



# Industrial Cybersecurity

Opportunities and challenges  
in Digital Transformation



## MAXIM NIKANDROV

iGrids  
Russia

- CEO of iGrids, a software company in energy industry
- Expert in the field of power management systems and industrial cybersecurity
- Head of the WG 2 of Russian National Committee of CIGRE on D2 / B5 "Cybersecurity of protection and automation devices and control systems for modern electric power facilities"

[linkedin.com/in/nikandrov-maxim-8236b280/](https://www.linkedin.com/in/nikandrov-maxim-8236b280/)



# The center for approbation Industrial Cyber Security solutions on the technological process models



Maxim Nakandrov






Ph.D., iGrids company director  
iGrids LTD

**iGrids**  
интеллектуальные сети

# Economy digitalization

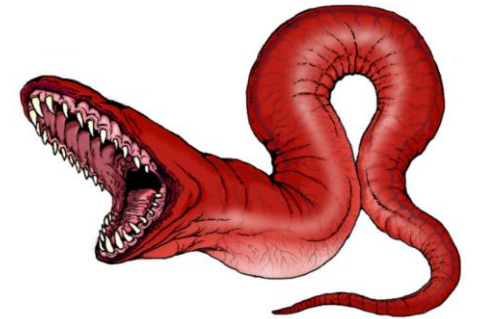


# APCS cybersecurity complexes

<b>Kaspersky Security for Business</b>		<p>Управление закупками материалов и отгрузками продукции, управленческо-учетное планирование, планирование ремонтов, формирование спецификаций, бухгалтерия</p>	<p>Уровень 4 ERP</p>
<b>Kaspersky Industrial Cyber Security (KICS)</b>		<p>Оперативное планирование, управление рецептами, APC, составление графика смен, отслеживание заказов, анализ производительности, управление техобслуживанием</p>	<p>Уровень 3 MES</p>
<b>Kaspersky Industrial Cyber Security (KICS)</b>		<p>Диспетчерское (операторское) управление, архивация технологических данных, техническое обслуживание комплекса средств АСУ ТП</p>	<p>Уровень 2 Операторское управление</p>
<b>Kaspersky Industrial Cyber Security (KICS)</b>		<p>Управление технологическим процессом с помощью программируемых логических контроллеров + противоаварийная автоматическая защита</p>	<p>Уровень 1 ПЛК</p>
<b>Kaspersky Industrial Cyber Security (KICS)</b>		<p>Датчики и исполнительные механизмы</p>	<p>Уровень 0 Полевой</p>



# Effectiveness and toxicity of cybersecurity means



# Grounds for establishing a testing center

- **FSTEC Order No. 31 of March 14, 2014 "On Approval of Requirements for Security .... "**

paragraph 14.1. The recommendation to carry out checks using layouts or a test zone, the correct functioning of the automated control system with the protection and compatibility of selected information protection tools with software and hardware of the automated control system"

- **FSTEC Order No. 239 dated December 25, 2017 "On Approval of Requirements for Ensuring Security ..."**

paragraph 11.1. For the purposes of testing the security subsystem of a significant object during the design process, it may be modeled or a test environment created.

paragraph 12.6. It is allowed to conduct vulnerability analysis on a mock-up (in the test zone) of a significant object or mock-ups of individual segments of a significant object.



It is necessary to understand first of all the technological process itself.

# Activities of the testing center

1

Tests, certification,  
attestation



2

Designing and  
commissioning of IS  
complexes



3

IS training and consulting



4

Scientific research and R&D





# Vulnerability analysis and certification



ФСТЭК России  
Федеральная служба  
по техническому и  
экспортному контролю

Capturing from Подключение по локальной сети 2 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Filter: (((ip.src == 10.0.0.11) || (ip.src == 10.0.0.201))) && !(ip.dst == 234.5.6.7) Expression... Clear Apply Save ip\_hj TCP\_MMS\_HJ

