

Средства защиты информации для автоматизированных систем
управления технологическими процессами

Александр Таранов
ОАО ИнфоТеКС

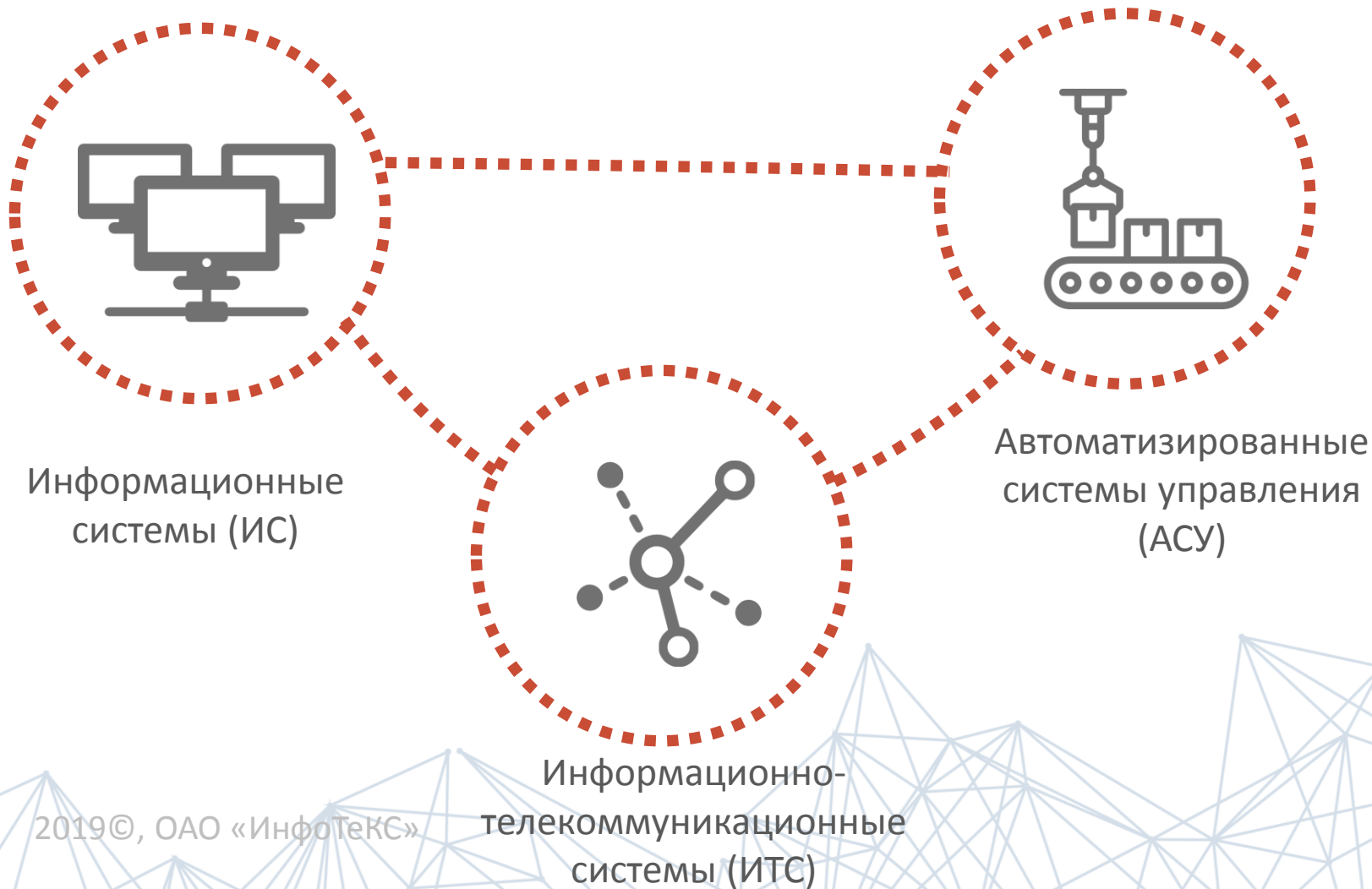
ФЗ №187-ФЗ «О безопасности КИИ»

Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также - критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

70% КИИ – промышленные предприятия



Что защищать в КИИ промышленных предприятий?



Как защищать КИИ промышленных предприятий?

**Приказ ФСТЭК №235
от 21.12.2017**

«Об утверждении
Требований к созданию
систем безопасности
значимых объектов КИИ
РФ и обеспечению их
функционированию»

**Приказ ФСТЭК №239 от
25.12.2017**

«Об утверждении
Требований по
обеспечению
безопасности значимых
объектов КИИ»

Какие задачи должны решаться ?



- Предотвращение неправомерного доступа к информации АСУ,
- Недопущение воздействия на программные и программно-аппаратные средства АСУ,
- Обеспечение функционирования объекта в условиях воздействия угроз безопасности,
- Обеспечение восстановления объекта

ПРОАКТИВНАЯ ЗАЩИТА ИНФОРМАЦИИ

Какие объекты АСУ защищать?



Информация о параметрах и объектах процесса АСУ

Входная и выходная информация, управляющая информация, контрольно-измерительная информация, иная критическая информация.



Средства защиты информации



Программные средства АСУ

Микропрограммное, общесистемное, прикладное программное обеспечение.



Архитектура и конфигурация АСУ



Программно-аппаратные средства АСУ

АРМ, промышленные серверы, телекоммуникационное оборудование, линии связи, ПЛК, производственное и технологическое оборудование, исполнительные устройства

