ОСОБЕННОСТИ И СРЕДСТВА ОБЕСПЕЧЕНИЯ КИБЕРЗАЩИТЫ АСУ ТП

Андрей Духвалов,
Руководитель Департамента Перспективных Технологий

Infosecurity
Москва, 20 Сент 2016

Проникновение цифровых технологий в реальный мир

АСУ ТП

Индустриальный интернет вещей

Цифровой мир

Information **T**echnology

Физический мир

Operational **T**echnology

KASPERSKY lab

Начало

КОГДА: 2010

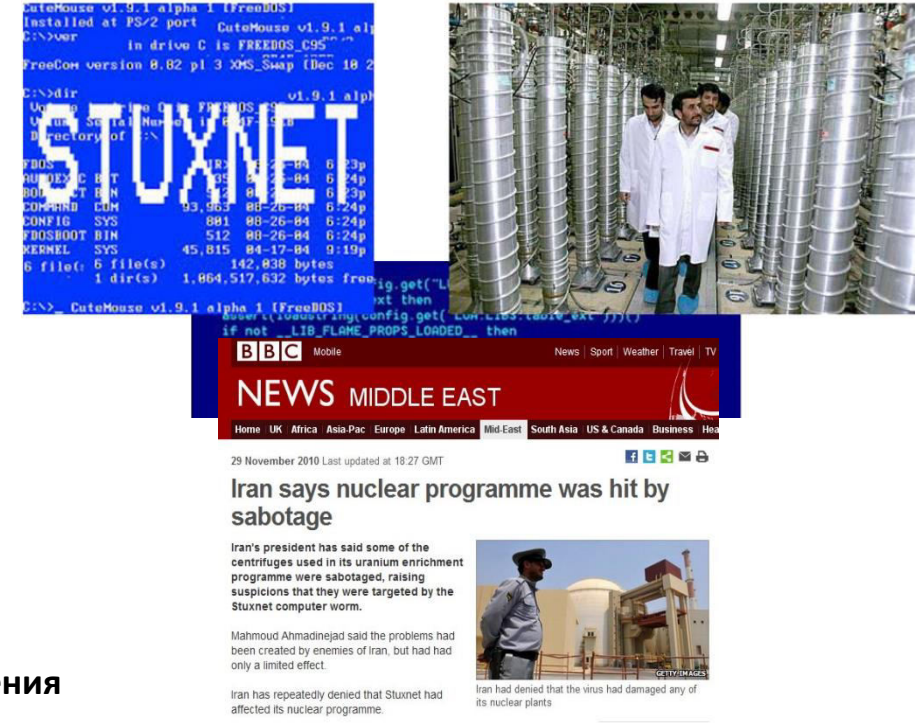
ГДЕ: Иран, Натанц

КИБЕР:

- инфицированные USB-устройства
- Уязвимости в MS Windows
- АСУ ТП пакет Win CC инфицирован
- S7 ПЛК микропрограмма изменена

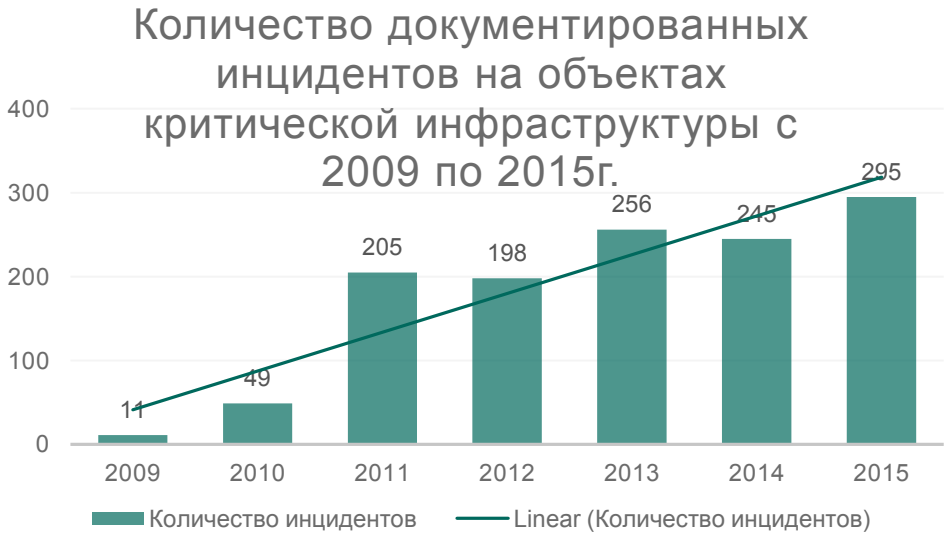
ФИЗИЧЕСКИЙ:

