



# LPWAN технологии

для интернета вещей

# СОДЕРЖАНИЕ

<b>СЕТИ IOT</b>	<b>3</b>
<b>LPWAN ТЕХНОЛОГИИ</b>	<b>4</b>
Технология LoRaWAN	
Технологии UNB LPWAN	
<b>ТЕХНОЛОГИЯ GOODWAN</b>	<b>5</b>
Классы устройств сети GoodWAN	
Технология обмена данными с конечными устройствами	
Оптимизированные протоколы	
Динамическое кодирование	
Сквозное шифрование данных	
<b>СРАВНИТЕЛЬНЫЙ АНАЛИЗ LPWAN ТЕХНОЛОГИЙ</b>	<b>9</b>
Дальность и помехозащищенность	
Емкость сети	
Пропускная способность сети	
Поддержка движущихся объектов	
Сетевой роуминг	
Обеспечение безопасности данных	
Необходимость получения лицензии	
GoodWAN альянс	
<b>ВЫВОД</b>	<b>12</b>

В настоящее время наблюдается взрывное развитие индустрии интернета вещей (в том числе индустриального интернета вещей). По прогнозам в ближайшее время прирост новых устройств IoT составит от 3,5 до 6 миллиардов устройств в год, что очевидно, накладывает серьезные требования на сети IoT.

Разработчики устройств и систем IoT используют несколько типов сетей, основные:

- Low Power Wide Area Network (**LPWAN**) сети.
- NarrowBand Internet of Things (**NB-IoT**) сети.

**LPWAN** представляет собой специально разработанную для IoT беспроводную технологию передачи небольших объемов данных на дальние расстояния. Особенности LPWAN являются: большая дальность передачи радиосигнала, низкое энергопотребление конечного устройства, работа в безлицензионном диапазоне частот.

**NB-IoT** является расширением традиционного стандарта сотовой связи для устройств IoT и использует существующую инфраструктуру сетей сотовой связи. Особенности NB-IoT являются: большая емкость сети, высокая пропускная способность, работа в лицензируемом диапазоне радиочастот.

С точки зрения практического развития IoT для конечного потребителя, можно говорить о ряде преимуществ **LPWAN** технологий и их большей перспективности за счет:

- использования безлицензионного диапазона радиочастот;
- большей площади покрытия одной базовой станцией (сетевым шлюзом);
- меньшей стоимостью конечного устройства IoT;
- большим сроком работы на одном элементе электропитания;
- простотой и меньшей стоимостью разворачивания IoT сети.

“

*В ближайшее время прирост новых устройств IoT составит от 3,5 до 6 миллиардов устройств в год*



# LPWAN ТЕХНОЛОГИИ

## Технология LoRaWAN

**LoRaWAN** сеть имеет топологию звезда. Конечные устройства через сетевые шлюзы (базовые станции) взаимодействуют с сервером сети. Обычно шлюзами и сервером владеет оператор сети, а конечными устройствами – абоненты. Абоненты имеют возможность прозрачной одно или двунаправленной и защищенной передачи данных до конечных устройств.

Широкополосный радиосигнал LoRaWAN представляет собой сигнал с линейной частотной модуляцией (ЛЧМ) или CSS (Chirp Spread Spectrum). Частота CSS радиосигнала может, как увеличиваться (up-chirp), так и уменьшаться (down-chirp). Такое решение, в отличие от технологии прямого расширения спектра, делает приемник устойчивым к отклонениям частоты от номинального значения и упрощает требования к тактовому генератору, что позволяет использовать недорогие кварцевые резонаторы.

Технология LoRaWAN использует асинхронный режим приема-передачи. Для синхронизации приемника с передатчиком используется преамбула, которая позволяет приемнику обнаружить активность передатчика. Принимающие станции LoRaWAN могут определять преамбулы на всех скоростях всех каналов, однако они не могут демодулировать более чем 8 пакетов одновременно.

