12 апреля 2018 г.

infotecs

ПРОМЫШЛЕННЫЕ ШЛЮЗЫ БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ АСУ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ 187-ФЗ

МАРИНА СОРОКИНА,
РУКОВОДИТЕЛЬ ПРОДУКТОВОГО НАПРАВЛЕНИЯ

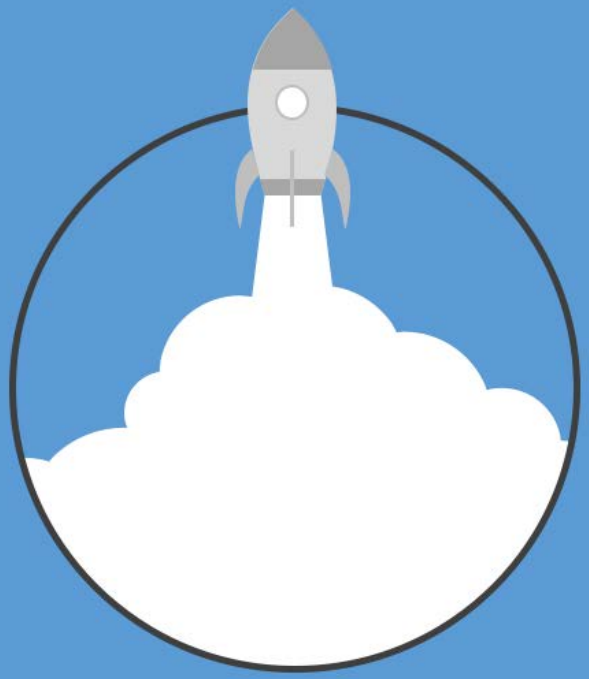
ПЛАН ВЕБИНАРА

01 **Требования Федерального Закона №187-ФЗ**
В части Автоматизированных систем управления

02 **Требования к промышленным шлюзам безопасности**
В части применения в АСУ

03 **ViPNet Coordinator IG**
Первый российский промышленный шлюз безопасности

04 **Основные сценарии использования шлюзов безопасности**
На примере линейки продуктов ViPNet Network Security

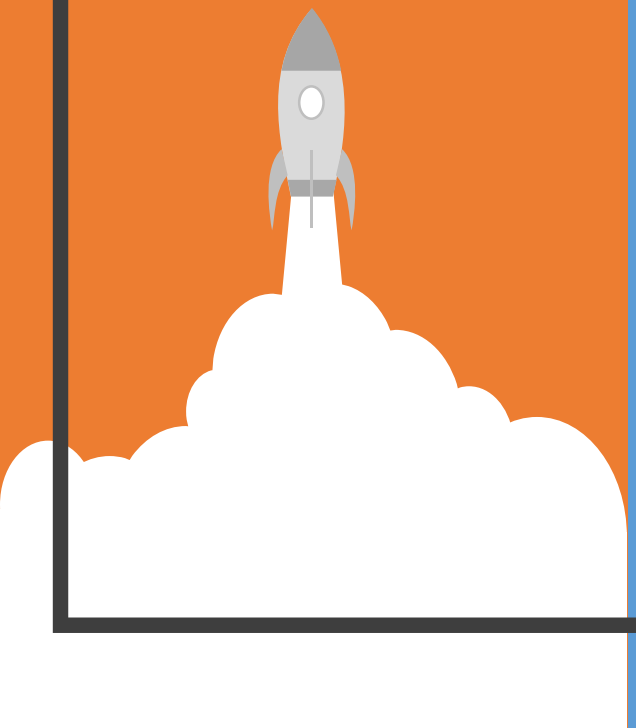


Требования ФЗ №187-ФЗ

В части Автоматизированных систем управления

Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

от 26 июля 2017 г.

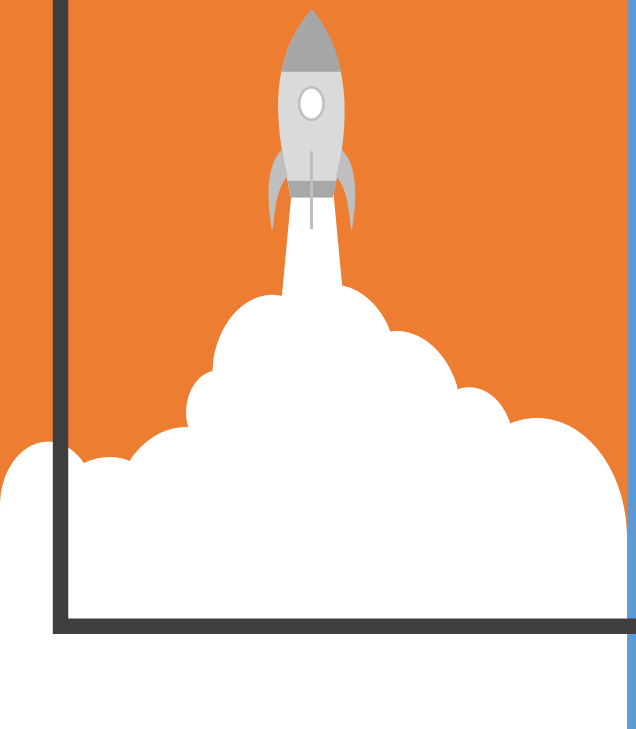


Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также - критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Вступил в силу **1 января 2018 г**.

Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

от 26 июля 2017 г.



- Федеральный закон от 26.07.2017 года № 193-ФЗ «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ»
- Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ»

СУБЪЕКТЫ КИИ

infotecs

В соответствии с ФЗ №187-ФЗ «О безопасности КИИ»

ГОСУДАРСТВЕННЫЕ ОРГАНЫ — АРЕНДА — **ГОСУДАРСТВЕННЫЕ УЧРЕЖДЕНИЯ** — ПРАВО СОБСТВЕННОСТИ — **РОССИЙСКИЕ ЮРЛИЦА** — ИНОЕ ЗАКОННОЕ ОСНОВАНИЕ — **ИП**


Здравоохранение


Наука


Связь


Транспорт


Банковская сфера


Энергетика


ТЭК


Атомная энергетика

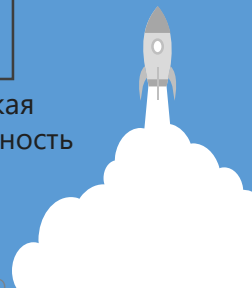

Оборонная промышленность


Ракетно-космическая промышленность


Горнодобывающая промышленность


Металлургическая промышленность

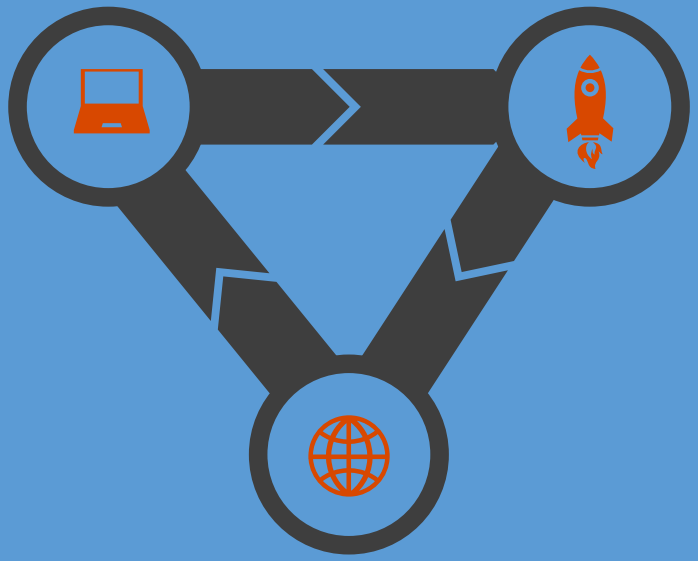

Химическая промышленность



ОБЪЕКТЫ КИИ

В соответствии с ФЗ №187-ФЗ «О безопасности КИИ»

Информационные системы (ИС)



Автоматизированные системы управления (АСУ)

Информационно-телекоммуникационные системы (ИТС)

ОСНОВНЫЕ МЕРОПРИЯТИЯ В СООТВЕТСТВИИ С 187-ФЗ

01

Категорирование объектов КИИ

Присвоение категории в соответствии со значимостью объекта.

02

Обеспечение безопасности объекта КИИ

Мероприятия по обеспечению безопасности КИИ и размещение на территории объекта КИИ ТЗКИ.

03

Противодействие компьютерным атакам

Взаимосвязь с ГосСОПКА, размещение на территории объекта КИИ ТЗИ ГосСОПКА .

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЪЕКТА КИИ

Обеспечение безопасности на всех стадиях жизненного цикла объекта

Создание, Эксплуатация, Вывод из Эксплуатации

Меры по обеспечению безопасности

Анализ угроз безопасности, Проектирование подсистемы безопасности, разработка документации, внедрение, анализ угроз безопасности для системы безопасности

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»

Задачи обеспечения безопасности

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

ОБЪЕКТЫ ЗАЩИТЫ АСУ

infotecs

В соответствии с Приказом ФСТЭК №239 от 25.12.2017 г.

