



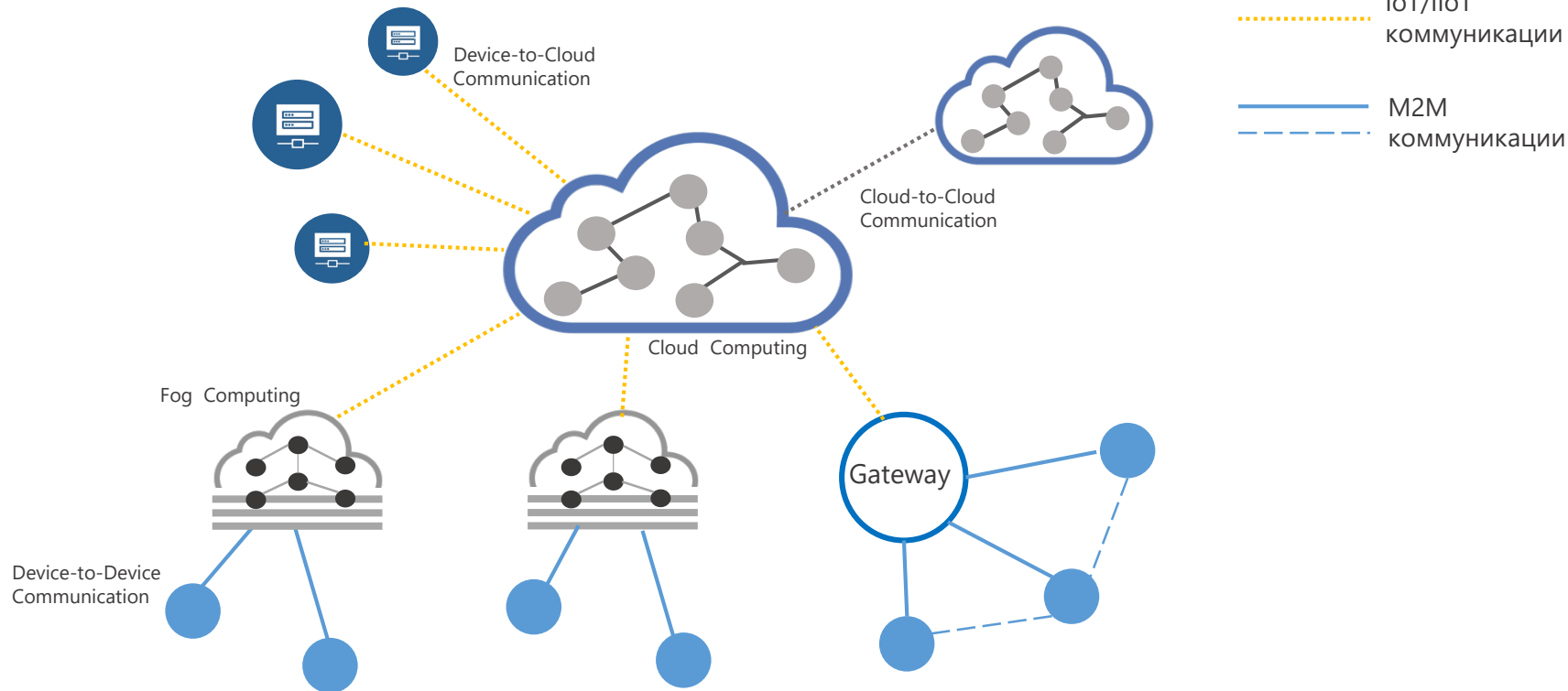
Стандартизованные в РФ протоколы для защиты M2M и IoT