В сети LoRaWAN предусмотрено три класса конечных устройств:

- *Класс А.* Устройства с двусторонним каналом. Связь инициируется конечным устройством, после чего выделяются два временных окна, в течение которых ожидается ответ от сети.
- *Класс В.* Устройства с двусторонним каналом. В дополнение к функциям устройств «класса А», открывают дополнительные окна приема по расписанию. Для этого конечное устройство синхронизируется по специальным сигналам от шлюза.
- *Класс С.* Устройства с двусторонним каналом и максимальным приемным окном. Конечные устройства имеют почти непрерывно открытое окно приема, закрывается только на время передачи данных.

Технология LoRaWAN спроектирована как универсальная сеть для обеспечения работы двунаправленных конечных устройств. Такая универсальность влечет за собой необходимость передачи большого количества служебной информации, что негативно влияет на пропускную способность сети (максимальное количество сообщений в единицу времени).

Еще одной особенностью LoRaWAN является открытость идентификаторов конечных устройств в радиозэфире, что позволяет злоумышленнику однозначно идентифицировать устройства и собирать передаваемую информацию.

## Технологии UNB LPWAN

Сети **SigFox**, **Стриж** и **ВАБИОТ**, в отличие от LoRa, используют сужение полосы спектра сигнала (Ultra Narrow Band) с целью увеличения соотношения сигнал/шум на приемнике и увеличения дальности.

Все указанные сети, включая LoRaWAN, имеют топологию звезда и используют асинхронный режим приема-передачи.

SigFox использует собственный проприетарный радиопrotocol, Стриж протокол XNB, ВАБИОТ радиопrotocol NB-Fi.

На физическом уровне для передачи сигнала используется модуляция DBPSK (фазовая модуляция, при которой битный поток на физическом уровне кодируется фазой несущей 0 или 180°. Для обеспечения высокой дальности, ширина полосы канала передающего устройств SigFox, Стриж и ВАБИОТ составляет 100 Гц. Вместе с высокой энергетикой на каждый бит передаваемой информации обеспечивается хороший энергетический потенциал канала связи (link budget) и высокую помехоустойчивость. ВАБИОТ заявляет значение энергетического потенциала в 166 дБм, Стриж 176 дБм и SigFox 163.3 дБм.

Стриж, ВАБИОТ и SigFox используют FDMA (Frequency Division Multiple Access) и TDMA (Time Division Multiple Access) технологию разделения канала.

В указанных LPWAN системах применяются устройства с обратным каналом передачи информации от сетевого шлюза, который инициируется конечным устройством, после чего выделяются окна, для получения ответа от сети.

Производители устройств заявляют дальность передачи сигнала от конечного устройства до 10 км в условиях города и до 45 км вне города.

Во всех указанных UNB LPWAN заявлено применение AES128 для шифрования передаваемых данных. В сети Стриж декларируется опция ГОСТ Р 34.12-2005. Шифрование применяется для передаваемых по радиоканалу данных.



# ТЕХНОЛОГИЯ GOODWAN

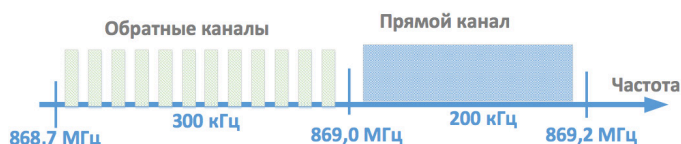
Разработчики технологии **GoodWAN** поставили перед собой задачу создания сети, которая смогла бы обеспечить все преимущества LPWAN технологий, связанных с низким энергопотреблением, низкой стоимостью конечных устройств и сетевых шлюзов с одновременным обеспечением высокой пропускной способности, увеличения емкости сети с одновременным обеспечением уровня защищенности, соответствующему актуальным угрозам безопасности.

Технология GoodWAN объединяет в себе как наиболее удачные подходы, также применяемые в других LPWAN, так и собственные уникальные разработки:

- Ultra Narrow Band с частотной модуляцией для прямого канала;
- Wide Band для обратного канала;
- оптимизированные радио протоколы для однопользовательных и двусторонних конечных устройств;
- оптимизацию объема передаваемой служебной информации;
- динамическое кодирование идентификаторов конечных устройств;
- поддержку движущихся конечных устройств;
- сквозное шифрование передаваемых конечным устройством данных.

