



Использование узкополосных беспроводных сетей связи "Интернета вещей" в информационной инфраструктуре цифровой экономики

Лашкевич Андрей Владимирович –
заместитель начальника отдела
НТЦ анализа ЭМС ФГУП «НИИ Радио»

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ РАДИО

Нормативно-техническое обеспечение развития ИВ (IoT)

Развитие узкополосных беспроводных сетей связи «Интернета вещей» как составной части «Интернета вещей» предусмотрено программой «Цифровая экономика Российской Федерации» (раздел «Построение узкополосных беспроводных сетей Интернета вещей на территории Российской Федерации») по направлению «Информационная инфраструктура».

Internet of Things (IoT)



Основная цель: узкополосные беспроводные сети связи Интернета вещей должны быть последовательно и повсеместно внедрены во всех отраслях экономики с территориальным покрытием всех малых городов и поселков городского типа, в том числе с использованием отечественного оборудования.

Структура рынка устройств ИВ (IoT) с использованием беспроводных технологий



	Технологии	Доля рынка
1.	Персональные локальные сети, малый радиус действия	Около 80%
2.	Узкополосные сети IoT, средний радиус действия	Около 20%
3.	Спутниковые и другие сети	Менее 1%



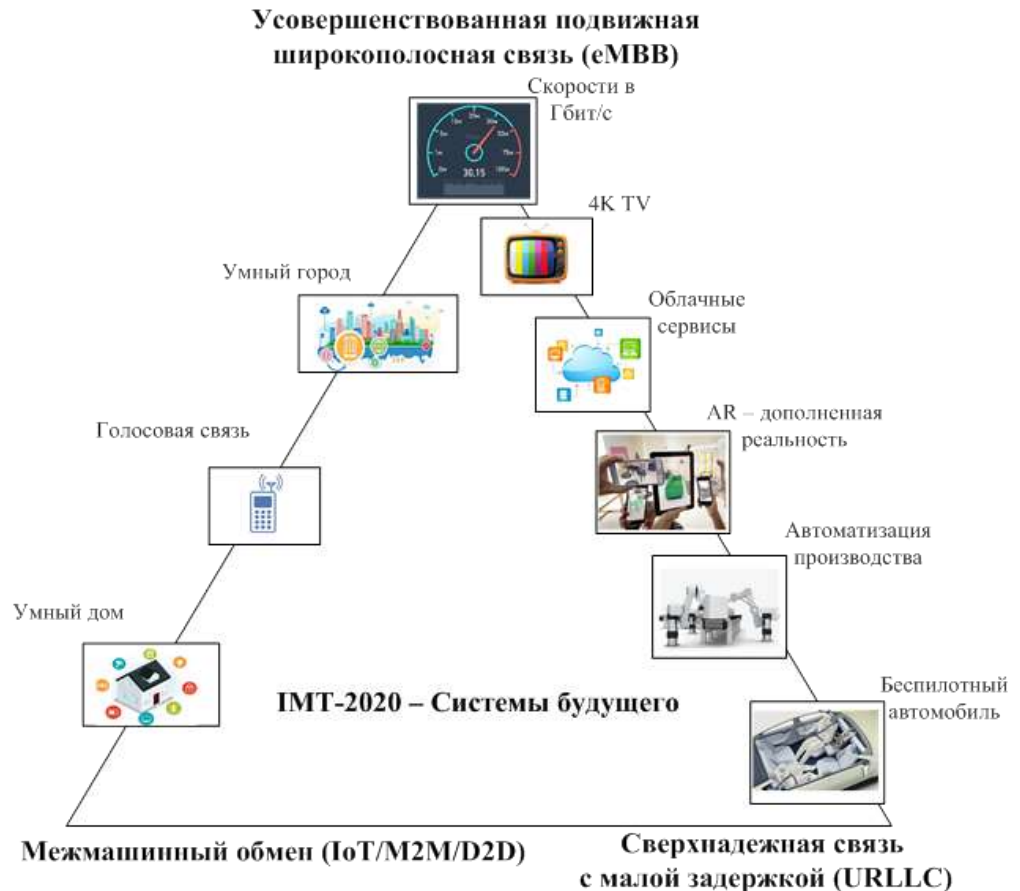
Технологии интернета вещей способны внести большой вклад в повышение технико-экономических показателей работы отраслей реальной экономики, снижение затрат, повышение эффективности и производительности труда.

