МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ № _____

Москва

Об утверждении Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации

В целях реализации национальной программы «Цифровая экономика Российской Федерации»,

ПРИКАЗЫВАЮ:

Утвердить прилагаемую Концепцию построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации.

Врио министра О.А. Иванов

Приложение 1

Концепция построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации

Москва 2019

Содержание

Введение

Настоящая Концепция разработана в соответствии с целями и задачами, установленными указом Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024» и программой «Цифровая экономика Российской Федерации», утвержденной Распоряжением Правительства Российской Федерации от 28 июля 2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»» (далее – Программа). Эффективное развитие рынков и отраслей (сфер деятельности) в цифровой экономике возможно только при наличии развитых платформ, технологий, институциональной и инфраструктурной сред.

Цифровая экономика представляет собой хозяйственную деятельность, ключевым фактором производства в которой являются данные в цифровой форме, и способствующую формированию информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений, развитию информационной инфраструктуры Российской Федерации, созданию и применению российских информационно-телекоммуникационных технологий, а также формированию новой технологической основы для социальной и экономической сферы.

Развитие сетей связи, обеспечивающие потребности экономики по сбору и передаче данных государства, бизнеса и граждан с учетом технических требований, предъявляемых цифровыми технологиями, а также внедрение цифровых платформ работы с данными для обеспечения потребностей власти, бизнеса и граждан являются одними из основных целей направления, касающегося информационной инфраструктуры.

«Интернет вещей» (IoT) является совокупностью сетей межмашинных коммуникаций и систем хранения/обработки больших данных, в которых за счет подключения датчиков и актуаторов (исполнительных механизмов) к сети реализуется цифровизация различных процессов и объектов. Использование полученных данных позволяет проводить оптимизацию

процессов и объектов на базе новых алгоритмов, а обратная связь с актуаторами позволяет реализовывать эту оптимизацию на практике без существенных затрат. Внедрение «Интернета вещей» позволяет через цифровизацию процессов и объектов снизить расходы и повысить производительность труда практически в любой отрасли.

В настоящее время устройства IoT подключаются через широкий набор радиотехнологий в рамках устройств малого радиуса действия, в том числе по таким стандартам как IEEE 802.11 и 802.15, а также с использованием сетей сотовой подвижной связи стандартов GSM, UMTS и LTE. Тем не менее, в дополнение к данным существующим решениям был разработан новый класс радиотехнологий для подключения широкого круга устройств IoT, в том числе в самых сложных условиях размещения таких устройств, оптимизированных для обслуживания различных датчиков и сенсоров, работающих долгое время от аккумуляторов. Данный класс радиотехнологий получил название узкополосные беспроводные сети связи «Интернета вещей», которые содержат в себе беспроводные радиоинтерфейсы передачи небольших по объёму данных на значительные расстояния, в первую очередь, для распределённых сетей телеметрии, межмашинного взаимодействия и сбора информации.

Узкополосные беспроводные сети связи «Интернета вещей» являются частью сетей передачи данных общего пользования (далее - СПД ОП) и выделенных сетей связи.

Выделение узкополосных беспроводных сетей связи «Интернета вещей» в отдельный объект рассмотрения определяется технологическими, экономическими и организационными особенностями, требующими создания условий для развития.

Ключевыми особенностями узкополосных беспроводных сетей связи «Интернета вещей» являются: низкая стоимость услуг в пересчете на одно устройство, низкие потребности в пропускной способности на одно устройство, низкое энергопотребление устройств, необходимость обеспечения высокой надежности и достоверности доставки сообщений

управления процессами и устройствами, требования к безопасности связи, сохранению персональных данных и пр.

В настоящее время на рынке инфокоммуникационных технологий наблюдаются следующие тенденции: увеличение объёма устройств и сервисов IoT, рост числа неуправляемых пользователем информационных процессов, увеличение влияния этих процессов на повседневную жизнь государства и пользователей, снижение маржинальности рынка телекоммуникационных услуг и другие требуют создания и развития рынка «Интернета вещей» в Российской Федерации за счет определения состава и правил поведения его участников. Существующее состояние нормативно-правовой базы отрасли не позволяет определить состав и правила поведения участников появляющегося рынка услуг интернета вещей на инфраструктуре узкополосных беспроводных сетей.

Отсутствие правил поведения приводит к возможностям потери управляемости сетями IoT, нарушением сфер безопасности личности, предприятий, Государства, возможности потери рынка IoT для экономики из-за поглощения услугами зарубежных операторов, оборудованием и программным обеспечением иностранного производства и предоставления услуг из-за пределов Российской Федерации за счет недобросовестной конкуренции.

Целью Концепции создания и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации на период до 2030 года является описание условий для создания и развития рынка услуг связи «Интернета вещей». Основной задачей государственного регулирования рынка беспроводных сетей связи «Интернета вещей» является создание такой системы регулирования, которая будет создавать условия для открытой и эффективной конкуренции, будет направлена на своевременное создание и развитие новых услуг в этой области и улучшение качества предоставляемых услуг, предоставления равного доступа к информационным ресурсам, защиты интересов общества и государства.

Обозначения и сокращения

АС - Абонентская станция

БД - База данных

БС - Базовая станция

ВРНС - Воздушная радионавигационная служба

ГКРЧ - Государственная комиссия по радиочастотам

ЕИТС – единая информационная телекоммуникационная среда

ЖКХ - Жилищно-коммунальное хозяйство

ИБ - Информационная безопасность

ИКТ - Информационно-телекоммуникационные технологии

Линия вверх, восходящий канал (UL) - Направление передачи от абонентской станции к базовой станции

Линия вниз, нисходящий канал (DL) - Направление передачи от базовой станции к абонентской станции

МСЭ - Международный союз электросвязи

МСЭ-Т - Сектор стандартизации электросвязи Международного союза электросвязи

ОРМ - Оперативно-розыскные мероприятия

ПО - Программное обеспечение

РИЧ – разрешение на использование радиочастот или радиочастотных каналов

РЛС – Радиолокационная служба

РСБН - Радиотехническая система ближней навигации

РЧС – радиочастотный спектр

РЭС - Радиоэлектронное средства

СПД ОП – система передачи данных общего пользования

ССОП – сеть связи общего пользования

ТМС – телематическая сеть

ЦОД - Центр обработки данных

ЭИМ - Эквивалентная излучаемая мощность

ЭКБ - Электронно-компонентная база

ЭМС - Электромагнитная совместимость

3GPP - 3rd Generation Partnership Project (Консорциум, разрабатывающий спецификации для мобильной телефонии)

5G/IMT-2020 - Стандарт пятого поколения мобильной связи

API - Application programming interface (Интерфейс прикладного программирования)

Bluetooth - Спецификация беспроводных персональных сетей

AS - Access Stratum (Алгоритмы, устанавливающие безопасность на уровне сети радиодоступа)

CAN - Controller Area Network (Шина сети локальных контроллеров)

CEN - Comité Européen de Normalisation (Европейский комитет по стандартизации)

DDoS атака - Distributed Denial of Service attack (Комплекс действий, способный полностью или частично вывести из строя интернет-ресурс)

DOA - Digital object Architecture (Цифровая архитектура объекта)

DOI - Digital object identifier (Цифровой идентификатор объекта – стандарт обозначения представленной в сети информации об объекте)

DONA - Digital object Numbering Authority (Ассоциация управления цифровыми объектами)

DSL - Digital subscriber line (Цифровая абонентская линия)

EC-GSM - Extended Coverage GSM (Расширение существующего стандарта GSM для внедрения сетей IoT)

Edge computing - Периферийные (граничные) вычисления

Ethernet - Технология построения локальной вычислительной сети

ETSI - European Telecommunications Standards Institute (Европейский институт по стандартизации в области телекоммуникаций)

eUICC - Embedded Universal Integrated Circuit Card (Встроенная универсальная интегральная схема)

GSM - Global System for Mobile Communications (Стандарт сотовой подвижной связи второго поколения)

GSMA - Ассоциация GSM

HSS - Home Subscriber Server (Сервер домашних абонентов)

ICANN - Internet Corporation for Assigned Names and Numbers (Корпорация по управлению доменными именами и IP-адресами)

IEEE - Institute of Electrical and Electronics Engineers (Институт инженеров электротехники и электроники)

IETF RFC 4282 - Internet Engineering Task Force Request for Comments (Документ из серии пронумерованных информационных документов Интернета инженерного совета Интернета)

IMSI - International Mobile Subscriber Identity (Международный идентификатор мобильного абонента)

IoT - Internet of Things (Интернет вещей)

IP - Internet Protocol (Межсетевой протокол)

ITS - Intelligent transportation system (Интеллектуальная транспортная система)

LBT - Listen before talk (Режим прослушивания перед излучением)

LPWAN - Low-power Wide-area Network (Энергоэффективная сеть дальнего радиуса действия)

LTE - Long-Term Evolution (Стандарт сотовой подвижной связи четвертого поколения)

LTE-eMTC - Long-Term Evolution enhanced Machine-Type Communications (Технология узкополосных беспроводных сетей связи «Интернета вещей» в выделенных для подвижной радиотелефонной связи полосах радиочастот на основе стандарта LTE)

LTE-V2X - Long-Term Evolution Vehicle-to-Everytning (Технология обмена данными между автомобилем и другими объектами дорожной инфраструктуры на основе стандарта сотовой подвижной связи четвертого поколения)

M2M - Machine-to-Machine (Межмашинное взаимодействие)

MAC - Media Access Control (Управление доступом к среде)

MFF - M2M Form Factor (Форм-фактор для межмашинного взаимодействия)

MME - Mobility Management Entity (Узел управления мобильностью сети)

MNC - Mobile Network Code (Код мобильной сети)

MTC-IFW - Machine Type Communication Interworking Function (Блок, используемый для организации сторонних приложений в рамках межмашинной связи и обеспечивающий аутентификацию)

MSISDN - Mobile Subscriber Integrated Services Digital Number (Номер мобильного абонента цифровой сети с интеграцией служб)

MVNO - Mobile Virtual Network Operator (Виртуальный оператор сотовой связи)

NAS - Non-Access Stratum (Алгоритмы, устанавливающие безопасность на уровне опорной сети)

NB-IoT - NarrowBand Internet of Things (Узкополосный режим работы сетей стандарта LTE и его последующих модификаций)

OID - Object Identifier (Идентификатор объекта)

OneM2M - Консорциум, разрабатывающий спецификации для технологий межмашинного взаимодействия и «Интернета вещей»

SCEF - Service Capability Exposure Function (Функция экспонирования возможностей услуги)

SCS - Service Capability Server (Блок, используемый для организации сторонних приложений в рамках межмашинной связи и обеспечивающий аутентификацию)

SDR - Software-Defined Radio (Программно-определяемая радиоподсистема)

SIM - Subscriber Identification Module (Модуль идентификации абонента)

SRD - Short Range Device (Устройство малого радиуса действия)

UICC - Universal Integrated Circuit Card (Расширенный стандарт микропроцессорной карты)

UNB - Ultra-Narrow Band (Сверх-узкополосная технология передачи данных)

URI - Uniform Resource Identifier (Унифицированный идентификатор ресурса)

VPN - Virtual Private Network (Виртуальная частная сеть)

Wi-Fi - Технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11

ZigBee - Спецификация сетевых протоколов верхнего уровня

Технологии и стандарты «Интернета вещей»

Ключевые термины и определения

Для целей настоящей Концепции используются следующие термины и определения.

Абонент - пользователь услугами связи, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации.

Абонентский терминал/абонентское устройство – оконечное оборудование, используемое в сетях «интернета вещей».

Актуатор (исполнительное устройство) - устройство, которое инициирует физическое действие после возбуждения входным сигналом.

Вещь интернета вещей - это предмет физического мира (физические вещи) или информационного мира (виртуальные вещи), который может быть идентифицирован и интегрирован в сети связи.

Вредоносное программное обеспечение - программное обеспечение, целенаправленно приводящее к нарушению законных прав абонента и (или) пользователя, в том числе к сбору, обработке или передаче с абонентского терминала информации без согласия абонента и (или) пользователя, либо к ухудшению параметров функционирования абонентского терминала или сети связи.

Выделение полосы радиочастот - разрешение в письменной форме на использование конкретной полосы радиочастот, в том числе для разработки, модернизации, производства в Российской Федерации и (или) ввоза в Российскую Федерацию радиоэлектронных средств или высокочастотных устройств с определенными техническими характеристиками.

Датчик (сенсор) - электронное устройство, которое измеряет физическое состояние или химический состав и доставляет электронный сигнал, соответствующий наблюдаемой характеристике.

Единая информационно-телекоммуникационная среда (ЕИТС) - комплекс телекоммуникационных средств, технических средств, информационных процессов и ресурсов, обеспечивающих решение задач ТК.

Идентификатор - представляет собой серию цифр, букв и символов или данных в любой другой форме, используемую для идентификации абонентов, пользователей, элементов сети, функций, объектов сети, предоставляющих услуги/приложения, или других объектов (например, физические или логические предметы).

Идентификационный модуль - электронный носитель информации, который устанавливают в пользовательском оборудовании и с помощью которого осуществляют идентификацию абонента (пользователя) и/или пользовательского оборудования и обеспечивает доступ оборудования абонента к сети.

«Интернет вещей» (Internet of Things (IoT)) - глобальная инфраструктура для информационного общества, обеспечивающая возможность предоставления сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий. Благодаря задействованию возможностей идентификации, сбора, обработки и передачи данных, в «Интернете вещей» обеспечивается наиболее эффективное использование вещей для предоставления услуг для всех типов приложений при одновременном выполнении требований безопасности и неприкосновенности частной жизни.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Конверсия радиочастотного спектра - экономические, организационные и технические мероприятия, направленные на расширение использования радиочастотного спектра радиоэлектронными средствами гражданского назначения.

Контроллер - электронный компонент передающий параметры считывания или управления физической вещью (интернета вещей)

Концентратор - в рамках документа устройство агрегации данных с контроллеров интернета вещей осуществляющее прием и передачу информации между устройствами и платформами верхнего уровня, а также управляющее устройствами и беспроводной сетью;

Концепция «Интернета вещей» - Концепция построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации.

Лицензия - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и (или) условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю. Модель «Интернета вещей» - совокупность уровня приложений IoT, уровня поддержки приложений и услуг, сетевого уровня и уровня устройств, сопряженных с уровнем управления.

Общий порядок использования РЧС – право на использование РЧС, не требующее обладания РИЧ.

Объекты транспортной инфраструктуры (ТИ) - технологический комплекс, включающий в себя: железнодорожные, автомобильные вокзалы и станции, метрополитены, тоннели, эстакады, мосты, морские терминалы, акватории морских портов, порты во внутренних водах, аэродромы, аэропорты, объекты систем связи, навигации и управления движением транспортных средств, участки автомобильных дорог, железнодорожных и внутренних водных путей (Федеральный закон "О транспортной безопасности" от 09.02.2007 № 16-ФЗ – далее 16-ФЗ).

Оперативно-розыскные мероприятия - закрепленные в федеральном законе от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» действия или совокупность действий, проводимые в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств.

Оператор связи - юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии.

Оркестрация - автоматизированная координация сложных сетевых систем и функций, включая промежуточное ПО для физических и виртуальных инфраструктур.

Персональное (локальное) пространство «Интернета вещей» пользователя - персональная сеть доступа абонента и подключенные к ней датчики и исполнительные устройства с набором идентификаторов, однозначно определяющих входящие в персональное пространство устройства. Персональное пространство контролируется исключительно абонентом. Данные персонального пространства «Интернет вещей» относятся к персональным данным абонента.

Персональная (локальная) сеть передачи данных пользователя-совокупность точек доступа и подключенных к ним устройств, входящих в персональное пространство. Персональная сеть передачи данных может быть проводной и беспроводной.

Платформа «интернета вещей» - это программно-аппаратный комплекс, предназначенный для подключения «интернета вещей» (датчиков, контроллеров и других устройств) к «облаку» и удаленного доступа к ним.

Пользовательское оборудование (абонентское, оконечное оборудование) - технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей.

Присвоение (назначение) радиочастоты или радиочастотного канала - разрешение в письменной форме на использование конкретной радиочастоты или радиочастотного канала с указанием конкретного радиоэлектронного средства, целей и условий такого использования.

Радиоэлектронные средства - технические средства, предназначенные для передачи и (или) приема радиоволн, состоящие из одного или нескольких

передающих и (или) приемных устройств либо комбинации таких устройств и включающие в себя вспомогательное оборудование.

Сети «Интернета вещей» - узкополосные беспроводные сети связи «Интернета вещей» (в рамках рассмотрения данной Концепции).

Сетевой адрес - номер из ресурса нумерации сети передачи данных, однозначно определяющий при оказании телематических услуг связи абонентский терминал или средства связи, входящие в информационную систему.

Сеть связи - технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи.

Субъекты транспортной инфраструктуры - юридические лица, индивидуальные предприниматели и физические лица, являющиеся собственниками объектов транспортной инфраструктуры и (или) транспортных средств или использующие их на ином законном основании (16-ФЗ).

Сухопутная подвижная служба – подвижная служба радиосвязи между базовыми станциями и сухопутными подвижными станциями или между сухопутными подвижными станциями.

Транспортный комплекс (ТК) - объекты и субъекты транспортной инфраструктуры, транспортные средства (16 ФЗ).

Транспортные средства (ТС) - устройства, предназначенные для перевозки физических лиц, грузов, багажа, ручной клади, личных вещей, животных или оборудования, установленных на указанных транспортных средствах устройств, в значениях, определенных транспортными кодексами и уставами (16-ФЗ).

Трафик - нагрузка, создаваемая потоком вызовов, сообщений и сигналов, поступающих на средства связи.

Упрощенный порядок использования РЧС – право на использование РЧС без необходимости получения РИЧ, проведения экспертизы на ЭМС и получения соответствующих разрешений.

Устройство Интернета вещей - это элемент оборудования, который обладает обязательными возможностями связи и дополнительными возможностями измерения, срабатывания, а также ввода, хранения и обработки данных.

Услуга связи - деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений.

Устройство малого радиуса действия - техническое средство, предназначенное для передачи и (или) приёма радиоволн на короткие расстояния, которое не относится ни к одной из радиослужб и используется при условии, что не создает помех другим станциям и не требуется защита от помех других станций.

Общая модель «Интернета вещей»

Общая модель IoT и определение места беспроводных сетей в данной модели основано на подходе, предложенном МСЭ-Т.

В качестве общей модели IoT предлагается использовать четырехуровневую модель IoT, показанную на рисунке 1. Из нее следует, что телекоммуникационная составляющая и, как следствие, беспроводные сети сосредоточены на уровне сети. При этом верхние уровни представляют собой различные интегрированные IT-системы и программное обеспечение, функционирующие на базе ЦОД, либо обрабатываются на периферии (FOG/EDGE вычисления).

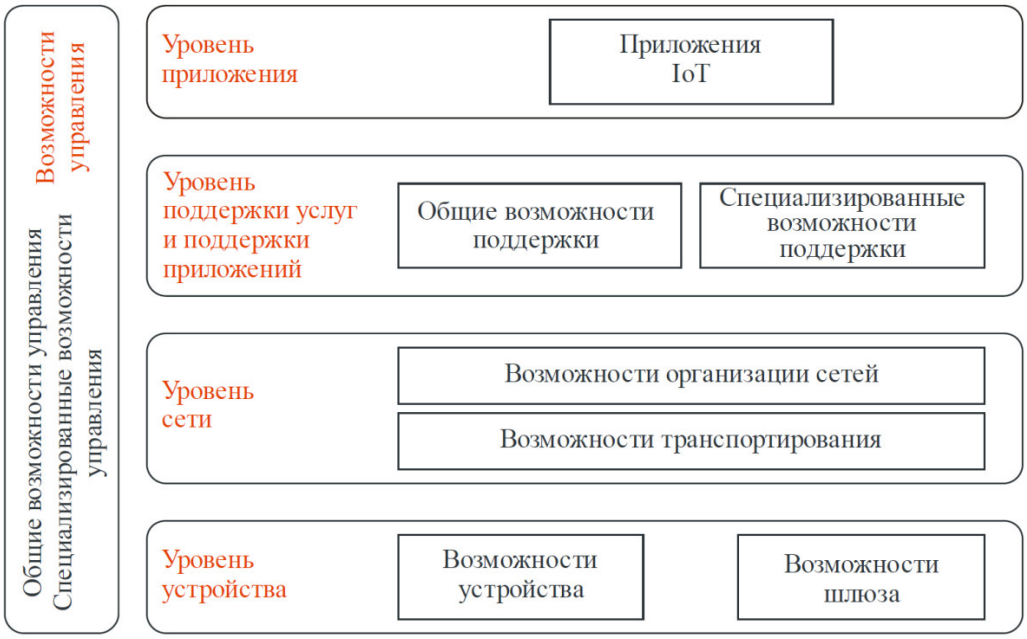

Рисунок 1 - Общая модель «Интернета вещей»

В рассматриваемой модели IoT уровень устройства состоит как из самих конечных устройств, так и из промежуточных шлюзов. При этом устройства могут обладать способностью собирать и получать информацию непосредственно из сети связи, а также непрямым образом, т. е. с помощью возможностей шлюза. В качестве шлюза выступают точки доступа, соединенные с оконечными устройствами с использованием различных проводных и беспроводных технологий (таких как шина сети локальных контроллеров (CAN), ZigBee, Bluetooth, Wi-Fi и др.). Шлюз необходим при наличии разнородных устройств или при осуществлении конвертации протоколов передачи. При этом шлюзы подключаются к уровню сети с использованием различных технологий: коммутируемая телефонная сеть общего пользования, сеть сотовой связи, Ethernet, линия DSL и т.д.

Уровень сети выполняет две базовых задачи: организацию сетей и транспортировку информации. В рамках организации сети предоставляются соответствующие функции управления сетевыми соединениями, такие как функции управления доступом и ресурсом транспортирования, управление мобильностью и аутентификация, авторизация и учет. Транспортировка информации заключается в установлении самих соединений для транспортировки информации в виде данных, относящихся к услугам и

приложениям IoT, а также транспортировки информации контроля и управления, относящейся к IoT.

