# Технология передачи данных LoRaWAN для IIoT-решений:

## мифы и реальность

**В последние годы сети индустриального «Интернета вещей» (IIoT) типа LPWAN (Low Power Wide Area Network) активно строятся по всему миру, однако, как и любое новое решение, их окружает множество домыслов, смущающих не только потенциальных клиентов, но и специалистов по телекоммуникациям.**

**Андрей Экономов, к. ф. -м. н.**
andrei.n.ekonomov@domru.ru

Попробуем разобраться с основными мифами на примере сети IIoT LPWAN LoRaWAN, построенной в 52 российских городах АО «ЭР-Телеком Холдинг», поскольку именно технология LoRaWAN сейчас является драйвером развития направления IoT во всем мире [1] и используется в качестве основного инструмента для управления критически важной инфраструктурой, транспортом, производством, здравоохранением, муниципальным и сельским хозяйством более чем в ста странах мира. Кроме того, технология LoRa рекомендована к применению в РФ концепцией, утвержденной приказом Минкомсвязи России от 29.03.2019 № 113 [2], а к концу 2019 года ожидается принятие LoRaWAN как национального стандарта технологии «Интернета вещей».

### Миф № 1: зависимость от импорта

Раз стандарт иностранный, якобы появляется технологическая зависимость от использования импортного оборудования и программного обеспечения (ПО). На самом деле, несмотря на молодость технологии, в РФ компаниями «Вега-Абсолют», «Гудвин», «Новоучет» и другими уже освоен выпуск и широкого спектра абонентских устройств, и базовых станций (БС) LoRaWAN. Причем в данном случае нужно говорить не о переупаковке китайских изделий, а о полноценной отечественной разработке и программной, и аппаратной составляющих. А компания «Лартех» создала ПО для сетевого сервера, управляющего сетью LoRaWAN, что также позволяет избавиться от мифа о возможной «неконтролируемой» утечке данных с абонентских устройств на серверы, находящиеся за пределами России.

### Миф № 2: опасность нелицензируемого диапазона

Сети LPWAN, как правило, работают в нелицензируемом диапазоне 868 МГц и, наверное, могут быть легко заглушены злоумышленниками или испытывать влияние неконтролируемых помех? Однако «нелицензируемость» спектра отнюдь не синоним слова «вседозволенность» — для любого передатчика согласно решению ГКРЧ № 07-20-03-001 от 07.05.2007 действуют ограничения, во-первых, на излучаемую мощность (на большинстве каналов — не более 25 мВт), во-вторых, на время нахождения в эфире (как правило, не более 1%). Если же говорить о протоколе LoRa, то в нем используются специальные механизмы повышения устойчивости радиоприема. Применение радиосигналов с линейно-частотной модуляцией (ЛЧМ) позволяет надежно принимать информацию ниже уровня шума и практически исключает влияние узкополосной помехи на соотношение сигнал/шум. В протоколе также реализованы алгоритмы разрешения «коллизий» сообщений: пакеты, переданные с разными Spreading Factor (коэффициент расширения спектра), ввиду особенностей ЛЧМ-сигналов не интерферируют между собой, а сообщение от одного устройства в большинстве случаев принимается сразу несколькими БС (и если на одной БС произойдет интерференционная коллизия, то другие примут сообщение успешно). При правильном планировании сети указанные меры обеспечивают весьма высокую вероятность доставки сообщений даже при наличии одновременно работающих в одной полосе частот систем различных владельцев, что подтверждается мировым опытом эксплуатации сетей LoRaWAN разных операторов на одной территории.

### Миф № 3: слишком скрытый обмен данными

Говорят, что сети IIoT LPWAN можно использовать для скрытого обмена электронными сообщениями, не контролируемыми со стороны СОРМ (систем технических средств для обеспечения функций оперативно-розыскных мероприятий). Фактически же абонентские