No.	Time	Source	Destination	Protocol	Length	Info
387	293.025020	10.0.0.11	10.0.0.201	TCP	60	[TCP Keep-Alive ACK] iso-tsap > 4265 [ACK] Seq=219
388	295.009469	10.0.0.201	10.0.0.11	MMS	91	confirmed-RequestPDU
389	295.012394	10.0.0.11	10.0.0.201	MMS	141	confirmed-ResponsePDU
390	295.136231	10.0.0.201	10.0.0.11	TCP	60	4265 > iso-tsap [ACK] Seq=2221 Ack=5221 win=64
391	297.952582	10.0.0.201	10.0.0.11	TCP	60	[TCP Keep-Alive] 4265 > iso-tsap [ACK] Seq=222
392	297.953527	10.0.0.11	10.0.0.201	TCP	60	[TCP Keep-Alive ACK] iso-tsap > 4265 [ACK] Seq=222
393	300.010593	10.0.0.201	10.0.0.11	MMS	91	confirmed-RequestPDU
394	300.013531	10.0.0.11	10.0.0.201	MMS	141	confirmed-ResponsePDU
395	300.165880	10.0.0.201	10.0.0.11	TCP	60	4265 > iso-tsap [ACK] Seq=2258 Ack=5308 win=64
396	302.982376	10.0.0.201	10.0.0.11	TCP	60	[TCP Keep-Alive] 4265 > iso-tsap [ACK] Seq=225
397	302.984323	10.0.0.11	10.0.0.201	TCP	60	[TCP Keep-Alive ACK] iso-tsap > 4265 [ACK] Seq=225
400	305.006798	10.0.0.201	10.0.0.11	MMS	91	confirmed-RequestPDU
401	305.009745	10.0.0.11	10.0.0.201	MMS	141	confirmed-ResponsePDU
402	305.094536	10.0.0.11	10.0.0.11	TCP	60	4265 > iso-tsap [ACK] Seq=2295 Ack=5395 win=65
403	307.912293	10.0.0.201	10.0.0.11	TCP	60	[TCP Keep-Alive] 4265 > iso-tsap [ACK] Seq=229
404	307.912366	10.0.0.11	10.0.0.201	TCP	60	[TCP Keep-Alive ACK] iso-tsap > 4265 [ACK] Seq=229
405	310.008951	10.0.0.201	10.0.0.11	MMS	91	confirmed-RequestPDU
406	310.011861	10.0.0.11	10.0.0.201	MMS	141	confirmed-ResponsePDU
407	310.224801	10.0.0.201	10.0.0.11	TCP	60	4265 > iso-tsap [ACK] Seq=2332 Ack=5482 win=65
410	312.940362	10.0.0.201	10.0.0.11	TCP	60	[TCP Keep-Alive] 4265 > iso-tsap [ACK] Seq=233

Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0

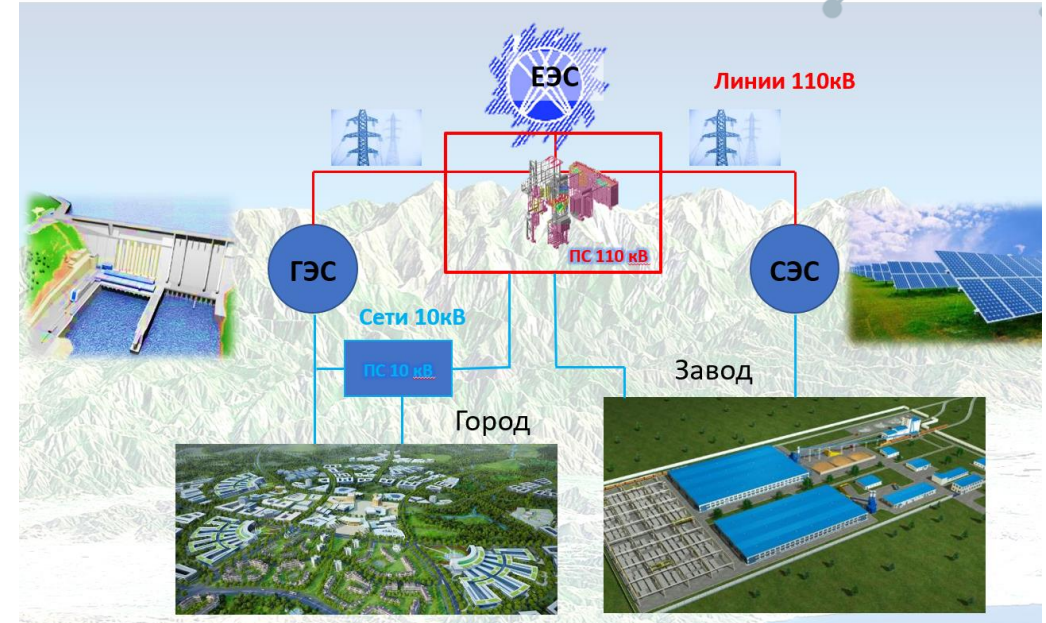
- Ethernet II, Src: QuantaCo\_88:48:2c (00:1b:24:88:48:2c), Dst: Ipcas\_fe:bb:ba (00:09:8e:fe:bb:ba)
- Internet Protocol Version 4, Src: 10.0.0.201 (10.0.0.201), Dst: 10.0.0.11 (10.0.0.11)
- Transmission Control Protocol, Src Port: 4265 (4265), Dst Port: iso-tsap (102), Seq: 1, Ack: 2336, Window: 65013, Length: 91, Options: (len=20) [MSS=576, SACK\_PERM=1, TSERIAL=2336, TSO=1, ECN=0, CWR=0, RST=0, SYN=1, URG=0]