Уровень поддержки услуг и поддержки приложений предоставляет возможности, которые используются приложениями. Разнообразные приложения могут использовать общие возможности поддержки. К таким примерам относятся общая обработка данных и управление БД. Специализированные возможности поддержки - это конкретные возможности, которые предназначены для удовлетворения потребностей конкретного подмножества приложений IoT.

Уровень приложений состоит из всех приложений, взаимодействующих с IoT-устройствами.

Уровень возможностей управления охватывает традиционные функции управления сетью, т.е. управление неисправностями, управление конфигурацией, управление учетом, управление показателями работы и управление безопасностью.

В качестве примеров общих возможностей управления следует перечислить:

- управление устройствами: примеры включают обнаружение устройств, аутентификацию, дистанционную активацию и деактивацию устройств, конфигурацию, диагностику, обновление прошивки и/или ПО, управление рабочим статусом устройства;

- управление топологией локальной сети: примером является управление конфигурацией сети;

- управление трафиком и перегрузками: например, обнаружение условий перегруженности сети и реализация резервирования ресурсов для срочных и/или жизненно важных потоков трафика.

Уровень возможностей обеспечения безопасности включает общие возможности обеспечения безопасности, которые не зависят от приложений. Примеры общих возможностей обеспечения безопасности включают:

- на уровне приложения: авторизацию, аутентификацию, защиту конфиденциальности и целостности данных приложения, защиту

неприкосновенности частной жизни, аудит безопасности и антивирусную защиту;

- на уровне сети: авторизацию, аутентификацию, конфиденциальность данных об использовании и данных сигнализации, а также защиту целостности данных сигнализации;

- на уровне устройства: аутентификацию, авторизацию, проверку целостности устройства, управление доступом, защиту конфиденциальности и целостности данных.

Как видно из приведенной модели IoT, верхние уровни модели описаны максимально абстрактно без какой-либо привязки к технологической основе. Причем сетевой компонент фигурирует только на двух нижних уровнях (уровень устройства и уровень сети), а также в некоторой части возможностей управления.

Таким образом, место беспроводных сетей в модели IoT возможно определить, как это показано на рисунке 2, разделив при этом беспроводные сети на опорную сеть и сеть радиодоступа.

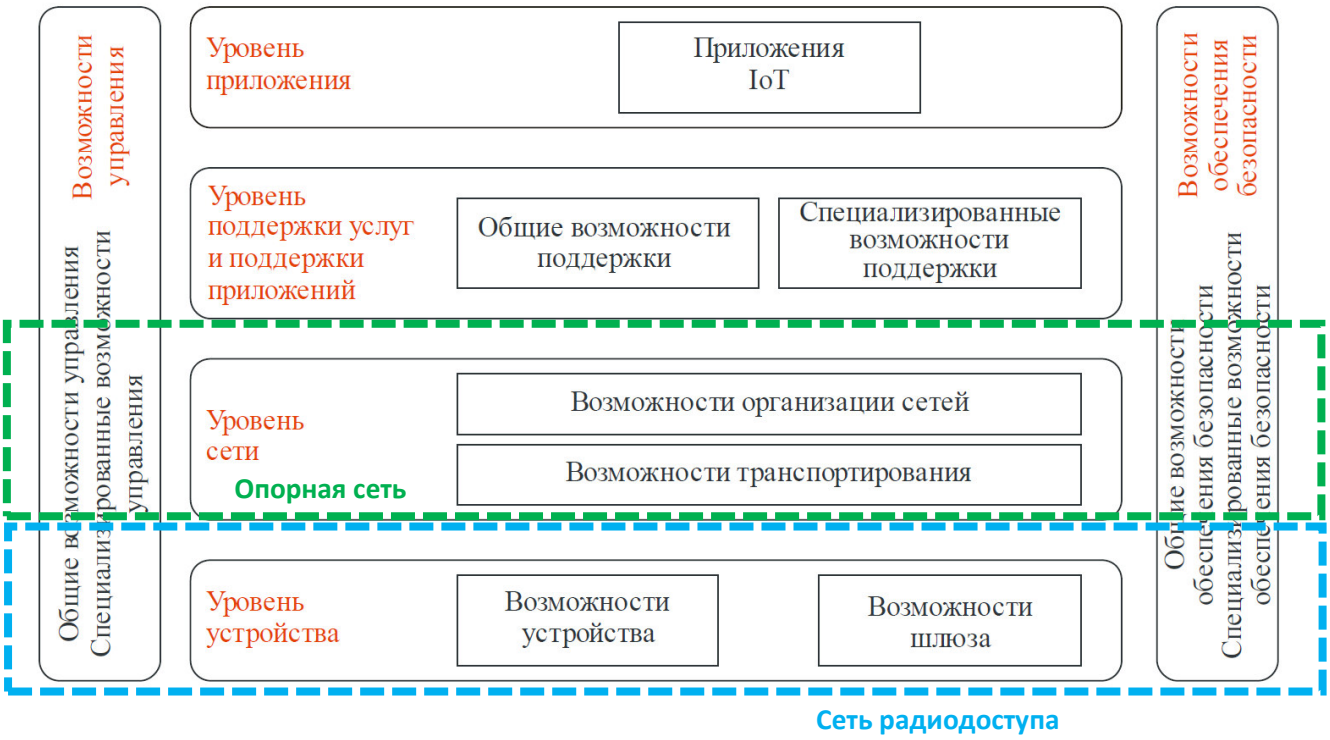

Рисунок 2 - Место беспроводных сетей в общей модели IoT

Как видно из рисунка 2, опорная сеть функционально является частью сетевого уровня. Центры обработки данных общего назначения, на которых

происходит накопление информации от устройств IoT, не являются частью опорной сети, даже если опорная сеть виртуальна и фактически работает на мощностях ЦОД. Таким образом, в рамках развития телекоммуникационных и IT стандартов преследуется цель максимального разделения функционала.

Исключения составляют системы управления (а точнее оркестрирования), обеспечивающие взаимодействие нескольких систем и системы безопасности, которое должно исключить риски как внутри отдельных уровней, так и на их стыках. Такой подход обеспечивает гибкость для оператора в выборе платформы IoT, включая базы данных накопления информации от устройств IoT и программные средства для обработки этих данных и преобразования их в конечные услуги.

Классификация основных технологий и стандартов

Для обеспечения подключения устройств IoT могут использоваться различные радиотехнологии и стандарты беспроводной связи. Тем не менее, подавляющее большинство беспроводных сетей для IoT возможно классифицировать в рамках шести крупных сегментов, показанных на рисунке 3. При этом узкополосные беспроводные сети связи IoT соответствуют двум отдельным сегментам в зависимости от использования полос радиочастот в общем или упрощенном порядке. Порядок (модель) использования радиочастотного спектра во многом определяет и технологическую основу сетей. Узкополосные беспроводные сети связи IoT, использующие РЧС в упрощенном порядке, представляют собой новые закрытые или открытые стандарты, разрабатываемые различными консорциумами и ассоциациями в рамках полос радиочастот, используемых устройствами малого радиуса действия.

Рисунок 3 - Классификация основных беспроводных технологий для IoT

Оценка доли рынка основных беспроводных технологий для IoT представлена на рисунке 4. Значительное число устройств IoT будут подключены через шлюзы на основе локальных и персональных сетей в полосах радиочастот, используемых в упрощенном порядке. При этом сами шлюзы потом могут быть подключены через сети сотовой подвижной связи или узкополосные беспроводные сети связи IoT.

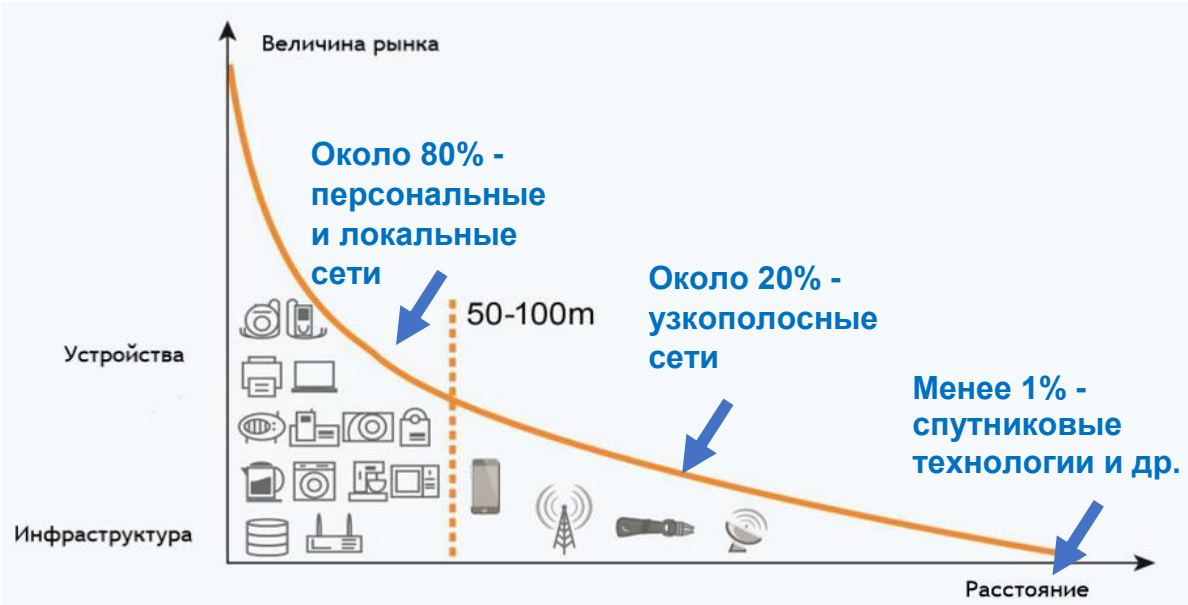

Рисунок 4 - Структура рынка устройств IoT по беспроводным технологиям

Несмотря на то, что узкополосные беспроводные сети связи IoT не рассматриваются в качестве самого массового сегмента беспроводных технологий для IoT, данный тип сетей предполагается использовать для подключения устройств IoT во многих отраслях экономики для широкого ряда применений, которые будет затруднительно или невозможно реализовать с использованием других типов беспроводной связи.

Узкополосные беспроводные сети связи IoT в полосах радиочастот, используемых в общем порядке, представлены тремя стандартами: EC-GSM, eMTC (также называется LTE-eMTC) и NB-IoT. Фактически все три технологии не являются самостоятельными стандартами, а представляют собой развитие существующих стандартов сотовой подвижной связи, доработанных для удовлетворения потребностей в подключении маломощных устройств, работающих, как правило, от батареи и имеющих ограниченные потребности в пропускной способности. В таблице 1 дано краткое описание стандартов и их основных характеристик.

Таблица 1 - Основные параметры узкополосных беспроводных сетей связи IoT.

Характеристики	EC-GSM	LTE-eMTC	NB-IoT
Диапазон радиочастот, МГц	900, 1800	Диапазоны LTE	Диапазоны LTE, в том числе 450, 800, 900, 1800, 2100, 2600 (FDD)
Количество диапазонов в устройстве	1 или 2	Несколько	Многодиапазонные чипы
Ширина радиочастотного канала	200 кГц	Задействуется шесть ресурсных блоков (1,08 МГц) в канале 5 МГц и шире	180 кГц
Число устройств IoT на сектор БС на один канал, ед., не более	50000	50000	50000
Скорость передачи данных	70 или 240 кбит/с (GMSK или 8PSK)	1 Мбит/с	127 кбит/с (линия вниз) 158 кбит/с или 15.6 кбит/с (линия вверх)

Бюджет радиолинии	До 154 дБ для UE с классом мощности 23 дБ или на 10 дБ лучше GPRS До 164 дБ для UE с классом мощности 33 дБ или на 20 дБ лучше GPRS	До 159 дБ для UE с классом мощности 23 дБ или на 15 дБ лучше GPRS	До 164 дБ для UE с классом мощности 23 дБ или на 20 дБ лучше GPRS
Мобильность	Полная	Полная	Ограниченная
Задержка	Секунды	Миллисекунды	Секунды

Технология EC-GSM является расширением существующего стандарта GSM и обеспечивает более плавный вариант внедрения сетей IoT без замены технологии сети радиодоступа. Однако новый функционал доступен только для новых абонентских устройств с поддержкой EC-GSM. В настоящее время данная технология рассматривается как промежуточная, и большие перспективы связаны с технологиями NB-IoT и LTE-eMTC, которые встроены в действующие стандарты LTE. Из сравнения, приведенного в таблице 1 видно, что технология LTE-eMTC в большей степени ориентирована на надежную связь, с поддержкой мобильности и возможностью более высокой скорости передачи при потере в максимальном покрытии и энергетике (в силу больших скоростей передачи). NB-IoT оптимизирована для сегмента IoT, где требуются максимальная дальность связи, малые скорости и большая энергоэффективность.

Особенностью узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в общем порядке, является возможность работы в предсказуемой помеховой ситуации, что позволяет использовать синхронные схемы доступа, гарантирующие предсказуемую задержку и обеспечивать более надежное покрытие. Возможность широкого покрытия территории также обеспечивается возможностью переиспользования существующей инфраструктуры сотовой подвижной связи, включая высокоэффективные антенны на базовых станциях.

Следует отметить, что в Российской Федерации принято решение ГКРЧ № 17-44-06 от 28 декабря 2017 г. по упрощению внедрения сетей NB-IoT поверх существующих сетей GSM и LTE без необходимости повторного получения разрешений на использование радиочастот или радиочастотных каналов для новой технологии, что существенно упростило порядок развертывания сетей NB-IoT.

Устройства малого радиуса действия, давно используются в различных отраслях экономики и являются неотъемлемой частью «Интернета вещей». Данные технологии за счет ограничения максимальной мощности применяемых устройств используются локально и без получения разрешения на использование радиочастот или радиочастотных каналов. Однако проникновение инфокоммуникационных технологий в новые сферы применения привело к тому, что для передачи небольших по объёму данных на значительные расстояния потребовалось создание нового класса технологий, таких как узкополосные беспроводные сети связи «Интернета вещей».

Формирование новых требований к устройствам «Интернета вещей», а именно их дешевизна, низкая скорость передачи и низкое энергопотребление, привело к возврату к хорошо изученным и реализованным методам создания радиотехники, но на новом этапе технологического развития. В этих условиях разработка собственного стандарта радиоинтерфейса для узкополосных беспроводных сетей связи «Интернета вещей» стала возможной для небольших групп разработчиков. С учетом наличия большого числа мощностей по производству микросхем и развитию аутсорсинга производства таких устройств, относительно небольшие компании смогли реализовать разработку микрочипов и их успешный массовый выпуск. Поэтому существует более десятка различных открытых и закрытых стандартов узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в упрощенном порядке. В этих условиях для успешного развития стандартов узкополосных беспроводных сетей связи IoT на первое место встают задачи создания экосистемы готовых

изделий (модемов, счетчиков со встроенными модемами и т.д.), экосистемы разработчиков услуг на базе данных сетей, наличие рынка сбыта (ЖКХ, телематика) и доступность радиочастотного ресурса (спектр для устройств малого радиуса действия).

В Российской Федерации в настоящее время существует несколько компаний, развивающих свой собственный стандарт радиоинтерфейса и экосистему всех уровней модели «Интернета вещей». Также присутствует большое количество локальных производителей оборудования и операторов, использующих международный стандарт LoRa. Технические параметры наиболее известных из отечественных стандартов и стандарта LoRa показаны в таблице 2.

В таблице 2 в отличие от таблицы 1 помимо технических характеристик также показана бизнес-модель разных стандартов и состояние формирования экосистемы, т.к. именно эти параметры являются ключевыми в дифференцировании между большим числом стандартов узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в упрощенном порядке. Помимо этого, из таблицы 2 следует, что стандарты узкополосных беспроводных сетей связи IoT в полосах, используемых в упрощенном порядке, можно разделить на две группы. С одной стороны, это набор сверхузкополосных технологий отечественной разработки, таких как «Стриж», XNB, NB-Fi и пр., аналогичные во многом более распространенной в других странах технологии Sigfox. Альтернативой к данным технологиям выступает «просто» узкополосная технология LoRa (радиоинтерфейс) или LoRaWAN (включает описание протоколов более высоких уровней).

Для приведенных стандартов наиболее востребованным диапазоном радиочастот является диапазон 863-876 МГц. Диапазон 433 МГц востребован в меньшей степени в силу ограниченных радиочастотных ресурсов, а также достаточно сильному шумовому фону от большого количества работающих устройств и необходимости использования больших антенн, что затруднительно для использования в небольших устройствах.

Таблица 2 - Основные технологии узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в упрощенном порядке, в Российской Федерации

Технология	Используемая модуляция	Ширина канала	Возможности по скорости	Возможности по задержке	Востребованные диапазоны радиочастот	Открытость архитектуры	Бизнес-модель
LoRa	Прямое расширение спектра (ЛЧМ)	Ширина спектра 125 кГц и канала порядка 200 кГц	100 бит/с - 50 кбит/с	Единицы секунд	863-876 МГц	Архитектура открытая, чип проприетарный	Операторские и частные сети
Sigfox	Сверхузкополосные каналы (UNB, DPSK)	Порядка 100 Гц (большое число каналов в рабочей полосе)	100 бит/с	Секунды	863-876 МГц	Частично открытая (Опубликованы все спецификации радиопротоколов, однако используется собственная платформа для сбора и анализа данных.)	Предоставление законченного бизнес решения. Любая компания может производить оборудование для сетей данного стандарта.
Weightless	Узкополосная	12.5 КГц	200 бит/с - 100 Кбит/с	Секунды	863-876 МГц	Закрытая	Ядро сети контролируется разработчиком
«Стриж»	Сверхузкополосные каналы (UNB, DPSK)	Порядка 100 Гц (большое число каналов в рабочей полосе)	100 бит/с	Секунды	863-876 МГц	Закрытая. (*Все элементы сети изначально являлись закрытыми. В настоящее время рассматриваются вопросы создания более открытой экосистемы*).	Ядро сети контролируется разработчиком
XNB ООО«ГЛОНАСС-ТМ»	Сверхузкополосные каналы	Ширина спектра 100-1000 Гц (большое число каналов в рабочей полосе) Опционально	100-1000 бит/с (до 10 кбит/с для сигнала 10 кГц)	Секунды	863-865 МГц 874-876 МГц	Открытая (*Разрабатывается как открытый стандарт, но пока реализуется только разработчиком стандарта*).	Модель не определена. Предположительно только операторская модель.

		порядка 10 кГц. Ширина канала в 1.5 больше, чем ширина спектра.					
NB-Fi	Сверхузкополосные каналы (UNB, DPSK)	Порядка 100 Гц (большое число каналов в рабочей полосе)	100 бит/с	Секунды	863-876 МГц 433 МГц	Открытая. (*Разрабатывается как открытый стандарт, но пока реализуется только разработчиком стандарта. Однако в настоящее время реализуется только на чипе одного производителя*).	Ядро сети контролируется разработчиком. Не исключено создание операторских сетей.
GoodWAN	Сверхузкополосные каналы (UNB, FSK)	Порядка 100 Гц (большое число каналов в рабочей полосе)	100 бит/с	Секунды	863-876 МГц 433 МГц	Открытая (*Разрабатывается как открытый стандарт, но пока реализуется только разработчиком стандарта, возможна реализация на чипах различных производителей).*	Ядро сети контролируется разработчиком. Не исключено создание операторских сетей.

С точки зрения радиочастотного обеспечения все технологии за исключением XNB рассматриваются только для упрощенного порядка использования РЧС. Для сети ФСТТ рассматривается гибридная схема, где закрепление полос радиочастот осуществляется за оператором или доверенными операторами в системе ФСТТ, но их использование данными операторами осуществляется без получения разрешений на использование радиочастот или радиочастотных каналов.

Федеральная сеть IoT на транспорте использует выделенный для целей построения сети сбора, обработки и передачи телематической информации радиочастотный ресурс: 863-865/874-876 МГц (выделен Решением ГКРЧ от 30.11.2018 № 18-47-05 о выделении полос 863-865/874-876 МГц для федеральной системы транспортной телематики).

Элементы федеральной сети IoT на транспорте могут использовать для целей построения сети сбора, обработки и передачи телематической информации на локальных объектах радиочастотный ресурс в полосах, выделенных для применения неспециализированных устройств малого радиуса действия: 433,92 МГц и 149,975-150,05 МГц, 866 – 868 МГц, 868,7 – 869,2 МГц и другие, возможность и условия использования которых определены действующими решениями ГКРЧ.

Элементы федеральной сети IoT на транспорте могут использовать выделенный для целей построения сети сбора, обработки и передачи телематической информации технологии NB IoT радиочастотный ресурс в диапазоне радиочастот 1800 МГц.

Сверхузкополосные технологии во многом ориентированы на бизнес-модель, в которой разработчик технологии реализует и функционал агрегатора информации, и предоставление сервисов для организаций, развернувших сеть радиодоступа. Для технологий XNB и NB-Fi также рассматривается модель организации отдельных операторов, но на данный момент данные о таких реализациях отсутствуют. Сверхузкополосные технологии при этом преимущественно ориентированы на сбор телеметрии с

некритических объектов. Ключевой особенностью LoRaWAN является ее открытая бизнес-модель (за исключением чипа), которая предусматривает как создание операторских сетей, так и создание локальных частных сетей.

Упрощенный принцип предполагает использование несинхронных схем доступа. Такое использование не позволяет обеспечить высокую надежность связи из-за риска возникновения помех от других сетей, что может приводит к временному прекращению предоставления сервиса. Тем не менее, простота таких систем, скорость их развертывания и относительная дешевизна при локальном применении, делает использование узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в упрощенном порядке, востребованным во многих сферах.

Все радиотехнологии (табл. 2) с открытой архитектурой являются рекомендуемыми для применения на территории Российской Федерации.

