

техно infotecs  
2019 Фест

ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

12  
09 2019

Обзор продуктов  
решения  
ViPNet SIES



Решение ViPNet SIES

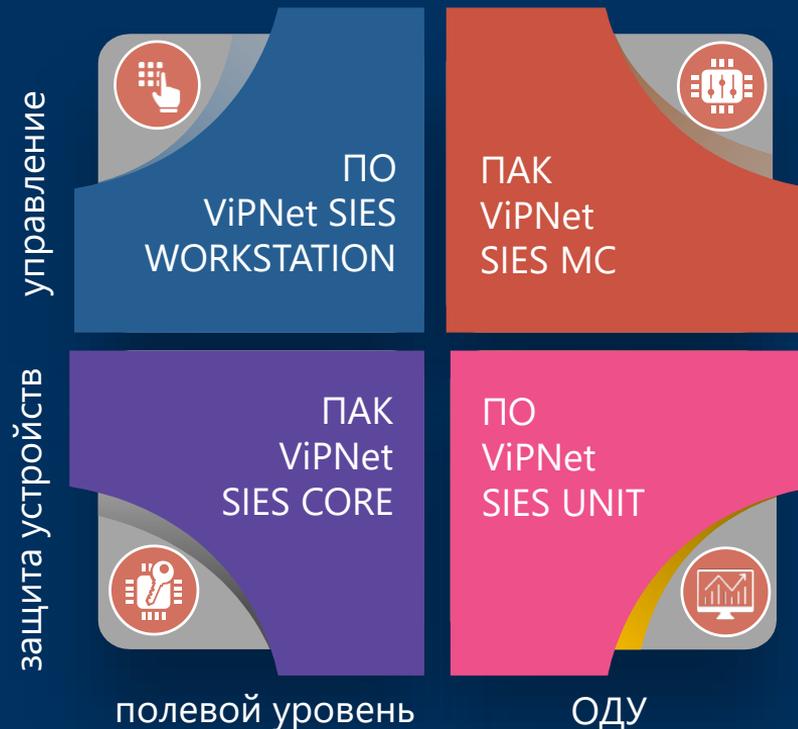


ВСТРАИВАЕМЫЕ КРИПТОГРАФИЧЕСКИЕ  
СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ  
ИНТЕГРАЦИИ В УСТРОЙСТВА  
АВТОМАТИЗАЦИИ НА ВСЕХ УРОВНЯХ АСУ

ЗАЩИТА КОММУНИКАЦИЙ • ЗАЩИТА КОНЕЧНЫХ УЗЛОВ • ЗАЩИТА ДАННЫХ • АУТЕНТИФИКАЦИЯ И ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

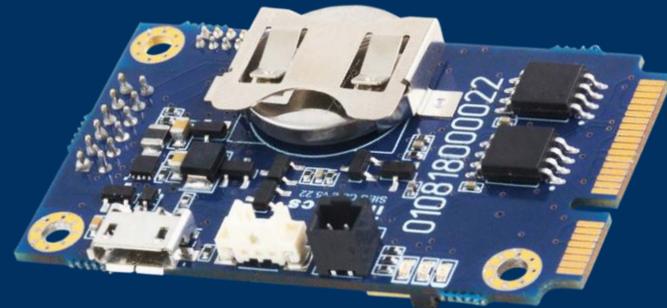


# Состав решения ViPNet SIES



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

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



На аппаратном уровне – USB, UART

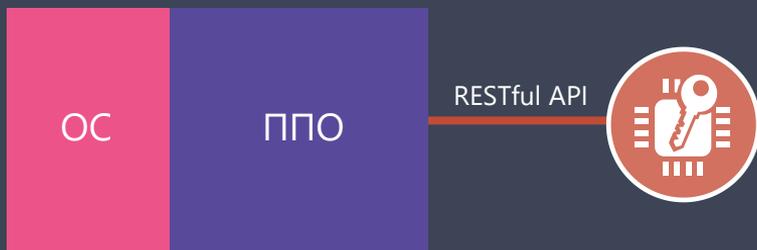
На программном уровне – SIES Core API  
(RATP+прикладной протокол)

Интеграция ПАК SIES Core



# Интеграция ПО ViPNet SIES Unit

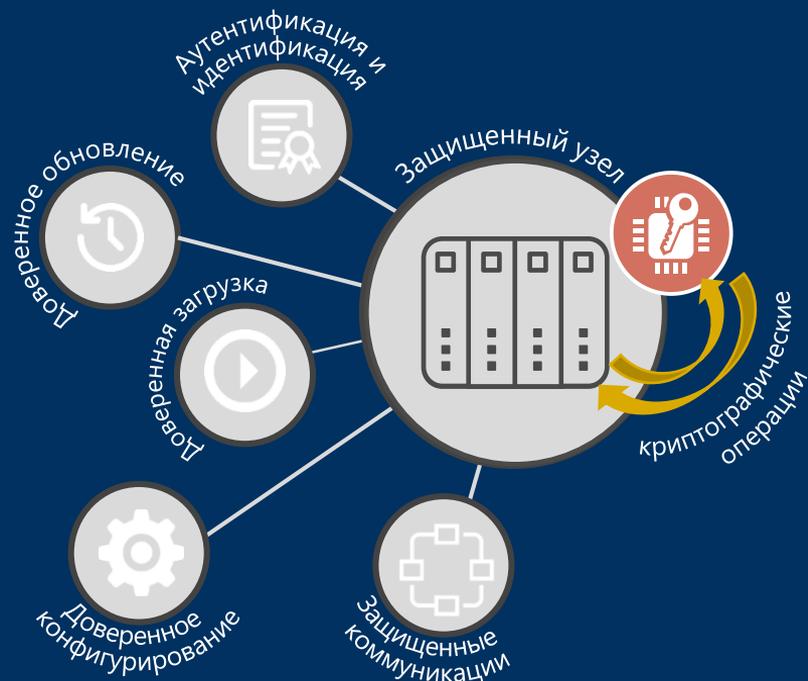
ЗАЩИЩАЕМОЕ УСТРОЙСТВО  
(SCADA, ОРС-СЕРВЕР, АРМ ОПЕРАТОРА,  
АРМ ИНЖЕНЕРА,...)



