


# Криптографический протокол CRISP Что? Где? Когда?

Марина Сорокина, Ольга Шемякина

A decorative orange circle is partially visible on the right edge of the slide.

# CRISP



Cryptographic Industrial Security Protocol –  
неинтерактивный протокол защищенной  
передачи данных для промышленных систем,  
M2M и IIoT коммуникаций

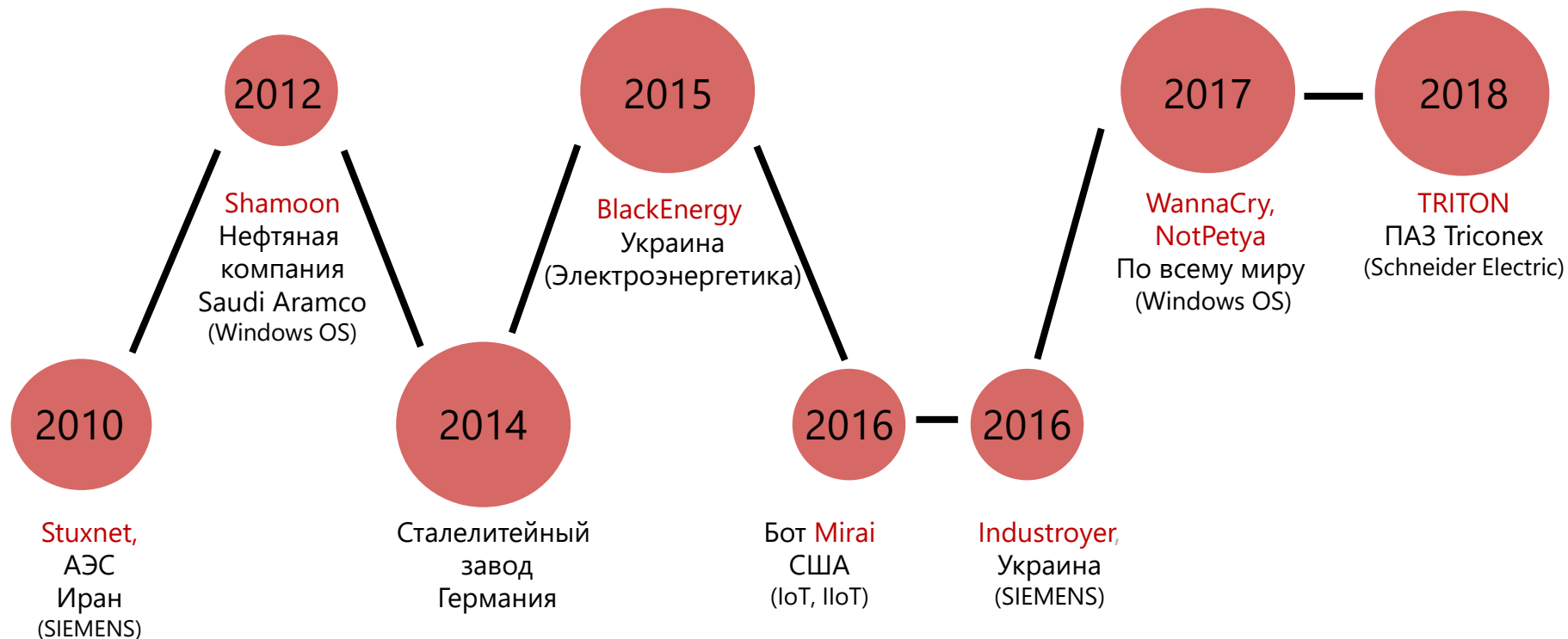
# План вебинара



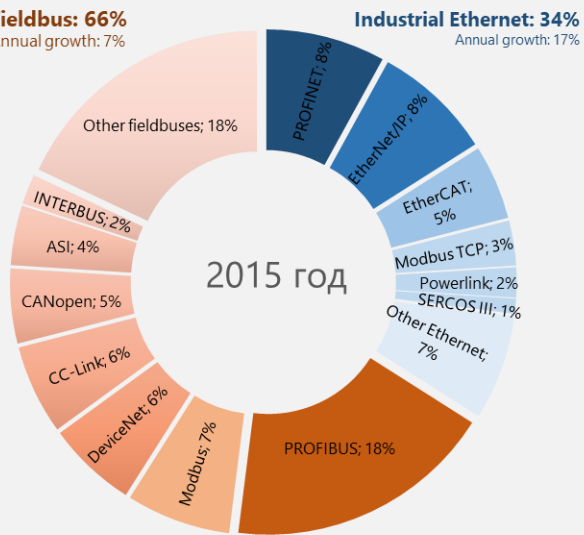
1. **Когда?** Как появилась необходимость разработки протокола CRISP?
2. **Что?** Что такое криптографический протокол CRISP?
3. **Зачем?** Какие преимущества несет в себе протокол CRISP?
4. **Где?** На каком этапе работ находится протокол CRISP?
5. **Как?** Как применять протокол CRISP?



# Атаки на промышленные системы



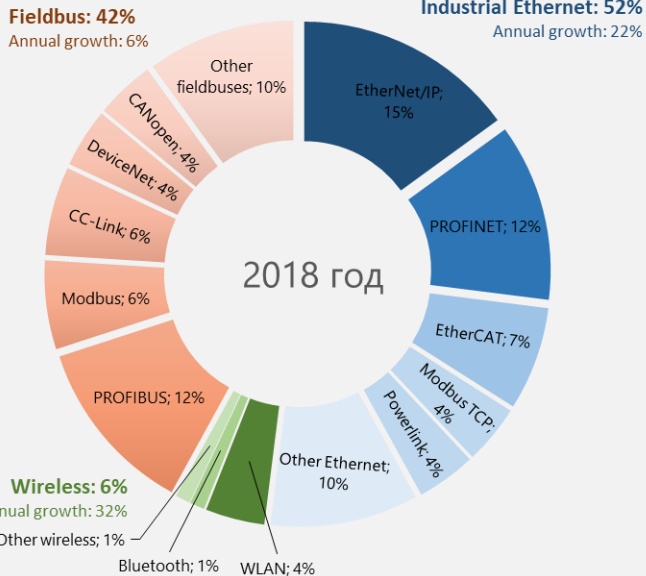
**Fieldbus: 66%**  
Annual growth: 7%



2015 год

Source: HMS Industrial Networks

**Fieldbus: 42%**  
Annual growth: 6%



2018 год

**Wireless: 6%**  
Annual growth: 32%

Почему трудно защищать промышленные сети?

