Проактивные средства защиты информации для систем РЗА и АСУ ТП

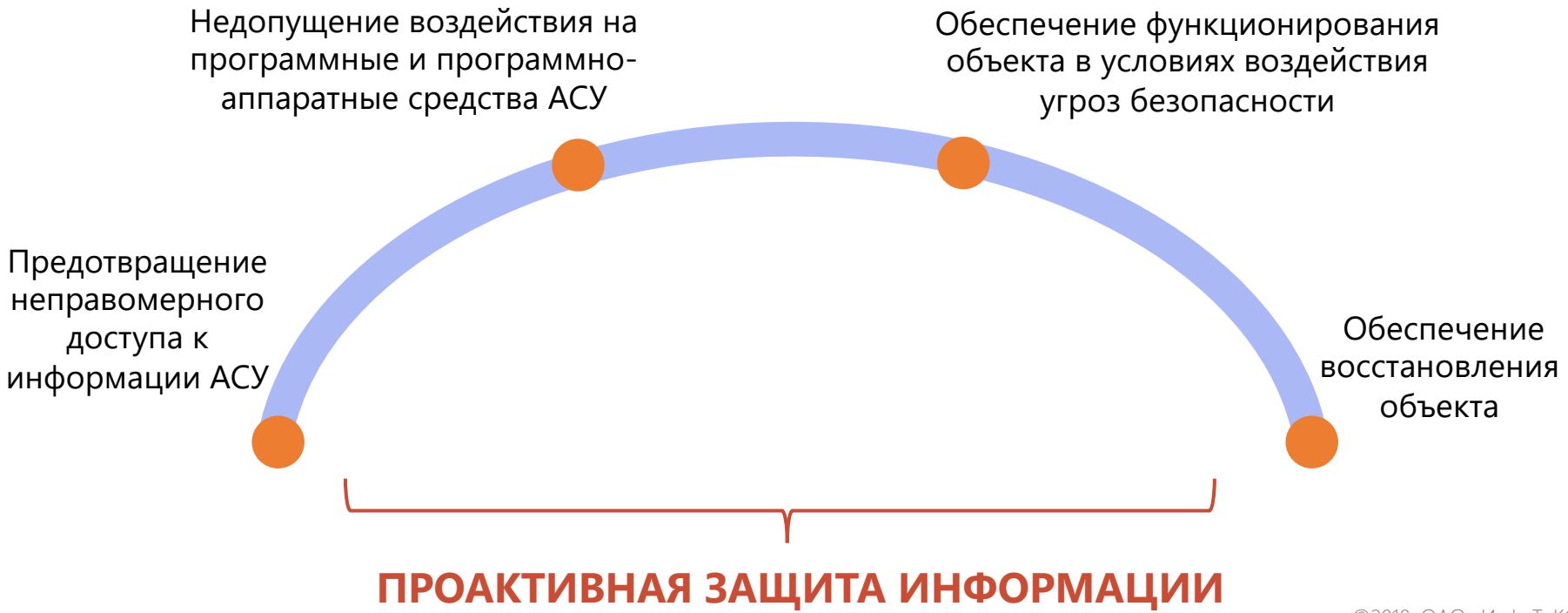
Марина Сорокина,
руководитель направления продуктового развития

Требования по обеспечению безопасности систем РЗА и АСУ ТП

Высокоуровневые требования ИБ

- Федеральный закон №187-ФЗ «О безопасности КИИ»
  - Приказ ФСТЭК России №235 от 21.12.2017 г.
  - Приказ ФСТЭК России №239 от 25.12.2017 г.
- Приказ ФСТЭК России №31 от 14.03.2014 г.

