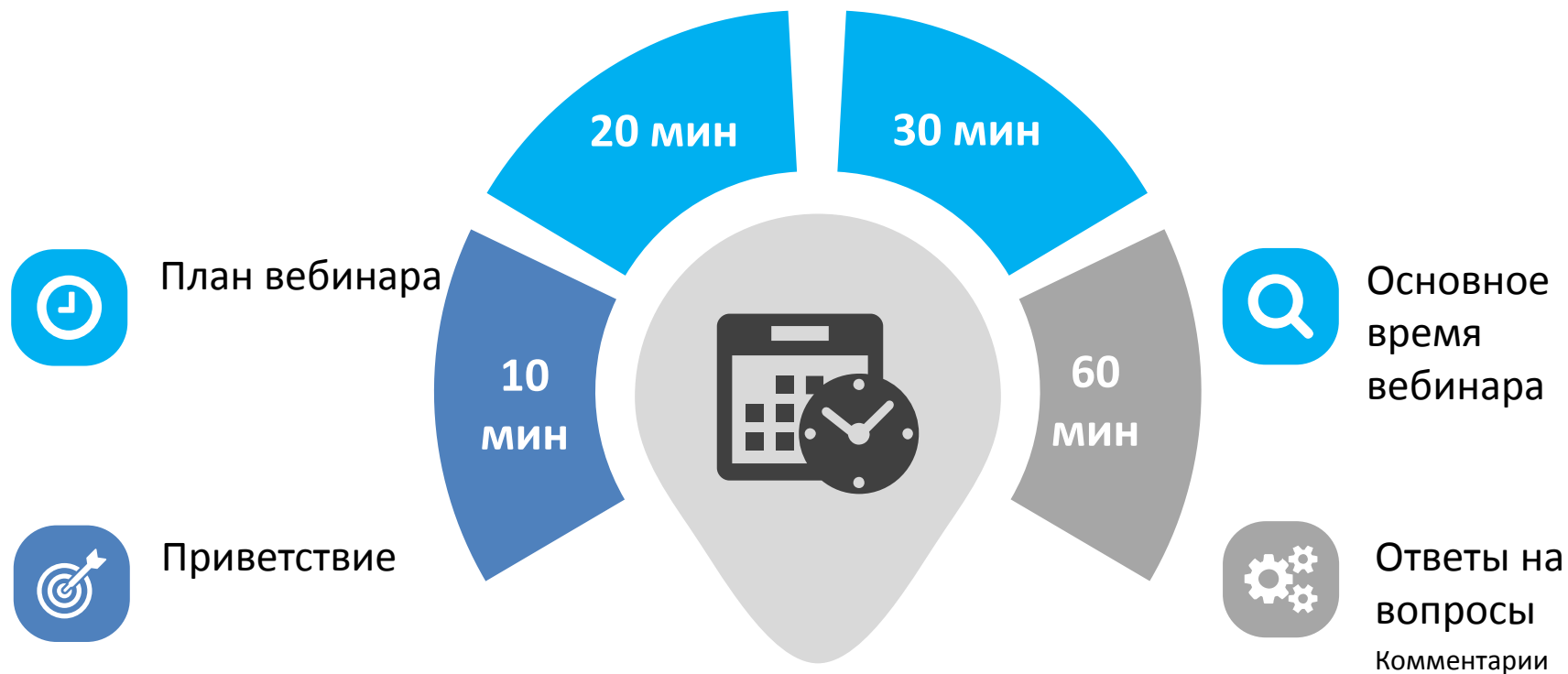
The background of the slide is a photograph of an industrial facility at night, with various towers and structures illuminated by warm lights against a dark blue sky. In the foreground, there is a semi-transparent white box containing text. To the right of the text box, there are two hard hats: one yellow and one white, resting on a white surface. In the background behind the text box, there is a faint image of a person's hands using a calculator and a pen on a document.

# Введение в тему индустриальной безопасности

---

**Карантаев Владимир / к.т.н. / Менеджер**  
**Отдел научных исследований и развития продуктов**  
**[Vladimir.Karantaev@infotecs.ru](mailto:Vladimir.Karantaev@infotecs.ru)**

# Регламент



# План вебинара:

- **Описание предметной области.**
  - Определения;
  - Тенденции развития;
  - Требования к системам автоматизации.
- **Предпосылки наличия проблем с ИБ АСУ ТП.**
- **Масштаб проблем с ИБ АСУ ТП.**
  - Инциденты;
  - Уязвимости;
  - Мотивация.
- **Нормативно-правовая база РФ.**
- **Решения ОАО «ИнфоТеКС» по ЗИ АСУ ТП.**
  - Решения ViPNet в индустриальном секторе;
  - Сценарии применения продуктов ViPNet.

# ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

# Определения: КВО, КИИ, КСИИ, АСУ ТП КВО ...

- Критически важный объект инфраструктуры Российской Федерации (Критически важный объект) - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок.

"Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ"

- Критически важный объект – объект, нарушение или прекращение функционирования которого может привести к потере управления экономикой РФ, субъекта РФ или административно-территориальной единицы, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени.

