Обзор продуктов решения ViPNet SIES

Решение ViPNet SIES

Решение ViPNet SIES

ТЕХНО 2020 infotecs ФЕСТ

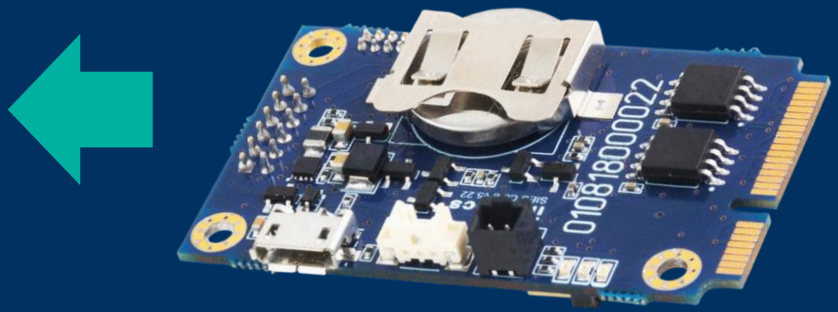
ВСТРАИВАЕМЫЕ КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ИНТЕГРАЦИИ В УСТРОЙСТВА АВТОМАТИЗАЦИИ НА ВСЕХ УРОВНЯХ АСУ

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

Состав решения ViPNet SIES

- Законченные СКЗИ класса КС1 и КС3
- Возможность использования криптографии на разных по вычислительной мощности устройствах полевого уровня
- Нет зависимости от ОС и архитектуры устройств полевого уровня

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



Интеграция ПАК SIES Core

На аппаратном уровне – USB, UART, SPI

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

Сертификат СКЗИ класса КС3 по требованиям ФСБ России

Интеграция ПО ViPNet SIES Unit

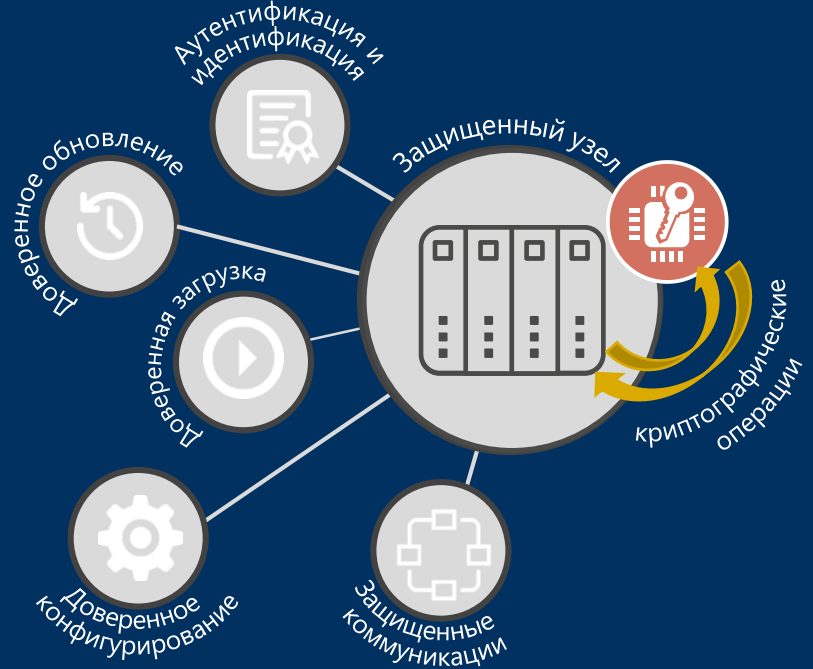
Поддерживаемые ОС:

- Windows 7/8/8.1/10 (x86/64)*
- Windows Server 2008/R2/2012/2012 R2/ 2016 *
- Debian 9, Ubuntu 16, Ubuntu 18 и др ОС Linux **:
  - gcc v.6 и выше,
  - systemd система инициализации,
  - x86/64 архитектура процессора
  - менеджер пакетов deb/rpm формата
- Astra Linux Special Edition (Смоленск) 1.6 (x86/64)