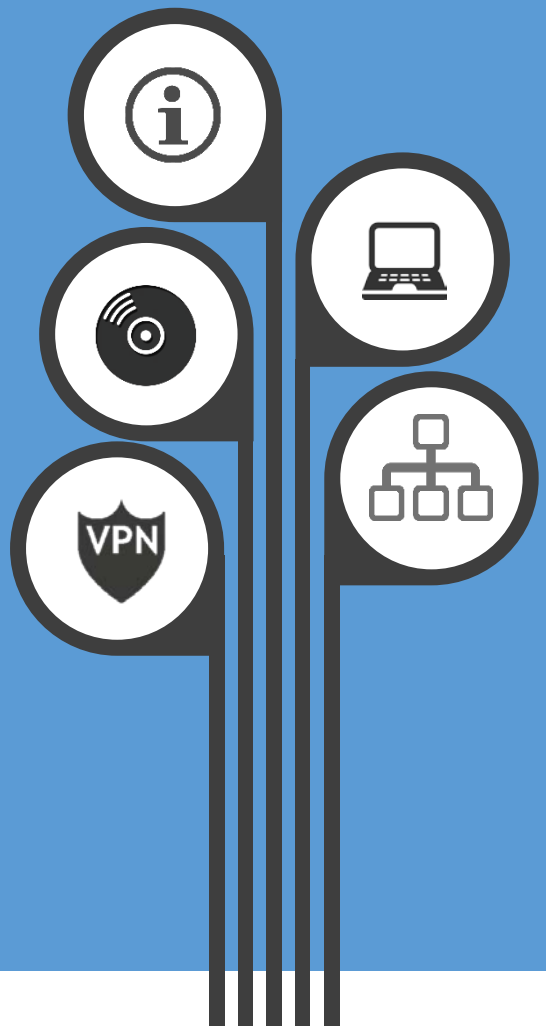
Информация о параметрах и объекта и процесса

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

Программные средства

Микропрограммное, общесистемное, прикладное программное обеспечение.

Средства защиты информации



Программно-аппаратные средства

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

Архитектура и конфигурация АСУ

ОСОБЕННОСТИ ПО МЕРАМ ЗАЩИТЫ

В соответствии с Приказом ФСТЭК №239 от 25.12.2017 г.

Гарантийная и техническая поддержка

Обязательна для программных и программно-аппаратных средств

Базовый набор мер

Организационные и технические меры с учетом угроз безопасности и категории значимости

Компенсирующие меры

При отсутствии возможности реализации отдельных мер

Применяемые СЗИ

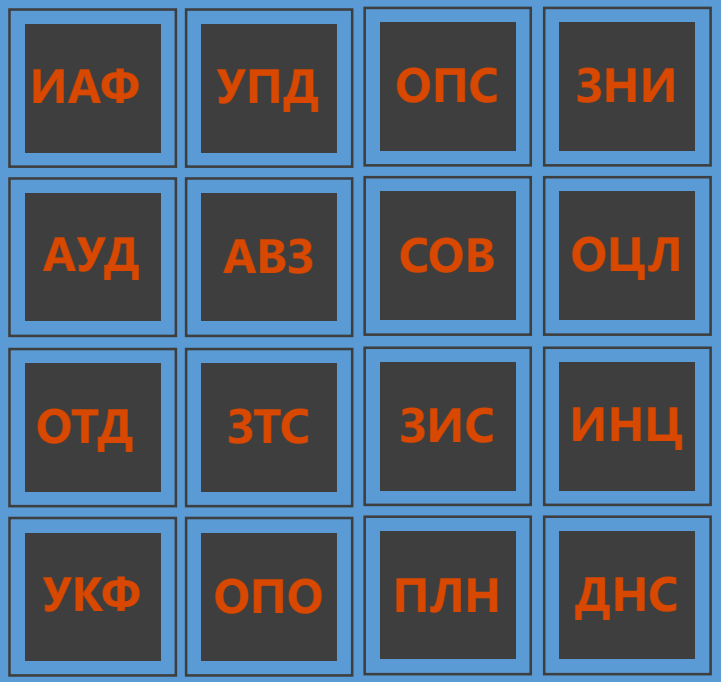
Сертифицированные или прошедшие оценку соответствия по требованиям безопасности

Запрет на сценарии

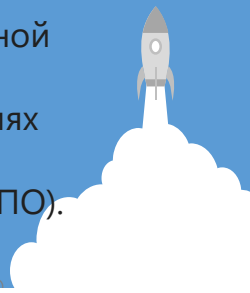
Удаленное и локальное обновление и управление со стороны лиц, не явл. работниками субъекта; Передача информации вендорам без контроля

СОСТАВ МЕР

В соответствии с Приказом ФСТЭК №239 от 25.12.2017 г.

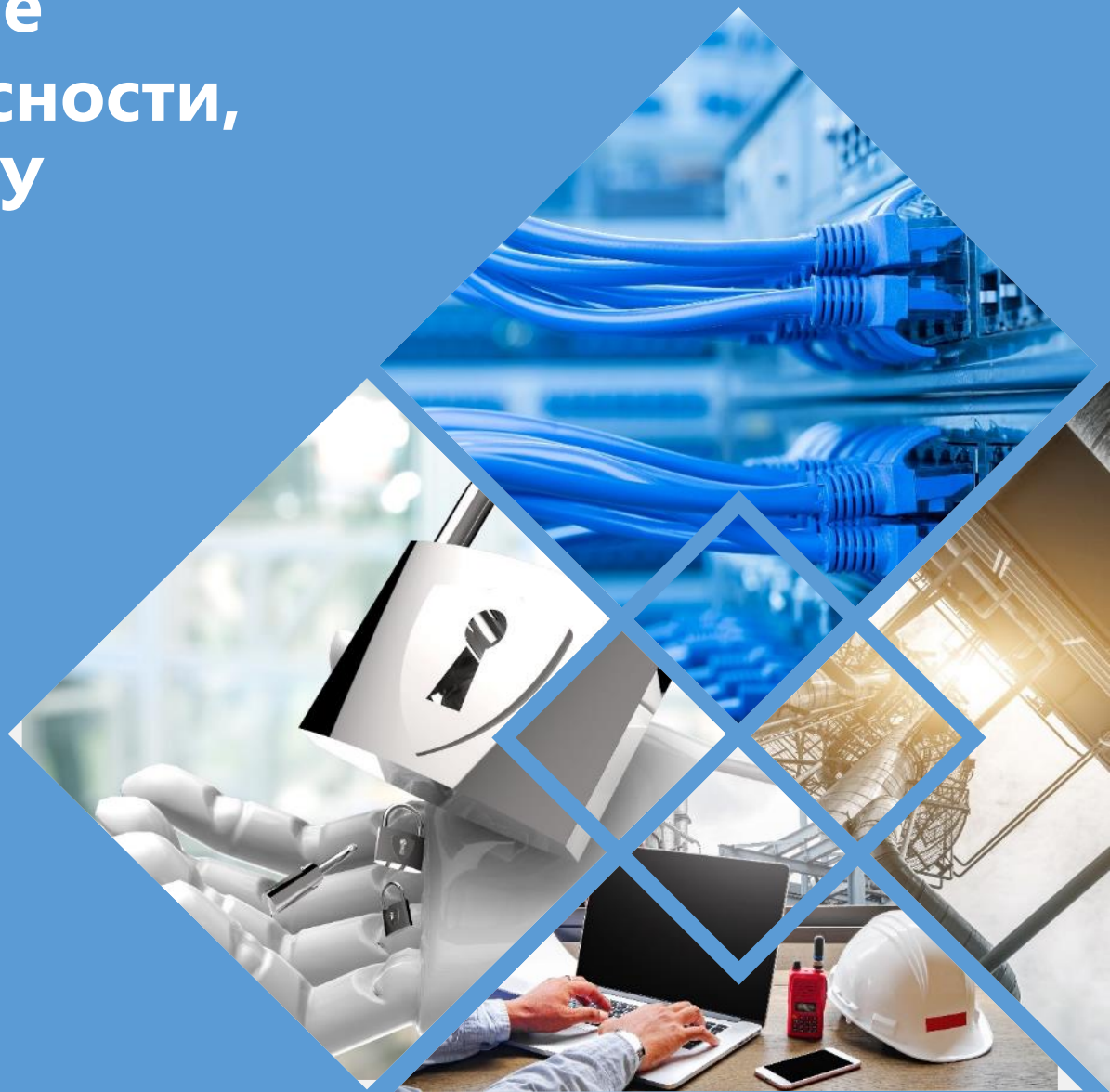


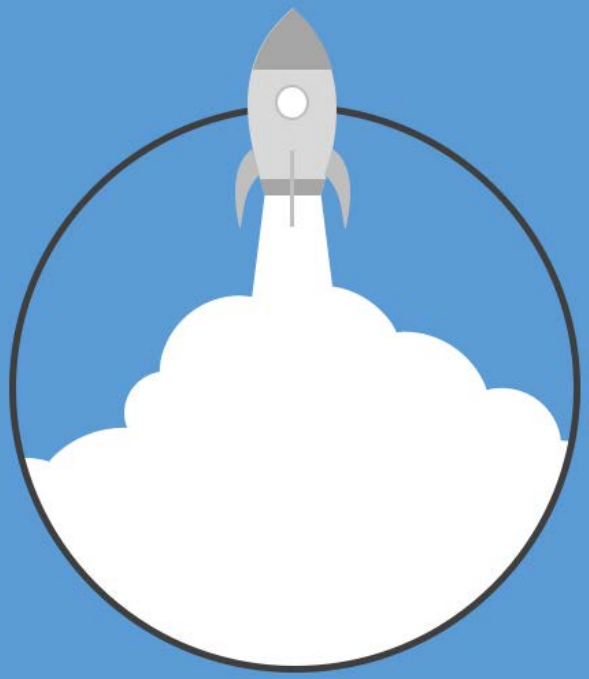
- идентификация и аутентификация (ИАФ);
- управление доступом (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации (ЗНИ);
- аудит безопасности (АУД);
- антивирусная защита (АВЗ);
- предотвращение вторжений (компьютерных атак) (СОВ);
- обеспечение целостности (ОЦЛ);
- обеспечение 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).