## Поддерживаемые ОС:

- Windows (32/64-разрядные) 7/8/8.1/10
- Windows Server 2008 R2/2012/  
2012 R2/ 2016

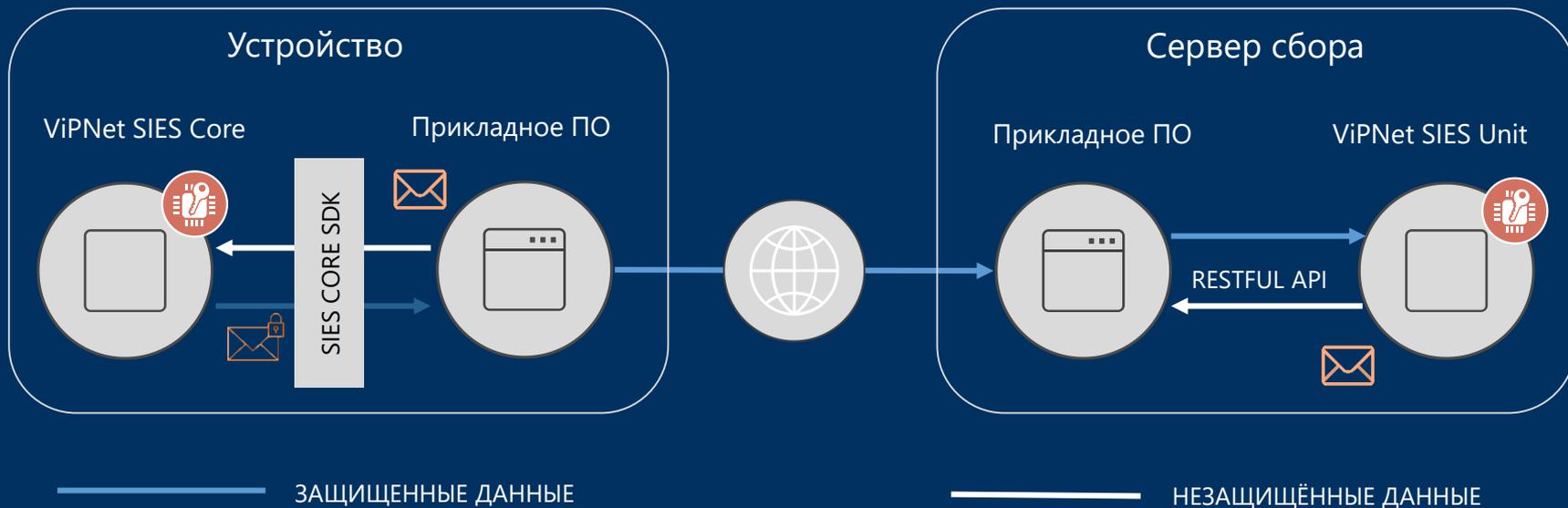
# Криптографические сервисы для защищаемых устройств



Сценарии защиты информации:

- Обеспечение конфиденциальности передаваемых данных
- Обеспечение аутентичности и целостности передаваемых данных
- Доверенное локальное и удаленное обновление ПО устройства
- Доверенное локальное и удаленное конфигурирование устройства
- Доверенная загрузка устройства
- Двухфакторная аутентификация на устройстве

# Защита коммуникаций с помощью ViPNet SIES



# Доверенное обновление контроллера с помощью ViPNet SIES



ГОСТ 28147-89



Вычисление хэш  
и проверка хэш



ГОСТ Р 34.11-2012  
ГОСТ 34.11-2018

Зашифрование и  
расшифрование  
в CMS

Зашифрование и  
расшифрование  
(CRISP)



ГОСТ Р 34.12-2015  
ГОСТ Р 34.13-2015  
ГОСТ 34.12-2018  
ГОСТ 34.13-2018



Создание ЭП и  
проверка ЭП в  
CMS

Создание  
имитовставки и  
проверка  
имитовставки  
(CRISP)

