

«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

Регламент



Значимые
инциденты

30 мин

60 мин



Анализ текущего
состояния ИБ АСУ
ТП



ИБ сегодня

5
МИН

90
МИН



Практическая
безопасность



Приветствие



Ответы на
вопросы
Комментарии

Информационная безопасность сегодня

NETWORK
SEARCH



DECODING

010101 3001 R0H 010



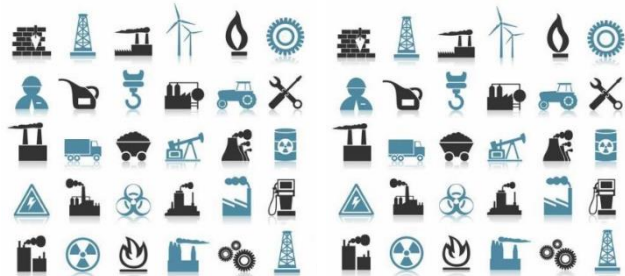
Информационная безопасность - это

ОФИСНЫЕ
РЕШЕНИЯ



Конфиденциальность
Целостность
Доступность

АСУ ТП



Доступность
Целостность
Конфиденциальность



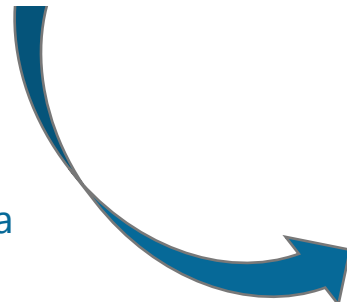
Мотивация нападений

Мотивация нападений, май 2013

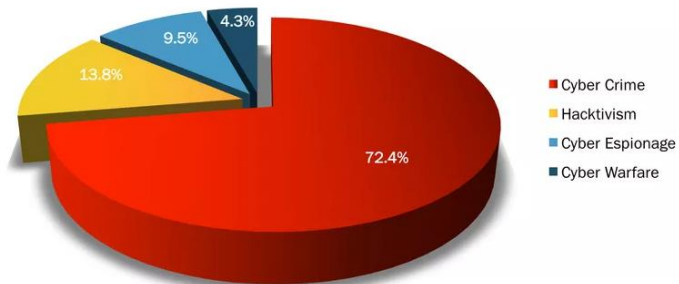


Cyber Crime – быстрая монетизация преступлений

3 года



Мотивация нападений, август 2016



Экономика киберпреступности



Что мы привыкли защищать?



НЕ БОЛТАЙ!



Мне это нравится!

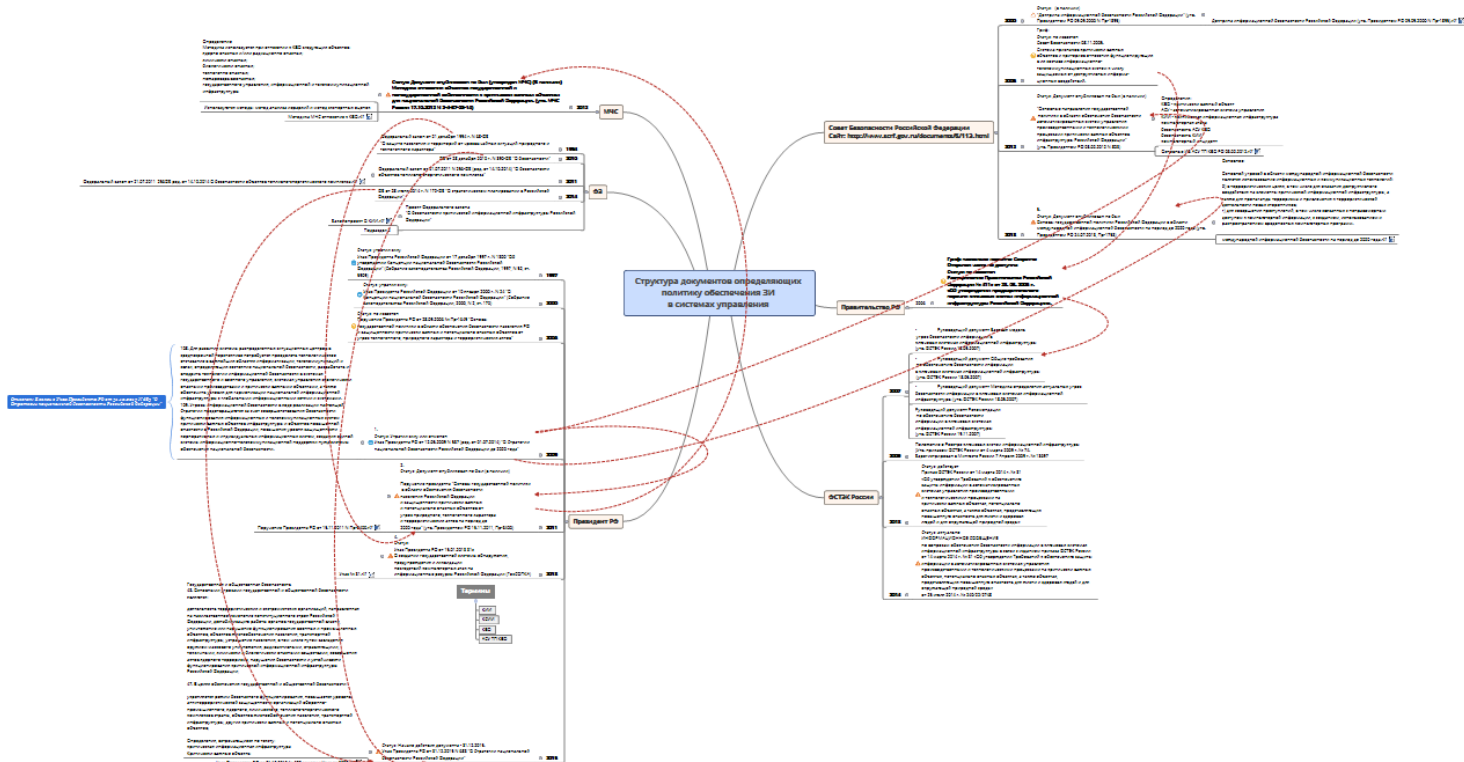


UC Browser

Необычные объекты защиты



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:

