

Платформа безопасности ViPNet SIES для защиты IIoT-систем

Марина Сорокина



Призы для участников вебинара

За самый интересный вопрос



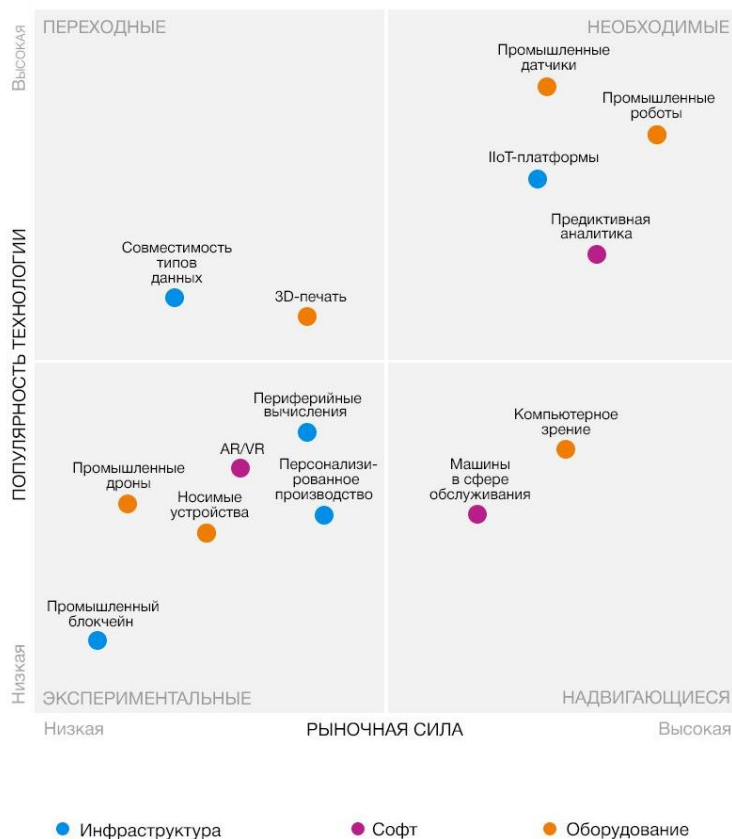
Силиконовая складная бутылка

За активное участие



Шторка для ноутбука и фонарик с функцией заливного света

Рынок IIoT



Технологические тренды в промышленности в 2019 г.

Технологии IIoT (IIoT-платформы и промышленные датчики) – необходимая реальность современного промышленного предприятия

Internet of Things (IoT) – система объединенных компьютерных сетей и подключенных физических объектов (вещей) со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека

Industrial Internet of Thing (IIoT) – интернет вещей для корпоративного / отраслевого применения - система объединенных компьютерных сетей и подключенных промышленных (производственных) объектов со встроенными датчиками и ПО для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека.

Рынок IIoT/M2M (на 2018 г)



Мировой
рынок IIoT
([IoT Analytics](#) на 2018г)

\$ 64 млрд.

Количество
соединений в
мире

407 млн.

Российский
рынок IIoT
(IDC на 2018 г)

**235 млрд.
руб.**

Количество
подключенных
устройств

15,9 млн.

Рынок IIoT/M2M к 2026 году

GLOBAL IIOT MARKET, EXECUTIVE SUMMARY

By SOFTWARE

DISTRIBUTION MANAGEMENT SYSTEM
FARM MANAGEMENT SYSTEM
REMOTE PATIENT MONITORING SYSTEM

By TECHNOLOGY

CAMERA
CONDITION MONITORING
INDUSTRIAL ROBOTICS
RFID



By GEOGRAPHY

OVERVIEW
NORTH AMERICA
EUROPE
ASIA PACIFIC
REST OF THE WORLD

COMPANY PROFILES

CISCO SYSTEMS, INC
GE
HONEYWELL
INTEL CORPORATION
IBM CORPORATION

GLOBAL IIOT MARKET OPPORTUNITIES AND FORECAST



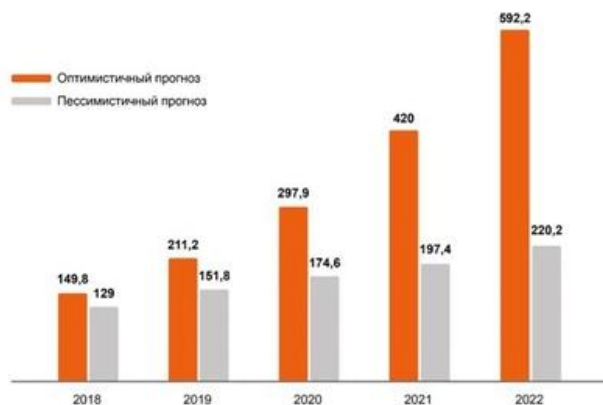
GLOBAL MARKET IS EXPECTED
TO REACH **US\$ 103.38 Bn**
BY 2026 GROWING AT A CAGR OF
6.7%

Рынок промышленного «интернета вещей» (IIoT): Россия и мир

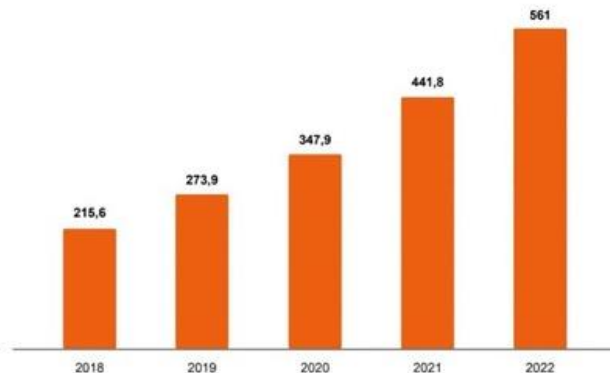
ГЛОНАСС-ТМ

Прогноз объема рынка интернета вещей в России,
2018-2022 гг., млрд. руб.

Прогноз объема рынка интернета вещей в мире,
2018-2022 гг., млрд. долл.



Источник: ГидМаркет



Источник: Statistics MRC

Информационная безопасность IIoT-систем



60% протоколов IIoT/ M2M не имеют встроенных механизмов защиты

80% протоколов IIoT/ M2M беспроводные

26% компаний внедрило криптографическую защиту в свои устройства



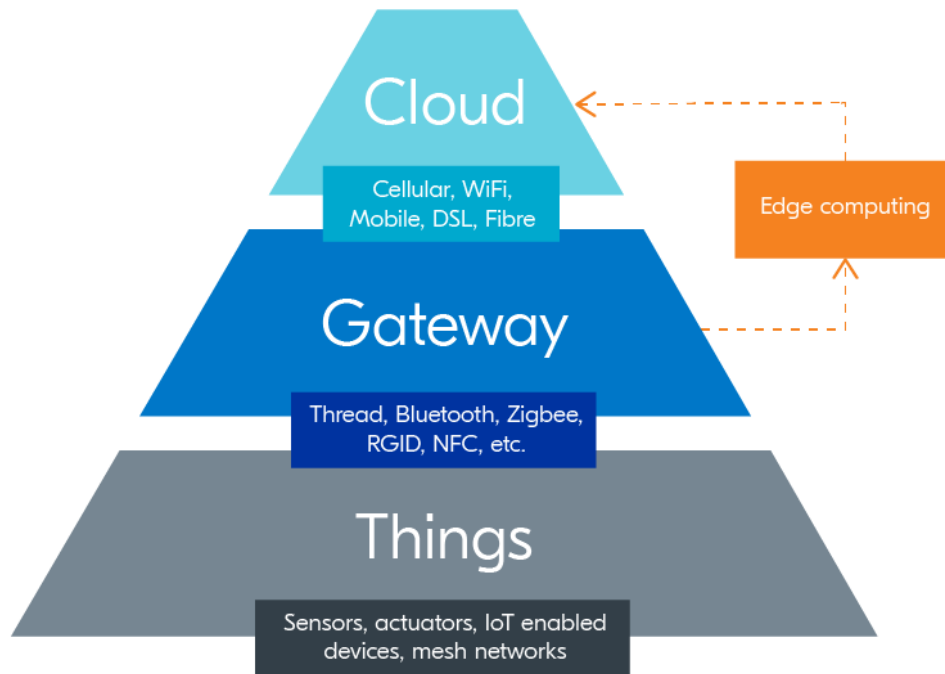
MIRAI - самая масштабная DDoS-атака в мире (2016 г) была проведена с использованием IIoT устройств

