LoRaWAN
как надежная и безопасная технология связи

Андрей ЭКОНОМОВ,
участник технического комитета LoRa Alliance, к. ф.-м. н.

В настоящее время в большинстве развитых стран мира в дополнение к мобильной связи активно развиваются радиосети нового типа – Интернета вещей (IoT) класса LPWAN (LowPower WAN), работающие на нелицензируемых (общедоступных) радиочастотах. В Российской Федерации с этой целью выделен диапазон 868 МГц (частоты 864–869,2 МГц), в котором уже построены сети как общемирового стандарта LoRaWAN, так и локальных спецификаций, например XNB и NB-Fi.

Базовые характеристики LoRa/LoRaWAN

По состоянию на начало 2020 г. именно стандарт LoRaWAN является драйвером развития направления IoT (Internet of Things) во всем мире и используется в качестве основного инструмента для управления критически важной инфраструктурой, транспортом, а также производством, здравоохранением, муниципальным и сельским хозяйством. И это далеко не пилотные проекты, например, в России уже более 10 тыс. уличных светильников управляются сетью LoRaWAN АО «ЭР-Телеком Холдинг».

Конференции, посвященные технологии LoRaWAN, собирают тысячи участников со всего мира, например ежегодная The Thing Conference в Нидерландах. В LoRa Alliance входит более 500 компаний, среди которых можно назвать мировых гигантов – Google, Alibaba, Orange, CISCO, NEC и IBM, а также отметить трех участников из России – «ЭР-Телеком», МТТ и «Лартех».

Спецификация LoRaWAN развивается с 2015 г.: LoRa – это сокращение от слов Long Range («дальнее действие»). Беспроводные сети базируются на методе модуляции радиоинтерфейса LoRa, запатентованном Semtech Corporation, и на открытом протоколе LoRaWAN, разработанном исследовательским центром IBM Research в партнерстве с Semtech Corporation.

К отличительным особенностям стандарта LoRaWAN следует отнести [2]:

- помехоустойчивую модуляцию, относящуюся к классу ЛЧМ (линейно-частотной модуляции), в англоязычной терминологии – CSS (Chirp Spread Spectrum), что позволяет уверенно принимать сигнал от абонентских устройств на уровнях ниже уровня шума;
- длительную работу абонентских устройств без подзаряда батарей (до десяти лет от одного аккумулятора типа «АА»);
- существование трех классов абонентских терминалов с разными скоростями отклика на сообщения от сети и уровнями энергопотребления;
- автоматический роуминг между сетями разных операторов;
- возможность дистанционного обновления программного обеспечения абонентских терминалов

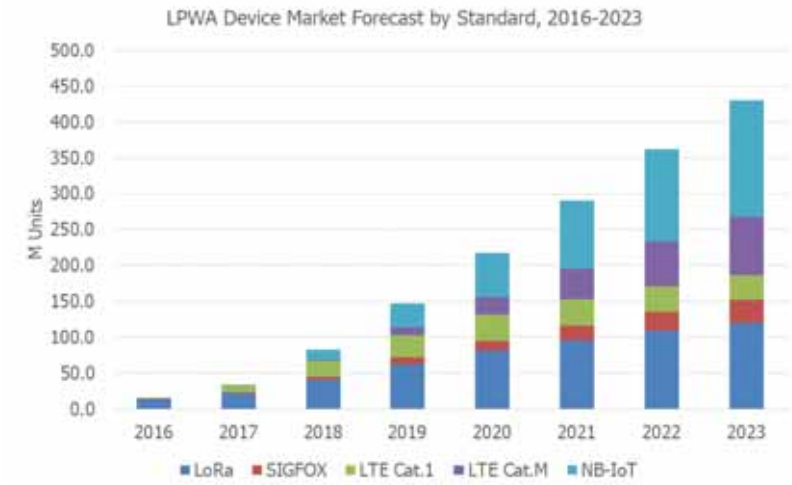

Рис. 1. *Статистика и прогноз поставок абонентских устройств IoT 2016–2023 гг. (в млн штук, по данным LoRa Alliance)*

через радиоэфир (технология FUOTA – Firmware Upgrade Over The Air);
- опцию беспроводного репитера с батарейным питанием для покрытия подвалов и экранированных помещений;
- режим вещания Multicast (одновременный прием одного сообщения несколькими датчиками);
- мультилатерационную геолокацию, позволяющую определять координаты абонентского терминала с точностью до 200 м без использования GPS-приемника.