- нарушение технологического процесса
- жизненный цикл центрифуги для обогащения урана значительно сокращен
- поломки оборудования



https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

Состояние информационной безопасности в мире промышленной автоматизации



	2014		2015	
Всего инцидентов	**245**	100%	**295**	100%
Critical manufacturing	27	11%	97	33%
Energy	32	13%	46	16%
Water	6	2%	25	8%
Government facility	5	2%	18	6%
Transportation	5	2%	23	8%
Chemical	2	1%	7	2%
Nuclear	2	1%	7	2%

По данным US ICS-CERT.

KASPERSKY lab

Целевая атака на немецкий сталеплавильный завод.

КОГДА: декабрь 2014

ГДЕ: Германия

КИБЕР:

- **фишинговая email-атака для получения доступа**
- **инфицированный компьютер в корпоративной сети**
- **проникновение в сеть АСУ ТП**
- **множественные отказы комопонентов АСУ ТП**

ФИЗИЧЕСКИЙ:

- **множественные отказы привели к прекращению нормального функционирования всего техпроцесса**
- **доменную печь невозможно было остановить в штатном режиме что привело к физическому выходу из строя всей системы**

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile%20

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

Целевая атака на электросети Украины

КОГДА: декабрь 2015

ГДЕ: Украина, 3 области


12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

КИБЕР:

- **один из управляющих компьютеров заражет BalckEnergy2 посредством фишинговой email-атаки**
- **резервные источники питания (UPS) атакованы**
- **RTU микропрограмма изменена**
- **средства удаленного управления уничтожены**
- **DDoS-атака на центры телефонной поддержки**

ФИЗИЧЕСКИЙ:

- **секционные выключатели удаленно управлялись злоумышленниками**
- **удаленное управление было заблокировано для легитимных операторов**
- **отключение электричества на 7-и 110 кВ и 23-х 35 кВ подстанциях**
- **3 области, более 225 000 потребителей осталось без электричества более чем на 6 часов.**

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Инциденты зарегистрированные за последние полгода

Hackers shut down power grid in Ukraine

It's thought to be the first cyber attack to cause a blackout.

Malware is no longer reserved for the millions of consumer PCs all over the world -- it's now used in corporate espionage, as tool to disrupt the infrastructure of entire countries. It's been revealed that just on December 23rd, attackers were successfully able to infect computers belonging to the Ukrainian national grid, which resulted in hundreds of homes in the Ivano-Frankivsk region going dark. It's thought to be the first cyber attack to result in a power outage.

DEC 2015

JAN 2016

Wed Apr 27, 2016 9:02am EDT
Related: TECH, GERMANY

German nuclear plant infected with computer viruses, operator says

FRANKFURT | BY CHRISTOPH STEITZ AND ERIC AUCHARD

FEB 2016

IRONGATE ICS MALWARE STEALS FROM STUXNET PLAYBOOK

by Tom Spring June 2, 2016 , 8:45 am

New malware that targets industrial control systems called Irongate was found by researchers who say the discovery should serve as another wakeup call to the security industry to shore up its detection capabilities around ICS and SCADA threats. Irongate, which shares some of the same attributes as the lethal Stuxnet malware, was found by researchers at FireEye Labs Advanced Reverse Engineering which published its findings today.

