Особенности индустриальных протоколов защищенного обмена и их сравнение с универсальными протоколами сетевой защиты

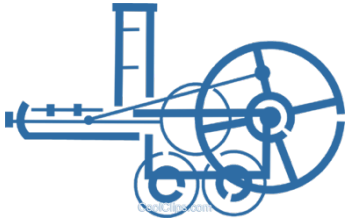
Шемякина Ольга,
системный аналитик

План лекции

- Что защищать?
- Зачем защищать?
- От чего защищать?
- Как защищать?

M2M + IoT = Industry 4.0

Индустрия 4.0



«Индустрия 1.0»

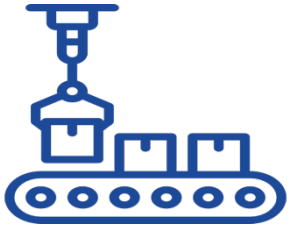
Механизация:
замена физической силы на энергию пара

1784 г.

«Индустрия 2.0»

Электрификация:
Внедрение конвеерного производства

1870 г.



«Индустрия 3.0»

Автоматизация:
Внедрение роботизированных систем с ЧПУ

1969 г.

«Индустрия 4.0»

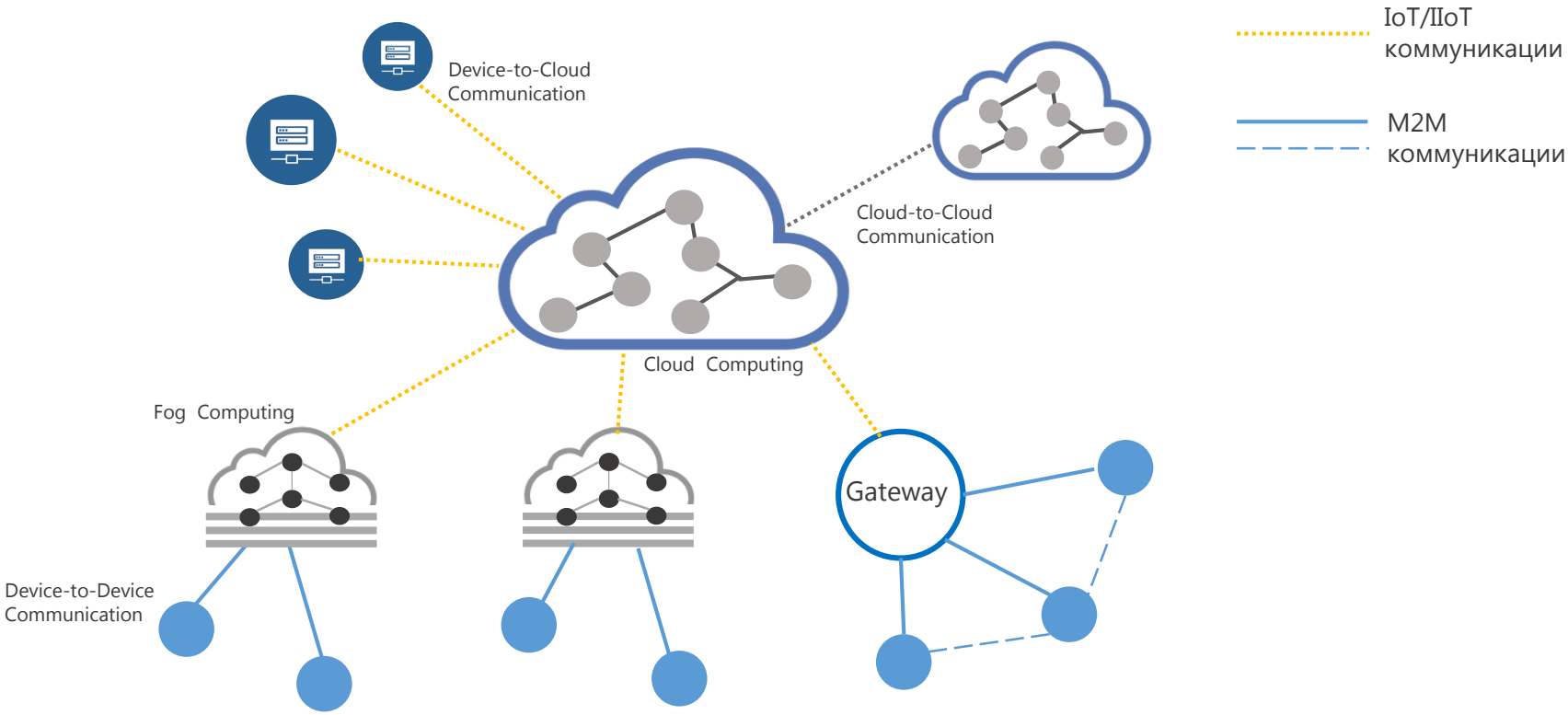
Цифровизация:
Умное производство и киберфизические системы