*Сертификат СКЗИ класса КС1 и КС3 по требованиям ФСБ России

** Сертификат СКЗИ класса КС1 и КС3 ожидается в 2021г.

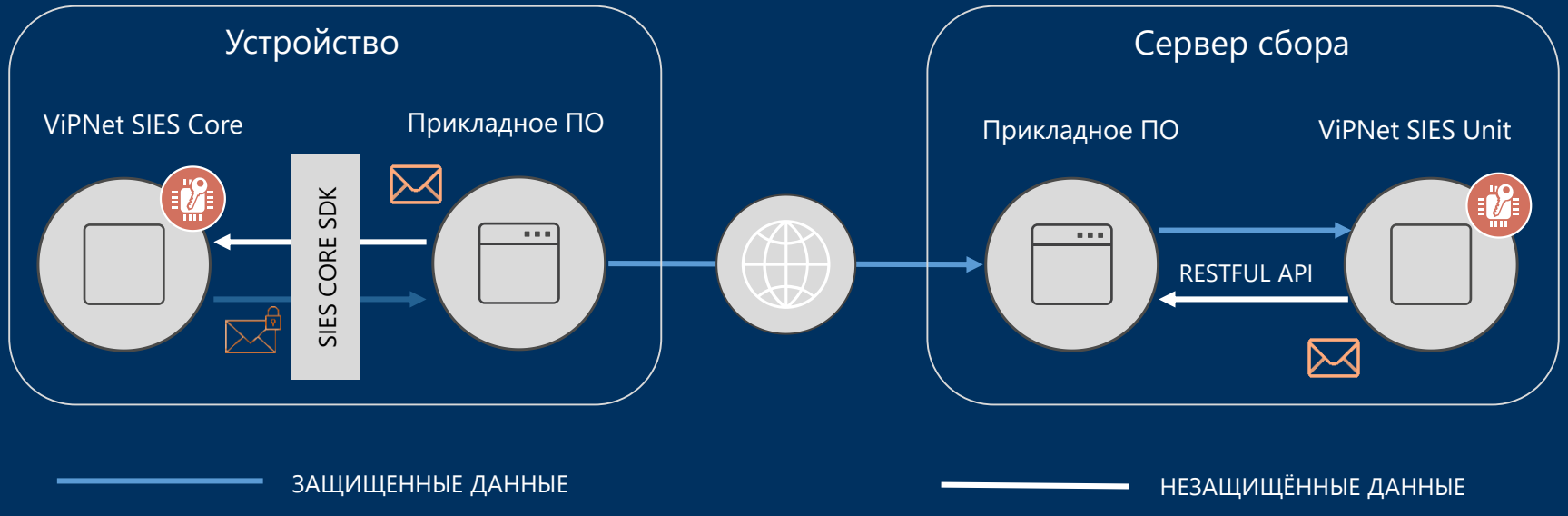
Криптографические сервисы для защищаемых устройств