Sequence number: 1 (relative sequence number)  
[Next sequence number: 38 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
Header length: 20 bytes  
Flags: 0x018 (PSH, ACK)  
window size value: 65013  
[Calculated window size: 65013]

```
0010 00 4d 08 29 40 00 80 06 dd ae 0a 00 00 c9 0a 00  .M.)@...
0020 00 0b 10 a9 00 66 b9 cf df 40 08 19 05 2f 50 18  ....fD.../P.
0030 fd f5 96 4f 00 00 05 00 00 23 02 f0 80 01 00 01  ...o.....%...
0040 00 61 18 30 16 02 01 03 a0 11 a0 0f 02 02 0a 1a  .a.o.....
0050 a1 09 a0 03 80 01 09 a1 02 80 00  .a.o.....
```

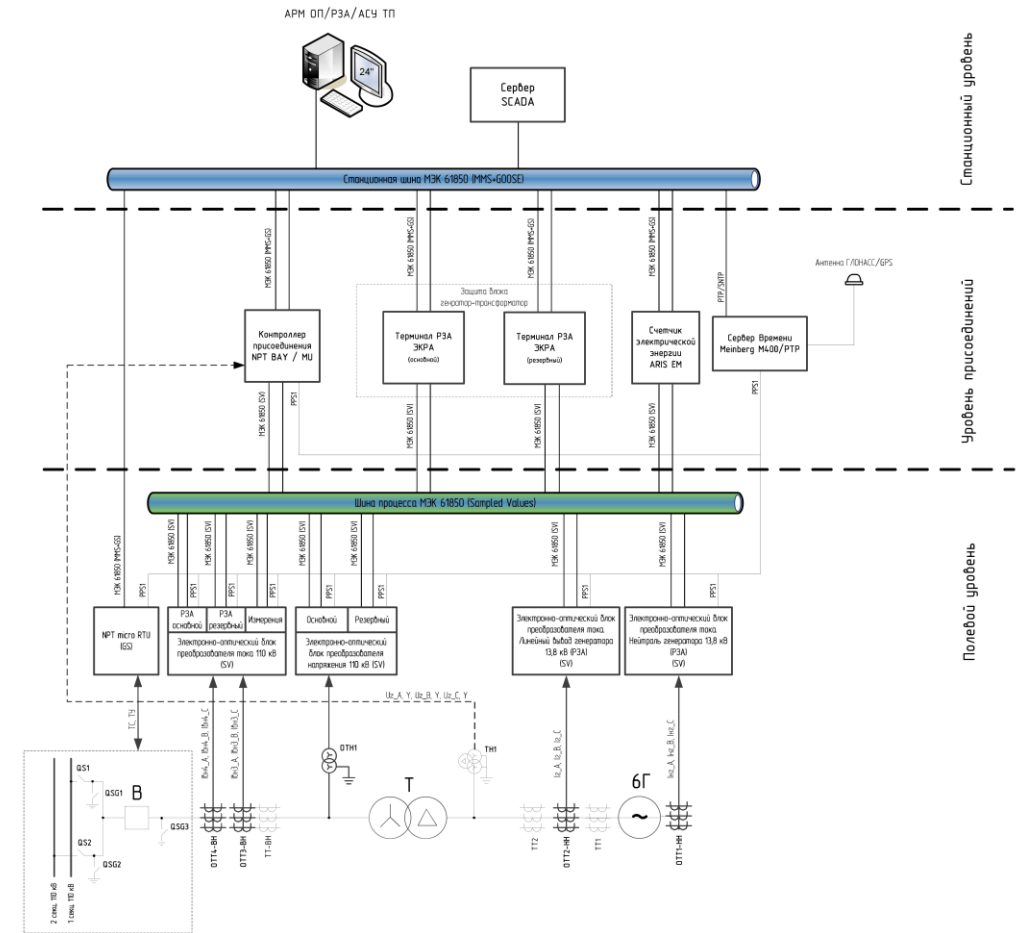
Administrators: tcp\_hj\_gen\_tools  
tcp\_hj\_gen\_tools\_for\_mms\_v...  
input sequence number and...  
Education use only  
...  
ack. HEX:0x39cfdf4d  
ack. HEX:0x0819052f\_

