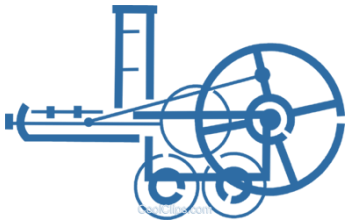
О деятельности по стандартизации протокола криптографической защиты информации для M2M и IoT

Шемякина Ольга,
системный аналитик

M2M + IoT = Industry 4.0

Индустрия 4.0



«Индустрия 1.0»

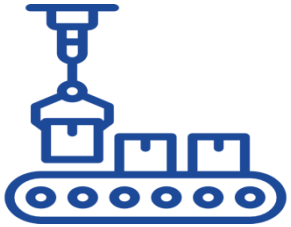
Механизация:
замена физической силы на энергию пара

1784 г.

«Индустрия 2.0»

Электрофикация:
Внедрение конвеерного производства

1870 г.



«Индустрия 3.0»

Автоматизация:
Внедрение роботизированных систем с ЧПУ

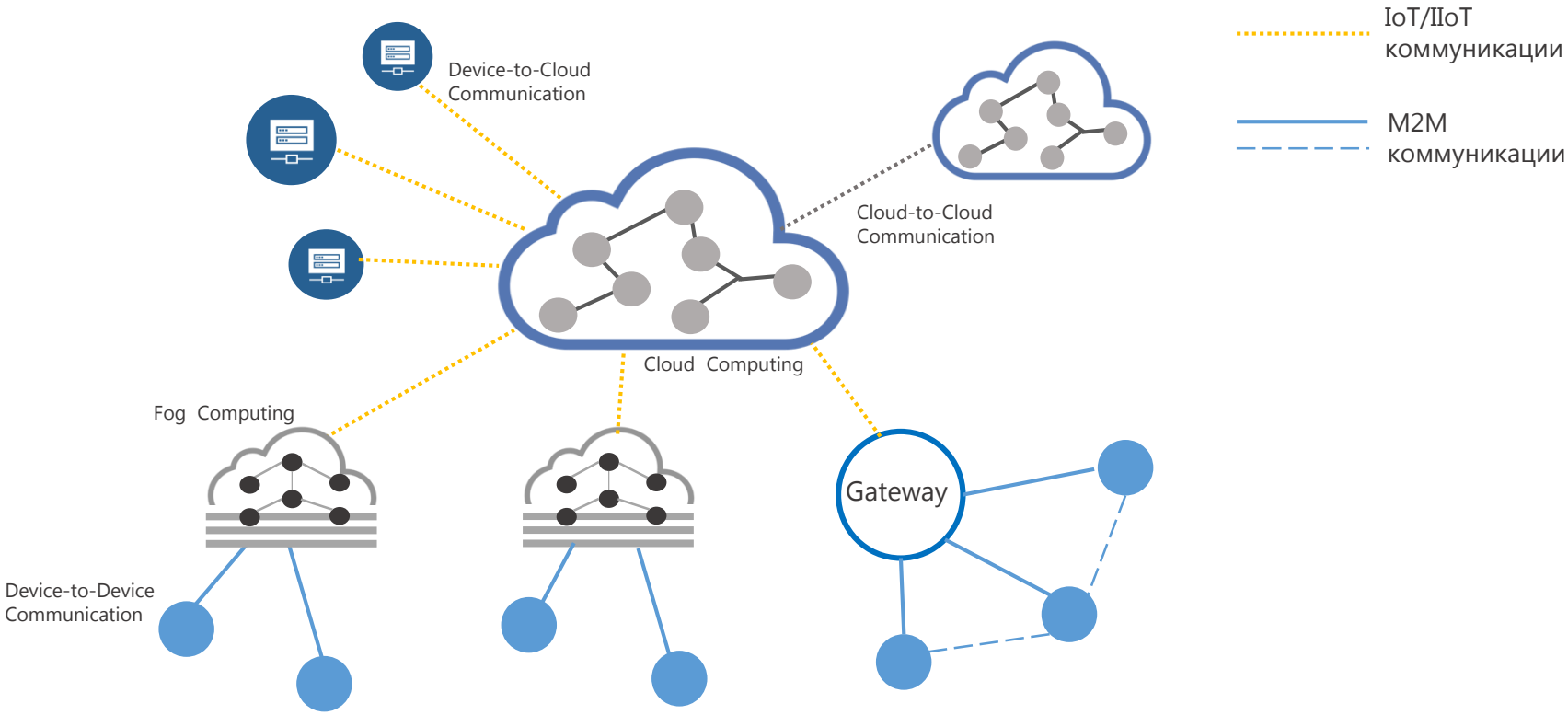
1969 г.