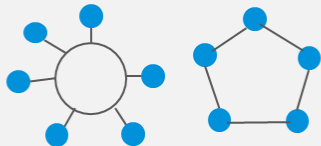
Большое количество промышленных протоколов:

- Полевые шины
- Industrial Ethernet
- Беспроводные сети

Общая шина



Кольцо



Полносвязная



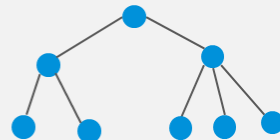
Звезда



Звезда-Иерархия



Дерево

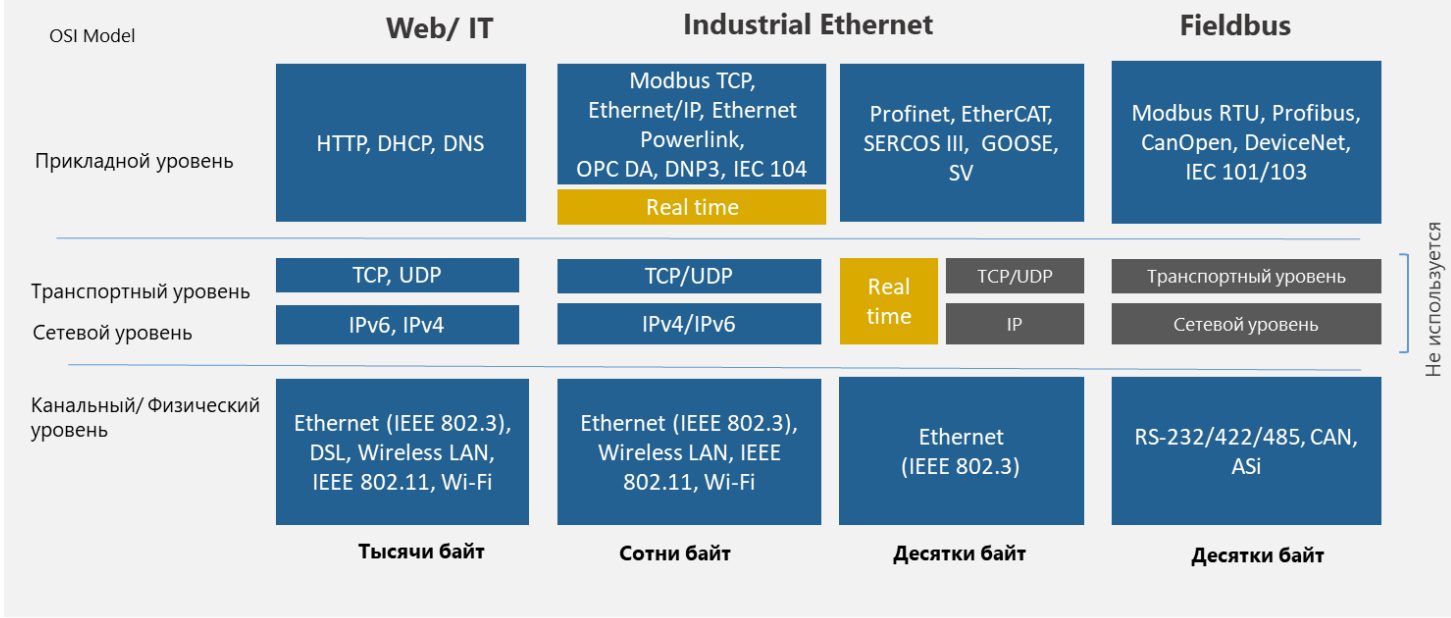


### Модель взаимодействия

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

Почему трудно защищать промышленные сети?


- Разная топология сети
- Различная модель взаимодействия объектов сети



## Почему трудно защищать промышленные сети?

- Стек протоколов для части протоколов не использует транспортный и сетевой уровни
- Размер пакетов ограничен десятками-сотнями байт
- Real-time



A close-up photograph of a blue, articulated robotic hand with multiple fingers, positioned over a computer keyboard. The lighting is dramatic, with a strong blue tint and highlights on the mechanical joints of the hand and the keys.

## Новые технологии – НОВЫЕ ВЫЗОВЫ

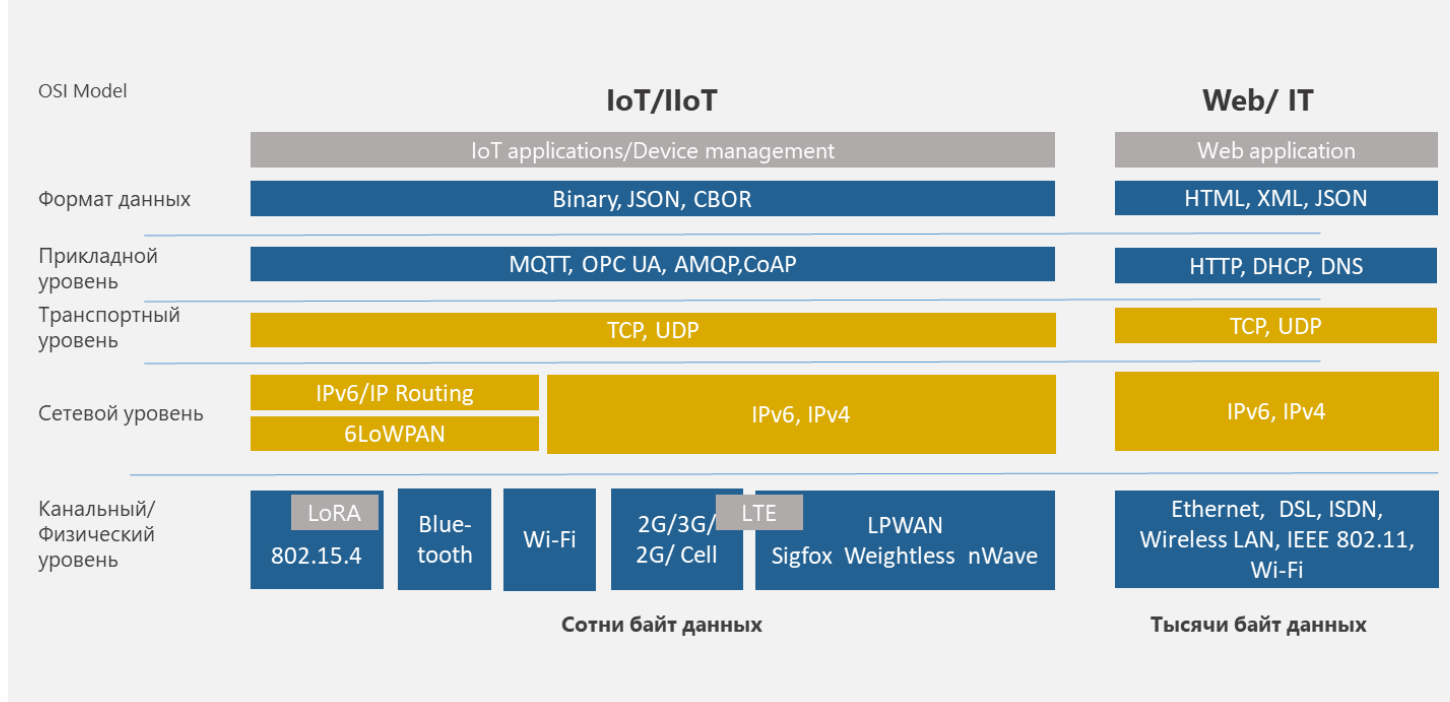
- LPWAN сети
- Mesh-сети
- IIoT



Почему трудно  
защищать IIoT?