60% IIoT устройств используется для DDoS-атак

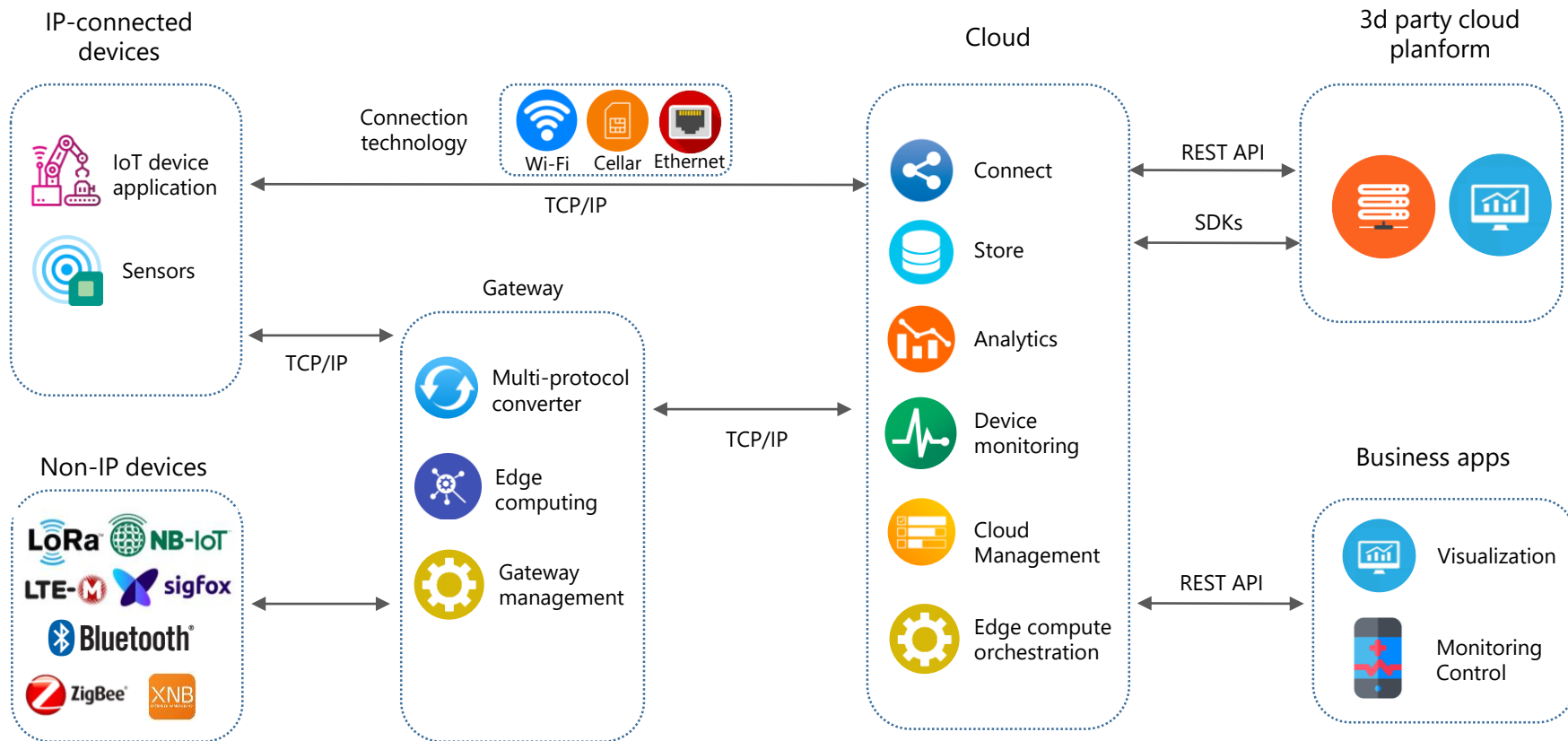
\$13,2 млн теряют компании в энергетической и коммунальной отраслях ежегодно из-за атак на IIoT-устройства

Архитектура IIoT системы

Структура IIoT системы



Архитектура IIoT-системы



Принцип работы IIoT-системы



Архитектура и особенности с точки зрения ИБ



Отсутствие
периметра



Территориально-
распределенное
размещение



Работа от
«батарейки»