# Определения: КВО, КИИ, КСИИ, АСУ ТП КВО ...



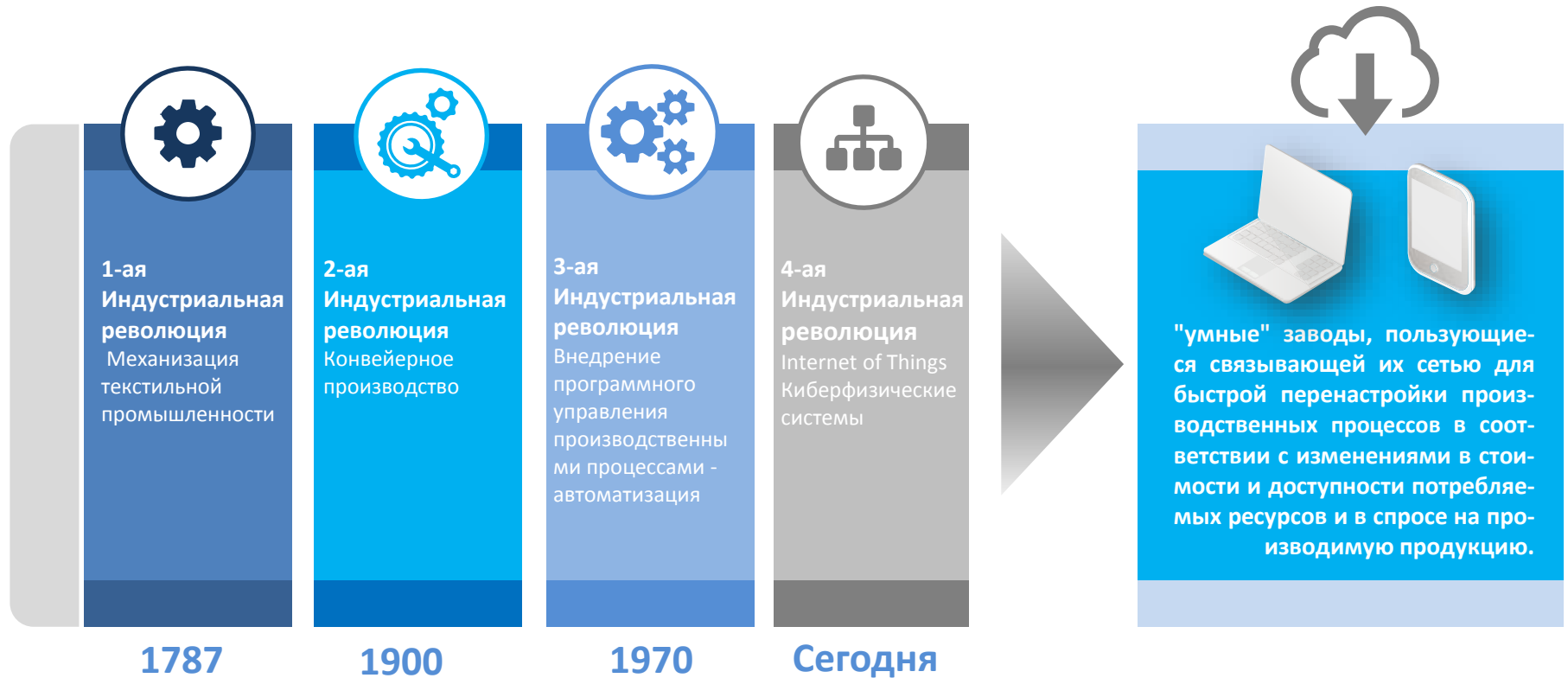
# Определения: КВО, КИИ, КСИИ, АСУ ТП КВО ...



# Определения: КВО, КИИ, КСИИ, АСУ ТП КВО ...



# Четвертая индустриальная революция



<http://www.arcweb.com/events/arc-industry-forum-orlando/arcindustryforumorlando2014presentations/Ethernet%20to%20the%20field%20of%20Process%20Automation.pdf>

# Векторы развития: Industry 4.0, Industrial Internet

## Industry 4.0

Инициатор: Правительство  
 Инвестиции: 40 миллиардов евро в год  
 Фокус на производстве: 22% немецкого ВВП

2011

Германия

## Industrial Internet

Консорциум промышленного интернета  
 Фокус на производстве, энергетике, медицине, транспорте, сельском хозяйстве, коммунальных услугах  
 Распространяется на 65-70% всей экономической активности.

2014

США

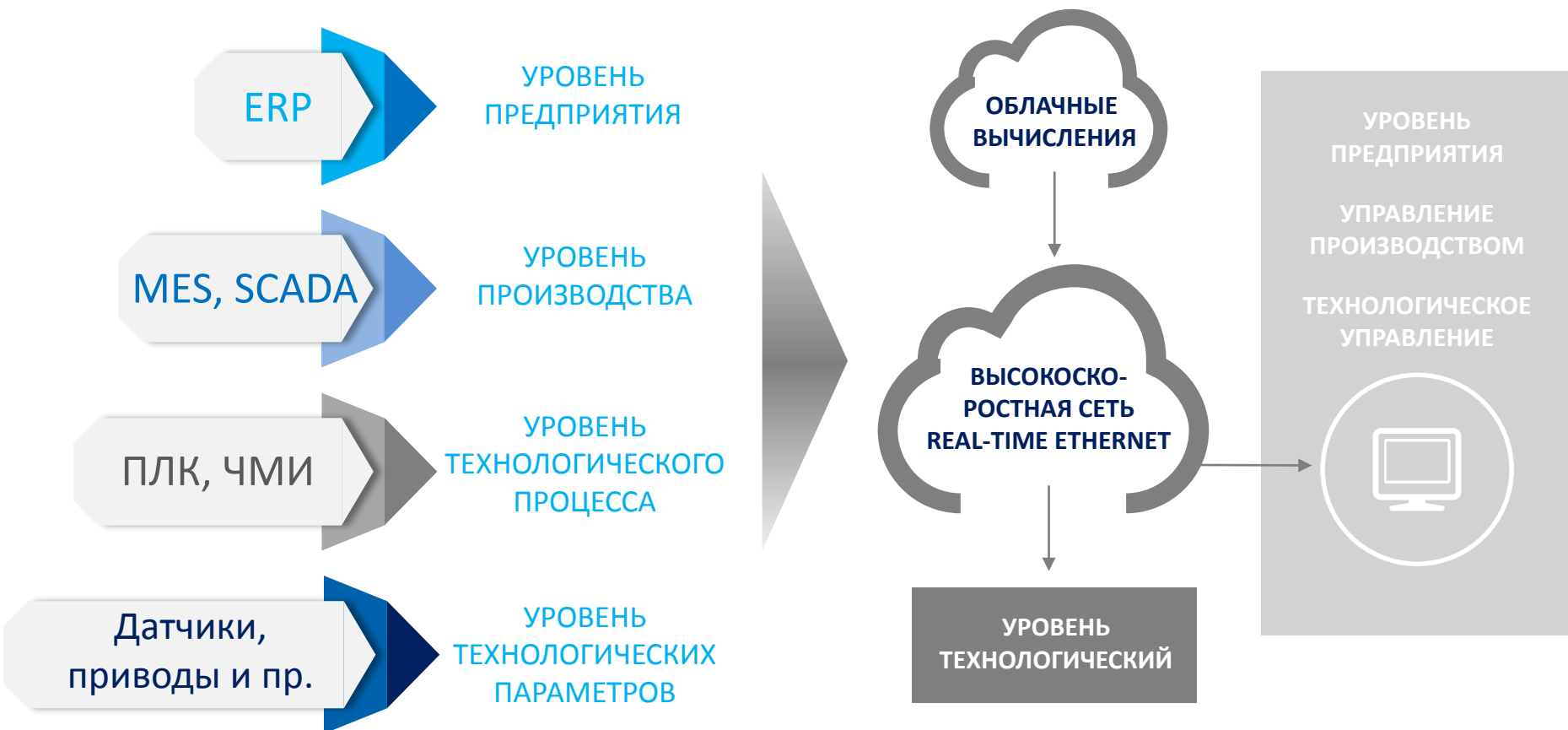
## Индустриальный Интернет

Фокус на транспорте, энергетике, производстве, медицине  
 Поручение: В.В. Путина от 29.01.2016  
 Ассоциация «Национальный консорциум Промышленного интернета»

