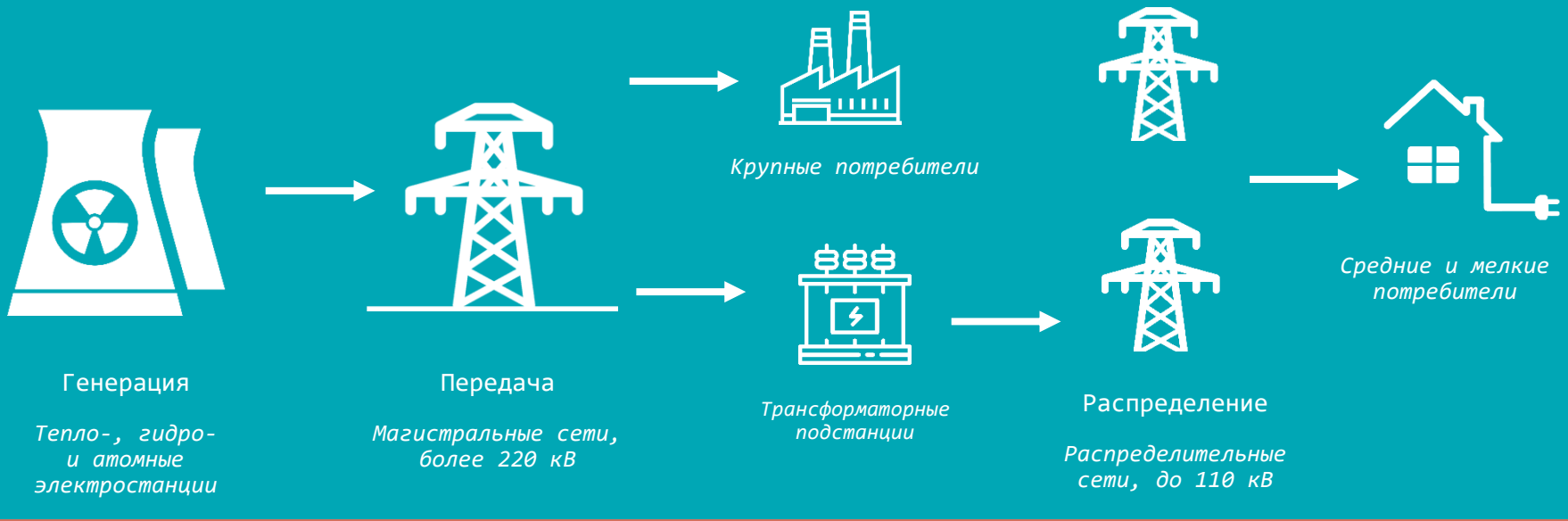
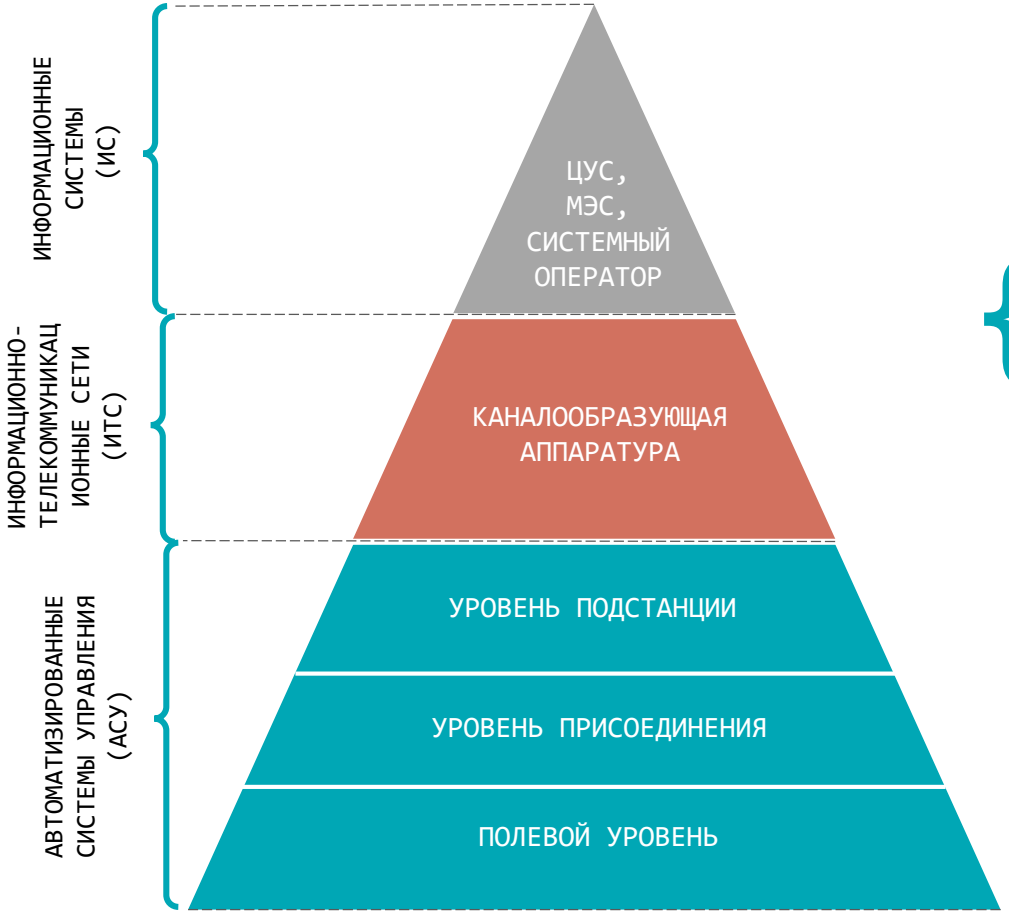
Продукты ИнфоТеКС для защиты объектов электроэнергетики

Марина Сорокина,
Руководитель продуктового направления

Электроэнергетика как объект защиты



Объекты КИИ согласно Федеральному закону №187-ФЗ «О безопасности КИИ РФ»



Требования ИБ к объектам ЗОКИИ

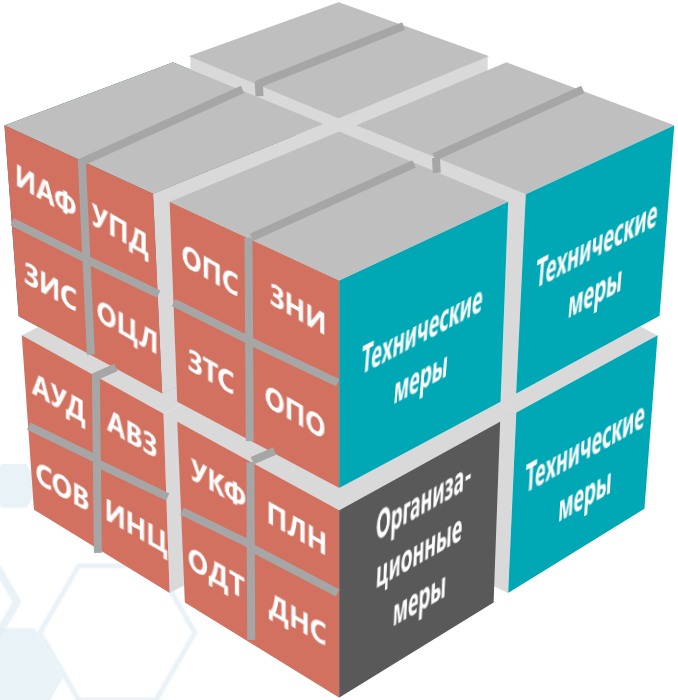
- Требования к созданию систем безопасности объектов КИИ (Приказ ФСТЭК России №235 от 21.12.2017г.)
- Требования по обеспечению безопасности объектов КИИ (Приказ ФСТЭК России №239 от 25.12.2017 г.)
- Порядок согласования объектов КИИ с ФСТЭК России подключения ЗОКИИ к сети общего пользования от 28.05.20 г.

Объекты защиты ЗОКИИ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ	ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ	АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ
○ **информация, обрабатываемая в ИС** ○ **программно-аппаратные средства** (серверы, АРМ, машинные носители информации, телекоммуникационное оборудование, линии связи, средства обработки буквенно-цифровой, графической, видео- и речевой информации) ○ **программные средства** (микропрограммное, общесистемное, прикладное ПО) ○ **средства защиты информации** ○ **архитектура и конфигурация ИС**	○ **информация, передаваемая по линиям связи** ○ **телекоммуникационное оборудование** (ПО, система управления) ○ **средства защиты информации** ○ **архитектура и конфигурация ИТС**	○ **информация о состоянии контролируемого объекта или процесса** (входная и выходная информация, управляющая информация, телеметрия, иная критически важная информация) ○ **программно-аппаратные средства** (АРМ, промышленные серверы, телекоммуникационное оборудование, линии связи, ПЛК, технологическое, производственное оборудование (исполнительные устройства) ○ **программные средства** (в том числе микропрограммное, общесистемное, прикладное ПО) ○ **средства защиты информации** ○ **архитектура и конфигурация АСУ**