Сегодня нередко можно столкнуться с утверждениями, что беспроводные системы связи в общедоступных диапазонах частот якобы не способны обеспечивать уверенную связь из-за неконтролируемых помех. На самом деле в нелицензируемых диапазонах для средств радиоэлектронной связи (РЭС) действуют даже более строгие правила, чем в лицензируемых. В частности, в полосе 868 МГц согласно [3] ограничены: во-первых, излучаемая мощность (на большинстве каналов – не более 25 мВт), во-вторых, время нахождения в эфире (как правило, не более 1%). Причем наказания за нарушения указанных величин точно такие же, как и за несанкционированное вещание на лицензируемых частотах. Так что любые радиосистемы гражданского назначения вне зависимости от способа выделения спектра – по стандартным процедурам (лицензионный) или по упрощенным (нелицензионный) – могут пострадать от преднамеренных радиопомех. Однако это в равной мере незаконно, и способы борьбы с такими помехами известны и одинаково доступны всем пользователям радиоспектра.

Ключевое преимущество работы в нелицензируемом диапазоне частот, особенно в отечественных реалиях, – это дешевизна и быстрота развертывания сети.

Целевая область применения технологии LoRa/LoRaWAN в системах IoT:
- автономные устройства без внешнего электропитания;
- устройства, генерирующие малые потоки данных;
- устройства, сравнительно редко выходящие в эфир;
- территории, покрытие на которых необходимо развернуть быстро и с минимальными затратами.

Таким образом, несмотря на возможный быстрый рост технологии NB-IoT, конкурирующей с LoRaWAN, последняя, по мнению большинства аналитиков отрасли, в перспективе сохранит значимую долю мирового рынка, что подтверждает прогноз поставок абонентских устройств IoT [4] (рис. 1).

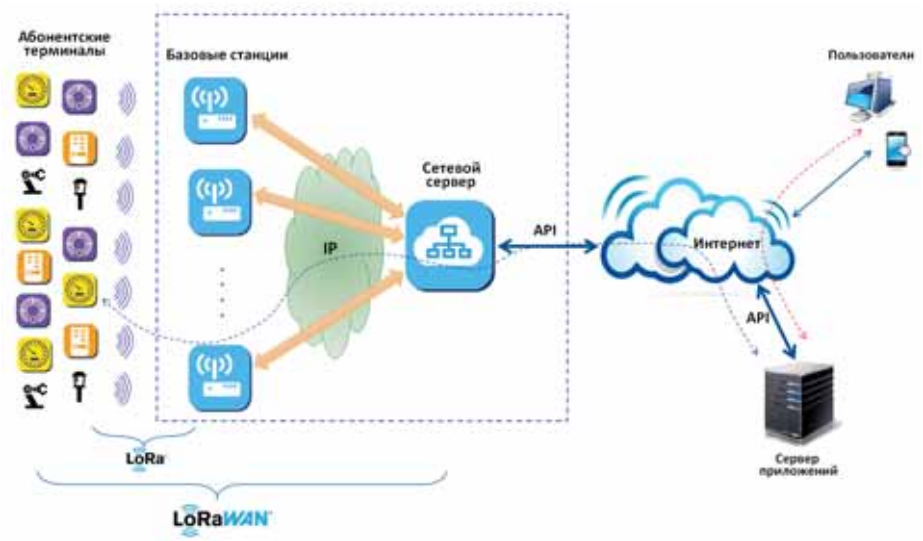

Рис. 2. *Архитектура сети LoRaWAN*

Описание архитектуры сети LoRaWAN

Сеть LoRaWAN состоит из следующих элементов: абонентские терминалы, базовые станции (шлюзы), сетевой сервер и сервер приложений (рис. 2).

Абонентский терминал представляет собой обобщающее наименование для сенсоров, датчиков, счетчиков, актуаторов и радиомодулей IoT, устанавливаемых на стороне пользователя. Стандарт LoRaWAN [2] определяет следующие классы терминалов (см. таблицу).

Таблица. Классы терминалов LoRaWAN

Класс устройства	Формат работы
A	Сеанс связи инициирует терминал. Его основная задача – передавать данные от устройства к сети; прием данных возможен только сразу после передачи – терминал открывает два окна приема. Терминалы класса A применяются в приложениях, где передача данных от сети возможна только как ответная реакция на получение данных от конечного устройства и требуется максимальное время работы от автономного источника питания.
B	В дополнение к ресурсам класса A здесь появляется возможность по расписанию принимать данные от сети, т. е. сеанс связи может быть инициирован как устройством, так и сетью. Терминалы класса B используются в случаях, когда прием данных от сети требуется, но не моментально, а по назначенному заранее расписанию (например, раз в 32 сек). Тем самым соблюдается баланс между скоростью реакции устройства на внешнюю команду и его энергопотреблением.
C	Устройства класса C постоянно готовы принимать данные от сети – прием данных прекращается только во время передачи данных самим устройством. Таким образом, сеанс связи, как и для устройства класса B, может быть инициирован и устройством, и сетью. Терминалы класса C применяются в приложениях, где быстрота реакции на команду, полученную от сети, важнее экономии электропитания, а также в тех кейсах, где устройству необходимо получать через IoT-сеть большие объемы данных.

