ViPNet SIES: что нового?

Марина Сорокина,
Руководитель продуктового направления


Решение ViPNet SIES

Решение ViPNet SIES

ВСТРАИВАЕМЫЕ СКЗИ ДЛЯ ИНТЕГРАЦИИ В УСТРОЙСТВА АВТОМАТИЗАЦИИ, M2M-УСТРОЙСТВА И IIOT-УСТРОЙСТВА С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИХ СОБСТВЕННОЙ БЕЗОПАСНОСТИ

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

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

Сценарии безопасности защищаемых устройств, которые можно реализовать

- Зашифрование/расшифрование по CRISP (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- Создание имитовставки/проверка имитовставки по CRISP (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- Создание ЭП/проверка ЭП в CMS (ГОСТ 34.10-2018)
- Зашифрование/расшифрование в CMS (ГОСТ 28147-89)
- Создание хэш/проверка хэш (ГОСТ 34.11-2018)

Концепция security-by-design

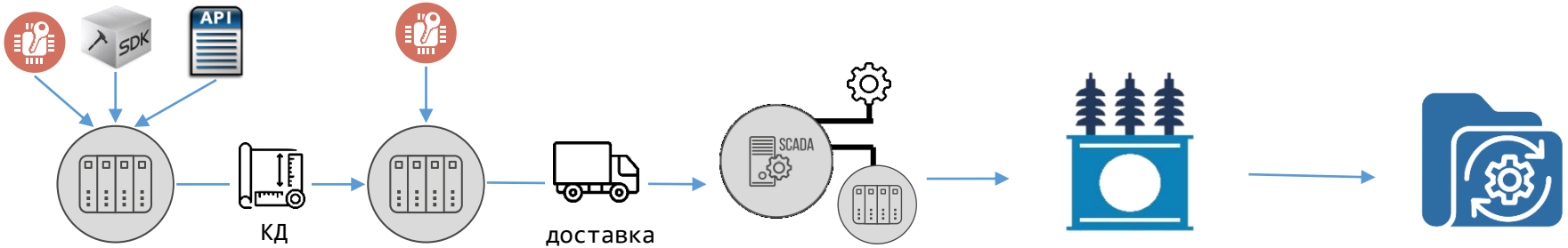
РАЗРАБОТКА УСТРОЙСТВА

ПРОИЗВОДСТВО УСТРОЙСТВА

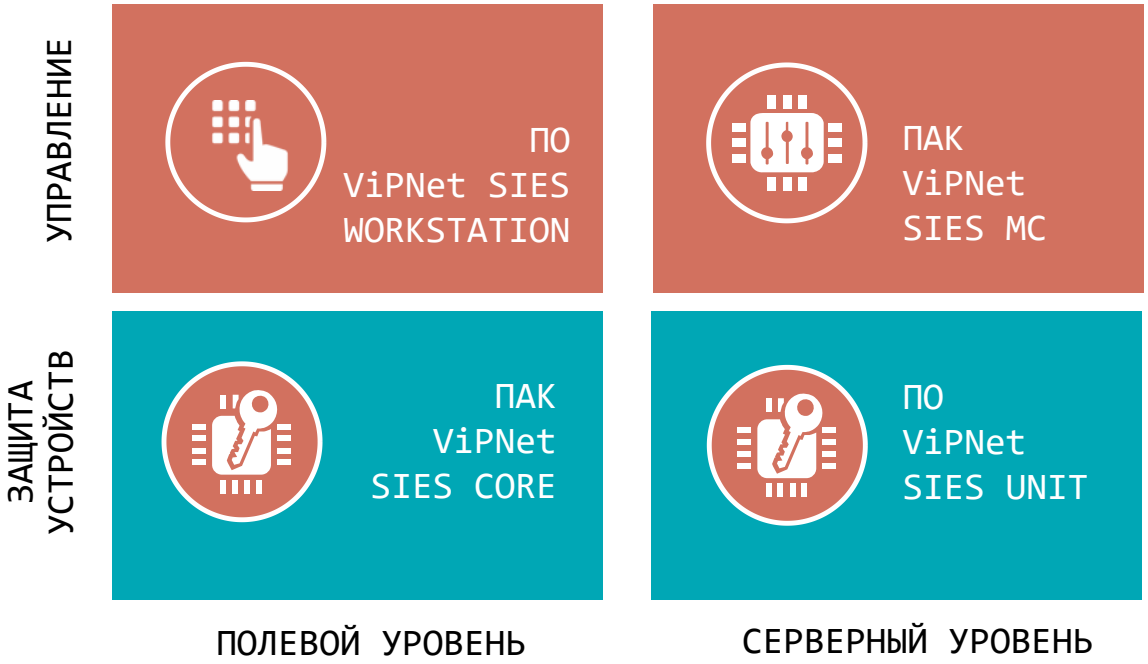
ВВОД В ЭКСПЛУАТАЦИЮ УСТРОЙСТВА

ЭКСПЛУАТАЦИЯ УСТРОЙСТВА

УПРАВЛЕНИЕ ОБНОВЛЕНИЕМ И КОНФИГУРАЦИЕЙ УСТРОЙСТВА



Состав решения ViPNet SIES

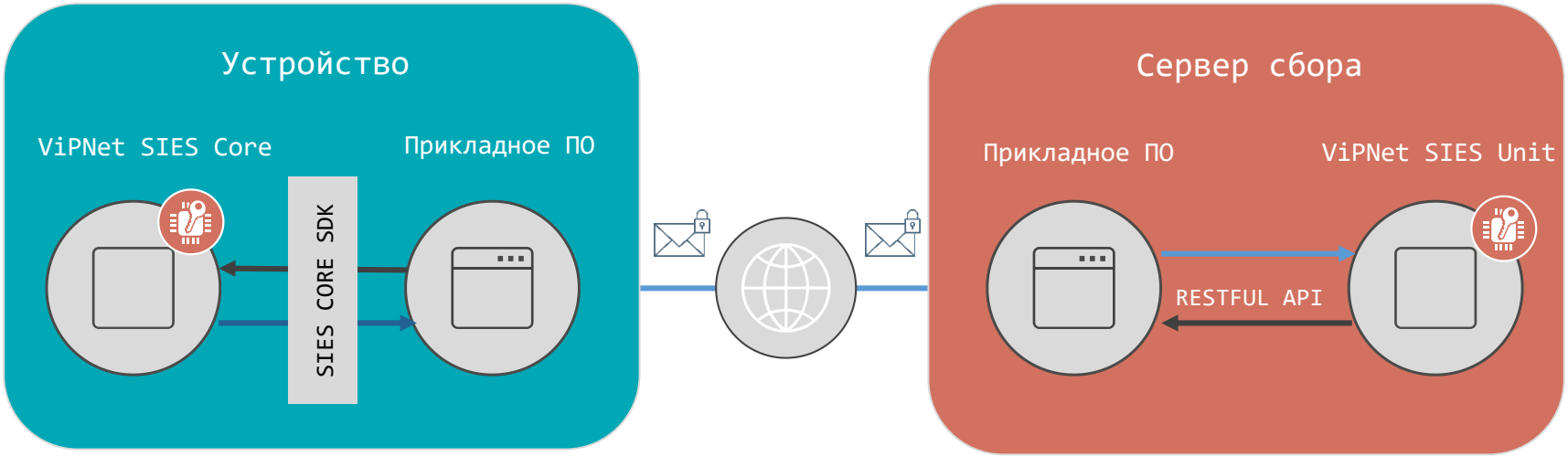


СКЗИ класса КС1 и КС3 по требованиям ФСБ России

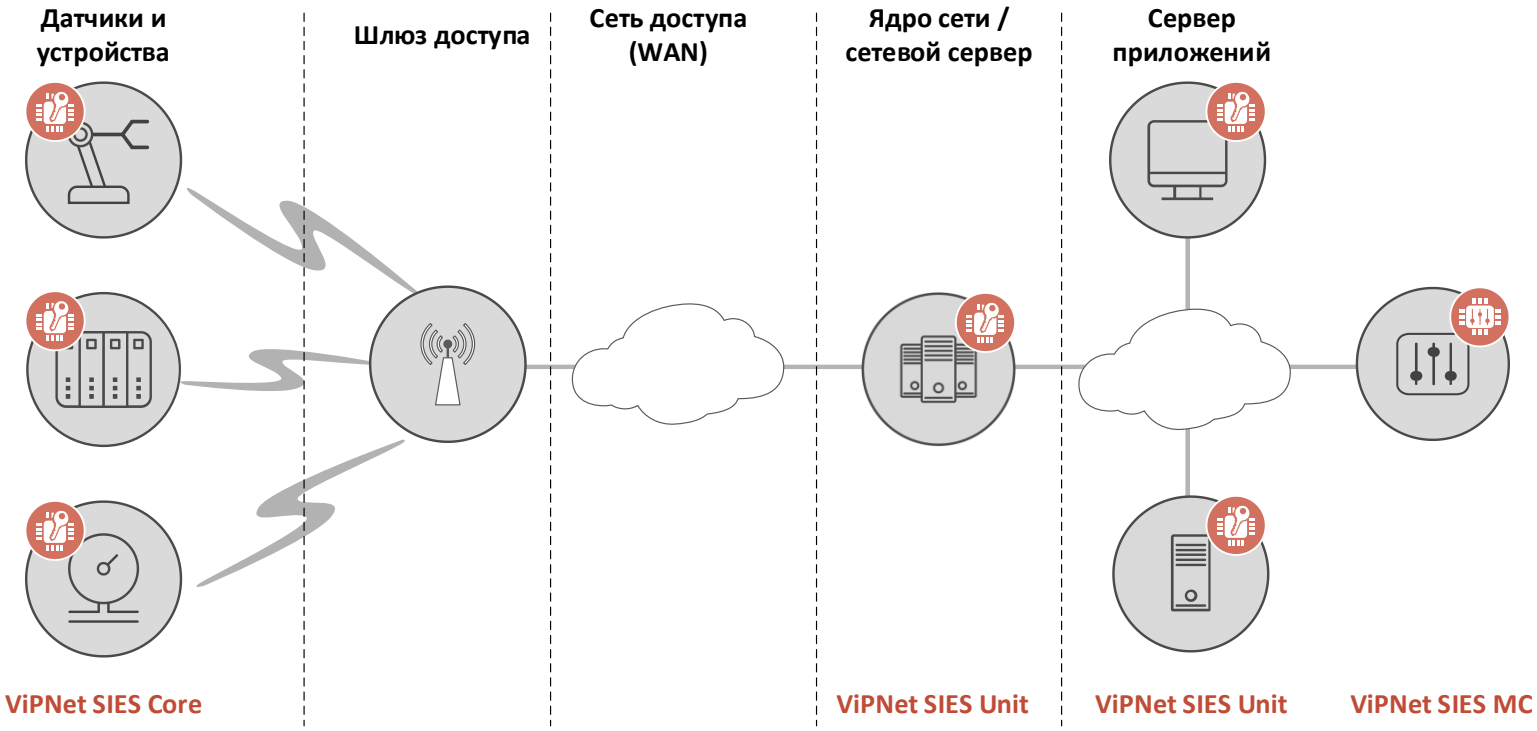
Возможность использования криптографии на разных по вычислительной мощности устройствах

Нет зависимости от ОС и архитектуры устройств

Решение ViPNet SIES



Защищенная IIoT-система




ViPNet SIES: What’s new?

Сертификация

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3908* от "*18*" *сентября* 2020 г.

