Новый национальный стандарт: криптографический протокол CRISP для АСУ ТП, IIoT и ИСУЭ

Марина Сорокина
Руководитель направления

infotecs

Новый национальный стандарт

ГОСТ Р 71252–2024
«Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем»

Вступает в силу 1 апреля 2024 года

ГОСТ Р 71252–2024. Криптографический протокол CRISP

Разработан в рамках ТК26

Основан на рекомендаций по стандартизации
Р 1323565.1.029–2019

Дата разработки 2017-2018 гг.

Проходил рассмотрение в ТК016 «Электроэнергетика», ТК023 «Нефтяная и газовая промышленность», ТК362 «Защита информации»

ГОСТ Р 71252–2024. Криптографический протокол CRISP

Предназначен для защиты данных в:

АСУ ТП / АСУ ОКИИ

IIoT-системах

M2M-системах

ИСУЭ

ГОСТ Р 71252-2024. Криптографический протокол CRISP

- Обеспечение целостности
- Обеспечение конфиденциальности (опционально)
- Аутентичность (Общий секретный ключ)
- Защита от навязывания повторных сообщений (Окно принятых сообщений)

IT/Web

1. Конфиденциальность
2. Целостность
3. Доступность

Industry

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

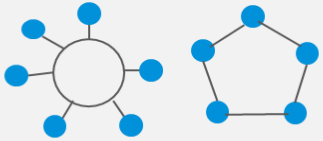
ГОСТ Р 71252-2024. Криптографический протокол CRISP

infotecs

Поддержка адресных сообщений (один-к-одному)

Общая шина

Кольцо



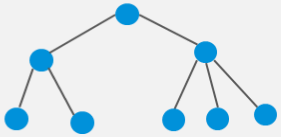
Звезда

Звезда-Иерархия

Поддержка многоадресных сообщений (один-ко-многим, подписочная модель)