Основные задачи защиты систем РЗА и АСУ ТП



Меры защиты

Меры защиты	Приказ ФСТЭК России №239 от 25.12.17	Приказ ФСТЭК России №31 от 14.03.17	Лучшие практики IEC 62443
Защита периметра системы	ЗИС.2	ЗИС.2	+
Эшелонированная защита	ЗИС.3	ЗИС.3	+
Сегментирование	ЗИС.4	ЗИС.4	+
Организация ДМЗ	ЗИС.5	ЗИС.5	+
Сокрытие архитектуры и конфигурации системы	ЗИС.8	ЗИС.8	
Защита информации при ее передаче по каналам связи	ЗИС.19, ЗИС.32	ЗИС.19, ЗИС.32	+
Защита неизменяемых данных	ЗИС.13	ЗИС.13	

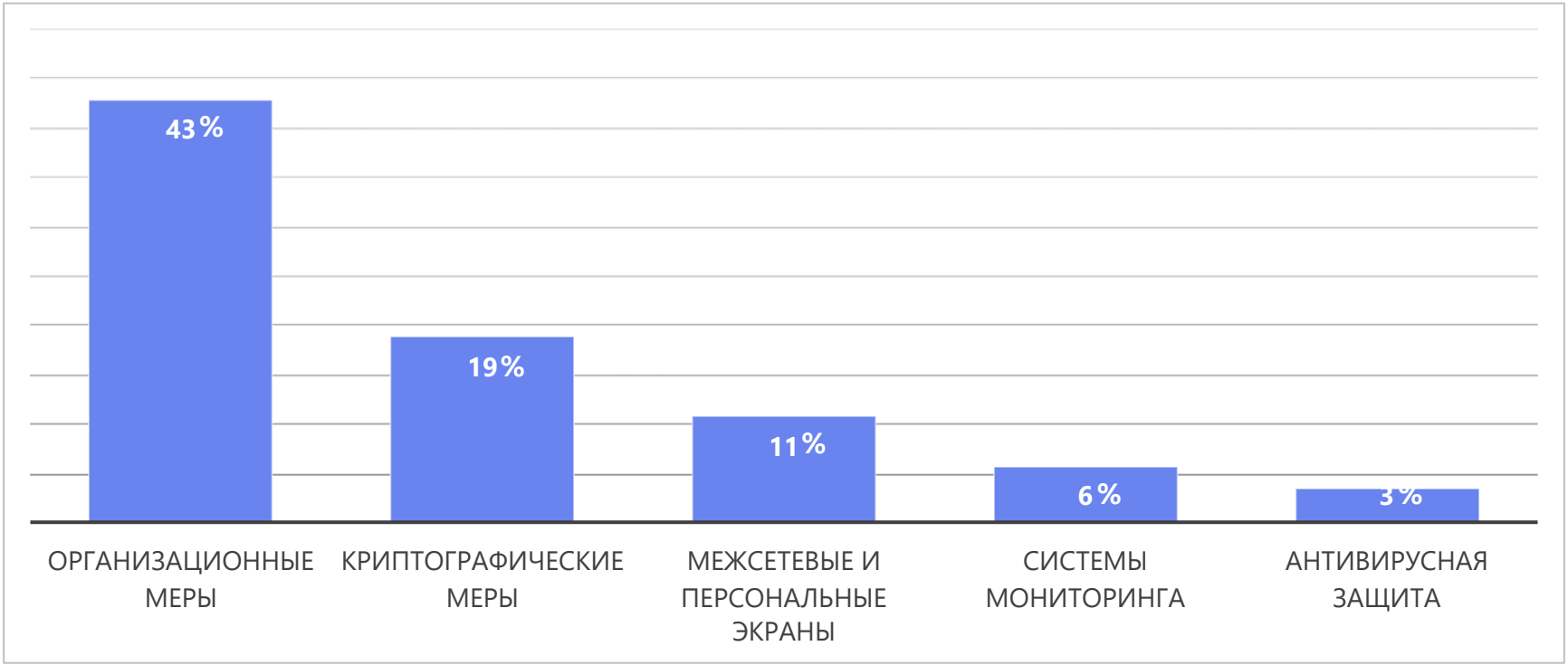
Меры защиты

Меры защиты	Приказ ФСТЭК России №239 от 25.12.17	Приказ ФСТЭК России №31 от 14.03.17	Лучшие практики
Обеспечение доверенных канала, маршрута	ЗИС.20	ЗИС.20	
Управление сетевыми соединениями	ЗИС.35	ЗИС.35	
Идентификация и аутентификация пользователей и устройств	ИАФ.1-ИАФ.6	ИАФ.1-ИАФ.6	+
Управление доступом	УПД.1, УПД.2, УПД.4	УПД.1, УПД.2, УПД.4	+
Доверенная загрузка	УПД.3	УПД.3	+
Реализация защищенного удаленного доступа	УПД.13	УПД.13	+