Ольга Шемякина, системный аналитик

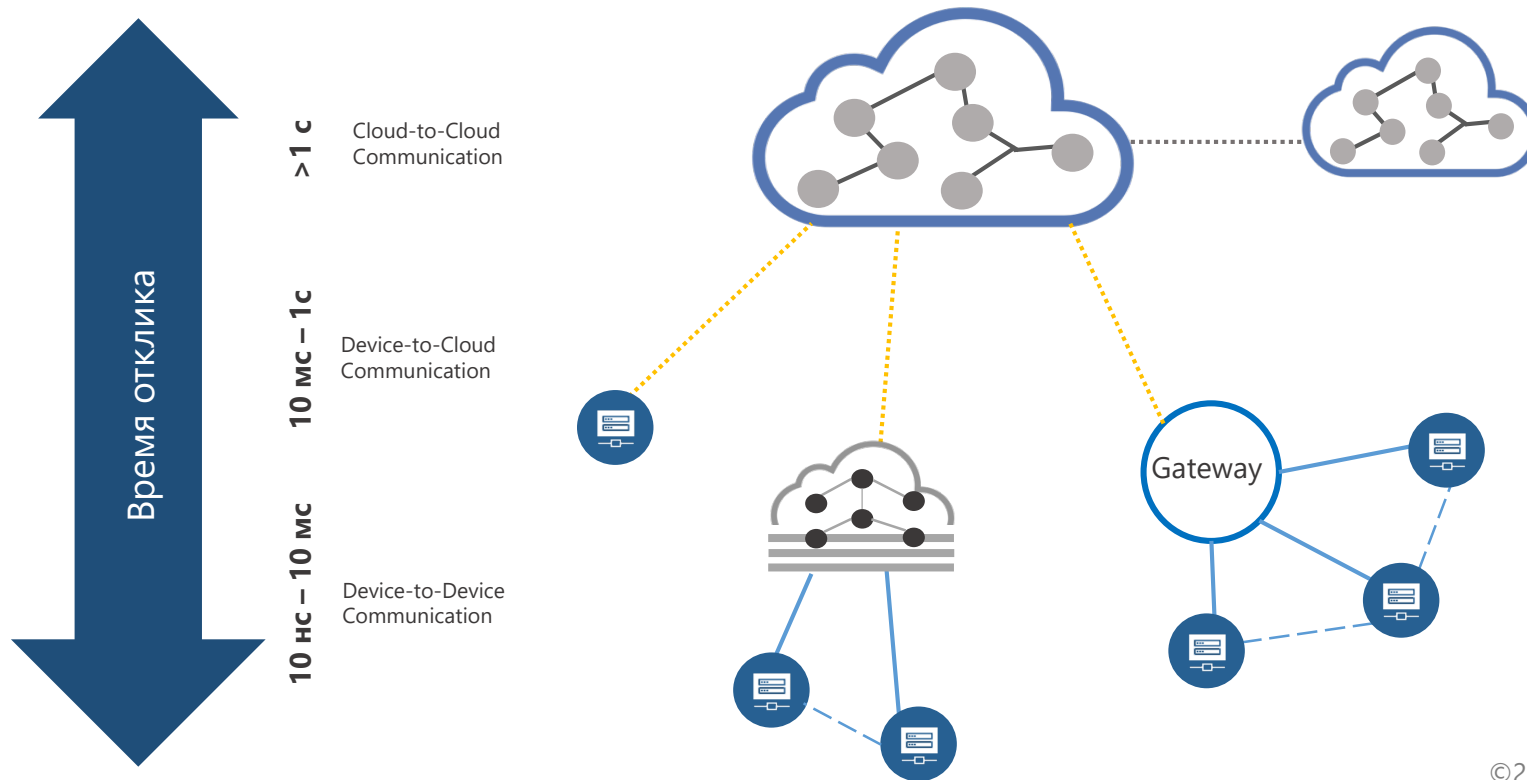


Особенности M2M и IoT/IIoT протоколов

M2M и IoT коммуникации



Латентность для IoT и M2M коммуникаций



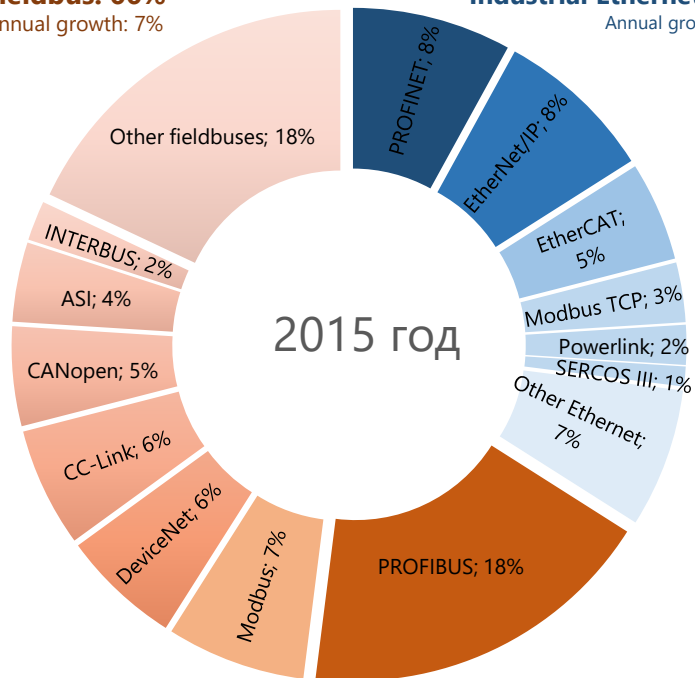
Промышленные M2M протоколы

Fieldbus: 66%

Annual growth: 7%

Industrial Ethernet: 34%

Annual growth: 17%

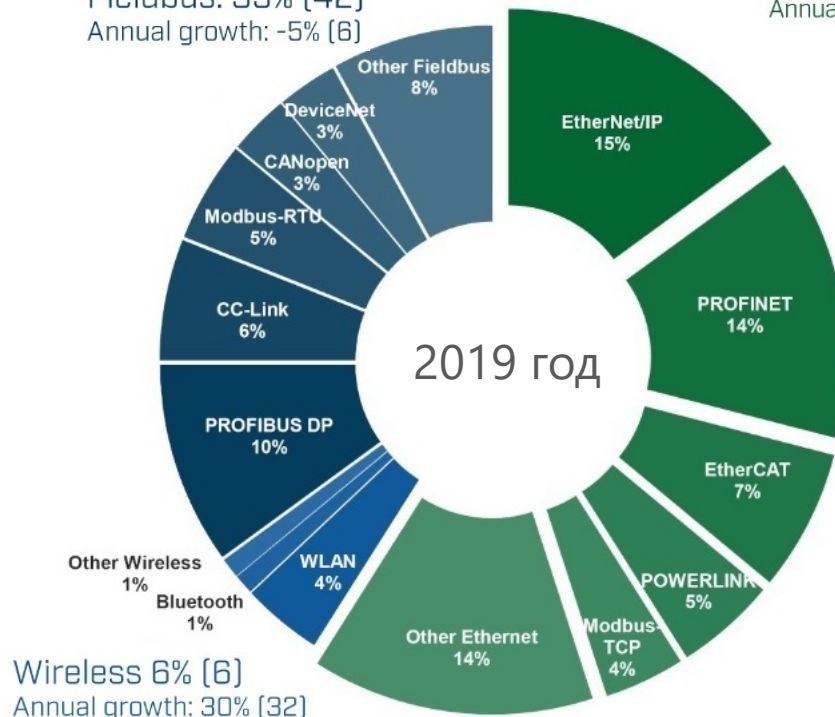


Fieldbus: 35% [42]

Annual growth: -5% [6]

Industrial Ethernet: 59% [52]

Annual growth: 20% [22]



Wireless 6% [6]

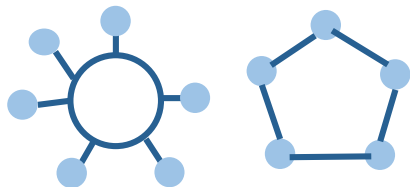
Annual growth: 30% [32]

Топология M2M протоколов

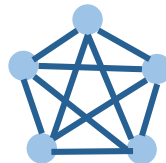
Общая шина



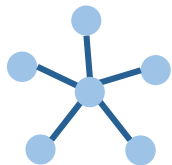
Кольцо



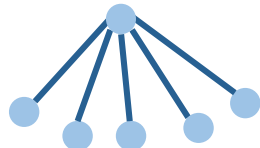
Полносвязная



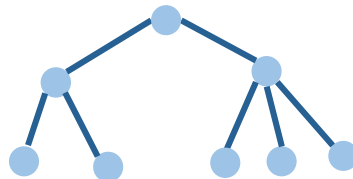
Звезда



Звезда-Иерархия



Дерево



Модель взаимодействия

- Точка-точка
- Широковещательная
