kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Марина Сорокина

Руководитель продуктового направления, ИнфоТеКС

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

Российский криптошлюз и межсетевой экран для промышленных систем

Марина Сорокина

Группа компаний ИнфоТеКС

infotecs

Топ-2
вендоров в сфере защиты информации в России

9
офисов по всей стране

> 50
продуктов для защиты информации

29
лет работы на рынке ИБ

> 1000
сотрудников

> 1 млн
рабочих станций защищенных продуктами ViPNet

Направление СЗИ для защиты АСУ от ИнфоТеКС

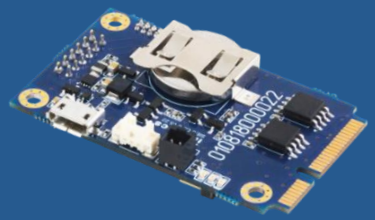
Сетевые средства защиты информации

ViPNet Coordinator IG10
ViPNet Coordinator IG100



Встраиваемые средства защиты информации

ViPNet SIES:
ViPNet SIES Core
ViPNet SIES Unit
ViPNet SIES MC



О чем будет презентация?

- Как выбрать сетевые средства защиты информации для АСУ?
- Что такое российские сетевые средства защиты информации для АСУ?
- Стоит ли уже сегодня инвестировать в их приобретение?
- Как ИнфоТеКС развивает свою линейку сетевых средств защиты информации для АСУ

Сетевые средства защиты информации для АСУ

Как выбрать средства сетевой безопасности для АСУ?

Нормативные требования по применению средств сетевой безопасности USA vs EU vs RU

NIST SP800-82 R2	IEC-62443-2-1	Приказ №239 от 25.12.2017 ФСТЭК России	Приказ №31 от 14.03.2014 ФСТЭК России
6.2.2 Physical and Environmental protection 6.3.4 System and communication Protection	9.1 Secure areas 11.4.6 Network connection control	ЗИС.2 Защита периметра	ЗИС.2 Защита периметра
5.2. Logically separated control work 5.3 Network segregation	11.4.5 Segregation in network	ЗИС.4 Сегментирование АСУ	ЗИС.4 Сегментирование АСУ
6.3.4 System and communication Protection	10.8 Exchange of information	ЗИС.19 Защита информации при ее передаче по каналам связи ЗИС.20 Обеспечение доверенных каналов, маршрутов	ЗИС.19 Защита информации при ее передаче по каналам связи ЗИС.20 Обеспечение доверенных каналов, маршрутов
6.3.4 System and Communication protection	10.6 Network security management	ЗИС.24 Обеспечение подлинности сетевых соединений	ЗИС.27 Обеспечение подлинности сетевых соединений

Нормативные требования по применению средств сетевой безопасности USA vs EU vs RU

NIST SP800-82 R2	IEC-62443-2-1	Приказ №239 от 25.12.2017 ФСТЭК России	Приказ №31 от 14.03.2014 ФСТЭК России
6.3.2.5 Wireless NIST SP800-48 and NIST SP800-97	11.7.3 Wireless Access Restrictions 11.7 Mobile computing and teleworking	ЗИС.32 Защита беспроводных соединений	ЗИС.32 Защита беспроводных соединений
6.3.4 System and Communication protection	10.6 Network security management	ЗИС.35 Управление сетевыми соединениями	ЗИС.35 Управление сетевыми соединениями
	11.4.6 Network connection control 11.4.10 Remote Access	УПД.13 Реализация защищенного удаленного доступа	УПД.13 Реализация защищенного удаленного доступа
6.2.6 System and Information Integrity in accordance with SP800-83	10.6.2 Security of network services	СОВ.1 Обнаружение и предотвращение компьютерных атак	СОВ.1 Обнаружение вторжений
6.2.8 Incident response NIST SP800-61	13.2 Management of cyber security incidents and improvements	ИНЦ.1 Выявление компьютерных инцидентов ИНЦ.2 Информирование о компьютерных инцидентах	ИНЦ.1 Выявление компьютерных инцидентов ИНЦ.2 Информирование о компьютерных инцидентах