Действителен до "*18*" *сентября* 2023 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс **ViPNet SIES Core** в комплектации согласно формуляру ФРКЕ.466219.011ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, криптографическая аутентификация абонентов при установлении соединения) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

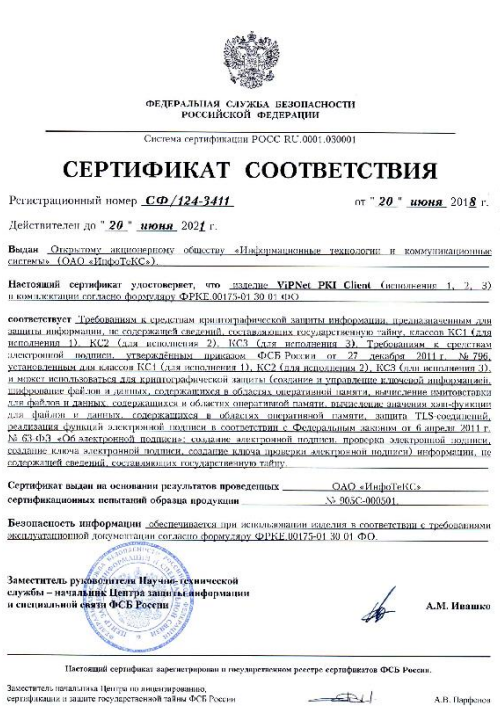
сертификационных испытаний образца продукции № 872-000501.

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.466219.011ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России О.В. Скрибин

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 18 сентября 2020 г.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России Д.Л. Круглов



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3411* от "*20*" *июня* 2018 г.

Действителен до "*20*" *июня* 2021 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).

Настоящий сертификат удостоверяет, что изделие **ViPNet PKI Client** (исполнение 1, 2, 3) в комплектации согласно формуляру ФРКЕ.00175-01 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1 (для исполнения 1), КС2 (для исполнения 2), КС3 (для исполнения 3). Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КС1 (для исполнения 1), КС2 (для исполнения 2), КС3 (для исполнения 3), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС» **сертификационных испытаний образца продукции** № 905С-000501.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00175-01 30 01 ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Ивашко

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

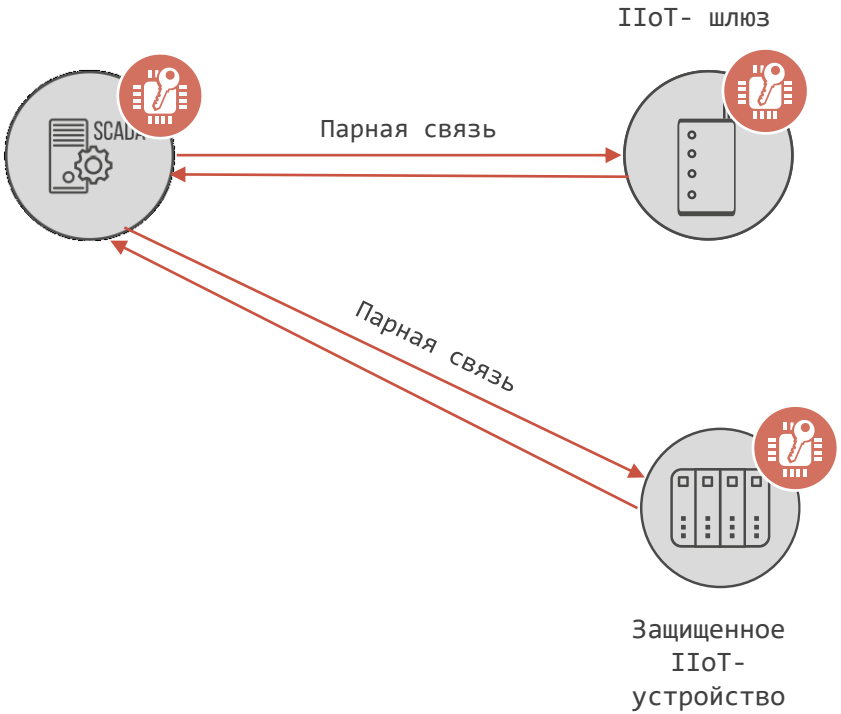
Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