Алгоритм обеспечения безопасности ЗОКИИ

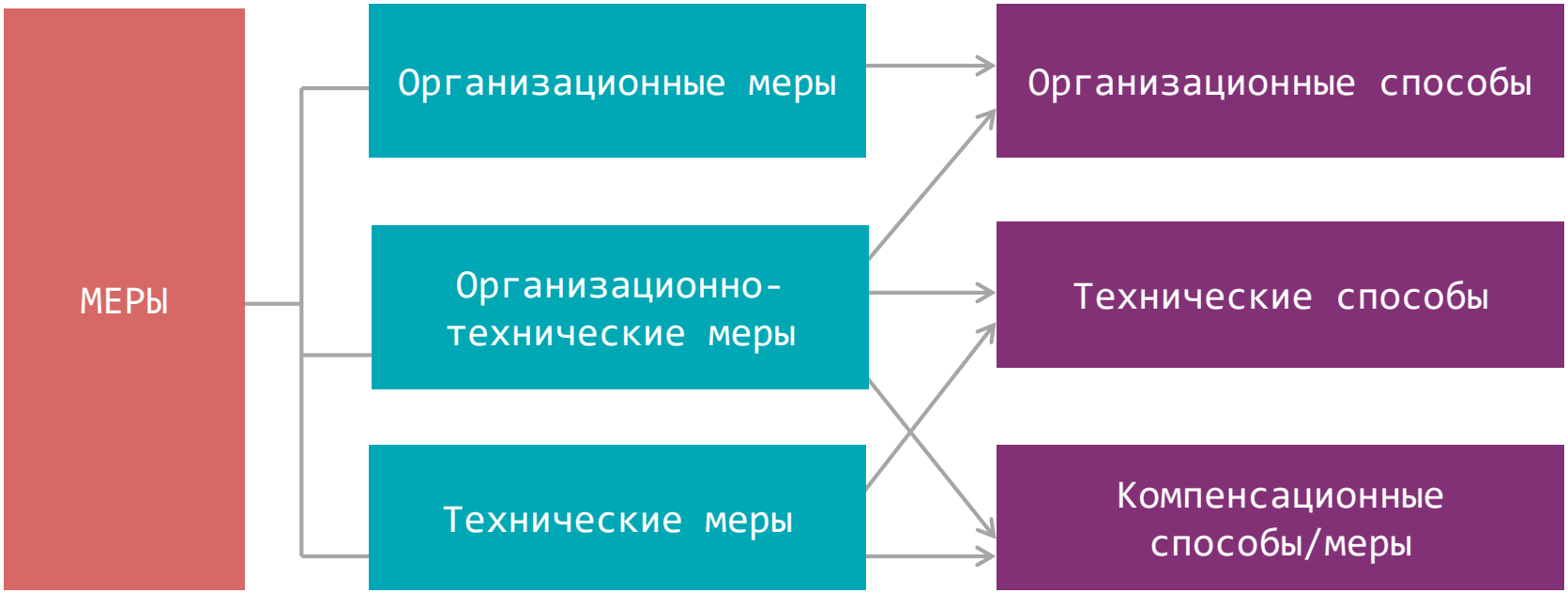
Меры по защите ЗОКИИ



- Идентификация и аутентификация (ИАФ)
- Управление доступом (УПД)
- Ограничение программной среды (ОПС)
- Защита машинных носителей информации (ЗНИ)
- Аудит безопасности (АУД)
- Антивирусная защита (АВЗ)
- Предотвращение вторжений (компьютерных атак) (СОВ)
- Обеспечение целостности (ОЦЛ)
- Обеспечение доступности (ОДТ)
- Защита технических средств и систем (ЗТС)
- Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
- Планирование мероприятий по обеспечению безопасности (ПЛН)
- Управление конфигурацией (УКФ)
- Управление обновлениями программного обеспечения (ОПО)
- Реагирование на инциденты информационной безопасности (ИНЦ)
- Обеспечение действий в нештатных ситуациях (ДНС)
- Информирование и обучение персонала (ИПО)

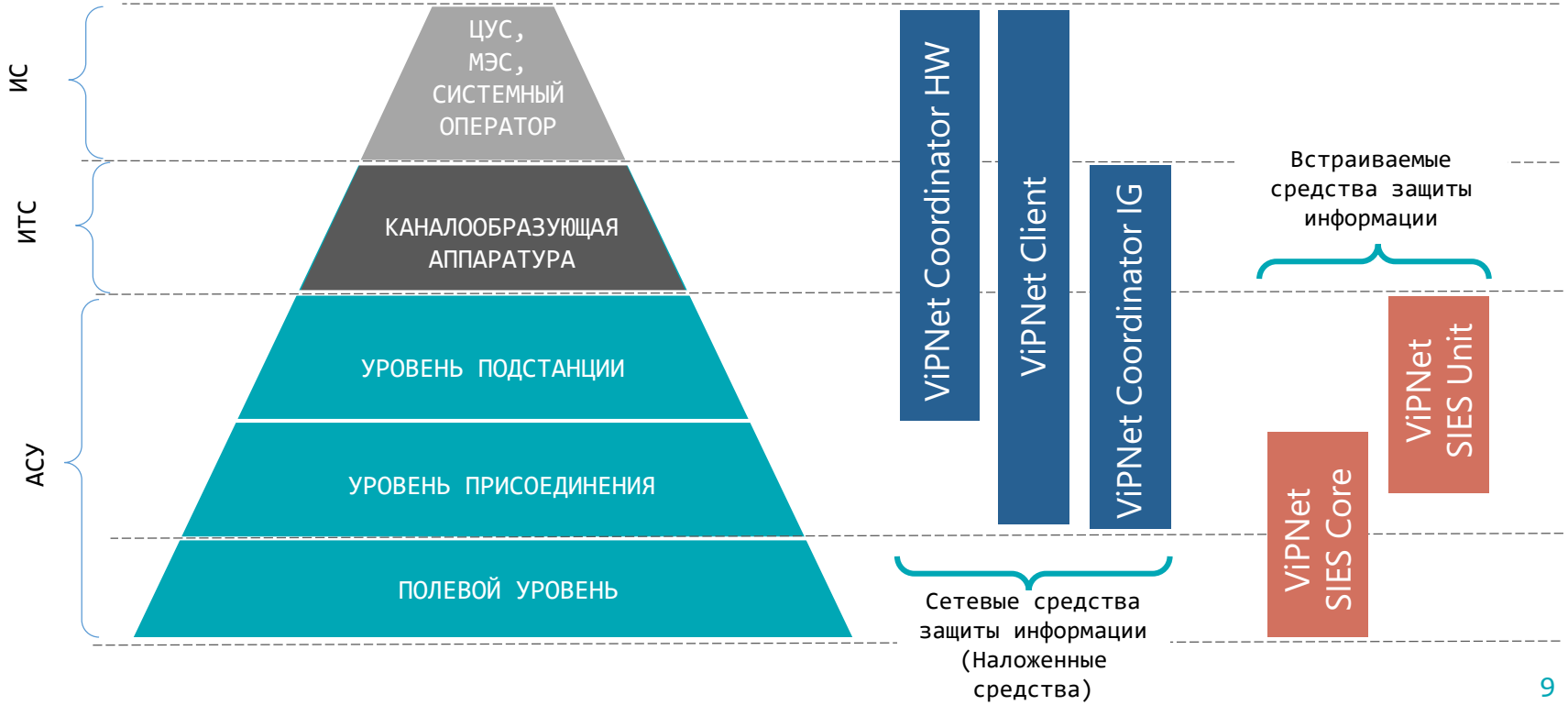
более 150 мер

Меры защиты ЗОКИИ



Продукты ИнфоТеКС для защиты объектов электроэнергетики

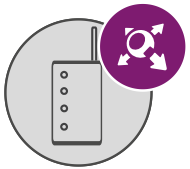
Продукты ИнфоТеКС для защиты объектов электроэнергетики



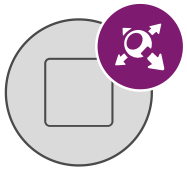
Сетевые средства защиты информации ViPNet Network Security для АСУ

Сетевые средства защиты информации ViPNet Network Security

Шлюзы безопасности:



ViPNet Coordinator IG



ViPNet Coordinator HW

Программные клиенты:

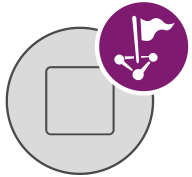
ViPNet Client (desctop)

ViPNet Client 4U (Linux based Os)

ViPNet Client (mobile)

Средства централизованного управления:

ViPNet Administrator



ViPNet PolicyManager

ViPNet Coordinator HW

ViPNet Coordinator IG

ViPNet Coordinator HW & ViPNet Coordinator IG

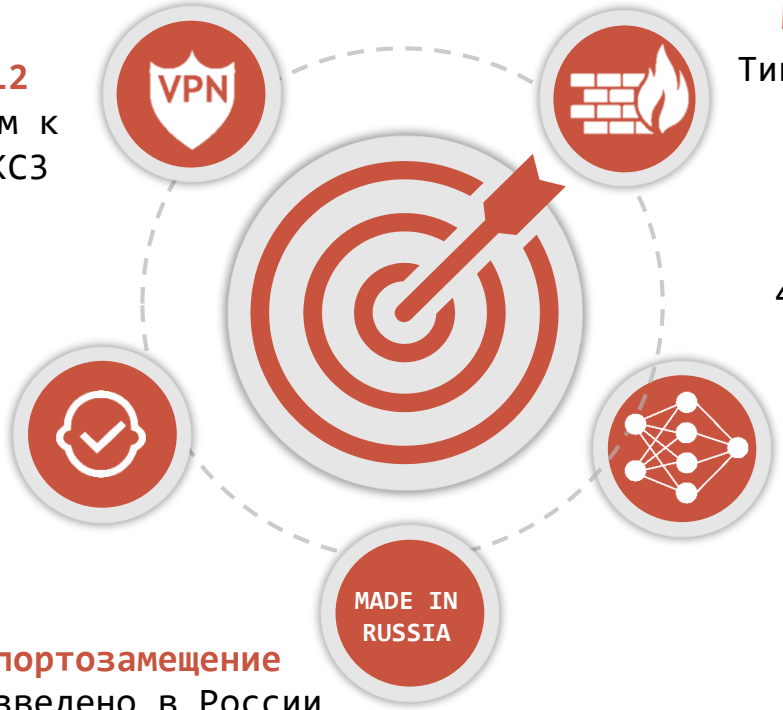
VPN – шлюз уровня L3, L2
По требованиям к СКЗИ класса КС3

Межсетевой экран
Типа «А» 4 класса (HW & IG)
Типа «Д» 4 класса (IG)
по требованиям ФСТЭК России