Общие требования к беспроводным сетям «Интернета вещей» и возникающие риски

Сравнение общих требований к сетям «Интернета вещей» с существующими традиционными беспроводными сетями связи с точки зрения взаимодействия с платформами «Интернета вещей» показывает, что большинство платформ «Интернета вещей» строится инвариантно от технологии обеспечения канала с устройством IoT в части сбора и систематизации информации. Тем не менее, в ряде случаев сети радиодоступа могут включать логические элементы сети, обеспечивающие трансляцию тех или иных параметров соединений для платформы «Интернета вещей». В наиболее широком понимании узкополосные беспроводные сети связи IoT должны обеспечивать предоставление следующих сведений в платформу «Интернета вещей»:

- идентификация оконечных устройств IoT;
- организация и управление соединениями с устройствами IoT;
- организация сбора и хранения данных;

- управление устройствами;

- обнаружение подключенных устройств и их регистрация в сети;

- получение данных о местоположении;

- работа с группами устройств;

- отслеживание срабатывания устройств/запуска услуг;

- регистрация;

- обеспечение безопасности и защиты информации между устройством интернета вещей и платформой;

- выставление платы за обслуживание;

- создание оповещений и поддержка пользователей услуг IoT.

Большинство из вышеописанных функций требует предоставления соответствующих сервисов от сети радиодоступа. По этой причине помимо радиоинтерфейса в узкополосных беспроводных сетях связи IoT требуются соответствующие функциональные блоки, позволяющие реализовывать данные функции в полной мере. Во многих случаях проприетарные стандарты реализуют данный функционал через фирменные технические решения. Однако в масштабах больших сетей целесообразно использовать стандартизованные решения, что упрощает организацию взаимодействия с платформами «Интернета вещей». Так, для реализации трансляции вышеописанных данных в 3GPP для сетей NB-IoT, EC-GSM и eMTC предусмотрели также и новые стандартизованные блоки, и интерфейсы на уровни ядра сети.

Помимо специализированных радиоинтерфейсов в 3GPP rel.13 для услуг IoT появился новый узел Service Capability Exposure Function (SCEF), который обеспечивает трансляцию возможностей и данных в сети сторонним организациям и разработчикам услуг верхних уровней через стандартизованные API. Блок SCEF дополнил два существующих блока: блоки MTC Interworking Function (MTC-IWF) и Service Capability Server (SCS). MTC-IWF и SCS используются в организации сторонних приложений для межмашинной связи и обеспечивают аутентификацию между

устройствами и сторонними серверами приложений, т.е. позволяют оператору устройств M2M использовать свою адресацию, не задумываясь об IP адресации или IMSI-номерах устройств в сети оператора.

Столь глубокая интеграция с платформами «Интернета вещей» и передача значительного объема служебной информации из сети радиодоступа обеспечивает возможность реализации новых услуг IoT. Однако эти же новые возможности порождают и новые регуляторные риски, связанные с обеспечением информационной безопасности, управлением использования собранных больших технологических данных, а также риски, связанные с реализацией системы оперативно-розыскных мероприятий для узкополосных беспроводных сетей связи IoT.

Информационная безопасность сетей связи напрямую связана с наличием рисков применения узкополосных беспроводных сетей «Интернета вещей».

Потенциальная уязвимость узкополосных беспроводных сетей «Интернета вещей» связана в первую очередь с появлением большого количества новых устройств IoT в Российской Федерации, осуществляющих не только сбор данных, но и управление процессами в различных областях экономики. Возникает необходимость защиты от злонамеренного воздействия на устройства, препятствий их работе и от утечек большого объёма информации, собираемой устройствами IoT.

Вместе с тем, достаточно остро стоит вопрос единой системы идентификации устройств IoT узкополосных беспроводных сетей «Интернета вещей», что позволит минимизировать затраты на реализацию комплекса оперативно-розыскных мероприятий, сократить затраты операторов сетей IoT и информационных систем, а также уменьшить время обработки и анализа большого объёма разнородной информации различных отраслей экономики.

Проведя анализ рисков, возникающих при реализации узкополосных беспроводных сетей «Интернета вещей», необходимо отметить, что к

наиболее уязвимым можно отнести беспроводные технологии, применяемые в устройствах малого радиуса действия.

Кроме того в соответствии с пунктом 22 приложения к Перечню радиоэлектронных средств и высокочастотных устройств, подлежащих регистрации, утверждённому постановлением Правительства Российской Федерации от 12 октября 2004 г. № 539 (в ред. Постановления Правительства Российской Федерации от 22.12.2018 № 1633), неспециализированные (любого назначения) устройства в полосах радиочастот 864-865 МГц и 868,7-869,2 МГц с максимальной эффективной излучаемой мощностью 25 мВт относятся к категориям радиоэлектронных средств, регистрация которых не требуется.

При использовании открытых и закрытых стандартов узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в упрощенном порядке, возникают следующие риски, связанные, в том числе, с информационной безопасностью:

- технологическая зависимость от иностранных поставщиков комплектующих изделий при строительстве сетей «Интернета вещей» с использованием импортного оборудования;

трудность поиска неправомерно используемых устройств, работающих в импульсном режиме с пониженной мощностью

- неконтролируемое возникновение взаимных радиопомех в сетях и между сетями «Интернета вещей»;

- возможность использования сетей «Интернета вещей» для скрытого обмена электронными сообщениями;

- использование иностранных криптографических алгоритмов с не декларируемыми свойствами для шифрования информации в оконечных устройствах сетей «Интернета вещей»;

- реализация в протоколе взаимодействия оконечных устройств IoT с аппаратно-программной платформой возможности передачи собранных

оконечными устройствами IoT на территории Российской Федерации данных на серверы, размещённые за пределами территории Российской Федерации;

- отсутствие требований по обеспечению доступа уполномоченных государственных органов к информации, хранящейся в информационных системах сервисных платформ сетей «Интернета вещей», для осуществления оперативно-розыскной деятельности.

Для снижения рисков, связанных с информационной безопасностью сетей «Интернета вещей» в различных отраслях экономики, необходимо предусмотреть обязательное подтверждение соответствия оборудования узкополосных беспроводных сетей «Интернета вещей» требованиям, установленным в соответствии с Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи», нормативными актами ФСБ России и соответствующими актами и рекомендациями федеральных органов исполнительной власти по типу конкретного использования беспроводных устройств и платформ интернета вещей в той или иной области хозяйственной деятельности.

Сферы применения сетей «Интернета вещей»

Цифровизация ключевых отраслей экономики требует развития телекоммуникационной составляющей и использования в большинстве случаев беспроводных технологий. Вместе с тем, узкополосные беспроводные сети связи IoT не являются единственным способом подключения устройств к «Интернету вещей». Применение тех или иных беспроводных технологий определяется сферой деятельности, требующей цифровизации. Предпочтительность использования узкополосных беспроводных сетей связи IoT определяется следующими факторами:

- требуется ли покрытие внутри помещений;

- требуется ли мобильность и постоянное отслеживание местонахождения;

- требуется ли работа только от батареи;

- критично ли удешевление оконечного устройства.

Помимо перечисленных факторов, связанных со сценарием использования, возможно также выделить и технические требования, влияющие на выбор технологии, такие как задержка и надежность связи. Наиболее эффективная технология беспроводной связи должна определяться в зависимости от рассматриваемого приложения в конкретной отрасли.

Целесообразно разработать отдельные отраслевые разделы Концепции по внедрению IoT в различных отраслях экономики Российской Федерации, после их детальной проработки профильными министерствами и ведомствами.

Жилищно-коммунальное хозяйство

ЖКХ - одна из отраслей, в которой в настоящее время активно внедряются узкополосные беспроводные сети связи IoT. Переход к использованию таких сетей позволяет создавать автономные приборы учета, способные работать годами, и собирать с них информацию в радиусе десятков километров от базовой станции в условиях прямой видимости или до нескольких километров в случае размещения устройств глубоко внутри помещений или подвалах. Одна базовая станция способна покрыть сетью целый микрорайон или небольшой город, что дает возможность получать показания и управлять счетчиками в режиме онлайн через сеть Интернет.

Внедрение счетчиков учета потребления с подключением через узкополосные беспроводные сети связи IoT позволяет организациям ЖКХ осуществлять мониторинг потребления воды, электричества, тепла и газа в онлайн-режиме, выявлять возможные вмешательства в работу приборов учета, снижать издержки на неучтенное потребление ресурсов, а также сокращать время на сбор показаний и выставление счетов.

Установка счетчиков на участках трубопроводов позволяет обнаруживать утечки воды и газа сразу после их появления, одновременно осуществляя определение их местоположения. Также распределенные

датчики могут использоваться для контроля качества воды. В энергосетях датчики обнаруживают места искрения, обрывы и несанкционированные отводы. В целом использование IoT в коммунальной инфраструктуре позволяет перейти от регулярного на превентивное техобслуживание и удаленное обнаружение неполадок без участия персонала.

Еще одним широко распространенным применением узкополосных беспроводных сетей связи IoT в ЖКХ является вывоз мусора. Мусорные баки оборудуются интегрированными датчиками наполненности (например, с использованием ультразвуковых датчиках объема или тензодатчиков веса), срабатывание которых принимается как сигнал о необходимости вывоза мусора. С учетом принятых решений и знания географических координат мусорных баков формируются наиболее оптимальные маршруты мусороуборочных машин.

Помимо сбора телеметрии в ЖКХ также существуют и применения с управлением устройствами. Примером является управление освещением на улице, в том числе и в совокупности с оценкой освещенности по показаниям датчиков освещения. Такой вариант применения не требует малой задержки или повышенной надежности. Другие применения в ЖКХ, такие как управление вентилями для перекрытия труб могут потребовать применения стандартов с малой задержкой и высокой надежностью.

Логистика и транспорт

К применениям IoT в сфере логистики и транспорта относят как системы частичной автоматизации транспорта и беспилотного транспорта, так и различные системы по управлению транспортными потоками, а также системы по оптимизации работы общественного транспорта в городских условиях. Данные системы получили общее название интеллектуальные транспортные системы (ITS). ITS - это системы, поддерживающие транспортировку товаров и людей, использующие информационные и коммуникационные технологии для эффективного и безопасного

использования транспортной инфраструктуры и транспортных средств (автомобилей, поездов, воздушных и морских судов). При этом понятие ITS является более широким, чем узкополосные беспроводные сети связи IoT.

Узкополосные беспроводные сети связи IoT подходят для решения таких задач, как отслеживание местоположения транспортных средств, получение телеметрических данных о состоянии транспортного средства и/или грузов. Все эти сведения могут собираться в соответствующих интеллектуальных системах для оптимизации технологических процессов. Наиболее эффективно такие задачи решаются узкополосными беспроводными сетями связи IoT в полосах радиочастот, используемых в общем порядке, в силу возможности переиспользования существующей инфраструктуры сетей сотовой подвижной связи. Но узкополосные беспроводные сети связи IoT в полосах радиочастот, используемых в упрощенном порядке, могут эффективней решить задачу контроля грузов в случае их локального применения, например, когда контроль грузов осуществляется локальной базовой станцией на борту железнодорожного состава или крупного контейнеровоза, т.к. морские суда и железнодорожные составы зачастую могут находиться за пределами зон покрытия узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в общем порядке.

С учетом того, что транспортные средства, как правило, не ограничены по мощности, необходимой для функционирования сетей связи IoT, а также имеют возможность установки качественных антенн, они в меньшей степени ограничены и в дальности связи. По этой причине ожидается, что в особенности на автотранспорте будут востребованы либо полноценные сети сотовой подвижной связи, либо узкополосные беспроводные сети связи IoT на базе Nb-IoT/LTE-eMTC, т. к. телеметрия с современного автомобиля имеет значительные объемы и может использоваться не только для отслеживания его нормальной работы, но и для предоставления новых «умных» электронных услуг. К тому же для автотранспорта требуется

максимальная поддержка мобильности, которая ограничена в наиболее простых узкополосных беспроводных сетях связи IoT.

Для автоматизации транспорта предполагается использовать специализированные стандарты в отдельных полосах радиочастот, такие как стандарты IEEE 802.11p или LTE-V2X в диапазоне 5855-5925 МГц, а также высокоскоростные сети сотовой подвижной связи для организации передачи видео или в случае необходимости обеспечения максимальной надежности связи.

Развитие транспортного комплекса (ТК) Российской Федерации требует создания и развития единой информационной телекоммуникационной среды (ЕИТС) и направлено на улучшение качества управления как отдельными транспортными средствами и транспортной инфраструктурой (ТИ), так и ТК Российской Федерации в целом с целью снижения издержек и увеличения доходности на единицу транспортной работы за счет использования возможностей оперативного получения информации о состоянии транспортной инфраструктуры через информационные и телекоммуникационные системы.

Оснащение транспортных средств обязательными системами помощи водителю, повышение требований к безопасности влекут требования по взаимодействию транспортных средств (ТС) со светофорами, дорожными знаками, другими участниками движения, что требует развития систем беспроводной передачи данных для обмена информацией ТС между собой и с объектами инфраструктуры с требуемыми показателями качества в рамках создания технологической сети транспортной отрасли.

«Интернет вещей» используется государством с целью организации транспортной системы в России. Нормативно закреплена обязанность устанавливать системы дистанционного мониторинга и контроля движения транспорта для коммерческих перевозок пассажиров и перевозки опасных грузов. Также к примерам государственной политики цифровизации транспорта можно отнести обязанность автопроизводителей с 1 января 2017

года оснащать все автомобили системой экстренного оповещения «ЭРА-ГЛОНАСС».

Промышленность

Сегодня практически все промышленные производства стремятся перейти на очередную ступень цифровой эволюции за счет внедрения технологий IoT. Причем в промышленности IoT в большей степени ориентирован на аналитику больших данных (big data) и направлен на повышение эффективности производства, надежности работы и производительности по всей цепочке поставок. Для оптимизации промышленного производства необходимо принимать своевременные решения на основе достоверной информации. Этого помогает достичь использование таких возможностей IoT, как обучение машин, большие данные и технологии автоматизации для создания «системы в системе». Все эти инструменты могут точно и последовательно выделять, принимать, анализировать и передавать данные с целью достижения большей эффективности, надежного управления и улучшения контроля качества по всей цепочке производственного цикла.

Примером применения такого подхода к промышленному производству является контроль и обеспечение исправности промышленного оборудования - одного из главных производственных активов. Если оно выходит из строя слишком часто, то, как правило, это значит, что отсутствует логический способ быстро проанализировать ситуацию и установить, в чем причина поломки: либо не хватает достоверной информации, либо специалистам требуется несколько часов или дней для анализа данных.

Промышленный IoT использует показания датчиков для превентивного ремонта оборудования, разработки и тестирования его модификаций, онлайн инвентаризации и мониторинга загрузки каждой производственной единицы. Например, использование датчиков вибрации в турбинах энергоустановок и сбор соответствующих больших данных позволил компании General Electric

сэкономить 35% на обслуживании турбин по всему миру и ввести модификации в их конструкцию. Таким образом, накопление данных по работе однотипного оборудования на различных производствах позволяет создать аналитические модели поломки оборудования. Использование данных моделей с результатами наблюдения в реальном времени над конкретным образцом оборудования позволяет прогнозировать поломку, а также оперативно определять ее причину и устранять ее. Во многих случаях особенности производственного процесса позволяют подключать оборудование только по беспроводным каналам с использованием тех или иных радиотехнологий. Выбор радиотехнологии существенно зависит от режима сбора информации. В случае необходимости получать данные ежесекундно с высокой гарантией по задержке и качеству, необходимо использовать сети связи на базе Nb-IoT/LTE-eMTC или переходить к высокоскоростным сетям сотовой подвижной связи. Если цикл передачи и объем данных менее критичны, возможно использование всего спектра узкополосных беспроводных сетей связи IoT.

Большой пласт задач, связанный с промышленностью, относится к логистике материалов, техники и персонала. Организация эффективного перемещения материалов, техники и персонала в рамках производственного процесса позволяет существенно повысить производительность труда и сократить издержки за счет анализа поступающих данных и контроля полного цикла производственного процесса. Как правило, для таких применений могут использоваться различные узкополосные беспроводные сети связи IoT. В случае, если производственный процесс локализован в рамках территории предприятия, возможно развертывание частной узкополосной беспроводной сети связи IoT в полосах радиочастот, используемых в упрощенном порядке. В случае необходимости организовывать логистику и координацию действий на территории города или субъекта Российской Федерации необходимо использовать узкополосные беспроводные сети связи IoT с широким охватом и

мобильностью в полосах радиочастот, используемых в общем порядке. Примером промышленного использования узкополосных беспроводных сетей IoT в географически распределенных инфраструктурах, таких как газо- и нефтепроводы, является управление заслонками, контроля температуры и давления, выявления утечек и скопления газов и возгораний.

Если говорить о процессах автоматизации производства, узкополосные беспроводные сети связи IoT, даже на основе стандарта Nb-IoT/LTE-eMTC, как правило, не могут выполнить требований по задержке и надежности, а в случае необходимости передачи видео и требования по пропускной способности, которые потребуются при автоматизации заводов и фабрик. В этом случае необходимо использовать либо специальные сети сотовой подвижной связи в полосах радиочастот, используемых в общем порядке, либо специальным образом адаптированные высокопроизводительные беспроводные технологии. При этом для беспроводных решений в промышленном «Интернете вещей» затруднительно использовать радиочастоты ниже 1 ГГц. В этом случае более востребованными являются узкополосные беспроводные сети связи IoT в полосах радиочастот, используемых в общем порядке, так как для промышленных применений характерно большое число IoT устройств, размещаемых на сравнительно небольшой территории предприятия. В таких условиях малое затухание сигнала, которое отмечается в низких диапазонах радиочастот, ведет к увеличению помех. Для обеспечения надежности промышленной автоматизации на международном уровне рассматривается вопрос выделения отдельной части полосы радиочастотного спектра, используемого в общем порядке.

Здравоохранение

Применение IoT в здравоохранении связано со сбором и анализом большого объема данных. Применение алгоритмов к анализу «больших данных» позволяет достичь высоких показателей в эффективности

использовании имеющихся в отрасли ресурсов и новых возможностей улучшения качества предоставляемых населению услуг. В здравоохранении существуют задачи, которые наилучшим образом решаются с использованием узкополосных беспроводных сетей связи IoT, а также задачи, которые требуют использования других беспроводных технологий.

При повсеместной поддержке идентификации, зондирования и коммуникационных возможностей IoT все объекты системы здравоохранения (пациенты, медицинский персонал, техника, лекарственные препараты и т.д.) возможно постоянно отслеживать и контролировать. Использование беспроводных технологий позволяет все необходимые медицинские сведения собрать, обработать и эффективно использовать с применением сложных алгоритмов. Данные сведения могут использоваться как для диагностики заболевания у конкретного пациента, так и для совершенствования диагностики определенного заболевания у всех пациентов. В случае необходимости проведения измерений с малым объемом данных и с относительно длительными периодами измерения в качестве основы возможно использовать практически любую узкополосную беспроводную сеть связи IoT. С учетом мобильности абонента или его нахождения в другом населенном пункте наиболее простым является использование узкополосных беспроводных сетей связи IoT в диапазонах радиочастот, используемых в общем порядке, которые будут иметь больший охват по территории в силу наличия существующей инфраструктуры. Для более регулярных медицинских анализов и измерений потребуется использовать узкополосные беспроводные сети связи IoT на основе стандарта Nb-IoT/LTE-eMTC.

При использовании персональных вычислительных устройств и мобильного доступа в медицинские службы и учреждения, услуги здравоохранения становятся мобильными и персональными. Широкое распространение сервисов мобильного Интернета ускоряет развитие основанных на технологиях IoT услуг здравоохранения «на дому» или передвижных медицинских центров в сельской местности. Однако в отличие

от отдельных медицинских датчиков, оборудование передвижных медицинских центров требует большей пропускной способности на основе использования современных сетей сотовой подвижной связи вместо узкополосных беспроводных сетей связи IoT. Аналогично ситуация обстоит со сложным медицинским оборудованием, управление и контроль над которым, может требовать меньших задержек и большей пропускной способности.

Учитывая требования законодательства Российской Федерации в области защиты персональных данных, целесообразно проведение дополнительных исследований в части правовых вопросов сертификации устройств «интернета вещей» в области медицины и здравоохранения, а также средств связи LPWAN в составе медицинских препаратов, протезов, устройств.

Сельское хозяйство

Применение сетей IoT в сельском хозяйстве позволит более эффективно использовать земельные ресурсы, оптимизировать систему хранения и в результате снизить себестоимость продукции. Для этого могут применяться различные виды датчиков, устройств для мониторинга, системы управления данными, самоуправляемая спецтехника.

Сегодня технологии IoT распространены только у 5-10% сельскохозяйственных производителей страны, при этом потребность в постоянном мониторинге сельскохозяйственных процессов достаточно высока, особенно в части технического состояния сельскохозяйственного оборудования и сооружений, что необходимо для оптимизации эксплуатации, своевременного техобслуживания и ремонта.

Кроме перечисленных выше отраслей экономики узкополосные беспроводные сети связи IoT будут востребованы в ряде других отраслей, таких как, «умная» энергетика, «умный» город и т.д.

Государство само является крупнейшим потенциальным потребителем услуг IoT, т. к. оно управляет колоссальной инфраструктурой: дорогами, объектами ЖКХ, зданиями и сооружениями, электрическими и тепловыми сетями и пр. Рынок государственных учреждений и госкомпаний обладает огромным экономическим потенциалом для внедрения технологий IoT с точки зрения повышения энергоэффективности и сокращения затрат на обслуживание производственных активов.

На рисунке 5 показан глобальный прогноз роста числа устройств в узкополосных беспроводных сетях связи IoT по отдельным видам экономической деятельности.

Нестандартное разбиение на отрасли, приведенное на рисунке, является следствием того, что одни и те же узкополосные беспроводные сети связи IoT могут обслуживать различные отрасли и их точный учет по конкретным отраслям затруднен. Тем не менее, рисунок 5 иллюстрирует потенциал возможностей использования узкополосных беспроводных сетей связи IoT.