Малые
вычислительные
ресурсы
устройств



Множество не
стандартизированных
протоколов



Возможность
физического
доступа



Высокая
латентность
полевых
протоколов

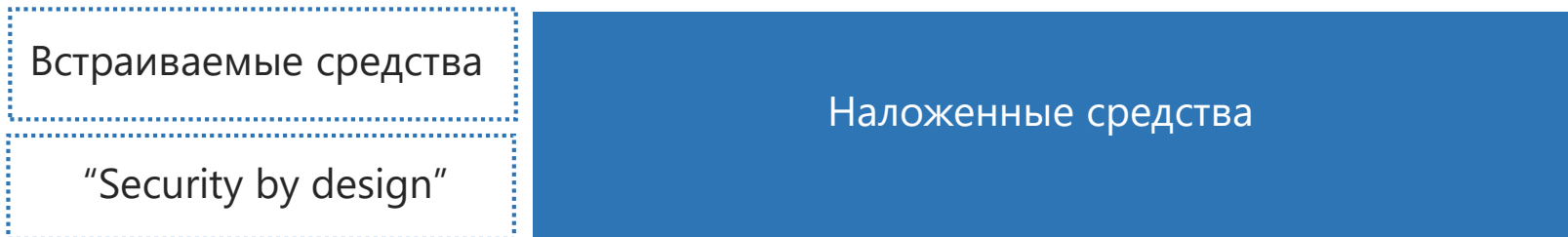


Низкая пропускная
способность полевых
протоколов



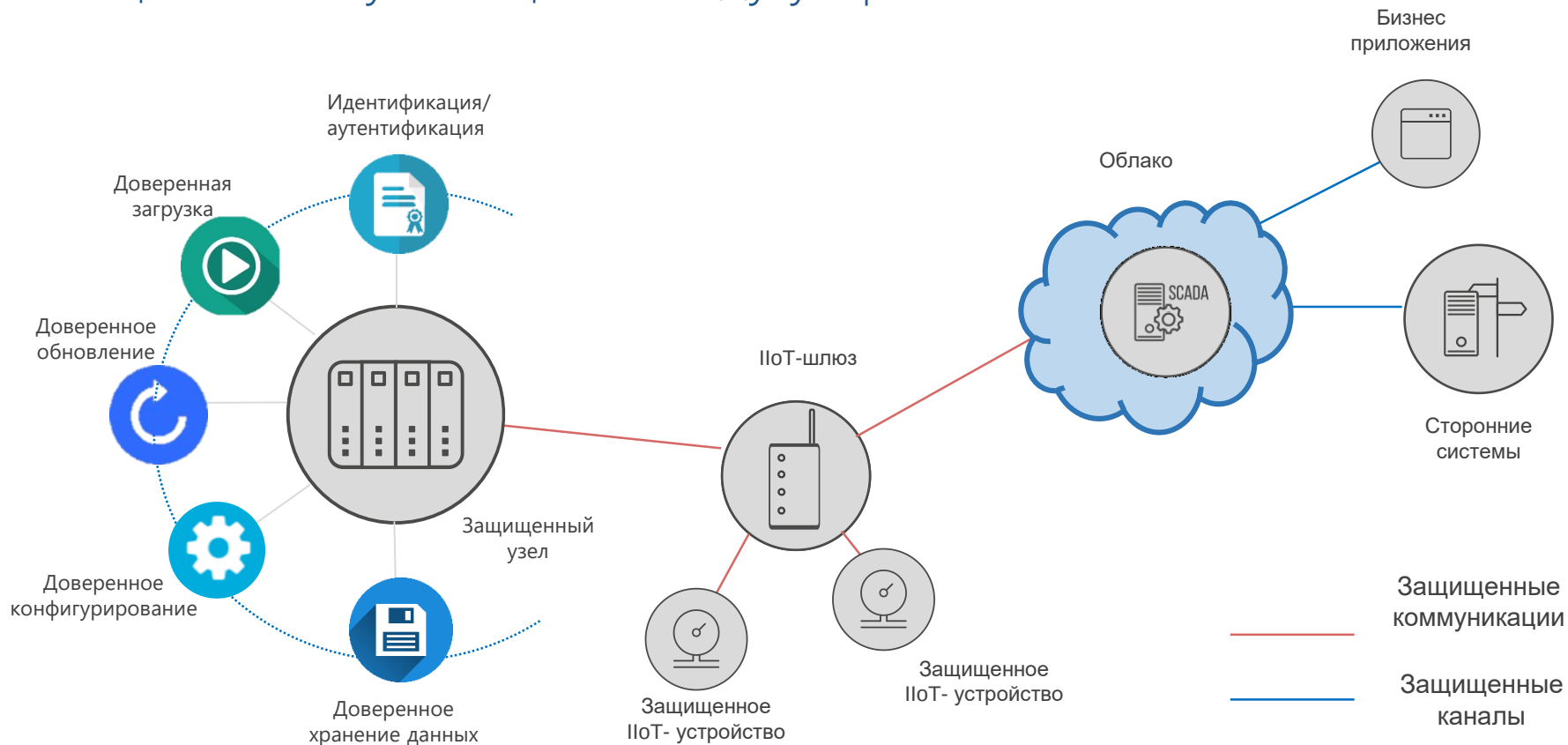
Групповые
операции

Средства защиты информации для IIoT/M2M

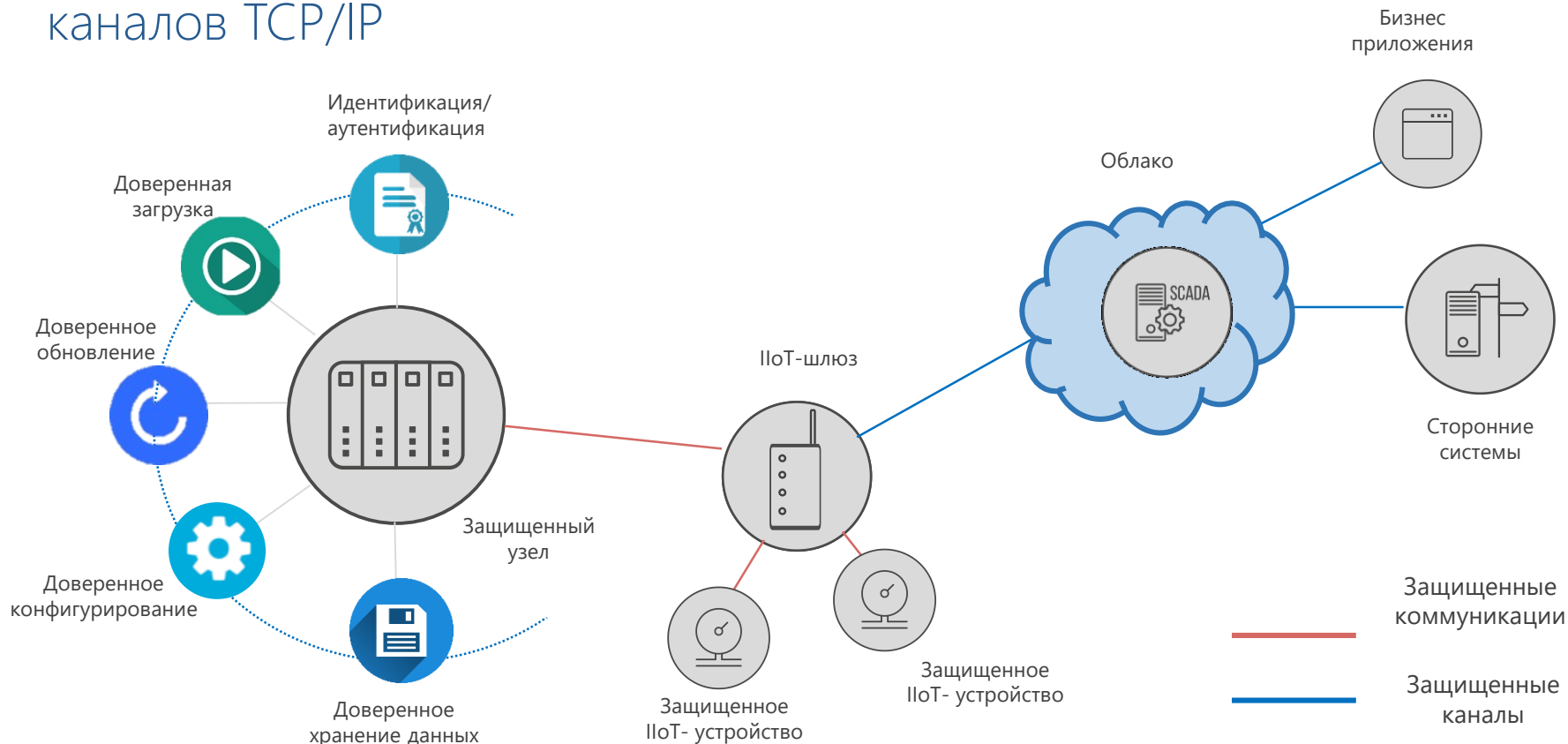


Как защитить IIoT систему?

Защита IIoT = защита конечных устройств + защита коммуникаций между устройствами

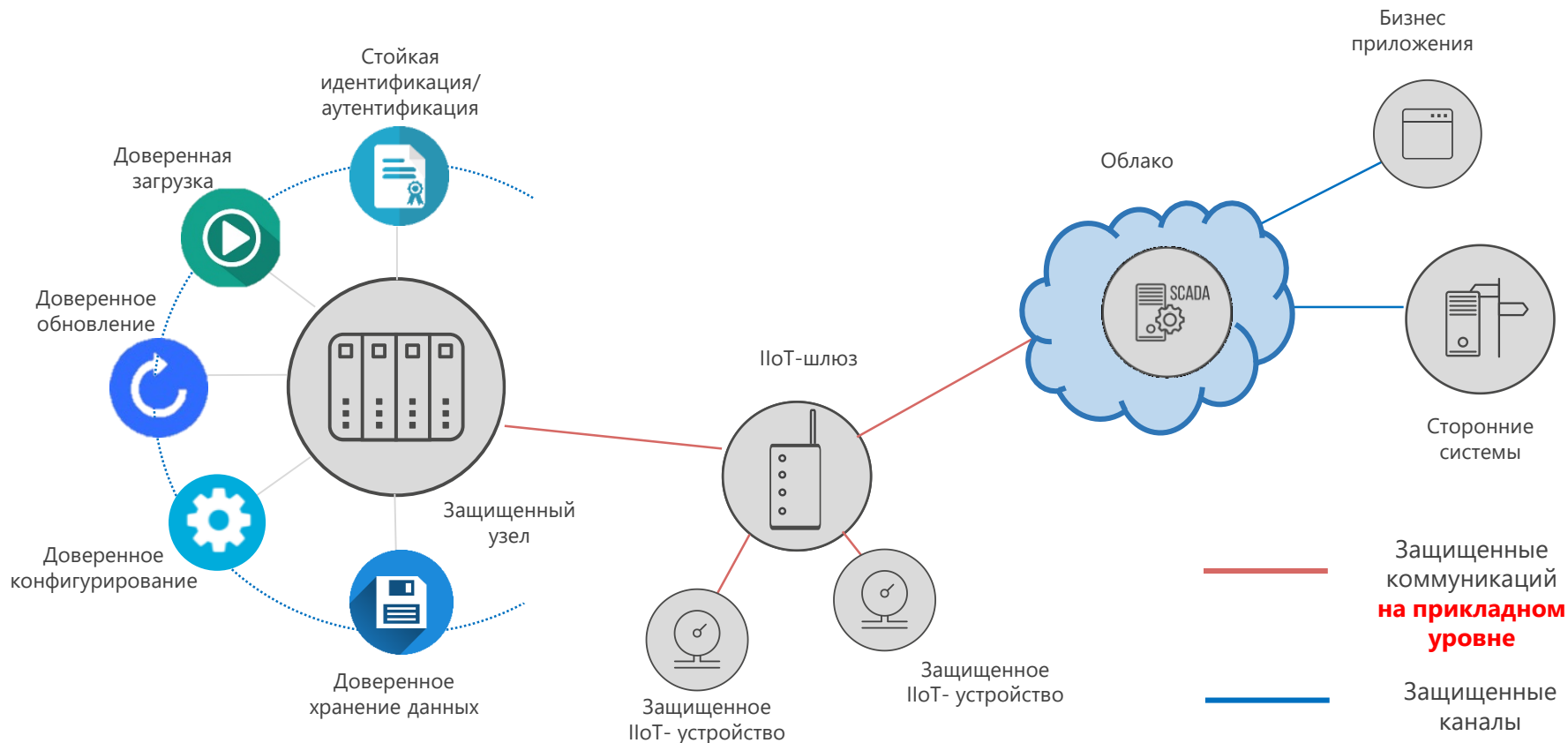


Защита IIoT = защита конечных устройств + защита коммуникаций между устройствами + + защита каналов TCP/IP



Как защитить IIoT систему в России?

Защита IIoT в России = защита коммуникаций на прикладном уровне + защита конечных устройств



Решение ViPNet SIES

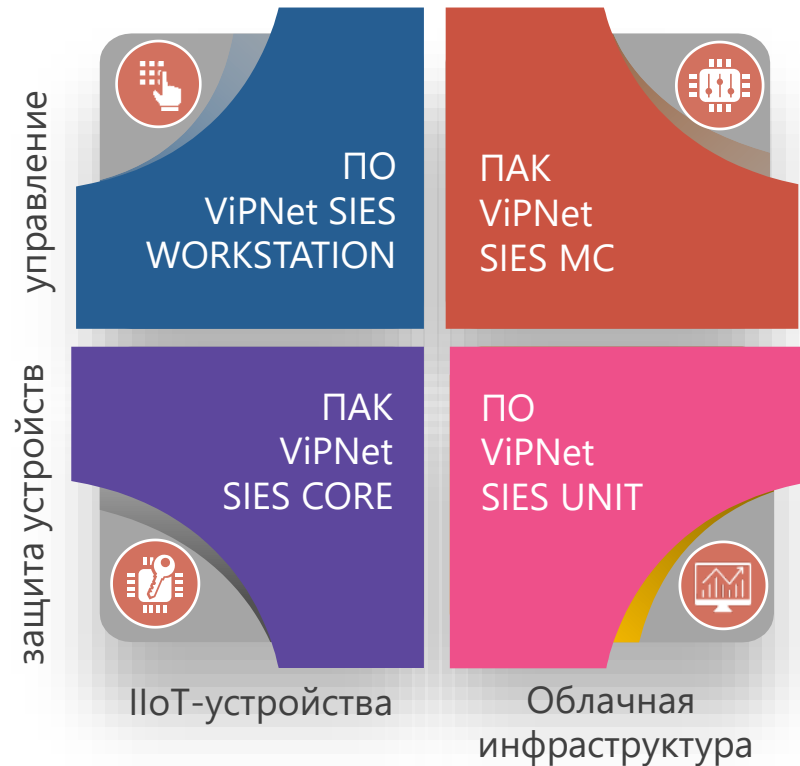


ВСТРАИВАЕМЫЕ КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА
ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ УСТРОЙСТВ
АВТОМАТИЗАЦИИ И IIOT-УСТРОЙСТВ.