4 класс защищенности по требованиям ФСБ России

4 уровень доверия

по требованиям ФСТЭК России

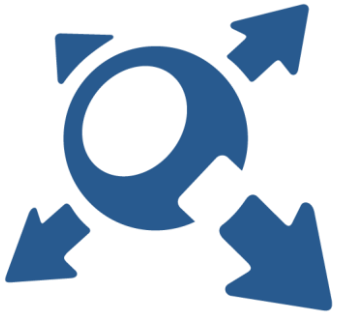


Коммуникации
Проводные, 3G/4G, Wi-fi

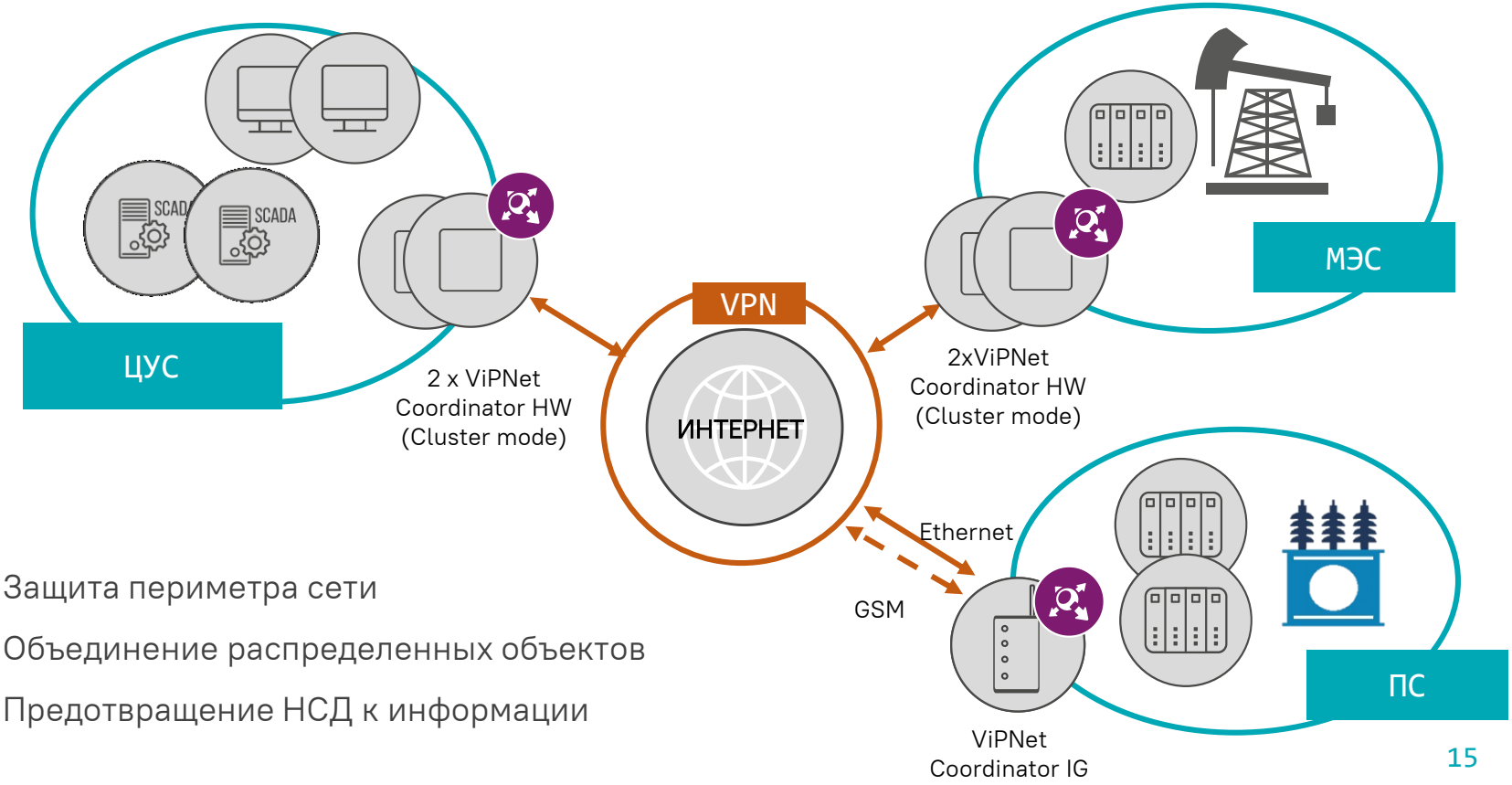
Импортозамещение
Произведено в России

Криптографическая защита

- Защита каналов передачи данных с использованием алгоритма ГОСТ 28147-89
- Построение защищенных каналов связи между сегментами АСУ
- Защита каналов связи при подключении к сетям общего пользования, в том числе и беспроводных каналов связи
- Защищенный доступ удаленных и мобильных пользователей
- Защищенный мониторинг
- Защищенное подключение для сервисного обслуживания
- Соответствие требованиям ФСБ России

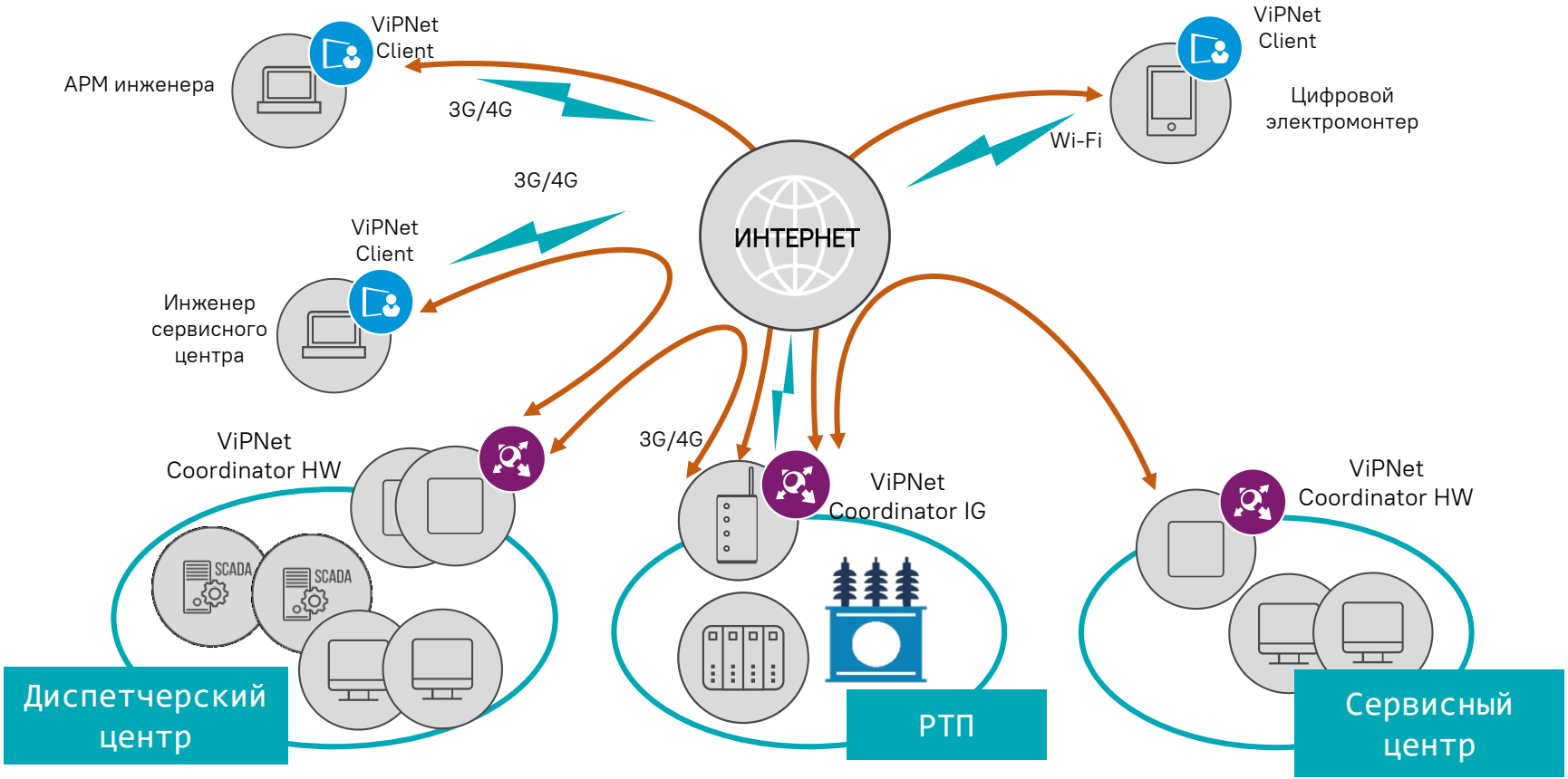


Защита каналов связи



- Защита периметра сети
- Объединение распределенных объектов
- Предотвращение НСД к информации