GoodWAN сеть имеет топологию звезда. Конечные устройства через сетевые шлюзы (базовые станции) взаимодействуют с сервером сети. Диапазон используемых GoodWAN радиочастот 863,0-870,0 МГц с мощностью от 25мВт до 100мВт, что позволяет использовать конечные устройства и создавать частные сети без получения лицензии на использование радиочастот.

Для прямого канала в сети GoodWAN применяется Ultra Narrow Band радиосигнал с частотной модуляцией. Для обратного канала используется радиосигнал с узкой полосой передачи с BW=15,6 кГц с частотной модуляцией с линейной, что позволяет выделить в одном диапазоне 500 кГц прямой канал 200 кГц и 12 обратных каналов с шагом

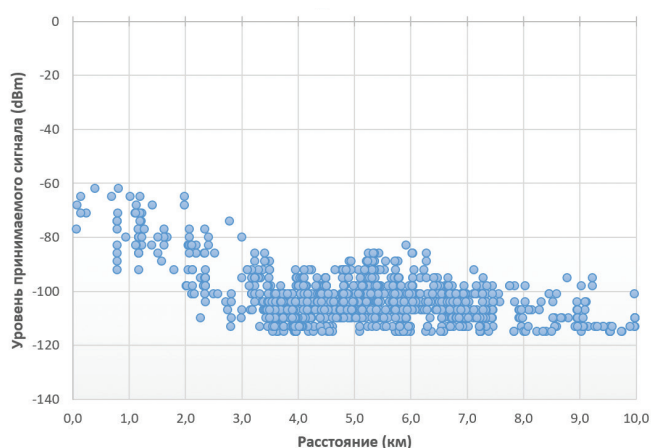


25 кГц. Такая конфигурация может обеспечить пропускную способность одновременно более 846 000 сообщений в прямом канале и отправку более 96 000 команд (от шлюза к конечному устройству) одним сетевым шлюзом в течение суток.

“

*GoodWAN обеспечивает все преимущества LPWAN технологий, связанных с низким энергопотреблением, низкой стоимостью конечных устройств и сетевых шлюзов с одновременным обеспечением высокой пропускной способности, увеличения емкости сети с одновременным обеспечением высокого уровня защищенности.*

Практические замеры дальности показали возможность приема с приемлемым уровнем сигнала сообщений на расстоянии до 8 км в условиях г. Москвы.



GoodWAN: RSSI – расстояние



## Классы устройств сети GoodWAN

Назначение и область применения конечных устройств IoT не всегда требует наличия обратного канала к устройству. Односторонние конечные устройства IoT имеют ряд преимуществ по стоимости и сроку службы на одном элементе питания. Так же отсутствие необходимости в обратном канале положительно сказывается на емкости сети.

В сетях **GoodWAN** выделены следующие классы устройств:

- **Класс А.** Устройства с односторонним каналом и статическим или динамическим кодированием идентификатора конечного устройства сквозным шифрованием информации и имитовставкой. Такие устройства могут применяться там, где требуется наиболее простые устройства с минимальной стоимостью и максимальным сроком работы и подходят для решения подавляющего большинства задач телеметрии. Такие устройства могут свободно перемещаться между базовыми станциями и обеспечивают максимальную защиту от прослушивания при использовании динамического кодирования.
- **Класс В.** Устройства с двусторонним каналом, динамическим кодированием и сквозным шифрованием данных и имитозащитой сообщений. Применяются в случаях, когда требуется обеспечить защищенный обратный канал управления автономным конечным устройством с высокой скоростью доставки управляющего сигнала.