ГОСТ Р 34.10-2012  
ГОСТ 34.10-2018



Криптографические  
операции, доступные  
защищаемым  
устройствам



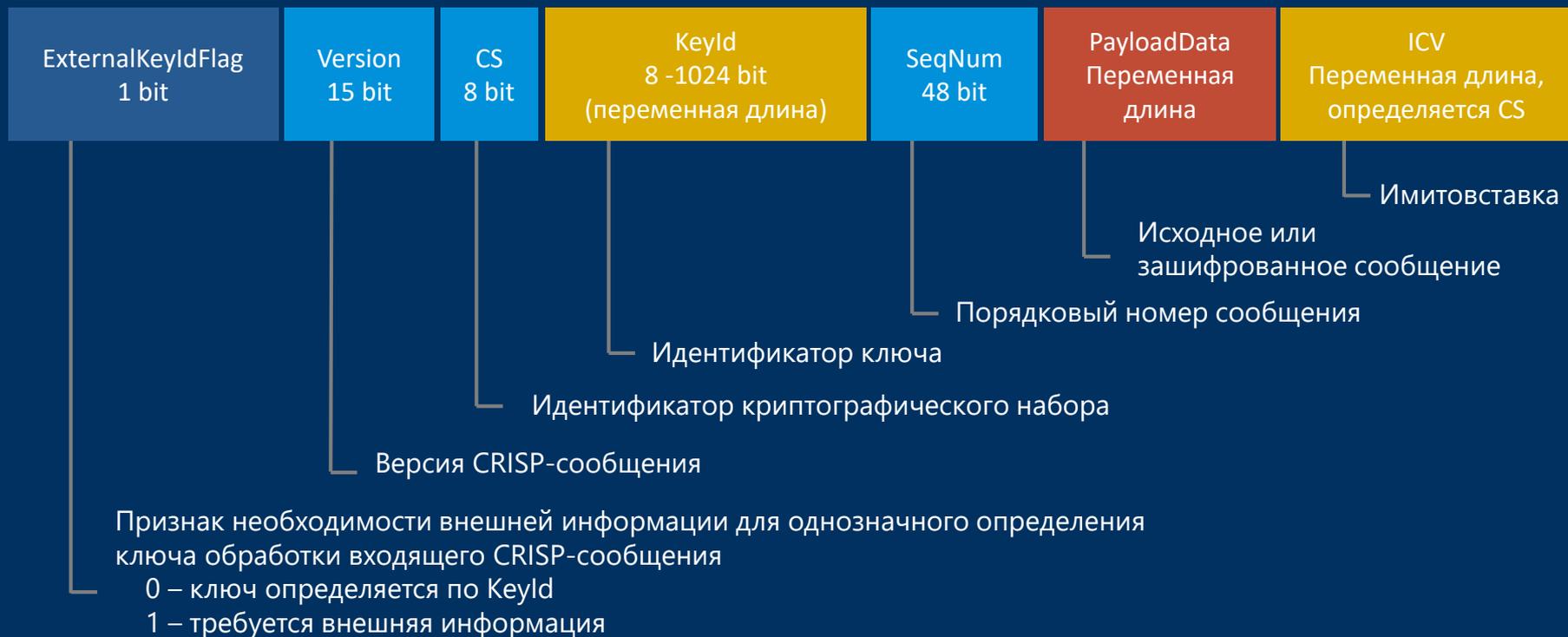


Cryptographic Industrial Security Protocol  
- неинтерактивный протокол защищенной  
передачи данных для промышленных систем,  
M2M и IIoT коммуникаций

- Обеспечение целостности
- Обеспечение конфиденциальности (опционально)
- Защита от навязывания повторных сообщений
- Окно принятых сообщений

- Общий секретный ключ
- Защита данных – блочный шифр, имитовставка
- Поддержка адресных (один-к-одному) сообщений
- Поддержка многоадресных (один-ко-многим, подписочная модель) сообщений
- Явная и неявная адресация абонентов

# Структура CRISP-сообщения



# CRISP: механизмы защиты

## 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



## C

---

Минимальный  
размер  
добавляемых  
данных

## R

---

Обеспечение  
минимальных  
задержек

## I

---

Работа  
на плохих  
каналах связи

## S

---

Высокая  
энергоэффе-  
ктивность

## P

---

Отсутствие  
влияния  
на доступность



# Какие промышленные протоколы можно защищать с помощью CRISP?

CRISP – Методические рекомендации Технического комитета по стандартизации «Криптографическая защита информации» (TK26)

IIoT – протоколы:

- NB-IoT
- LoRaWan
- MQTT



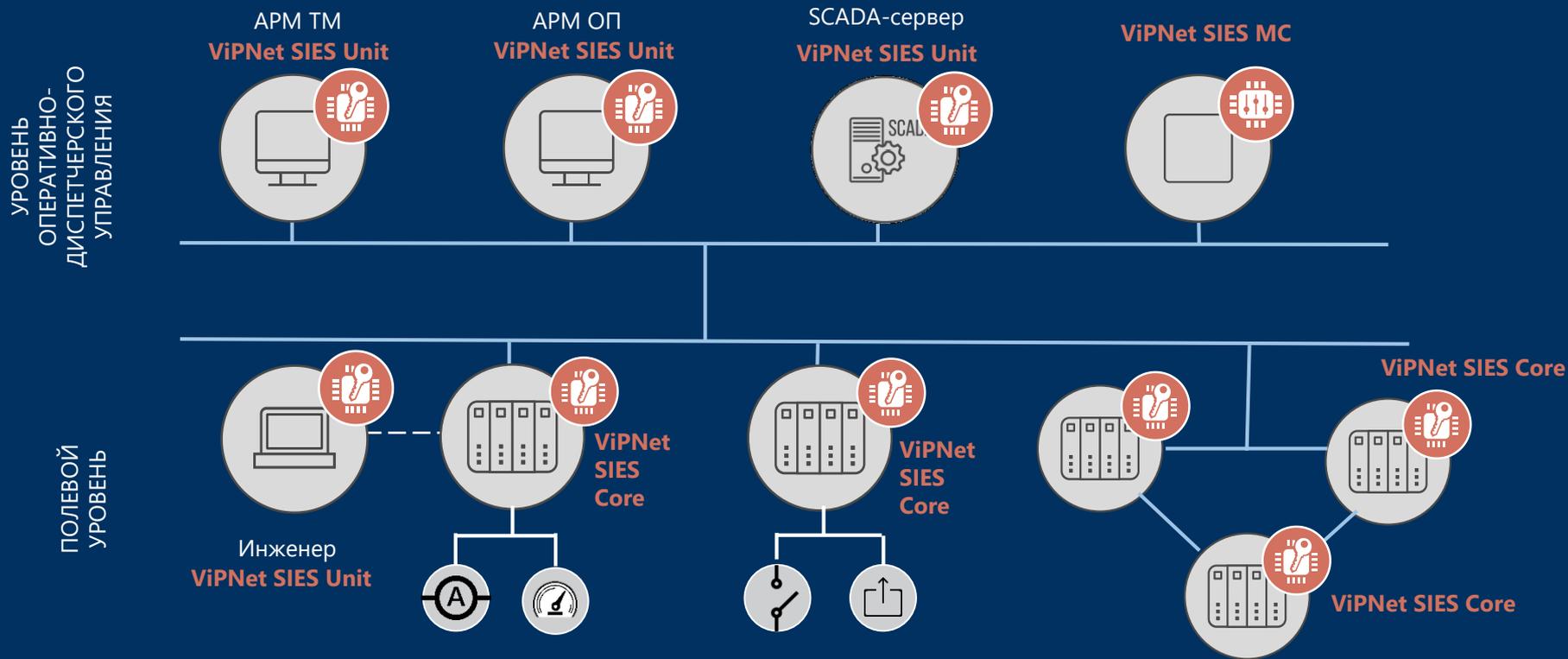
Industrial Ethernet:

- МЭК 60870-5-104
- Modbus TCP
- GOOSE

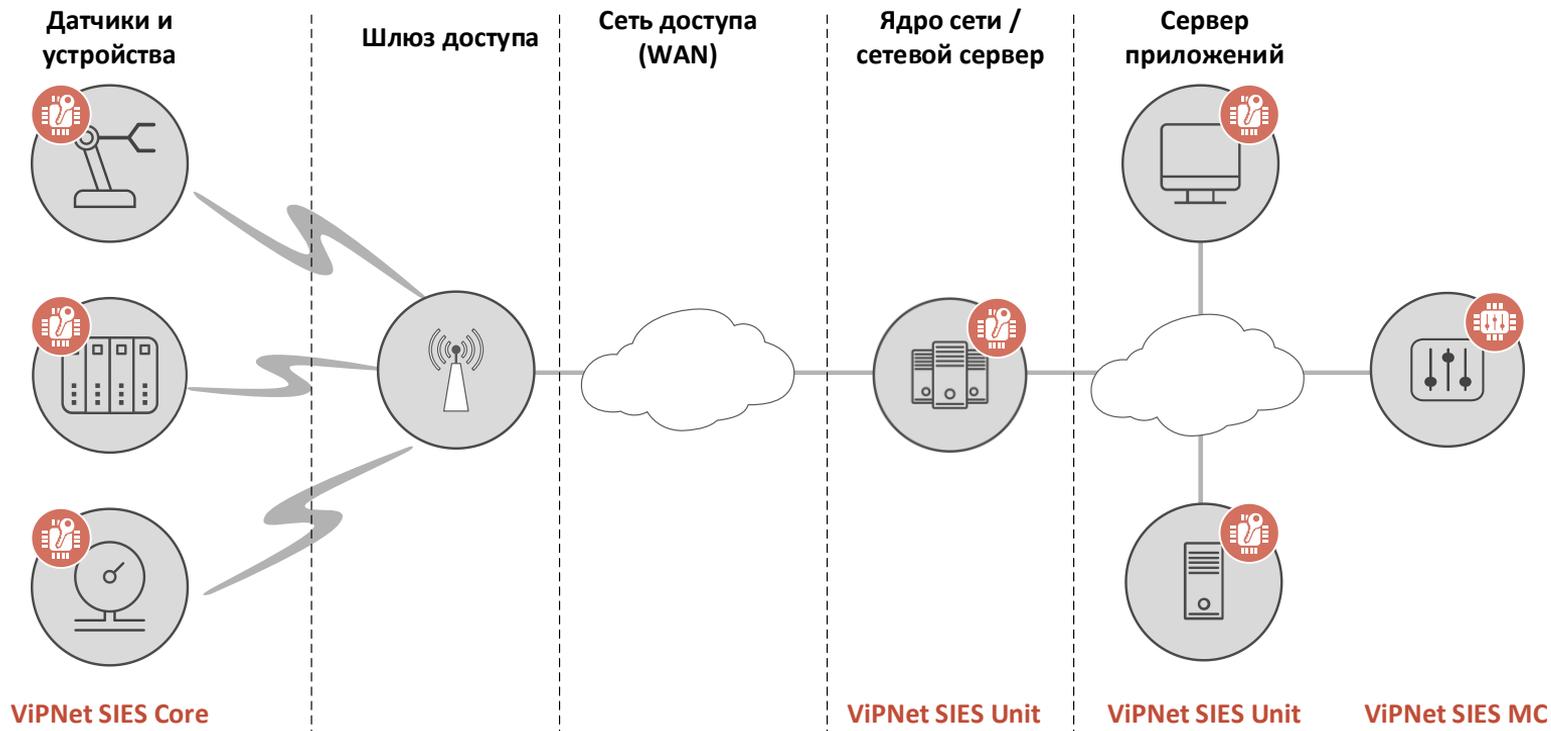
Fieldbus:

- МЭК 60870-5-101
- Modbus RTU

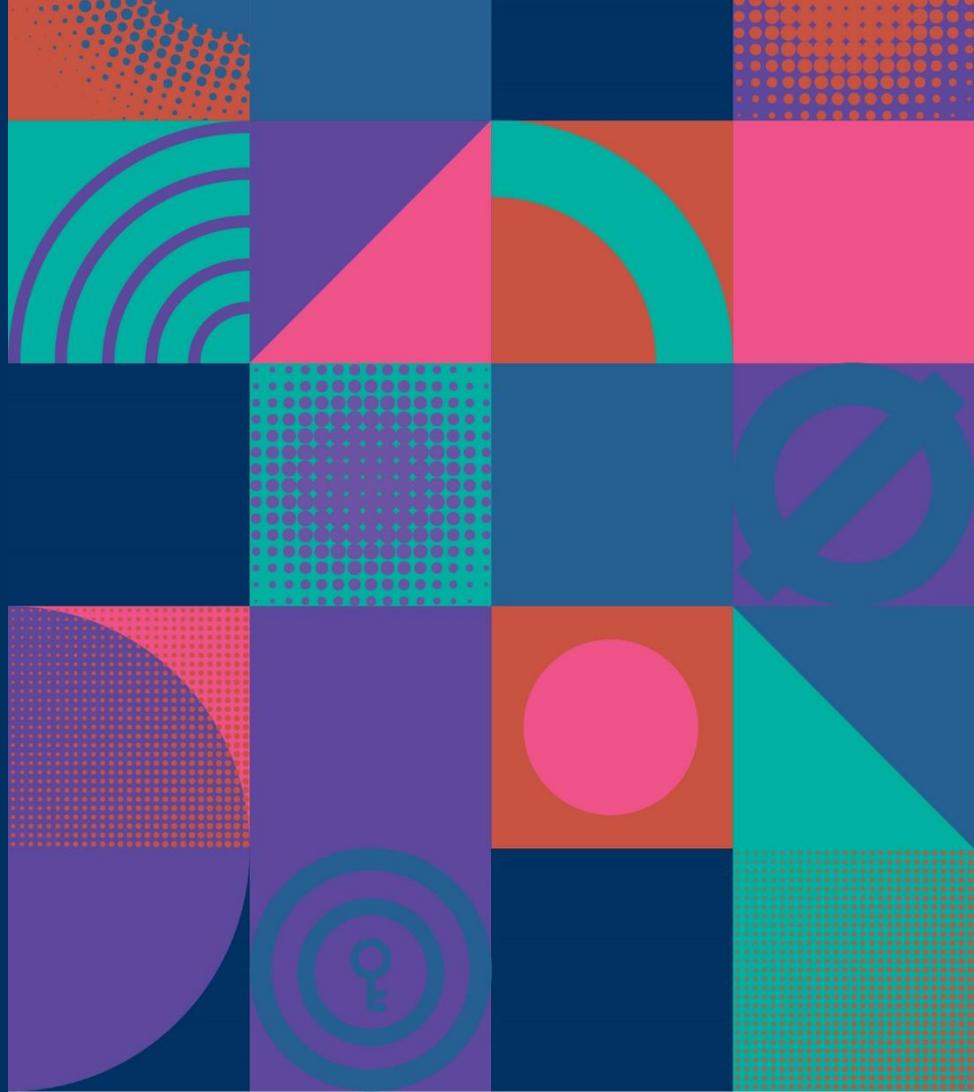
# Защищенная АСУ ТП



# Защищенная IoT-система



Управление решением  
ViPNet SIES



# Центр управления ViPNet SIES MC



## ViPNet SIES MC10000

- Max: 10000-узлов
- Max: 2000 администраторов безопасности
- Сертификация как СКЗИ КСЗ по требованиям ФСБ России



