducing the Time to Value for Internet of Things Deployments, White Paper, IDC // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.oracle.com/webfolder/s/delivery_production/docs/FY16h1/doc25/IDCWhitePaperFinal.pdf
- 1.56 Internet of Things spending nearing \$800 billion mark in 2018 – spending shifts and context // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.i-scoop.eu/internet-things-spending-2018/>
- 1.57 BI Intelligence projects 34 billion devices will be connected by 2020 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.businessinsider.com/bi-intelligence-34-billion-connected-devices-2020-2015-11>

- 1.58 The Ultimate Internet of Things Research Bundle // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.businessinsider.com/intelligence/bi-intelligence-iot-research-bundle?vertical=iot>
- 1.59 Business Insider Intelligence, IoT Report: How Internet of Things technology is now reaching mainstream companies and consumers // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.businessinsider.com/internet-of-things-report>
- 1.60 IoT platforms: enabling the Internet of Things, IHS TECHNOLOGY, March 2016 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://technology.ihs.com/576272/iot-platforms-enabling-the-internet-of-things>
- 1.61 The Internet of Things: A movement, not a market, IHS Markit Technology // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://ihsmarkit.com/Info/1017/internet-of-things.html>
- 1.62 IoT trend watch 2018, IHS Markit Technology // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://ihsmarkit.com/Info/0118/iot-trend-watch-2018.html>
- 1.63 ERICSSON MOBILITY REPORT JUNE 2016 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.ericsson.com/assets/local/mobility-report/documents/2016/Ericsson-mobility-report-june-2016.pdf>
- 1.64 Internet of Things forecast // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.ericsson.com/en/mobility-report/internet-of-things-forecast>
- 1.65 Ericsson Mobility Report | June 2018 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf>
- 1.66 State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>
- 1.67 Bain & Company predicts the Internet of Things market will more than double to \$520 billion by 2021 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.bain.com/about/media-center/press-releases/2018/bain-predicts-the-iot-market-will-more-than-double-by-2021/>

- 1.68 Internet of Things (IoT) Market: Global Demand, Growth Analysis & Opportunity Outlook 2023 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.researchnester.com/reports/internet-of-things-iot-market-global-demand-growth-analysis-opportunity-outlook-2023/216>
- 1.69 IoT Investment Heats Up in January 2017, Harbor Research // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://harborresearch.com/iot-investment-update-january-2017/>
- 1.70 IOT ~ THE INTERNET OF TRANSFORMATION 2018 Whitepaper Juniper Research // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.juniperresearch.com/document-library/white-papers/iot-the-internet-of-transformation-2018>
- 1.71 Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://newsroom.cisco.com/press-release-content?articleId=1847422>
- 1.72 IoT Breakdown: VCs betting billions on the connected world, PitchBook URL: // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://pitchbook.com/newsletter/the-8-most-active-vc-investors-in-us-iot>
- 1.73 Growing Pains: The 2018 Internet of Things Landscape // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://matttuturck.com/iot2018/>
- 1.74 Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gartner.com/newsroom/id/2636073>
- 1.75 McKinsey Global Institute/ How can we recognize the real power of the Internet of Things? // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/how-can-we-recognize-the-real-power-of-the-internet-of-things>
- 1.76 Zinnov Zones 2017 for IoT Technology Services // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://zinnov.com/zinnov-zones-2017-for-iot-technology-services/>
- 1.77 BCG, Winning in IoT. It's all about business processes // Электрон. дан. – Заглавие с экрана. – Режим доступа:

- <https://www.bcg.com/ru-ru/publications/2017/hardware-software-energy-environment-winning-in-iot-all-about-winning-processes.aspx>
- 1.78 The Top 10 IoT Segments in 2018 – based on 1,600 real IoT projects // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/>
 - 1.79 GrowthEnabler, MARKET PULSE REPORT, INTERNET OF THINGS (IoT) // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf>
 - 1.80 Spending on the Internet of Things in CEE to Exceed \$11 Billion in 2018, According to IDC // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.idc.com/getdoc.jsp?containerId=prCEMA43526318>
 - 1.81 IoT Spending in the Middle East & Africa Set to Almost Double over Coming Years // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.idc.com/getdoc.jsp?containerId=prCEMA43387417>
 - 1.82 Latest IDC Forecast Sees Technology Spending on the Internet of Things in Asia/Pacific (excluding Japan) Valued at USD 291.7 Billion in 2018 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.idc.com/getdoc.jsp?containerId=prAP44138418>
 - 1.83 IoT Spending in Central and Eastern Europe to Grow by 15% // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.idc.com/getdoc.jsp?containerId=prCEMA44194618>
 - 1.84 Интернет вещей, IoT, M2M рынок России TAdviser // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://goo.gl/KKigQ>
 - 1.85 ИНДУСТРИАЛЬНЫЙ ИНТЕРНЕТ ВЕЩЕЙ. ПЕРСПЕКТИВЫ РОССИЙСКОГО РЫНКА/ IDC MARKET SPOTLIGHT. По заказу ПАО «Ростелеком» // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.company.rt.ru/projects/IIoT/study_IDC.pdf
 - 1.86 Рынок Интернета вещей в России: прогнозы IDC на 2017-2021 гг. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://idcrussia.com/ru/about-idc/press-center/65015-idc-2017-2021>

- 1.87 Интернет вещей и межмашинные коммуникации. Обзор ситуации в России и мире // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://json.tv/ict_telecom_analytics_view/internet-veschey-i-mejmashinnye-kommunikatsii-obzor-situatsii-v-rossii-i-mire
- 1.88 Российский рынок межмашинных коммуникаций и Интернета Вещей по итогам 2017 года, прогноз до 2022 года Market Watch J'son & Partners Consulting // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://json.tv/ict_telecom_analytics_view/rossiyskiy-rynok-mejmashinnyh-kommunikatsiy-i-interneta-veschey-po-itogam-2017-goda-prognoz-do-2022-goda--20180109112137
- 1.89 Объем российского рынка интернета вещей в 2016 году достиг \$1,2 млрд // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.vedomosti.ru/technology/articles/2017/05/15/689785-rinka-interneta-veschei>
- 1.90 Исследование Orange Business Services и iKS-Consulting показывает стабильный среднегодовой рост российского рынка Интернета вещей на 12% до 2020 года // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.orange-business.com/ru/press/issledovanie-orange-business-services-i-iks-consulting-pokazyvaet-stabilnyy-srednegodovoy-rost>
- 1.91 GDP (current US\$), World, World Bank national accounts data, and OECD National Accounts data files // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD>
- 1.92 A World Bank Group Flagship Report Global Economic Prospects. The Turning of the Tide? JUNE 2018/ World Bank Group // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.worldbank.org/en/publication/global-economic-prospects>
- 1.93 GDP (current US\$), Russia, World Bank national accounts data, and OECD National Accounts data files // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=RU>
- 1.94 Обзор рынка IoT в России, Декабрь 2017 AC&M-Consulting // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://www.acm-consulting.com/data-downloads/doc_download/191-iot-report-in-russian.html