«Индустрия 4.0»

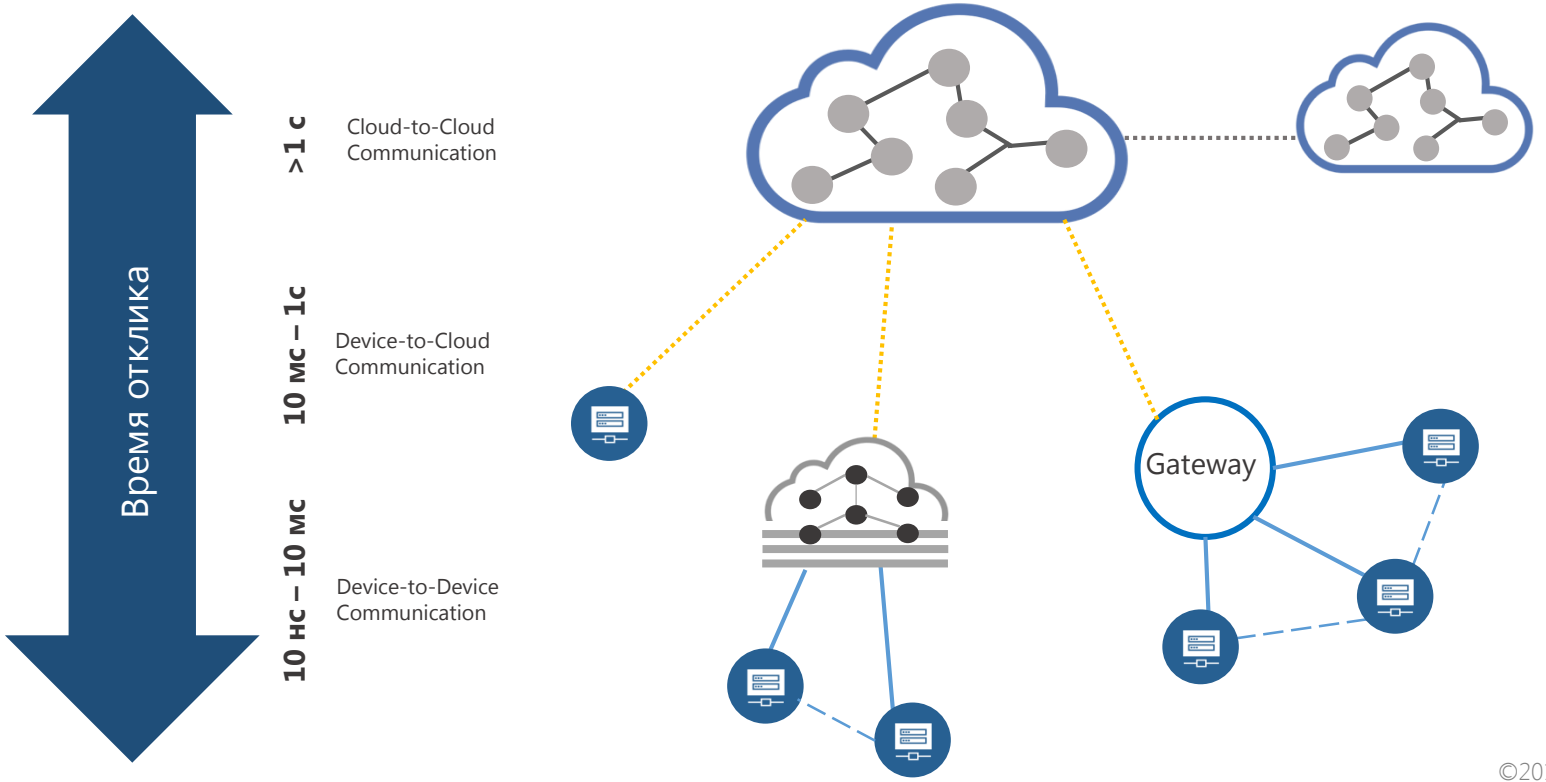
Цифровизация:
Умное производство и киберфизические системы