ViPNet SIES Core2.0
СКЗИ класса КС3

ViPNet PKI Client с SIES Unit
СКЗИ класса КС1,КС3

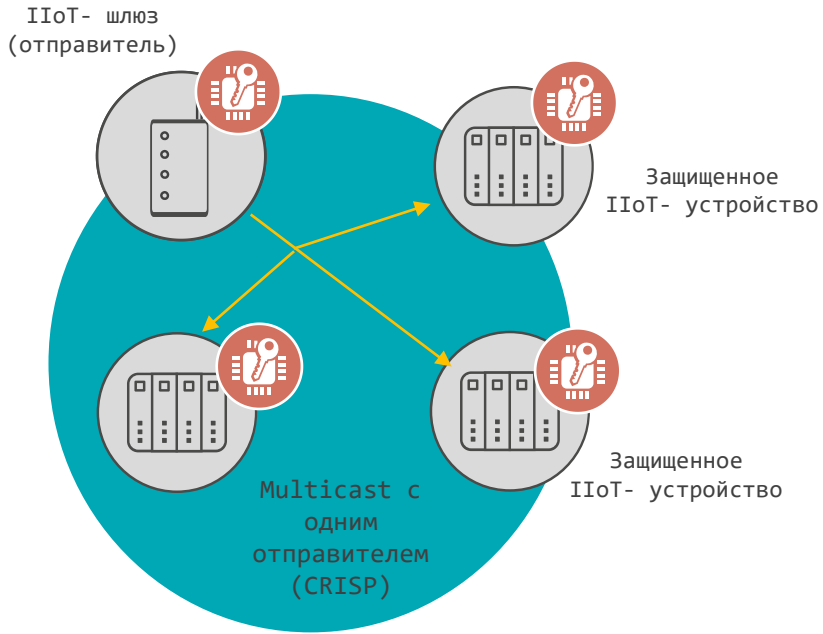
ViPNet SIES MC 2.0
СКЗИ класса КС3

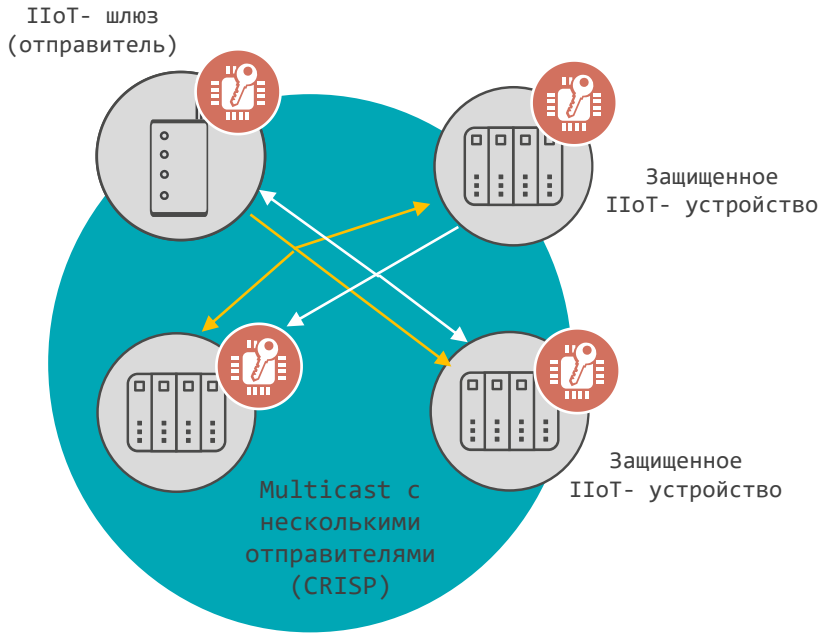
Защита сообщений точка-точка



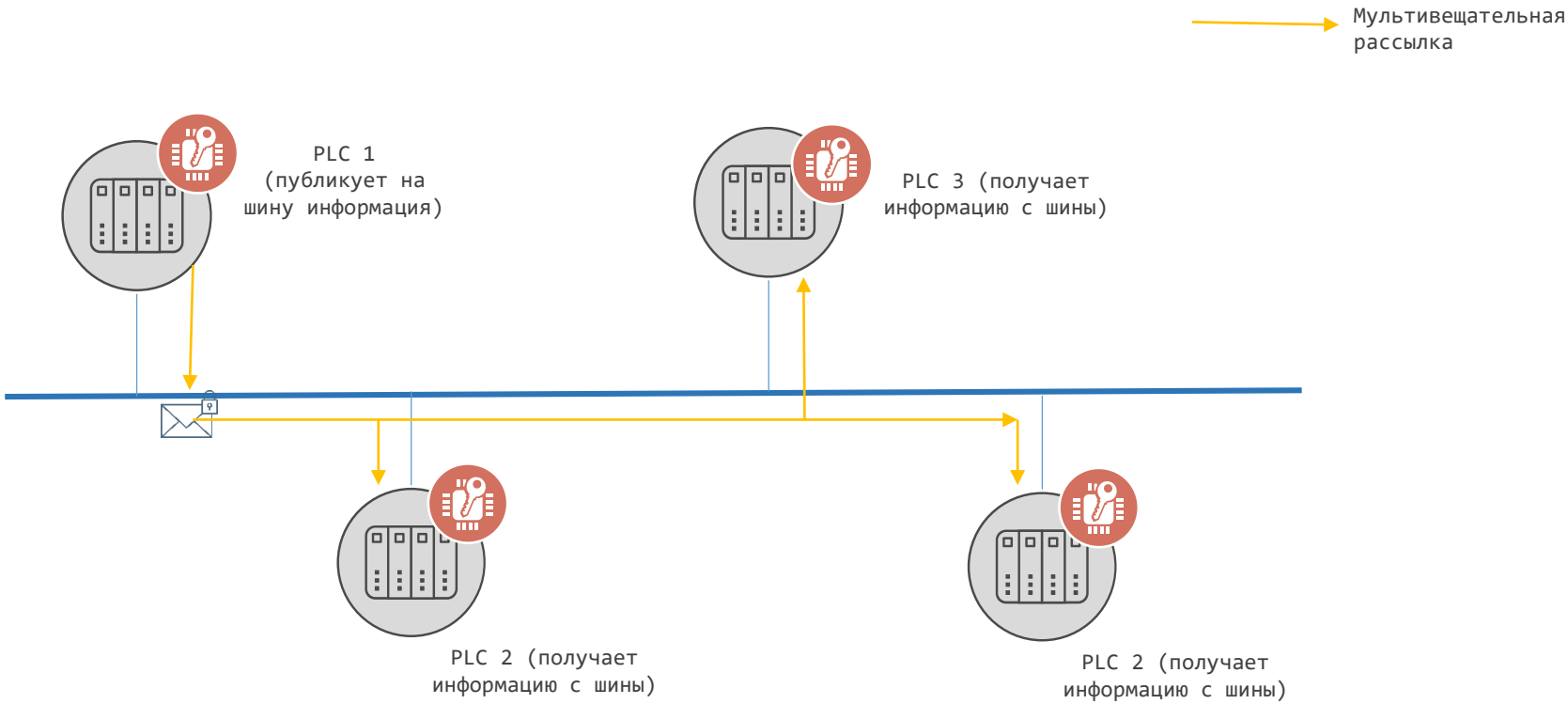
Логическое взаимодействие

Защита многоадресных сообщений (SIES 2.2)

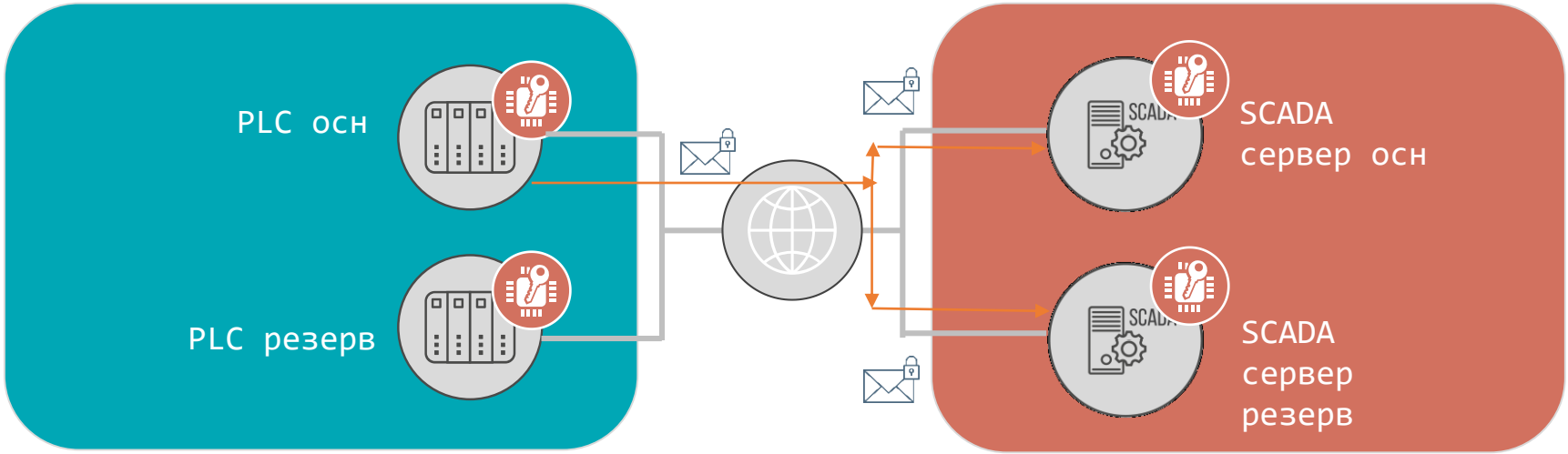




Защита коммуникаций «общая шина» или «подписочная модель» (SIES 2.2)



Защита коммуникаций с системах с резервированием (SIES 2.2)