Меры защиты

Меры защиты	Приказ ФСТЭК России №239 от 25.12.17	Приказ ФСТЭК России №31 от 14.03.17	Лучшие практики
Управление запуском компонентов ПО	ОПС.1	ОПС.1	
Управление установкой компонентов ПО	ОПС.2, УКФ.3	ОПС.2, УКФ.3	+
Реализация антивирусной защиты	АВЗ.1	АВЗ.1	
Обнаружение и предотвращение компьютерных атак	СОВ.1	СОВ.1	
Контроль целостности ПО	ОЦЛ.1	ОЦЛ.1	+
Доверенное обновление	ОПО.1-ОПО.4	ОПО.1-ОПО.4	+

Меры защиты согласно Приказу ФСТЭК №239 от 25.12.2017



Какие объекты АСУ защищать?

Информация о параметрах и объектах процесса АСУ

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

Программные средства АСУ

Микропрограммное, общесистемное, прикладное программное обеспечение.

Программно-аппаратные средства АСУ

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

Средства защиты информации

Архитектура и конфигурация АСУ

Выбор соответствующих мер

Базовый набор мер

Меры должны быть выбраны с учетом угроз безопасности и значимости категории

Компенсирующие меры

При отсутствии возможности реализации отдельных мер, можно использовать компенсирующие меры.

Подходы к построению системы безопасности

Построение подсистемы безопасности

НАЛОЖЕННЫЕ СРЕДСТВА

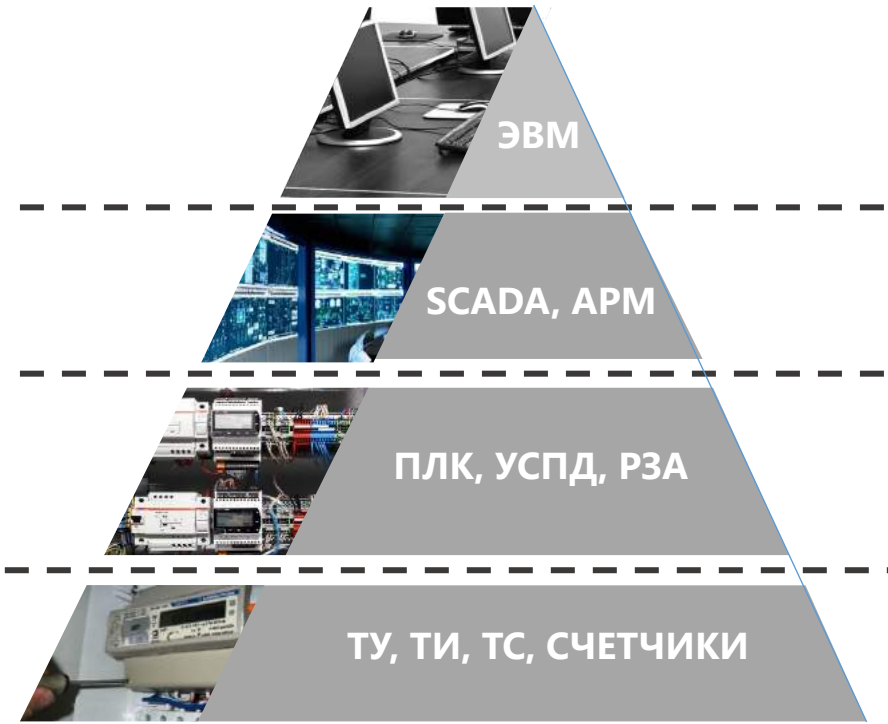
- МЕЖСЕТЕВЫЕ ЭКРАНЫ
- КРИПТОШЛЮЗЫ
- УСТРОЙСТВА АУТЕНТИФИКАЦИИ
- СРЕДСТВА АНТИВИРУСНОЙ ЗАЩИТЫ