*Односторонние конечные устройства IoT имеют ряд преимуществ по стоимости и сроку службы на одном элементе питания*

Характеристика	Класс А	Класс В
Ширина полосы прямого канала	200Гц	200Гц
Скорость передачи данных	100 б/с	100 б/с
Избыточное кодирование CR	4/8	4/8
Время передачи сообщения (секунд)	1.6/2.1/3.1	1.1/1.6/2.1/3.1
Объем передаваемых данных	60/84/132 бит	36/60/84/132 бит
Контроль целостности	CRC16/MIC	CRC16/MIC
Наличие обратного канала	нет	да
Динамическое кодирование	да	да
Сквозное шифрование данных	да	да
Поддержка мобильных конечных устройств	да	да
Поддержка сетевого роуминга	да	да

Таблица 1. Характеристики классов устройств GoodWAN

## Технология обмена данными с конечными устройствами

В сети GoodWAN применяется **Ultra Narrow Band** радиосигнал с частотной модуляцией для прямого канала и **Wide Band** радиосигнал с линейной частотной модуляцией для обратного канала.

Применение узкополосного сигнала с высокой энергетикой на каждый бит передаваемой информации обеспечивает хороший энергетический потенциал канала связи и высокую помехоустойчивость. Пропускная способность в не лицензируемом диапазоне радиочастот составляет 846 тыс. сообщений в сутки для разных классов устройств.

Применяемая технология обратного канала позволяет минимизировать мощность обратного сигнала до разрешенного уровня от 25 мВт до 100 мВт.

С точки зрения пользователя GoodWAN применение UNB с частотной модуляцией в прямом канале позволяет:

- на порядок увеличить пропускную способность и емкость сети по сравнению с LoRaWAN;
- повысить помехозащищенность;

## Оптимизированные протоколы

Назначение конечных устройств IoT можно разделить на две группы: телеметрия и телеуправление. Большинство конечных устройств IoT выполняют именно функции телеметрии, не требующей наличия обратного канала к устройству. Конечные устройства, предназначенные для дистанционного управления или требующие наличия обратного канала (трекеры, устройства умного дома, пейджеры, устройства управления поливом и пр.) используют его существенно реже, чем прямой. Необходимый контроль наличия канала связи осуществляется за счет передачи регулярных контрольных сообщений.

Дальность работы любого радиоканала на физическом уровне определяется следующими физическими параметрами:

- энергией информационного бита (мощность передатчика, помноженная на время передачи бита);
- уровнем собственного шума приемника и уровнем шума эфира.

Иными словами:

- чем больше энергии (мощность сигнала, умноженная на время его передачи) будет выделено на передаваемый бит, тем дальше его можно передать;
- чем меньше собственные шумы приемника и шумы эфира, тем большая дальность приема будет обеспечена.

Для улучшения соотношения сигнал/шум в различных LPWAN протоколах используются различные методы расширения спектра сигнала: DSSS (каждый бит кодируется длинной псевдослучайной последовательностью) или FHSS (каждый бит долго передается на фиксированной псевдослучайной частоте). При этом, увеличение длины времени передачи негативно влияет как на энергоэффективность, так и на емкость сети.

Таким образом, для обеспечения энергоэффективности технология передачи данных должна использовать максимально короткие сообщения. Уменьшения объема передаваемых данных можно достигнуть за счет минимизации объема служебной информации.

В сети GoodWAN созданы специализированные протоколы для однонаправленных и двунаправленных конечных устройств IoT, что позволяет:

- минимизировать стоимость конечных устройств;
- минимизировать стоимость сетевых шлюзов;
- увеличить пропускную способность сети;
- увеличить срок работы датчика от одного элемента питания.

Отсутствие необходимости обеспечения универсальности сети (как LoRaWAN) позволяет отказаться от передачи ряда данных и минимизировать объем служебных сообщений.

- повысить дальность передаваемого сигнала;
- обеспечить поддержку движущихся конечных устройств.

Цифровая обработка сигнала на сетевом шлюзе (базовой станции) реализована на основе производительного специализированного сигнального процессора, что с одной стороны уменьшает стоимость шлюза без ухудшения характеристик, а с другой стороны повышает устойчивость к «зависаниям» и снижает энергопотребление.

## Динамическое кодирование

Динамическое кодирование разработано для обеспечения аутентификации конечных устройств. Обычно для подтверждения идентификатора конечного устройства используется результат криптографического преобразования, аргументами которого является идентификатор устройства и секрет (известный устройству и сети), который передается в сообщении и является служебной информацией.

