«Обеспечение информационной безопасности объектов энергетического комплекса РФ»

Открытая лекция
Казанский Государственный Энергетический Университет



О себе



Карантаев Владимир Геннадьевич

Кандидат технических наук, член «РНК СИГРЭ»

Менеджер

Отдел развития продуктов ОАО «ИнфоТеКС»

Руководитель РГ 4 D2 РНК СИГРЭ

Практический опыт работы в области ИБ: 8 лет.

Практический опыт работы в области ИТ: 14 лет.

Опыт преподавания: 8 лет.

skype: karantaev1980

Vladimir.karantaev@infotecs.ru

©2016, ОАО «ИнфоТеКС».

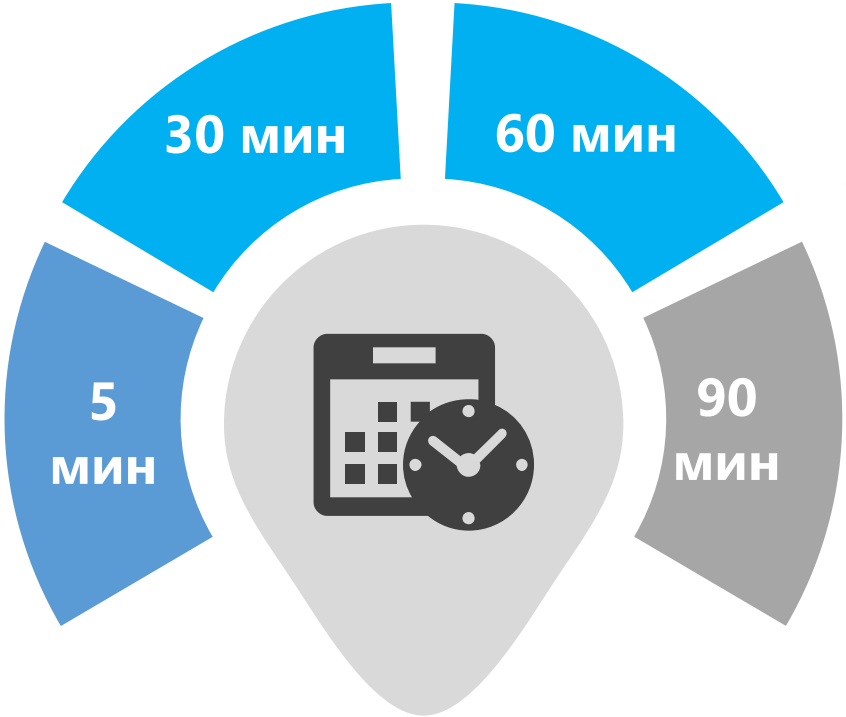
Регламент



Значимые инциденты

ИБ сегодня

Приветствие



Анализ текущего состояния ИБ АСУ ТП

Практическая безопасность

Ответы на вопросы

Комментарии

©2016, ОАО «ИнфоТеКС».

Информационная безопасность сегодня



Информационная безопасность - это

ОФИСНЫЕ РЕШЕНИЯ



Конфиденциальность
Целостность
Доступность

АСУ ТП



Доступность
Целостность
Конфиденциальность

©2016, ОАО «ИнфоТеКС».

Информационная безопасность сегодня

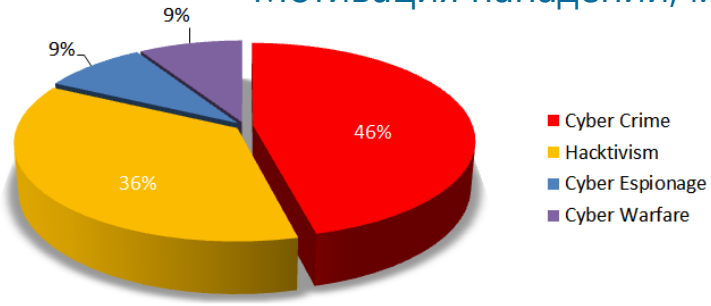


https://www.fireeye.com/cyber-map/threat-map.html

©2016, ОАО «ИнфоТеКС».

Мотивация нападений

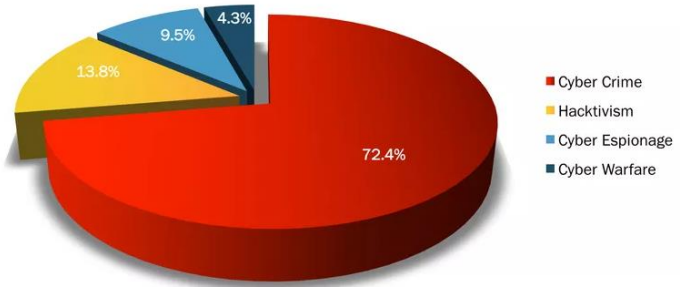
Мотивация нападений, май 2013



Cyber Crime –
быстрая монетизация
преступлений

3 года

Мотивация нападений, август 2016



http://www.hackmageddon.com/

©2016, ОАО «ИнфоТеКС».

Экономика киберпреступности



http://www.bmstu.ru/master/news/?newsid=3558

©2016, ОАО «ИнфоТеКС».

Что мы привыкли защищать?







©2016, ОАО «ИнфоТеКС».

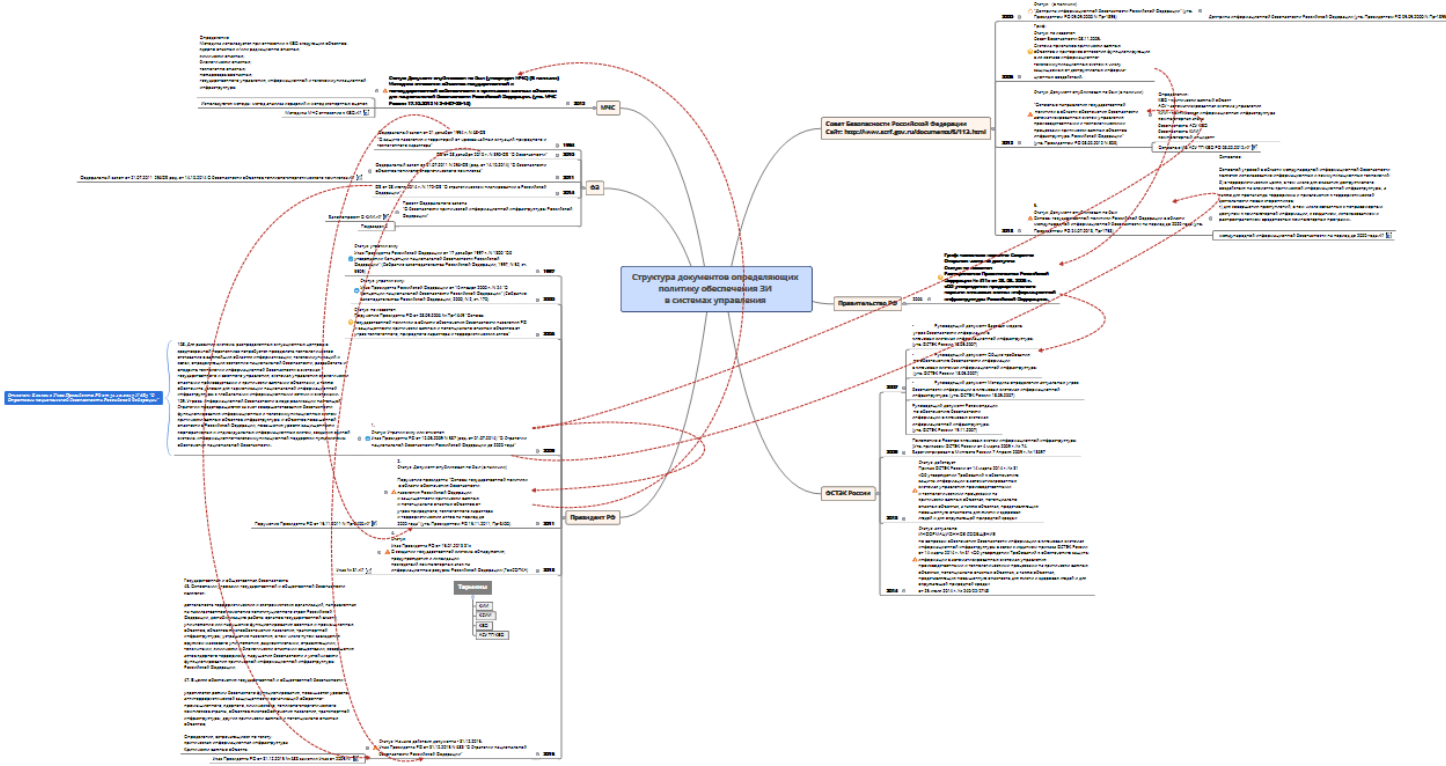
Необычные объекты защиты





©2016, ОАО «ИнфоТеКС».