Полносвязная

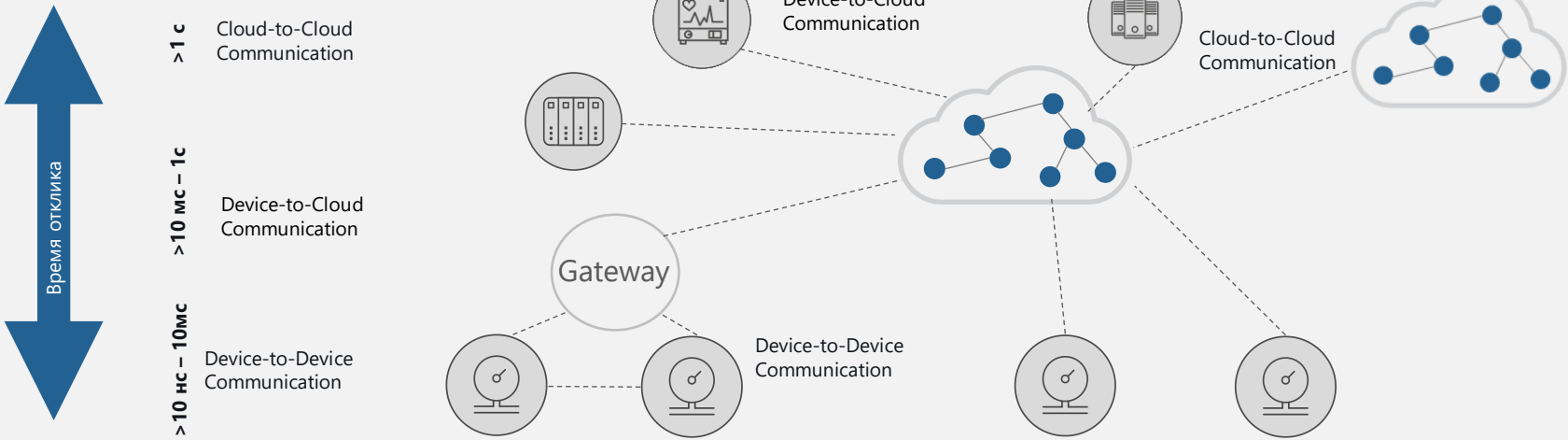
Дерево



Модель взаимодействия

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

ГОСТ Р 71252-2024. Криптографический протокол CRISP

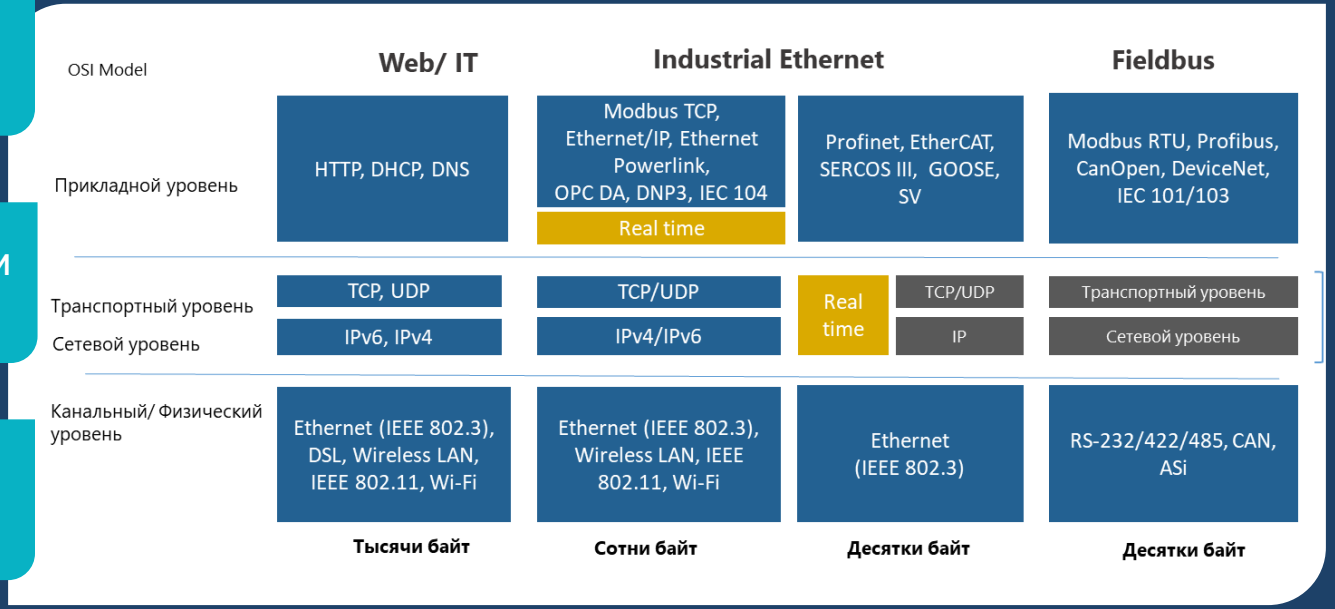


Бессессионный криптографический протокол

- Плохие каналы связи
- Real-time
- Однонаправленная передача данных

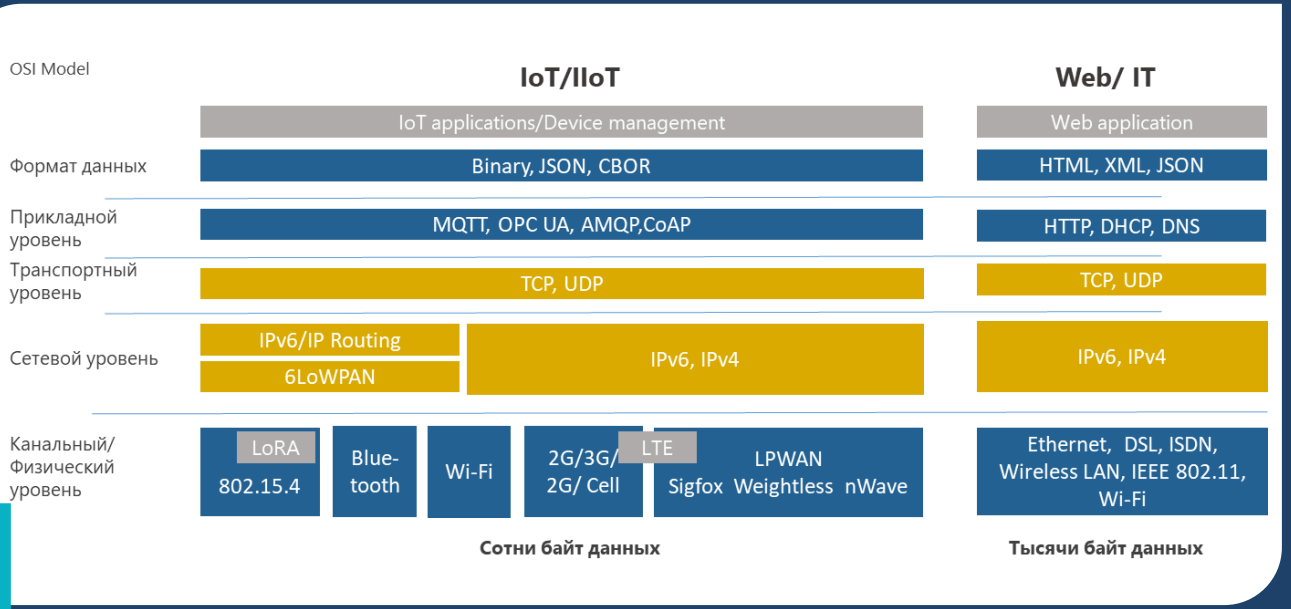
ГОСТ Р 71252-2024. Криптографический протокол CRISP

- Минимальные накладные расходы
- Минимальные задержки на обработку
- Явная и неявная адресация абонентов



ГОСТ Р 71252-2024. Криптографический протокол CRISP

- Минимальные накладные расходы
- Минимальные задержки на обработку
- Явная и неявная адресация абонентов
- Независимость от интерфейсов и протоколов передачи данных



ГОСТ Р 71252–2024. Криптонаборы

Криптонабор CS=1

Целостность и аутентичность
- блочный шифр «Магма» ГОСТ 34.12-2018 в режиме выработки имитовставки по ГОСТ 34.13-2018
- Имитовставка 4 байта

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» ГОСТ 34.12-2018 в режиме выработки имитовставки по ГОСТ 34.13-2018
- Имитовставка 4 байта

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

ГОСТ Р 71252–2024. Криптонаборы

Криптонабор CS=3

Целостность и аутентичность
- блочный шифр «Магма» ГОСТ 34.12-2018 в режиме выработки имитовставки по ГОСТ 34.13-2018
- Имитовставка 8 байт