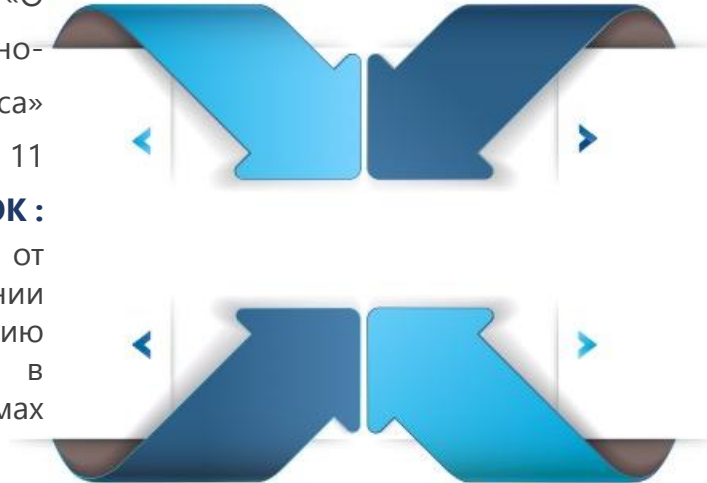
- Проект Открытых требований к СКЗИ

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»



Возможные последствия инцидентов ИБ



А такие последствия возможны?



Может быть хуже...



Тенденции развития



NETWORK
SEARCH



NEW GREAT PRODS BY NEW GREAT SHER
BY GREAT PRODS
RECOMMENDATION
RECOMMENDATION
BY NEW



NEW GREAT PRODS BY NEW GREAT SHER
BY GREAT PRODS
RECOMMENDATION
RECOMMENDATION
BY NEW



NEW GREAT PRODS BY NEW GREAT SHER
BY GREAT PRODS
RECOMMENDATION
RECOMMENDATION
BY NEW



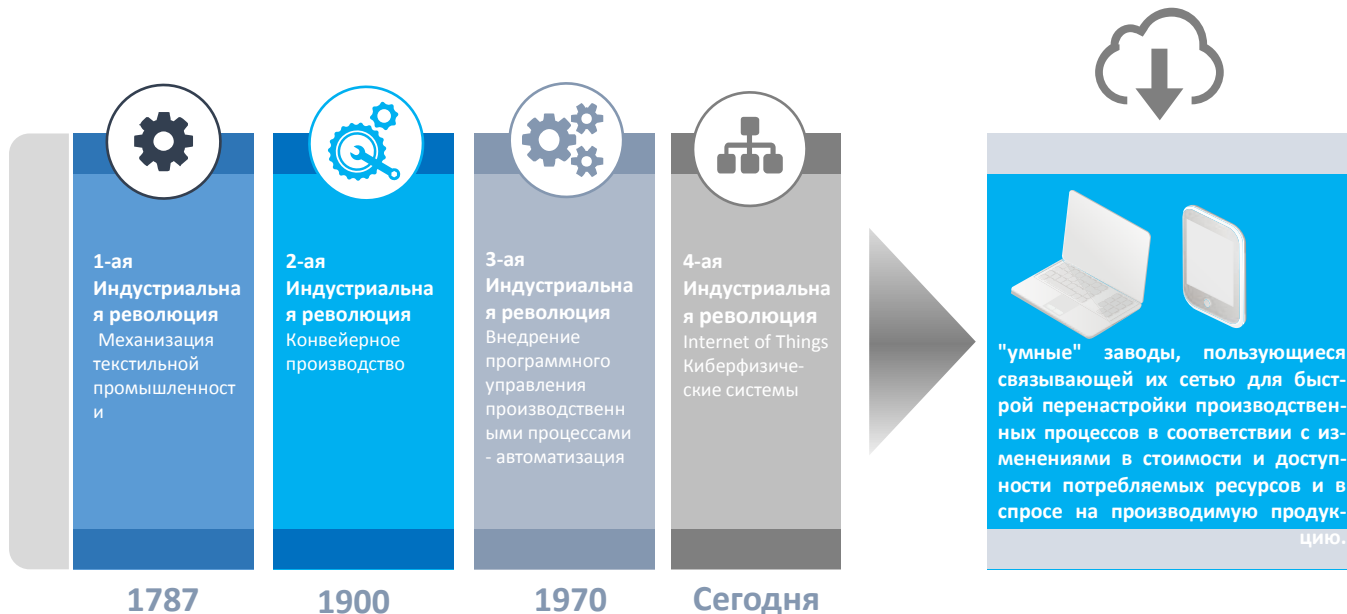
NEW GREAT PRODS BY NEW GREAT SHER
BY GREAT PRODS
RECOMMENDATION
RECOMMENDATION
BY NEW