2016

Россия

# Трансформация структуры информационных систем

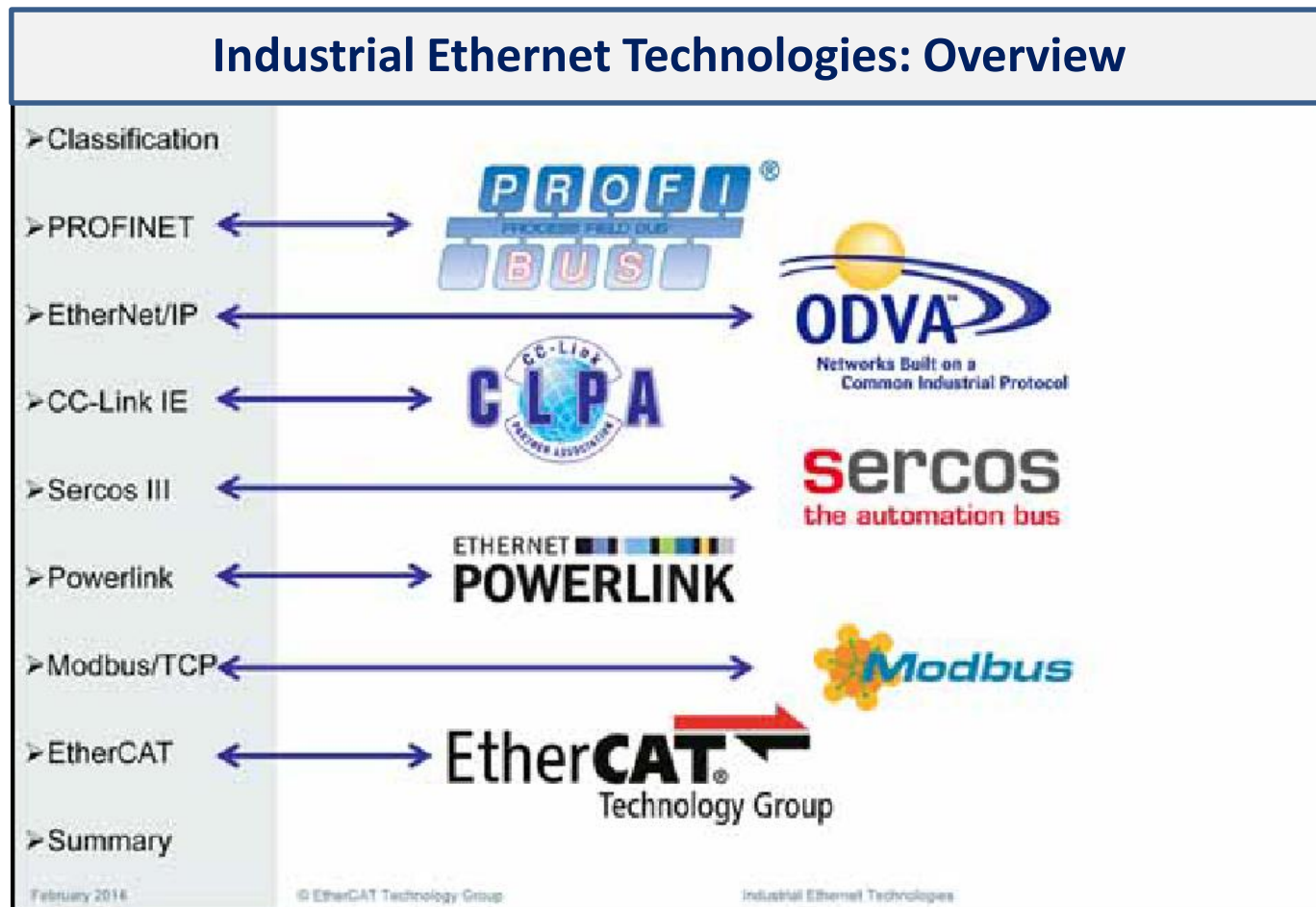


# Выводы:

- Необходимо законодательно закрепить основной понятийный аппарат;
- Новый этап экономического развития предъявит иные требования к системам автоматизации;
- Изменившаяся структура информационных систем предприятий потребует нового взгляда на средства защиты информации.

# Предпосылки наличия проблем с ИБ АСУ ТП

# Применение Ethernet, TCP/IP технологий

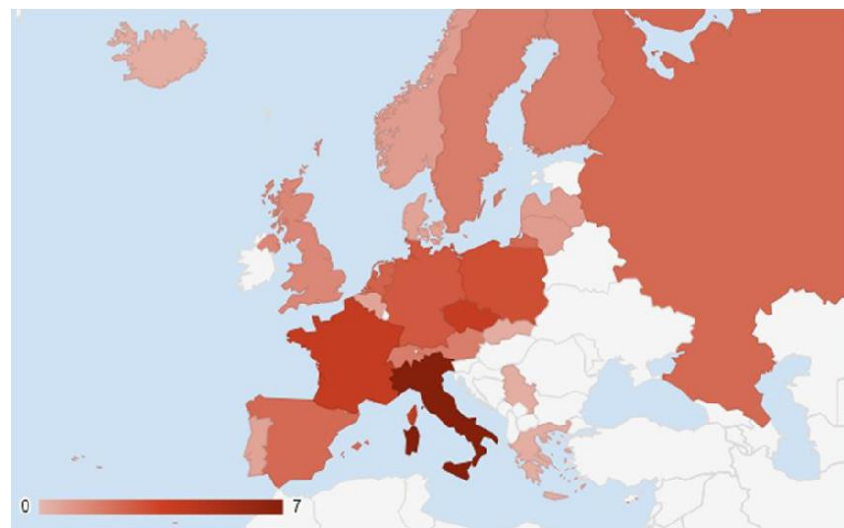
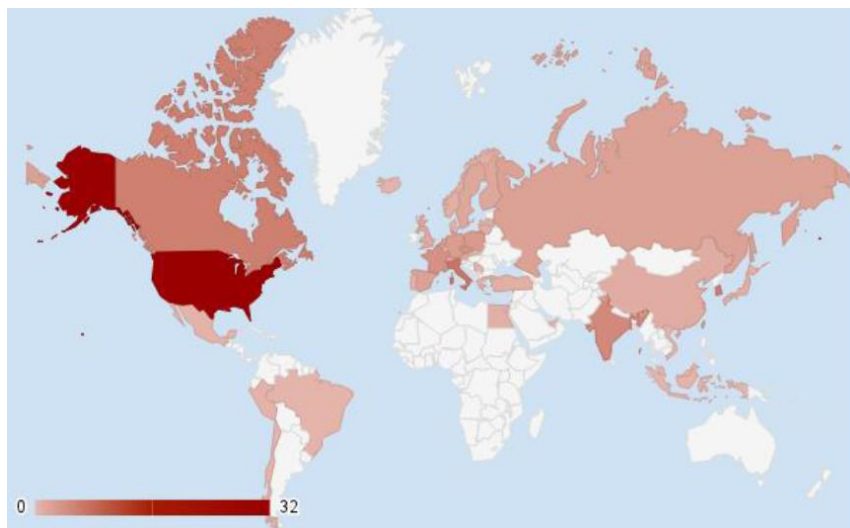