# Control systems modeling



- Consists of digital equipment of a typical modern substation or station
- It allows to simulate the technological process and fault modes in electric power systems

# Process simulation and testing the IS solution



Nizhny Novgorod hydroelectric power station. Before the installation of the IS complex, a full cycle of adjustment and testing was carried out on the object model.

# Specialized expert support of "GosSOPKA"

# ГОССОПКА

Обнаружение • Предупреждение • Ликвидация •

Specialized expert support of "GosSOPKA"



# World analogues :

## Idaho National Laboratory

### National Supervisory Control and Data Acquisition Test Bed



INL cyber researcher Jared Verba reviews circuit breaker settings on a power grid SCADA system.



**M**assive. Interconnected. Essential. These words describe the nation's critical energy infrastructures ranging from systems that light cities to networks that deliver oil and gas. Owned privately, but used publically, these complex, interdependent systems affect every person in each county, community, and parish in the country. And increasingly, the supervisory control and data acquisition (SCADA) systems that monitor and manage them are susceptible to malicious cyber attacks.

These attacks have been used to disrupt power equipment in regions outside the U.S. In at least one case, the disruption caused a power outage affecting multiple cities. Nation-states are also actively

At INL, full-scale, industry-provided SCADA systems undergo regular cyber analysis by experts widely recognized for securing control systems. The laboratory also conducts onsite assessments and training at electricity transmission, generation, and oil and natural gas facilities to better understand real-world installations and provide mitigation strategies to owners and operators. Assessments are backed up by immersive training courses that teach owners and operators about emerging cybersecurity techniques and malware trends.