сегодня

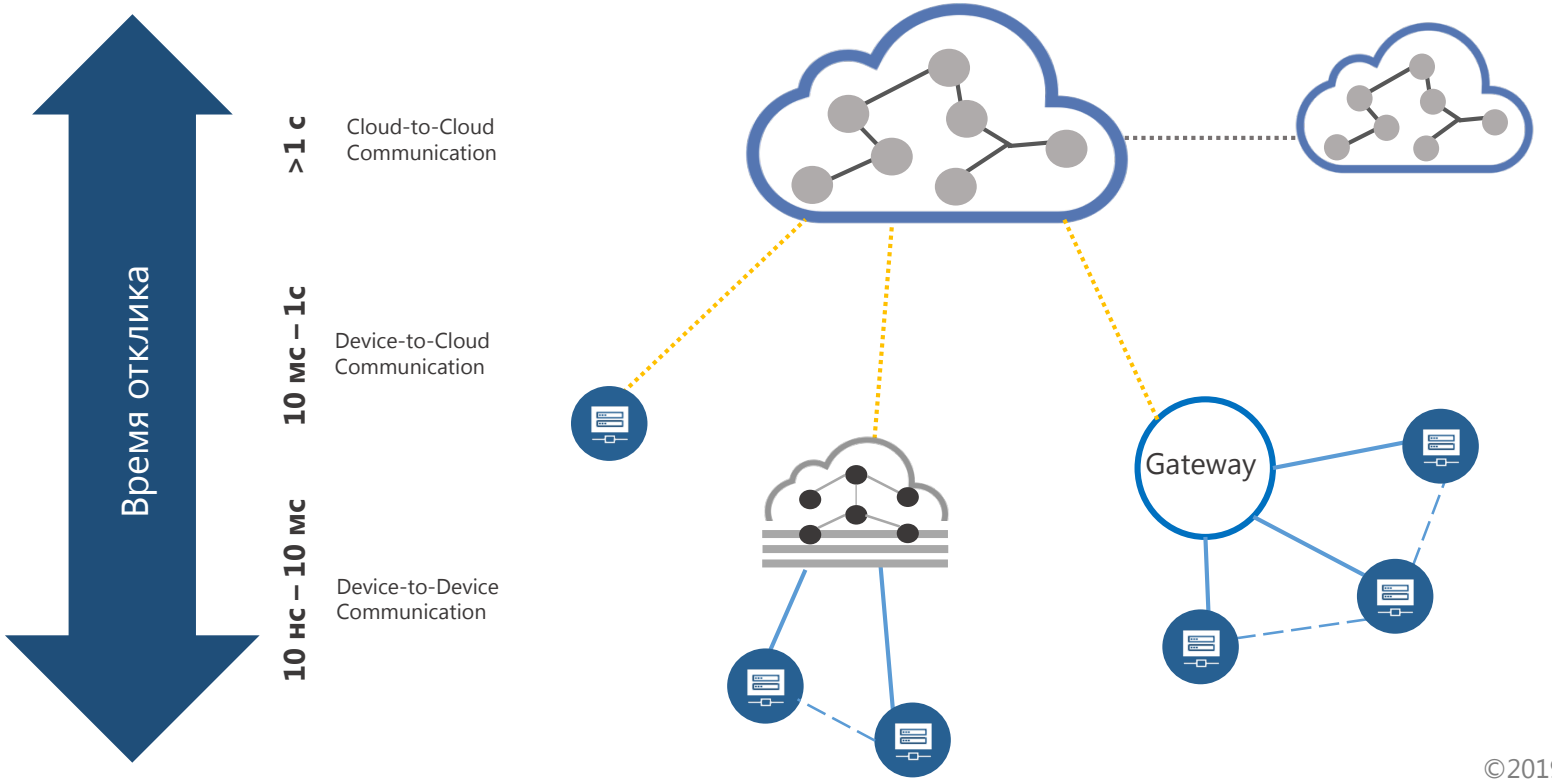
Ключевые технологические тенденции

- Большие данные и аналитика
- Автономные роботы
- Моделирование и симуляторы
- Облачные вычисления
- Интернет вещей
- Информационная безопасность
- 3D-печать
- Дополненная реальность