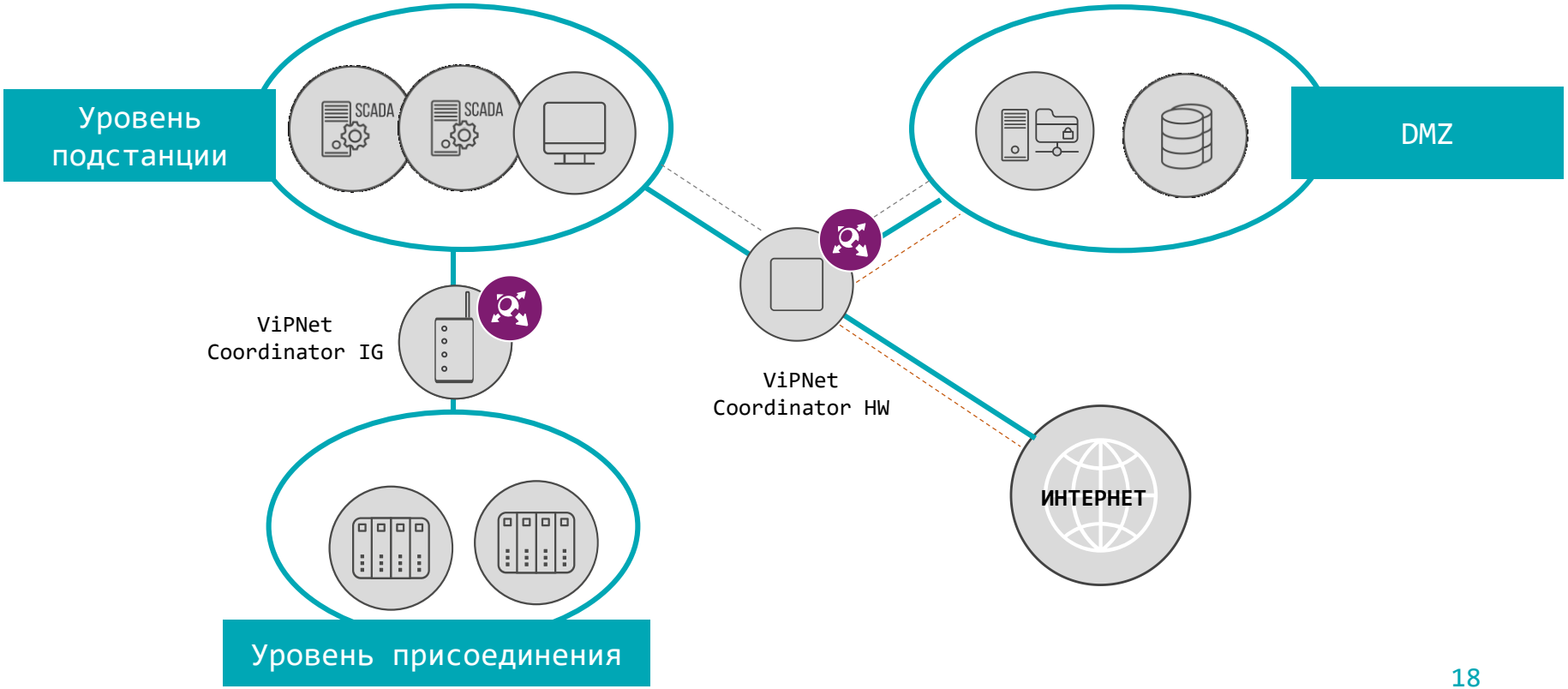
Защищенный удаленный доступ



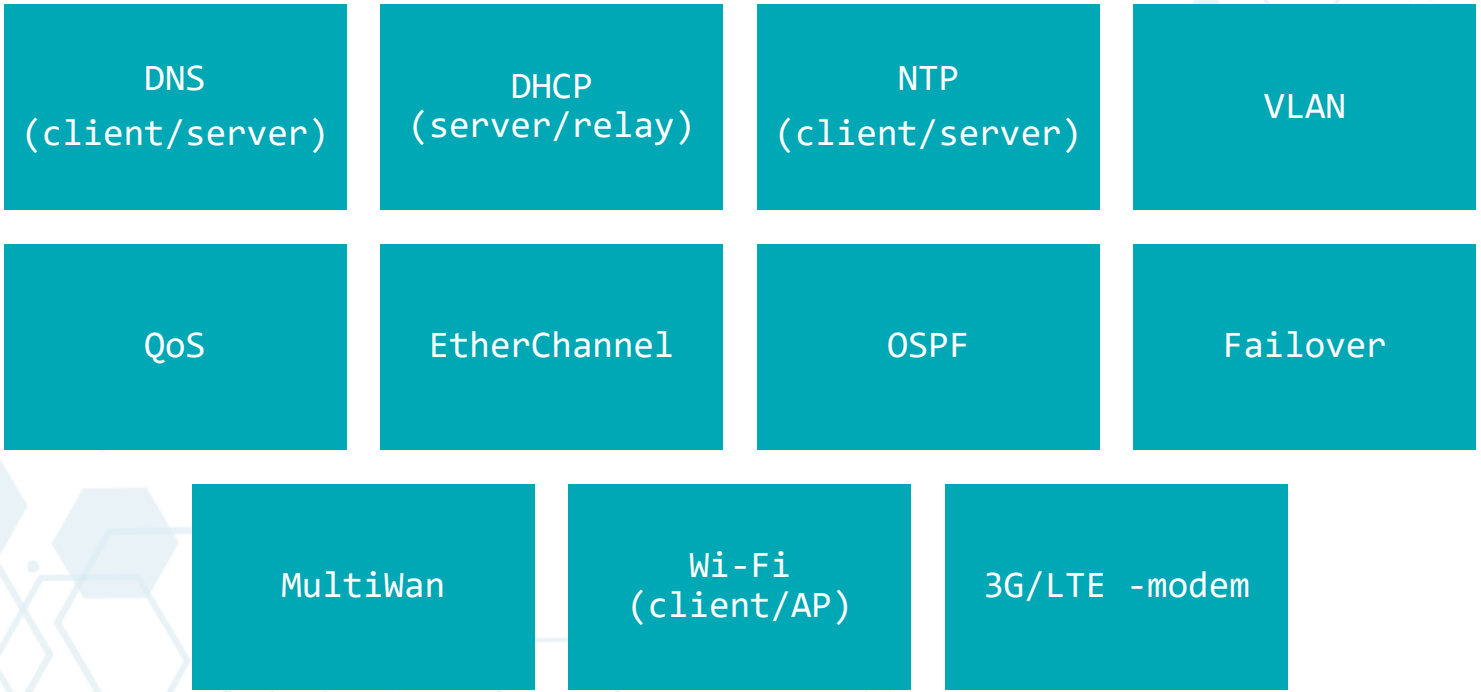
Межсетевое экранирование

- Фильтрация сетевых соединений и поддержка политики безопасности
- Сегментация внутренних сетей
- Организация DMZ
- Сокрытие адресов и информации о структуре сети
- Создание безопасных соединений при выходе в интернет
- Соответствие требованиям ФСТЭК России и ФСБ России

Сегментирование сетей



Сетевые сервисы



Надежность и резервирование

- Возможность работать в режиме кластера
- Возможность использовать разные GSM-операторы связи и разные точки доступа для узлов кластера (для ViPNet Coordinator IG)
- Возможность резервирования каналов (переключение на резервный канал в случае отсутствия связи)
- Наличие исполнений ViPNet Coordinator IG и ViPNet Coordinator HW с двумя портами питания

Прокси-сервер и контентная фильтрация

Прокси-сервер

- «Прозрачный» режим работы
- Режим кеширования

Контент-фильтрация

ViPNet Coordinator HW

Фильтрация по источнику, назначению, HTTP методу, MIME-типу файла

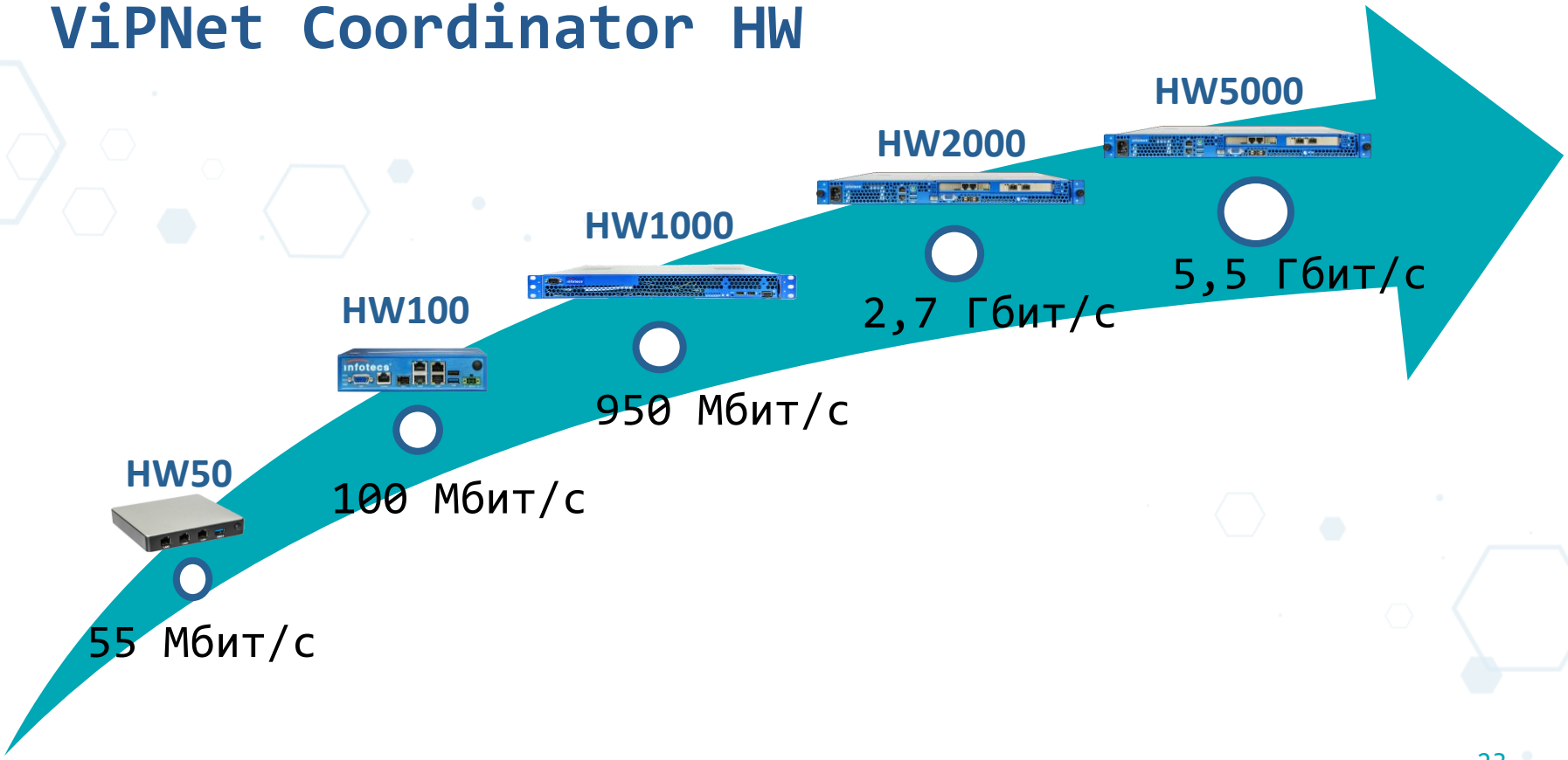
ViPNet Coordinator IG

Фильтрация промышленных протоколов на прикладном уровне (Modbus TCP)

Антивирус в ViPNet Coordinator HW

- Встроенный Антивирус Касперского
- Выявление вредоносного содержимого в файлах
- Автоматическое обновление антивирусных баз

Исполнения ViPNet Coordinator HW



Исполнения ViPNet Coordinator IG

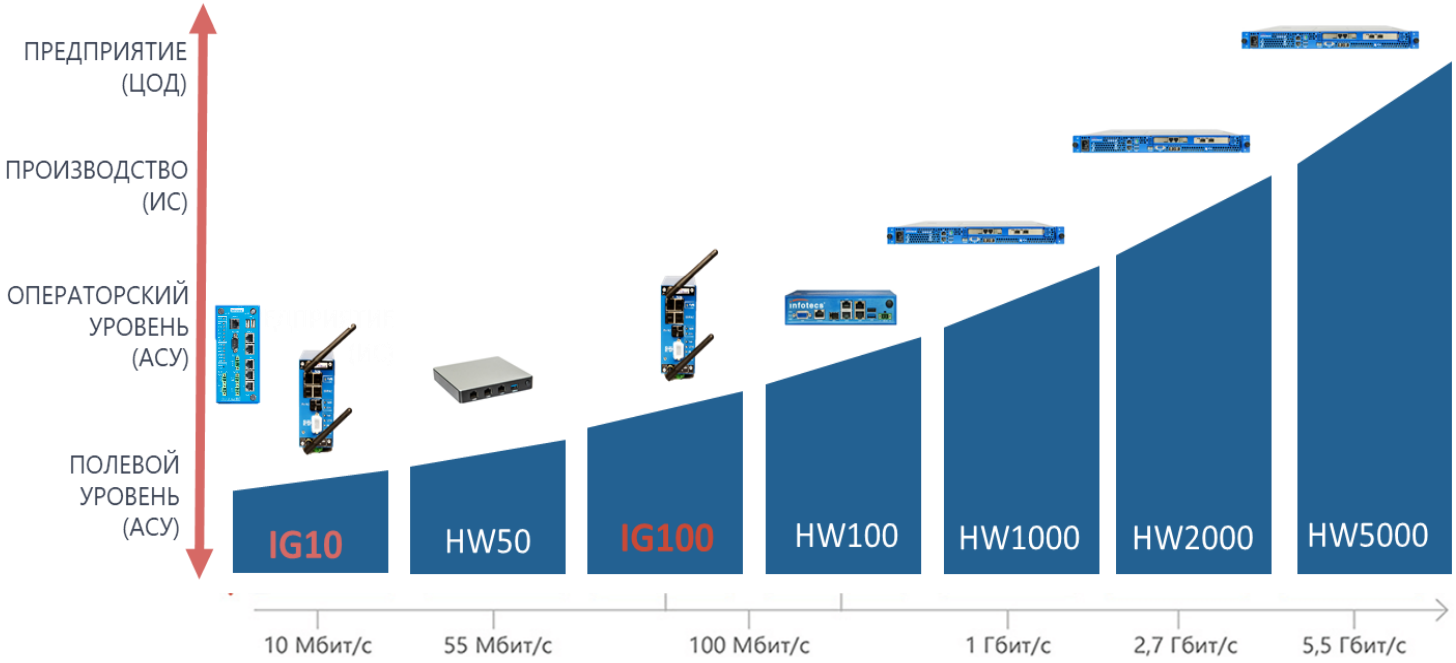
ViPNet Coordiantor IG10 на аппаратной платформе IG10 I1