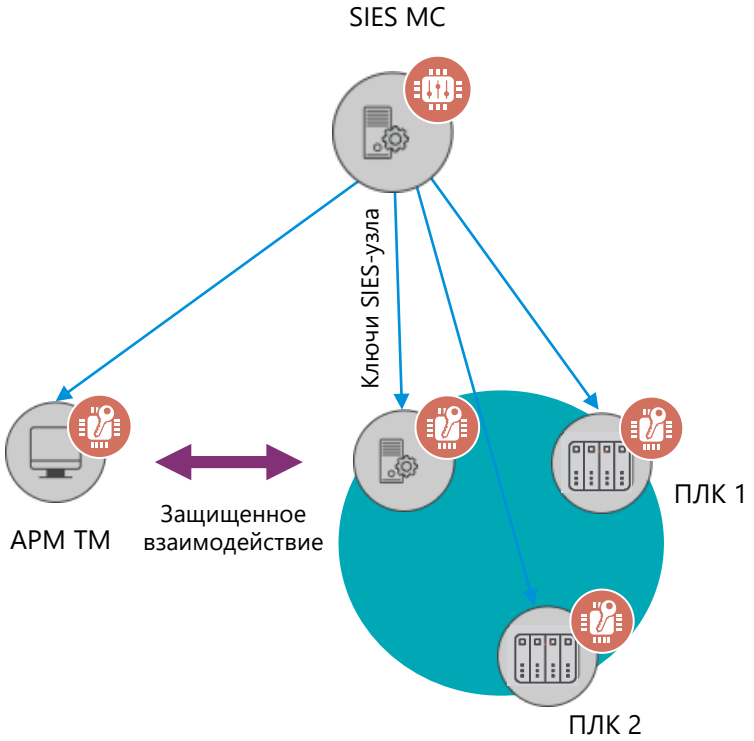
Прикладная ключевая подсистема SIES (симметричная подсистема)

В SIES MC:

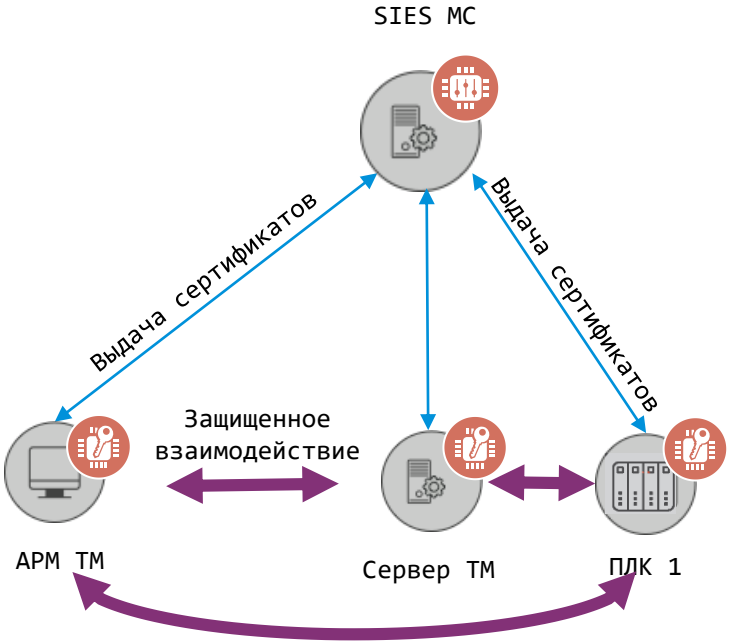
- Прикладной мастер-ключ
- Ключи SIES-узлов

На SIES-узлах:

- Ключи узла для парного взаимодействия
- Групповые ключи



Прикладная ключевая подсистема SIES 2.2: Асимметричная подсистема



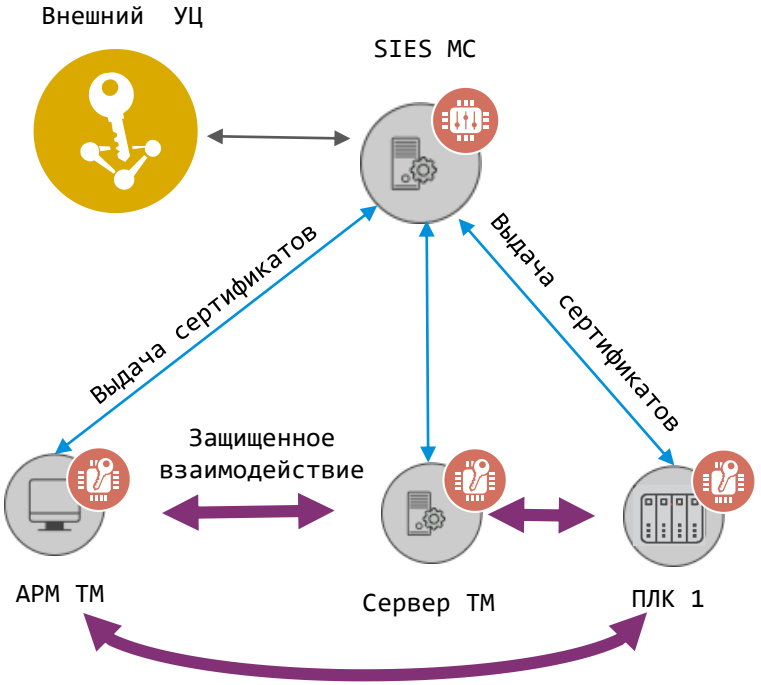
В SIES MC:

- Корневой сертификат прикладной ключевой подсистемы SIES MC
- Прикладные сертификаты SIES-узлов

На SIES-узлах:

- Корневой сертификат прикладной ключевой подсистемы SIES MC
- Прикладной сертификат SIES-узла
- Прикладные сертификаты связанных SIES-узлов

Прикладная ключевая подсистема SIES 2.3: Асимметричная подсистема



- Возможность подключения ViPNet Удостоверяющий центр в качестве внешнего УЦ для прикладной ключевой подсистемы
- Дистрибуция сертификатов, выпущенных во внешнем УЦ, на SIES-узлы
- Работа с точками распространения CRL для прикладной ключевой подсистемы
- Управление связями SIES-узлов на основе CRL

ViPNet SIES Core: What’s new?

Интеграция по интерфейсу SPI (начиная с SIES Core 2.2)

Интеграция ПАК SIES Core

- На аппаратном уровне –

USB, UART, SPI

- На программном уровне –

SIES Core API (RATP + прикладной протокол)

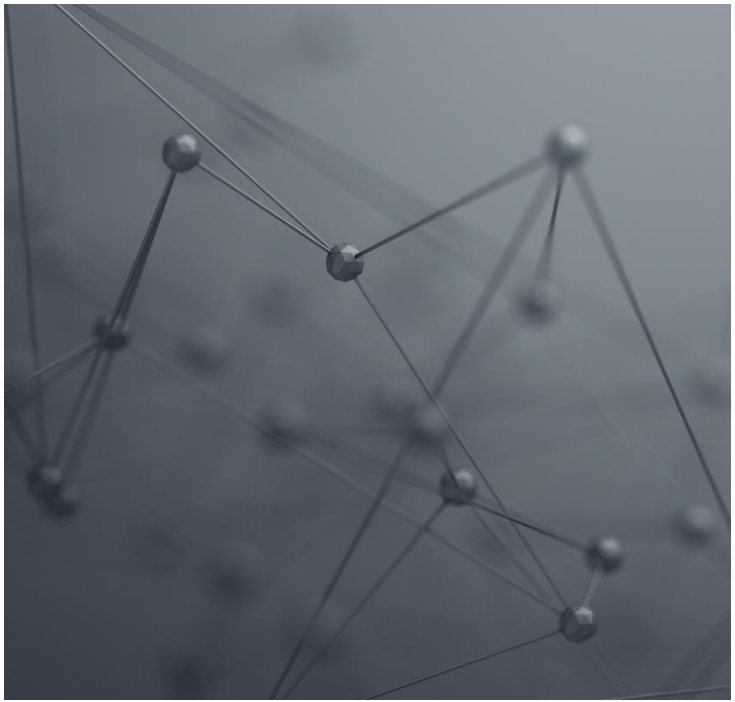
Измерения уровня заряда батареи (SIES Core 2.3)

Появилась возможность получить значение уровня заряда батареи через SIES Core SDK:

- под ОС Linux (Debian 7 (armel, armhF), Ubuntu 12);
- под ОС Windows (Windows 8/8.1, Windows 10, Windows Embedded Standard 7 (SP1), Windows Embedded 8/ 8.1, Windows 10 IoT Enterprise, Windows XP Embedded);
- библиотеки в исходных кодах для встраиваемых систем на языке «СИ»