- 1.95 The Six Forces Driving the Internet of Things // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.pwc.com/gx/en/technology/pdf/six-forces-driving-iot.pdf>
- 1.96 The key IoT market drivers and IoT market barriers // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.i-scoop.eu/key-iot-market-drivers-iot-market-barriers/>
- 1.97 Тихвинский В.О., Минов А.В. Сценарии производственной деятельности операторов услуг Интернета вещей на телекоммуникационном рынке // Тезисы к седьмой отраслевой научной конференции «Технологии информационного общества». Тез. докл. Междунар. конф. М. 2013. С. 170.
- 1.98 Минов А.В. Сценарии производственной деятельности операторов услуг Интернета вещей на телекоммуникационном рынке // Технологии информационного общества. 2013. № 1. С. 170-180.
- 1.99 Тихвинский В.О. Партнерский проект oneM2M: Новая парадигма в развитии телекоммуникаций // Электросвязь. 2012. № 11. С. 18-20.
- 1.100 Тихвинский В.О. Перспективные бизнес модели и сферы применения M2M. Оценка эффективности // Connect! Мир связи. 2012. № 6. С. 124-127.
- 1.101 Тихвинский В.О. Перспективы и модели услуг в сетях M2M // Connect! Мир связи. 2011. № 2. С. 86-91.
- 1.102 Al-Debei M., El-Haddadeh R., Avison D. Defining the Business Model in the New World of Digital Business. London: Brunel University, 2008, 99 с.
- 1.103 Ballon P. Control and Value in Mobile Communications: A political economy of the reconfiguration of business models in the European mobile industry. Brussel: Vrije Universiteit, 2009. 99 с.
- 1.104 Boswarthick D., Elloumi O., Hersent O. M2M Communications: A systems Approach. Hoboken: John Wiley & Sons, 2012, 308 с.
- 1.105 Murroni F. Exploring the ultimate middleware to enable new business models and establishing how to implement an innovative M2M ecosystem. Bogliasco: ABO DATA, 2012. 28 с.
- 1.106 Oswald J., Riaan W. Value Chain scenarios for M2M Ecosystem // University of Stellenbosch. 2011. № 6. С. 58-68.

- 1.107 Goncalves V., Dobbelaere P. Business Scenarios for Machine-to-Machine Mobile Applications // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5496676&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D5496676
- 1.108 M2M and the Supply Chain. The Power and Potential of M2M in the Supply Chain: A Network of Manufacturing and Distribution Facilities and Processes // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.opto22.com/documents/1425_White_Paper_M2M_and_the_Supply_Chain.pdf
- 1.109 Market Report, Machine-to-Machine (M2M) Companies and Applications 2011 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.companiesandmarkets.com/Market-Report/machine-to-machine-%28m2m%29-companies-and-applications-2011-634027.asp>
- 1.110 Lucero S. Maximizing Mobile Operator Opportunities in M2M: The Benefits of an M2M-Optimized Network // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/mobile-operators/ABI-CISCO_M2M_Operator_Opportunity.pdf
- 1.111 Анализ технологических платформ M2M/IoT и провайдеров специализированного ПО // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://json.tv/ict_telecom_analytics_view/analiz-tehnologicheskikh-platform-m2miot-i-provayderov-spetsializirovannogo-po-20150706024809
- 1.112 M2M Communications Turn Potential into Profit // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.informatandm.com/wp-content/uploads/2012/04/M2M-Communications.pdf>
- 1.113 Обзор рынка M2M. Общее состояние и перспективы развития // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://www.directinfo.ru/index.php?option=com_content&view=article&id=133%3A-2010-07-06-13-57-09&catid=1%3A2008-11-27-09-05-45&Itemid=84&lang=ru
- 1.114 Рынок M2M-коммуникаций в России и в мире // Электрон. дан. – Заглавие с экрана. – Режим доступа:

http://web.json.ru/poleznye_materialy/free_market_watches/analytics/rynok_m2m-kommunikacij_v_rossii_i_v_mire.

- 1.115 Стратегии мобильных операторов и возможности для новых игроков и MVNO на российском и мировом рынке M2M/IoT // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://json.tv/ict_telecom_analytics_view/rynok-m2miot-v-rossii-i-mire-struktura-i-dinamika-uspeshnye-strategii-i-biznes-modeli-monetizatsiya-rekomendatsii-20150629033006.
- 1.116 Официальная информация//ПАО "МТС". // Электрон. дан. – Заглавие с экрана. – Режим доступа: URL. <http://www.mts.ru/>
- 1.117 Официальная информация//ПАО "Мегафон". // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://megafon.ru/>
- 1.118 Официальная информация//ПАО "Вымпел-Коммуникации". // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://beeline.ru/>
- 1.119 Официальная информация//ООО "Т2Рус" // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://tele2.ru/>
- 1.120 Официальная информация//ПАО "Ростелеком" // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://rostelecom.ru/>.
- 1.121 Тихвинский В.О., Ким А.В. Мобильный телеком на распутье. Итоги MWC-14 // Электросвязь. 2014. № 3. С. 3-5.
- 1.122 Numbering and Addressing for Machine -to Machine (M2M) Communications Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.erodocdb.dk/Docs/doc98/official/pdf/REC1103.PDF>.
- 1.123 Analyzing Internet of Things Market Opportunities // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://harborresearch.com/wp-content/uploads/2013/08/Harbor-Research_IoT-Market-Opps-Paper_2013.pdf.
- 1.124 Минов А.В. Разработка организационно-управленческого механизма выбора модели производственной деятельности оператора интернета вещей// Электрон. дан. – Заглавие с экрана. – Режим

доступа: http://195.19.40.226/dissertations/var/www/uch/assets/dissertations/%D1%80%D1%83%D0%BA%D0%BE%D0%BF%D0%B8%D1%81%D1%8C_%D0%B4%D0%B8%D1%81%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D0%B8%D1%8F_%D0%BC%D0%B8%D0%BD%D0%BE%D0%B2_20180304_532_%D1%81%D0%BE_%D1%81%D0%BA%D0%B0%D0%BD%D0%B0%D0%BC%D0%B8.pdf.

- 1.125 Льюис М. Новейшая новинка. История Силиконовой долины. М.: Олимп-Бизнес, 2004. 384 с.
- 1.126 Портер М. Конкурентное преимущество. Как достичь высокого результата и обеспечить его устойчивость. М.: Альпина Паблишер, 2008, 720 с.
- 1.127 Codrea-Rado A. Until the 1990s, companies didn't have "business models". New York: Quartz, 2013, 232 с.
- 1.128 Drucker P.F. The Theory of the Business // Harvard Business Review. 1994. № 1. С. 99-109.
- 1.129 Johnson M. Seizing the White Space: Business Model Innovation for Growth and Renewal. Harward: Harvard Business Press, 2010, 208 с.
- 1.130 Johnson M., Christensen C., Kagermann H. Reinventing Your Business Model // Harvard Business Review. 2008. № 12. С. 9-19.
- 1.131 Magretta J. Why business models matter // Harvard Business Review. 2002. № 5. С. 99-109.
- 1.132 Osterwalder A. A Better Way to Think About Your Business Model // Harvard Business Review. 2013. № 6. С. 88.
- 1.133 Ovans A. What Is a Business Model? // Harvard Business Review. 2015. № 1. С. 36.
- 1.134 Rozeia M., Werthner H. Business Models and Business Strategy – Phenomenon of Explicitness // International Journal of Global Business & Competitiveness. 2011. № 1. С. 88-108.
- 1.135 Timmers P. Business Models for Electronic Markets // Journal on Electronic Markets. 1998. № 4. С. 80.
- 1.136 Jones G. M. Educators, Electrons, and Business Models: A Problem in Synthesis // Accounting Review. 1960. № 35(4). С. 619-626.
- 1.137 Osterwalder A. The business model ontology: a proposition in a design science approach. Lausanne: University of Lausanne, 2004. 172 с.