Технология динамического кодирования GoodWAN осуществляет смену идентификатора устройства каждые 256 секунд. Выработка нового идентификатора производится путем криптографического преобразования ключа, известному устройству и сети. В сообщении вместо открытого идентификатора устройства (как в других LPWAN) передается динамический идентификатор. Сеть GoodWAN по динамическому идентификатору определяет реальный идентификатор устройства. Для приложения пользователя, использующего данные с конечных устройств, применение динамического кодирования является полностью прозрачным.

Длина динамического идентификатора конечного устройства составляет 32 бита, динамический идентификатор может принимать более 4-х миллиардов значений.

Такой подход имеет ряд преимуществ:

- сокрытие данных о составе сети и конечных устройствах;
- усложнение для злоумышленника процесса выделения конечных устройств;
- защита от атаки повторной отправки сообщений;
- максимально возможная минимизация объема передаваемой информации;
- отсутствие у приложения необходимости проведения аутентификации датчика.

Необходимо отметить, что такой способ динамического кодирования может привести к коллизии данных, когда два или более датчика могут в момент передачи данных иметь одинаковый динамический идентификатор. При возникновении такой коллизии сеть определяет принадлежность сообщения к конкретному датчику по значению хеш-функции, которая передается в полезной нагрузке.

## Сквозное шифрование данных

Защита данных конечного устройства (payload) осуществляется путем шифрования устройством и расшифровкой приложением пользователя. Так же защита осуществляется и при передаче команд в обратном канале (от приложения к устройству).

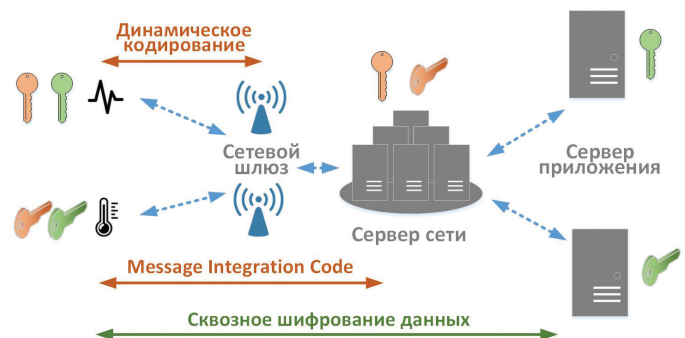
В сети GoodWAN применяется шифрование AES128. Каждое конечное устройство имеет идентификатор и персональный ключ 128 битный ключ AppPKey. При активации устройства (или отключении/подключении элемента питания) ключ аутентификации приложения AppPKey используется для вычисления ключа приложения AppSKey.

Сквозное шифрование осуществляется на ключе AppSKey.

Архитектура GoodWAN предусматривает вынесение сервиса отвечающего за выработку ключа приложения AppSKey на сторону приложения, что дает возможность пользователю обеспечить безопасность независимо от оператора сети.

Применение шифрования позволяет обеспечить:

- аутентичность данных конечного устройства и команд им;
- конфиденциальность информации;
- безопасное хранение информации.





# СРАВНИТЕЛЬНЫЙ АНАЛИЗ LPWAN ТЕХНОЛОГИЙ

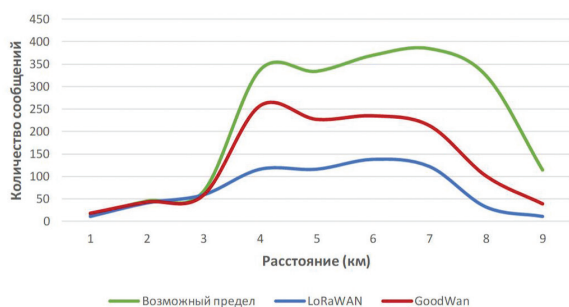
## Дальность и помехозащищенность

LoRaWAN обладает сравнительно низкой избирательностью по соседнему каналу, блокирующим помехам и интермодуляции. На практике, при большой плотности конечных устройств это приводит к уменьшению эффективной дальности приема сигнала и необходимости увеличения количества сетевых шлюзов (базовых станций) для обеспечения приемлемого качества работы сети.