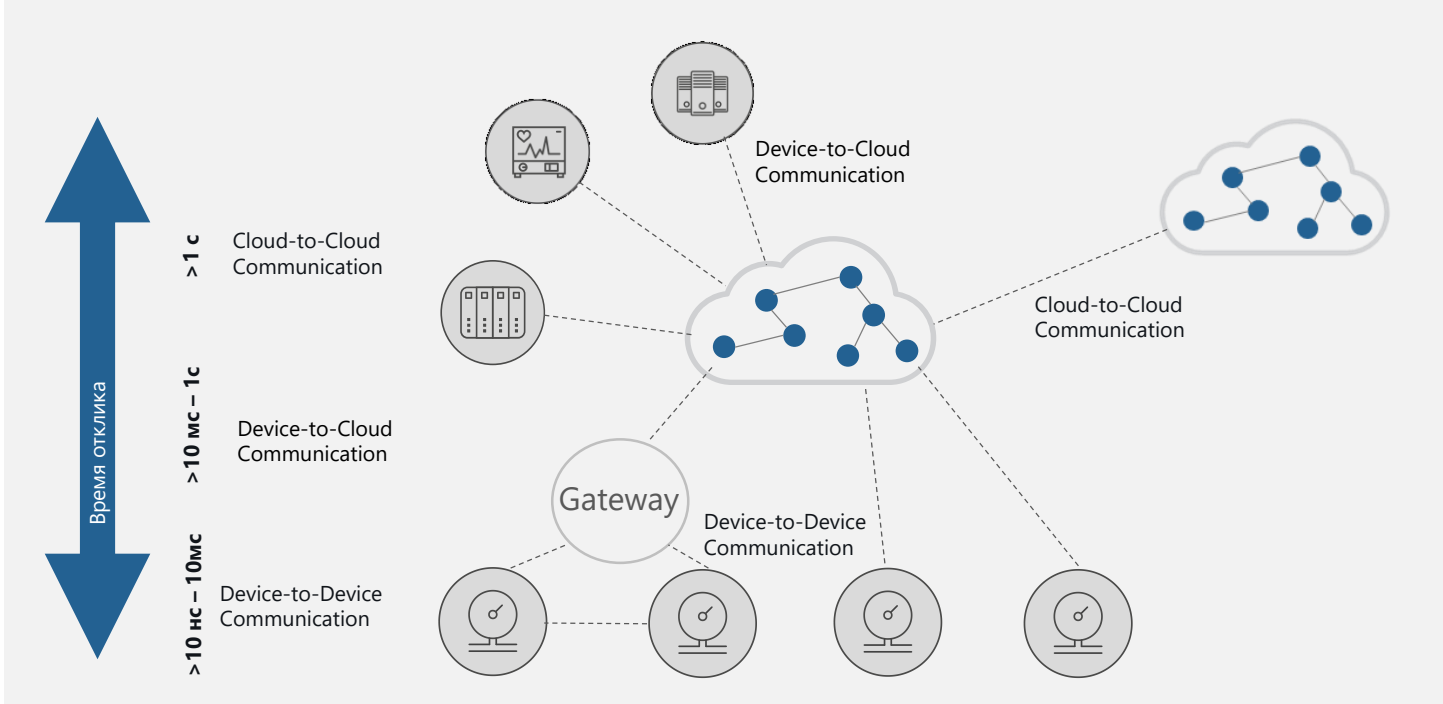
Большое количество протоколов:

- MQTT
- OPC UA
- CoAP
- REST/HTTP
- LoRaWan
- NB-IoT
- XNB



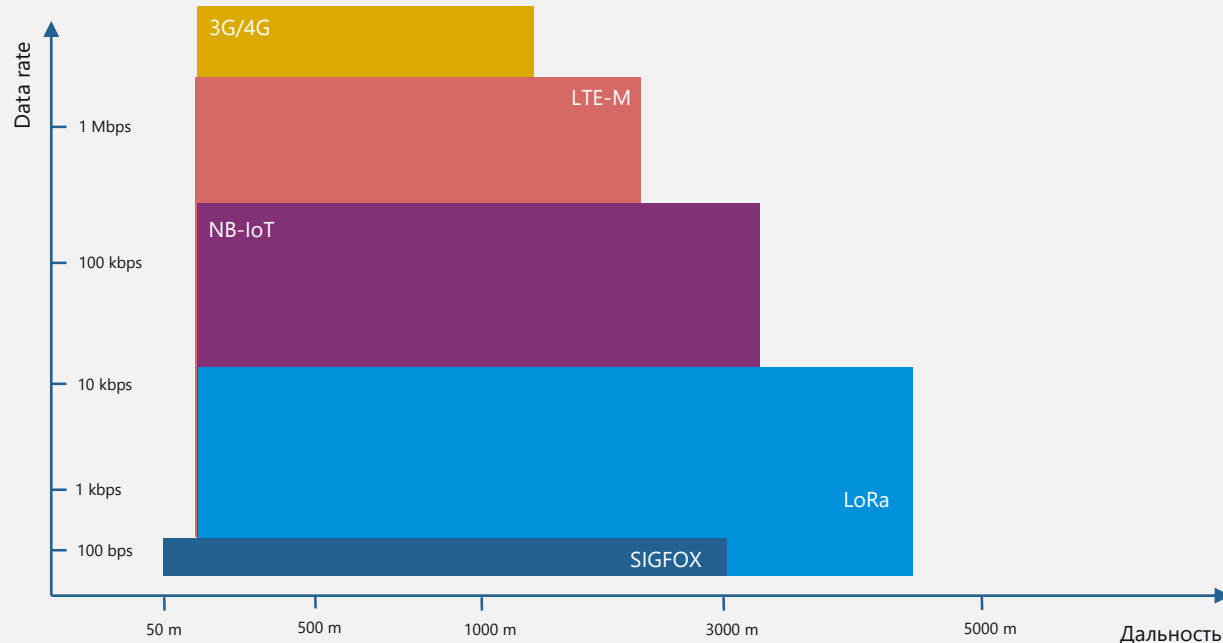
## Почему трудно защищать IIoT?

- Размер пакетов ограничен десятками-сотнями байт
- Низкая пропускная способность
- Высокие требования к энергоэффективности



Почему трудно  
защищать IIoT?

Требования по латентности



Почему трудно защищать LPWAN-сети?

- Малая скорость передачи данных
- Ограниченный объем пакетов
- Высокие требования к энергоэффективности

# Задачи ИБ при защите промышленных протоколов и IIoT



1. Конфиденциальность
2. Целостность
3. Доступность



1. Доступность
2. Целостность
3. Аутентичность
4. Конфиденциальность

# Резюме по проблеме защиты промышленных протоколов и IIoT



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



Что? Что такое криптографический  
протокол CRISP?