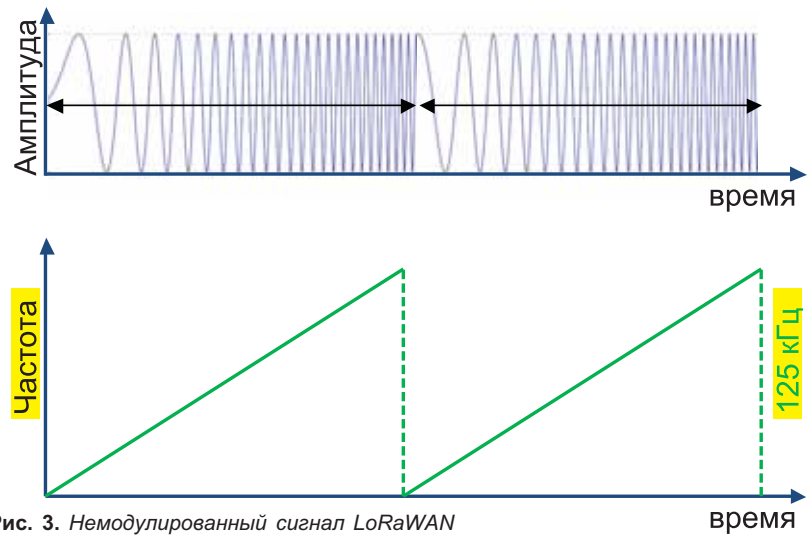

Рис. 3. *Немодулированный сигнал LoRaWAN*

Базовая станция – типовое понятие для многих радиосистем, в том числе и для радиосетей IoT. Применительно к сети LoRaWAN (как и во многих других радиосетях) базовая станция (БС) выполняет функции сопряжения и взаимодействия радиосети с абонентским терминалом и концентрации нагрузки с группы терминалов, поэтому в документации LoRa Alliance она именуется шлюзом и/или концентратором. Тем не менее обычно в текстах используется более широкое и общепринятое понятие «базовая станция».

Сигнал от одного терминала может приниматься несколькими БС. Совокупность базовых станций оператора связи обеспечивает территорию радиопокрытия сети и прозрачную двунаправленную передачу данных между конечными устройствами и сетевым сервером. Базовая станция оснащена приемно-передающей антенной (секторной или всенаправленной – омни), а также (опционально) GPS/ГЛОНАСС-антенной для прецизионной синхронизации внутренних часов и определения точных координат приемно-передающей антенны.

Сетевой сервер представляет собой программно-аппаратный комплекс (ПАК), управляющий радиосетью, контролирующий радиосеть и выполняющий маршрутизацию пакетов данных от абонентских терминалов до соответствующих серверов приложений.

- **Управление радиосетью**. Сетевой сервер сети LoRaWAN выбирает БС для передачи сообщений в направлении «вниз» (downlink), принимает решения о необходимости изменения скорости передачи данных для каждого терминала, мощности передатчика, контролирует заряд батарей конечных устройств, шифрует данные и т. п.
- **Контроль радиосети** включает в себя функции мониторинга, сбора статистики и аварийного информирования.
- **Маршрутизация**. Каждый пакет данных, отправляемый абонентским терминалом, имеет в своем составе уникальный идентификатор DevAddr, а на сетевом сервере хранится запись о соответствии DevAddr и URL сервера приложений, которому предназначена информация от терминала (датчика). На основании этого соответствия сетевой сервер выполняет маршрутизацию пакета до сервера приложений, где и происходит его дальнейшая обработка приложением сервис-провайдера.

Сервер приложений – это платформа, которая выполняет первый уровень шифрации/дешифрации и обработку данных, получаемых от терминалов и направляемых к ним. Помимо работы с данными сервер приложения может управлять терминалами с уровня приложения, например, переводить их в режим работы другого класса, управлять опцией адаптивной передачи данных, Multicast и т. п.

Особенности радиопротокола LoRaWAN

Модуляция LoRa базируется на импульсах линейно-частотной модуляции (ЛЧМ) (Chirp Spread Spectrum – CSS) (рис. 3). В отличие от систем Sigfox, XNB и NB-Fi, использующих для связи узкую полосу в 100 Гц и фазовую модуляцию, данные в сетях LoRaWAN передаются датчиками в полосе шириной 125 кГц, т. е. более чем в 1000 раз шире.