ПРОДУКТЫ РЕШЕНИЯ ПОЗВОЛЯЮТ УСТРОЙСТВАМ
РЕАЛИЗОВЫВАТЬ КОНЦЕПЦИЮ «SECURITY BY
DESIGN»

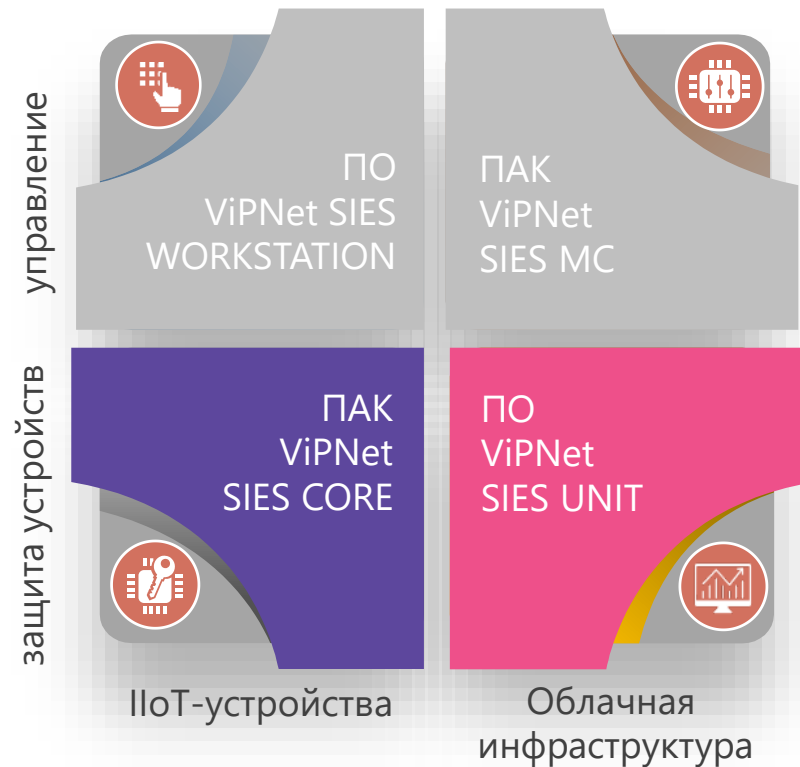
ЗАЩИТА КОММУНИКАЦИЙ • ЗАЩИТА КОНЕЧНЫХ УЗЛОВ • ЗАЩИТА ДАННЫХ • АУТЕНТИФИКАЦИЯ И ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Состав решения ViPNet SIES



- СКЗИ класса КС1 и КС3
- Возможность использования криптографии на разных по вычислительной мощности устройствах для полевого уровня
- Нет зависимости от ОС и архитектуры устройств
- Возможность реализации security-by-design при разработке устройств

Защита IoT-устройств, IoT-шлюзов и IoT-серверов



- СКЗИ класса КС1 и КС3
- Возможность использования криптографии на разных по вычислительной мощности устройствах для полевого уровня
- Нет зависимости от ОС и архитектуры устройств
- Возможность реализации security-by-design при разработке устройств

Сертификация ViPNet SIES Core и ViPNet SIES Unit

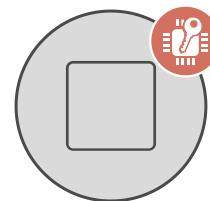
ViPNet SIES Core



СКЗИ класса КС1 и КС3 по требованиям
ФСБ России:

- Получено положительное заключение (04.2020)
- Ожидание сертификата (06.2020)

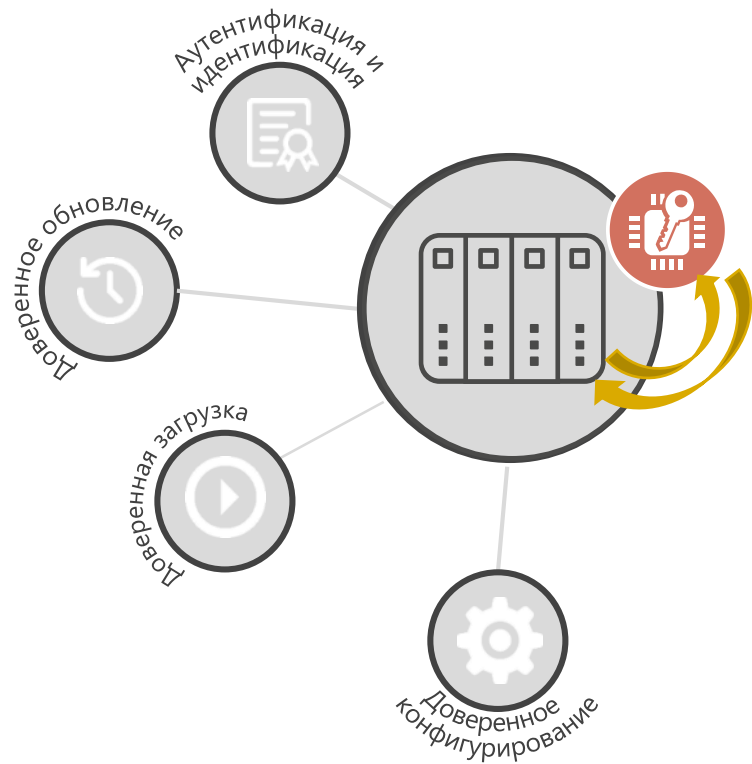
ViPNet SIES Unit



СКЗИ класса КС1 и КС3 по требованиям
ФСБ России:

- Получен сертификат (06.2020) по контролю изменений на ViPNet PKI Client с SIES Unit

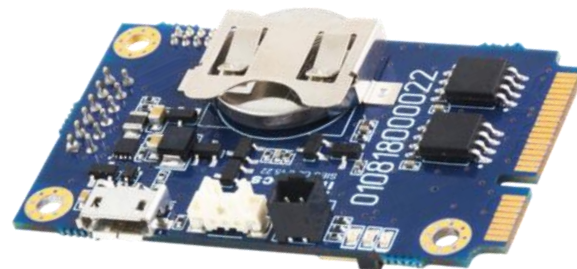
Защита конечных устройств с помощью ViPNet SIES Core и ViPNet SIES Unit



- Создание «корня доверия» для устройства
- Хранение ключевой информации
- Предоставление криптографического сервиса для устройства в виде ответов на запрос
- Белый список команд

ViPNet SIES Core

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



Интеграция ПАК SIES Core

- На аппаратном уровне – USB, UART, SPI
- На программном уровне – SIES Core API (RATP+прикладной протокол)

ОБЛАЧНАЯ СИСТЕМА ОБРАБОТКИ (SCADA, OPC-СЕРВЕРА)



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)