Структура нормативно-правовых документов РФ



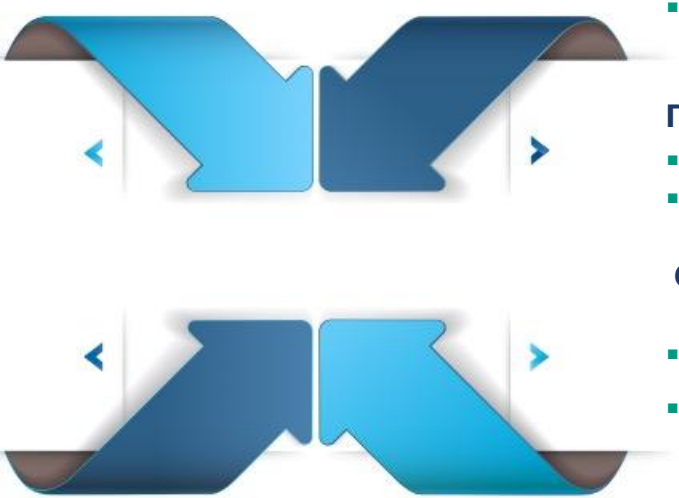
Регулирование ИБ АСУ ТП

Федеральные законы:

- ФЗ от 21 июля 2011 г. N 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» Статья 11

Документы ФСТЭК :

- Приказ ФСТЭК России от 14.03.2014 N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления ...»
- Документы КСИИ
- Требования к межсетевым экранам



Документы ФСБ:

- Проект Открытых требований к СКЗИ

ГОСТ:

- ГОСТ Р МЭК 62443-2-1-2015
- ГОСТ Р 56205-2014 (ISO / IEC 62443-2-1

Отраслевые стандарты:

- СТО РЖД 02.049-2014
- Проект СТО ПАО «Россети» «ВСЗИ»

©2016, ОАО «ИнфоТеКС».

Возможные последствия инцидентов ИБ



©2016, ОАО «ИнфоТеКС».

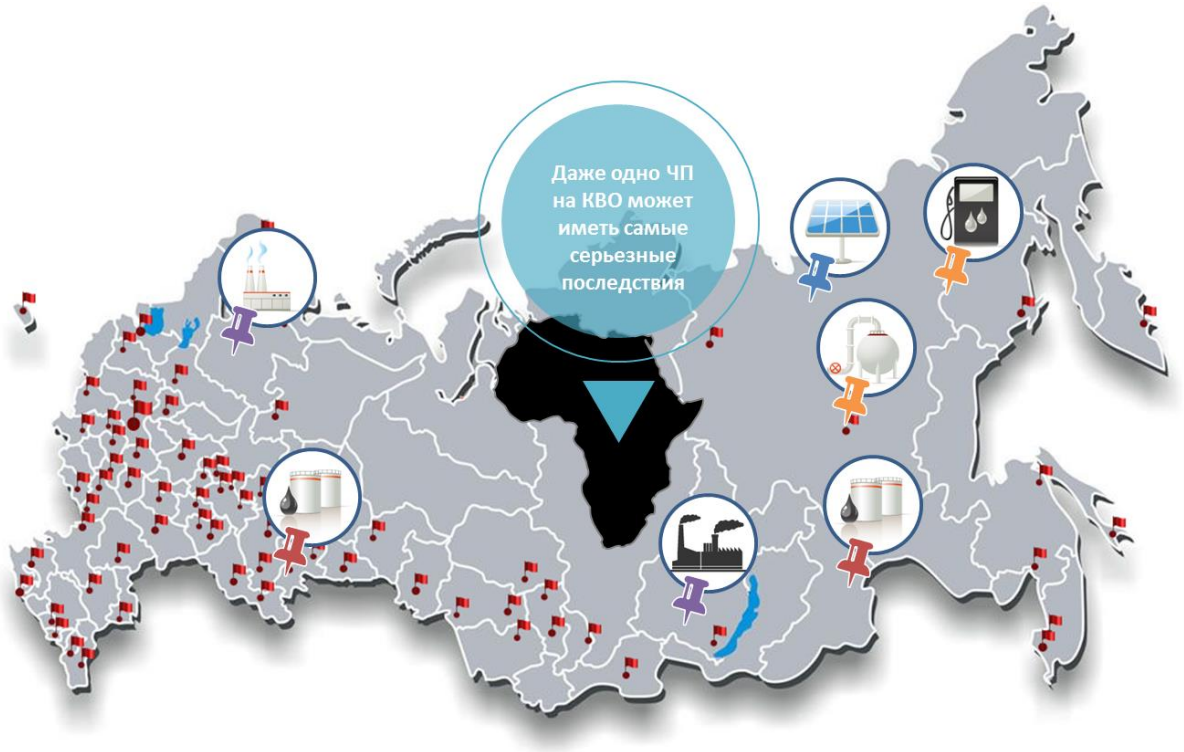
А такие последствия возможны?





©2016, ОАО «ИнфоТеКС».

Может быть хуже...



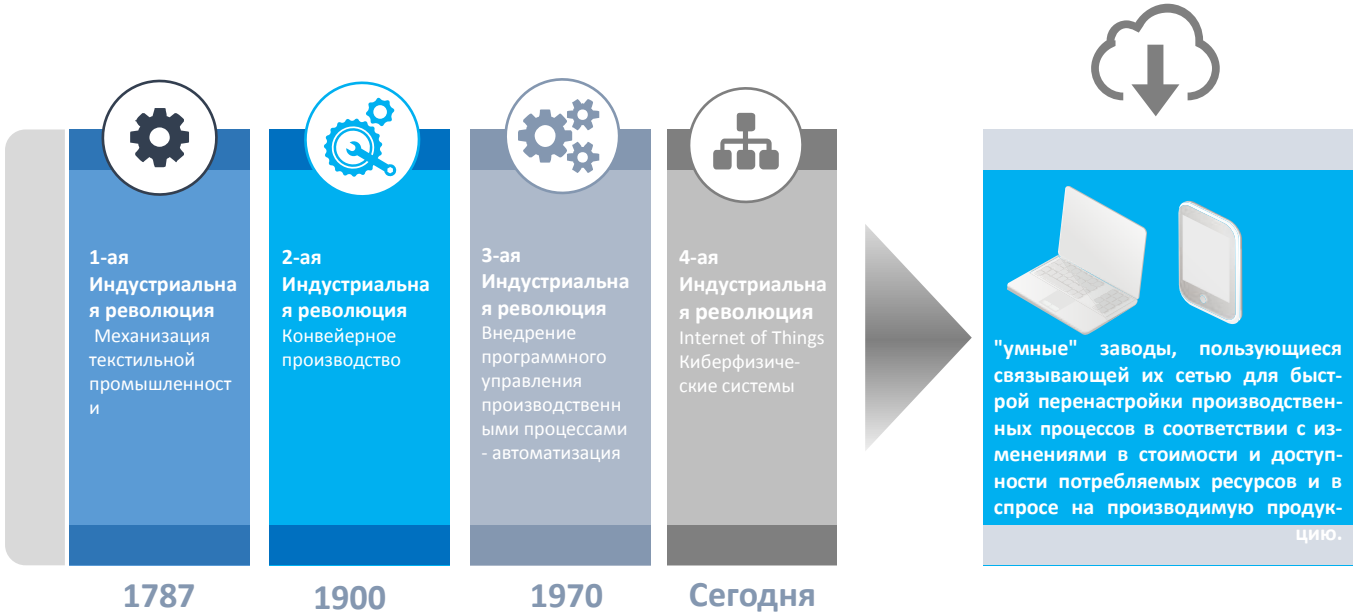
©2016, ОАО «ИнфоТеКС».

