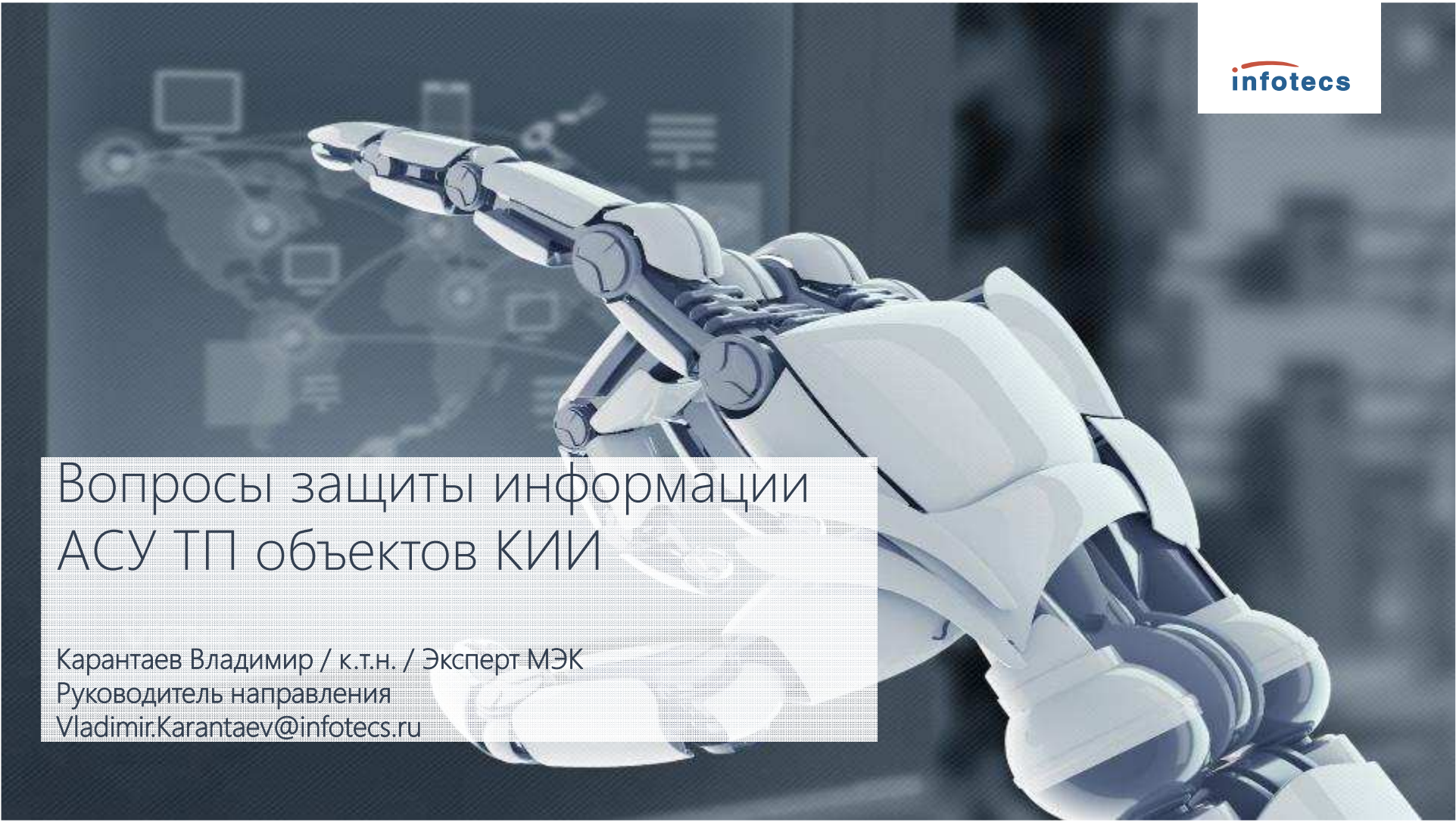


The background of the slide features a close-up of a white and blue robotic arm pointing towards the left. In the background, there is a faint, glowing network diagram with various nodes and connecting lines, suggesting a digital or technological theme.

Вопросы защиты информации АСУ ТП объектов КИИ

Карантаев Владимир / к.т.н. / Эксперт МЭК
Руководитель направления
Vladimir.Karantaev@infotecs.ru

Регламент



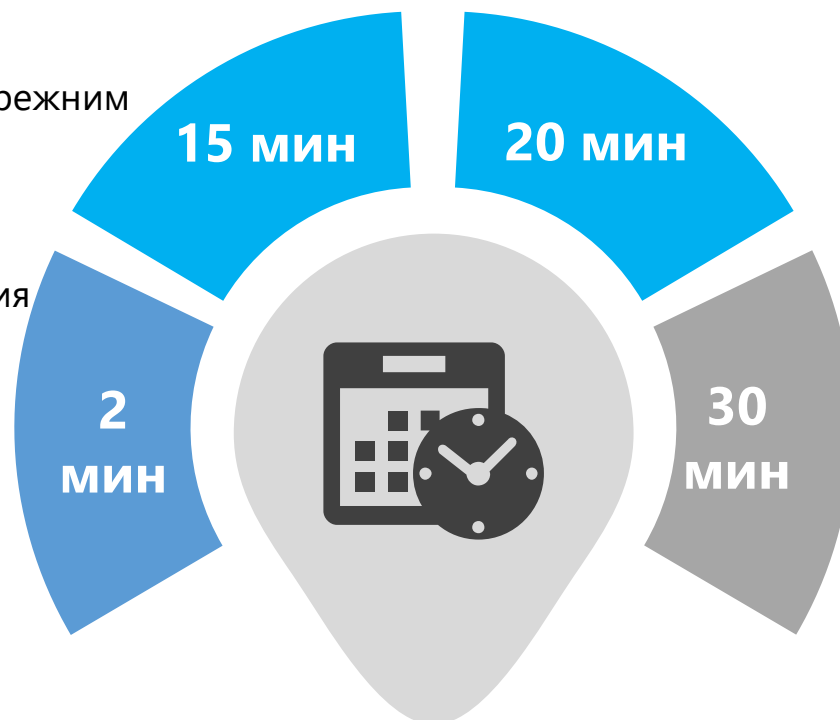
Мир не будет прежним



Тенденции развития



Приветствие



Время реагировать



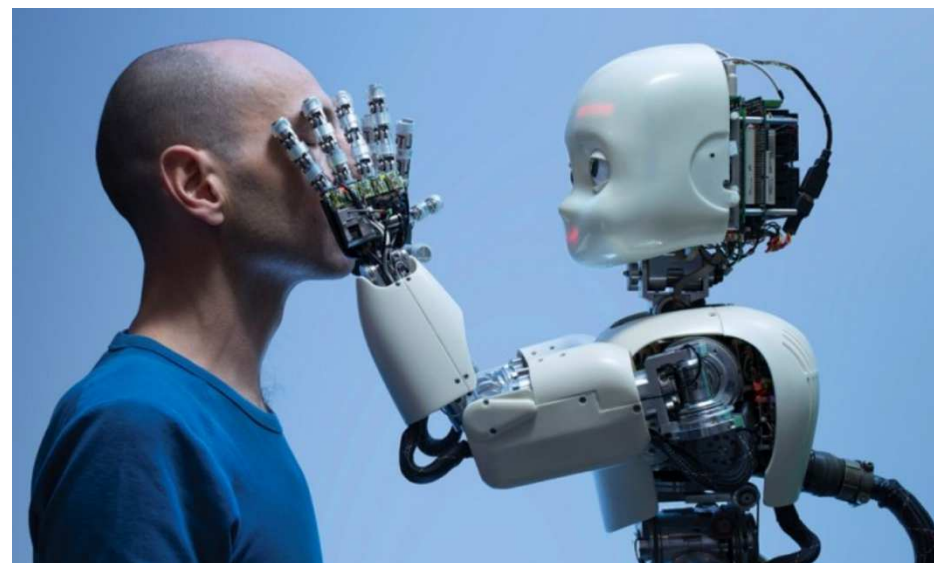
Функциональная и
информационная
безопасность



Ответы на
вопросы
Комментарии

КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ

1. Робот не может причинить вред человеку или своим бездействием допустить, чтобы человеку был причинён вред.
2. Робот должен повиноваться всем приказам, которые даёт человек, кроме тех случаев, когда эти приказы противоречат Первому Закону.
3. Робот должен заботиться о своей безопасности в той мере, в которой это не противоречит Первому или Второму Законам.