сегодня

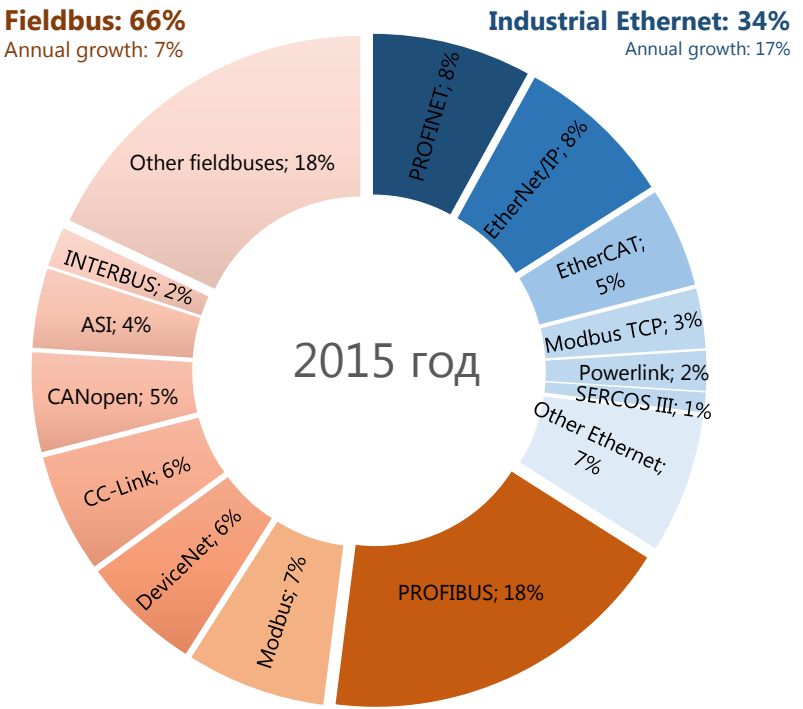
M2M и IoT коммуникации

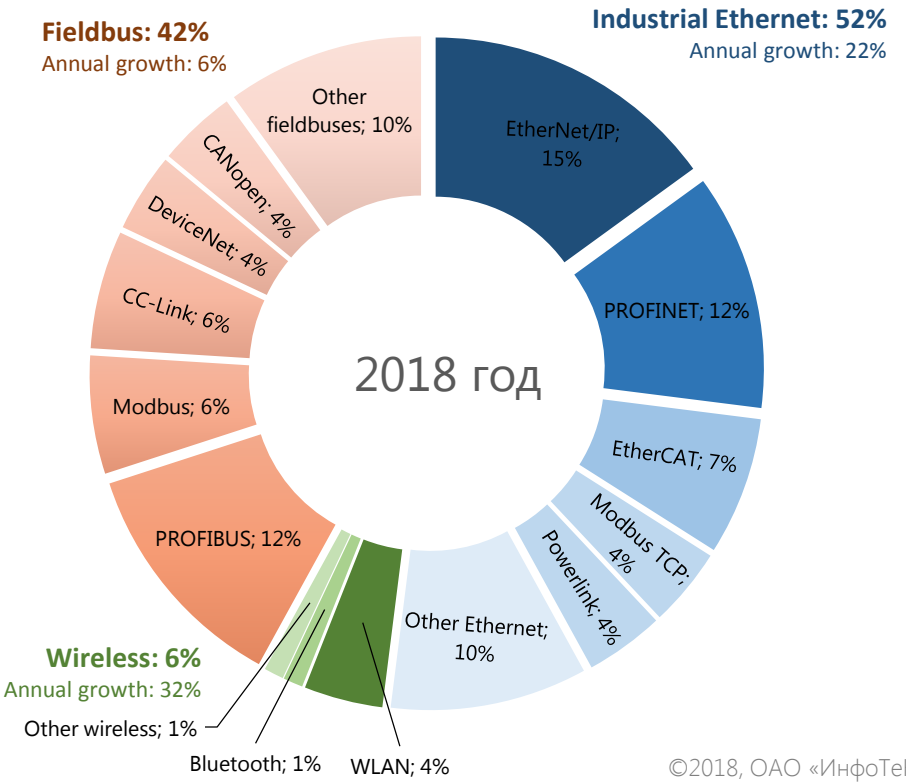


Латентность для IoT и M2M коммуникаций



Промышленные M2M протоколы



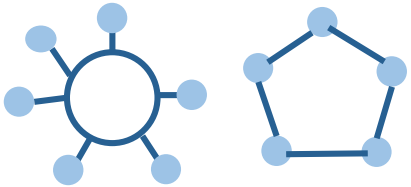


Source: HMS Industrial Networks

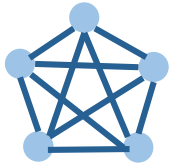
Топология M2M протоколов