В компании GoodWAN провели сравнительные практические замеры качества покрытия LoRaWAN и GoodWAN. Оба конечных устройства (LoRaWAN и GoodWAN) находились в одинаковых условиях, включались и выключались одновременно.

В процессе испытаний оценивалось количество принятых сообщений от каждого конечного устройства и зависимость количества принятых сообщений от расстояния до шлюза (базовой станции). Всего за время испытаний было принято 1522 сообщения конечного устройства GoodWAN и 771 сообщения от конечного устройства LoRaWAN.

На графике представлено соотношение количества всех принятых сообщений и расстояния до шлюза LoRaWAN и GoodWAN.



Абсолютное количество сообщений в зависимости от расстояния в км

Необходимо отметить, что:

- конечные устройства передавали сообщения с одинаковым интервалом и в идеальных условиях они все должны быть получены сетью. Однако условия плотной застройки города и большое количество помех в радиозфере снижают количество принимаемых сообщений.
- передвижение на автомобиле по дорогам г. Москвы не позволило обеспечить одинаковое (по времени) нахождение на разных дистанциях до шлюза ввиду расположения дорог в городе и дорожных условий. Линия «Мах» показывает время работы конечного устройства на определенном расстоянии до шлюза. Фактически линия «Мах» определяет максимальное теоритическое количество сообщений от конечного устройства.

Еще одной слабостью LoRaWAN является возможность блокировки работы базовой станции достаточно простым устройством, которое генерирует помехи поочередно на разных каналах. Использование UNB прямого канала позволяет устранить эти недостатки.

## Емкость сети

Возможности LPWAN сетей зависят от ширины разрешенных полос в разных странах. Например, в США для свободного использования выделена полоса в 26 МГц (902 - 928 МГц), в Европе 2 МГц (867-869), а в России для этих же целей выделено 0,5 МГц и 3,5 МГц с ограничениями 0,1% рабочего цикла и запретом работ в районе аэропортов, это делает крайне ограниченным использованием обратного канала в этом диапазоне. Ширина канала LoRaWAN составляет 125 кГц, плюс буферная зона для каждого канала (это увеличивает полосу до 200 кГц). В США в разрешенный диапазон «помещается» 80 каналов LoRaWAN (SF7-SF10), в Европе 10 каналов (SF7-SF12). Емкость шлюза GoodWAN соответствует 244 каналам шлюза LoRaWAN с SF=12 (эквивалентное количество каналов определено на основании результатов практических замеров пропускной способности сети).

Заявленное максимальное теоретическое количество каналов Стриж и ВАБИОТ составляет 5000 в полосе 500 кГц. На практике же используются приемники с шириной канала 100 - 200 кГц с 16-ти разрядным АЦП, что снижает заявленную пропускную способность и динамический диапазон шлюза, в UNB сетях практически не возможно передать сообщение в конкретном узком канале ввиду невозможности точной установки частоты передачи на конечном конечном устройстве. В случае с UNB сетями емкость следует оценивать по максимальному количеству передаваемых сообщений в единицу времени. Тем не менее количество каналов в UNB сетях на порядок больше, чем у LoRaWAN.



## Пропускная способность сети

Одним из популярных критериев сравнения LPWAN технологий является скорость передачи данных датчиком по радиоканалу. Необходимо понимать, что устройства передают достаточно малый объем данных и скорость передачи между устройством и сетевым шлюзом (базовой станцией) не оказывает принципиального влияния на итоговое время получения данных приложением. Необходимо учитывать и соотношение объема полезной информации к объему служебной информации и необходимость избыточного кодирования на физическом уровне. Обычно соотношение полезной информации к общей составляет не более 0,25. То есть на каждый полезный бит данных в радиоканал отправляется 4 бита служебных и избыточных данных.