Промышленные шлюзы безопасности, как СЗИ для АСУ КИИ

- предотвращают неправомерный доступ к информации,
- не допускают воздействия на программные и программно-аппаратные средства,
- обеспечивают функционирования объекта в условиях воздействия угроз безопасности,
- защищают конфигурацию АСУ при удаленном конфигурировании

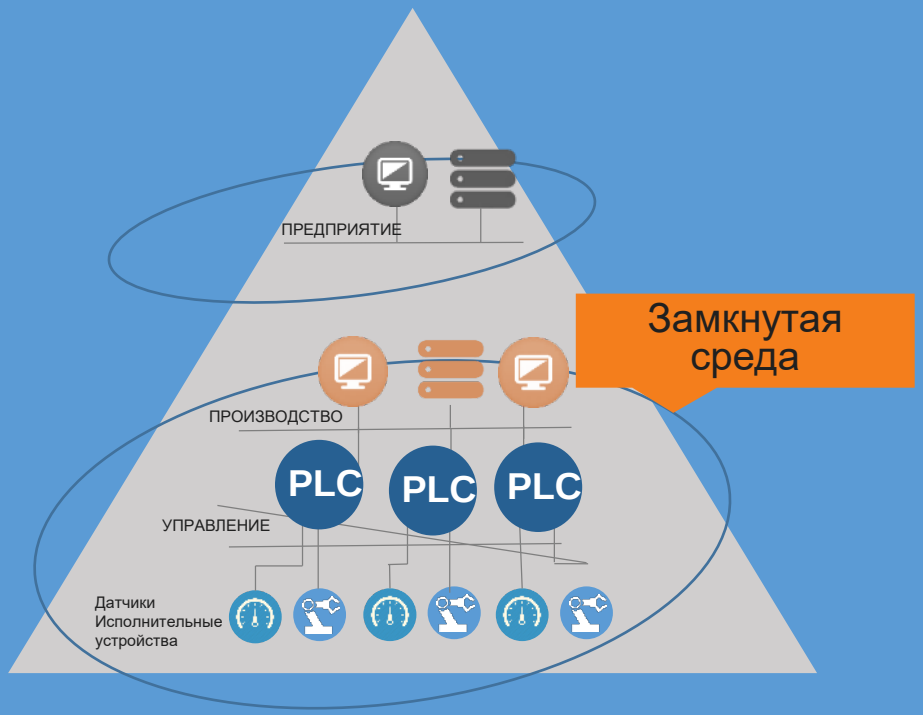




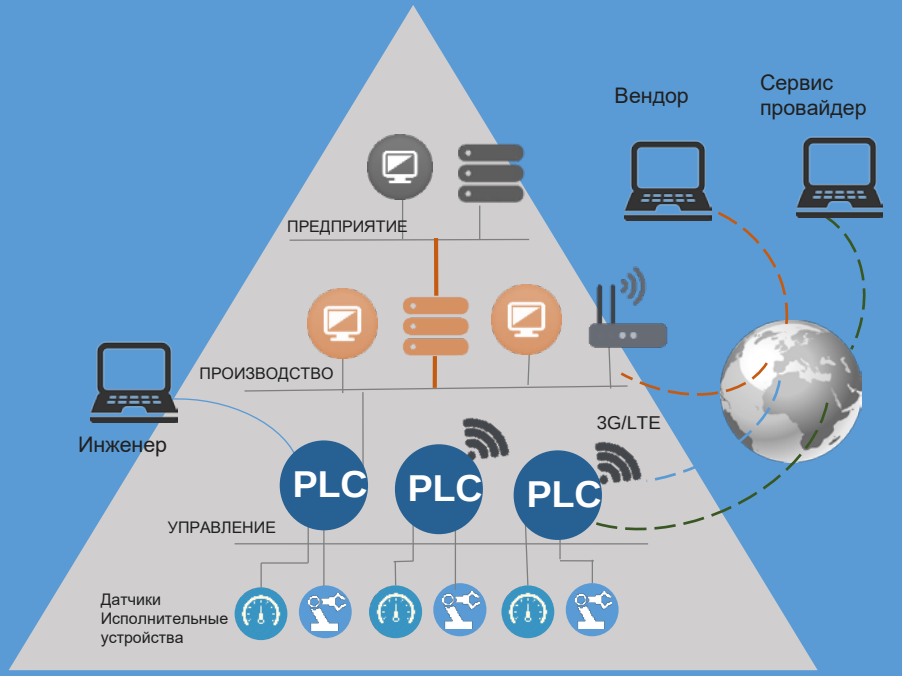
Требования к промышленным шлюзам безопасности

В части применения в Автоматизированных систем управления

СОВРЕМЕННЫЕ АСУ



КЛАССИЧЕСКАЯ АСУ



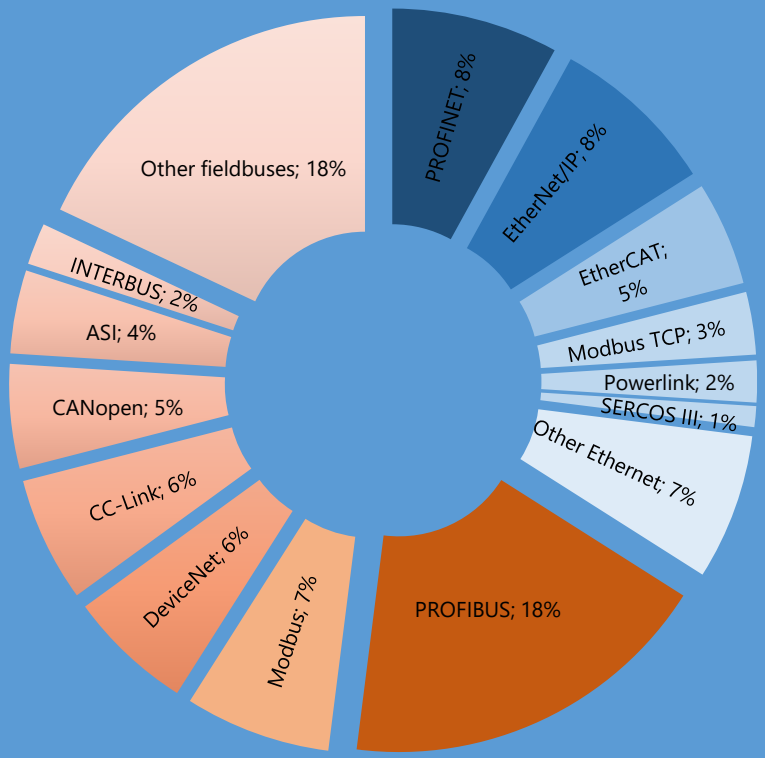
СОВРЕМЕННАЯ АСУ

СОВРЕМЕННЫЕ ПРОМЫШЛЕННЫЕ СЕТИ

2015 год

Fieldbus: 66%
Annual growth: 7%

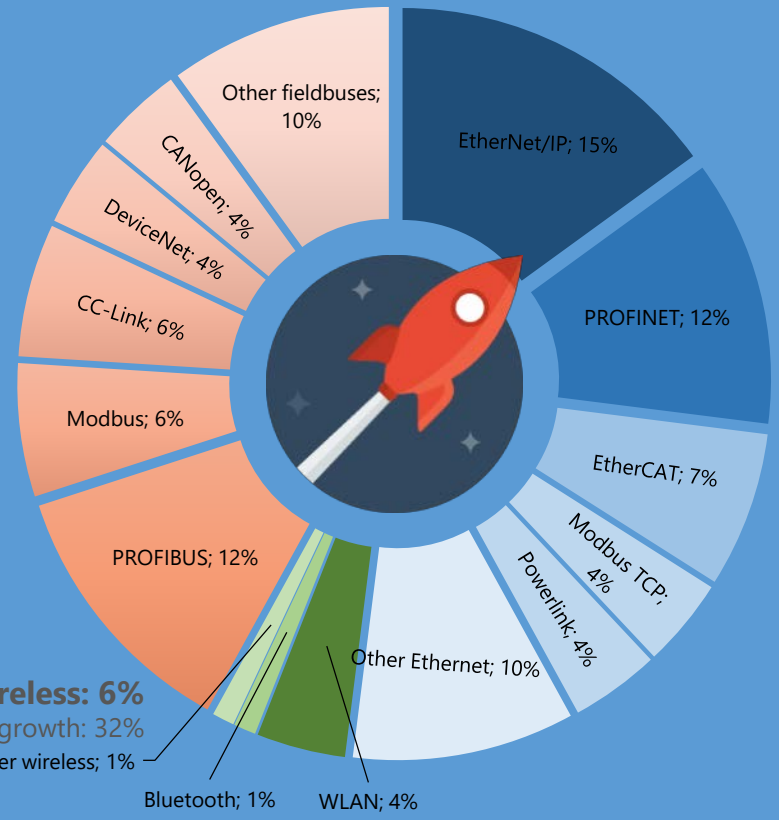
Industrial Ethernet: 34%
Annual growth: 17%



2018 год

Fieldbus: 42%
Annual growth: 6%

Industrial Ethernet: 52%
Annual growth: 22%



Wireless: 6%
Annual growth: 32%

Source: HSM Industrial Networks

INDUSTRIAL ETHERNET

infotecs

Основные характеристики

OSI Model	Web/ IT	Industrial Ethernet			Fieldbus	
ПРИКЛАДНОЙ УРОВЕНЬ	HTTP, DHCP, DNS	Modbus TCP, Ethernet/IP, Powerlink, DNP3, OPC DA, IEC 104 Real time		Profinet, EtherCAT, SERCOS III, GOOSE, SV	Modbus RTU, Profibus, CanOpen, DeviceNet, IEC 101/103	
ТРАНСПОРТНЫЙ УРОВЕНЬ	TCP, UDP	TCP/UDP	Real time	TCP/UDP	Транспортный уровень	Не используется
СЕТЕВОЙ УРОВЕНЬ	IPv6, IPv4	IPv4/IPv6		IP	Сетевой уровень	
КАНАЛЬНЫЙ/ ФИЗИЧЕСКИЙ УРОВЕНЬ	Ethernet (IEEE 802.3), DSL, ISDN, Wireless LAN, IEEE 802.11, Wi-Fi	Ethernet (IEEE 802.3), Wireless LAN, IEEE 802.11, Wi-Fi		Ethernet (IEEE 802.3)	RS-232/422/485, CAN, ASi	
	Тысячи байт	**Сотни байт**		**Десятки байт**	**Десятки байт**	