Каждое устройство стандарта LoRaWAN излучает сигнал с изменяющейся частотой (см. рис. 3). Модуляция LoRaWAN заключается в обрыве цикла на одной из промежуточных частот (рис. 4) и новом его начале, именно это и кодирует передаваемый символ. Всего существует 128 возможных различных частот обрыва цикла в каждом частотном канале (шириной, напомним, 125 кГц), а значит, один ЛЧМ-импульс кодирует 7 бит данных.

Поскольку частота сигнала LoRaWAN меняется в диапазоне 125 кГц, узкополосная помеха практически не оказывает влияния на успешность декодирования сигнала LoRaWAN. Еще одно преимущество, вытекающее из особенности модуляции LoRaWAN, – устойчивая работа на движущихся объектах (поездах, автомобилях и т. п.), поскольку доплеровский сдвиг частоты заметно не влияет на успешность передачи сигнала.

И последнее. Модуляция и канальное кодирование LoRaWAN позволяют осуществлять прием полезной информации даже при отрицательных значениях отношения сигнал/шум (SNR до –20 дБ). Кодирование (не путать с шифрованием) – это добавление к передаваемым пользовательским данным избыточной (контрольной) информации для повышения

вероятности успешного приема. Степень избыточности определяется соотношением CodeRate (CR) вида 4/5, означающим, что на каждые 5 бит передаваемой информации 4 бита – полезные данные и один – контрольный бит. От значения CodeRate зависит скорость передачи полезной информации. В LoRaWAN используются CodeRate от 4/5 до 4/8.

В целях экономии заряда батарей абонентских устройств и емкости сети датчики системы LoRaWAN выходят в эфир на одном из восьми частотных каналов [1] без предварительной синхронизации с сетью, в отличие от, скажем, GSM, где каждому абоненту сеть выделяет на время разговора персональный таймслот на определенном частотном канале. Это создает вероятность внутрисетевых коллизий: вдруг две двери откроются одновременно, и соответствующие сенсоры выйдут в эфир в один и тот же момент на одном частотном канале? Примет ли сеть сигнал от них, или они заглушат друг друга, или один заглушит другой?

Стандартом LoRaWAN [2] определены так называемые Spreading Factor (SF) – коэффициенты расширения спектра. Спецификацией [1] их предусмотрено всего шесть – от SF7 до SF12. SF – это «скорость» изменения частоты в ЛЧМ-импульсе: чем выше SF, тем медленнее меняется частота (рис. 5). Изменение SF на единицу означает увеличение длительности импульса в два раза. Для SF7 и полосы 125 кГц длительность импульса минимальна и составляет 1,024 миллисекунды.

Чем больше значение SF, тем медленнее передаются данные, но тем выше способность системы распознать их без ошибок: время передачи одного сообщения в сетях LoRaWAN составляет от 0,2 до 2,5 сек. SF каждому абонентскому устройству назначает сетевой сервер (NS – Network Server) по алгоритму ADR (Adaptive Data Rate – адаптивная скорость передачи данных) на основании измерений отношения сигнал-шум (Signal-to-Noise