Три закона робототехники

Айзек Азимов

ОНИ ВОШЛИ В ИСТОРИЮ



Совершили революцию Объявил о свершении революции



Р. Морли, Т. Боиссейвайн, Г. Чвенк, Й. Ландао



Henning Kagermann
Глава Немецкой Академии наук и инженерии
German National Academy of Science and Engineering (Acatech)
©2017, ОАО «ИнфоТекс».

БОРЬБА ЗА СТРАТЕГИЧЕСКОЕ ЛИДЕРСТВО



Инициатива
Представителей
научных и и
академические кругов,
представителей
крупного бизнеса
2011



IIC международная
организация в составе
из 260 компаний
участников 27
лабораторий (стендов)
работающих в 31
стране.
Основана:
AT&T, Cisco, General
Electric, IBM, and Intel
27 March 2014



53 Японских
производителя
более 140
участников
June 2015



Made in China 2025
MIC 2025

Правительство
2015

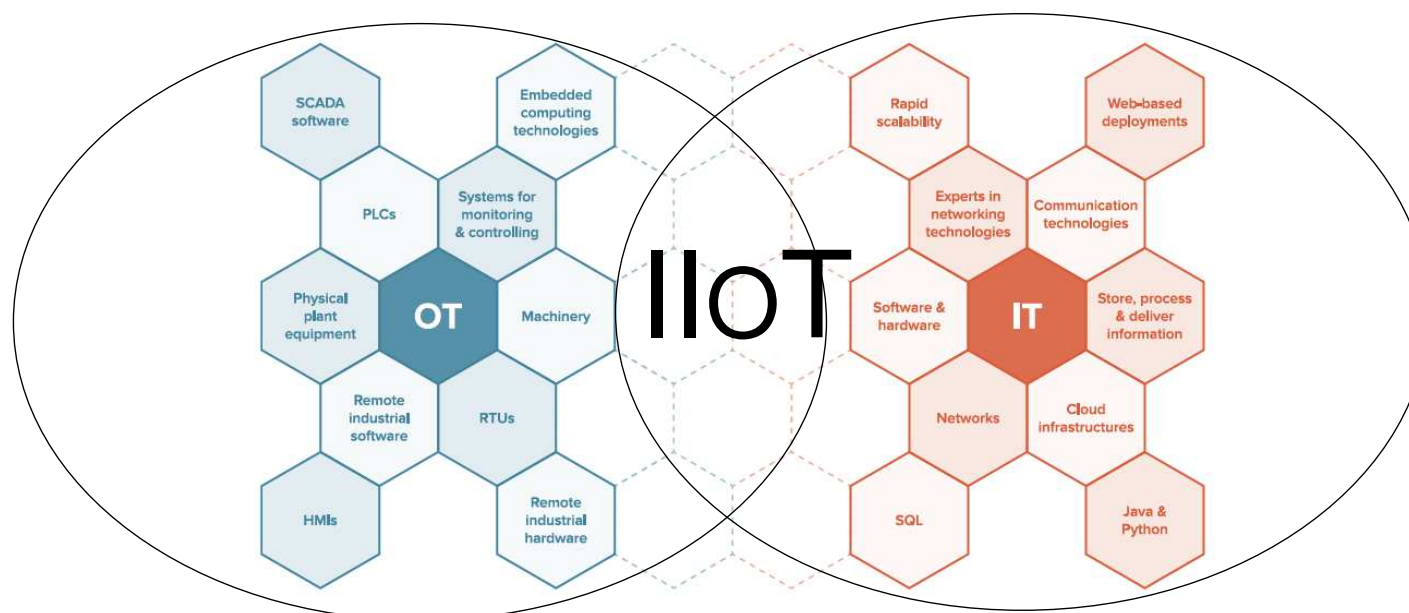


Индустриальный интернет
Цифровая экономика

Поручения Президента РФ В.В.
Путина по итогам
форума "Интернет Экономика»
НАПИ

2016 год

IIoT: КОНВЕРГЕНЦИЯ АСУ ТП И СОВРЕМЕННЫХ ИКТ

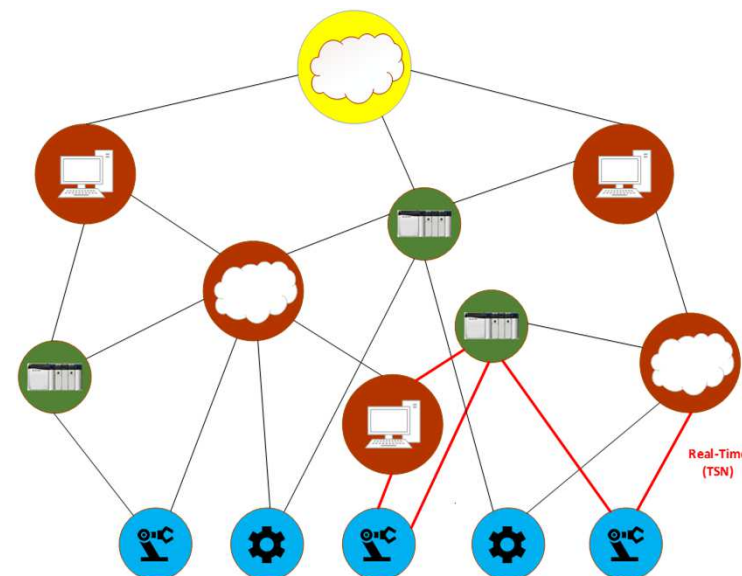
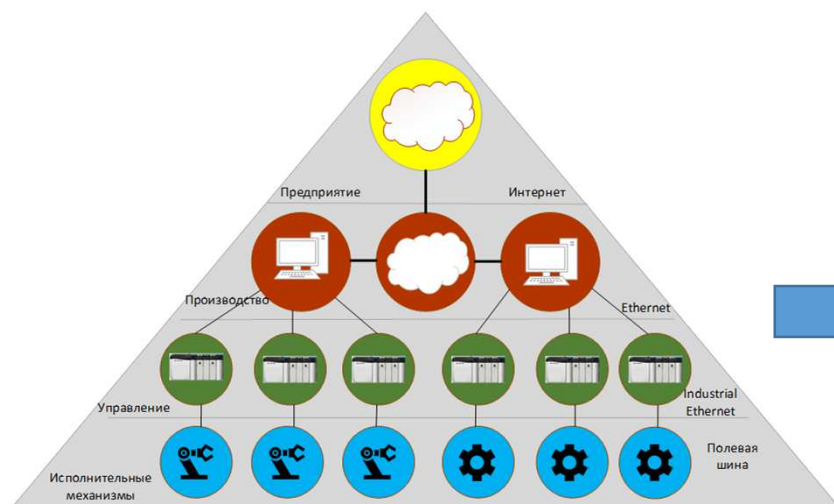


White Paper. IIoT: Combining the Best of OT and IT

©2017, ОАО «ИнфоТекС».