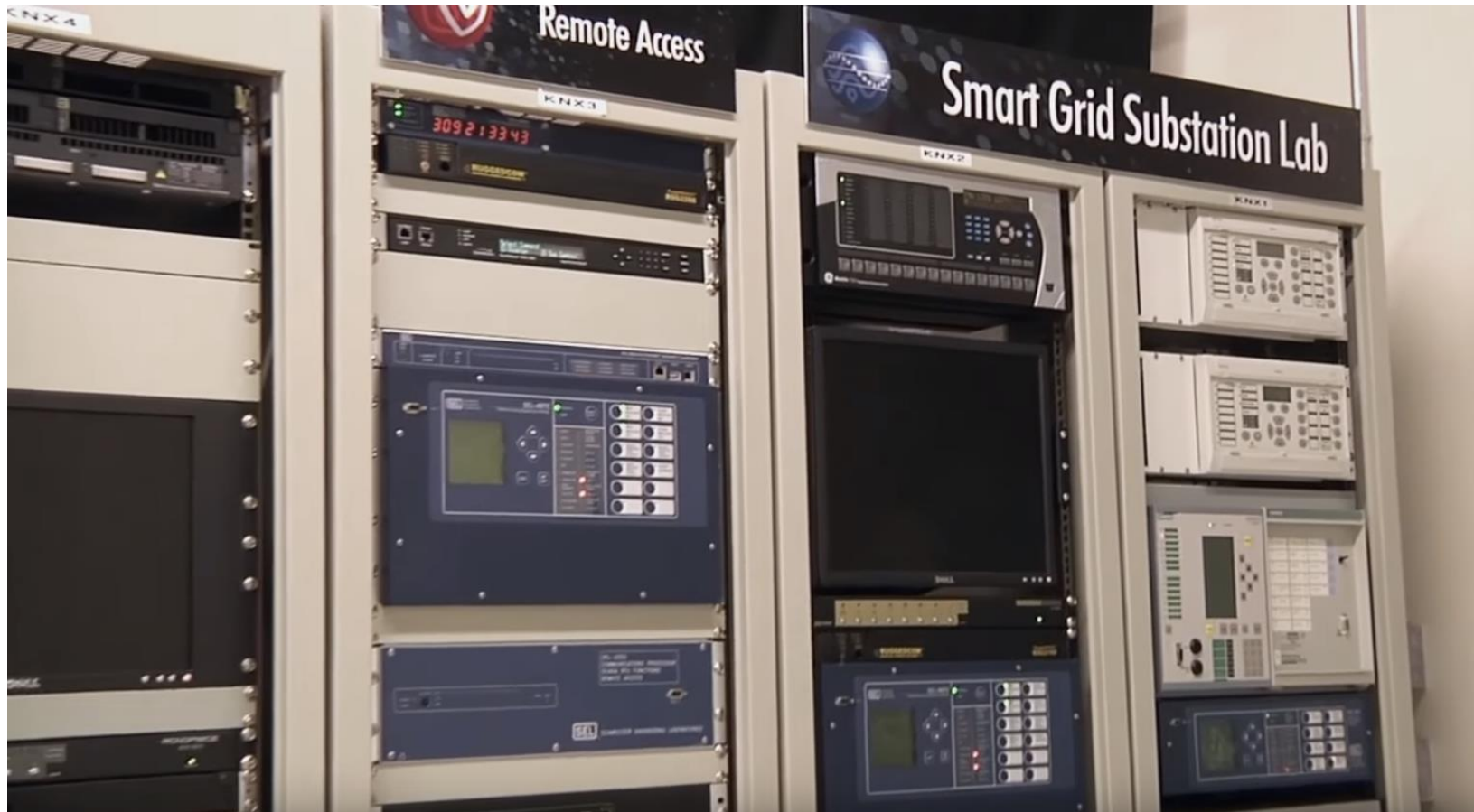
#### Quick Facts

- NSTB is a collaborative DOE initiative for securing SCADA and energy-related control devices.



# World analogues :

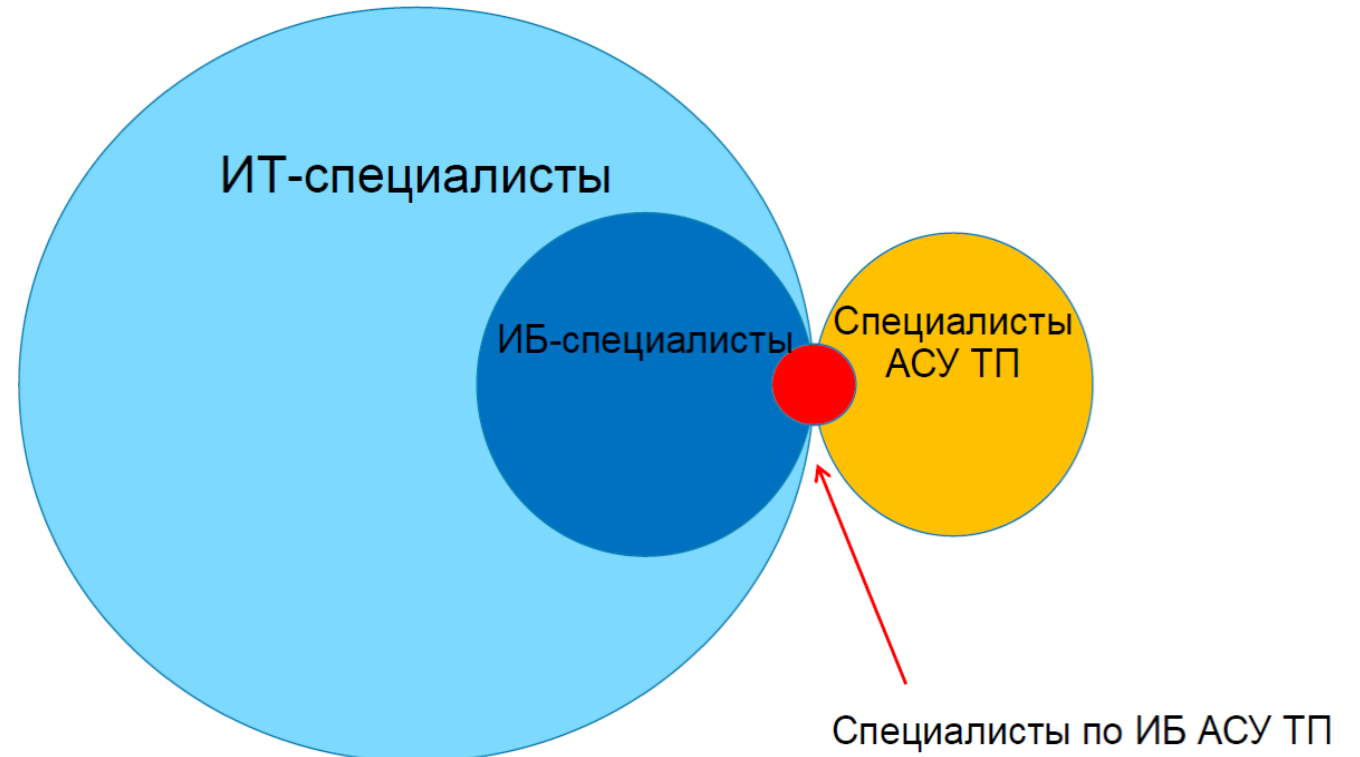
Electric Power Research Institute  
Cyber Security Research Laboratory