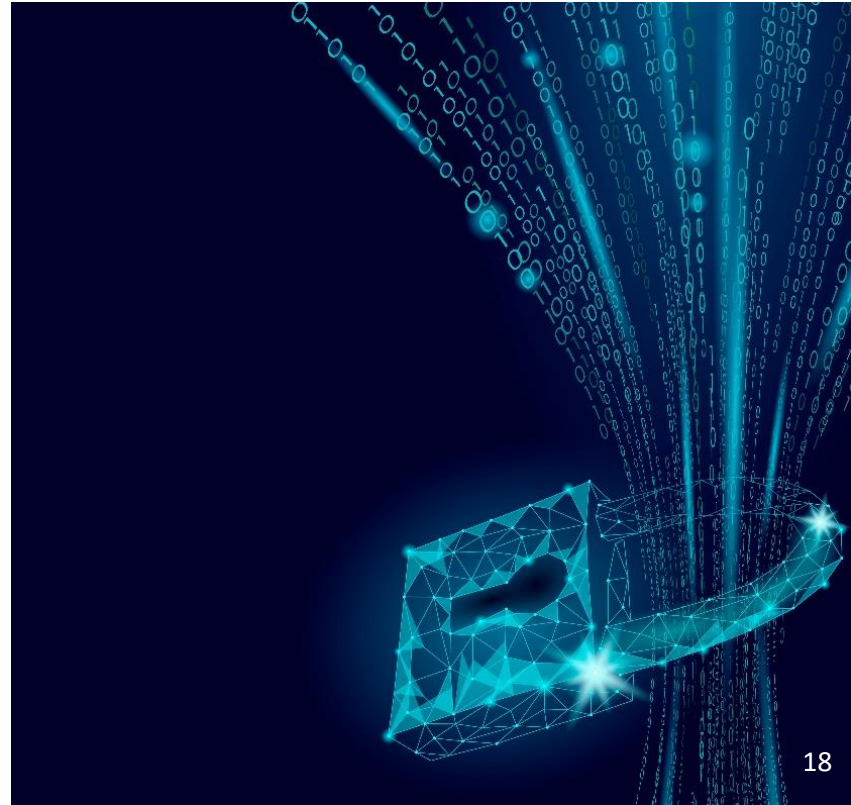
## Основные постулаты при разработке CRISP

1. Не всегда надежные каналы и серьезные ограничения пропускной способности
  - Отсутствие механизмов установления сессии -> предварительно распределенные ключи
  - Каждое сообщение несет всю необходимую информацию для обработки



# Основные постулаты при разработке CRISP

2. Целостность и аутентичность важнее конфиденциальности
  - Обязательная имитозащита и опциональное шифрование
  - Защита от «чтения назад» не обязательна





### 3. Минимальные накладные расходы

- Адресация абонентов неявная, через протоколы целевой системы
- Все криптографические детали определяются номером криптографического набора

4. Минимальные задержки обработки
  - Только симметричные механизмы
  - На одном производном ключе можно обработать несколько сообщений





Обеспечение целостности

У абонентов общий базовый секретный ключ

Обеспечение конфиденциальности  
(опционально)

Защита данных – блочный шифр, имитовставка

Аутентификация источника  
сообщений

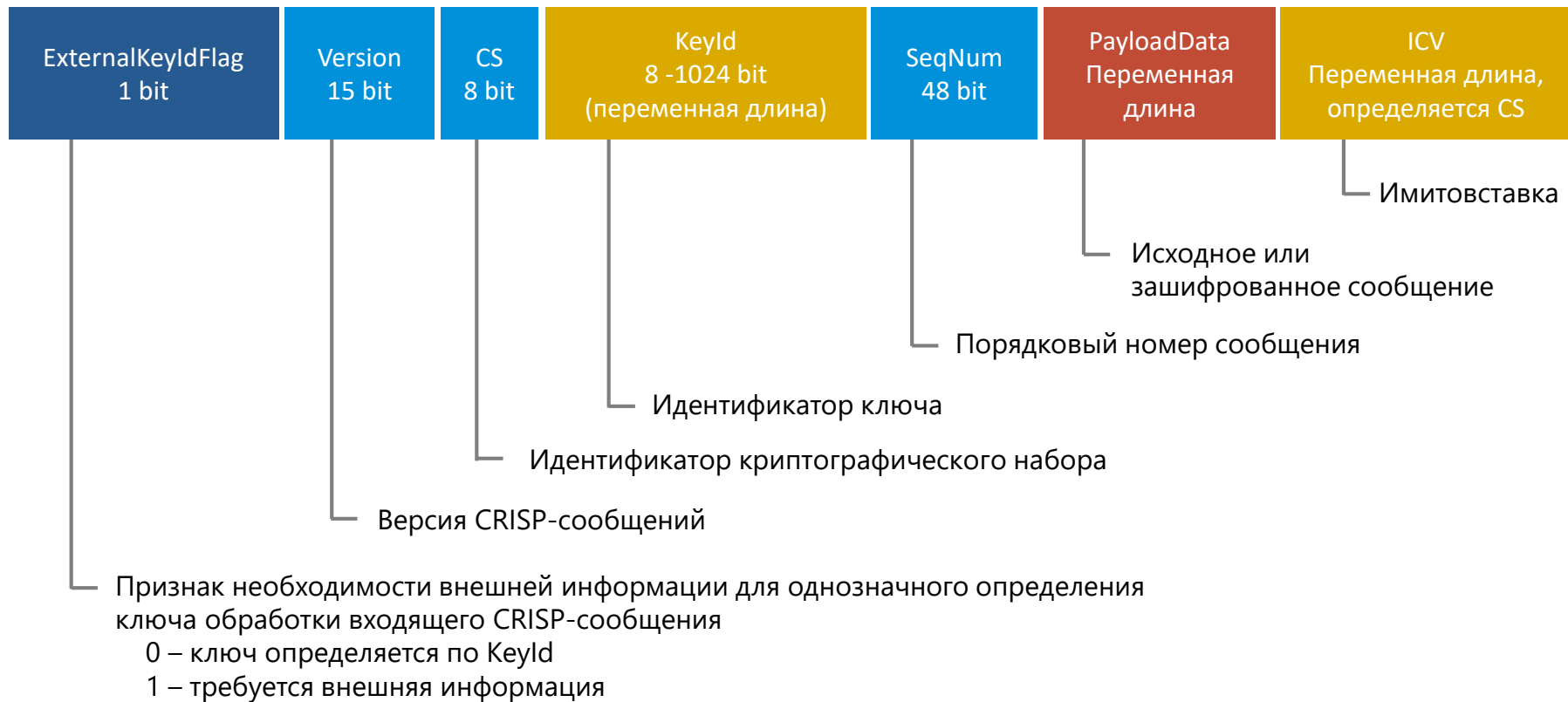
Малый размер добавляемых данных – от 14 байтов