- 1.138 Остервальдер А., Пинье И. Построение бизнес-моделей: Настольная книга стратега и новатора. М.: Альпина Паблишер, 2012. 288 с.
- 1.139 Макдоналд М., Данбар Я. Сегментирование рынка: Практик. рук. М.: Дело и сервис, 2002. 282 с.
- 1.140 Котлер Ф. Основы маркетинга. М.: Вильямс, 2012. 751 с.
- 1.141 IMFDataMapper GDP // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD>
- 1.142 INOUE T., HAYAKAWA A., KAMEI T. China's Initiative for the Internet of Things and Opportunities for Japanese Businesses //Corporate Communications Department, Nomura Research Institute, Ltd. NRI Papers. – 2011. – С. 1-13.
- 1.143 Kshetri N. The evolution of the internet of things industry and market in China: An interplay of institutions demands and supply //Telecommunications Policy. – 2017. – Т. 41. – №. 1. – С. 49-67.
- 1.144 European Commission (DG CONNECT) and China Academy of Information and Communication Technology (2016) EU-China Joint White Paper on the Internet of Things. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://ec.europa.eu/digital-single-market/en/news/eu-china-joint-white-paper-internet-things>.
- 1.145 A GSMA INTERNET OF THINGS REPORT. JULY 2018. HOW GREATER CHINA IS SET TO LEAD THE GLOBAL INDUSTRIAL IOT MARKET // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.gsma.com/iot/wp-content/uploads/2018/06/GSMA_Report-How_Greater_China_Is_Set_To_Lead_Global_Industrial_IoT_Market-en-July2018.pdf
- 1.146 Report on Future Internet Chinese projects for future collaboration/ EXCITING Consortium 2016-2018 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://euchina-iot5g.eu/wp-content/uploads/D2.2-Projects-for-Future-Collaboration.pdf>
- 1.147 Internet of things gets even techier // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://www.chinadaily.com.cn/china/2017-09/11/content_31833613.htm
- 1.148 OPPORTUNITIES IN THE CHINESE IOT MARKET, June 2016, Business Sweden // Электрон. дан. – Заглавие

- с экрана. – Режим доступа: <https://www.business-sweden.se/contentassets/12018cf5fd6f4757aa0638f7065e8a83/iot-market-in-china.pdf>
- 1.149 Understanding the Role of Governments in Promoting the Industrial Internet of Things, Frost & Sullivan APAC // Электрон. дан. – Заглавие с экрана. – Режим доступа: [https://www.gevme.com/sites/iot-asia/sites/default/files/MI%20-%20Government%20IoT%20APAC_March%202017%20\(Revised\).pdf](https://www.gevme.com/sites/iot-asia/sites/default/files/MI%20-%20Government%20IoT%20APAC_March%202017%20(Revised).pdf)
- 1.150 R&D Center for Internet of Things of Chinese Academy of Sciences/ // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://english.ime.cas.cn/Research/ResearchDivisions/IoT1/>
- 1.151 National Intelligence Council, “Disruptive Civil Technologies: Six Technologies With Potential Impacts on U.S. Interests Out to 2025” // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.hsdl.org/?abstract&did=485606>
- 1.152 S.Res.110 - A resolution expressing the sense of the Senate about a strategy for the Internet of Things to promote economic growth and consumer empowerment. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.congress.gov/bill/114th-congress/senate-resolution/110/text>
- 1.153 FACT SHEET: Administration Announces New “Smart Cities” Initiative to Help Communities Tackle Local Challenges and Improve City Services // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://obamawhitehouse.archives.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help>
- 1.154 FACT SHEET: Announcing Over \$80 million in New Federal Investment and a Doubling of Participating Communities in the White House Smart Cities Initiative // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://obamawhitehouse.archives.gov/the-press-office/2016/09/26/fact-sheet-announcing-over-80-million-new-federal-investment-and>
- 1.155 Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things // Электрон. дан.

- Заглавие с екрана. – Режим доступа: <https://www.ntia.doc.gov/federal-register-notice/2017/request-comments-benefits-challenges-and-potential-roles-government>
- 1.156 Green Paper: Fostering the Advancement of the Internet of Things // Электрон. дан. – Заглавие с екрана. – Режим доступа: <https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-things>
- 1.157 S.88 - DIGIT Act // Электрон. дан. – Заглавие с екрана. – Режим доступа: <https://www.congress.gov/bill/115th-congress/senate-bill/88>
- 1.158 S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017// Электрон. дан. – Заглавие с екрана. – Режим доступа: <https://www.congress.gov/bill/115th-congress/senate-bill/1691>
- 1.159 H.R.6032 - SMART IoT Act // Электрон. дан. – Заглавие с екрана. – Режим доступа: <https://www.congress.gov/bill/115th-congress/house-bill/6032>
- 1.160 H.R.3388 - SELF DRIVE Act // Электрон. дан. – Заглавие с екрана. – Режим доступа: <https://www.congress.gov/bill/115th-congress/house-bill/3388>
- 1.161 TECHNOLOGY ASSESSMENT Internet of Things. Status and implications of an increasingly connected world// Электрон. дан. – Заглавие с екрана. – Режим доступа: <https://www.gao.gov/assets/690/684590.pdf>
- 1.162 Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD// Электрон. дан. – Заглавие с екрана. – Режим доступа: <https://www.gao.gov/products/GAO-17-668>
- 1.163 Internet of Things: Communities Deploy Projects by Combining Federal Support with Other Funds and Expertise// Электрон. дан. – Заглавие с екрана. – Режим доступа: <https://www.gao.gov/products/GAO-17-570>
- 1.164 Internet of Things: FCC Should Track Growth to Ensure Sufficient Spectrum Remains Available// Электрон. дан. – Заглавие с екрана. – Режим доступа: <https://www.gao.gov/products/GAO-18-71>
- 1.165 NSTAC Report to the President on the Internet of Things November 19, 2014// Электрон. дан. – Заглавие с екрана. – Режим доступа: <https://www.hsdl.org/?abstract&did=789743>

- 1.166 U.S. Dept. of Health and Human Services, Radio Frequency Wireless Technology in Medical Devices: Guidance for Industry and Food and Drug Administration Staff (Aug. 14, 2013), // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf>.
- 1.167 NHTSA, Vehicle-to-Vehicle Communications, // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.safercar.gov/v2v/index.html>.
- 1.168 Internet of Things. Privacy and Security in a Connected World, FTC (Jan. 2015), // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>
- 1.169 Careful Connections: Building Security in the Internet of Things // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf>
- 1.170 IoT Rules // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.ftc.gov/news-events/contests/iot-rules>,
- 1.171 IoT Home Inspector Challenge // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.ftc.gov/iot-home-inspector-challenge>
- 1.172 Internet of Things: FCC Should Track Growth to Ensure Sufficient Spectrum Remains Available // GAO -18-71, November 2017, 44 P., // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gao.gov/assets/690/688450.pdf> (обращение 28.09.2018).
- 1.173 DoD Policy Recommendations for The Internet of Things (IoT) December 2016 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.hsdl.org/?abstract&did=799676>
- 1.174 STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT) // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