Криптографические
операции, доступные
защищаемым
устройствам



Защита конечных устройств



infotecs



Защита онлайн коммуникаций

Криптографические операции, доступные защищаемым устройствам

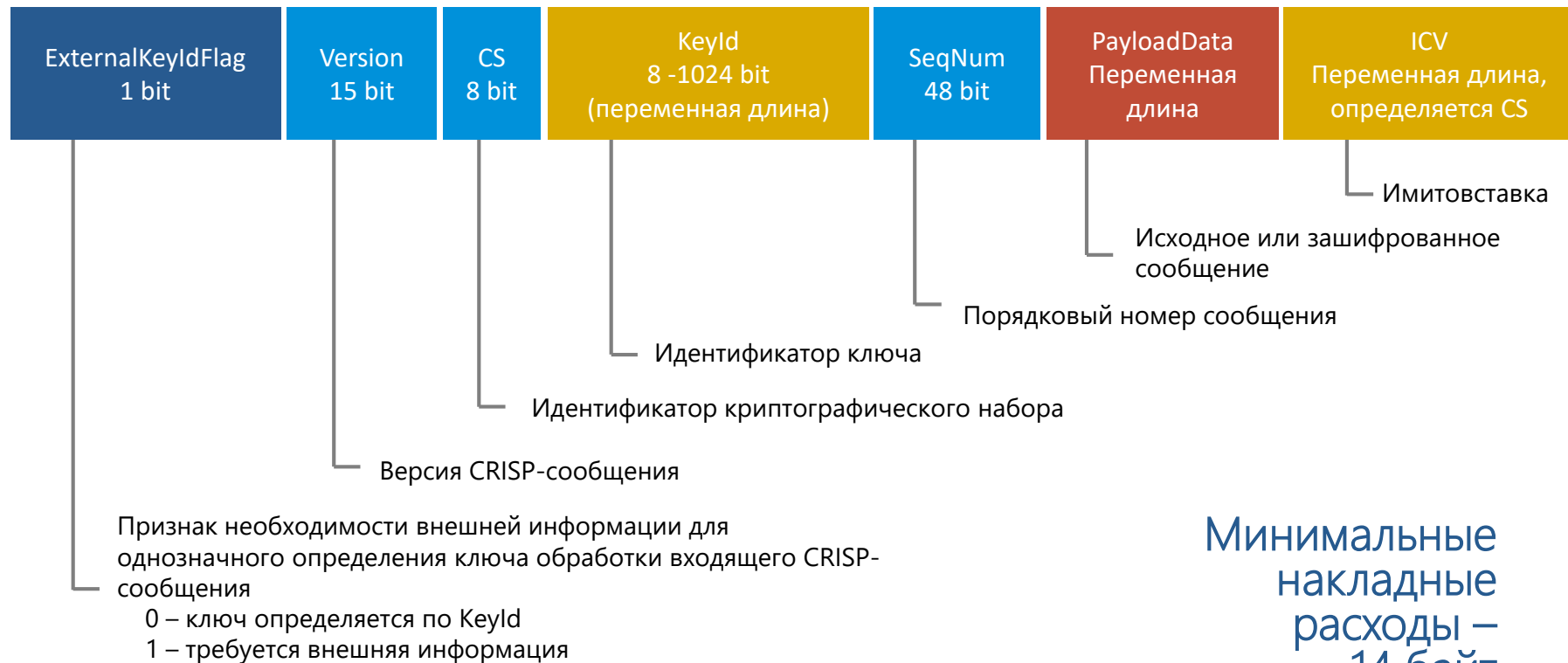
Р 1323565.1.029-2019. Протокол защищенного обмена CRISP



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

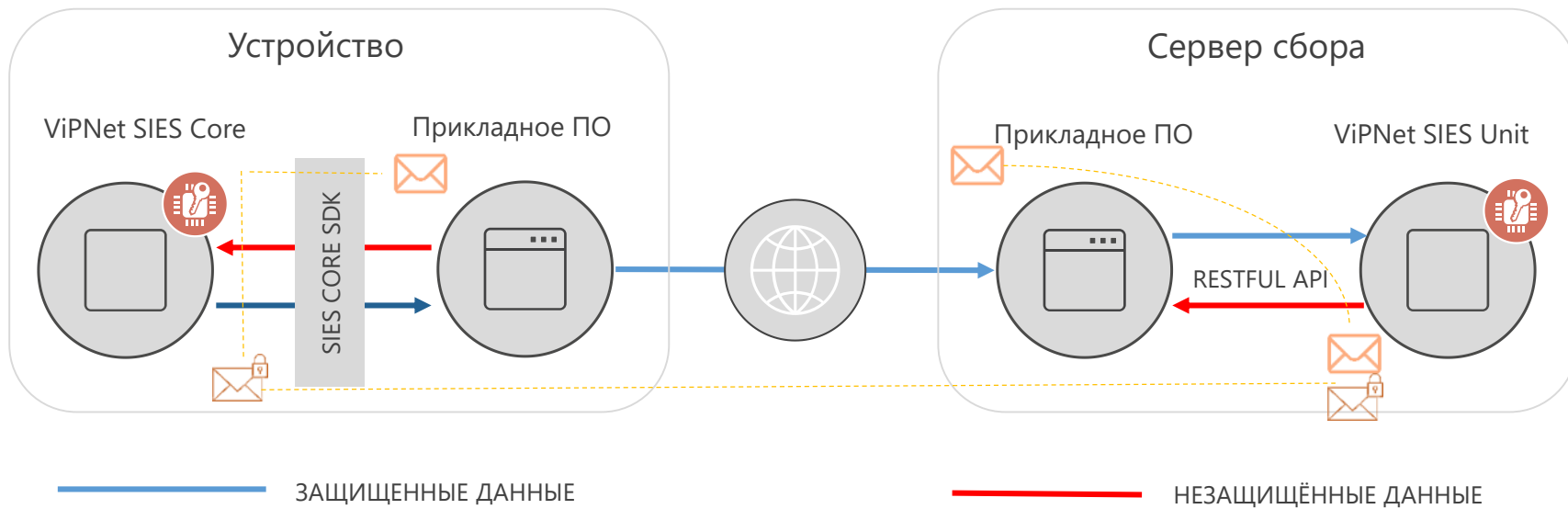
- Обеспечение целостности
- Обеспечение конфиденциальности (опционально)
- Защита от навязывания повторных сообщений
- Окно принятых сообщений
- Общий секретный ключ
- Защита данных – блочный шифр, имитовставка
- Поддержка адресных (один-к-одному) сообщений
- Поддержка многоадресных (один-ко-многим, подписочная модель) сообщений
- Явная и неявная адресация абонентов