DECODING

010101 3001 R0H 010

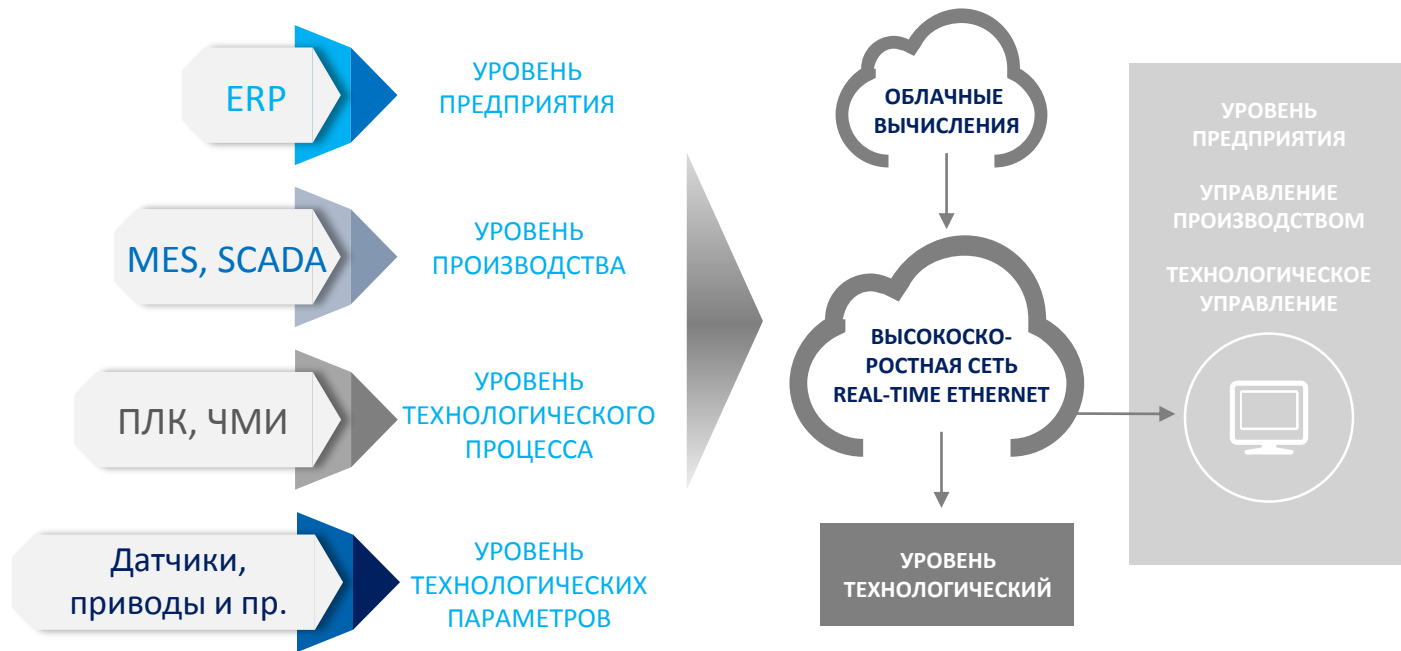


Четвертая индустриальная революция



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

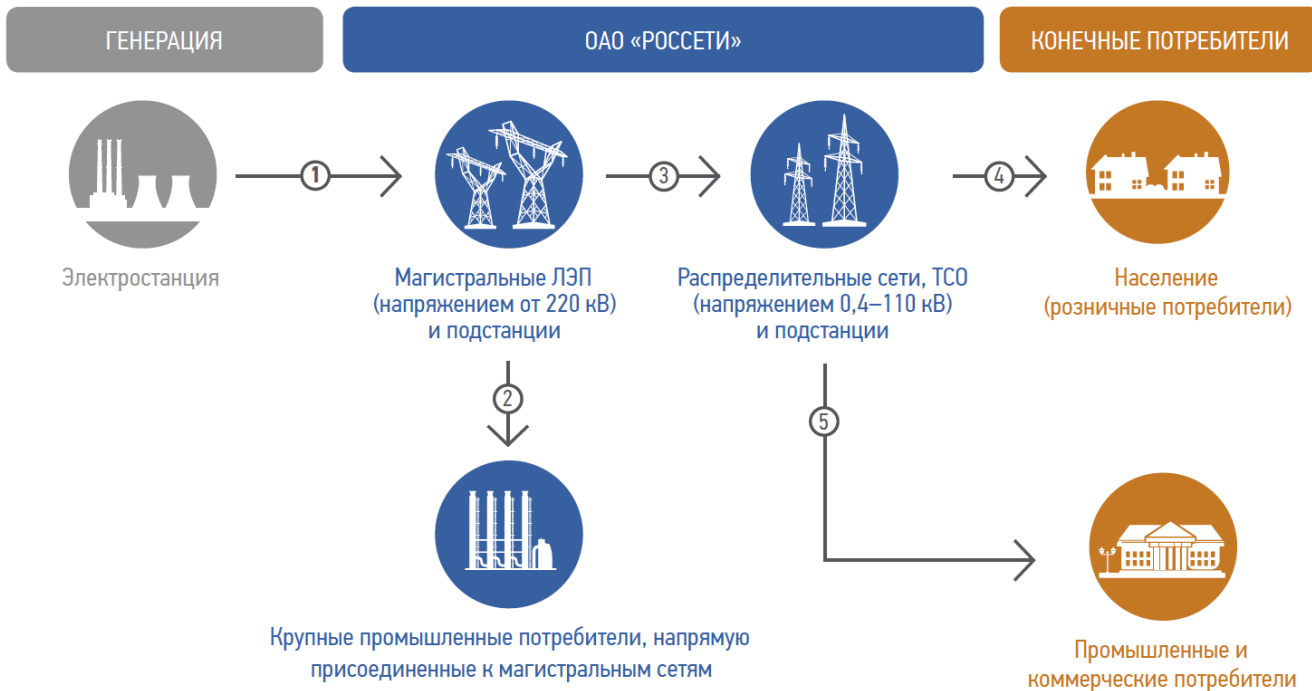
Тенденции развития АСУ ТП



Путь поставки электроэнергии



Путь поставки электроэнергии



Перспективные направления развития ЭЭС 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