©2016, ОАО «ИнфоТеКС».

Тенденции развития



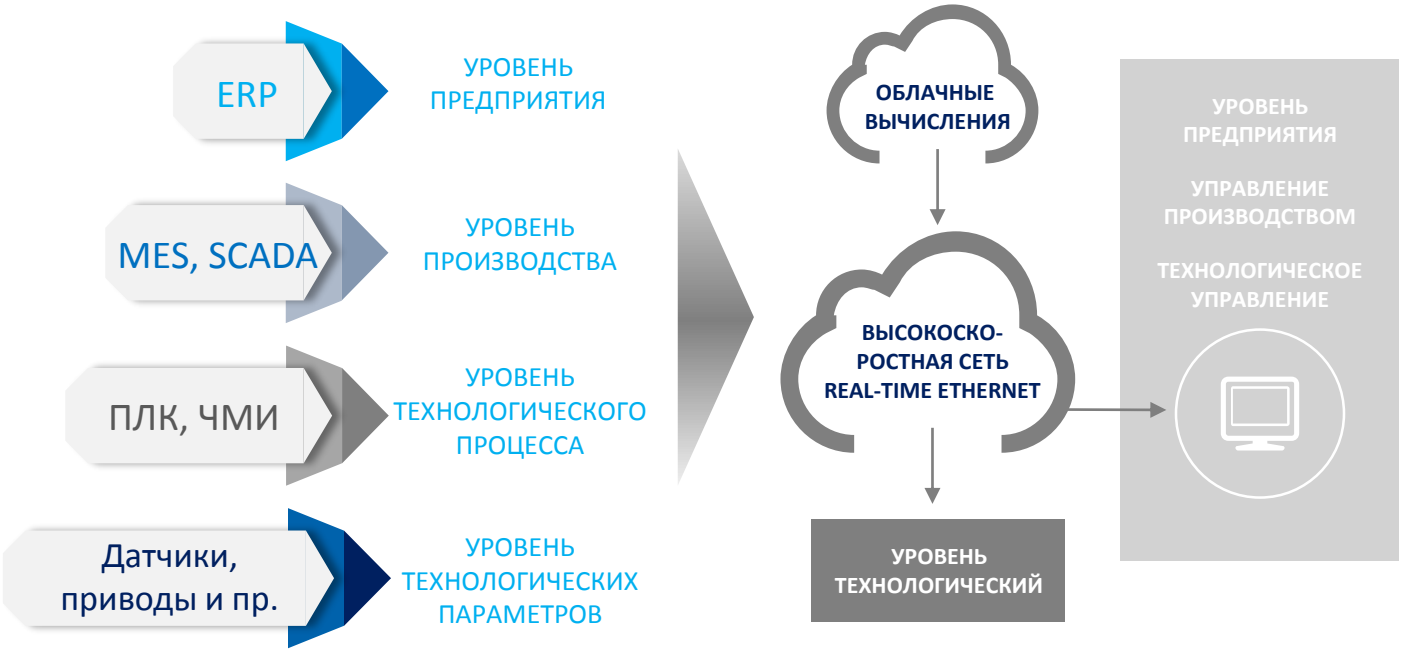
Четвертая индустриальная революция



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

©2016, ОАО «ИнфоТеКС».

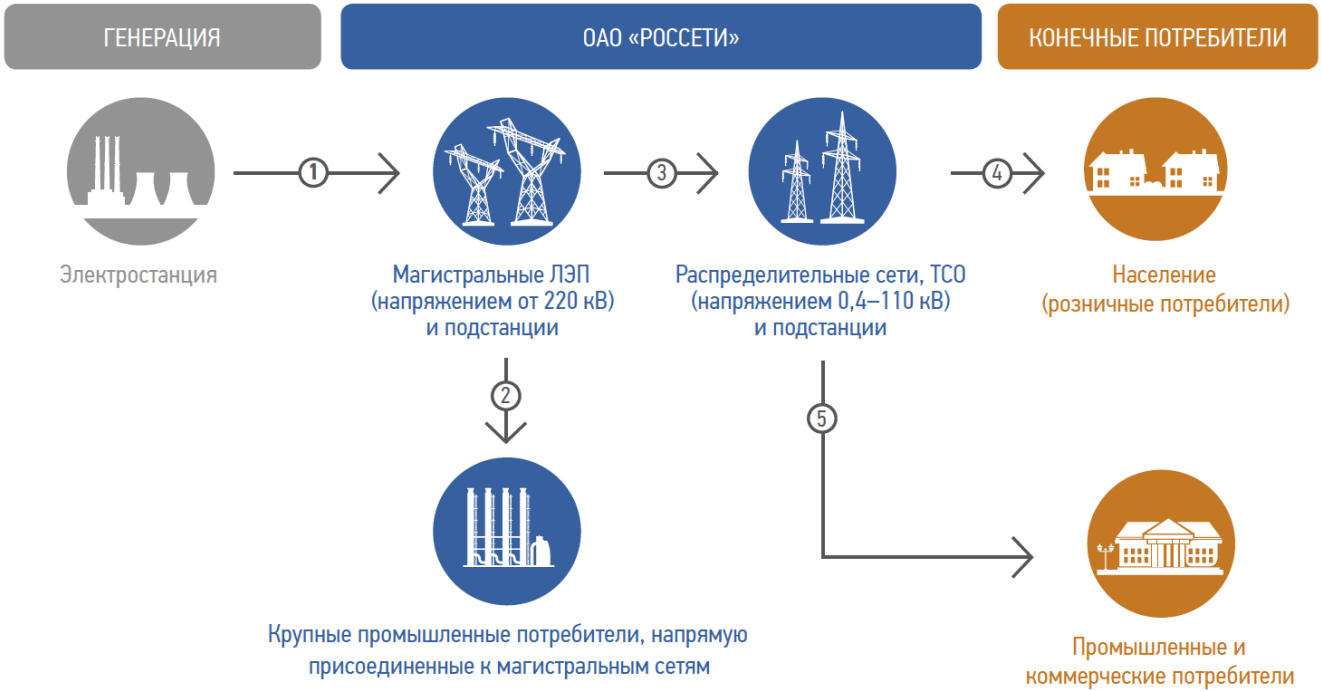
Тенденции развития АСУ ТП



©2016, ОАО «ИнфоТеКС».
©2016, ОАО «ИнфоТеКС».

Путь поставки электроэнергии

Путь поставки электроэнергии



©2016, ОАО «ИнфоТеКС».

Перспективные направления развития ЕЭС РФ

- Внедрение технологий Smart Grid.
- Внедрение нового управляемого силового оборудования в ААС.
- Внедрение цифровых ПС с учетом развития цифровой обработки.



«Концепция развития релейной защиты и автоматики электросетевого комплекса», Россети, 2015

©2016, ОАО «ИнфоТеКС».