Основные функциональные требования к сетевым средствам защиты информации

infotecs

Криптошлюз, VPN-шлюз

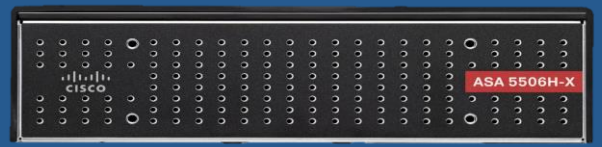
Межсетевой экран

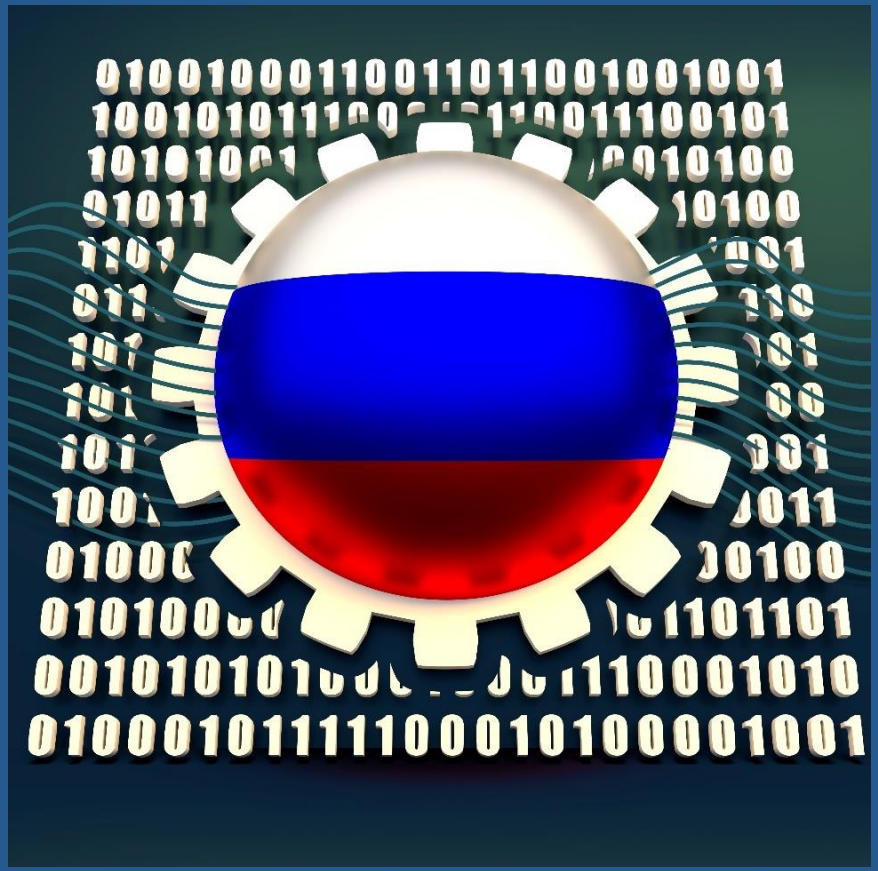
Обнаружение вторжений

Сетевой функционал

Если функционал одинаковый, то как сделать выбор?

infotecs





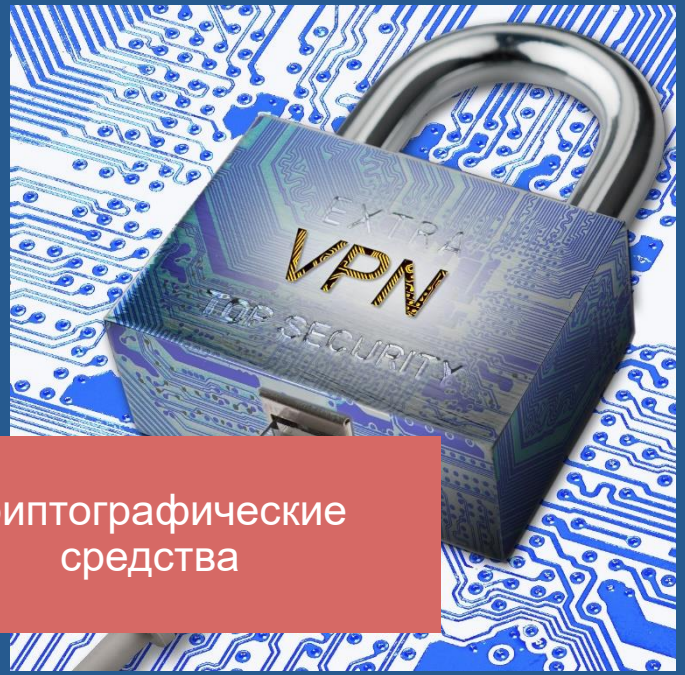
Российские нюансы в требованиях по защите АСУ