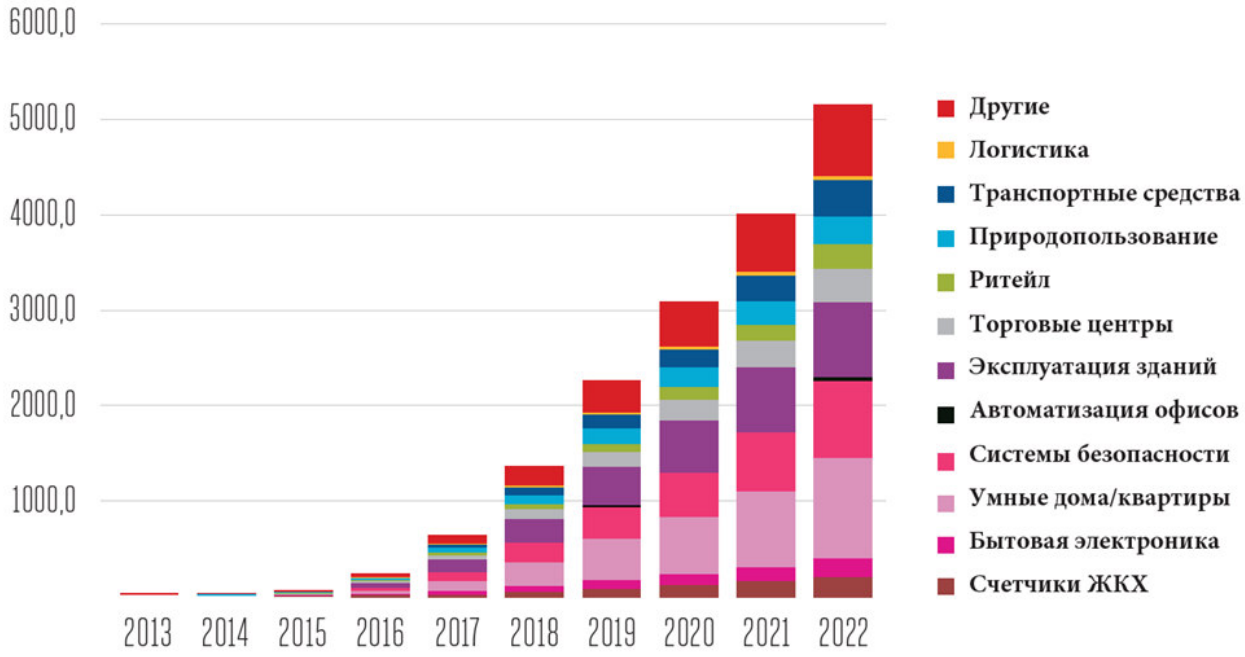

Рисунок 5 - Глобальный прогноз роста числа устройств в узкополосных беспроводных сетях связи IoT

Также следует отметить, что внедрение «Интернета вещей» и цифровизация различных отраслей экономики является более широкой

задачей, чем построение и развитие узкополосных беспроводных сетей связи IoT. Практически в каждой отрасли есть применения, которые могут быть реализованы только с использованием узкополосных беспроводных сетей связи IoT, так и применения, которые требуют использования других беспроводных технологий. При этом более высокие уровни модели «Интернета вещей» во многих случаях являются общими вне зависимости от использования того или иного типа беспроводных технологий.

Сеть передачи данных федеральной системы транспортной телематики

Потребности транспортного комплекса определяются эксплуатационными задачами по мониторингу и управлению транспортной инфраструктурой и транспортными средствами, потребностями пользователей в сервисах, основой которых является информация, получаемая посредством телематических служб.

Потребности в сборе, передаче и обработке информации характеризует количество потребителей: более 50 млн. автомобилей (из них более 8 млн. грузовых), более 3 млрд. тонно-км грузов, более 40 млн. т. ТБО, 85 тысяч км. железнодорожных путей, 4 тысячи станций, 1.2 млн. вагонов, более 1 млн. км. дорог, более 150 млн. приборов систем безопасности и 500 млн. приборов учета ресурсов.

Системы сбора, обработки и передачи данных в интересах мониторинга и управления транспортной инфраструктурой и транспортными средствами в единой транспортной системе страны включают (рис. 6): устройства и оборудование, размещаемые на ТИ и ТС, сеть передачи данных (СПД) и цифровую платформу.

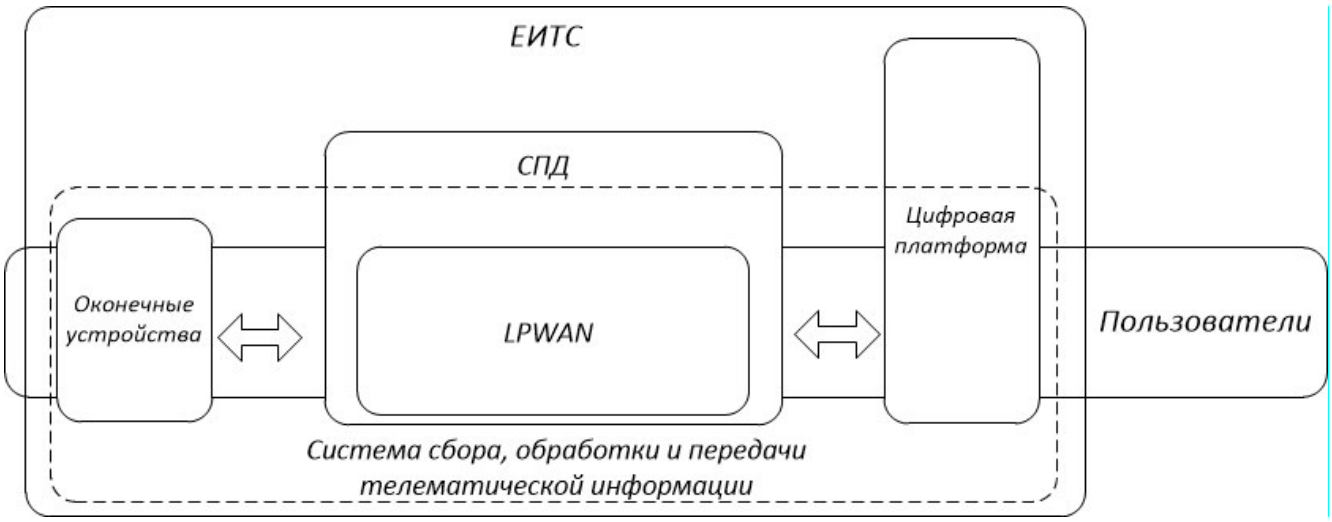

Рисунок 6 - Место сети сбора, передачи и обработки телематической информации на основе технологий LPWAN в ЕИТС

ЕИТС обеспечивает общую телекоммуникационную среду, которая позволяет подключить все устройства и пользователей к единой инфокоммуникационной среде для создания прикладных систем мониторинга и управления, функционирующих по алгоритмам, реализующим заданные критерии оптимизации по известным показателям качества.

Пользователи на основе инструментов цифровой платформы, ЕИТС, федеральной сети LPWAN на транспорте создают собственные прикладные системы сбора, обработки и передачи данных, устанавливают собственные датчики, исполнительные устройства с использованием общей телекоммуникационной инфраструктуры. Доступ пользователей к федеральной сети LPWAN на транспорте осуществляется посредством цифровой платформы.

Распоряжением Правительства Российской Федерации от 11 сентября 2018 г. № 1912-р определено, что в целях создания федеральной системы транспортной телематики, расширения применения и массового внедрения глобальной навигационной спутниковой системы ГЛОНАСС в гражданских отраслях экономики Российской Федерации использование полос радиочастот радиоэлектронными средствами на территории Российской Федерации может осуществляться ООО «ГЛОНАСС-ТМ».

Вопрос выделения радиочастотного ресурса в объеме 2×2 МГц в диапазоне 863-876, а именно 863-865 МГц и 874-876 МГц для создания федеральной системы транспортной телематики решен, указанные полосы радиочастот выделены решением Государственной комиссии по радиочастотам от 30 ноября 2018 г. № 18-47-05 компании ООО «ГЛОНАСС-ТМ».

Фактически, ООО «ГЛОНАСС-ТМ» использует XNB технологию LPWAN, технические характеристики которой представлены в Таблице 4.

Таблица 4 - Технические характеристики технологии XNB

Технические характеристики	Значение	
	БС	АС
Э.И.М. (возможные номиналы)	25 мВт, 200 мВт, 500 мВт и 5 Вт	25 мВт, 100 мВт и 200 мВт
ДН антенны	Omni	
Поляризация	Вертикальная	
Репрезентативная ширина канала	15 кГц (выбрана самая широкая полоса)	
Описание спектра излучения передатчика для канала 150 Гц (скорость 1 кбит/с)	110 Гц на -3 дБ 140 Гц на -30 дБ 160 Гц на -60 дБ	
Описание спектра излучения передатчика для канала 1.5 кГц (скорость 1 кбит/с)	1100 Гц на -3 дБ 1400 Гц на -30 дБ 1600 Гц на -60 дБ	
Описание спектра излучения передатчика для канала 15 кГц (скорость 10 кбит/с)	11000 Гц на -3 дБ 14000 Гц на -30 дБ 16000 Гц на -60 дБ	
Репрезентативная высота антенны над уровнем Земли	10 м и 40 м	1.5 м и до 10 м
Рабочий цикл	До 100%	До 3%

План мероприятий программы «Цифровая экономика» по разделу «Информационная инфраструктура» предполагает, что сеть LPWAN будет строиться только вдоль транспортных объектов - автомобильных и железных дорог.

Полосы радиочастот, выделенные ООО «ГЛОНАСС-ТМ», представлены на рисунке 7 одновременно с полосами радиочастот,

выделенными в диапазоне 863-870 МГц для различных применений устройств малого радиуса действия.

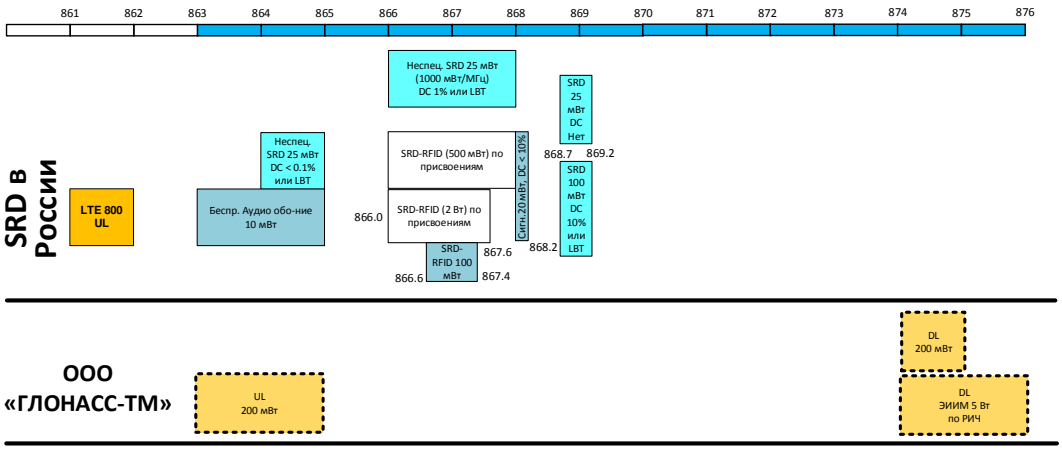

Рисунок 7 - Выделенные полосы радиочастот для ООО «ГЛОНАСС-ТМ»

Следует отметить, что в соответствии с Таблицей распределения полос радиочастот между радиослужбой Российской Федерации полоса радиочастот 863-876 МГц распределена воздушной радионавигационной службе (на первичной основе) и радиовещательной службе (на вторичной основе) и имеет категорию ПР. В этой связи использование указанных полос радиочастот с повышенной ЭИМ в интересах ООО «ГЛОНАСС-ТМ» может быть существенно ограничено территориально по условиям ЭМС с РЭС военного (специального) назначения.

Система Федеральной системы транспортной телематики будет строиться с радиочастотным дуплексом для упрощения реализации более мощных станций с мощностью до 5 Вт в специальных применениях. Для исключения помех на РЭС LTE800 и исключения помех от других SRD в прямом канале, обратный канал размещается в нижней части диапазона 863-876 МГц, а канал DL - в верхней его части.

Стоит отметить, что по своим характеристикам в части дальности связи сети ФСТТ будут сопоставимы с сетями NB-IoT в диапазонах ниже 1 ГГц, разворачиваемыми на основе базовых станций сотовых операторов.

Несмотря на некоторый выигрыш в бюджете радиолинии технологий UNB над технологией NB-IoT, данный выигрыш в значительной степени нивелируется наличием направленных антенн на БС NB-IoT и высокой плотностью существующей инфраструктуры сотовых операторов, которая будет переиспользована для сетей NB-IoT. Причем внедрение сетей NB-IoT фактически начато и данные сети возможно считать действующими. Таким образом, в среднесрочной перспективе невозможно выделить районы с существующей инфраструктурой операторов связи, которые не были бы обеспечены покрытием в стандарте NB-IoT.

Для реализации ГАИС «ЭРА-ГЛОНАСС» развернута сеть связи full MVNO, обеспечивающая максимальную зону покрытия сигналом GSM с собственной номерной ёмкостью. В настоящее время ожидается активное развертывание сетей NB-IoT в полосах радиочастот GSM с максимальным географическим охватом, в том числе для сбора, обработки и передачи телеметрической информации. При этом вся инфраструктура full MVNO, а также многие из технических решений по терминалам «ЭРА-ГЛОНАСС», могут быть относительно просто адаптированы для работы в новых сетях NB-IoT в силу принадлежности данного стандарта LPWAN к сотовым технологиям и развертыванию в диапазонах сетей GSM, что позволит задействовать существующую инфраструктуру операторов связи.

Радиочастотное обеспечение технологий и стандартов сетей «Интернета вещей»

Сети «Интернета вещей» в полосах радиочастот, используемых в общем порядке

В настоящее время узкополосные беспроводные сети связи IoT в полосах радиочастот, используемых в упрощенном порядке используют полосы, выделенные для устройств малого радиуса действия (SRD), в первую очередь, для так называемых неспециализированных устройств малого радиуса действия. Условия использования устройств малого радиуса

действия в части неспециализированных устройств в соответствии с текущей редакцией решения ГКРЧ от 7 мая 2007 г. № 07-20-03-001 показаны в таблице 3. Существуют и другие полосы радиочастот для SRD, которые потенциально могут быть использованы для узкополосных беспроводных сетей связи IoT, например, в диапазоне 433 МГц, однако именно диапазон 862-876 МГц является основным.

Таблица 3 - Условия использования неспециализированных устройств SRD в России в диапазоне 862-876 МГц

Полосы радиочастот	Технические характеристики			Рабочий цикл	Разнос каналов	Дополнительные условия использования
	Наименование	Значение	Размерность			
864 - 865 МГц	Максимальная ЭИМ	25	мВт	0,1% или режим LBT*		Запрещается использование в пределах аэропортов (аэродромов)***
868,7 - 869,2 МГц	Максимальная ЭИМ	25	мВт			***
866-868 МГц	Максимальная ЭИМ** Максимальная спектральная плотность ЭИМ**	25 1000	мВт мВт/МГц	1% или режим LBT*		Запрещается использование в пределах аэропортов (аэродромов)***
868,7-869,2 МГц	Максимальная ЭИМ**	100	мВт	10% или режим LBT*		***

* LBT - режим прослушивания перед излучением.

** При указании ограничений на максимальное значение ЭИМ и спектральной плотности ЭИМ является обязательным выполнение одновременно этих двух условий.

*** Применение базовых станций в сетях связи для сбора и обработки телематической информации осуществляется при условии:

- регистрации базовых станций в установленном в Российской Федерации порядке;

- ввода в эксплуатацию сетей связи в установленном в Российской Федерации порядке;
- Начиная с 1 декабря 2020 года допускается использование базовых станций, произведенных на территории Российской Федерации, которым присвоен статус телекоммуникационного оборудования российского происхождения (условие не распространяется на базовые станции, зарегистрированные до 1 декабря 2020 года)».

При этом ключевым диапазоном радиочастот для узкополосных беспроводных сетей связи IoT является диапазон радиочастот 868,7 - 869,2 МГц, где отсутствуют ограничения на рабочий цикл. Именно данные каналы могут использоваться БС узкополосных беспроводных сетей связи IoT, которым может требоваться периодически посылать сообщения множеству различных устройств. В полосах 864 - 865 МГц и 866-868 МГц размещаются дополнительные каналы траффика для разгрузки основных каналов, которые также могут использоваться и для сбора данных от абонентских устройств.

Для узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в упрощенном порядке, в России возможно выделить две основные особенности. Первая заключается в существенном отличии российского распределения полос радиочастот для устройств малого радиуса действия от европейского, к которому исторически тяготеет Российская Федерация. На рисунке 8 показано сравнение текущего использования в России с устоявшимся использованием полос радиочастот в Европе, а также в сравнении с новыми выделениями полос радиочастот для узкополосных беспроводных сетей связи IoT. Причем в Европе для узкополосных беспроводных сетей связи IoT начали выделять каналы с большей мощностью не только в рамках неспециализированных устройств, но и в рамках полос радиочастот для сбора телеметрии.

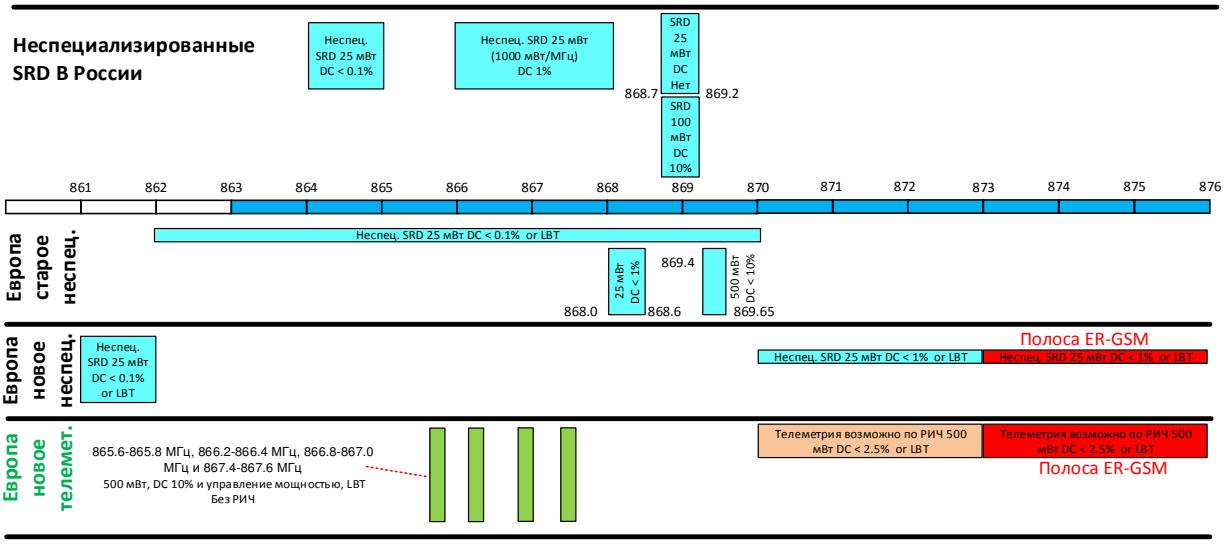

Рисунок 8 - Сравнение использования полос радиочастот, используемых в упрощенном порядке, в России и Европе

Как видно из рисунка, в России не выделены полосы радиочастот, которые в Европе имеют больший рабочий цикл или большую разрешенную мощность. Именно в этих полосах радиочастот развиваются все стандарты узкополосных беспроводных сетей связи IoT в Европе, при этом в России присутствуют стандарты собственной разработки. Так сети компании «Стриж», NB-FI и GoodWAN развиваются в полосе 868,7-869,2 МГц, а будущим сетям ФСТТ выделены полосы радиочастот 863-865 МГц и 874-876 МГц. Организации, заинтересованные в создании сетей на базе иностранного стандарта LoRaWAN были вынуждены подготовить профиль оборудования для Российской Федерации, отличный от других регионов, где для ключевых управляющих каналов в направлении DL установлена полоса радиочастот 868,7 - 869,2 МГц. Т.к. наибольшая добавленная стоимость приходится на приложения IoT, а не на услугу предоставления подключения по беспроводной технологии, общий позитивный эффект для экономики от гармонизации может оказаться более существенным.

Из рисунка 6 очевидна и вторая особенность использования узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в упрощенном порядке, а именно нехватка радиочастотного ресурса для полноценного развития. Первоначальное распределение полос

радиочастот в Европе оказалось недостаточным для внедрения узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в упрощенном порядке, что привело в последние годы к постоянному расширению данных полос радиочастот. Причем это расширение происходило как для абонентских устройств с излучаемой мощностью 25 мВт, так и для базовых станций с излучаемой мощностью 500 мВт. В России большая часть полос радиочастот выделена для использования с мощностью 25 мВт, а их общий объем в 3-4 раза меньше, чем в Европе. Для повышенной ЭИМ величиной 100 мВт в России выделена только полоса радиочастот 868,7-869,2 МГц, в то время как в Европе для ЭИИМ 500 мВт выделено в общей сложности более 1 МГц с возможностью расширения на национальном уровне до 4 МГц. Несмотря на расширение радиочастотного ресурса для неспециализированных устройств малого радиуса действия в России, в рамках существующего объема выделенного радиочастотного ресурса для устройств малого радиуса действия в диапазоне 863-876 МГц широкомасштабное внедрение узкополосных беспроводных сетей связи IoT несколькими операторами на одной территории будет существенно затруднено из-за повышения уровня взаимных помех.

Таким образом, сейчас сети LPWAN в России работают в участках диапазона 864-876 МГц: 864-865 МГц, 866-868 МГц и 868,7-869,2 МГц. В соответствии с условиями использования данных полос радиочастот применение базовых станций в сетях связи для сбора и обработки телематической информации осуществляется при условии регистрации базовых станций и ввода в эксплуатацию таких сетей связи. С 1 декабря 2020 года допускается только использование базовых станций, произведенных на территории Российской Федерации, которым присвоен статус телекоммуникационного оборудования российского происхождения. Данное условие не распространяется на базовые станции, зарегистрированные до 1 декабря 2020 года.

Сети «Интернета вещей» в полосах радиочастот, использующихся в общем порядке

Ситуация с радиочастотным обеспечением узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в общем порядке, более оптимистичная. И сети NB-IoT для наиболее низкоскоростных и энергоэффективных устройств, и сети LTE-eMTC могут внедряться в рамках ранее выделенных полос радиочастот.