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

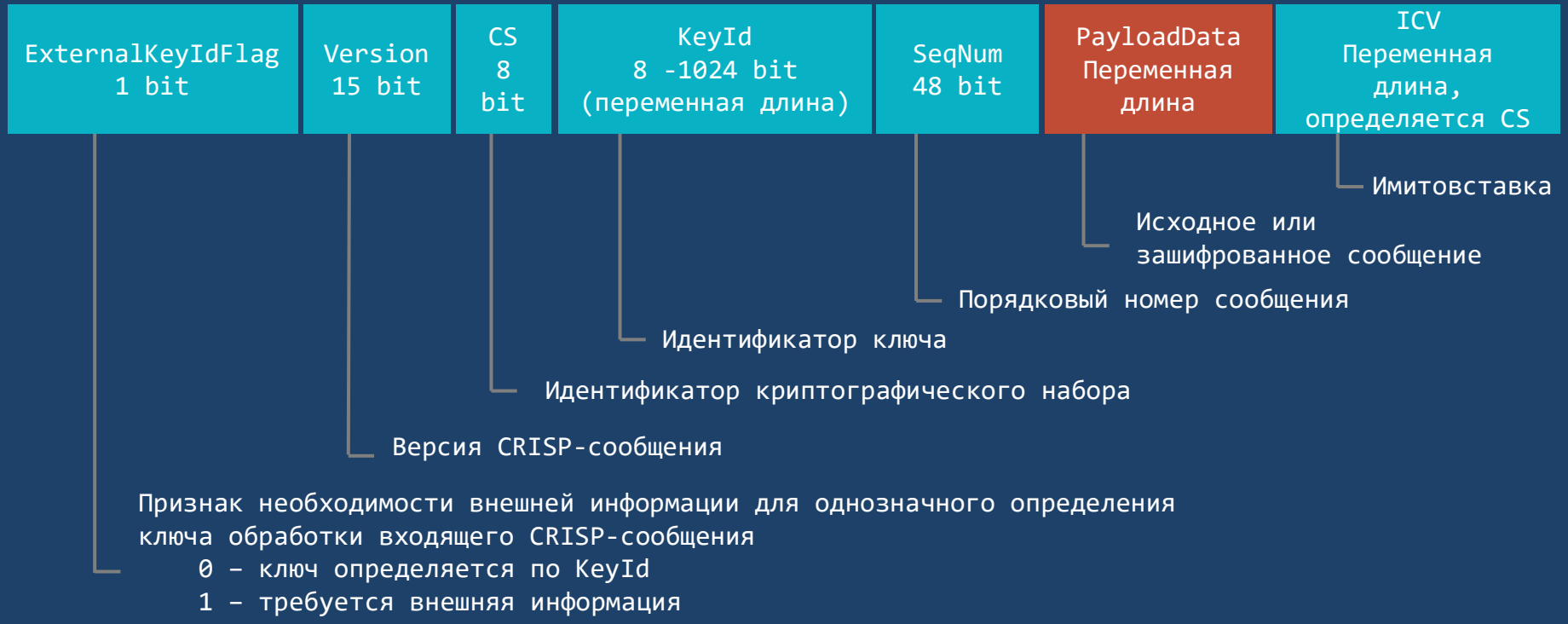
Криптонабор CS=4

Целостность и аутентичность
- блочный шифр «Магма» ГОСТ 34.12-2018 в режиме выработки имитовставки по ГОСТ 34.13-2018
- Имитовставка 8 байта