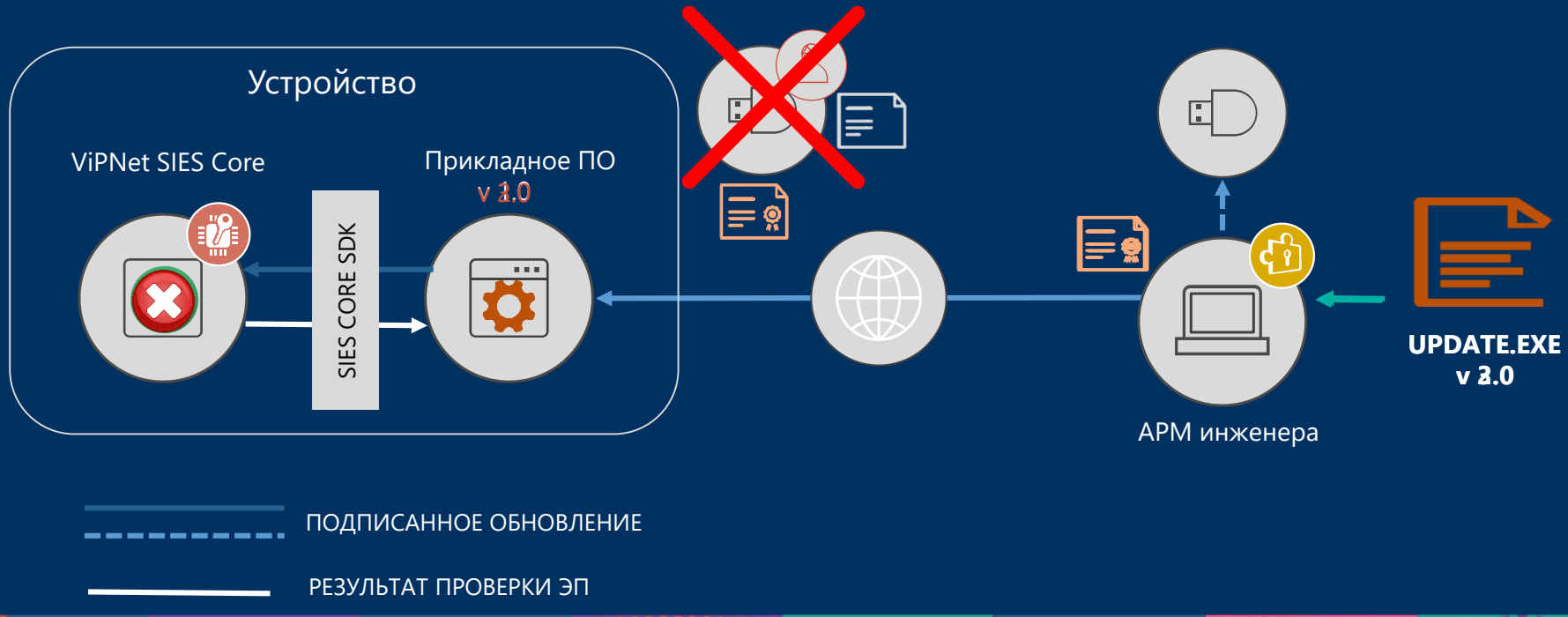
Сценарии защиты информации:

- 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



ТЕХНО 2020 infotecs ФЕСТ

ГОСТ 28147-89

ГОСТ Р 34.11-2012
ГОСТ 34.11-2018

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

ГОСТ Р 34.10-2012
ГОСТ 34.10-2018

Криптографические операции, доступные защищаемым устройствам

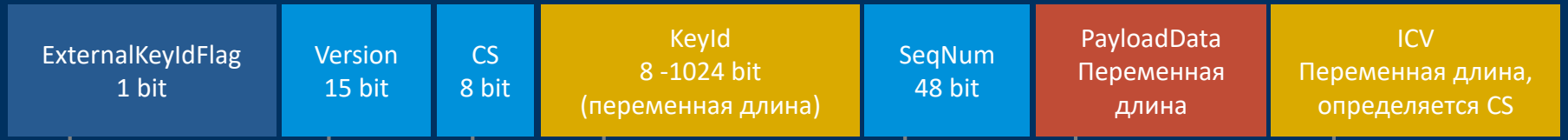
CRISP: протокол защищенной передачи данных для индустриальных систем, M2M и IIoT коммуникаций

ТЕХНО 2020 infotecs ФЕСТ

Рекомендация по стандартизации РФ:
Р 1323565.1.029-2019. Протокол защищенного обмена CRISP

- 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



Имитовставка

Исходное или
зашифрованное сообщение

Порядковый номер сообщения

Идентификатор ключа

Идентификатор криптографического набора

Версия CRISP-сообщения

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

0 – ключ определяется по KeyId

1 – требуется внешняя информация

CRISP: механизмы защиты

Криптонабор CS=1,3

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=2,4

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

CRISP

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

Какие промышленные протоколы можно защищать с помощью CRISP?