Защита от навязывания  
повторных сообщений

Поддержка адресных сообщений  
(один-к-одному)

Поддержка многоадресных сообщений  
(один-ко-многим)

# Структура CRISP-сообщений



## Криптонабор CS=1

### Целостность и аутентичность

- блочный шифр «Магма» ГОСТ 34.12-2018 в режиме выработки имитовставки по ГОСТ 34.13-2018

### Конфиденциальность

- блочный шифр «Магма» в режиме гаммирования по ГОСТ 34.13-2018

### Диверсификация ключей

- блочный шифр «Магма» в режиме выработки имитовставки
- счетчик сообщений *SequenceNumber*

### Защита от навязывания повторных сообщений

- счетчик сообщений *SequenceNumber* + движущееся окно принятых сообщений
- уникальность значений счетчика в сроки действия одного базового ключа

## Криптонабор CS=2

### Целостность и аутентичность

- блочный шифр «Магма» в режиме выработки имитовставки

### Диверсификация ключей

- блочный шифр «Магма» в режиме выработки имитовставки
- счетчик сообщений *SequenceNumber*

### Защита от навязывания повторных сообщений

- счетчик сообщений *SequenceNumber* + движущееся окно принятых сообщений
- уникальность значений счетчика в сроки действия одного базового ключа



Зачем? Какие преимущества несет в себе протокол CRISP?



# CRISP

C

Минимальный  
размер  
добавляемых  
данных

R

Обеспечение  
минимальных  
задержек

I

Работа  
на плохих  
каналах связи

S

Высокая  
энергоэффе-  
ктивность

P

Отсутствие  
влияния  
на доступность

# Возможные альтернативы CRISP

Рекомендованы ТК26:

- TLS
- CMS
- МР 26.4.003-2019 «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств»

Находятся в стадии рассмотрения:

- IPSec (IKEv2, ESP)
- Iplir
- DLMS

# CRISP vs TLS

Параметр	CRISP	TLS
Универсальность	Да	Защита TCP
Защита от повторов	Да	Да
Установление сессии	Нет	Да
Установка общего ключа	За рамками протокола	Определяется протоколом
Размер добавляемых данных	От 14 байт	От 8 байт (для передачи прикладных данных)
Использование асимметричных алгоритмов	Нет	Да
Поддержка многоадресных сообщений	Да	Нет
Необходимость гарантированной доставки сообщений	Не требуется	Требуется
Максимальный размер сообщения	2034 байт	16384 байт

# CRISP vs CMS

Параметр	CRISP	CMS
Универсальность	Да	Да
Защита от повторов	Да	Нет
Установление сессии	Нет	Нет
Установка общего ключа	За рамками протокола	Определяется протоколом
Размер добавляемых данных	От 14 байт	Больше 200 байт
Использование асимметричных алгоритмов	Нет	Да
Поддержка многоадресных сообщений	Да	Да однако размер сообщения существенно увеличивается
Необходимость гарантированной доставки сообщений	Не требуется	Не требуется
Максимальный размер сообщения	2034 байт	Любой

# CRISP vs MP 26.4.003-2019

Параметр	CRISP	MP 26.4.003-2019
Универсальность	Да	Да
Защита от повторов	Да	Нет
Установление сессии	Нет	Да
Установка общего ключа	За рамками протокола	Определяется протоколом
Размер добавляемых данных	От 14 байт	От 20 байт (для передачи прикладных данных)
Использование асимметричных алгоритмов	Нет	Да
Поддержка многоадресных сообщений	Да	Нет
Необходимость гарантированной доставки сообщений	Не требуется	Не требуется
Максимальный размер сообщения	2034 байт	16384 байт

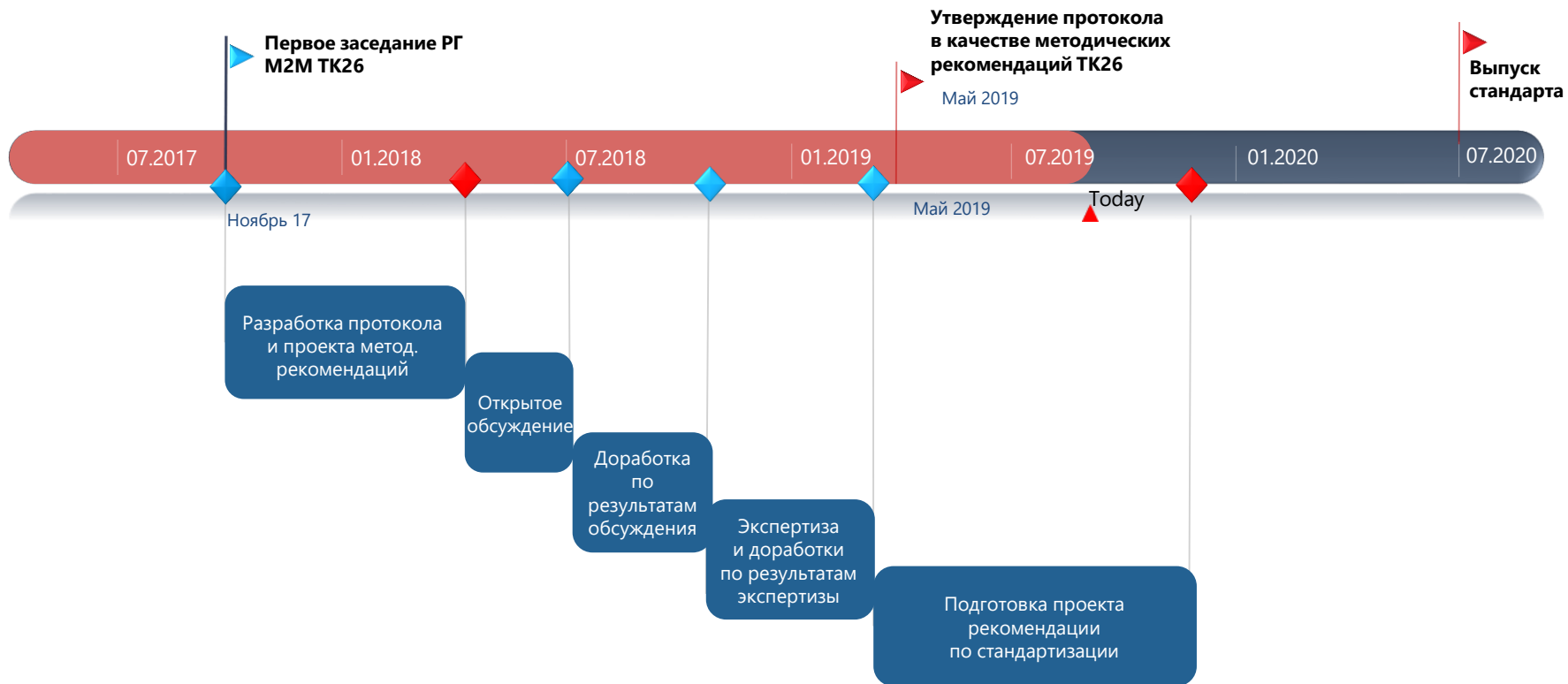
# Потенциальные альтернативы CRISP

- IPSec (IKEv2, ESP)
  - Iplir
- } предназначены для защиты IP трафика (IKEv2 использует в качестве транспорта UDP или TCP)
- DLMS
- проект методических рекомендаций описывает применение отечественных криптографических алгоритмов, но не описывает сам протокол, который не является общедоступным
- DLMS/COSEM – прикладной протокол, разработанный для электроэнергетики



Где? На каком этапе работ  
находится протокол CRISP?