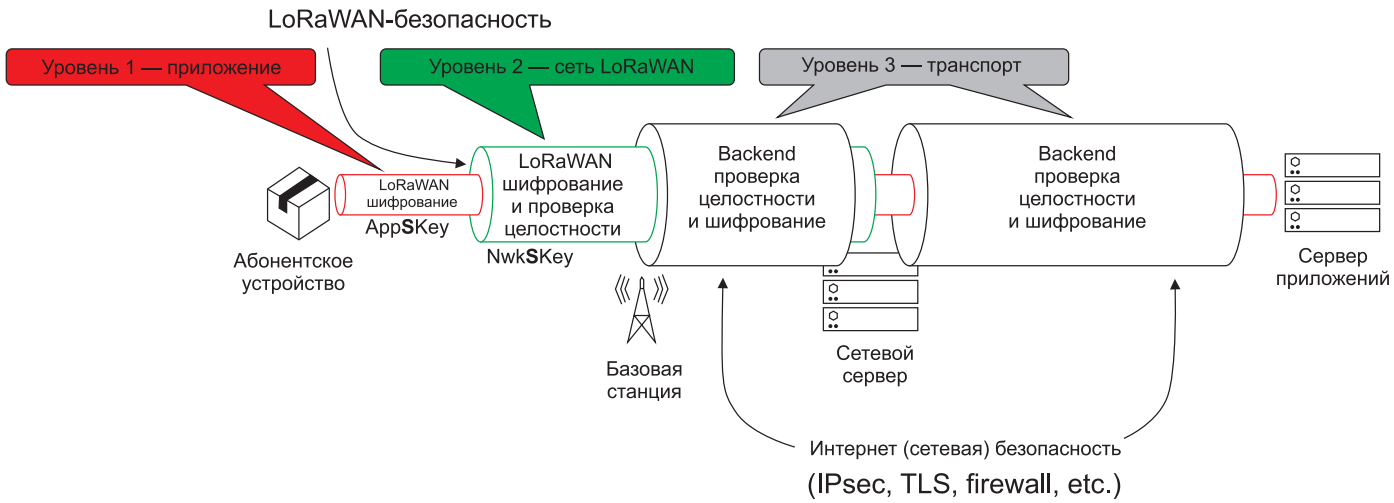


**Рис. 1.** Общая схема безопасности данных в сети LoRaWAN

устройства LoRaWAN передают сообщения только на клиентский сервер приложений, режим передачи сообщений между абонентскими устройствами в протоколе не применяется. Кроме того, сети LoRaWAN ориентированы на исходящий от абонентских устройств трафик (то есть сбор данных), режим двусторонней передачи нежелателен с точки зрения емкости сети.

## Миф № 4: недостаточная защищенность

Считается, будто из-за дешевизны абонентских устройств сетей IIoT LPWAN, а также низкой абонентской платы прочитать или подменить данные от датчика по силам даже талантливому школьнику. Это совершенно не так, в сетях LoRaWAN используются одни из самых совершенных на текущий момент алгоритмов авторизации устройств и защиты пользовательской информации. Рассмотрим этот вопрос подробней.

Защита данных в любой сети «Интернета вещей», независимо от конкретного стандарта или технологии, должна удовлетворять следующим критериям:

- end-to-end-конфиденциальность пользовательских данных на уровне приложения;
- взаимная идентификация абонентского устройства и сети;
- проверка целостности данных при передаче на радиоинтерфейсе;
- конфиденциальность сигнальной информации (управляющих команд);
- безопасное хранение идентификаторов абонентского устройства и его полномочий;
- оперативное устранение найденных уязвимостей в ПО компонентов сети и абонентских терминалов;
- возможность использования отечественных СКЗИ (средств криптографической защиты информации) для критической информационной инфраструктуры (КИИ).

Следует также отметить необходимость защиты от атак серверов (операторских, управляющих сетью, и клиентских, на которых запускаются приложения обработки пользовательских данных), однако этому вопросу посвящено уже множество статей и целых книг, а потому касаться его мы не будем.

Для обеспечения защиты передаваемой информации и проверки целостности данных при передаче их на радиоинтерфейсе в сети IoT LoRaWAN предусмотрена многоуровневая система безопасности (рис. 1):

- 1-й уровень. AES-шифрование на уровне приложения (end-to-end, то есть между абонентским терминалом и сервером приложений) с помощью 128-битного переменного сессионного ключа Application session key (AppSKey). Данный ключ шифрования хранится в абонентском терминале и на сервере приложений и 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 во время процедуры активации терминала — через эфир AppSKey не передается.
- 2-й 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). Данный уровень шифрования предназначен для защиты передаваемых сигнальных команд на MAC-уровне, а так-