SECURE BY DESIGN

- ВСТРАИВАЕМЫЕ СРЕДСТВА (ЗАКОНЧЕННЫЕ СЗИ)
- БИБЛИОТЕКИ
- СОБСТВЕННАЯ РАЗРАБОТКА

ПРОДУКТЫ ИНФОТЕКС для ЗАЩИТЫ АСУ

ViPNet Industrial Security



ViPNet Coordinator HW

ViPNet Client

ViPNet Coordinator IG

ViPNet SIES

ViPNet SIES Core

ViPNet SIES Unit

Сетевые средства

Встраиваемые средства

ViPNet Coordinator IG

Основные сценарии применения

ViPNet Coordinator IG10

ViPNet Coordinator IG100

- Защита периметра автоматизированной системы (ЗИС.2)
- Сегментирование автоматизированной системы (ЗИС.4)
- Организация ДМЗ со стороны автоматизированной системы (ЗИС.5)
- Удаленный защищенный доступ к сегменту и его оборудованию
- Организация защищенных каналов, в том числе и для беспроводных сетей (ЗИС.19, ЗИС.20, ЗИС.32)
- Защищенный канал для последовательных сетей (ЗИС.19, ЗИС.20)
- Телеуправление и телеконтроль - защищенный удаленный мониторинг и управление (ЗИС.28, ЗИС.29)
- Телесервис – удаленное сервисное обслуживание
- Удаленный защищенный доступ с мобильных устройств для конфигурирования и обслуживания устройств внутри защищенного сегмента (ЗИС.38)

ViPNet Coordinator IG на стендах РЭЛАВЭКСПО

ViPNet Coordinator IG

ViPNet Coordinator IG

VPN

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

МЕЖСЕТЕВОЙ ЭКРАН ТИП Д.4 и А.4

- NAT
- Пакетная фильтрация по IP-адресу источника и назначения (или диапазону IP-адресов), портам и типам протоколов
- Контроль фрагментированных пакетов
- Раздельная фильтрации для открытого трафика и шифруемого трафика
- Поддержка промышленных протоколов: EtherNet/IP, Modbus TCP, PROFINET, DNP, IEC 60870-5-104, MMS, OPC, LonWorks, bacnet
- DPI для Modbus TCP/RTU
- Штатный, режим обслуживания АСУ, аварийный режимы для МЭ типа Д