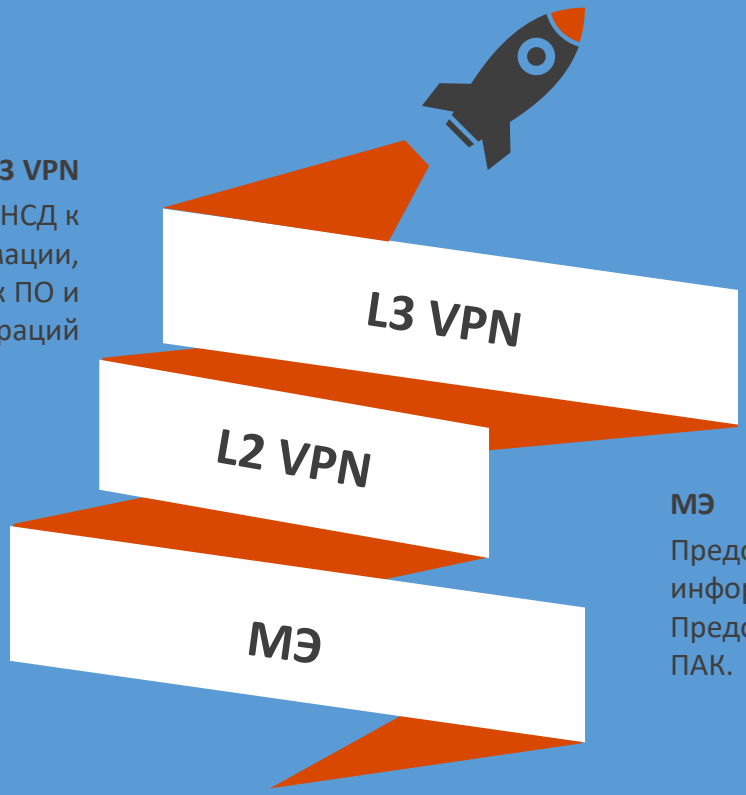
ЗАЩИТА ПРОМЫШЛЕННЫХ СЕТЕЙ

infotecs

Каким образом защищать промышленные сети?

L3 VPN

Предотвращение НСД к информации, Предотвращение доступа к ПО и ПАК, защита конфигураций



L2 VPN

Предотвращение НСД к информации, Предотвращение доступа к ПО и ПАК.

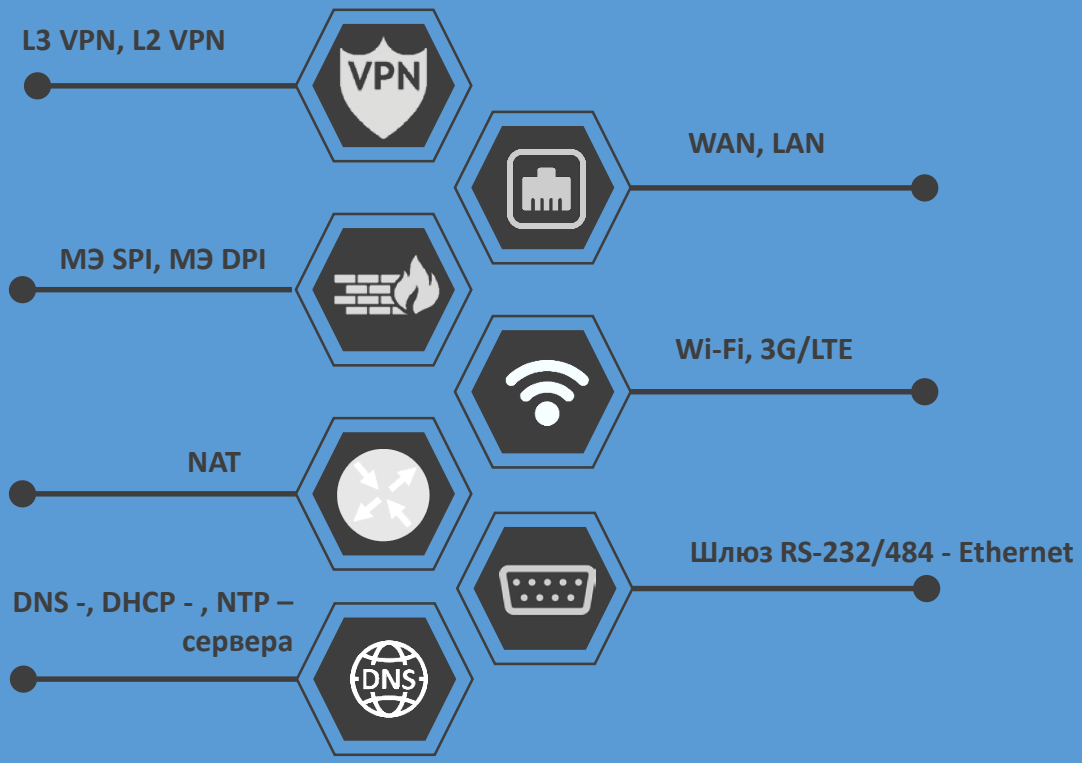
МЭ

Предотвращение НСД к информации, Предотвращение доступа к ПО и ПАК.

ПРОМЫШЛЕННЫЙ ШЛЮЗ БЕЗОПАСНОСТИ

infotecs

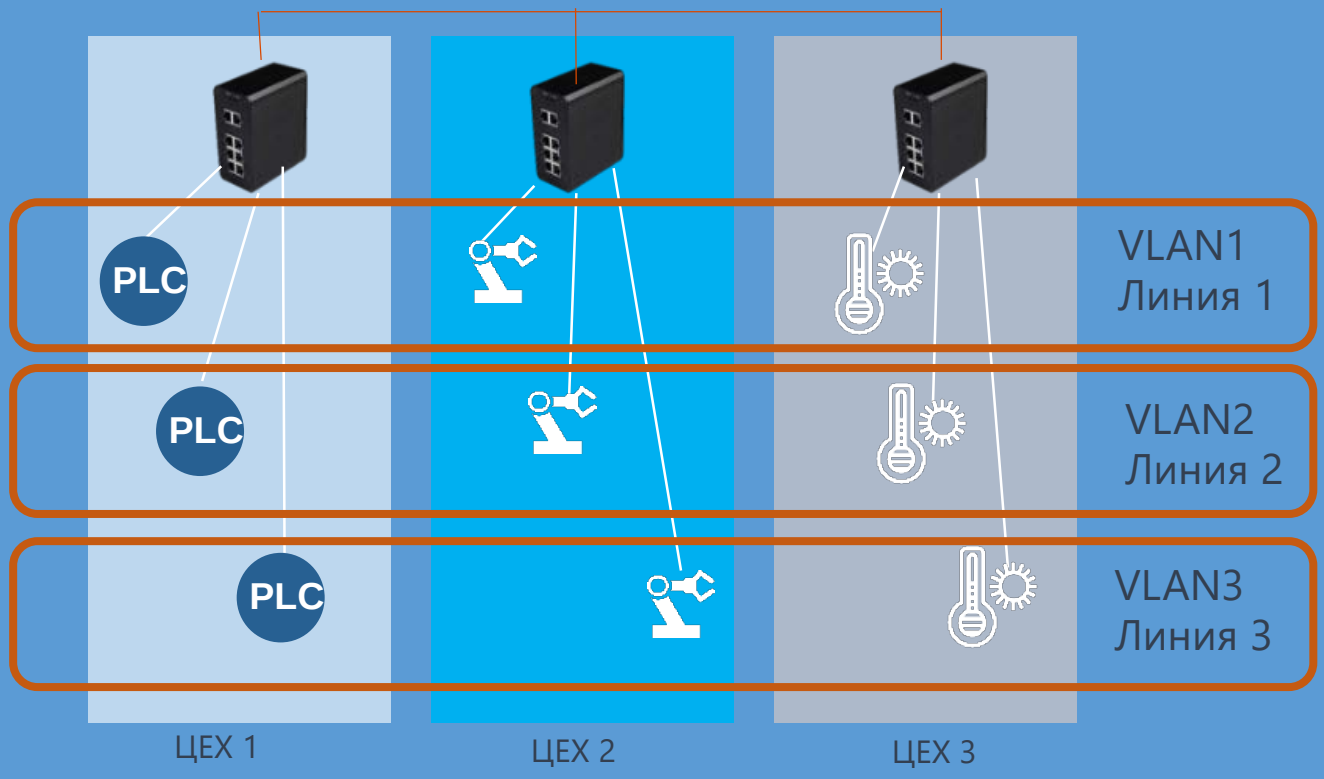
Какими должен быть основной функционал?



ПРОМЫШЛЕННЫЙ ШЛЮЗ БЕЗОПАСНОСТИ

infotecs

Какими должен быть основной функционал?



ПРОМЫШЛЕННЫЙ ШЛЮЗ БЕЗОПАСНОСТИ

Какими должен быть основной функционал?