ПЕРЕМЕНЫ, ВЫЗВАННЫЕ INDUSTRY 4.0

infotecs®

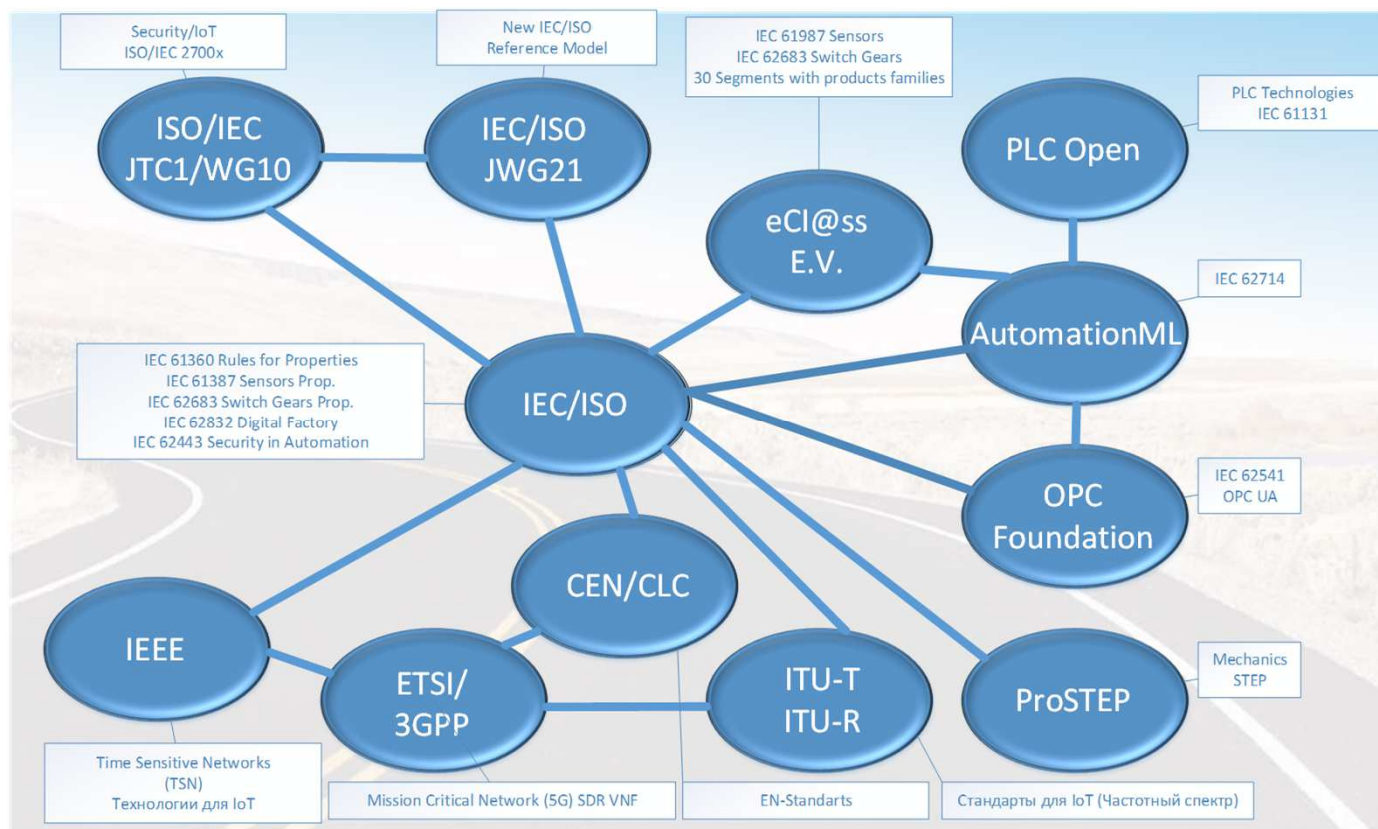


От традиционной автоматизации к автоматизации на основе
CPS: Cyber Physical Systems

CPC UA
IEEE TSN

https://www.vdi.de/uploads/media/Stellungnahme_Cyber-Physical_Systems.pdf ©2017, ОАО «ИнфоТеКс».

ОСНОВНЫЕ СТАНДАРТЫ INDUSTRY 4.0

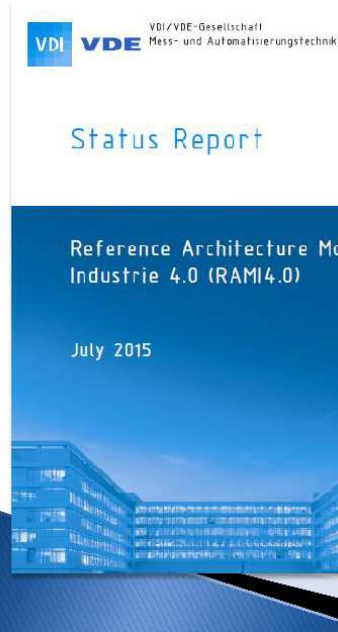


Strategy and Roadmap of Industry 4.0 for International Standardization, 2017
<http://www.omg.org/cgi-bin/doc?mantis/2017-06-11>

<http://www.zvei.org/Download.aspx>
Report ZVEI Reference

North America: Industrial Internet Consortium
Listing OPC UA in the standards / Technical
China National Standard

<https://www.iiconsortium.org>



www.dcs.org

Smart factory based on 'Manufacturing Industry Innovation 3.0 (MII3.0)' in response to the paradigm shift of the 4th Industrial Revolution.

- ▶ TC124 (*National Time Measurement and China*) has held first meeting in October
 - ▶ The first OPC UA r
 - 20090699-T-60
 - 20090700-T-60
 - 20090701-T-60
 - 20090702-T-604
 - ▶ OPC China will full standard
 - ▶ Continue with Part



МИР ДО И ПОСЛЕ STUXNET

infotecs®

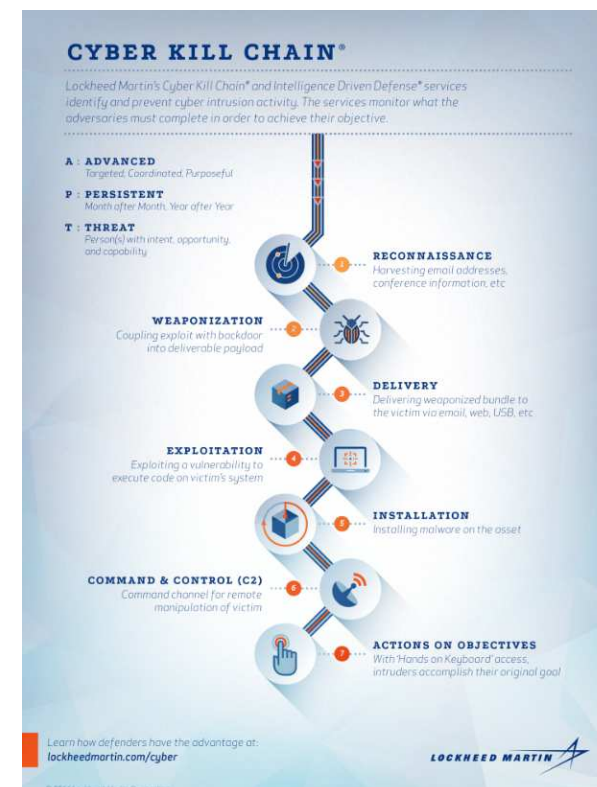
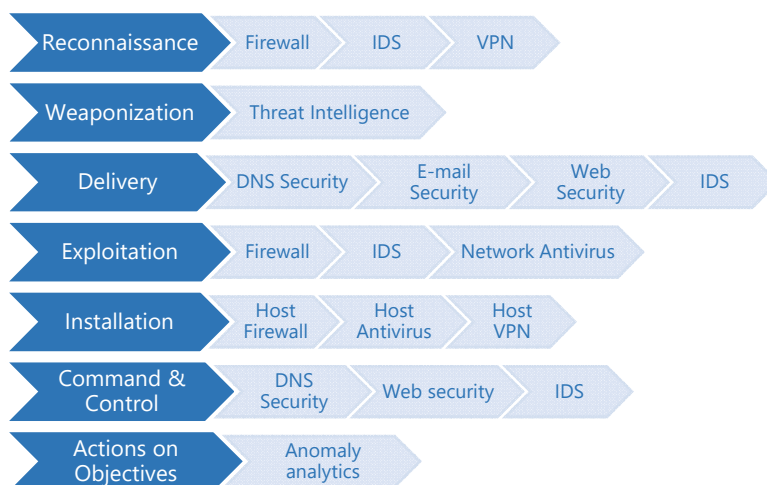


<https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>

©2017, ОАО «ИнфоТеКС».

