

The background of the slide is a blurred image of a person in a dark suit and tie, holding a large, metallic, 3D-rendered gear. The gear is the central focus, with several other smaller gears and mechanical parts visible in the background, creating a sense of depth and complexity. The overall color palette is cool, with blues and greys.

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

Шемякина Ольга,
системный аналитик



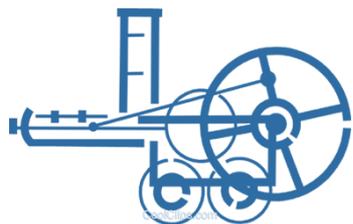
M2M + IoT = Industry 4.0

DATA

IOT



Индустрия 4.0



«Индустрия 1.0»

Механизация:
замена физической силы
на энергию пара

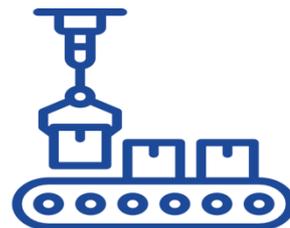
1784 г.



«Индустрия 2.0»

Электрфикация:
Внедрение конвейерного
производства

1870 г.



«Индустрия 3.0»

Автоматизация:
Внедрение
роботизированных
систем с ЧПУ

1969 г.

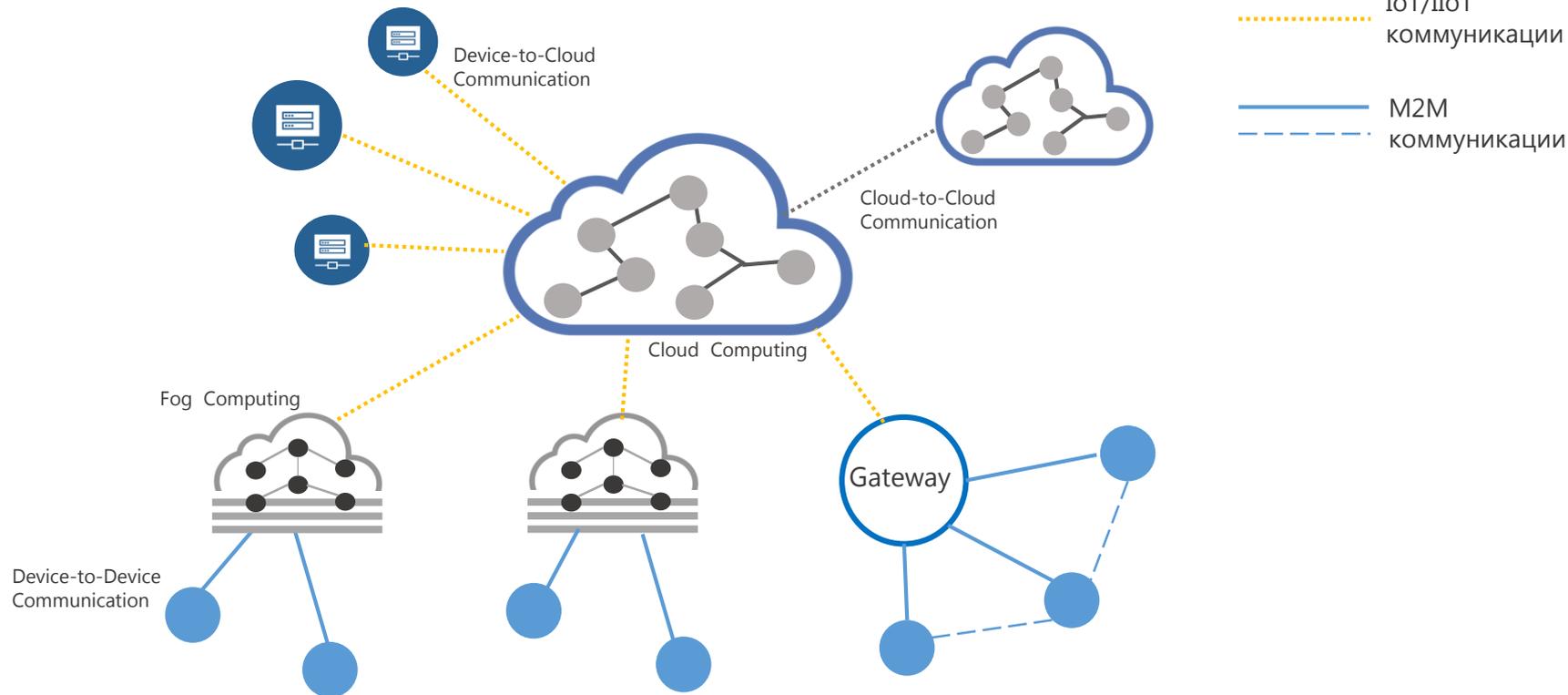


«Индустрия 4.0»