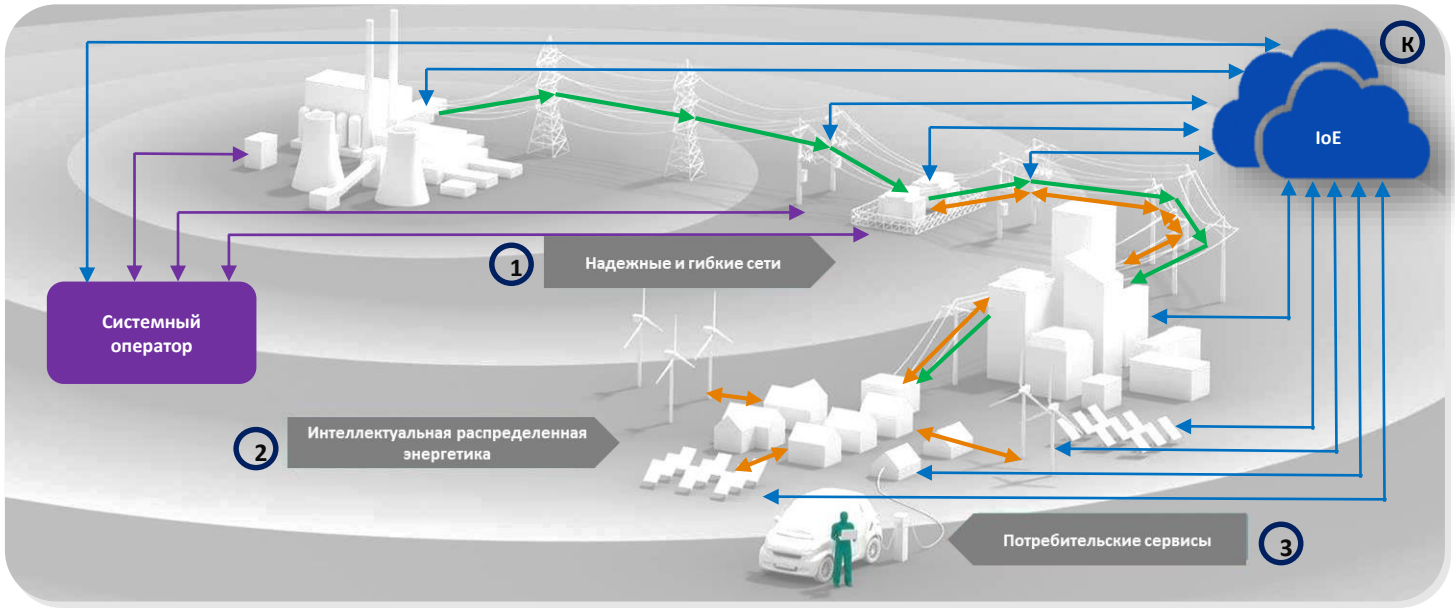
Планомерное развитие ЕЭС РФ

- Внедрение подстанций нового поколения.
- Развитие автоматизированных систем технологического управления (АСТУ).
- Переход к необслуживаемым подстанциям.



©2016, ОАО «ИнфоТеКС».

Архитектура рынков Energynet



Энергетические потоки

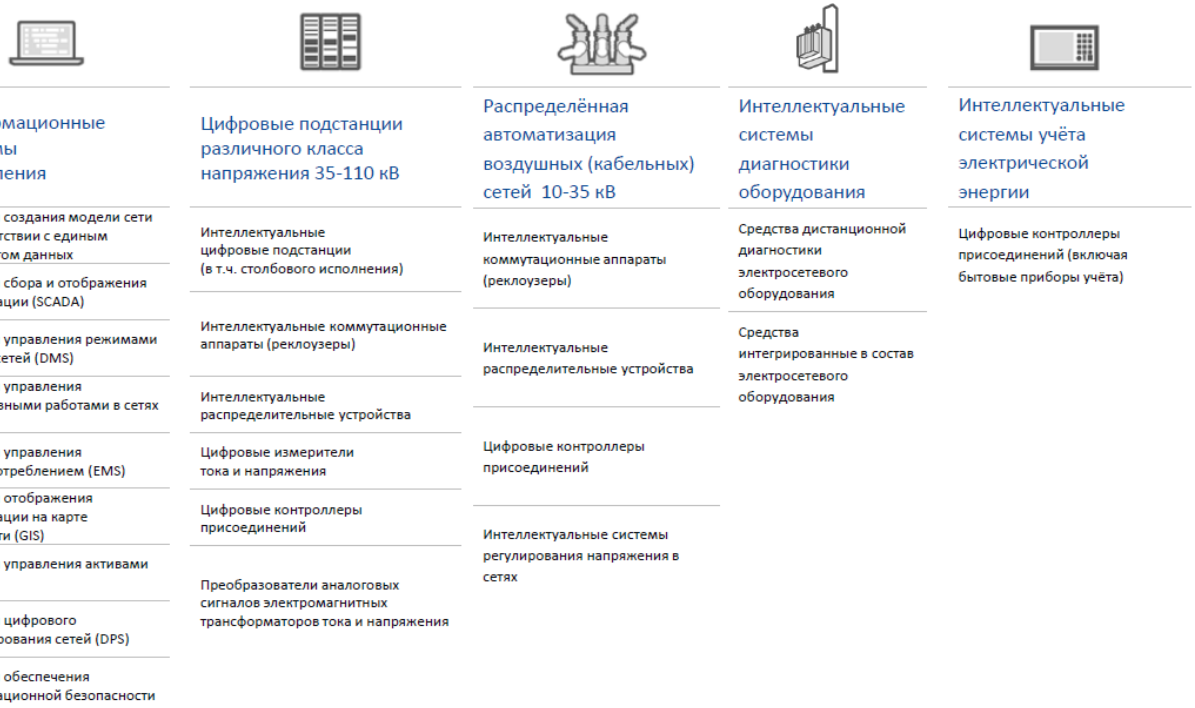
«как есть» «как будет»

Информационные потоки

«как есть» «как будет»

©Владислав ВОРОТНИЦКИЙ «Таврида Электрик» ©2016, ОАО «ИнфоТеКС».

Технологии Energynet : «Надёжные и гибкие сети».



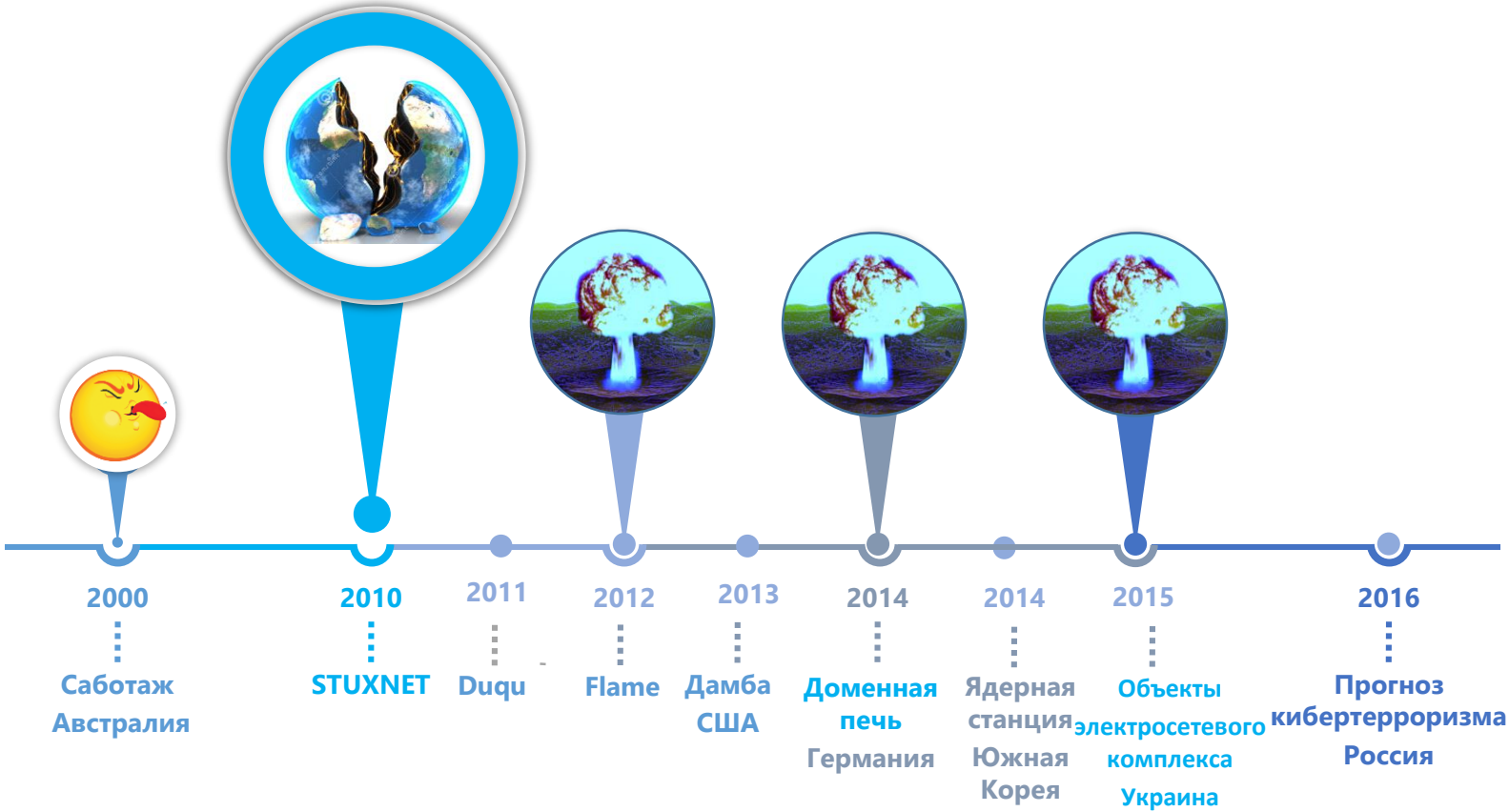
*Проекты первой волны (преимущественно на существующих технологиях)

©Владислав ВОРОТНИЦКИЙ «Таврида Электрик» ©2016, ОАО «ИнфоТеКС».