Следует отметить, что решением ГКРЧ от 28 декабря 2017 года № 17-44-06 «Об использовании полос радиочастот радиоэлектронными средствами стандарта LTE и последующих его модификаций в режиме NB-IoT» разрешено использование полос радиочастот 453-457,4 МГц и 463-467,4 МГц, 791-820 МГц, 832-862 МГц, 880-890 МГц, 890-915 МГц, 925-935 МГц, 935-960 МГц, 1710-1785 МГц, 1805-1880 МГц, 1920-1980 МГц, 2110-2170 МГц, 2500-2570 МГц и 2620-2690 МГц для применения РЭС стандарта LTE и последующих его модификаций в режиме NB-IoT (далее - РЭС в режиме NB-IoT) на территории Российской Федерации. Основные технические характеристики РЭС в режиме NB-IoT, утверждены и указаны в приложении к решению ГКРЧ от 28 декабря 2017 года № 17-44-06.

При этом наибольшую емкость при прочих равных условиях показывают узкополосные беспроводные сети связи IoT в полосах радиочастот, используемых в общем порядке, в силу их синхронного радиоинтерфейса и отсутствия внешних помех. Так, одна базовая станция с одной несущей NB-IoT с шириной 200 кГц может обслуживать 67 тыс. устройств с достаточно интенсивным трафиком, эквивалентным получению 7500 сообщений в секунду. Каждая последующая несущая будет добавлять возможность подключения порядка 110 тыс. устройств или 12,3 тыс. сообщений в секунду. Выделение 10 каналов или 2 МГц на одной базовой станции только для NB-IoT позволит обслуживать порядка 1 млн. устройств или 100 тыс. сообщений в секунду.

Более сложная ситуация наблюдается с развитием сетей связи стандарта LTE-eMTC, который как ожидается будет внедрен в дополнение к сетям связи стандарта NB-IoT. Данные сети могут быть внедрены в различных диапазонах радиочастот, и, в частности, в наиболее востребованном в Российской Федерации диапазоне радиочастот 1800 МГц. Однако будущее использование LTE-eMTC ожидается и за пределами крупных городов, что потребует расширения зон обслуживания сетей. Для такого использования необходимо использование диапазонов LTE ниже 1 ГГц. В настоящее время ограничения от систем ВРНС в диапазонах 800 МГц и 900 МГц существенно сдерживают такое использование, а диапазон 700 МГц используется для эфирного телевизионного вещания. Для развития сетей LTE-eMTC потребуется высвобождение диапазонов радиочастот 700 МГц, 800 МГц и 900 МГц особенно вне городов в рамках проведения конверсии и перераспределения радиочастотного ресурса.

Таким образом, возможными радиочастотными диапазонами для создания сетей связи «Интернета вещей» с учетом опыта их внедрения за рубежом являются диапазоны 700 МГц, 800 МГц, 900 МГц и 1800 МГц.

В части узкополосных беспроводных сетей следует отдельно рассматривать ситуацию с радиочастотным обеспечением для сетей NB-IoT и eMTC.

Так, единственной сложностью использования диапазонов ниже 1 ГГц для развертывания сетей NB-IoT является наличие ограничений со стороны систем ВРНС (за исключением диапазона 450 МГц), что может быть решено путем частотно-территориального планирования.

Особенности внедрения узкополосных беспроводных сетей связи IoT на основе стандарта eMTC схожи с особенностями традиционных сетей сотовой подвижной связи стандарта LTE, а именно существенные территориальные и мощностные ограничения на работу оборудования, исключающие возможность обеспечения сплошного покрытия. Данные ограничения в будущем могут стать препятствием на пути цифровизации

ключевых отраслей экономики за пределами крупных городов, где требуется развертывание сетей LTE в диапазонах радиочастот ниже 1 ГГц. Нужно отметить следующие задачи и мероприятия по их решению:

- в диапазоне 900 МГц требуется проведение конверсии с системами ВРНС;

- в диапазоне 800 МГц требуется проведение конверсии с системами ВРНС и РЛС;

- в диапазоне 700 МГц требуется проведение конверсии с системами ВРНС, а также вывод сетей наземного эфирного телевещания в полосы радиочастот ниже 694 МГц и установление гармонизированного радиочастотного плана для сетей подвижной службы.

Основным преимуществом сетей LPWAN, таких как NB-IoT и LTE-eMTC, в полосах радиочастот, используемых в общем порядке, перед сетями LPWAN в полосах радиочастот, используемых в упрощенном порядке, является предсказуемость электромагнитной обстановки и возможность использования безколлизионных методов распределения частотно-временных ресурсов канала. Все это позволяет формировать услуги с заданным уровнем качества и надежности, которые путем настройки сети могут варьироваться в широких пределах в зависимости от потребностей той или иной отрасли. Помимо вопросов ЭМС, узкополосные беспроводные сети связи IoT в полосах радиочастот, используемых в общем порядке, подлежат сертификации и проверке при вводе в эксплуатацию, что также обеспечивает более высокий уровень надежности и контроля со стороны регулятора.

Данные свойства узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в общем порядке, особенно важны для основных социально значимых для государства сфер и областей применения, в которых принципиален высокий уровень надежности и готовности сети. К таким социально значимым сферам деятельности возможно отнести достаточно широкий круг применений IoT. Так, данные о потреблении энергоресурсов или воды могут использовать для управления нагрузками на

сети, что требует постоянства и надежности в получении измеряемых значений с таких счетчиков. Нарушения в работе датчиков и актуаторов в системах освещения, тепло-, энерго- и водоснабжения, канализации могут привести к катастрофическим последствиям в плотно заселенных городах.

Кроме того, использование технологий IoT в полосах радиочастот, используемых в упрощенном порядке, в городском хозяйстве, которое является наиболее массовым сегментом применения IoT, может дать техническую возможность для атак на городскую инфраструктуру с использованием множества источников помех на основе взломанных IoT устройств, что практически невозможно в сетях LPWAN в полосах радиочастот, используемых в общем порядке, в силу других принципов организации таких сетей. Таким образом, применение IoT для ЖКХ и коммунальных структур критически важно для жизни и здоровья населения, а их помехозащищенность и надежность целесообразно обеспечивать за счет использования узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в общем порядке.

Значительная часть промышленных применений IoT, например, таких как управление заслонками, контроль температуры и давления, поиск утечек на трубопроводах, также являются критичными и требуют обеспечения максимальной надежности. Многие медицинские применения, связанные с контролем приема лекарств, также требуют высокого уровня контроля, надежности и информационной безопасности.

Таким образом, можно определить перечень социально значимых для государства сфер и областей применения, включающий: ЖКХ и городское хозяйство, здравоохранение, промышленное производство, которые являются наиболее критичными для жизни и здоровья граждан страны, а также для сохранности ЖКХ и промышленной инфраструктуры, и ограничить в них применения IoT в полосах радиочастот, используемых в упрощенном порядке, за счет использования только лицензируемых средств связи и сертифицированных устройств.

Предложения по радиочастотному обеспечению сетей «Интернета вещей»

Предложения по радиочастотному обеспечению узкополосных беспроводных сетей связи IoT следует различать для полос радиочастот, используемых в общем и упрощенном порядках.

Для узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в упрощенном порядке, ключевым мероприятием является расширение возможности использования отдельных полос радиочастот в диапазоне 862-876 МГц. В первую очередь речь идет о гармонизации полос радиочастот с европейским рынком в части полос радиочастот с повышенной ЭИМ или большим разрешенным рабочим циклом. К таким полосам радиочастот относятся полоса радиочастот 868,0-868,6 МГц с мощностью 25 мВт и рабочим циклом 1% и полоса радиочастот 869,4-869,65 МГц с мощностью 500 мВт и рабочим циклом 10%.

Также для применения узкополосными беспроводными сетями связи IoT целесообразно рассмотреть возможность использования полос радиочастот 866,2-866,4 МГц, 866,8-867,0 МГц и 867,4-867,6 МГц с мощностью 500 мВт и рабочим циклом 10%. Помимо этого, следует продолжить планомерное увеличение доступного для устройств малого радиуса действия объема радиочастотного ресурса в диапазоне 863-876 МГц с мощностью 25 мВт и рабочим циклом 1%, в частности в полосах 862-863 МГц и 870-874 МГц.

Для выполнения вышеописанных задач в полном объеме требуется проведение организационно-технических мероприятий, обеспечивающих совместное использование радиочастотного спектра радиоэлектронными средствами, предназначенными для нужд государственного управления, нужд обороны страны, безопасности государства и обеспечения правопорядка, с радиоэлектронными средствами гражданского назначения в рамках конверсии радиочастотного спектра с целью расширения применения РЭС гражданского назначения в указанных полосах радиочастот. Но в

краткосрочной перспективе целесообразно принять по результатам необходимых исследований решение ГКРЧ по тем полосам радиочастот, которые могут быть выделены в упрощенном порядке без проведения конверсии.

Для узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в общем порядке, большинство полос было выделено ранее. Тем не менее, особенности внедрения узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в общем порядке, схожи с особенностями традиционных сетей сотовой подвижной связи, в диапазонах радиочастот ниже 1 ГГц, используемых для обеспечения покрытия за пределами крупных городов

С учетом сроков проведения конверсии в диапазонах 800 МГц и 900 МГц в краткосрочной перспективе следует сосредоточить усилия на высвобождение полосы радиочастот 694-790 МГц от сетей наземного эфирного телевизионного вещания, что позволит без проведения конверсии внедрять сети на основе технологии LTE-eMTC с широким охватом территории. Несмотря на возможность развертывания сетей NB-IoT в диапазонах от 450 МГц до 2600 МГц, целый ряд применений будут требовать использования стандарта LTE-eMTC, что и делает приоритетным высвобождение радиочастотного ресурса для сетей LTE в диапазоне 694-790 МГц.

Вместе с тем, при рассмотрении перспектив развертывания сетей «Интернета вещей» и, в частности, технологии NB-IoT следует руководствоваться решением ГКРЧ № 17-44-06 от 28 декабря 2017 г., которым разрешено использование на территории Российской Федерации для указанных целей диапазонов радиочастот: 453-457,4 МГц и 463-467,4 МГц, 791-820 МГц, 832-862 МГц, 880-890 МГц, 890-915 МГц, 925-935 МГц, 935-960 МГц, 1710-1785 МГц, 1805-1880 МГц, 1920-1980 МГц, 2110-2170 МГц, 2500-2570 МГц и 2620-2690 МГц.

Внедрение узкополосных беспроводных сетей связи IoT на основе технологии LTE-eMTC требует решения вопроса радиочастотного обеспечения сетей LTE в диапазонах ниже 1 ГГц. Из всех рассматриваемых диапазонов радиочастот, с точки зрения необходимости проведения конверсии, только диапазон 700 МГц может быть высвобожден в среднесрочной перспективе без проведения длительной и дорогостоящей конверсии. Тем не менее, внедрение сетей LTE-eMTC в полосе радиочастот 694-790 МГц требует проведения целого ряда мероприятий, охватывающих вопросы социального, организационно-технического и экономического характера. Общий перечень мероприятий и действий для внедрения сетей LTE-eMTC в полосе радиочастот 694-790 МГц возможно охарактеризовать следующим образом:

- оценить необходимое количество мультиплексов ЦТВ для работы федеральных и региональных каналов с учетом оценки необходимости перехода ТВ вещания на телевидение высокой четкости в рамках эфирного телевизионного вещания;

- на государственном уровне зафиксировать решение о внедрении сетей LTE (включая LTE-eMTC) в полосе радиочастот 694-790 МГц с указанием конкретных сроков;

- для гармонизированного использования диапазона 694-790 МГц сетями LTE (включая LTE-eMTC) внести изменение в решение ГКРЧ №11-12-02 от 8 сентября 2011 года, в части изменения радиочастотного плана;

- провести оптимизацию частотно-территориального плана ЦТВ для заданного числа мультиплексов и с учетом планов отключения аналогового вещания и планов по объему ЦТВ с высвобождением максимально возможного радиочастотного ресурса в полосе 694-790 МГц для всей территории страны.

В части внедрения узкополосных беспроводных сетей связи IoT различных технологий в полосах радиочастот, используемых в упрощенном порядке, необходимо продолжить расширение полос радиочастот для

неспециализированных устройств малого радиуса действия с учетом возможной международной гармонизации использования таких полос радиочастот:

- расширение полос радиочастот с ЭИМ порядка 25 мВт и рабочим циклом до 1%, в первую очередь, за счет рассмотрения полос радиочастот 862-863 МГц и 870-874 МГц;

- расширение полос радиочастот с ЭИИМ 100 мВт и более (предпочтительно 500 мВт) с рабочим циклом до 10%, в первую очередь за счет полос радиочастот 866,2-866,4 МГц, 866,8-867,0 МГц и 867,4-867,6 МГц, а также в полосе радиочастот 870-874 МГц.

Проведенный анализ ситуации по радиочастотному обеспечению российских сетей «Интернета вещей» позволяет сделать следующие выводы:

1. Сети в полосах радиочастот, используемых в общем порядке, (NB-IoT, LTE-eMTC) могут внедряться в рамках ранее выделенных полос радиочастот. На сегодняшний день доступна полоса более 20 МГц для применения как узкополосных сетей LPWAN в составе сетей ПРТС, так и узкополосных сетей технологий LPWAN. Сети Интернета Вещей не требуют в среднесрочной перспективе дополнительного выделения радиочастотного ресурса для своей эффективной работы.

2. Для развития сетей LTE-eMTC может быть использован диапазон 1800 МГц, в перспективе потребуется высвобождение диапазонов радиочастот 700 МГц, 800 МГц, в первую очередь - в диапазоне 694-790 МГц.

3. Из-за недостатка радиочастот для внедрения узкополосных беспроводных сетей связи IoT в полосах, используемых в упрощенном порядке, предлагается провести конверсию с целью гармонизации с европейскими радиочастотами (868,0-868,6 МГц, 869,4-869,65 МГц), а также выделить другие дополнительные радиочастоты (в диапазоне 862-876 МГц).

4. Сети LPWAN для федеральной системы транспортной телематики должны функционировать на основе радиочастотного диапазона

863-865/874-876 МГц, выделенного Решением ГКРЧ №18-47-05 (дсп) от 30 ноября 2018 года, а также могут использовать:

- на локальных объектах радиочастотный ресурс в полосах, выделенных для применения неспециализированных устройств малого радиуса действия: 433,92 МГц и 149,975-150,05 МГц, 866-868 МГц, 868,7 - 869,2 МГц и другие.

- выделенный для целей построения сети сбора, обработки и передачи телематической информации по технологии NB-IoT радиочастотный ресурс в диапазонах 1800 МГц.

Взаимоувязанное развитие сетей «Интернета вещей» и цифровых платформ «Интернета вещей» в Российской Федерации

Типовая архитектура сетей связи «Интернета вещей»

Для взаимоувязанного развития различных узкополосных беспроводных сетей связи IoT и в целях обеспечения регулирования, целесообразно определить типовую архитектуру таких сетей и выделить ключевые интерфейсы, отвечающие за взаимодействие отдельных уровней модели «Интернета вещей».

Узкополосные беспроводные сети связи IoT в широком смысле представляют собой полную цепочку всех уровней модели «Интернета вещей». Однако для целей регулирования развития различных узкополосных беспроводных сетей связи IoT нет необходимости воспроизводить все элементы такой модели, достаточно указать ключевые уровни взаимодействия и абстрактные интерфейсы между этими уровнями, к которым могут быть выработаны требования на государственном уровне, обеспечивающие системный подход к развитию услуг IoT. Структура такой модели приведена на рисунке 9, на котором показаны ключевые блоки, формирующие всю цепочку IoT-услуг и ключевые интерфейсы, формирование требований к которым необходимо для создания взаимоувязанной инфраструктуры IoT.

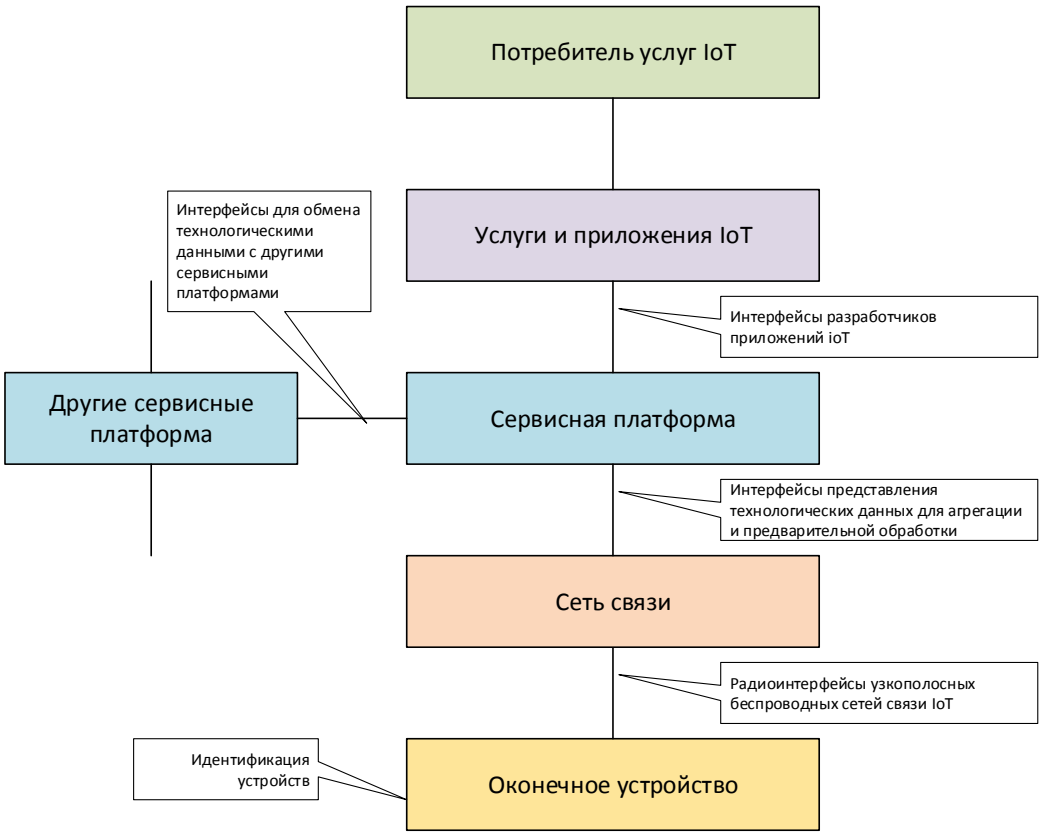

Рисунок 9 - Предлагаемая типовая архитектура узкополосных беспроводных сетей связи IoT

Важно отметить, что в предлагаемой типовой архитектуре допускается, что практически все уровни цепочки услуг IoT могут принадлежать различным компаниям и организациям. Более того, может существовать большое количество различных технических реализаций стека протоколов от оконечного устройства IoT до пользователя услуг IoT. Как видно из рисунка, все многообразие различных беспроводных технологий занимает лишь один нижний интерфейс. Более того, это многообразие не ограничено только узкополосными беспроводными сетями связи IoT.

По указанным причинам взаимоувязанное развитие различных узкополосных беспроводных сетей связи IoT необходимо регулировать отдельно для каждого уровня в максимально гибкой и технологически нейтральной форме для исключения создания необоснованных барьеров для развития услуг IoT. Тем не менее, регулирование, направленное на развитие узкополосных беспроводных сетей связи IoT, требуется для эффективного использования всей экосистемы IoT, в особенности в следующих сферах:

- информационной безопасности;

- идентификации устройств IoT;

- управляемости устройствами IoT, включая возможности удаленного отключения от сети и запроса данных и вычислительной мощности;

- стандартизации открытых протоколов между уровнями обмена накопленными технологическими данными;

- общего контроля хранения, агрегации и доступа к технологическим данным, накапливаемым в ключевых отраслях экономики;

- подключения технических средств для реализации системы оперативно-розыскных мероприятий;

- возможности обновления программного обновления (прошивки) устройств IoT через радиоэфир.

Приведенные выше направления касаются не только технического, но и административного регулирования процессов, связанных с оборотом технологических данных в общей экосистеме IoT.

В первую очередь государственное регулирование должно быть направлено на обеспечение совместимости различных элементов и подсистем в сфере IoT и обеспечение их информационной безопасности. Не менее важным является сохранение достаточно общего характера регулирования, которое бы способствовало развитию IoT в Российской Федерации и было бы одинаково применимо ко всем участникам рынка IoT.

Идентификация устройств «Интернета вещей»

Для обеспечения возможности накопления «больших данных» от разнородных систем сбора информации и создания алгоритмов обработки таких данных с целью выявления действий по оптимизации тех или иных процессов в экономике в целом или конкретном приложении требуется однозначная идентификация источника информации (например, сенсора) и получаемой информации. При отсутствии идентификации устройств IoT ожидается накопление разрозненной информации в различных сегментах

экономики или в разных узкополосных беспроводных сетях связи IoT, которая в последствии не может быть сопоставлена между собой без сложной обработки, требующей раскрытия внутренней идентификации всех задействованных систем.

По этой причине целесообразно введение той или иной системы идентификации устройств IoT на международном и на национальных уровнях. В настоящее время существует большое количество систем идентификации устройств, которые используются для управления устройствами IoT. Причем на разных уровнях типовой архитектуры IoT могут существовать разные подходы к идентификации. Так, например, на сетевом уровне IoT устройствам могут присваиваться IP адреса для маршрутизации данных, но при этом IP адреса могут быть динамическими, что не позволяет использовать их в качестве уникального идентификатора. Помимо этого, во многих узкополосных беспроводных сетях связи IoT адресация по IP может не использоваться в силу ее слабой энергоэффективности.

Необходимо отметить, что от уровня к уровню идентификация устройств может подменяться, т.е. оконечному IoT устройству с определенным физическим адресом на канальном уровне сначала назначается соответствующий логический адрес на сетевом уровне, который в последствии может быть заменен на идентификатор на уровне платформы. При этом очень важным свойством является фиксированность соотношения идентификатора с фактическим устройством IoT (физическим адресом), а также универсальность в применении идентификатора в различных отраслях.