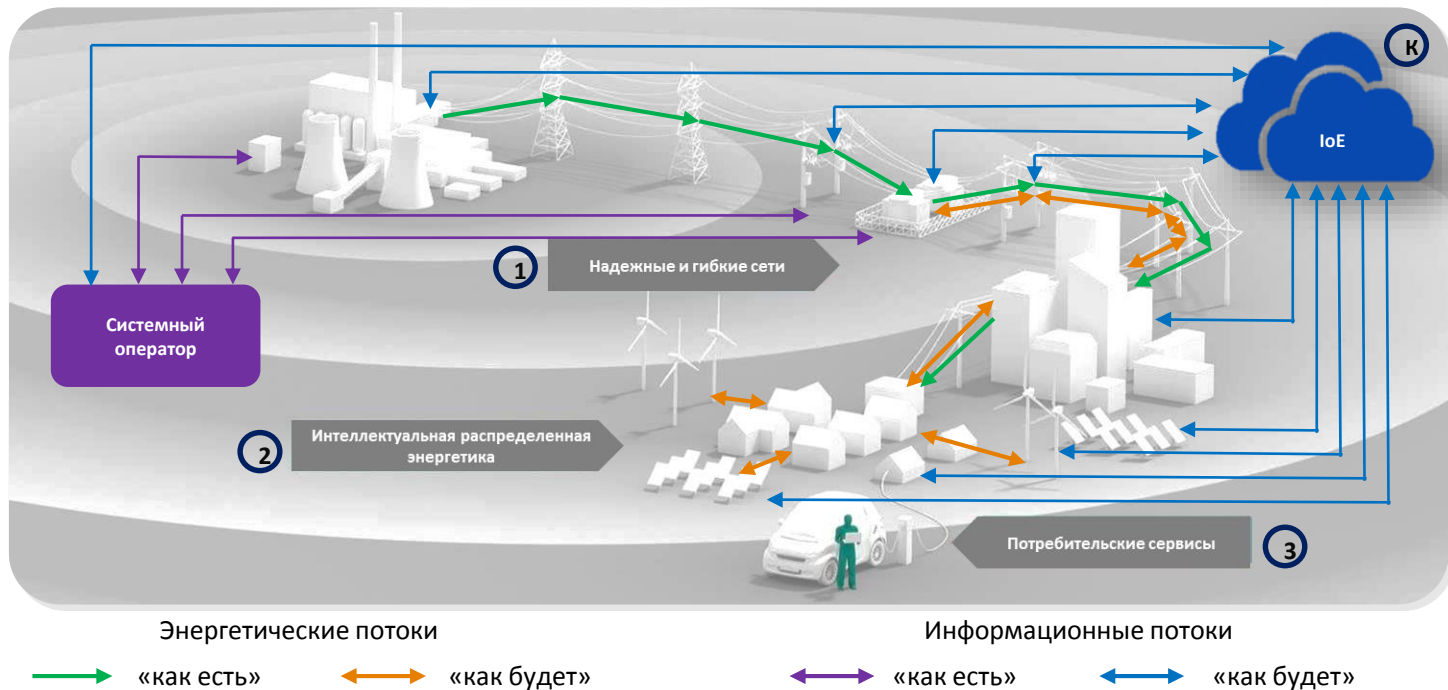
Планомерное развитие ЕЭС РФ



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



Архитектура рынков Energynet



Технологии Energynet : «Надёжные и гибкие сети».



Информационные системы управления

Системы создания модели сети в соответствии с единым стандартом данных

Системы сбора и отображения информации (SCADA)

Системы управления режимами работы сетей (DMS)

Системы управления оперативными работами в сетях (OMS)

Системы управления энергопотреблением (EMS)

Системы отображения информации на карте местности (GIS)

Системы управления активами (AMS)

Системы цифрового проектирования сетей (DPS)

Системы обеспечения информационной безопасности

2017*



Цифровые подстанции различного класса напряжения 35-110 кВ

Интеллектуальные цифровые подстанции (в т.ч. столбового исполнения)

Интеллектуальные коммутационные аппараты (реклоузеры)

Интеллектуальные распределительные устройства

Цифровые измерители тока и напряжения

Цифровые контроллеры присоединений

Преобразователи аналоговых сигналов электромагнитных трансформаторов тока и напряжения

2017*



Распределённая автоматизация воздушных (кабельных) сетей 10-35 кВ

Интеллектуальные коммутационные аппараты (реклоузеры)

Интеллектуальные распределительные устройства

Цифровые контроллеры присоединений

Интеллектуальные системы регулирования напряжения в сетях

2017*



Интеллектуальные системы диагностики оборудования

Средства дистанционной диагностики электросетевого оборудования

Средства интегрированные в состав электросетевого оборудования

2018*



Интеллектуальные системы учёта электрической энергии

Цифровые контроллеры присоединений (включая бытовые приборы учёта)