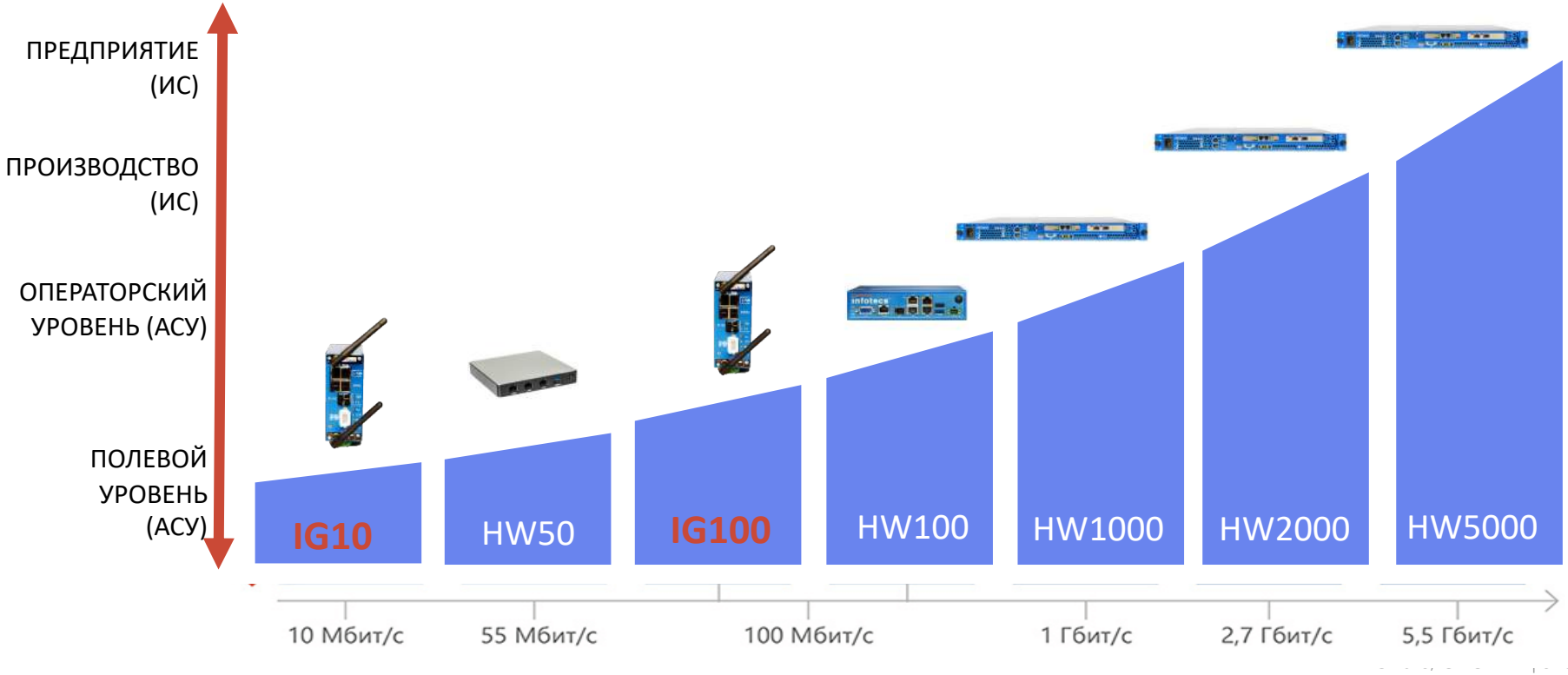
СЕТЕВЫЕ ФУНКЦИИ

- Статическая и динамическая маршрутизация
- DNS-сервер, DHCP-сервер, DHCP-relay
- VLAN, QoS, EtherChanel
- NTP-сервер
- WAN: 1xRJ45 10/100 Мбит/с
- LAN: 2xRJ45 10/100 Мбит/с
- Wi-Fi: IEEE 802.11 b/g, беспроводной клиент, внешняя антенна
- UMTS/HSPA, GSM/GPRS/EDGE
- Шлюза Modbus TCP - Modbus RTU
- Дискретные выводы 2xGPIO

ФОРМ-ФАКТОР

- ARM-платформа
- Безвентиляторный дизайн
- Рабочая температура: -20^0C(-40^0C) … $+60^0$C
- IP30 + бокс IP65
- Напряжение питания: 12…24 В DC
- Крепление на din-рейку
- 50x120x120 мм, 0.6 кг
- ЭМС: ГОСТ 51318.22/CISPR22, ГОСТ CISPR 24
- Собственная схемотехника

Непрерывная безопасность от АСУ до ИС



Единые средства эксплуатации для продуктов линейки

- Удаленное управление :ViPNet Administrator
- Удаленное обновления: ViPNet Administrator