## ViPNet SIES MC VA

- Max: 5000-узлов
- Max: 1000 администраторов безопасности



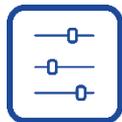
# Основные задачи ViPNet SIES MC



Управление  
ключами и  
сертифика-  
тами SIES-  
узлов



Защищенный  
обмен  
с SIES-узлами



Управление  
SIES-узлами



Мониторинг  
состояния  
SIES-узлов

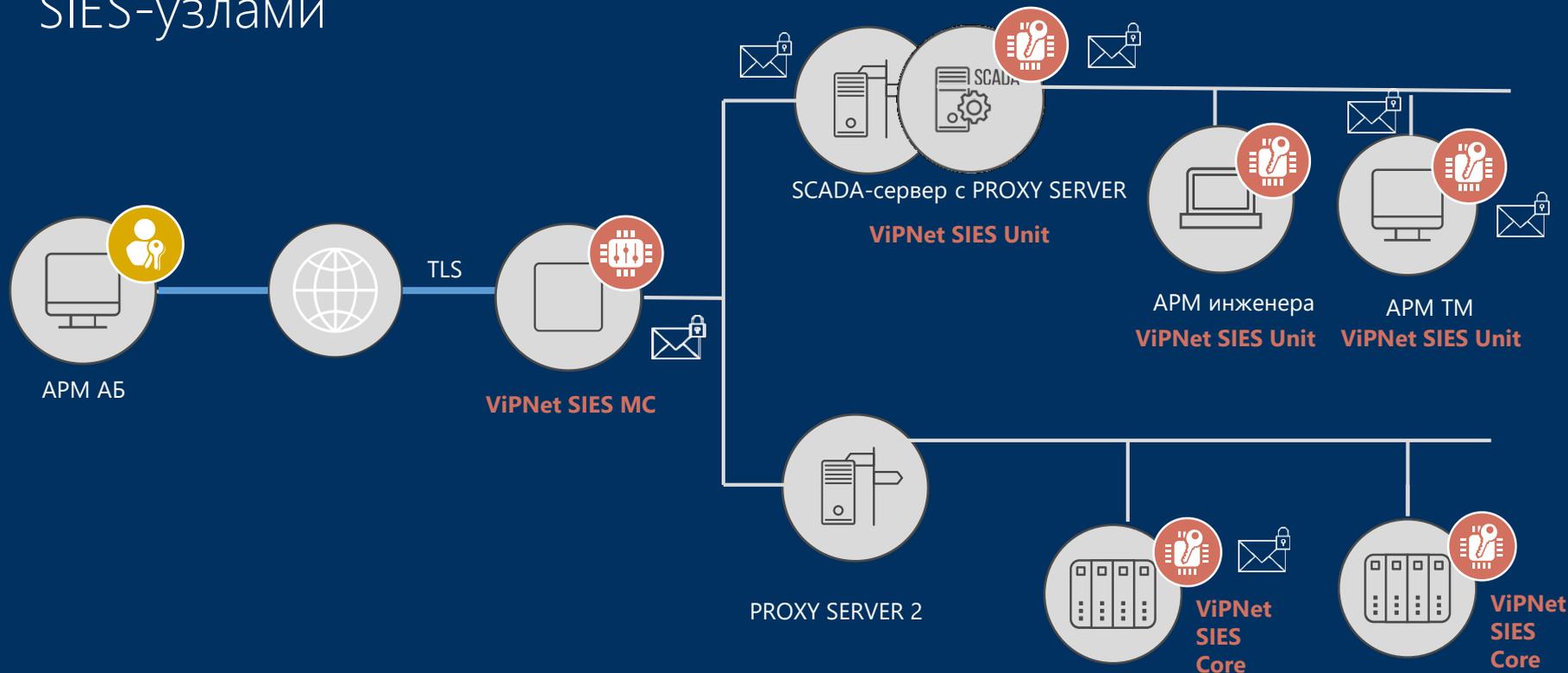


Настройка  
SIES MC

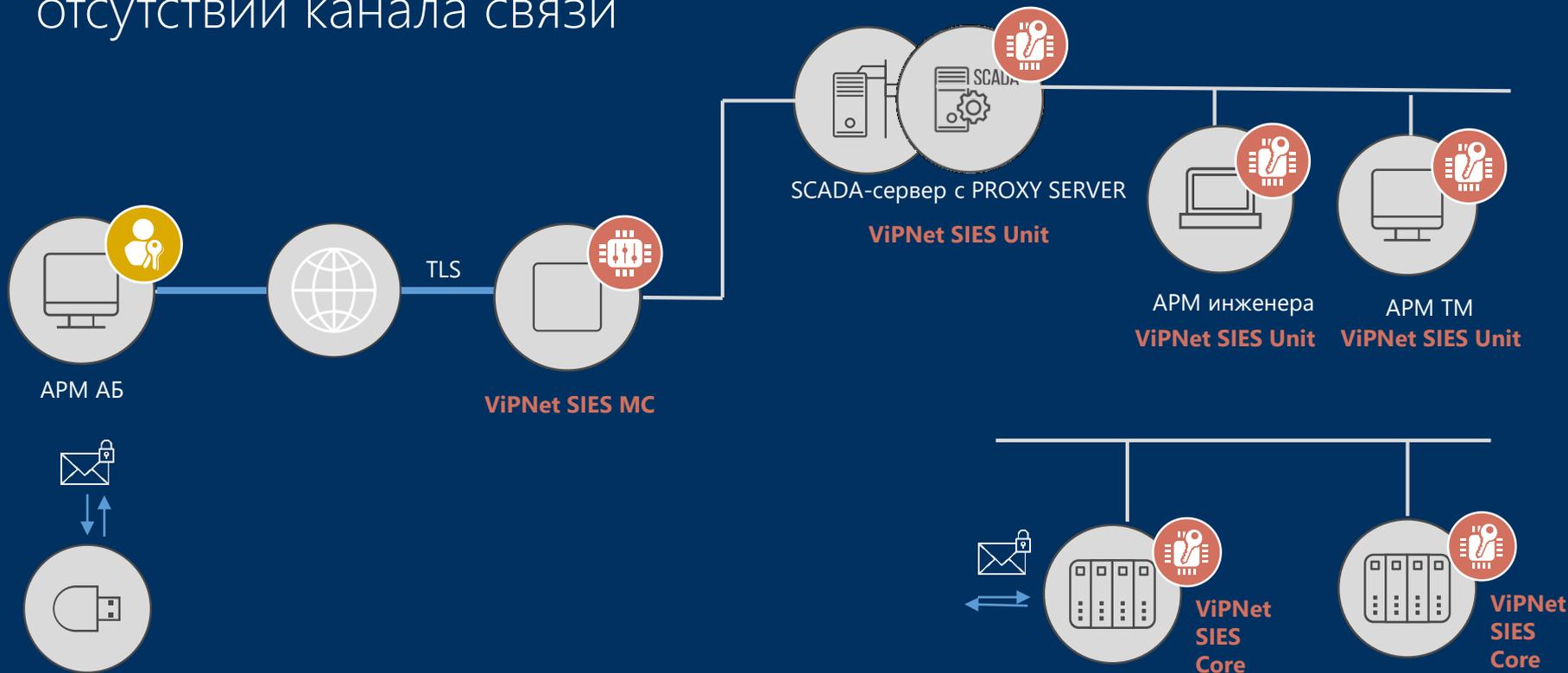


Разграничение  
прав доступа  
к решению  
SIES

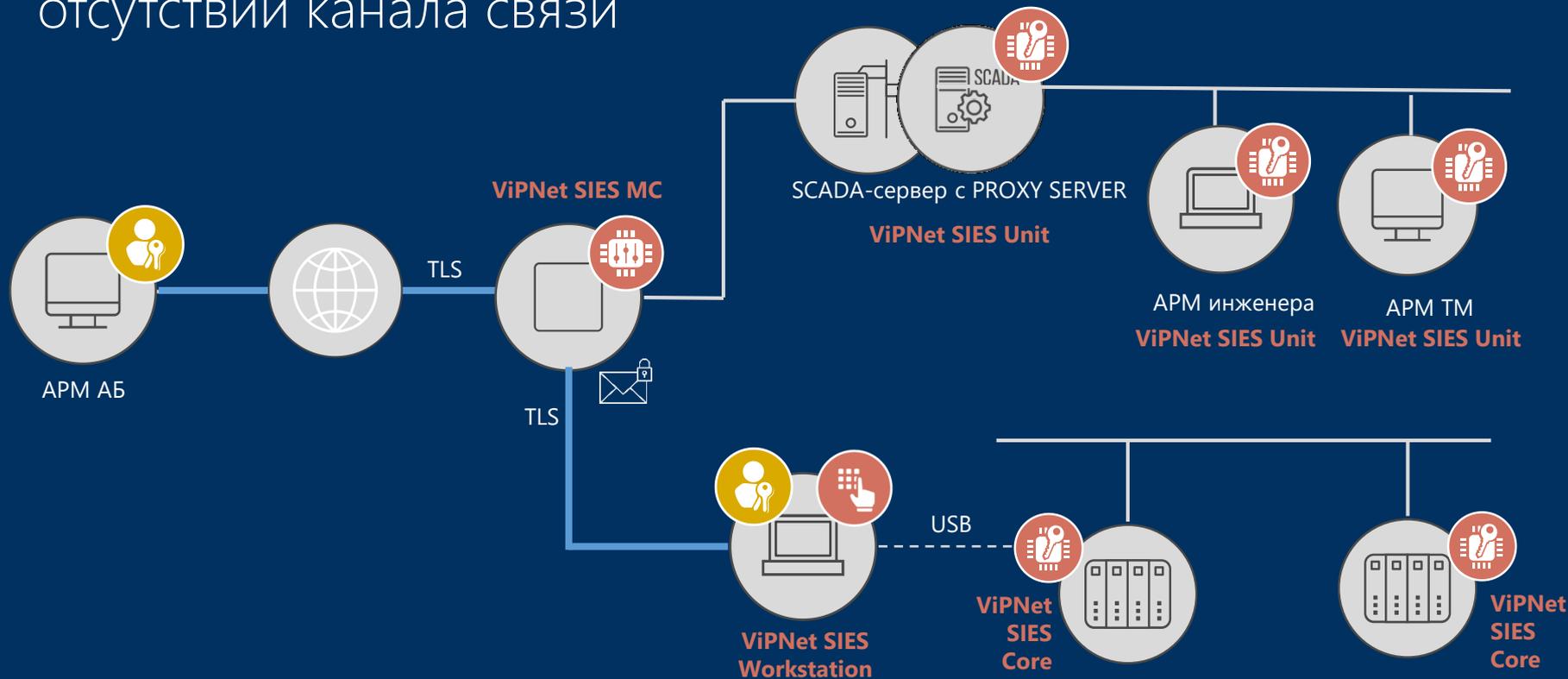
# Дистанционный защищенный обмен с SIES-узлами