Структура CRISP-сообщения

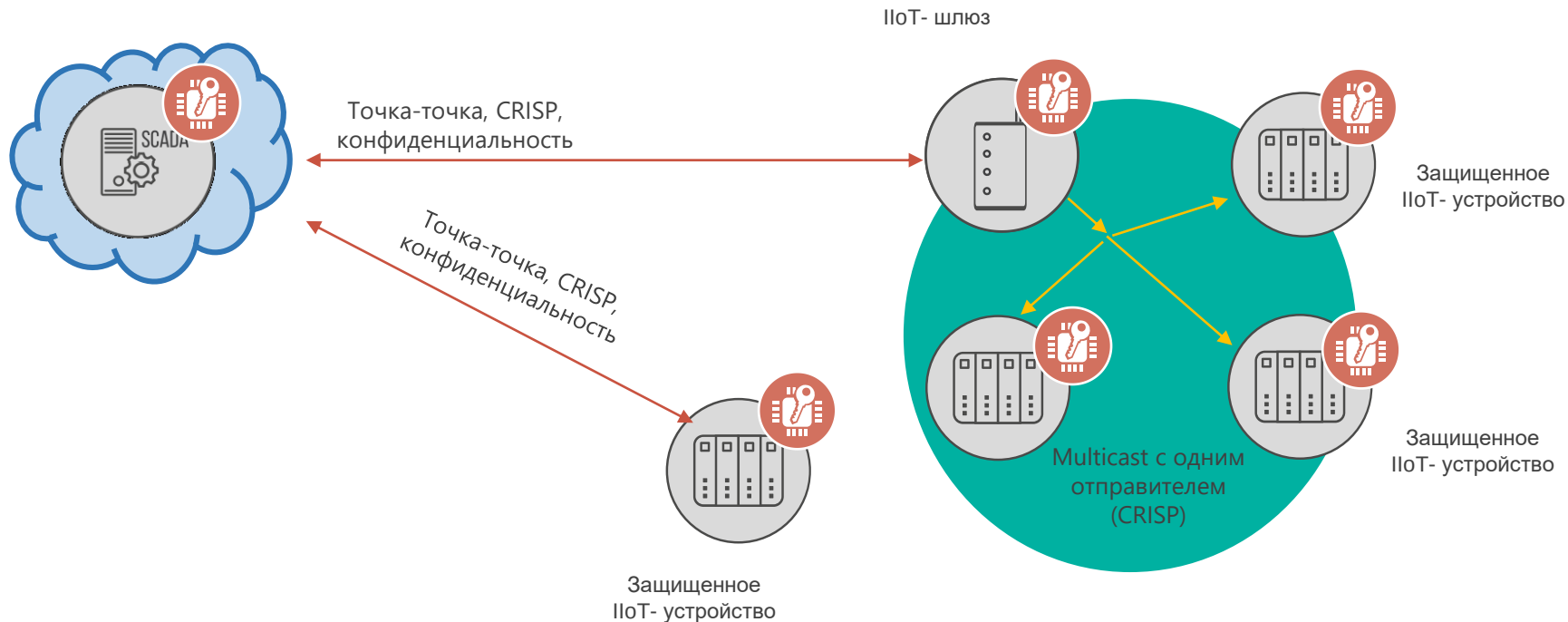


Минимальные
накладные
расходы –
14 байт

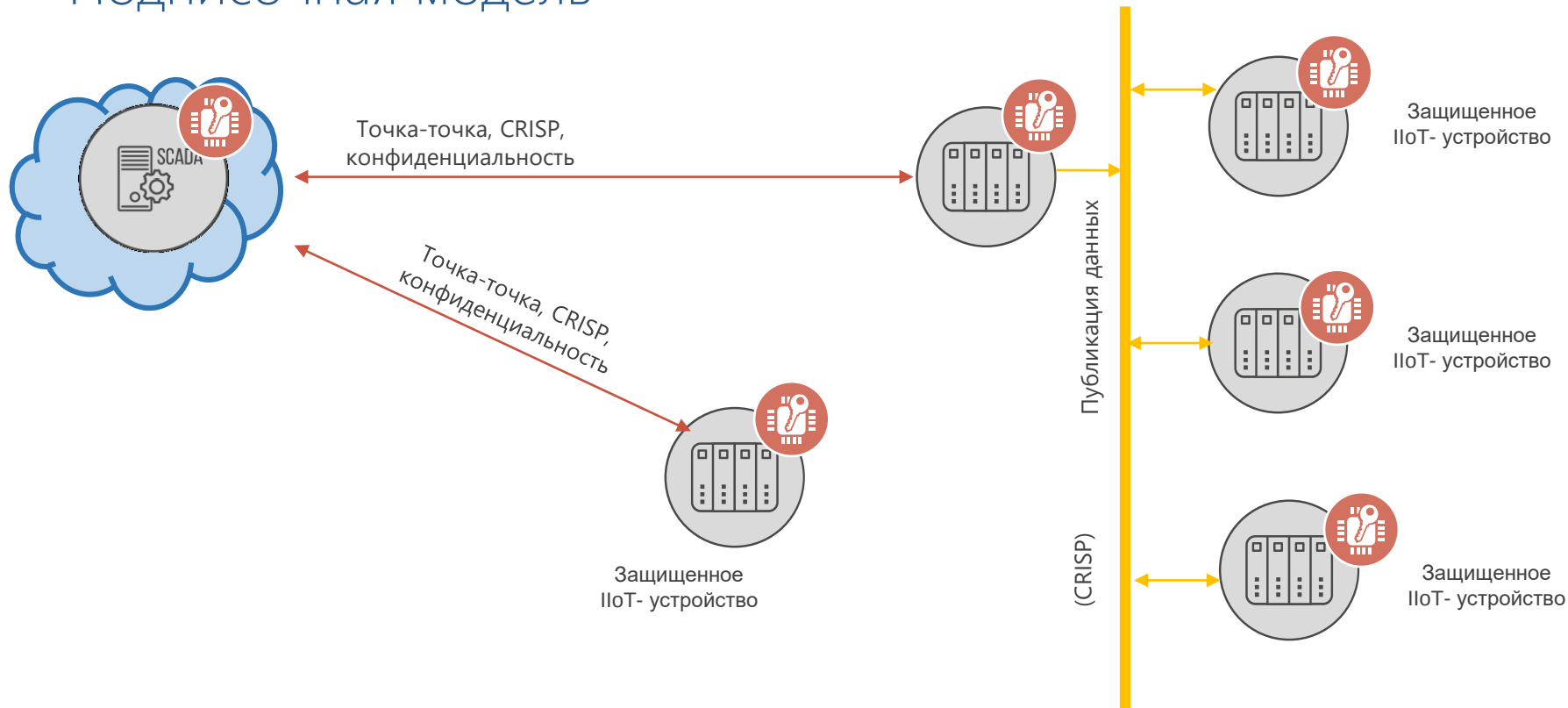
Защита коммуникаций точка- точка с помощью CRISP



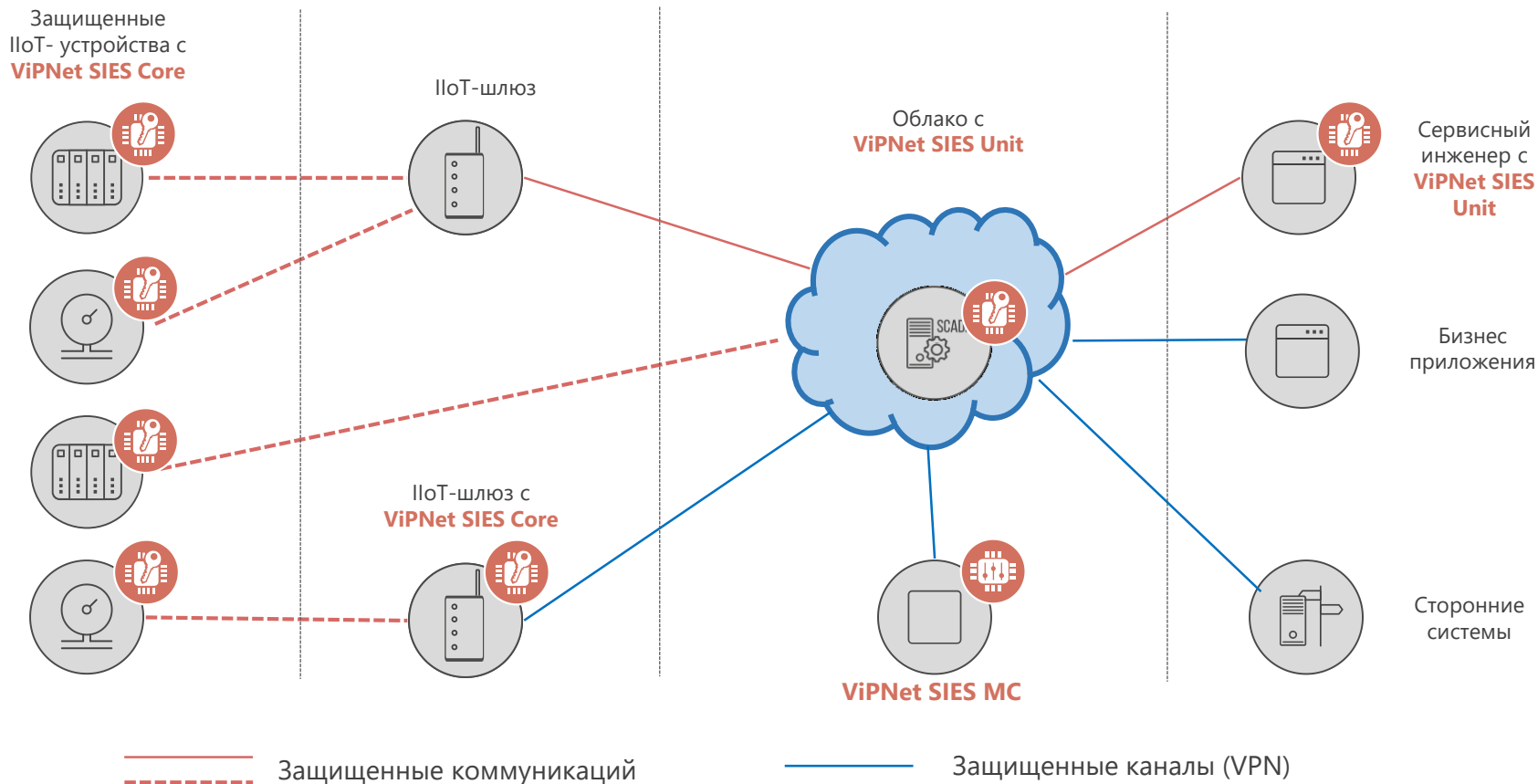
Защита многоадресных сообщений: Multicast с одним отправителем