- 1.175 Nouvelle France Industrielle - Internet des objets // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.entreprises.gouv.fr/politique-et-enjeux/projet-internet-des-objets-iot>
- 1.176 PROSPECTIVE Marchés des objets connectés à destination du grand public // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.entreprises.gouv.fr/files/files/directions_services/etudes-et-statistiques/prospective/Numerique/2018-05-24-Etude-objets-connectes.pdf
- 1.177 INTERNET DES OBJETS. NOUVELLE FRANCE INDUSTRIELLE, 14 décembre 2016 // Электрон. дан. – Заглавие с экрана. – Режим доступа:
- 1.178 La French Tech // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.entreprises.gouv.fr/agence-du-numerique/la-french-tech>
- 1.179 Инициатива French Tech – витрина Франции в области креативности и инноваций// Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.diplomatie.gouv.fr/ru/politique-etrangere/diplomatie-economique-et-commerce-exterieur/povyshenie-privlekatel-nosti-francii/article/la-french-tech-ambassade-de-la-creativite-et-de-l-innovation-a-la-francaise>
- 1.180 La French Tech // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.bpifrance.fr/A-la-une/Dossiers/La-French-Tech>
- 1.181 LE LABEL MÉTROPOLE FRENCH TECH à destination des écosystèmes de start-up les plus remarquables en France // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.economie.gouv.fr/files/files/PDF/french-tech_dossier-de-presse12112014.pdf
- 1.182 La feuille de route du Réseau Thématique #IOT #Manufacturing // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://iotmanufacturing.lafrenchtech.com/8/la-feuille-de-route>
- 1.183 LE RÉSEAU THÉMATIQUE FRENCH TECH #IoT #Manufacturing // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://iotmanufacturing.lafrenchtech.com/>

- 1.184 Pass French Tech // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.lafrenchtech.com/en-action/pass-french-tech>
- 1.185 ARCEP'S STRATEGIC REVIEW CONCLUSIONS AND PRIORITIES FOR 2016 /2017// Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.arcep.fr/uploads/tx_gspublication/strategic-review-conclusions-priorities-jan2016.pdf
- 1.186 Comprendre // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://iot.arcep.fr/comprendre/>
- 1.187 NOUVELLE-FRANCE-INDUSTRIELLE Financez vos projets // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.economie.gouv.fr/nouvelle-france-industrielle/financez-vos-projets>
- 1.188 Le Fonds Ambition Numérique // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://investissementsdavenir.bpifrance.fr/financement_des_entreprises/fsn_pme_fonds_ambition_numerique
- 1.189 Fonds Ambition Amorçage Angels (F3A) // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.bpifrance.fr/Qui-sommes-nous/Nos-metiers/Fonds-propres/Fonds-directs-Bpifrance/Capital-Innovation/Fonds-Ambition-Amorçage-Angels-F3A>
- 1.190 Derrière des levées de fonds record, une génération montante // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.lesechos.fr/09/10/2017/LesEchos/22546-115-ECH_derriere-des-levees-de-fonds-record--une-generation-montante.htm
- 1.191 Wavestone global survey on Deep Tech investments: Europe is Deep Tech and France is thriving // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.wavestone.com/en/trade-report/wavestone-global-survey-on-deep-tech-investments-europe-is-deep-tech-and-france-is-thriving/>
- 1.192 A BOOMING STARTUP ECOSYSTEM, la French Tech // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.lafrenchtech.com/sites/default/files/documents/ft-boomingstartup-175x240-corrige.pdf>
- 1.193 SIG FOX signe un contrat avec TDF et prévoit une levée de 100 m€ en 2013 SIGFOX french Internet to objects network

- company – Object hyperlinking ‘phylinking’ network // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.tactis.fr/nos-actualites/sig-fox-leve-10-millions-e-pour-deployer-son-reseau-bas-debit-dedie-aux-objets-communicants-en-france-et-a-linternational/>
- 1.194 Le Fonds Ambition Numérique du Programme d’Investissements d’Avenir (PIA) et Bpifrance via son fonds Large Venture participent à la levée de fonds de 100 M€ de Sigfox // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.bpifrance.fr/A-la-une/Actualites/Sigfox-leve-100-millions-d-euros-10011>
 - 1.195 Large Venture // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.bpifrance.fr/Qui-sommes-nous/Nos-metiers/Fonds-propres/Fonds-directs-Bpifrance/Capital-Innovation/Large-Venture>
 - 1.196 SIGFOX // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.crunchbase.com/organization/sigfox#section-overview>
 - 1.197 Sigfox expands its global network to 45 countries // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.sigfox.com/en/node/656>
 - 1.198 Why France may lead in the Internet of Things // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.idgconnect.com/abstract/29120/why-france-lead-internet-things?connect_token=cHJlbW11bV9hcnRpY2xlMTUzMjk0MDIzMA==
 - 1.199 IoT: Plus de 5 millions de produits achetés et 1 milliard € de revenu généré en 2017 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gfk.com/fr/insights/press-release/iot-plus-de-5-millions-de-produits-achetes-et-1-milliard-eur-de-revenu-genere-en-2017/>
 - 1.200 La French Tech. Rechercher Une Startup // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.lafrenchtech.com/annuaire>
 - 1.201 LES START-UP FRANÇAISES CHAMPIONNES À L’INTERNATIONAL Banque Populaire - Groupe BPCE // Электрон. дан. – Заглавие с экрана. – Режим доступа:
 - 1.202 10 Prédications Sur l’Internet Des Objets (IoT) En 2018 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.forbes.fr/technologie/10-predictions-sur-linternet-des-objets-iot-en-2018/?c%e2%80%a6>

- 1.203 WHAT CAN POLICYMAKERS LEARN FROM GERMANY'S INDUSTRIE 4.0 DEVELOPMENT STRATEGY? // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.unido.org/api/opentext/documents/download/11712839/unido-file-11712839>
- 1.204 Initiatives & Programs: “Digital Germany 2015” // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gtai.de/GTAI/Navigation/EN/invest,t=-initiatives--programs-digital-germany-2015,did=323412.html>
- 1.205 THE INTERNET OF THINGS – WHAT IS IT? // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Markets-by-industry-sector/industrie-4-0-internet-of-things-what-is-it.html>
- 1.206 Policy // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Why-germany/industrie-4-0-why-germany-policy.html>
- 1.207 Digital Transformation Monitor. Germany: Industrie 4.0// Электрон. дан. – Заглавие с экрана. – Режим доступа: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%204.0.pdf
- 1.208 The background to Plattform Industrie 4.0 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.plattform-i40.de/I40/Navigation/EN/ThePlattform/PlattformIndustrie40/plattform-industrie-40.html>
- 1.209 Map of Industry 4.0 Use Cases // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.plattform-i40.de/I40/Navigation/Karte/SiteGlobals/Forms/Formulare/EN/map-use-cases-formular.html>
- 1.210 Use cases // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.plattform-i40.de/I40/Navigation/EN/InPractice/UseCases/use-cases.html>
- 1.211 Testbeds // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.plattform-i40.de/I40/Redaktion/EN/Standardartikel/in-practice-testbeds.html>
- 1.212 International cooperation // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.plattform-i40.de/I40/Navigation/EN/InPractice/International/international.html>