# Training and consulting



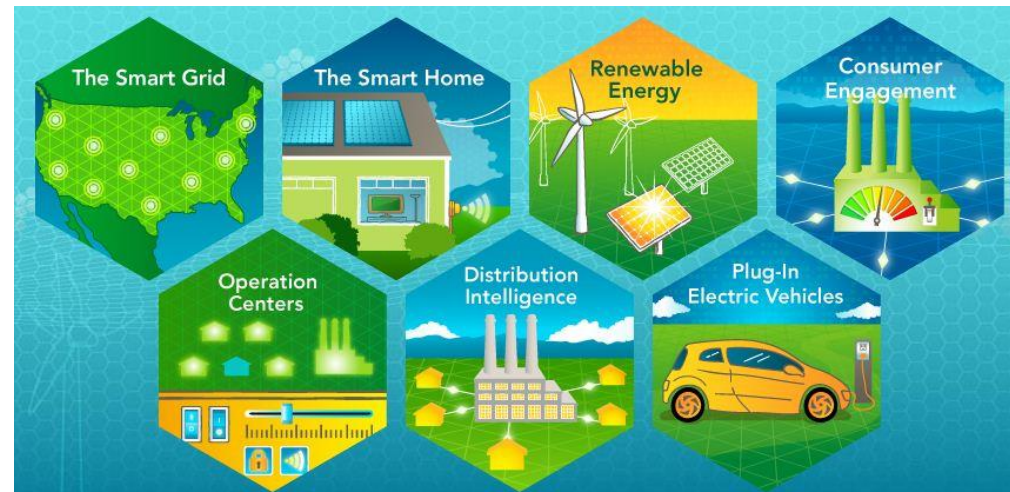
**Scientific and Technical Center  
Kaspersky Labs**  
Master's program and refresher courses