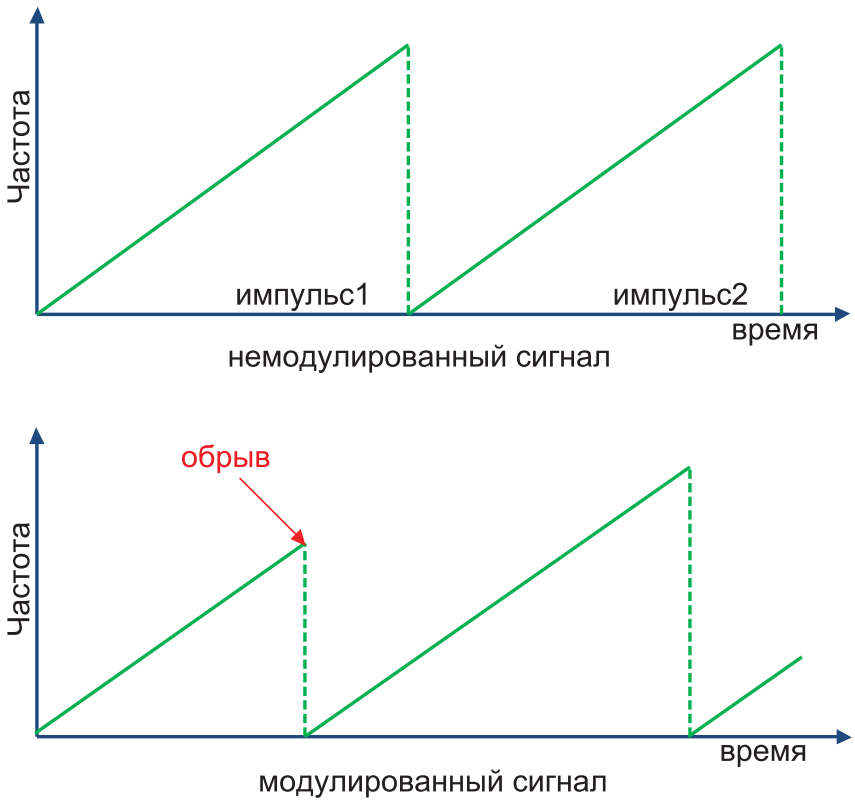

Рис. 4. *Модулированный сигнал LoRaWAN в сравнении с немодулированным*

Ratio – SNR), выполненных базовой станцией. Если абонентские терминалы находятся в разных радиоусловиях относительно базовой станции (например, один – рядом с БС, другой – далеко, или одно устройство – у окна квартиры, второе – за капитальной стеной), то передавать данные они будут с разными SF и интерферировать друг с другом не будут, даже в случае наложения сигналов друг на друга по времени на одном частотном канале. Ведь в силу разных скоростей изменения частоты у передатчиков с разными SF такие устройства будут представлять друг для друга лишь узкополосную помеху, что, как уже было сказано, легко компенсируется канальным кодированием.

А что будет, если базовая станция примет одновременные сообщения от двух устройств с одинаковым SF? Возникнет коллизия: либо одно, либо оба сообщения будут потеряны в результате интерференции. Однако это произойдет только на одной базовой станции, в то время как сигнал от каждого абонентского устройства LoRaWAN в профессионально спланированной и грамотно построенной сети принимают минимум три БС – именно такое количество базовых

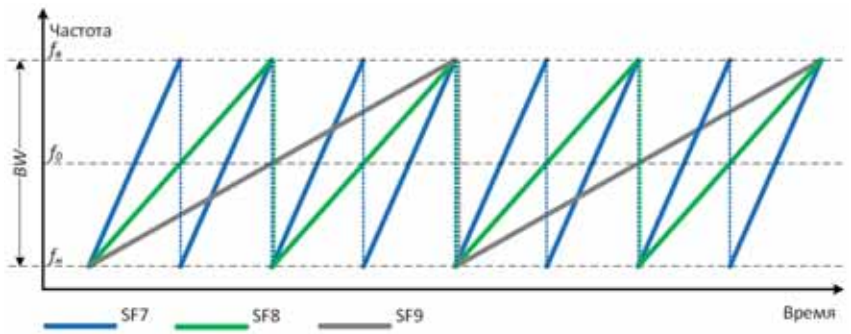

Рис. 5. *Модулированный сигнал LoRaWAN в сравнении с немодулированным*

станций необходимо для корректной работы опции геолокации методом TDoA. И если на одной БС возникнет коллизия, то прием сообщений успешно пройдет через другие базовые станции. В сетевом сервере LoRaWAN даже существует специальный таймер (длительностью 250 мс), чтобы дождаться, пока сообщение от определенного абонентского устройства будет получено всеми возможными БС с целью выбрать среди них наилучшую (с точки зрения SNR) на тот случай, если потребуется отправка сообщения от сети к датчику (подтверждение приема или MAC-команда).

В исследовании [5], проведенном компаниями MachineQ и Semtech, установлено, что восемь восьмиканальных БС LoRaWAN за сутки в состоянии принять один миллион сообщений от абонентских устройств. А если надо больше? Ответ простой – нужно увеличивать количество базовых станций. Ведь в отличие от сотовых систем связи базовые станции LoRaWAN не ведут постоянного вещания пилотных (как в LTE) или широковещательных (как в GSM) сигналов, так что установка новых БС не приводит к повышению внутрисетевой интерференции. Основную часть времени БС LoRaWAN работают на прием, а режим передачи включается лишь в редких случаях отправки команды управления или подтверждения приема на абонентское устройство. Также для покрытия помещений можно использовать репитер LoRaWAN (его спецификация на данный момент находится на финальном утверждении в техническом комитете LoRa Alliance). Репитер позволит улучшить (т. е. уменьшить номер) SF для сообщений, отправляемых indoor-датчиками, что снизит вероятность коллизий, поскольку, как уже было отмечено, сообщения с низким SF передаются многократно быстрее, чем сообщения с высоким SF.

Обеспечение безопасности передаваемых данных

В сети IoT LoRaWAN используется многоуровневая система безопасности передачи данных (рис. 6).

Первый уровень. AES-шифрование на уровне приложения (End-to-End, т. е. между абонентским терминалом и клиентским сервером приложений) с помощью 128-битного переменного сессионного ключа Application session key (AppSKey). Такой ключ шифрования хранится в абонентском терминале и на сервере приложений – он недоступен оператору сети (доступ к AppSKey есть только у клиента – владельца сервера приложений). Формирование сессионного ключа AppSKey происходит параллельно в абонентском терминале и на стороне сети в процессе активации терминала – через эфир AppSKey не передается.