# Интеграция информационных систем предприятия:

Доступ к корпоративной сети:

Согласно результатам последних исследований министерства внутренней безопасности США Department of Homeland Security (DHS), в среднем технологическая сеть имеет 11 (!) точек прямого подключения к корпоративной сети.

# Доступность элементов автоматики из сети Интернет



2013 г. - 68 000, Positive Technologies  
2014 г - 82 000 , Homeland Security, NCCIC

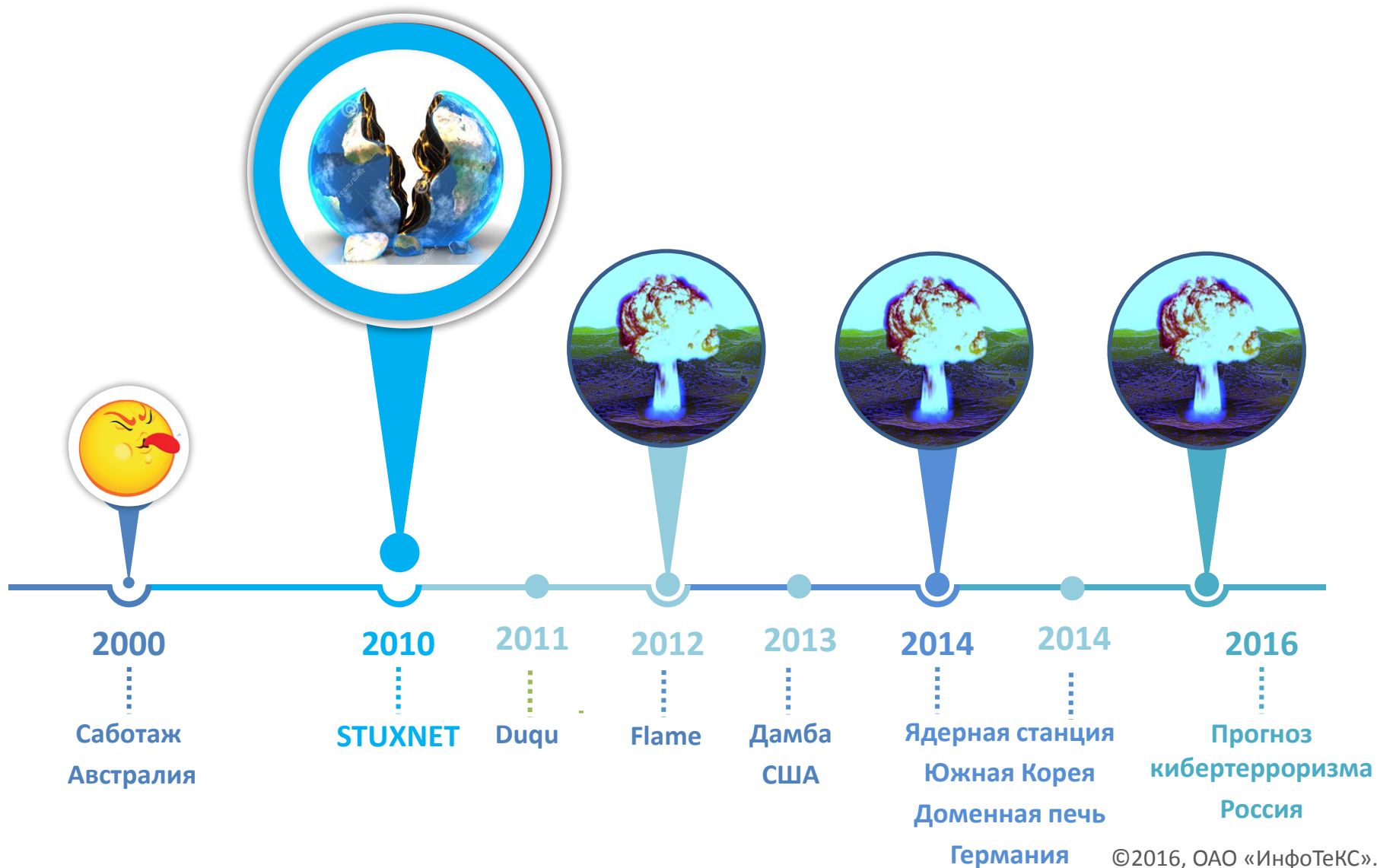
# Состояние ИБ АСУ ТП

Последнее исследование, проведенное институтом SANS, показало, что лишь 9% IT-специалистов в промышленном секторе уверены, что безопасность их систем ни разу не нарушалась.

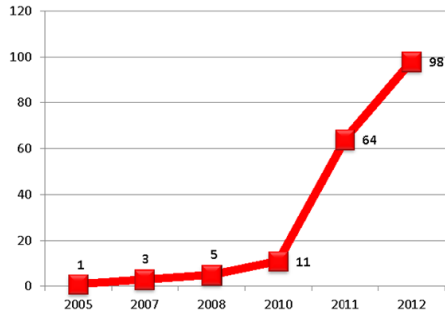
При этом 16% заявили, что не проводят никаких регулярных процедур для обнаружения угроз, в том числе из-за того, что не хотят привлекать лишнее внимание к уязвимостям системы.