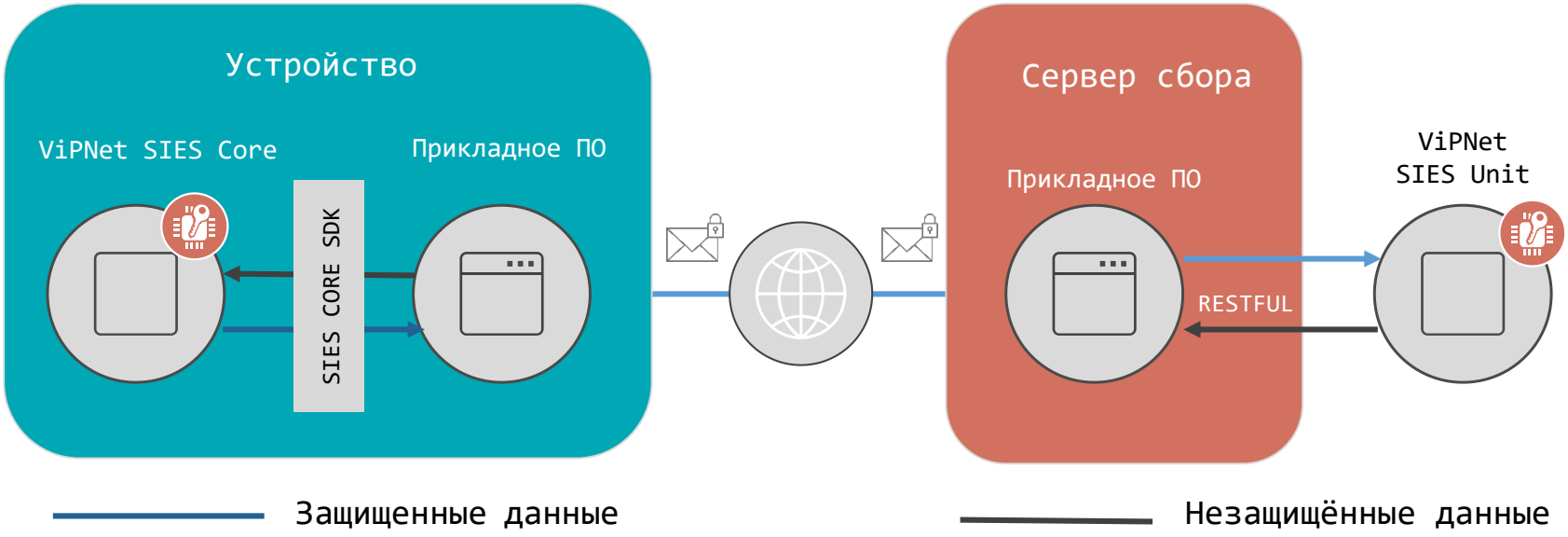
Улучшение характеристик работы

- Количество одновременно открытых контекстов увеличилось до числа загруженных прикладных связей
- После обновления инициализирующей последовательности не нужно синхронизировать связи

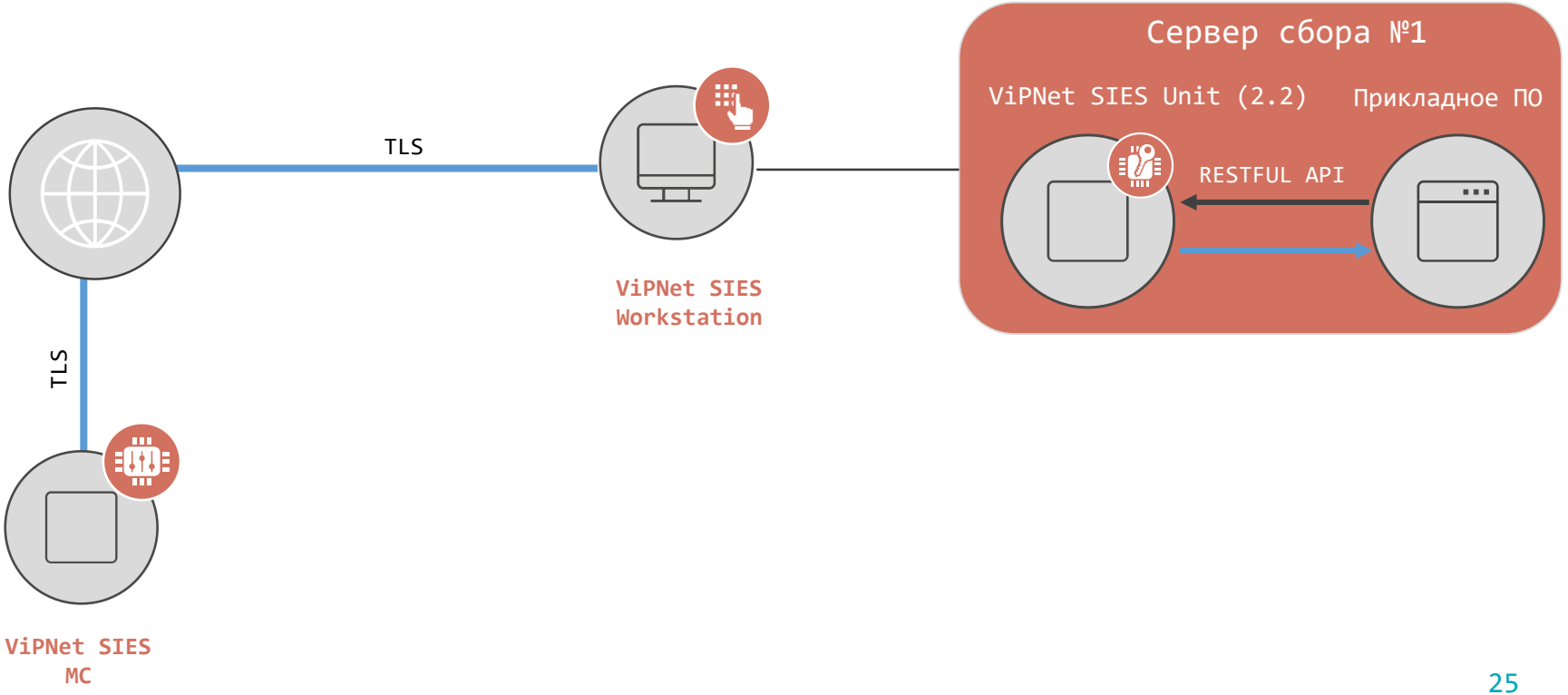


ViPNet SIES Unit: What’s new?

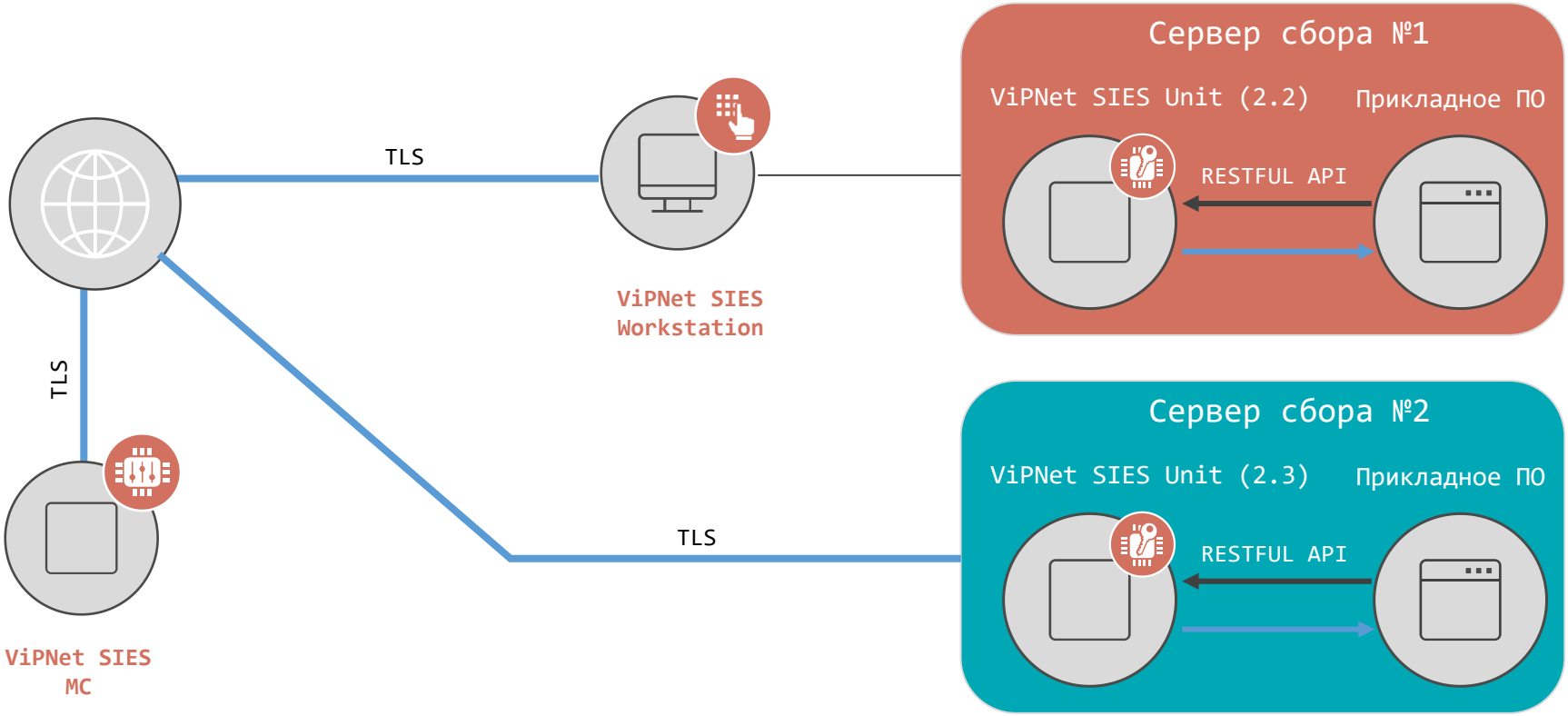
ViPNet SIES Unit на отдельной платформе (SIES 2.3)