Общая шина

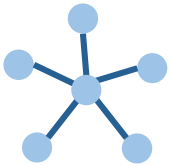
Кольцо



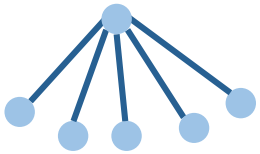
Полносвязная



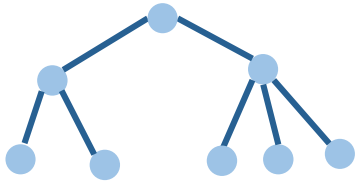
Звезда



Звезда-Иерархия



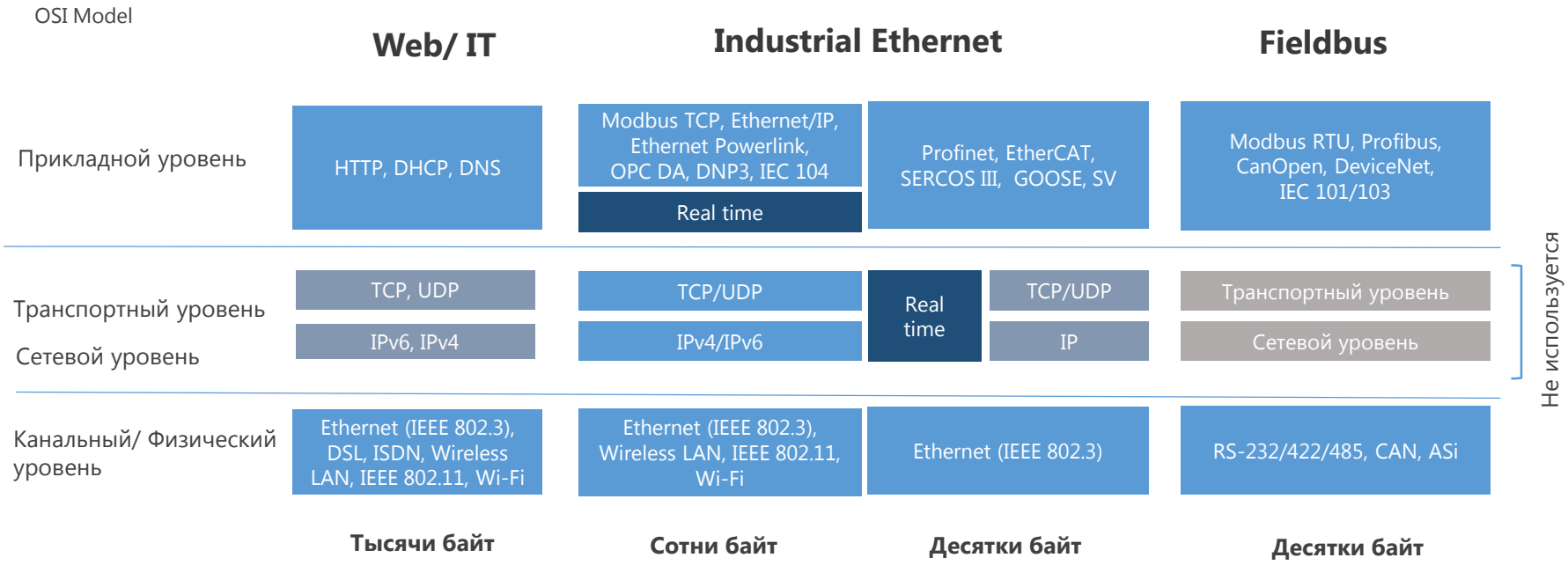
Дерево



Модель взаимодействия

- Точка-точка
- Broadcast
- Multicast
- Подписочная модель
- Request/Response