2017*



Инциденты ИБ

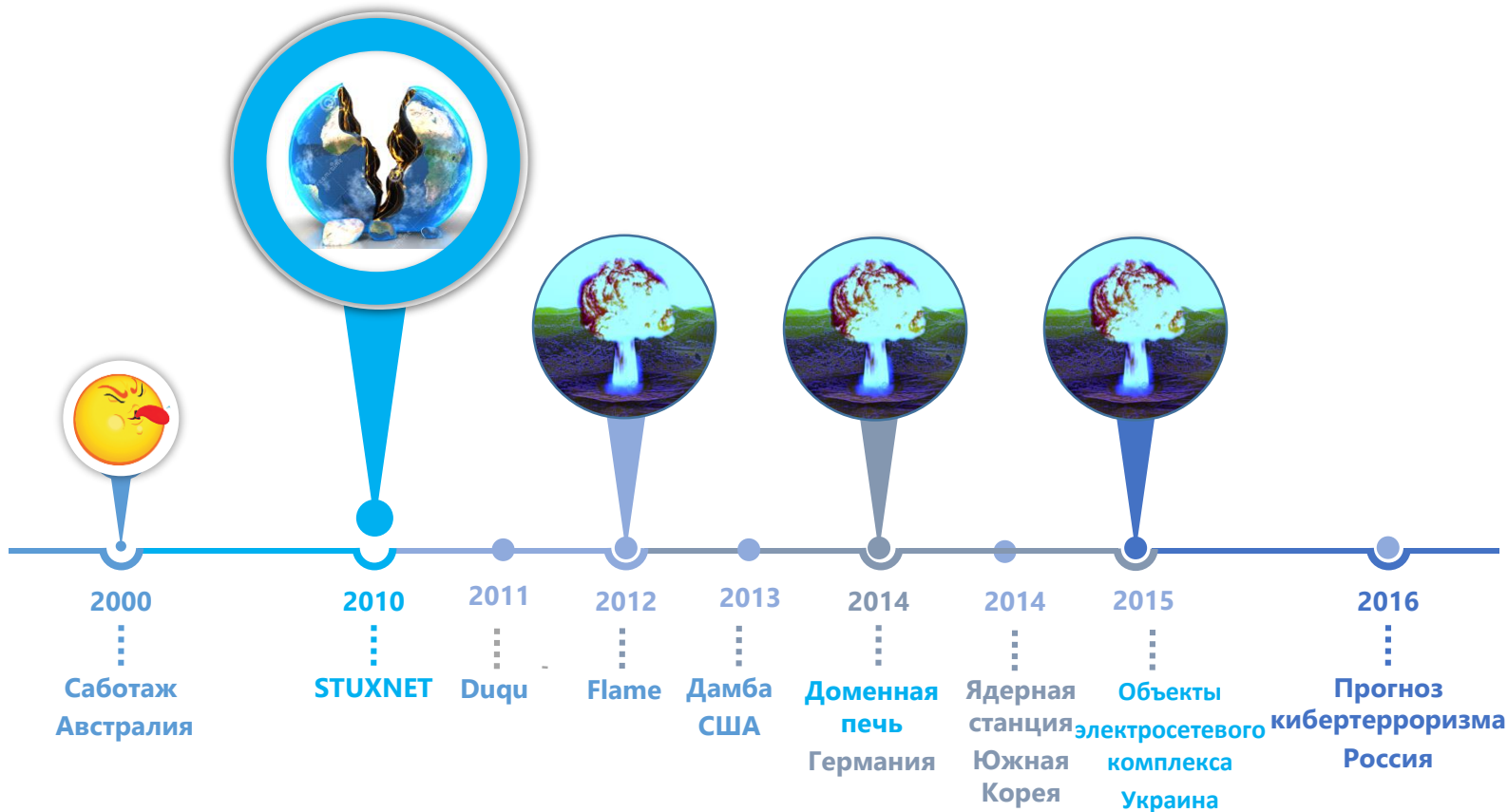


DECODING

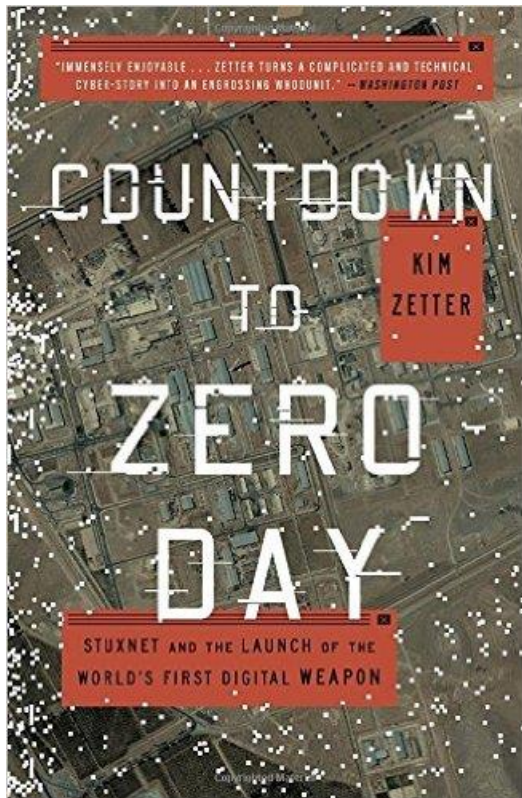
010101 3001 R0H 010



Мир до и после Stuxnet



Десятилетие со Stuxnet



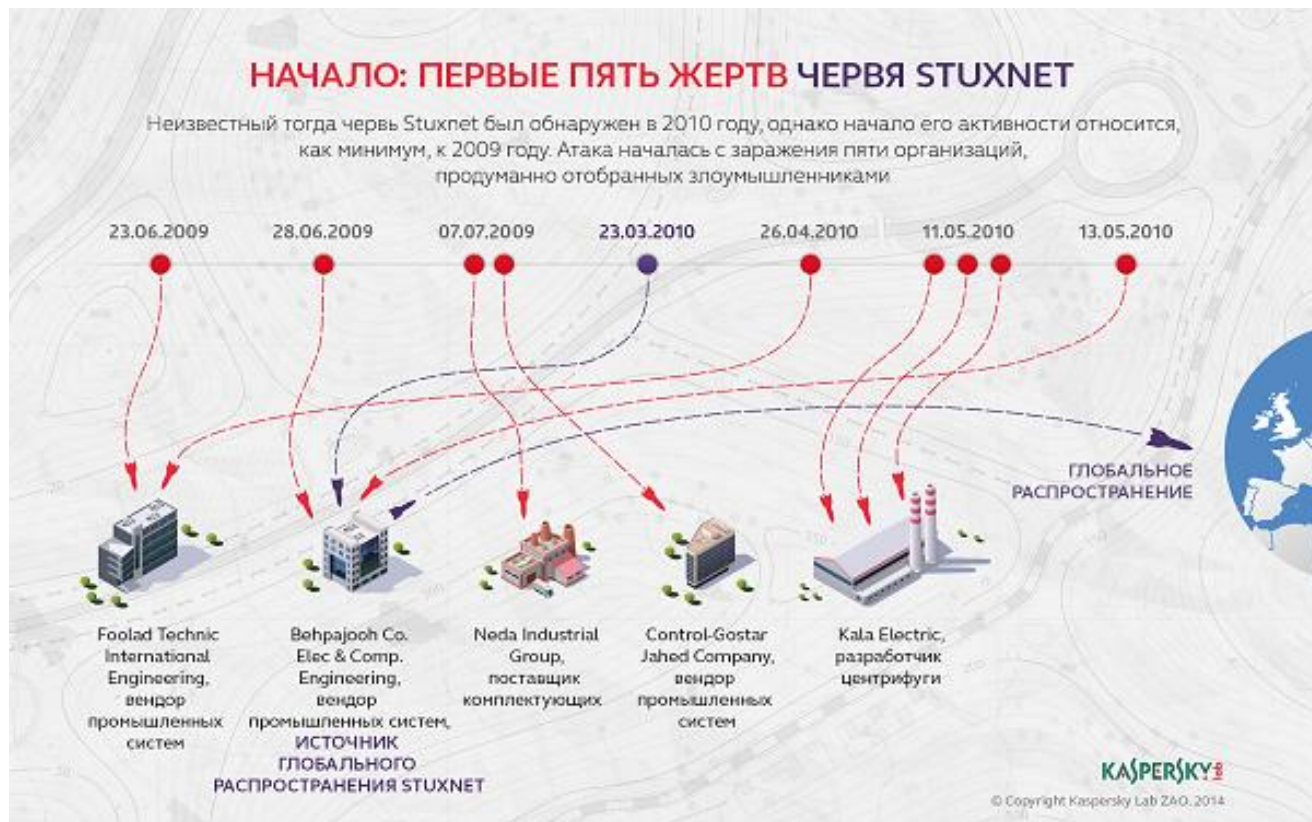
«Обратный отсчет» — это удачная попытка подняться выше строчек кода, свести воедино все, что известно о первой и по сей день наиболее масштабной специализированной атаке на промышленные системы.