Инциденты ИБ

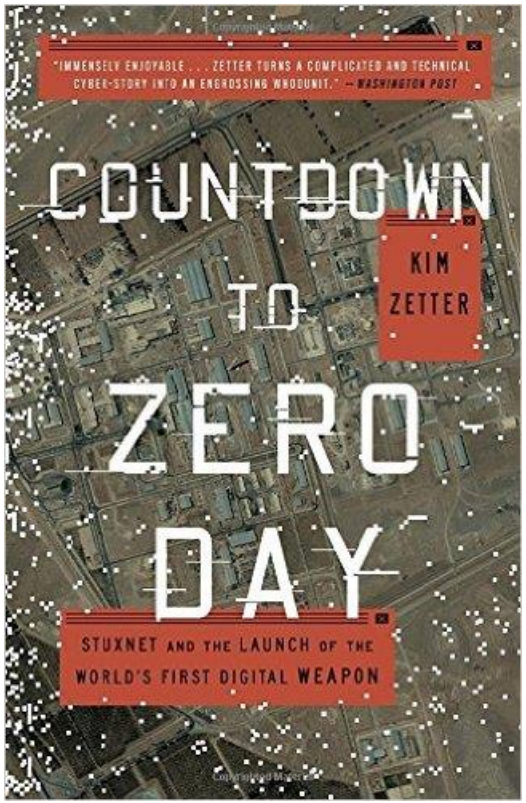


Мир до и после Stuxnet



©2016, ОАО «ИнфоТеКС».

Десятилетие со Stuxnet



https://www.amazon.com/dp/0770436196/ref=rdr_ext_tmb

«Обратный отсчет» — это удачная попытка подняться выше строчек кода, свести воедино все, что известно о первой и по сей день наиболее масштабной специализированной атаке на индустриальные системы.

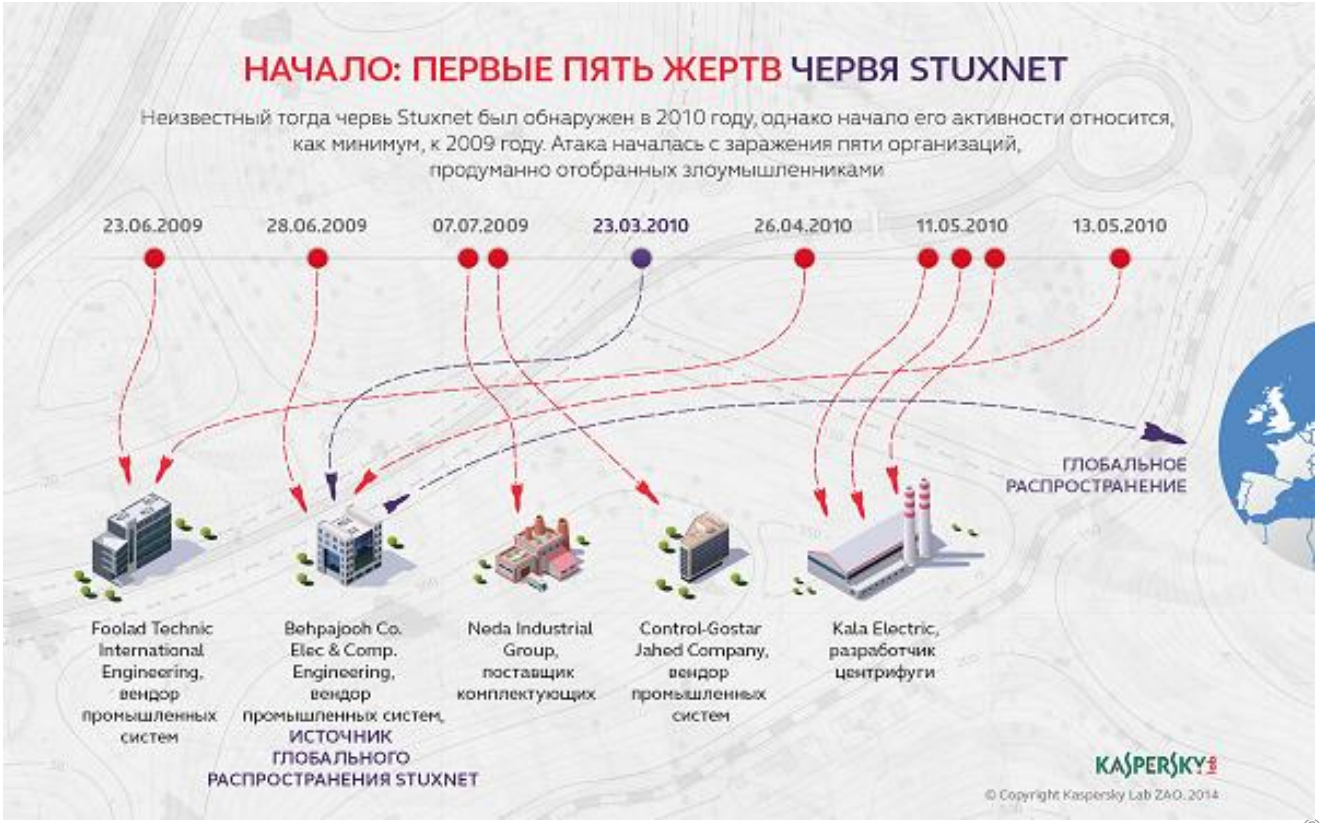
https://habrahabr.ru/company/kaspersky/blog/310398/

С момента обнаружения Stuxnet прошло шесть лет, семь — с момента начала атаки, больше десяти, предположительно, с начала разработки.

https://habrahabr.ru/company/kaspersky/blog/310398/

©2016, ОАО «ИнфоТеКС».

Исследование Лаборатории Касперского



https://habrahabr.ru/company/kaspersky/blog/310398/

©2016, ОАО «ИнфоТеКС».

Последователи Stuxnet: Duqu и Flame



©2016, ОАО «ИнфоТеКС».

RISI Online Incident Database

Industrial Security Incidents Database (ISID) – создана в 2001, в рамках исследовательского проекта.

В 2008 году получил дальнейшее развития в рамках проекта по созданию:

«Repository of Industrial Security Incidents (RISI)».