Применение сертифицированных СЗИ в случаях, установленных законодательством РФ

(п.28 Приказ ФСТЭК России №239 от 25.12.2017)

Российские нюансы в требованиях по защите АСУ

- Обязательная сертификация СКЗИ в соответствии с Приказом ФСБ России от 9.02.2005 г №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»
- Выбор класса СКЗИ зависит от модели угроз и нарушителя:
  - СКЗИ КС1 – внешний нарушитель
  - СКЗИ КС3 и выше – внутренний нарушитель



Криптографические средства

Российские нюансы в требованиях по защите АСУ

КИИ:

- Для несертифицированных СЗИ необходима оценка в виде испытаний и приемки, проводимая субъектами КИИ самостоятельно или с привлечением организаций, имеющих соответствующие лицензии (п.28 Приказ ФСТЭК России №239 от 25.12.2017)
- Для сертифицированных СЗИ должны быть проведена сертификация по требованиям доверия (п.29 Приказ ФСТЭК России №239 от 25.12.2017)

АСУ ТП:

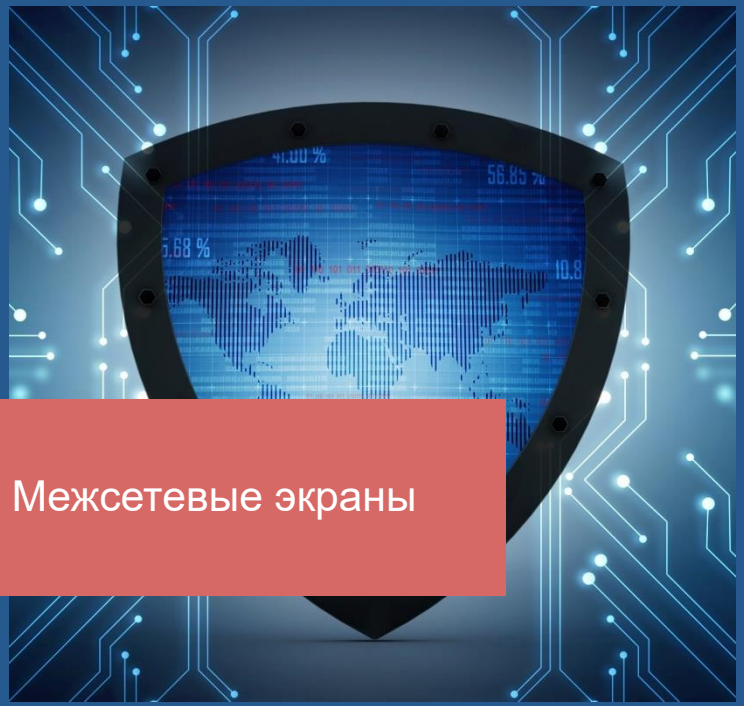
- применяются СЗИ, прошедшие оценку соответствия в соответствии с законодательством РФ о техническом регулировании (п.11 Приказ ФСТЭК России №31 от 14.03.2014)

Российские нюансы в требованиях по защите АСУ

- Требований к межсетевым экранам от 28.04.2016 г. No 240/24/1986.
- Профили защиты МЭ от 12.19.2016 г.

Межсетевой экран уровня промышленной сети (типа «Д»)

Межсетевой экран типа «А» на физической границы промышленной сети



Российские нюансы в требованиях по защите АСУ

- Требований к СОВ от 06.12.2011 г. No 638
- Профили защиты СОВ от 2012 г.