- Мультикаст
- Подписочная модель
- Запрос / Ответ

Стек M2M протоколов

OSI Model

Web/ IT

Industrial Ethernet

Fieldbus

Прикладной уровень

HTTP, DHCP, DNS

Modbus TCP, Ethernet/IP,
Ethernet Powerlink,
OPC UA, DNP3, IEC 104

Real time

Profinet, EtherCAT,
SERCOS III, GOOSE, SV

Modbus RTU, Profibus,
CanOpen, DeviceNet,
IEC 101/103

Транспортный уровень

TCP, UDP

TCP/UDP

Real
time

TCP/UDP

Транспортный уровень

Сетевой уровень

IPv6, IPv4

IPv4/IPv6

IP

Сетевой уровень

Канальный/ Физический
уровень

Ethernet (IEEE 802.3),
DSL, ISDN, Wireless
LAN, IEEE 802.11, Wi-Fi

Ethernet (IEEE 802.3),
Wireless LAN, IEEE 802.11,
Wi-Fi

Ethernet (IEEE 802.3)

RS-232/422/485, CAN, ASi

Тысячи байт

Сотни байт

Десятки байт

Десятки байт

Не используется

Основные IoT/IIoT протоколы

- OPC UA
- MQTT
- AMQP
- CoAP
- REST/HTTP
- LoRaWAN
- LoWPAN
- И многие другие ...