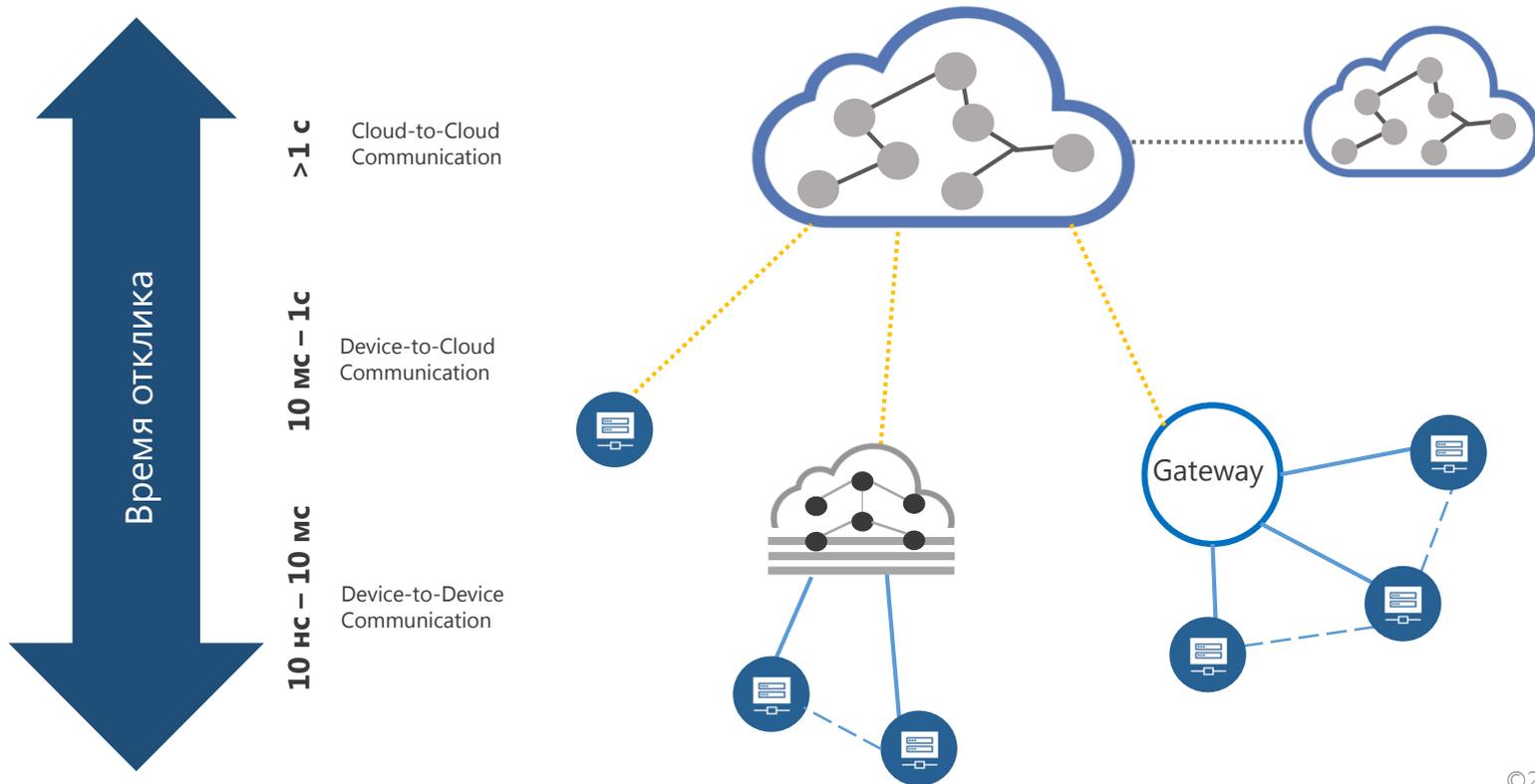
Цифровизация:
Умное производство и
киберфизические
системы