Системы обнаружения вторжений

Промышленный шлюз безопасности от ИнфоТеКС

Российский шлюз безопасности ПАК ViPNet Coordinator IG

NAT

Антиспуффинг

Раздельная фильтрация для открытого и шифруемого трафика

DPI для Modbus

Раздельные наборы для режимов работы

infotecs

ViPNet VPN-шлюз уровня L3

ViPNet VPN-шлюз уровня L2 (L2OverIP)

VPN-сервер

Аутентификация для каждого зашифрованного IP-пакета

VPN–шлюз
по требованиям к СКЗИ класса КС3

Межсетевой экран
SPI,DPI
Типа «Д» 4 класса
Типа «А» 4 класса

Сетевые функции

Статическая и динамическая маршрутизация

DNS-сервер, DHCP-сервер, DHCP-relay

VLAN, QoS, Etherchannel

NTP-сервер

Эксплуатации в промышленных средах

Безвентиляторный дизайн

Рабочая температура от-40^{0}C … +60^{0}C

ЭМС промышленного класса

Исполнения ViPNet Coordinator IG

ViPNet Coordiantor
IG10 I1

ViPNet Coordiantor
IG100 I1

ViPNet Coordiantor
IG10 I2*

* Планы Q4 2020

Исполнения ViPNet Coordinator IG

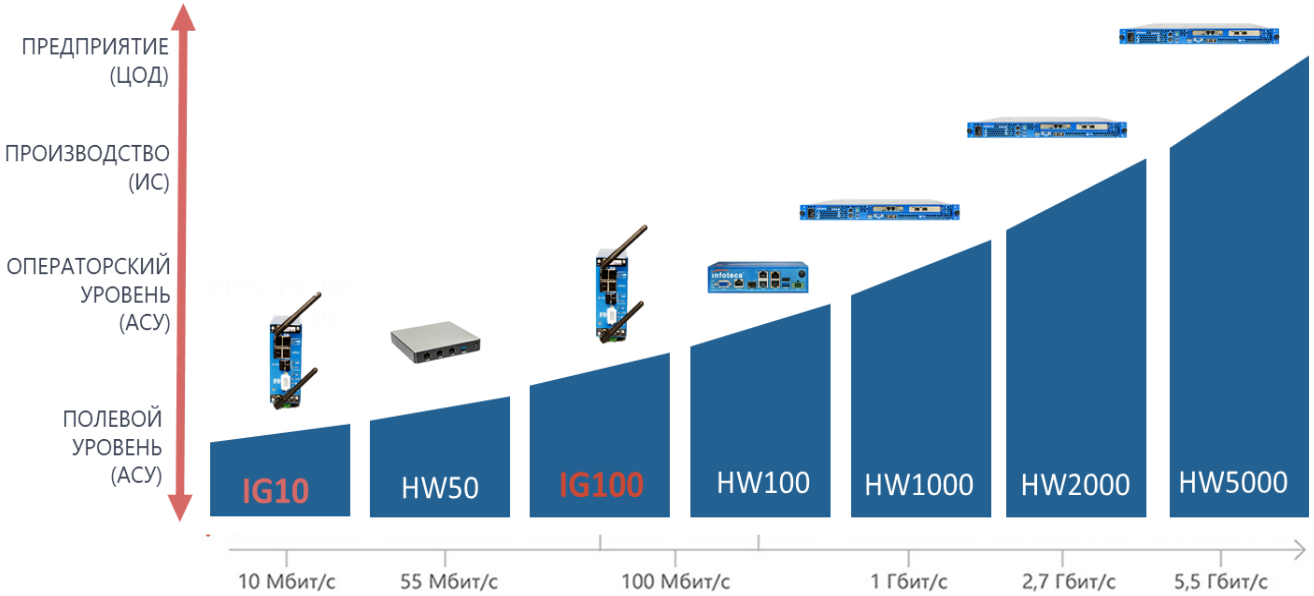
	ViPNet Coordinator IG10 I1	ViPNet Coordinator IG100 I1	ViPNet Coordinator IG10 I2
Производительность L3 VPN и L2 VPN	до 10 Мбит/с	до 60 Мбит/с	до 100 Мбит/с
Производительность МЭ	до 10 Мбит/с	до 60 Мбит/с	до 100 Мбит/с
Проводные интерфейсы	Ethernet 3xRJ45	Ethernet 3xRJ45	Ethernet 5xRJ45
Беспроводные 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^{0}C (-40 ^{0}C)...+60^{0}C	-20^{0}C...+60^{0}C	-40^{0}C…+60^{0}C
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)