С учетом рассмотрения узкополосных беспроводных сетей связи IoT можно также рассматривать системы идентификации, которые предлагаются в качестве основы для сетевого уровня, а также для использования на более высоком уровне. Так, для узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в общем порядке, сейчас существует однозначная система идентификации всех абонентов на основе номера

MSISDN, описанная в Рекомендации МСЭ-Т F.748.1 «Requirements and common characteristics of the IoT identifier for the IoT service». Данный 15-значный номер в десятеричной системе исчисления должен являться уникальным адресом в сетях 3GPP, в том числе и в сетях NB-IoT и LTE-eMTC, который и обеспечивает как идентификацию, так и возможность прямой адресации.

Однако ожидается, что этого объема может быть недостаточно для обслуживания устройств в глобальном масштабе. По этой причине в 3GPP для межмашинных коммуникаций также существует вариант работы устройств без MSISDN на основе назначения внутрисетевых идентификаторов. При этом для глобального доступа к таким устройствам из внешних сетей определен формат нового внешнего идентификатора на основе формата IETF RFC 4282, который позволяет привязывать устройства к доменным именам.

Такой тип идентификатора может использоваться в тех устройствах IoT, для которых не будет назначаться номер MSISDN. При этом связь между внешним идентификатором и конкретным устройством внутри сети предполагается осуществлять по номеру IMSI. При этом стоит отметить, что IMSI тоже является 15-значным номером. Вместе с этим, важно отметить что IMSI также подвержена клонированию и подделкам, в связи с чем требуется рассмотреть более универсальный подход для идентификации IoT-устройств.

Вопросы ненадежности кодов IMEI и связанных с ним технологий описаны в Техническом отчете МСЭ-Т «О безопасности и надежности идентификаторов IMEI» TD730-R1 от 15.02.2019 года.

В узкополосных беспроводных сетях связи IoT в полосах радиочастот, используемых в упрощенном порядке, отсутствует унифицированный метод идентификации и адресации. Так, например, в стандарте Sigfox или GoodWAN идентификация устройств производится на уровне облачной инфраструктуры Sigfox или GoodWAN по 32-битному идентификатору, который дает возможность дать уникальный идентификатор порядка 4.3

млрд. устройств. По всей видимости дальнейшее различение устройств возможно только за счет единого централизованного облака Sigfox или GoodWAN, где помимо данного идентификатора возможно использовать информацию о географическом расположении устройства.

В сетях LoRaWAN для идентификации используется 64-битный номер в формате IEEE EUI-64. В настоящее время данный номер привязан напрямую к 48-битному MAC-адресу, используемому в MAC-протоколе LoRaWAN. При этом адресное пространство в LoRAWAN фактически привязано к MAC-пространству адресов IEEE (порядка 281 трлн. комбинаций). 16-бит зарезервировано в IEEE EUI-64 для дальнейшего развития технологий.

Для создания более универсальной системы идентификации, которая могла бы играть роль системы адресации, в МСЭ-Т в настоящее время разрабатывается новая Рекомендация МСЭ-Т «Internet of Things Naming Numbering Addressing and Identifiers». Данная рекомендация, в частности, рассматривает возможность расширения стандартной телефонной нумерации, описанной в Рекомендации МСЭ-Т E.164, в коде 878, определенном для межмашинных коммуникаций без привязки к территории.

Предполагается, что данная 15-символьная конструкция, изначально определенная для устройств с телефонным номером, может быть расширена до универсального номера. В частности, в случае расширения алфавита кодирования с использованием всех 4-х бит (в шестнадцатеричном коде) данный идентификатор позволяет описать до 255 триллионов устройств или, например, выделить каждой стране не менее одного триллиона идентификаторов. Если же расширить кодирование до полного ASCII кода, т.е. до 8 бит на символ, ресурс идентификаторов возможно будет считать неограниченным. При этом МСЭ-Т сможет переиспользовать систему и принципы глобального выделения номеров для стран мира. Окончание работы над данной Рекомендацией МСЭ-Т ожидается к 2020 году.

На данный момент ни одна из систем идентификации не получила статуса эталонной, более того, существует несколько конкурирующих систем идентификации.

Важной особенностью при выборе технологии идентификации является обеспечение ее подлинного международного управления и независимости распределения ресурсов идентификации. Данным критериям отвечает технология Digital Object Architecture (DOA), стандартизированная в МСЭ (Рекомендация МСЭ-Т X.1255, разрабатываемая Рекомендация МСЭ-Т Y.4459 «Architecture for IoT interoperability») и управляемая некоммерческой неправительственной организацией DONA Foundation. Глобальная система администрирования DOA предполагает развертывание и функционирование нескольких администраторов, равно представляющих различные регионы мира. Сама DONA Foundation управляется Советом, который состоит из представителей региональных администраторов. Россия является членом Совета. В сентябре 2018 года в России был развернут национальный администратор системы DOA – МРА.

Использование идентификации на базе DOA позволит учитывать все существующие уникальные идентификаторы (например, MAC, IMEI, ID, IPv4/IPv6 и др.), обеспечив идентификацию устройств и приложений интернета вещей без привязки к конкретному идентификатору.

Согласно Концепции архитектуры цифровых объектов предусматривает, что каждый объект - обладает набором признаков, определяющих его сущность и, благодаря этому, выделяющих его из множества других. Т.е., фактически, можно задействовать все существующие идентификаторы (физический + логический адрес, а также мета данные о самом объекте, например, версия прошивки, местоположение и др.).

Таким образом, различные признаки суммарно являются идентификаторами.

Идентификация необходима для решения таких задач, как:

- однозначное определение объекта;

- распознавание объекта по его свойствам;
- группирование объектов по определенным признакам;
- выделение объекта из множества подобных.

Цифровая объект (согласно концепции международных рекомендаций МСЭ-Т X.1255) – «структура обнаружения информации по управлению определением идентичности», общепринятая структура данных, состоящая из одного или нескольких элементов, благодаря которой обеспечивается функциональная совместимость информационных систем в интернете.

По факту, цифровой объект – это объект, состоящий из структурированной последовательности битов, имеющий название, уникальный идентификатор и атрибуты, описывающие его свойства.

В контексте архитектуры DOA, цифровой объект – данные, которые не зависят от платформы. Для управления цифровыми объектами используются три архитектурных компонента. Каждый из компонентов может использоваться самостоятельно, но в комбинации они обеспечивают распределенную и масштабируемую систему управления информацией в интернете. Три основных компонента:

1. масштабируемая и распределенная система идентификаторов и резолюции цифровых объектов;
2. репозитории доступа и управления цифровыми объектами;
3. реестры для поиска и обнаружения объектов.

Система резолюции связывает идентификаторы с информацией о состоянии цифровых объектов. К примеру, такая информация может содержать местонахождение данного объекта в интернете или требования к доступу, информацию об аутентификации и т.п. Создатель объекта или авторизованный администратор предоставляет эту информацию с использованием инфраструктуры публичных ключей, которая интегрирована в DOA. Технология публичных ключей предполагает использование двух ключей для шифрования – публичного и частного.

Цифровые объекты – ключевой элемент, вокруг которого выстроены другие компоненты и сервисы. Цифровые объекты не заменяют существующие форматы и структуры данных, но обеспечивают общепринятые способы представления этих форматов и структур. Это позволяет их однозначно интерпретировать и перемещать между различными гетерогенными информационными системами в ходе изменений в системах с течением времени.

На уровне управления распределенная архитектура технологии позволяет создавать сервисы и регламентировать процессы на уровне отдельно взятого МРА, то есть каждый из текущих девяти МРА может разрабатывать собственную бизнес-модель, обеспечивая полностью независимую систему эмиссии идентификаторов и управления системой на национальном или региональном уровне.

Таким образом, в перспективе для всех сетей, предлагается ввести идентификацию устройств на основе схем, рассматриваемых в МСЭ-Т, частности DOA, при условии обеспечения государственного суверенитета в использовании выбранной системы идентификации. При этом идентификацию целесообразно вводить на более верхних уровнях типовой архитектуры между сетевым уровнем и сервисной платформой или на уровне сервисной платформы, сохранив при этом собственные методы идентификации внутри радиоинтерфейса узкополосных беспроводных сетей связи IoT или внутри сетевого уровня.

Таким образом, систему идентификации DOA целесообразно рассматривать, как один из возможных методов идентификации устройств IoT. Окончательное решение о применении/не применении того или иного метода идентификации должно приниматься на уровне регулятора отрасли, с учетом результатов мероприятий федеральных проектов Национальной программы «Цифровая экономика Российской Федерации».

Регулятор отрасли должен также определять правила функционирования Реестра идентификаторов устройств IoT. которые не распространяются на устройства, используемые в рамках частных сетей.

Стандартизация протоколов и форматов данных при взаимодействии различных сетей «Интернета вещей» и цифровых платформ «Интернета вещей»

Совместимость различных систем и интерфейсов оказывает практически такое же влияние на целостность экосистемы IoT как и идентификация. Использование большого числа закрытых стандартов и несовместимых интерфейсов не позволяет объединять и обрабатывать данные от различных источников без трудоёмких и дорогостоящих доработок. Более того, отсутствие открытых и доступных для всех стандартов создает ситуацию жесткой привязки клиентов IoT-услуг к поставщикам платформ и сервисов, что может создавать риски монополии или необоснованного отключения от таких услуг со стороны поставщика. В связи с этим возникает необходимость установления общих требований и норм по использованию открытых стандартов и интерфейсов для реализации недискриминационного доступа к узкополосным беспроводным сетям связи IoT, в особенности на верхних уровнях типовой архитектуры. Для критичных применений следует установить стандарты на структуру первичных данных, например, стандартные поля для показаний счетчиков, транспортных данных и т.п. Форматы целесообразно стандартизовать в рамках конкретных отраслей.

Фрагментация экосистемы IoT в целом является одной из ключевых проблем, стоящих перед построением и развитием узкополосных беспроводных сетей связи IoT во всем мире. Страны Евросоюза, США, Китай, другие развитые страны, а также технологические компании и международные организации (МСЭ-Т, OneM2M, ETSI, CEN/ISO, IEEE и ITEF) ведут работу по созданию международных стандартов для IoT для

обеспечения совместимости между различными уровнями типовой архитектуры, а также между различными сервисными платформами для исключения фрагментации экосистемы IoT в будущем.

В качестве примера протоколов предоставления услуг IoT можно привести совместную работу МСЭ-Т и OneM2M над системой протоколов для универсальных сервисных платформ, применимых к различным сетям связи, включая узкополосные беспроводные сети связи IoT. На рисунке 10 показаны разрабатываемые OneM2M протоколы для предоставления услуг IoT и их место в типовой архитектуре узкополосных беспроводных сетей связи IoT.

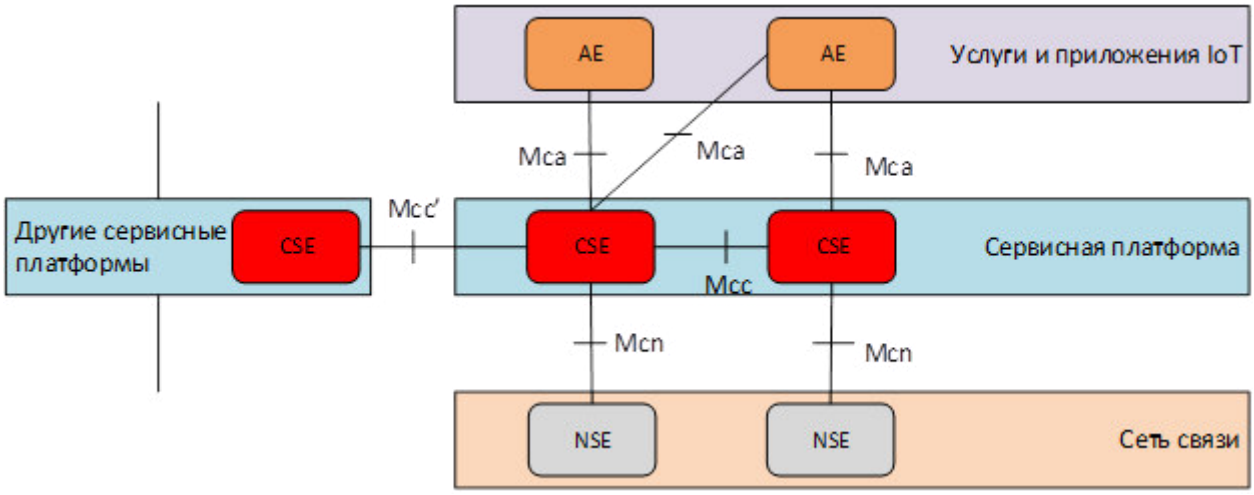

Рисунок 10 - Пример стандартизации протоколов OneM2M в МСЭ-Т для открытой экосистемы IoT

На рисунке использованы следующие сокращения:

AE (Application Entity) - программно-аппаратная реализации конкретного приложения IoT (например отслеживание транспорта);

CSE (Common Services Entity) - программно-аппаратная реализация общих для различных услуг функций (например, управление данными, управление устройствами, учет местоположения на уровне сервисной платформе т.д.);

NSE (Network Services Entity) - представление сетевых узлов, отвечающих за информационный обмен с оконечными устройствами,

управление данными устройствами на уровне сети, отслеживание их метаположение на уровне сети и т.д.);

Mca, Mcn, Mcc, Mcc’ - стандартизованные протоколы между различными уровнями типовой архитектуры.

Как видно из рисунка 10, в представленном подходе отсутствуют предложения по стандартизации сетей доступа и реализации доступа к приложениям IoT и конечным пользователям, т.к. считается, что данные вопросы в меньшей степени нуждаются в жесткой стандартизации. Помимо стандартизации протоколов, на уровне услуг IoT также идет существенная работа по стандартизации форматов сбора данных от счетчиков и сенсоров в других стандартизующих организациях. Однако данные прикладные форматы целесообразно стандартизовать в рамках регулирования отдельных сфер экономики и не включать в более общее регулирование узкополосных беспроводных сетей связи IoT.

Таким образом, в рамках регулирования сетей связи для IoT, включая узкополосные беспроводные сети связи IoT, целесообразно определить на национальном уровне ключевые международные стандарты общих протоколов и интерфейсов для создания открытой экосистемы IoT и недискриминационного доступа к сервисным платформам IoT, которые впоследствии должны быть внедрены участниками рынка IoT вне зависимости от конкретной технологии радиодоступа. Исключение могут составить только ведомственные и технологические сети связи, выполняющие задачи в интересах конкретного предприятия или организации и не предоставляющие услуги IoT сторонним пользователям.

Стандартизация методов защиты в протоколах взаимодействия различных сетей «Интернета вещей» и цифровых платформ «Интернета вещей», а также их отдельных компонентов

Помимо обеспечения совместимости между различными сегментами экосистемы IoT и возможности осмысленного сбора данных за счет

идентификации устройств IoT наиболее важным фактором для внедрения услуг IoT является информационная безопасность. В определенной степени вопрос информационной безопасности является краеугольным для массового внедрения услуг IoT, в особенности в критически важных отраслях экономики.

Появление сотен миллионов новых подключенных устройств IoT, осуществляющих сбор информации и управление различными процессами, создает новые риски информационной безопасности и требует доработки существующей нормативно-правовой базы. Вопросы информационной безопасности должны охватывать все уровни типовой архитектуры узкополосных беспроводных сетей связи IoT, а точнее, всех уровней модели IoT.

Комплексные вопросы информационной безопасности, применимые, в том числе, к узкополосным беспроводным сетям связи IoT, рассматриваются в отдельном направлении реализации программы «Цифровая экономика Российской Федерации». По этой причине в рамках данной Концепции рассматриваются только ключевые аспекты регулирования методов защиты и информационной безопасности, необходимые для успешного построения и развития узкополосных беспроводных сетей связи IoT. Данные аспекты проиллюстрированы на рисунке 11.

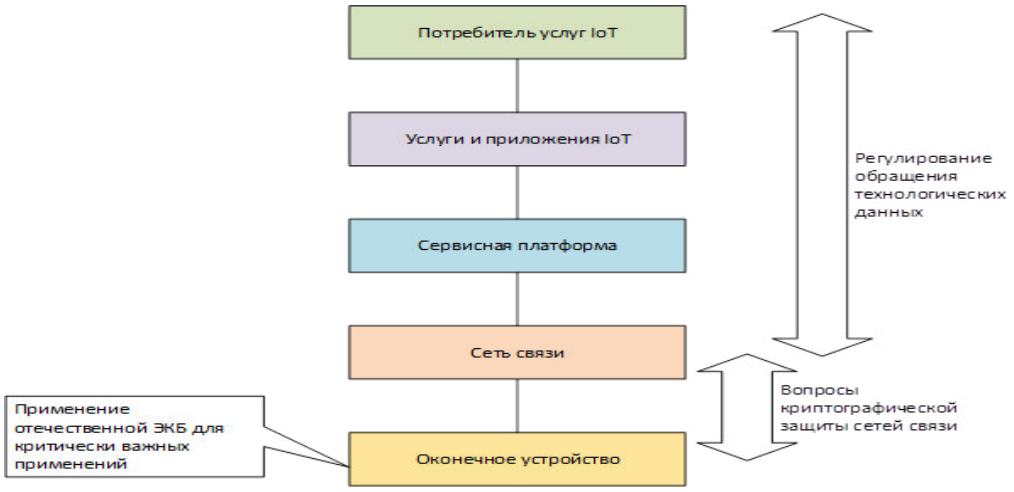

Рисунок 11 - Отдельные аспекты обеспечения информационной безопасности узкополосных беспроводных сетей связи IoT

Наиболее глобальным вопросом методов защиты и информационной безопасности в узкополосных беспроводных сетях связи IoT является регулирование хранения и обработки огромных массивов данных, собираемых от множества датчиков и сенсоров. Такие данные могут нести в себе критически важную информацию, которая может являться основой для принятия решений по управлению критически важными процессами. Таким образом, внесение искажений даже в данные телеметрии, может впоследствии приводить к нарушению работы инфраструктуры. По этой причине необходимо на уровне государства установить изначально достаточно высокий уровень требований к хранению и обработке таких данных. Данный вопрос целесообразно рассматривать в рамках регулирования «больших данных». Регулирование «больших данных» включено в федеральный проект «Нормативное регулирование цифровой среды» национальной программы «Цифровая экономика Российской Федерации».

Вопрос обеспечения информационной безопасности тесно связан с вопросами стандартизации протоколов обмена между различными уровнями типовой архитектуры узкополосных беспроводных сетей связи IoT, в особенности на уровне взаимодействия сервисных платформ. Необходимо обеспечить баланс между информационной безопасностью для передаваемых данных и возможностью обмена данной информацией между участниками цифровой экономики. В частности, необходимо установить различные уровни информационной безопасности для различных типов технологических данных, чтобы исключить блокирование развития сервисов IoT на основе некритически важной информации из-за чрезмерно завышенных требований по безопасности в целом.

С ростом числа подключенных устройств и использованием беспроводных технологий в сетях «Интернета вещей» растут риски информационной безопасности. Поэтому помимо регулирования обмена информацией на более высоких уровнях типовой архитектуры требуется

обеспечение информационной безопасности и на уровне сетей радиодоступа, а в наиболее критически важных применениях и на уровне самих оконечных устройств.

Защита рынка услуг «Интернета вещей»

С целью защиты рынка услуг «Интернета вещей» необходимо сформировать контролируемую с точки зрения управления и контроля сеть «Интернета вещей» на территории Российской Федерации через Реестр разрешенных на территории Российской Федерации идентификаторов устройств, точек доступа, узлов телематических служб, элементов сети передачи данных общего пользования, однозначно определяющих каждое отдельное устройство и его тип, и правила их разрешенного оборота, гарантирующих однозначную идентификацию устройств, процессов и их субъектов.

Реестр ID формируется на основе международных рекомендаций по установлению форматов идентификаторов с учетом особенностей рынка телекоммуникаций Российской Федерации. Применение устройств без использования разрешенных идентификаторов на территории Российской Федерации должен быть ограничен.

Узлы ТМС или СПД ОП, хранилища данных и прочие элементы, входящие в инфраструктуру интернета вещей, участвующие в предоставлении услуг абонентам на территории Российской Федерации, должны находиться на территории Российской Федерации.

Изготовители оборудования или операторы связи должны будут получить в уполномоченном органе требуемую емкость идентификаторов, входящих в Реестр, и установить идентификаторы в устройства и точки доступа, входящие в персональные сети абонентов, которые поступают в свободную продажу на рынок Российской Федерации.

Оператор услуг связи для предоставления услуг IoT на территории Российской Федерации должен получить в установленном порядке лицензию на предоставление услуг связи в СПД ОП или ТМС.

Абоненты (пользователи) получают идентификаторы у оператора при заключении договора на получение услуг.

Такой набор мер обеспечивает невозможность предоставления услуг по мониторингу и управлению персональными сетями IoT несанкционированными организациями.

Также целесообразным является разработка системы требований по криптографической защите радиоинтерфейсов узкополосных беспроводных сетей связи IoT, в которой была бы введена классификация применений, требующих использования тех или иных видов криптографии. Для критически важных применений должны быть установлены требования по использованию отечественных алгоритмов криптографии. Данное требование наиболее просто реализуется в узкополосных беспроводных сетях связи IoT в полосах радиочастот, используемых в общем порядке, для которых предусмотрена возможность замены алгоритмов шифрования без модификации сети радиодоступа за счет замены алгоритмов в SIM-картах и системах аутентификации. Так, для технологии NB-IoT, данные ключи заранее загружаются в UICC в защищенном режиме, а также специально хранятся в ядре сети для однозначной аутентификации абонента.

Для IoT разработан стандарт встраиваемой карты UICC, так называемый eUICC, который в отличие от отдельной SIM-карты выполняется в виде распаиваемой платы с пониженным энергопотреблением. Однако форм-фактор не главное отличие eUICC. В отличие от SIM карт, в которых запись профиля оператора осуществлялась на программаторе, в eUICC данные оператора и обновление постоянных ключей и алгоритмов шифрования возможно по радиоканалу. Для обеспечения безопасной загрузки профилей в eUICC в рамках GSMA была разработана соответствующая архитектура Embedded SIM Remote Provisioning

Architecture, специально ориентированная на управление устройствами IoT. Данный механизм в IoT является особенно востребованным, т.к. рекомендуется изменять ключи не реже одного раза в 5 лет, что для многих устройств IoT означает хотя бы одну смену ключей в процессе эксплуатации. Соответствующие механизмы смены ключей предусмотрены и на уровне ядра сети.