ViPNet Coordiantor IG100 на аппаратной платформе IG100 I1

ViPNet Coordiantor IG10 на аппаратной платформе IG10 I2

Исполнения ViPNet Coordinator IG

	ViPNet Coordinator IG10 I1	ViPNet Coordinator IG100 I1	ViPNet Coordinator IG10 I2
Производительность L3 VPN и L2 VPN	до 10 Мбит/с	до 60 Мбит/с	до 10 Мбит/с
Производительность МЭ	до 10 Мбит/с	до 60 Мбит/с	до 10 Мбит/с
Проводные интерфейсы	Ethernet 3xRJ45	Ethernet 3xRJ45	Ethernet 5xRJ45
Беспроводные модули	3G или LTE*, Wi-Fi 2,4 ГГц	3G или LTE*, Wi-Fi 2,4 ГГц	3G или LTE*, 2 Sim Wi-Fi 2,4 ГГц
Питание	12 - 24 В DC, 15 Вт	12 - 24 В DC, 10 Вт	2 входа питания: 12 - 24 В DC, 25 Вт
Рабочая температура	-20°С (-40 °С)…+60°С	-20°С…+60°С	-40°С...+60°С
ЭМС	ГОСТ Р51318-22 (СИСПР 22), ГОСТ CISPR 24 2013 (СИСПР 24)	ГОСТ Р51318-22 (СИСПР 22), ГОСТ CISPR 24 2013 (СИСПР 24)	ГОСТ Р51318-22 (СИСПР 22), ГОСТ CISPR 24 2013 (СИСПР 24), ГОСТ Р 51317.6.5-2006 (МЭК 61000-6-5:2001)



Экосистема ViPNet Network Security

- Встречная работа
- Единое управление

Управление

- Централизованное управление ключевой информацией
- Централизованное обновление оборудования
- Централизованное управление политиками безопасности и режимами работы
- Централизованный мониторинг

Сертификация

ViPNet Coordinator HW и ViPNet Coordinator IG имеют сертификаты по требования ФСБ России:

- Сертификат на СКЗИ класса КС3
- Сертификат на МЭ 4 класса защищенности

ViPNet Coordinator HW имеет сертификат по требованиям ФСТЭК России:

- Сертификат на МЭ типа А 4 класса и 4 уровень доверия по ТДБ

ViPNet Coordinator IG имеет заключение и ожидает получение сертификата по требованиям ФСТЭК России:

- Сертификат по МЭ типа А.4 и Д.4 и 4 уровень доверия по ТДБ

Сертификация

ViPNet Coordinator HW & ViPNet Coordinator IG

имеют сертификаты по требованиям Минкомсвязи России:

- Сертификат на оборудование коммутации и маршрутизации пакетов информации для сетей общего пользования и технологических сетей

ViPNet Coordinator IG по требованиям

Минкомсвязи России имеет:

- Сертификаты на оборудование радиодоступа для беспроводной передачи данных в диапазоне от 30 МГц до 66 ГГц
- Декларации на оборудование проводных и оптических систем передачи и на абонентские устройства связи стандартов GSM (GSM-900/1800, UTMS, LTE)

Российское оборудование

- ПО ViPNet Coordinator HW и ПО ViPNet Coordinator IG включены в реестр российского ПО (реестр Минкомсвязи России) под регистрационным номером 2798 и 5102 соответственно
- Исполнения ViPNet Coordinator HW и ПО ViPNet Coordinator IG включен в реестр телекоммуникационного оборудования российского происхождения (ТОРП) и единый реестр российской радиоэлектронной продукции Минпромторга России. Реестровые записи:
  - ТКО-520/20 – ПАК Coordinator HW1000 (аппаратная платформа HW1000 Q7)
  - ТКО-517/20 – ПАК ViPNet Coordinator IG10 на платформе IG10 I1
  - ТКО-518/20 – ПАК ViPNet Coordinator на платформе IG10 I2
  - ТКО-519/20 – ПАК ViPNet Coordinator IG100 на платформе IG100 I1

ViPNet Client

ViPNet Client – защита каналов связи рабочих станций и конечных устройств

КОМПЬЮТЕРЫ
НОУТБУКИ

ТЕЛЕФОНЫ
ПЛАНШЕТЫ

Встраиваемая версия ViPNet Client 4U

LINUX BASED

x86 ARM docker MIPS МЦСТ ЭЛЬБРУС

КОНТРОЛЛЕРЫ

ViPNet Client – защита каналов связи рабочих станций и конечных устройств

SCADA LEVEL

Operator workstation
ViPNet Client for Windows
ViPNet Client for Linux

HMI
ViPNet Client for Windows
ViPNet Client for Linux

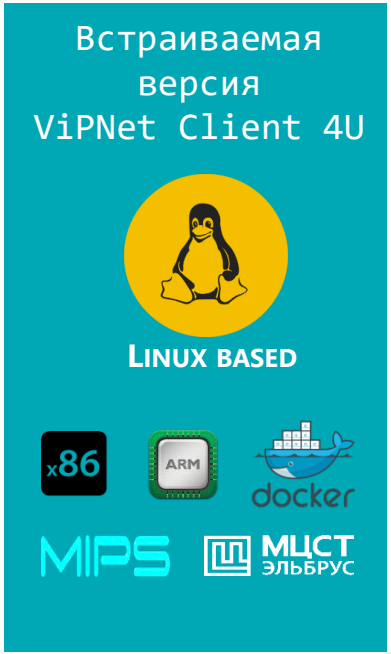
Mobile Workstation
ViPNet Client for Android
ViPNet Client for iOS

AUTOMATION LEVEL

Engineer Workstation
ViPNet Client for Windows
ViPNet Client for Linux

PLC
Встраиваемый
ViPNet Client 4U

ViPNet Client – защита каналов связи рабочих станций и конечных устройств



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-3560* от "*12*" *декабря* 2018 г.

Действителен до "*12*" *декабря* 2021 г.

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

Настоящий сертификат удостоверяет, что программный комплекс **ViPNet Client 4 for Linux** (исполнения 1, 2) в комплектации согласно формуляру ФРКЕ.00149-03 30 01 ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 1) и класса КС2 (для исполнения 2) и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов, данных, содержащихся в областях оперативной памяти, и IP-трафика, вычисление имитовставки для файлов, данных, содержащихся в областях оперативной памяти, и IP-трафика) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС»
сертификационных испытаний образца продукции № 782/I-000501.

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00149-03 30 01 ФО.

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

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 12 декабря 2018 г.

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

- Сертифицировано на соответствие требованиям к СКЗИ классов КС1-КС3 (в зависимости от варианта исполнения)
- Поддерживаются различные аппаратные архитектуры (x86, ARM, MIPS)
- Минимальные системные требования (CPU 1x300 MHz, 15 Mb, Flash 100 Mb)
- Работа в фоновом режиме
- Автоматический старт
- Удаленное обновление, удаленное управление ключами
- Не требует привилегированного пользователя

Встраиваемые средства защиты информации ViPNet SIES

ViPNet SIES – платформа по защите информации

ВСТРАИВАЕМЫЕ СКЗИ ДЛЯ ИНТЕГРАЦИИ В УСТРОЙСТВА АВТОМАТИЗАЦИИ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИХ СОБСТВЕННОЙ БЕЗОПАСНОСТИ