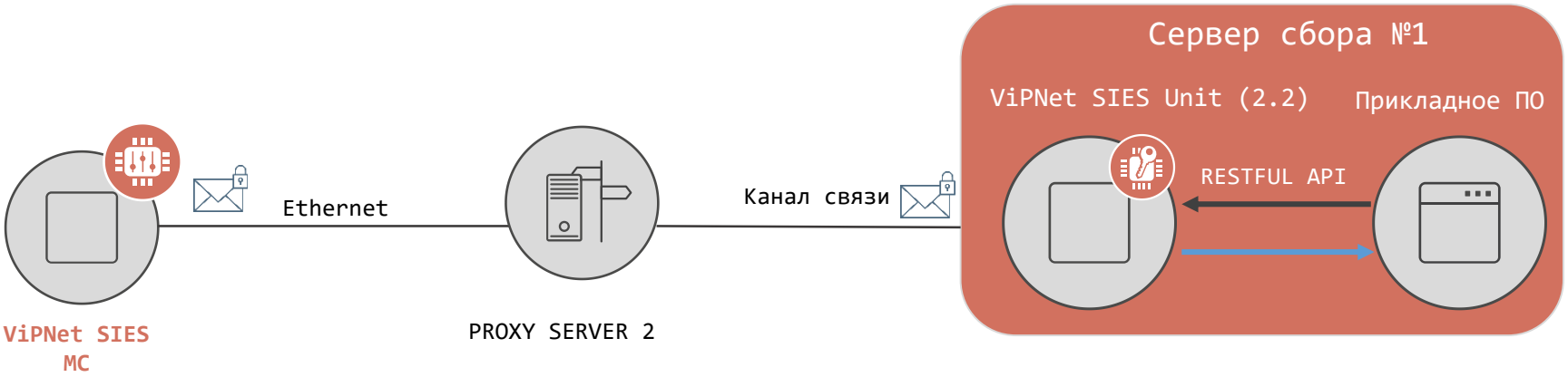
Инициализация ViPNet SIES Unit (через ViPNet SIES Workstation)



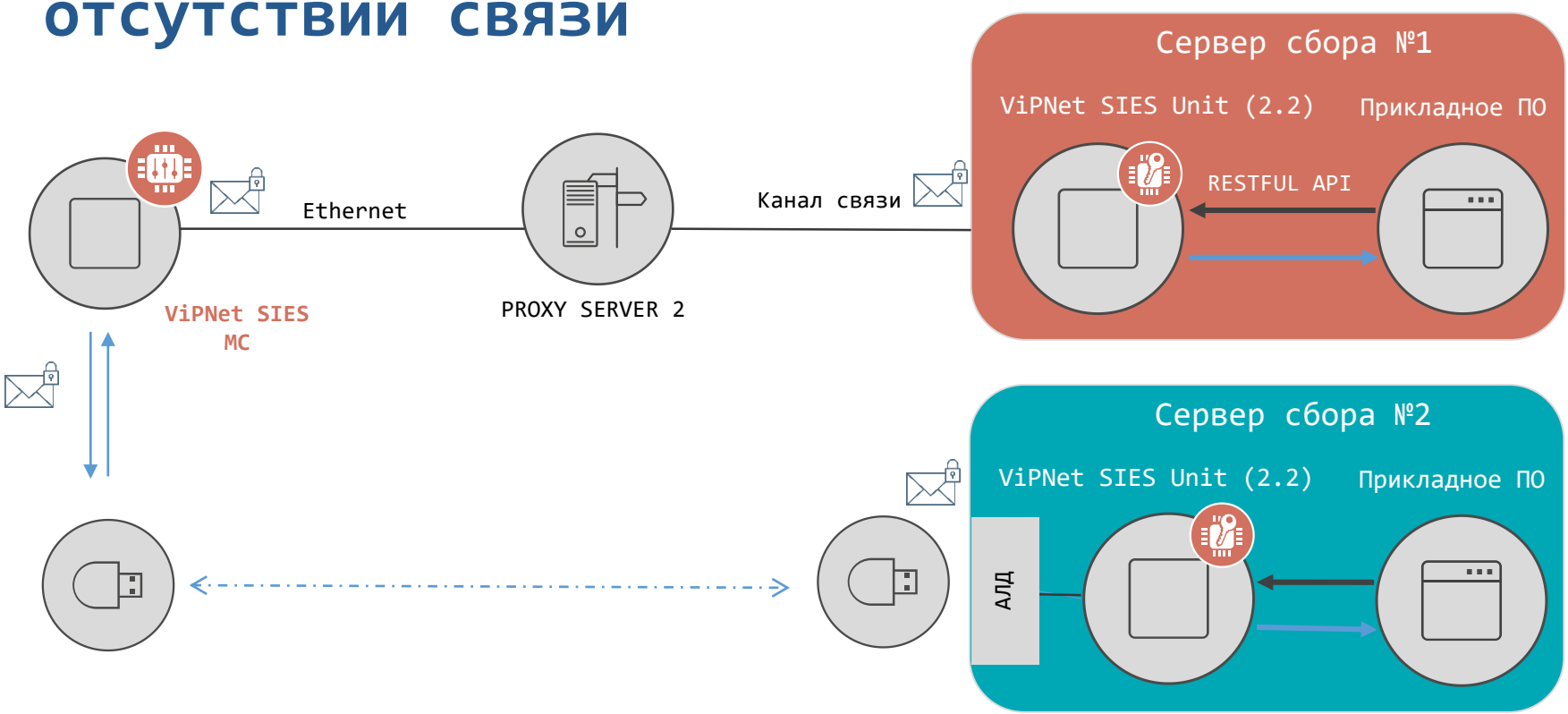
Прямая инициализация ViPNet SIES Unit 2.3



Защищенный обмен между ViPNet SIES Unit и ViPNet SIES MC

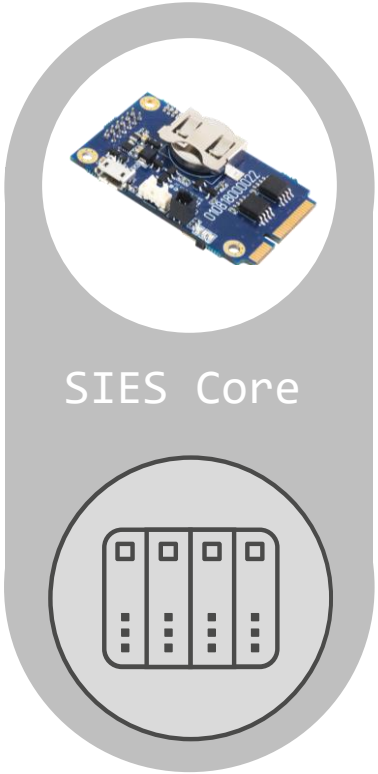


Защищенный обмен между ViPNet SIES Unit и ViPNet SIES MC при отсутствии связи




ViPNet SIES MC:
What’s new?

