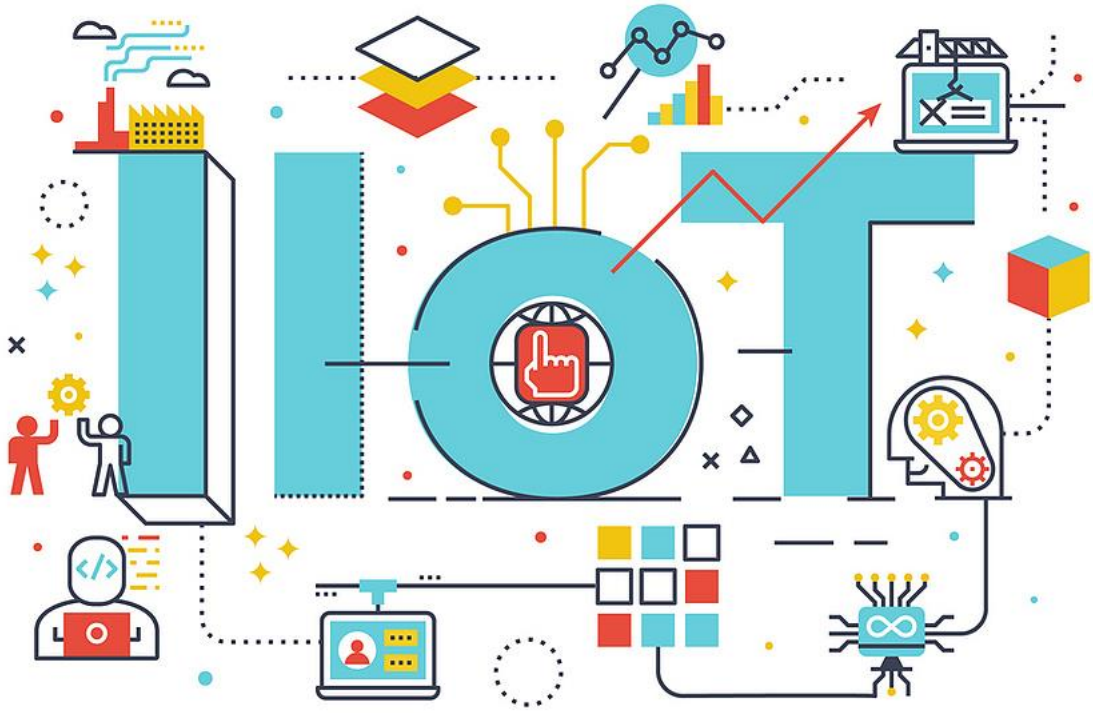
# Современное состояние IoT



## Термины и таксономия

Сейчас довольно часто встречается упоминание понятия «Интернет вещей», однако у разных людей смысл этого словосочетания может сильно различаться. Это также видно по прогнозам объема этого рынка – нередко оценки разных экспертов отличаются на порядки.

«Википедия» дает следующее определение: «“Интернет вещей” — концепция вычислительной сети физических предметов (“вещей”), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека». На мой взгляд, это хорошее определение, особенно в части того, что касается участия человека. Согласно этому определению получается, что, например, беспилотный железнодорожный локомотив – из мира «Интернета вещей», а смартфон – нет. Самым массовым сегментом обещают стать маломощные автономные подключенные устройства, способные работать от одной батарейки несколько лет. Такие устройства иногда называют LPWAN (Low Power Wide Area Network) – по способу подключения.

Также нередко встречается термин «киберфизические системы» – это во многом относится к «Интернету вещей», так как подключенные «умные» вещи стоят на границе двух миров – кибернетического и физического.

## «Интернет вещей» и Интернет людей – общности и различия

Человек взаимодействует в Интернете от своего имени, тем или иным способом подтверждая свою личность, когда это необходимо. Поэтому он несет ответственность за эти действия.

С устройствами сложнее: устройство совершает действия от своего имени, при этом указывая свою принадлежность владельцу. Вместе с этим ответственность может быть размыта между владельцем устройства, арендатором (как в случае каршеринга) и владельцем инфраструктуры (например, аэропорта). Вот почему важна надежная аутентификация устройств в инфраструктуре, так же как и взаимная аутентификация владельца и инфраструктуры на устройствах.

Gartner для устройств «Интернета вещей» ввел новый тип атаки – *denial-of-sleep* («отказ в спящем режиме»), когда устройству, работающему долго от батарейки, не дают уйти в режим глубокого сна, оно быстро теряет заряд и выключается.