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

Концепция security-by-design

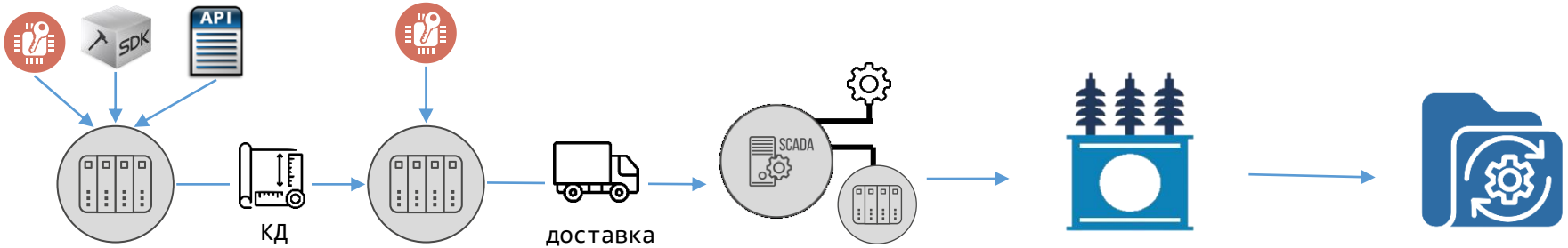
РАЗРАБОТКА УСТРОЙСТВА

ПРОИЗВОДСТВО УСТРОЙСТВА

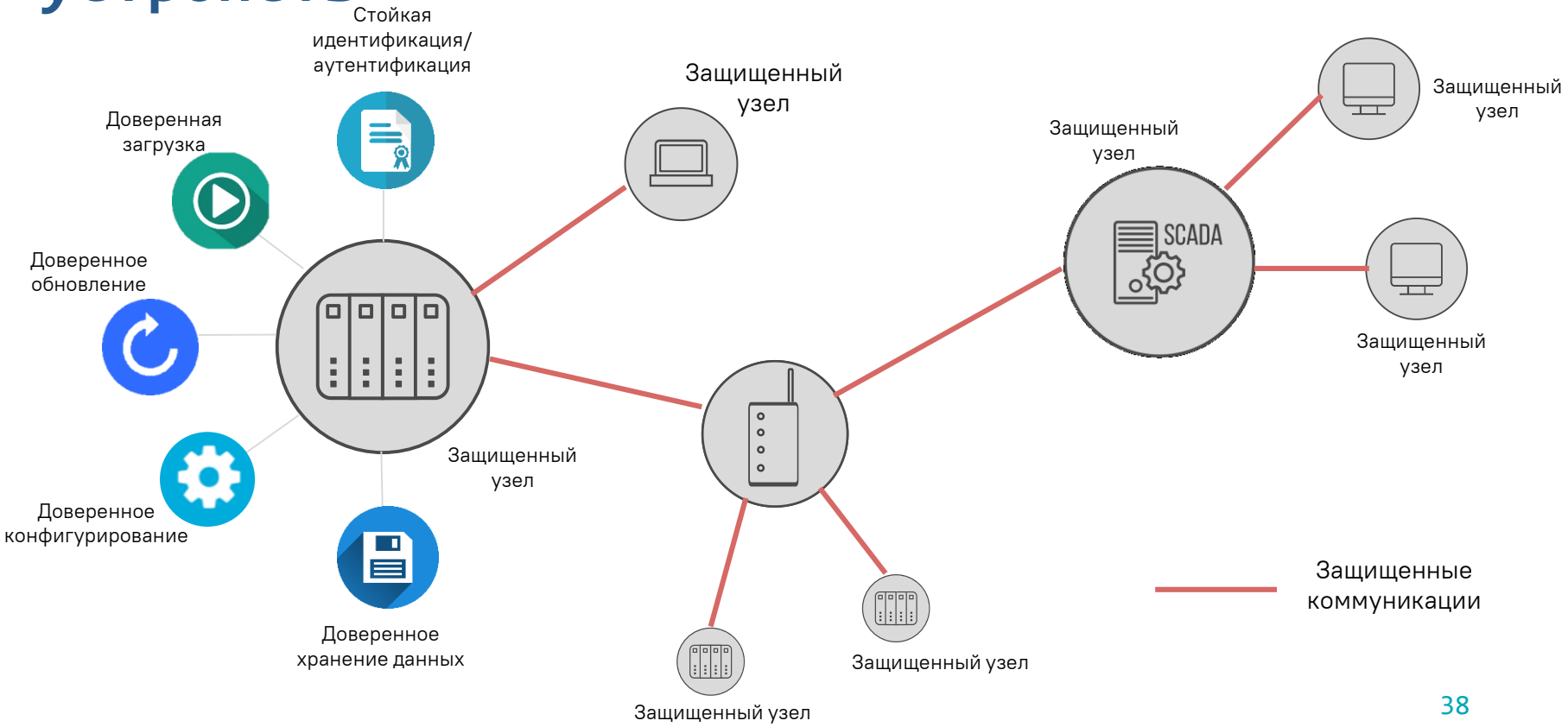
ВВОД В ЭКСПЛУАТАЦИЮ УСТРОЙСТВА

ЭКСПЛУАТАЦИЯ УСТРОЙСТВА

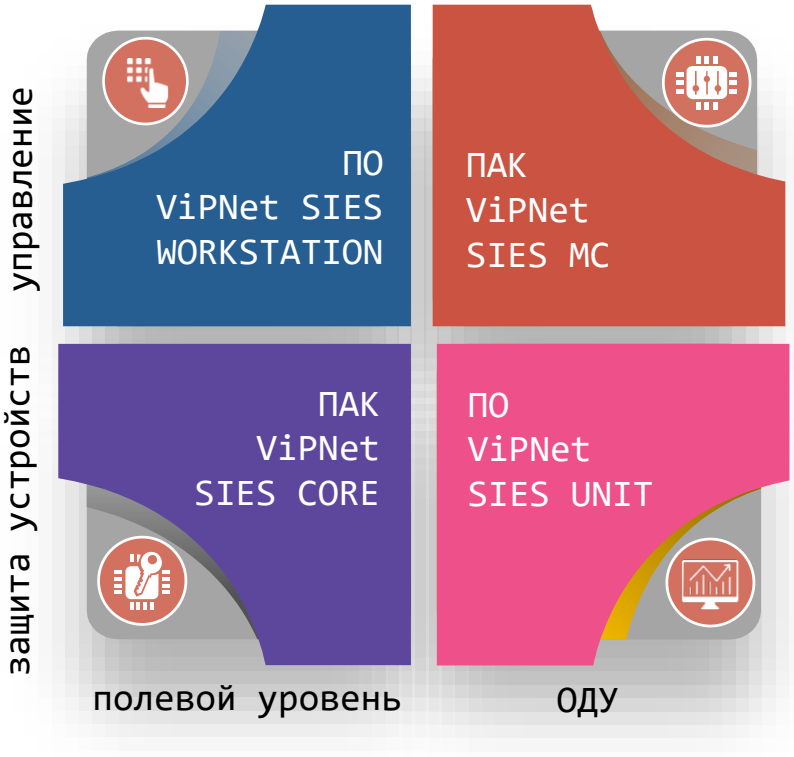
УПРАВЛЕНИЕ ОБНОВЛЕНИЕМ И КОНФИГУРАЦИЕЙ УСТРОЙСТВА



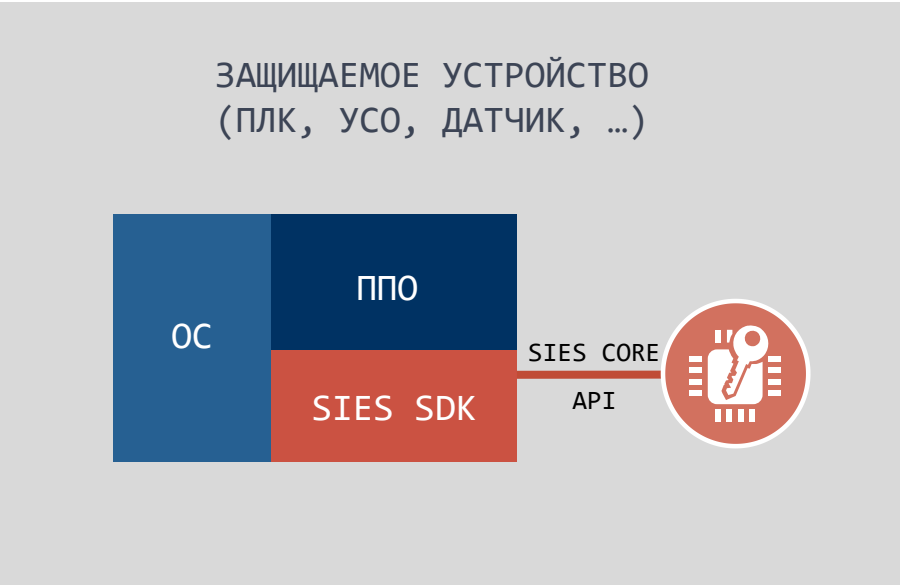
Концепция защиты конечных устройств

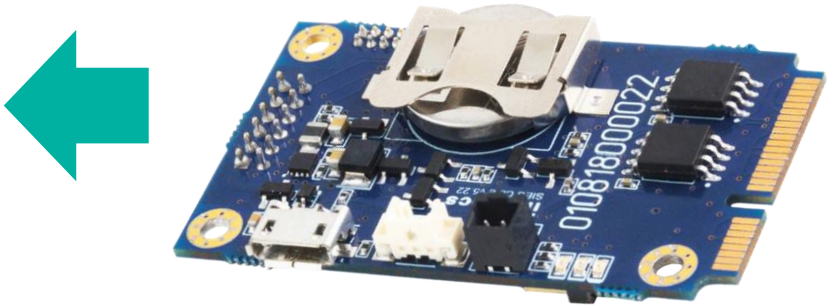


Состав решения ViPNet SIES



- Законченные СКЗИ класса КС1 и КС3
- Возможность использования криптографии на разных по вычислительной мощности устройствах
- Нет зависимости от ОС и архитектуры устройств
- Поддержка разных моделей взаимодействия: точка-точка, мультивещательные связи, подписочная модель
- Поддержка сценариев резервирования



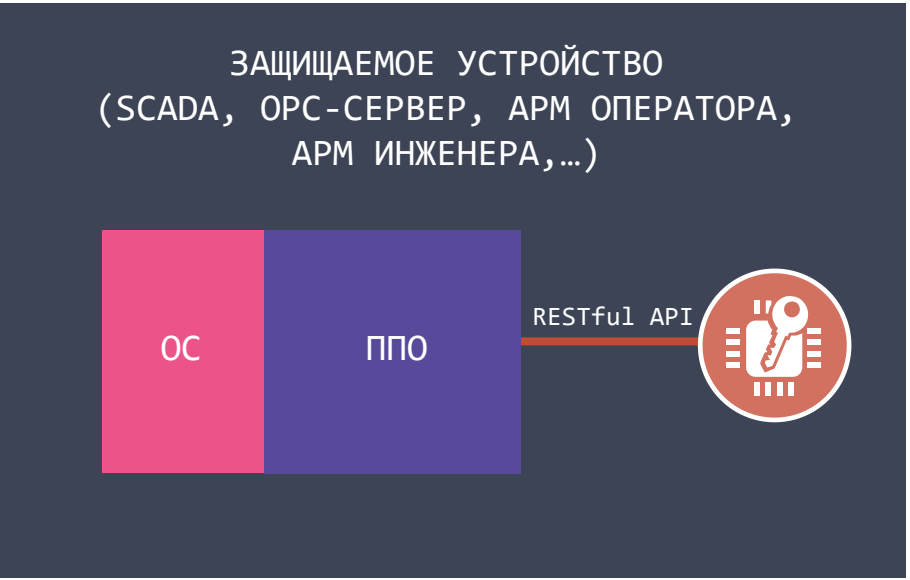


Интеграция ПАК SIES Core

На аппаратном уровне – USB, UART, SPI

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

Интеграция ПО ViPNet SIES Unit



Поддерживаемые ОС:

- Windows 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)

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

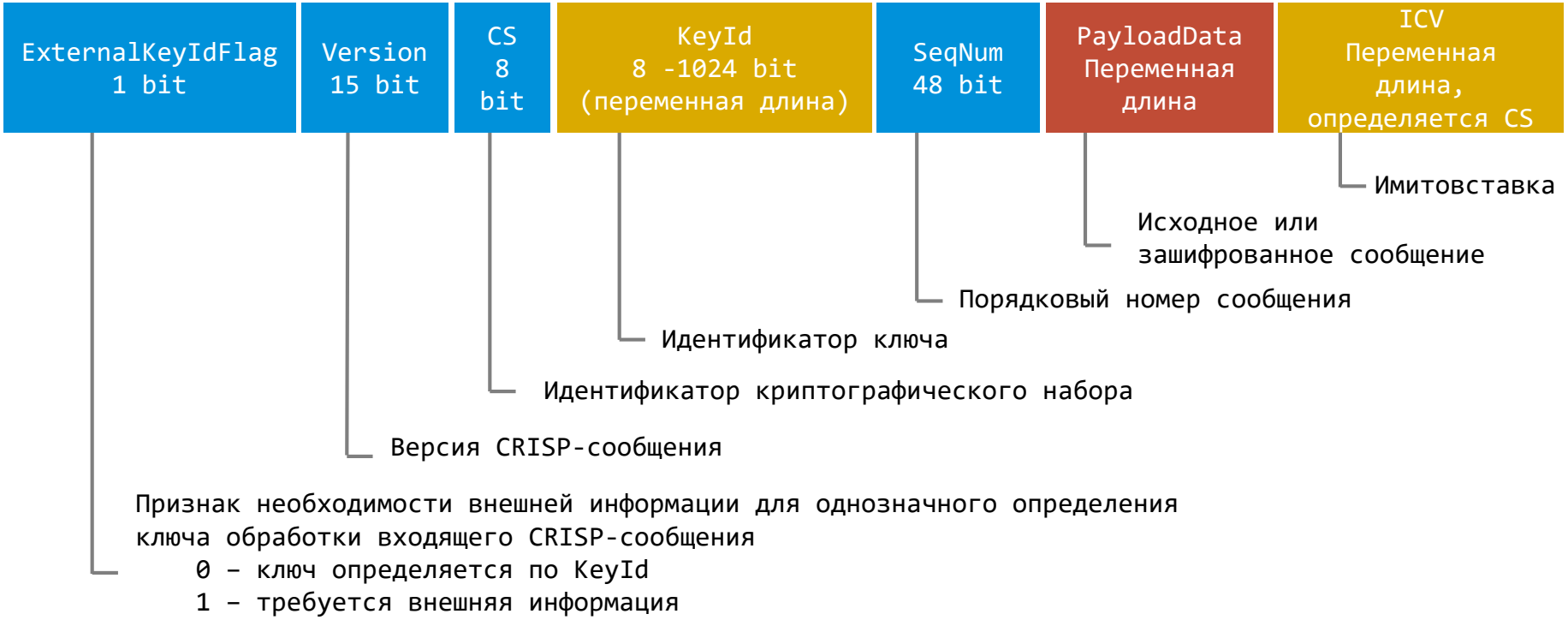
Криптографические операции, доступные защищаемым устройствам