KILL CHAIN VIEW

infotecs®

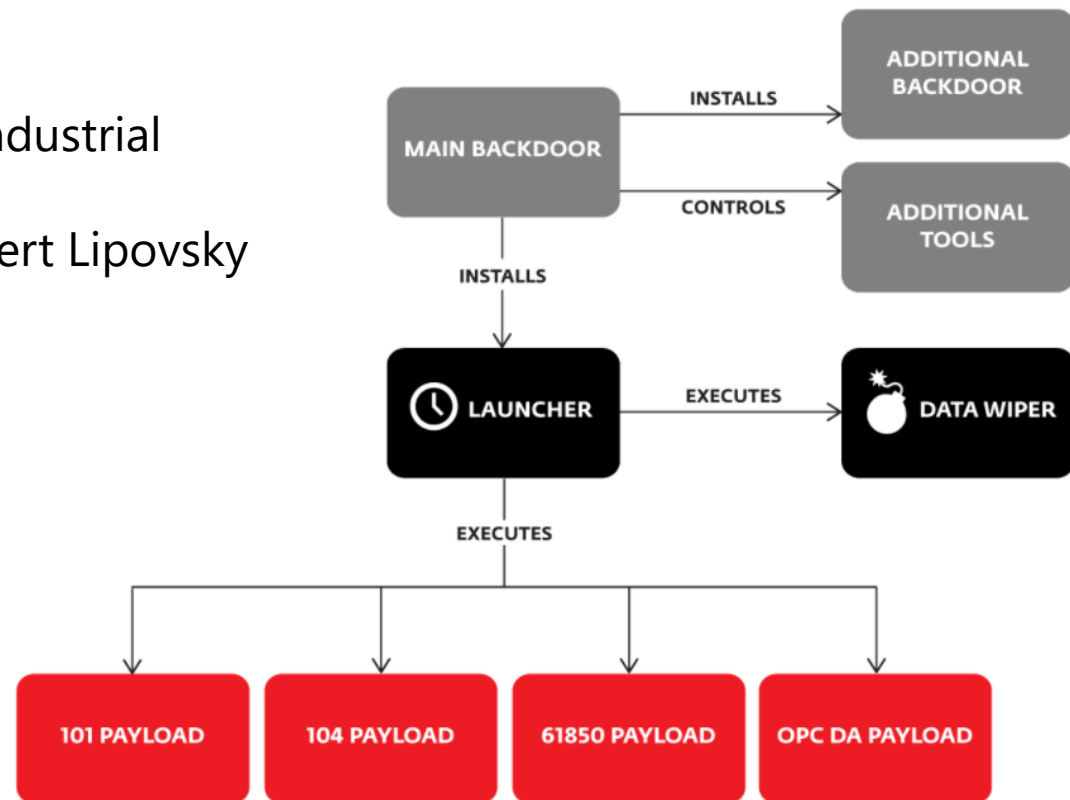


<http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html> ©2017, ОАО «ИнфоТеКС».

INDUSTROYER:

Industroyer: Biggest threat to industrial control systems since Stuxnet.

Robert Lipovsky



https://cdn1-prodint.esetstatic.com/ESET/INT/Landing/2017/black-hat/WIN32_Industroyer-USLetter-WEB.pdf

©2017, ОАО «ИнфоТеКС».

Уязвимости на разных уровнях

➤ **Уязвимости на уровне системного программного обеспечения:**

- Базовая система ввода-вывода (BIOS);
- Операционная система .

➤ **Уязвимости на уровне прикладного программного обеспечения:**

- Программные средства (ПС) общего назначения;
- ПС специального назначения;
- ПС профессионального уровня.

➤ **Уязвимости используемых телекоммуникационных протоколов:**

- МЭК 60870-5-104;
- MMS, GOOSE, SV;
- PTP, SMTP.



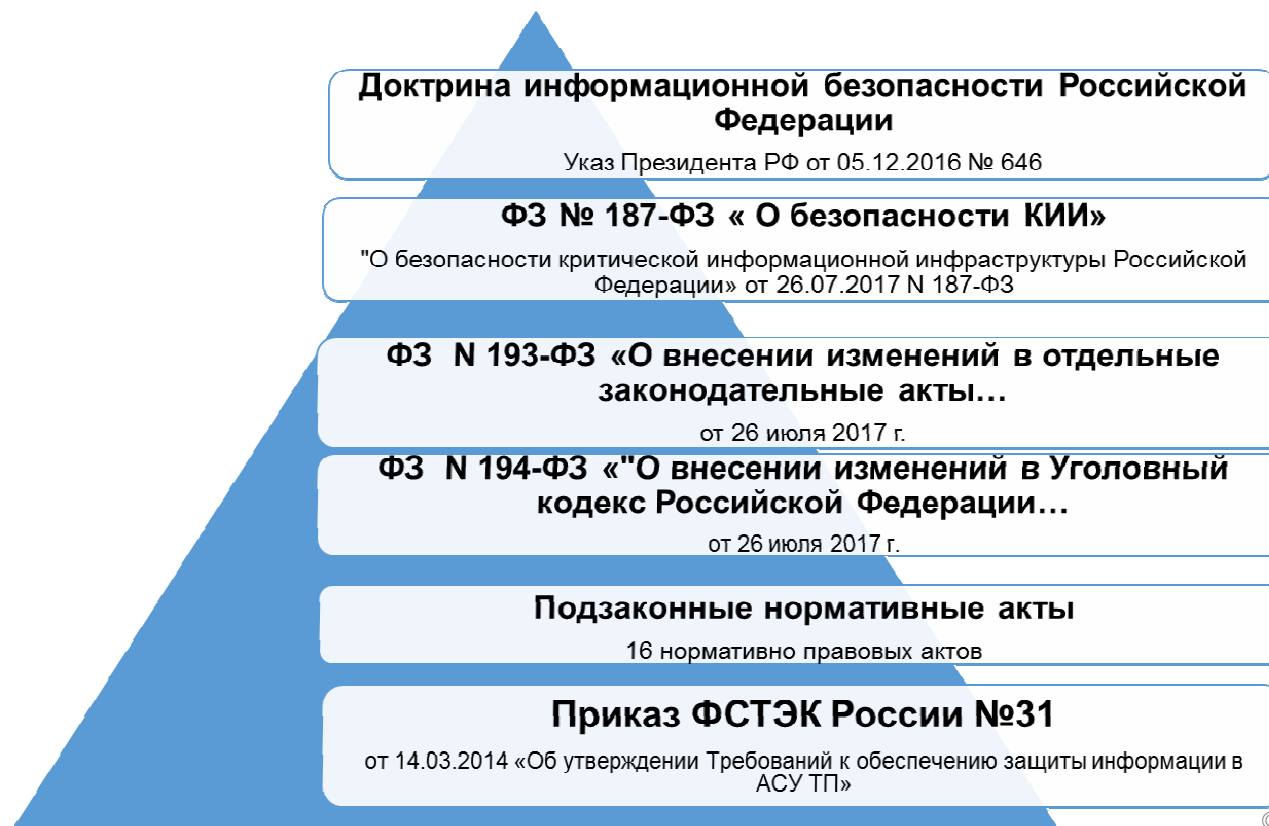
КАК МЫ МОЖЕМ ОЦЕНИТЬ НАДЕЖНОСТЬ?

infotecs®

Аварии могут быть
индикатором надежности
промышленных систем.



РЕАКЦИЯ НА ВЫЗОВЫ



ФСТЭК России

infotecs®



Указ Президента Российской Федерации от 25.11.2017 № 569 "О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085"

Дата опубликования: 25.11.2017

ДОКТРИНА ИБ РФ

infotecs®

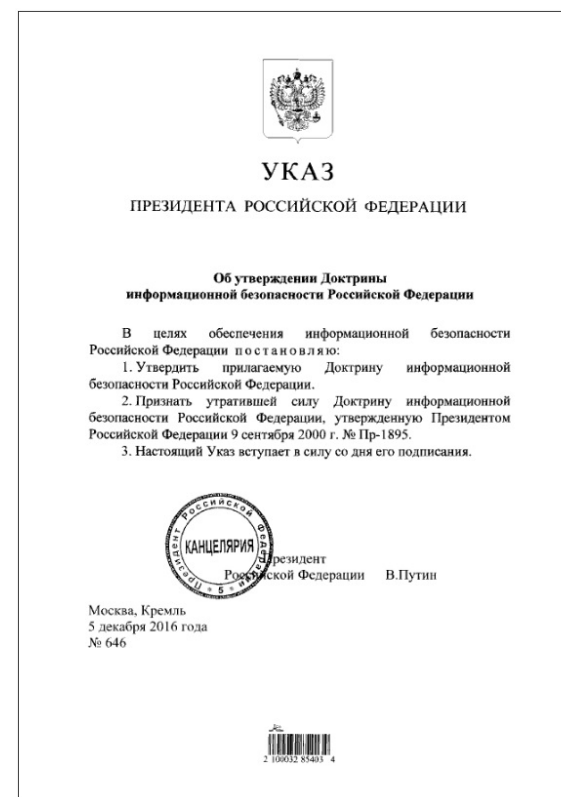
- **Национальные интересы в информационной сфере:**

Обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры Российской Федерации.