- Удаленное управление политиками: ViPNet Policy Manager

- Удаленный мониторинг: ViPNet StateWatcher

Встраиваемые средства для защиты информации АСУ на примере решения SIES

Решение ViPNet SIES

УПРАВЛЕНИЕ
ПАК ViPNet SIES MC
ПО ViPNet SIES WorkStation

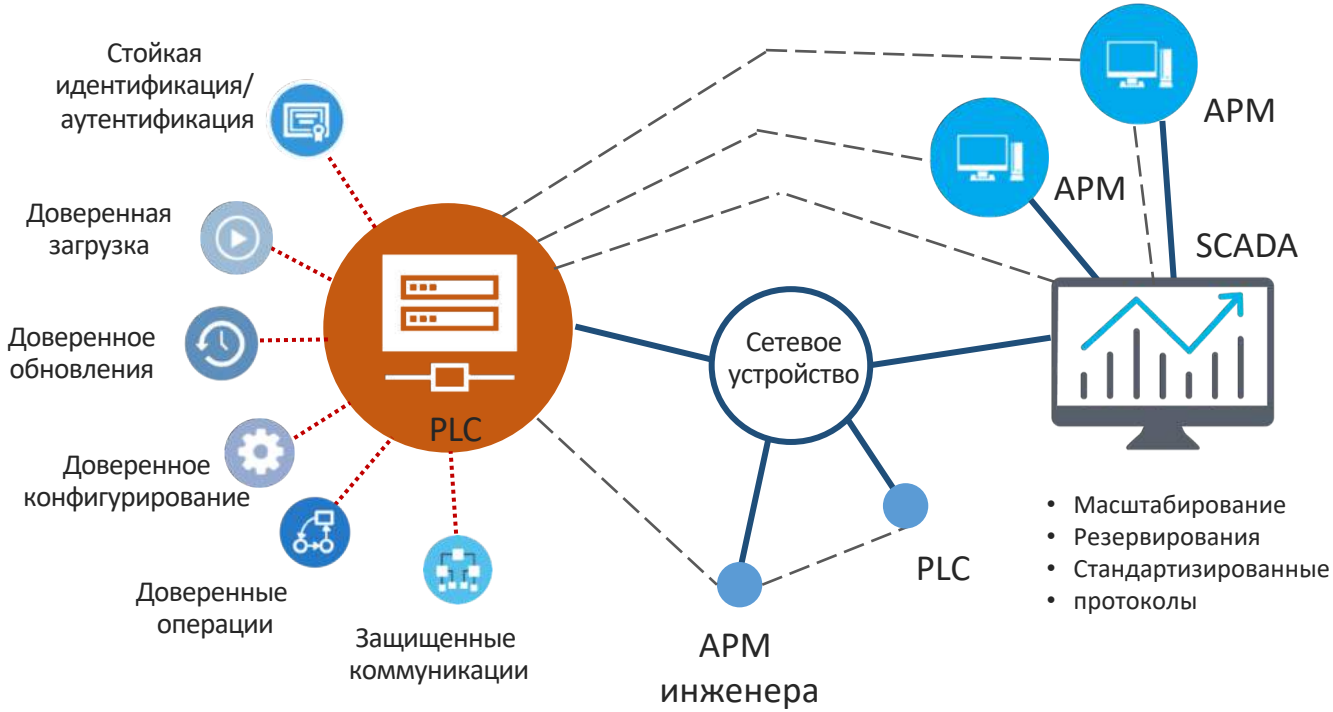
ОПЕРАТОРСКИЙ УРОВЕНЬ
ПО ViPNet SIES Unit

ПОЛЕВОЙ УРОВЕНЬ
ПАК ViPNet SIES Core

Решение ViPNet SIES

- Функционально законченное СКЗИ, соответствующее классам КС1, КС3
- Интеграция по интерфейсам UART, USB для ПАК и по Web API для ПО
- Доступ к криптографическим функциям по SIES API и SIES Core SDK
- Поддержка промышленных протоколов
- Пассивное устройство, выполняет функции защиты по вызову ППО
- Шифрование, имитозащита, усиленная неквалифицированная ЭП (ГОСТ)
- Индустриальное исполнение (-40^0... +75^{0}C)