Приоритезация real-time траффика за счет QoS (Quality of Service)

КОНФИГУРИРОВАНИЕ
High Priority

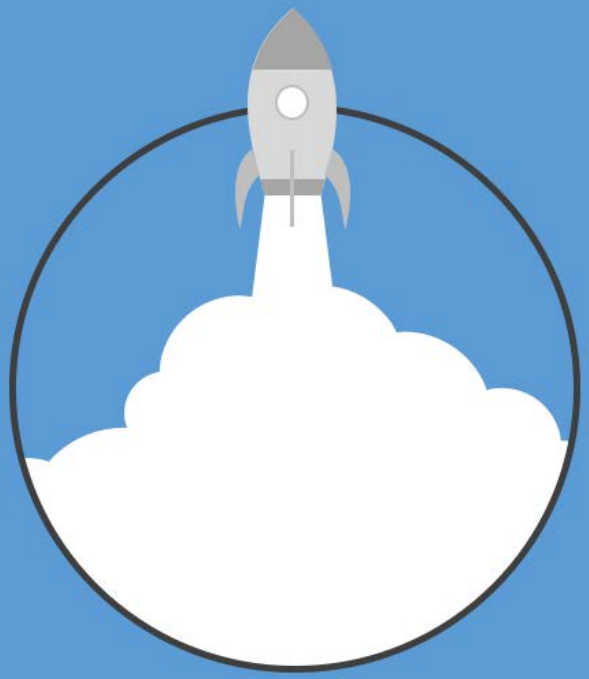
КОМАНДЫ
Top Priority

МОНИТОРИНГ
Low Priority

infotecs

ПРОМЫШЛЕННЫЙ ШЛЮЗ БЕЗОПАСНОСТИ

- Резервирование
- Промышленное исполнение
- Надежность



ViPNet Coordinator IG

Первый российский промышленный шлюз безопасности

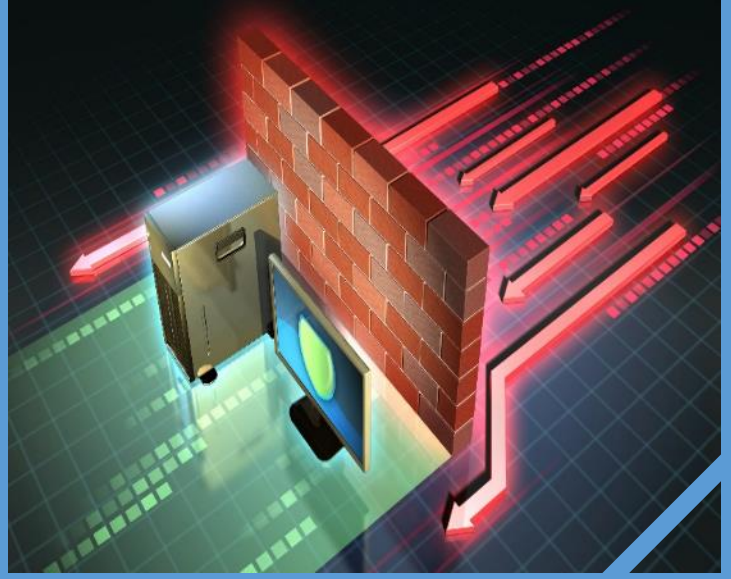
ViPNet Coordinator IG

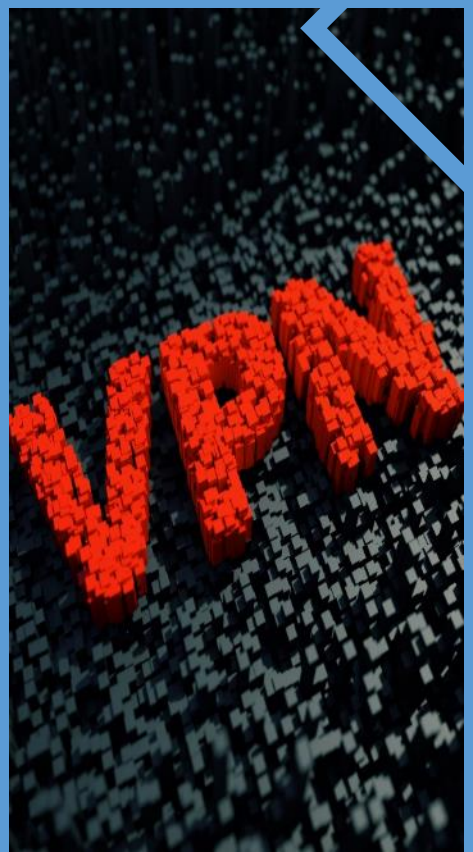
VPN – шлюз
По требованиям к СКЗИ
класса КС3

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

Доверенная платформа
Собственная схемотехника

Импортозамещение
Произведено в России





ViPNet Coordinator IG

infotecs

VPN

Шифрование канала для удаленного подключения

Аутентификация

МЭ типа Д

Защита периметра

Блокирование неавторизованного доступа

Фильтрация пакетов

Сетевые функции

Маршрутизация

Беспроводные сети

Шлюз последовательных интерфейсов

Форм-фактор

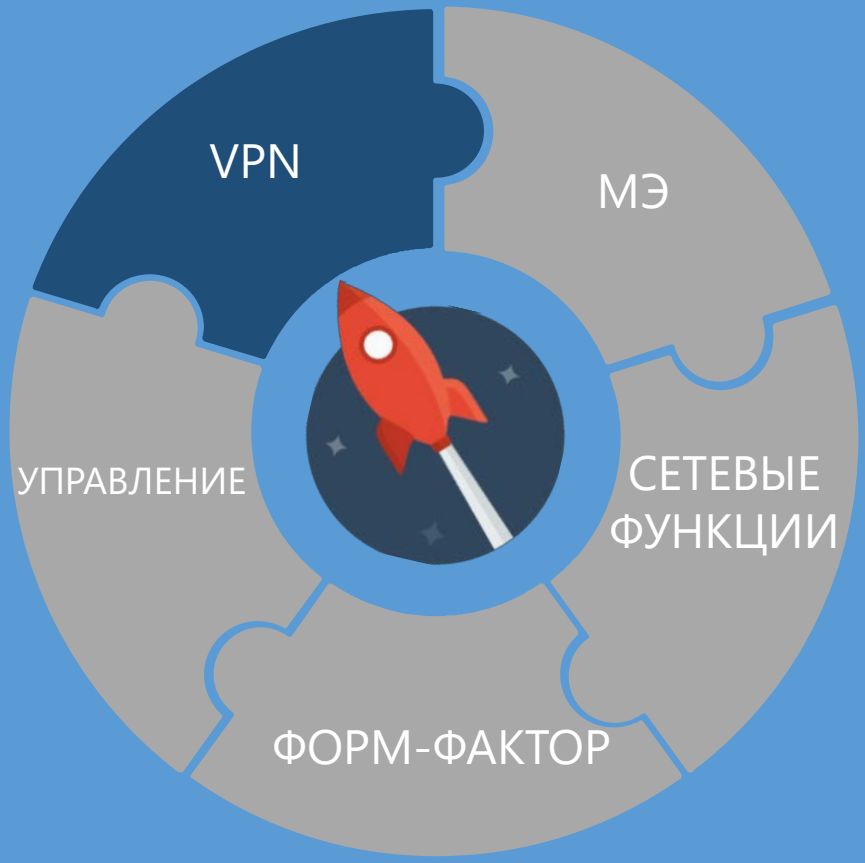
Тяжелые условия эксплуатации

Крепление на din-рейку

ViPNet Coordinator IG

VPN

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

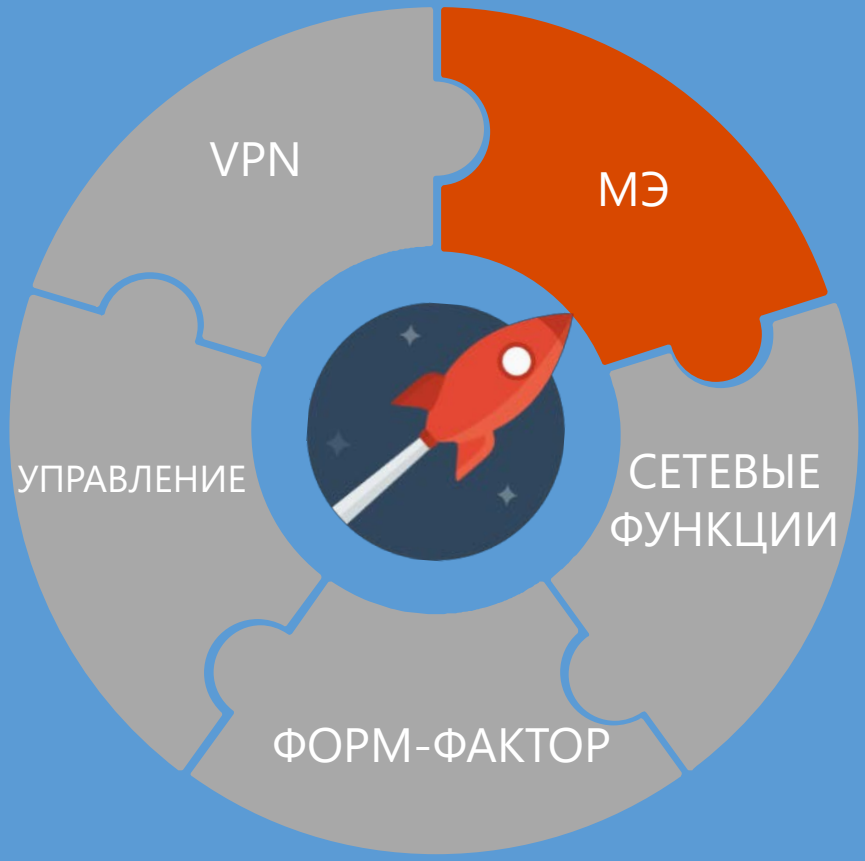


ViPNet Coordinator IG

infotecs

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, LonWorks, bacnet
- DPI для Modbus TCP/RTU