- 1.213 2018 PROGRESS REPORT. Applying Industrie 4.0. Forward Thinking. Practical. Connected. // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.plattform-i40.de/I40/Redaktion/EN/Downloads/Publikation/hm-2018-fortschrittsbericht-eng.pdf?__blob=publicationFile&v=6
- 1.214 CYBER-PHYSICAL SYSTEMS // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Markets-by-industry-sector/industrie-4-0-internet-of-things-physical-systems,t=cyberphysical-systems-and-the-internet-of-things-data-and-services,did=1798536.html>
- 1.215 Federal Government-supported Smart Home // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gtai.de/GTAI/Navigation/EN/invest,t=federal-governmentsupported-smart-home-activities,did=324064.html?view=renderPdf>
- 1.216 ICT Strategy of the German Federal Government: Digital Germany 2015 // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.unapcict.org/ecohub/ict-strategy-of-the-german-federal-government-digital-germany-2015>
- 1.217 Digital Strategy 2025 // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.de.digital/DIGITAL/Redaktion/EN/Publikation/digital-strategy-2025.pdf?__blob=publicationFile&v=9
- 1.218 Тоганова Н. В. «Промышленность 4.0» в Германии: идеология, программа или интегральный взгляд на экономические процессы? // Интеграционные и дезинтеграционные процессы в мировой экономике и политике. – 2015. – С. 81-89.
- 1.219 Поручение Стратегического совета по инвестициям в новые индустрии при Министерстве промышленности и торговли Российской Федерации от 8 июля 2015 года № 76-МД/12.
- 1.220 ФРИИ начинает отбор стартапов для пилотных проектов в IoT // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.iidf.ru/media/articles/fond/frii-nachinaet-otbor-startapov-dlya-pilotnykh-proektov-v-iot/>
- 1.221 Инвестируем в проекты в области «Интернет вещей» // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.iidf.ru/startups/accelerator/iot>

- 1.222 ФРИИ инвестирует 43,8 млн рублей в 22 стартапа 13-го Акселератора // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.iidf.ru/media/articles/accelerator/frii-investiruet-43-8-mln-rublej-v-22-startapa-13-go-akseleratora-/>
- 1.223 «Ростелеком», ФРИИ и Фонд «Сколково» начинают отбор технологических стартапов // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.iidf.ru/media/articles/accelerator/rostelekom-frii-skolkovo-2017/>
- 1.224 Портфельные компании // Электрон. дан. – Заглавие с экрана. – Режим доступа: https://www.iidf.ru/fond/projects/?NUMBER_F=14
- 1.225 Сэйфнет // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.nti2035.ru/markets/safenet>
- 1.226 Перечень центров компетенций. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.nti2035.ru/technology/competence>
- 1.227 Фонд НТИ привлек первых инвесторов // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.rvc.ru/press-service/news/company/130132/>
- 1.228 РВК начинает отбор управляющего товарища для венчурного фонда НТИ // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.rvc.ru/press-service/news/company/117514/>

Раздел 2

- 2.1 International Organization for Standardization // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.iso.org/members.html>
- 2.2 International Electrotechnical Commission // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.iec.ch/about/profile/members.htm>
- 2.3 International Telecommunication Union // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.itu.int/en/about/Pages/default.aspx>
- 2.4 Уткин Н.А. Цифровая экономика и кибер-физические системы // Вестник Федерального агентства по техническому регулированию и метрологии. 2017. № 3.
- 2.5 Проект международного стандарта ISO/IEC CD 20924 Information technology -- Internet of Things (IoT) -- Definition and vocabulary.

- 2.6 Проект международного стандарта ISO/IEC 21823-1 CD Internet of things (IoT) -- Interoperability for internet of things systems -- Part 1: Framework
- 2.7 Международный стандарт ISO/IEC 30141:2018 Internet of Things (IoT) -- Reference Architecture.
- 2.8 Федеральный закон «О стандартизации в Российской Федерации» от 29.06.2015 г. N 162-ФЗ.
- 2.9 ГОСТ Р 57564-2017 «Организация и проведение работ по международной стандартизации в Российской Федерации».
- 2.10 ГОСТ Р 1.1 «Стандартизация в Российской Федерации. Технические комитеты по стандартизации. Порядок создания и деятельности».
- 2.11 Internet of Things (IoT): Preliminary report 2014. ISO/IEC JTC 1, 2015.
- 2.12 IoT 2020: Smart and secure IoT platform. White Paper. Geneva: IEC, 2016.
- 2.13 Намиот Д. Е. и др. Стандарты в области больших данных // International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 11.
- 2.14 Aerts D. Quantum structure in cognition //Journal of Mathematical Psychology. – 2009. – Т. 53. – №. 5. – С. 314-348.
- 2.15 NIST Big Data Information // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.nist.gov/el/cyber-physical-systems/big-data-pwg>.
- 2.16 He K. et al. Delving deep into rectifiers: Surpassing human-level performance on imagenet classification // Proceedings of the IEEE international conference on computer vision. – 2015. – С. 1026-1034.
- 2.17 Майер-Шенбергер В., Кукьер К. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим // М.: Манн, Иванов и Фербер. – 2014.
- 2.18 Zeleny M. Management support systems: Towards integrated knowledge management //Human systems management. – 1987. – Т. 7. – №. 1. – С. 59-70.
- 2.19 Ackoff R. L. From data to wisdom //Journal of applied systems analysis. – 1989. – Т. 16. – №. 1. – С. 3-9.

- 2.20 Пальчунов Д. Е., Яхъяева Г. Э. Нечеткие алгебраические системы // Вестник Новосибирского государственного университета. Серия: математика, механика, информатика. — 2010. — Т. 10. — № 3. — С. 76–93.
- 2.21 S.S. Goncharov, D.I. Svidirenko. Semantic modeling and hybrid models // Proceedings of Siberian Symposium on Data Science and Engineering. Preprint. — 2018, Oct. — pp.30-31.
- 2.22 Coecke B., Sadrzadeh M., Clark S. J. Mathematical foundations for a compositional distributional model of meaning // Linguistic Analysis. — 2010. — Т. 36. — №. 1. — С. 345-384.
- 2.23 Zhang P. et al. A Quantum Many-body Wave Function Inspired Language Modeling Approach // Proceedings of the 27th ACM International Conference on Information and Knowledge Management. — ACM, 2018. — С. 1303-1312.
- 2.24 Витяев Е. Е. Принципы работы мозга, содержащиеся в теории функциональных систем ПК Анохина и теории эмоций ПВ Симонова // Нейроинформатика (электронный рецензируемый журнал). — 2008. — Т. 3. — № 1. — С. 25–78.
- 2.25 2018 Low-Power Image Recognition Challenge // Электрон. дан. — Заглавие с экрана. — Режим доступа: <https://arxiv.org/ftp/arxiv/papers/1810/1810.01732.pdf>