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

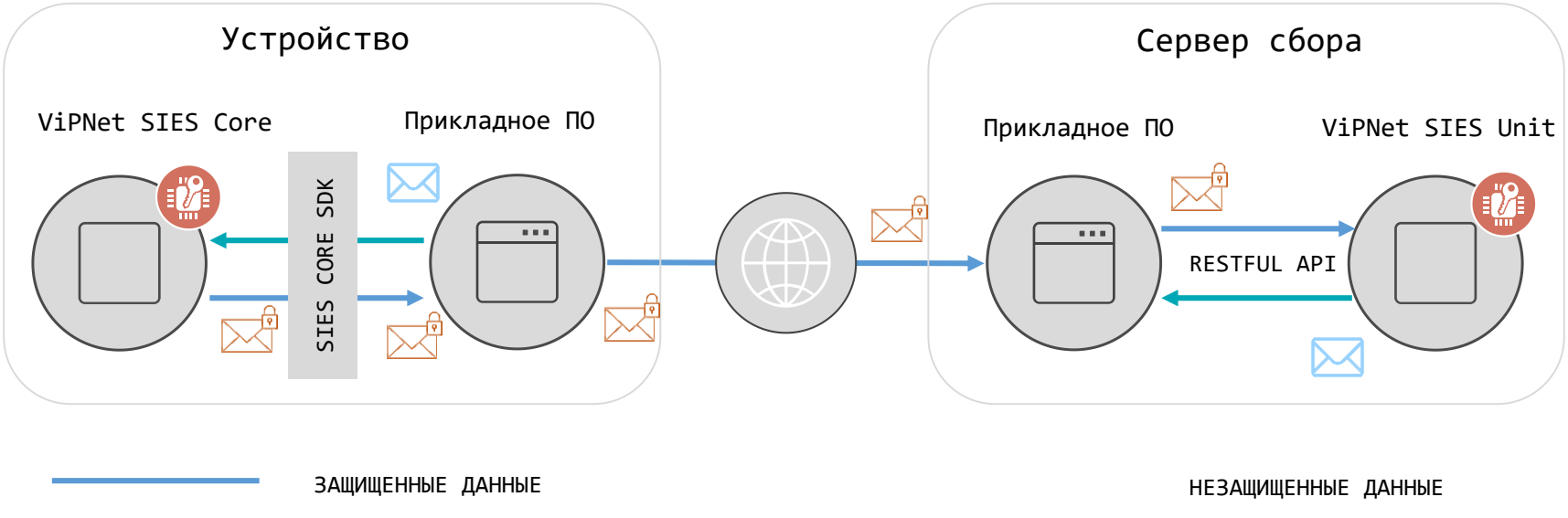
Рекомендация по стандартизации РФ:
Р 1323565.1.029-2019.
Протокол защищенного обмена CRISP

- Предраспределенные симметричные ключи
- Аутентификация источника сообщений (у абонентов общий секретный ключ)
- Поддержка адресных и широковещательных сообщений
- Обязательное обеспечение целостности при помощи имитовставки
- Обеспечение конфиденциальности при помощи блочного шифра
- Защита от навязывания повторных сообщений
- Малый размер вспомогательных данных

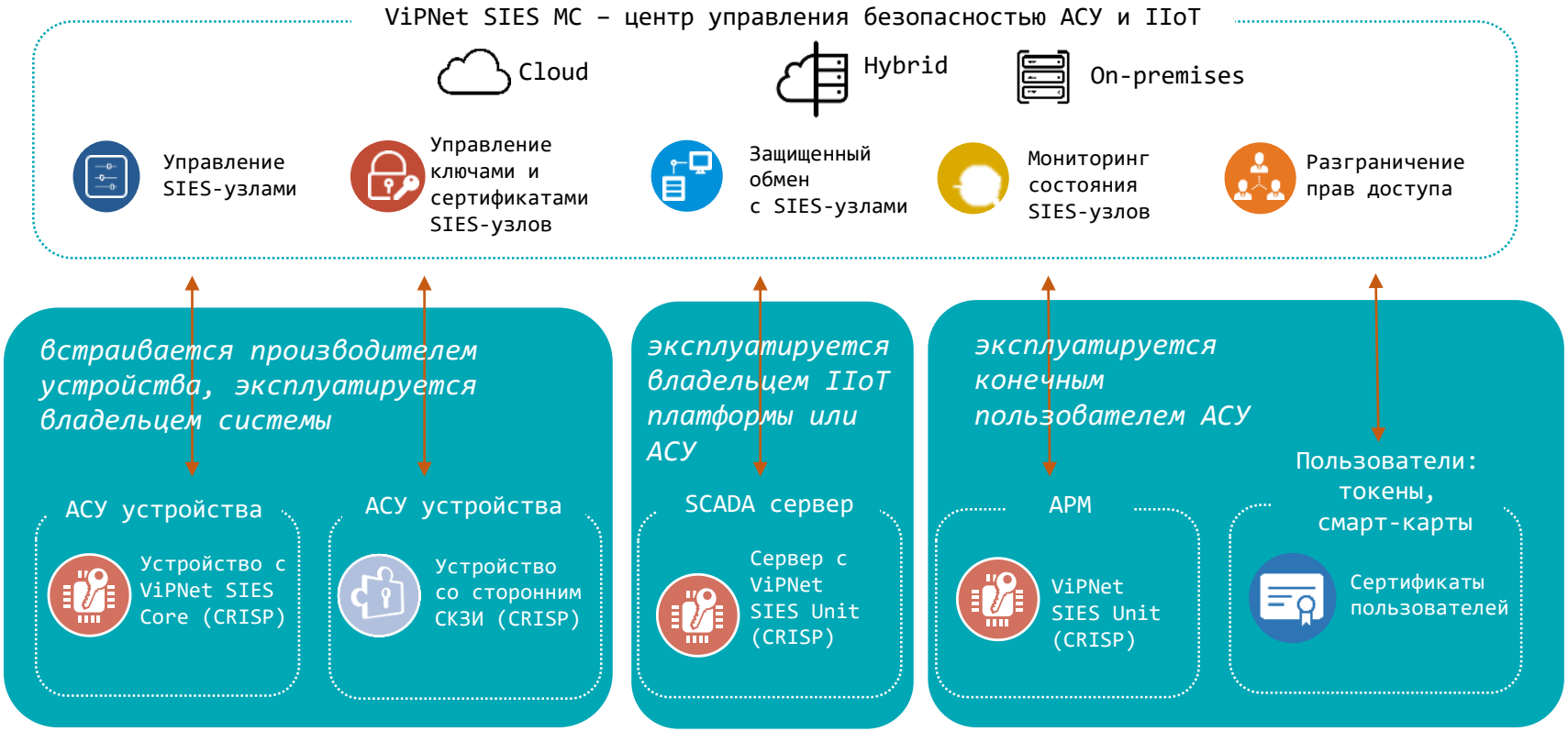
Структура CRISP-сообщения



Защита коммуникаций с помощью ViPNet SIES



ИБ платформа на основе ViPNet SIES для АСУ и IIoT



Сертификация

Продукты ViPNet SIES имеют сертификаты по требованиям ФСБ России:

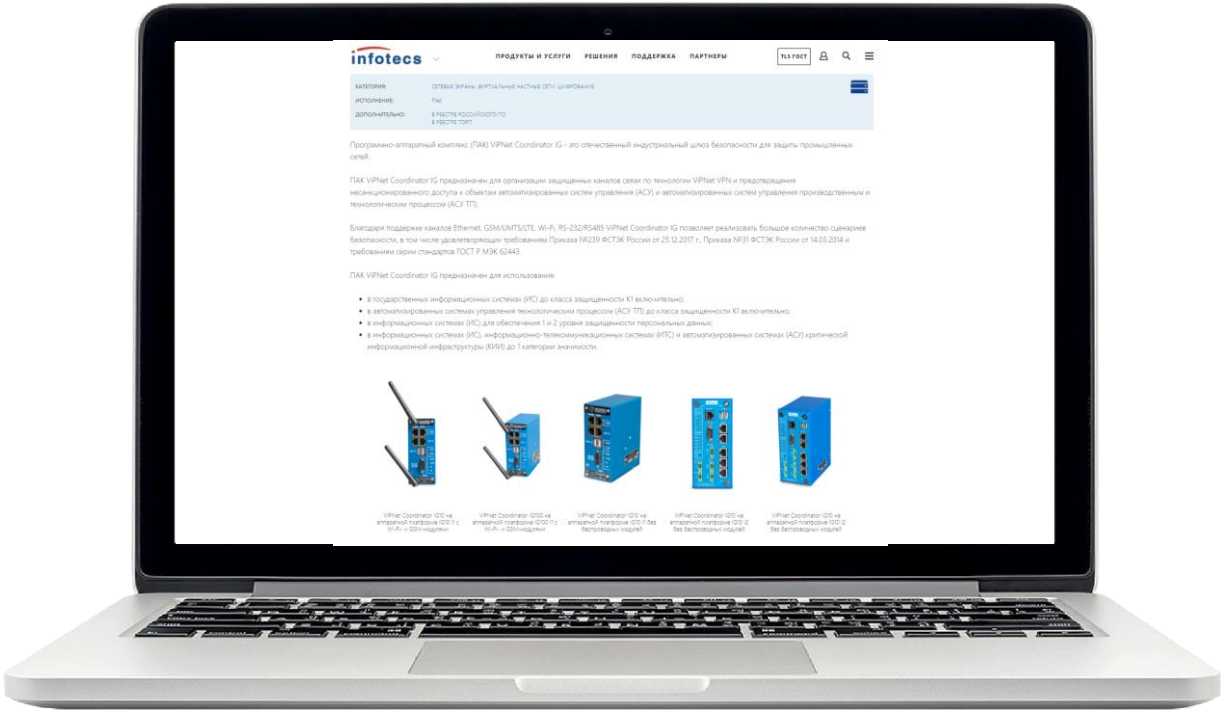
- ViPNet SIES Core как СКЗИ класса КС3
- ViPNet PKI Client с SIES Unit как СКЗИ класса КС1, КС2, КС3
- ViPNet SIES MC как СКЗИ класса КС3