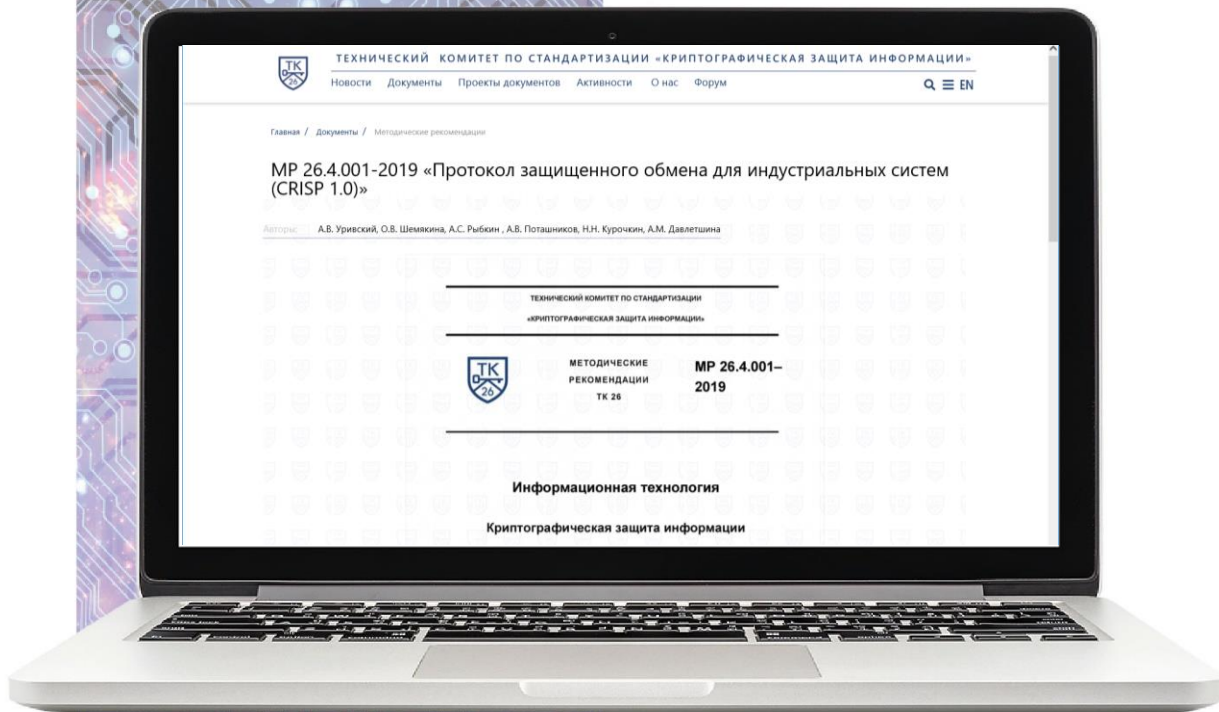
# Дорожная карта





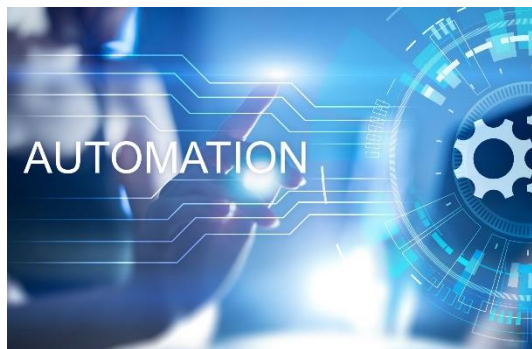
## Текущий статус

Криптографический протокол CRISP – методическая рекомендация Технического комитета по стандартизации «Криптографическая защита информации» (TK26) ([www.tc26.ru](http://www.tc26.ru))

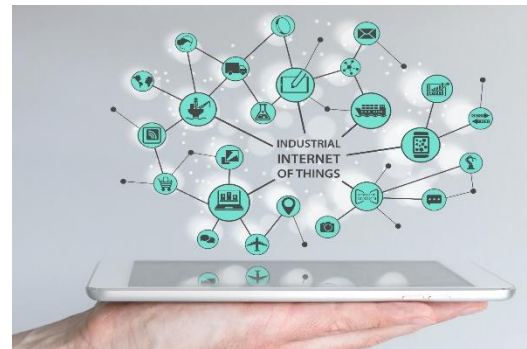




# Протоколы, которые можно защищать с помощью CRISP



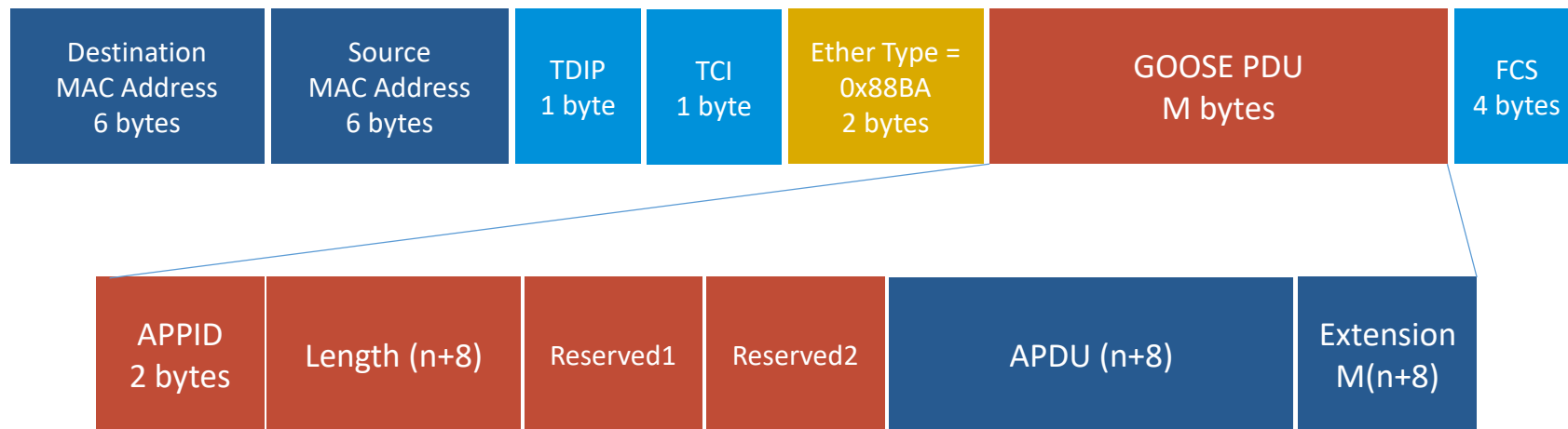
1. МЭК 60870-5-101, МЭК 60870-5-104, МЭК 60870-5-103
2. Modbus TCP, Modbus RTU
3. GOOSE, SV
4. И другие ...