Подход №1

Наложенные СЗИ

Защита каналов

Защита периметра

Сегментирование



Подход №2

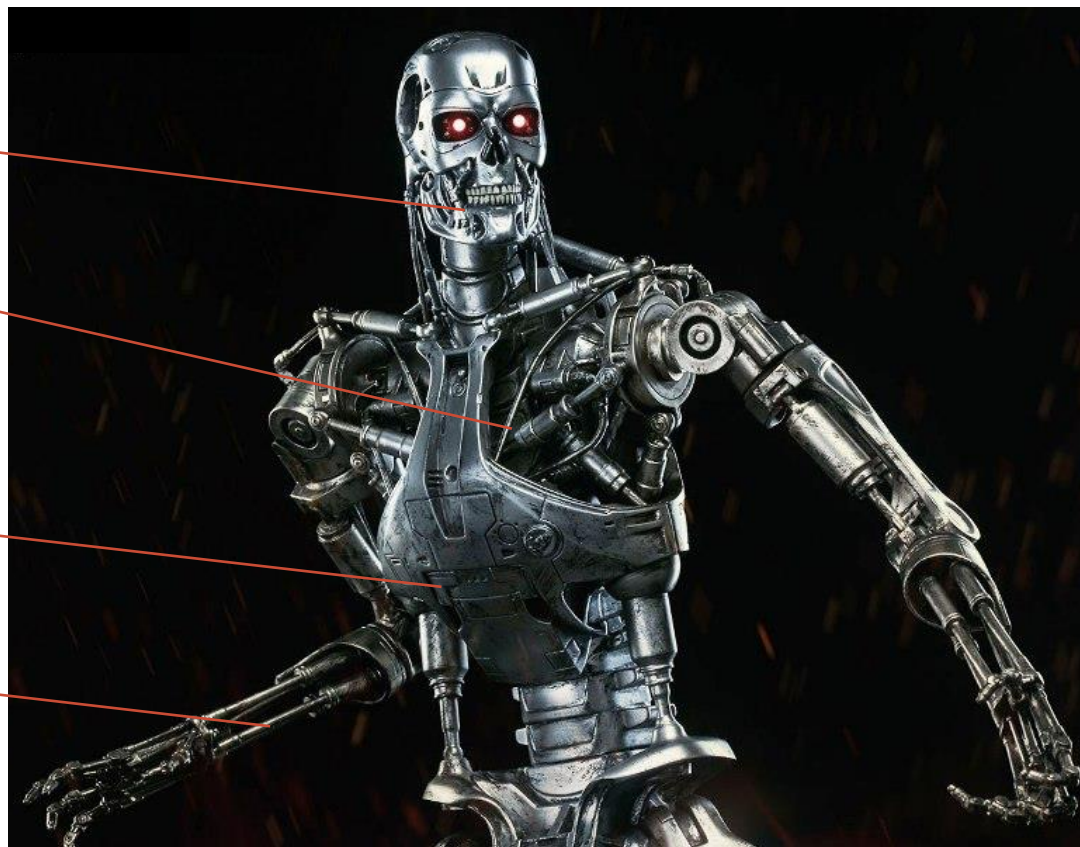
ПО и ПАК АСУ с функциями СЗИ

Аутентификация

Доверенная
загрузка

Доверенное
обновление

Доверенные
коммуникации



Подход №1

Средства защиты информации:
ViPNet Coordinator IG и линейка ViPNet
Network Security

Возможности ViPNet Coordinator IG



- Защита цифрового периметра промышленной сети
- Сегментация сети и защита доступа к сегменту
- Удаленный защищенный доступ к сегменту и его оборудованию
- Защищенные каналы для беспроводных сетей
- Защищенный канал между сегментами сети, в том числе для распределенных систем
- Защищенный канал для последовательных сетей
- Телеуправление и телеконтроль - защищенный удаленный мониторинг и управление
- Телесервис – удаленное сервисное обслуживание
- Удаленный защищенный доступ с мобильных устройств для конфигурирования и обслуживания устройств внутри защищенного сегмента

Если коротко: ViPNet Coordinator IG

VPN – шлюз
По требованиям
к СКЗИ класса
КСЗ



Межсетевой экран
Типа «Д» 4 класса
Типа «А» 4 класса



**Доверенная
платформа**
Собственная
схемотехника



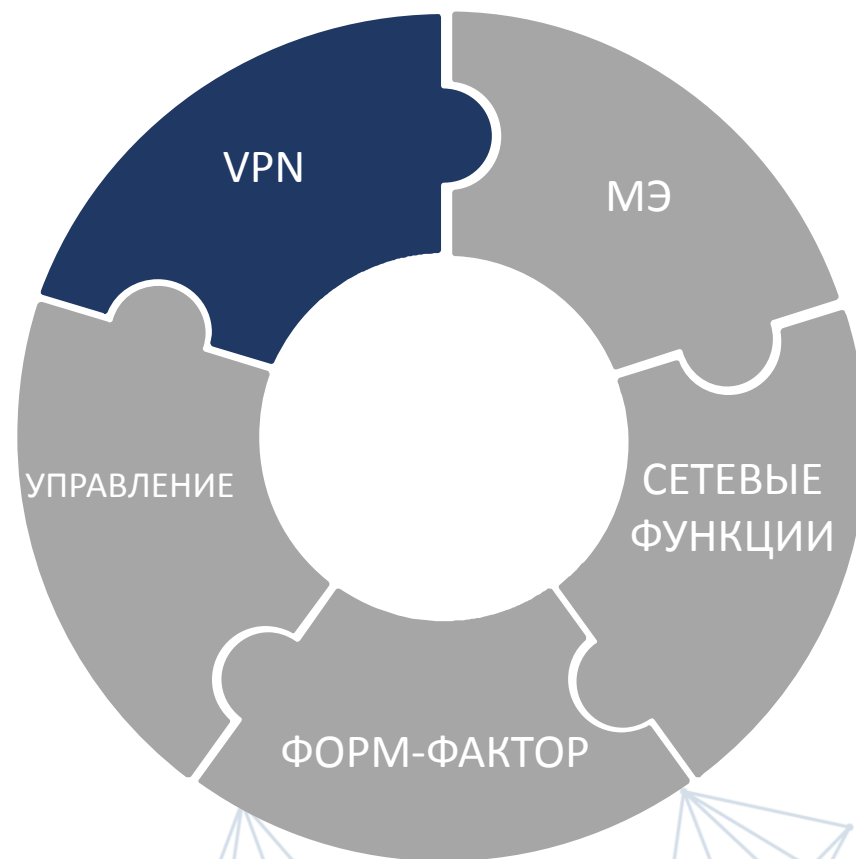
Импортозамещение
Произведено в России

ViPNet Coordinator IG: характеристики

VPN

- ViPNet VPN-шлюз сетевого уровня L3
- ViPNet VPN-шлюз сетевого уровня L2 (L2OverIP)
- VPN-сервер
- 10 Мбит/с и 100 Мбит/с
- ГОСТ 28147-89 (256 бит)
- Аутентификация для каждого зашифрованного IP-пакета