сегодня

M2M и IoT коммуникации



Латентность для IoT и M2M коммуникаций



Промышленные M2M протоколы

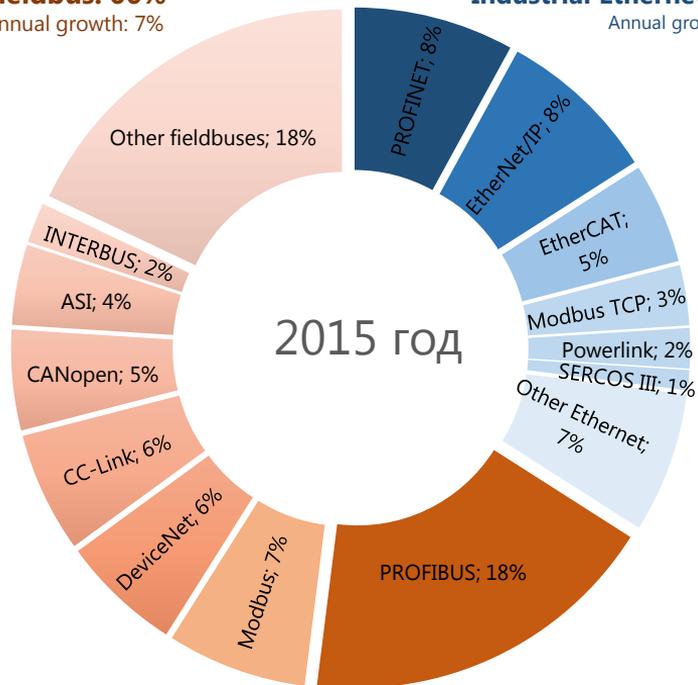


Fieldbus: 66%

Annual growth: 7%

Industrial Ethernet: 34%

Annual growth: 17%



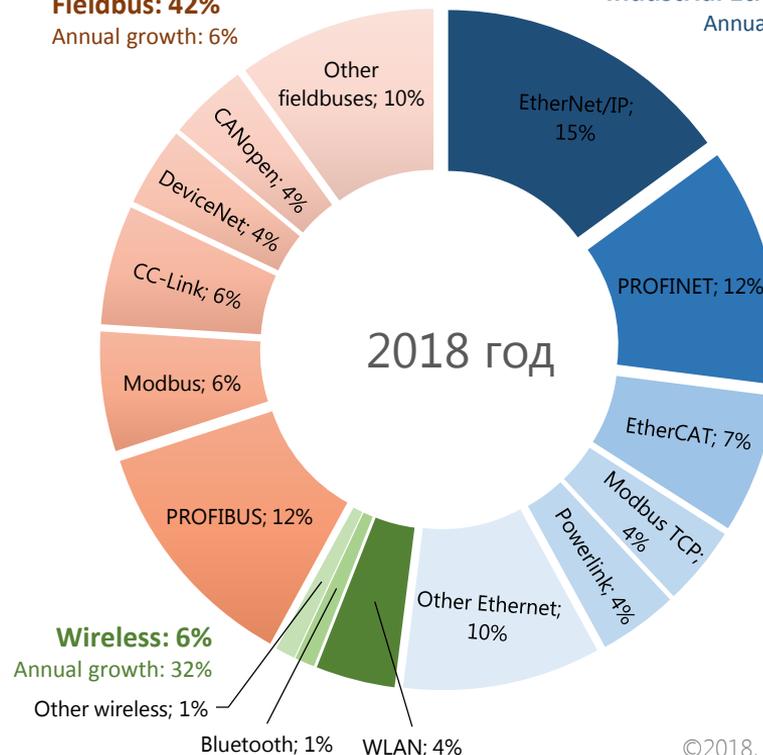
Source: HMS Industrial Networks

Fieldbus: 42%

Annual growth: 6%

Industrial Ethernet: 52%

Annual growth: 22%



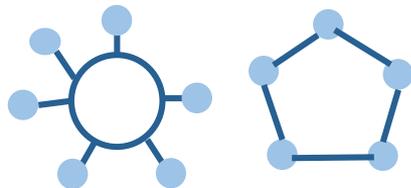
©2018, ОАО «ИнфоТеКс».

Топология M2M протоколов

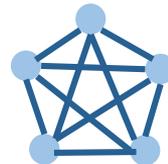
Общая шина



Кольцо



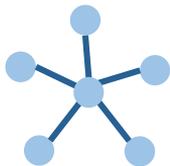
Полносвязная



Модель взаимодействия

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

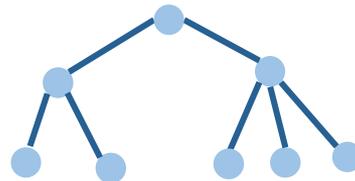
Звезда



Звезда-Иерархия



Дерево



Стек M2M протоколов

OSI Model

Web/ IT

Industrial Ethernet

Fieldbus

Прикладной уровень

HTTP, DHCP, DNS

Modbus TCP, Ethernet/IP,
Ethernet Powerlink,
OPC DA, 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