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

Структура CRISP-сообщения

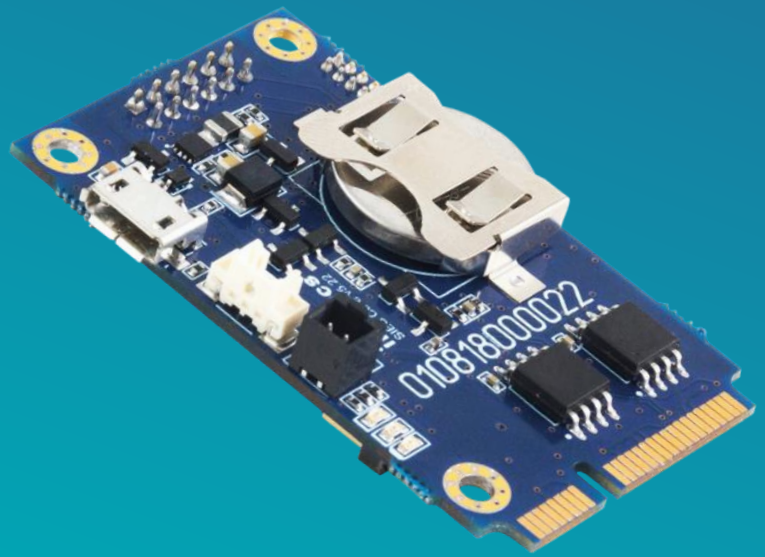


ГОСТ Р 71252-2024. Криптографический протокол CRISP

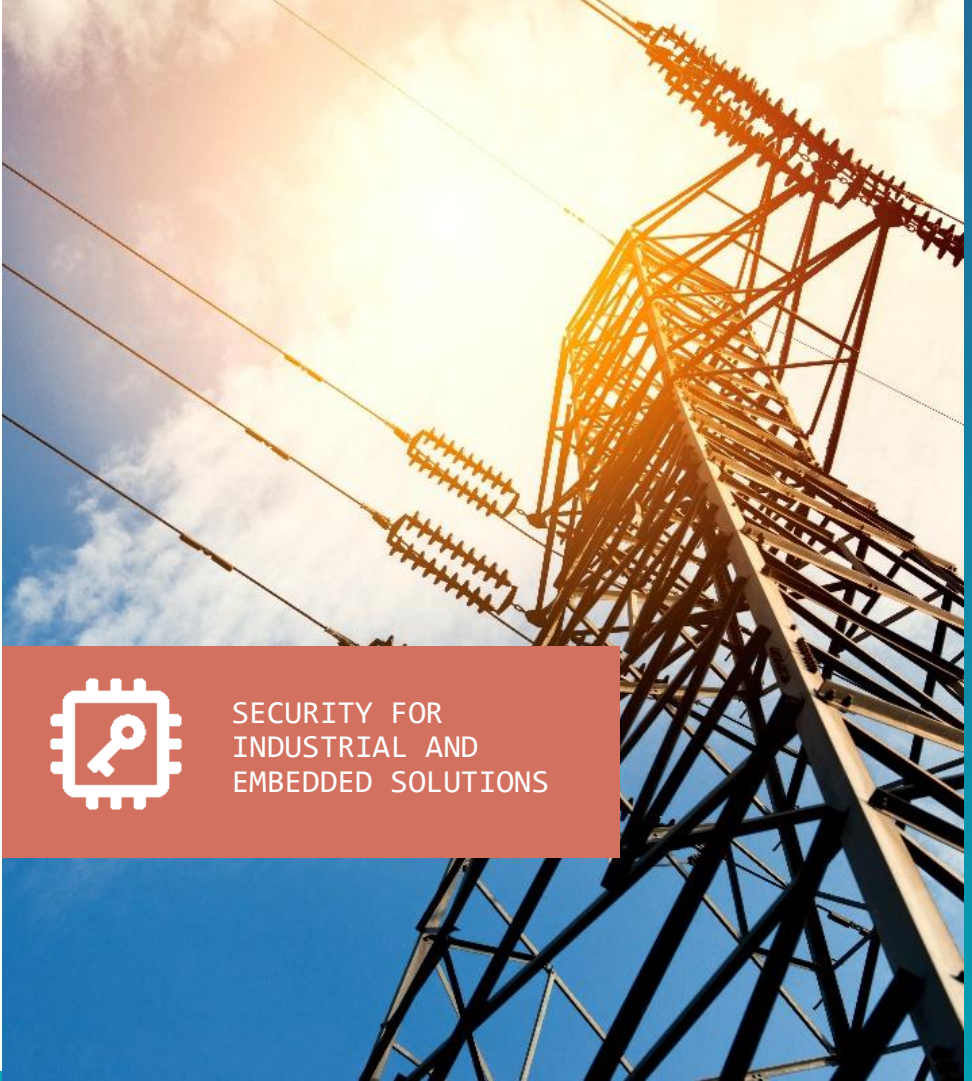
C	R	I	S	P
Минимальный размер добавляемых данных	Обеспечение минимальных задержек	Работа на плохих каналах связи	Высокая энергоэффек-тивность	Универсальность

Пример: Защита протоколов и интерфейсов в ИСУЭ

Протокол	Тип протокола	Интерфейс	Уровни использования	Способ защиты
СПОДЭС	Прикладной протокол	GSM, PLC, Ethernet, RS-485	ПУ - УСПД (ИВКЭ) ПУ - ИВК	Защита DLMS **CRISP**
СПОДУС	Прикладной протокол	GSM, Ethernet	УСПД (ИВКЭ) – ИВК	Защита DLMS **CRISP** Любой VPN (УСПД-ИВК)
ПИРС	Транспортный протокол (+ прикладной протокол реализуется каждым производителем самостоятельно)	Любой, но по факту ZigBee, GSM, Ethernet	Радиомодем ПУ - ИВК Радиомодем ПУ – УСПД (ИВКЭ) УСПД (ИВКЭ) - ИВК	**CRISP**
NB-Fi	Транспортный протокол + прикладной протокол	NB-Fi	Радиомодем ПУ - ИВК	Собственный механизм **CRISP**
LoRAWAN	Транспортный протокол (+ прикладной протокол реализуется каждым производителем самостоятельно)	LoRAWAN	Радиомодем ПУ - ИВК	**CRISP**
XNB	Транспортный протокол + прикладной	XNB	Радиомодем ПУ - ИВК	**CRISP**