1. LoRaWAN
2. NB-IoT
3. MQTT
4. И другие...

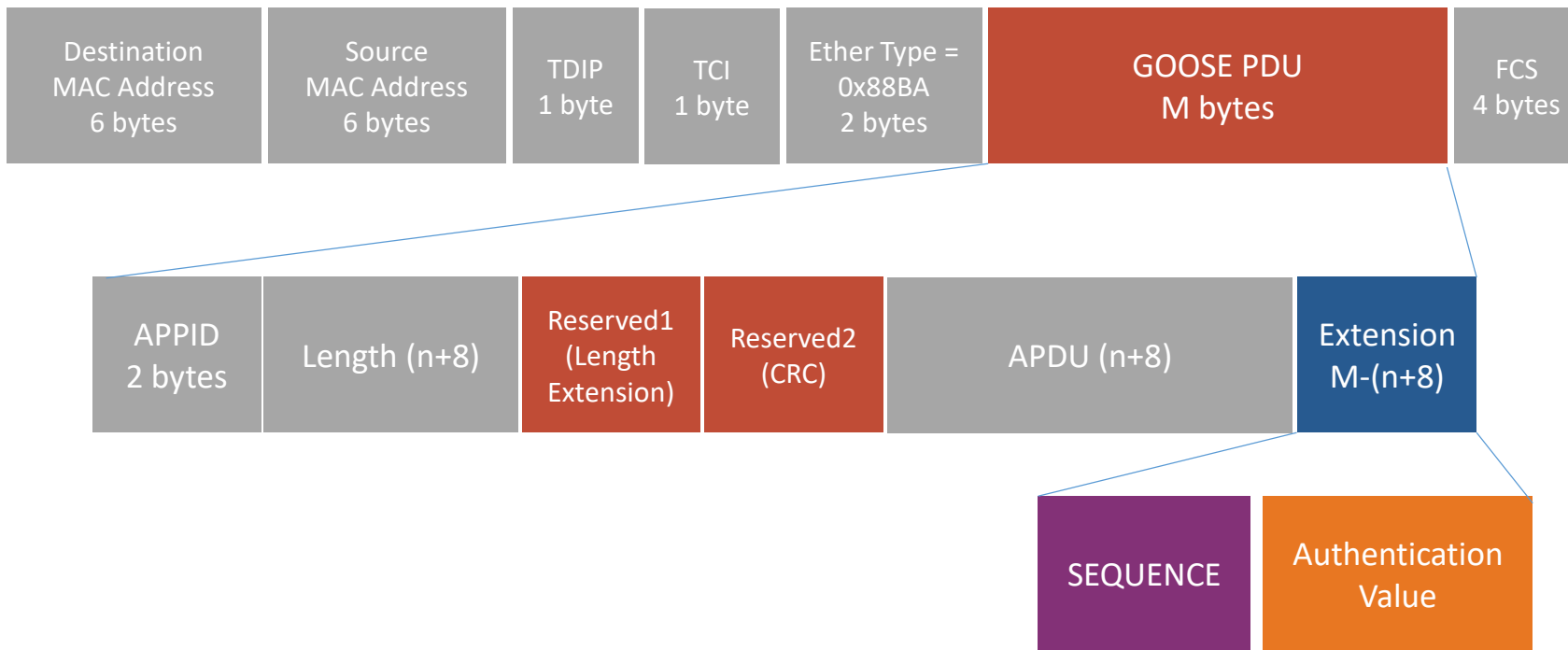
# Пример использования CRISP в протоколе GOOSE