NEW

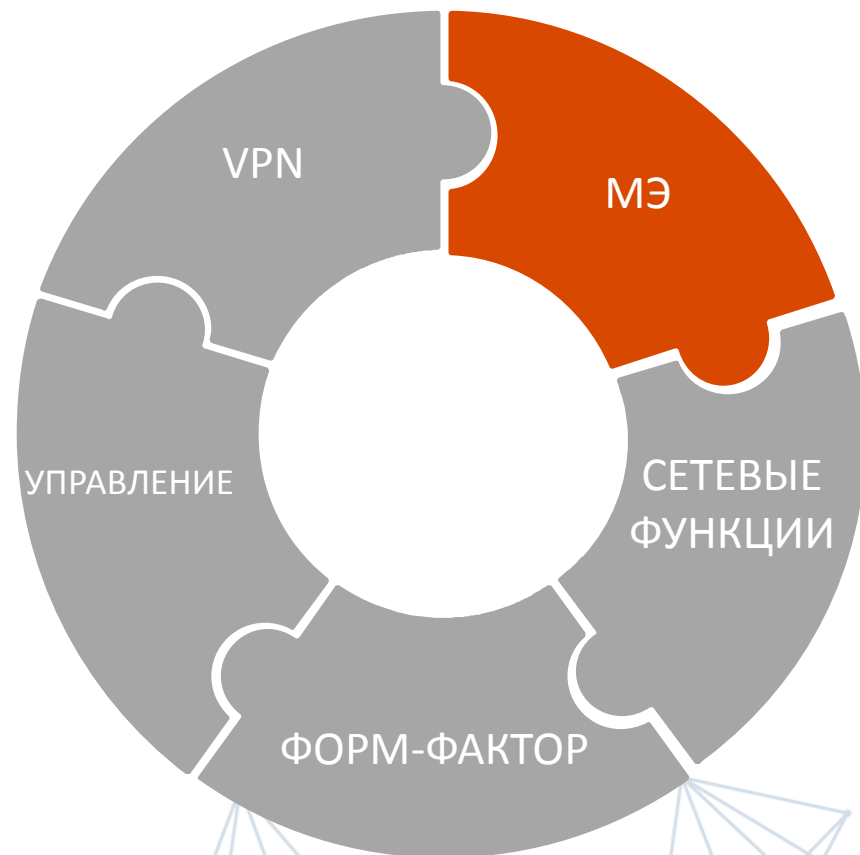


ViPNet Coordinator IG: характеристики

МЕЖСЕТЕВОЙ ЭКРАН

- NAT
- Антиспуффинг
- Пакетная фильтрация по IP источника и назначения, портам и типам протоколов
- Раздельной фильтрации для открытого IP-трафика и шифруемого IP-трафика
- Поддержка промышленных протоколов: EtherNet/IP, Modbus TCP, PROFINET, DNP, IEC 60870-104, MMS, OPC, PTP, bacnet
- DPI для Modbus TCP/RTU

NEW



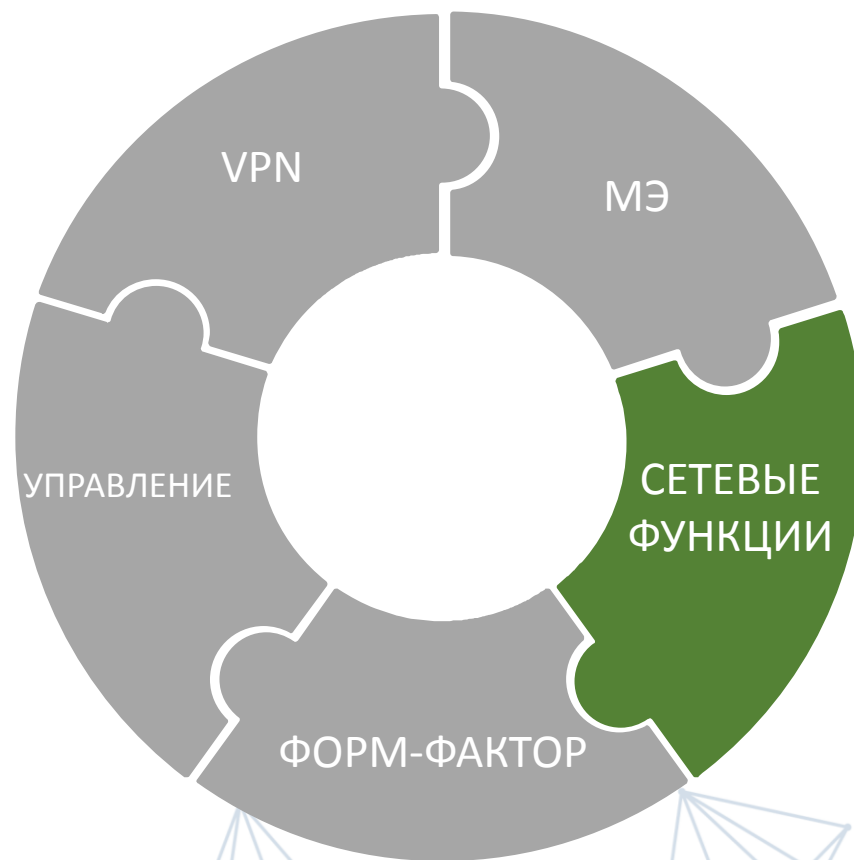
ViPNet Coordinator IG: характеристики

СЕТЕВЫЕ ФУНКЦИИ

- Статическая и динамическая маршрутизация
- DNS-сервер, DHCP-сервер, DHCP-relay
- VLAN, QoS, EtherChanel
- NTP-сервер
- WAN: 1xRJ45 10/100
- LAN: 2xRJ45 10/100
- Wi-Fi: IEEE 802.11 b/g,
- UMTS/HSPA, GSM/GPRS/EDGE
- Шлюза Modbus TCP/RTU
- 2xGPIO (режимы, наз-ние)