End-to-end решение



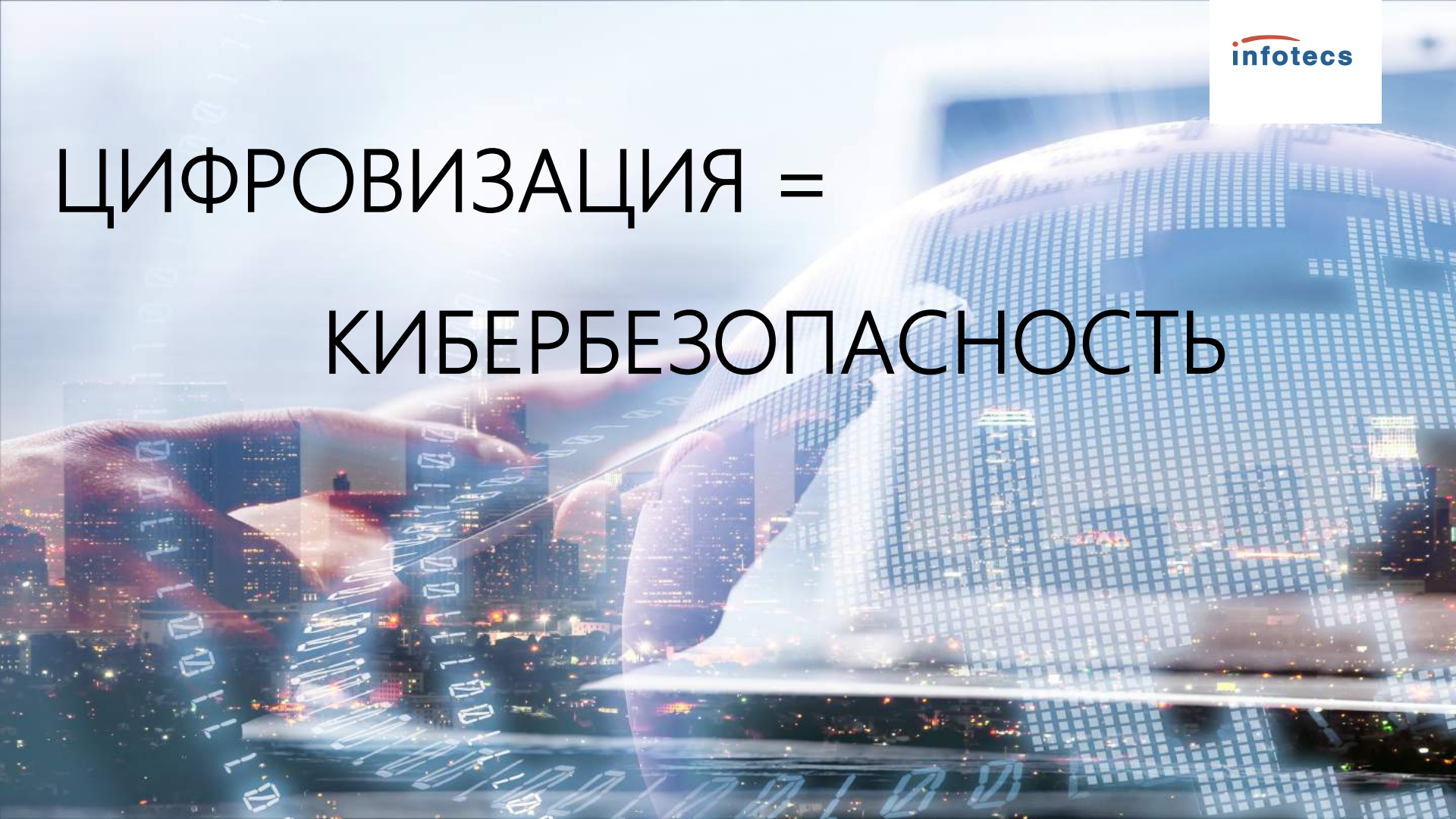
Прикладные криптографические операции

- Зашифрование и расшифрование данных в CMS контейнере с использованием X.509 сертификатов по ГОСТ 28147-89
- Создание и проверка усиленной неквалифицированной в CMS по ГОСТ 34.10.2012
- Зашифрование и расшифрование данных по алгоритму «МАГМА» ГОСТ Р 34.12-2015 (CRISP)
- Вычисление имитовставкии проверка по алгоритму Магма ГОСТ Р.34.12-2015 (CRISP)
- Вычисление значения хэш-кода и проверка по алгоритму ГОСТ Р 34.11-2012

Cryptographic Industrial Security Protocol

CRISP - протокол защищенной передачи данных для индустриальных систем, M2M и IoT/IIoT коммуникаций

- Предраспределённые симметричные ключи
- Аутентификация источника сообщений (у абонентов общий секретный ключ)
- Поддержка адресных (один к одному) сообщений
- Обязательное обеспечение целостности при помощи имитовставки
- Обеспечение конфиденциальности при помощи блочного шифра
- Защита от навязывания повторных сообщений
- Малый размер вспомогательных данных – 10 байт + имитовставка


infotecs
ЦИФРОВИЗАЦИЯ =
КИБЕРБЕЗОПАСНОСТЬ

Спасибо !

Marina.Sorokina@infotecs.ru