Ожидается, что лидерами по объему инвестиций в Интернет вещей в России будут производственный сектор, сектор услуг ЖКХ, транспортные компании, энергетика, потребительский сегмент и госсектор.

Роль узкополосных сетей ИВ (IoT) в составе цифровой экономики



Базовым уровнем развития Интернета вещей (включая автоматизацию на производстве) обычно считается использование подключенных устройств для сбора информации, мониторинга и автоматизации производственных процессов.



Наибольший экономический эффект от внедрения технологий Интернета вещей может быть получен при условии применения **совместно** с такими технологиями как аналитика больших данных, мобильные и облачные вычисления.

Выбор стандартов и полос частот для сетей ИВ (IoT)



По условиям использования полосы частот ИВ (IoT) подразделяются на:

- лицензируемые (для сетей операторов связи)
- нелицензируемые (для устройств малого радиуса действия)



- Преимуществом сетей ИВ/IoT в лицензируемых полосах радиочастот является предсказуемая электромагнитная обстановка и контроля уровня помех на соответствующих частотах.
- Преимуществом сетей ИВ/IoT в нелицензируемых полосах радиочастот является возможность работы без получения разрешения на использование радиочастот, что снижает стоимость владения и упрощает развертывание.

Узкополосные сети ИВ/IoT в лицензируемых полосах частот

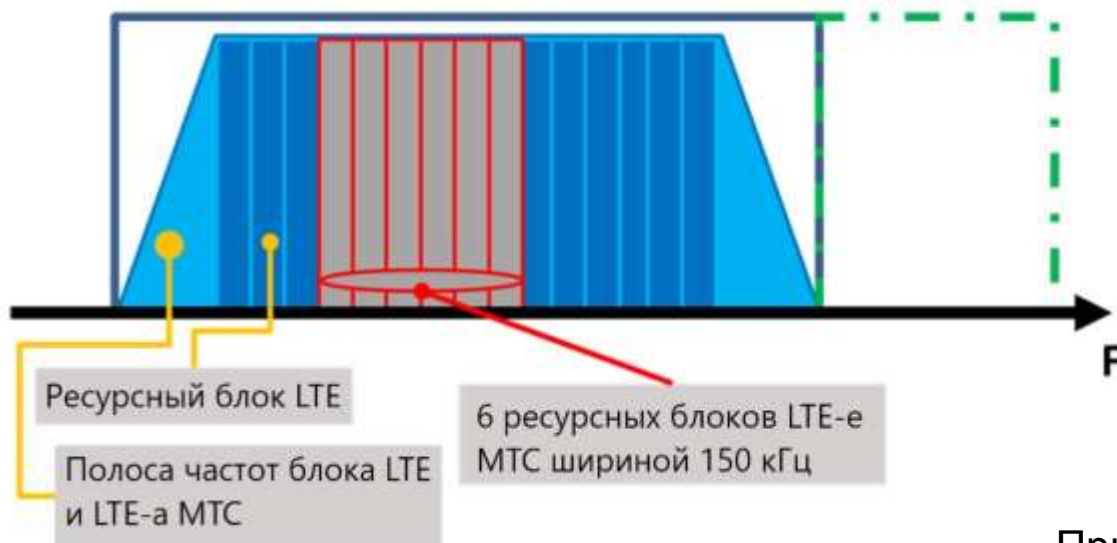


Технология	EC-GSM	LTE-eMTC	NB-IoT
Диапазон радиочастот, МГц	900, 1800	Частоты LTE	Частоты LTE
Ширина частотного канала	200 кГц	6x180 кГц (1,08 МГц)	180 кГц
Максимальное число устройств IoT на сектор БС на один канал	50000	50000	50000
Скорость передачи данных	70 или 240 кбит/с	1 Мбит/с	127 кбит/с на линии вниз 158 кбит/с или 15.6 кбит/с на линии вверх
Мобильность	Полная	Полная	Ограниченная