NEW

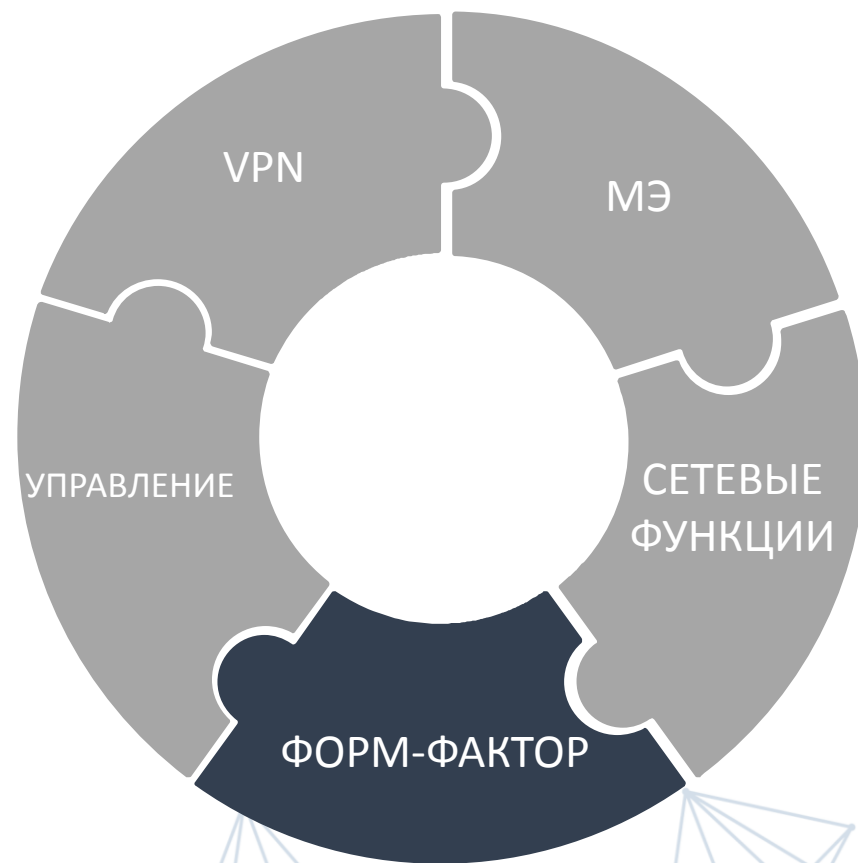
NEW



ViPNet Coordinator IG: характеристики

ФОРМ-ФАКТОР

- ARM-платформа
- Безвентиляторный дизайн
- Рабочая температура: 20°C(-40°C)
... +60°C
- IP30 и бокс IP65 для кластера 
- Напряжение питания: 12...24 В DC
- Крепление на din-рейку
- 50x120x120 мм, 0.6 кг
- ЭМС: ГОСТ 51318.22/CISPR22, ГОСТ CISPR 24

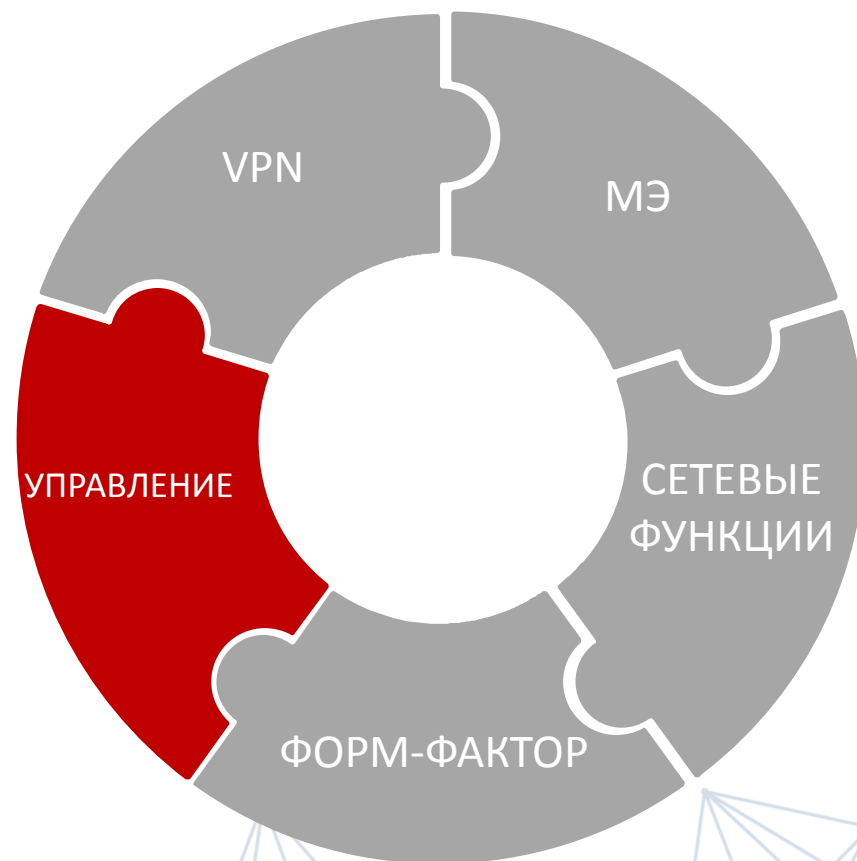


ViPNet Coordinator IG: характеристики

УПРАВЛЕНИЕ

- Настройка: Web-интерфейс, консоль, SSH,
- Обновления: локально, ViPNet Administrator
- Удаленное управление : ViPNet Administrator, ViPNet Policy Manager
- Удаленный мониторинг: ViPNet StateWatcher, SNMP, Syslog
- Event log: Firewall Event, System Security Event
- Штатный, режим обслуживания АСУ, аварийный режимы для МЭ типа Д

NEW



ViPNet Coordinator IG: Надежность



- Кластер горячего резервирования (Failover)
- 24/7/365 режим работы
- 350 тыс. часов наработка на отказ

ViPNet Coordinator IG: Исполнения

	ViPNet Coordinator IG10	ViPNet Coordinator IG100
Платформа	IG10 I1	IG100 I1
Количество туннелей	• 5 туннелей • без ограничений	• 5 туннелей • без ограничений
Дополнительные беспроводные модули	• Wi-fi - модуль • GSM-модуль (3G)	• Wi-fi - модуль • GSM-модуль (3G)
Поддержка интерфейсов	• Ethernet • Ethernet + Serial interface	• Ethernet • Ethernet + Serial interface

ViPNet Coordinator IG: Сертификация

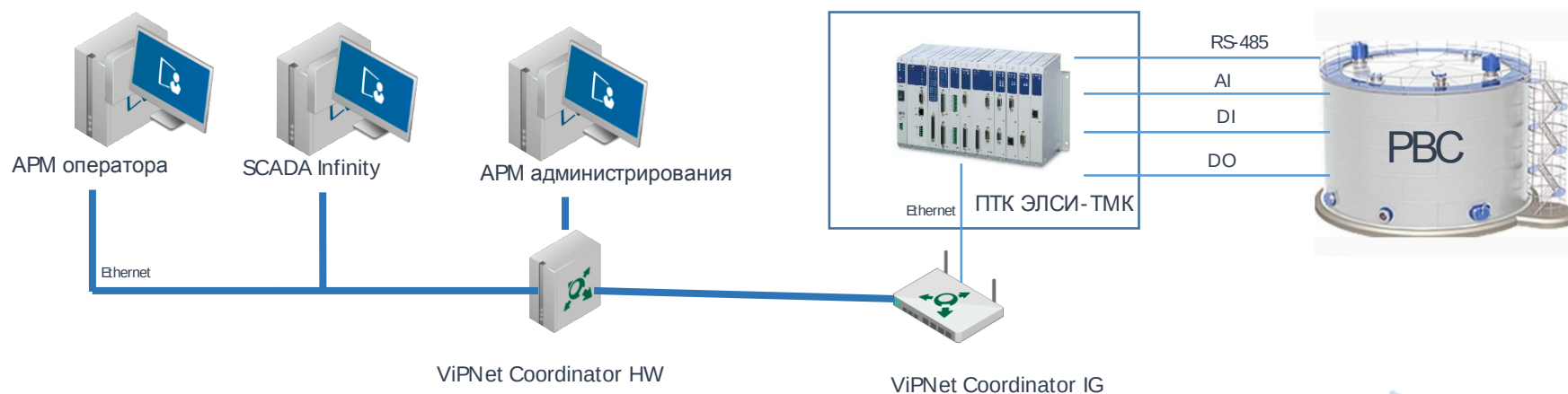
- ViPNet Coordinator IG
 - по требованиям ФСБ к КСЗ
 - по требованиям МЭ типа А.4 и типа Д.4