Еще одним вопросом, влияющим на пропускную способность сети является обеспечение гарантии доставки сообщений. Если квитирировать каждое сообщение по обратному каналу, то сеть очень быстро перегрузится. В момент, когда шлюз передает информацию, он не может принимать сообщения от устройства. Подавляющее большинство устройств обеспечивают передачу сообщений телеметрии, которые не требуют гарантированной доставки каждого сообщений. Поэтому наиболее оптимальным вариантом является использование датчиков без подтверждения сообщений по обратному каналу. Вместе с тем, есть сообщения критического характера (срабатывание сигнализации, выход параметра за пределы установленных значений и пр.), которые подразумевают гарантии доставки сообщений. Для обеспечения необходимой доставки сообщений без квитанции и их достоверности, во всех LPWAN системах применяют многократную отправку сообщений. Например, в сети SigFox каждое сообщение отправляется три раза подряд.

Это означает, что декларируемые разработчиками значения скоростей передачи данных невозможно использовать для оценки реальной пропускной способности сети LPWAN. Одним из приближенных к практике способов оценки «скорости» сети является оценка максимального количества сообщений от датчиков, при которых вероятность их наложения друг на друга является приемлемой (в пределах 5-15% и обеспечивается декларируемая дальность работы сети).

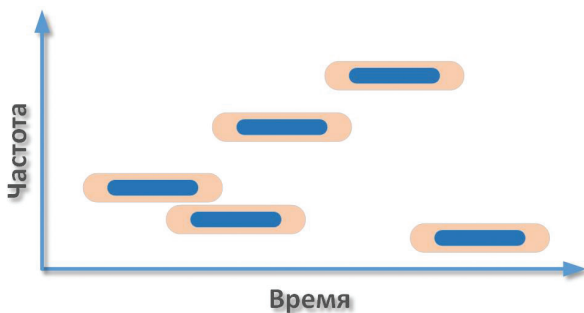


диаграмма распределения UNB посылок по частоте и времени.

UNB сигнал сосредоточен в темной области размером равным  $F \cdot T$ , где  $F$  – ширина полосы посылки,  $T$  – время сообщения в эфире. Оранжевая область – это защитный интервал вокруг каждого сообщения размером  $2F \cdot 2T$ . Сообщения расположены случайно, а площадь, занимаемая ими многократно меньше площади, на которой они расположены.

Вероятность  $P$  наложения нового сообщения на существующие можно оценить, как отношение свободной площади к полной площади рисунка:

$$P = N \times \frac{2F \times 2T}{W \times I}$$

где:

- $N$  – количество посылок за время измерения  $I$
- $I$  – интервал времени измерения (например 1 час)
- $W$  – ширина UNB канала

Указанная формула является оценочной, так как:

- применима при небольших процентах заполнения (уже при 10% необходимо учитывать, что изначальные посылки имеют тоже 10% перекрытие и надо сделать поправку +10%);
- на практике, при наложении пропадают не все сообщения (более мощное сообщение «побеждает» слабое);
- на практике применяется помехозащищенное кодирование (CR=4/8), что допускает частичное перекрытие посылок;
- ширина канала зависит от качества модуляции передатчика и избирательности шлюза по соседнему каналу.

Практические испытания подтвердили оценки пропускной способности сети GoodWAN в 846 000 сообщений в сутки при вероятности наложения не выше 10%. Теоритическая оценка пропускной способности сети LoRaWAN составляет 28 280 сообщений в сутки при вероятности наложения не выше 10% и значении коэффициента расширения спектра (SF) равном 12. При этом практический радиус покрытия одним сетевым шлюзом LoRaWAN меньше аналогичного показателя сети GoodWAN. Сеть LoRaWAN позволяет обеспечить сравнимую теоритическую пропускную способность около 600 000 сообщений в сутки с вероятностью наложения не выше 10% путем уменьшения коэффициента расширения спектра до 7. При этом происходит существенное уменьшение площади покрытия до не сопоставимой с зоной покрытия любой UNB сети. Так же это ведет к росту количества «граничных» зон, в которых конечные устройства могут работать не стабильно.

## Поддержка движущихся объектов

SigFox, Стриж и ВАБИОТ для передачи сообщений в прямом канале используют фазовую модуляцию, что приводит к ухудшению качества приема сигнала с движущихся объектов за счет многолучевого распространения узкополосного сигнала и существенному сокращению дальности работы системы.

GoodWAN использует UNB сигнал с частотной модуляцией которая менее чувствительна к движению конечного устройства.