С 2009 года проект находится под управлением: **Security Incidents Organization™.**

Источники обновления данных:

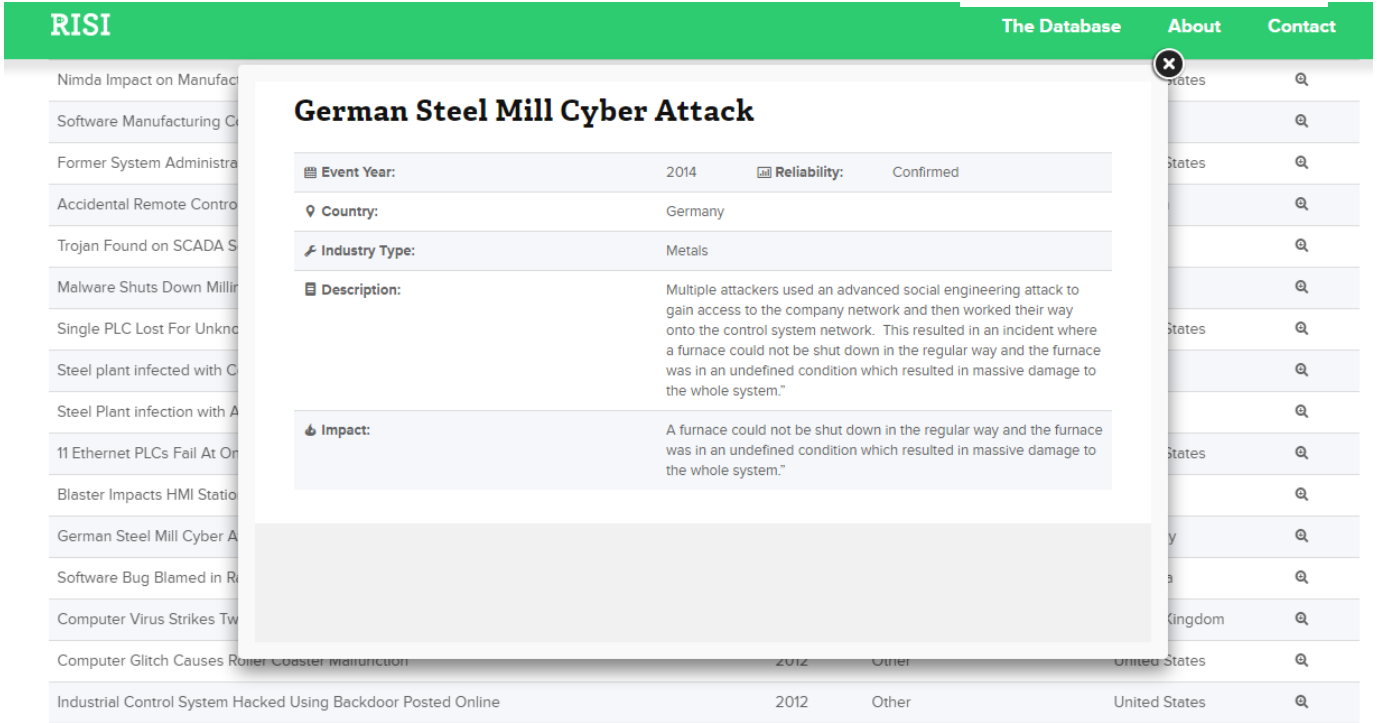
- Участники Security Incidents Organization™
- Общедоступные источники
- Стратегические партнеры, например, **International Information Sharing and Analysis Centers (ISACs).**

http://www.risidata.com/Database

©2016, ОАО «ИнфоТеКС».

RISI Online Incident Database

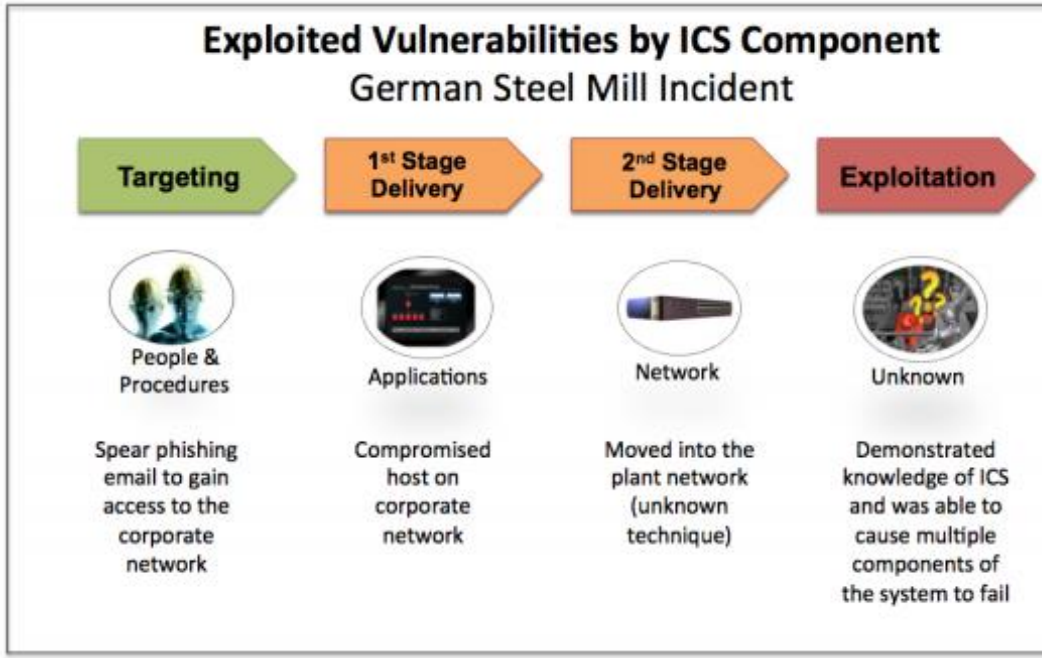
База данных инцидентов содержит около 270 записей.



http://www.risidata.com/Database

©2016, ОАО «ИнфоТеКС».

Атакован металлургический завод в Германии 2014



SANS Industrial Control Systems

ICS Defense Use Case (DUC) Dec 30, 2014

Authors:

Robert M. Lee
Michael J. Assante
Tim Conway

ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper –
German Steel Mill Cyber Attack

Note: We are providing a summary of the available information and are basing the details of the incident on the publicly available report. Open-source data gathered throughout 2014 regarding incidents can reveal information about the potential identity of the facility in question. However, the identity of the facility was not released and in an effort to protect the privacy of those involved none of the other open-source information will be presented in this report. The identity of the facility and specific process are not important to establishing lessons-learned.

Incident Summary

https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

©2016, ОАО «ИнфоТеКС».

Киберинцидент в Энергосистеме Украины



SANS ICS Industrial Control Systems

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

TLP: White

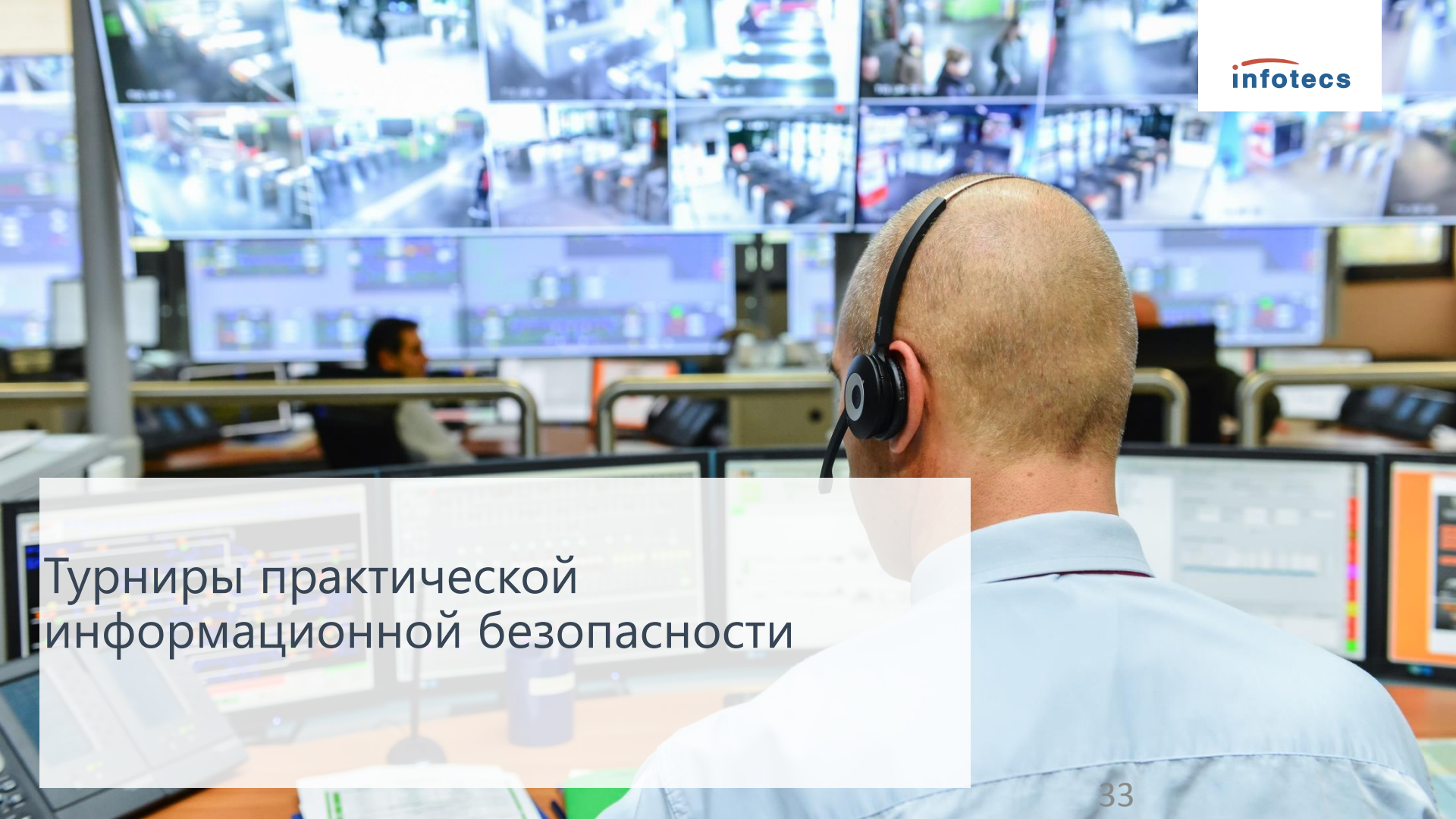
Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