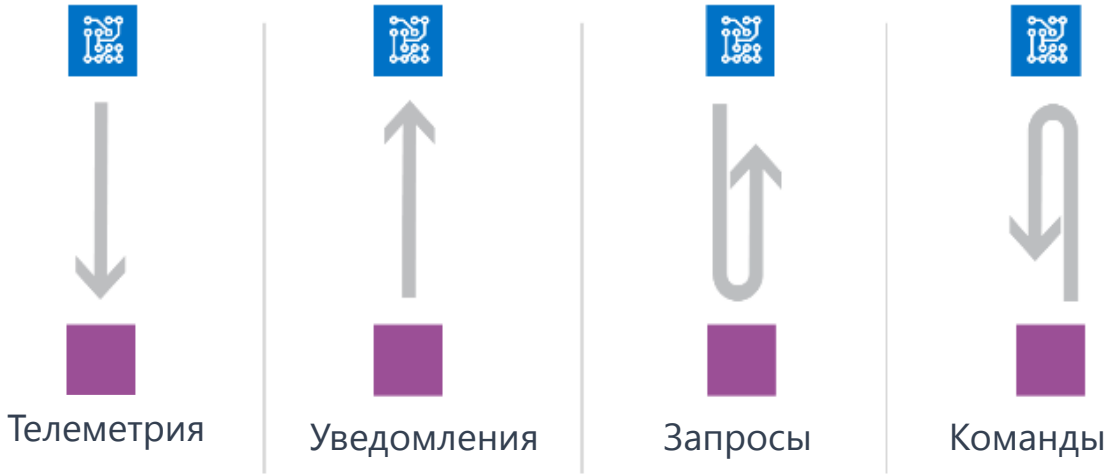
Стек M2M протоколов



Особенности ИБ для M2M и IoT

Основные угрозы

Назначение M2M и IoT/IIoT коммуникаций



Модель угроз

- Изменения команд/ данных (нарушение целостности)
- Подмена команд
- Навязывание ложных данных
- Изменение конфигурации
- Навязывание старых данных
- Подмена устройства