Масштаб проблем с ИБ АСУ ТП  
Инциденты, уязвимости, мотивация

# Мир до и после Stuxnet



# Динамика обнаружения уязвимостей:



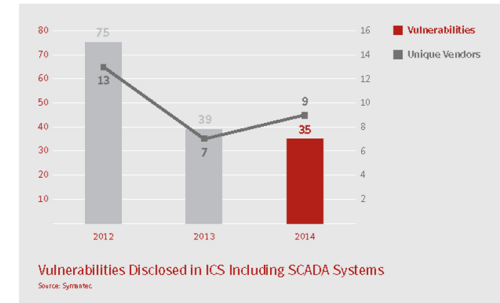
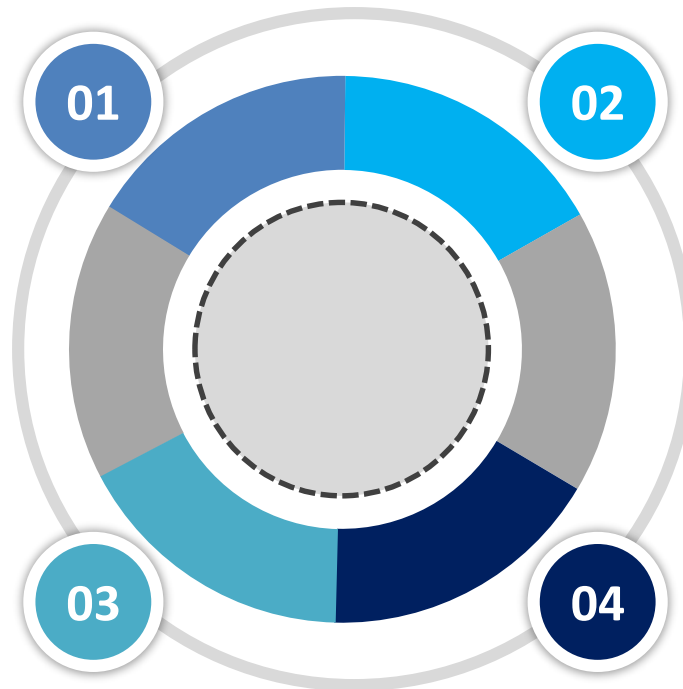
Динамика количества выявленных уязвимостей

[http://www.ptsecurity.ru/download/SCADA\\_analytics\\_russian.pdf](http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf)



Open-Source Vulnerability Database

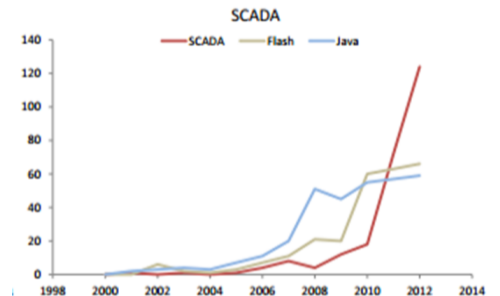
<http://osvdb.org/>



internet-security-threat-report Symantec

Internet-security-threat-report Symantec

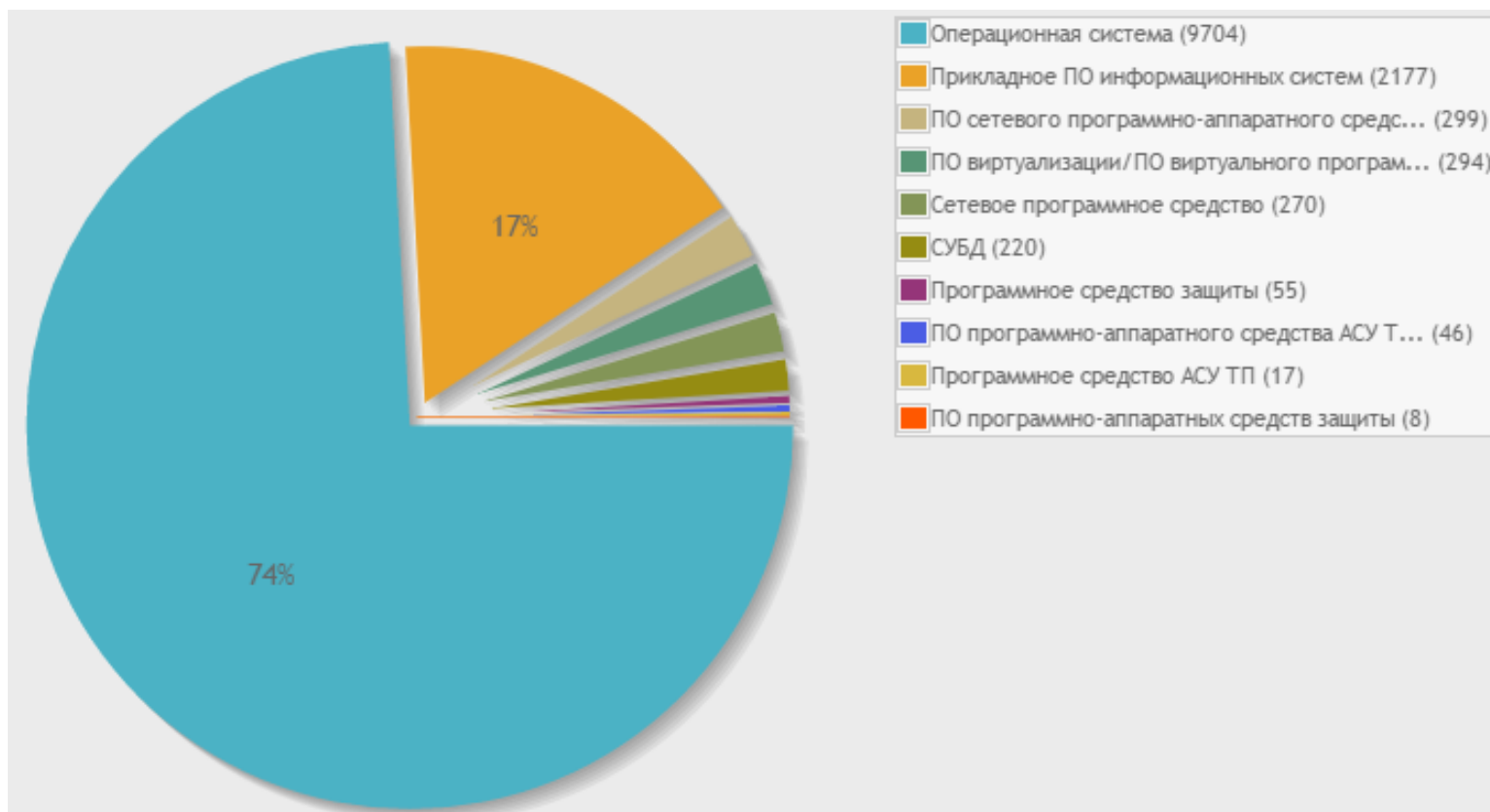
[https://www.symantec.com/content/en/us/enterprise/other\\_resources/21347933\\_GA\\_RPT-internet-security-threat-report-](https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-)