## Стандартное GOOSE-сообщение

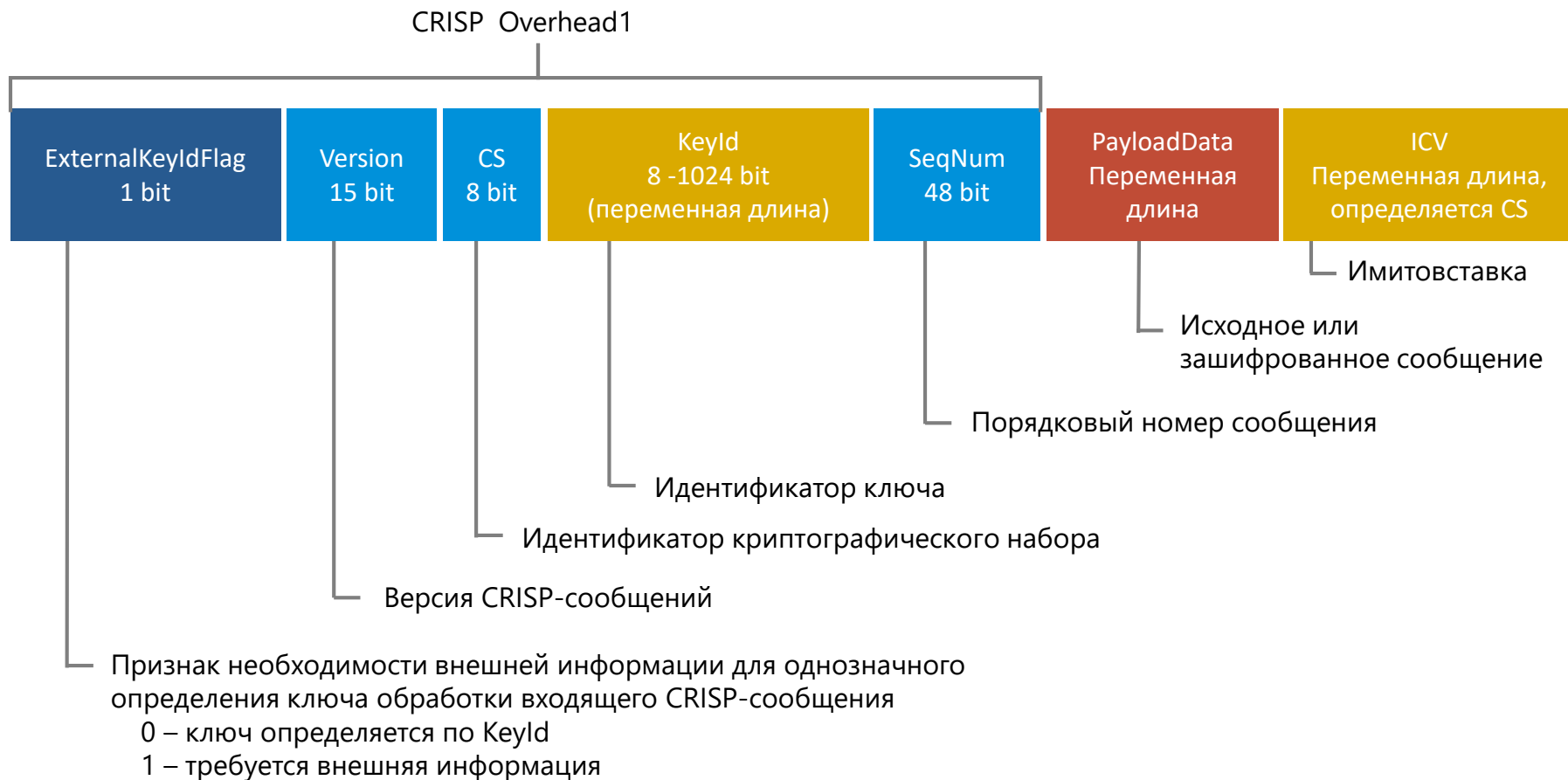


# Пример использования CRISP в протоколе GOOSE

## Защищенное GOOSE-сообщение согласно IEC 62351

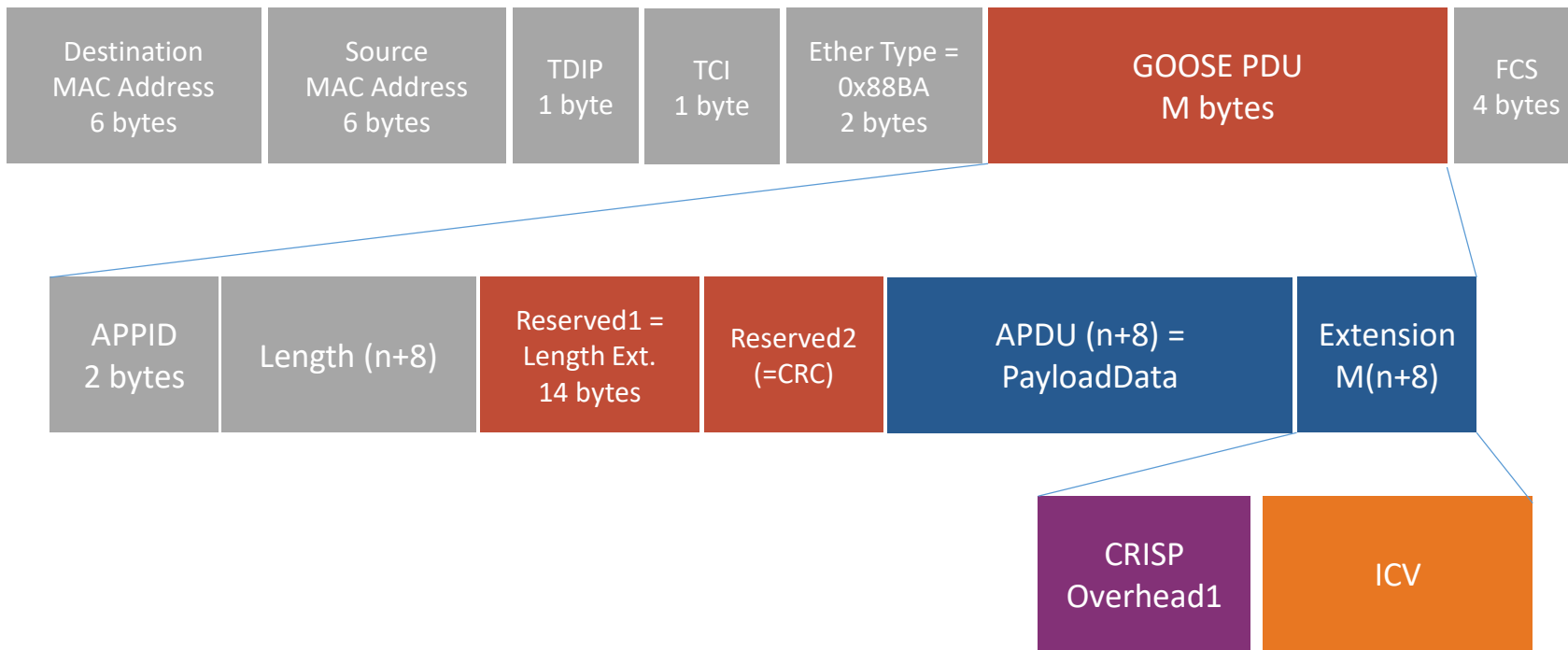


# Структура CRISP-сообщений



# Пример использования CRISP в протоколе GOOSE

## Защищенное GOOSE-сообщение с CRISP



# Как попробовать CRISP?

## Решение ViPNet SIES –

встраиваемые криптографические средства защиты информации, в которых уже реализован CRISP:

- для устройств автоматизации на всех уровнях АСУ
- для M2M-устройств
- для IIoT-устройств



SECURITY FOR  
INDUSTRIAL AND  
EMBEDDED SOLUTIONS





# Состав решения



- Законченные СКЗИ класса КС1 и КС3, не требуют проведения корректности встраивания
- Возможность использования криптографии на разных по вычислительной мощности устройствах
- Нет зависимости от ОС и архитектуры устройств

ЗАЩИЩАЕМОЕ УСТРОЙСТВО  
(ПЛК, УСО, ДАТЧИК, ...)



## Интеграция ПАК SIES Core

На аппаратном уровне – USB, UART

На программном уровне – SIES API  
(RATP+прикладной протокол)

# Интеграция ПО ViPNet SIES Unit

ЗАЩИЩАЕМОЕ УСТРОЙСТВО  
(SCADA, ОРС-СЕРВЕР, АРМ ОПЕРАТОРА,  
АРМ ИНЖЕНЕРА,...)



## Поддерживаемые ОС:

- Windows (32/64-разрядные) 7/8/8.1/10
- Windows Server 2008 K2/2012/2012 K2/ 2016

Протокол/ Операции	UART (115200-8-E1)		USB	
	Среднее время выполнения операции (мс)	Средняя скорость (Кбит/с)	Среднее время выполнения операции (мс)	Средняя скорость (Кбит/с)
Зашифрование	250	32,7	18	453,4
Расшифрование	252	32,4	27	302,5
Создание имитовставки	137	59,7	12	651,9
Проверка имитовставки	154	52,9	16	511,4

## Производительность CRISP на SIES Core

- Все замеры сделаны для размера сообщения в 1024 байт;
- Все замеры сделаны на ОС Linux с помощью SIES Linux SDK



Спасибо  
за внимание!