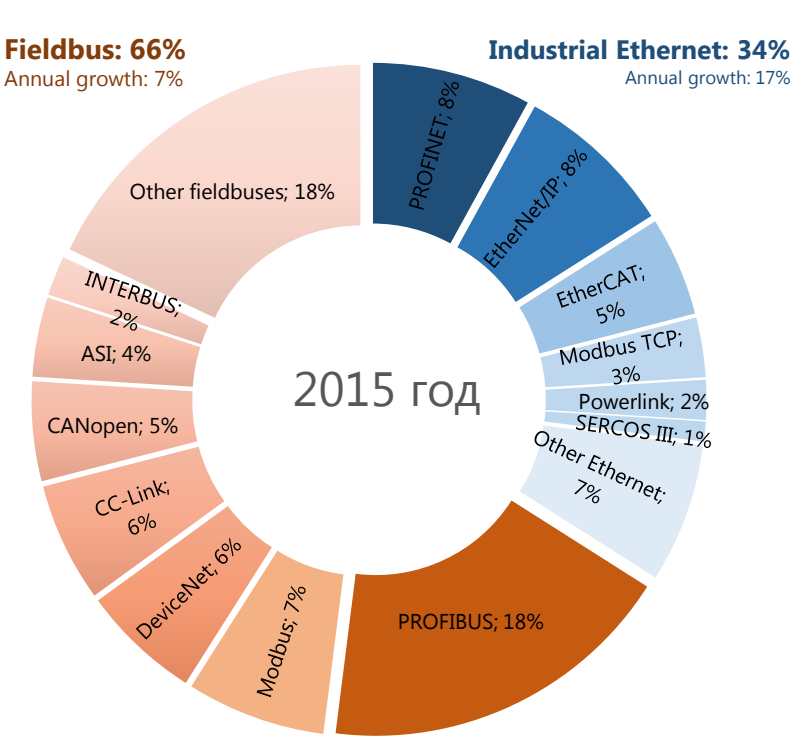
M2M и IoT коммуникации

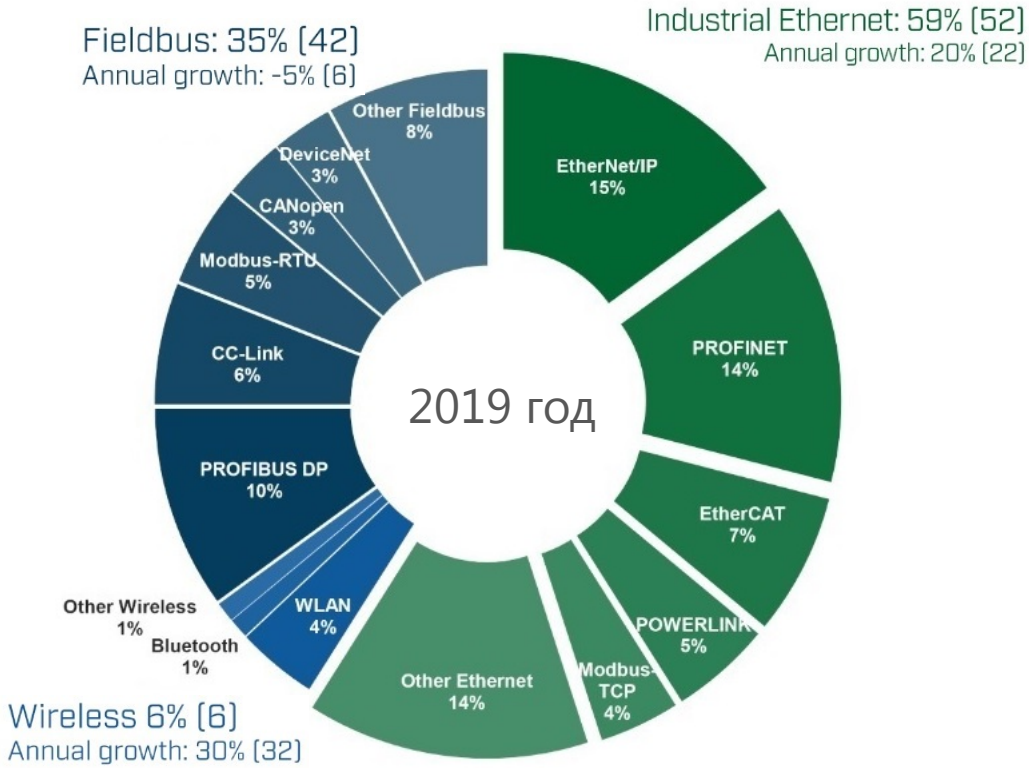


Латентность для IoT и M2M коммуникаций



Промышленные M2M протоколы



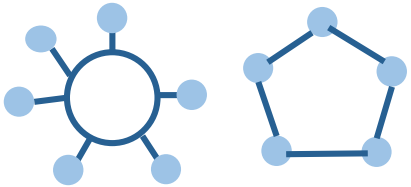


Source: HMS Industrial Networks

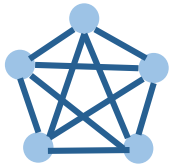
Топология M2M протоколов

Общая шина