КАК ПРАВИЛЬНО ВЫБРАТЬ СРЕДСТВА ЗАЩИТЫ ДЛЯ ОБЪЕКТОВ ЭЛЕКТРОЭНЕРГЕТИКИ

Алгоритм выбора СЗИ

	ViPNet Network Security	ViPNet SIES
Требуемые к реализации меры защиты	Защита каналов связи, защита периметра, сегментация сети, ДМЗ, сокрытие архитектуры, защита удаленного доступа	Защита данных при передаче, доверенное конфигурирование, доверенное обновление, доверенная загрузка, идентификация и аутентификация пользователей и устройств
Форма внедрения подсистемы безопасности	Существующая инфраструктура	Модернизация или строительство
Требования организационно-технические	Наличие периметра	Отсутствие периметра
Требования к применяемым сетевым технологиям	TCP/IP сети	Non TCP/IP сети, не Ethernet сети

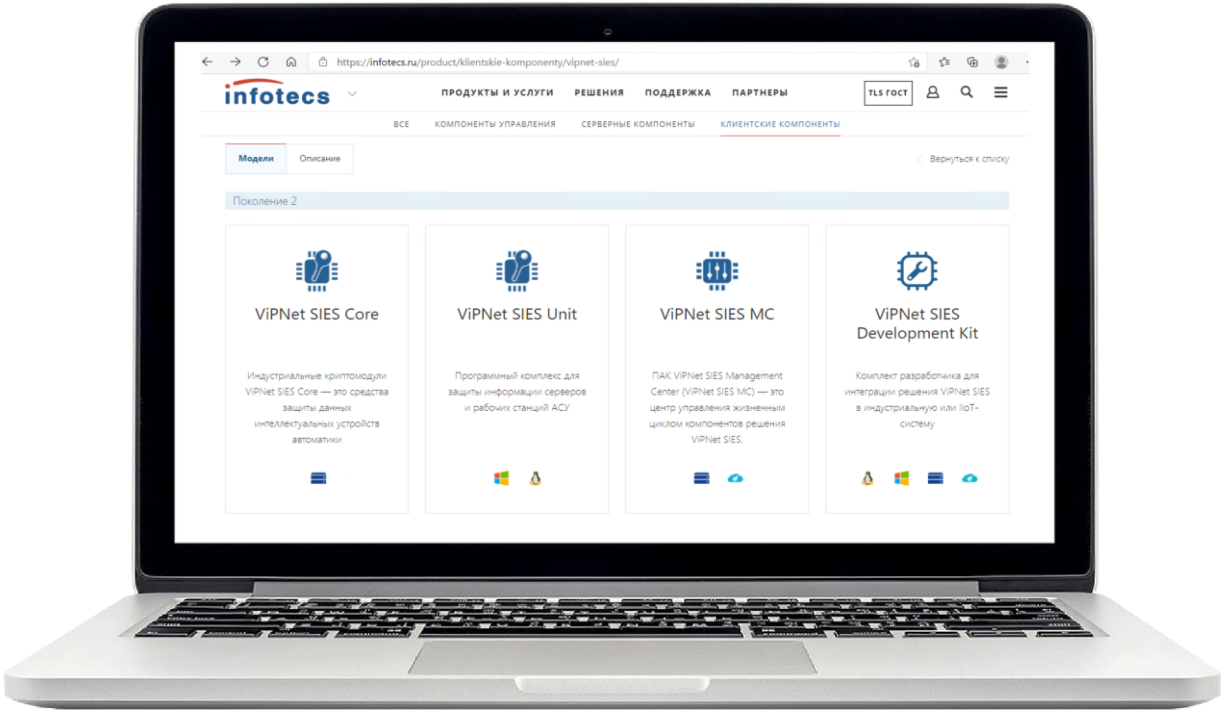
Информация
по ViPNet Coordinator IG & HW



Вся новая информация доступна на сайте –

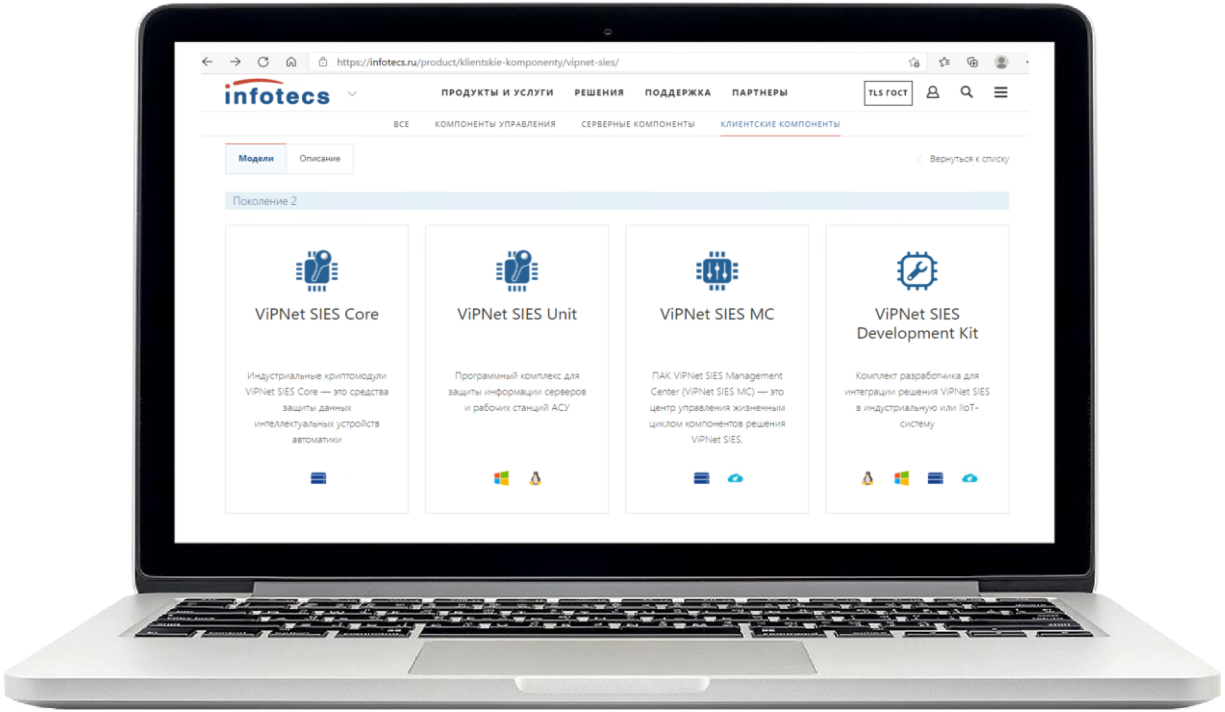
- ViPNet Coordinator IG | ИнфоТеКС (infotecs.ru)
- ViPNet Coordinator HW | ИнфоТеКС (infotecs.ru)

Информация по ViPNet SIES



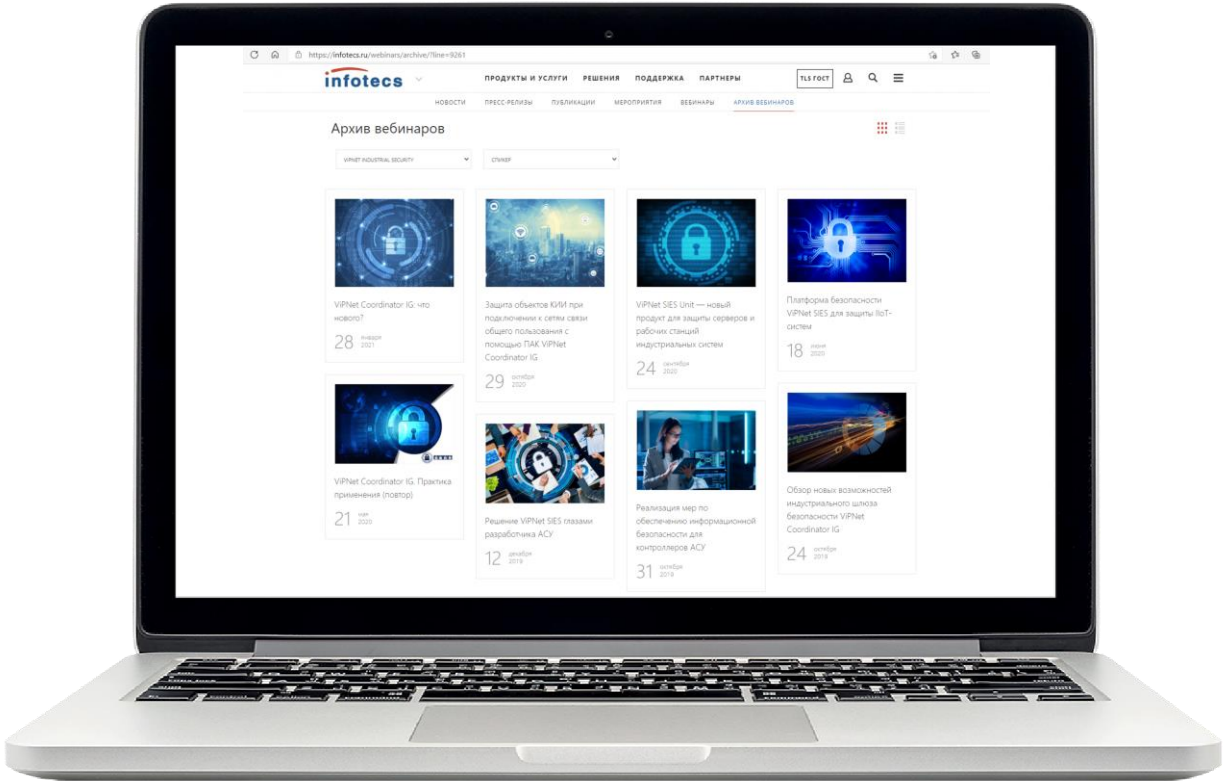
Вся новая информация доступна на сайте – [ViPNet SIES | ИнфоТеКС (infotecs.ru)]

Архив вебинаров



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

Информация по ViPNet SIES



Информация по прошедшим вебинарам (видео и презентации) –

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

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