Раздел 3

- 3.1 Астахова Е., Партида Э. Основные тенденции развития агропромышленного комплекса в условиях рыночной экономики. // RJOAS, 10(70) – 2017.
- 3.2 Обзор рынка сельского хозяйства. Исследовательский центр «Делойт» в СНГ, Москва, 2017 // Электрон. дан. — Заглавие с экрана. — Режим доступа: <https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/consumer-business/russian/snapshot-of-the-russian-2017-agroindustry-rus.pdf>
- 3.3 База данных поиска поддержанных грантов, патентов, статей Dimensions // Электрон. дан. — Режим доступа: URL: <https://www.dimensions.ai/>
- 3.4 Global ag tech startup investments rise 29 percent in 2017–study // Электрон. дан. — Заглавие с экрана. — Режим

- доступа: <https://www.reuters.com/article/agriculture-tech-investment/global-ag-tech-startup-investments-rise-29-percent-in-2017-study-idUSL2N1QO1PW>
- 3.5 Farm Computer Usage and Ownership, August 2017, USDA // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://usda.mannlib.cornell.edu/usda/current/FarmComp/FarmComp-08-18-2017_correction.pdf
- 3.6 Итоги Всероссийской сельскохозяйственной переписи 2016 года (в 8 томах) Том 2. Число объектов Всероссийской сельскохозяйственной переписи 2016 года. Трудовые ресурсы и их характеристика // Электрон. дан. – Заглавие с экрана. – Режим доступа: http://www.gks.ru/free_doc/new_site/business/sx/vsxp2016/VSPX_2016_T_2_web.pdf
- 3.7 Semios. Integrated Pest Management // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://semios.com/ipm/>
- 3.8 Katsoulas, N., Bartzanas, T., & Kittas, C. Online professional irrigation scheduling system for greenhouse crops. // Acta Hortic. 1154 – 2017.– p. 221-228.
- 3.9 Plantlink Welcome to the connected plant world. USDA // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://myplantlink.com/>
- 3.10 GetSenso. Enterprise IoT Solutions. Need for Monitoring Greenhouse // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.getsenso.com/iot-solution/greenhouse-monitoring/>
- 3.11 Monnit Remote Monitoring Systems for Greenhouse Monitoring // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.monnit.com/solutions/greenhouse-monitoring>
- 3.12 Sensaphone. Greenhouse remote monitoring systems // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.sensaphone.com/industries/greenhouse.php>
- 3.13 Указ Президента Российской Федерации от 07.05.2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.kremlin.ru/acts/bank/43027>

- 3.14 Внедрение Интернета Вещей принесет АПК 469 млрд рублей // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.agroinvestor.ru/technologies/news/28325-vnedrenie-interneta-veshchey-prineset-apk-469-mlrd-rubley/>
- 3.15 Портал Федеральных государственных образовательных стандартов высшего образования. Профессиональные стандарты СЕЛЬСКОЕ ХОЗЯЙСТВО // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://fgosvo.ru/docs/101/69/2/13>
- 3.16 Исаева И.А. Защита данных в беспроводных сетях связи// Мир Телекома – 2014 – №1 – С.66-70.
- 3.17 Соколов М. Н., Смолянинова К. А., Якушева Н. А. Проблемы безопасности интернет вещей: обзор //Вопросы кибербезопасности. – 2015. – №. 5 (13). – С.32-35.
- 3.18 Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей. // М.: Горячая линия - Телеком – 2008.
- 3.19 Gou Q. et al. Construction and strategies in IoT security system //Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCoM), IEEE International Conference on and IEEE Cyber, Physical and Social Computing. – IEEE, 2013. – pp. 1129-1132.
- 3.20 Zhang B., Zou Z., Liu M. Evaluation on security system of internet of things based on fuzzy-AHP method //E-Business and E-Government (ICEE), 2011 International Conference on. – IEEE, 2011. – pp. 1-5.
- 3.21 Zhang Z. K. et al. IoT security: ongoing challenges and research opportunities //Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. – IEEE, 2014. – pp. 230-234
- 3.22 Fernandez E. B., VanHilst M. An overview of WiMAX security //WiMAX. – CRC Press, 2007. – pp. 201-209.
- 3.23 Жуков А. Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. – 2015. – №. 1 (9) – С. 26-43.
- 3.24 Paar C. Lightweight Cryptography for Ubiquitous Computing. Securing Cyberspace Workshop IV: Special purpose hardware for cryptography – Attacks and Applications. University of California at Los Angeles, December 4, 2006 // Электрон. дан. – Заглавие с экрана. – Режим доступа:

- https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/vortrag/lwc_ucla_dec2006.pdf
- 3.25 Perspectives on Industrial IoT: Gartner and PTC. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://medium.com/diskerrett/perspectives-on-industrial-iot-gartner-and-ptc-727bc5273a53>
 - 3.26 Predictive Maintenance Drives IoT in Manufacturing Operations. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gartner.com/doc/3858470/report-highlight-market-trends-predictive>
 - 3.27 Predictive Maintenance Drives IoT in Manufacturing Operations. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.gartner.com/doc/3856379/market-trends-predictive-maintenance-drives>
 - 3.28 Maintenance optimization. Airplane health management. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.boeing.com/resources/boeingdotcom/commercial/services/assets/brochure/airplanehealthmanagement.pdf>
 - 3.29 S. Alestra, C. Bordry, C. Brand, E. Burnaev, P. Erofeev, P. A., and C. Silveira-Freixo. Application of rare event anticipation techniques to aircraft health management. In *Advanced Materials Research*, volume 1016, pages 413-417. Trans Tech Publ, 2014.
 - 3.30 S. Alestra, C. Bordry, C. Brand, E. Burnaev, P. Erofeev, A. Papanov, and C. Silveira-Freixo. Evolution of aircraft maintenance and logistics based on prognostic and health management technology. In *Proceedings of the joint WCCM-ECCM-ECFD 2014 Congress*, 20-25 July, Barcelona, Spain, page 12, 2014.
 - 3.31 J. Dai and H. Wang. Evolution of aircraft maintenance and logistics based on prognostic and health management technology. In *Lecture Notes in Electrical Engineering. Proceedings of the First Symposium on Aviation Maintenance and Management-Volume II*, volume 297, pages 665-672. Springer, 2014.
 - 3.32 T. Shen, F. Wan, W. Cui, and B. Son. Application of prognostic and health management technology on aircraft fuel system. In *IEEE Proceedings of 2010 Prognostics and System Health Management Conference*. 12-14 Jan. Macao, pages 1-7. IEEE, 2010.