Приоритеты

Web/IT

- Конфиденциальность
- Целостность
- Доступность

M2M
IoT/IIoT

- Доступность
- Целостность
- Аутентичность
- Конфиденциальность

Основные аспекты защиты M2M и IoT/IIoT коммуникаций

- Очень большое разнообразие протоколов
- Использование разных каналов / Использование слабых каналах
- Распространенность мультикаста и подписочной модели
- Многие протоколы являются real-time и критичны к задержкам
- Передача данных объемом в десятки-сотни байт/ критичность к оверхеду
- Большая часть M2M протоколов не являются TCP/IP base
- M2M протоколы в большинстве не подразумевают механизмов защиты коммуникаций
- Беспроводные IoT протоколы имеют встроенную в чипы защиту коммуникаций на западных алгоритмах
- Аутентичность и целостность важнее конфиденциальности

Подходят ли стандартные криптографические протоколы?

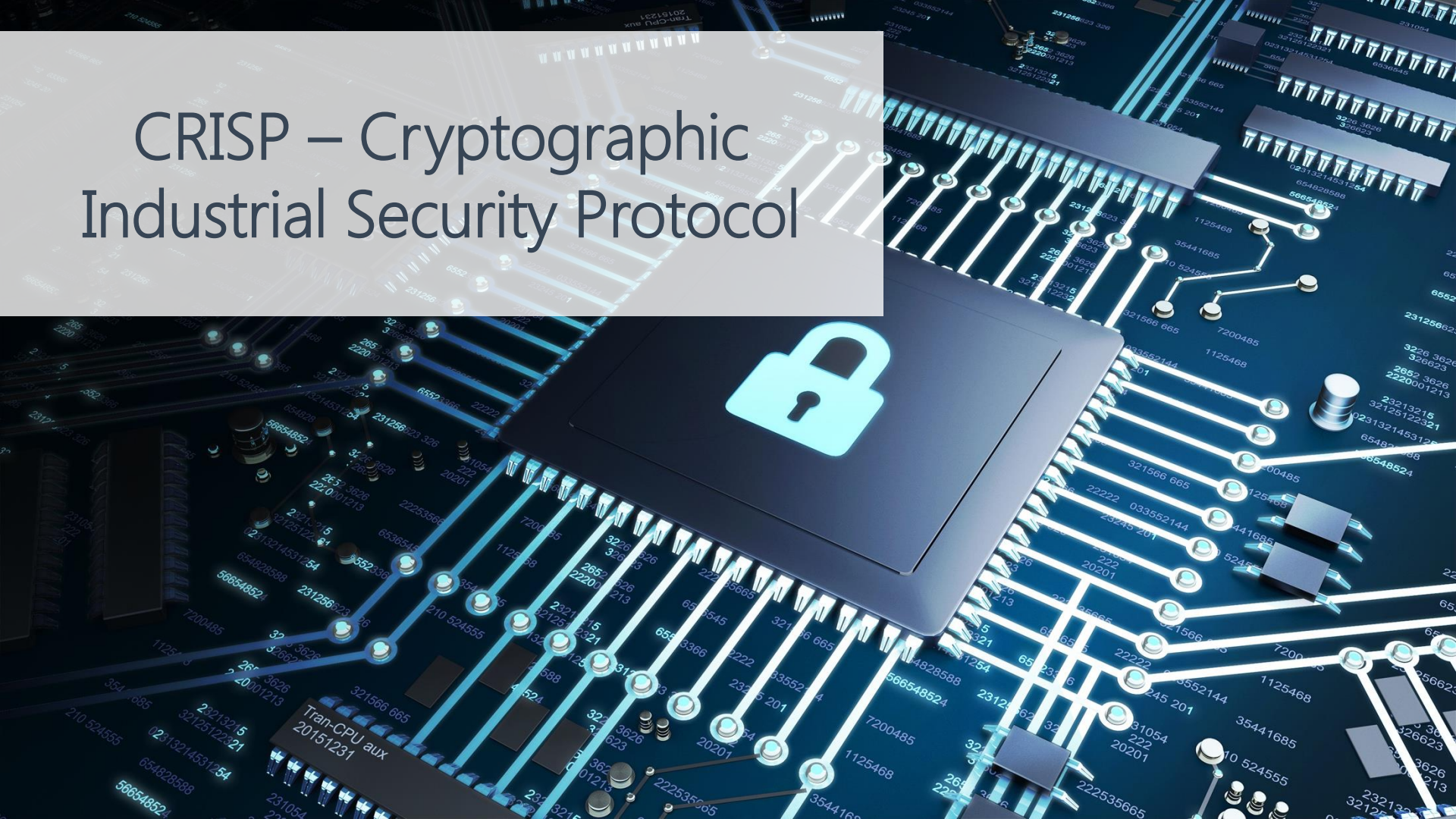
- IPSec – требует установления сессии, плохо работает на слабых каналах, IP based
- TLS – требует установления сессии, TCP/IP based
- CMS – большой оверхэд, большие задержки