Пример защиты АСУ на основе ПТК ОАО «ЭлеСи»

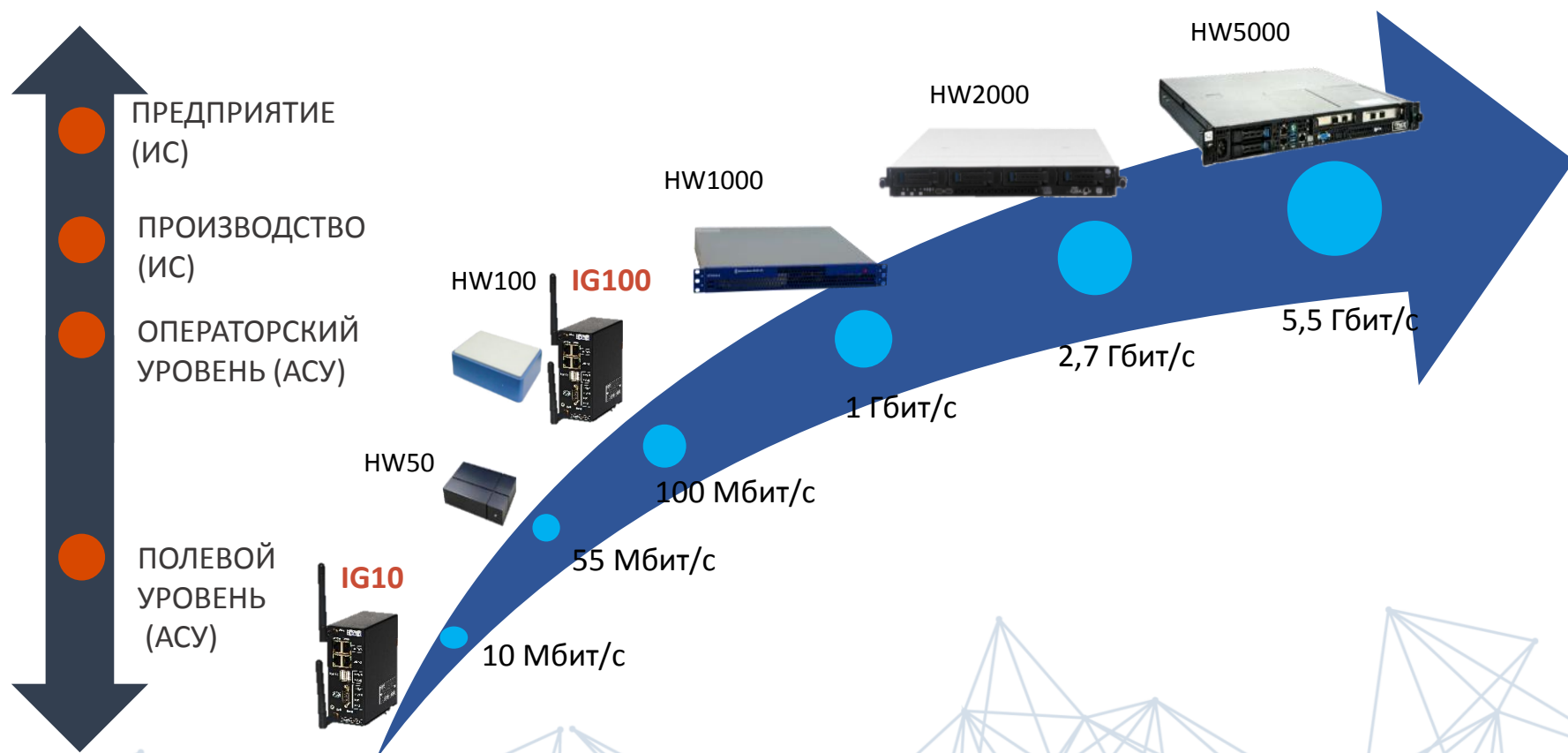
«Верхний» уровень

«Средний» уровень

«Нижний» уровень



НЕПРЕРЫВНАЯ БЕЗОПАСНОСТЬ ОТ АСУ до ИС



Соответствия требованиям По защите информации



ViPNet Administrator

Требования по
обеспечению
защиты
информации
в АСУ ТП
Приказ ФСТЭК
№ 31 от 14.03.2014



ViPNet Coordinator
HW/IG

Требования по
обеспечению
безопасности
значимых объектов
КИИ
Приказ ФСТЭК
№239 от 25.12.2017



ViPNet Client



SAILFISH OS

Требования о защите
информации в ГИС
Приказа ФСТЭК
№ 17 от 11.03.2013



ViPNet Policy
Manager

Требования о защите
персональных
данных в ИС
Приказа ФСТЭК
№ 21 от 18.02.2013



ViPNet
Statewatcher

Требования о защите
информации в ИС
общего пользования
Приказы ФСБ/ФСТЭК
№ 416/489 от
31.08.2010