Второй уровень. AES-шифрование и проверка целостности сообщений на сетевом уровне (между абонентским терминалом и сетевым сервером) с помощью 128-битного переменного сессионного ключа Network session key (NwkSKey). Такой уровень шифрования используется для защиты передаваемых сигнальных команд на MAC-уровне, а также для вычисления MIC (Message Integrity Code) в целях проверки целостности данных, передаваемых на радиоинтерфейсе. NwkSKey хранится в абонентском терминале и на сетевом сервере и недоступен клиенту (доступ к NwkSKey имеется только у оператора сети связи – владельца сетевого сервера). Формирование сессионного ключа NwkSKey также происходит параллельно в абонентском терминале и на стороне сети в процессе активации терминала – через эфир NwkSKey не передается.

Третий уровень. Стандартные методы аутентификации и шифрования интернет-протокола (IPsec, TLS и т. п.) при передаче данных по транспортной сети между узлами сети – базовая станция, сетевой сервер, Join-сервер, сервер приложений.

По команде приложения или сетевого сервера в любой момент возможен переход на новую

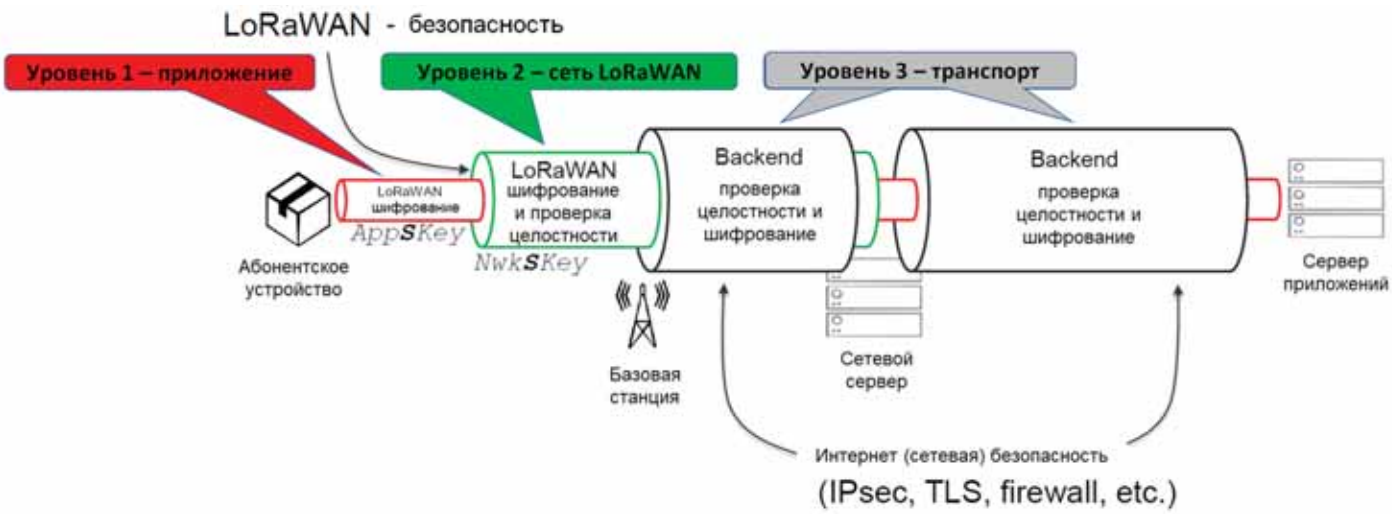

Рис. 6. *Общая схема безопасности данных в сети LoRaWAN*

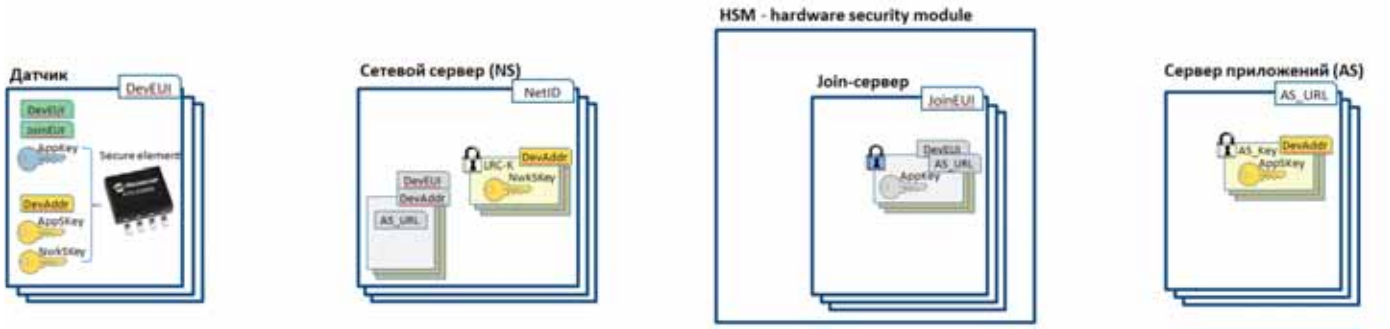

Рис. 7. *Схема хранения ключей шифрования*

сессию с генерацией нового комплекта ключей шифрования, что делает бесполезными старые ключи. Также есть возможность установки периодической генерации нового комплекта ключей NwkSKey и AppSKey.

В версии стандарта LoRaWAN V1.0.x [2] формирование сессионных ключей на стороне сети производится на сетевом сервере (NS), однако в версии V1.1 [6] для этих целей определяется выделенный сервер (так называемый Join-сервер) (рис. 7). Join-сервер может быть дополнительно защищен отдельным аппаратным модулем безопасности HSM (Hardware Security Module).

В этом случае для безопасной передачи сгенерированных сессионных ключей между серверами, а также хранения их на сетевом сервере и сервере приложений внедряются дополнительные ключи: AS_Key – для ключа AppSKey и LRC_K – для ключа NwkSKey.

На абонентском устройстве ключи шифрования опционально могут защищаться специальным аппаратным элементом безопасности Secure element (например, микроконтроллером Microchip ATECC608A), что исключит их компрометацию в случае физического воздействия на терминал.