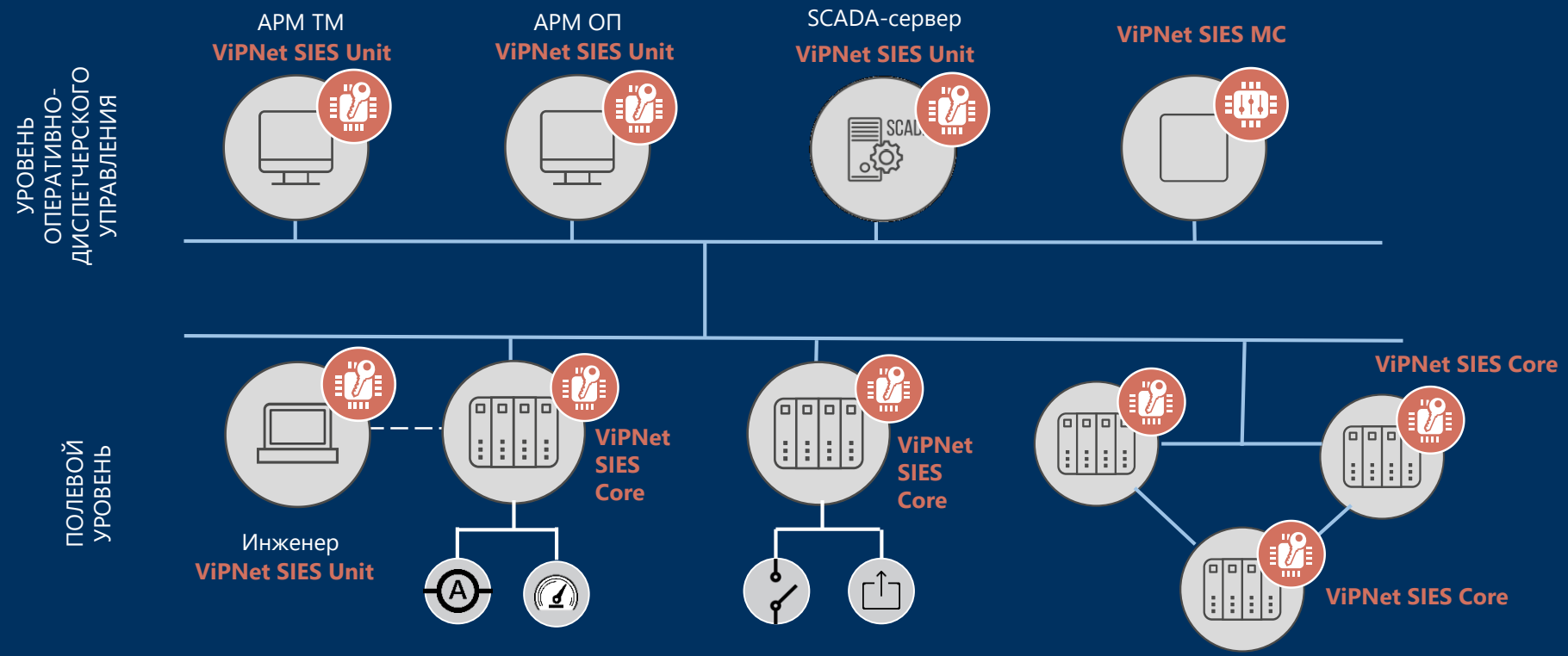
CRISP – Рекомендация по стандартизации РФ
Р 1323565.1.029-2019