- 3.33 S7 Airlines внедряет машинное обучение в техобслуживание самолетов. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.s7.ru/ru/about/news/s7-airlines-vnedryaet-mashinnoe-obuchenie-v-tekhobsluzhivanie-samoletov/>
- 3.34 L. Tegtmeier. Math and maintenance. Aviation Week and Space Technology, 174(39), 2012.
- 3.35 Компания DATADVANCE: ПО для анализа данных, инженерной оптимизации и предсказательного моделирования. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://www.dataadvance.net/ru/>
- 3.36 E. Burnaev, P. Erofeev, A. Papanov. Influence of Resampling on Accuracy of Imbalanced Classification. Proc. SPIE9875, Eighth International Conference on Machine Vision, 987521 (December 8, 2015); 5 P.
- 3.37 D. Smolyakov, A. Korotin, P. Erofeev, A. Papanov, E. Burnaev. Meta-Learning for Resampling Recommendation Systems. Proc. 11th International Conference on Machine Vision, 2018.
- 3.38 Barnett V. The study of outliers: purpose and model // Journal of the Royal Statistical Society. Series C (Applied Statistics). – 1978. – vol. 27 – no. 3 – pp. 242-250.
- 3.39 Banerjee A. et al. Anomaly detection: A tutorial //Tutorial SIAM Conf. on Data Mining. – 2008.
- 3.40 L. Tarassenko, P. Hayton, N. Cerneaz, and M. Brady. Novelty detection for the identification of masses in mammograms. In Proceedings of the 4th International Conference on Artificial Neural Networks, pages 442-447. IET, 1995.
- 3.41 L. Clifton, D. Clifton, P. Watkinson, and L. Tarassenko. Identification of patient deterioration in vital-sign data using one-class support vector machines. In Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS), pages 125-131. IEEE, 2011.
- 3.42 J.A. Quinnand, C.K. Williams. Known unknowns: Novelty detection in condition monitoring. In Pattern Recognition and Image Analysis, volume 4477, pages 1-6. Springer, 2007.
- 3.43 L. Tarassenko, D. Clifton, P. Bannister, S. King, and D. King. Novelty detection. Encyclopedia of Structural Health Monitoring, 2009.
- 3.44 C. Surace and K. Worden. Novelty detection in a changing environment: a negative selection approach. Mechanical Systems and Signal Processing, 24 (4): 1114-1128, 2010.

- 3.45 A. Patcha and J. Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer networks*, 51(12): 3448-3470, 2007.
- 3.46 V. Jyothsna, V. Prasad, K. Prasad, and A. Prasard. A review of anomaly based intrusion detection systems. *International Journal of Computer Applications*, 28 (7): 26-35, 2011.
- 3.47 V. Barnett and T. Lewis. *Outliers in Statistical Data*, volume 286. Wiley and Sons, 1994.
- 3.48 F. Grubbs. Procedures for detecting outlying observations in samples. *Technometrics*, 11 (1): 1-21, 1969.
- 3.49 C. Aggarwal and S. Philip. Outlier detection with uncertain data. In *Proceedings of the SIAM International Conference on Data Mining*, volume 8, pages 483-493. SIAM, 2008
- 3.50 C. Chow. On optimum recognition error and reject tradeoff. *Information Theory, IEEE Transactions on*, 16 (1): 41-46, 1970.
- 3.51 D. Scott. *Multivariate density estimation: theory, practice, and visualization*. John Wiley & Sons, 2008.
- 3.52 V. Chandola, A. Banerjee, and V. Kumar. Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41 (3): 1-58, 2009.
- 3.53 M. Markou and S. Singh. Novelty detection: a review—part 1: statistical approaches. *Signal processing*, 83 (12): 2481-2497, 2003.
- 3.54 D. Miljkovic. Review of novelty detection methods. In *Proceedings of the 33rd International Convention (MIPRO)*, pages 593-598, 2010.
- 3.55 R. Duda, P. Hart, and D. Stork. *Pattern classification*. John Wiley & Sons, 2001.
- 3.56 V. Hautamaki, I. Karkkainen, and P. Franti. Outlier detection using k-nearest neighbor graph. In *Proceedings of the 17th International Conference on Pattern Recognition, ICPR 2004*, volume 3, pages 430-433, 2004.
- 3.57 J. Zhang and H. Wang. Detecting outlying subspaces for high-dimensional data: the new task, algorithms, and performance. *Knowledge and information systems*, 10 (3): 333-355, 2006.
- 3.58 M. Breunig, H. Kriegel, R. Ng, and J. Sander. LOF: identifying density-based local outliers. In *Proceedings of the ACM SIGMOD International Conference on Management of Data*, volume 29, pages 93-104. ACM, 2000.

- 3.59 A. Srivastava. Enabling the discovery of recurring anomalies in aerospace problem reports using high-dimensional clustering techniques. In Proceedings of the IEEE Aerospace Conference, 2006, pages 1-17. IEEE, 2006.
- 3.60 A. Srivastava and B. Zane-Ulman. Discovering recurring anomalies in text reports regarding complex space systems. In Proceedings of the IEEE Aerospace Conference, pages 3853-3862, 2005.
- 3.61 M. Augusteiijn and B. Folkert. Neural network classification and novelty detection. *International Journal of Remote Sensing*, 23 (14): 2891-2902, 2002.
- 3.62 S. Hawkins, H. He, G. Williams, and R. Baxter. Outlier detection using replicator neural networks. In *Data warehousing and knowledge discovery*, volume 2454, pages 113-123. Springer, 2002.
- 3.63 G. Williams, R. Baxter, H. He, S. Hawkins, and L. Gu. A comparative study of RNN for outlier detection in data mining. In Proceedings of the IEEE International Conference on Data Mining, pages 709-712. IEEE, 2002.
- 3.64 I. Jolliffe. Principal component analysis. Wiley Online Library, 2002.
- 3.65 H. Dutta, C. Giannella, K. D. Borne, and H. Kargupta. Distributed top-k outlier detection from astronomy catalogs using the DEMAC system. In Proceedings of the 7th SIAM International Conference on Data Mining, pages 473-478. IEEE, 2007.
- 3.66 M. Shyu, S. Chen, K. Sarinnapakorn, and L. Chang. A novel anomaly detection scheme based on principal component classifier. Technical report, DTIC Document, 2003.
- 3.67 H. Hoffmann. Kernel pca for novelty detection. *Pattern Recognition*, 40(3): 863-874, 2007.
- 3.68 B. Scholkopf, A. Smola, and K. Muller. Nonlinear component analysis as a kernel eigenvalue problem. *Neural computation*, 10(5): 1299-1319, 1998.
- 3.69 L. Manevitz and M. Yousef. One-class svms for document classification. *Journal of Machine Learning Research*, 2: 139-154, 2002.
- 3.70 B. Scholkopf, R. Williamson, A. Smola, J. Shawe-Taylor, J. Platt, et al. Support vector method for novelty detection. In *NIPS*, volume 12, pages 582-588. Citeseer, 1999.

- 3.71 D. Tax and R. Duin. Support vector domain description. Pattern recognition letters, 20(11): 1191-1199, 1999.
- 3.72 E. Burnaev, P. Erofeev, D. Smolyakov. Model Selection for Anomaly Detection // Proc. SPIE 9875, Eighth International Conference on Machine Vision, 987525 (December 8, 2015)
- 3.73 Michele Basseville, Igor Nikiforov. Detection of Abrupt Changes - Theory and Application. Prentice Hall, Inc., pp.550, 1993.
- 3.74 Burnaev E., Ishimtsev V., Bernstein A., Nazarov I. Conformal k-NN Anomaly Detector for Univariate Data Streams // The 6th Symposium on Conformal and Probabilistic Prediction with Applications (COPA) 2017. Proceedings of Machine Learning Research, 60:213-227, 2017.
- 3.75 Volkhonsky D., Burnaev E., Nouretdinov I., Gammerman A., Vovk V. Inductive Conformal Martingales for Change-Point Detection // The 6th Symposium on Conformal
- 3.76 Artemov A., Burnaev E. Detecting Performance Degradation of Software-Intensive Systems in the Presence of Trends and Long-Range Dependence // 16th International Conference on Data Mining Workshops (ICDMW), IEEE Conference Publications, pp. 29 - 36, 2016. DOI: 10.1109/ICDMW.2016.0013.
- 3.77 Artemov A., Burnaev E. Ensembles of Detectors for Online Detection of Transient Changes // Proc. SPIE 9875, Eighth International Conference on Machine Vision, 98751Z (December 8, 2015)
- 3.78 Alexey Artemov, Evgeny Burnaev and Andrey Lokot. Nonparametric Decomposition of Quasi-periodic Time Series for Change-point Detection // Proc. SPIE 9875, Eighth International Conference on Machine Vision, 987520 (December 8, 2015); 5 P.
- 3.79 L Chapman, DT Young, CL Muller, P Rose, C Lucas, and J Walden. Winter road maintenance and the internet of things. In Proceedings of the 17th International Road Weather Conference, volume 18, 2014.
- 3.80 Jonathan J Rutz and Chris V Gibson. Integration of a road surface model into nws operations. Bulletin of the American Meteorological Society, 94 (10): 1495-1500, 2013.
- 3.81 Т.В. Самодурова. Оперативное управление зимним содержанием дорог: Научные основы. Изд-во Воронеж. гос. Ун-та, 2003.