# Защищенный обмен с SIES-узлами при отсутствии канала связи



# Защищенный обмен с SIES-узлами при отсутствии канала связи



# Объекты управления SIES MC: SIES-узлы



ПАК ViPNet SIES  
Core



ПО ViPNet SIES  
Unit

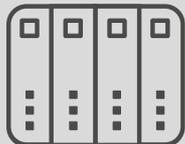


Пользователь АСУ  
Сервисный инженер,  
Инженер КИП

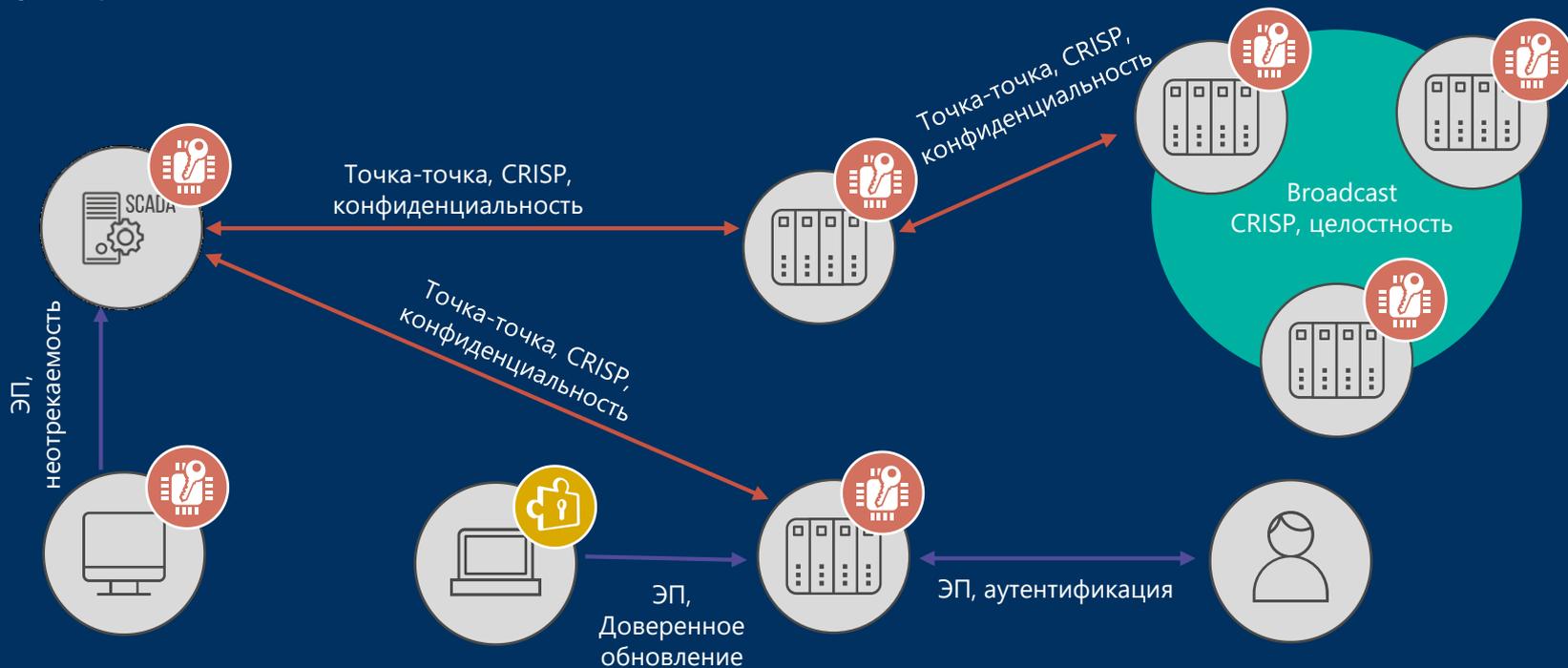


Другой SIES-узел  
Криптопровайдеры  
и прочие PKI-продукты

# Объекты управления SIES MC: устройства АСУ, в которые встраиваются SIES-узлы



# Задание направлений взаимодействия устройств





В качестве заключения

# Меры Приказа №239 ФСТЭК России, реализуемые с помощью решения ViPNet SIES

Аутентификация и  
идентификация

---

ИАФ.1, ИАФ.2,  
ИАФ.3, ИАФ.4,  
ИАФ.5, ИАФ.7,

Ограничение  
программной  
среды

---

ОПС.1, ОПС.2

Обеспечение  
целостности

---

ОЦЛ.1, ОЦЛ.2,  
ОЦЛ.3, ОЦЛ.4,  
ОЦЛ.5

Защита ИС/АСУ и  
ее компонентов

---

ЗИС.8, ЗИС.19,  
ЗИС.32

Управление  
обновлениями ПО

---

ОПО.1, ОПО.2,  
ОПО.4

Управление  
доступом

---

УПД.1, УПД.2,  
УПД.3, УПД.4,  
УПД.13

Аудит  
безопасности

---

АУД.4, АУД.6

Обеспечение  
доступности

---

ОДТ.4, ОДТ.5,  
ОДТ.6

Управление  
конфигурацией

---

УКФ.3, УКФ.4

Компенсирющие  
меры для:

---

Антивирусная  
защита:  
АВЗ.1, АВЗ.3,  
АВЗ.4, АВЗ.5



ТЕХНО infotecs  
2019 ФЕСТ

Спасибо  
за внимание!