ViPNet Coordinator IG

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

ViPNet Coordinator IG

ФОРМ-ФАКТОР

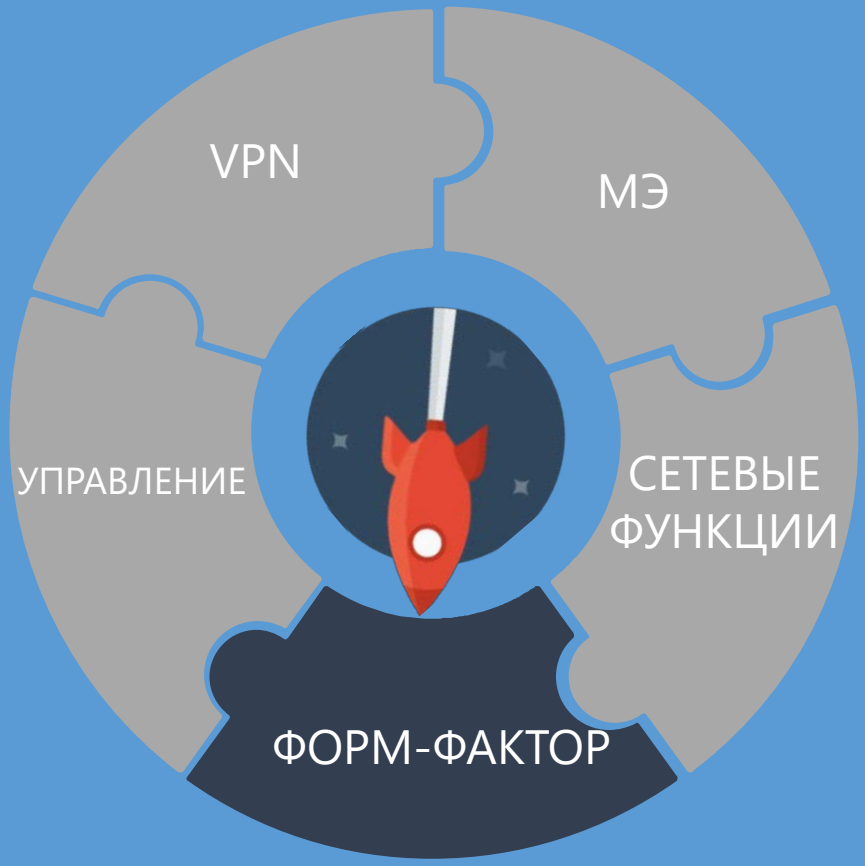
ARM-платформа

Безвентиляторный дизайн

Рабочая температура: -20^{0}C(-40^{0}C) … +60^{0}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

УПРАВЛЕНИЕ

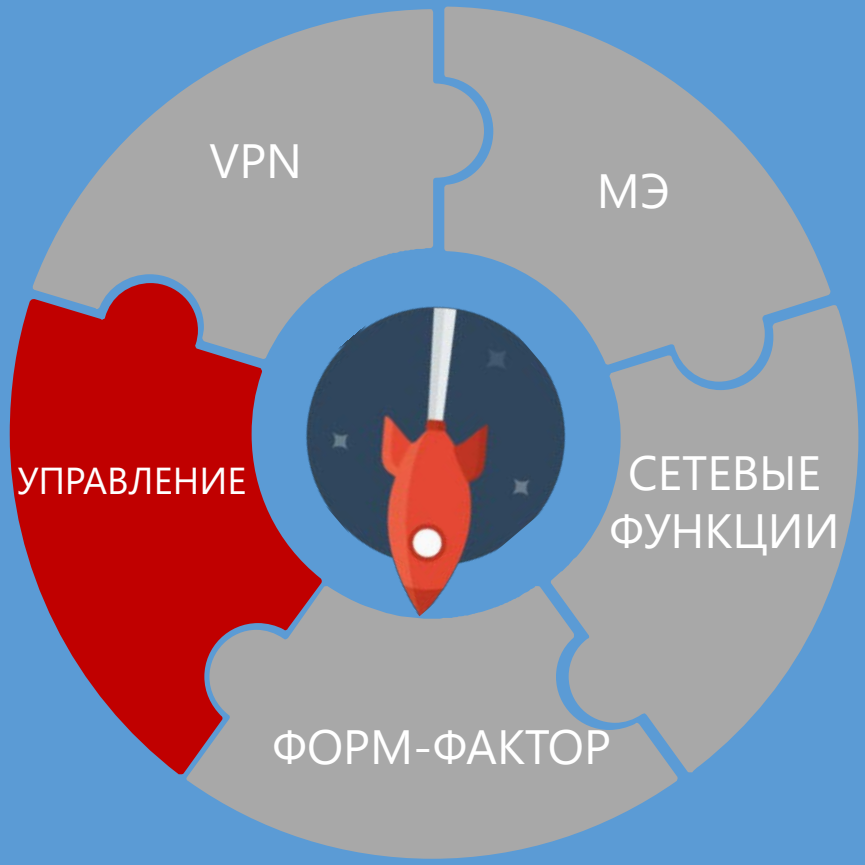
Настройка: Web-интерфейс, консоль, SSH,

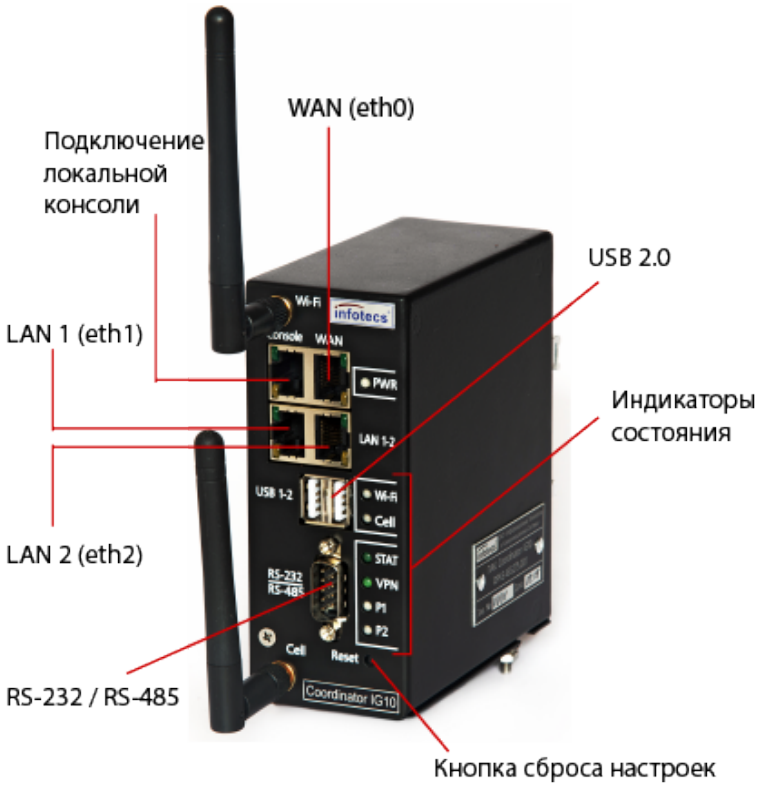
Обновления: локально, ViPNet Administrator

Удаленное управление : ViPNet Administrator, ViPNet Policy Manager

Удаленный мониторинг: ViPNet StateWatcher, SNMP, Syslog

Event log: Firewall Event, System Security Event





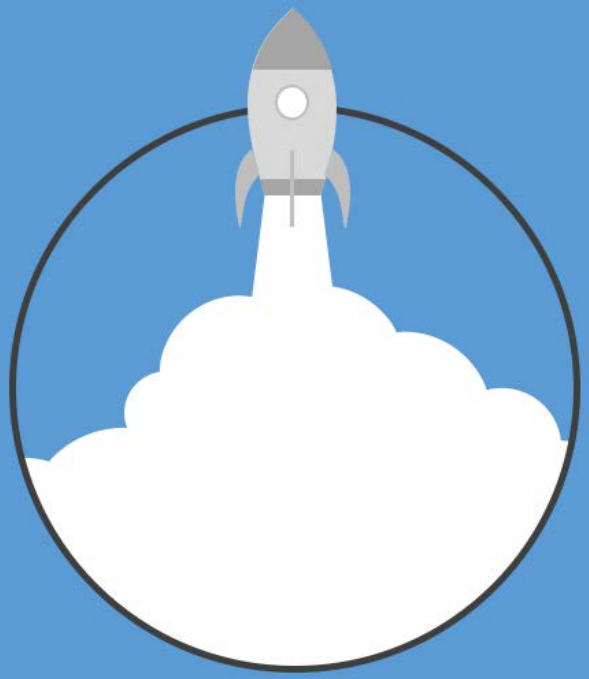
ViPNet Coordinator IG

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

ViPNet Coordinator IG

ИСПОЛНЕНИЯ

- Платформа:
  - ViPNet Coordinator IG10 - Базовое (WAN, LAN)
  - ViPNet Coordinator IG10 + Wi-fi- модуль
  - ViPNet Coordinator IG10 + GSM-модуль
  - ViPNet Coordinator IG10 + Wi-fi- модуль + GSM-модуль
- Поддержка промышленных протоколов:
  - Базовый вариант - Ethernet
  - Промышленный - Ethernet + Serial interface