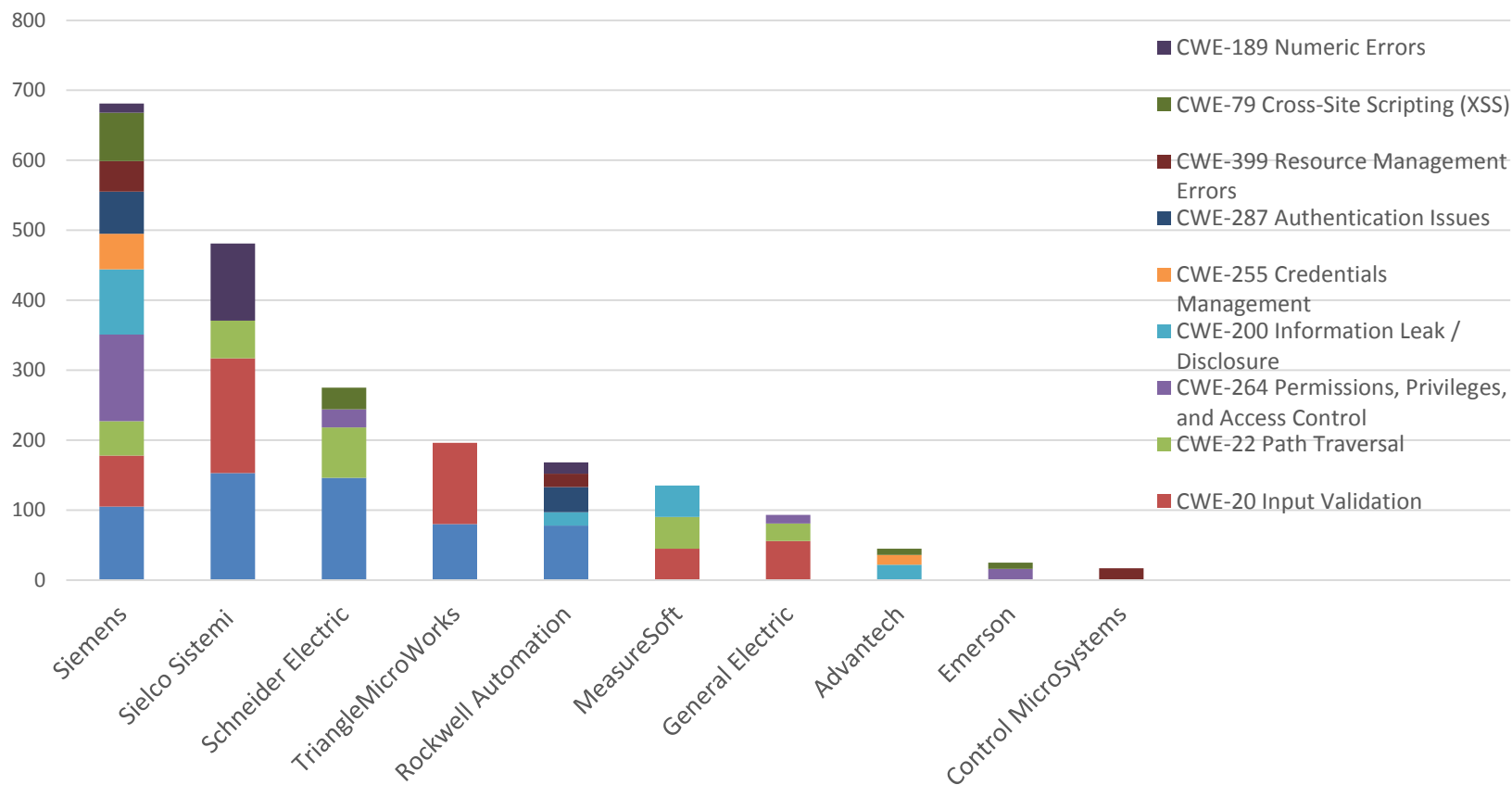
ANALYST BRIEF Vulnerability Threat Trends

<https://www.nsslabs.com>

# Банк данных угроз безопасности информации ФСТЭК России



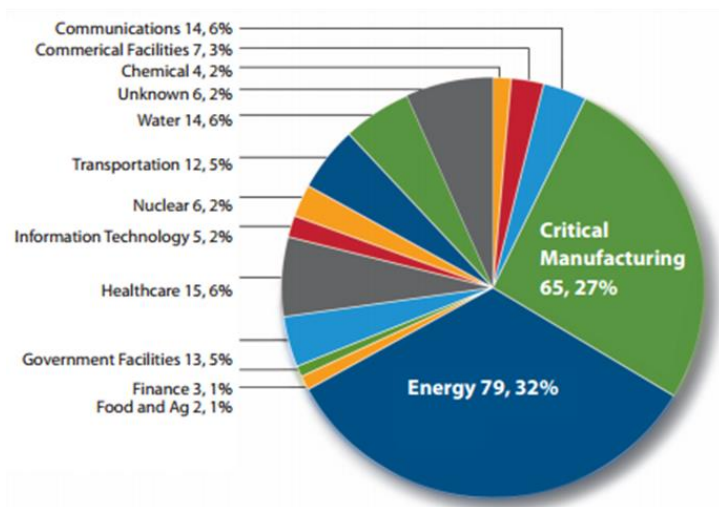
# Статистика уязвимостей 2015 год



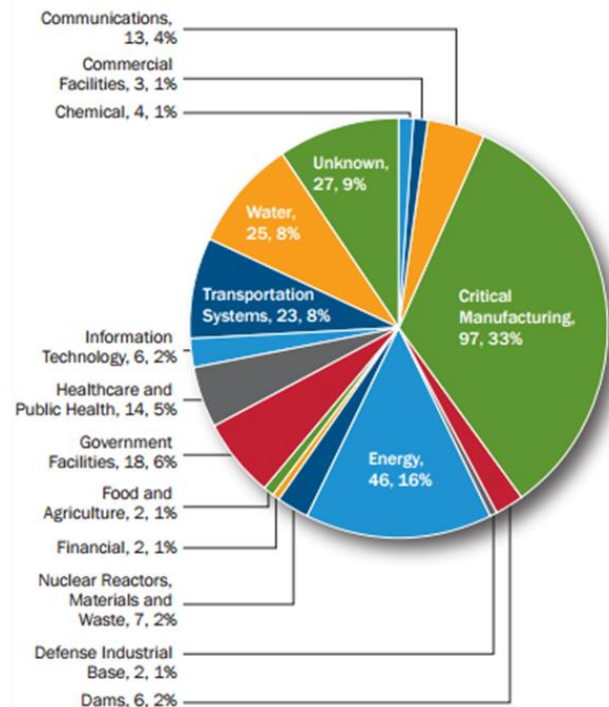
<https://web.nvd.nist.gov> –National Vulnerability Database