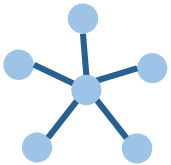
Кольцо



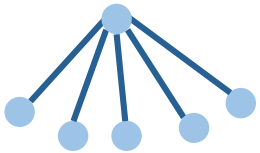
Полносвязная



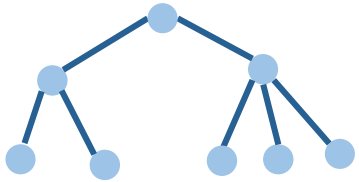
Звезда



Звезда-Иерархия



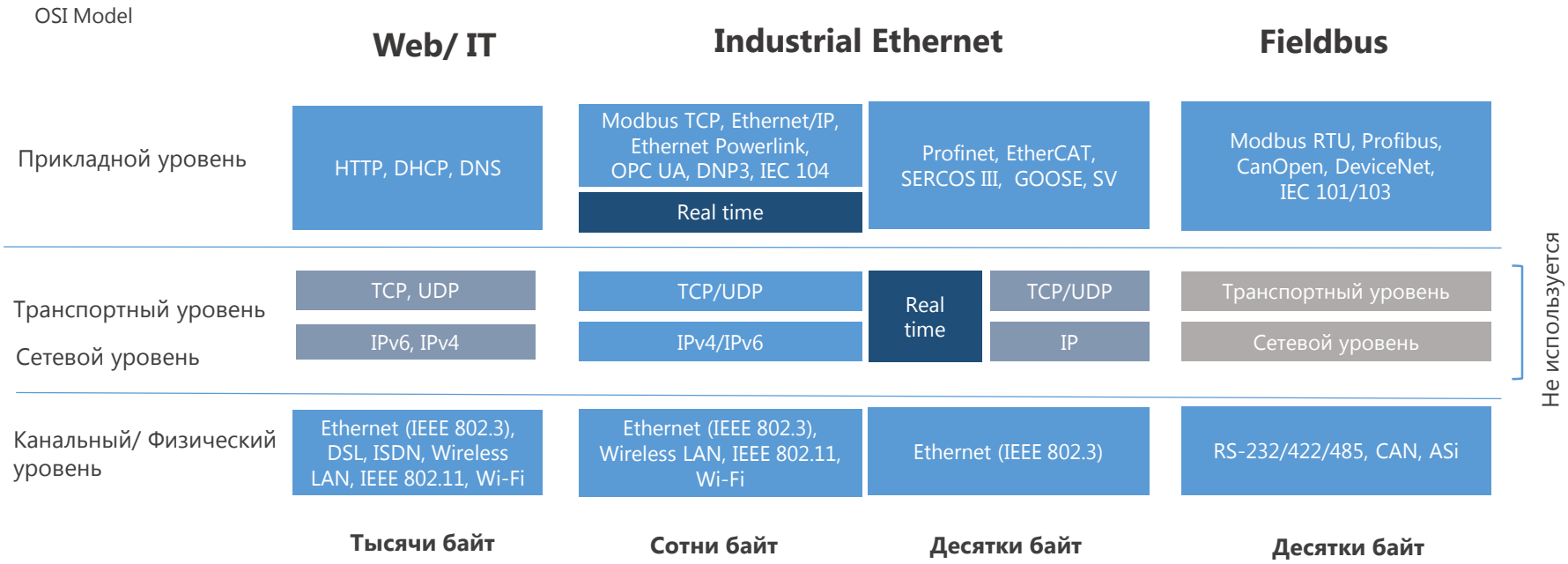
Дерево



Модель взаимодействия

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

Стек M2M протоколов



Защищать?