Основные сценарии использования шлюзов безопасности

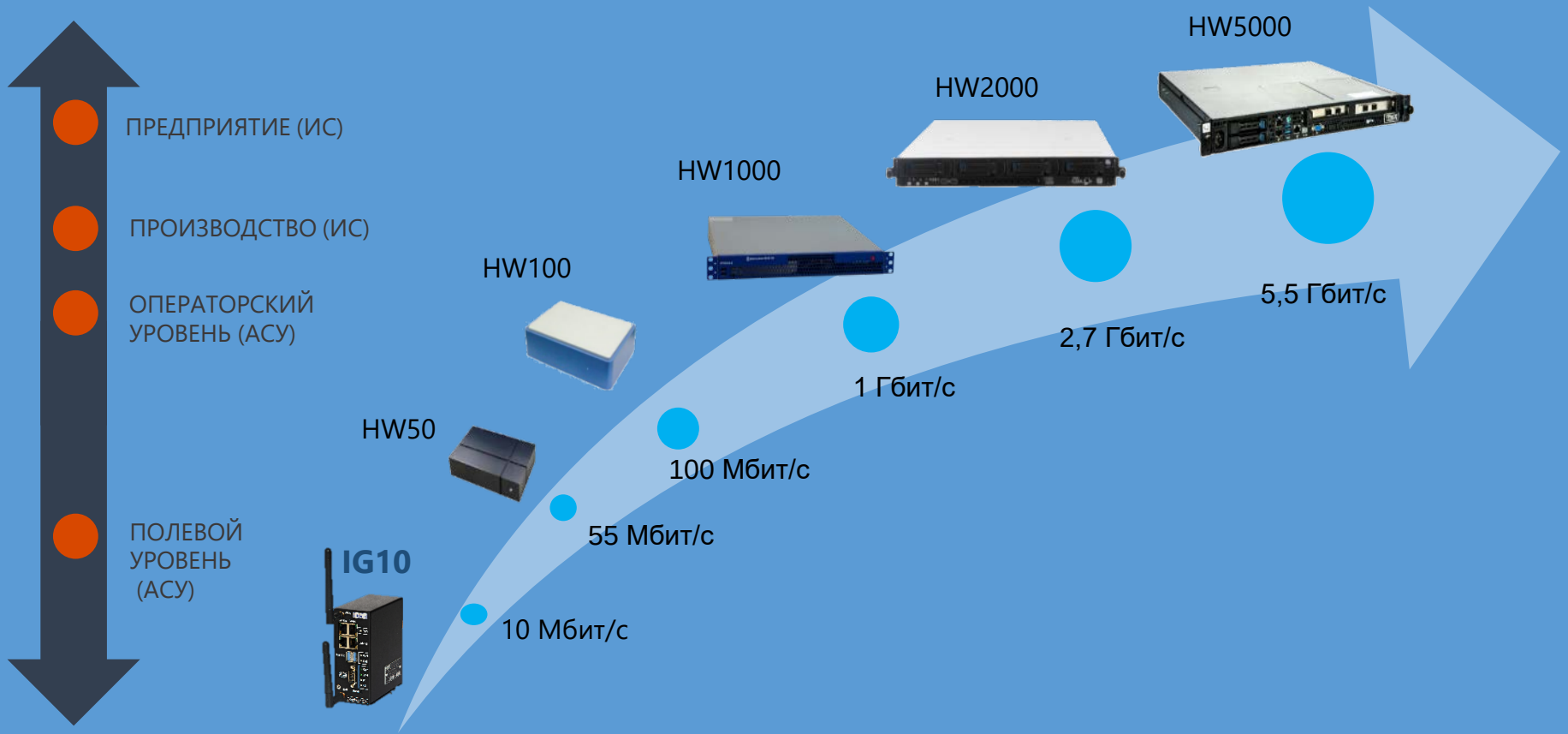
На примере линейки продуктов ViPNet Network Security

ОСНОВНЫЕ СЦЕНАРИИ ЗАЩИТЫ ИНФОРМАЦИИ

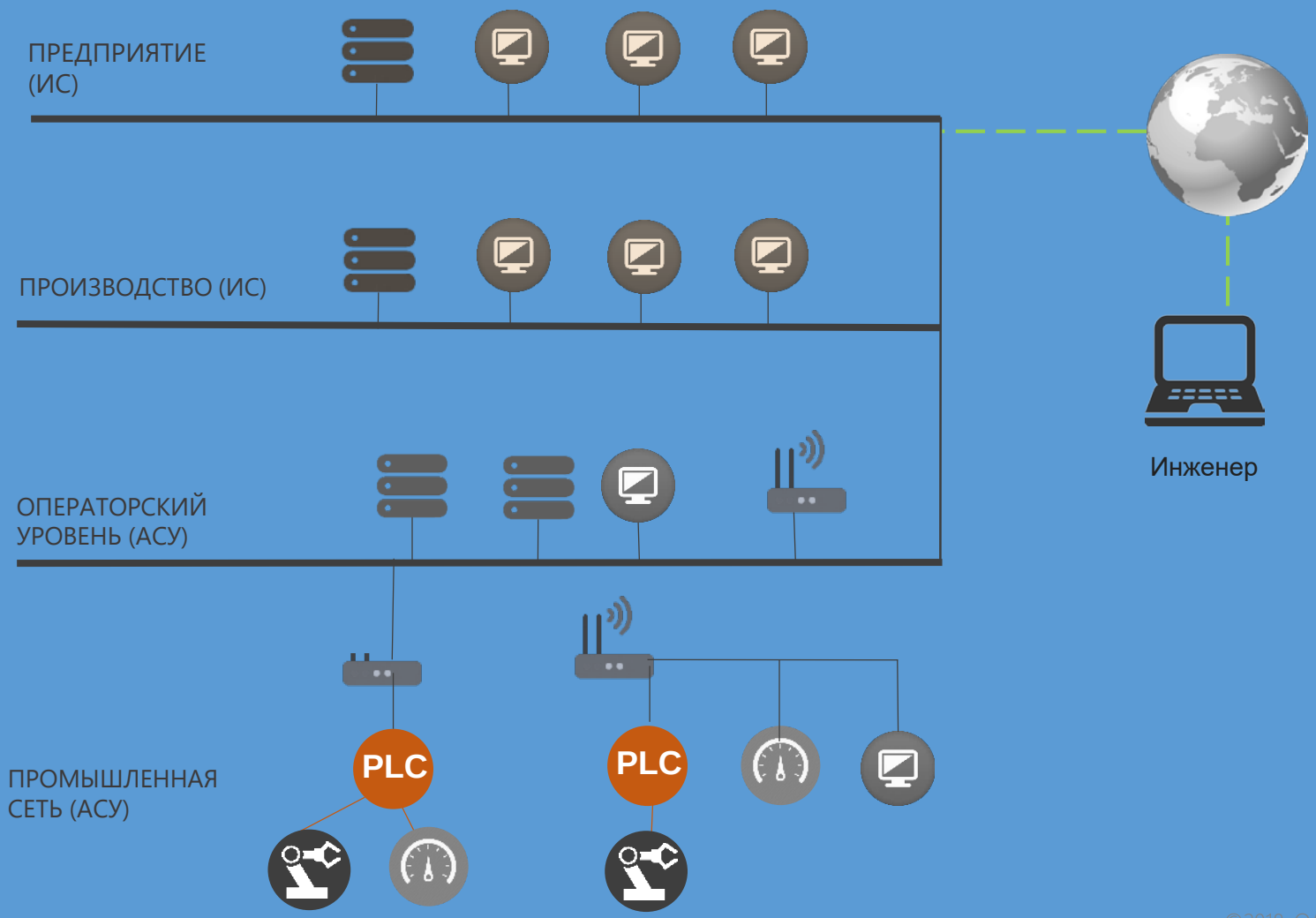
- Защита цифрового периметра промышленной сети
- Сегментация сети и защита доступа к сегменту
- Удаленный защищенный доступ к сегменту и его оборудованию
- Защищенные каналы для беспроводных сетей
- Защищенный канал между сегментами сети, в том числе для распределенных систем
- Защищенный канал для последовательных 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