Защита многоадресных сообщений: Подписочная модель



Защищенная IIoT система

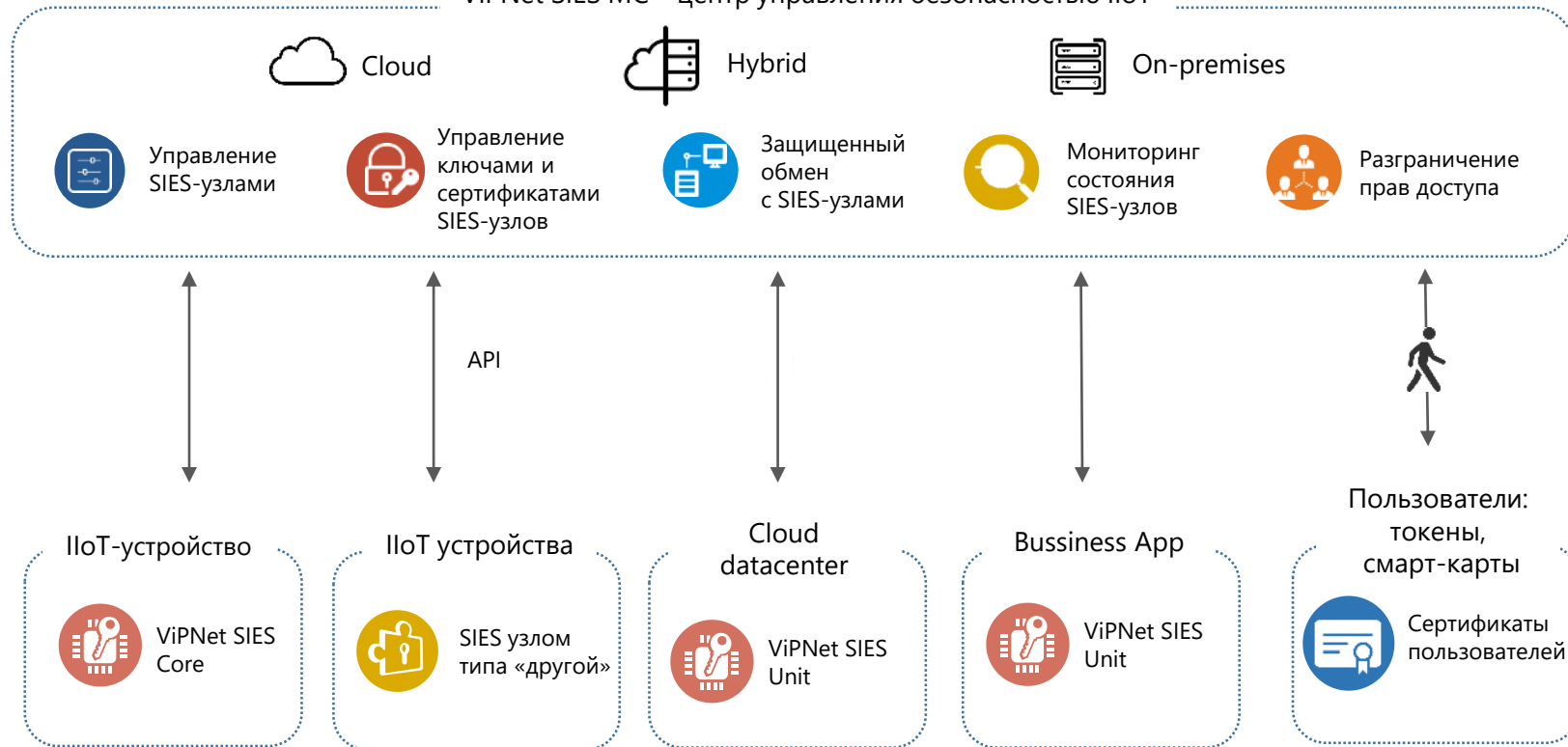




Платформа ViPNet SIES

Платформа ViPNet SIES

ViPNet SIES MC – центр управления безопасностью IIoT



Возможности



Простота
управления
системой
безопасности



Дистанционное
управление
ключевой
информацией



Центр генерации
ключей и
удостоверяющий
центр



Управление
активами

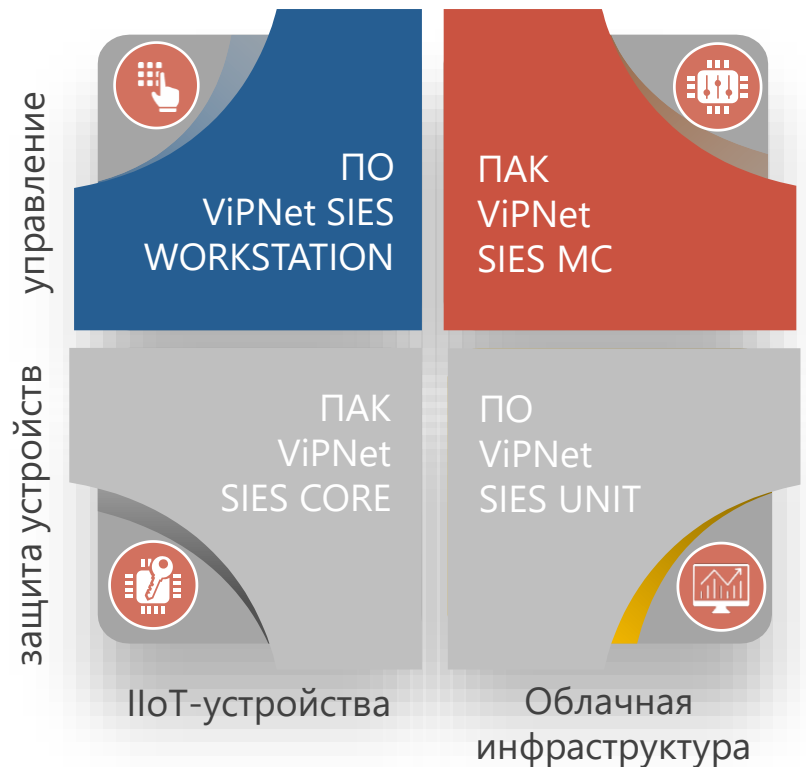


Интеграция
сторонних СКЗИ



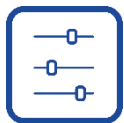
Ролевая модель
доступа

Средства управления ViPNet SIES – основа платформы ViPNet SIES



- ViPNet SIES MC – управления решением SIES и основа платформы SIES
- ViPNet SIES Workstation - средство инициализации и локального обслуживания ViPnet SIES Core и ViPNet SIES Unit

Функциональность ViPNet SIES MC



Управление
SIES-узлами



Управление
ключами и
сертифика-
тами SIES-
узлов



Защищенный
обмен
с SIES-узлами



Мониторинг
состояния
SIES-узлов



Настройка
SIES MC



Разграничение
прав доступа
к решению
SIES

Исполнения ViPNet SIES MC



ViPNet SIES MC10000

- Max: 10000-узлов
- Max: 1000 администраторов безопасности
- Сертификация как СКЗИ КС3 по требованиям ФСБ России



ViPNet SIES MC3000

- Max: 3000-узлов
- Max: 300 администраторов безопасности
- Сертификация как СКЗИ КС3 по требованиям ФСБ России



ViPNet SIES MC VA

- Max: 5000-узлов
- Max: 500 администраторов безопасности
- Сертификация как СКЗИ КС1 по требованиям ФСБ России

Объекты управления SIES MC: SIES-узлы



ПАК ViPNet SIES
Core



ПО ViPNet SIES
Unit

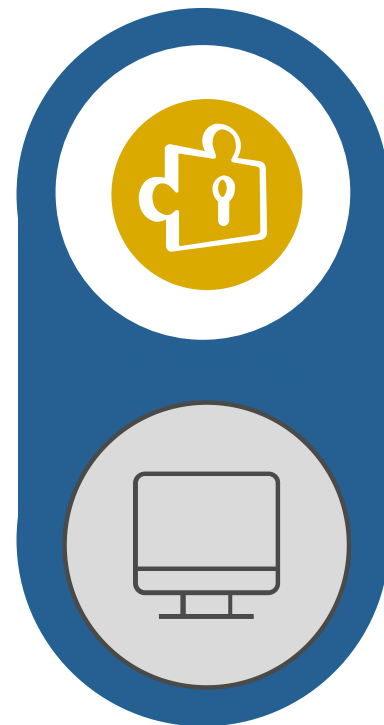
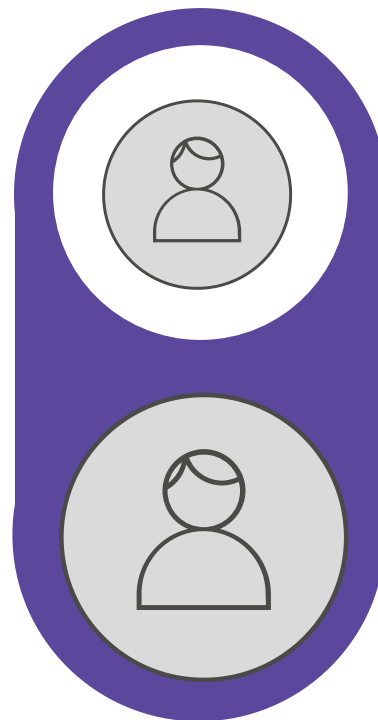
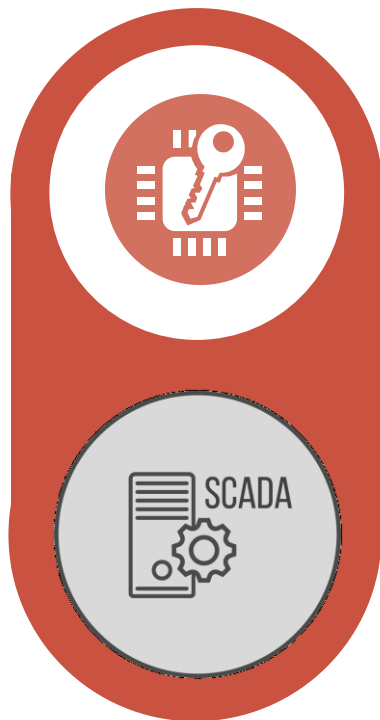
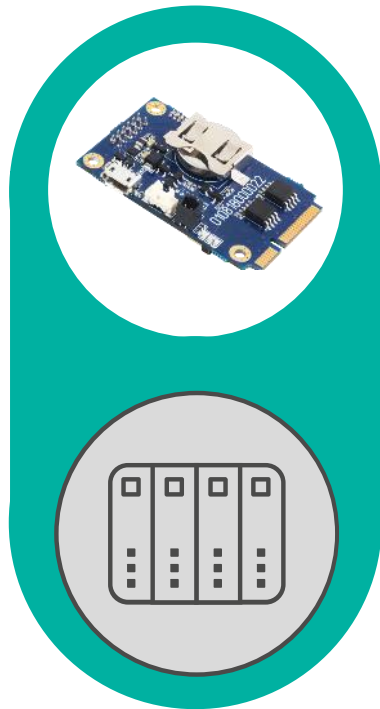


Пользователь АСУ
Сервисный инженер,
Инженер КИП



Другой SIES-узел
Криптопровайдеры
и прочие PKI-продукты
CRISP-узлы

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



Управление ключами и сертификатами SIES-узлов и криптографическими функциями



Выпуск, смена,
компрометация
служебных
(транспортных)
ключей и
сертификатов



Выпуск, смена,
компрометация
прикладных
ключей и
сертификатов (PKI),
работа с CRL



Выпуск, смена,
компрометация
прикладных
симметричных
ключей для CRISP
(парных и
групповых)