Примеры кибер-атак

- 2000, Австралия – Миллионы литров сточных вод попали в реку
- 2001, Европа – Отключение подачи газа для домашних и корпоративных клиентов
- 2002, Венесуэла – В PDVSA снижена добыча нефти с 3 млн до 370 тыс баррелей
- 2006, Лос-Анжелес – Взлом светофоров привел к пробкам
- 2008, Лодзь – 4 трамвая сошли с рельсов, пострадали 12 человек
- 2014, Германия – Огромный ущерб металлургическому заводу
- 2015, Украина – Более 600 тыс человек осталось без света

Масштаб угрозы

- Наиболее известный пример кибер-атаки на АСУ ТП – вирус Stuxnet – нарушение ядерной программы Ирана

- Даже **единичное ЧП на КВО** (критически важном объекте) может иметь **фатальные последствия** – гибель людей, серьезное влияние на экологию, разрушение экономики

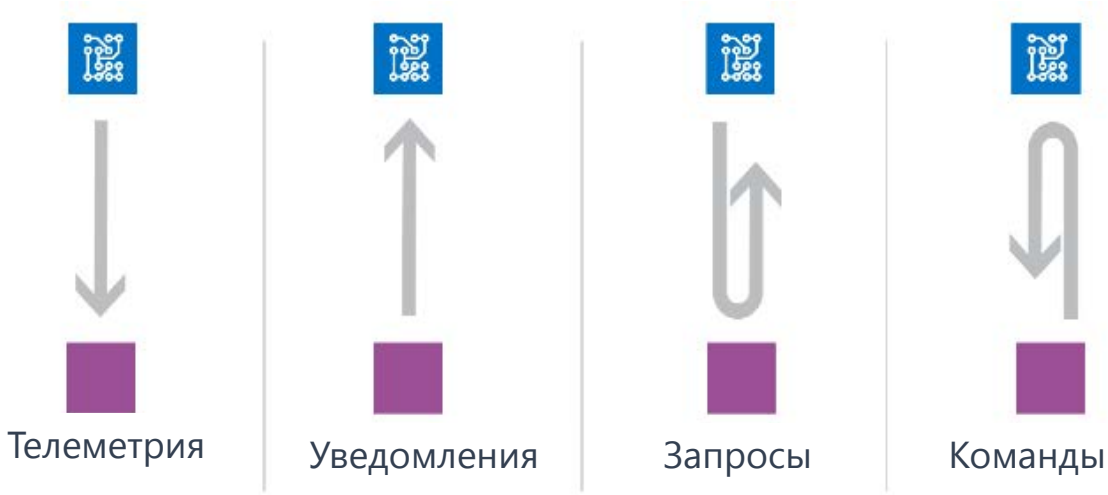
Угрозы осознаны

- Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ
- Приказ ФСТЭК N 235
  (Требования к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования)
- Приказ ФСТЭК N 239
  (Требования по обеспечению безопасности значимых объектов КИИ РФ)

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 каналов
- Распространенность мультикаста и подписочной модели
- Многие протоколы являются протоколами реального времени и критичны к задержкам
- Передача данных объемом в десятки-сотни байт, важен размер добавляемых данных
- Многие M2M протоколы не работают «поверх» TCP/IP
- 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 универсальные криптографические протоколы?

- IPSec – требует установления сессии, плохо работает на слабых каналах, основан на IP
- TLS – требует установления сессии, основан на TCP/IP
- CMS – большой объем добавляемых данных, большие задержки

Вывод:

Универсальные криптографические протоколы не в полной мере решают поставленную задачу, не соответствуют аспектам защиты M2M

Особенности асимметричных алгоритмов

- Удобны для распределенных систем со сложной или неизвестной топологией
- Ресурсоёмкие (проблема энергопотребления)
- Медленные
- Часто не приспособлены для групповых коммуникаций
- Сложное управление сертификатами

Вывод:

Для защиты M2M желательно отказаться от асимметричных алгоритмов

Защищенные индустриальные протоколы

Международный опыт: IEC

Защита протоколов электроэнергетики (IEC 62351):

- IEC 62351-4 – защита MMS (ГОСТ Р ИСО 9506-2-2014)
- IEC 62351-5, IEC 60850-5-7 – защита IEC 60870-5 и производных (ГОСР Р МЭК 60870-5-101/104)
- IEC 62351-6 – защита GOOSE, SV
- IEC 62351-9 – управление ключами

IEC 62351-9

В основе IEC 62351-9:

- PKI:
  - Формирование запросов на сертификаты
  - Выпуск сертификатов
  - Управление сертификатами
  - CMS
  - TLS
  - HTTPS
- GDOI (RFC 6407) – управление групповыми ключами