<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/>

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



Последователи Stuxnet: Duqu и Flame



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>

База данных инцидентов содержит около 270 записей.

RISI
The Database About Contact

Nimda Impact on Manufac			
Software Manufacturing C			
Former System Administra			
Accidental Remote Contro			
Trojan Found on SCADA S			
Malware Shuts Down Millir			
Single PLC Lost For Unkn			
Steel plant infected with C			
Steel Plant infection with A			
11 Ethernet PLCs Fail At Or			
Blaster Impacts HMI Statio			
German Steel Mill Cyber A			
Software Bug Blamed in R			
Computer Virus Strikes Tw			
Computer Glitch Causes Rorer Coaster malfunction	2012	Other	United States
Industrial Control System Hacked Using Backdoor Posted Online	2012	Other	United States

German Steel Mill Cyber Attack

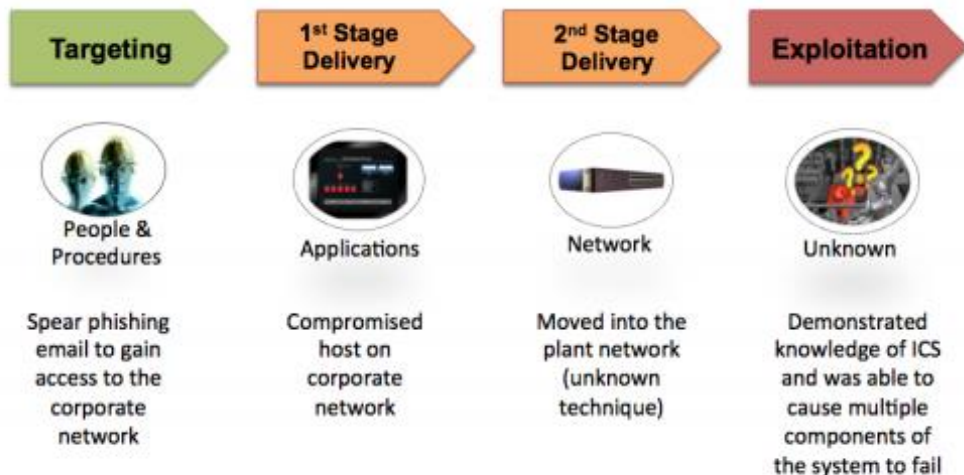
📅 Event Year:	2014	📄 Reliability:	Confirmed
📍 Country:	Germany		
🏭 Industry Type:	Metals		
📖 Description:	<p>Multiple attackers used an advanced social engineering attack to gain access to the company network and then worked their way onto the control system network. This resulted in an incident where a furnace could not be shut down in the regular way and the furnace was in an undefined condition which resulted in massive damage to the whole system."</p>		
👉 Impact:	<p>A furnace could not be shut down in the regular way and the furnace was in an undefined condition which resulted in massive damage to the whole system."</p>		