APRIL 2016

MAY 2016

S. Korea accuses North of hacking railway systems and officials' phones

Published time: 8 Mar, 2016 07:31
Edited time: 8 Mar, 2016 08:17

Get short URL

533

South Korea's National Intelligence Service has accused Pyongyang of attempting to hack into railway control systems and wiretap officials' smartphones as tensions continue to mount on the peninsula.

The National Intelligence Service (NIS) said in a press release on Tuesday that North Korean hackers penetrated the smartphones of dozens of senior South Korean officials, stealing text and voice messages, Yonhap news agency reported.

MAR 2016

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWA

Security

Michigan electricity utility downed by ransomware attack

Don't click on the links, don't click on the links, don't …

3 May 2016 at 01:40, Richard Chirgwin 64 530

A water and electricity authority in the US State of Michigan has needed a week to recover from a ransomware attack that fortunately only hit its enterprise systems.

PLC-Blaster: A Worm Living Solely in the PLC

Ralf Spenneberg, Maik Brüggemann, Hendrik Schwartke

[1]OpenSource Security Ralf Spenneberg

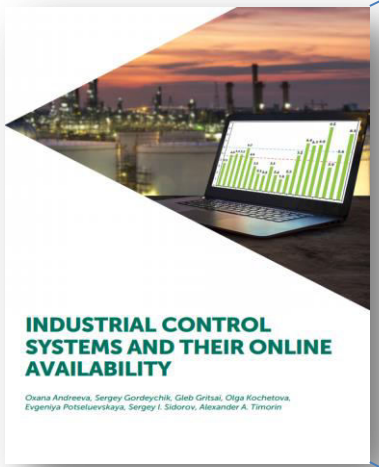
info@os-s.de

Abstract. Industrial processes are controlled by programmable logic controllers (PLC). Many PLCs sold today are equipped with Ethernet ports and can communicate using IP. Based on the Siemens SIMATIC S7-1200 we will demonstrate a worm. This worm does not require any additional PCs to proliferate. The worm lives and runs only on the PLC. The worm scans the network for new targets (PLCs), attacks these targets and replicates itself onto the found targets. The

KASPERSKY lab

Состояние информационной безопасности в мире промышленной автоматизации

92% подключенных к Интернету компонентов АСУ ТП подвержены удаленным атакам



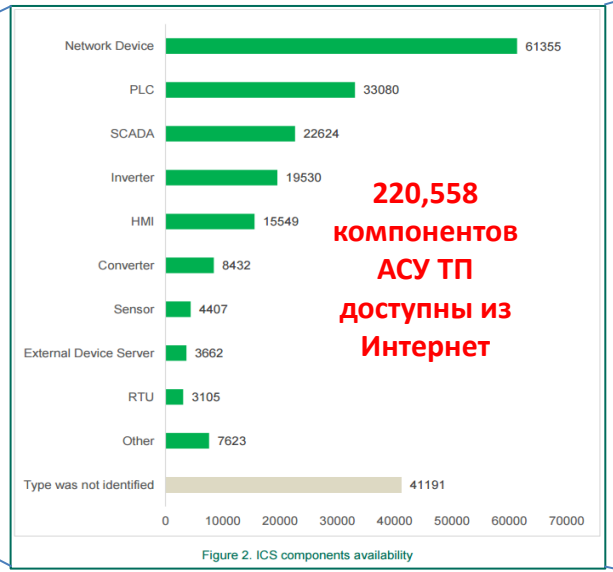


Figure 2. ICS components availability

Figure 5. ICS availability by country (Top-20)