Сравнение IoT/IIoT протоколов

	MQTT	OPC UA	AMQP	REST	CoAP	LoRaWAN LoWPAN
Транспорт	TCP/IP	TCP/IP	TCP/IP	TCP/IP	UDP/IP	TCP/IP
Взаимодействие	Publish-Subscr.	Request-Respon	Point-to-point	Request-Respon	Request-Respon	Point-to-point
Применение	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud Device-to-Device	Device-to-Cloud Cloud-to-Cloud Device-to-Device	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud
Латентность	низкая	низкая	низкая	высокая	высокая	низкая
Real-time	условно	Real-time	условно	нет	нет	нет
ИБ	TLS	профиль	TLS	HTTPS	DTLS	TLS/ DTLS На уровне чипа

Архитектура и особенности



Малые вычислительные ресурсы устройств



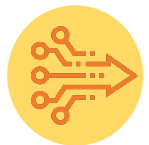
Низкая пропускная способность полевых протоколов



Работа от «батарейки»



Чувствительность к размеру добавляемых данных



Большая вариативность технологий



Высокая латентность полевых протоколов



Множество протоколов



Групповые операции



Особенности
ИБ для M2M и IoT

Основные атаки на IIoT/M2M



Навязывание
устаревших данных
(REPLAY ATTACK)



Подмена IIoT/M2M
устройств



Подмена команд
(COMMAND INJECTION)



«Перепрошивка»
IIoT/M2M устройств



Подача команды
аварийного останова



DDOS-атака для отказа
в обслуживании

Приоритеты защиты

Web/IT



Конфиденциальность
Целостность
Доступность

M2M
IoT/IIoT



Доступность
Целостность
Аутентичность
Конфиденциальность

Требования к протоколам защиты M2M и IoT/IIoT коммуникаций

- Работа на прикладном уровне и независимость от протоколов передачи данных
- Отсутствие установления сессии
- Защита от повторов
- Поддержка групповых операций
- Простая ключевая система

Требования к алгоритмам защиты M2M и IoT/IIoT коммуникаций

- Небольшой размер добавляемых данных
- Быстрые алгоритмы
- Энергоэффективные алгоритмы
- Минимальный набор алгоритмов



Симметричные алгоритмы

Защищенные индустриальные протоколы



Защищенные протоколы ТК26

- «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств» (Р 1323565.1.028–2019)
- «Протокол защищенного обмена для промышленных систем» (CRISP 1.0) (Р 1323565.1.029–2019)
- «Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS»
- «Протокол безопасности сетевого уровня» (IPlir)

Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств

- Работает на прикладном уровне, не зависит от протоколов передачи данных
- Требуется установления соединения
- Нет защиты от повторов
- Не поддерживаются групповые связи
- Алгоритмы: блочный шифр, хэш-функция, HMAC, вычисление точек эллиптической кривой + опционально: ЭП

CRISP

- Работает на прикладном уровне, не зависит от протоколов передачи данных
- Не требует установления соединения
- Есть защита от повторов
- Поддерживаются групповые связи
- Алгоритмы: блочный шифр в режимах CTR и CBC
- Предраспределенные ключи

Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS

- Защита DLMS
- Установление соединения опционально
- Нет защиты от повторов
- Поддерживаются групповые связи
- Алгоритмы: блочный шифр в режимах CTR* и CMAC*, KExp15* / KImp15* + опционально: VKO, ЭП, HMAC
- Предраспределенные ключи или механизмы согласования ключей

IPsec

- Защита IP-трафика
- Может использоваться для построения полноценных VPN
- Не требует установления соединения
- Защита от повторов опциональна
- Не поддерживаются групповые связи
- Алгоритмы: блочный шифр в режимах CTR (MGM) и CBC
- Предраспределенные ключи

The background of the slide is a photograph of a wind farm at sunset. Several wind turbines are silhouetted against a bright orange and yellow sky. In the foreground, there are high-voltage power lines and pylons stretching across the landscape. The overall scene is a mix of renewable energy and traditional power infrastructure.

Спасибо за внимание!