Вывод: Рекомендованные в РФ криптографические протоколы не решают поставленной задачи

Алгоритмы, основанные на PKI:

- Удобны для распределенных систем со сложной топологией
- Ресурсоёмкие
- Медленные
- Часто не приспособлены для групповых коммуникаций

CRISP – Cryptographic Industrial Security Protocol



Криптографический протокол для M2M и IoT

Cryptographic Industrial Security Protocol

CRISP

Не всегда надежные каналы/ ограниченная пропускная способность
- без установления сессии -> предварительно распределенные ключи
- каждое сообщение несет всю необходимую информацию для обработки

Целостность и аутентичность важнее конфиденциальности
- обязательная имитозащита/опциональное шифрование
- защита от «чтения назад» не обязательна

Минимальный overhead
- адресация абонентов может быть неявная, через протоколы целевой системы
- все криптографические детали определяются номером криптографического набора

Минимальные задержки обработки
- только симметричные механизмы
- минимальный набор механизмов

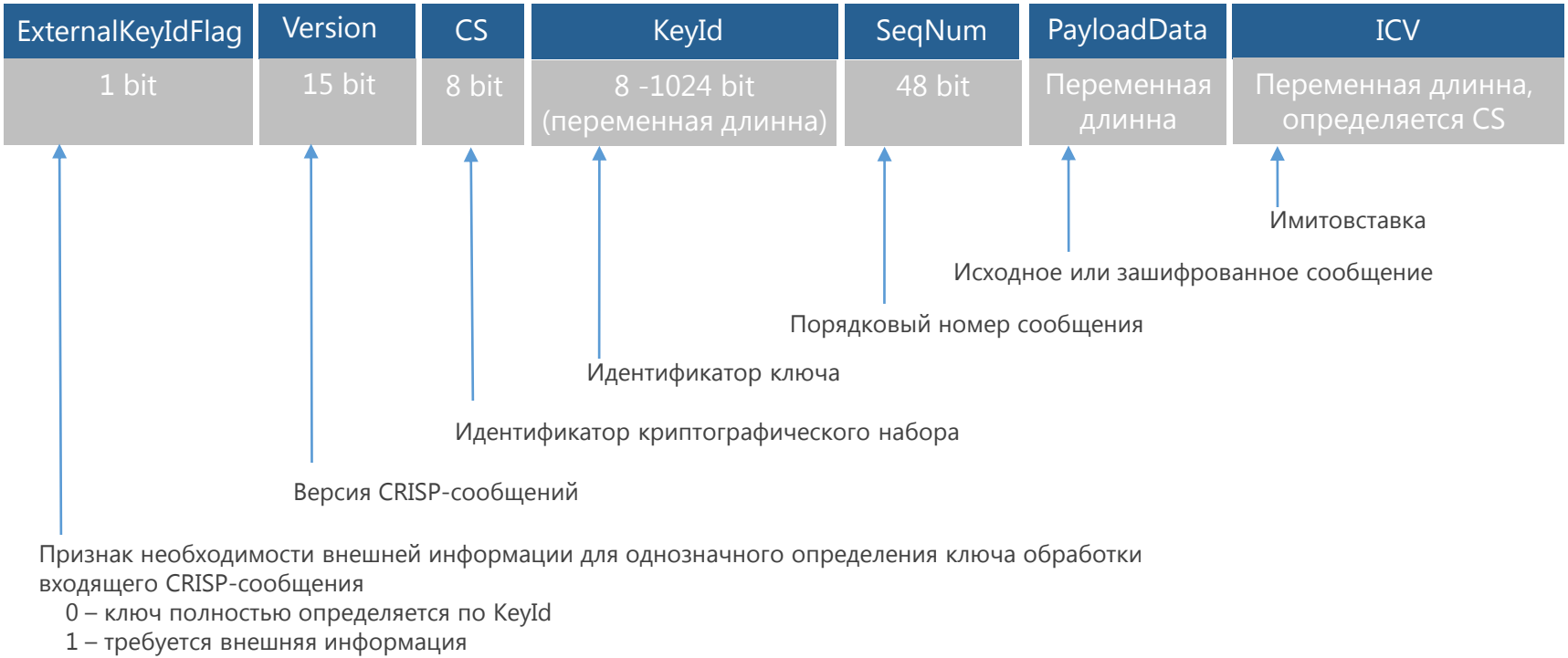
Криптографический протокол CRISP

CRISP (Cryptographic Industrial Security Protocol) - бессесионный протокол защищенной передачи данных для индустриальных систем, M2M и IoT/IIoT коммуникаций

- Обеспечение целостности,
- Обеспечение конфиденциальности
- Аутентификация источника сообщений
- Защита от навязывания повторных сообщений

- У абонентов общий секретный ключ (может быть получен с помощью протоколов, основанных на PKI)
- Защита данных – блочный шифр, имитовставка
- Малый размер вспомогательных данных
- Поддержка адресных (один к одному) сообщений
- Поддержка многоадресных (один ко многим) сообщений

Структура CRISP-сообщений