Более сложно ситуация обстоит с узкополосными беспроводными сетями связи IoT в полосах радиочастот, используемых в упрощенном порядке, где замена криптографических алгоритмов может быть сопряжена с более существенными доработками оборудования сети радиодоступа. При этом в узкополосных беспроводных сетях связи IoT в полосах радиочастот, используемых в упрощенном порядке, отсутствуют стандартизованные аналоги eUICC. Так, зачастую обмен ключами шифрования между радиомодулем и контроллером может быть перехвачен, что позволяет создавать дубликаты устройств. При этом отсутствуют проработанные системы перезарузки долгосрочных ключей или алгоритмов шифрования по радиоканалу в случае их компрометации, что усугубляется отсутствием механизма подтверждения приема информации для гарантирования полного приема информации практически во всех стандартах узкополосных сетей LPWAN в полосах радиочастот, используемых в упрощенном порядке.

Необходимо стремиться к приоритетному использованию отечественных криптографических алгоритмов и/или отечественной ЭКБ в устройствах IoT.

Обеспечение информационной безопасности в сетях «Интернета вещей» на основе использования российских технологий обеспечения целостности, конфиденциальности, аутентификации и доступности передаваемой информации и процессов ее обработки

Информационная безопасность сетей «Интернета вещей» это способность противостоять возможности реализации нарушителем угроз информационной безопасности.

Угрозами информационной безопасности сетей «Интернета вещей» являются нарушения конфиденциальности, целостности, достоверности и доступности информационных ресурсов, вследствие воздействия нарушителя на информационную сферу сети «Интернета вещей», включающую в себя:

- информационные ресурсы (передаваемая по сети информация пользователей, управляющая информация, базы данных и т.д.);

- информационную инфраструктуру (программное обеспечение, интерфейсы, протоколы управления);

- информационные технологии, технические средства и архитектуру построения, реализующие информационные процессы.

Угрозы информационной безопасности реализуются через возможные уязвимости информационной сферы сети, основными причинами появления которых являются:

- нарушение технологии процесса передачи информации пользователей;

- нарушение технологии системы управления сетью;

- использование в сети аппаратных компонентов или программного обеспечения, содержащих недекларированные возможности, нарушающие нормальное функционирование сети;

- использование в сети аппаратных компонентов или программного обеспечения, содержащих преднамеренно внесённые нарушителем скрытые изменения, приводящие к нарушению их функционирования.

Преднамеренные уязвимости могут быть внесены на этапах проектирования, разработки и изготовления оборудования сети в:

- алгоритмы, программы и средства, применяющиеся в сети;

- процедуры, протоколы и интерфейсы (связные и управления);

- проектные решения по созданию или модернизации системы обеспечения информационной безопасности сети.

Принципы обеспечения конфиденциальности, целостности, достоверности и доступности информационных ресурсов являются направлениями выполнения требований по обеспечению ИБ, которые делятся на два вида:

- функциональные требования;

- требования доверия к безопасности.

Функциональные требования определяют требования к функциям системы обеспечения ИБ и реализующим их средствам.

Требования доверия к безопасности определяют требования, выполнение которых даёт соответствующую степень уверенности в том, что при создании сетей «Интернета вещей» приняты меры, обеспечивающие достижение поставленных целей безопасности информации.

Функциональные требования фактически задают механизмы обеспечения ИБ (защиты от угроз), а требования доверия к безопасности определяют уровни доверия их реализации и направления достижения уровней.

Таким образом, принципы обеспечения ИБ характеризуются механизмами защиты от угроз и механизмами достижения уровней доверия реализации механизмов защиты (уровней ИБ).

Защита от угроз нарушения конфиденциальности, целостности, достоверности и доступности информационных ресурсов обеспечивается следующими механизмами.

Обеспечение конфиденциальности информационных ресурсов достигается путём применения средств защиты информации от

несанкционированного доступа, реализации правил разграничения доступа к информации, использования средств криптографической защиты информации при её передаче по каналам связи и хранении баз данных, обеспечения аутентификации абонентов на уровне абонентских терминалов, проведения специальных работ по предотвращению утечки конфиденциальной информации по техническим каналам, а также организационных мер по предотвращению разглашения конфиденциальной информации и неправомерных действий со стороны лиц, имеющих право доступа к конфиденциальной информации.

Обеспечение целостности информационных ресурсов достигается путём разработки и внедрения технологий резервирования и восстановления информационных ресурсов, применения средств защиты и выработки/проверки электронной цифровой подписи, физической охраной технических средств сетей «Интернета вещей» и носителей информации, другими организационными мерами.

Обеспечение достоверности информационных ресурсов достигается применением процедур подтверждения верности идентификационной информации объекта (физического лица, устройства, услуги, приложения) путём установления процедур идентификации и аутентификации.

Обеспечение подконтрольности информационных ресурсов достигается путём аудита и регистрации событий и действий, применения технологий электронной цифровой подписи, а также организационными мерами.

Обеспечение доступности информационных ресурсов достигается путём:

- применения средств защиты от несанкционированного доступа к информационным ресурсам (например, обеспечения аутентификации сетевым оборудованием абонентских терминалов и оконечных устройств), серверам и рабочим станциям, системам управления, активному сетевому, коммутационному и абонентскому оборудованию сетей «Интернета вещей»;

- применения средств криптографической защиты каналов управления оборудованием;

- применения средств защиты внутрисетевого трафика;

- применения средств сканирования сетевой инфраструктуры сети (систем мониторинга состояния оборудования) и средств обнаружения вторжений и атак на отдельные её компоненты и подсистемы;

- применения средств обеспечения регистрации и учёта действий операторов (эксплуатационного персонала), а также отдельных абонентов, которым разрешён доступ к определённым сервисам и услугам, использование которых может привести к нарушению информационной безопасности информационной инфраструктуры сети «Интернета вещей»;

- применения средств разграничения и управления доступом к защищаемым ресурсам сети «Интернета вещей»;

- применения специализированных средств фильтрации и блокировки сигналов управления при подключении внутренних информационных ресурсов к глобальным сетям информационного обмена;

- обеспечения замкнутости управления ресурсами сети связи на территории Российской Федерации;

- определения устойчивой архитектуры построения проектируемой сети включая номенклатуру необходимого телекоммуникационного оборудования и программно-аппаратного обеспечения платформы «Интернета вещей» (резервирования технических средств, дублирования каналов передачи данных в сети, разветвлённая топология);

- использования определённой конфигурации как абонентского, так и сетевого оборудования;

- обеспечения защиты от перегрузок;

- обеспечения приоритетности обслуживания привилегированных пользователей;

- проведения исследований оборудования сети и его программного обеспечения и определения необходимых специализированных настроек

абонентских интерфейсов, коммутационного оборудования и оборудования внутрисетевого информационного обмена;

- проведения проверок оборудования по поиску недекларированных аппаратных возможностей;

- проведения исследований программного обеспечения оборудования сети и анализа его аппаратной составляющей по поиску функциональных возможностей оборудования, реализация которых приводит к его некорректному функционированию или отказу;

- обеспечения организационных мер.

Принимая во внимание, что данный документ имеет направленность исключительно гражданского характера, вопросы применения в военно-технической сфере в Концепции не рассматриваются.

Таким образом, возможно определить следующие общие рекомендации по обеспечению информационной безопасности узкополосных беспроводных сетей «Интернета вещей», принимая во внимание, в том числе, использование имеющихся российских технологий обеспечения целостности, конфиденциальности, аутентификации и доступности информации и процессов её обработки.

В организационной части

1) Необходима разработка единой терминологии и классификации объектов, методов и средств, применяемых в сфере «Интернета вещей» на территории Российской Федерации. Отсутствие единой терминологии и классификации препятствует структурированной работе по созданию надлежащих средств обеспечения информационной безопасности, провоцирует ошибки в интерпретации.

2) Необходима разработка специфических требований по обеспечению информационной безопасности для отдельных сфер применения, дополняющих общие рекомендации. Общие рекомендации не способны учесть технологические особенности отдельных сфер применения и гарантировать применимость и достаточность таких рекомендаций. Должна

быть разработана модель угроз, на основании которой выбран класс криптографической защиты.

3) Необходимо обеспечить регулярную просветительскую работу среди операторов и пользователей сети «Интернета вещей» направленную на ответственное отношение и соблюдение норм информационной безопасности на всём периметре сети.

В части сети доступа

Следует отдать предпочтение открытым, хорошо задокументированным стандартам узкополосных беспроводных сетей «Интернета вещей», для которых устойчивость встроенных механизмов обеспечения информационной безопасности анализируется большим по величине сообществом исследователей и разработчиков, уменьшая таким образом риск наличия не выявленных уязвимостей.

В части платформы и приложений

1) Целесообразно рассмотреть возможность применения криптографической защиты и контроля целостности сообщений, передаваемых между абонентским устройством и платформой "Интернета вещей". Реализация криптографической защиты и контроля целостности должна обладать свойством оказывать минимально возможное влияние на энергопотребление абонентского устройства. При этом перед введением данного требования в качестве обязательного, целесообразно провести пилотный проект на отдельном регионе для отработки возможных рисков такой замены.

2) Следует стимулировать и поощрять регулярное проведение внутренних и внешних аудитов информационной безопасности.

Для узкополосных беспроводных сетей «Интернета вещей», применяемых в критически важных сегментах, дополнительно необходимо рассмотреть к применению следующие рекомендации.

В части абонентских устройств и встроенного в них ПО

1) Следует обеспечить доверенность аппаратного обеспечения оконечных устройств, путём локализации процессов его разработки и производства либо за счёт декларирования их соответствия установленным требованиям. Наибольшее внимание следует обратить на доверенность таких аппаратных компонент оконечных устройств как контроллер и приёмо-передающий модуль.

2) Следует обеспечить доверенность программного обеспечения оконечных устройств, путём локализации процессов его разработки.

3) Для обеспечения информационной безопасности в сетях, применяемых в критически важных сегментах, следует рассмотреть вопрос обеспечения использования абонентским устройством и платформой интернета вещей средств криптографической защиты информации, сертифицированных по классу не ниже КС3[1].

В части сети доступа следует обеспечить использование для аутентификации абонентов средств криптографической защиты информации, сертифицированных по соответствующему классу защиты с учетом подлежащих защите объектов и совокупности возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак на указанные объекты, с учетом применяемых информационных технологий, среды функционирования и аппаратных средств.

В части платформы и приложений следует исключить использование платформ «Интернета вещей» импортного производства и обеспечить доверенность платформ, разрабатываемых в Российской Федерации.

[1] Учитывая типовую модель нарушителя выбранную при формировании Концепции, рекомендуется использовать защиту устройств IoT не ниже класса КС3.

Организация и проведение оперативно-розыскных мероприятий в сетях «Интернета вещей»

Сети «Интернета вещей» присоединяемые к ССОП должны быть объектом системы СОРМ. Для этого необходимо внести правку в Закон «О связи», предусматривающую введение определения отдельного вида услуги связи, оказываемого в целях реализации межмашинного взаимодействия.

Существует ряд объективных причин, обуславливающих необходимость специфического подхода к построению технических средств содействия оперативно-розыскным мероприятиям в сетях связи «Интернета вещей», отличного от методов, используемых для сетей передачи данных. Такими причинами являются следующие:

1) Интерес для правоохранительных органов может представлять анализ не только информации по отдельным пользователям и их группам, но и комплексный анализ больших массивов данных для поиска различных корреляций в том числе с учётом данных, получаемых из других источников.

2) Индивидуальный формат структуры передаваемых данных может быть свойственен не только каждому отдельному сценарию применения, но и каждому конкретному виду устройств, модели, версии программного обеспечения, конкретному набору настроек и так далее. Создаваемая в таких условиях вариативность структуры данных, усложняет проведение комплексного анализа, даже с применением современных методик обработки «больших данных».

3) Криптографическая защищённость передаваемых данных (что должно являться нормой для сетей «Интернета вещей») осложняет легальный перехват на уровне транспортных каналов.

4) Применяемые в сетях «Интернета вещей» идентификаторы устройств и абонентов могут принципиально отличаться от используемых в традиционных решениях СОРМ, особенно на уровне транспортных каналов.

5) Отсутствие стандартизованных механизмов СОРМ для сетей «Интернета вещей» в полосах радиочастот, используемых в упрощенном порядке.

Принимая во внимание приведённые особенности сетей «Интернета вещей», встаёт задача по разработке соответствующих им принципов организации доступа технических средств СОРМ к переданной по сети «Интернета вещей» информации.

Исходя из предлагаемой типовой архитектуры узкополосных беспроводных сетей связи «Интернета вещей», показанной на рисунке 12 возможно рассмотреть в качестве кандидатов на взаимодействие с техническими средствами СОРМ такие наборы интерфейсов, как интерфейсы представления технологических данных для агрегации и предварительной обработки, интерфейсы разработчиков приложений IoT, интерфейсы для обмена технологическими данными с другими сервисными платформами.

Рисунок 12. Предлагаемая типовая архитектура узкополосных беспроводных сетей связи IoT

1) Интерфейсы представления технологических данных для агрегации и предварительной обработки.

В рассматриваемой концепции, на данном уровне архитектуры может применяться широкий спектр различных типов транспортных протоколов, идентификаторов абонентов, алгоритмов шифрования и структур данных. Вся представленная вариативность существенно затрудняет систематизацию и анализ данных, получаемых на этом уровне архитектуры. В то же время, попытки снизить вариативность применяемых на данном уровне методов может привести к неоправданному созданию барьеров в развитии услуг «Интернета вещей». Подключение технических средств ОРМ на данном уровне архитектуры «Интернета вещей» возможно рассматривать гипотетически возможным для организации пассивного съема данных.

2) Интерфейсы разработчиков приложений IoT.

В рассматриваемой концепции, на данном уровне архитектуры возможны сценарии, когда между сервисной платформой, услугами и приложениями IoT передаётся только сигнальная и управляющая информация, в то время как сам массив данных, получаемый с уровня оконечных устройств, остаётся на уровне сервисной платформы. Таким образом, подключение технических средств ОРМ на данном уровне архитектуры «Интернета вещей» не позволяет обеспечить полноту получаемых данных и не может быть рекомендовано.

3) Интерфейсы для обмена технологическими данными с другими сервисными платформами.

Данный уровень предполагает возможность получения наиболее полной и структурированной информации, накопленной на уровне сервисной платформы, включая данные и события от оконечных устройств, управляющие сигналы, данные и события с уровней потребителей услуг и приложений IoT. На данном уровне архитектуры существует техническая возможность определить и использовать единый формат идентификатора абонента / устройства вне зависимости от используемых на других уровнях

архитектуры протоколов и промежуточных идентификаторов. В этом случае, возможно реализовать как запрос данных по отдельным критериям, так и полное копирование базы данных для последующего анализа с использованием технических средств ОРМ. Интерфейсы данного уровня архитектуры следует рассматривать как приоритетные при подключении технических средств ОРМ к сетям «Интернета вещей».

Таким образом, возможно, сформулировать следующие общие предложения по организации и проведению оперативно-розыскных мероприятий в узкополосных беспроводных сетях «Интернета вещей».

1) При разработке методов взаимодействия платформы «Интернета вещей» и технических средств ОРМ необходимо учитывать разработанные в данной области нормативные правовые акты, а также набор спецификаций, разрабатываемый стандартизующей организацией OneM2M.

2) При выборе уникальных идентификаторов устройств «Интернета вещей» использовать рекомендации МСЭ и других международных организаций.

3) Ограничить информационный обмен устройств «Интернета вещей» таким образом, чтобы все передаваемые данные и факты о событиях могли быть структурированы и сохранены сервисной платформой «Интернета вещей».

4) Предусмотреть возможность организации пассивного съема информации, передаваемой по каналам связи между оконечными устройствами и сервисной платформой «Интернета вещей», и ее передачи на технические средства ОРМ.

5) Должен быть предусмотрен ограниченный перечень сценариев (и соответствующих ему устройств и приложений) для которых, в качестве исключения, допускается информационный обмен устройств «Интернета вещей» без использования сервисной платформы «Интернета вещей». Для каждого из таких сценариев, должен быть определён и согласован альтернативный способ сбора и хранения информации, необходимой для

проведения ОРМ. Примером такого сценария, может быть информационный обмен между автотранспортными средствами с целью предупреждения аварийной ситуации.

6) Для всех основных сфер применения «Интернета вещей», для обработки и хранения данных на уровне сервисной платформы, следует разработать шаблоны данных, где основные поля имели бы регламентируемый формат, для целей облегчения последующего анализа данных.

Предпосылки к развитию на территории Российской Федерации сетей «Интернета вещей» технологии NB-IoT

Технология NB-IoT является в большей степени эволюционной разработкой, нежели простой адаптацией стандарта LTE к требованиям IoT. NB-IoT предполагает интеграцию с LTE, однако при его внедрении изменяется не только программное, но и аппаратное обеспечение (в случае отсутствия поддержки необходимого функционала SDR на БС). Несмотря на это, радиоинтерфейс NB-IoT не является отдельным стандартом, а описывается как специальный режим стандарта LTE, что связано с целесообразностью унификации инфраструктуры сетей радиодоступа LTE для предоставления всего спектра услуг IoT.

Использование полос радиочастот для технологии NB-IoT (рисунок 13) предусматривается в трех возможных вариантах: в качестве отдельного радиочастотного канала вне канала LTE, в защитной полосе радиочастот, обязательной для обеспечения совместимости сетей LTE различных операторов, а также непосредственно за счет выделения полосы радиочастот в канале сети LTE. Для простоты данные режимы именуются: обособленный (stand alone), внутриканальный (guard-band) и внутрисигнальный (inband) соответственно.

Такая вариативность обусловлена тем, что радиоинтерфейс NB-IoT разрабатывался с учетом выполнения требования полной совместимости с действующими радиоинтерфейсами GSM и LTE.

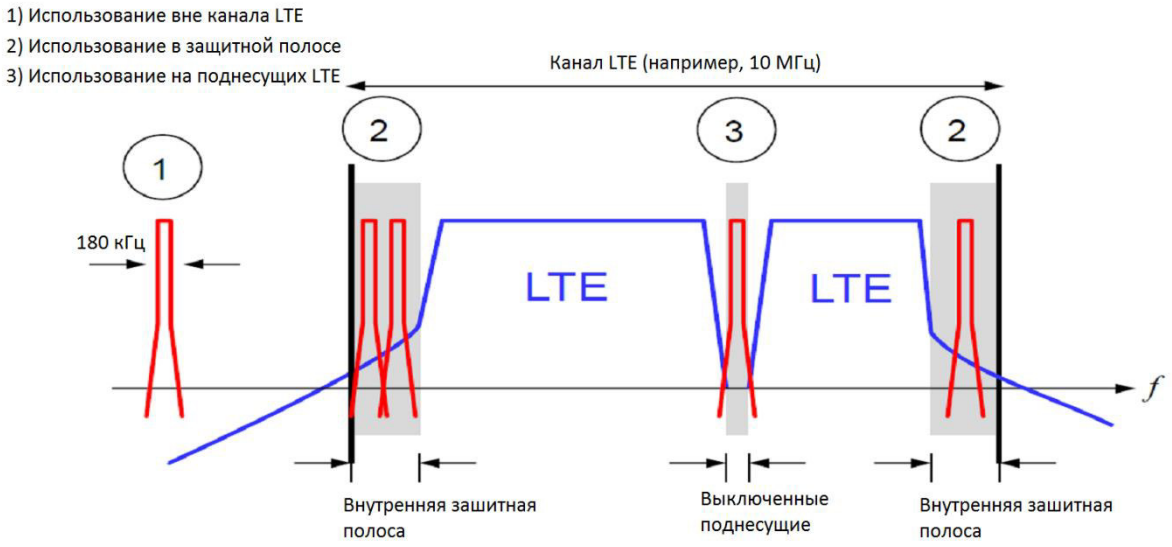

Рисунок 13. Варианты использования радиочастот для технологии NB-IoT

Фактически, установление защищенного соединения между устройством NB-IoT и ядром сети полностью повторяет аналогичную процедуру для стандарта LTE. В частности, переиспользуются алгоритмы аутентификации, шифрования и контроля целостности передаваемой пользовательской и контрольной информации. При этом в NB-IoT разделяют механизмы обеспечения шифрования и проверки целостности на механизмы, устанавливаемые в протоколах между АС и БС - Access Stratum (AS), и механизмы, устанавливаемые в протоколах между АС и MME - Non-Access Stratum (NAS). К механизмам AS относятся алгоритмы, которые устанавливают безопасность на уровне сети радиодоступа, включая пользовательские данные и данные управления. К механизмам NAS относятся алгоритмы, которые устанавливают безопасность на уровне опорной сети, включая данные управления и пользовательские данные, если они в небольшом объеме инкапсулированы в структуру данных управления NAS (используется в NB-IoT для исключения необходимости установления радиосоединения для пользовательских данных).

Отдельно следует отметить центр авторизации опорной сети, в котором участвует сервер домашних абонентов (HSS). При этом процедура установления защищенного соединения между устройством NB-IoT и сетью радиодоступа/опорной сетью подразумевает использование широкого набора ключей шифрования.

Для обеспечения безопасной загрузки профилей SIM карт в eUICC в рамках GSMA была разработана соответствующая архитектура Embedded SIM Remote Provisioning Architecture, специально ориентированная на управление устройствами IoT. Данный механизм в IoT является особенно востребованным, т.к. рекомендуется изменять ключи не реже одного раза в 5 лет, что для многих устройств IoT означает хотя бы одну смену ключей в процессе эксплуатации. Соответствующие механизмы смены ключей предусмотрены и на уровне HSS.

Помимо перезагрузки ключей, сеть NB-IoT поддерживает возможность перезагрузки алгоритмов шифрования или алгоритмов проверки целостности на уровне сети и на уровне SIM-карт, что обеспечивает возможность замены алгоритмов в случае выявления уязвимостей в них. Для установки алгоритмов шифрования используются специальные сообщения и процедуры, прописанные в стандартах на опорную сеть и на SIM-карты.