Внедрение аппаратных средств защиты в сети и на терминале делает бесполезными попытки перехвата сессионных ключей при передаче их между серверами и попытки взлома серверов или абонентских устройств в целях извлечения сессионных ключей.

Рассмотренные мероприятия создают условия и для защищенного роуминга данных – безопасной авторизации датчиков в гостевой сети и защищенной передачи данных «домашнему» серверу приложений из «гостевой» сети.

В целях дополнительной защиты процесса генерации сессионных ключей Join-сервер может быть физически вынесен на территорию клиента или производителя устройств (рис. 8). В этом случае даже сотрудники оператора не смогут получить доступ к сессионным и корневым ключам шифрования абонентского терминала.

Несмотря на то что в России не требуется обязательная сертификация средств кодирования (шифрования) при передаче сообщений, не составляющих государственную тайну, по требованию заказчика используемые в стандарте LoRaWAN уровни шифрования AES-128 могут быть дополнены одним из стандартизованных в РФ алгоритмов, входящих в семейство ГОСТ Р 34.10-2012 [7], ГОСТ Р 34.11-2012 [8], или по алгоритму «Кузнечик» – согласно ГОСТ Р 34.12-2015 [9] и ГОСТ Р 34.13-2015 [10].

Для этого при производстве абонентских терминалов LoRaWAN предлагается устанавливать в них дополнительный микроконтроллер СКЗИ (средства криптографической защиты информации), сертифицированный ФСБ России и соответствующий требованиям, предъявляемым к шифровальным средствам класса КС3 (дистанционное банковское обслуживание, электронный документооборот в государственном секторе и т. д.). В качестве такого микроконтроллера могут быть использованы, например, микропроцессоры MIK51SC72D или MIK51AD144D отечественного производства компании «Микрон», сертифицированные ФСТЭК и ФСБ России, имеющие небольшие размеры (около 14 мм²) и малое энергопотребление.

Схема безопасности данных в сети LoRaWAN с дополнительным уровнем СКЗИ представлена на рис. 9.

Ключ шифрования уровня СКЗИ, например SubSKey (согласно ГОСТ Р 34.12-2015 [9]), прошивается в абонентский терминал LoRaWAN при производстве, как и корневой ключ уровней