Подход №2

Встраиваемое решение ViPNet SIES для защиты информации АСУ объектов КИИ

Решение ViPNet SIES

УПРАВЛЕНИЕ

ПАК ViPNet SIES MC
ПО ViPNet SIES WorkStation



ОПЕРАТОРСКИЙ УРОВЕНЬ

ПАК ViPNet PKI Service
ПО ViPNet SIES Unit

NEW

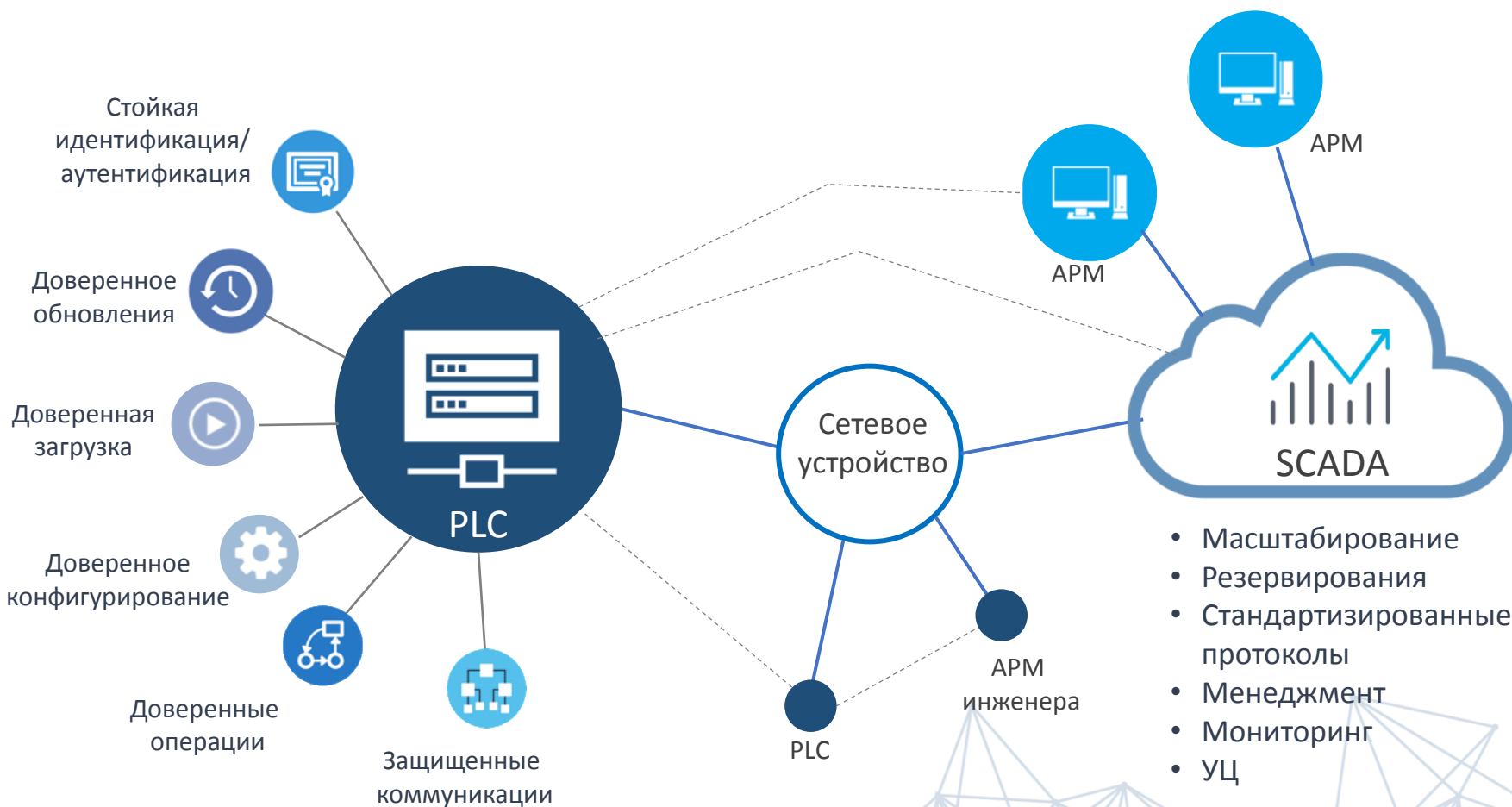


ПОЛЕВОЙ УРОВЕНЬ

ПАК ViPNet SIES Core
KAM200-80



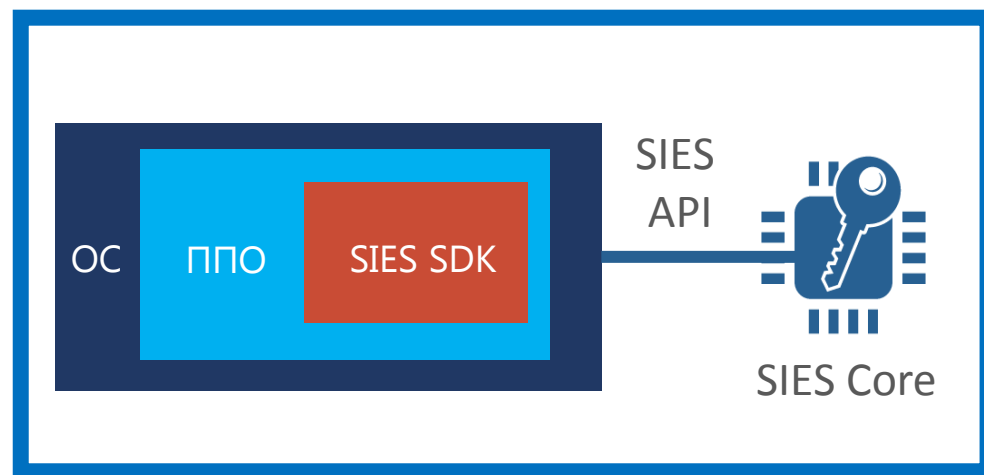
End-to-end решение



Встраивание ViPNet SIES

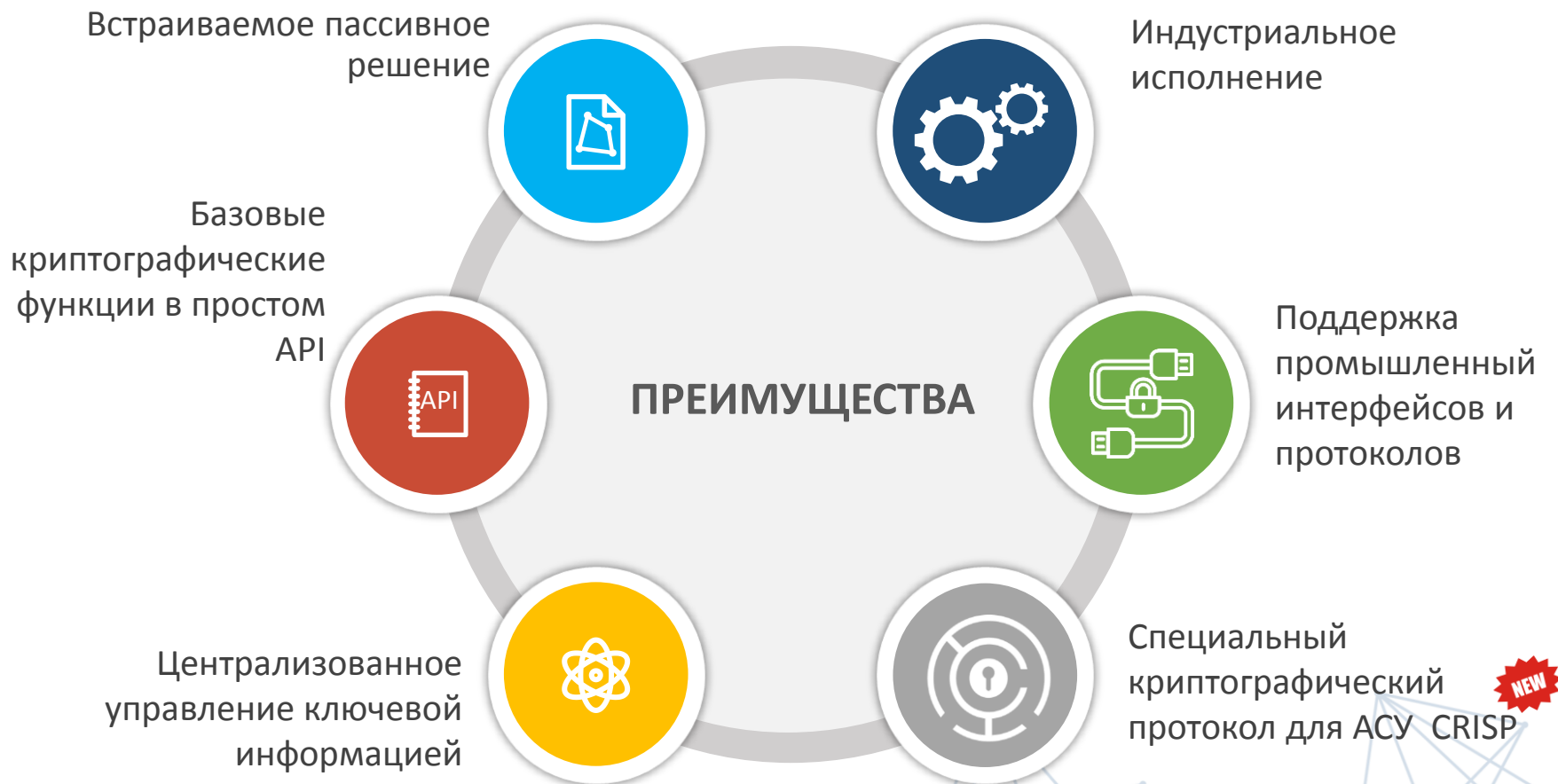


Криптомодуль
SIES Core



Контроллер (PLC, IED, счетчик и т. д.)