- **Основные информационные угрозы и состояние информационной безопасности:**

.... практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

.... в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.



ДОКТРИНА ИБ РФ

infotecs®

- **Стратегические цели и основные направления обеспечения информационной безопасности:**

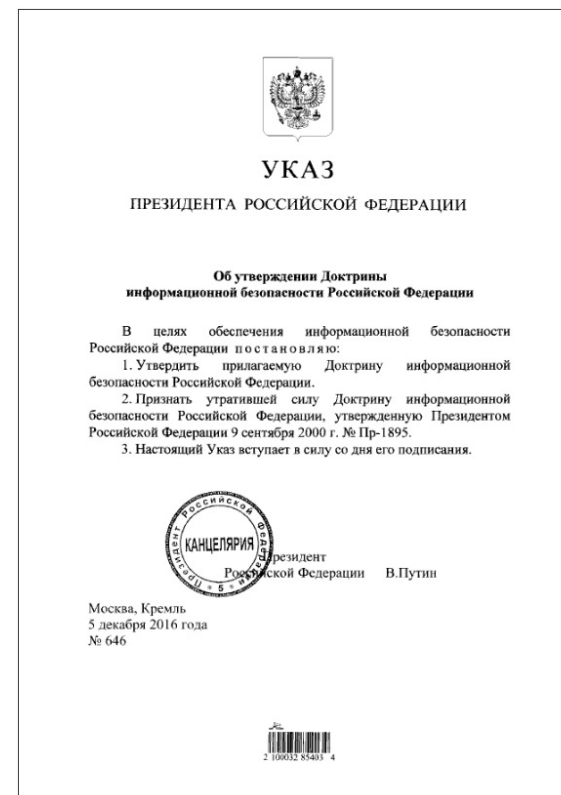
...защита критической информационной инфраструктуры.

Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

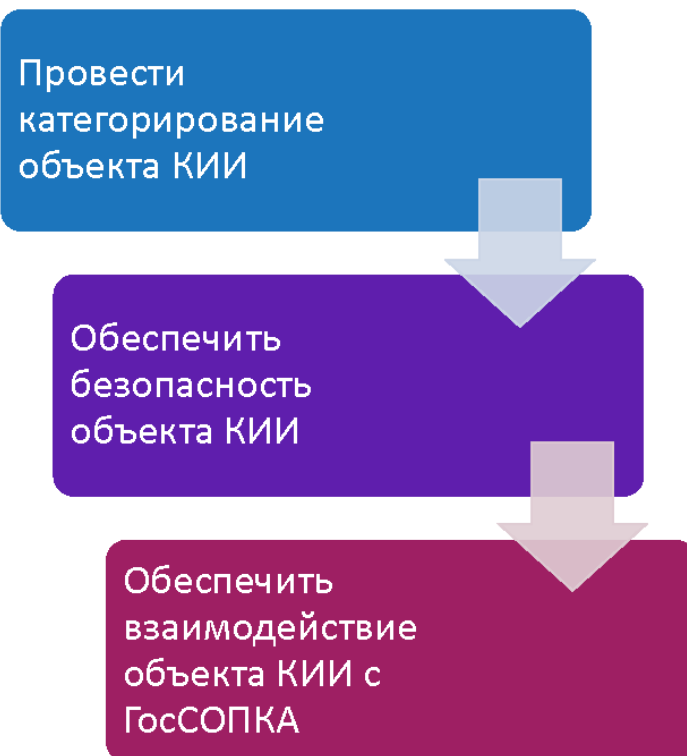
создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры



№ 187-ФЗ О БЕЗОПАСНОСТИ КИИ

infotecs®



РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

**О безопасности критической информационной
инфраструктуры Российской Федерации**

Принят Государственной Думой
Одобен Советом Федерации

12 июля 2017 года
19 июля 2017 года

Статья 1. Сфера действия настоящего Федерального закона

Настоящий 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.

**Статья 2. Основные понятия, используемые в настоящем
Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:



2 100039 04259 6

ФСТЭК России

infotecs®



Приказ ФСТЭК России от 9 февраля 2016 г. № 9.

Утверждены Требования к межсетевым экранам:

- межсетевой экран уровня промышленной сети (тип «Д») – межсетевой экран, применяемый в автоматизированной системе управления технологическими или производственными процессами.

Приказ ФСТЭК России от 19 августа 2016 г. N 119.

Утверждены Требования безопасности информации к операционным системам:

- встраиваемая операционная система (тип «Б») – операционная система, встроенная (прошитая) в специализированные технические устройства, предназначенные для решения заранее определенного набора задач;
- операционная система реального времени (тип «В») – операционная система, предназначенная для обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности.

ФСТЭК России

infotecs®

Планы:

Приказ ФСТЭК России «Об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ».

На основе Приказов ФСТЭК России № 31 и № 17.



ФСБ России

infotecs®



- Методические рекомендации ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Утверждены в декабре 2016 г.

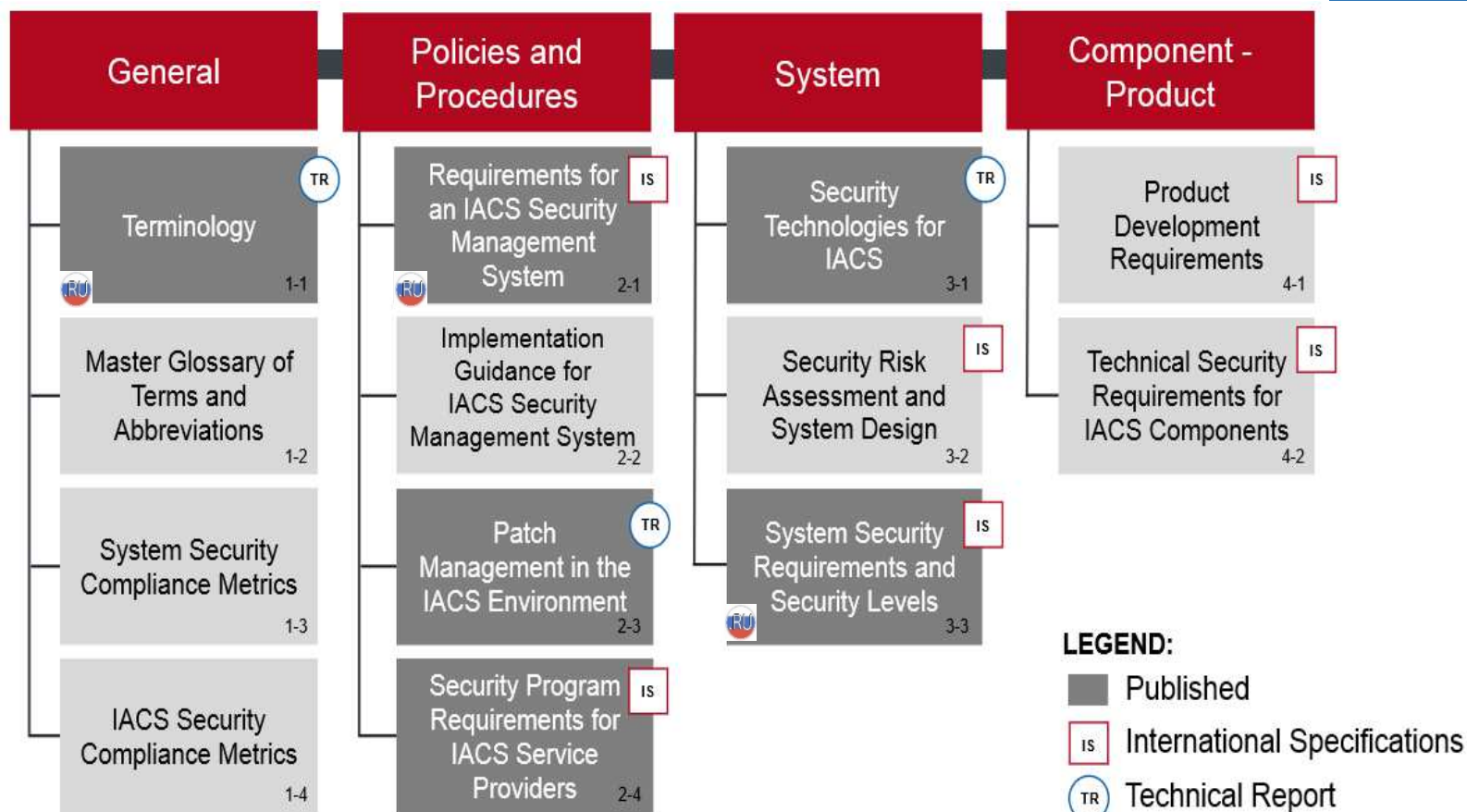
РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД

infotecs®



СЕРИЯ СТАНДАРТОВ IEC 62443

infotecs®



Webinar, Scalable Solutions for ICS Cybersecurity Assurance ©2017, ОАО «ИнфоТеКС».