11.07.2016 Лаборатория Касперского опубликовала отчет

http://www.kaspersky.ru/about/news/virus/2016/ics-vulnerabilities

KASPERSKY lab

Атака на модель цифровой подстанции

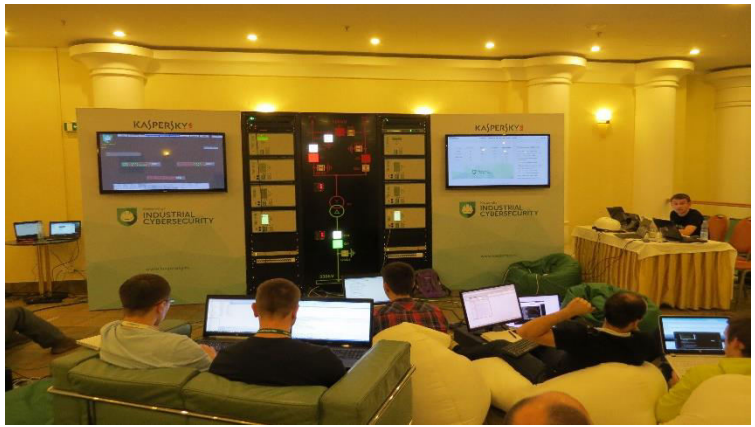
В октябре 2015 года Лаборатория Касперского в рамках своей конференции, посвященной информационной безопасности АСУ ТП провела соревнования среди команд, специализирующихся на поисках уязвимостей в информационных системах (CTF)

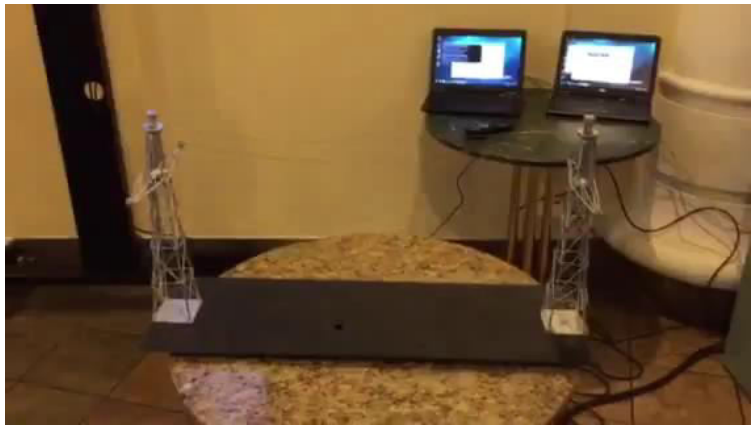
Стадии атаки:

- Перехват сетевого трафика
- Получение доступа к системе
- Отключение защитной автоматики (РЗА)
- Короткое замыкание на макете ЛЭП

Три из четырех команд-финалистов раелизовали аварийную ситуацию в первый день знакомства с объектом:

- Специалисты в области РЗА – за 3 часа
- Хакеры широкого профиля – за 5 часов





IT секьюрити в сравнении с АСУ ТП секьюрити

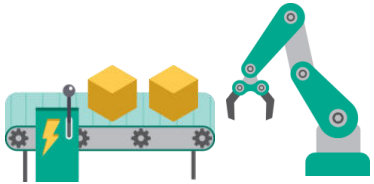
CIA – конфиденциальность

Другие цели и приоритеты

IAC – целостность и доступность

PC, SERVER, MOBILE

Другие объекты защиты



ПЛК, HMI, SCADA, …

IT директор

IT Security

Другие заказчики

Гл.инженер

СБ

СТРУКТУРНАЯ МОДЕЛЬ ПРЕДПРИЯТИЯ – ISA-95

LEVEL 4

Business planning and logistics

Managing end-to-end supply chain. Establishing the basic plant schedule – production, material use, delivery, and shipping.

LEVEL 3

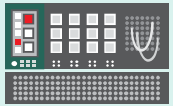
Manufacturing Operations management

Work flow/recipe control to produce the desired end products. Maintaining records and optimizing the production process.

LEVEL 2, 1

Batch Control.
Continuous Control.
Discrete Control.