Объекты управления на уровне АСУ



Сторонний СКЗИ или SIES-узел типа «другой»

Другой SIES-узел

=

Крипто-провайдер

Крипто-библиотека

CRISP-реализация с хранилищем

+

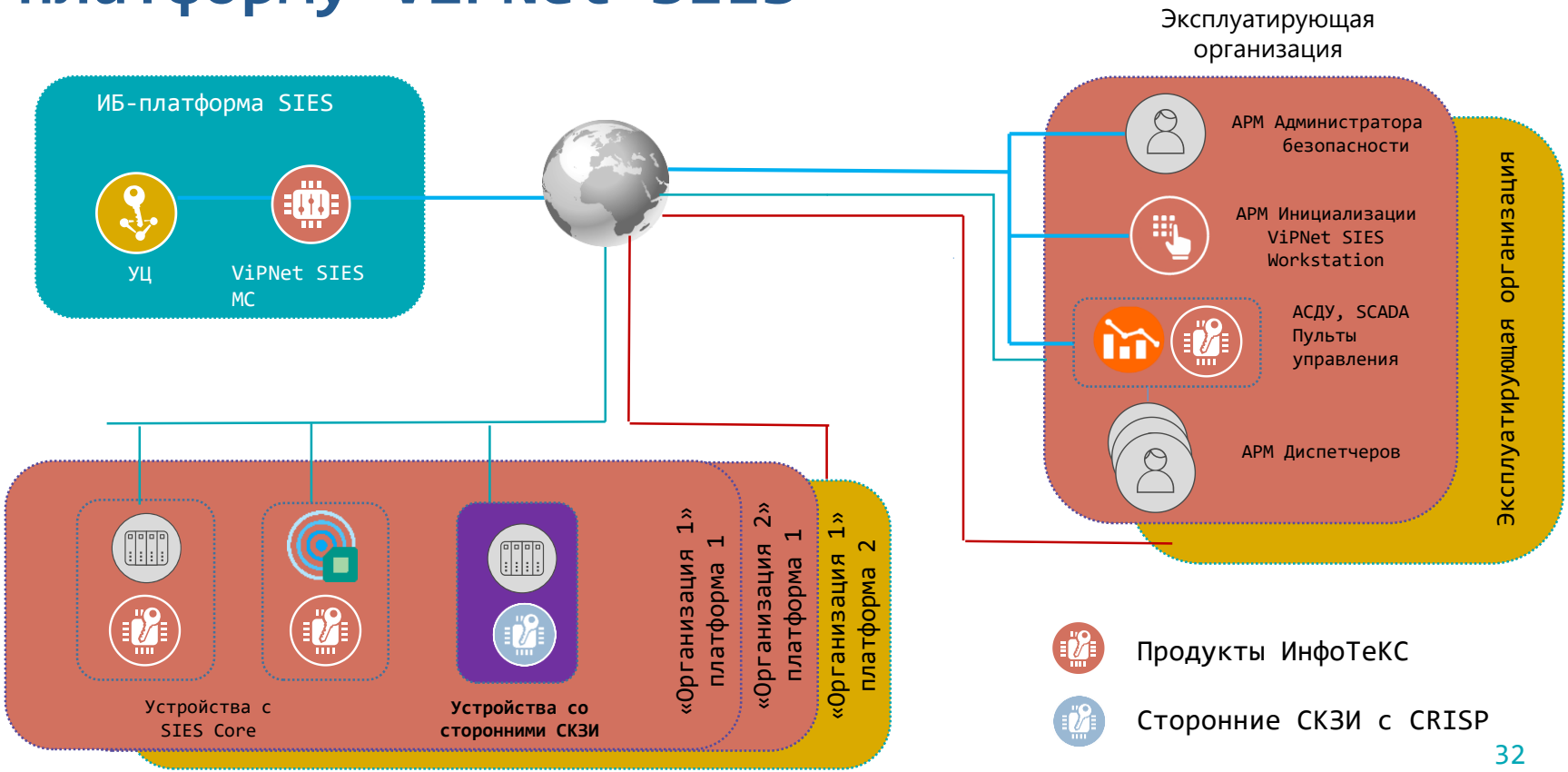
Реализация защищённого транспорта

+

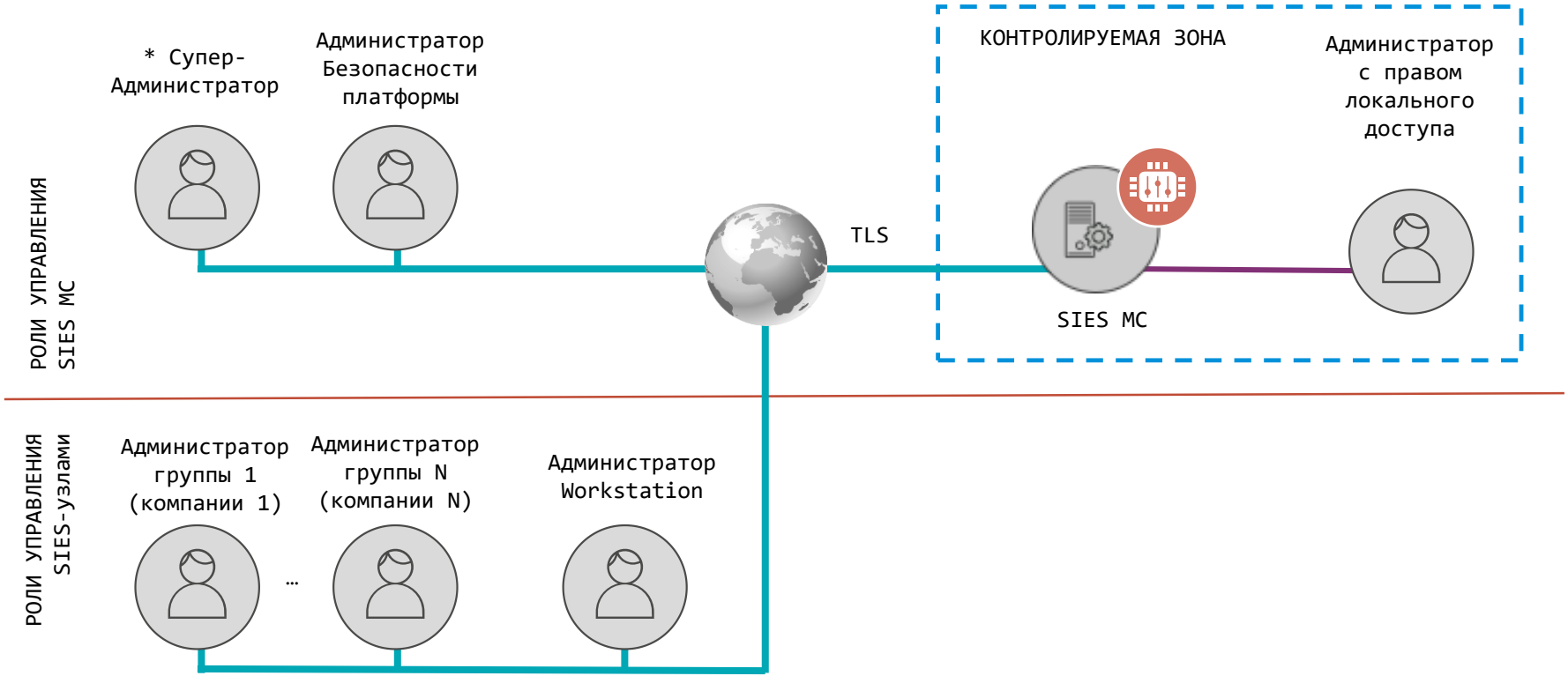
Реализация API команд

API для интеграции в ViPNet SIES MC (опционально)