ГОСТ Р МЭК 62443



- **ГОСТ Р 56205-2014 IEC/TS 62443- 1- 1:2009**

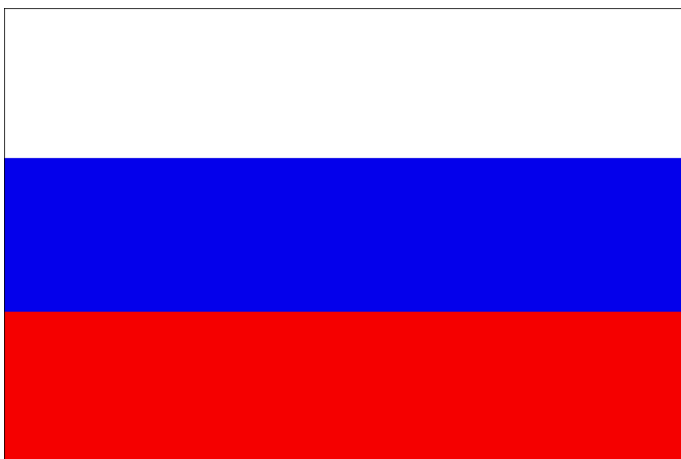
«Терминология, концептуальные положения и модели».

- **ГОСТ Р МЭК 62443-2-1-2015**

Составление программы обеспечения защищенности
(кибербезопасности) системы управления и промышленной автоматике.

- **ГОСТ Р МЭК 62443-3-3—2016**

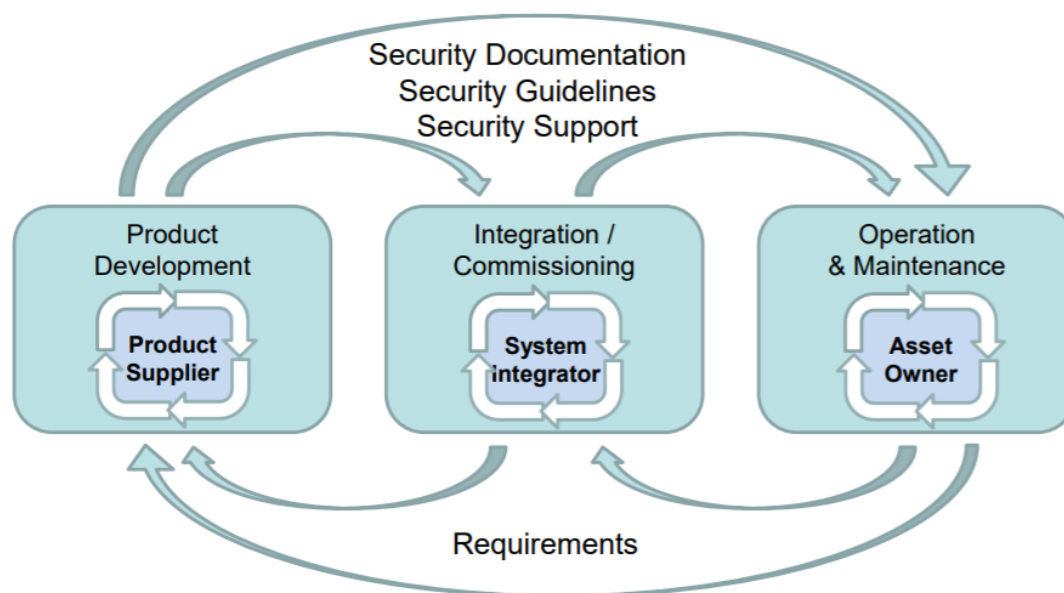
«Требования к системной безопасности и уровни безопасности».



ПРИОРИТЕТЫ ПРИЗИ

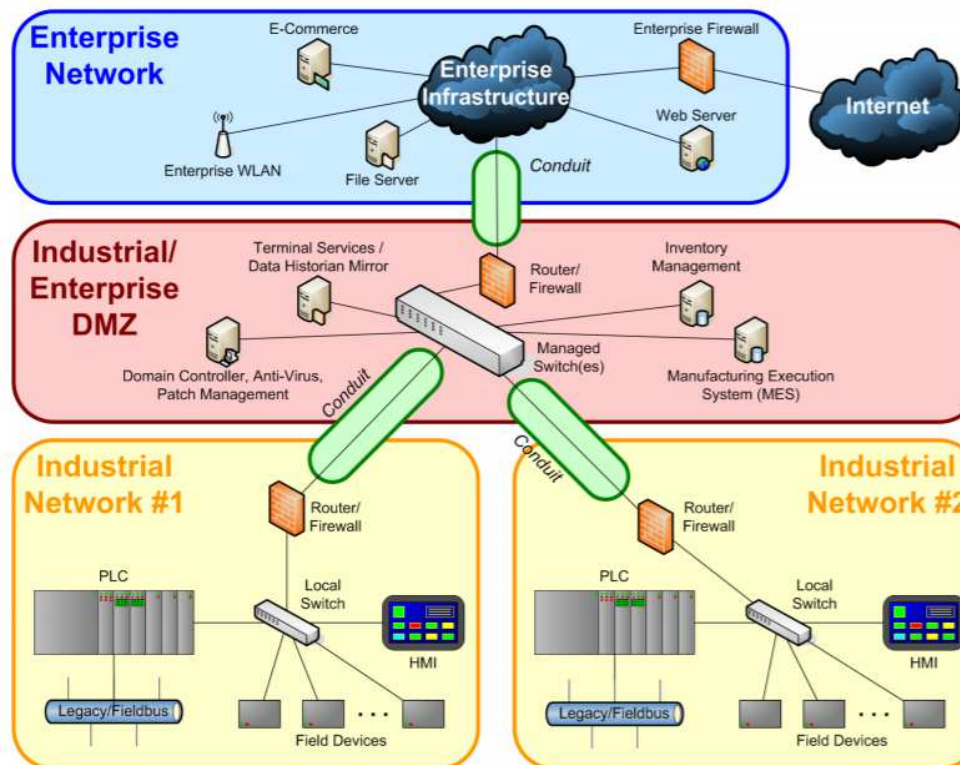


ВЗАИМОСВЯЗАННЫЕ ЖИЗНЕННЫЕ ЦИКЛЫ



Based on VDI 2182

МОДЕЛЬ ЗОНИРОВАНИЯ АСУ ТП IEC 62443



КАК СНИЗИТЬ РИСКИ?