- 3.82 Т.В. Самодурова. Математические модели для оценки выходных параметров системы оперативного управления зимним содержанием дорог, Т. 1, 2003.
- 3.83 Ben C Bernstein, Jamie K Wol, and W Myers. Verification of the road weather forecast system run during the 2003 demonstration at the Iowa department of transportation. In Sixth Annual Symposium on Snow Removal and Ice Control Technology, Transportation Research Board, Spokane, WA, pages 109-126, 2004.
- 3.84 Louis-Philippe Crevier and Yves Delage. Metro: A new model for road-condition forecasting in Canada. *Journal of Applied Meteorology*, 40 (11): 2026-2037, 2001.
- 3.85 Tina M Greenfield, Eugene S Takle, Brian J Tentinger, Jose J Alamo, Dennis Burkheimer, and Diane McCauley. Bridge frost occurrence and prediction. In Sixth Annual Symposium on Snow Removal and Ice Control Technology, Transportation Research Board, Spokane, WA, pages 391-398, 2004.
- 3.86 CL Meng. A numerical forecast model for road meteorological services in Beijing. In 17-th SIRWEC Conference, Proceedings. Andorra, 2014.
- 3.87 Duick T Young, Lee Chapman, Catherine L Muller, Xiao-Ming Cai, and CSB Grimmond. A low-cost wireless temperature sensor: Evaluation for use in environmental monitoring applications. *Journal of Atmospheric and Oceanic Technology*, 31 (4): 938-944, 2014.
- 3.88 Jiandong Zhao, Hongqiang Wu, and Liangliang Chen. Road surface state recognition based on svm optimization and image segmentation processing. *Journal of Advanced Transportation*, 2017.
- 3.89 Masahiko Aki, Teerapat Rojanaarpa, Kimihiko Nakano, Yoshihiro Suda, Naohito Takasuka, Toshiki Isogai, and Takeo Kawai. Road surface recognition using laser radar for automatic platooning. *IEEE Transactions on Intelligent Transportation Systems*, 17 (10): 2800-2810, 2016.
- 3.90 V. Garcia-Font, C. Garrigues, et al.: A comparative study of anomaly detection techniques for smart city wireless sensor networks. *Sensors* 16 (6) (2016) 868.
- 3.91 Brereton R. G., Lloyd G. R. Support vector machines for classification and regression // *Analyst*. – 2010. – Т. 135. – №. 2. – pp. 230-267.

- 3.92 Hastie, T., Tibshirani, R., Friedman, J. (2001). The Elements of Statistical Learning. New York, NY, USA: Springer New York Inc.
- 3.93 Novelty detection and outlier detection with Scikit // Электрон. дан. – Заглавие с экрана. – Режим доступа: <http://www.hongyusu.com/imt/technology/novelty-detection.html>
- 3.94 D. Smolyakov, N. Sviridenko, E. Burikov, E. Burnaev. Anomaly Pattern Recognition with Privileged Information for Sensor Fault Detection. 8-th IAPR TC3 Workshop, ANNPR 2018, Siena, Italy, September 19–21, 2018, Springer LNCS Proceedings, Vol. 11081, pp. 320-332.
- 3.95 E. Burnaev, D. Smolyakov. One-Class SVM with Privileged Information and Its Application to Malware Detection // 16th International Conference on Data Mining Workshops (ICDMW), IEEE Conference Publications, pp. 273 - 280, 2016. DOI: 10.1109/ICDMW.2016.0046
- 3.96 Zbynek Sokol, Petr Zacharov, Pavel Sedlak, Jiri Hosek, Vojtech Bliznak, Zuzana Chladova, Petr Pesice, and Miroslav Skuthan. First experience with the application of the metro model in the Czech Republic. Atmospheric research, 143:1-16, 2014.
- 3.97 A Khalifa, M Marchetti, L Bouilloud, E Martin, M Bues, and K Chancibaut. Accounting for anthropic energy flux of traffic in winter urban road surface temperature simulations with teb model. Geoscientific Model Development Discussions, 8(6), 2015.
- 3.98 60. Lee Chapman. Probabilistic road weather forecasting. In Proceedings of the Standing International Road Weather Conference (SIRWEC'12), 2012.
- 3.99 Veronica J Berrocal, Adrian E Raftery, Tilmann Gneiting, and Richard C Steed. Probabilistic weather forecasting for winter road maintenance. Journal of the American Statistical Association, 105 (490): 522-537, 2010.
- 3.100 Rok Krsmanc, Alenka Sajn Slak, and Janez Demsar. Statistical approach for forecasting road surface temperature. Meteorological Applications, 20 (4): 439-446, 2013.
- 3.101 Mohamed Akram Zaytar and Chaker El Amrani. Sequence to sequence weather forecasting with long short-term memory recurrent neural networks. Int J Comput Appl, 143 (11), 2016.

- 3.102 Andre Gensler, Janosch Henze, Bernhard Sick, and Nils Raabe. Deep learning for solar power forecasting - an approach using autoencoder and lstm neural networks. In Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on, pages 002858-002865. IEEE, 2016.
- 3.103 R Martin, Ricardo Aler, Jose Maria Valls, and Ines Maria Galvan. Machine learning techniques for daily solar energy prediction and interpolation using numerical weather models. *Concurrency and Computation: Practice and Experience*, 28 (4): 1261-1274, 2016.
- 3.104 Siyuan Lu, Youngdeok Hwang, Ildar Khabibrakhmanov, Fernando J Marianno, Xiaoyan Shao, Jie Zhang, Bri-Mathias Hodge, and Hendrik F Hamann. Machine learning based multi-physical-model blending for enhancing renewable energy forecast-improvement via situation dependent error correction. In Control Conference (ECC), 2015 European, pages 283-290, IEEE, 2015.
- 3.105 Faranak Hosseini, SM Kamal Hossain, Liping Fu, Marc Johnson, and Yuheng Fei. Prediction of pavement surface temperature using meteorological data for optimal winter operations in parking lots. In Cold Regions Engineering 2015, pages 440-451, 2015.
- 3.106 Scikit-learn: machine learning in Python. // Электрон. дан. – Заглавие с экрана. – Режим доступа: <https://scikit-learn.org/stable/>

ISBN 978-5-6042289-0-6



9 785604 228906