Monitoring, supervisory control and automated control of the production process



Sensing the production process, manipulating the production process

LEVEL 0

Physical

Physical devices

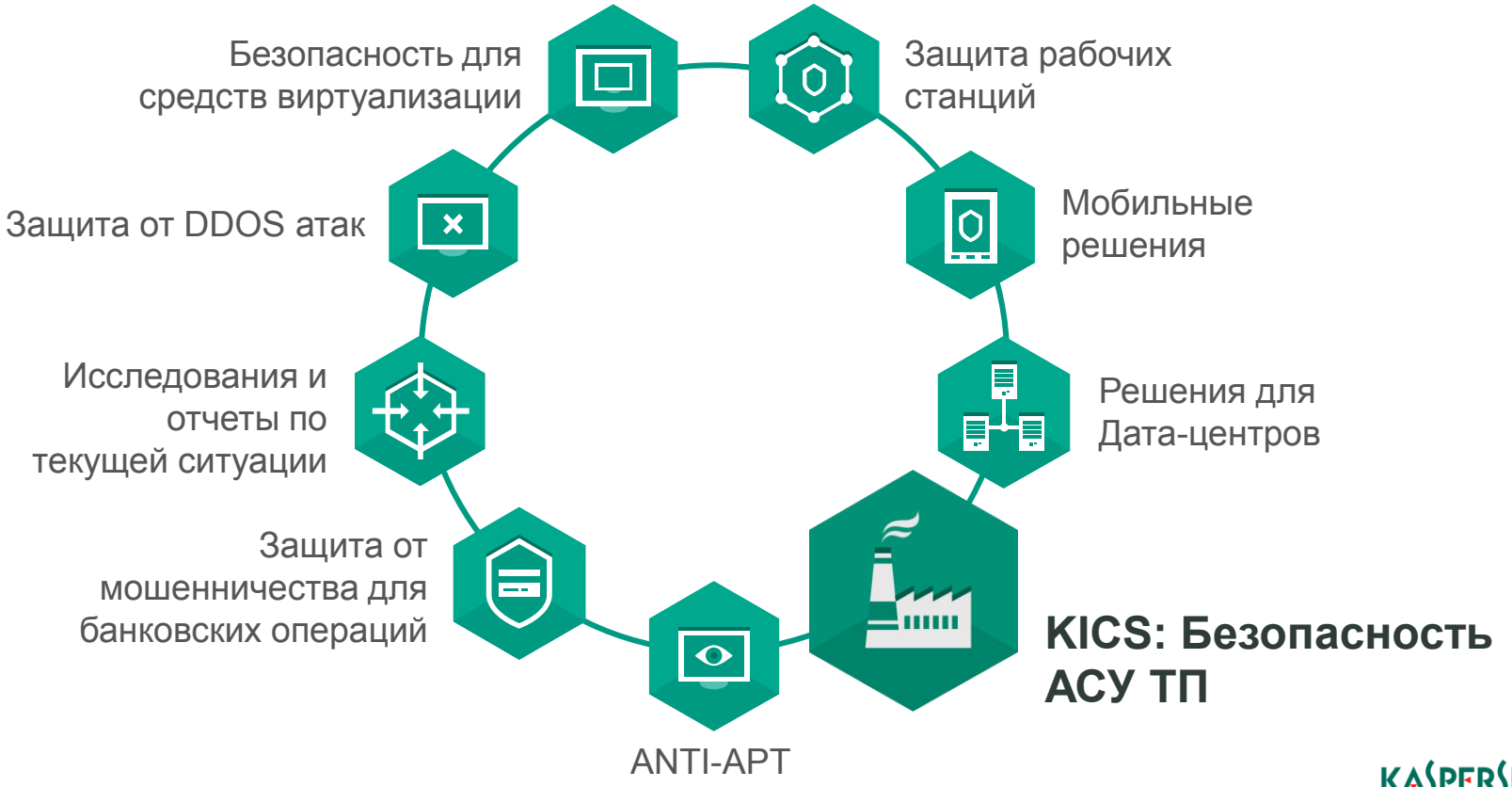
Kaspersky Security for Business + Professional Services