infotecs®



1. Приказ ФСТЭК России №31

Мера: Обеспечение безопасной разработки

2. ГОСТ Р ИСО/МЭК 27034-1. Безопасность приложений

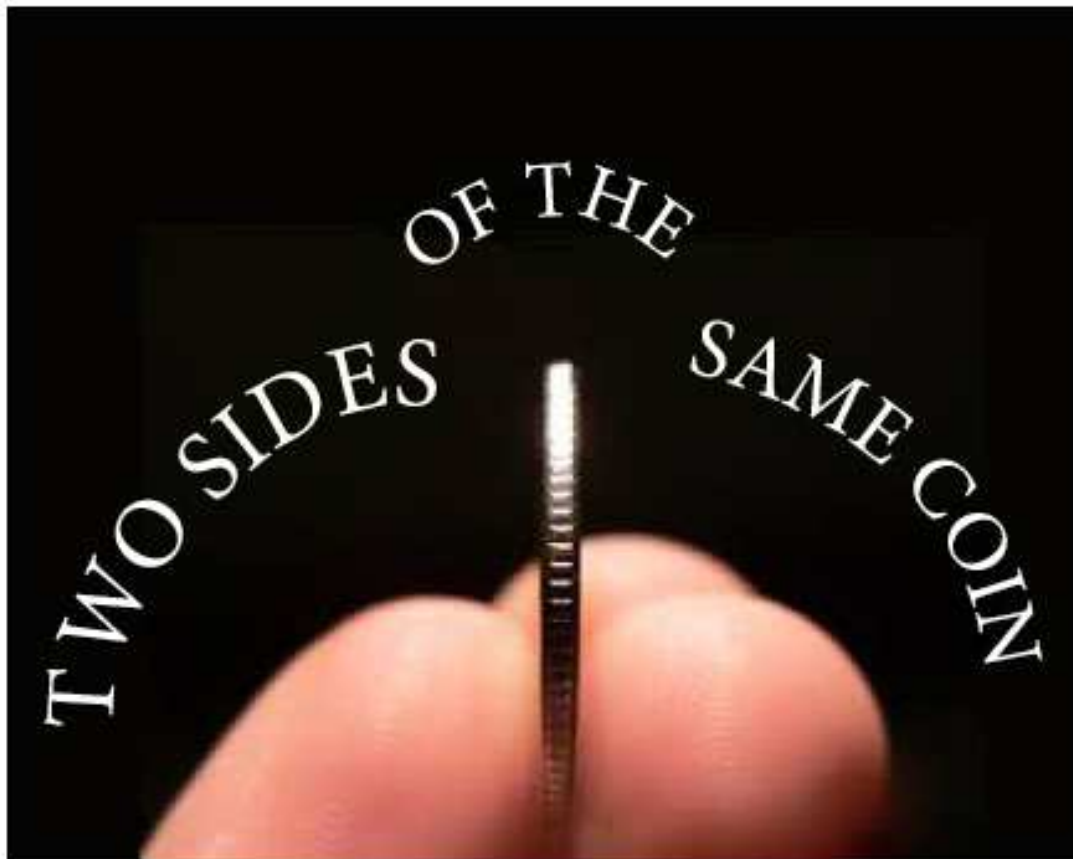
3. ГОСТ Р 56939-2016 «Разработка безопасного программного обеспечения».

4. Методические рекомендации по обновлению сертифицированных средств защиты информации

5. Создан и развивается Банк данных угроз безопасности информации <http://bdu.fstec.ru/>

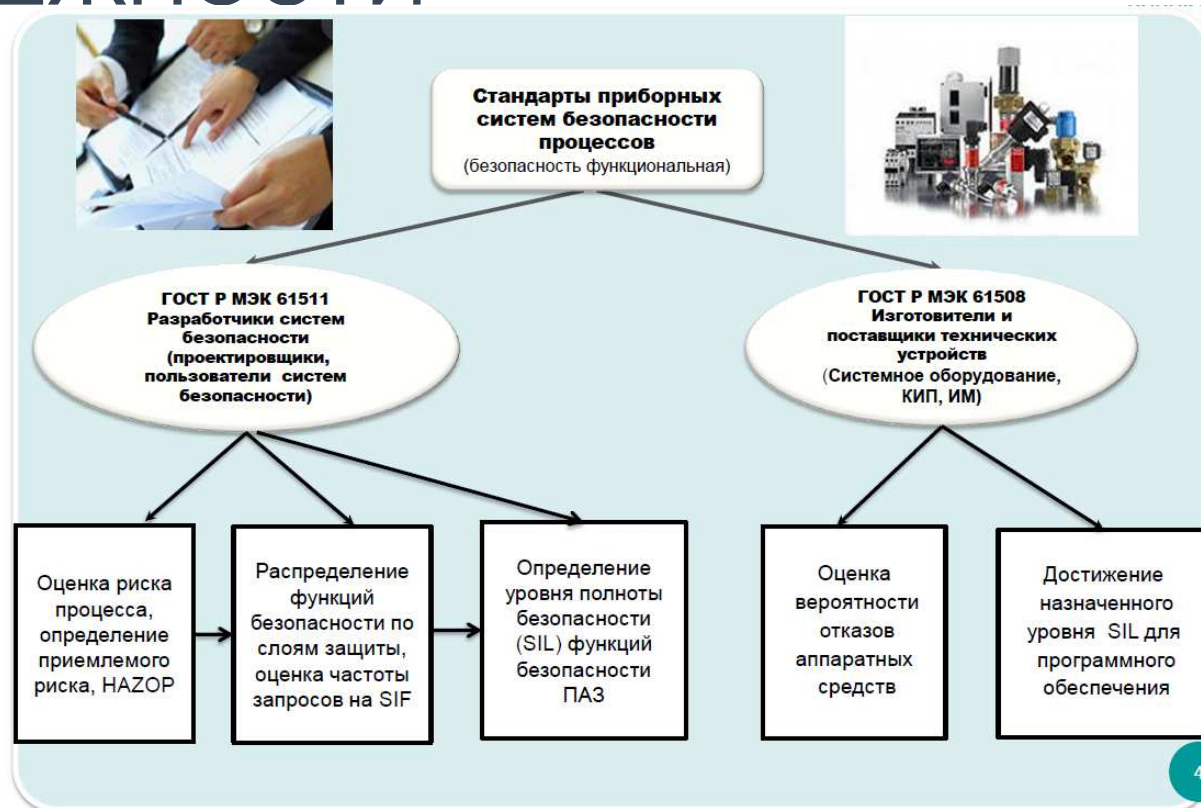
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

infotecs®



©2017, ОАО «ИнфоТеКС».