<http://www.toolswatch.org/wp-content/uploads/2015/11/ICSSCADA-Top-10-Most-Dangerous-Software-Weaknesses.pdf>

# Статистика инцидентов ICS-CERT USA



2014 год  
245 Инцидентов

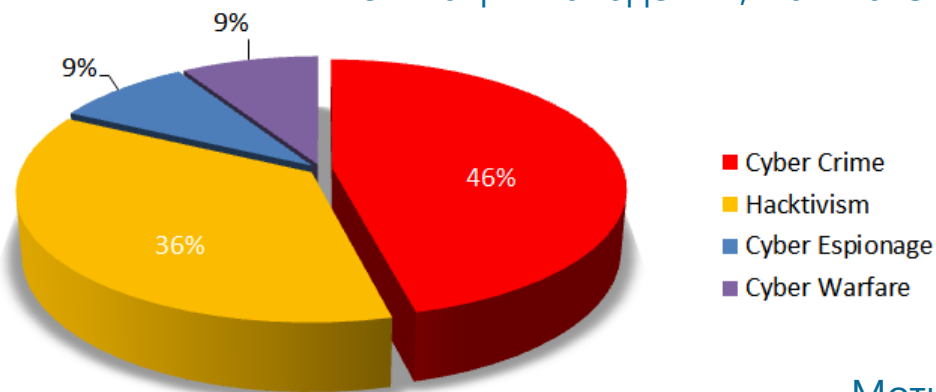


2015.  
295 Инцидентов

8 из которых привели к ущербу, превышающему 1 миллион долларов.

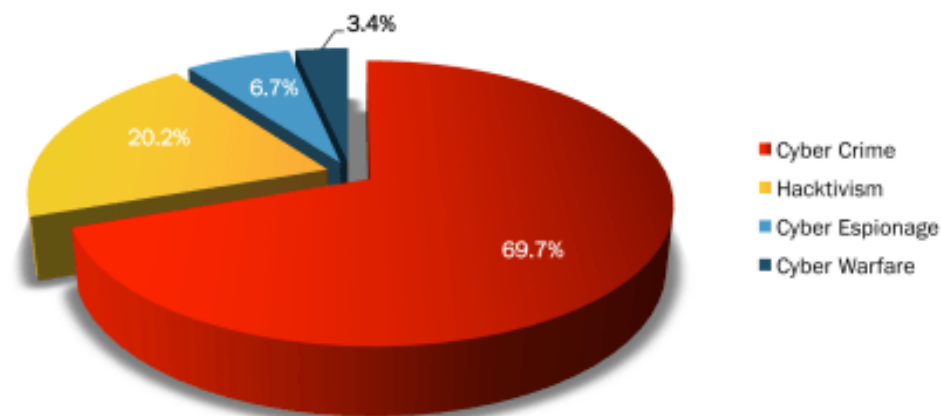
# Мотивация

Мотивация нападений, май 2013



Cyber Crime –  
быстрая монетизация  
преступлений

Мотивация нападений, ноябрь 2015



1,5 года

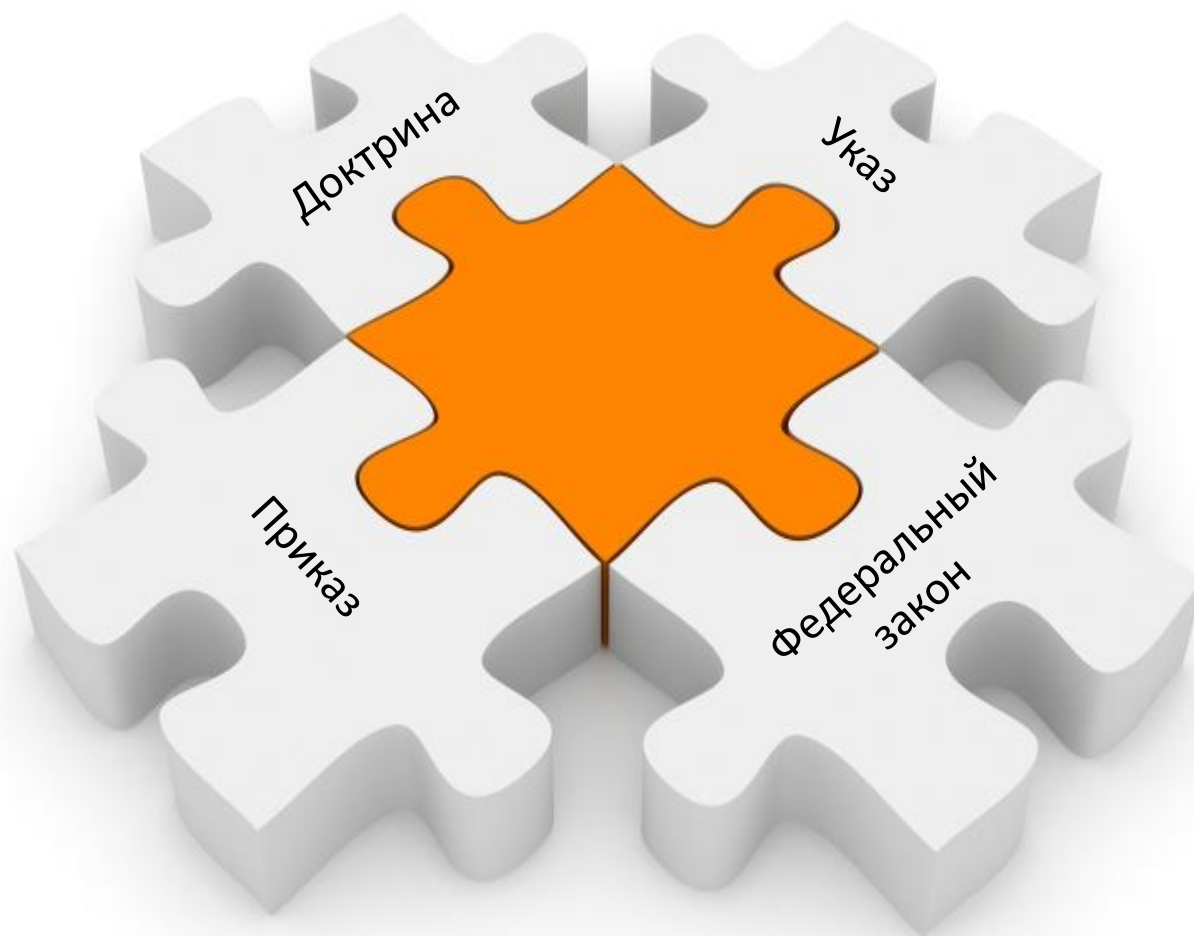
# Выводы:

- Традиционная преступность (киберкриминал) пришла в цифровой мир – это всерьез и надолго;
- Количество инцидентов, связанных с воздействием на информационные системы предприятий будет только возрастать;
- Построение современных систем ИБ АСУ требует нового взгляда:
  - Обеспечения юридической значимости обрабатываемой и хранимой информации;
  - Проектирование систем ИБ АСУ ТП с учетом возможности проведения криминалистического расследования (forensic investigation);
  - Внедрения цикла безопасной разработки .

# Нормативно-правовая база РФ



# Структура нормативно-правовых документов РФ:



Меры ЗИ в АСУ



Методика определения угроз безопасности информации в АСУ

**Проект  
2016**

Порядок выявления и устранения уязвимостей в АСУ



Порядок реагирования на инциденты, связанные с нарушением безопасности информации

# Планы ФСБ

Методика обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети



Порядок обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах

Порядок обмена информацией между федеральными органами исполнительной власти и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах

Методические рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак

# Выводы:

- Структура нормативно-правовой базы не однородна и требует доработки;
- Отрасль находится в ожидании «главного» федерального закона;
- Продолжится развития отраслевых стандартов, определяющих подход к ИБ в системах автоматизации.

# Решения ОАО «ИнфоТекС» по ЗИ АСУ ТП

# Отраслевые особенности СЗИ для АСУ ТП

- Особенности конструктивного исполнения;
- Функциональные особенности;
- Не функциональные особенности;
- Эксплуатационные особенности.

# Различные приоритеты в подходах ИБ

ОФИСНЫЕ  
РЕШЕНИЯ



Конфиденциальность  
Целостность  
Доступность

АСУ ТП



Доступность  
Целостность  
Конфиденциальность

# Решения ViPNet в индустриальном секторе

## ERP, MES

Системы управления  
предприятием

Системы планирования  
производства



ViPNet Network Security

ViPNet IDS

---

## Верхний уровень АСУ ТП

SCADA

АРМ оператора

Центры управления и  
мониторинга



ViPNet Network Security

ViPNet IDS

**ViPNet Coordinator IG**

**ViPNet SIES**

---

## Полевой уровень

ПЛК

Исполнительная среда



**ViPNet Coordinator IG**

**ViPNet SIES**

# Промышленный криптошлюз ViPNet Coordinator IG



Защищенный канал VPN с поддержкой L2overIP (до 10 Мбит/с)

Межсетевой экран

Индустриальное исполнение (-20<sup>0</sup>... +60<sup>0</sup>С, 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)

# Индустриальный криптомодуль ViPNet SIES



Встраиваемое решение (пассивный модуль)

Реализация криптоалгоритмов ГОСТ (шифрование, имитозащита, ЭП)

Управление ключами защиты

Доступ к криптографическим функциям через Modbus\*

Поддержка промышленных интерфейсов

Индустриальное исполнение (-40°... +60°С, IP66, промышленный диапазон питания)

# Линейка продуктов ViPNet SIES



ViPNet SIES Core



ViPNet SIES Pack

## Форм-фактор

SOM, 64x36 мм

Блочное исполнение с разъемами типа M12

## Процессор

ARM CORTEX M

ARM CORTEX M

## Интерфейсы

UART, SPI, I2C

Ethernet, RS-232, RS-485, CAN, USB,  
GSM/GPRS/EDGE/UMTS/HSPA, Wi-Fi

## Питание

4 ...17В DC, 0,7 Вт (при 5В)

9 ...36В, 18...36, 36...75 В DC; 3 Вт/5Вт (при 24В)

## Рабочая температура

-40...+75 °C

-40...+60 °C

# Сценарии применения продуктов ViPNet в промышленном сегменте


- Обеспечение конфиденциальности, целостности, аутентичности и неотъемлемости данных,
- Аутентификация и идентификация субъектов доступа и объектов доступа,
- Управление доступом (авторизация) субъектов доступа к объектам доступа,
- Доверенное обновление,
- Управление конфигурацией,
- Организация удаленного доступа, в том числе и с переносных технических средств,
- Обнаружение вторжений.

# Выводы:


- Формирование состава нормативно-правовой базы, регулирующей вопросы обеспечения информационной безопасности в АСУ ТП не завершено;
- В краткосрочной перспективе мотивация злоумышленников не поменяется, традиционная преступность будет закрепляться в киберпространстве.
- Создаваемые продукты ИБ должны удовлетворять всему множеству специфических особенностей систем автоматизации.

# Анонс вебинаров:

- Тема: «Решения ИнфоТеКС для обеспечения ИБ в АСУ ТП».  
Дата: 01.03.2016 с 10:00 до 11:00.
- Тема: «Программно-аппаратный комплекс ViPNet IDS».  
Дата: 10.03.2016 с 10:00 до 11:00.

A sunset scene with wind turbines and power lines. The sky is filled with orange and yellow clouds, and the sun is low on the horizon. In the foreground, several wind turbines are silhouetted against the bright sky. In the background, a series of power lines and towers stretch across the landscape. The overall atmosphere is warm and serene.

Давайте  
пообщаемся!

A large industrial facility, possibly a refinery or chemical plant, is shown at night. The scene is illuminated by numerous bright lights, highlighting various towers, pipes, and structures. In the foreground, there is a semi-transparent white box containing text. To the right of the text box, there are two hard hats: one yellow and one white. Below the text box, there are some office supplies like a pen and a calculator on a desk.

# Введение в тему индустриальной безопасности

**Карантаев Владимир / к.т.н. / Менеджер  
Отдел научных исследований и развития продуктов  
[Vladimir.Karantaev@infotecs.ru](mailto:Vladimir.Karantaev@infotecs.ru)**