Узкополосные сети ИВ/IoT в лицензируемых полосах частот



Пример использования LTE-e MTC

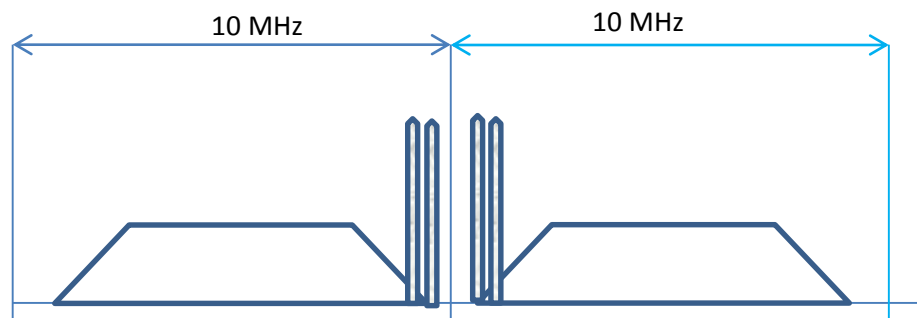


Режимы использования NB-IoT:

- внутрисигнальный
- внутриканальный
- обособленный

Решение ГКРЧ № 17-44-06 от 28 декабря 2017 г. упростило внедрение сетей NB-IoT поверх существующих сетей GSM и LTE без необходимости повторного получения разрешений на использование радиочастот

Пример использования внутриканального режима NB-IoT



- **Традиционные сотовые сети** – широко распространенные модули сотовой связи на основе GSM/EDGE и других стандартов сотовой связи поколения 2G, на основе обычных модемов UMTS и LTE без каких-либо специальных доработок для ИВ/IoT;
- **LPWA (Low Power Wide Area Networks)** – устройства мобильного широкополосного доступа и новые специализированные интерфейсы для сетей M2M широкого охвата. Помимо специализированных интерфейсов сетей сотовой подвижной связи в данную категорию также входят применения, реализуемые в нелицензируемых полосах частот, т.е. относящиеся к устройствам малого радиуса действия, но спроектированные для широкого охвата территории. К таким стандартам относятся такие стандарты как LoRa, Weightless и Sigfox;
- **Технологические сети** на основе стандартов профессиональной подвижной связи, таких как TETRA или DMR являются нишевым, но тем не менее значимым сегментом сетей M2M или IoT.



ИВ (IoT) в нелицензируемых полосах радиочастот Технологии M2M/ИВ(IoT) с ограниченным охватом (LPLA)



Локальные и персональные сети, или LPLA (Low Power Local-Area Networks). Примеры: Wifi, ZigBee и Bluetooth. Не имеют прямого подключения к сетям передачи данных, но могут использовать различные шлюзы для расширения своего охвата. Гибридные решения тоже относятся к LPLA.

Частотный ресурс для таких устройств определен достаточно давно и располагается в диапазонах 434 МГц и 868 МГц, хотя в последнее время также осваиваются новые полосы частот 870-876 МГц и 915-921 МГц. Диапазон частот 434 МГц гармонизирован на международном уровне и не подпадает под ограничения рабочего цикла, которые действуют для диапазона частот 868 МГц и новых полос частот. Этим объясняется значительная загруженность диапазона 434 МГц.

Технологии ИВ (IoT) с большой площадью покрытия (LPWA)



Технология	LoRa	«Стриж»	«Глонасс»	NB-Fi
Тип сигнала	Прямое расширение спектра (ЛЧМ)	Сверхузкополосный канал	Сверхузкополосный канал	Сверхузкополосный канал
Ширина канала	200 кГц	100 Гц	100-1000 Гц Опционально порядка 10 кГц.	100 Гц
Скорость в канале	От 300 бит/с до 50 кбит/с	100 бит/с	100-1000 бит/с, до 10 кбит/с для сигнала 10 кГц	100 бит/с
Полосы частот	863-876 МГц 915-921 МГц	863-876 МГц	863-865 МГц 874-876 МГц	863-876 МГц 915-921 МГц 433 МГц
Открытость	Чип проприетарный, остальные элементы открыты	Закрытый стандарт	Открытый стандарт, реализован только разработчиком	Открытый стандарт, реализован только разработчиком

Вопросы обеспечения информационной безопасности и устойчивости сети ИВ (IoT)



С ростом числа подключенных устройств и использованием беспроводных технологий растут и риски информационной безопасности. По этой причине, требуется обеспечение информационной безопасности на уровне сетей радиодоступа, а в наиболее критически важных случаях и на уровне конечных устройств.