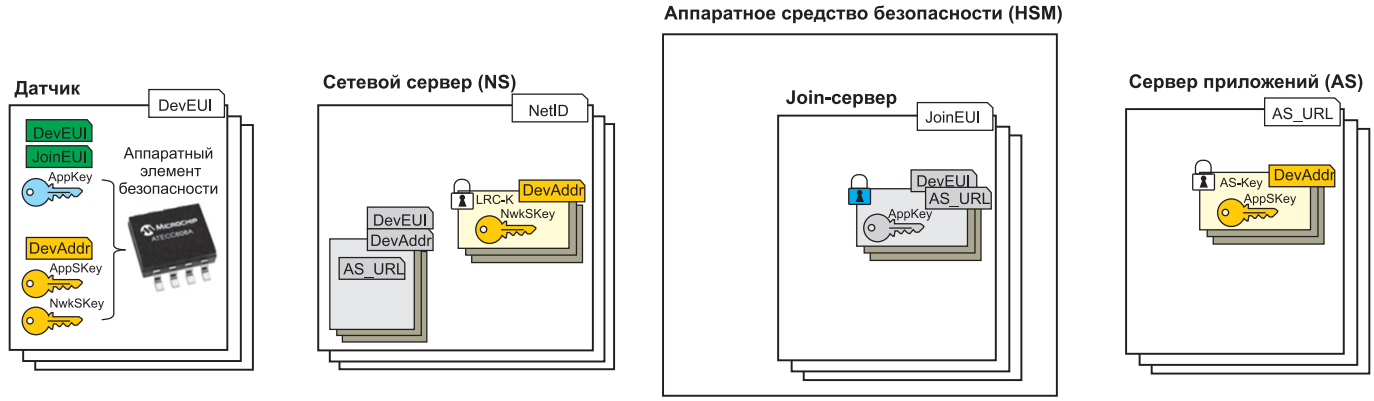


**Рис. 2.** Схема хранения ключей шифрования: DevEUI (Device Extended Unique Identifier) — уникальный идентификатор датчика; JoinEUI (JoinServer Extended Unique Identifier) — уникальный идентификатор Join-сервера; AppKey (Application Key) — корневой ключ шифрования; DevAddr (Device Address) — укороченный адрес терминала в сети; AppSKey (Application Session Key) — сессионный ключ приложения; NwkSKey (Network Session Key) — сетевой сессионный ключ; NetID (Network Identifier) — идентификатор сети; AS_url (Application Server URL) — адрес сервера приложения в сети Интернет; LRC-K (Long-Range Controller Key) — ключ шифрования сетевого сервера (контроллера дальнего действия)

же для вычисления MIC (Message Integrity Code) с целью проверки целостности данных, передаваемых по радиоинтерфейсу. NwkSKey хранится в абонентском терминале и на сетевом сервере и недоступен клиенту (доступ к NwkSKey есть только у оператора сети — владельца сетевого сервера). Формирование сессионного ключа NwkSKey также происходит параллельно в абонентском терминале и на стороне сети во время процедуры активации терминала — через эфир NwkSKey не передается.

- 3-й 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 (см. далее), сервер приложений).

По команде приложения или сетевого сервера в любой момент возможен переход на новую сессию с генерацией нового комплекта ключей шифрования, что делает бесполезными старые ключи шифрования. Также есть возможность установки периодической генерации нового комплекта ключей NwkSKey и AppSKey.

В версии стандарта LoRaWAN V1.1 [3] формирование сессионных ключей на стороне сети производится на специальном, выделенном сервере (так называемый Join-сервер) (рис. 2). Join-сервер может быть дополнительно защищен отдельным аппаратным модулем безопасности HSM (hardware security module).

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 с целью извлечения сессионных ключей, обеспечивая, таким образом, безопасное хранение идентификаторов абонентского устройства и его полномочий.

В целях дополнительной защиты процесса генерации сессионных ключей Join-сервер может быть физически вынесен на территорию клиента или производителя устройств (рис. 3). В этом случае даже сотрудники оператора не смогут получить доступ к сессионным и корневым ключам шифрования абонентского терминала.

Несмотря на то, что в РФ не требуется обязательная сертификация средств кодирования (шифрования) при передаче сообщений, не составляющих государственную тайну [9], по требованию заказчика используемые в стандарте LoRaWAN уровни шифрования AES-128 могут быть дополнены одним из стандартизованных в РФ алгоритмов, входящих в семейство ГОСТ [4–7].

Для этого при производстве абонентских терминалов LoRaWAN предлагается устанавливать в них дополнительный микроконтроллер СКЗИ, 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 отечественного производства «Микрон» MIK51SC72D или MIK51AD144D, сертифицированные ФСТЭК и ФСБ России, имеющие небольшие размеры (около 14 кв. мм) и малое энергопотребление.

Оперативное устранение найденных уязвимостей на абонентских терминалах в сетях LoRaWAN осуществляется с помощью дистанционного обновления ПО через эфир с помощью специфицированного LoRaAlliance механизма FUOTA (Firmware Upgrade Over The Air) [8].