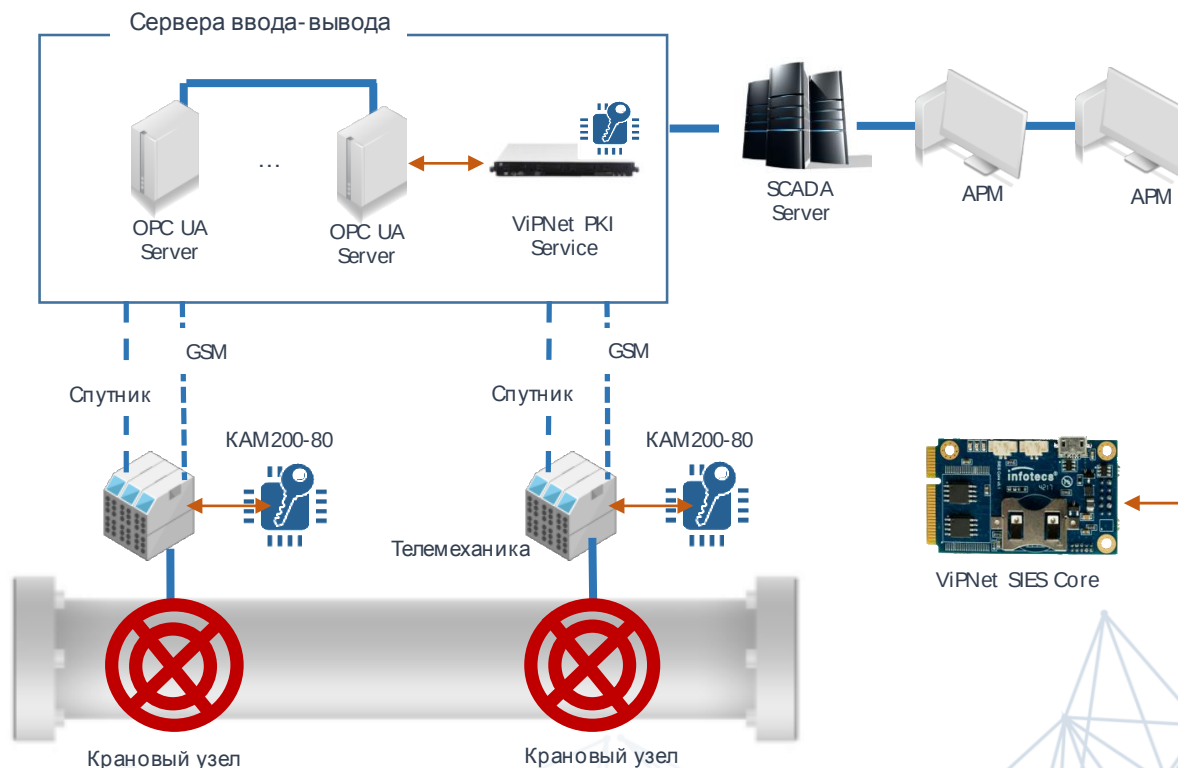
Решение ViPNet SIES



Компоненты решения ViPNet SIES

	ViPNet SIES Core	PKI Service (SIES Server)	ViPNet SIES Unit + PKI Client 
Уровень АСУ	Автоматизированного управления, Полевой	Операторский	Операторский
Интерфейс встраивания в устройство	UART, USB	Ethernet	WebAPI
API	SIES API	REST API	WebAPI
Форм-фактор	SOM-модуль, 4 -15 В DC, -40 ⁰ ...+75 ⁰ C	Сервер, 220В AC, 0...+40 ⁰ C	ПО
Криптография	ГОСТ 2814789, ГОСТ Р34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.13-2015  		