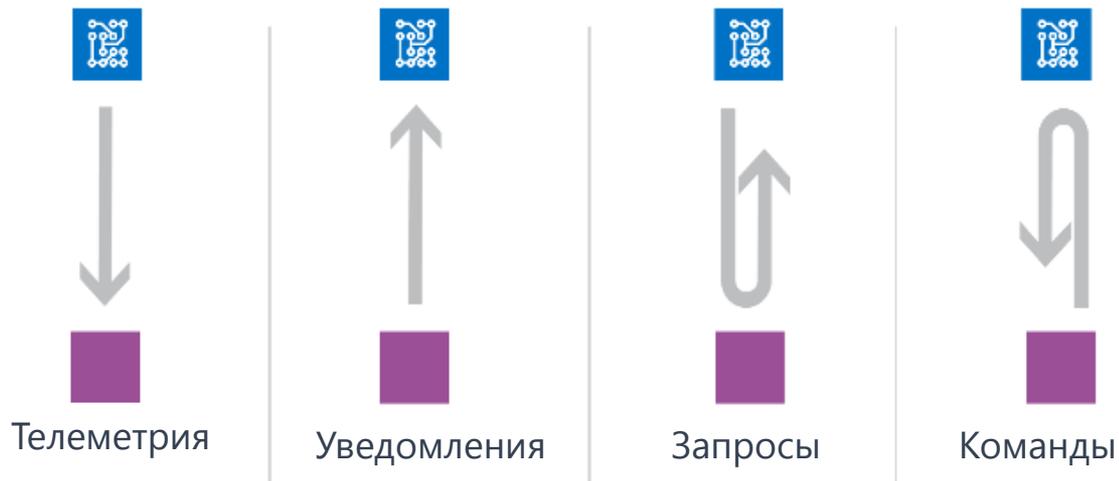
Не используется



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

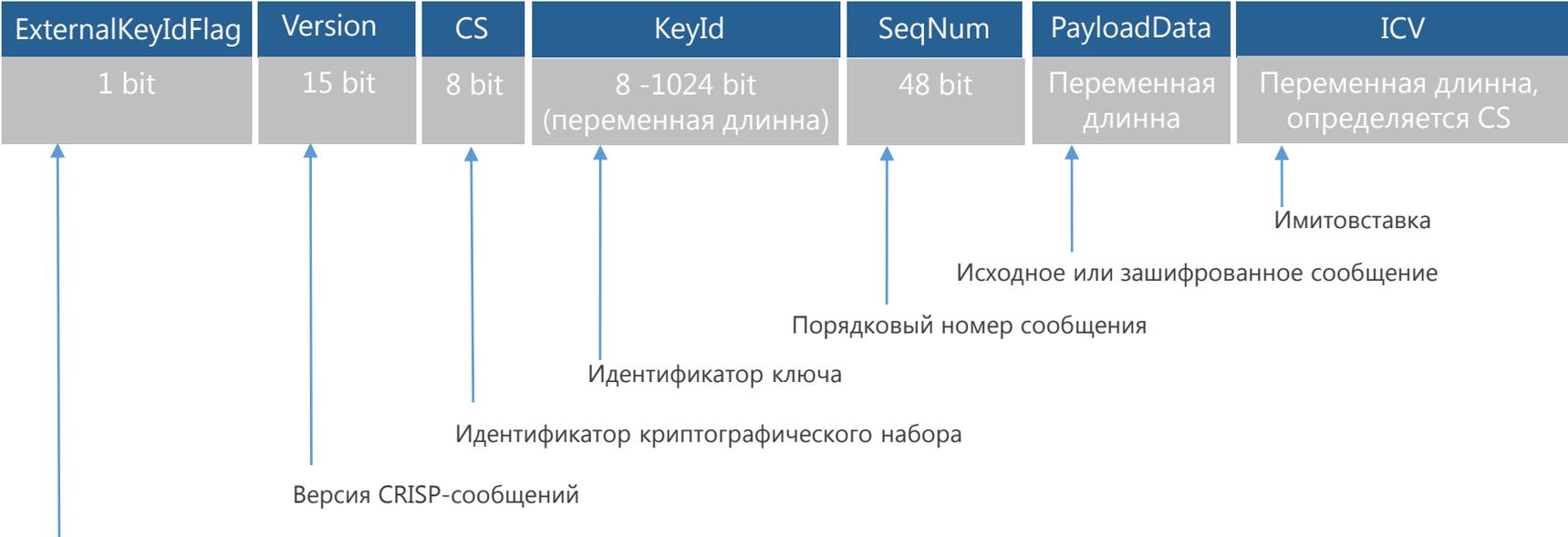
- только симметричные механизмы
- минимальный набор механизмов

Криптографический протокол CRISP

CRISP (Cryptographic Industrial Security Protocol) - бессессионный протокол защищенной передачи данных для промышленных 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



Признак необходимости внешней информации для однозначного определения ключа обработки входящего CRISP-сообщения

- 0 – ключ полностью определяется по KeyId
- 1 – требуется внешняя информация

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 промышленных 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 промышленных объектах

The background of the slide is a photograph of a landscape at sunset. In the foreground, several wind turbines are silhouetted against the bright orange and yellow sky. In the middle ground, several high-voltage power line towers are visible. The sun is low on the horizon, creating a strong glow and casting long shadows. The overall scene is a mix of renewable energy (wind) and traditional infrastructure (power lines).

Спасибо за внимание!