<http://www.risidata.com/Database>

Атакован металлургический завод в Германии 2014



Exploited Vulnerabilities by ICS Component German Steel Mill Incident



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

Киберинцидент в Энергосистеме Украины

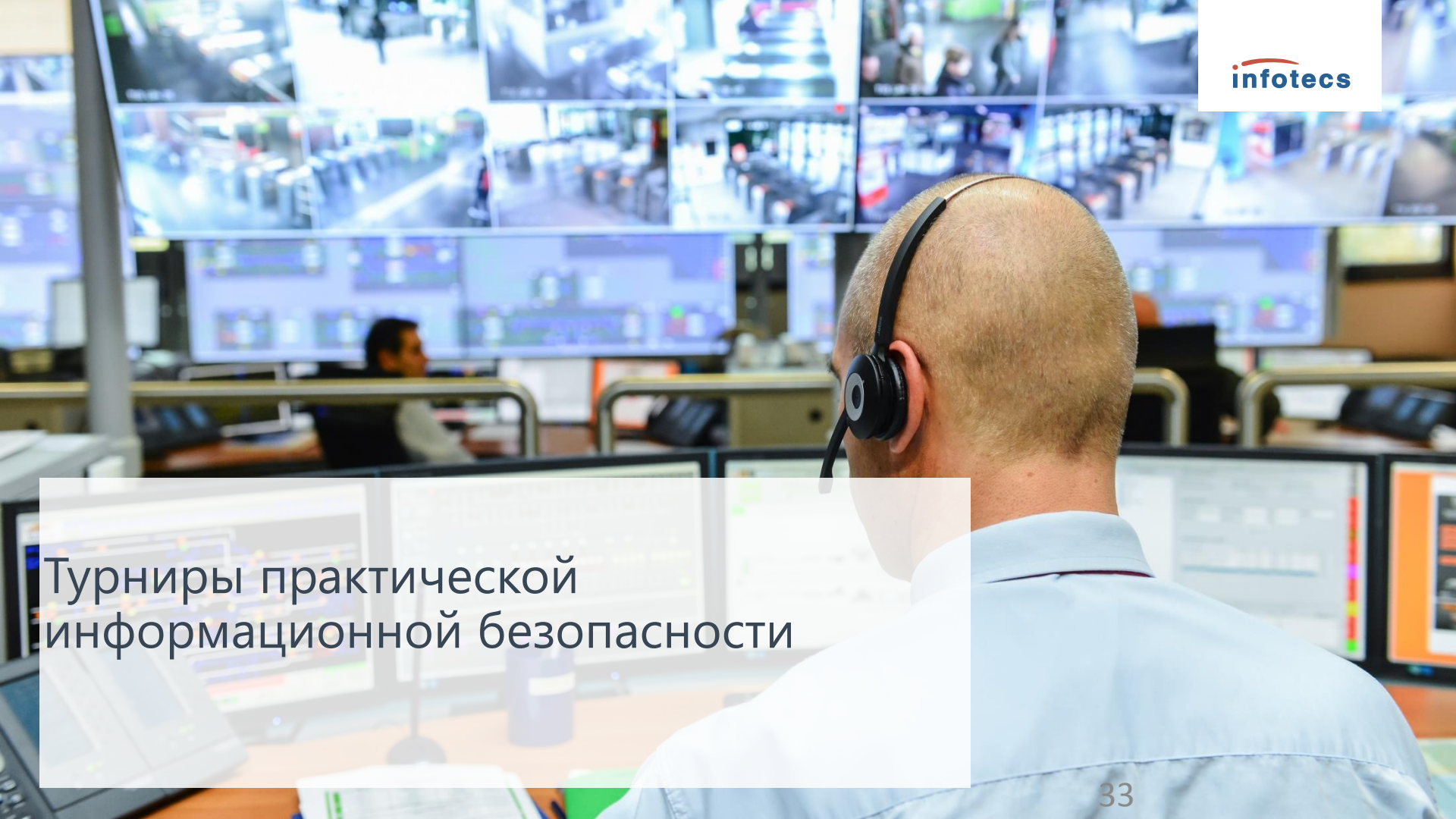


TLP: White

Analysis of the Cyber Attack on the Ukrainian Power Grid

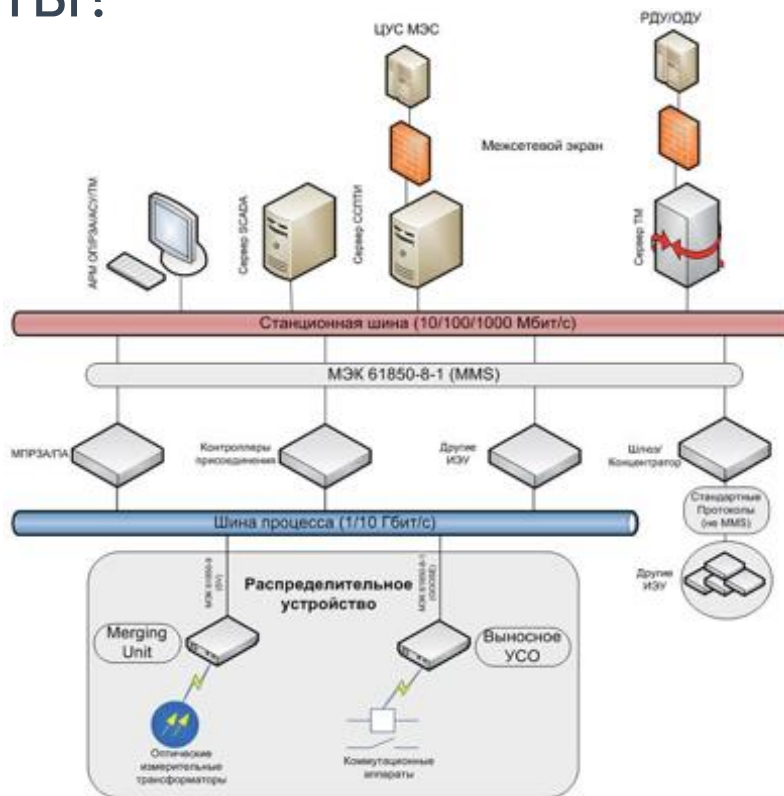
Defense Use Case

March 18, 2016

The background of the slide is a photograph of a security operations center. In the foreground, a man with a shaved head is seen from the back, wearing a light blue shirt and a black headset with a microphone. He is looking at several computer monitors. In the background, other staff members are visible at their workstations, and a large wall of monitors displays various security camera feeds and data dashboards.

Турниры практической информационной безопасности

«Цифровая подстанция» Объект защиты?