* Планы Q4 2020

infotecs

Вопросы надежности

- Кластер горячего резервирования (Failover)
- MultiWan
- 24/7/235 режим работы
- 350 тыс. часов наработки на отказ



Экосистема VIPNet VPN

- Встречная работа
- Единое управление

Экосистема VIPNet VPN:
ПК ViPNet Client для конечных устройств

infotecs

КОМПЬЮТЕРЫ
НОУТБУКИ

ТЕЛЕФОНЫ
ПЛАНШЕТЫ

Встраиваемая
версия
ViPNet Client 4U

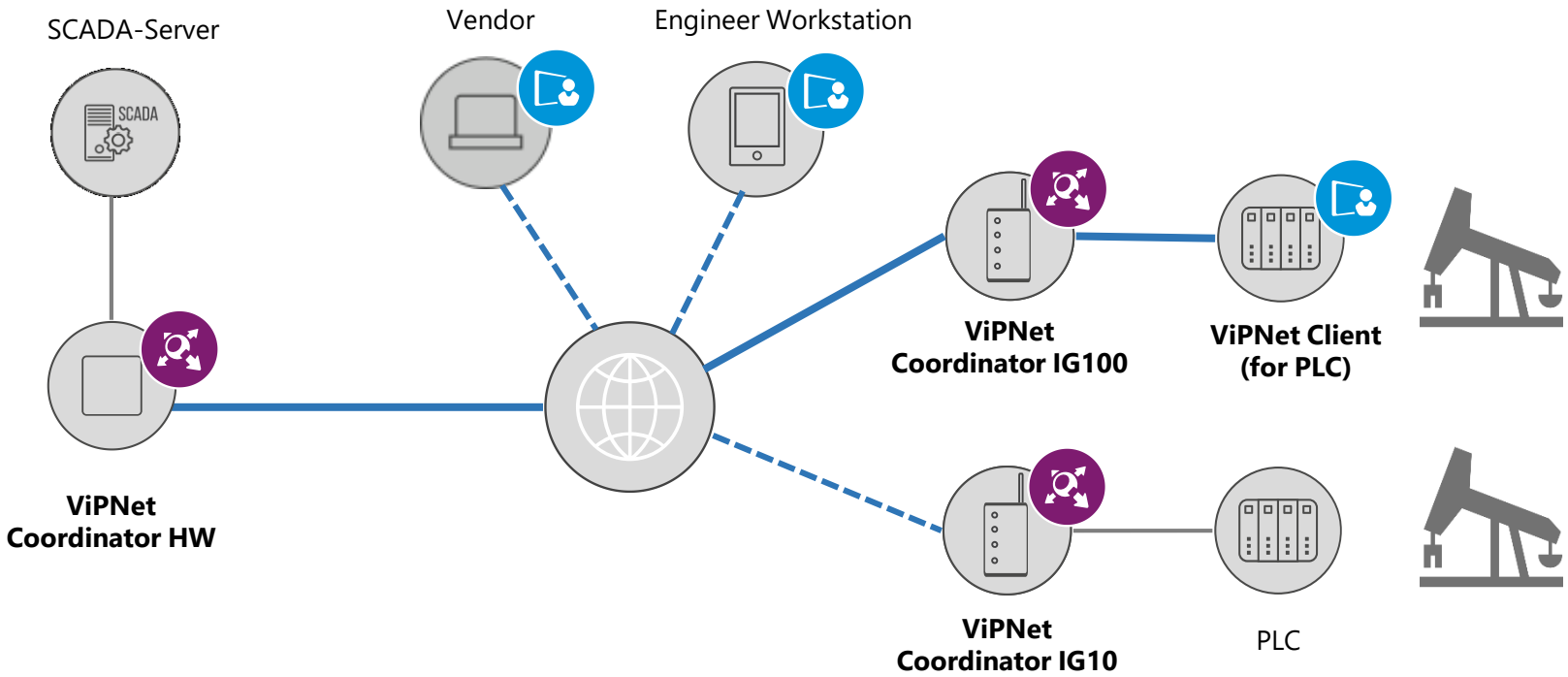
LINUX BASED

КОНТРОЛЛЕРЫ

Экосистема VIPNet VPN: Управление

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

ViPNet VPN позволяет реализовывать самые сложные сценарии



infotecs

Импортозамещение или круг сужается

Тренды в российском законодательстве

Аннотация к проекту изменений Приказа ФСТЭК России №239 от февраля 2020 г:

«Изменения направлены на использование в критической информационной инфраструктуре Российской Федерации преимущественно отечественного программного обеспечения и оборудования в целях обеспечения её технологической независимости и безопасности, а также создания условий для продвижения российской продукции.