Если говорить об опорной сети в целом, то начиная с узла MME для данных, передаваемых NAS, и для шифрованных пользовательских данных начиная с узла БС, используется протокол IP. Для защиты опорной сети при этом используются ставшие традиционные механизмы, такие как организация VPN-тоннелей и другие стандартные методы защиты IT-инфраструктуры.

Помимо исключительно криптографических алгоритмов защиты информации в сетях NB-IoT есть и другие механизмы, косвенно обеспечивающие более высокий уровень безопасности передаваемой информации. Например, сертификация устройств на соответствие стандартам обеспечивает сложность создания нестандартных устройств. Передача

уникального идентификатора IMSI осуществляется только при первом подключении к сети после включения аппарата, а в другие моменты используется его временный аналог TMSI. Режим передачи данных с подтверждением, доступный в NB-IoT, обеспечивает возможность гарантированных обновлений важной информации без риска умышленного подавления такой информации в радиоканале или ее случайной потери из-за флуктуаций сигнала. Последнее, в частности, позволяет проводить обновление критических установок устройства по радиоканалу. Наконец, в NB-IoT существуют классы приоритезации трафика для критически важной информации, что позволяет избежать потери критической информации при появлении перегрузок в сети.

Кроме того, радиоинтерфейс NB-IoT в совокупности с функционалом ядра 3GPP позволяет реализовать полную управляемость услугами и устройствами IoT не только в рамках собственной сети, но и обеспечить доступ к данному функционалу для сторонних компаний-партнеров, которые могут реализовывать сложные услуги IoT, специфические для конкретной отрасли или применения.

Все вышеперечисленное в совокупности с возможностью использования полос радиочастот, ранее выделенных для применения РЭС стандарта LTE и последующих его модификаций в режиме NB-IoT позволяет рассматривать данную технологию, как одну из наиболее востребованных, при реализации различных проектов «Интернета вещей» с использованием узкополосных беспроводных сетей связи IoT на территории Российской Федерации.

Применение концепции «импортозамещения» в критически важных сегментах экономики

Использование отечественного программного обеспечения и оборудования при внедрении узкополосных беспроводных сетей «Интернета вещей» на территории Российской Федерации является важной задачей для

обеспечения информационной безопасности и защиты информации особенно для критически важных сегментов экономики Российской Федерации.

Это требование актуально как для сетей, подключаемых к СОП, так и для технологических сетей, не имеющих выхода в сеть ОП. Например, построение федеральной сети LPWAN на транспорте для ЕИТС подразумевает расширение рынка оконечных устройств. В этой связи требуется принять меры по поддержке отечественного производителя технических средств и разработчиков программного обеспечения.

К таким мерам относятся:

- предоставление преимуществ отечественным производителям при проведении закупочных процедур;

- разработка целевых программ, направленных на разработку нового оборудования;

- разработка национальных стандартов технологий, оборудования и процессов;

- ограничение ввоза иностранного оборудования в полосах радиочастот, разрешенных для создания ФСТТ;

- ограничения использования телекоммуникационного оборудования иностранного происхождения.

При разработке отечественного программного обеспечения для сервисных платформ, которое планируется использовать для внедрения узкополосных беспроводных сетей «Интернета вещей», необходимо руководствоваться требованиями пункта 5 раздела II «Порядка формирования и ведения реестра российского программного обеспечения», Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов евразийского экономического союза, за исключением Российской Федерации, утверждённых постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении

запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (вместе с «Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации», «Порядком подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств (за исключением программного обеспечения, включённого в единый реестр программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации), в целях осуществления закупок для обеспечения государственных и муниципальных нужд»), а также включения в реестр российского программного обеспечения.

Это обусловлено тем, что на уровне сервисной платформы будут решаться наиболее критичные задачи, связанные с работой и применением узкополосных беспроводных сетей «Интернета вещей» с учётом обеспечения информационной безопасности, а именно:

- агрегация данных и их обработка;

- обеспечение информационной безопасности в части собираемых технологических данных;

- управление глобальными идентификаторами устройств;

- формирование IoT услуг;

- организация круглосуточного удалённого доступа к информационной системе, эксплуатируемой оператором узкополосной беспроводной сети «Интернета вещей», с целью предоставления данных уполномоченному государственному органу для проведения ОРМ.

Кроме того, при построении узкополосных беспроводных сетей «Интернета вещей» на территории Российской Федерации, в особенности для

критически важных отраслей экономики Российской Федерации, необходимо предусмотреть поэтапный переход на отечественную электронно-компонентную базу для оконечных устройств IoT. Для таких оконечных устройств должны учитываться следующие требования к промышленной продукции, предъявляемые в целях её отнесения к продукции, произведённой на территории Российской Федерации:

- наличие у юридического лица - налогового резидента стран - членов Евразийского экономического союза:

- прав собственности либо иных законных оснований на конструкторскую, технологическую документацию в объёме, подтверждающем возможность производства, модернизации и развития соответствующей продукции, на срок не менее 5 лет в соответствии со спецификацией на готовое изделие, содержащей: технические условия; спецификацию на готовое изделие с указанием сборочных единиц и деталей; руководство (инструкция) по эксплуатации; схему деления изделия; схему электрическую функциональную; технологическую инструкцию; Gerber-файлы (трассировка печатной платы и схема расположения элементов), перечень комплектующих;

- прав собственности либо иных законных оснований на использование, модификацию, модернизацию, изменение встроенного микропрограммного обеспечения для схемотехнического решения на срок не менее 5 лет, в том числе комплект программной документации, включающий: комплект текстов программ (исходных кодов) и двоичных файлов-микрокодов; руководство по компиляции и сборке встроенного микропрограммного обеспечения и инсталляции его двоичного образа в составе продукции;

- документы, подтверждающие проведение на территории Российской Федерации следующих технологических операций: сборка и монтаж всех элементов электронной компонентной базы на печатную плату (для печатных плат, содержащих в своём составе центральные процессоры); запись в

энергонезависимую память микропрограммного обеспечения для схемотехнического решения; сборка и монтаж готовой продукции; проведение технического контроля соответствия требованиям технических условий готового изделия;

- проведение контроля количественных и качественных характеристик свойств готового изделия;

- наличие на территории одной из стран - членов Евразийского экономического союза, сервисного центра, уполномоченного осуществлять ремонт, послепродажное, гарантийное и постгарантийное обслуживание продукции.

Кроме того, требуется планомерное снижение процентной доли стоимости, использованных при производстве иностранных комплектующих изделий. При определении процентной доли стоимости использованных при производстве иностранных комплектующих изделий учитываются только следующие комплектующие изделия (при наличии):

- радиомодем;
- контроллер;
- дискретные RLC компоненты;
- источник питания;
- соединители;
- печатная плата;
- антенны.

В настоящее время на сетях связи используются зарубежные алгоритмы аутентификации и установления ключей парной связи.

В целях повышения защищённости от несанкционированного доступа к информации, передаваемой посредством сетей подвижной радиотелефонной связи, приказами Минкомсвязи России от 13.06.2018 г. № 275 «О внесении изменений в Правила применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VI. Правила применения узлов связи с территориально распределённой архитектурой стандартов UMTS

и/или GSM 900/1800, утверждённые приказом Министерства связи и массовых коммуникаций Российской Федерации от 27.06.2011 №160» и от 25.06.2018 г. № 319 «Об утверждении Правил применения оборудования коммутации сетей подвижной радиотелефонной связи. Часть VII. Правила применения оборудования коммутации стандарта LTE» с 1 декабря 2019 г. устанавливаются требования к реализации процедур аутентификации и идентификации абонентов с использованием средств криптографической защиты информации, имеющих подтверждение соответствия требованиям по безопасности информации класса КА для оборудования коммутации узлов связи, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

Кроме того, осуществляется работа по актуализации Требований по защите сетей связи от несанкционированного доступа к ним и передаваемой по ним информации, утверждённых приказом Министерства информационных технологий и связи Российской Федерации от 09.01.2008 г. № 1, в том числе для повышения защищённости от несанкционированного доступа к информации, передаваемой посредством сетей подвижной радиосвязи, сетей подвижной радиотелефонной связи, сетей подвижной спутниковой радиосвязи, и предусматривается, что операторы связи должны обеспечивать реализацию процедур аутентификации и идентификации абонентов с использованием средств криптографической защиты информации, имеющих подтверждение соответствия требованиям по безопасности информации, установленным федеральным органом исполнительной власти в области обеспечения безопасности, класса КА для оборудования коммутации узлов связи и класса не ниже КС3 для модуля идентификации абонентов USIM (R-UIM) в составе абонентского оборудования.

Модуль идентификации абонентов USIM (R-UIM) представляет собой сменную идентификационную карточку пользователя, которая может выполнять множество различных функций, является хранилищем ключевой

информации и совместно с центром аутентификации оператора, проводит процедуры аутентификации абонентского устройства при регистрации в сети путём проведения определённого стандартом 3GPP криптографического протокола, в результате которого удостоверяется равенство ключей, а также вырабатывается сессионный ключ, который в дальнейшем используется для симметричного шифрования в радиоканале.

Таким образом, путём использования в криптографическом протоколе отечественных алгоритмов и соответствующей сертификации их реализации обеспечивается доверенность криптографического протокола.

Кроме того, обеспечивается доверенность процедуры выработки и загрузки ключевой информации за счёт использования по соответствующему классу отдельного аппаратного модуля безопасности на стороне оператора связи, выполняющего криптографические функции аутентификации абонентских устройств.

Описанное выше, в первую очередь, будет использоваться при аутентификации оконечных устройств IoT для узкополосных беспроводных сетей «Интернета вещей», использующих инфраструктуру операторов связи.

Для технологий, которые будут использоваться для развёртывания узкополосных беспроводных сетей «Интернета вещей», не предусматривающих использование инфраструктуры операторов связи, также должна учитываться необходимость реализации отечественных криптографических алгоритмов.

Для оборудования и инфраструктуры, используемой для обеспечения государственных и муниципальных нужд, а также компаниями с государственным участием, особенно важное значение имеют отсутствие незадекларированных возможностей в применяемом оборудовании и инфраструктуре, а также снятие рисков невозможности обновления и модернизации оборудования, инфраструктуры и программного обеспечения в случае введения односторонних запретов (санкций) со стороны иностранных государств.

В связи с чем, представляется целесообразным предусмотреть дополнительные меры по защите государственных инвестиций от указанных рисков путем внесения соответствующих положений в законодательство о закупочной деятельности в государственном сегменте, а также принятие мер по поддержке отечественного производства технических средств и разработчиков программного обеспечения при внедрении узкополосных беспроводных сетей «Интернета вещей» на территории Российской Федерации в государственном сегменте. При этом важным является закрепление положений об обязательном использовании интегральных схем 1 и 2 уровней в соответствующей критически значимой инфраструктуре в целях повышения уровня безопасности и независимости создаваемых систем.

В рамках развития законодательства представляется целесообразным разработка и принятие проекта постановления Правительства Российской Федерации «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, а также закупок отдельными видами юридических лиц» и внесение изменений в постановление Правительства Российской Федерации от 17.07.2015 № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации», постановление Правительства Российской Федерации от 26.09.2016 № 968 «Об ограничениях и условиях допуска отдельных видов радиоэлектронной продукции, происходящих из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд», постановление Правительства Российской Федерации от 16.09.2016 № 925 «О приоритете товаров российского происхождения, работ, услуг, выполняемых, оказываемых, российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым, иностранными лицами» в части приоритетного использования отечественного оборудования и программного обеспечения.

Кроме того, при построении узкополосных беспроводных сетей «Интернета вещей» на территории Российской Федерации, применяемых для обеспечения государственных и муниципальных нужд, а также отдельными видами юридических лиц, компаниями с государственным участием, необходимо предусмотреть поэтапный переход на отечественную электронно-компонентную базу для оконечных устройств IoT и для сервисных платформ при условии их конкурентоспособности.

Предложенные меры создадут дополнительные условия для долгосрочного развития и формирования конкурентных преимуществ производителей российской продукции для узкополосных беспроводных сетей «Интернета вещей» на территории Российской Федерации и повысят безопасность и независимость создаваемых систем для государственных и муниципальных нужд, а также отдельных видов юридических лиц, компаний с государственным участием.

Лицензирование деятельности операторов сетей «Интернета вещей»

В настоящее время в Российской Федерации действуют Постановление Правительства Российской Федерации от 18 февраля 2005 года №87 «Об утверждении перечня наименования услуг связи, вносимых в лицензии, и перечней лицензионных условий» и Правила оказания телематических услуг связи, утвержденные Постановлением Правительства Российской Федерации от 10 сентября 2007 года №575, конечным потребителем телематических услуг связи всегда является абонент и (или) пользователь, т.е. человек, который с помощью программного обеспечения (интернет-браузер и почтовый клиент), установленного на пользовательском оборудовании, получает возможность доступа к информации, размещенной в сети интернет.

Стратегией развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 года №203, «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 (межмашинное взаимодействие).

Таким образом, появляется необходимость уточнения определения телематических услуг связи путем допущения возможности отсутствия участия человека на всех этапах осуществления связи между вещами (физическими предметами).

Принимая во внимание данное уточнение, услуги, связанные с Интернетом вещей, подлежат обязательному лицензированию в соответствии с законодательством Российской Федерации.

Подходы к взаимоувязанному развитию сетей «Интернета вещей»

Для реализации взаимоувязанного развития различных узкополосных беспроводных сетей связи IoT, а в значительной степени и развития всей экосистемы IoT в Российской Федерации необходимо реализовать:

1) Создание и развитие системы управления идентификацией устройств IoT на верхних уровнях типовой архитектуры узкополосных беспроводных сетей связи IoT.

2) Формирование требований к открытым стандартам на интерфейсах между сервисными платформами IoT, между сервисными платформами IoT и сторонними разработчиками приложений IoT, между сервисными платформами IoT и различными узкополосными беспроводными сетями связи IoT. При этом целесообразно сформировать перечень рекомендованных открытых международных стандартов, удовлетворяющих данным требованиям, для внедрения в Российской Федерации.

3) Классификацию критически важных сегментов экономики и применений узкополосных беспроводных сетей связи IoT в данных сегментах с точки зрения установления соответствующих требований по использованию стандарта NB-IoT для таких применений в совокупности с

требованиями по методам защиты и информационной безопасности, в части использования отечественных криптографических алгоритмов и/или отечественной ЭКБ в оконечных устройствах. При этом также требуется определить какие отечественные криптографические алгоритмы должны использоваться и порядок их использования.

4) Стимулирование развития отечественной ЭКБ, удовлетворяющей требованиям узкополосных беспроводных сетей связи IoT с целью её использования для наиболее критически важных применений IoT, а также для реализации импортозамещения в сфере IoT.

5) Стимулирование развития отечественных сервисных платформ для предоставления услуг IoT и управления оконечными устройствами IoT, а также создания открытого и независящего от иностранных разработчиков программного обеспечения рынка услуг IoT.

6) Необходимо стремиться к приоритетному использованию отечественных криптографических алгоритмов и/или отечественной ЭКБ в устройствах IoT.

Вышеописанные мероприятия по взаимоувязанному развитию узкополосных беспроводных сетей предполагается проводить путем внедрения новой лицензии для услуг IoT в рамках действующей нормативно-правовой базы с целью реализации регулирования операторов сервисных платформ «Интернета вещей», данные в которые будут поступать, в том числе, из узкополосных беспроводных сетей связи IoT.

Таким образом, для регулирования передачи и обработки огромных массивов данных, собираемых от множества датчиков и сенсоров и передаваемых по узкополосным беспроводным сетям связи «Интернета вещей» необходимы подходы к сбалансированному законодательству, стимулирующему переход к цифровой экономике и одновременно способному предотвращать негативные последствия от непрофессиональной или незаконной обработки информации.

Нормативно-правовое обеспечение построения и развития сетей «Интернета вещей» на территории Российской Федерации

В целях упрощения построения и развития сетей «Интернета вещей» на территории Российской Федерации требуется разработать и внести изменения в части регулирования узкополосных беспроводных сетей связи IoT в следующие нормативно-правовые акты:

1) Постановление Правительства Российской Федерации от 18 февраля 2005 года №87 «Об утверждении перечня наименования услуг связи, вносимых в лицензии, и перечней лицензионных условий»

2) Правила оказания телематических услуг связи, утвержденные Постановлением Правительства Российской Федерации от 10 сентября 2007 года №575.

3) постановление Правительства Российской Федерации об исчерпывающих перечнях процедур в сфере строительства объектов сетей связи и правилах ведения реестров описаний процедур по аналогии с другими инфраструктурными отраслями, где действуют подобные Постановления Правительства Российской Федерации для упрощения и унификации процедур;

4) изменения нормативно-правовой базы Роспотребнадзора о порядке проведения санитарно-эпидемиологической экспертизы по форме Р1 (экспертиза проектируемых решений) и Р2 (экспертиза построенного объекта). В частности, требуется исключение избыточного административного барьера в виде существующей на сегодня двухзвенной (Р1 – Р2) разрешительной процедуры и её замены на уведомительную процедуру с использованием электронного документооборота между территориальным органом Роспотребнадзора и оператором связи;

5) новые правила применения оборудования узкополосных беспроводных сетей связи IoT для установления требований к средствам связи, устанавливаемым в сети связи общего пользования, или в технологических сетях связи и сетях связи специального назначения в случае

их присоединения к сети связи общего пользования (в настоящее время, такие правила применения разработаны только для узкополосных беспроводных сетей связи IoT в полосах радиочастот, используемых в общем порядке);

6) постановление Правительства Российской Федерации от 12 октября 2004 г. №539 «О порядке регистрации радиоэлектронных средств и высокочастотных устройств» с целью исключения необходимости регистрации оконечных устройств узкополосных беспроводных сетей связи IoT. В настоящее время такое исключение действует только на узкополосные беспроводные сети связи IoT в полосах радиочастот, используемых в общем порядке, для которых оконечные устройства приравниваются к абонентским терминалам сетей сотовой подвижной связи;

7) постановление Правительства Российской Федерации «Об утверждении Порядка идентификации оконечного оборудования узкополосных беспроводных сетей «Интернета вещей» (единая система идентификации оконечного оборудования узкополосных беспроводных сетей «Интернета вещей») для утверждения единого Порядка идентификации оконечных устройств оконечного оборудования узкополосных беспроводных сетей «Интернета вещей», позволяющего упростить сбор и анализ большого массива данных;

8) в некоторые акты Правительства Российской Федерации в части создания правовых основ для легализации узкополосных беспроводных сетей «Интернета вещей» (постановление Правительства Российской Федерации от 25 июня 2009 г. № 532 «Об утверждении перечня средств связи, подлежащих обязательной сертификации», от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи», от 18 февраля 2005 г. № 87 «Об утверждении перечня наименований услуг связи, вносимых в лицензии, и перечней лицензионных условий») для уточнения перечня наименований услуг связи, вносимых лицензии, на осуществление деятельности в области оказания услуг связи, содержащего дополнительную лицензию на оказание

телематических услуг связи в выделенной сети для создания правовых основ для легализации узкополосных беспроводных сетей «Интернета вещей» и расширения существующего перечня лицензионных условий на осуществление деятельности в области оказания телематических услуг связи с созданием правовых основ для легализации узкополосных беспроводных сетей «Интернета вещей». При этом сертификация (декларирование) средств связи узкополосных беспроводных сетей «Интернета вещей» будет являться, в том числе, формой раскрытия данных об используемом оборудовании;

9) постановление Правительства Российской Федерации о внесении изменений в Требования к промышленной продукции, предъявляемые в целях ее отнесения к продукции, произведенной на территории Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 17 июля 2015 г. № 719 «О подтверждении производства промышленной продукции на территории Российской Федерации» для утверждения критериев отнесения оконечного оборудования, технических и программных средств информационных систем сервисных платформ узкополосных беспроводных сетей «Интернета вещей» к промышленной продукции, произведенной на территории Российской Федерации;

10) требования к оконечному оборудованию узкополосных беспроводных сетей «Интернета вещей» (для различных отраслей экономики Российской Федерации с учетом специфики), в том числе в части информационной безопасности и криптографической защиты информации с использованием криптографических алгоритмов и аппаратных средств;

11) требования к техническим и программным средствам информационных систем сервисных платформ узкополосных беспроводных сетей «Интернета вещей», в том числе в части информационной безопасности и криптографической защиты информации с использованием криптографических алгоритмов и аппаратных средств;

12) требования к техническим и программным средствам информационных систем сервисных платформ узкополосных беспроводных

сетей «Интернета вещей», обеспечивающим выполнение установленных действий при проведении оперативно-розыскных мероприятий;

13) национальный стандарт «Информационные технологии. Интернет вещей. Термины и определения»;

14) национальный стандарт «Информационные технологии. Интернет вещей. Эталонная архитектура Интернета вещей и индустриального Интернета вещей»;

15) отечественный стандарт на формат и структуру хранимых сервисной платформой узкополосных беспроводных сетей «Интернета вещей» данных, получаемых от оконечного оборудования (единый стандарт для различных отраслей экономики Российской Федерации);

16) отечественный стандарт на криптографический протокол, используемый на уровне доступа оконечного оборудования к узкополосной беспроводной сети «Интернета вещей» (между оконечным оборудованием и базовой станцией/точкой доступа);

17) отечественный стандарт на шифрование между оконечным оборудованием и техническими и программными средствами информационных систем сервисных платформ узкополосной беспроводной сети «Интернета вещей»;

18) рассмотреть необходимость внесения изменений в существующие Технические регламенты Таможенного союза в части установления требований к оконечному оборудования узкополосных беспроводных сетей «Интернета вещей» (для различных отрасли экономики Российской Федерации с учетом специфики).

Кроме того, целесообразно рассмотреть возможность разработки национальных стандартов интернета вещей, в том числе в области криптографической защиты информации. Разработка устройств IoT, планируемых к использованию в РФ, должна проводиться с приоритетностью использования национальных стандартов РФ.

Целесообразно принять соответствующие меры для отражения основных положений разработанных национальных стандартов в соответствующих международных организациях.

Данный перечень НПА не является исчерпывающим и может корректироваться с учетом результатов реализации мероприятий федеральных проектов Национальной программы «Цифровая экономика Российской Федерации».