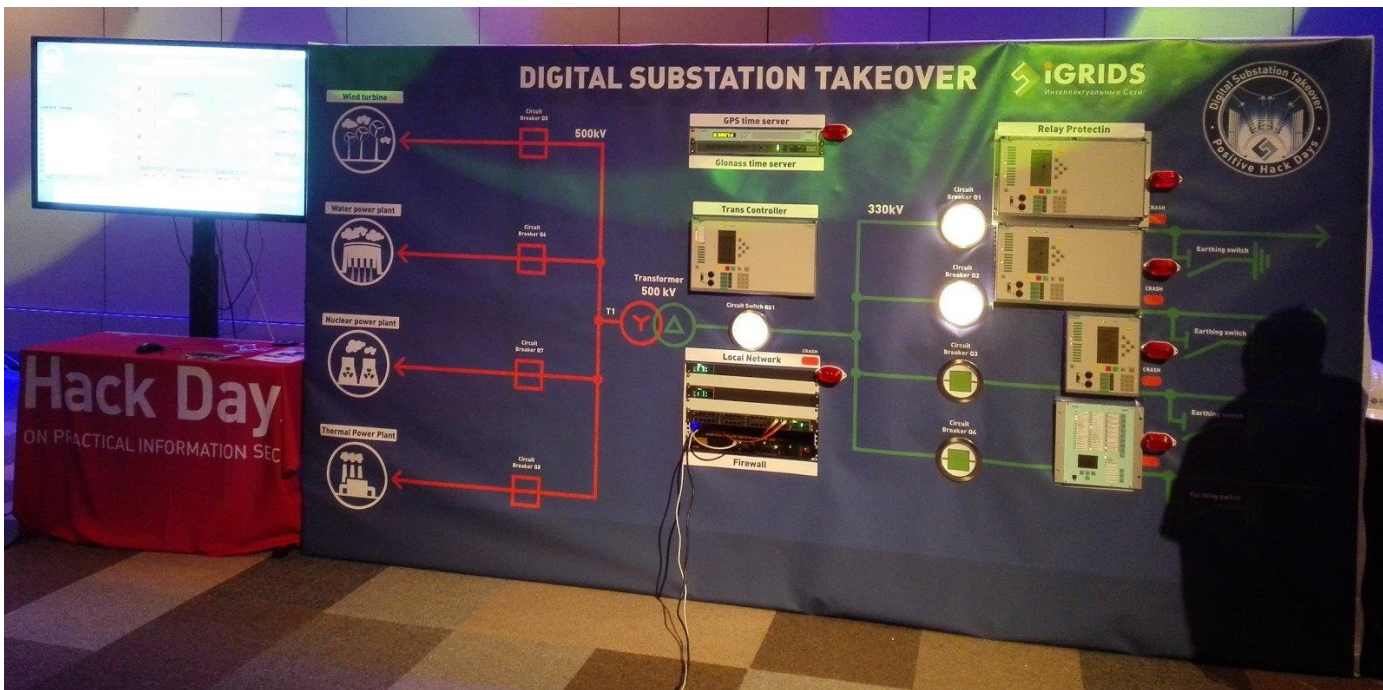


Конкурсы по практической безопасности



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

PHDaysV Цифровая подстанция



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

PHDaysVI:Standoff



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

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



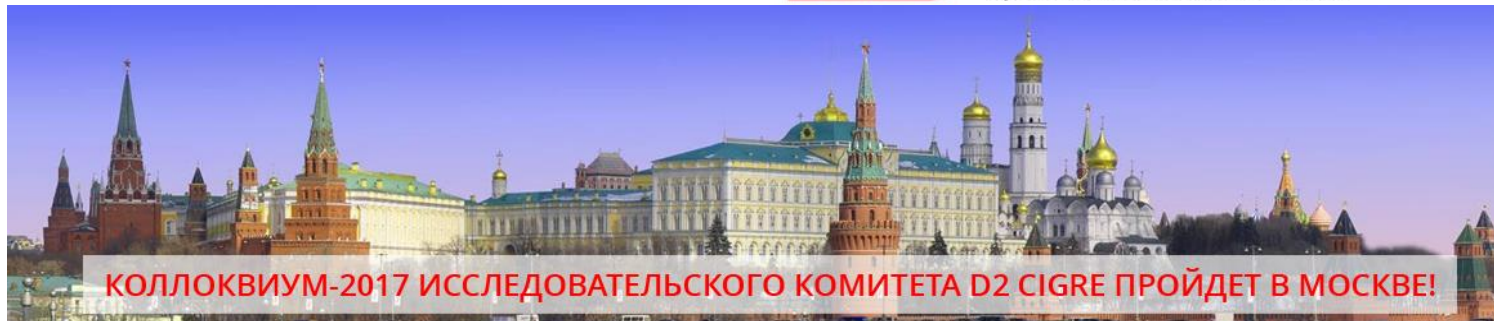
Киберфизическая модель Micro Grid



Исследователи за работой

The background of the slide is a photograph of a control room. In the foreground, the back of a man's head and shoulders are visible. He is wearing a light blue button-down shirt and a black headset with a microphone. He is looking at several computer monitors. The monitors display various data, including what appears to be a network diagram or map on the left and other technical information on the right. In the background, another person is seated at a desk, also working at a computer. The room is filled with rows of desks and monitors, suggesting a large-scale operations center.

РНК СИГРЭ



Устойчивость к киберугрозам информационных и телекоммуникационных систем в электроэнергетике.

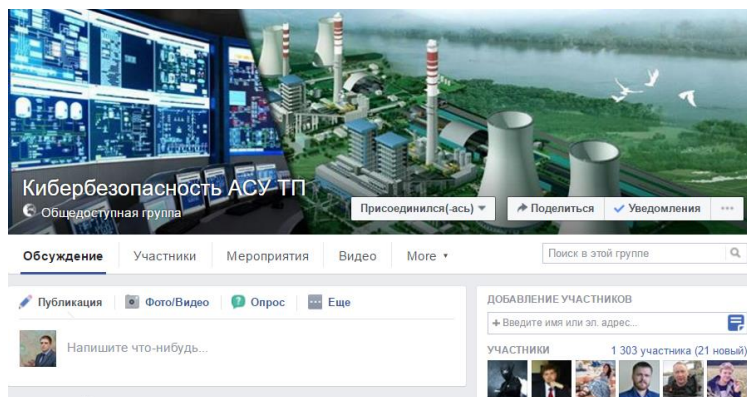
- Безопасность систем управления распределенной генерацией (DER).
- Облачные вычисления и технологии IoT: границы применения с точки зрения информационной безопасности.
- Сертификация информационных систем и телекоммуникаций на устойчивость к киберугрозам.
- Инструменты моделирования угроз и мер информационной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

Работа экспертных групп

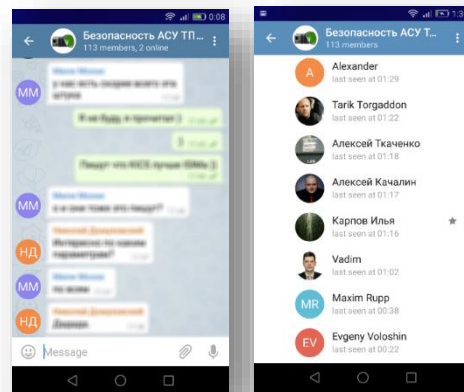


- Проблемная рабочая группы «Кибербезопасность РЗА и систем управления современных объектов электроэнергетики» (ПРГ-2 D2/B5);
- Рабочая группа «Обеспечение информационной безопасности для систем связи и управления в электроэнергетике» подкомитета D2 «Информационные системы и телекоммуникации»;
- Молодежная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

Профессиональные сообщества в социальных сетях



facebook.com/groups/RusCyberSec



telegram.me/RuScadaSec