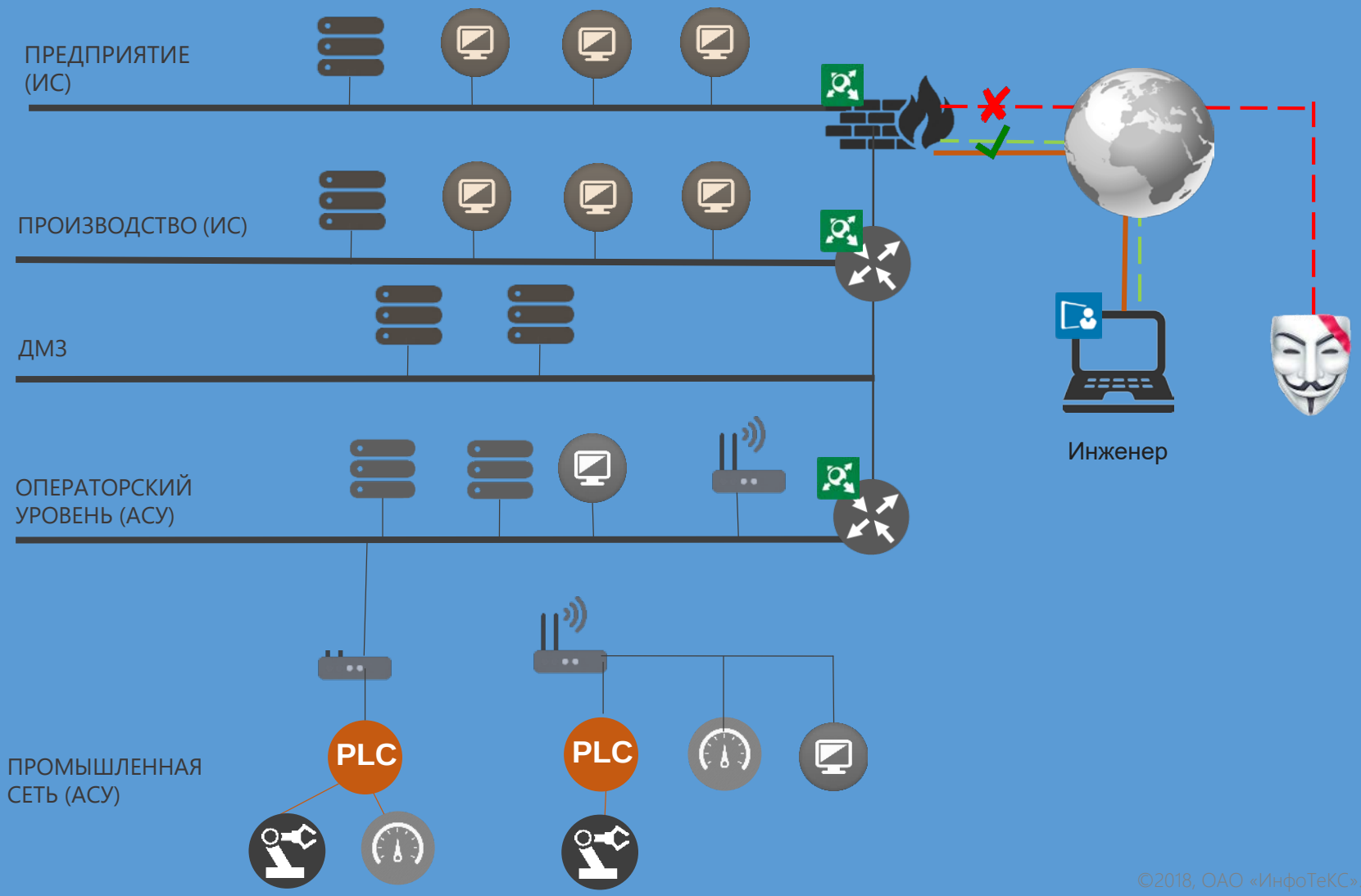
НЕПРЕРЫВНАЯ БЕЗОПАСНОСТЬ ОТ ПОЛЕВОГО УРОВНЯ ДО БИЗНЕС-ПРОЦЕССОВ



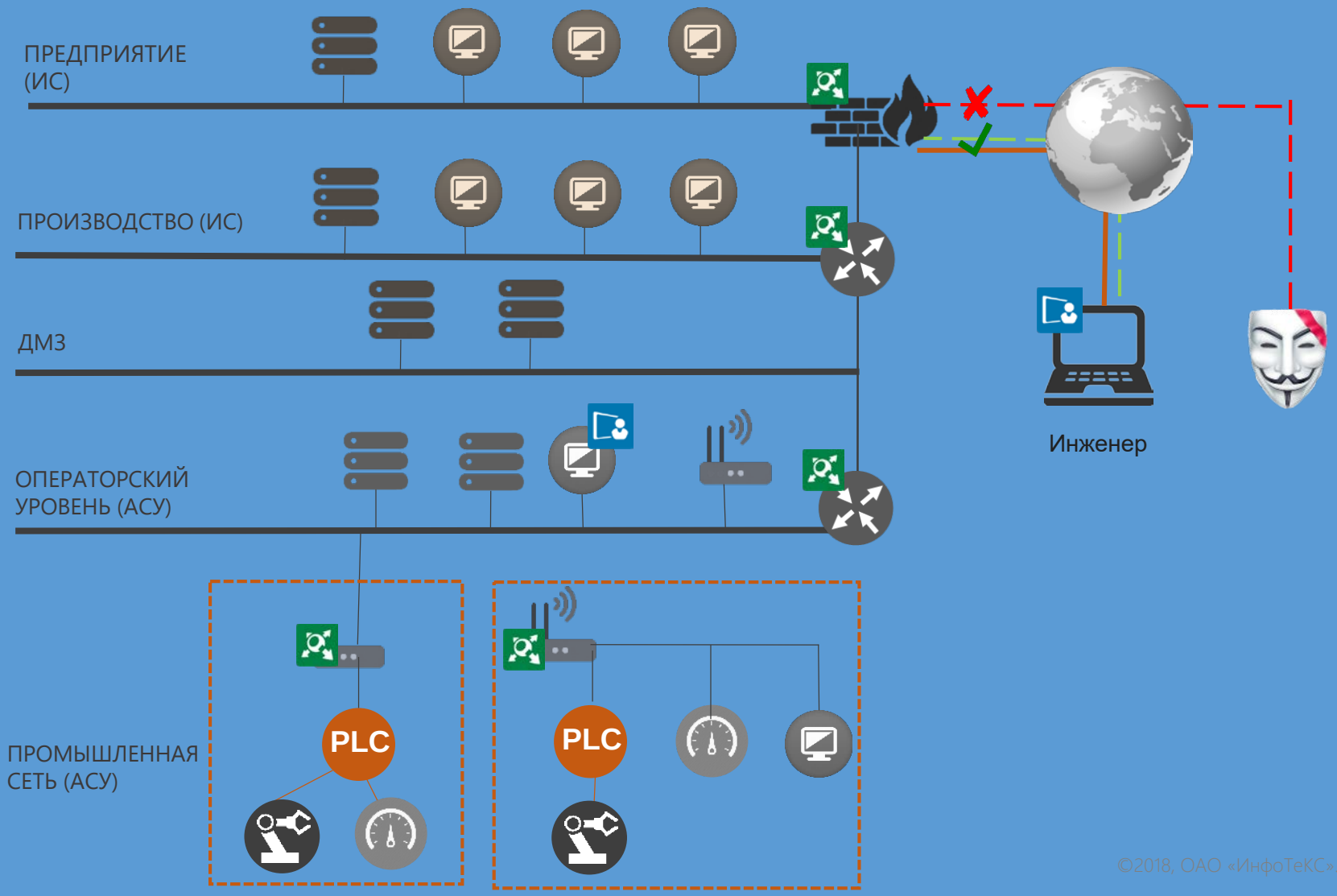
СЦЕНАРИИ ЗАЩИТЫ ИНФОРМАЦИИ



СЦЕНАРИИ ЗАЩИТЫ ИНФОРМАЦИИ

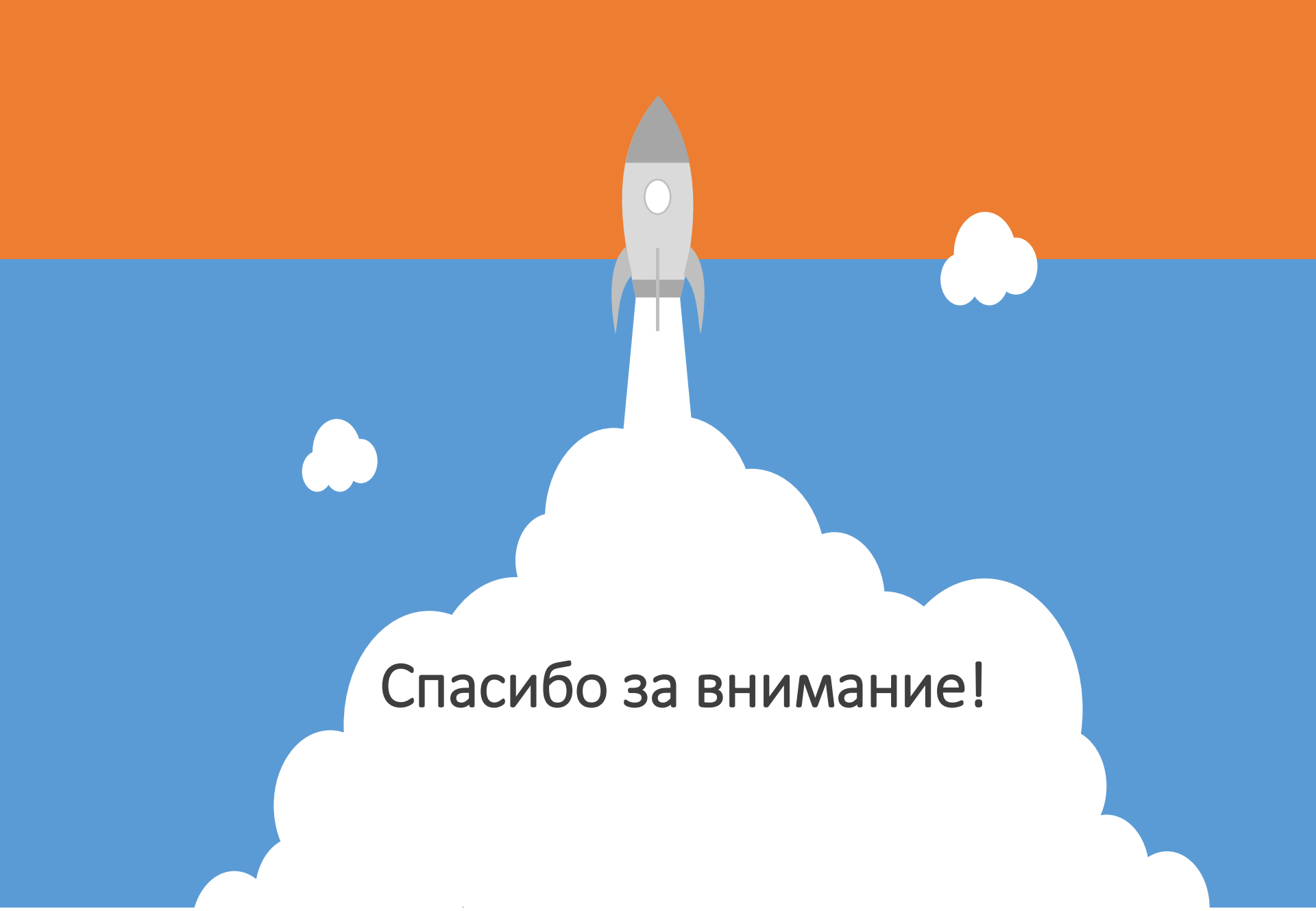


СЦЕНАРИИ ЗАЩИТЫ ИНФОРМАЦИИ



СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕШЕНИЯ NETWORK SECURITY

 ViPNet Administrator	Требования по обеспечению защиты информации в АСУ ТП Приказ ФСТЭК № 31 от 14.03.2014	 ViPNet Coordinato HW/IG	Требования по обеспечению безопасности значимых объектов КИИ Приказ ФСТЭК №239 от 25.12.2017	  ViPNet Client
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


Спасибо за внимание!