## Чему доверять?

Устройство можно аутентифицировать по различным показателям: локации, серийному номеру, MAC-адресу и т. п., однако строгая криптографическая аутентификация по-прежнему хороша, остальные же параметры могут быть вторыми или косвенными факторами. То есть необходимо наделить каждое устройство неким уникальным секретом, который трудно подделать.

## Криптография

Казалось бы, криптография – зрелая область информационной безопасности и здесь все вопросы уже должны быть решены. Давайте посмотрим, как развивалась криптография. В XX веке перед ней стояла задача: применяя относительно короткий ключ шифрования, зашифровать как можно больший объем данных, при этом таким образом, чтобы у стороны, не имеющей ключа и располагающей разумными вычислительными ресурсами, на расшифровку ушло больше времени, чем время актуальности информации.

## Что изменилось с тех пор?

1) Устройства класса LPWAN, как правило, передают малые объемы данных, зачастую нерегулярно, без постоянного соединения. Вместе в тем они чувствительны к объему передаваемых данных: чаще всего такие устройства передают данные посредством радио, на что расходуется заряд батареи и используется радиочастотный ресурс. Поэтому необходимо свести к минимуму накладные расходы (overhead) от шифрования.

2) Часто для таких задач целостность (подлинность) данных и команд важнее конфиденциальности.

3) На горизонте 10–15 лет ожидается приход квантовых вычислений. Помимо революционного ускорения ряда вычислительных задач, такие вычисления

представляют угрозу для имеющихся криптографических алгоритмов, особенно асимметричных. При этом срок жизни устройств может вполне превышать 10 лет с трудностью или невозможностью замены. Представим, например, датчик вибрации, который замурован в конструктиве железобетонного моста при его строительстве.

На сегодняшний день идет активный поиск решений этих задач. Хорошими кандидатами выглядят симметричные алгоритмы шифрования с достаточно частой сменой ключей и квантовое и постквантовое распределение ключей для этого.

## Где хранить секреты?

Предположим, мы решили все задачи, связанные с криптографическими алгоритмами и распределением ключей, но где теперь их безопасно хранить, а также выполнять криптографические операции? Для этого необходим какой-то модуль безопасности (secure element), которому мы доверяем.

Очевидно, что в компактном конструктиве мы не можем применить полноценный HSM или даже TPM. В мобильных сетях в качестве secure element применяют SIM-карты, начинается применение eSIM (отдельный впаянный чип) и iSIM (интеграция в основной чип устройства). GSMA продвигает инициативу IoT SAFE (IoT SIM Applet for Secure End-2-End Communication) – использование xSIM не только для идентификации в сети мобильного оператора, но и как mini crypto-safe для хранения ключей и выполнения криптоопераций.

## Стандарты

Пожалуй, трудно найти что-то, что больше, чем стандарты, влияет на безопасность. Сегодня как раз то время, когда зарождаются стандарты «Интернета вещей». Помимо безопасности, стандарты – это и экосистема, и интероперабельность, и, как следствие, конкуренция, когда пользователь не замкнут в экосистеме одного производителя, а может легко перейти к соседу по цеху.

В России стоит отметить усилия в этом направлении:

· ТК-194 «Киберфизические системы», благодаря которому мы получили в этом году серию национальных стандартов;

· ТК-26 «Криптографическая защита информации», где ведется активная работа, направленная на то, чтобы новые протоколы «Интернета вещей» были безопасными.

Особенно отрадно, что наладилось конструктивное взаимодействие между различными техническими комитетами, что положительно влияет на качество и сроки появления новых стандартов. На мой взгляд, расслабляться пока рано, но наблюдается явно позитивная тенденция.

Ассоциация «Доверенная платформа» консолидирует активность российских разработчиков и иных организаций в направлении кибербезопасности (доверенности) «Интернета вещей». Если говорить о зарубежных практиках, то

в мире значительный вклад заметен со стороны ассоциаций GlobalPlatform и oneM2M.

Компания «Аладдин Р.Д.» уделяет особое внимание технологиям и разработкам в сфере «Интернета вещей». Так, компанией выпущено сертифицированное ФСТЭК России решение с применением технологии TrustZone, которое представляет собой средство доверенной загрузки для ARM-процессоров Trusted Security Module и соответствует требованиям по безопасности информации, установленным в документах «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013).

Доверенная платформа от «Аладдин Р.Д.» — единственное на сегодняшний день решение по доверенной загрузке ОС на ARM-процессорах. С каждым днем применений доверенной платформы и TSM становится больше.

Олег Гурин,

директор по развитию бизнеса «Доверенная платформа IoT» компании «Аладдин Р.Д.»

https://www.it-world.ru/it-news/reviews/167960.html