...

Вносимые изменения касаются уточнения условий выбора программного обеспечения и оборудования, используемого в составе значимых объектов критической информационной инфраструктуры, а также порядка его принятия к эксплуатации на таких объектах.»

Проект изменений Приказа ФСТЭК России №239 от 25.12.2017 г.

- Запрет технической поддержки ПО и ПАК со стороны организаций, находящихся под прямым или косвенным контролем иностранных юр.лиц
- Запрет прямого удаленного доступа сотрудникам организаций, находящихся под прямым или косвенным контролем иностранных юр.лиц
- Применение 5-го уровня доверия и выше для всех СЗИ
- Необходимость проверки как защищены несертифицированные СЗИ

Импортозамещение

- Ужесточение требований по применению иностранного ПО и оборудования в КИИ (выступление представителя Минпромторг на ТБ Форуме)
- Единый реестр отечественного ПО
- Постановление правительства №878 от 10.07.2019 «О мерах стимулирования производства радиоэлектронной продукции на территории РФ»
- Единый реестр отечественной радиоэлектронной продукции

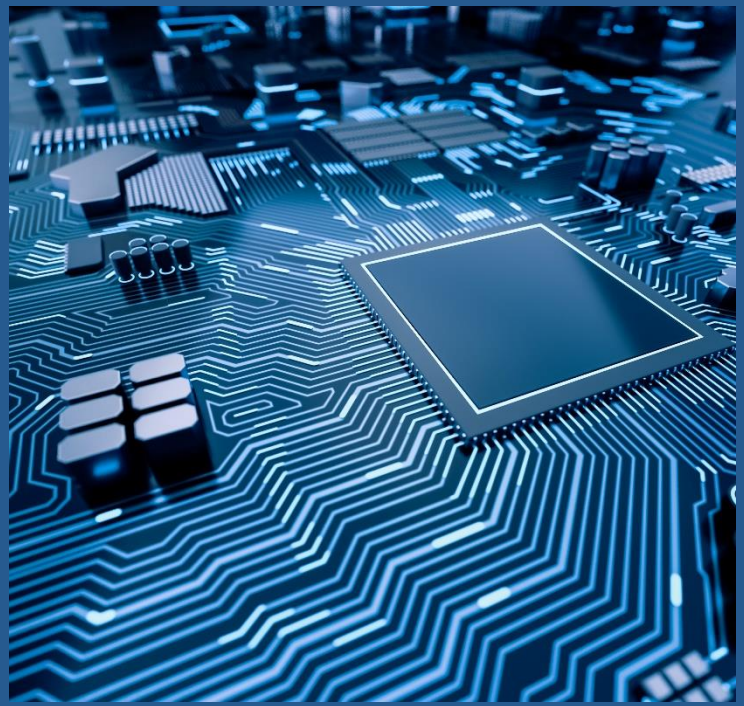
Единый реестр радиоэлектронной продукции

- Состав заявки:
  - конструкторская, программная, технологическая документация,
  - протоколы и акты ПИ, ПСИ
  - сведения о производственной базе и средствах измерения
  - отчетные документы по закупке комплектующих
  - логи с производственных станков
- Подтверждение статуса каждый год

Единый реестр радиоэлектронной продукции

Необходимость перехода на российскую элементную базу:

- Пассивные элементы
- Интегральные микросхемы



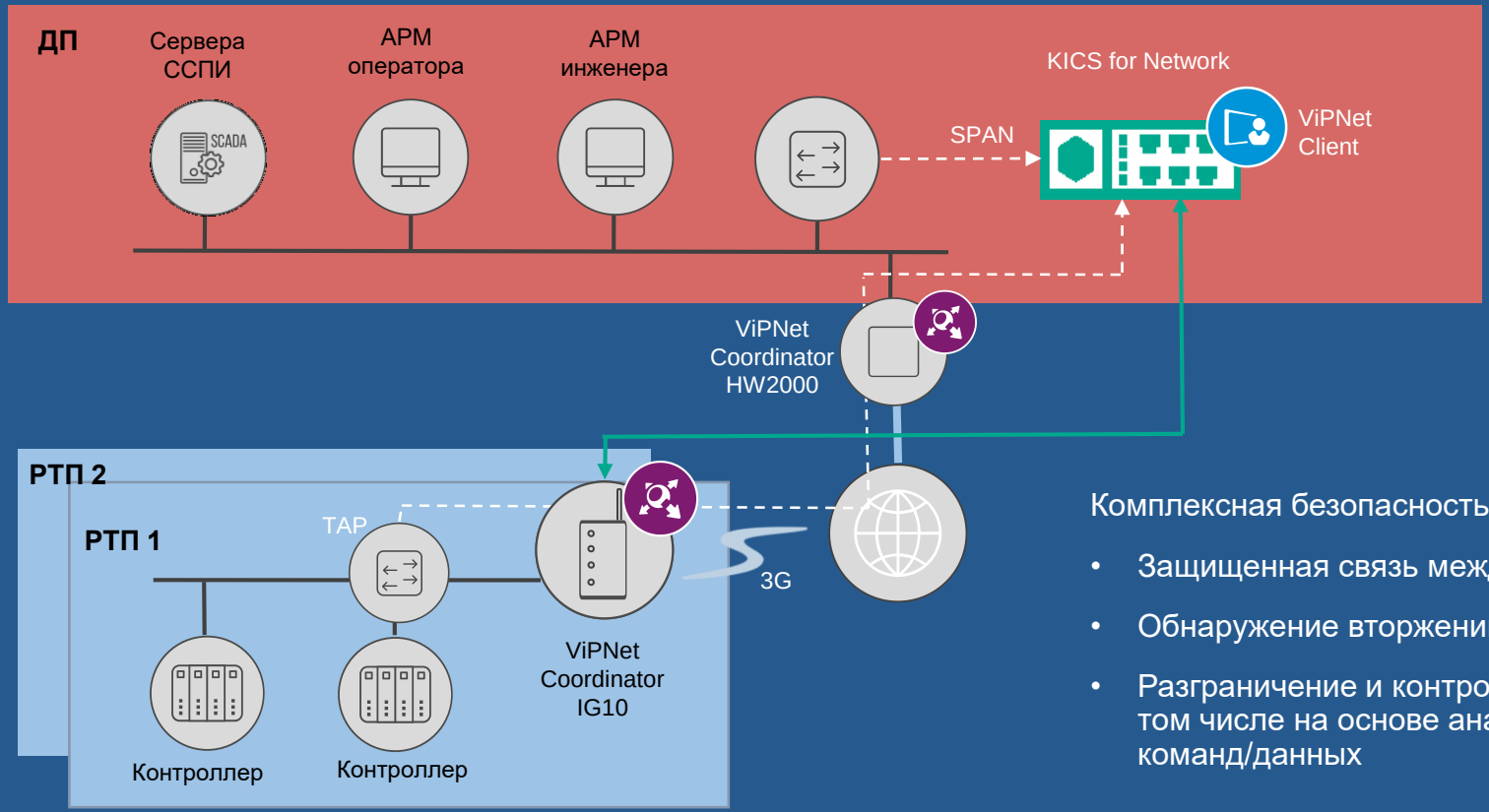
Опыт ИнфоТеКС в части импортозамещения

Статус присвоения ТОРП для ViPNet Coordinator IG

Подана заявка на включение ViPNet Coordinator IG в реестр отечественной радиоэлектронного оборудования в качестве телекоммуникационного оборудования

Интеграция с KICS

Совместная интеграция с KICS



Комплексная безопасность:

- Защищенная связь между объектами
- Обнаружение вторжений в АСУ
- Разграничение и контроль доступа, в том числе на основе анализа команд/данных

Вместо заключения

Выбор российских средств сетевой безопасности - это хорошая стратегия в долгосрочной перспективе российских реалий.

Marina.Sorokina@infotecs.ru
Марина Сорокина

Спасибо за внимание!