Industrial Ethernet:
- МЭК 60870-5-104
- Modbus TCP
- GOOSE

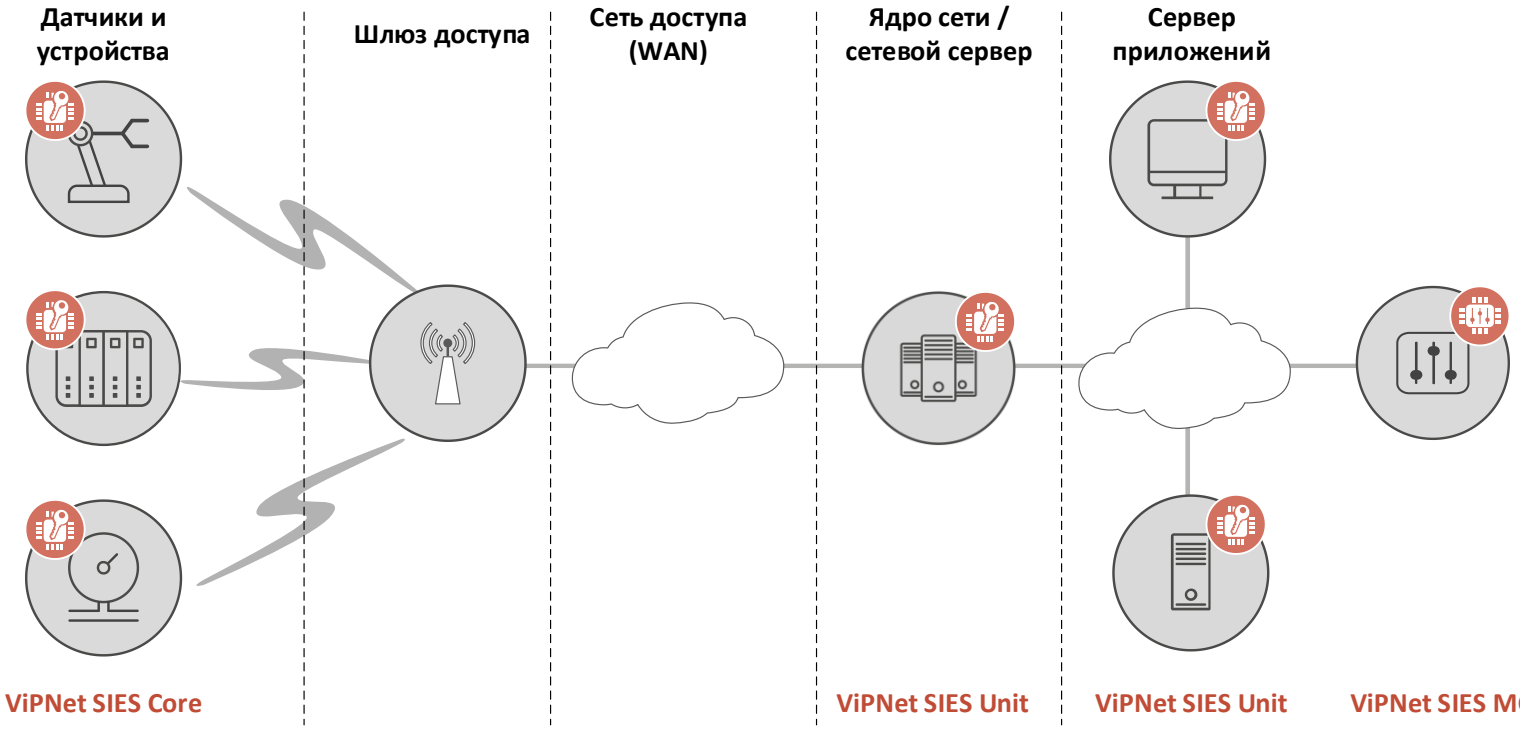
IIoT – протоколы:
- NB-IoT
- LoRaWan
- MQTT

Fieldbus:
- МЭК 60870-5-101
- Modbus RTU

Защищенная АСУ ТП



Защищенная IIoT-система



Управление решением ViPNet SIES

Центр управления ViPNet SIES MC

ViPNet SIES MC10000

- Max: 10000-узлов
- Max: 2000 администраторов безопасности
- Сертификация как СКЗИ КС3 по требованиям ФСБ России