Резюмируя все вышеизложенное, можно сделать вывод, что защищенность от информационных угроз системы, построенной на протоколе LoRaWAN, находится на высших уровнях, характерных для сетей связи общего пользования. С применением отечественного оборудования и программного обеспечения, а также упомянутых в материале мер защиты информации, на базе этой технологии может быть построена система мониторинга и управления любыми, в том числе и самыми критичными объектами. ■

## Литература


1. LoRaWAN Members Meeting. Tokyo, 2018.
2. Министерство цифрового развития РФ. Приказ об утверждении Концепции построения и развития узкополосных беспроводных сетей связи «Интернета вещей» на территории Российской Федерации, 2019.
3. LoRaWAN 1.1 Specification, 2018.
4. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи», 2012.
5. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования», 2012.
6. ГОСТ Р34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры», 2015.
7. ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров», 2015.
8. LoRa Alliance, FUOTA Process Summary Technical Re 1 commendation TR002 v1.0.0, 2019.
9. Извещение по вопросу использования несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети Интернет. ФСБ РФ, 2016.
10. LoRaWAN Specification, Version V1.0.3, 2018.
11. LoRaWAN 1.0.3 Regional Parameters, 2018.
12. ГОСТ Р34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры», 2015.
13. LoRaWAN 1.1 Regional Parameters, 2018.


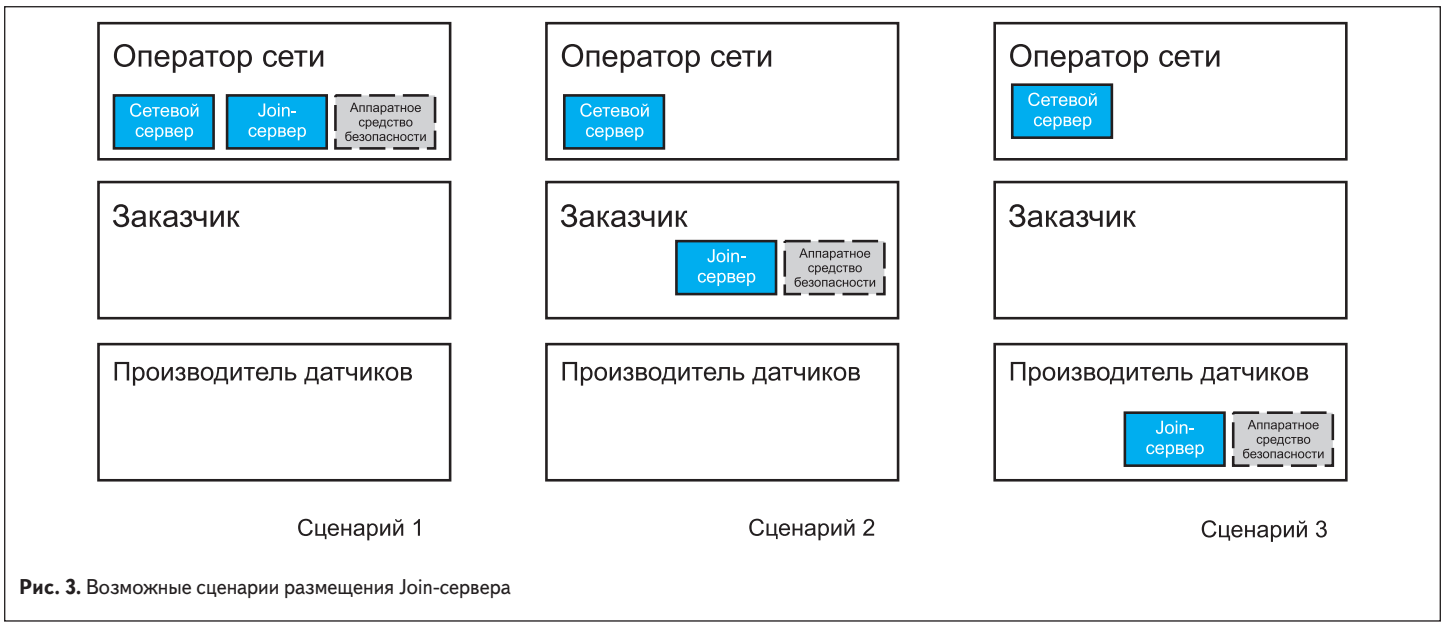


**Рис. 3.** Возможные сценарии размещения Join-сервера