Рис. 8. *Возможные сценарии размещения Join-сервера*

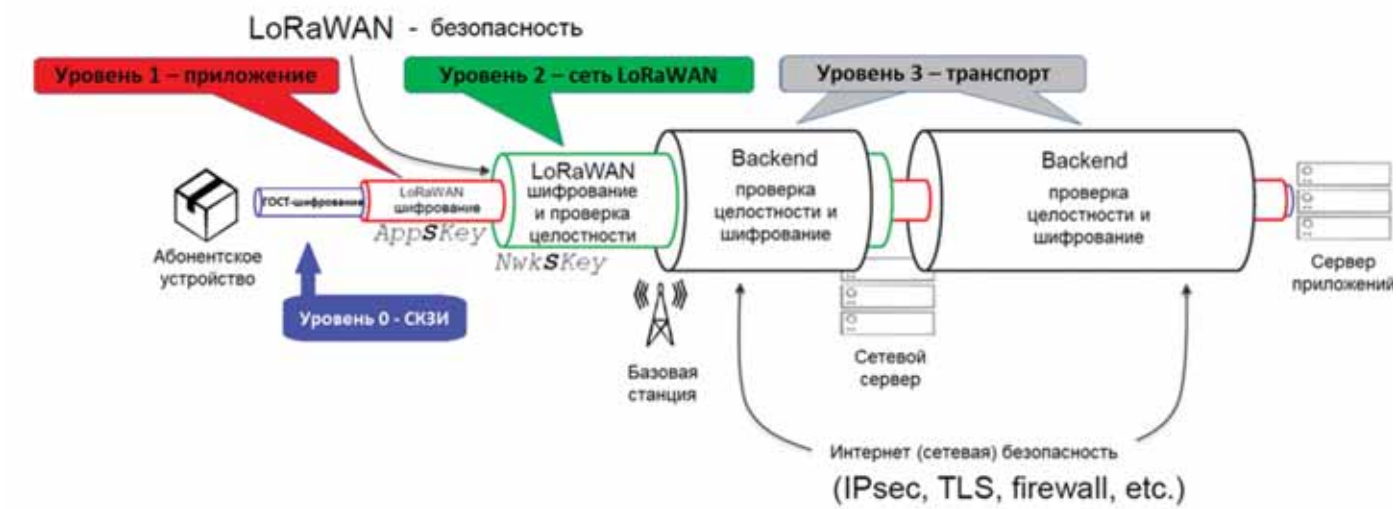

Рис. 9. *Схема внедрения отечественной СКЗИ в структуру шифрования данных сетей LoRaWAN*

шифрования 1–2 LoRaWAN, либо внедряется в терминал LoRaWAN вместе с микроконтроллером СКЗИ при введении терминала в эксплуатацию (с помощью специального слота). Дешифрация данных уровня СКЗИ выполняется на территории заказчика сервером приложений после дешифрации уровня приложения сессионным ключом AppSKey. Ключ шифрования SubSKey передается клиенту вместе с датчиком непосредственно самим производителем абонентского терминала и недоступен сотрудникам оператора сети LoRaWAN.

В завершение нашего обзора обобщим критерии безопасной передачи данных в сетях IoT и способы, которыми они реализуются в сети стандарта LoRaWAN.

End-to-End конфиденциальность пользовательских данных на уровне приложения – AES-шифрование с помощью сессионного ключа AppSKey.

Взаимная идентификация устройства и сети – процесс авторизации терминала при первичном подключении к сети (или по специальной команде о повторе авторизации).

Проверка целостности данных при передаче на радиоинтерфейсе – вычисление MIC-кода на основе сессионного ключа NwkSKey.

Конфиденциальность сигнальной информации (управляющих команд) – AES-шифрование MAC-команд с помощью сессионного ключа NwkSKey.

Безопасное хранение идентификаторов абонентского устройства и его полномочий – внедрение аппаратного элемента безопасности Secure element в абонентский терминал и защита HSM-модулем Join-сервера.

Оперативное устранение найденных уязвимостей на сетевой стороне и на абонентских терминалах – дистанционная смена ПО абонентских терминалов через эфир с помощью специфицированного LoRa Alliance механизма FUOTA (Firmware Upgrade Over The Air) [11] и установка обновлений на сетевой сервер и сервер приложений.

Возможность использования отечественных СКЗИ для критической инфраструктуры (КИ) – внедрение дополнительного, «нулевого» уровня End-to-End шифрования по сертифицированным ФСБ РФ алгоритмам. ■

Литература

1. *LoRaWAN 1.0.3 Regional Parameters, 2018.*
2. *LoRaWAN Specification, Version V1.0.3, 2018.*
3. *Решение ГКРЧ № 18-46-03-1 от 11.09.2018. О выделении полос радиочастот, внесении изменений в решения ГКРЧ и продлении срока действия решений ГКРЧ.*
4. *LoRaWAN Members Meeting. Tokyo, 2018.*
5. *Ross Gilson, Michael Grudsky. LoRaWAN capacity trial in dense urban environment, 2018.*
6. *LoRaWAN 1.1 Specification, 2018.*
7. *ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи, 2012.*
8. *ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. 2012.*
9. *ГОСТ Р34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. 2015.*
10. *ГОСТ Р 34.13–2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. 2015.*
11. *LoRa Alliance, FUOTA Process Summary Technical Re 1 commendation TR002 v1.0.0, 2019.*
12. *Извещение по вопросу использования несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети Интернет. ФСБ РФ. 2016.*