ViPNet SIES MC 3000

- Max: 3000-узлов
- Max: 300 администраторов безопасност.
- Сертификация в 2021 г

ViPNet SIES MC VA

- Max: 5000-узлов
- Max: 500 администраторов безопасности
- Сертификация в 2021 г

Основные задачи ViPNet SIES MC

ТЕХНО 2020 infotecs ФЕСТ

Управление ключами и сертифика-тами SIES-узлов

Защищенный обмен с SIES-узлами

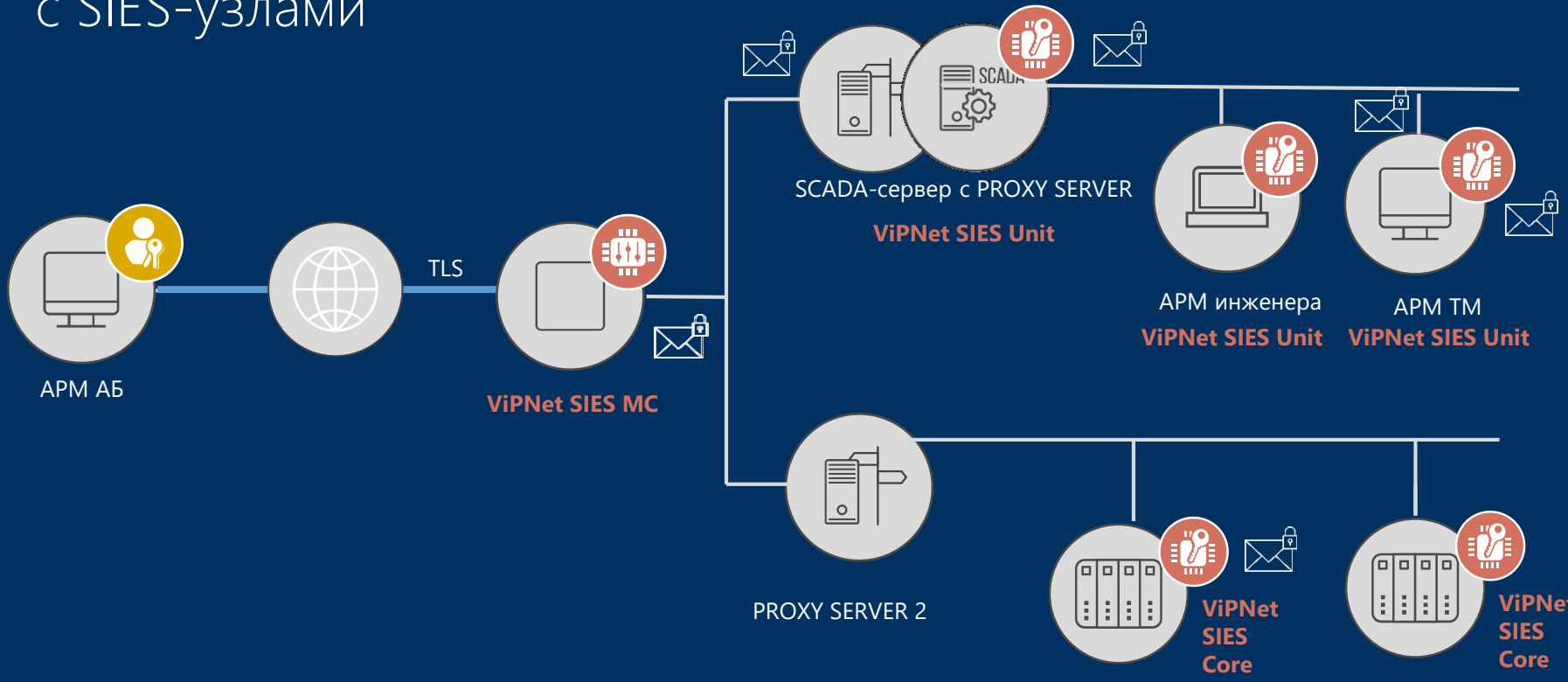
Управление SIES-узлами

Мониторинг состояния SIES-узлов

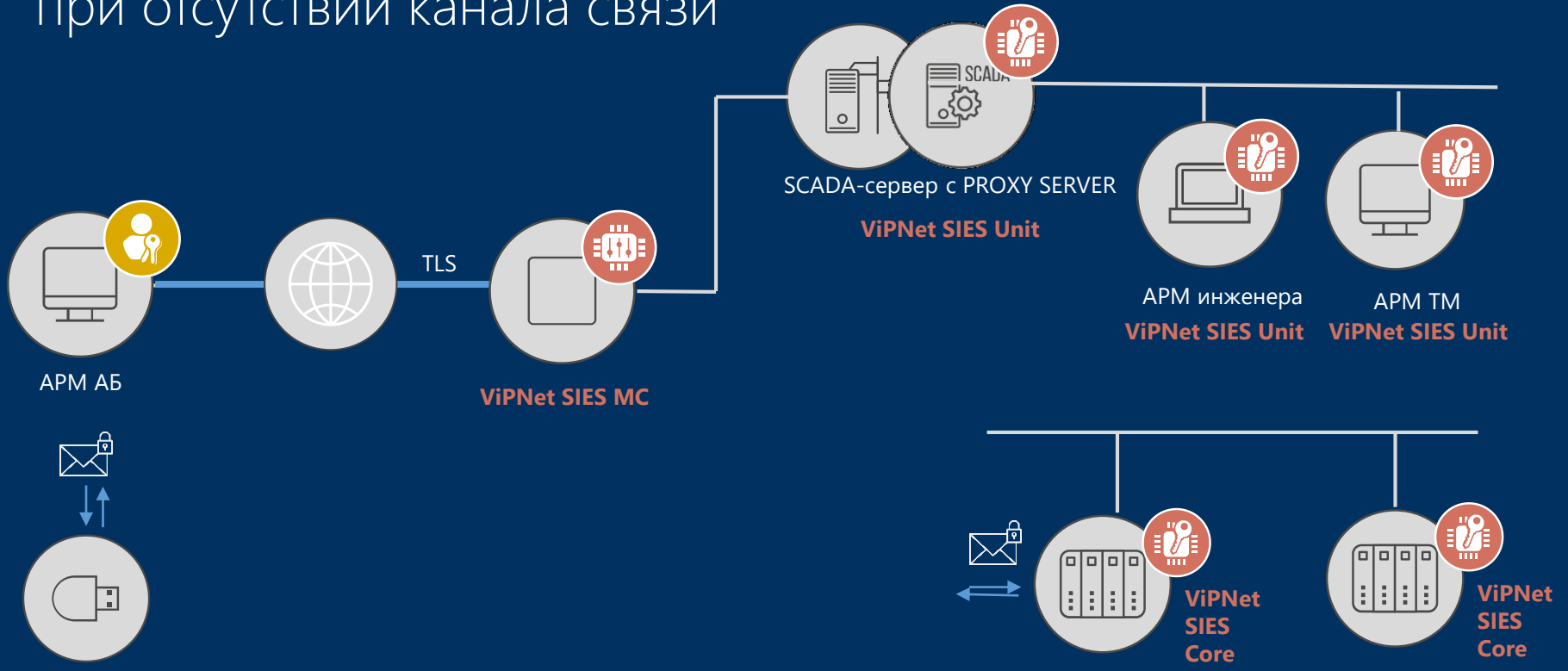
Настройка SIES MC

Разграничение прав доступа к решению SIES

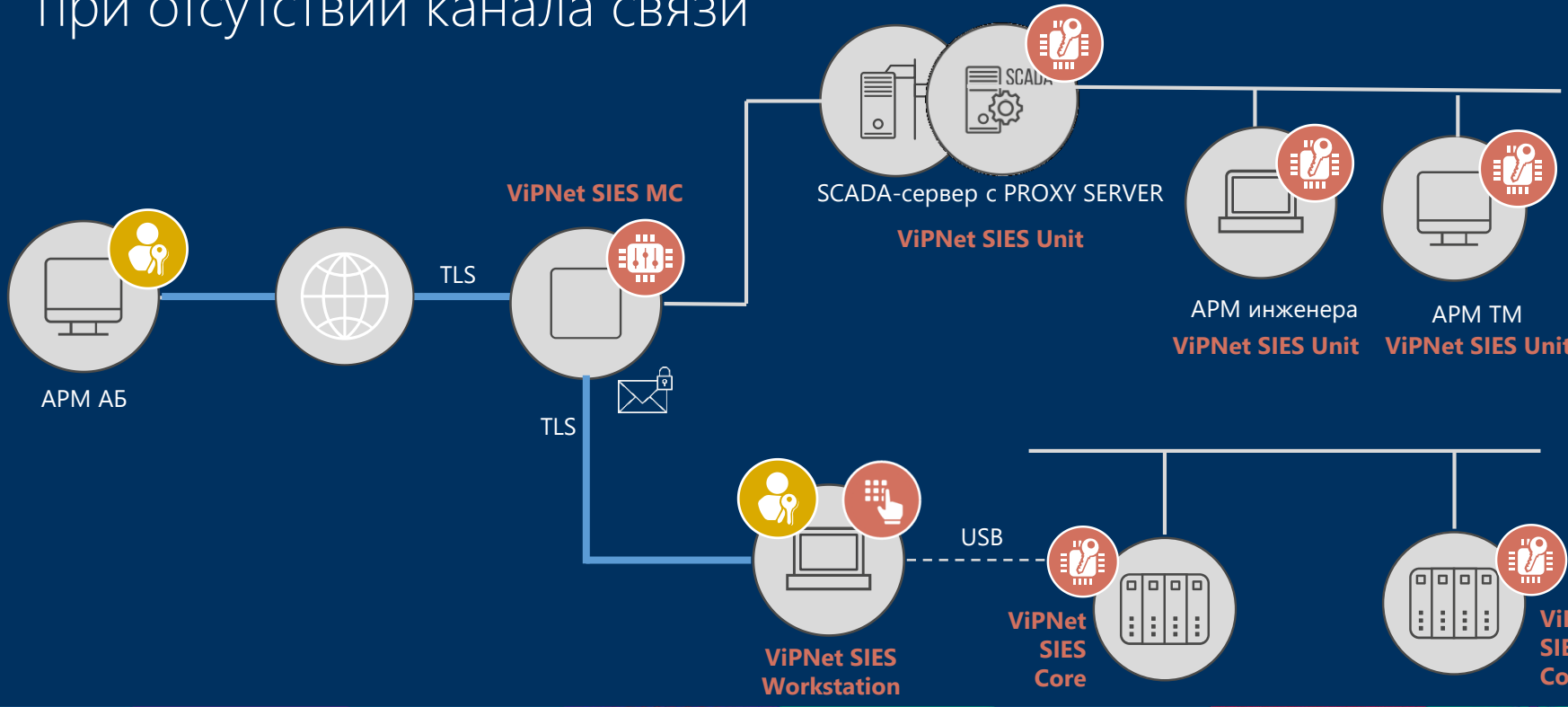
Дистанционный защищенный обмен с SIES-узлами



Защищенный обмен с SIES-узлами при отсутствии канала связи



Защищенный обмен с SIES-узлами при отсутствии канала связи



Объекты управления SIES MC: SIES-узлы

ТЕХНО 2020 infotecs фест

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

ТЕХНО 2020 infotecs фест

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	Компенсирующие меры для: Антивирусная защита: АВЗ.1, АВЗ.3, АВЗ.4, АВЗ.5

ТЕХНО 2020 infotecs Фест

Спасибо за внимание!