## Сетевой роуминг

Архитектура GoodWAN поддерживает роуминг движущихся объектов в рамках единого оператора сети GoodWAN из множества пространственно распределенных сетевых шлюзов (базовых станций) за счет безусловного приема всех сообщений от всех датчиков и обеспечения агрегации и фильтрации на уровне сети. Сети LoRaWAN располагают возможностями обеспечения международного пассивного роуминга.

## Обеспечение безопасности данных

GoodWAN имеет технологию динамического кодирования, аналоги которой отсутствуют в других LPWAN сетях. Шифрование, применяемое в них, для защиты данных на уровне радиоканала, является традиционным подходом для более «крупных» сетей.

Сквозное шифрование данных между конечным устройством и приложением обеспечивается только сетями LoRaWAN и GoodWAN. Сети SigFox, Стриж и ВАБИОТ обеспечивают шифрование только на этапе передачи по радиоканалу. Это означает, что оператор связи имеет доступ к данным, передаваемым конечными устройствами и команд им.

## Необходимость получения лицензии

В сетях SigFox, Стриж и ВАБИОТ для обеспечения симметричного по дальности обратного канала требуется повышенная мощность передатчика базовой станции (до 0,5 - 2 Вт). Это приводит к необходимости получения лицензии на использование радиочастот. Что в свою очередь негативно сказывается на скорости и простоте разворачивания сети SigFox и создает сложности при построении частных сетей в России.

## GoodWAN альянс

Альянс, который мы создаем, объединит не только операторов связи, но и разработчиков конечных устройств, интеграторов, разработчиков ПО. Мы субсидируем установку шлюзов нашей сети. У пользователей отсутствует абонентская плата, предусматривается только однократный разовый платеж для начального подключения конечных устройств к сети на все время жизни устройств. Этот платеж направляется на развитие и поддержку сети, а также формируют фонд, который мы делим с членами нашего альянса. Единое частотное планирование сети и распределенный сервер сети позволяет предлагать межоператорские решения и решить проблему роуминга устройств. Это значит, что разработчики могут создавать свои IoT системы без капитальных вложений в сеть.



# ВЫВОД

Взрывное развитие IoT технологий обеспечит потребность в наличии как универсальных, так и нишевых технологий. Сети, построенные по технологии NB-IoT займут существенную часть рынка, однако LPWAN сети станут по-настоящему массовыми за счет минимальной стоимости и простоты разворачивания.

Приведенный выше анализ показывает, что GoodWAN в наибольшей степени соответствует идеологии IoT и имеет преимущества перед LoRaWAN, SigFox, Стриж и ВАБИОТ по одновременной сумме ключевых параметров LPWAN сетей:

- низкая стоимость конечных устройств в самом массовом классе односторонних устройств (по сравнению с LoRaWAN)
- большая пропускная способность (по сравнению с LoRaWAN)
- высокая помехозащищенность от легальных источников помех в безлицензионном диапазоне частот (по сравнению с LoRaWAN)
- возможность работы на движущихся объектах без потери дальности (по сравнению с SigFox, Стриж и ВАБИОТ)
- наличие эффективного обратного канала (по сравнению с SigFox, Стриж и ВАБИОТ)
- высокой защищенности данных за счет возможности динамического кодирования ID устройств (по сравнению с LoRaWAN, SigFox, Стриж и ВАБИОТ)
- наличие специальных помехозащищенных и энергоэффективных протоколов управления движущимися объектами в классе B (по сравнению с LoRaWAN, SigFox, Стриж и ВАБИОТ)

Несмотря на большое количество альтернативных LPWAN технологий, GoodWAN по отдельным показателям и по их совокупности обладает рядом преимуществ и предоставляет уникальные возможности, которых не предусмотрено в альтернативных технологиях.

“

*GoodWAN обладает рядом преимуществ и предоставляет уникальные возможности, которых не предусмотрено в альтернативных технологиях.*



117587, г. Москва, Варшавское шоссе, д. 125Ж, корп.7

Тел.: +7 499 455 04 35

[info@goodwan.ru](mailto:info@goodwan.ru)  
[www.goodwan.ru](http://www.goodwan.ru)