Основные угрозы безопасности и устойчивости работы сети ИВ (IoT):

- Электромагнитные шумы и радиочастотные помехи
- Перегрузка узкополосного радиоканала при пике нагрузки или в следствие информационных атак на отказ в обслуживании
- Информационные атаки на транспортные узлы сети, узлы обработки данных, конечные устройства (устройства управления, сенсоры и др.)
- Нецелевое использование элементов и узлов сети

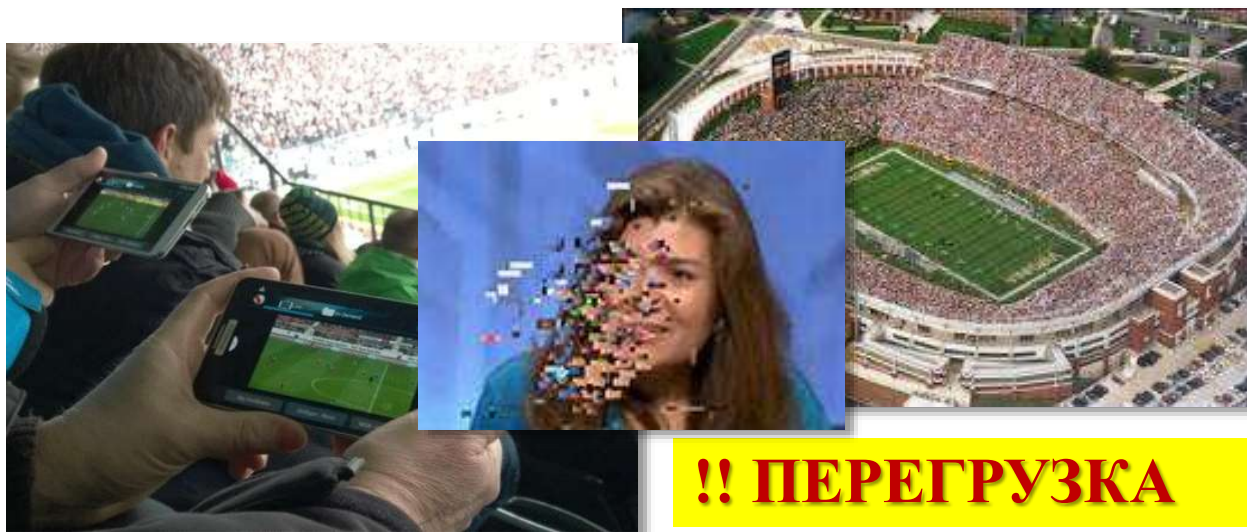


Нарушение конфиденциальности, целостности, достоверности и доступности информационных ресурсов сетей ИВ (IoT) может привести к значительному ущербу и тяжелым последствиям

Проблематика перегрузки канала при высоких нагрузках в сетях передачи данных актуальна для ИВ (IoT)



Типичные ограничения технологии индивидуальной передачи данных в сети передачи данных на примере трансляции видеопрограмм



В условиях высокой абонентской нагрузки негативно влияют:

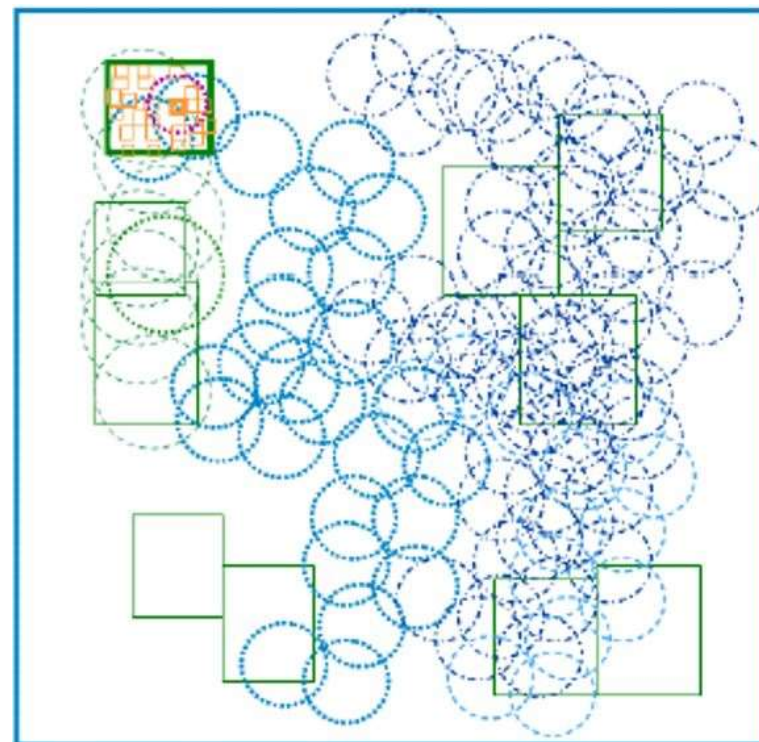
- Общие ограничения пропускной способности сетевой инфраструктуры
- Ограничения вычислительных мощностей и канала связи контент-провайдера
- Недостаток общей пропускной способности местного канала ШПД (например, сети 4G/5G)
- Конкуренция с другими видами трафика