March 18, 2016

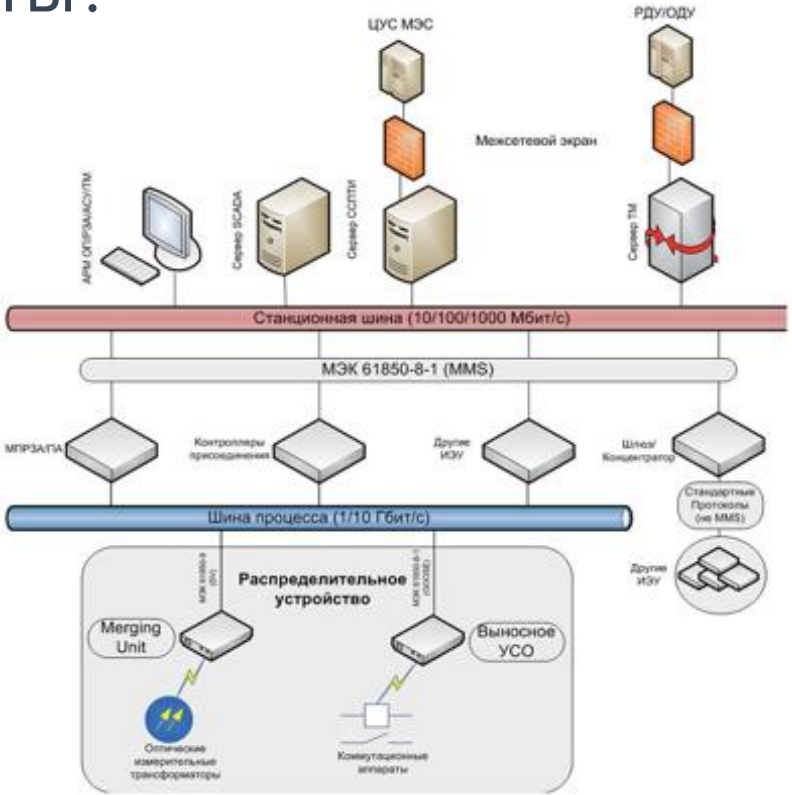
https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

©2016, ОАО «ИнфоТеКС».



Турниры практической информационной безопасности

«Цифровая подстанция»
Объект защиты?



©2016, ОАО «ИнфоТеКС».

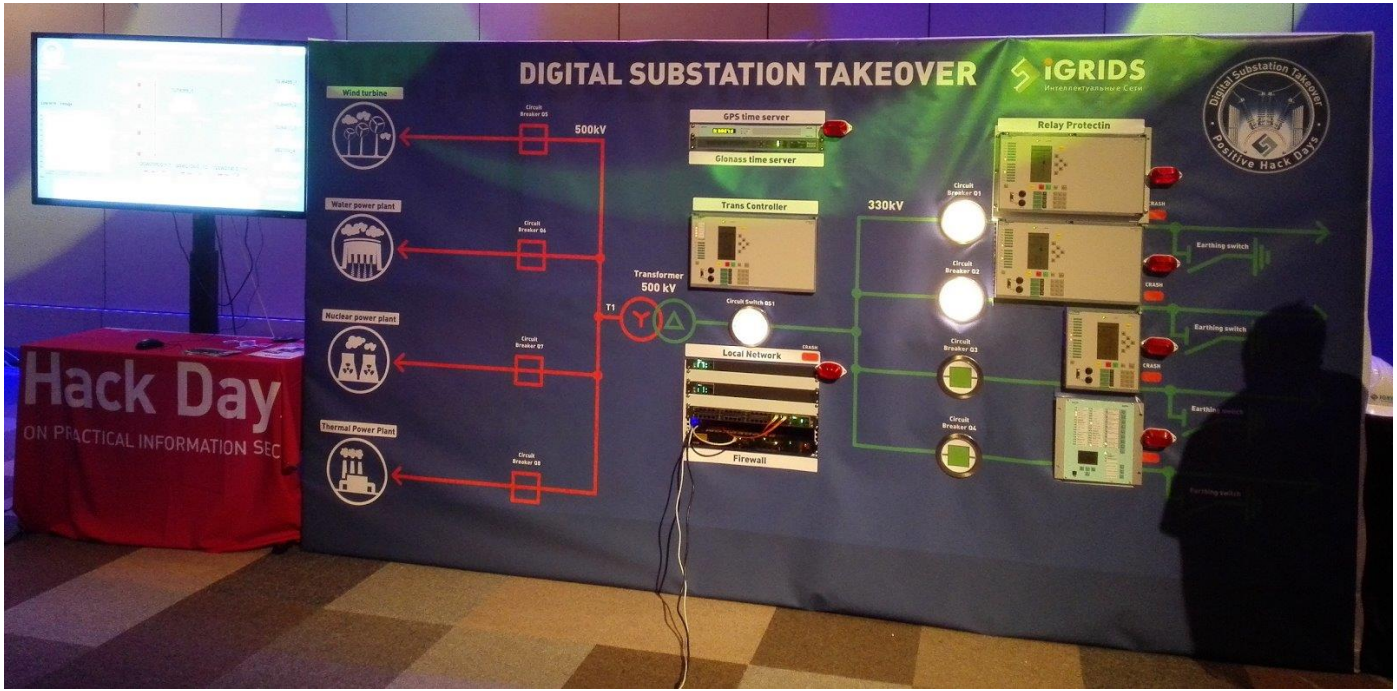
Конкурсы по практической безопасности



http://digitalsubstation.ru/blog/2015/10/29/kiberbezopasnost-asu-tp-kaspersky-industrial-cybersecurity/

©2016, ОАО «ИнфоТеКС».

PHDaysV
Цифровая подстанция



https://habrahabr.ru/company/pt/blog/259905/

©2016, ОАО «ИнфоТеКС».

PHDaysVI:Standoff



http://igrids.ru/news.php?id=34 Максим Никандров

©2016, ОАО «ИнфоТеКС».