IEC 60850-5-7

В основе IEC 60850-5-7:

- Только симметричные алгоритмы
- Требования и механизмы IEC 62351 сведены к минимуму

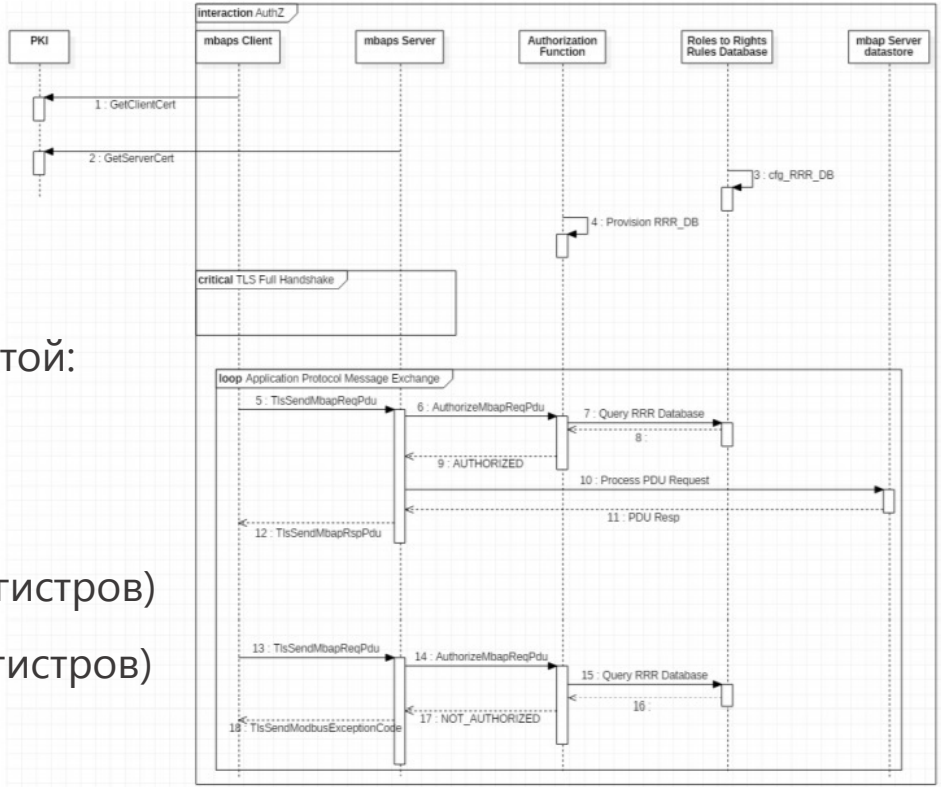
Ограничения:

- Только имитозащита
- Взаимодействие не симметричное

Международный опыт: Modbus

Защищенная версия Modbus TCP:

использование TLS



Базовый протокол Modbus крайне простой:

- Команда – ответ на команду
- 16 команд:
  - чтение регистра (нескольких регистров)
  - запись регистра (нескольких регистров)

Беспроводные протоколы

Предварительные национальные стандарты (ТК194, 2019 год):

- ПНС «Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi)»
- Проект ПНС «Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением»

Нет обоснования стойкости →

Есть опасения по поводу безопасности данных протоколов

Защищенные протоколы в РФ

Методические рекомендации ТК26:

- МР 26.4.003-2018 «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств»
- МР 26.4.001-2019 «Протокол защищенного обмена для индустриальных систем (CRISP 1.0)» (CRISP - Cryptographic Industrial Security Protocol)

Основные принципы

- Небольшой размер добавляемых данных
- Отказ от использования асимметричных алгоритмов

  (для МР 26.4.003-2018 - опционально)
- Большое количество сообщений, обрабатываемых на одном ключе
- Обязательная имитозащита и опциональное шифрование
- Независимость от протоколов передачи данных
- Могут поддерживаться различные криптографические механизмы

  (например, различных алгоритмы шифрования)

Основные отличия

Параметр	МР 26.4.003-2018	CRISP
Установление сессии	Требуется	Не требуется
Ключевая система	Определена полностью	Не определена (предраспределенные ключи)
Защита от повторов	Не предусмотрена	Предусмотрена
Поддержка групповых сообщений	Не предусмотрена	Предусмотрена
Текущий набор алгоритмов	«Магма», «Кузнечик», AEAD-режим	«Магма»


infotecs
Спасибо за внимание!