Для устранения всех «узких мест» потребуются дополнительные меры, следствие: повышенная стоимость услуг либо падение качества услуг при высокой загрузке

Вопросы обеспечения информационной безопасности и устойчивости сети



Основные особенности применения сетей ИВ (IoT) в составе промышленных информационных систем и систем управления:



Устойчивость сети требует **резервирования каналов, узлов и других элементов сети** на нескольких уровнях

Уровни сети IoT предприятия:

- **инфраструктурный**
- **производственный**
- **ЛОГИСТИЧЕСКИЙ**



Целесообразно разработать систему требований по криптографической защите радиointерфейсов сетей IoT, в которой была бы введена классификация применений, требующих использования тех или иных видов криптографии.



В узкополосных беспроводных сетях связи IoT в безлицензионных полосах радиочастот отсутствуют стандартизированные аналоги SIM-карт. Замена криптографических алгоритмов может быть связана с доработками оборудования сети радиодоступа



- В сетях NB-IoT предусмотрена возможность замены алгоритмов шифрования без модификации сети радиодоступа за счет замены алгоритмов в SIM-картах (включая программные) и системах аутентификации.

Помимо самих криптографических механизмов также требуется регламентировать требования по защищенности хранения криптографических ключей в конечных устройствах.

- В сетях NB-IoT данная проблема решается за счет использования применения функционального аналога SIM-карты - модуля идентификации абонента UICC.



Риски использования иностранного оборудования и ПО

Санкционные

Прекращение поставок, в том числе из-за санкций

Прекращение технической поддержки, отказ в продлении лицензий на ПО

Информационные

Доступ в глобальную сеть, обновления ПО и дистанционный сбор данных, мониторинг оборудования с момента установки



Оборудование ИВ (IoT) открыто по прямому доступу (перехват управления, закладки)

Комплекс работ с целью нормативно-технического обеспечения построения и развития узкополосных беспроводных сетей Интернета вещей :

- Регулирование использования радиочастотного спектра сетей Интернета вещей, использующих лицензируемые полосы радиочастот.
- Регулирование использования радиочастотного спектра сетей Интернета вещей, использующих безлицензионные полосы радиочастот включая условия использования нелицензируемых полос радиочастот устройствами малого радиуса действия.
- Регуляторные условия развертывания сетей Интернета вещей различных технологий.
- Вопросы лицензирования деятельности операторов сетей Интернета вещей.
- Создание отечественных стандартов и гармонизации с существующими зарубежными стандартами узкополосных беспроводных сетей связи Интернета вещей.
- Организация производства и внедрения отечественного телекоммуникационного оборудования для узкополосных беспроводных сетей связи Интернета вещей.
- Требования к сертификации оборудования.
- Нормативная база в области обеспечения информационной безопасности.
- Контроль качества работы узкополосных сетей NB-IoT.

Основные выводы



- Рынок Интернета вещей быстро растет и будет играть важную роль в цифровой трансформации и экономическом развитии, в частности производственных систем, ЖКХ, систем «умный город».
- Для развития ИВ/IoT на одной территории могут быть использованы сразу несколько систем и полос радиочастот.
- Большинство ИВ/IoT соединений вне помещений и внутренних производственных сетей будет узкополосным в формате LPWA.
- Гармонизация используемых стандартов при одновременном обеспечении защиты от информационных угроз и отказоустойчивости является ключевым фактором для обеспечения экономически эффективных решений IoT.
- Для развертывания оптимизированных систем на основе IMT для узкополосной связи IoT LPWA (например, работающих с 200 кГц (NB-IoT) и 1,4 МГц (eMTC)) рекомендуется использование уже идентифицированного спектра для подвижной связи (IMT)
- Потребности широкополосного ИВ/IoT можно обеспечить с помощью существующих и будущих широкополосных систем радиосвязи.



СПАСИБО ЗА ВНИМАНИЕ!

**Лашкевич Андрей Владимирович –
заместитель начальника отдела
НТЦ анализа ЭМС ФГУП «НИИ Радио»**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ РАДИО**