Суммарный оверхэд – от **14 байтов**

CRISP: Механизмы защиты

Криптонабор CS=1

Целостность и аутентичность
- блочный шифр «Магма» в режиме выработки имитовставки по ГОСТ 34.13-2015

Конфиденциальность
- блочный шифр «Магма» в режиме гаммирования по ГОСТ 34.13-2015

Диверсификация ключей
- блочный шифр «Магма» в режиме выработки имитовставки
- контроль нагрузки на ключ/данные для диверсификации – *SequenceNumber*

Защита от навязывания повторных сообщений
- счетчик сообщений *SequenceNumber* + движущееся окно принятых сообщений
- уникальность значений счетчика в сроки действия одного *KeyIdentifier*

Криптонабор CS=2

Целостность и аутентичность
- блочный шифр «Магма» в режиме выработки имитовставки по ГОСТ 34.13-2015

Диверсификация ключей
- блочный шифр «Магма» в режиме выработки имитовставки
- контроль нагрузки на ключ/данные для диверсификации – *SequenceNumber*

Защита от навязывания повторных сообщений
- счетчик сообщений *SequenceNumber* + движущееся окно принятых сообщений
- уникальность значений счетчика в сроки действия одного *KeyIdentifier*

Планы по CRISP

- Завершено обсуждение протокола как методических рекомендаций в рамках рабочей группы №4 «Криптографические механизмы для M2M и индустриальных сетей» ТК26
- Сентябрь 2018 – Завершение криптографических исследований
- Ноябрь 2018 – Принятие методических рекомендаций
- Апрель 2019 – Редакция рекомендаций по стандартизации
- Сентябрь 2019 – Утверждение рекомендаций по стандартизации
- Разработка рекомендаций по использованию CRISP в протоколах M2M и IoT: Modbus TCP, Modbus RTU, OPC UA, GOOSE, МЭК-60870-5-104, МЭК-60870-5-101
- Пилотирование в составе продуктов партнеров на индустриальных объектах


infotecs
Спасибо за внимание!