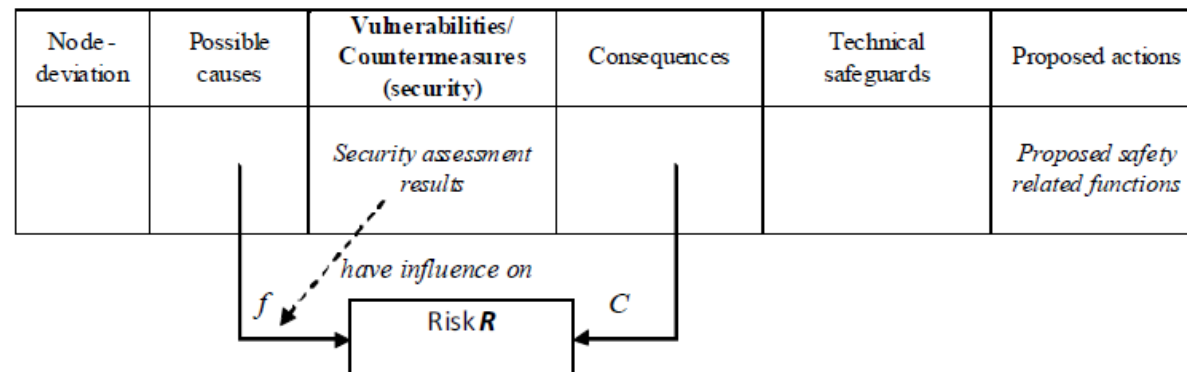
ТРАКТОВКА ФУНКЦИОНАЛЬНОЙ НАДЕЖНОСТИ



HAZOP и ИБ



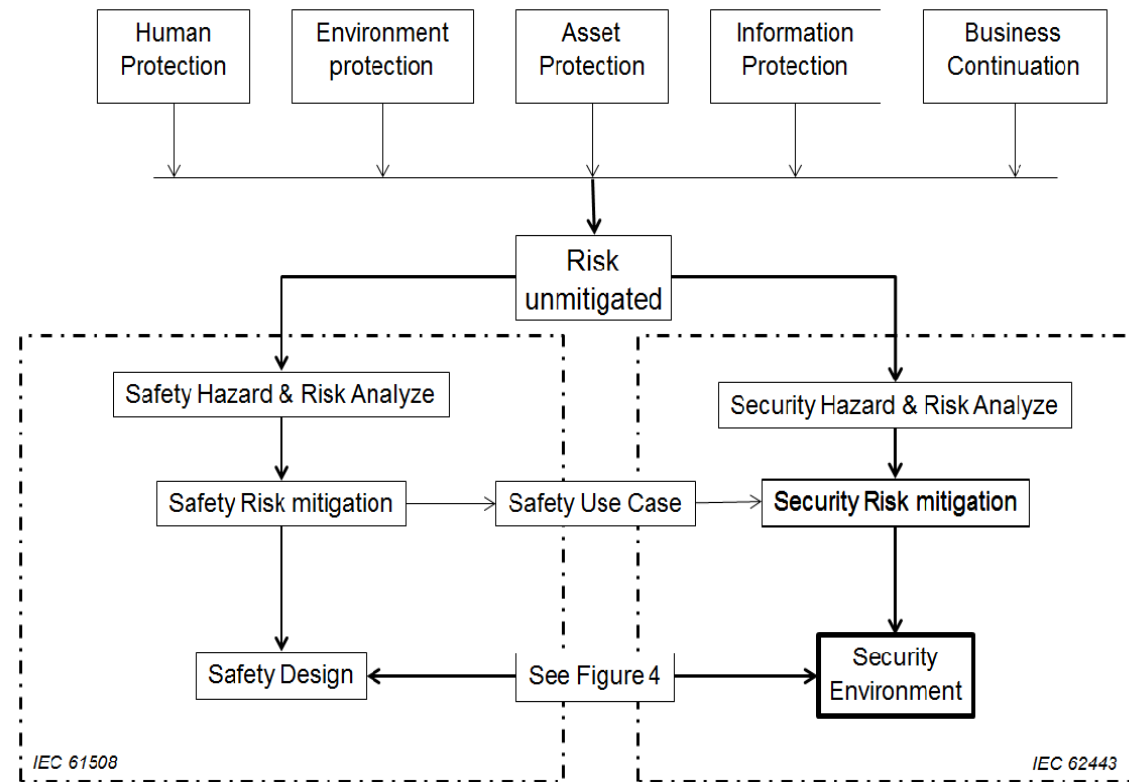
IEC 61511 Edition 2.0 «Safety instrumented system for the process industry sector»



Journal of Polish Safety and Reliability Association/Security aspects in functional safety analysis

©2017, ОАО «ИнфоТеКС».

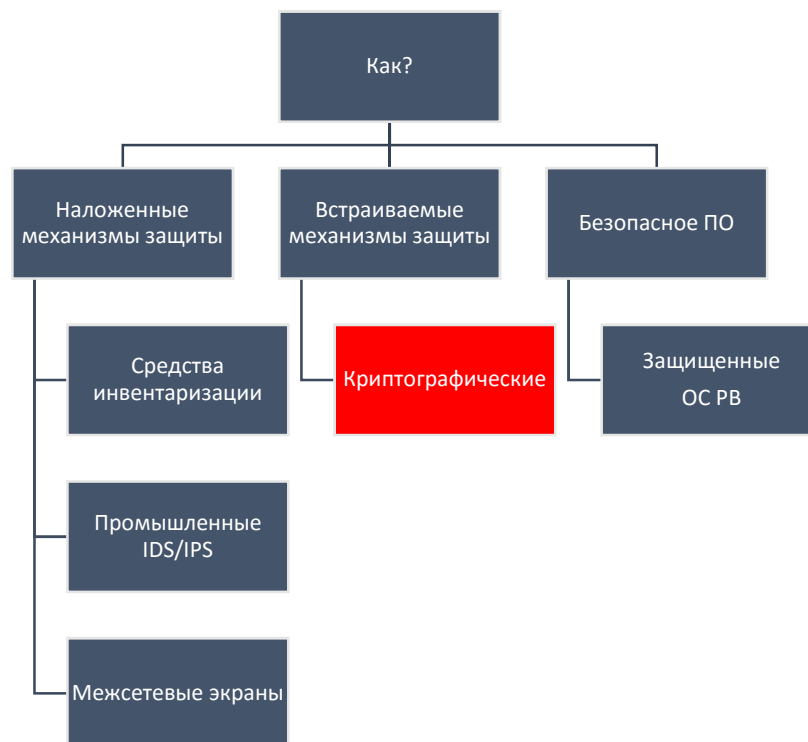
МЕТОДОЛОГИЯ



IEC TC 65: Industrial Process measurement, control and automation

IEC TR 63069 ED1 ©2017, ОАО «ИнфоТеКС».

КАК ЗАЩИЩАТЬ АСУ ТП?



ПРОМЫШЛЕННЫЙ КРИПТОШЛЮЗ VIPNET COORDINATOR IG

infotecs®



Защищенный канал VPN с поддержкой L2overIP (до 10 Мбит/с), межсетевой экран, резервирование

Индустриальное исполнение (-20°... +60°C, IP30, 10...30 V DC, DIN-рейка)

Маршрутизатор (DNS, DHCP, VLAN)

Беспроводные интерфейсы (3G, LTE, Wi-Fi)

Работа в режиме шлюза (Ethernet - RS-232/RS-485) и моста Modbus TCP - Modbus RTU

Дискретные порты ввода-вывода (GPIO) для подключения внешних датчиков/исполнительных устройств

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ КРИПТОГРАФИИ В АСУ ТП



Защита данных и команд

- Целостность
- Конфиденциальность
- Защита от повторного навязывания
- Аутентичность
- Юридическая значимость

Авторизация и аутентификация персонала

- Многофакторная аутентификация
- Разделение секрета



КРИПТОГРАФИЯ НА ПОЛЕВОМ

УРОВНЕ



- Встраиваемый в защищаемое устройство программно-аппаратный модуль (ПАК)
- Предоставляет базовые криптографические операции для реализации сценариев безопасности в виде простого API
- Управление и хранение ключевой информации
- Пассивное подключение к защищаемому устройству по техническим интерфейсам UART, SPI, USB, I2C
- Выполнен в виде SOM-модуля, 64x36 мм
- Индустриальное исполнение и питание: -40...+75°C, 4 ...17В DC, 0.7 Вт (при 5В)

или

- Набор программных библиотек для встраивания для ОС Windows/Linux и архитектур x86, ARM, MIPS (Байкал)

infotecs®

Аппаратное исполнение

ПО

КОМПЛЕКСНЫЙ ПОДХОД



Этап 1: Систематизация и уточнение нормативных требований ИБ и ПБ применительно к отраслевой специфике.

Этап 2: Формирование модели угроз и модели нарушителя.

Этап 3: Формирование концепции совместного решения.

Этап 4: Разработка решения.

Этап 5: Разработка программы комплексных испытаний:

- Лабораторные

- Стендовые

- Полигонные

- Натурные испытания

- и другие виды испытаний...

Этап 6: Представление заказчику.



©2017, ОАО «ИнфоТеКС».

ВЫВОДЫ:

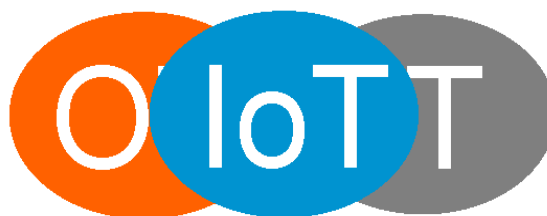
- Важной задачей является задача разработки инженерных методик расчета функциональной надежности.
- Системы должны разрабатываться исходя из анализа угроз функциональной надежности и информационной безопасности.
- В условиях необходимости удовлетворять комплексу требований по функциональной надежности, безопасности, наличия требований по быстрдействию телекоммуникационных протоколов, оптимальности затрат реализация концепции «secure by design» (встроенных средств защиты информации в промышленных системах автоматизации), требований безопасной разработки – выглядит наиболее перспективно.

Давайте пообщаемся!

Карантаев Владимир / к.т.н. / Эксперт МЭК
Руководитель направления
Vladimir.Karantaev@infotecs.ru / +7 915 221 15 96

- interoperability, portability, security and privacy
 - Connect production facilities with ICT infrastructure
 - Merge customer and machine data
 - Machines communicate with machines

- ✓ Machine Safety
- ✓ Robustness
- ✓ Real-time (μ s)
- ✓ High availability



- ✓ Performance
- ✓ Security
- ✓ Cloud Computing
- ✓ Virtualization