Датчик случайных
чисел для
SIES-узлов



Управление
журналами
аудита SIES-
узлов

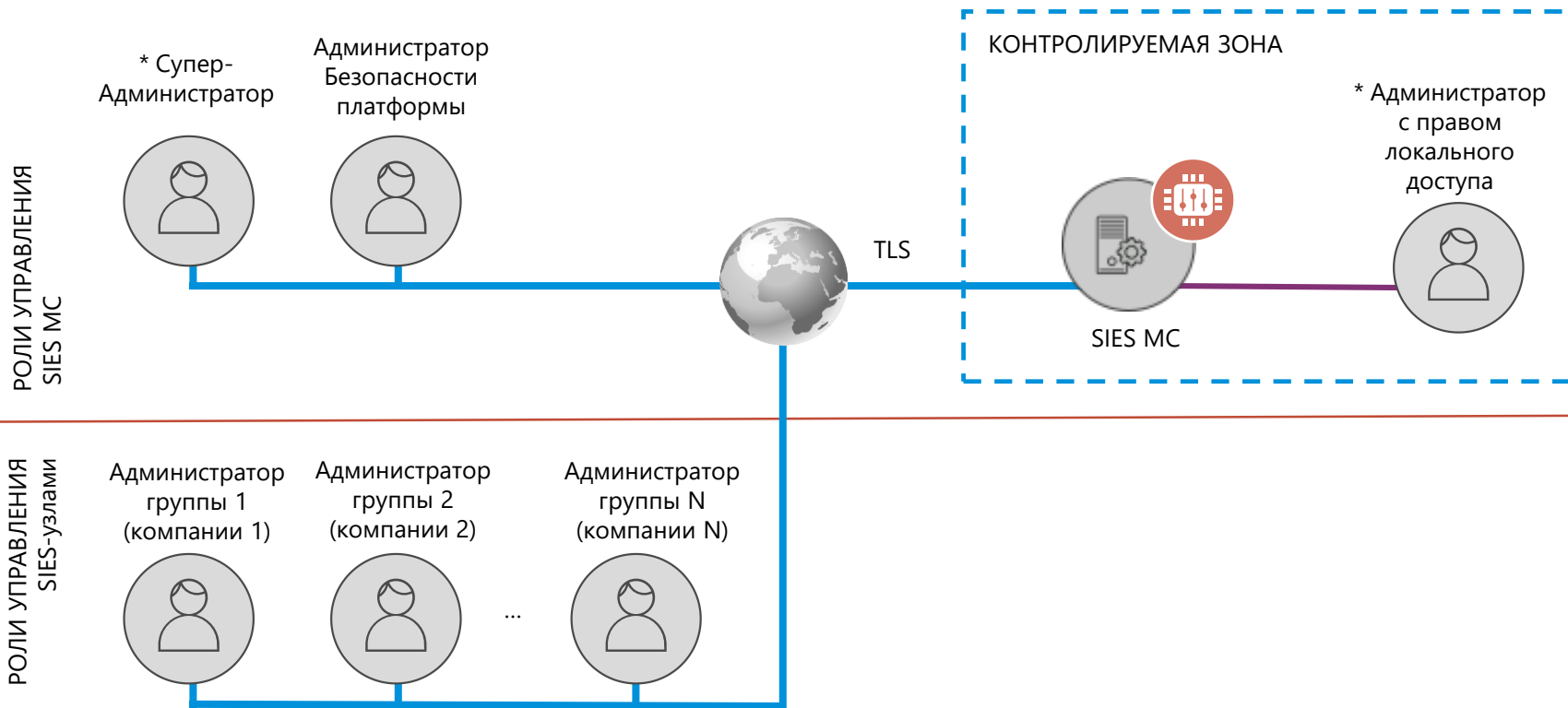


Регламентный
контроль

SIES-узел типа «другой»



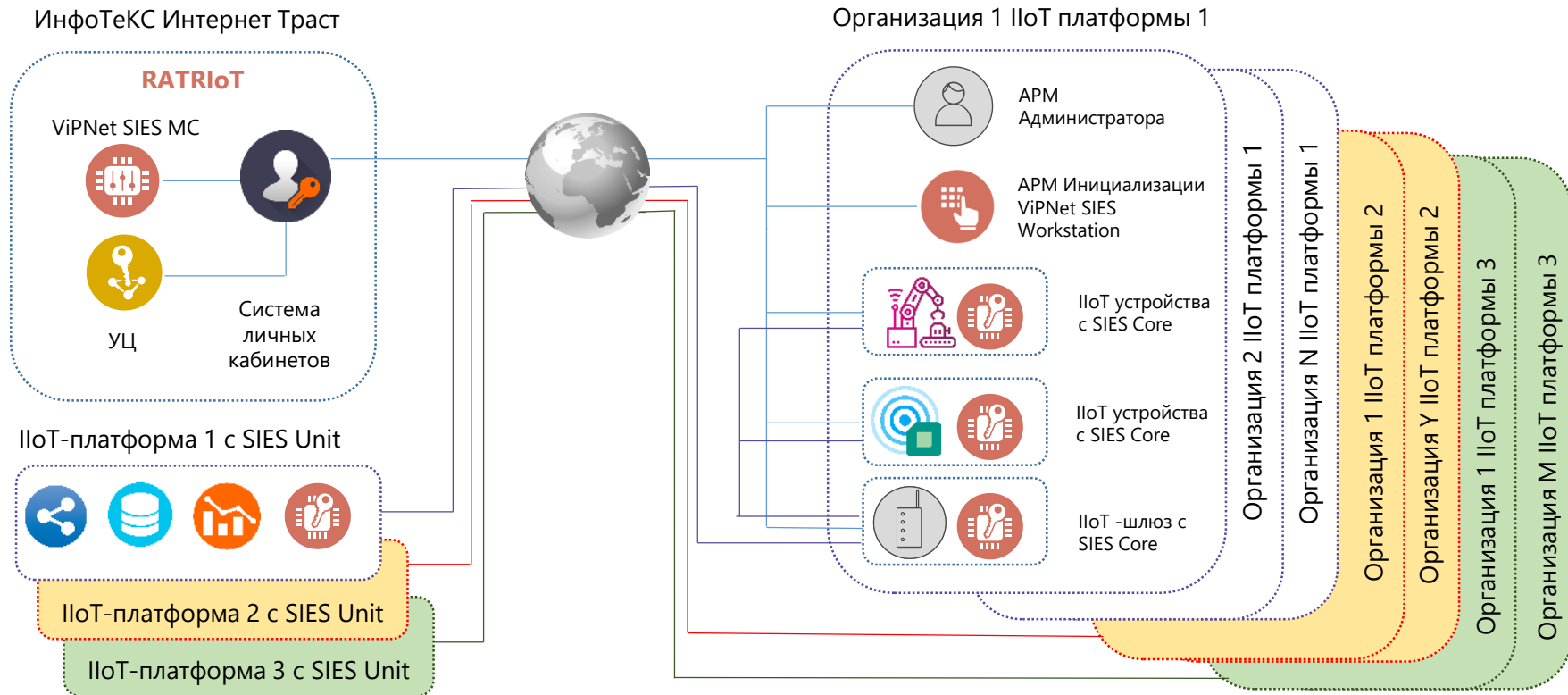
Ролевая модель доступа к ViPNet SIES MC





PATRIoT – ViPNet SIES как сервис
(ИнфоТеКС Интернет Траст)

Platform for All-Trusted Russian Internet of Things (PATRIoT) по модели SECaaS



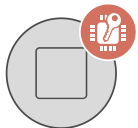


Средства разработки ViPNet SIES

ViPNet SIES Development kit для разработчика IIoT-устройств и IIoT-платформы



Продукты решения ViPNet SIES



2 x ПАК ViPNet
SIES Core



1 x ПО ViPNet
SIES Unit
(на 50 связей)



1 x ПО ViPNet
SIES Workstation
(Windows)



1 x ПО ViPNet
SIES MC VA
(1 администратор)

или

Сертификат на
подключение
1 администратора к
платформе PATRIoT

Средства инфраструктуры



2 x ПО ViPNet PKI Client
с TLS Unit (для ViPNet
SIES Workstation и
администратора)

Средства разработки



ViPNet SIES
Core SDK



Утилита SIES Core

Документация



Описание
протоколов



Пользовательская
документация
на продукты



Инструкция по
разворачиванию
решения

ViPNet SIES Development kit для разработчика СКЗИ SIES-узел типа «другой»

Продукты решения ViPNet SIES



или

Сертификат на
подключение
1 администратора к
платформе PATRIoT

1 x ПО ViPNet
SIES MC VA
(1 администратор)

Средства инфраструктуры



2 x ПО ViPNet PKI Client
с TLS Unit (для ViPNet
SIES Workstation и
администратора)

Средства разработки



Примеры реализации

Документация



Описание
Протоколов
взаимодействия
с ViPNet SIES MC



Описание
команд
ViPNet SIES MC



Описание реализации
CRISP



Описание ключевой
служебной и прикладной
системы



Инструкция по
разворачиванию
решения



Спасибо
за внимание!