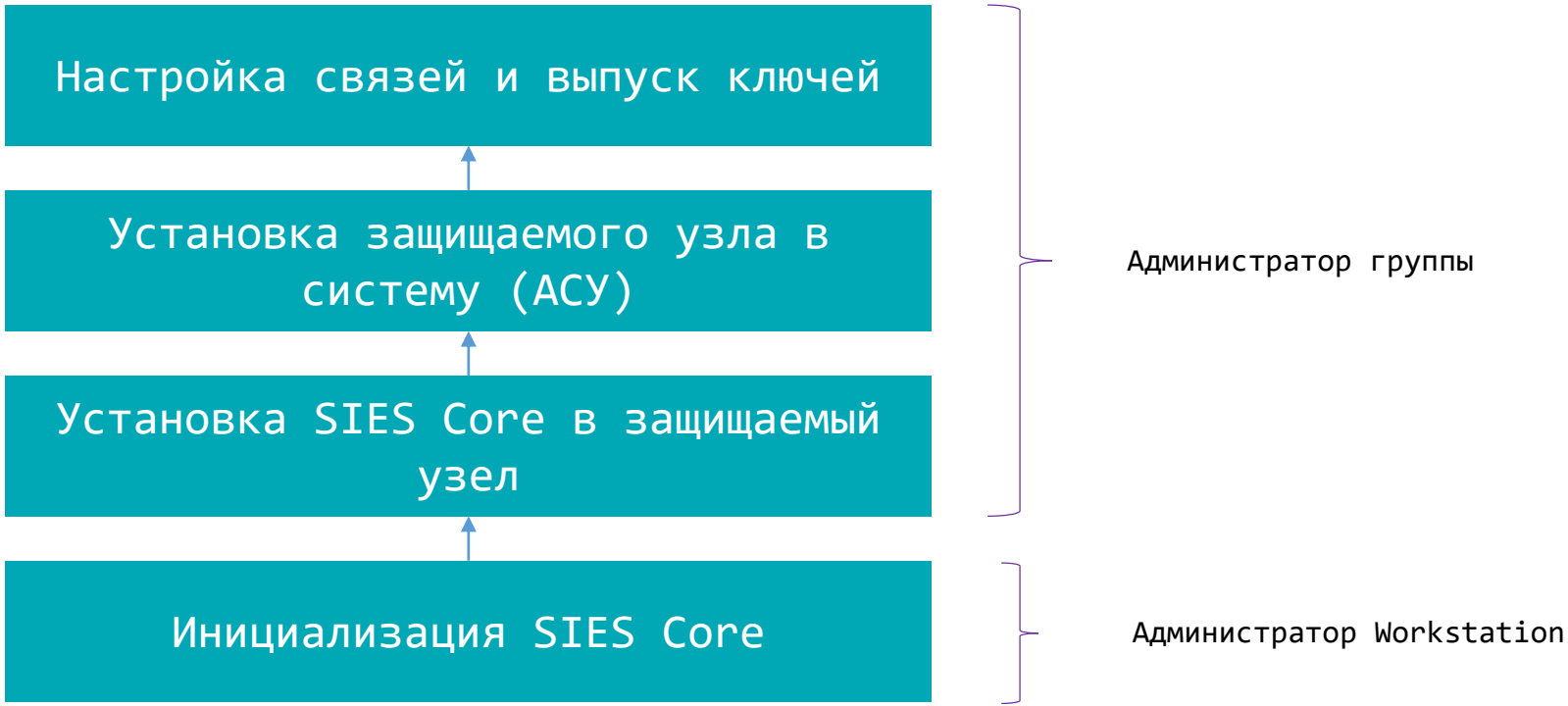
Открытое API для интеграции в платформу ViPNet SIES



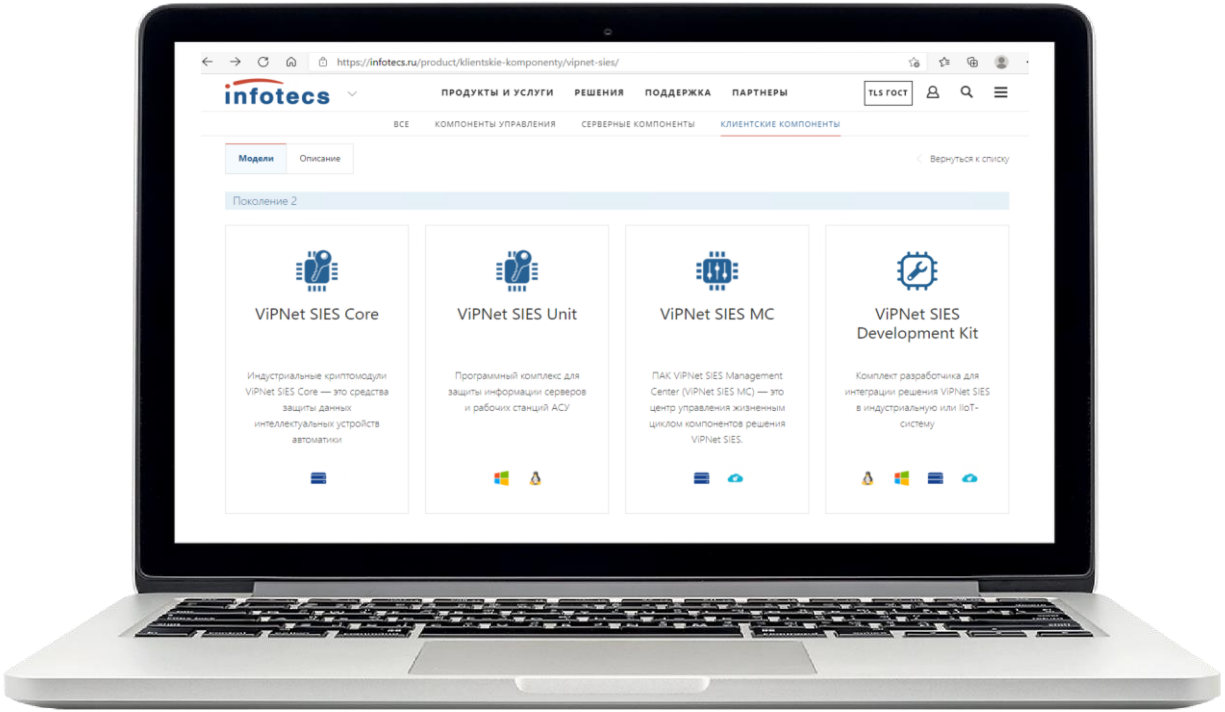
Добавлена роль ViPNet SIES Workstation



Добавлена роль ViPNet SIES Workstation

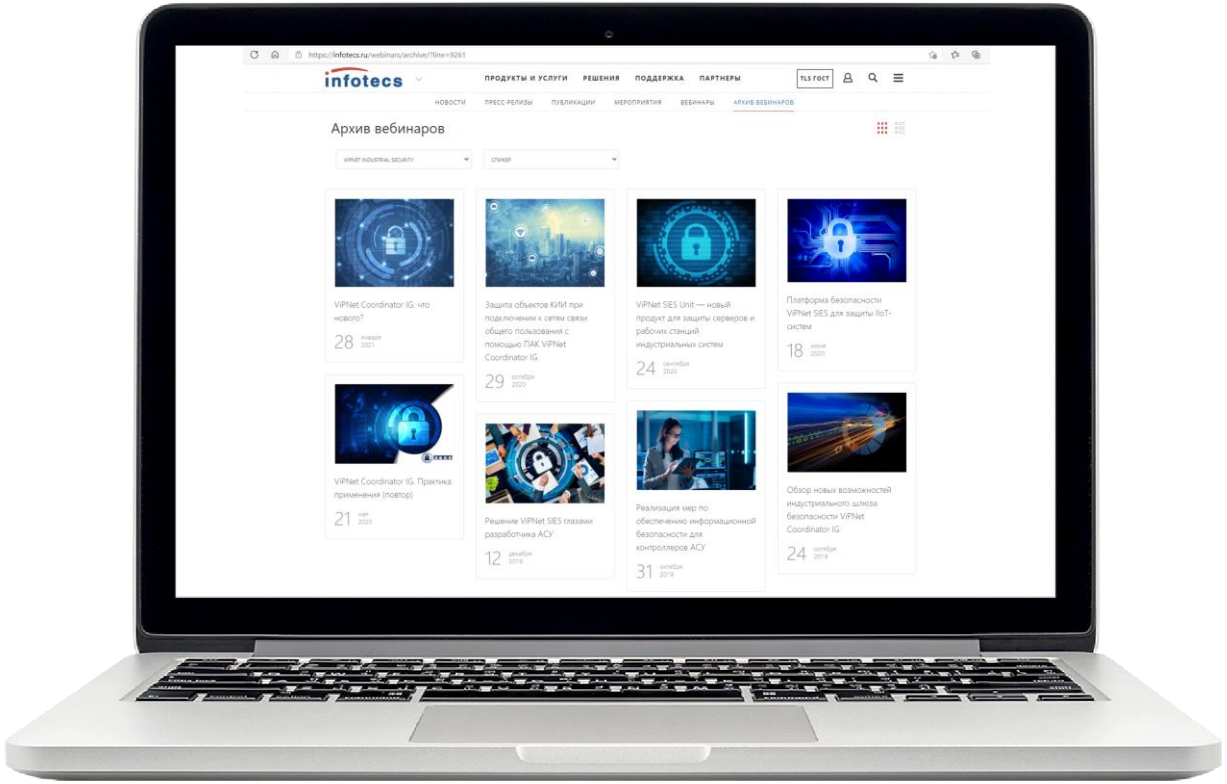


Информация по решению ViPNet SIES



Вся новая информация доступна на сайте – [ViPNet SIES | ИнфоТеКС (infotecs.ru)]

Информация по решению ViPNet SIES



Информация по прошедшим вебинарам (видео и презентации) –

[Архив вебинаров | ИнфоТеКС (infotecs.ru)](https://infotecs.ru/webinars/archive/)

https://infotecs.ru/webinars/archive/