"Кибербезопасность АСУ ТП 2016: Время действовать вместе! 11.10.2016 Иннополис

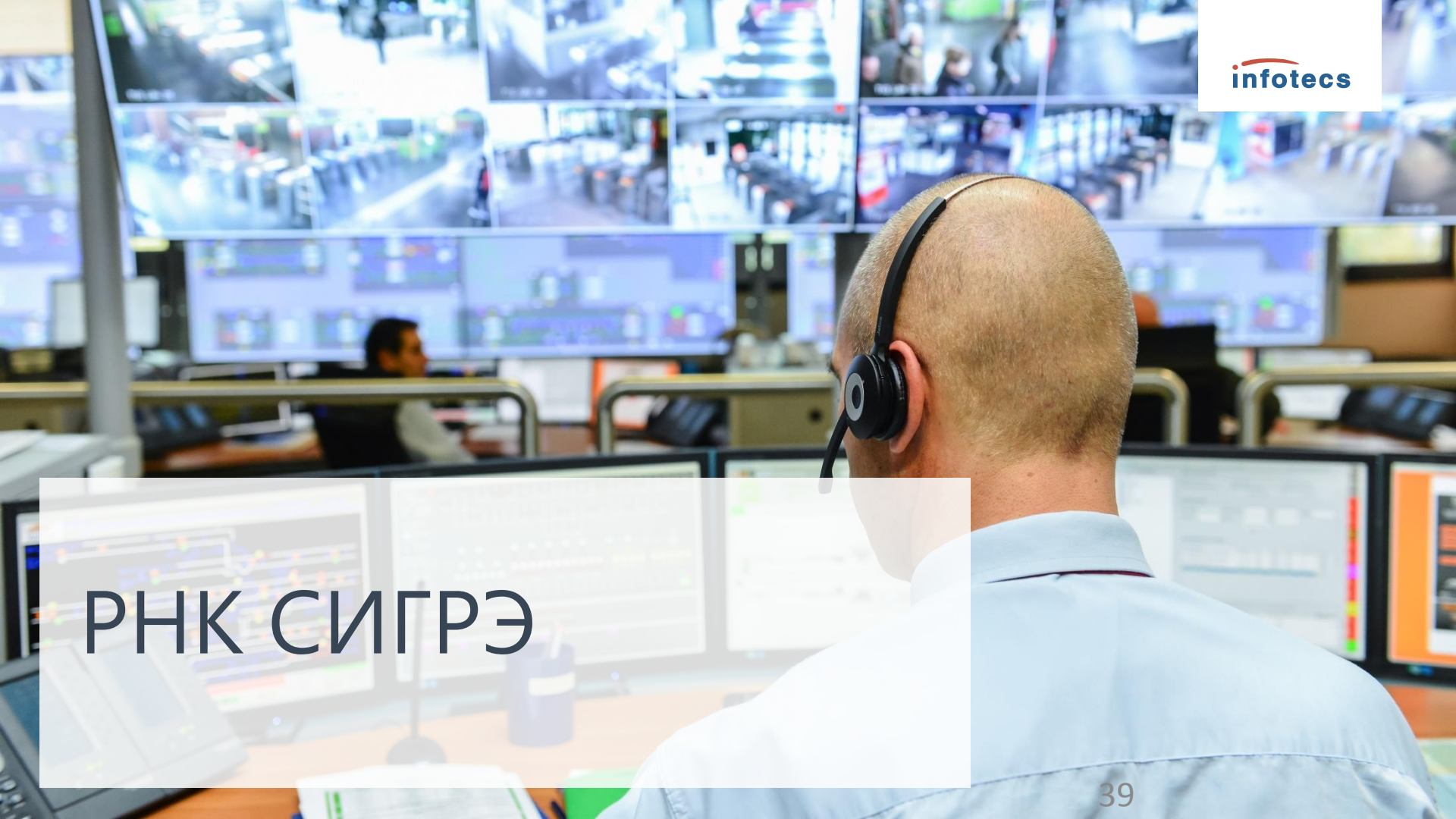


Киберфизическая модель Micro Grid



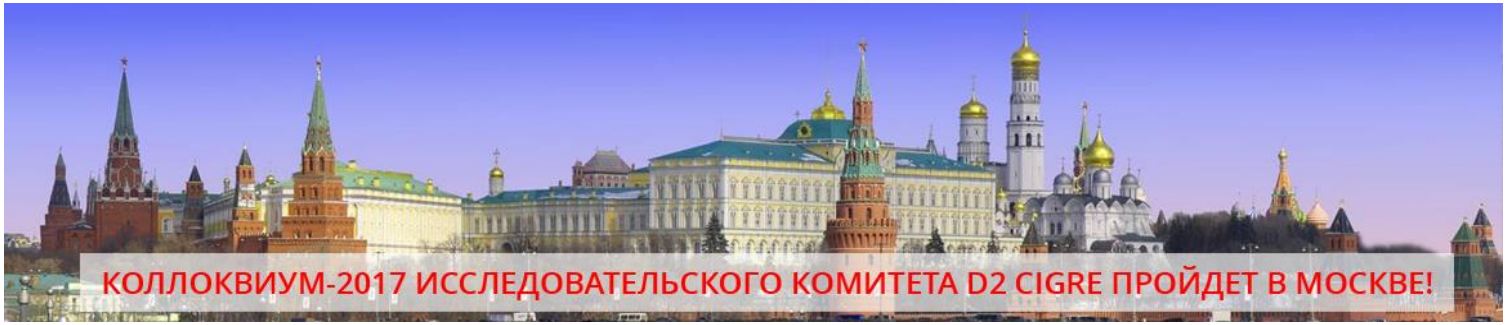
Исследователи за работой

©2016, ОАО «ИнфоТеКС».



РНК СИГРЭ

D2 РНК СИГРЭ



Устойчивость к киберугрозам информационных и телекоммуникационных систем в электроэнергетике.

- Безопасность систем управления распределенной генерацией (DER).
- Облачные вычисления и технологии IoT: границы применения с точки зрения информационной безопасности.
- Сертификация информационных систем и телекоммуникаций на устойчивость к киберугрозам.
- Инструменты моделирования угроз и мер информационной безопасности.

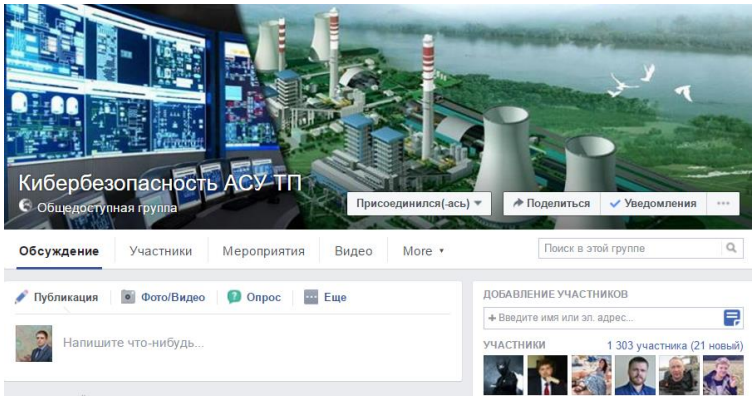
©2016, ОАО «ИнфоТеКС».

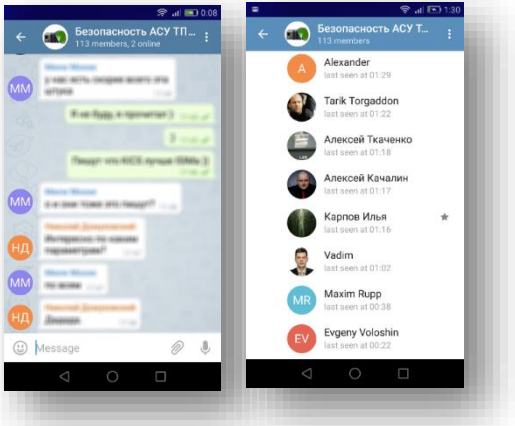
Работа экспертных групп

- Проблемная рабочая группы «Кибербезопасность РЗА и систем управления современных объектов электроэнергетики» (ПРГ-2 D2/B5);
- Рабочая группа «Обеспечение информационной безопасности для систем связи и управления в электроэнергетике» подкомитета D2 «Информационные системы и телекоммуникации»;
- Молодежная секция РНК СИГРЭ

©2016, ОАО «ИнфоТеКС».

Профессиональные сообщества в социальных сетях





facebook.com/groups/RusCyberSec

telegram.me/RuScadaSec

©2016, ОАО «ИнфоТеКС».