Пример защиты системы управления задвижками газопровода



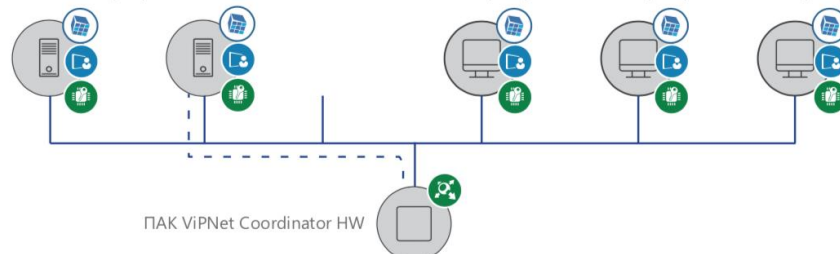
Подход №3

Наложенные СЗИ + Встраиваемые СЗИ

ViPNet Coordinator IG и ViPNet SIES с Master SCADA

«Верхний уровень»

Кластер из SCADA-Серверов MasterSCADA APM оператора APM оператора APM оператора



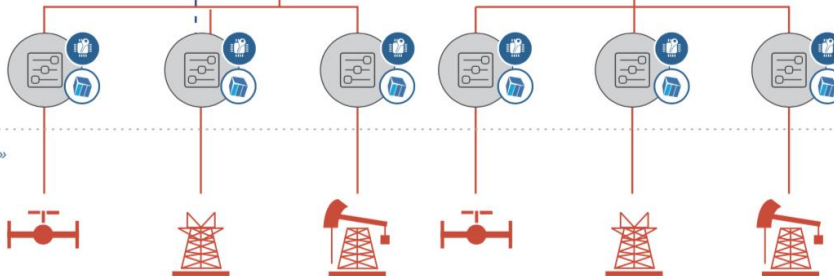
Коммуникационный уровень



«Средний» уровень



«Нижний» уровень

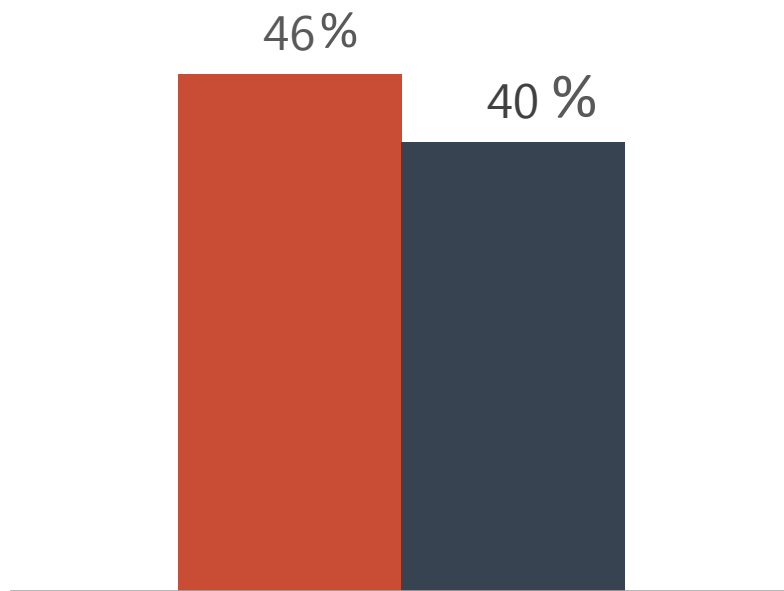


Датчики и технологическое оборудование

Датчики и технологическое оборудование

- ПК ViPNet Client
- ПАК ViPNet Coordinator IG/HW
- ПАК ViPNet SIES Core
- ПК ViPNet SIES Server
- MasterSCADA
- MasterPLC

Соответствие мерам Приказа ФСТЭК №239



Меры за исключением
организационных

- Coordinator IG/HW
- ViPNet SIES

Можно закрыть

~55%

мер

Комбинированный
подход

Дирекция автодорог Кемеровской области

Список узлов

11.0.0.2/nodeList.action

Operator

Инфопанель Мониторинг История событий

Список Карта Каскад

Узлы мониторинга: 39

Опробовать группу Экспорт Все группы Все события Сбросить

Тип узла	Имя узла	События	Идентиф...	IP-адрес	Версия ПО VIPNet	Время узла	Время опроса	Состояние
Группа по умолчанию								
☒	СМ 'ЦОД Дирекция автодорог Кузбасса' (H4W1...		2H2000a	172.20.1.1	4.2.4.2443	17:50:59 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
Модули криптозащиты								
☒	СМ 'Прокопьевск, Серова, 27'		2H2000f	11.0.0.6	4.2.1.704	17:53:42 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'Прокопьевск, Строителей, 29 (1)'		2H2000e	11.0.0.5	4.2.1.704	17:51:18 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'Киселевск, Геологическая - Пихтовая'		2H20013	11.0.0.10	4.2.1.704	17:51:38 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'Л-К-Прокопьевск-Нк, км 30'		2H2000c	11.0.0.3	4.2.1.704	17:50:57 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'ЛК - Нк - Межд., км 187'		2H20014	11.0.0.11	4.2.1.704	17:50:27 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'Прокопьевск, Проспектная,16'		2H20010	11.0.0.7	Неизвестно	17:49:33 - 18.12.2018	17:49:33 - 18.12.2018	Недоступен
☒	СМ 'Киселевск, Панфилова - Багратиона'		2H20011	11.0.0.8	4.2.1.704	17:50:16 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'Мыски, Советская, 28'		2H20016	11.0.0.13	4.2.1.704	17:50:53 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'ЛК - Нк - Межд., км 195'		2H20015	11.0.0.12	4.2.1.704	17:50:49 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'Киселевск, Красный камень'		2H20012	11.0.0.9	4.2.1.704	17:50:49 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'АС, Матросова,111'		2H20017	11.0.0.14	4.2.1.704	17:49:40 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'Белово, Южная - Кошелева'		2H2001e	11.0.0.21	Неизвестно	17:49:33 - 18.12.2018	17:49:33 - 18.12.2018	Недоступен
☒	СМ 'АС, Мира, 13'		2H20019	11.0.0.16	4.2.1.704	17:49:34 - 18.12.2018	17:49:33 - 18.12.2018	Доступен
☒	СМ 'АС, Желязова, 13'		2H2001a	11.0.0.17	4.2.1.704	17:49:45 - 18.12.2018	17:49:33 - 18.12.2018	Доступен

Справка О программе



Информация о партнере

ООО «КриптоСвязь»

www.infotrust.ru

+7(3412)918-100

crypto@infotrust.ru

Спасибо за внимание!

Таранов Александр
ОАО ИнфоТеКС