Kaspersky Industrial CyberSecurity

Physical security

KASPERSKY lab

КОМПЛЕКСНОЕ РЕШЕНИЕ ЛК ДЛЯ КОРПОРАЦИИ

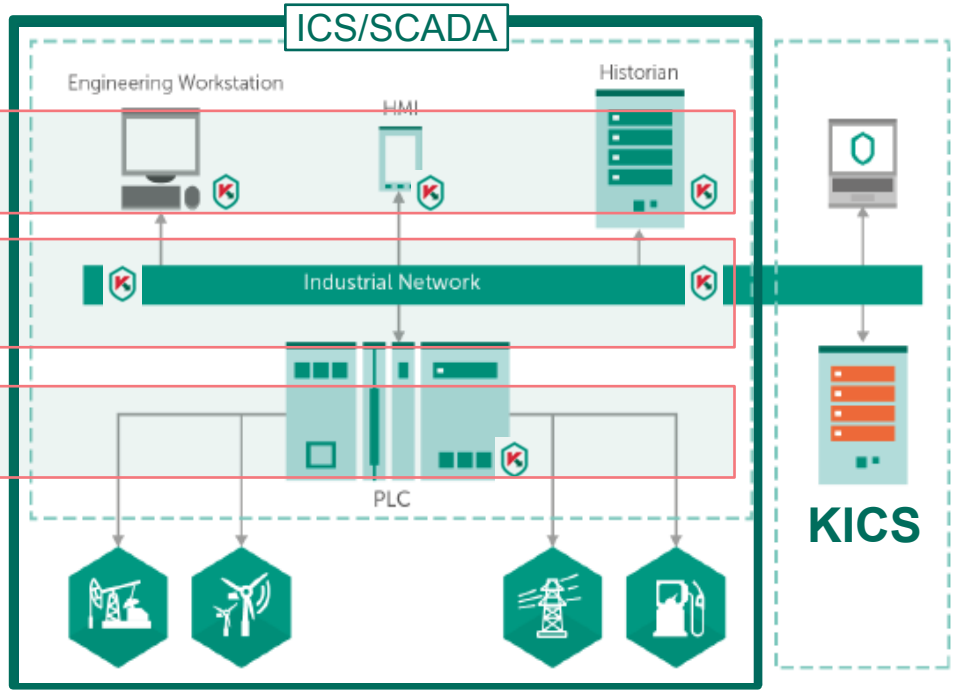


KICS: ПАССИВНЫЙ МНОГО-КОМПОНЕНТНЫЙ МОНИТОРИНГ

3 уровня защиты:

- Целостность среды (whitelisting)
- Целостность сетевых взаимодействий и мониторинг аномалий
- Целостность программ ПЛК

Основная цель – целостность и доступность



KICS – Kaspersky Industrial CyberSecurity

KASPERSKY lab

KICS: структура решения

БЕЗОПАСНОСТЬ - ЭТО ПРОЦЕСС, А НЕ ПРОЕКТ

ПРИМЕР ИСПОЛЬЗОВАНИЯ: ТАНЕКО, ТАТАРСТАН

Заказчик – ТАНЕКО

Объем переработки – 8,5 млн тонн сырой нефти в год

Новый завод, начало строительства – 2005 год

Уровень надежности для производства – 99,99%

СТОИМОСТЬ НЕЗАПЛАНИРОВАННОГО ПРОСТОЯ – 250.000$ в час

Внедрение KICS – декабрь 2015 года

Этапы: обследование, модель угроз, анализ рисков, пилотный объект (линия разгрузки тяжелого газойля), внедрение

Результаты за первые три месяца эксплуатации

- **Попытка неавторизованного доступа к сети АСУ ТП**
- **Попытка проведения регламентных работ с использованием несоответсвующей версии SCADA проекта**
- **Ненамеренное изменение инженерного диапазона PID-регулятора**

KASPERSKY lab

Спасибо за внимание

В современных условиях, ответсвенные технологические процессы должны иметь надежную киберзащиту

Андрей Духвалов

Руководитель Департамента Перспективных технологий

Andrey.Doukhvalov@kaspersky.com

KASPERSKY lab

infosecurity RUSSIA

20–22 Сентября 2016
КРОКУС ЭКСПО, МОСКВА