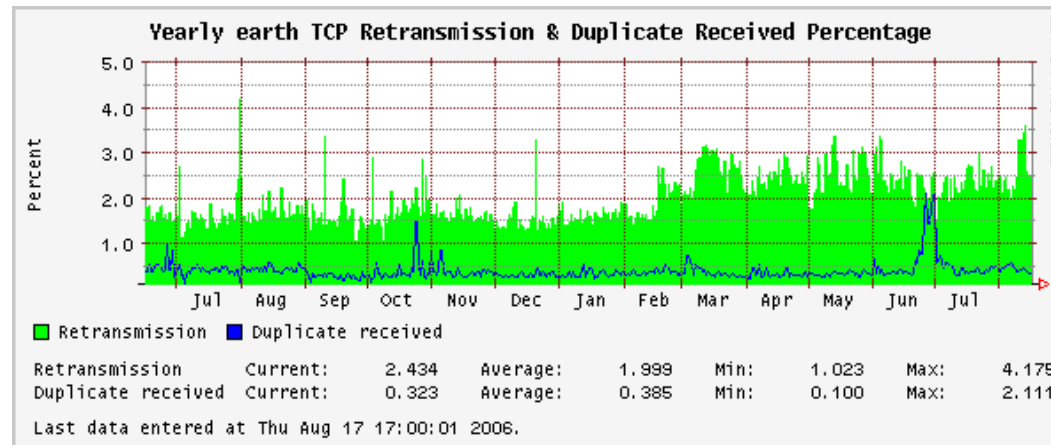
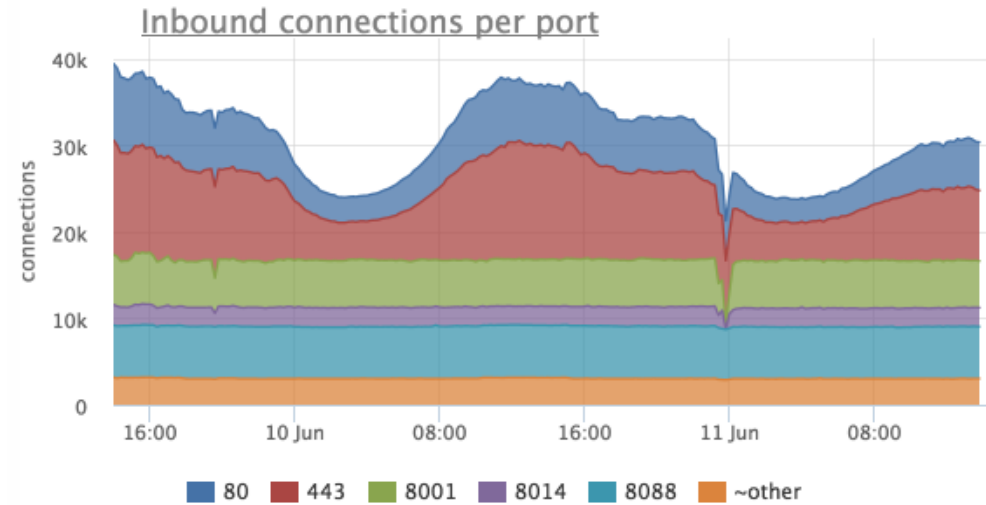
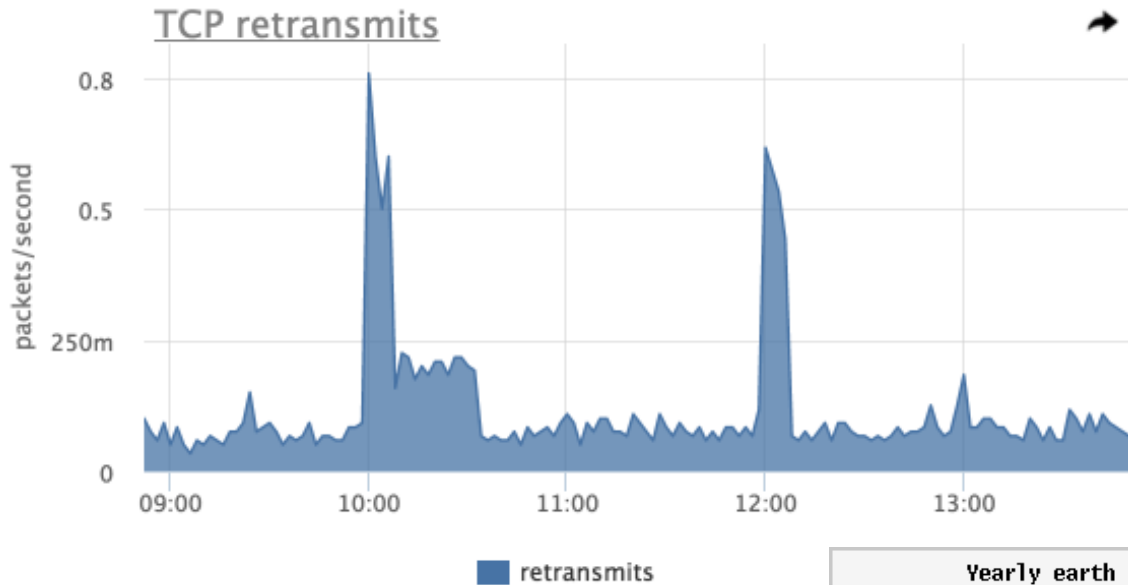


# Promising technology initiatives scope

- Digital Distribution Electrical Networks
- Microgride
- Smart metering, billing and consumption management
- Cloud services in the energy sector
- Digital substations
- Virtual stations



# Development and approbation of new cybersecurity technologies



# Conclusions

1. The implementation of the economy digital transformation program is not possible without addressing the issues of cybersecurity.
2. Before implementation on real objects testing and approbation on process models is mandatory.
3. The laboratory can become part of the State system for detection, prevention and elimination of the computer attacks consequences ("GosSOPKA").



**Thank you for attention!**



**Maxim Nakandrov**  
Ph.D., iGrids company director