Криптографический протокол CRISP реализован в решении ViPNet SIES



SECURITY FOR
INDUSTRIAL AND
EMBEDDED SOLUTIONS

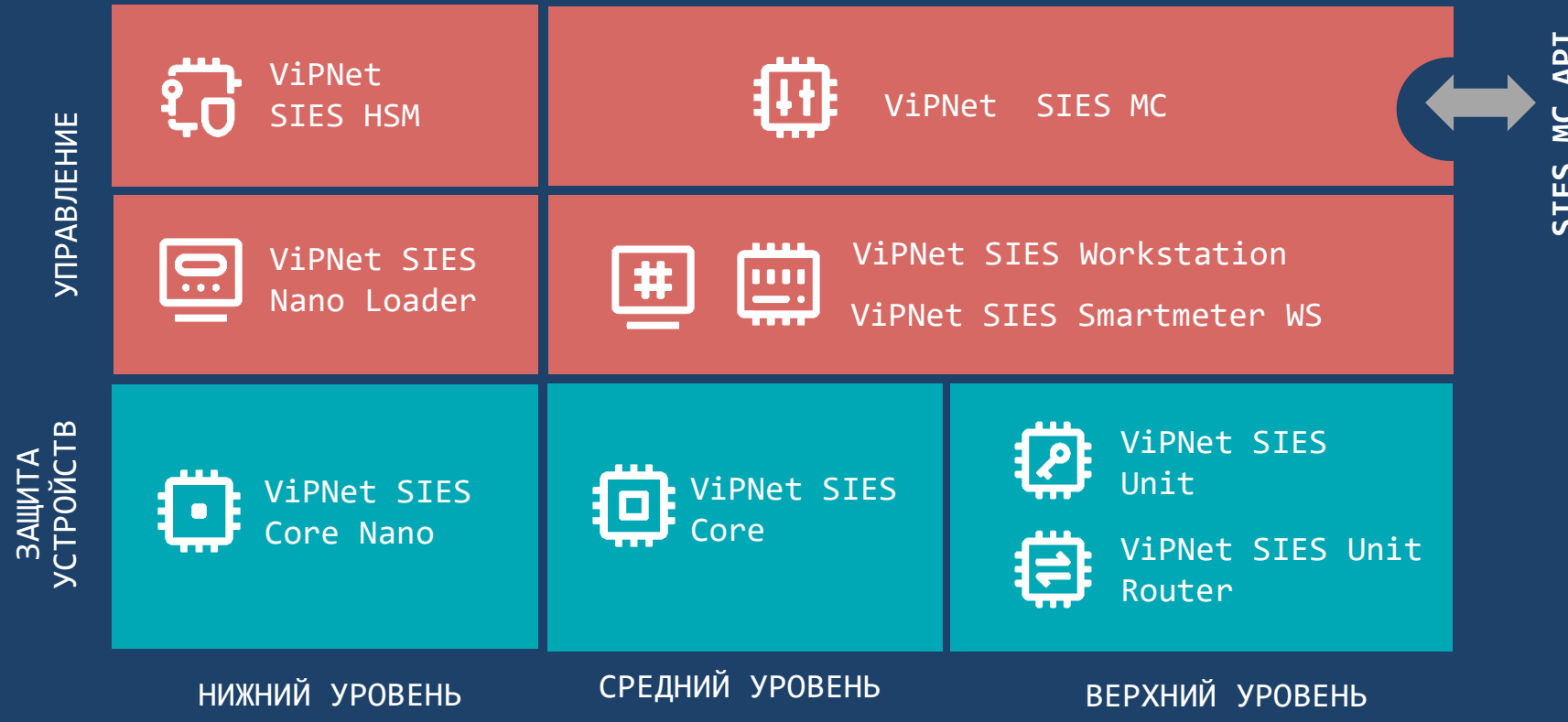
infotecs

Решение ViPNet SIES

Встраиваемые криптографические средства защиты информации:

- для устройств автоматизации на всех уровнях АСУ
- для M2M-устройств
- для АСКУЭ/ИСУЭ
- для IIoT-устройств

Состав решения ViPNet SIES



infotecs

Демонстрация использования протокола CRISP в IIoT и ИСУЭ

> Стенд 6.4 ИнфоТеКС

Спасибо за внимание!

Марина Сорокина

Marina.Sorokina@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363